JOURNAL OF ANALYSIS OF APPLIED MATHEMATICS

Volume 11, 2018

JOURNAL OF

ANALYSIS OF APPLIED MATHEMATICS

At AAM, we are passionate about mathematics education and devoted to motivating students to expand their knowledge of applied math through research.

JOURNAL OF

ANALYSIS OF APPLIED MATHEMATICS

The International Journal of Applied Mathematics for Secondary School Students.

AIM AND SCOPE

Analysis of Applied Mathematics (AAM) is a journal devoted to the publication of original research papers in applied mathematics for high (secondary) school students. Our mission is to promote academic curiosity in the field of mathematics by encouraging students to produce quality research. AAM provides a unique opportunity for high school students to publish a mathematics-based research article in a journal. The topics considered for publication can involve any aspect of applied mathematics including topics from the medical, scientific, engineering, finance and business fields. Examples of applied mathematics topics are:

- Electronics: televisions, computers, video games, smart phones, and modern appliances
- Transportation: Automobiles, air planes, space shuttles
- Systems and Processes: Traffic light systems, social choice theory, inventory systems, internet search engines, algorithm improvement

There are a number of possible applied mathematics papers that would qualify for the Analysis of Applied Mathematics. For more information, please visit us at analysisofappliedmathematics.org. If you have any questions about whether your topic is eligible for submission, please contact us at info@analysisofappliedmathematics.org.

Contents

Zandon: A Country Run Entirely on the Blockchain; Game Theory Analysis on the Universal Adoption and Non-Adoption of Blockchain Technology

By Jay Chiruvolu
Menlo School

1.0 Introduction/Purpose of the Research Paper

Statistics provided by the World Bank reveal the extent to which poverty grips our world today. In 2012, 900 million people around the world were impoverished, as dictated by the global poverty line (an income of less than $1.90 a day). While this number decreased to 700 million by 2015, this is still an astronomical number, approximately 10% of the world's population. There remain far more than 50 countries with over half of their population living in abject poverty, spread across several continents. Countries facing this issue will find it hard to develop, as they have no way to assist their citizens who remain in poverty.[1]

The purpose of this research paper is to investigate the possibility and effects of shifting a country's entire economic system onto a revolutionary new technology known as the blockchain. As a decentralized network, the blockchain offers a poor country a unique chance to globalize, efficiently run its internal affairs, and maintain a functional governance on its people. It could also offer this country a way to massively boost its economic power in the world. Therefore, this study expects to confirm a hypothesis that if a poverty-stricken country adopts the blockchain to run its economic system, its socioeconomic status could improve dramatically.

This paper will explore the implications for that country's socioeconomic growth, trade, GDP, and the standard of living for its people. Any country that adopts the blockchain as the medium for running all its economic activities experiences a multitude of opportunities to advance its economy. There is also likely an attractive first-mover advantage for such a country, and it could entice its peers to follow suit.[2] This possibility is further explored by the application of game theory to better understand how other nations can benefit from the same blockchain technology.[3]

2.0 Literature Review

Highlighted below are related literature analyses that go along with the subject matter discussed in this research.

2.1 A Digital Society

Estonia is referred to as a digital or virtual society because it has almost completely moved all its economic, socio-political, educational, and developmental activities to the internet.[3,4] This entails that the entire country, irrespective of its size, is being run on the internet, from citizen registry to setting up business endeavors. What better way to improve this online jurisdiction (internet-based nation) than the introduction of a fully decentralized network such as the blockchain?[5]

The growth of blockchain technology further liberalizes the procedures for running a country online. In a more technical parlance, the introduction of the blockchain makes it possible for effortless management of every section of a country's operations, from its national economic agendas, healthcare system, social and political processes, educational, and industrial development.

2.2 The Game Theory

Generally, the game theory approach is a mathematical model or a set of mathematical models that analyzes the conflict and resolution policies of decision-makers based on their rational (cognitive) intelligences and behavioral activities. Game theory is a useful instrument for interpreting social interactions among people, especially the psychology of human minds.[6] It has been applied in various aspects of human experiences and fields such as philosophy, economics, politics, industrial production, educational development, geology and meteorology, and so on.

In this research paper, some game theories will be used to analyze the application of blockchain technology in one poor country in order to create a model for other countries to improve their quality of life and development:

2.2.1 Cooperative game type:

This example of game theory entails all the players in the game forming a cooperative bond unanimously enforced through a binding set of contracts (or laws).7 Incidentally, the rules of the game ensue from the collaboration and agreements among the players. In other words, the contracts are mutually agreed upon, and the laws guiding their interactions are not imposed on the members/players by an external entity.

2.2.2 Symmetric game type:

This is a kind of game where the payoffs do not depend on who is playing the game but only on the strategies employed by the others participating in the game.[8] All players adopt the same strategies, and this can only be reasonable for a short-term game. In long-term games, the number of options available to the players increases, and this may complicate the nature of the strategies that will be adopted.

2.2.3 Zero-sum game type:

This is a type of constant-sum game whereby the choices or moves made by any of the players will not increase or decrease the available resources.[9] A critical aspect of this type of game is that a gain by a player in a group is equal to a loss for another player in the same group.

2.2.4 Perfect information game type:

This is a subset of the sequential game theory type, whereby players fully understand/know the actions and moves made by the previous players.[10] Every move in the game represents a node. So, the next player can understand what node or who has played before them. This principle is very applicable in the multi-node decentralized networks/blockchains where the next miner can fully understand the preceding node or identity of the miner before them.

2.2.5 Pooling games:

This is the kind of game where all games prevail over all forms of society.[11] This is a repeated game with changing payoff tables. In terms of its applicability, it reveals through a nexus of computational operations how much exposure population will have to variables such as economic benefits, political relevance, and social growth within a set jurisdiction.

2.3 How Game Theory Explains the Application of the Bitcoin Blockchain

As a matter of fact, game theory investigates human behaviors in terms of playing their parts in a society. The behavioral tendencies of the people in the virtual country named Zandon will be investigated based on their citizenry acts in their digital socio-economy.

The purpose of adopting new technologies in a national economy is to see how they transform the day-to-day living standards of the citizens. Game theory is used to bridge the gap between innovative technology adoption and its expressed impacts on the real GDP and economic and industrial activities within the jurisdiction where they are adopted. This can also have a far-reaching effect on the markets in the area.[12]

3.0 A Case Study

This case study indicates what transpires (the complete list of procedures) when a virtual country is run entirely on the blockchain technology.

3.1 Country Overview

The country addressed in this research paper is named Zandon. It is a digital country that has a population of fifteen million people, eight million of which are poor, unemployed, and have no access to other welfare facilities. Four million people are gainfully employed in various kinds of industries. The tax rate is forty percent, with the people making 180 billion Zand in total. Therefore, the government receives seventy-two billion from its people's earnings. The country is connected to the internet and has unlimited access to electricity.

3.2 National Currency

The country creates a new national currency (cryptocurrency) named Zand. It is an entirely digital token, no paper format. As an estimate, 1 Zand is equal to USD$0.5. This cryptocurrency is made available to all players in Zandon's economy after a two-year advance notice that the national currency is going to be virtualized. National Currency Orientation offices are established to teach or provide people the technologies associated with the use of the new cryptocurrency: such as wallets, information about protocols and mining, lessons on computer programming, computer and laptop hardware, et cetera. These offices will brief both citizens and businesses on how the currency works and how to accept it. To avoid mass inflation of the currency in the economy, the government will first keep 70 percent of the total currency and release it at a rate proportional to the growth of the economy to stabilize the token's value and control its ownership/management. Once the maximum supply has been reached, it will be increased in proportion to the country's growth in the previous year.[13]

3.3 Governance and Citizenry on the Blockchain

The Government of Zandon officially owns all the assets in the country and can track people's property on the blockchain. This will help solve the documentation problems faced by many countries.. The government has the power to apportion the property to whoever may be qualified for asset redistribution. Zandon is not a socialist or communist nation—it maintains a capitalist economy but with tighter governmental control.

The Government of Zandon handles all the identity processes of its people. Zandon people are given fully digitalized identity services on the blockchain that can be tracked. People in poverty often cannot engage with the financial system due to their lack of legal identity, credit, and verification. Digitizing identity brings excluded members of the population into the fold. Knowing every member of the society/community creates better public safety as well (see the Wabi project).[5,14]

3.4 Socio-Economic Activities

The Zandon government can track all incomes. Wages are no longer paid in cash, allowing the government to follow the payments on their blockchain. Many weaker countries (see India prior to Modhi) maintain black markets for tax evasion, money laundering and other illegal activities. Having all transactions visible to the government and currency be digital eliminates the possibility of such black markets. Zandon people do not require permission from their government to conduct any interpersonal transactions. Those transactions are done on the blockchain, and the consensus-building within the blockchain is used for this purpose. Since the Zandon governing system is based on bitcoin, it utilizes the Proof-of-Work (PoW) mining consensus.

The government automatically collects taxes from its people (decentralized tax collection system situated on the blockchain) and then invests some of the revenue in building social infrastructure to improve the life of its citizens.[15,16]

3.5 Commercial Activities

Payments (OMG) are made with cryptocurrency, which drastically simplifies the payment system in the country. This helps businesses to process payments on time, and currency circulation becomes efficient. Since the third-party is removed from the payment structure, Zandon citizens can use Zerocoin-like protocol which makes payment possible in seconds. This method of payment increases commercial performance and adds value to business operations in Zandon.[17] The payment structure is secured and allows for a great deal of anonymity, which means that despite using digital identities, it is possible for the identities of the blockchain users to be hidden during their transactions. In this case, the blockchain is secured and people's transactions—whether it be shopping, buying books online, watching online movies, or even studying online—will not be publicly available to all users. Since the OMG arrangement is quick and safe, this increases the rate of contract finalization and revenue generation for small- and medium-sized enterprises in Zandon. Debt rates are cut in half and people can pay for services at light speed.

3.6 Educational system

The education system in this virtual country is run entirely on the blockchain. To promote better understanding of commercialized technology, Zandon's government creates university training programs in Solidity. This becomes their number one source of labor in the computing industry and also trains Solidity programmers to pick up jobs in the newly formed industry. The government brings in prestigious professors from all over the world after building nice and highly efficient campuses, which provides an incentive for young and up-and-coming people in the industry to come and live/study/work there.[18,19] In doing so, Zandon is established as a bastion of ingenuity, and all high-profile people in the space are enticed to live in Zandon, creating a Library of Alexandria-esque scenario. By monopolizing thought in a rapidly developing field, Zandon's economy skyrockets.

3.7 Industrial Development

Zandon's government creates tax incentives for blockchain companies so that they can expand their operations and engage in meaningful research and development (R&D). A comfortable environment is created for startups so that they can be capable of undertaking prototyping/betas within the country. The government allows companies like OMG to roll out their payment test products in that country. The citizens of Zandon are mandated to buy and use only the products/services produced by the businesses in the country, as most people are already blockchain-integrated and doing so would allow the country's economy to be self-sustaining in the long-term.[20] The fundamental aim of Zandon's government is to create an economic boom that is self-sustaining and prosperous for the Zandon people. The blockchain, which is decentralized, facilitates international trades and economic expansion of the businesses operating in the country.

3.8 Healthcare System

The country's healthcare is run completely on the blockchain. The Zandon Ministry of Health produces some decentralized applications (dApps) that are used by people in the country for various purposes. Some of these dApps provide services that include making reservations for doctor's appointments, receiving medicines from the pharmacy, arranging nursing care for the elderly, and scheduling regular medical examination procedures. The value of having medical applications on the blockchain is to make sure that their functionalities are not interrupted by the actions of third parties. They can operate smoothly and fast, protected by the solid security and autonomy guaranteed by the decentralized system. Another advantage of hosting medical services on the blockchain is to reduce the cost of running public or national health services. With a virtualized health structure, Zandon people can enjoy e-hospital services such as receiving diagnosis and prescription accurately through the internet, enjoying the pleasure of having a digital medical assistant (application) that can guide Zandon in all matters of health requirements. The efficiency of this health system takes into consideration the issue of blockchain security, otherwise some lapses in security may threaten the smooth operations of some clinical or medical dApps. So it is essential, as was done by Timicoin, which adopted the Factom network, to have a parallel blockchain that is more secure and compatible with the functionalities of the dApps used by the healthcare providers in Zandon in association with the Zandon central government's initiatives.[21,22]

4.0 Results (Findings) and Analyses

The Zandon case study used in this research reveals a number of interesting facts shown in the results and findings highlighted in this section. The relevant aspects of game theory are used to analyze the findings in a way that support, strongly or fairly, that adopting a blockchain technology can increase a country's statutory functions and services to its citizens while improving their wellbeing, prosperity, and longevity.

4.1 The Game Theory Analyses of the Case Study

Game theory has been applied in various fields of study to explain human interactions, interdependency, and cooperation. The major purpose of the game theory is to strengthen mutually accepted rules, agreements, and understanding with the hope of creating results that may or may not have widespread effects on the population, because every player in the game is in a state of competition.[23]

4.1.1 Cooperative game type and Zandon people's activities

Applying this game theory, Zandon people, like players in a game, form a cooperative bond unanimously enforced through a binding set of rules and regulations laid down by the Zandon central government. These kinds of unbending rules require collaboration and mutually beneficial interactions among the Zandon people. In this way, it is very easy for the Zandon central government to manage the entire country with little or no resistance from the citizens. This facilitates easy implementation of national policies, which makes it possible for the citizens to feel the impacts of their government's efforts in rebuilding their lives as quickly as possible. Since the blockchain does not permit third-party interference, most of the rules in Zandon are internally generated and observed for the benefit of the Zandon people. Despite the anticipated competition among the Zandon people, which is expected in a competitive game theory setting, they are still expected to play fair in their efforts to win the game in activities they routinely participate in within their jurisdiction. However, their attitudes are incompatible with the rules in Zandon which, in effect, makes it possible for their government to effectively control the actions of every citizen in the country. In cryptocurrency parlance, the central Zandon government acts as a blockchain (network) that connects all various players (miners, in the case of Zandon people) to successfully execute smart contracts (transactions) between one another. The existing competition in Zandon may be between some groups and people from different socio-economic classes, but their cooperative behaviors are still centrally managed by the Zandon central government, which performs the functions of a blockchain in a truly decentralized economic setting.

4.1.2 Symmetric game type and Zandon people's activities

This type of game theory reveals that the payoffs for participating in the game do not depend on the demographics of those involved, but rather the common strategies they employ.[8] For Zandon people, no other determinants matter per the outcomes of their participations in the virtual economy but the strategies dictated by the central government. Over time, Zandon people may have access to more strategies to live freely in this virtual country; however, that will not change the fact that the strategies are enforced by their government and must be adopted. The payoffs in this symmetric game type could be the benefits Zandon people enjoy because of their citizenship. If any of them move from one

position to another location within Zandon, they will still be able to enjoy those benefits irrespective of who is participating in the game. Imagine this scenario: if a lawyer in Zandon had access to some welfare packages within the country because he/she is a citizen of Zandon, and then someone who is a scientist now fills the same position previously occupied by that lawyer, he/she will still have unhindered access to the same welfare packages. The Zandon government guarantees a constant payoff in order to run an egalitarian community for all Zandon members.

4.1.3 Zero-sum game type and Zandon people's activities:

A zero-sum game type is one where the choices or moves made by any of the players will not increase or decrease the available resources.[9] Applying this to the actions of the Zandon people, since their economy is centrally controlled, any financial losses incurred by one member of Zandon community will be offset by the gains by the others. In fact, the Zandon central government runs a welfare-based economy using the generous revenues obtained from its citizens' taxes. This is to say, a losing member of the Zandon community can have his/her account replenished by either the Zandon government or the activities of the remaining members in the Zandon community. A better way to describe this incident is that when a member of Zandon community loses some money through a business endeavor, he/she may receive other business opportunities from the community members or some financial assistance from the Zandon central government to regain the lost fortune. A zero-sum game type creates a socio-economic environment that is similar to that of a socialist or communist governance. Every Zandon citizen considers themselves unique and sees the collective property of the country as a shared heritage with the other citizens. In this setting, losses are not counted as personal, but as a community's share of responsibility. To make up for the losses, there are other ample opportunities in the community to pay for any losses incurred by a member. In a zero-sum game, emphasis is placed on mutual benefits through communal sacrifices and dedication. This cohesive nature of the communities within Zandon makes it possible for the central Zandon government to administer the country through its laws.

4.1.4 Perfect information game type and Zandon people's activities:

This is a subset of sequential game theory type, whereby players fully understand/know the actions and moves made by the previous players.[10] The Zandon people are ruled by the same set of rules. This makes it possible for them to know exactly what a previous player/citizen has done concerning one situation or the other. Every move in the game represents a node. In the blockchain, a node represents a miner or an entity creating a transaction block on the network. Politically, it rests on the Zandon government to provide its citizens with prior information about every procedure they should be aware of to streamline the governing process. When players are aware of the steps taken previously, they will be able to adjust their wants/desires within the frameworks provided by their government. This will not only lead to peaceful co-existence among the Zandon people but also make it possible for the government to lead with no resistance from its

people. However, the opposite occurs when there is a lot of misinformation in a country; those who are angered by the lack of appropriate information may take the laws into their hands and frustrate their government's efforts at smoothly running the country.

4.1.5 Pooling games and Zandon people's activities:

In this type of game, all games prevail over all forms of society.[11]Before the Zandon central government moved to the virtual economy, the country was possibly ruled by different socio-political norms and ideologies. However, switching to a new form of government entailed that the new system overtook all other forms of societal governance. This is a repeated game with changing payoff tables. Applying this notion to the Zandon people's activities means that the people adopt similar lifestyles and economic styles in order to have access to several beneficial playoffs such as economic benefits, political relevance, and social growth within the country. As for people lived in Zandon before it adapted its fiscal and economic digitalization, they will have to embrace the new paradigm with no complaints. The central government should take all the necessary precautions to make sure that its citizens implement every new policy and program. Naturally, it takes a concerted effort from all community members and their leadership to forge a new method of governance. Likewise, the central Zandon government should collaborate with its people through periodic education and training so that they can gradually accept the new way of life with no rancor. For this to take place, all players must pool their resources together and overcome the restrictions posed by the former societal or governance system that was previously in place.

4.2 How Other Nations Can Benefit from this Arrangement

It is evident from the bulk of information highlighted above that the Zandon people and their central government have a lot to gain from the virtual economy/government in place. Other nations can derive similar benefits and drastically improve the quality of their people's lives. Outlined below are four strategic ways other countries can transform the lives of their citizens using the same approach adopted by Zandon:

I. Better coordination:

Most countries that live under the poverty level have incredibly poor system coordination. In several instances, public records are non-existent, and the laws guiding public behavior are largely unapplied. With a centrally managed governance like that of Zandon, it is possible to eradicate such circumstances.

II. Conformity to the laid-down principles:

Zandon people unanimously conduct their business, governmental, and healthcare activities through the procedures provided by their central government. This streamlines all their behavioral tendencies and make them work together in unison on most of their projects. Another poor country can adopt the same system and make it easier for its citizens to engage in business, political, and socio-economic activities without any hassles or problems.

III. Higher standard of living:

Game theory specifically reveals how dramatically the adoption of a virtual economy and governance have changed the lives of the Zandon people for good: losses are shared or centrally compensated for, access to medical treatment has greatly improved, commercial activities and access to high-quality education are activated, and people can work on mutually beneficial projects by first concentrating on the general well-being of their communities. These are dynamic improvements every poor nation in the world needs to systematically transform the lives of its inhabitants.

IV. Better security due to distinct identity:

With every citizen in Zandon having his/her identity etched or provided by the central government on the blockchain, the uniqueness of each person's identity makes it possible for their activities to be tracked, documented, and analyzed when necessary to determine whether such a person's behavior conforms with the rules of the country or not. This approach will gradually reduce the rate of crime as people are aware that they will be detected if they undertake any criminal activities involving money.

The four elements of a national transformation described above clearly show that any poor country can overcome its challenges commonly found in governance, political processes, commerce, education, healthcare, and other areas of human endeavors where the actions of the central government are required to administer and manage people's daily behavior and activities. When compared with other types of governance, a centrally managed virtual country can speedily develop because unnecessary diplomatic or bureaucratic hurdles have been systematically removed, and the central government can smoothly run the affairs of its people without any bottlenecks.

Additionally, with this new system, countries can work together more directly as well. MIT is developing a new cryptocurrency called Tradecoin, a currency that is tied to a real-world basket of goods, like land or oil.[24] A country can leverage its natural resources in order to generate large amounts of money. Countries could also pool resources and enter an alliance around a currency. There could be a mutual fund shared by the countries in this alliance: a fund able to be drawn from in times of national emergency, like a large natural disaster or epidemic. With the real-world goods tied to the coin, countries would be held

accountable for paying back the fund or their goods would be held as collateral. This alliance of third-world countries helping each other out could greatly benefit each of them.

Finally, a country like Zandon taking the lead and adopting the blockchain could be the impetus that the countries in similar scenarios need to take the plunge. There are major risks associated with tearing up a country's economic status quo, but all it would take would be one successful endeavor to convince other countries to try out similar systems. This could benefit people all over the world as they experience the same forward-thinking changes as the people of Zandon.

4.3 Building the Necessary Technologies and Commercialization Prospects

It must be stated that the success of any virtual country or economy depends, to a large extent, on the effectiveness of a series of technologies used in running its day-to-day governing activities. For another country to record similar progress or success as Zandon, efforts must be placed in developing the following kinds of technologies:

1. Adoption of the blockchain: This is the very first kind of technology that must be adopted to establish a solid background for running a virtual economy/country.
2. Payment gateway: OMG, as a payment gateway, can be built to cater to the financial needs of the people in a virtual economy. The country has autonomy to choose or develop a payment method that best suits their needs.
3. Timicoin-like healthcare technology: It is necessary to build a suite of decentralized applications (dApps) for medical or clinical service delivery.
4. Wabi-like public security technology: This technology is built to harness all the information about the citizens of a virtual country stored on a blockchain and use the data to map their activities to detect if any crimes have been committed against the government and other members of the society.
5. Educational technology: The communalization of the Solidity programming language will help those who studied it become an active programmer and develop the country's new Solidity-based economy.

5.0 Conclusions and Recommendations

The game theory used above clearly reveals the possibility of transforming the lives of people located in the poorest parts of the globe through the adoption of a blockchain-based virtual economy. This creates an atmosphere of smooth governance and better and faster implementations of governmental policies, programs, and agendas. People in a virtual economy can soon feel the effects of their government's actions in their daily life. This is not possible in a fully capitalist economy where only the rich and mighty control the most profitable sections of the nation's economy.

The technologies utilized in this setup are all compatible with one blockchain infrastructure. This is very important because technologies or protocols that are not compatible with the selected blockchain or decentralized network may lead to operational glitches.

It must be stated that this approach is still purely theoretical, even though countries such as Estonia, Georgia, Ireland, and others are rapidly turning into digital economies. A lot of research and testing is required to see if this approach will be applicable to all nations willing to eradicate poverty among their people while creating a safer, better, and more functional society.

In recommendation, it will be helpful if future research were conducted on how the inhabitants would react in the long-term to sudden changes in their lifestyles. Would they reject their central government's bid to automatically claim their taxes? Would they fight against the use of new technologies that may take months for them to fully learn how to use or operate? And would they be willing to sacrifice their personal privacy to accept security measures that are potentially too intrusive?

References

[1] "FAQs: Global Poverty Line Update." *World Bank.* Last modified April 20, 2018. www.worldbank.org/en/topic/poverty/brief/global-poverty-line-faq

[2] Invest in Blockchain (2018). Estonia, a blockchain model for other countries? Available at: https://www.investinblockchain.com/estonia-blockchain-model/ (Accessed: 30 March 2018).

[3] Hammersley, B. (2018). Concerned about Brexit? Why not become an e-resident of Estonia? *Wired.* Available at: www.wired.co.uk/article/estonia-e-resident (Accessed: 21 April 2018).

[4] A.K.K (2013). How did Estonia become a leader in technology? *The Economist.* Available at: https://www.economist.com/blogs/economist-explains/2013/07/economist-explains-21 (Accessed: 21 April 2018).

[5] U.K. Government (2016). *Digital transformation in government and blockchain technology.* Available at: https://www.gov.uk/government/speeches/digital-transformation-in-government-and-blockchain-technology (Accessed 30 March 2018).

[6] Herzig, A., and Lorini, E. (2015). *The cognitive foundation of group attitude and social interaction.* New York: Springer.

[7] Curiel, I. (2013). *Cooperative game theory and applications: Cooperative games arising from combinatorial optimization problems.* New York: Springer Science & Business Media.

[8] Webb, J.N. (2007). *Game theory: Decisions, interaction, and evolution.* New York: Springer Science & Business Media.

[9] Thomas, L.C. (2012). *Games, theory, and applications.* Massachusetts: Courier Corporation.

[10] Myerson, R.B. (2013). *Game theory.* London: Harvard University Press.

[11] Gibbons, R. (1992). *Game theory for applied economics.* New Jersey: Princeton University Press.

[12] Christiansen, B. (2013). *Economic behavior, game theory, and technology in emerging markets.* Hershey, Pennsylvania: IGI Global.

[13] Bloomberg (2017). *China is developing its own digital currency.* Available at: https://www.bloomberg.com/news/articles/2017-02-23/pboc-is-going-digital-as-mobile-payments-boom-transforms-economy (Accessed: 30 March 2018).

[14] Brainard, L.A., and McNutt, J.G. (2010). Virtual government-citizen: Informational, transactional, or collaborative? *Administration & Society,* 42 (7), 836-858.

[15] CCN (2018). *Blockchain will enhance the economic and socio-political emancipation of Humankind.* Available at: https://www.ccn.com/blockchains-will-enhance-the-economic-and-socio-political-emancipation-of-humankind/ (Accessed 30 March 2018).

[16] Brainard, L.A., and Brinkerhoff, J.M. (2006). Sovereignty under siege, or a circuitous path for strengthening the state? Digital diasporas and human rights. *International Journal of Public Administration,* 29, 595-618.

[17] Bacaj, L. (2017). eCommerce on the blockchain. *Hackernoon*. Available at: https://hackernoon.com/ecommerce-on-the-blockchain-7bfdc2af8c46 (Accessed: 30 March 2018).

[18] Hall, M. (2016). The blockchain revolution: Will the universities use it, or abuse it? *Times*

Higher Education. Available at: https://www.timeshighereducation.com/blog/blockchain-revolution-will-universities-use-it-or-abuse-it (Accessed: 30 March 2018).

[19] Schneider, N. (2018). An internet of ownership: Democratic design for the online economy. *The Sociological Review,* 66 (2), 320-340.

[20] Kayondo, D.M. (2017). Blockchain: Redefining the fourth industrial revolution. *Market Mogul.* Available at: https://themarketmogul.com/blockchain-redefining-fourth-industrial-revolution/ (Accessed: 30 March 2018).

[21] Timicoin (2018). *Health information on the blockchain. Available at: https://timicoin.io/* (Accessed 30 March 2018).

[22] Lupton, D. (2017). Digital health now and in the future: Findings in a participatory design stakeholder workshop. *Digital Health,* 3, Doi: https://doi.org/10.1177/2055207617740018 (Accessed 30 March 2018).

[23] Miller, J.D. (2003). *Game theory at work: How to use game theory to outthink and outmaneuver your competition.* New York: McGraw Hill Professional.

[24] Lipton, A., et al. (2018). Digital Trade Coin (DTC): Towards a more stable digital currency. *Royal Society Open Science.* (Accessed 7 July 2018).

Comparing RSA, ECC, and Post Quantum Cryptography

By William Yunsoo Seo
Seoul International School

Abstract

With the development of quantum computing just around the corner, modern day cryptography is in the need of a makeover. Newly developed post-quantum encryption schemes, developed to resist quantum cryptanalysis, will need to become the new face of public key encryption. In anticipation of this large overhaul of public key cryptography, this paper looks into how these upcoming post quantum replacements are comparable to the currently prominently used cryptosystems in terms of execution on modern devices. Specifically, this paper compares the key generation, encryption, and decryption speeds of two promising post quantum cryptosystems (NTRU and Lizard) with two prevalent modern cryptosystems (RSA and ECC) on a modern computer. In this comparison, the two post quantum cryptosystems, in general, exhibited faster speeds than the two modern cryptosystems. Our conclusions suggest that in regard to efficiency, post quantum cryptosystems are more than capable of replacing modern cryptosystems. However, further cryptographic analysis will need to be undergone before these post quantum cryptosystems can be completely trusted.

Introduction

In the era of technology, electronic communication has become a vital foundation of society. Never before did so many people have the connection to the rest of the world in their workplace, home, and pockets. "The need for confidentiality, integrity, authenticity, and non-repudiation in data transmission and data storage" in the modern world has made "the science of cryptography one of the most important disciplines in information technology" [1].

Cryptography is the study of encryption, the process of encoding a message or information so that it cannot be comprehended by anybody without a secret key. "Humans have been communicating with codes and ciphers for thousands of years, using rudimentary encryption methods to protect trade secrets and military orders, or simply to keep information private from neighbors" [2]. Throughout history, the complexity of encryption

has risen significantly. Modern day encryption can be categorized into two large groups; symmetric encryption and asymmetric encryption.

Symmetric (Private Key) Encryption

When most people think of encryption, it is symmetric encryption that comes to mind. Symmetric Encryption, the standard form of encryption, encompasses a vast majority of the most widely used cryptosystems, including AES (Advanced Encryption Standard), DES (Data Encryption Standard), and TwoFish.

Symmetric Encryption is defined as a cryptosystem which uses the *same key* for the encryption and decryption processes, as suggested by its name. In other words, two people communicating using Symmetric Encryption must share prior knowledge about a shared key.

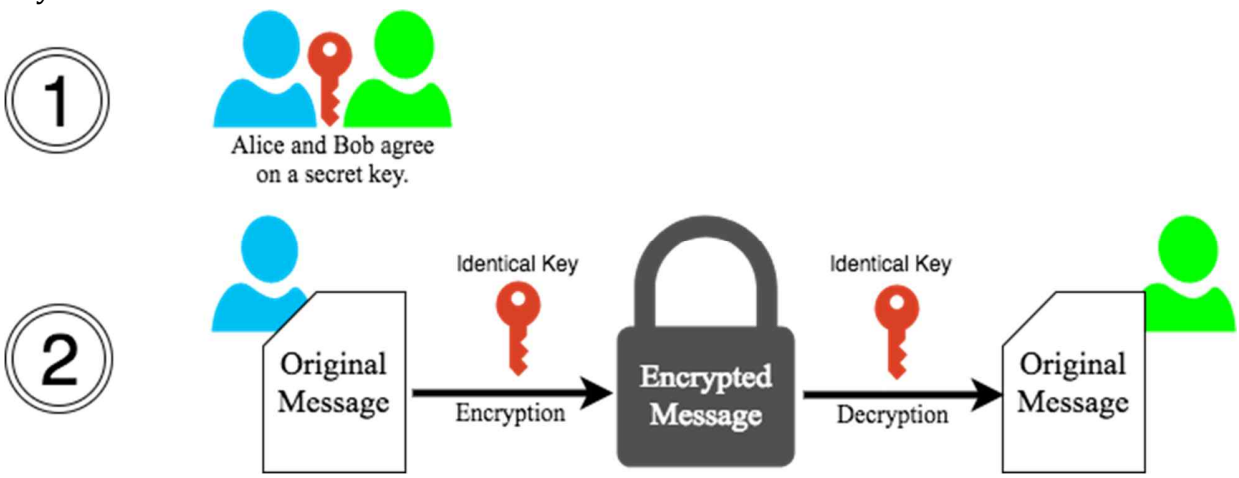


***Fig. 1**: Symmetric Encryption*

Asymmetric (Public Key) Encryption

Asymmetric Encryption is encryption which uses two different keys: the public key which is used for encryption, and the private key which is used for decryption. Asymmetric encryption starts off with the message-receiver publicizing his or her public key. Any person can encrypt a message using the public key of the receiver, and this message can only be decrypted with the receiver's private key. This system allows two people to securely communicate without establishing a secret shared key in advance. Due to its characteristics, asymmetric encryption schemes are mainly used to implement digital signatures and for key establishment. “They play a crucial role in ensuring the confidentiality and authenticity of communications on the Internet and other networks” [3].

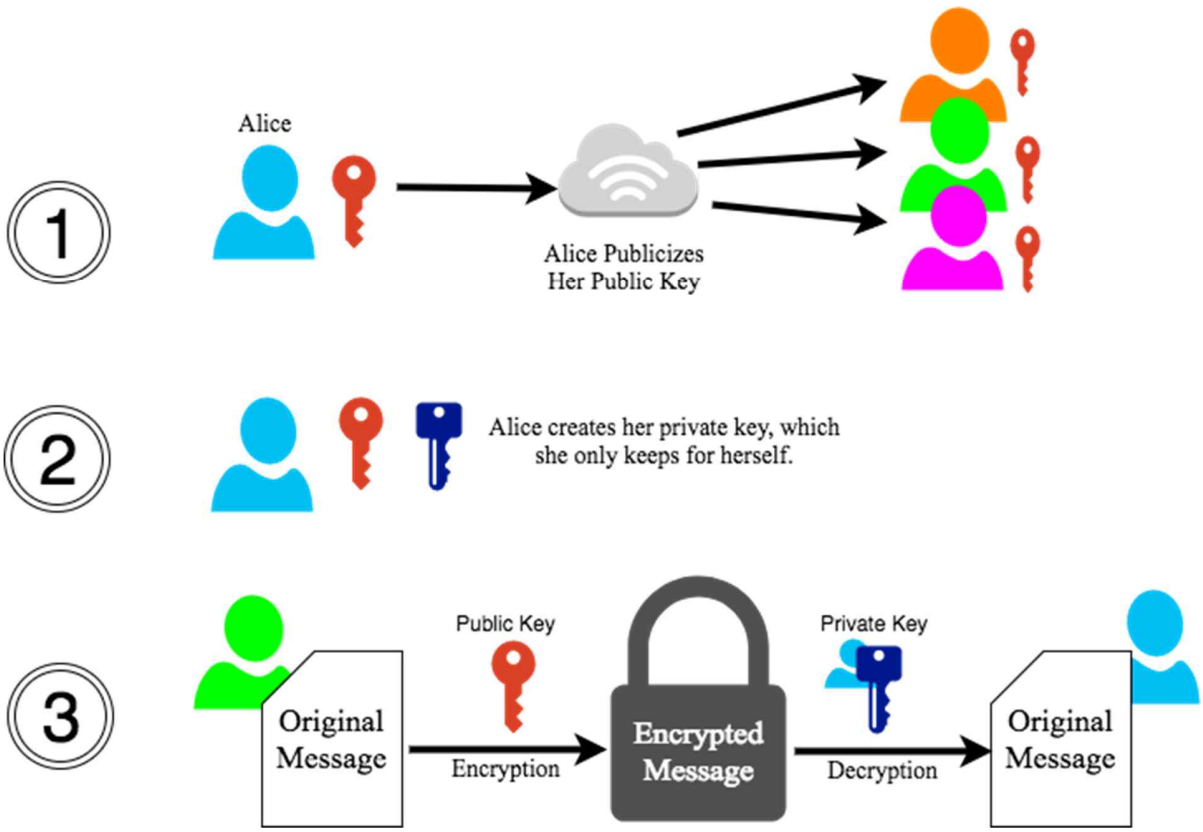


***Fig. 2**: Asymmetric Encryption*

However, "due to their unique nature, [asymmetric cryptosystems] are more computationally costly than" and "more vulnerable to brute force attacks than" their counterparts in secret-key cryptography [4]. Thus, they are more vulnerable to the incoming threat of quantum computing.

Quantum Computing

Currently, scientists are rigorously developing quantum computers: "machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional computers" [3]. If scientists manage to develop a large-scale functioning quantum computer, it will be able to run algorithms that "compromise the security of many commonly used cryptographic algorithms" [3]. One such algorithm is Shor's algorithm [5], a quantum-PC algorithm developed by mathematician Peter Shor in 1994. Due to its ability to factor large bi-prime numbers and solve discrete logarithm problems in polynomial time, this algorithm alone compromises the security of RSA, Elliptic Curve Cryptography, and Finite Field Cryptography, three of the most commonly used public key encryption schemes for digital signatures, key exchange, and key establishment.

These predictions regarding the computational capabilities of quantum computers have stirred up a concern regarding the security of encryption. After quantum machines inevitably crush RSA or DSA encodings, maybe cryptographers will conclude that the age of

reliable encryption is over; that there is no expectation of scrambling data to make it undecipherable by aggressors. A more intensive look uncovers, however, that there is no avocation for the jump from "quantum PCs decode RSA or ECDSA" to "quantum machines decode cryptography" [6, 7]. There are numerous essential classes of cryptographic frameworks that can resist the quantum computer, also known as post-quantum cryptographic frameworks:

1. Secret-key cryptography (symmetric encryption). A popular example is "Rijndael" [8] selected by NIST as the new Advanced Encryption Standard (AES)
2. Hash-based cryptography. A great illustration is Merkle's hash-tree open key mark framework (1982) [9], expanding upon a one-message-signature thought of Lamport and Diffie.
3. Code-based cryptography. An exemplary illustration is McEliece's concealed Goppa-code open key encryption framework (1978) [10]
4. Lattice-based cryptography. A case that has maybe pulled in the most intrigue, not the primary illustration verifiably, is the NTRU open key-encryption framework (1998) [11].
5. Multivariate-quadratic-conditions cryptography. One of many fascinating illustrations is Patarin's open key-signature framework from 1996 [12], summing up a proposition by Matsumoto and Imai.
6. Learning-with-error cryptography. A recently developed and novel illustration is the Lizard public key encryption framework (2016) [13].

These encryption schemes are expected to be resistant to traditional and quantum attacks. So far no efficient attacks has been discovered applying Shor's algorithm on these schemes. Another popular quantum algorithm, "Grover's calculation," [14] has a few applications to these frameworks. However, Grover's calculation is not as efficient as Shor's calculation, and cryptographers can effectively adjust for it by picking to some degree bigger key sizes. These particular cryptographic frameworks hold substantial importance as they must take the place of RSA and other currently prominent open key schemes before the effective development of an extensive quantum PC is declared. Keeping in mind that it "has taken almost 20 years to deploy our modern public key cryptography infrastructure," we can reasonably conclude that the replacement of these currently prominent schemes with post-quantum schemes will take a "significant effort" [3]. Thus, process of replacement must be initiated in the near future.

At that point in time, post quantum frameworks such as NTRU will be the new face of public key encryption. The security and efficiency of online communication will be determined by these frameworks. In this paper, we will assume a hypothetical situation in which the effective development of an extensive quantum PC is declared at this very moment. If post quantum encryption schemes were to replace the currently prominent public key encryption schemes, would they be able to accomplish comparative levels of execution on modern phones, laptops, and computers?

Data Collection

To answer the research question above, we will investigate how the key generation, encryption, and decryption speeds of post quantum cryptosystems compare to the speeds of the currently prominent public key cryptosystems. Speed is an essential quality to compare, as cryptosystems must be capable of handling bustling Internet servers which deal with countless customers each second.

Since it would be impossible to analyze the speeds of all post-quantum cryptosystems and modern public key cryptosystems, I decided to select two suitable representatives from each side and compare them. To represent the currently prominent public key cryptosystems, I chose RSA and ECC. Following is a brief overview of these two cryptosystems and why I chose each one.

RSA [15]

RSA is a public key encryption scheme invented by Ronald Rivest, Adi Shamir, and Leonard Adleman in 1977. RSA establishes security by utilizing Euler's theorem (*If m and N are relatively prime, then* $m^{\phi[N]} \equiv 1 \bmod N$) and exploits the difficulty of factoring large semiprime numbers. Thus, RSA is vulnerable to quantum computers, which can run a fast factoring algorithm: Shor's Algorithm.

I chose RSA to be a representative because it is widely considered to be "one of the most important public-key schemes" [1]. Not only was RSA one of the first public key encryption schemes developed, but it also has maintained its place as one of the most commonly used public key cryptosystems for decades.

ECC [16]

Short for elliptic curve cryptography, ECC is an approach to public key encryption based on the algebraic structure of elliptic curves. The security of ECC lies on the difficulty of solving the discrete logarithm problem: determining the integer r such that $g^r = x \bmod p$. Unfortunately, a modified Shor's algorithm can be used to decrypt data encrypted using elliptic-curve cryptography, making ECC vulnerable to quantum computers as well [17].

I chose ECC as a representative of the modern public key cryptosystems because it is "considered the most secure and efficient asymmetric cryptosystem" in the modern (pre-quantum) world [1].

To represent the post quantum cryptosystems, I chose NTRU and Lizard. Following is a brief overview of these two cryptosystems and why each is a suitable representative.

NTRU [18]

Developed in 1996 by mathematicians Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman, NTRU is a lattice based public key cryptosystem based on the shortest vector problem in a lattice. NTRU relies on the difficulty of factoring certain polynomials into a quotient of two polynomials, making it resistant to Shor's algorithm.

I chose NTRU as a representative of post quantum cryptosystems because the cryptosystem is considered "the most efficient and secure" lattice-based cryptosystem and the "most promising candidate" for the replacement of RSA and ECC [1].

Lizard [13]

Proposed by Jung Hee Cheon, Duhyeong Kim, Joohee Lee, and Yongsoo Song in 2016, Lizard is a novel public key encryption scheme based on LWE (learning with error) and LWR (learning with rounding). By utilizing a "conceptually simple encryption procedure consisting of subset sum and rounding operations without Gaussian samplings," Lizard boasts a fast encryption speed, practicality, and strong security [13].

I chose Lizard as a representative of post quantum cryptosystems because it is a unique and promising cryptosystem that is designed to work quickly and efficiently on our everyday devices.

I will compare the speeds of RSA, ECC, NTRU, and Lizard side by side. The implementation of each scheme was written in C, and performed on iMac containing Intel(R) Core(TM) i7 CPU running at 3.4GHz. The version of the gcc compiler is 7.1.0. For each of the cryptosystems, we set the parameters such that each scheme had around a 128-bit security level. Then, we measured the average time it took each cryptosystem to encrypt and decrypt message blocks over thousands of trials.

Data Collection Methods

RSA

Source	Key Generation: OpenSSL [19]. Encryption and Decryption: LibreSSL [20].
Parameters	For RSA at 128-bit security level, the National Institute of Standards and Technology recommends the use of a 3072-bit key [21]. Key Generation: RSA 3072 Encryption and Decryption: RSA 2048* *Unfortunately, LibreSSL did not have an option for RSA 3072. As a result, I used RSA 2048 for measuring the encryption and decryption speeds.
Method of Data Collection	Key Generation: Found the average value for 1000 trials. Encryption and Decryption: Recorded how many message blocks could be encrypted/decrypted in a span of 10 seconds, then used this info to find the speeds.

ECC

Source	Key Generation: Chilkat Software [22]. Encryption and Decryption: LibreSSL [20].
Parameters	For ECC at 128-bit security level, the National Institute of Standards and Technology recommends the use of a 256-bit to 383-bit key [21]. Key Generation: ECC-256 Encryption and Decryption: ECC-283
Method of Data Collection	Key Generation: Found the average value for 1000 trials. Encryption and Decryption: Recorded how many message blocks could be encrypted/decrypted in a span of 10 seconds, then used this info to find the speeds.

NTRU

Source	All Measurements: Github [23].
Parameters	For NTRU, the parameter n indicates the scheme is run using polynomials of degree n $-$ 1 in the ring $Z[x]/(X^n - 1)$ [24]. For 128-bit security NTRU, setting the n value to 701 is recommended [25]. All Measurements: NTRU $n = 743$* *This was the closest option I could find.
Method of Data Collection	All Measurements: Found the average value for 1000 trials.

Lizard

Source	All Measurements: Github [26].

Parameters	For all measurements, I used the suggested parameter sets for 128-bit security included in a paper written by Lizard's creators [13].
Method of Data Collection	All Measurements: Found the average value for 1000 trials.

Data

Encryption Scheme	Key Generation Time (milliseconds)	Encryption Time (milliseconds)	Decryption Time (milliseconds)
RSA	275.477	0.782	28.118
ECC	8.184	6.5	1.5
NTRU	3.829	0.438	0.826
Lizard	15.521	0.009	0.009

***Table 1**: Encryption and Decryption Speeds of Various Cryptosystems*

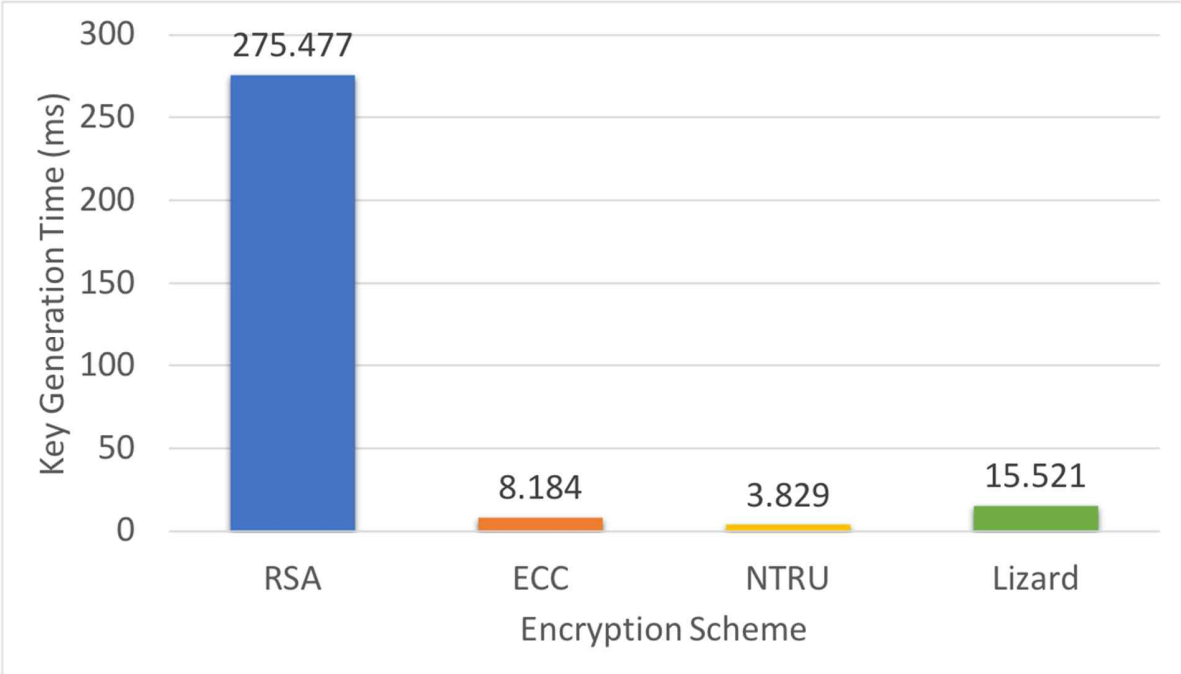


***Fig. 3**: Key Generation Speeds of Cryptosystems*

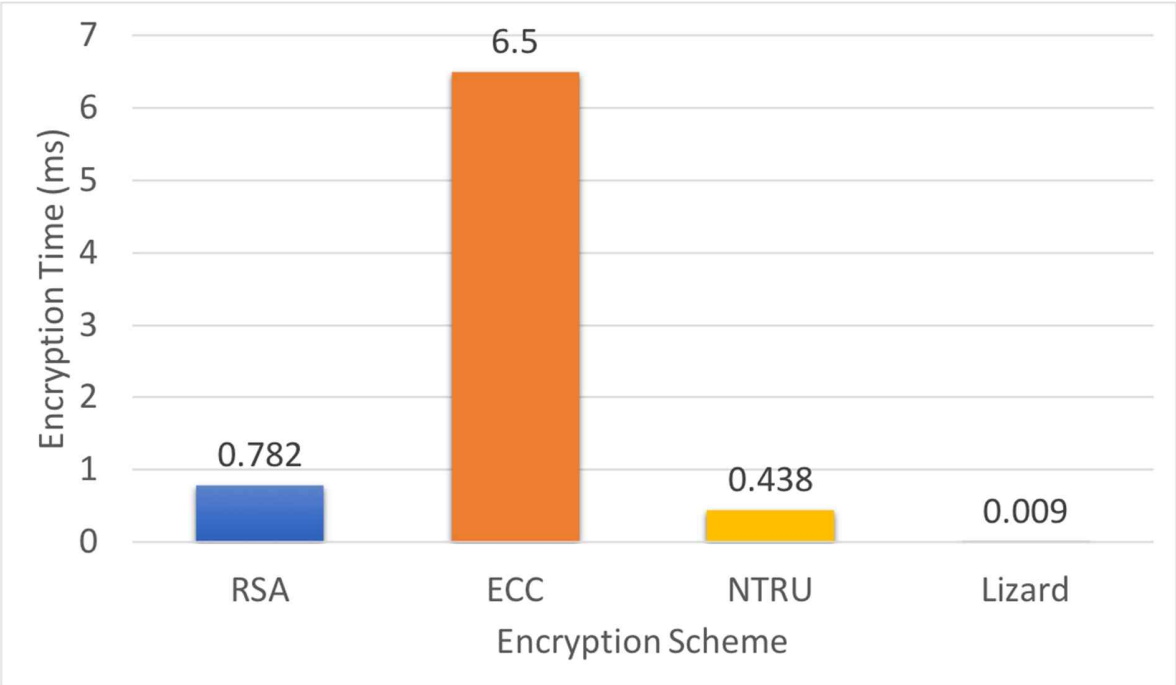


***Fig. 4**: Encryption Speeds of Cryptosystems*

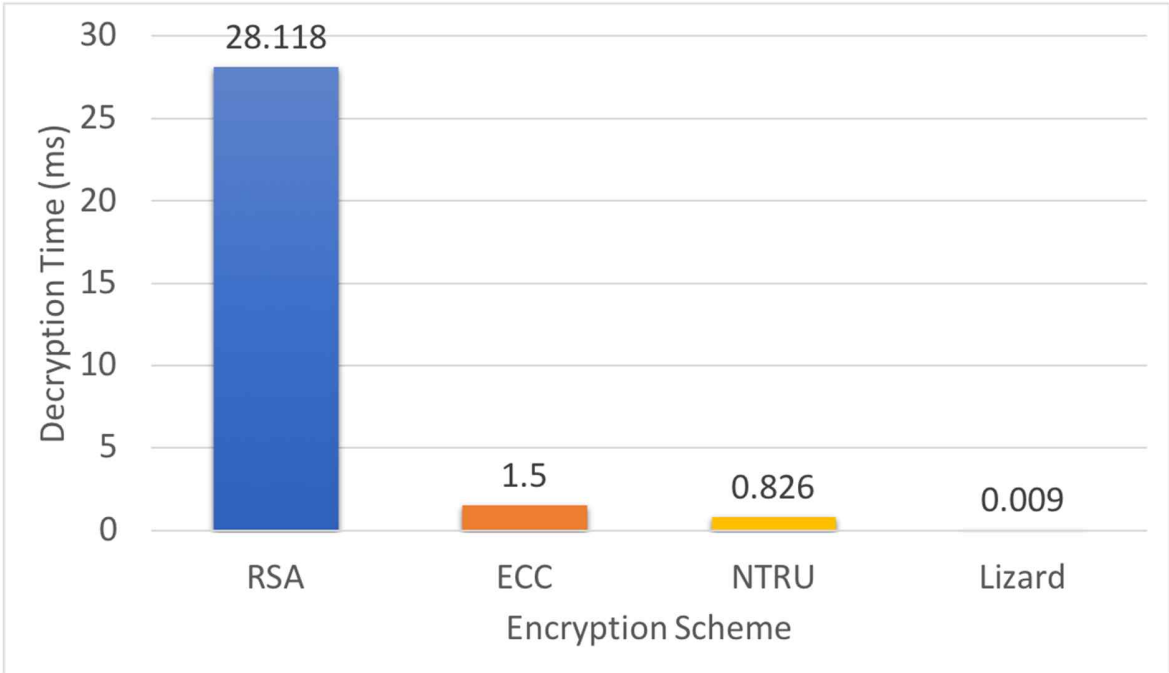


***Fig. 5**: Decryption Speeds of Cryptosystems*

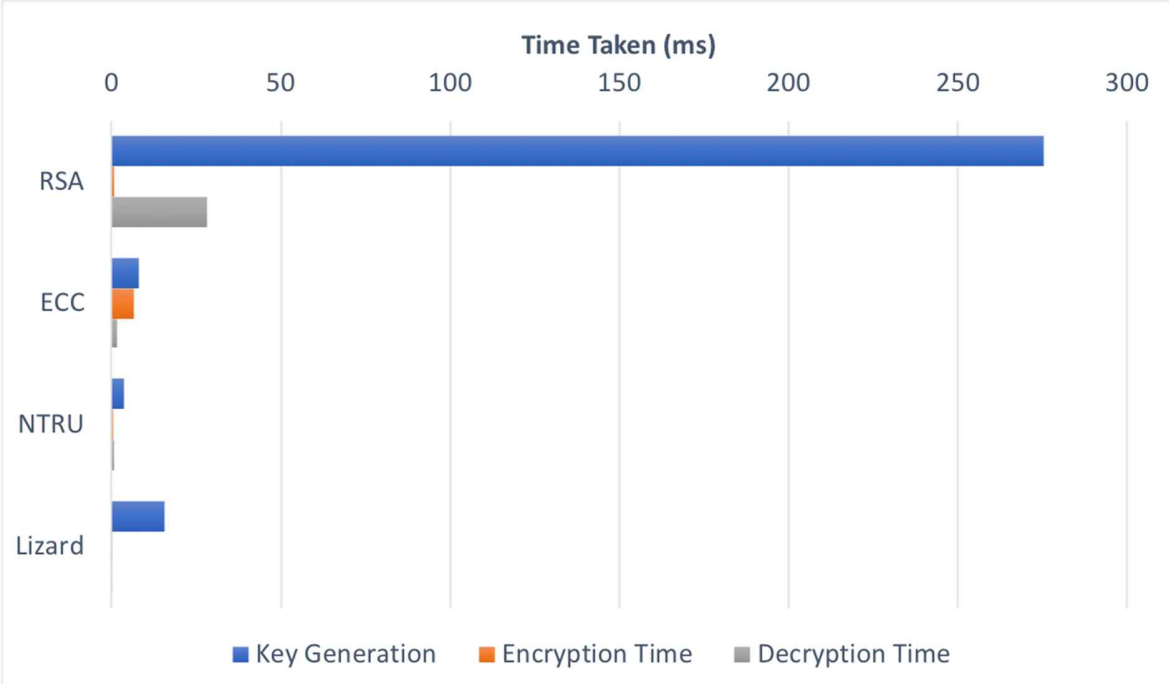


***Fig. 6**: Key Generation, Encryption, and Decryption Speeds of Cryptosystems*

Analysis of the Data

RSA vs ECC

In Figure 6, ECC's superiority in efficiency to RSA is clearly shown. While the data shows the RSA is more efficient in terms of encryption times, it is inferior to ECC in terms of key generation time and decryption times. My data shows why ECC is "considered the most secure and efficient asymmetric cryptosystem" in the modern world [1].

Regarding NTRU

The data indicates that even though NTRU is quantum-proof, it is faster than both RSA and ECC in all three categories. My data justifies why NTRU is considered the "most promising candidate" for the replacement of RSA and ECC [1]. These results were not an anomaly. In fact, in "An Overview of the NTRU Cryptographic System", a master's thesis paper based on the NTRU cryptosystem, the author Hien Ba Nguyen found similar results across multiple security levels.

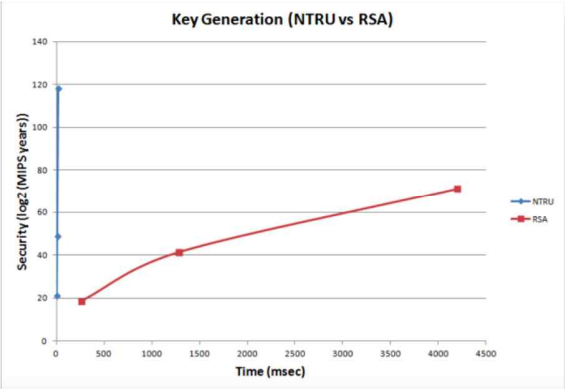


***Fig. 7**: Keygen. (NTRU vs RSA)*

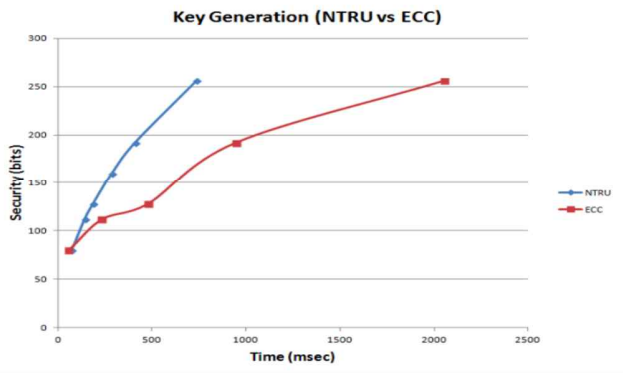


***Fig. 8**: Keygen. (NTRU vs ECC)*

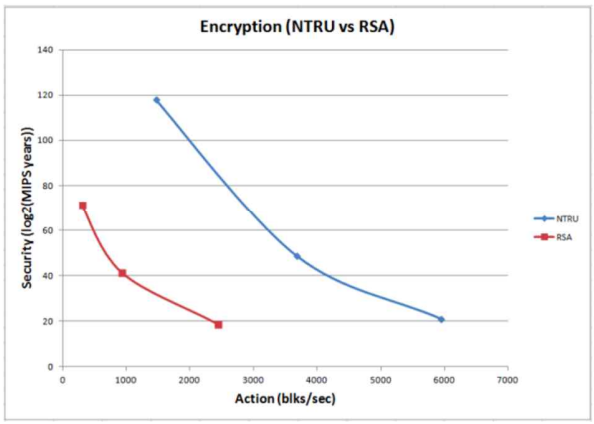


***Fig. 9**: Encryption (NTRU vs RSA)*

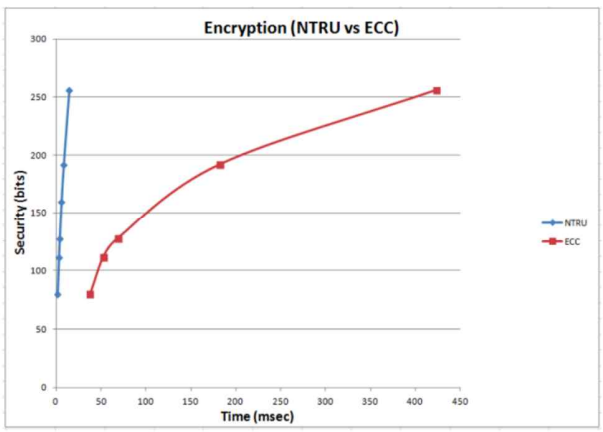
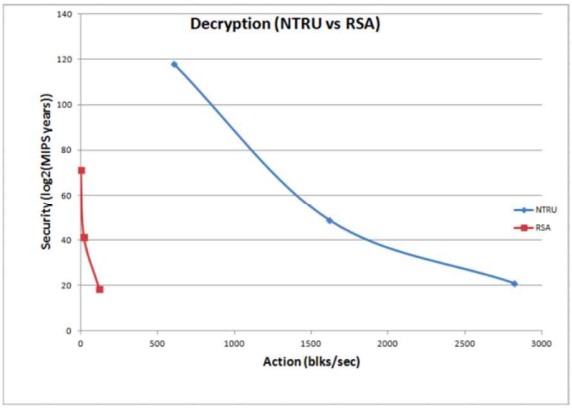


***Fig. 10**: Encryption (NTRU vs ECC)*



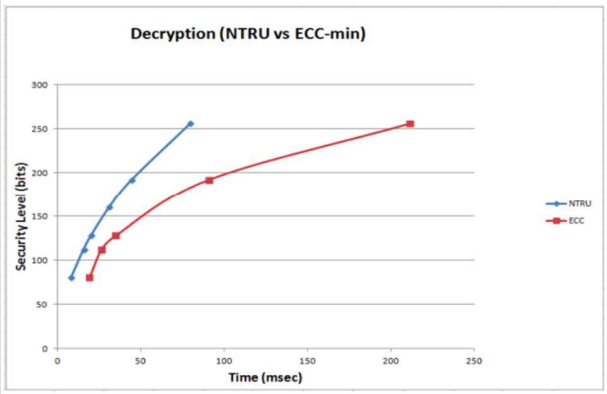


***Fig. 11**: Decryption (NTRU vs RSA)*

***Fig. 12**: Decryption (NTRU vs RSA)*

*Graphs from [24].

Regarding Lizard

One key trait I noticed about Lizard from my data was its tremendously fast encryption and decryption speeds, which were a few hundred times faster than RSA or ECC. Its encryption and decryption speeds were also 47 times and 97 times faster than those of NTRU, respectively. These results make good sense, as Lizard was specifically designed to be "competitive for applications requiring fast encryption and decryption phases" [13]. However, Lizard's key generation speed was not as impressive, as it was outclassed by both ECC and NTRU. From the data, we can see that Lizard will be able to have better efficiency in situations where one unchanging key is used to encrypt and decrypt many messages.

Conclusions

From our data, we can see that post quantum encryption schemes, especially NTRU, are completely capable of replacing RSA and ECC based on their efficiency. However, before jumping to the conclusion that post quantum cryptosystems are prepared to replace RSA and ECC, there is one more quality of post quantum cryptosystems that we must analyze: security.

As the intrinsic purpose of encryption is to establish secure communication, strong security is a must-need for any cryptosystem. While it is obviously true that post quantum cryptosystems are superior to RSA and ECC when it comes to security against quantum computers, this does not guarantee that these cryptosystems can be trusted to manage the security of the Internet. In order to develop trust in particular frameworks researchers must contribute enormous measures of time and vitality in cryptographic analysis.

In comparison to RSA, ECC, and other widely used encryption schemes, post quantum cryptosystems have not undergone nearly as much cryptographic analysis. This is due to the fact that quantum computing is and post quantum cryptography are new areas of study. Even NTRU, "the most thoroughly researched and widely implemented alternative to RSA and

ECC" [27] is considered to have "not yet undergone enough amount of cryptographic analysis" [28].

In conclusion, it is difficult to firmly assert at this moment that post quantum cryptosystems are equipped to become the replacements of the currently prominent cryptosystems. Cryptosystems like Lizard have yet to be tested by the cryptographic community and cannot be judged as a safe cryptosystem yet. In addition, the transition to changing security protocol infrastructure to quantum proof encryption will be quite expensive and may not be worth it at this time to implement. The creation of quantum computers may not even come to fruition, in which case the current cryptographic landscape would be sufficient for reliable security.

However, the future is promising, as post quantum cryptosystems are completely capable of matching and even exceeding the efficiency of the currently prominent cryptosystems. They also may just provide benefits in efficiency that give an investment into systems like Lizard some value to save time. As long as our post quantum cryptosystems do not break under the pressure of cryptographic analysis, the advent of quantum computing won't do much harm to internet security.

References

[1] Mavroeidis, Vasileios, and Kamer Vishi. "The Impact of Quantum Computing on Present Cryptography." *International Journal of Advanced Computer Science and Applications*, 31 Mar. 2018, arxiv.org/pdf/1804.00200.pdf.

[2] Waddell, Kaveh. "The Long and Winding History of Encryption." The Atlantic, Atlantic Media Company, 13 Jan. 2016, www.theatlantic.com/technology/archive/2016/01/the-long-and-winding-history-of-encryption/423726/.

[3] Moody, Dustin. "ITL Bulletin for February 2018." *Computer Security Resource Center*, National Institute of Standards and Technology, 27 Feb. 2018, ws680.nist.gov/publication/get_pdf.cfm?pub_id=925321.

[4] Blumenthal, Matt. "Encryption: Strengths and Weaknesses of Public-Key Cryptography." Department of Computing Sciences Villanova University.

[5] Shor, Peter W. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer." *IEEE Computer Society Press*, 20 Nov. 1994, arxiv.org/pdf/quant-ph/9508027.pdf.

[6] Bleichenbacher, Daniel. "Chosen Ciphertext Attacks against Protocols Based on the RSA Encryption Standard PKCS #1." *CRYPTO 1998: Advances in Cryptology*, 1998, pp. 1–12., doi:10.1007/BFb0055716.

[7]Bernstein, Daniel J., et al. *Post-Quantum Cryptography*. Springer, 2009.

[8] Daemen, Joan, and Vincent Rijmen. "The Block Cipher Rijndael." *CARDIS*, 1998, pp. 277–284., doi:10.1007/10721064_26.

[9] Merkle, Ralph C. "Method of providing digital signatures." U.S. Patent No. 4,309,569. 5 Jan. 1982.

[10] McEliece, Robert J. "A Public-Key Cryptosystem Based On Algebraic Coding Theory." *DSN Progress Report*, pp. 114–116.

[11] Hoffstein, Jeffrey, Jill Pipher, and Joseph H. Silverman. "Public key cryptosystem method and apparatus." U.S. Patent No. 6,081,597. 27 Jun. 2000.

[12] Patarin, Jacques, et al. "QUARTZ, 128-Bit Long Digital Signatures." *CT-RSA*, 2 Apr. 2001, pp. 282–297., doi:10.1007/3-540-45353-9_21.

[13] Cheon, Jung Hee, et al. "Lizard: Cut off the Tail! Practical Post-Quantum Public-Key Encryption from LWE and LWR." *Cryptology EPrint Archive: Report 2016/1126*, 1 Dec. 2016, eprint.iacr.org/2016/1126.

[14] Grover, Lov K. "A Fast Quantum Mechanical Algorithm for Database Search." *28th Annual ACM Symposium on the Theory of Computing (STOC)*, 29 May 1996, pp. 212–219., arXiv: quant-ph/9605043v3.

[15] Rivest, R. L., et al. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems." *Communications of the ACM*, 1 Feb. 1978, pp. 120–126., doi:10.21236/ada606588.

[16] Koblitz, Neal. "Elliptic Curve Cryptosystems." *Mathematics of Computation*, vol. 48, no. 177, 1987, pp. 203–209. *JSTOR*, JSTOR, www.jstor.org/stable/2007884.

[17] Proos, John, and Christof Zalka. " Shor's Discrete Logarithm Quantum Algorithm for Elliptic Curves." *QIC 3*, 2003, pp. 317–344., arXiv:quant-ph/0301141.

[18] Hoffstein, Jeffrey, et al. "NTRU: A Ring-Based Public Key Cryptosystem." *International Algorithmic Number Theory Symposium*, 1998, pp. 267–288., citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.25.8422&rep=rep1&type=pdf.
[19] The OpenSSL Project. "OpenSSL." *OpenSSL*, 1.1.0, OpenSSL Foundation, Inc, 27 Mar. 2018, www.openssl.org/.
[20] "LibreSSL." *LibreSSL*, OpenBSD, 5 May 2018, www.libressl.org/.
[21] Barker, Elaine. "Recommendation for Key Management." *NIST Special Publication 800-57 Part 1 Revision 4*, Jan. 2016, nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf.
[22] "(C) Generate an ECC Key." *Chilkat C Language Examples*, Chilkat Software, Inc., www.example-code.com/C/ecc_genkey.asp.
[23] Etzel, Mark, et al. "NTRUOpenSourceProject." *GitHub*, GitHub, Inc., 2016, github.com/NTRUOpenSourceProject/ntru-crypto.
[24] Nguyen, Hien Ba. "An Overview of the NTRU Cryptographic System." *San Diego State University*, 2014.
[25] Hülsing, Andreas, et al. "High-Speed Key Encapsulation from NTRU." *CHES 2017: Cryptographic Hardware and Embedded Systems*, 25 Aug. 2017, pp. 232–252., cryptojedi.org/papers/ntrukem-20170627.pdf.
[26] Cheon, Jung Hee, et al. "LizardOpenSource." *GitHub*, GitHub, Inc., 19 Sept. 2017, github.com/LizardOpenSource.
[27] "NTRU Post Quantum Cryptography." *OnBoard Security*, OnBoard Security, Inc., www.onboardsecurity.com/products/ntru-crypto.
[28] Vizev, Nikolay Vasilev. "Side Channel Attacks on NTRUEncrypt." *University of Technology Darmstadt*, 2007.

Using Neural Networks for Translation Tasks

Fang Chan

1. Introduction

Software translation from one language to another has experienced significant advances in recent years. The opportunities that are provided by quality, error free translation are enormous. These potential opportunities for machine translation range from making books written in English available to German speaking customers to providing mission critical software systems, such as medical systems, available to any doctor in the world.

Because of the advantages machine translation would provide, exploration of different translation models continue. Likewise, the predominant industry paradigms are not yet error free (Goldberg, 2015). As such, machine translation is an incredibly exciting area of research with far reaching consequences.

Other important areas of research for machine translation abound. Are we interested in translating spoken word? Written text? A document? Additionally, a language may have words with multiple meanings, or may literally mean something in another language that does not have the required context (such as a colloquialism). Adequate machine translation needs to account for all of these pitfalls.

There are several ways to write a machine translation program. One could, obviously, write a program with guidelines provided by a bilingual speaker. Unfortunately, the domain would be immense. It would be impossible to write software that would take into account every possible rule of translation for each word, each context of a word, each context of a phrase, etc.

One of the more successful methods from recent years for machine translation has been the use of learning or training models. That is, "teaching" a computer to correctly recognize proper translation. These methods have advanced machine translation greatly, and they will be the focus for discussion.

This paper will discuss the current dominant paradigms of machine translation, including statistical machine translation and the recurrent neural network encoder-decoder approach. There are advantages and disadvantages to both. Additionally, we will summarize and discuss recent work proposed by Kyunghyun Cho (2015) regarding a potential advancement in the use of the RNN Encoder-Decoder approach.

2. Issues With Current Paradigms of Machine Translation

Statistical Machine Translation

Revisiting our example of a potential machine translator from earlier, what could we do differently? Well, one common technique is to program a machine to take some text in one language and the same text in another language so it can "learn" which words map to other words.

The statistical aspect comes in with mapping words to other words. Using Bayesian calculations, probabilities are assigned to word pairings. Why do we use statistics? The answer is because a sentence in one language doesn't have a single translation in another language. It can be translated into multiple different words or sentences. As such, we use probabilities to represent the likelihood that a sentence in one language is the likely translation of the sentence in the original language (Brown, 1990).

The likelihood that an output word adequately represents the same word from the original language is referred to as the "log likelihood". Once we've provided the statistical machine translator with a set of input and output translations, the machine can start to make inferences about novel data and provide us with probabilities that reflect the log likelihood that the outputs are accurately translated (Brown, 2003).

There are several drawbacks to this type of system, however.

First, errors are difficult to discover and fix. Related to this problem, SMT systems are very good at providing understandable translations that disguise errors during the translation process. Additionally, when word order matters, SMT systems aren't as accurate. SMT translations between similar western languages are much more successful than translating between a western language and Chinese, for example. Finally, it's difficult for SMT to take into account specific contextual clues regarding a metaphor in one language and correctly translate it into an understandable phrase in the output language (Brown, 1990).

3. Neural Machine Translation and the RNN Encoder-Decoder Approach to Machine Translation

Both IBM and Google have utilized neural networks to great success. Google, specifically, has been a pioneer in the use of a neural network to increase the speed and accuracy of language translation (see Mikolov, 2013 and Sutskever, 2014). More recently, natural language processing has been advancing with hybrid neural networks and SMT approaches. Cho has extensively detailed this newer paradigm in a 2014 paper.

Before we can get into neural machine translation, however, we must discuss what a neural network is.

A neural network is, essentially, a computer system that is designed to function similarly to the human brain's system of neurons. Information is stored and computed in nodes and is propagated to other nodes with a system of edges, or connections to other nodes (neurons) (Sutskever et al. 2014). The internal nodes are considered "hidden". These nodes

are assigned probability weights based on Gaussian distributions. Input is "forward-propagated" through the hidden layers to produce output that is closer to the expected output (Goldberg, 2015).

At its most basic operation level, there are two visible sets of neurons. One set represents the input neurons and the second set represents the output neurons (Goldberg, 2015). The network itself is considered "hidden", a black box where the system of internal processing neurons manage the data to produce outputs. The motivation behind developing a system this way is that the machine teaches itself based on the data it is provided. There is no dependency, like with an SMT, on the functions the machine is provided in its programming

A *Recurrent Neural Network,* or RNN, is a system that maintains an internal, hidden state. This is in contrast with a typical feed-forward neural network which computes the system's state from scratch at every node. RNNs utilize information sequentially which is why they make for good machine translation architectures. Later neuron processing is dependent on what previous neurons have calculated allowing for inputs of arbitrary length. This is the main advantage of designing a machine translation system with an RNN - an input can be of variable size in relation to the output. The variable input is compressed to a fixed-length vector for processing (Cho, 2014).

Here is an excellent graphic demonstrating RNN computation. The variable x represents a given time step through the network, s is each hidden state, o is the output passed to later neurons, and U, V and W represent the parameter matrices that are shared with each neuron:

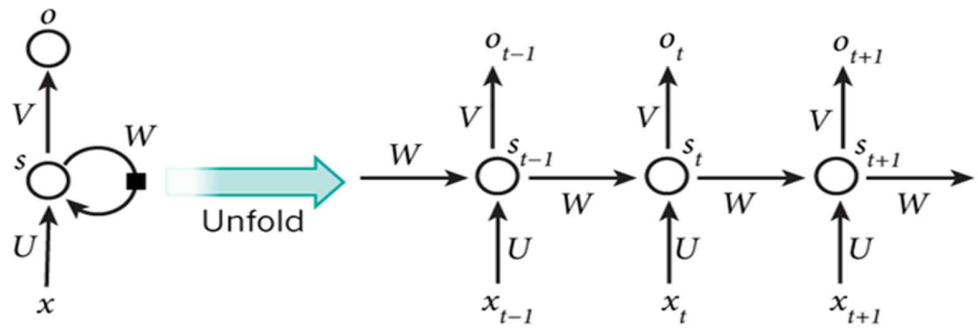


Figure 1: Visual representation of a neural network (LeCun, 2015)

For the purpose of this paper, we have implemented some code in Python demonstrating an RNN. Please assume that this network has already been supplied training data and the data has been compressed into the vector. The x parameter of the run method represents the input sequence vector and returns an output vector that must be decoded into the output language:

```
class recurrent_neural_network:
    def __init__(self, word_dimension, hidden_dimension=100, bptt_truncate=4):
        # Assign instance variables
        self.word_dimemnsion = word_dimension
        self.hidden_dimension = hidden_dimension
        self.bptt_truncate = bptt_truncate
        # With this code we are randomly initializing our U,V and W matrices
        self.U = numpy.random.uniform(-np.sqrt(1./word_dimension), np.sqrt(1./word_dimension), (hidden_dimension, word_dimension))
        self.V = numpy.random.uniform(-np.sqrt(1./hidden_dimension), numpy.sqrt(1./hidden_dimension), (word_dimension, hidden_dimension))
        self.W = numpy.random.uniform(-np.sqrt(1./hidden_dimension), numpy.sqrt(1./hidden_dimension), (hidden_dimension, hidden_dimension))

    def forward_prop(self, x):
        time_steps = len(x)
        states = numpy.zeros((time_steps + 1, self.hidden_dimension))
        states[-1] = numpy.zeros(self.hidden_dimension)
        # Outputs at each time step
        outputs = numpy.zeros((time_steps, self.word_dimension))
        # Iterate through time_steps
        for t in numpy.arange(time_steps):
            states[t] = numpy.tanh(self.U[:,x[t]] + self.W.dot(states[t-1]))
            outputs[t] = numpy.softmax(self.V.dot(s[t]))

        return [outputs, states]


    recurrent_neural_network.forward_prop = forward_prop

    def run(self, x):
        #return highest score
        o,s = self.forward_prop(x)
        return numpy.argmax(o, axis=1)

    recurrent_neural_network.run = run
```

Here is an example of code that encodes input text to a vector that can be supplied to the RNN pictured above:

And finally, here is a method that decodes the prediction values provided by the RNN to actual machine predicted text:

```
def generate_sentence(model):
    # We start the sentence with the start token
    new_sentence = [word_to_index[sentence_start_token]]
    # Repeat until we get an end token
    while not new_sentence[-1] == word_to_index[sentence_end_token]:
        next_word_probs = model.forward_propagation(new_sentence)
        sampled_word = word_to_index[unknown_token]
        # We don't want to sample unknown words
        while sampled_word == word_to_index[unknown_token]:
            samples = numpy.random.multinomial(1, next_word_probs[-1])
            sampled_word = numpy.argmax(samples)
        new_sentence.append(sampled_word)
    sentence_str = [index_to_word[x] for x in new_sentence[1:-1]]
    return sentence_str

num_sentences = 10
sentence_min_length = 7

for i in range(num_sentences):
    sent = []
    # We want long sentences, not sentences with one or two words
    while len(sent) < sentence_min_length:
        sent = generate_sentence(model)
    print " ".join(sent)


model = recurrent_neural_network(vocabulary_size)
```

Cho (2014) has previously proposed a model of machine translation that relies on two recurrent neural networks. This approach, referred to as an RNN Encoder-Decoder model, is described as "[o]ne RNN encodes a sequence of symbols into a fixed length vector representation, and the other decodes the representation into another sequence of symbols" (Cho, 2014).

Similar to the neural networks described above, the encoder and decoder are both "trained" to provide output with the greatest likelihood of an accurate translation from the input. In this proposed model, input and output phrase lengths can differ.

The decoder RNN provides the sequence vector and predicts, probabilistically, what the likely translations are, given the training corpora the system has been provided. Phrase pairs are scored with this probability and the output phrase or sequence is constructed from these likelihood scores (Cho, 2014).

To summarize above Encoder-Decoder model works as depicted in the diagram below,

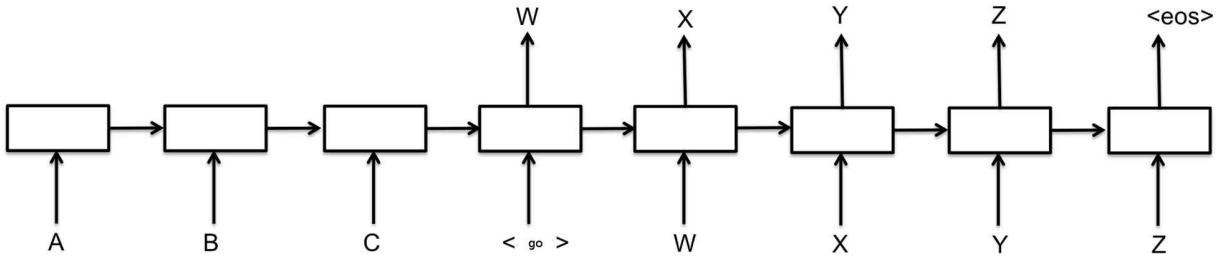


Figure 2: Process of encoder and decoder

Here, "ABC" is the source text and these input units (first 3) comprise the encoder. The following 5 units constitute the decoder for target text ("WXYZ"). RNNs can do the following:

1. Summarize a string into state vector,
2. Predict next word, based on previously processed string (given "AB" able to predict "ABC")

The code described previously, does the second task. For the encoder-decoder model we construct and encoder to do the first task, then we train both the encoder-decoder simultaneously to do the translation. The black boxes in the above diagram are GRU cells (Cho, 2014).

For our implementation, we have used the tensorflow library for GRUcell implementation.

```
def single_cell():
      return tf.contrib.rnn.GRUCell(size)
cell = single_cell()
```

Next, we create a sequence to sequence model as depicted in the code:

```
def seq2seq_f(encoder_inputs, decoder_inputs, do_decode):
      return tf.contrib.legacy_seq2seq.embedding_attention_seq2seq(
          encoder_inputs,
          decoder_inputs,
          cell,
          num_encoder_symbols=source_vocab_size,
          num_decoder_symbols=target_vocab_size,
```

```
          embedding_size=size,
          output_projection=output_projection,
          feed_previous=do_decode,
          dtype=dtype)
```

After training, this architecture is good enough to translate. But we have to train the model for maximum log likelihood (described previously). We use the SGD method for training, see code:

```
# This is the training loop.
    step_time, loss = 0.0, 0.0
    current_step = 0
    previous_losses = []
    while True:
      # Choose a bucket according to data distribution. We pick a random number
      # in [0, 1] and use the corresponding interval in train_buckets_scale.
      random_number_01 = np.random.random_sample()
      bucket_id = min([i for i in xrange(len(train_buckets_scale))
                       if train_buckets_scale[i] > random_number_01])

      # Get a batch and make a step.
      start_time = time.time()
      encoder_inputs, decoder_inputs, target_weights = model.get_batch(
          train_set, bucket_id)
      _, step_loss, _ = model.step(sess, encoder_inputs, decoder_inputs,
                                   target_weights, bucket_id, False)
      step_time += (time.time() - start_time) / FLAGS.steps_per_checkpoint
      loss += step_loss / FLAGS.steps_per_checkpoint
      current_step += 1
```

```
# Decrease learning rate if no improvement was seen over last 3 times.
        if len(previous_losses) > 2 and loss > max(previous_losses[-3:]):
          sess.run(model.learning_rate_decay_op)
        previous_losses.append(loss)
```

The step method (in code above), is derived from the tensorflow library to make a complete step comprising of doing a forward pass, calculating losses, back propagating errors and modifying weights.

```
def step(self, session, encoder_inputs, decoder_inputs, target_weights,
           bucket_id, forward_only):
```

To optimize performance of the code, bucketing is used, which we will ignore for now.

There are some significant drawbacks to the RNN Encoder-Decoder approach. Primarily, there is a drop off after sentences reach a length of 20 words. The BLEU scores drop from between 20 and 25 to eventually below 10 (Cho, 2015). Additionally, there can be significant errors at the end of long sentences (Cho, 2015). The current alignment model that focuses on word for word translations result in very poor output sentences for languages with different grammatical structures. For example, English and German can have very different rules about where nouns and verbs should be present in sentences. This model struggles with translation between these languages.

A quick aside: the Bleu score is a metric proposed by Papieni et al. (2002) that seeks to measure how accurately a machine translated a word by comparing it to a translation performed by a human. Translations are judged by a precision metric which "counts up the number of candidate translation words (unigrams) which occur in any reference translation and then divides by the total number of words in the candidate translation" (Papieni et al. 2002).

Cho (2015) provides an excellent graphic demonstrating the current models of machine translation with SMTs and neural networks:

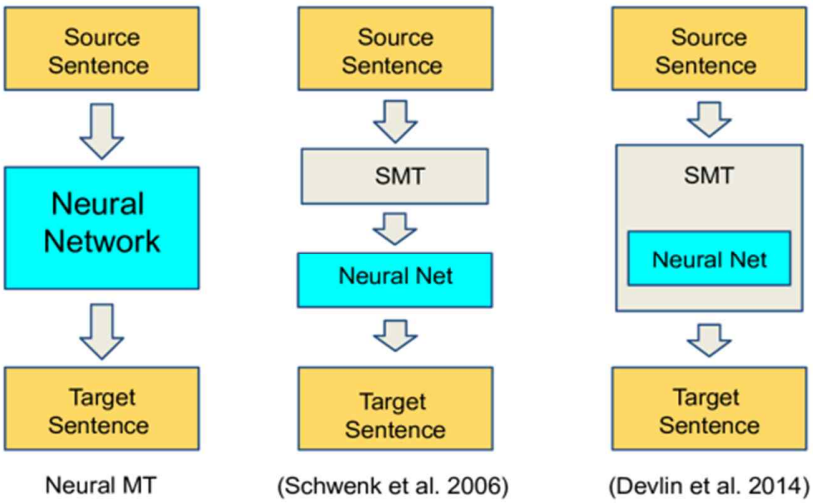


Figure 3: Current models of SMT's and neural networks (Cho 2015)

4. Jointly Learning to Align and Translate

Cho (2015) proposed a potential significant advancement in neural network machine translation over the previously discussed RNN Encoder-Decoder approach. This novel approach, referred to as RNN Encoder-Decoder jointly learning to align and translate, has state-of-the-art advancements that we will discuss at length.

This approach to machine translation depends, much like the earlier proposed system, on two RNNs. Except, the encoder is bidirectional and the decoder is modeled to behave similarly to a search algorithm (Cho, 2015). A context vector is implemented that

depends on "a sequence of annotations… to which an encoder maps the input sentence. Each annotation contains information about the whole input sequence with a strong focus on the parts surrounding the i-th word of the input sequence" (Cho, 2015). The figure to the right is a visual model of the system.

A bidirectional RNN consists of RNN architecture that runs both forward and backward (unlike our code example that only implements forward propagation). Hidden states for both directions are created and concatenated together to form single states. Why would we want to use a bidirectional RNN? Especially in the case of language translation, later words in a sequence are just as useful as the previous words in generating a highly likely output (Goldberg, 2015). The concatenation approach also allows for words to be computed *in context*, so the words are considered with their immediate neighbors.

Here is a brief summary of the concatenation process:

> In this way, the annotation hj contains the summaries of both the preceding words and the following words. Due to the tendency of RNNs to better represent recent inputs, the annotation hj will be focused on the words around xj. This sequence of annotations is used by the decoder and the alignment model later to compute the context vector (Cho, 2015).

The decoder is additionally described as such:

"It should be noted that unlike the existing encoder–decoder approach, here the probability is conditioned on a distinct context vector c(i) for each target word y(i). The context vector c(i) depends on a sequence of annotations (h1, $\cdots$, hTx) to which an encoder maps the input sentence. Each annotation h(i) contains information about the whole input sequence with a strong focus on the parts surrounding the i-th word of the input sequence. The context vector c(i) is, then, computed as a weighted sum of these annotations h1" (Cho, 2015).

The decoder depends on an accurate alignment model that computes a "soft alignment" between the input sequence around a position with the output at a corresponding position. These positions are assessed on how well they match and this score is backpropagated through the network (Cho, 2015). This is precisely how phrases are translated "in context" so that word order isn't as important a factor for the inputs and outputs.

We will discuss the results in greater detail later on, however here we would like to point out some of the advantages the results indicate. First, unlike the RNN Encoder-Decoder approach, the bidirectional approach has no significant drop off in performance after sentence lengths of 20 words. Additionally, the bidirectional approach achieves BLEU scores up to 25% higher than the RNN Encoder-Decoder approach. We also must mention that word and phrase alignment is much better with the proposed architecture. For example, Cho translates from English to French, which can have very different grammatical rules and word alignments. This model handles them superbly. Finally, this implementation will encode into a variable sized vector.

The performance is better for several reasons, including eliminating the fixed vector bottleneck, and removing the need for the RNN to remember the whole sentence as a state in memory (Cho, 2015). The experimental results will prove these hypotheses.

5. Experimental Results

Cho (2015) ran an evaluation experiment to test this idea on an English to French dataset. They compared the performance of the proposed RNN with the previously described RNN Encoder-Decoder architecture. Each model was trained twice with sentences as long as 30 words and sentences as long as 50 words. Here is a graph underscoring the resulting BLEU scores (RNNsearch is the bidirectional jointly learning to align and translate approach):

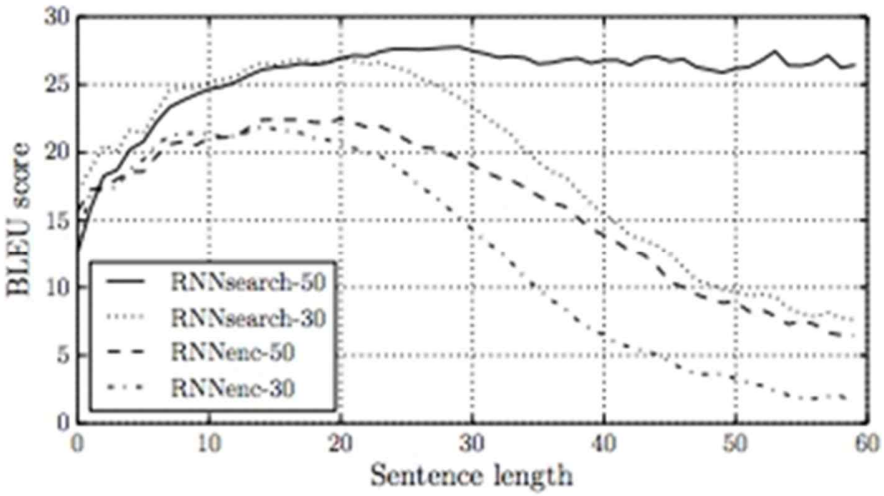


Figure 4: Graph of BLEU score relative to sentence length

The figure above illustrates that performance is generally better for nearly all sentence lengths. Additionally, examining the outputs reveals that words are correctly aligned with their grammatically correct French translations. Cho writes: "we see that the model correctly translates a phrase [European Economic Area] into [zone economique europeen]" (Cho, 2015). The alignment correctly handled this translation by considering the entire phrase at a given location, rather than each individual word.

As was predicted, fixed length vectors create a bottleneck in the translation of long sentences. However, there are other probable reasons why longer sentences have higher BLEU scores. For example, the RNNsearch paradigm "does not require encoding a long sentence into a fixed-length vector perfectly, but only accurately encoding the parts of the input sentence that surround a particular word" (Cho, 2015). The model is able to primarily direct its attention to the information relevant to the production of the next word. All of these aspects work in conjunction to produce excellent log-probability of output translations.

These results would mark a significant leap forward in the development of neural network machine translation. The performance is "comparable to the existing phrase-based statistical machine translation" (Cho, 2015). There is still room for improvement,

however. The systems must be able to translate untrained, novel words- so work toward developing a paradigm is greatly needed.

6. Summary

Machine translation has advanced tremendously in the past few years. Novel methods in statistical approaches have driven much of the improvements. However, in recent years paradigms have emerged that rely on neural network architectures. Neural network architectures, in conjunction with the statistical approaches, have led to explosive growth in machine translation and natural language processing in general. This discussion was focused on summarizing the architecture proposed by Cho (2015). A bidirectional RNN with a variable sized vector, alignment model and decoder that computes output based on context, not just word for word. This approach represents a significant potential advancement in the use of neural networks for machine translation.

As was shown, the experimental results are promising. BLEU scores for the proposed architecture were significantly higher than the other RNN approach. Additionally, BLEU scores did not drop off when sentences were longer than 20 words. Finally, the concluding phrases of output sentences remained high quality based on BLEU scores, also an improvement over the RNN encoder-decoder implementation.

If given more time and resources, using the above created encoder-decoders, this research project would have entailed training our RNNs more using proper datasets that were available. In addition, the research would have attempted to fine tune the translation encoder-decoders similar to Cho (2015).

References

Brown, P., J. Cocke, S. Dell, and A. Pietra. "A STATISTICAL APPROACH TO LANGUAGE TRANSLATION." *Computational Linguistics* 16.2 (1990): 79-85. Web.

Brown, P., S. Della Pietra, V. Della Pietra, R. Mercer. "The Mathematics of Statistical Machine Translation: Parameter Estimation." *Computational Linguistics* 19.2 (1993): 263-311. Web.

Dzmitry Bahdanau, Kyunghyun Cho: "Neural Machine Translation by Jointly Learning to Align and Translate", 2014; [http://arxiv.org/abs/1409.0473 arXiv:1409.0473].

Ilya Sutskever, Oriol Vinyals: "Sequence to Sequence Learning with Neural Networks", 2014; [http://arxiv.org/abs/1409.3215 arXiv:1409.3215].

Kyunghyun Cho, Bart van Merrienboer, Caglar Gulcehre, Dzmitry Bahdanau, Fethi Bougares, Holger Schwenk: "Learning Phrase Representations using RNN Encoder-Decoder for Statistical Machine Translation", 2014; [http://arxiv.org/abs/1406.1078 arXiv:1406.1078].

Kyunghyun Cho, Bahdanau, D.: "Neural Machine Translation by Jointly Learning to Align and Translate", 2015; [http://arxiv.org/abs/1409.0473 arXiv:1409.0473].

Mikolov, T., V. Le Quoc., I. Sutskever. "Exploiting Similarities among Languages for Machine Translation."

Papieni, K., S. Roukos, T. Ward, W. Zhu. "BLEU: a Method for Automatic Evaluation of Machine Translation." *Computational Linguistics* (2002): 311-318. Web.

Tomas Mikolov, Quoc V. Le: "Exploiting Similarities among Languages for Machine Translation", 2013; [http://arxiv.org/abs/1309.4168 arXiv:1309.4168].

Yoav Goldberg: "A Primer on Neural Network Models for Natural Language Processing", 2015; [http://arxiv.org/abs/1510.00726 arXiv:1510.00726].

Y. LeCun, Bengio, Y., Geoffrey, H. "Deep Learning." *Nature* (2015): 436-444. Web.

Blockchain in Food Supply Chain

Jin Young Kim
Athenian School

Abstract

This paper provides a review of the use of blockchain in food supply chain. A food supply chain involves the process of production followed by processing, distribution, retailing and finally consumption. Food supply chain has been becoming complex with the movement of people for work across the globe. Due to the migration of people, the demand for food products from across the globe is now quite common. A food supply chain comprises of different products and companies operating in different markets spread across the globe and selling a variety of products. The chain is significantly affected by the regulatory environment in which it works. Any food supply chain connects the agricultural sector, food processing sector and the distribution sector. With the rapidly changing economic environment, the biggest challenge that has come up is to provide sustainability of food supply. Contaminated food due to fraud in the food business is becoming a common phenomenon. Food quality and security are the most important factors in a food supply chain. Food supply chain security is increasingly becoming challenging due to a number of actors involved. This paper provides an insight on how blockchain technology can help overcome the complexities of food supply chain.

Some of the benefits of blockchain technology for enhancing management of the food supply chain include: 1) reduction or elimination of fraud and errors, 2) reduced delays from paperwork, 3) improved inventory management, 4) identifying issues more rapidly, 5) improved traceability, 6) improved food regulation and safety, 7) improved food security, 8) reduced food wastage and 9) increased consumer and partner trust. In spite of their usefulness, majority of the blockchain systems are still in proof-of-concept or controlled pilot phase.

1. Introduction – what is food supply chain?

The rice on your plate reaches you through a network of distributors/retailers after it is harvested by the farmer. A food supply chain is a process wherein the food produced by farmers is delivered to our tables. A food supply chain involves the process of production

followed by processing, distribution, retailing and finally consumption. It comprises the network of stakeholders (Carlos and Graham, 2010).

The main parties in a food supply chain are:

1. Farmer or food producers – Producers or farmers are those people who produce food and supply in a raw form such as wheat, rice, cereals, fish, poultry so on. These include small farmers as well as large corporations engaged in farming.
2. Processor – These are entities that purchase the produce from farmers and convert them into products that meet consumer demands.
3. Retailers & Distributors – Distributors are those corporates that act as a link between the producers and markets or between processors and markets. They ensure distribution of food through various channels to the final consumer. They buy in bulk and sell as per the requirements of consumers. They form an important part of food supply chain especially when the food is being distributed across the globe. This is so as they deal with local regulations. Retailers are those entities that showcase the product to end consumer. The products offered by food sector are showcased by retail outlets such as a local shop or a supermarket.
4. Consumers – People like you and me who shop, purchase and consume food.
5. Government, regulators – They ensure fairness by monitoring the entire food supply chain.

To understand it better take, for example, the chips we eat. Pringles would buy potatoes from farmers, process them to make chips, and finally, it would pass through distributors and retailers such as JD Distributors, WalMart etc before it reaches us (Carlos and Graham, 2010).

As shown below in the diagram, food moves from farmer to processor then to distributor and retailer before it reaches the final consumer, whereas money moves from the consumer to retailer to distributor and finally to farmer.

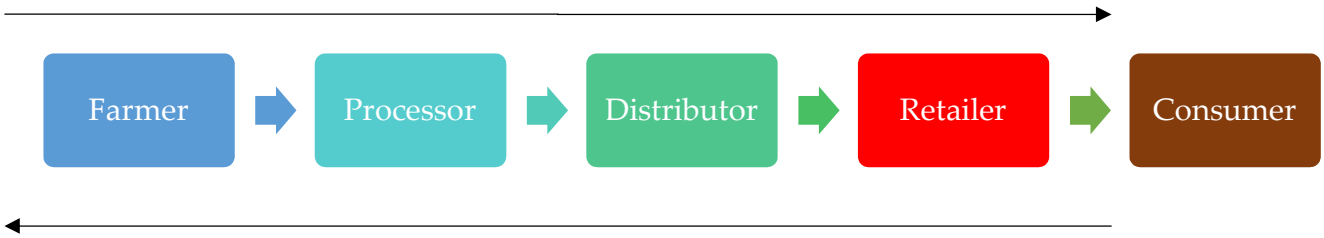


***Figure 1**: A Visualization of Food Supply Chain*

Obviously, this food chain is affected by the consumer's demand for food as well as the supply of food by producers. So here the producers, that is, the farmers would push food whereas the consumers would push the money. So, if there is any weakness in producers pushes for food or consumer's push for money then food supply chain might get interrupted.

2. How does current food supply chain work?

Food supply chain has been becoming complex with the movement of people for work across the globe. Due to the migration of people, the demand for food products from across the globe is now quite common. For example, with so many Asian migrants specifically, migrants from China and India settled in the US the demand for Indian spices as well as Chinese food in the US such as sea cucumber has gone up.

It is quite common nowadays for food to travel across the globe before it reaches consumers. For example, fish caught in the Indian Ocean is frozen and sent to the US for processing where it would be defrosted filleted repacked and sent to Europe for consumption.

To understand the complexity of food supply chain in today's world can be understood with few examples:

1. India is the largest producer of spices in the world but demand for spices is across the globe specifically from countries such as UAE, US Europe as well as few countries in Asia such as Malaysia.
2. Buffalo milk is produced the most in Asia continent, but it finds consumers in Italy too (Mozzarella cheese) after India and Pakistan.
3. Tomatoes are largely produced by Mexico, North Africa, Spain, China and France but consumed the most in the US, European Union

Thus, over the years, development of better transport, increasing travel across the globe and increase in a number of migrants has led to the development of complex food chain. Any food supply chain across the globe would aim to satisfy the demand of consumers and secondly ensure that it is economically sustainable.

For any food supply chain to work efficiently it is necessary that it has following elements:

1. The food quality,
2. Minimum food wastage,
3. Food safety
4. Supply chain efficiency

A food supply chain comprises of different products and companies operating in different markets spread across the globe and selling a variety of products. The chain is significantly affected by the regulatory environment in which it works. Any food supply chain would connect the agricultural sector, food processing sector and the distribution sector (Carlos and Graham, 2010).

In terms of sectors, any food supply chain involves three major sectors. They are -:

1. Agricultural sector
2. Food processing industry and
3. Distribution sector

Agricultural sector comprises of farmers who grow crops and also includes the raising of livestock. Agricultural produces different commodities resulting in diverse distribution channels. As mentioned earlier this sector would sell their produce to the food processing

industry or directly to end consumers or retailers. Also, they sometimes consume the produce directly.

The food processing industry in any country is varied and comprises a different type of activities. For example: refining of products such as sugar, milling of produce such as cereals, drying, cutting and cleaning of vegetables and fruits. Each of the inputs is then processed at different degrees based on the requirements and then packaged and sold to customers.

Apart from processing the food, the food industry also carries out market and product research. This activity results in the development of new products. Apart from this, they also engage in the marketing of the products and create awareness among consumers about their products. The distribution sector especially the retail sector is the main passage for food products. It is also the final link in the supply chain, as it interacts directly with end consumers. While the retail sector's main activity is the sale of products, but they also carry out promotional activities for the processor.

We can actually divide the food chains into different types. The major types of food chains are:

1. Producer focused chain – In this kind of supply chain, Producers sell to the processors all their produce. This supply chain will typically have few buyers but many sellers. Generally, the raw materials purchased from the farmers are at a pre-determined price.
2. Consumer-driven value chains – Here the number of buyers is more. This supply chain is increasingly becoming popular due to growing awareness and concerns about food security (Dani, 2015).

3. Factors influencing food supply chain

With the rapidly changing economic environment, the biggest challenge that has come up is to provide sustainability of food supply. The biggest task is to ensure food security which is endangered due to rapidly rising population, limited access to food intake, volatility in prices and regulations imposed especially in developing countries such as India and China and also in the poor and underdeveloped countries such as Swaziland (Dani, 2015).

The major influencers of any food supply chain are:

1. Consumers;
2. Agricultural produce;
3. Governmental and non-governmental agencies;
4. Technology;
5. Logistic companies
6. Food Quality
7. Consumer as well market choices and
    i. Small companies providing secondary value.

Consumers are the biggest influencers in a food supply chain. The demand for food would purely depend on them. Consumers now days prefer food that is not only safe but also

high in terms of quality. Consumer demand for food is also influenced by other factors such as social justice, environmental concerns, labor conditions, work ethics etc.

With the advent of Internet and ease of availability of information the consumer has become more informed and empowered. They now ask questions and are curious to know:

1. How the food was grown,
2. What kind of processing was done,
3. Was it stored in safe and hygienic conditions or not?
4. Is the food detrimental to Environment?
5. Is there any kind of ethical issue when it comes to the supply chain?

For example, a mother is interested to know the tomato puree she is buying for her children is safe to consume, contains no GMOs or pesticides and was grown in a favorable socio-environment. Manufacturers, distributors, and retailers have experienced a significant impact on the demand when even one issue wasn't addressed by them or was handled in a poor manner.

Post Consumers Regulation is another factor that influences the food supply chain. Regulations are enacted for protecting consumers, ensuring their safety and warranting compliance with the environmental norms. Regulations ensure that proper resources are allocated, and right efforts invested in random checks and audits of various food processing companies.

Apart from consumers and regulations, information technology now-days too has an impact on food supply chain. IT links individual parts of the supply chain and helps in smooth functioning of the entire system. Technological innovations significantly impact the food supply chain and make the processing industries to rethink on fulfillment & effectiveness parameters.

With the advent of blockchain and smart contracts, we now can have fridges that would inform all related parties to food contracts about its functioning and the conditions at which food and the contracts will execute based on what this mute device has to say.

Food quality also one of the most important factors in a food supply chain. The demand for food nowadays is directly proportional to the quality of food provided. More than half of consumers around the world are concerned about quality as well as the safety of food.

Billions of dollars are being pumped by processing industry to ensure quality and in advertisement & marketing. This is so as every brand wish to ensure consumers associate quality with the brand (Dani, 2015).

4. Common problems of food supply chains

As the complexity of our food supply grows so does the possibilities of food-related fraud. Adulteration or counterfeiting food for financial gains is not new and has been in practice for ages. As per a report by PWC, food fraud losses are estimated to be $40 billion every year. With the advent of globalization and supply chain becoming more and more complex fraudsters can do more fraud and damage the supply chain (Shirani, 2013).

The major issues faced by a global food supply chain are:

1. Traceability

Consumers nowadays demand traceability of the food they consume. This demand has been growing stronger and stronger with the passage of time. If food were traceable, it would lead to lesser production as well as the distribution of poor food or food that is unsafe for consumption. As of today, the food labeling system prevalent across the globe is not good enough to provide an assurance for the food in terms of its safety as well as quality.

However, traceability is not that easy as it sounds. If a product says for example Milk passes through many steps, then it wouldn't be possible to keep checks on each and every step. Even if checks are introduced at each step then it would slow down the process of distribution considerably and also lead to increased cost of the product.

Consumers feel an urge to trace their food just as they have a tracking system for every activity of their life such as a number of steps we've taken, heart rate, shipping packages, etc. Innovations have made traceability possible. For example, nanochips implants help us to trace as well as track the food, the case or the carrier of the food and even the consumer. Similarly, smart carts help in the automatic checkout of consumers from a retail shop.

Today we have smart refrigerators that trace when an item is running low – ex Juice carton and has the capability of automatically ordering it through use of the internet. With such innovations, consumers now demand a system which would help them to trace as well track the food as it lows globally from one place to another. For example, using a smartphone we could trace the source of foods and also other value-added information.

Technology in future would be smart as well as intelligent. It will help consumers to trace test foods as well as they move the value chain. However, it is not an easy task and would still require years of research before technology become intelligent enough to trace the food on our plate and inform each detail about it.

2. Transparency

A very popular issue found in transparency is when one country let's say country A bans or impose high tariff on goods from another country that is country B. In such scenario country B sends its goods to country C. IN country C the product is rebranded, repackaged and sold in country A. This is the most common fraud found in the food supply chain system. When any processing company behaves in such a manner then the trust of the consumer is broken and hence transparency is the key to a food supply chain.

A survey done in the year 2016 by Label insight indicated that 94% of the respondents believed that the manufacturers who sell the product and the brands they buy should be transparent about the food. They should clearly tell the consumers what is there in the food and how it was made. Transparency helps to create consumer trust as well as brand loyalty (Levinson, 2010).

As of now, it is not legally necessary to disclose all details about the food manufactured and sold by them. However, Consumers demand transparency and hence it becomes necessary to share the information.

The problem arises when a manufacturer is unable to print everything on the package. He has too much information to be printed on the package which is not possible. However, this problem can be addressed with the innovative solutions. For examples, nowadays manufacturers provide QR codes on packages. These QR codes when clicked helps to link to online product profile of the product and consumer can get all detailed information about the product. From details about the ingredients used in the product to the history about the

company as well the product to photos of the people who were behind the product and relevant certifications, all such relevant information can be provided through QR codes.

Apart from that dedicated helpline numbers are also provided on the packages that provide the information about the product and helps to solve queries raised by the consumer when he dials in.

A producer can share their unique story about the product through QR enhanced labels. These labels act as a bridge between on-package and the online data available to a consumer. It also helps a manufacturer to connect with the consumer virtually and create a relationship specifically when physical face to face meeting is not possible.

When a company or a brand can do such type of communication then they are able to open different possibilities for themselves. It helps them to enhance their brand, increase demand for the product as well as enhance the respect for the brand.

3. Communication between actors

To trace any kind of food the biggest challenged faced as of today is the fragmented nature of the food supply chain. There are various actors involved in a food supply chain that is spread across the globe and either have very less information about other actor or no knowledge about another actor.

For example, a burger would have meat, lettuce, mayonnaise and other items. So when a consumer traces a burger it will have to trace various actors that lettuce producer, meat provider etc. These actors would have no knowledge of others.

In such scenario, it becomes important that communication among suppliers is prioritized by stakeholders. This could be done by implementing various traceability solutions or otherwise, the stakeholders can ensure that they engage only trustworthy suppliers.

This will help both the consumer and also the producers/processors of the food. This is so as the communication will ensure traceability which in turn will ensure that the reputation of the producer/processor is maintained.

4. Organized crime in the food supply chain

Various raids have from time to time revealed presence of organized criminals in the food industry. OPSON V which was carried out, for example, led to the seizure of more than 10,000 tonnes of hazardous food and more than 1.4 liters of fake foods and drinks.

This has necessitated the need for deploying additional resources across the globe for combating such crimes. This is a major challenge currently for the food supply chain

5. Food security

As the global population keeps increasing and is estimated to cross the 9-billion mark in coming years, it has become important for all countries to ensure food security for their population. Common threats to a supply chain security are theft terrorism, adulteration, sabotage, smuggling, et cetera.

Supply chain security is relevant to the food industry. This is so as the industry supply foods that are ultimately consumed by humans. If anything goes wrong, it will become a significant threat to millions of human lives as well on the standard of living (Shirani, 2013). Supply chain security is increasingly becoming challenging due to a number of actors involved. For example, a large grocery store in a country like the US would have around 30,000 plus suppliers which would be a mix of local as well international suppliers.

Managing and maintaining the security of the food supply chain is not a small task. Various organizations such as International organization for Standardization (ISO) have taken initiatives to ensure supply chain security. For example, they introduced ISO 28000 that specifically deals with supply chain security. In the US, the FDA Safety Modernization Act (FSMA) of 2011 was instituted by the Food and Drug Administration (FDA) to better the safety of the food supply chain.

However, to ensure supply chain security any processor should have few minimum-security criteria such as:

a. Employee identification system to ensure personnel security
b. Ensuring all containers and trailers go through a proper security & inspection procedure. Steps such as reporting and controlling unauthorized entry into containers/trailers sections, managing all entries into container/trailer areas on a regular basis, correct sealing, and putting up reliable locking mechanisms and doors should be systematically followed.
c. Ensuring that secured procedures are followed when it comes to transportation, storage, and handling of cargo.
d. Control of documentation. The processor must ensure that cargo documents are accurate and legible. Any cargo coming inside or going outside should be verified through purchase and delivery orders. One must also ensure that the drivers are positively identified.
e. Apart from above-mentioned security steps, the processor must maintain adequate securities at the warehouse. Facilities must set up physical hindrances and deterrents, such as alarm systems, fencing, gates, proper lighting, secured parking, locking systems and video surveillance.
f. Most important thing is to maintain IT security. This can be done by implementing various IT security procedures and policies, such as password protection, authorized access and also proper training to concerned employees.

6. Food regulation and safety

Stringent legislations are needed when it comes to food supply chain. When the legislation is strong it acts as a deterrent to organized crime which is currently prevalent in the food industry.

When it comes to food safety, it involves a variety of practices that are intended to prevent any foodborne illness. As of now, ISO 22000 is the standard that deals with food safety. It was developed by International organization for standardization. ISO 22000 sets out the necessities for food safety management. It ensures that any organization that is awarded this certification has the capability to control food safety hazards. This certification can be used by any organization irrespective of their size and position in the supply chain. Many firms use this certification and implement prerequisite programs and HACCP. Firms also go for FSSC 22000 certification and it is granted after a third-party audit. The audit done verifies if the company complies with the requirements of the FSC 22000 standard.

Apart from this, every country across the globe are updating as well modernizing legislation related to food safety. Not only the food safety regulations becoming more transparent but now they are aligning to across border to ensure the free flow of goods across the globe (Hutter, 2011).

A few steps taken by different countries are:

a. US have enacted the Food Safety Modernization Act (FSMA). This act addresses the way food safety is regulated. It has allowed FDA sweeping powers to monitor the private sector regarding food safety issues.
b. Canada has enacted Safe Food for Canadians Act (SFCA). This act was enacted to strengthen food safety rules, provided new ways for food inspectors as well as laboratories to operate effectively and to keep consumers updated on food safety issues.
c. European food safety authority (EFSA) is the risk assessment body for food safety of the European Union (EU). It provides advice as well communication on existing as well as emerging risks. It works in close collaboration with the national authorities of EU nations.
d. When it comes to Australia and New Zealand they have Food Standards Australia New Zealand agency that develops as well as administers the Australia New Zealand Food Standards Code.
e. China has its China Food and drug administration (CFDA). CFDA ensures comprehensive supervision on safety management of food, health food as well as cosmetics and drugs.
f. While India has Food Safety and Standards Authority of India (FSSAI). It was established in the year 2011 under the Food Safety and Standards Act, 2006 which is a consolidating statute related to food safety and regulation in India. FSSAI is mainly responsible for protecting and promoting public health through the regulation and supervision of food safety.

In spite of the above prevalent acts, high scale food fraud does take place across the world.

7. Wastage

Food loss or food wastage is wastage of resources such as water, land, energy and also other natural resources. The level of losses would differ for each of the food.

Food loss happens due to the fault of the food production and supply system or its institutional and policy framework. This might happen due to various limitations related to the managerial and technical skills. For example, improper storage facilities, cold chain, improper food handling practices, lack of infrastructure, incorrect packaging, or efficient marketing systems.

Food waste, on the other hand, refers to the removal of the food from the food supply chain. The food is still fit for human consumption. This is done either by choice of the consumer or due to contamination of the food or food getting expired due to poor stock management or neglect.

Ideally, Food waste typically but not exclusively occurs at the retail and consumer stages when food loss occurs at the earlier stages of the food supply chain – in the course of production, post-harvesting, and processing stages.

Although we haven't been able to quantify correctly the amount of food wastage that is happening across the globe few estimates say that almost half of the total food produced is wasted even before it reaches the final consumer. In a food supply chain, food wastage would occur at different points. This happens as food is subject to degradation over the time period.

If we are able to reduce the losses as well wastages in the food supply chain then it will be an effective solution for reducing the environmental impacts of agriculture, improving the income and livelihood of various actors and improve food as well as the nutrition security for low-income consumers.

If we wish to reduce the environmental impacts of agricultural we need to utilize the food supply chain as and solution to reduce loss and wastages. To ensure that there is no or minimum food wastage or food loss we need to develop efficient solutions by interlinking different stages in food supply chain. As food supply chain becomes complex so we need to shun the traditional approach and adopt a modern approach towards food wastage (Hutter, 2011).

Few tried and tested ways to ensure the loss is minimized are:

a. Investing and implementing in low cost and sustainable processing technologies
b. Ensuring adequate storage solutions
c. Increasing the efficiency of the food chain

8. Legislation

Although governments across the world are increasingly ensuring food safety through various enactments there is a need for addressing the food fraud that is happening across the globe separately. Apart from that, there is a need for strong legislation in other areas such as food labeling.

5. Food supply chain – what lies ahead?

Let's understand what lies ahead for various stakeholders in the food supply chain industry (Leadley, 2015):

1. Producers

With the growth of developing countries such as China and India, the demand for protein-rich diet would increase and this would require the producers to double the food production. This would be a big challenge especially with increasing climate change, solid degradation, scarcity of resources such as water.

Changing environment and unpredictability of climate has led to highly volatile input costs as well as the selling price. This has made farming extremely difficult in today's environment and also made production cycles longer. Farmers' in future will have to be more adaptive to risk management. This can be done by farming across different types of weather, hedging against price movements, getting proper insurance, ensuring alternative income through the growth of fruit-bearing trees etc.

If today's producers speak about subsidy and surplus, future producers would deal with shortages and a lack of security. The future would call for efficiency, which would be achievable only through more collaboration among the actors of the food supply chain.

With so much change in the environment, farmers would have to be more innovative in their ways of farming. Extensive farm research would be required for increasing efficiency meeting new demands of the consumers.

Value chain collaboration would be required to ensure innovative ways of farming are used. Value chain collaboration would help in understanding the demand of consumer; their

changing preferences on one hand and on other hand collaboration with manufacturers of pesticides, insecticides would help in increasing the yield of crops.

2. Processors

With the expansion of population, food processors will have to ensure that their productivity is enhanced in the near future. Future requires processors to not only adapt to changing consumer preferences, demographics but also to the complex food supply chain.

Significant changes would be required in the near future to support the food value chain. Processors would be required to change their supply chain, product lines and also distribution channels. They would be expected to meet the new consumer demands due to growing health awareness, diverse diets etc. Processors would require strong partnerships with not only producers but also with retailers.

In future, developing economies will be the drivers of growing demand for food. Processors need to adopt new ways to produce and distribute food to such a population. With the increase in international trade, processors will have to ensure proper collaborations are made and diversity is adopted in the food processed.

In order to sustain as well grow in these developing economies, processors would require securing market channels, acquiring relevant new assets, considering mergers, or entering into a joint venture with relevant entities.

Processors would be faced with the problem of complex supply chains in these economies as well as poor infrastructure.

With growing concerns about food safety processors need to ensure that proper procedures are followed to maintain public confidence in their brand. For this future requires processors to secure their supply chain, enhance product labels and traceability of product sold by them. Proper compliance systems would be needed in all those geographies where the product of the processor would be consumed.

Processors would further need to ensure transparency by using proper tracking technologies. This would require extensive collaboration would be required to ensure that the systems operate efficiently.

Apart from that processors would need to work on the efficient use of carbon-based fuels to ensure minimum carbon footprint. Many processors will have to work on reducing their carbon footprint and ensure setting up clear energy usage goals.

Processors would also require keeping waste management as one of the top priority. With Plastics and related product becoming a serious threat to environment Processors would require managing their waste more efficiently. Innovativeness and relevant tie-ups with private players as well as government would be needed to manage waste.

3. Distributors and retailers

Distribution and retail industry is highly competitive. Today consumers can choose from a wide number of retail outlets. Hence it requires retailers to keep on distinguishing themselves from their peers.

Future would require retailers to monitor on continuous basis consumer trends and capitalize on them. It would be required understand the willingness of consumers to pay for a product that is different from others coupled with high quality.

In future retailers would be required to continuously experiment new retail channels, formats and keep customizing their portfolio as per the local tastes and preferences. For

example, if Walmart wishes to be successful in a country like India then it will have to not only adapt to local needs but also ensure local tastes are taken care of.

Retailers would also require balancing between the cost of a customizable and dispersed supply chain and the benefits of providing the consumer with a wide variety of food products.

Retailers in future will have to understand the ever-growing importance of e-commerce too. More and more people would be engaged in online grocery shopping. Availability of the facility of online shopping would enhance the reputation of the retailer in eyes of the consumer. It has been researched and proved that retailers having an online channel that is popular tend to perform better even in their physical stores (Leadley, 2015).

To have an online presence retailer would be required to work on innovative solutions to ensure cost-effective logistics leveraging of online sales channels. To ensure growth in online grocery stores retailers would need to ensure factors such as:

a. Low delivery costs;
b. Easily accessible pick-up points
c. Highly punctual delivery

For this, retailers would also require collaborating vertically as well horizontally. They would have taken initiatives such as putting joint effort into warehouse operations, joint inventory management, order management, and fulfillment; creation and operation of online stores; and providing home delivery.

Retailers would also be required to carry out a significant number of sizable M&A. The initiatives especially in the online retail market, with mergers and acquisitions, retailers would be able to broaden their product ranges while sharing operational processes and thus enjoy the advantages of an online sales channel with reduced effort and cost.

Just like processors, even retailers would need to address the issue f packaging in coming years. A research indicates that 50% of decisions made by consumers are based on how innovative and differentiated packaging is provided. This differentiating effect that is created by packaging helps in not only communicating brand information to shoppers but also helps in driving in-store sales.

Packaging offers retailers value-added functionality. For example, it helps in active packaging, smart tagging etc. for example if there is odor absorbing pad in a fish package then it can help in distinguishing products from each other and influence the buying behavior of the consumer. Smart tags on other involve the use of sensors to keep track of freshness of product in the entire food value chain. These indicators are available not only to sellers but also to consumers.

Retailers will have to adopt innovative and less taxing packaging in future. Many retailers have already moved towards sustainability initiatives such as recycling, energy saving etc. Retailers need to capitalize on these initiatives as it will enable them to save cost in a significant manner and differentiate themselves from competitors.

4. Consumers

As highlighted earlier, today's consumer is concerned about food safety, price as well as food security. Apart from that, they are forced to face problems such as high prices, adulterated foods, food riots, genetically modified foods etc. Consumers would have to face high food prices and food security issues in future. Lack of adequate water, the adequate land has resulted in demand exceeding supply. This has resulted in growing concerns across the

nation to feed the ever-increasing population. As more and more people would soon be part of the middle-class income group there would be more demand for high-value foods but additional pressure production.

The retail price of food items is set to rise due to high energy price resulting in high cost of production and increased transport costs. This would force consumers to be selective in their purchases and settle for cheap locally made food instead of organic foods, imported foods, store-prepared foods, or specialty foods. This would also affect retailers, processor as well as producers. They will have to come with smaller size packs, more functional foods, and efficient marketing to emphasize the value of their product to end consumer.

With developing countries becoming more affluent, consumers would increasingly move to a healthier lifestyle and adopt changes in their diet accordingly. Producers, processors are already seeing a move towards high protein food and a developing dislike towards fatty and sugary foods.

With more and more consumers facing obesity, high blood pressure, cholesterol problems due to a sedentary lifestyle which involves sitting at a desk for long hours, less walks and more use of cars, bikes etc producers and processors will have to come up with healthier products. They would see demand for such products rising and subsequent change in consumer patterns and lifestyles.

Producers and processors will also be forced to label their food as junk or non-junk food due to new legislation and interventions of governments where they sell their product.

As the food has become global so has the risk of contamination. Today consumers are not only concerned with contamination, bacteria E. coli but they are also worried about farming practices adopted by the producer, use of pesticides, food handling, additives and preservatives used by the processor. This has resulted in more demand for transparency which includes the origin of food, the content of food, preservatives used etc. Consumers not only now but in future too would be careful as to what goes into their stomach. They will not be satisfied with a plain label such as Made in the US with domestic as well as imported ingredients.

Producers, as well as processors, will have to adapt themselves to such growing consumer concerns.

Processors will have to additionally teach consumers as to how the food should be cooked before consumption to avoid any contamination during cooking. Pamphlets distribution at retailer stores, advertisement and proper labeling on packages would help producers/processors reduce food-borne illness (Levinson, 2010).

5. Regulators

As the food markets globalize to feed an ever-increasing affluent population the role of regulators becomes important.

With the movement of people across the globe and technological advancements, regulators are faced with new challenges as well opportunities. The traditional regulatory response would now have to be changed as food is produced and distributed at global scale. Regulators would see newer relationships developing among the public and the private sector in the food value chain.

The foremost issued that regulators would have to address is changing relationships between the food importing and food exporting nations. Today each and every country is sourcing food from various other countries based on local demand. Regulators would have

to ensure that food supply is secured. Producers and processors, on one hand, are experiencing lower tariff while on the other hand are experiencing non-tariff barriers.

Producers and processors, especially from small less developed countries who import to developed economies, are facing stringent certification standards, quality issues, labeling as well as are required to meet strict technical necessities.

On one hand producers and processor face such strict rules laid by regulators in developed nations and on another hand they face inconsistent national rules and regulations in developing and under-developed economies.

Most of the rules and regulations set in these developing and underdeveloped economies aren't harmonized with global rules. Apart from that regulator in such countries often face the problem of lack of resources resulting in an inadequate number of the food quality certification bodies. Regulators of such countries often levy export taxes, inspection requirements as they are accustomed to requirements of large buyers.

Many times they have imposed export quota resulting in a shock to world's commodity markets.

Regulators would also have to adapt themselves to increasing complexity of trade relationships. As there would be a surge of global trade among developing nations such as BRICS, regulators from such countries would have to align rules and regulations with the entire world.

With the improvement in purchasing power of emerging nations as well as the development of the efficient marketing channels, MNCs would have access to new sources of supply of food. Regulators need to ensure that more and more cooperative agreements are signed among MNC and governmental organizations. This will help in building a sustainable food supply chain. It will also help in integrating small farmers, improve transport infrastructure of the country and reduce the food security risk.

ON the other hand, regulators in the importing countries will have to gear up to support imports from new suppliers that belong to emerging economies. They will also have to support capacity-building for compliance with standards, certifications and safety, labeling, and other requirements.

In next decade we would see that major developing countries would become global drivers of both food consumption and production. With this development, many of such countries are already reconsidering multilateral agreements like WTO and expanding their bilateral trade relationships. This is done by them to maintain constant supplies and reduce unnecessary disruptions from their trading partners.

Regulators in future would also have to face another burning issue that is agro/bioterrorism infrastructure.

Regulator of any country would have the most important responsibility of sustaining consistent and reliable distribution of safe food. This has become important with outbreaks of food-illness in past. Regulators would be required to take steps to assure consumers that the food consumed by them is safe. It has now become very common for any food-borne illness to spread on a global basis unlike in past where it used to be restricted to a region or nation. To counter these many regulators have adopted highly stringent and sophisticated food regulatory systems. One example of such regulator is the US. However, US is seen worst outbreaks of food-related illness.

Regulators in the U.S. are leading food safety and traceability campaigns, resulting in the establishment of the world-renowned Centre for Produce Safety, a public-private

partnership with UC Davis. The US also ensured harmonization of food standards by multilateral organizations and food industries. This was done with an aim to strengthen food safety worldwide. They also have organizations such as the U.S. Animal and Plant Health Inspection Service work to protect agriculture from plant and animal pests and diseases. This organization works with international trading partners to address problems that can spread across the borders, from one location to another.

It also ensures utilizing the services of certifiers and capable third-party auditors, which is compatible with the global trade practices such as Global GAP. Regulators across the world would have to adopt such steps in future to safeguard their population against any potential foodborne illness.

Regulators in future would also have to face the growing threat of agro/bioterrorism. The world has seen growing attacks against agriculture infrastructure and the food supply system. Such an agro-terrorist attack has the capability of creating major economic crises in the agricultural sector and also, loss of confidence in the ability of regulators to protect the health and welfare of their populace. Various countries have been adopting step to counter this issue. For example, U.S. Food and Drug Administration (FDA) has teamed up with Customs and Border Protection to staff the Department of Homeland Security National Targeting Centre to perform risk analysis and target suspicious food imports.

One cannot forget the 2008 milk contamination scandal. It highlighted the inability of China as a nation to ensure proper food safety. Such inabilities of developing nations are a growing concern (Levinson, 2010). In the year 2008, we saw the milk contamination scandals were caused by the toxic chemical melamine. The exposure resulted in global recalls and bans on products made with Chinese dairy ingredients.

Again in 2011, we saw the use of leather hydrolyzed protein to boost milk prices, led to the closure of half of China's dairies. It's not just the developing nations even the developed nations experience challenges and deaths due to food safety; for instance, as a result of E. coli poisoning as seen in beef, processed foods and vegetables in the United States, and fenugreek sprouts in Germany.

Regulators would also be faced with rising issues of land acquisition by rich investors. In past, we saw investors getting attracted towards the acquisition of land used for farming due to rising commodity prices and an evident shortage of land, water and other resources that will occur in future.

Research done by Deloitte has estimated that at least 50 million hectares of the agricultural land—enough to feed 50 million families in India—have been transferred from family farmers to corporations since 2008.

Although there are advantages of such acquisitions, one cannot ignore potential threats of such acquisitions such as employment of local people, sustainable use of resources, ensuring proper food security for the local population. If a government acquires such land the issues such as sovereignty, acquisition of land grabbing and insensitivity. Responsible Agricultural Investment that Respect Rights, Livelihoods, and Resources (RAI) is an effort of the World Bank to ensure fair play when investors acquire such large farmlands.

The trend of global land acquisition is not going to die. Regulators would have to prepare themselves for ensuring the resilience of their food supplies and ensuring a level playing field for local investors. Regulators would have to provide sustainable policies for acquiring farmland as well a consistent stand on its acquisition of land.

6. Background of blockchain technology

Blockchain has been referred to as a decentralized system or a distributed ledger on which series of transactions can be recorded. A transaction ledger is maintained all over a nexus of unrelated servers or computers mainly called “nodes” simultaneously. The transaction ledger is capable of duplicating thousands of transactions across this network of computers. The ledger contains complete record (the chain) of transactions that were performed. These transactions are grouped into blocks.

A block gets added to the chain if the nodes are members in the blockchain network. With high levels of computing power, they reach consensus on the next ‘valid’ block to be added to the chain. When all nodes on the network confirm a transaction is valid it gets added to the block. A highly complex algorithm is used to verify the validity of a block. This algorithm is called as "Proof of Work". Miners compete to solve this compete to solve this complex algorithm to verify the block.

There are four pieces of information in a block: hash, summary, timestamp, and proof of work. Hash contains information of the previous block. The summary contains the information about the transaction. The timestamp is the date and time on which the block was created. Proof of work is the algorithm used in creating the block (Mougayar, 2016).

In short, blockchain is a self-maintained database or app development platform. A blockchain network can either be public (permission less) or private(permissioned).

The most important features of blockchain are the complex cryptography and distributed ledger. This makes blockchain virtually unhackable as computing power required to hack or corrupt the nodes would be half of the nodes present in the blockchain.

Since blockchain is a decentralized system that exists between all parties so there is no need to pay the intermediaries. All the transactions happen directly between the parties that save time. As there no need to pay the intermediaries it makes blockchain cheaper than the current system. All the transactions happen through the self-executing contracts called as Smart contracts (Mougayar, 2016).

7. How will blockchain technology affect food supply chain?

Blockchain has something for every industry including the food supply chain. Contaminated food due to fraud in the food business is becoming a common phenomenon. As per a report released by World Health Organization (WHO), 1 in 10 people is affected due to contaminated food every year. It also said that every year 4.2 million die from eating contaminated food.

Every company, that finds themselves in a food scandal end up losing a lot monetarily as well as non-monetarily. The loss starts from loss of consumer trust, annual revenue losses are as high as 15% and of course brand loyalty.

Blockchain can be helpful in avoiding such scandals. We all know that blockchain is a decentralized ledger wherein transactions are recorded, and the information is stored on a global network. This is done in such a manner that it prevents any kind of change in future.

This makes blockchain a huge asset for supply chain industry. For food owners, blockchain can help them to identify quickly any kind of tampering that is attempted when

it moves in the value chain. This ensures that food that has contaminated or food that is unfit for consumption is removed even before it reaches the shelves.

If due to some reasons the food reaches shelves, then retailers can identify it immediately and remove them. This would help the processors and retailers from avoiding batch recalls which are a costly affair for any company.

8. Why use blockchain for food supply chain?

Blockchain should be used in food supply chain as it has the potential to give the power of information to the end consumer. As of today, food supply chain is plagued with food fraud, recalls due to contamination, adulteration and similar problems. There are technologies available that can help in reducing such issues, but they are costly and time-consuming (Swan, 2015).

For example, on an average, a single product goes through six to eight stages in the food supply chain before reaching the final consumer. In such scenario's end-to-end traceability is next to impossible when we use methods such as sampling.

Blockchain, when used in food supply chain industry, will increase transparency, efficiency in the supply chain and food safety.

1. Transparency

A simple QR code and a smartphone will give consumer all the information they seek at the point of sale. They can receive full information from where the food was produced, where it was processed and how it reached the point of sale.

Blockchain would be of tremendous help when it comes to traceability. With blockchain in place, no one would be able to make false claims. Grey areas of traceability such as labeling, country of origin etc can be addressed through blockchain technology (Swan, 2015).

For example, as of today, it is difficult to trace if the manufacturer is making a false claim or a true one. So, if the product says its origin is from Sri Lanka, we cannot differentiate if the claim is true or false. However, with blockchain, this will not be difficult at all.

In blockchain technology, each and every interaction with the food item would be recorded and a digital certificate shall be assigned. What it implies is that no company in the entire value chain would be able to adulterate the food item later or hide the truth about its origin.

When blockchain would be applied to a food supply chain, all the digital product information that is the origin of product, batch number, factory where it was processed, date of expiry, temperatures in which it was stored, and also the shipping details would be digitally connected to the food item and the information would be entered as and when each step is completed.

The beauty of blockchain is that whatever information that is captured in each and every transaction is first agreed by all parties of the concerned business. Once every part provides its consent it becomes a permanent record, and nobody would be able to alter it.

Every piece of information in blockchain would provide critical data about the food item that can reveal potential food safety issues with the product. This record which is created would help retailers to manage more efficiently the shelf life of products in individual stores. It will also help in strengthening safeguards related to the authenticity of the food item sold.

For example, Walmart would be able to trace from where the meat has come from, where it was processed, where it was stored and also its sell-by date.

Now think about few past scandals which could have been avoided if blockchain was in place. For example, Maradol papayas from Mexico that infected more than 200 people in the USA and was the reason behind the outbreak of Salmonella. If blockchain technology would have been used, it could have been prevented and controlled quickly and easily. The quickness of this technology can be understood from Forbes report which said that conventional methods used by Wal-Mart took six-plus days to extract farm location of a product (Mango) whereas blockchain did the same for them in 3 seconds.

A very common food fraud which is seen today is Honey fraud. Honey being the most expensive form of sugar is the most tampered product in the world. Due to its texture, it is very susceptible to adulteration. Blockchain technology can help in avoiding such fraud. The honey fraud happens in different ways. The most common form of honey fraud is:

a. Selling cheaper multi-flora honey as single source honey at a higher selling point.
b. Manufacturers also add sugar syrups for increasing the volume
c. Sometimes they harvest it before time and dry it artificially to cut time and cost
d. Honey is an opaque colored liquid, so manufacturers take advantage of that by adding any other sweetener such as corn syrup, beet sugar etc. By adding real or artificial sweeteners producers or resellers can increase their profit margins.

Food fraud are becoming more common nowadays. As of today, food supply chain comprises of multiple players with diverse functionality and spread across different geographies. Many of players as mentioned earlier are unaware of each other and also have different economic agenda. Blockchain, when introduced, will reduce such kind of food fraud, adulterations significantly and increase consumer confidence as accountability of related parties would increase.

Transparency brought in by blockchain will allow customers to know that the companies from which they are buying the products share the same values and ethics especially when it comes to the environment and sustainable manufacturing (Hnatio, 2014). As of now Walmart, Nestle, Unilever have been experimenting with blockchain technology in their businesses.

2. Efficiency in the food supply chain

Blockchain will bring in a lot of efficiency in the entire food supply chain system. This is so as blockchain technology will help in removing inaccuracies that are found in the current system especially in manual inspection, paper tracking etc.

Blockchain would also help in reducing food wastage and increase in savings tremendously. For example, there is a difference in identifying few tainted lettuce packages and shunning entire stock of lettuce from all stores where they were supplied.

3. Food Safety

To understand how food safety would be enhanced through blockchain let's recall few incidents that happened in past.

Chipotle and E. coli scandal –Chipotle had to suffer severe revenue losses and saw significant cut in revenue share due to its customers as well employees suffering from E. coli

infections. As per a report they had to spend around $15-16 million on crisis management. If Chipotle had blockchain in place, then they could have pinned down the specific restaurants and closed them. Damage control would have been faster, and many people would have been saved from suffering this disease.

No company would ever want to be in place of Chipotle. Using blockchain's three value propositions, decentralization, verification and immutability, companies can prevent such incidents (Bahga and Madisetti, 2017).

If we go back in history, then we cannot forget the recall made in the year 2011 by Cargill. A total of 36,000,000 pound of ground turkey were recalled as the company suspected that it might have been polluted by a strain of Salmonella, which is found to be drug-resistant. In 2017 too, they recalled 185,000 pounds of meat for the same reason. Blockchain would have helped Cargill to find out the contaminated batch and reach the origin of the contamination hereby saving costs of recalling all batches.

9. How food supply chain can benefit from blockchain technology

The primary benefits of adopting blockchain would be:

1. Consumer confidence

Blockchain will help in building the dwindling confidence of consumers in the food industry. Consumer confidence will be built in the following manner.

2. Food recalls

The food industry has seen tremendous setback with the outbreak of various foodborne illness-causing recalls and loss of trust. Blockchain will help in preventing it. As of now, when cases such as Hydrolysed vegetable protein recalls due to salmonella poisoning happens it takes a lot of time to isolate the concerned product recall or contamination in the food supply chain. Blockchain will help in enhancing tracking abilities in future. As of today, big giant such as Walmart is already working on it. Walmart along with IBM are using blockchain to improve food tracing abilities.

Recently they did the mango pilot project and presented it to investors. In this test, they involved 16 farms, two packing houses, two import warehouses, three brokers and a processing facility. For a month they captured 23 different lot codes and were able to trace the slices of mangoes in seconds which otherwise took days. So, the primary benefit which every player in a food supply chain will enjoy is immediate and quick tracking and tracing of food.

When cases such as Chipotle happens then such restaurants or even grocery store who served food or sold the item are most of the times left fidgeting their hands while promising to address the serious problems quickly. However, this could be avoided with blockchain, as foods would be tracked and traced immediately thereby avoiding further damage.

Take, for example, a chain of restaurant is faced with dozens of its customers falling ill after dining at their restaurants. After testing the food, they find out that the culprit is the pork used by them. With the ability of a blockchain to track and trace foods, the restaurant can conveniently trace the infected foods' serial and batch number and would be able to find the associated distributor and subsequently the supplier. Post that, they would be able to

flag the concerned supplier and further prevent damage to anyone who has sourced or bought the vegetables will be made aware of the danger (Bahga and Madisetti, 2017).

However, implementing such solution would be dependent on few things. First, it would be necessary that every crate, shipment and individual package procured by the company is identifiable in a unique manner. As of now, GTIN is being provided by global standards body GS1. It is being introduced to ensure serialization efforts wherein each product is given a unique code GTIN. Secondly, in such technology, it would be necessary that the participants transfer the custody of product at every step of the supply chain.

The secondary benefits that this technology would provide are:

3. Ability to audit anywhere and any time

Once any information is recorded in blockchain then the information becomes undisputable and can be referred to at any point in future. This allows parties in the supply chain to verify that the information has not been tampered with.

4. Information

Unlike the present technologies that are restricted to a particular format, blockchain technology has the capability to capture and storewide variety of information. So, if the present system records only specific information that is related to an inventory management system, unique identification of a batch or lot, GPS tracking, blockchain technology would be able to record all of this information in it thereby serving as a middleware.

This would allow easy interaction among the different software platforms that are required to exchange information.

The efforts made by IBM currently are permission-based blockchains. The access to blockchain is restricted. In future, if there is the development of multiple restricted access blockchain that is independent of each other then we would be unable to create the substantially better world then what we have today.

To understand this, take, for example, Walmart. Walmart as of today uses enterprise software such as SAP if they wish to pass on information and data to a company like Pepsi. So, communication happens through enterprise-based information. In future, if IBM creates an independent blockchain which has to communicate with the blockchain used by Pepsi then it would be necessary that the two protocols are interoperable.

The other issue would be that these blockchains so developed would limit access to information and as a result, limit transparency.

Hence to enjoy the benefits of this technology we should ensure the information is accessible to third parties which include consumers.

If a company doesn't aim at supply chain transparency, still blockchain technology would be useful to post encrypted information. This information can be used later when and if required in case of a recall of food item or regulatory event.

5. Evaluation of quality assertions

Blockchain would facilitate quality assertions. For example, if a food processor wants to assert the information that is of interest and value to the consumer such as a particular product they supply contains sugar-free honey. When they make this assertion on the blockchain, then it would go beyond traditional product labeling. It would digitize this data, which can now be used in other automates systems like a grocery purchasing manager requirements, smart-menu, diet planning software, and so on. The food processor may

further request that a certification agency undergoes a review concerning their assertions about sugar-free honey. The certification agency, in carrying out their functions, may visit or do tests on the product samples. If the assertions are found to be untrue, the agency may post a certification on the blockchain of food and reinforce the processor's declarations.

6. Exchange of information

Blockchain would facilitate sharing of recipes, proprietary information, measures, methods, and other essential data in a secure environment with only selected participants. For example, if a Vegan restaurant wants to claim the bun that was used is 100% vegan then it can be done by giving temporary access to the ingredient list used by baker so as to certify that his/her vegan is compliant with the necessary requirements. Here, nobody would need nor would be allowed to have access to the recipe. It is a smart contract that is coded with the appropriate instructions will be reviewed by all parties involved so as to ensure that no duplication occurred.

7. Smart marketplace

Participants of the food value chain would be more engaged. Blockchain enables buyers and sellers matched by shared but trusted need for data. This can be combined and later used by a third party, such as a consumer. Participants won't be required to know each other personally. Smart contracts will evaluate the assertions made on the blockchain and notify the respective account holders when it makes matches in quality, timing, quantity, etc.

If proper collaboration happens among different parties of the food supply chain, then blockchain will help each of the party in the food supply chain in different ways. Let's understand how it would be useful:

8. Farmers/Producers

Blockchain would help producers to find a market for their produce. A major problem seen today is matching of demand with supply. It is estimated that around 20% of the cultivable land is unused, blockchain would help them to utilize their land efficiently and increase their profits. Blockchain will facilitate new real-time, local produce market. This would be done due to transparency for evidence of high quality (as observed in safety, freshness, taste), traceability (for measuring brand integrity and active risk management), food sustainability that necessitated fair incentives provided by the buyer to grower, fighting against food fraud and promoting essential regulatory compliance that is made possible by blockchain technology.

9. Distributors

Distributors rely on verbal assurances and sample checks done by them while purchasing food from farmers. At the same time, they are under tremendous pressure to increase transparency from processors and consumers. Demand for product type, farming practices used, harvest date of the crop, treatment information, fair-trade, certifications, etc is increasing. Blockchain will give them access to information they need for each purchase made. Distributors would be the major adopters of this technology apart from processors (Jiang, 2018).

10. Packers

Blockchain technology will help Packers to increase their value in current food supply chain. They can use smart containers, having a blockchain identity, product labeling, location where the item was packed etc to enhance their value. They can document their value in the

supply chain and thus add value to data shared bringing in more transparency in the supply chain.

11. Processors

It is many times difficult for processors to validate the origin of their product used as inputs. Trust of consumers on processed food purely depends on the capability of the processor to communicate to the consumer about processing data but also the origin of the raw material used in the product. For example, providing information on potatoes used in making of chips. As of today, processors are guarded as they do not wish to share their practices and methods used by them to produce or process food. Blockchain will help processors to share information with producers in a private and secure manner. Further, it helps the supply chain to validate the information without making any violation of individual entity trust.

To understand this more, let's take an example of a processor selling frozen hot dogs. They claim that buns used in these hot dogs are made of specific flour. They buy the bun from a local bakery. Assuming the baker uses blockchain technology for making an assertion to the public that buns are made of specified flour. Here, the restaurant will post a smart contract which would be a self-executing code. It would be using data on blockchain in a unique manner. It would be programmed to identify the specified ingredients. The baker would privately expose his list of ingredients as evidence to the restaurant's smart contract. After going through the list of ingredients the smart contract would certify the baker's claims, and thus reinforce these assertions in the mind of the consumer. The smart contract will continue to monitor this list of ingredients for every order placed by the processor. This will ensure the authenticity of the claim made by baker and in turn, will make processor claim boldly that a certain type of flour was used in making buns.

12. Restaurants

There is a direct relationship between a restaurant and consumer. IT has been becoming increasingly common to provide information about the food served by them to consumers. With the advent of online ordering and use of smartphone apps, demand for food data that are ingredients used in food is increasing. This trend has become so popular that health-conscious consumers are willing to pay more price for food that is good for them. Blockchain can be used to connect smart menus in real time so as to provide the correct history of specific produce being used on a particular day in the store.

13. Traders

Cargill, Bunge are powerful names that currently move food grains and commodity product around the world. These traders manage the huge amount of data. They are primarily in the institutional trading and risk management of all these elements.

These traders have vested interest in having control over the management of commodity business. What it means is that information related to port infrastructure, trading know-how, pricing relationship with different producers can be of dominant competitive advantage.

Traders are those entities that would be first people interested to opt blockchain for their business. They would like to add to their infrastructure to serve their purposes (Richard, 2018).

They would force adoption or go for leveraging of large company efforts such as SAP or IBM to enable others to connect to their chains.

Most of these traders have a connection with traditional brokerages, financial exchanges, and institutional trading markets. As of now, there are several large group efforts for blockchains such as Digital Assets, R3, and Hyperledger and some distributed ledgers to participate in exchange trading (via derivatives) on new, distributed ledger systems. They connect financial risk management to crops in real time. This will result in the creation of new "alpha" trading opportunities for these trading houses based on new shared information on disparate blockchain functions.

14. Grocers

Online retailers are nowadays giving stiff competition to Grocers. It is becoming increasingly difficult for premium grocery shops to justify their premium prices. Customers are demanding more and more transparency. Blockchain can help grocers by providing a Web-of-Trust system. This system would allow all the participants to review and validate claims made about the food safety. What will happen in turn is that it will bind the information value that is provided by local farmers to the claims that are made by grocers and shared in the blockchain of related foods to effectively create new, distributed, chain-wide, self-certification of quality, transport, freshness. This would be a powerful and unprecedented transformational activity to assist in solve the problem of low levels of consumer trust in their foods (Marke, 2018).

15. Labeling of the product

Today a consumer decides whether to buy or not a product based on the information given on the label. If a consumer wishes to buy a food item that is organic, then how do we trust that the label is accurately providing information about the product?

As of now, there are various companies who that helps in confirming what is written on the label is accurate. However, blockchain would be one step further than these companies. It will help in bringing the food industry together around the consumer demand and regulations. The standards set by blockchain will ensure the integrity of market claims.

As the labels would be traceable so the trust in supplier and its reputation would increase manifold.

16. Information about farm and distributor

IT would not be only consumers who would be the primary beneficiaries of blockchain technology. Even distributors would stand to benefit from this technology.

Farmers and producers would have real-time access to commodity prices and the market data. If the producers have real-time data, then they would be able to be more competitive and productive.

Block commodities ltd, a blockchain technology company, has entered into a partnership with the Global Markets Exchange Group International LLP. The partnership was created for developing a blockchain based platform for the commodity markets in Africa.

This platform aims to help farmers that are based in the sub-Saharan region to connect with buyers, brokers. Thus, this platform helps them to get better prices for their crops and also competitive interest rates on loans.

This partnership aimed at providing farmers better interest rates on loans as well as better prices for their crops. It is possible only due to blockchain technology as the interest rates and the commodity prices are registered and logged in blockchain enabling easy access to information needed by these farmers.

Thus, the most important and primary benefit provided by blockchain technology would be of building trust in consumers due to ease of tracking the food as well as damage control in case of contamination. Food fraud, Food-related illness would be controlled significantly due to this technology.

10. Companies that are currently applying blockchain to food supply chain

1. TE Food

TE food is a company that is hoping to improve the traceability between the farm and consumers, tracking the items through the supply chain and ensuring food quality. For over a few years, TE food now performs over 6000+ business customers tracking numerous animals and dairy products daily.

TE Food is now striving to espouse blockchain technology to decentralize the currently centralized ledger for better transparency for both consumers and producers. Moreover, the transaction and food-related data will be stored in a private blockchain with an internal technical token as governmental customers do not approve the public blockchain network.

TE food is hoping to tokenize the transactions as it provides credibility for both consumers and supply chain companies. Tokenization through smart contract diminishes the unpredictability during transactions via unification of financial transaction into one ledger. So, not only TE food use blockchain for simple ledgers, but they also implement it for a token and wallet.

Purchasing TFD for authorization money, supply chain participants can cover the price of the preferred number of transactions and keep it in their TFD wallet. On a private blockchain, TE food will deposit the transactions brought into the transaction wallet for the participants. Later, blockchain enables participants and consumers to trade their tokens remaining through the exchange, making a selling offer on the market.

2. ii. AgriDigital

AgriDigital is a platform that is designed to aid transactions, sales, and storage of agricultural commodities for producers and consumers. AgriDigital and CBH group have pilot tested the implementation of blockchain in a grain industry in Australia.

They performed payments through blockchain, using a token known as “Agricoin” which rested on the Australian dollar. The payment had some advantages over the conventional method as it happened in real time and was programmable; it was also more transparent and secure.

Another usage of blockchain was to enhance the traceability of agricultural commodities, and each consumer confirmed the organic status of these commodities by matching the digital assertions to the business process. These assertions were hashed and documented on the block as well as reported to the farmers/producers whether the consumer has confirmed or denied the freshness status of the food.

3. iii. Food Coin

Foodchain Ecosystem a blockchain ecosystem where it provides equitable access to the global food market for all producers and consumers with 1000 Ecofarm platform, creating a wide market for organizing food with affordable prices.

This ecosystem is founded on Ethereum technology; their primary goal of applying blockchain is to dwindle the transaction costs, provide higher efficiency, and enhance the food system. The Ethereum technology allows the combination of distributed database storage system, smart contracts(Smaco), and user verification on the platform remotely.

Another application of blockchain is by providing a peer to peer network, where each node has a duplicate of FCE blockchain in the form of private and public structure to prevent unauthorized data modification.

Lastly, there are few purposes that blockchain serves which are similar to previous startups such as crypto wallet(Wallok), payment system(Dipay), and product authentication. Through blockchain, they manage a hierarchical system for monitoring and administration of the commodities.

11. Challenges in using blockchain technology

Like all the other new technologies blockchain too comes with its own set of challenges. What are key significant challenges that suppliers and customers might face while adopting blockchain technology?

With the rapid growth in the size of records and transactions, blockchain can face scalability and performance challenges. As new transactions or records are written on the blockchain, a number of blocks get added thus increasing the size of the database and decreasing speed to access transactions on the blockchain. As speed is the essence it may make blockchain unsuitable for supply chains with a huge number of transactions (Laurence, 2017).

As blockchain based use cases are emerging in food supply chain the major challenge faced by the supply chain companies is the awareness and understanding of the use of blockchain as technology. There is a widespread lack of knowledge and understanding of food supply chain sector how this technology works.

In adopting any new technology, initial costs like software, hardware and setup are involved. And as technology is new, trained professionals in the field are difficult to find, making it more expensive to implement blockchain technology. Due to the high cost involved small and medium-sized businesses would be reluctant in adopting (Bashir, 2017).

For any organization, it's difficult to remodel old systems and adopt new ones. In the initial phase, for a smooth transition, a solution to integrate legacy systems with blockchain is required. Currently, there are no solutions available that can integrate legacy systems and new systems using blockchain. For the implementation of blockchain technology across company would require planning, time, expertise and funds. Management of many organizations understand the benefits of blockchain technology but still are hesitant in implementing it due to the elevated costs involved.

Regulations and governance in food supply chain management are based on centralized systems. Since blockchain is decentralized technology, new blockchain applications will not work with existing regulatory structures. New regulatory systems would be required to use blockchain-based applications (Bashir, 2017).

12. Conclusions

Globalization has fuelled the growth of food supply chain. Food supply chain now has its own set of complexities as well as challenges. These challenges would aggravate further as we see advancement in technologies and growth in population. Nations across the world should ensure food safety and security by making stringent legislation and placing strict punitive actions in place. Various actors in the food supply chain should take help of the technologies and synchronize their processes to ensure significant benefits. With the introduction of the blockchain, this supply chain would see a tremendous increase in trust, consumer confidence and a decrease in food-related fraud. It is still at its infant stage and would take some time before organizations adopt it fully. If we want blockchain to work, then there would be a need for collaboration across the industry. We would also need the stakeholders to adopt data standards and formats. Many of the larger players such as Walmart, Nestle, Tyson foods etc as mentioned above have been working on pilot projects for integrating blockchain into their supply chain. However, the industry needs to ensure all partners join and work together. This would fuel standardization and would stop the creation of several independent blockchains.

References

Bahga, Arshdeep, and Madisetti, Vijay. *Blockchain Applications: A Hands-on Approach.* Uttar Pradesh: VPT, 2017.

Bashir, Imran. *Mastering Blockchain.* Birmingham: Packt Publishing, 2017.

Carlos, Mena, and Graham, Stevens. *Delivering Performance in Food Supply Chain.* Amsterdam: Elsevier Science, 2010.

Dani, Samir. *Food Supply Chain Management and Logistics: From Farm to Fork.* London: Kogan Page, 2015.

Hnatio, John. *Fighting Food Fraud: A Primer for the European Food Industry.* Maryland: FoodQuestTQ, 2014.

Hutter, Bridget. *Managing Food Safety and Hygiene: Governance and Regulation as Risk Management.* Massachusetts: Edward Elgar, 2011.

Jiang, Pingyu. *Social Manufacturing: Fundamentals and Applications.* New York: Springer, 2018.

Laurence, Tiana. *Blockchain for Dummies*. London: John Wiley & Sons, 2017.

Leadley, Craig. *Innovation and Future Trends in Food Manufacturing and Supply Chain Technologies.* Amsterdam: Elsevier Science, 2015.

Levinson, Daniel. *Traceability in the Food Supply Chain.* Pennsylvania: DIANE Publishing, 2010.

Marke, Alastair. *Transforming Climate Finance and Green Investment with Blockchains.* Amsterdam: Elsevier Science, 2018.

Mougayar, William. *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology.* London: John Wiley & Sons, 2016.

Richard, Sandor. *Electronic Trading and Blockchain: Yesterday, Today, and Tomorrow.* World Scientific Publishing Company, 2018.

Shirani, Mohsen. *Risk Analysis and Assessment in Perishable Food Supply Chain.* Munich: GRIN Verlag, 2013.

Swan, Melanie. *Blockchain: Blueprint for A New Economy.* Cambridge: O'Reilly Media, 2015.

Nash Equilibriums for Bimatrix Games

Keith Blakesly

Abstract

Game theory has been a subject of interest for decades due to the fact that the analysis of different strategies provides the best possible strategy for a given situation. Its application is endless from war to business. More specifically, the Nash equilibrium looks at a competitive situation which is more applicable in our world. After learning about game theory, I was instantly mesmerized by the simple, yet complex rules and analysis of different strategies. Specifically for this paper, I used Mathematica which enabled me to recreate the payoff matrices and analyze them for the Nash equilibrium looking at different situations.

1. Introduction

Like the French philosopher, Jean-Paul Sartre once said, "Life is **C**hoice between **B**irth and **D**eath." In our lives, we make countless decisions and choices based on multiple variables. This, the study of decision making, is also known as game theory. Whether one is aware of the concept of game theory or not, game theory is used all the time. Game theory can be used in games like chess and poker but it is also used in business and more complicated matters.

Although game theory is used ubiquitously, the first tangible evidence of game theory dates back to 1713 when James Waldegrave wrote a strategic solution about a card game le Her. However, it wasn't until John von Neumann that game theory became big. He was able to prove his minimax theorem which established that in zero-sum games, there are certain moves that allows the player to minimize their losses and maximize their gains. In game theory, this is one of the most important concepts.

Prisoner's dilemma is one of the most famous example used in game theory. Basically, in prisoner's dilemma, two criminal gets arrested and each prisoner is given a choice to either stay quiet, or confess that his partner committed the crime. If both prisoners remain quiet, both will only have to serve 1 year in prison. However, if prisoner A betrays B (while B remains quiet), prisoner A will be free but prisoner B will have to serve 3 years (and vice versa). Finally, if both prisoner betray each other, both of them will have to serve 2 years in prison. Although this seems like a quite simple scenario, there is a lots of variables in this situation. The best situation for both

prisoners would be to betray and hope that the other doesn't, but if both prisoners betrays, it leads to the worst case scenario.

Among the countless components of game theory, this paper will look specifically into Nash equilibrium. Nash equilibrium is a strategic solution in a non-cooperative game involving more than one player. In Nash Equilibrium, all the players knows each other's strategy and does nothing because they know that nobody can benefit from making a change. The Nash Equilibrium comes from John Forbes Nash. John Nash was a mathematician who earned a PH.D degree with a paper on non-cooperative game which contained the main properties of Nash Equilibrium.

2. Nash Equilibriums

Before moving on, there are some terms that should be discussed. When a game has N number of players, it is called non-cooperative game (given that N≥2). Both players have their own set of strategies z, of strategies Zi with the payoff function Hi(z), where zZ is a situation defined on the set. Like the name suggest, in a non-cooperative game, players are competing with each other to earn the highest possible point or gain. Non-cooperative game falls under a bigger category known as the constant sum game, if there exists a constant C, which is $\sum_{i\in N} H_i(z) = C$ for all situations $z \in Z$. The non-cooperative two player game in addition with the non-zero sum is called the bimatrix game. Let 1st player has m strategies $A_1, \ldots, A_m$; 2nd player – has n strategies $B_1, \ldots, B_n$. Winnings of the 1st and 2nd player is set by the payoff matrices $A=[a_{ij}]_{mxn}$; $B=[b_{ij}]_{mxn}$.

Example 1

For example, picture two companies competing with each other to sell their product.

Corresponding tensor P (double matrix) has a view

$$P = \begin{pmatrix} (0,4) & (4,0) & (5,3) \\ (4,0) & (0,4) & (5,3) \\ (3,5) & (3,5) & (6,6) \end{pmatrix}.$$

Here first elements of pairs in P refer to the player A and second one – to the player B. So, player's A payoff matrix is $A = \begin{pmatrix} 0 & 4 & 5 \\ 4 & 0 & 5 \\ 3 & 3 & 6 \end{pmatrix}$ and player's B payoff matrix is $B = \begin{pmatrix} 4 & 0 & 3 \\ 0 & 4 & 3 \\ 5 & 5 & 6 \end{pmatrix}$.

They can have up to three different modifications on a market and their products are measured in million dollars. Company A's strategies are represented as the payment matrix A, and the Company B's strategies are represented as payment matrix B. If company A chose the second modification while company B chooses the third modification, company A will make $ 5 million while company B will make $ 3 million. An important point that should be

taken into consideration is that this case is a zero sum game, players will play with their optimal strategies. However, for non-antagonistic games, players will choose an optimal strategy for the whole group so all the players can benefit from the action. Thus, the solution to a non-cooperative game is to find an equilibrium situation.

2.1 Nash Equilibriums in Bimatrix Games

Specifically, this section of the article would be looking into Nash equilibrium. Under $a_{i0,j0} \geq a_{i,j0}$ $(i=1,\ldots,m)$; $b_{i0,j0} \geq b_{i0,j}$ $(j=1,\ldots,n)$, the Nash equilibrium strategies stand. All equilibrium strategies relates to the concept of the saddle point. A saddle point can be viewed as the lowest point in the x axis while being the highest point on the y axis. This can be used in game theory because players in equilibrium situation try to minimize their maximum loss. In game theory, we have to look for the maximal element in matrix A and B. Then all pairs of the strategies (i,j) would be known as a_{ij} and b_{ij} in. equilibrium situations Now let's take a look at some examples:

Example 2

Let's find equilibrium situations in the game of Example 1.

For the matrix A we have $A^* = \begin{pmatrix} 0 & 4^* & 5 \\ 4^* & 0 & 5 \\ 3 & 3 & 6^* \end{pmatrix}$,

for the matrix B – $B^* = \begin{pmatrix} 4^* & 0 & 3 \\ 0 & 4^* & 3 \\ 5 & 5 & 6^* \end{pmatrix}$.

As we see, there are two asterisks for element with indexes $i=j=3$.

So, Nash equilibrium for players in this game corresponds to issue 3-d modification of production. Expected profit of the both firms equals to $ 6 million.

Example 3

Let's generate simple code in Mathematica to help us find Nash equilibrium for given payoff tensor P with interactive input of payoff matrixes A and B

Exercise 1

Find equilibrium situations in the game, characterized by the tensor P:

$$P = \begin{pmatrix} (3,2) & (4,3) & (5,1) & (6,2) \\ (5,5) & (2,1) & (8,4) & (3,6) \\ (8,7) & (3,0) & (9,6) & (2,8) \end{pmatrix}$$

a. without computer;
b. with help of Mathematica

Solution

a. Let's separate payoff matrixes of the players: $A = \begin{pmatrix} 3 & 4 & 5 & 6 \\ 5 & 2 & 8 & 3 \\ 8 & 3 & 9 & 2 \end{pmatrix}$,

$$B = \begin{pmatrix} 2 & 3 & 1 & 2 \\ 5 & 1 & 4 & 6 \\ 7 & 0 & 6 & 8 \end{pmatrix}.$$

Then we mark maximal elements: $A^* = \begin{pmatrix} 3 & 4^* & 5 & 6^* \\ 5 & 2 & 8 & 3 \\ 8^* & 3 & 9^* & 2 \end{pmatrix}$; $B^* = \begin{pmatrix} 2 & 3^* & 1 & 2 \\ 5 & 1 & 4 & 6^* \\ 7 & 0 & 6 & 8^* \end{pmatrix}$.

As we see, there is one equilibrium situation (A_1,B_2).Corresponding winnings are 4 conditional units for the player A and 3 conditional units for the player B.

b. Let's use the code, generating in Example 3. The changes are minimal (see Fig.2)

```
InputField[MatrixForm[Array[A, {3, 3}]], FieldSize → Automatic]
(* Interactive input of 1-st payoff matrix elements *)

{{0, 4, 5}, {4, 0, 5}, {3, 3, 6}}

Z = Array[A, {3, 3}]; MatrixForm[Z] (* Z iz matrix of vectors *)

( 0  4  5
  4  0  5
  3  3  6 )

InputField[MatrixForm[Array[B, {3, 3}]], FieldSize → Automatic]
(* Interactive input of 1-st payoff matrix elements *)

{{4, 0, 3}, {0, 4, 3}, {5, 5, 6}}

V = Array[B, {3, 3}]; MatrixForm[V] (* Z iz matrix of vectors *)

( 4  0  3
  0  4  3
  5  5  6 )

ZT = Transpose[Z]; MatrixForm[ZT] (* Prepare for find maximums *)

( 0  4  3
  4  0  3
  5  5  6 )

k1 = 0 k2 = 100; For[i = 1, i ≤ 3, i++,
  (* i will be a number of line in the matrixe Z and number of a column in the matrix V *)
 For[j = 1, j ≤ 2, j++; If[Z[[i, j]] == Max[ZT[[i]]], k1 = i];
  (* j will be a number of column in the matrixe Z and number of a line in the matrix V *)
  If[V[[j, i]] == Max[V[[j]]], k2 = j]]; If[k1 = k2, Print["i=", i, " j=", j,
   " - Nash equilibrium. Winnings of players are ", "A: ", Z[[i, j]], " B: ", V[[j, i]]]];
 k1 = -10;
 k2 = -1]

i=3 j=3 - Nash equilibrium. Winnings of players are A: 6 B: 6
```

Figure 1. Mathematica code for find Nash equilibrium (Exercise 1 b).

2.2 Dominated strategies

By definition, dominated strategies are when the strategies I of Player A is greater than or equal to all elements of strategies J of Player B. In other words, a dominated strategy is when there is always an option of playing a better hand. However for this definition to stand, the solution to the bimatrix must be a constant even though we delete the rows and the columns of the matrix.

Example 4

a. Simplify payoff tensor P of the game and find its solution without.

$$\begin{matrix} & L & M & R \end{matrix}$$

P= $\begin{matrix} u \\ m \\ d \end{matrix}\begin{pmatrix} (4,3) & (5,1) & (6,2) \\ (2,1) & (8,4) & (3,6) \\ (3,0) & (9,6) & (2,8) \end{pmatrix}$.

```
InputField[MatrixForm[Array[A1, {3, 4}]], FieldSize → Automatic]
(* Interactive input of 1-st payoff matrix elements *)

3

Z = Array[A1, {3, 4}]; MatrixForm[Z] (* Z iz matrix of vectors *)

⎛0 4 5 6⎞
⎜4 0 5 3⎟
⎝3 3 6 2⎠

InputField[MatrixForm[Array[B1, {3, 3}]], FieldSize → Automatic]
(* Interactive input of 1-st payoff matrix elements *)

{{4, 0, 3}, {0, 4, 3}, {5, 5, 6}}

V = Array[B, {3, 3}]; MatrixForm[V] (* Z iz matrix of vectors *)

⎛4 0 3⎞
⎜0 4 3⎟
⎝5 5 6⎠

ZT = Transpose[Z]; MatrixForm[ZT] (* Prepare for find maximums *)

⎛0 4 3⎞
⎜4 0 3⎟
⎝5 5 6⎠

k1 = 0 k2 = 100; For[i = 1, i ≤ 3, i++,
 (* i will be a number of line in the matrixe Z and number of a column in the matrix V *)
 For [j = 1, j ≤ 2, j++; If[Z[[i, j]] == Max[ZT[[i]]], k1 = i];
  (* j will be a number of column in the matrixe Z and number of a line in the matrix V *)
  If[V[[j, i]] == Max[V[[j]]], k2 = j]];
 If[k1 = k2, Print["i=", i, " j=", j, " - Nash equilibrium. Winnings of players are ",
   "A: ", Z[[i, j]], " B: ", V[[j, i]]]];
 k1 = -10;
 k2 = -1]
i=3 j=3 - Nash equilibrium. Winnings of players are A: 6 B: 6
```

Figure 2. Mathematica code for find Nash equilibrium (Example 4).

Because player B's strategy R gives him/herself a definite win which is greater than the strategy M. Thus, strategy m is a dominated strategy and it is obvious that the rational player B would not play it. I.e. tensor P is reduced to P_1:

$$P_1 = \begin{pmatrix} (4,3) & (6,2) \\ (2,1) & (3,6) \\ (3,0) & (2,8) \end{pmatrix}$$

However, if player A knows that player B will not use his strategy M, then his strategy U will be better than strategy M or D. I.e. tensor P_1 is reduced to the line P_2:

$$P_2 = ((4,3) \quad (6,2)).$$

On the other hand, if player B is aware that player A will play strategy Y, then he has to find an alternative strategy L. After the last reduction was the only element of the payment tensor - (4, 3). Thus optimal pair of strategies is *(u,L)*. They give a win, equal to *4* conditional units to the player *A* and *3* conditional units to the player *B*.

b. Simplify payoff tensor P of the game and find its solution using interactive input of P with help of Mathematica.

Solution

```
{InputField[m, FieldSize → 5], InputField[n, FieldSize → 5]}
(* Interactive input of the payoff matrixes dimesion *)
```

{ 3 , 3 }

```
InputField[MatrixForm[Array[A, {m, n}]], FieldSize → Automatic]
(* Interactive input of the payoff matrix elements *)
```

{{4, 5, 6}, {2, 8, 3}, {3, 9, 2}}

```
a = Array[A, {m, n}]; MatrixForm[a]
```

$$\begin{pmatrix} 4 & 5 & 6 \\ 2 & 8 & 3 \\ 3 & 9 & 2 \end{pmatrix}$$

```
InputField[MatrixForm[Array[B, {m, n}]], FieldSize → Automatic]
(* Interactive input of the payoff matrix elements *)
```

{{3, 1, 2}, {1, 4, 6}, {0, 6, 8}}

```
b = Array[B, {m, n}]; MatrixForm[b]
```

$$\begin{pmatrix} 3 & 1 & 2 \\ 1 & 4 & 6 \\ 0 & 6 & 8 \end{pmatrix}$$

```
a = Array[A, {m, n}]; b = Array[B, {m, n}]; y = 0; x = Array[0 &, n]; z = x; v = y;
```

Figure 3. Mathematica code for payoff matrix reduction (Example 4). Part 1

Exercise 2

a. Simplify payoff tensor of the game using the rule of dominated strategies deleting and find its solution without computer.

	gies	Player B					
		k	*k*	*m*	*n*	*p*	*r*
	a				)		)
	b			)			)

	c						
	d		)				

```
(* Organizing 1-st iteration loop for reducing rows of payoff matrixes A and B *)
For[i = 1, i < m, i++,
 For[k = i + 1, k < m + 1, k++,
  For [j = 1, j < n + 1, j++,
   If[TrueQ[a[[i, j]] ≥ a[[k, j]]], x[[j]] = 0, x[[j]] = 1]; y = y + x[[j]];
   If[TrueQ[b[[j, i]] ≥ b[[j, k]]], z[[j]] = 0, z[[j]] = 1]; v = v + z[[j]] ];
  If[y = 0, a = Drop[a, {k, k}];
   b = Drop[b, {k, k}];
   Print [k, "-th line of the matrixes A and B reducing"]];
  If[y = 3, a = Drop[a, {i, i};
     b = Drop[b, {i, i}]];
   Print [i, "-th line of the matrixes A and B reducing"]];
  If[v = 0, b = Drop[b, None, {k, k}]; a = Drop[a, None, {k, k}];
   Print [k, "-th column of the matrixes A and B reducing"] ;
  If[v = 3, b = Drop[b, None, {i, i}];
   a = Drop[a, None, {i, i}];
   Print [i, "-th column of the matrixes A and B reducing"]]];
 y = 0;
 v = 0 ] ;
Print["Reducing payoff matrix A after excluding dominated rows ", MatrixForm[a]];
Print["Reducing payoff matrix B after excluding dominated rows ", MatrixForm[b]]
2-th column of the matrixes A and B reducing
Reducing payoff matrix A after excluding dominated rows
( 4  6 )
( 2  3 )
( 3  2 )
Reducing payoff matrix B after excluding dominated rows
( 3  2 )
( 1  6 )
( 0  8 )
{InputField[m1, FieldSize → 5], InputField[n1, FieldSize → 5]}
(* Interactive input of new payoff matrix dimesion *)
{ 3 , 2 }
```

Figure 4. Mathematica code for payoff matrix reduction (Example 4). Part 2

Solution to Exercise 2a)

Let's separate giving tensor on two matrixes, *A* and B:

$$A = \begin{pmatrix} 2 & -3 & -1 & -5 & 4 & -3 \\ 3 & 3 & -1 & 4 & 4 & -3 \\ 2 & 2 & 0 & 0 & -2 & -2 \\ -5 & -3 & 2 & -3 & 0 & 0 \end{pmatrix}; B = \begin{pmatrix} -3 & 2 & 2 & -3 & -5 & -5 \\ 1 & 3 & -1 & 4 & -4 & -4 \\ 1 & -3 & -5 & -5 & 3 & 0 \\ 4 & -5 & -1 & 3 & 1 & -2 \end{pmatrix}.$$

Beginning with the matrix B, one can see, that its last column B^6 has the elements less or equal of the column's B^5 corresponding elements. For brevity, we denote this fact as $B_5 \geq B_6$. So, reduced matrix B will have a view:

$$B1 = \begin{pmatrix} -3 & 2 & 2 & -3 & -5 \\ 1 & 3 & -1 & 4 & -4 \\ 1 & -3 & -5 & -5 & 3 \\ 4 & -5 & -1 & 3 & 1 \end{pmatrix}.$$

We should also reduce a matrix A by the same matter, so

$$A1 = \begin{pmatrix} 2 & -3 & -1 & -5 & 4 \\ 3 & 3 & -1 & 4 & 4 \\ 2 & 2 & 0 & 0 & -2 \\ -5 & -3 & 2 & -3 & 0 \end{pmatrix}.$$

There is a dominance situation: line $A_2 \geq$ line A_1. Thus, A1 and B1 can be reduced:

$$A2 = \begin{pmatrix} 3 & 3 & -1 & 4 & 4 \\ 2 & 2 & 0 & 0 & -2 \\ -5 & -3 & 2 & -3 & 0 \end{pmatrix}; B2 = \begin{pmatrix} 1 & 3 & -1 & 4 & -4 \\ 1 & -3 & -5 & -5 & 3 \\ 4 & -5 & -1 & 3 & 1 \end{pmatrix}.$$

One can see, that column $B^1 \geq$ column B^3, so next step of reduction leads to

$$A3 = \begin{pmatrix} 3 & 3 & 4 & 4 \\ 2 & 2 & 0 & -2 \\ -5 & -3 & -3 & 0 \end{pmatrix}; B3 = \begin{pmatrix} 1 & 3 & 4 & -4 \\ 1 & -3 & -5 & 3 \\ 4 & -5 & 3 & 1 \end{pmatrix}.$$

There is also dominance situation: line $A_1 \geq$ line A_2 and line $A_1 \geq$ line A_3. Therefore, we can reduce 2 lines at once:

$$A4 = (3 \quad 3 \quad 4 \quad 4); B4 = (1 \quad 3 \quad 4 \quad -4).$$

Finally, we choose maximum element in the matrix-line $B4$ and corresponding element of the matrix-line $A4$. Return to the initial tensor help us to determine optimal strategies of the players:

			)		)
		)			)
	)				

Ergo, solution of this game concerns a choice 2-nd strategy by the player A and 4-th strategy by the player B. Herewith they gain the same win, equal to 4 cond. u.

a. Simplify payoff tensor P of the game and find it's solution using interactive input of P with help of Mathematica.

Solution to Exercise 2 b)

To do this we use the code, generated for the Example 4 b).

This particular situation was when the payoff matrices were squares. However, of the situation contains a payoff matrix that is not a square, things become more difficult to compare. The cycles, generated for reducing of these matrices reduction, should be organized separately.

```
y = 0; x = Array[0 &, n]; z = x; v = y;
(* Organizing 2-nd iteration loop for reducing rows of payoff matrixes A and B *)
For[i = 1, i < m, i++,
 For[k = i + 1, k < m + 1, k++,
  For [j = 1, j < n + 1, j++,
   If[TrueQ[a[[i, j]] ≥ a[[k, j]]], x[[j]] = 0, x[[j]] = 1]; y = y + x[[j]];
   If[TrueQ[b[[j, i]] ≥ b[[j, k]]], z[[j]] = 0, z[[j]] = 1]; v = v + z[[j]] ;
          ]; If[y = 0, a = Drop[a, {k, k}];
   b = Drop[b, {k, k}];
   Print [k, "-th line of the matrixes A and B are reduced"]];
  If[y = 3, a = Drop[a, {i, i};
     b = Drop[b, {i, i}]];
   Print [i, "-th line of the matrixes A and B are reduced"]];
  If[v = 0, b = Drop[b, None, {k, k}]; a = Drop[a, None, {k, k}];
   Print [k, "-th column of the matrixes A and B are reduced"]] ;
  If[v = 3, b = Drop[b, None, {i, i}];
   a = Drop[a, None, {i, i}];
   Print [i, "-th column of the matrixes A and B are reduced"]]];
 y = 0;
 v = 0 ] ;
Print["Reducing payoff matrix A after excluding dominated rows ", MatrixForm[a]];
Print["Reducing payoff matrix B after excluding dominated rows ", MatrixForm[b]]
```

Reducing payoff matrix A after excluding dominated rows $\begin{pmatrix} 4 \\ 2 \\ 3 \end{pmatrix}$

Reducing payoff matrix B after excluding dominated rows $\begin{pmatrix} 3 \\ 1 \\ 0 \end{pmatrix}$

```
{InputField[m2, FieldSize → 5], InputField[n2, FieldSize → 5]}
(* Interactive input of new payoff matrix dimesion *)
```

{3, 1}

Figure 5. Mathematica code for payoff matrix reduction (Example 4). Part 3

3. Mixed Strategies in 2x2 Bimatrix Games.

One of the most well-known example in game theory is called battle of the sexes (BoS) which is a two player coordination game. The backstory behind BoS is that a male and a female is planning to go on a date and they are deciding how to spend their time together. The male wants to go watch a soccer game while the female wants to go shopping. (The specific activities doesn't matter) But more importantly, both the male and the female want to go together. The following table shows the possible outcome.

		woman	
man		soccer	theatre
	soccer	(2 times happy, happy)	(not happy, not happy)
	theatre	(not happy, not happy)	(happy, 2 times happy)

This table shows that there are four possible outcome. The best options in this situation would be that the male and the female decide on the same thing while the worst options in this situation would be that they decide on different things. For example, if the man and the woman decide to watch the soccer game, the man is extremely happy because he gets to watch soccer and be with the women while the woman is happy because she gets to be together with the man. This game can be divided up into two cases.

1. With probability
2. Without probability

If the man and the woman make the same choice, and equilibrium is achieved, given the situation that they don't regret their own decisions. However, things get more complicated if we assume that the man and the women will choose their strategy/activty based on some probability.

***Definition* 2** *Mixed strategies* of the players A and B in bimatrix game 2x2 are a set of probabilities $X=(p,1-p)$, $Y=(q,1-q)^T$, with which the players choose their pure strategies.

Here we suppose that the players have next payoff matrices:

$$A=\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix},\ B=\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$$

***Definition* 3** The result of multiplying matrix $A=\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ by the column $C=\begin{pmatrix} c_1 \\ c_2 \end{pmatrix}$ is a column $D=\begin{pmatrix} d_1 \\ d_2 \end{pmatrix}$, where $d_i = a_{i1}c_1 + a_{i2}c_2$ [9].

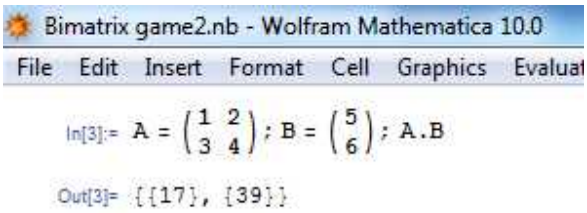
Example 5

Let's multiply $A=\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ by $C=\begin{pmatrix} 5 \\ 6 \end{pmatrix}$.

Due to rule, we have

$$AC=D=\begin{pmatrix} 1\cdot 5+2\cdot 6 \\ 3\cdot 5+4\cdot 6 \end{pmatrix}=\begin{pmatrix} 17 \\ 39 \end{pmatrix}.$$

This can performed in MATHEMATICA:



Exercise 3

Multiply $A=\begin{pmatrix}-1 & 2\\ -3 & 0\end{pmatrix}$ by $C=\begin{pmatrix}4\\ -5\end{pmatrix}$

a. "by hand"

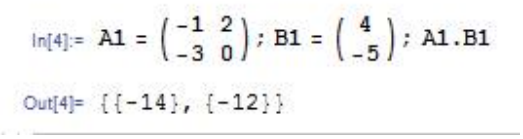
b. with help of MATHEMATICA

Solution

a. Due to rule, we have

$$AC=D=\begin{pmatrix}-1\cdot 4+2\cdot(-5)\\ -3\cdot 4+0\cdot(-5)\end{pmatrix}=\begin{pmatrix}-14\\ -12\end{pmatrix}$$

b.



***Definition* 4** *The expected payoff* of the players A and B are the values $H_1=X\cdot(AY)$ and $H_2=(XB)\cdot Y$ respectively.

Example 6

Let's define expected payoff in the game "family dispute", if both players choose their pure strategies with equal probabilities: X=(1/3,2/3); Y=(2/3,1/3).

Solution

First we write payoff matrices in numeric format:

$$A=\begin{pmatrix}2 & 0\\ 0 & 1\end{pmatrix},\ B=\begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix}.$$

Then we calculate $H_1=\left(\frac{1}{3}\ \frac{2}{3}\right)\begin{pmatrix}2 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}2/3\\ 1/3\end{pmatrix}=\left(\frac{1}{3}\ \frac{2}{3}\right)\begin{pmatrix}4/3\\ 1/3\end{pmatrix}=4/9+2/9=2/3$[1].

And, by the similar way we get $H_2=\left(\frac{2}{3}\ \frac{1}{3}\right)\begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix}\begin{pmatrix}1/3\\ 2/3\end{pmatrix}=\left(\frac{2}{3}\ \frac{1}{3}\right)\begin{pmatrix}1/3\\ 4/3\end{pmatrix}=2/9+4/9=2/3.$

In MATHEMATICA one can do it as

$$X = (1/3\ \ 2/3);\ Y = \begin{pmatrix} 2/3 \\ 1/3 \end{pmatrix};\ A2 = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix};\ B2 = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix};$$

In[6]:= H1 = X.A2.Y

Out[6]= $\left\{\left\{\frac{2}{3}\right\}\right\}$

In[7]:= H2 = X.B2.Y

Out[7]= $\left\{\left\{\frac{2}{3}\right\}\right\}$

Definition 5: In essence, the Nash mixed equilibrium in the bimatrix game is a combination of mixed strategies of x and y where x is the most appropriate response to the strategy y and vice versa.

In other words, in a mixed equilibrium an action of an individual player changing his strategies alone does not bring profit to anyone. To demonstrate this definition we prove, that X=(1/3,2/3); Y=(2/3,1/3) is mixed equilibrium in the game "family dispute" or also known as Battle of Sexes as we already talked about in this paper.

Example 7

Let's denote pure strategies of the players as S (soccer game) and T (theatre) (or any stereotypical male and female activities); equilibrium mixed strategies $P^*=(p^*,1-p^*)$ for husband and $Q^*=(q^*,1-q^*)$ for wife.

Due to the definition 5 we have

$$H_1(S, q^*) = H_1(T, q^*), \qquad (2)$$

i.e. the win of the player 1 should not change, if he will play his pure strategy "S" or "T" instead of his mixed equilibrium strategy p^* (provided player 2 – wife – plays her mixed equilibrium strategy q^*).

Similar situation for the win of the second player:

$$H_2(p^*,S) = H_2(p^*,T), \qquad (3)$$

i.e. the win of the player 2 should not change, if she will play his pure strategy "S" or "T" instead of his mixed equilibrium strategy q^* (provided player 1 – husband – plays his mixed equilibrium strategy p*).

Calculating $H_1(S, q^*)$ and $H_1(T, q^*)$ using formula (1) with S=(1,0) and T=(0,1) we get

$$H_1(S, q^*)=(1,0)\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}\cdot\begin{pmatrix} q^* \\ 1-q^* \end{pmatrix}=2\cdot q^*+0\cdot(1- q^*)=2\, q^*;$$

$H_2(T, q^*)=(0,1)\begin{pmatrix}2 & 0\\ 0 & 1\end{pmatrix}\cdot\begin{pmatrix}q^*\\ 1-q^*\end{pmatrix}=0\cdot 2q^*+1\cdot(1-q^*)=1-q^*.$

Equality (2) gives

$$2\,q^*=1-q^*\Rightarrow q^*=1/3.$$

Thus, $Q^*=(1/3,2/3)$.

Analogically,

$H_2(p^*,S)=(p^*,1-p^*)\begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix}\cdot\begin{pmatrix}1\\ 0\end{pmatrix}=p^*;$

$H_2(p^*,T)=(p^*,1-p^*)\begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix}\cdot\begin{pmatrix}0\\ 1\end{pmatrix}=2-2p^*.$

Equality (3) gives

$p^*=2-2p^*\Rightarrow p^*=2/3.$

Thus, $P^*=(2/3,1/3)$.

Such equilibrium means, that each player should choose what he likes in two thirds of cases, and what likes his opponent – in one third of cases.

Exercise 4

Another example we can investigate is known as the "The struggle for markets".

In "the struggle for markets" there are essentially two players, player 1 (a small company) and player 2 (a bigger company).In this specific situation, player 1 wants to sell a large quantity of goods in one of the two markets controlled by another. To accomplish this, he has two options. The first option is that he can take one of the market (for example, to develop an advertising campaign). In response to this certain strategy, the dominant player 2 might take precautionary measure to prevent this from happening. If player 1 doesn't encounter any obstacles, player 1 captures the market. However, if he encounters any obstacle, he is defeated. Selection markets by firms are their pure strategies.

Let the first market be more favorable for the player 1, but fighting for the first market requires a lot of budget. It is known that winning the first market would bring player 1 the double the profit compared from the second market. In the same sense, if player 1 loses the first market (his loss is 10) and player 2 gets rid of his competitor (his payoff is 2)

Described bimatrix game can be defined by the payoff matrices:

$$A=\begin{pmatrix}-10 & 2\\ 1 & -1\end{pmatrix},\ B=\begin{pmatrix}2 & -2\\ -1 & 1\end{pmatrix}$$

where 1 unit is equal to \$100 000.

The task is

a. Find mixed equilibrium with help of formulas (2)-(3) with help of MATHEMATICA.
b. Calculate the expected payoff of the firms, if they choose their mixed equilibrium strategies "by hand".

Solution

a. Let's denote pure strategies of the players as *I* and *II*; equilibrium mixed strategies $P^*=(p^*,1-p^*)$ for the 1-st firm and $Q^*=(q^*,1-q^*)$ for the 2-nd firm.

Conditions of mixed equilibrium will have a form:

$H_1(I, q^*) = H_1(II, q^*);\qquad H_2(p^*,I) = H_2(p^*,II).$

Do the same procedure as in example 7, we get

$H_1(I, q^*)=(1\ \ 0)\begin{pmatrix}-10 & 2\\ 1 & -1\end{pmatrix}\begin{pmatrix}q^*\\ 1-q^*\end{pmatrix}$=2-12q*.

$H_1(II, q^*)=(0\ \ 1)\begin{pmatrix}-10 & 2\\ 1 & -1\end{pmatrix}\begin{pmatrix}q^*\\ 1-q^*\end{pmatrix}$=-1+2q* (4)

So, $H_1(I, q^*) = H_1(II, q^*)$ gives equation 2-12q*=-1+2q* ⇒ q*=3/14. Hence, Q*=(3/14;11/14).

Analogically,

$H_2(p^*,I)= (p^*,1-p^*)\begin{pmatrix}2 & -2\\ -1 & 1\end{pmatrix}\cdot\begin{pmatrix}1\\ 0\end{pmatrix}$=-1+3p*;

$H_2(p^*,II)= (p^*,1-p^*)\begin{pmatrix}2 & -2\\ -1 & 1\end{pmatrix}\cdot\begin{pmatrix}0\\ 1\end{pmatrix}$=1-3p*. (5)

So, $H_2(p^*,I)=H_2(p^*,II)$ gives equation $-1+3p^*=1-3p^*\Rightarrow p^*=1/3$. Hence, P*=(1/3;2/3).

This result have got by the next action in MATHEMATICA:

```
In[10]:= X3 = {0, 1}; A3 = {{-10, 2}, {1, -1}}; Y3 = {{q}, {1 - q}}; X3.A3.Y3
Out[10]= {-1 + 2 q}

In[11]:= X4 = {1, 0}; X4.A3.Y3
Out[11]= {2 (1 - q) - 10 q}

In[21]:= X5 = {p, 1 - p}; B5 = {{2, -2}, {-1, 1}}; Y5 = {{0}, {1}}; X5.B5.Y5
Out[21]= {1 - 3 p}

In[22]:= X5 = {p, 1 - p}; B5 = {{2, -2}, {-1, 1}}; Y5 = {{1}, {0}}; X5.B5.Y5
Out[22]= {-1 + 3 p}
```

b. To calculate the expected payoff of the firms sufficient to substitute into expressions (4) and (5) found values $p^*=1/3$ and $q^*=3/14$. Thus we have $H_1=-1+2q^*=-4/7\approx-0.57$; $H_2= -1+3p^*=0$.

As we see, an expected loss of the 1-st firm is $57000 and expected profit of the 2-nd firm is zero.

4. Conclusion

In this paper, we have looked at Nash equilibrium and I've learned how it can be specifically applied to our world. By looking at different instances and exercises, we have proved that in Nash equilibrium, the relative playoffs are always balanced. If given more time, I would like to further investigate about the ultimatum game because of its complexity. It has an infinite number of strategies per player and I would like to learn how the maximum benefit is calculated. Like the name suggests, game theory is in essence a theory which means that it is not perfect. So, another part I would like to learn more about is how accurate game theory actually is when applied to real-life scenarios and actual data.

References

A.P. Jurg. Some topics in the theory of bimatrix games / Nijmegen: NICI, Nijmeegs Instituut voor Cognitie en Informatie.-III. 1993.

Ferguson Thomas S. Game Theory, Second Edition, 2014 URL: http://www.math.ucla.edu/~tom/Game_Theory/Contents.html

Hands-on Start to Mathematica [Internet source] URL: https://www.wolfram.com/broadcast/screencasts/handsonstart/

J. Nash, R. Selten, and J. Harsanyi. A Brief Introduction to NON-COOPERATIVE GAME THEORY. URL: http://www.ewp.rpi.edu/hartford/~stoddj/BE/IntroGameT.htm

Myerson R.B. Game theory. Analysis of Conflict. Harvard University Press, 1997

Solving the Traveling Salesman Problem with Genetic Algorithms

Sarah Bayer

Abstract

The Traveling Salesman Problem is a classic optimization problem, which entails finding the most efficient path when commuting to several cities given the number of cities and the distances between each one. For problems such as these, it is inefficient to use conventional programming methods, such as brute force. Instead, a heuristic or meta-heuristic method is more appropriate. I modelled my research paper around using genetic algorithms to solve this problem.

1. Introduction

For decades, humans have been fascinated by the concept of artificial intelligence. This curiosity has been reflected in our science fiction works, such as the chilling tale of HAL 9000 in 2001: A Space Odyssey (1968), the M-5 computer controlling the Enterprise in Star Trek: The Original Series (1968), and the destructive Skynet portrayed in the Terminator series (1984). As computational power grows exponentially greater, the line between these science fiction concepts and reality becomes blurred In fact, research firm Gartner claims that 85% of all customer interactions will not require a human by 2020 and Forrester predicts that artificially intelligent machines will replace up to 16% of all US jobs in the same time period. Just earlier this year, Google's AlphaGo, a computer program which uses an algorithm to find moves, defeated Go World Champion Lee Sedol for the first time in human history. It is clear that AI is becoming more developed and increasingly prevalent in our lives.

One of the pioneers of artificial intelligence was the British computer scientist Alan Turing. After helping the Allies defeat Nazi Germany in WWII by decrypting the Enigma Machine, Turing's curiosity settled on machines that "think" in 1950. He developed the Turing test to determine whether or not a machine can "think" like a human. During this same period, many computer scientists began studying evolutionary systems, recognizing its potential to be used as an optimization tool for engineering problems. The concurrent developments of these ideas led to the invention of genetic algorithms by John Holland in 1960.

Charles Darwin's publication, On the Origin of Species, was the first to propose the idea that a population could evolve over generations through random mutations and the process of natural selection. Darwin's publication held major implications for optimization using artificial intelligence. Holland realized that many optimization problems could be solved by simulating the process of natural selection described by Darwin. Genetic algorithms work by performing a search using a set of chromosomes and updating them at each generation during a search. These algorithms are different to traditional random search algorithms, which are inherently inefficient due to the directionless nature of their search. Genetic algorithms are random search algorithms that are not directionless. Genetic algorithms utilize information from previous generations in order to ensure that the new generation being constructed will approach an optimal solution. In other words, they use past knowledge to direct the search.

Every genetic algorithm begins with an initial randomly generated population of N chromosomes where each chromosome represents a different solution to the problem. The algorithm calculates a fitness score, which is proportional to how effectively the chromosome solves the problem, for each of these chromosomes. Two members are selected from the population based upon the fitness score. Once they are selected, the crossover rate is used to determine whether or not the chromosomes should exchange their bits (genetic information). If the crossover rate is met, the two chromosomes exchange bits at a randomly chosen point and produce an offspring chromosome containing a mixture of both parents' genetic information. The algorithm now steps through each bit of this offspring and flips it depending on the mutation rate. The member of the population with the lowest fitness score is eliminated to maintain a population of N chromosomes. This process is repeated until at least one member of the population possesses a desired fitness score.

1.1 Searching

Search plays a major role in solving many Artificial Intelligence (AI) problems, and is a universal problem solving mechanism in AI. In many problems, the sequence of steps is not known in advance but must be known by systematic trial.

In single-player games such as tile games, Sudoku, crossword, etc., the search algorithms help you to search for a particular position[11].

1.2 Problem Solving by Search

An important aspect of intelligence is goal-based problem solving. The solution of many problems (e.g. noughts and crosses, timetabling, chess) can be described as finding a sequence of actions that lead to a desirable goal. Each action changes the *state* and the aim is to find the sequence of actions and states that lead from the initial (start) state to a final (goal) state.

1.3 Steps in Searching[12]

1. Check whether the current state is the goal state or not.
2. Expand the current state to generate the new sets of states.
3. Choose one of the new states generated for search depending upon search strategy.
4. Repeat step 1 to 3 until the goal state is reached or there are no more state to be expanded.

A well-defined problem can be described by:

Initial state

Operator or successor function - for any state x returns $s(x)$, the set of states reachable from x with one action
State space - all states reachable from initial state by any sequence of actions
Path - sequence through state space
Path cost - function that assigns a cost to a path. Cost of a path is the sum of costs of individual actions along the path
Goal test - test to determine if at goal state

1.4 Types of Search

1. Uninformed (Blind) Search
2. Informed (Heuristic) Search
3. Best First Search
4. Greedy Best First Search
5. A * search

1.4.1 Uninformed Search (Blind Search)

In uninformed search, we do not try to evaluate which of the nodes on the frontier are most promising; we never "look-ahead" to the goal. While moving forward, a heuristic algorithm gives advance knowledge of the path to be followed at each node.

1.4.2 Informed Search (Heuristic Search)

Informed search has problem specific knowledge apart from the problem definition. The use of heuristic search improves efficiency of the search process [14]. The idea is to develop a domain specific heuristic function $h(n)$ which guesses the cost of getting to the goal from node n.

1.4.3 Best First Search

In this, node is selected for expansion based on evaluation of function $f(n)$. Node with lowest evaluation function is expanded first. The evaluation function must represent some estimate of the cost of the path from state to the closest goal state. The heuristic function $h(n)$ estimates the cost of the cheapest path from node n to the goal[15].

1.4.4 Greedy Best First Search

The algorithm tries to get as close as it can to the goal. It expands the node that appears to be closest to the goal and evaluates the node by only using a heuristic function[18].
The Evaluation function is $f(n) = h(n)$

where
(heuristic)= (estimate of cost from n to goal)
$h(n) = 0$ for goal state

1.4.5 A * search

Greedy best first search analyses nodes with the lowest cost of node n to reach the goal, but it may get stuck in search of its goal. The idea of the A * search is to avoid expanding paths that are already expensive.
The Evaluation function is given by $f(n) = g(n) + h(n)$

where
$g(n)$ = cost so far to reach n
$h(n)$ = estimated cost from n to goal
$f(n)$ = estimated total cost of path through n to goal

The search process requires proper nodes or states that are created through the state space. The search process is carried out by constructing a search tree and involves systematic trial and error exploration of alternative solutions. Proper nodes are created through this search tree. Many problems do not have a simple algorithmic solution, because the sequence of actions required to solve the problem is not known[19]. Casting these problems as search problems is often the easiest way of solving them.

- Path finding problems, e.g. eight puzzle, traveling salesman problem
- Two player games, e.g. chess and checkers
- Constraint satisfaction problems, e.g. eight queens

2. Travefling Salesman Problem

The problem is as follows: A salesman wishes to visit a list of cities, each exactly once, for his business. He begins and ends his journey at his hometown, which is included in the list of cities. Our objective is to find out the shortest possible round trip route for the salesman given the distance between each pair of cities [1, 2].

We have labeled the hometown of the salesman City 1. He wishes to visit eight other cities: City 2, City 3, City 4, City 5, City 6, City 7, City 8 and City 9. The salesman must start his journey from City 1, visit all eight cities once, and return to his hometown, City 1. Our goal is to optimize his route by finding out the order in which he should visit each city so that his total traveling distance is minimized. The distances between each city are displayed in Table 1 below.

Table 1: *Matrix showing distance between each pair of cities*

	City 1	City 2	City 3	City 4	City 5	City 6	City 7	City 8	City 9
City 1	0	3852 km	3352 km	3417 km	1000 km	3006 km	3539 km	3002 km	2550 km
City 2	3852 km	0	700 km	790 km	4800 km	965 km	595 km	2523 km	1295 km
City 3	3352 km	700 km	0	442 km	4364 km	831 km	196 km	2662 km	1276 km
City 4	3417 km	790 km	442 km	0	4375 km	403 km	541 km	2234 km	849 km
City 5	1000 km	4800 km	4364 km	4375 km	0	3965 km	4903 km	3527 km	3509 km
City 6	3006 km	965 km	831 km	403 km	3965 km	0	932 km	1845 km	455 km
City 7	3539 km	595 km	196 km	541 km	4903 km	932 km	0	2768 km	1395 km
City 8	3002 km	2523 km	2662 km	2234 km	3527 km	1845 km	2768 km	0	1496 km
City 9	2550 km	1295 km	1276 km	849 km	3509 km	455 km	1395 km	1496 km	0

We initially solve the problem at a smaller scale using four cities without genetic algorithms so that we can later apply similar principals to solve for nine cities using genetic algorithms. We are only considering the first four cities in the matrix, with City 1 being the hometown of the salesman. In this scenario, we have six possible paths, as shown in Figure 1, and we wish to find the shortest one. We can represent Path 1 as 1 – 2 – 3 – 4 – 1, where 1 means City 1, 2 means City 2 and so on. If the salesman chooses Path 1, he will visit the cities in the following order:

City 1 – City 2 – City 3 – City 4 – City 1

Let us evaluate each path as follows:

Path 1 is represented by 1-2-3-4-1. Total traveling distance of Path 1 is: 3852 km + 700 km + 442 km + 3417 km = 8411 km.

Path 2 is represented by 1-2-4-3-1. Total traveling distance of Path 2 is: 3852 km + 790 km + 442 km + 3352 km = 8436 km.

Path 3 is represented by 1-3-2-4-1. Total traveling distance of Path 3 is: 3352 km + 700 km + 790 km + 3417 km = 8259 km.

Path 4 is represented by 1-3-4-2-1. Total traveling distance of Path 4 is: 3352 km + 442 km + 790 km + 3852 km = 8436 km.

Path 5 is represented by 1-4-2-3-1. Total traveling distance of Path 5 is: 3417 km + 790 km + 700 km + 3352 km = 8259 km.

Path 6 is represented by 1-4-3-2-1. Total traveling distance of Path 6 is: 3417 km + 442 km + 700 km + 3852 km = 8411 km.

Therefore, the shortest path is path 3 and path 5, both with a total travelling distance of 8259 km. So, the salesman should follow either Path 3, which is 1 – 3 – 2 – 4 – 1, or Path 5, which is 1 – 4 – 2 – 3 – 1, for his business journey.

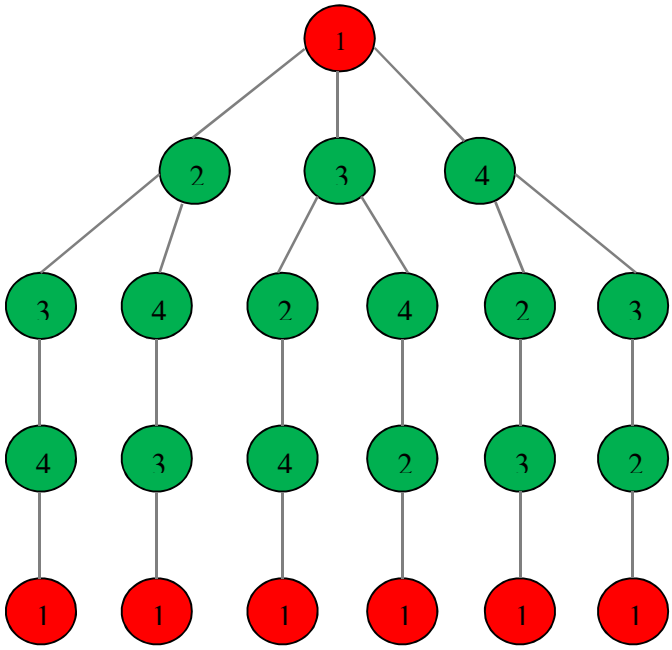


Figure 1: *A tree showing six different possible paths*

3. P, NP and NP-Complete Problems

Computational complexity theory is branch of theory of computation in computer science and mathematics that focus on classifying computational problems according to their inherent difficulties or complexity. It includes the efficiency of algorithms and the inherent difficulty of problems of practical and or theoretical importance[13].

In other words, computational complexity theory is a part of theory of computation that deals with the resources required during computation to solve a given problem. The most common resources are time (how many steps it takes to solve a problem) and space (how much memory it takes).

There are two kinds of measures with Complexity Theory: (a) time and (b) space.

a. **Time Complexity**: It is a measure of how long a computation takes to execute. As far as a Turing machine is concerned, this could be measured as the number of moves which are required to perform a computation. In the case of a digital computer, this could be measured as the number of machine cycles which are required for the computation.

b. **Space Complexity**: It is a measure of how much storage is required for a computation. In the case of a Turing machine, the obvious measure is the number of tape squares used, while for a digital computer, it is the number of bytes used.

The Class P[16]

Computing practice reveals that many problems which are solvable in theory cannot be solved in practice due to the excessive time requirement. For example, in the Traveling Salesman Problem, if there are n cities to visit, it requires $(n-1)!$ itineraries (record of root of journey). If there are 10 cities, it requires $9! = 362880$ itineraries. However, if there are 40 cities it requires considerably more itineraries than for 10 cities. Hence we can say that some problems which are theoretically compostable are not practically feasible at all.

In order to be a practically feasible algorithm, we must limit our computational devices to only run for a certain number of steps that is bound by a polynomial in the length of inputs.

We can define solvable problems as:

When the space and time required for implementing the steps of the particular algorithm are reasonable, then we can say that problem is solvable or tractable in practice.

5. The Class NP

A nondeterministic computation is viewed as[17]:

a. When a choice point is reached, an infallible oracle can be consulted to determine the right option.
b. b) When a choice point is reached, all choices are made and computation can proceed simultaneously.

A non-deterministic polynomial time algorithm is one that can be executed in polynomial time on a nondeterministic machine. The machine can either consult an oracle in constant time, or it can spawn an arbitrarily large number of parallel processes.

3.1 Examples of Class NP Problems

3.1.1. Traveling Salesman Problem

See above.

3.1.2. The Hamiltonian Circuit Problem[18]

Every capital city has direct air flights to at least some capital cities. Our intrepid salesman wants to visit all the capitals, and return to his starting point, taking only direct air flights. Can he find a path that lets him do this?

3.1.3. Linear Programming

We have on hand X amount of butter, Y amount of flour, Z eggs etc. We have cookie recipes that use varying amounts of these ingredients. Different kinds of cookies have different prices. What mix of cookies should we make in order to maximize profits?

In computational complexity theory, there are fundamentally two classes of problems: P and NP. P-type problems, which stands for polynomial time, indicates the set of all problems that are solvable in deterministic polynomial time. NP-type problems, which stands for non-deterministic polynomial time, indicates the set of all problems that are verifiable, but not solvable, in polynomial time. A problem p in NP is also NP-Complete only if every other problem in NP can be polynomial time reducible to p. No deterministic polynomial time algorithm exists for solving the problems in the class NP-Complete. Therefore, P problems can be considered the set of easy or tractable problems and NP-Complete problems the set of hard or intractable problems, so we will find that P $\neq$ NP. However, if a deterministic polynomial time algorithm, which can solve any one problem from class NP-Complete, is found then all the problems contained in class NP-Complete will be solvable in polynomial time and we will find that P = NP. Some examples of NP-Complete problems are the traveling salesman problem, bin packing problem, machine layout problem, subset-sum problem, and the job-shop scheduling problem [3, 4, 5].

Consider the traveling salesman problem with n number of distinct cities. Solving the problem would require an exponential or factorial amount of time. If we assume that generating a single path requires 1 time unit and the total number of all possible paths is $(n-1)!$, generating all possible paths will require $1\,x\,(n-1)! = (n-1)!$ time units. Furthermore, evaluating a single path requires n time units, so the total time for this search is $(n-1)!\ x\,n = n!$ time units [1].

4. Genetic Algorithms

The traveling salesman problem is an optimization problem, making genetic algorithms a viable option to solve it. When dealing with a small number of cities, conventional programming can be used to solve this problem. However, as the number of cities increases, conventional programming becomes impractical. In these cases, heuristic or meta-heuristic methods are more appropriate, such as the case when there are more than 8 cities in the traveling salesman problem. For example, a greedy algorithm, which makes the optimal choice at each local stage (so that it always chooses the nearest neighbouring city), is a heuristic approach capable of finding a quick solution to the problem. However, the quality of the solution may not be globally optimal. A meta-heuristic genetic algorithm can optimally solve the problem when there are more than 8 cities.

4.1 Basics of Genetic Algorithms

Figure 2 shows a flow chart of a genetic algorithm. First, an initial population of size N is randomly generated. Each chromosome in the population is evaluated by a problem-specific fitness function. This function will give each chromosome a fitness score; the higher

the score, the more optimal the solution. In each iteration, the chromosomes with the highest fitness scores are stored by the computer. If the termination criteria is met, the computer searches through the stored chromosomes and returns the one with the highest fitness score. If the termination criteria is not met, the algorithm applies selection, crossover, and mutation operations until N offspring have been generated. The old population is replaced by these offspring, and this process is repeated until the termination criteria is met.

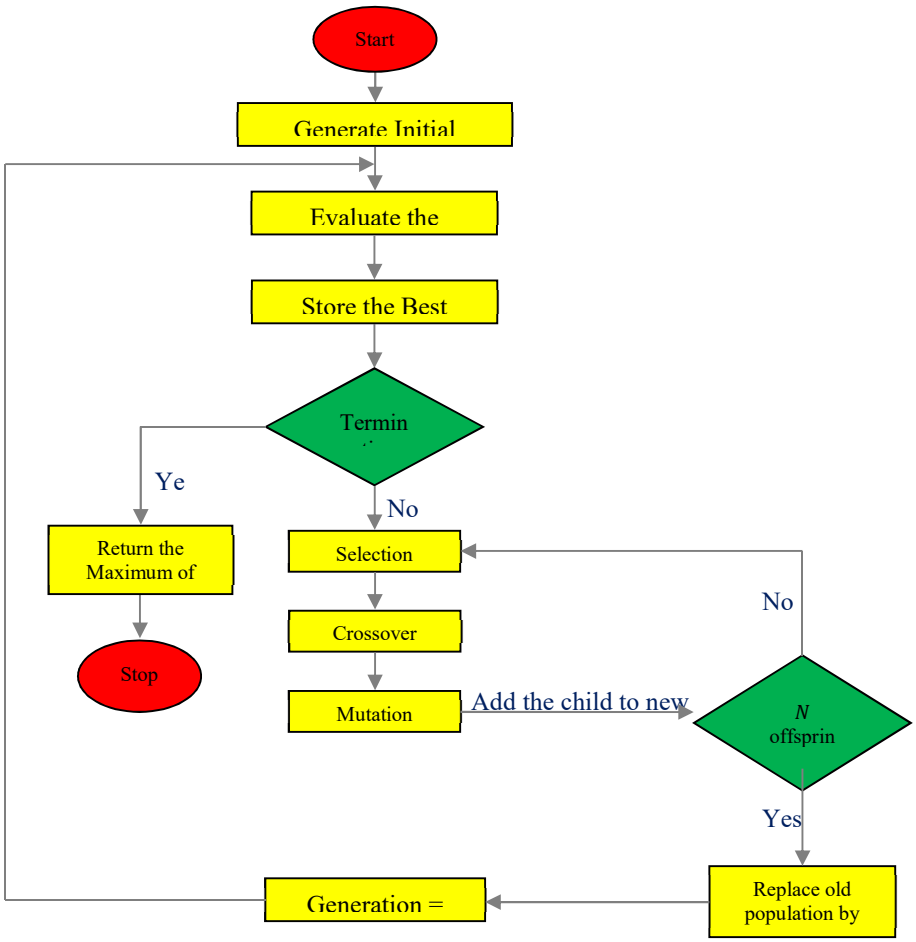


Figure 2: *Flow chart of genetic algorithm*

The following basic components of a genetic algorithm can be used to solve the problem [6]:

- Chromosome representation
- Initial population
- Fitness function
- Reproduction (selection) operator
- Genetic operators (crossover and mutation)
- Replacement strategy
- Parameters of genetic algorithm

- Termination criteria

The design of a genetic algorithm is as follows:

1. [**Start**]
2. **[Initial population]** Randomly generate an initial population of N chromosomes. Each chromosome represents a possible solution to the problem.
3. **[Fitness]** Evaluate the fitness $f(x)$ of each chromosome x in the population.
4. **[Store]** Store the best solutions in each iteration.
5. **[Test]** If the termination criteria is met, then return the maximum of the best solutions stores in each iteration as the final solution and **[stop]**. Otherwise, go to **step 6**.
6. **[New population]** Create a new population by repeating the following steps until N offspring have been generated.
   a. **[Selection]** Select two parent chromosomes from a population according to their fitness score.
   b. **[Crossover]** Using a crossover probability, apply the crossover operation on the selected parents to form offspring. If no crossover is performed, the offspring is an exact copy of the selected parents.
   c. **[Mutation]** Using a mutation probability, apply the mutation operation on the offspring.
   d. **[Accepting]** Place the new offspring in the new population.
7. **[Replace]** Replace the old population with the new population.
8. **[Increment]** Increment the generation completed by one.
9. [Loop] Go to step 3.

5. Steps of a Genetic Algorithm to Solve the Traveling Salesman Problem

5.1 Chromosome Representation

Binary encoding, permutation encoding, value encoding, tree encoding and others can be used to represent chromosomes. In permutation encoding [7], every chromosome is a string of numbers creating a sequence which makes it the best suited for ordering problems, such as the traveling salesman problem. When using permutation encoding, each chromosome represents a possible solution. The length of a chromosome is equal to one more than the number of cities considered in the problem.

Example of a chromosome:

1	4	6	2	5	9	8	3	7	1

In the example chromosome above, the length is 10 because we are considering 9 cities in the problem. Each gene represents a city, so 1 represents City 1, 2 represents City 2, and so on. This sequence of numbers shows the route that the salesman will take. In the above example, the salesman will travel from City 1 to City 4 to City 6 and so on, until he ends his journey back in City 1.

5.2 Initial Population

40 randomly generated chromosomes are used as the initial population. Therefore, the initial population size N = 40. Each chromosome in the population must meet the following requirements:

1. The starting and ending gene in the chromosome must represent the hometown of the salesman.
2. All cities, except the hometown of the salesman, must appear exactly once in a chromosome.

5.3 Fitness Function

The fitness score represents how optimal the solution is and is evaluated using the fitness function. In the traveling salesman problem, the optimal solution is one which contains a smaller total traveling distance. Therefore, the fitness function is simply the inverse of the total traveling distance as follows:

$f(x)$ = 1 / total traveling distance represented by chromosome x

5.4 Selection Operator

The Roulette wheel selection method can be used in the traveling salesman problem [8]. This is a method of selection in which chromosomes are placed into the mating pool according to their fitness score. This can be visualized as a literal roulette wheel containing all the members of the population. The size of each chromosome in the wheel represents the magnitude of its fitness score. As shown in figure 3, chromosomes with a higher fitness score occupy a larger section of the roulette wheel.

Now imagine that we spin the roulette wheel and throw a marble in it while it rotates. When the roulette wheel stops, the chromosome containing the marble is selected. Through this visualization, we can see that the chromosomes with a higher fitness score are more likely to be selected.

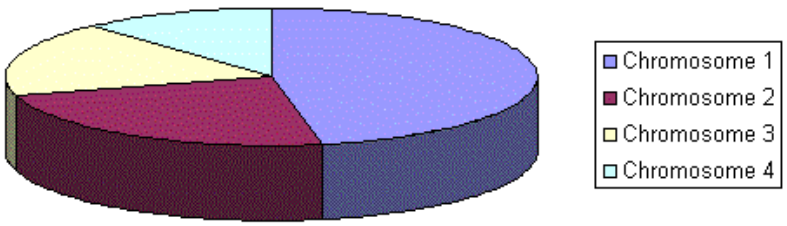


Figure 3: *Roulette wheel selection*

5.5 Crossover Operator

Crossover is the process used to combine information from two parents into an offspring. This operation is applied to all the chromosomes selected into the mating pool. Single point crossover is a common method of crossover used in genetic algorithms. When using this method, 1 crossover point is randomly selected in both parents (the crossover point should be at the same position in both chromosomes). The substring before the crossover point from Parent 1 is copied into Offspring 1 and the substring after the crossover point of Parent 2 is also copied into Offspring 1. The roles of Parent 1 and Parent 2 are reversed to create Offspring 2. This method of crossover can be demonstrated as the following:

In this example, we have omitted the hometown of the salesman in the first and last position of the chromosome because they are fixed. For the same reasons, the hometown of the salesman is also omitted in the mutation operation that follows. When the mutation operation is complete, we will append the hometown of the salesman to the first and last position of the chromosomes.

Note that in this example both offspring present infeasible solutions. Offspring 1 is infeasible because City 4 appears twice and City 3 no longer appears. In Offspring 2, City 3 appears twice and city 4 no longer appears. Due to the potential of infeasible solutions, single point crossover cannot be used to solve the traveling salesman problem. Instead, we will use order crossover [9], which never generates an infeasible solution. The process begins with two parents as follows:

As the diagram shows, we have selected two crossover points at positions 3 and 6 instead of just one. Order crossover is applied in the following steps:

1. Copy all genes between first and second crossover point from Parent 1 into Offspring 1 as follows:

2. Select a gene after the second crossover point from Parent 2. In this case, it is 7 and it does not yet exist in Offspring 1, so it is copied as follows:

Offspring 1

-	-	-	5	9	8	7	-

3. Select the next gene from Parent 2. In this case, it is 9 but it already exists in Offspring 1, so it is discarded.
4. Select the next gene from Parent 2. In this case, it is 3 and it does not yet exist in Offspring 1, so it is copied as follows:

Offspring 1

-	-	-	5	9	8	7	3

5. Select the next gene from Parent 2. In this case, it is 2 and it does not yet exist in Offspring 1, so it is copied as follows:

Offspring 1

2	-	-	5	9	8	7	3

6. Select the next gene from Parent 2. In this case, it is 6 and it does not yet exist in Offspring 1, so it is copied as follows:

Offspring 1

2	6	-	5	9	8	7	3

7. Select the next gene from Parent 2. In this case, it is 8 and but it already exists in Offspring 1, so it is discarded.
8. Select the next gene from Parent 2. In this case, it is 4 and it does not yet exist in Offspring 1, so it is copied as follows:

Offspring 1

2	6	4	5	9	8	7	3

Through these steps, we have created Offspring 1. The above steps are repeated, with the roles of Parent 1 and Parent 2 reversed, in order to create Offspring 2.

5.6 Mutation Operator

The mutation operator is used to model Darwin's theory of evolution through natural selection and to restore lost genetic information into the population. A common method of mutation is bitwise mutation which flips a randomly selected bit value from 0 to 1 or vice versa. However, we cannot use this method for the traveling salesman problem because it may generate infeasible solutions. Bitwise mutation applied at position 4 is demonstrated in the following diagram:

The new mutated offspring represents an infeasible solution because City 5 no longer exists in the chromosome and City 7 appears twice.

An alternative method is swap mutation [10], which never generates an infeasible solution. The process goes as follows:

1. Randomly select two genes from offspring.
2. Swap positions of genes selected in Step 1.

Swap mutation applied at position 3 and 6 is demonstrated in the following diagram:

5.7 Replacement Strategy

In every iteration, once all the offspring have been generated, all chromosomes in the old population are replaced by the new offspring population.

5.8 Parameters of a Genetic Algorithm

A set of parameters [6] are needed for a genetic algorithm. In order to converge to an optimal solution, these parameters must be fine-tuned. The following subsections describe each of these parameters.

5.8.1 Population Size

In a genetic algorithm, it is beneficial to have a larger population because it provides the algorithm more genetic material for selection, crossover and mutation. This allows it to converge to a more optimal solution. Therefore, a genetic algorithm that can handle better solutions are bigger, which causes an issue for the algorithm's speed. In each iteration, every chromosome's fitness must be evaluated. A larger population means that the computer must perform additional evaluations. As a result, the algorithm is performing computationally expensive procedures. Taking this into account, a population size of around 40 chromosomes is ideal. This number can vary depending on the evaluation complexity.

5.8.2 Crossover Rate

In the literature regarding genetic algorithms, crossover rate is conventionally denoted as p_c, the probability of crossover. As with any probability, the crossover rate varies from 0 to 1. It is calculated in genetic algorithms by solving for the number of pairs to be crossed to some fixed population. Typically, for a population size between 30 and 200, the crossover rate ranges from 0.5 to 1.

When we perform crossover on two chromosomes, we can see that there will be instances when the offspring produced may not contain a combination of ideal substrings based upon whether the crossover points fall into a beneficial place. However, our genetic algorithm accounts for this by ensuring that additional copies of appropriate offspring are added to the next mating pool at a higher rate. Furthermore, if high fitness chromosomes are not generated by crossover, the selection operators will ensure that they do not survive by selecting them at a low rate in subsequent generations. The crossover operator can have a beneficial or detrimental effect. In order to preserve the beneficial chromosomes in the mating pool, not all chromosomes are used in crossover.

If a crossover rate of Pc is applied, $100Pc$ % of the population will go through crossover while $100(1 - Pc)$ % will remain as it is in the current generation. We could deterministically copy the best chromosomes in the $100(1 - Pc)$ % of the current population to the new population, but we will do this at random because a crossover operation is mainly responsible for discovering new chromosomes.

To summarize, the crossover operation will not be applied on all selected chromosomes. In our algorithm, we will set *Pc* at 0.6 in order to preserve some of the chromosomes already represented in the mating pool. Therefore, the probability of crossover occurring is 60% for each selected chromosome.

5.8.3 Mutation Rate

The mutation rate is the probability of mutation occurring, which is the ratio of the number of offspring to be mutated to some fixed population. The mutation operator preserves the diversity among the population by providing more genetic material, which is important when searching for an optimal solution. In natural populations, mutation probabilities are quite small, which leads us to conclude that mutation is appropriately considered a secondary mechanism of genetic algorithm adoption.

It is difficult to decide on a fixed mutation rate for many reasons. A very high mutation rate will render the search ineffective because it will reduce it to being random as opposed to randomized. On the other hand, a very low mutation rate would cause premature convergence due to the lack of genetic material. Premature convergence may mean that high-quality solutions are never found. Therefore, we must strike a balance between the randomness of a high mutation rate and the risk of premature convergence posed by a low mutation rate. Typically, for a population size between 30 and 200, the mutation rate ranges from 0.001 to 0.5.

Just like the crossover operation, the mutation operation is not applied on all the selected chromosomes. However, the crossover and mutation rate must differ because, according to genetics, the crossover rate is always greater than the mutation rate. In our algorithm, we will set the mutation rate to 0.4, so the probability of mutation occurring is 40% for each selected chromosome.

5.8.4 Number of Genetic Generations

The number of genetic generations refers to how many iterations we perform before we stop the genetic algorithm. This will depend on the complexity of the task. Therefore, instead of hard-coding a predetermined number of iterations, we will stop when there is no improvement in the quality of the solution for a certain time. We can implement this by defining a set of limit conditions, taking the task's dimensions into account.

The following are common stopping criteria for genetic algorithms:

- Best chromosome found in population has not improved for last t generations.
- 90% or more of the best chromosomes share the same fitness score.
- Solution that satisfies minimum criteria has been found.
- Allocated budget (computation time, money, etc.) reached.
- Predetermined number of generations reached.
- Combinations of the above.

5.9 Stopping Criteria

The stopping criteria can also be called the number of genetic generations. In our algorithm, we will make it stop when it has completed 600 generations.

6. Advantages and Disadvantages of Genetic Algorithms

We can understand the strengths and weaknesses of genetic algorithms by comparing it with other search methods. This will also help highlight some important features of this class of algorithms. David Goldberg has performed this comparison to identify the ways in which genetic algorithms differ from other search and optimization methods. We can use these differences to discuss the advantages and disadvantages of genetic algorithms as follows:

- Genetic algorithms search a number of points at once rather than a single point at a time and uses this information to guide it. In a multi-modal search space, a point-to-point optimization method is particularly susceptible to false peaks. Because a genetic algorithm searches an entire population which represents a family of points in the search space, the likelihood of finding false peaks is lower than for a single-point method. However, single-point methods can be more efficient in certain search spaces.
- Genetic algorithms do not work by directly set parameters but rather with encoded parameters. It may be difficult to encode all problems in an appropriate way but the traveling salesman problem can be easily encoded.
- Genetic algorithms use a fitness function rather than auxiliary knowledge, to analyse the fit of a solution and therefore does not need any auxiliary information. Once a genetic algorithm analyses the fit of a point, it can use this to direct its search towards the optimal solution. Heuristic search techniques use domain-specific knowledge to guide the search. Their success depends on how a suitable heuristic is framed. For the traveling salesman problem, a genetic algorithm outperforms a heuristic search technique because the latter may not generate high quality solutions.
- A genetic algorithm's transition rules are probabilistic and not deterministic. Selection, crossover and mutation are all randomized processes so there is always a possibility that genetic material from unfit chromosomes will be passed on to the next generation. This stochastic nature of genetic algorithms means that it can find the optimal or near-optimal solution of optimization problems with a large input size in a practical length of time.
- Genetic algorithms are inherently parallel as it can deal with a large number of points simultaneously. This feature makes a genetic algorithm very powerful.
- Genetic algorithms possess robustness, efficiency and flexibility when searching a search space for the optimal solution.
- Genetic algorithms use both an exploration and exploitation mechanism to discover the optimal solution.

7. Conclusions

This tutorial has presented the basics of genetic algorithms, in the context of finding a near-optimal solution for an NP-Complete problem, such as the traveling salesman problem. We began by solving the problem with 4 cities without using algorithms. For slightly larger numbers such as 6, 7 or 8 cities, conventional programming methods, such as brute force, can be used to solve it but the length of time needed in order to solve for more than 8 cities is impractical. We used a genetic algorithm instead and have successfully solved the traveling salesman problem for 9 cities. While a genetic algorithm is capable of finding a near-optimal solution to the problem, it may return slightly different solutions.

References

Elaine Rich, Kevin Knight and Shivashankar B. Nair, 2008. Artificial Intelligence, Third Edition. *Tata McGraw-Hill Education Pvt. Ltd.*

Hoffman, K.L., Padberg, M. and Rinaldi, G., 2013. Traveling salesman problem. In *Encyclopedia of Operations Research and Management Science*(pp. 1573-1578). Springer US.

Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest and Clifford Stein, 2006. Introduction to Algorithms, Second Edition. *Prentice-Hall of India.*

Patel, J.N. and Patel, S.V., 2014. Approaches to solve cell formation, machine layout and cell layout problem: A Review. *Transactions on Machine Learning and Artificial Intelligence*, *2*(5), pp.80-96.

Chakraborty, S. and Bhowmik, S., 2015. Blending roulette wheel selection with simulated annealing for job shop scheduling problem. *Michael Faraday IET International Summit.*

Patel, J.N., 2011. Accuracy Comparison of Various Techniques to Solve Machine Layout Problem. *International Journal of Advanced Research in Computer Science*, *2*(1), pp.121-126.

Tian, Y., Ping, X.L., Bai, L.L. and Jiang, Y., 2015. An Improved Genetic Algorithm for the Travelling Salesman Problem. *International Journal of Electronics Communication and Computer Engineering*, *6*(6), pp.671-673.

Abdoun, O. and Abouchabaka, J., 2012. A comparative study of adaptive crossover operators for genetic algorithms to resolve the traveling salesman problem. *International Journal of Computer Applications,* 31(11), pp.49-57.

Abdoun, O., Abouchabaka, J. and Tajani, C., 2012. Analyzing the performance of mutation operators to solve the travelling salesman problem. *International Journal Of Emerging Sciences (IJES),* 2(1).

Önder, E., Ozdemir, M. and Yıldırım, B.F., 2013. Combinatorial Optimization Using Artificial Bee Colony Algorithm and Particle Swarm Optimization Supported Genetic Algorithm. *Kafkas University Journal of Economics and Administrative Sciences Faculty*, *4*(6), pp.59-70.

D. W. Patterson, 2010. Artificial Intelligence and Expert Systems, Prentice Hall.

P. H. Winston, 2008. Artificial Intelligence, Addison Wesley.

H. R. Lewis, C. H. Papadimitriou, "Elements of theory of computation", Pearson Education.

P. H. Winston, 2008, Artificial Intelligence, Addison Wesley.

Stuart Russel and Peter Norvig, 2010. Artificial Intelligence A Modern Approach, Pearson

Michael Sipser, "Introduction to the Theory of Computation", Thomson Course Technology.

Michael S., 2006. Introduction to the Theory of Computation (second edition), Thomson Course Technnology, Boston

Nils J. N., 2009. "Artificial Intelligence: A New Sythesis", Elsevier

N. P. PADHY, 2005. Artificial Intelligence and Intelligent Systems 1st Edition, Oxford University Press, USA.

Glossary

- **Chromosome:** The candidate solution to a problem.

- **Crossover:** The process of exchanging the part of representation solutions between two candidate solutions.
- **Encoding:** Expressing the possible solutions in an appropriate way.
- **Exploitation:** To make use of knowledge found at points previously visited to help find better points.
- **Exploration:** To investigate new and unknown areas in the search space.
- **Fitness:** A measure of the suitability of a possible solution to be selected to create the next generation.
- **Gene:** The smallest unit in a genome. Each city is represented by a gene in the permutation encoding of the traveling salesman problem.
- **Generation:** An iteration of the genetic algorithm.
- **Meta-heuristics:** A framework of heuristics used to update a set of solutions during a search.
- **Mutation:** The process of changing the candidate solution possibly by swapping positions of two genes.
- **Optimum solution:** The best solution
- **Population:** The entire set of chromosomes.
- **Selection:** The genetic operator that selects the chromosomes, according to their fitness score, into the mating pool in order to apply the crossover operation on them.
- **Search Space:** The space for all possible feasible solutions.

Neural Network Key Exchange Protocol for Encrypted Communication

Daniel Lee and Ivan Stanimirovic
Charterhouse School

Abstract

Given the huge increase in the use of smartphones, tablets, notebooks and Internet as a means of communication and collaboration, it is necessary to develop security mechanisms to protect the private information of each user. Thus, cryptography has become an ever growing field responsible for the security of our online activities. An important aspect of any symmetric encryption protocol is the key exchange protocol, during which the sender and receiver of information agree upon a specific key that will be used in the encryption and decryption processes. However, this key exchange process must also be secure in order to ensure the security of the encryption scheme that it supports. Surprisingly, artificial neural networks can aid in this key exchange process. In this paper, we delineate how neural networks work generally, show briefly how RSA encryption works, outline the process in which neural networks are used to exchange keys, and then successfully implement the neural network key exchange protocol using Mathematica.

1. Introduction

The study of neural networks began in 1943 by working on neurophysiology and mathematical logic by McCulloch and Pitts. From then on, it is developed as models to represent and simulate how the human brain performs a task or a function. Normally, artificial neural network would require a lot of research within the topics of: neuroscience, mathematics, statistics, computer science and physics. For instance, the most important feature of our body that we need to be aware of two research on artificial neural network is shown in Figure 1. This diagram represents a schematic of a biological neuron. Its key elements are the cell body, dendrites structures formed by the (receiving stimuli), the axon and synaptic terminals, the end of the axon, which transmit the output signals as electrical pulses. These impulse starts in the cell body and transmitted through the axon to other neurons. These output signals could stimulate or inhibit other neurons.

Not only this, the ability to learn and study the given information, neural networks benefits various application areas, such as pattern recognition, sensor systems, signal processing, image processing and cryptography, and others.

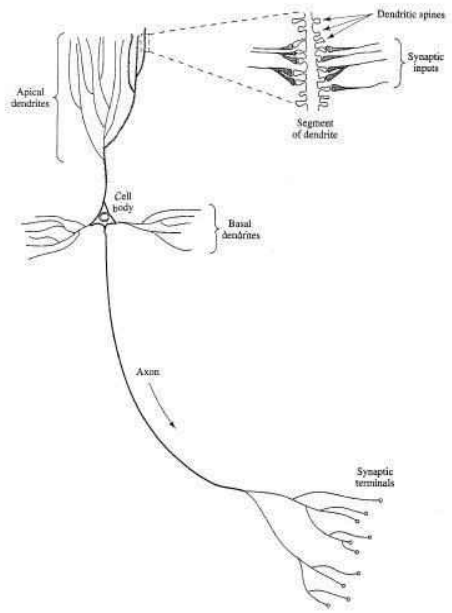


Figure 1: Schematic view of a biological neuron

Firstly, talking about encryption which takes a big part in the study of neural networks, it is important for us to know its roots and how it developed over the years. In the early days, encryption was used mainly by the Romans to conceal their military tactics, so that when or if the message was intercepted by the enemy at any point, they wouldn't be able to figure out what the Romans were intending to do. This was mainly done using the Caeser cipher.

Nowadays, encryption is more essential than ever because there is no doubt the Internet has revolutionised our lifestyle and the importance of encryption and security in overall has grown exponentially in recent years. There is a lot of information circulating on the Internet through emails, Facebook, military secrets, trade secrets, etc. Though the Internet is a public, insecure network, in which there are trusted users and on the other hand, the untrusted ones. It is common to read news on websites that have been hacked, credit card cloning, adulteration of images, etc. This motivates the need to protect information with mechanisms to prevent unauthorised users (intruders or hackers) access it. This need for protection of information has led us to develop security mechanisms to protect the private information of each user, such as electronic commerce and data protection in banking transactions. Therefore, in recent years it has explored the development of cryptography based on neural networks.

Moreover, talking about cryptography; the study and applications of mathematical techniques for secret communication or hiding from the presence of an uncalled third party trying to look into your details, which are considered to be unsafe. So we talk about crypto systems or coding systemisation to protect the original information in an encrypted or unencrypted message.

Now talking about cryptanalysis, it is the study of mathematical techniques for extracting hidden information from an encrypted message. Thus, cryptanalysis is important when a new crypto-system is proposed, to prove resistance to attack. Here, we talk about breaking or the break of crypto-system, then to extract the original information and make it available to an unauthorised (intruder) user.

Intuitively the essence of cryptography is to create certain functions that are easy to evaluate but whose inverse is very difficult to obtain with existing computational means. These functions and their inverses are called a crypto-system, as mentioned in the previous paragraph. For instance, the key number and a credit card is valuable information for 2 or 3 years because the card expires or is closed. Thus, if a crypto-system is effective if you can protect the key number and credit card for more than 3 years. With this example, we want to explain that a crypto-system is safe if it is able to protect your private information until the time it loses its value.

2. Basics of Artificial Neural Networks

An artificial neural network (ANN) is a distributed and massively parallel processor, i.e a computer able to process many tasks at the same time. It consists of many individual processing units called neurons.

Figure 2 shows a model for a neuron, where $\{x_1, x_2, \dots, x_m\}$ is the set of input signals, and $\{w_{k1}, w_{k2}, \dots, w_{km}\}$ is the set of synaptic weights for the kth neuron. The parameter b_k is called the bias of the kth neuron and it is also the local field induced or activation potential. $\varphi(\cdot)$ is the activation function and y_k is the output signal of the kth neuron.

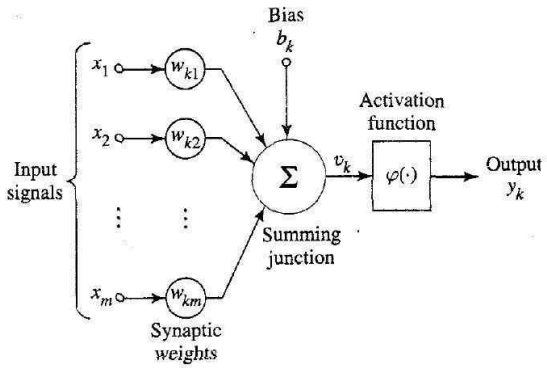


Figure 2: Model of a neuron [2].

The induced local field is calculated as

$$v_k = \left[\sum_{j=1}^{m} x_j w_{kj}\right] + b_k = \sum_{j=0}^{m} x_j w_{kj}$$

where a signal can be considered $x_0 = 1$ and a synaptic weight $w_{k0} = b_k$

An ANN can gain knowledge from experience or learning processes if given proper training data, similar to the brain, and store the synaptic weights of neurons.

2.1 Activation functions

The activation function $\varphi(\cdot)$ is used to limit the amplitude of the output of a neuron to a value information, which can be between:

$$\mathbf{0} \leq \boldsymbol{y_k} \leq \mathbf{1} \qquad -\mathbf{1} \leq \boldsymbol{y_k} \leq \mathbf{1}$$

1. Heaviside function: It is the McCulloch-Pitts model and has the property of all or nothing.

$$\boldsymbol{y_k} = \boldsymbol{\varphi}(\boldsymbol{v_k}) = \{\mathbf{1} \quad \textit{if} \quad \boldsymbol{v_k} \geq \mathbf{0}\ \mathbf{0} \quad \textit{if} \quad \boldsymbol{v_k} < \mathbf{0}$$

2. Linear function: It is defined as

$$y_k = \varphi(v_k) = \{1 \quad \textit{if} \quad v \geq \frac{1}{2} \quad v \quad \textit{if} \quad -\frac{1}{2} < v < \frac{1}{2}\ 0 \quad \textit{if} \quad v \leq -\frac{1}{2}$$

1. $y = \varphi(v) = \frac{1}{1+e^{-av}}$

2.2 Representations of neural networks with directed graphs

Graphs ux signal (or signal directed graphs) provides an orderly method to describe the flow of signals in a neural network. Signals circulate on a network of undirected links that interconnect at points called nodes.

For these graphs, the following consideration are made:

1. The j-th node has associated signal x_j.
2. A link with initial node in the j-th node and node in the k-th node has an associated transfer function, which specifies how the signal Y_k depends on the signal x_j in the j-th node. See Figures 3 and 4.
3. The signal flow satisfies three basic rules:
   a. A signal moves in the direction of the Take along a link considered. Figure 3 shows a synaptic connection with a linear relationship between input signals and output. While Figure 4 shows a link to a nonlinear relationship.

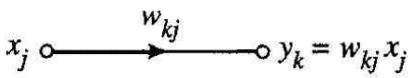


Figure 3: linear synaptic Link [2].

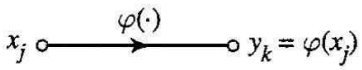


Figure 4: Link nonlinear synaptic [2]

b. The output signal of a node is the algebraic sum of all signals coming into this node. This is called synaptic convergence. The Figure 5 shows this rule.

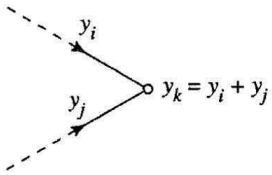


Figure 5: Convergence Synaptic [2].

c. A signal at a node is transmitted through all the links leaving the node, independently of the transfer functions. This is called synaptic divergence. Figure 6 shows this rule.

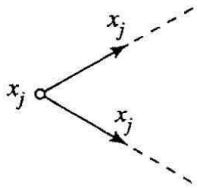


Figure 6: Synaptic Divergence [2].

Thus, a neuron and a neural network can be represented by directed graphs as shown in Figures 7 and 8, respectively.

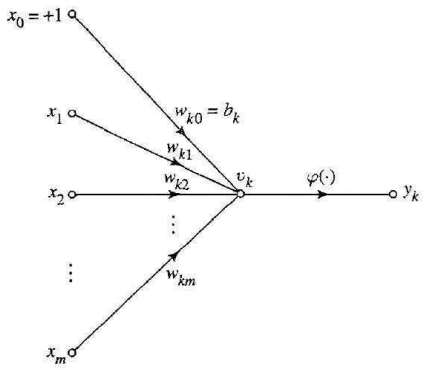


***Figure 7**: Pattern of a neuron as a directed graph [2].*

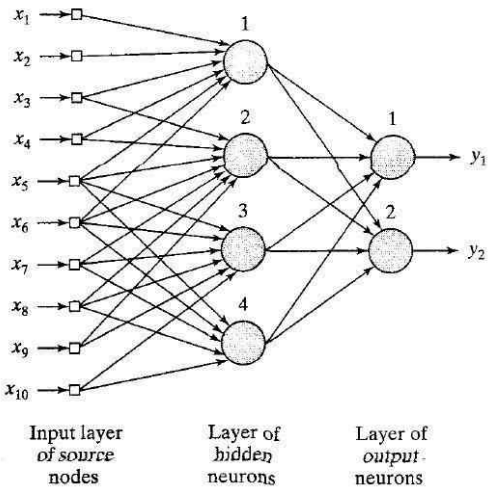


***Figure 8**: Pattern of a neural network as a directed graph [2]*

The mathematical definition of an ANN: a neural network is a directed graph consisting of nodes and links interconnecting with synaptic activation, and has the following properties:

a. Each neuron is represented as a set of linear synaptic bonds, a bias applied externally and link possibly nonlinear activation. The bias is shown as a synaptic link connected to an input in $x_0 = 1$.
b. Synaptic neuron links give weight to their respective input signals.
c. The sum of the input signals with their respective weights and the local field induced a neuron.
d. The activation link acts on the local field induced neuron to produce an output.

The state of the neuron can be defined in terms of their local field induced or output signal.

2.3. Architecture of Artificial Neural Networks

The architecture of an ANN is a directed graph that describes the organization and interaction between neurons that form the network.

There are three different sorts of architecture for an ANN:

a. Simple Layer Feedforward Networks (Single-Layer Feedforward Networks). This network is organized in layers, and has an input layer of node sources (these nodes do not perform any calculations) which transmits to the output layer (computing nodes) of neurons, but not vice versa. Therefore, the network is said to be strictly feedforward or acyclic type. The single layer re-refers to the output layer formed by computing nodes (neurons). Figure 9 shows the architecture of these nodes.

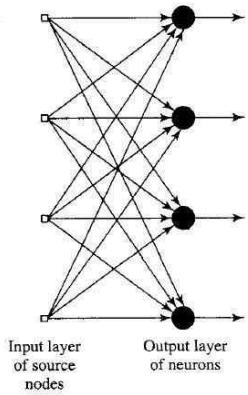


***Figure 9**: Pattern of a Feedforward Neural Network Layer Simple [2].*

b. Multi-Layer Feedforward Networks (Multilayer Feedforward Networks).
This is distinguished by having one or more hidden layers, whose computing nodes are called hidden neurons or hidden units. The function of this is to perform calculations between the external input and output of the network in some useful way. The source nodes in the input layer of the network provide the respective elements of the activation pattern (input vector), which constitute the input signals applied to the neurons (computing nodes) in the second layer (the first hidden layer). The output signals of the second layer are used as inputs for the third layer, and so on for the rest of the network. Neurons in each network layer have as inputs only the output signals of the preceding layer. The set of output signals of the neurons in the output layer (last) network forming the overall network response to activation pattern given by the source nodes in the input layer (first layer). The Figure 12 shows this architecture.

c. Recurrent networks (Recurrent Networks)
These networks are characterized by having at least one feedback loop. In Figure 10, the network has no self-feedback loops because for any output, the neuron does not feed directly back into itself. Also there is no hidden layer. Moreover, in Figure 11, there are hidden neurons and feedback originates from the hidden neurons as well as neurons in the output.

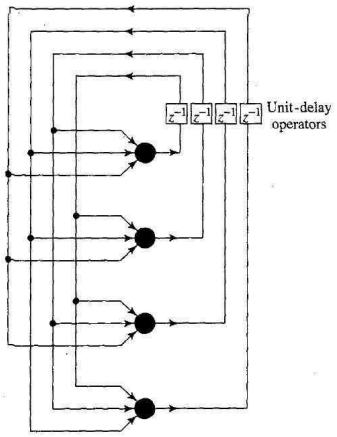


***Figure 10**: Pattern of Recurrent Neural Network [2].*

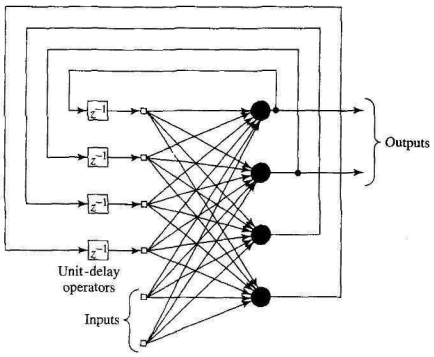


***Figure 11**: Pattern of a neural network with hidden neurons (recursive) [2].*

Recurrent structures have a profound impact on the learning capacity of a network and its performance. Delay units produce nonlinear dynamic behavior, assuming that the neural network contains nonlinear units.

2.4. Perceptron multilayer

A multiple perceptron, or multi-layer ANN consists of an input layer formed by sensory units (nodes sources), one or more hidden layers of computing nodes, and an output layer of node calculations. The input signal propagates through the network in the forward direction layer by layer.

The multilayer perceptron is trained using an error propagation algorithm called the back-propagation algorithm, which is based on the error correction learning rule.

Features of Multilayer Perceptron:

a. Each neuron in the network has a nonlinear differentiable function activation everywhere. The most common is the non-linear sigmoid function by the logistic function as show in equation (5)
$a = 1$.

b. The network has one or more hidden layers outside the entrance or exit. These hidden layers allow the network to learn complex tasks through feature extraction valid from patterns (vectors) input.

c. The network has a high degree of connectivity, determined by synapses in the network. A change in network connectivity required to make a change in the population of synaptic connections or their respective weights.

Figure 12 shows an ANN corresponding to a multilayer perceptron conn-graph, that is, a neuron layer that has links to all neurons or nodes of the previous layer. The signals are moving in the forward direction, left to right.

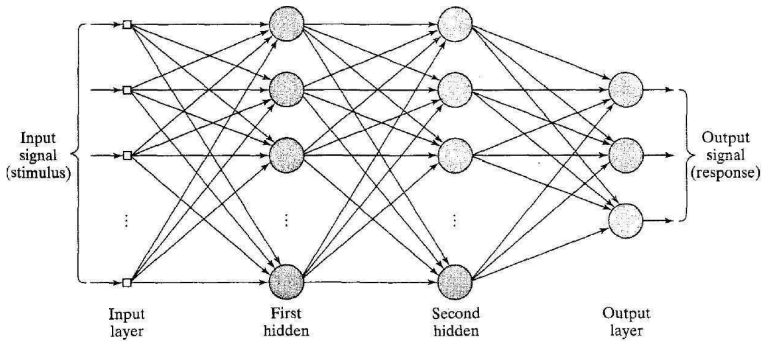


***Figure 12**: Diagram of a multilayer perceptron with two hidden layers [2].*

In Figure 13, movement signals are shown through the network in a forward direction, represented by a solid line. While the movement of the error signals is in the opposite direction and represented by segmented lines.

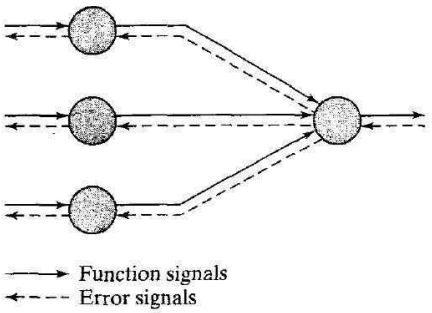


***Figure 13**: Address forward and backward in an ANN [2].*

Each hidden node or output (computation) node of a multi-layer perceptron neuron is designed to perform two calculations:

1. Calculate function signal appearing at the output of a neuron, which is expressed as a nonlinear continuous function of the input signal and synaptic weights associated with this neuron.

2. Calculate an estimate of the gradient vector (supergradient error with respect to the weights connected to the inputs of a neuron), which is necessary to spread back through the network.

3. Cryptography and Neural Networks

There are lots specific goals of cryptography. Most significant ones being listed below:

1. Privacy or confidentiality of information: only available to those authorized by the user. For instance, the specific details of one's credit card.
2. The integrity of information is to block out unauthorized users from making any changes in the information, i.e. intruders. For instance, changing password for an account for another user.
3. The authentication of a verified user and the identity that is accessed to information.
4. The authentication of a message is achieved by **veriCando** an identity and the source of the message. Like emails with dummy links for purposes like Phishing or Spoofing.
5. A digital signature is used to identify and differentiate a specific user from others.
6. Non-repudiation is also a mechanism to disallow people users from denying or descripting their actions. For instance, denying the purchase of a specific product from a website after receiving it.

3.1. Public-key cryptography

This section portrays three solutions to a huge problem of secret key exchange between authorized users due to (all the channels of transmissions are unsafe and presented?). These are classified within a discrete logarithmic problem and the factorization of large numbers into their prime factors. There are other problems which aren't addressed here as well.

RSA algorithm and neural networks

Another solution to the problem of key exchange cryptographic algorithm is called RSA (Rivest, Shamir and Adleman), which was published in 1978, this is currently available and used all around the world. It's strength is in the difficulty of factoring the product of two large prime numbers. Encryption algorithms and decryption are realized by using a whole ring of $Z_n = \{0,1,2, \dots, n-1\}$, and modular arithmetic. The original message shown as "m", is represented as an element of Zn, which must be less than n.

Key Generation:

To generate your public and secret keys Bob follow these steps:

1. Choose two distinct prime numbers p and q to be extremely large (1024 bits or 100 digits at least) of equal length to ensure system security. It then calculates

$$\boldsymbol{n = pq}$$

Attention: The two prime numbers p and q must remain secret.

2. Calculate
$$\varphi(n) = (p-1)(q-1)$$
3. Select your public random key (exponent) k from the list $\{1,2,\dots,\varphi(n)-1\}$ such that $gcd\ (k;\ \varphi(n))\ =\ 1$.
4. Calculate your private key (exponent) d such that
$$d\ k \equiv 1\ mod(\varphi(n)), i.e.\ d \equiv k^{-1}\ mod\ (\varphi(n))$$
and $\boldsymbol{gcd\ (d, n)\ =\ 1}$.

Encryption Algorithm:

Bob determines the values n and k.
Alice encrypts a message m, Bob follows:
$= E_k\ (M) = m^k \bmod (n)$
where m, c are integers from Z_n.

Decryption algorithm:

Bob receives the encrypted message c and decrypts as follows:
$= D_d\ (C) \equiv c^d \bmod (n) = (m^k)^d \bmod (n) = m^{kd} \bmod (n)$
where m, c are from Z_n.

Example: Suppose p = 47, q = 71, n = 3337. The public key and must not have factors in common with 46x70 = 3220. Thus, Bob can choose k = 79. Then calculates your private key as $d \equiv 79^{-1} \bmod (3220) = 1019$.
If Alice wants to send Bob the message m = 688 encrypts it using Bob's public key, e = 79 and n = 3337. Calculate
$c = E_{79}\ (688) \equiv 688^{79} \bmod (3337) = 1570$
Then Bob receives the encrypted message c = 1570, And calculating decrypted message
$1570^{1019} \bmod (n) = 688^{79\ 1019} \bmod (3337) = 688$

3.2. Key exchange based on artificial neural networks

In this section, a scheme for exchanging keys between two users using a pair of ANNs occur. As stated above, the scheme uses two ANNs feedforward type, which can synchronize their synaptic weights y learning and exchange where the output of one feeds the input of the other, and vice versa.

Below in Figure 14, it shows the architecture used by the transmitter S, and receiver R, which in this case is a double-layer perceptron with K, and hidden neurons N, input signals by each hidden neuron. Therefore, the vector of this input signals has K times by N components, $x_{kj}\ =\ -+1$ with $1\ \le k \le K\quad 1\ \le j \le N$. For which, the outputs of each of

the hidden neurons are $y_1, \ldots, y_k$ between different signals. Synaptic weights are integers $w_{kj} \in [-L;\ L]$, which represents an estimate weight kth hidden neuron. To the number L, it's called the synaptic depth of the network. Also the output of each 0 network is the result of multiplying each outputs of the K number of hidden neurons, i.e.

$$\boldsymbol{O = y_1 \cdot y_2 \cdot \ldots \cdot y_K}$$

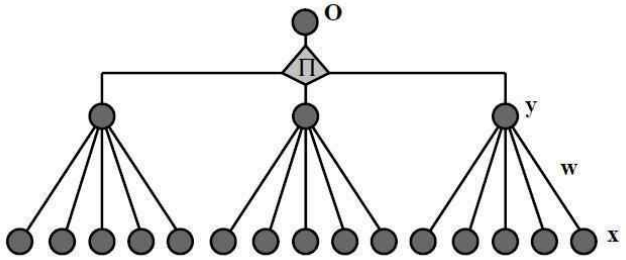


***Figure 14**: Architecture with K and hidden neurons N neuron input signals [12]*

Private keys (secret), the transmitter and receiver are the initial values of the weights synaptic each network, where w_{kj}^{s} and w_{kj}^{R} are respective weights. Also, each network is trained with the output of the other, for instance, considering a vector of input signal (x_{kj}), common and public for transmitters and receivers.

Figure 14 also considers the fact that K=3 and N=5. Therefore, the output signal at each network is obtained as:

$$\boldsymbol{y_k = sgn\left(\sum_{j=1}^{N} w_{kj} x_{kj}\right), k = 1, 2, 3}$$

where the sign function is defined as follows

$$sgn\ (x) = \{1 \quad if \quad x > 0 \ -1 \quad if \quad x < 0$$

For the particular case x = 0. The transmitter considers $sgn\ (X) = 1$, while the receiver considers $sgn\ (X) = 1$.

Then, the output signal of each network is calculated as follows:

$$\boldsymbol{O^S = y_1^S \cdot y_1^S \cdot y_3^S \quad O^R = y_1^R \cdot y_1^R \cdot y_1^R}$$

For which, the transmitter and the receiver output signals exchanged O^S and O^R decade network, for use at the start of the function. Then the training follows if $O^S\ O^R < 0$, i.e. while they are different, and ends when both networks have the same output.

Also, during training weights are adjusted according to the following learning rule in each network:

$$\boldsymbol{O \cdot y_k > 0 \Rightarrow w_{kj} = w_{kj} - O \cdot x_{kj}}$$
$$\boldsymbol{w_{kj} > L \Rightarrow w_{kj} = sgn\ (w_{kj}) \cdot L}$$

Only synaptic weights belonging to the hidden neurons that are in the same state adjust its output unit, in each both networks.

The security of this method of key exchange is guaranteed by the following facts:

a. For a particular output, or from one of the RNAs, they have different representations with departures $y_1, y_2, \dots, y_K$ of hidden neurons. For instance, for Figure 14, O=1, which might be the result of multiplying one of the gyrations: (1; 1; 1) , (1; -1; -1) , (-1; 1; -1) , (-1; -1; 1). Thus, the "attacker" can't determine the vector of synaptic weighs being used.

b. Due to each component being bounded by synaptic network depth L, the intruder cannot invest to operations listed in the equations above, since the network forgets.

This procedure is being repeated in the process until the weights of both neural networks are equal. The paired key is the value of the weights of the networks. Figure 15 below, shows the neural network graph for encryption generated in Wolfram Mathematica, along with the corresponding weights and values.

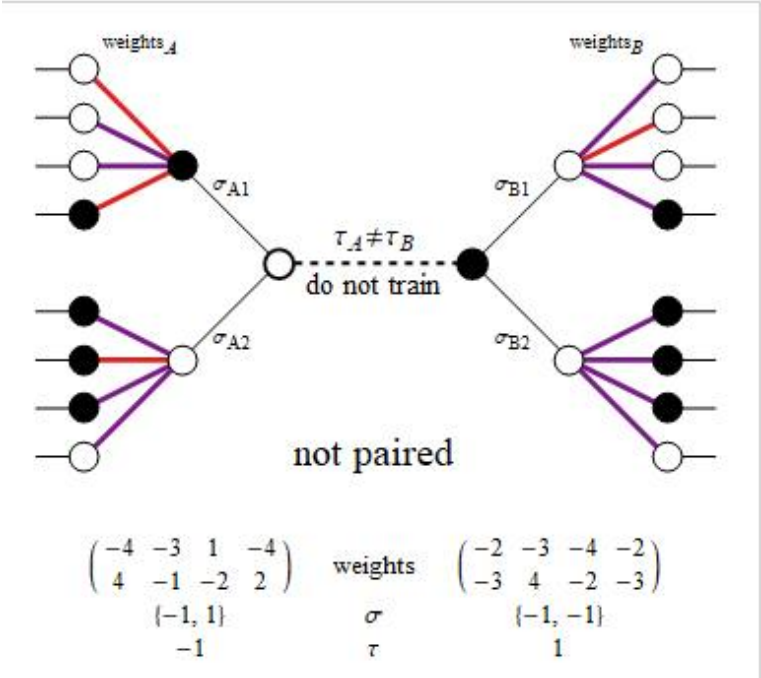


***Figure 15**. Neural network graph for encryption, generated in Wolfram Mathematica.*

The Wolfram Mathematica code to generate the entire demonstration is given as follows:

```
Manipulate[Graphics[{Thick, If[data[[step]][[4]][[1]] == data[[step]][[4]][[2]], Thick, Dashed],
    Line[{{-x, 0}, {x, 0}}], Thickness[0.0025], Dashing[None],
     Table[Flatten[{Line[{{-2*x, i*y}, {-x, 0}}], Line[{{-2*x, (-i)*y}, {-x, 0}}]}], {i, 1, sigmas/2}],
    Table[Flatten[{Line[{{2*x, i*y}, {x, 0}}], Line[{{2*x, (-i)*y}, {x, 0}}]}], {i, 1, sigmas/2}],
```

```
  Thickness[0.0075],
Table[Flatten[{Table[Flatten[{nLineColor[data[[step]][[2]][[1]][[j]][[i]]],
Line[{{-3*x, Sign[(-1)^j]*(neurons/2+0.5)+(Sign[(-1)^(j + 1)]*(i*0.5))*y}, {-2*x, Sign[-1]^j*y}}]}],
    {i, 1, neurons}]}], {j, 1, sigmas}],
  Table[Flatten[{Table[Flatten[{nLineColor[data[[step]][[2]][[2]][[j]][[i]]],
Line[{{3*x, Sign[(-1)^j]*(neurons/2 + 0.5) + (Sign[(-1)^(j + 1)]*(i*0.5))*y}, {2*x, Sign[-1]^j*y}}]}], {i, 1, neurons}]}],
  {j, 1, sigmas}], Black, Thickness[0.0025], Table[Table[Line[{{-3*x, Sign[(-1)^j]*(neurons/2 + 0.5) + (Sign[(-1)^(j + 1)]*(i*0.5))*y},
    {-3.5*x, Sign[(-1)^j]*(neurons/2 + 0.5) + (Sign[(-1)^(j + 1)]*(i*0.5))*y}}], {i, 1, neurons}], {j, 1, sigmas}],
  Table[Table[Line[{{3*x, Sign[(-1)^j]*(neurons/2 + 0.5) + (Sign[(-1)^(j + 1)]*(i*0.5))*y},
{3.5*x, Sign[(-1)^j]*(neurons/2 + 0.5) + (Sign[(-1)^(j + 1)]*(i*0.5))*y}}], {i, 1, neurons}], {j, 1, sigmas}],
  EdgeForm[{Thickness[0.005]}], If[data[[step]][[4]][[1]] == 1, Black, White], Disk[{-x, 0}, d],
If[data[[step]][[4]][[2]] == 1, Black, White], Disk[{x, 0}, d], EdgeForm[{Thickness[0.0025]}],
  Flatten[Table[{If[data[[step]][[3]][[1]][[i]] == 1, Black, White], Disk[{-2*x, Sign[((-1)^i*i)*y]}, d]}, {i, 1, sigmas}]],
  Flatten[Table[{If[data[[step]][[3]][[2]][[i]] == 1, Black, White], Disk[{2*x, Sign[((-1)^i*i)*y]}, d]}, {i, 1, sigmas}]],
  Flatten[Table[Table[{If[data[[step]][[1]][[1]][[j]][[i]] == 1, Black, White],
Disk[{-3*x, Sign[(-1)^j]*(neurons/2 + 0.5) + (Sign[(-1)^(j + 1)]*(i*0.5))*y}, d]}, {i, 1, neurons}], {j, 1, sigmas}]],
  Flatten[Table[Table[{If[data[[step]][[1]][[2]][[j]][[i]] == 1, Black, White],
Disk[{3*x, Sign[(-1)^j]*(neurons/2 + 0.5) + (Sign[(-1)^(j + 1)]*(i*0.5))*y}, d]}, {i, 1, neurons}], {j, 1, sigmas}]],
  If[data[[step]][[4]][[1]] == data[[step]][[4]][[2]], Text[Style["A", 15], {0, 0.25}],
```

```
Text[Style["\!\(\*SubscriptBox[\(\[Tau]\),
\(A\)]\)!=\!\(\*SubscriptBox[\(\[Tau]\), \(B\)]\)", 15], {0, 0.25}]],
If[data[[step]][[4]][[1]] == data[[step]][[4]][[2]], Text[Style["train", 15], {0, -0.25}],
  Text[Style["do not train", 15], {0, -0.25}]], If[data[[step]][[2]][[1]] ==
data[[step]][[2]][[2]],
Text[Style["paired", 20], {0, -2}], Text[Style["not paired", 20], {0, -2}]],
  Text[Style["\!\(\*SubscriptBox[\(\[Sigma]\), \(A1\)]\)", 10], {-1.45, 0.8}],
Text[Style["\!\(\*SubscriptBox[\(\[Sigma]\), \(A2\)]\)", 10], {-1.45, -0.8}],
  Text[Style["\!\(\*SubscriptBox[\(\[Sigma]\), \(B1\)]\)", 10], {1.45, 0.8}],
Text[Style["\!\(\*SubscriptBox[\(\[Sigma]\), \(B2\)]\)", 10], {1.45, -0.8}],
  Text[Style["\!\(\*SubscriptBox[\(weights\), \(A\)]\)", 10], {-2.4, 2.25}],
Text[Style["\!\(\*SubscriptBox[\(weights\), \(B\)]\)", 10], {2.4, 2.25}],
  Text[Style[Grid[{{data[[step]][[2]][[1]], " weights ", data[[step]][[2]][[2]]},
{data[[step]][[3]][[1]], "\[Sigma]", data[[step]][[3]][[2]]},
{data[[step]][[4]][[1]], "\[Tau]", data[[step]][[4]][[2]]}}], 13],
  {0, -3.5}]}], {{step, 1000, "epoch"}, 1, 1000, 1}, Button["randomize", wA =
wRand[neurons, sigmas, limit]; wB = wRand[neurons, sigmas, limit];
  data = Table[input = xRand[neurons, sigmas]; \[Sigma]A = \[Sigma]Full[wA,
input];
\[Sigma]B = \[Sigma]Full[wB, input]; \[Tau]A = \[Tau][\[Sigma]A]; \[Tau]B =
\[Tau][\[Sigma]B]; \[CapitalDelta]wA = If[\[Tau]A == \[Tau]B,
\[CapitalDelta]whebb[wA, input, \[Sigma]A, \[Tau]A], 0];
   \[CapitalDelta]wB = If[\[Tau]A == \[Tau]B, \[CapitalDelta]whebb[wB, input,
\[Sigma]B, \[Tau]B], 0]; wA = wAdd[wA, \[CapitalDelta]wA, limit];
wB = wAdd[wB, \[CapitalDelta]wB, limit]; {{input, input}, {wA, wB}, {\[Sigma]A,
\[Sigma]B}, {\[Tau]A, \[Tau]B}}, {i, 0, n}]],
 ControllerLinking -> True, Initialization :> ({ x = 1, y = 1, sigmas = 2,
  nLineColor[value_] := Module[{}, Switch[value, -4, Red, -3, Cyan, -2, Gray, -1,
Magenta, 0, Black, 1, Green, 2, Blue, 3, Purple, 4, Orange]],
neurons = 4, d = 0.15, wA = {{3, -1, 3, 0}, {1, 1, -4, 1}},
```

```
wRand[neurons_, sigmas_, L_] := Module[{}, Table[Table[RandomInteger[{-L, L}],
{i, 1, neurons}], {j, 1, sigmas}]],
limit = 4, wB = {{3, -3, 3, -2}, {0, 1, 3, 1}}, input = {{-1, 1, 1, -1}, {-1, 1, 1, 1}},
xRand[neurons_, sigmas_] := Module[{}, Table[Table[If[RandomInteger[] == 0, -1,
1], {i, 1, neurons}], {j, 1, sigmas}]], \[Sigma]A = {-1, -1},
\[Sigma]Full[w_, x_] := Module[{}, Table[\[Sigma][w[[i]], x[[i]]], {i, 1, Length[w]}]],
\[Sigma][w_, x_] := Module[{}, If[Sign[w . x] == 0, -1, Sign[w . x]]], \[Sigma]B = {-1, 1},
\[Tau]A = 1,
\[Tau][\[Sigma]_] := Module[{}, Fold[#1*#2 & , 1, \[Sigma]]], \[Tau]B = -1,
\[CapitalDelta]wA = 0, \[CapitalDelta]whebb[w_, x_, \[Sigma]Full_, \[Tau]a_] :=
Module[{\[CapitalDelta]w},
Table[((\[Sigma]Full[[i]]*(x[[i]]*\[Tau]a))*UnitStep[\[Tau]a*\[Sigma]Full[[i]]])*Uni
tStep[\[Tau]a^2],
{i, 1, Length[w]}]], \[CapitalDelta]wB = 0, wAdd[w_, \[CapitalDelta]w_, L_] :=
Module[{added}, added = w + \[CapitalDelta]w; Table[Table[If[added[[j]][[i]] < -L, L,
If[added[[j]][[i]] > L, L, added[[j]][[i]]]], {i, 1, Length[added[[1]]]}],
{j, 1, Length[added]}]], n = 1000};
ReleaseHold[HoldComplete[{xRand[neurons_, sigmas_] :=
Table[Table[If[RandomInteger[] == 0, -1, 1], {i, 1, neurons}], {j, 1, sigmas}],
wRand[neurons_, sigmas_, L_] := Table[Table[RandomInteger[{-L,
L}],{i,1,neurons}],{j,1,sigmas}], \[Sigma][w_,x_]:=If[Sign[w.x]==0,-1,Sign[w.x]],
\[Sigma]Full[w_, x_] := Table[\[Sigma][w[[i]], x[[i]]], {i, 1, Length[w]}],
\[Tau][\[Sigma]_] := Fold[#1*#2 & , 1, \[Sigma]], \[CapitalDelta]whebb[w_, x_,
\[Sigma]Full_, \[Tau]a_] :=
Module[{\[CapitalDelta]w},
Table[((\[Sigma]Full[[i]]*(x[[i]]*\[Tau]a))*UnitStep[\[Tau]a*\[Sigma]Full[[i]]])*Uni
tStep[\[Tau]a^2], {i, 1, Length[w]}]],
wAdd[w_, \[CapitalDelta]w_, L_] := Module[{added}, added = w +
\[CapitalDelta]w; Table[Table[If[added[[j]][[i]] < -L, L,
If[added[[j]][[i]] > L, L, added[[j]][[i]]]], {i, 1, Length[added[[1]]]}], {j, 1,
Length[added]}]],
```

```
wSub[w_, \[CapitalDelta]w_, L_] := Module[{added}, added = w - \[CapitalDelta]w; Table[Table[If[added[[j]][[i]] < -L, L,
If[added[[j]][[i]] > L, L, added[[j]][[i]]]], {i, 1, Length[added[[1]]]}], {j, 1, Length[added]}]],
\[CapitalDelta]wWalk[w_, x_, \[Sigma]Full_, \[Tau]a_] := Module[{\[CapitalDelta]w},
Table[((x[[i]]*\[Tau]a)*UnitStep[\[Tau]a*\[Sigma]Full[[i]]])*UnitStep[\[Tau]a^2], {i, 1, Length[w]}]],
cutToL[value_, L_] := If[value > L, L, If[value < -L, -L, value]],
nLineColor[value_] := ColorData["Rainbow"][value + 4/8.],
((((((x = 1; y = 1; d = 0.15; )*(limit = 4; ))*(neurons = 4; sigmas = 2; ))*(wA = wRand[neurons, sigmas, limit]; ))*
(wB = wRand[neurons, sigmas, limit]; ))*(n = 1000; ))*(data = Table[input = xRand[neurons, sigmas];
\[Sigma]A = \[Sigma]Full[wA, input]; \[Sigma]B = \[Sigma]Full[wB, input]; \[Tau]A = \[Tau][\[Sigma]A]; \[Tau]B = \[Tau][\[Sigma]B];
\[CapitalDelta]wA = If[\[Tau]A == \[Tau]B, \[CapitalDelta]whebb[wA, input, \[Sigma]A, \[Tau]A], 0]; \[CapitalDelta]wB = If[\[Tau]A == \[Tau]B, \[CapitalDelta]whebb[wB, input, \[Sigma]B, \[Tau]B], 0];
wA = wAdd[wA, \[CapitalDelta]wA, limit]; wB = wAdd[wB, \[CapitalDelta]wB, limit];
{{input, input}, {wA, wB}, {\[Sigma]A, \[Sigma]B}, {\[Tau]A, \[Tau]B}}, {i, 0, n}]; )}]])]
```

4. Conclusions

The application of neural networks for key exchange purposes has been outlined above, with explanation of how artificial neural networks work, a brief overview of RSA encryption, and the key exchange process. In addition, we were successful in exchanging keys using Mathematica to create the neural network. Although the security of the neural network itself has not be properly tested, it seems at first observation that the key exchange process works sufficiently.

All in all, whilst writing the paper, I learnt about the importance of key exchange within cryptography helping two parties to agree on a method to share information and exchange their cryptographic keys without letting any other unknown party interfere or

intercept the message and decrypt it. Also, I was able to learn about neural networks and how they work, something that I didn't know could be applied to cryptography. Lastly, through successfully generating code to exchange keys through a neural network, I was able to learn how to use Wolfram Mathematica.

Finally, for the future I would like to research and study about other types of artificial intelligence to deepen my knowledge within the new software systems and work on how the hardware of a product could link and work with these encryptions and networks.

References

Internet Live Stats, http://www.internetlivestats.com/ .

S. Haykin, Neural Networks. A Comprehensive Foundation, Second Edition, ISBN: 81-7808-300-0. Pearson Prentice Hall. 1999.

MA Arbib, The Handbook of Brain Theory and Neural Networks, Second Edition, ISBN: 0262011972. Bradford Book The MIT Press. 2003

J. Hertz, A. Krogh, Palmer RG, Introduction to the Theory of Neural Computation, ISBN: 0-201-51560-1. Addison-Wesley Publishing Company, 1990.

S. Vaudenay, A Classical Introduction to Cryptography: Applications for Communications Security, ISBN-13: 978-1-4419-3797-1. Springer, 2010.

C. Paar, J. Pelzl, Understanding Cryptography. A Textbook for Students andractitioners, ISBN: 978-3-642-04100-6. Springer-Verlag, Berlin, 2010.

B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition, ISBN: 0471117099. John Wiley and Sons, Inc. 1995.

W. Diffie, MEHellman, New Directions in Cryptography, IEEE Transactions on Information Theory 22 (1976), pp. 644-654.

R. Rivest, A. Shamir, L. Adleman , A Method for Obtaining Digital Signatures and Public Key Cryptosystems-, Communications of the ACM, Vol. 21 (2), pp.120-126, 1978.

T. ElGamal, A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, IEEE Transactions on Information Theory 31 (4): 469472, 1985.

HCA van Tilborg, Fundamentals of Cryptology. A Professional Reference and Interactive Tutorial, ISBN: 0792386752. Kluwer Academic Publishers, 2002.

I. Kanter, W. Kinzel, E. Kanter , Secure exchange of information by synchronization of neural networks, Europhysics Letters, 57 (1), pp. 141147, 2002.

Cheng Chao-Jung, Teh-Lu Liao, Yan Jun-Juh, Chi-Chuan Hwang , Synchronization of neural networks by decentralized feedback control Physics Letters A 338 (2005) 2835. Elsevier BV 2005.

S. Santhanalakshmi, TSB Sudarshan, GK Patra, Neural Synchronization by Mutual Learning Using Genetic Approach for Secure Key Generation, Thampi SM et al (Eds.). SNDS 2012, CCIS 335, pp. 422431, Springer-Verlag Berlin Heidelberg 2012.

N. Mu, X. Liao, An Approach for Designing Neural Cryptography, C. Guo, Z.-G. Hou, and Z. Zeng (Eds.): ISNN 2013, Part I, LNCS 7951, pp. 99108. Springer-Verlag Berlin Heidelberg 2013.

J. Giesl, R. Pisani, Neural Network Synchronization Protocol , Journal of Emerging Trends in Computing and Information Sciences, Vol. 4, No. 1 Jan 2013, ISSN 2079-8407, 2013.

Computational Modeling of the Immune Response Using Cellular Automata

Yechan Cho and Carlos Alciuri
Valor International Scholar

Abstract

The human immune response regarding tumors, or carcinogenic cells, is an extremely convoluted process that scientists have long been struggling to comprehend. The process has yet to be fully understood, but there have been some attempts of scientists to emulate the process by utilizing physical concepts and mathematical techniques based on differential equations. These attempts, however, had unequivocal limitations. They weren't able to thoroughly explicate the complexity of the human immune system and sometimes included intricate equations that would hamper scientists from processing it further. In this paper, cellular automata (CA), instead of numerical calculations, are harnessed as a major tool to imitate the human immune response to tumors, engendering a synthetic human immune system. A cellular automaton is a computational model that comprises of several units called "cells" that have certain states depending on the rules of the automaton. The state of each cell constantly changes after a successful generation and is determined by the states of other cells that surround it. By facilitating this technique, scientists are able to examine the immunological process deeper into the molecular level and observe the effect that certain changes in initial conditions have on the overall process of the response. It is hoped that through this system, scientists would have additional grasp on the methodology of human immune system response and late improve the model to make more practical simulations. Mathematica was successfully used to recreate a simplified version of the CA models found in the references.

Introduction

For over two decades the studies to understand the complexity of the immune system (IS) have proliferated in the area of computational biology (Perelson, 2018). This biological system consists of a series of organs, tissues and cells that protect the body against infection pathogens. For it is capable to recognize the components of the infectious agent and initiate

a series of responses designed to eliminate the fundamental characteristics are the specificity and memory. There are two types of immune response: immune response, when antibody-mediated. Cellular Response, when cell-mediated. Both types of response may have characteristic of being specific to a particular pathogen or otherwise cause a general and unspecific mode. One of the most important properties of the immune response is the great variety of molecules which can be recognized by receptors, especially by antibodies. These are produced in large amounts by cells called B lymphocytes, identifying specific antigens that are marked for deletion.

The reaction of the insusceptible framework to transformed and possibly carcinogenic cells is the body's regular guard against tumor development. Both the working of the insusceptible framework and the development of tumors include exceptionally perplexing procedures, and coupled, the tumor-resistant collaborations shape an intricate framework that isn't yet completely comprehended by either experimentalists or then again theoreticians.

Tumor development and the progression of the safe framework have been a critical concentration for scientific displaying in the course of recent decades. Advancing from the early compound dissemination and differential condition models of Burton and Greenspan, portrayals of tumor development have been introduced all the more as of late utilizing halfway differential conditions (PDEs) and cell automata (CA).

Due to the large number of cells and biomolecules that interact and participate in various processes, the IF is a complex system that handles a large set of variables and experiments in Vivo and in Vitro results in a difficult and costly task, besides presenting ethical dilemmas. In this context mathematical modeling and simulation computational tools are useful for testing new theories in the field of immunology that despite being consolidated as an independent science, still eludes the understanding of experts, knowledge about certain defense mechanisms of the human body.

In this sense different modeling techniques most commonly used are differentiated into two groups based on equations and Automata (Castiglione et al. 1999). In the first group, the population dynamics of the cells participating in the immune response is obtained by ordinary differential equations and partial; the second group deeper into the interactions between cells and molecules simulating behavior of a dynamic is obtained population as a result of cooperation between the entities. One of the models that came to a representation more real if constitutes the model Seiden and Celada for the immune response, which IMMSIM computational implementation corresponds to software developed in language APL2. This tool implement a particular model of cellular automata and constituting Examples contributions in studies of various theories of immune response (Seiden, 1992, Bezzi, 1997, Santoni, 2008).

However these computational tools have the common limitation of responding to a specific model if at that biological entities and cellular mechanisms that describe their operation are predefined and correspond to the design of each development team, preventing researchers recreate different scenarios to test their theories on the functioning of the immune response.

The procedure of tumor development with insusceptible rivalry is exceptionally intricate (even in the avascular stage) because of the heterogeneity of associations that happen both on the entomb and intracellular levels. It is getting to be apparent that both hypothetical and viable inquiries in tumor immunology can't be tended to by performing

exclusively in vivo and in vitro analyzes [1]. Scientific demonstrating has turned into an imperative piece of research in tumor development (see e.g. [2-4]). Specifically, a superior comprehension of the procedures happening in the development of dangerous tumors originated from the plan of numerical models which can be observed from the minute level and from the plainly visible level in the meantime. These models give the essential diagnostic structures required for the comprehension of the development forms. It is realized that cooperation at the phone level are activated by synthetic substances or by specific signs coming from the sub-cell level. These communications thusly have an effect at the naturally visible level [5]. In the physical sciences, the association between the infinitesimal world and the naturally visible world is given by measurable mechanics.

A few scientific systems have been created which can be utilized to examine natural and biochemical wonders in which the collaborations can just completely comprehended when they are taken a gander at from alternate points of view, i.e., from various timescales (for surveys see [6-10]). Among them are the self-repeating machines [11]. The cell automata (CA) worldview utilized by these machines is extremely valuable for organic demonstrating, particularly to model tumor development. The explanation behind this is it is anything but difficult to present the cell and sub-cell systems into a cell based depiction of the tumor development. This is done by applying the deterministic and stochastic guidelines (in view of the real instruments overseeing the development of the cells) to refresh the conditions of each cell after each time step. Lately, the quantity of papers utilizing the CA method to think about tumor development which considers invulnerable communications has been expanding [12-18]. The significance of this technique is to a limited extent identified with the capacity to reproduce elements of phenomenological perception with PC recreations. By the by, demonstrating with CA absences of much profundity investigation and ends up being hard to give advancement conditions to the plainly visible scale [11].

The Mathematica tool can be used to simulate the immune response from the creation of the models by the researcher. The proposal is based on the ability to generate these models from the creation by researchers, new types of molecules and cells (biological entities) and interactions between these entities. Operation model implemented with Mathematica is verified by a series of experiments whose results can be compared with other software.

Computational Models for the Immune Response

Ordinary and partial differential equations have been traditionally used to model complex systems. Perelson and Weisbuch (Perelson, 1997) used physical concepts and mathematical methods based on differential equations for the modeling of problems in the field of immunology. One example is the work of Farmer et al (Farmer, 1986) on immunological memory and more recently researchers analyzed the evolution of immunological memory using mathematical models, where some authors (Klienstein, 2000) have listed some of the drawbacks of the models of differential equations for modeling that, resulting in the average behavior of the system.

- They cannot represent the complexity of IS, with its enormous number of cells, molecules, and processes interactions. (Eg. the cells have a history and individual characteristics that influence their behavior).

- The models often involve (The more realistic you will, the greater the complexity of the system differential equations), nonlinearities that hinder solving equations with numerical methods.

The difficulties to build and manage these equations are precisely the reason why it is more appropriate in many cases to use computational methods to simulate the immune response.

The ability to study the global behavior of a complex system through the behavior of each of its parties, is the reason that determines the great advantages of mathematical computer models. With these models is more intuitive description of system behavior based on the biological significance of the interactions local and the use of discrete models to work with a larger repertoire of entities (or objects) involved in these interactions. Another advantage of this type of model is the ability to change the rules governing local interactions to see how these changes impact on the entire global system.

Many models of the immune response are based on simple automatons connected networks are known locally Cellular Automata (CA) (Wolfram, 1984; 1986, Dewdney, 1989) and are defined by a uniform grid representing space and a finite set of rules that are applied to each cell in the network. AC are classified as the counterpart of differential equations as possible to describe the dynamics of systems not linear. The model proposed Seiden and Celada to study the immune response is an extension of cellular automata and its main features are:

- Each cell evolves according to the same probabilistic rules.
- The rules for the development of a cell depend on the entities that are on the site.
- Entities of a cell can jump or spread to neighboring cells.

An important feature of this model is the diversity of clonotypes (receptors, epitopes and peptides) entities (Antigens, cells and molecules), represented by binary strings. These entities are presenting a set of states and rules interactions that define their behavior. They are modeled using an Agent-based model (ABM), in which each entity has a history and a unique behavior. For this use is made Paradigm object-oriented programming, in which each entity (agent) has internal states that are characterized by all receivers that each cell has a given time.

Three modules are represented in the model that correspond to regions anatomical of the human body: Bone marrow, the thymus gland and lymph node. The bone marrow is where the process is simulated production of new cells by the stochastic differential equation that in the context of research for regulating the number of cells that take part in the immune response. Space simulation is where the immune response takes place. It represents a portion of a lymph node using a probabilistic model AC in which each cell is a model based agents. There are cells that are selected in the thymus before passing the lymph node by the process of Clonal selection 1 and it is represented by a set of probabilistic equations.

With this model implemented in the Mathematica package, a significant set of parameters can be varied to perform simulations, however, entities that interact in space simulation are predefined, so the users can not change its characteristics or its rules of operation. Below presented implementation allows to modify this representation from the generalizability of a set of biological entities, and interactions between them, with the aim of giving the researcher the ability to define the entities participating in the immune response,

the characteristics required and interactions or rules that should govern their behavior in a flexibly. The components that define the general model are presented.

Types of Entities and Interactions

Receivers and biological entities: entities in IMMSIM two types are divided. The first is one of the components that influence the rate of immune response. Are composite objects by a name and a value represented by the model bit-string.

Biological entities are divided into cells and molecules. All main feature is an average life time represented in time steps. Cells are handled as objects grouped into classes that are derived from a parent class. One of the functions that may have a cell is to create a special type of entity called cell generating antibody (Cell PLB 2), whose function is to generate a certain amount of antibodies in each step of time and also comes from the parent class. All kinds of cells have a group of common features summary: The age, the average life expectancy, the state presented at a given time, the body where such mature cell before moving into space simulation, the time it takes to double, potential receivers may have during his lifetime and cell receptors expressed at birth.

Molecules in turn are divided into antibodies, antigens (bacteria or segments to model these vaccines) and simple molecules (cytokines and immunoglobulins), and are represented by quantities. All kinds of antigens present and characteristics: A set peptides 3, a set of epitopes 4 and replication rate. MATHEMATICA provides interfaces for creating feature types described.

Interactions occur locally within each site space simulation. The investigator then determines how to create each interaction. It is defined as a quadruple pattern of interaction of the form:

$$(Number, \{Entities\}, \{Conditions\}, \{Actions\})$$

where:

1. Processes that takes place in the thymus by T cells that recognize self-antigens are removed
2. By stands for Plasma B cell. In immunology, cells that generate antibodies are named.
3. Internal antigen receptors are present
4. External antigen receptors are present

Therefore, it specifies the name given to the interaction, it represents the set of entities that produce interaction and . In the set of ideal conditions defined to choose the interaction takes place. The term is the set of possible interaction results from conditions.

The model defines four patterns of interaction: Cell-cell, cell-antigen, antibody-antigen and Status change. From formally each interaction is a function that takes one or two entities according to a group of conditions returns a set of actions that affect each entity involved in said interaction. These actions can implicitly activating processes such as death by cell lysis of an infected or cell division. Mathematica presents user interfaces that allow the creation of new types of interactions from each pattern interaction.

The processes are identified in the model as called biological processes are carried out at different organs and influence biological entities by modifying the system dynamics. They are predefined in the model ensure the phenomenology of the biological system has been modeled. The possible processes which can be implemented using cellular automata approach are:

- Birth and death by apoptosis of cells in bone marrow.
- Clonal selection in the thymus.
- Aging cells.
- Cellular division.
- Replication antigens.
- Digestion and antigen presentation.
- Antibody Production.

Creating the CA Model of the Immune Response

Then the entities and interactions that make up the model is about to be performed the predictions. This model reproduces exactly the entities and interactions model that implements C-IMMSIM.

The feature classes in the model will be the CB, CT, MA, DC and PLB cells, the latter will be a cell type plasma generating antibodies. Other entities are the type of antibody Ab, type of antigens Ag, and simple molecules IL2 and DSignal.

The diagram simplified representation of the mechanisms involved in the immune response model was created with Mathematica. The first barrier is represented by the action of MA and DC constituting the first body defense, eliminated lesser extent to antigens and has a non-specific. The second defense is characterized by specificity and enters action when these entities are not able to recognize or completely eliminate the pathogen. In this second plays a role essential the presence of CB entities are those that produce PLB cells eventually they release large amounts of antigen specific antibodies.

Initial Parameters for the Simulation

Created after the model proceeds to create space simulation and model parameters define a Bitstring receiver chain length 12 and a minimum affinity between the chains 9 bits to take place interactions with this definition space is automatically represented by 256 cells.

All experiments simulate microliter (uL) of a subsidiary body, the system is scaled according to the amount of micro liter simulate desired. The initial number of entities for the simulation is defined by the formula of leukocytes blood by C-IMMSIM.

A standard scheme of the resistant reaction (Mayer et al. 1995) is labeled by a structure of the following few conventional differential equations:

$$\frac{dT}{dt} = rT - kTE,$$

$$\frac{dE}{dt} = f(T) + g(E) - \delta E,$$

Therefore, T denotes the goal, such as an organic substantial conditional on an immune reply (such as virus or bacteria); E is the removal volume of the immune structure, here characterized using cells; r and k are the degrees of replica and obliteration of the goal substance; δ is the degree of the cell demise; and t denotes the period.

Here, the function f denotes the creation of cells because of the occurrence of an organic substantial, and the function g is a catalytic cell growth. Regarding the replication, let us consider

$$f(T) = p\frac{T^2}{(1+T^2)},$$

$$g(E) = s\frac{E^2}{(1+E^2)}.$$

These conditions relate to a sigmoid shape for these capacities and underscore that the safe framework may overlook low bacterial fixations, and that a basic number of invulnerable cells might be important to get an autocatalytic impact. The constants p and s speak to antecedent cell pool sizes. These conditions are comprehended utilizing Mathematica's worked-in operation NDSolve, and the outcomes are exhibited in plots of T and E versus time and in the T-E plane. Right now zero, no specific cells are available and E(0) is zero.

In light of an underlying measurements of microscopic organisms, the dynamic cells increment and merge toward the safe state where no microorganisms, yet just memory cells, are available. In an optional contamination (the spotted lines), the safe framework reacts quicker; alternately, the resistant framework can be overpowered by microscopic organisms that have a high proliferation or low annihilation rate.

Implementation of the General Model

The specific needs for application development require a programming language facilities using standardized libraries, little development time and flexibility for handling objects. All types of biological entities are meta-object classes from which are created instances of these in time execution, according to the characteristics that it considers the user. Interaction patterns are methods basis from which are created dynamic methods (interactions classes) at runtime.

The main advantage of creating each of the biological entities and their respective interactions in which they participate, lies the possibility to obtain a flexible new models describing the operation of the immune response. Mathematica provides a set of facilities aimed at creating and simulating models of the immune response. Similarly, it can be defined as a "shell, outline or skeleton" from which the researcher can create your own representations of immunological phenomenon under study.

Verification of model implementing Mathematica has two main objectives:

1. Check with the defined models can make predictions that reflect behavior correct qualitative.
2. Check the flexibility of the model to represent different approaches to the immune response.

For the first objective is decided recreate the immune response model that implements C-IMMSIM and reproduced from the facilities provided by Mathematica. Several typical phenomena of the immune response is then simulated from the parameters used by the model C-IMMSIM for the same experiments (Castiglione et al., 2006), such as the immune response to an inactive antigen replication. A typical case corresponds to a vaccine. Immunological memory to injections of two kinds of inactive antigens.

The Mathematica implementation is given as follows:

```
Manipulate[Module[{eqn1, soln1, plt1, eqn2, soln2, plt2, txt},
  eqn1 = {cT'[t] == r cT[t] - k cT[t] cE[t],
    cE'[t] == g[t, s] + f[t, p] - cE[t], cE[0] == 0, cT[0] == dose1};
  soln1 = NDSolve[eqn1, {cE, cT}, {t, 0, 20}];
  plt1 = Plot[{cE[t], cT[t]} /. soln1, {t, 0, t2}, PlotStyle -> {Blue, Thick}];
  eqn2 = {cT'[t] == r cT[t] - k cT[t] cE[t], cE'[t] == g[t, s] + f[t, p] - cE[t],
    cE[t2] == First[cE[t2] /. soln1], cT[t2] == dose2};
  soln2 = NDSolve[eqn2, {cE, cT}, {t, 0, 20}];
  plt2 = Plot[{cE[t], cT[t]} /. soln2, {t, t2, 20},
    PlotStyle -> {{Blue, Thick, Dotted}, {Blue, Thick, Dotted}}];
  txt = {Text[Style["bacteria", 12, Background -> White, Blue, Italic], {12.5,
      0.1 + First[cT[t] /. soln2 /. t -> 12.5]}, Left],
    Text[Style["cells", 12, Blue, Italic, Background -> White], {12.5,
      First[cE[t] /. soln2 /. t -> 12.5]}, Left]};
  show1 = Show[Graphics[{Blue, Dotted, Thick, Line[{{t2, (cT[t2] /. soln2)[[1]]},
{t2, (cT[t2] /. soln1)[[1]]}}]}], plt1, plt2, Graphics[txt],
    PlotRange -> {{0, 20}, {0, All}}, Frame -> True, FrameLabel -> {"time",
"concentration"}, AspectRatio -> 1/GoldenRatio];
  plt1p = ParametricPlot[Evaluate[{cT[t], cE[t]} /. soln1], {t, 0, 20},
    PlotStyle -> Thick];
  plt2p = ParametricPlot[Evaluate[{cT[t], cE[t]} /. soln2], {t, 0, 20},
    PlotStyle -> {Dotted, Thick}];
  show2 = Show[plt1p, plt2p, PlotRange -> {{0, All}, {0, All}},
    Frame -> True, FrameLabel -> {"bacteria", "cells"},
    AspectRatio -> 1/GoldenRatio]];
 GraphicsRow[{show1, show2}, {0.01, 0.01}, ImageSize -> 1.2 {500, 180}],
 {{dose1, 1.0, "Initial Amount"}, 1.0, 7.5, Appearance -> "Labeled",
  ImageSize -> Tiny},
 {{r, 7.5, "bacteria Multiplication"}, 1., 7.5,Appearance->"Labeled", ImageSize ->
Tiny},
```

```
 {{k, 3.06, "bacteria Reduction Rate"}, 1, 4.55,Appearance->"Labeled", ImageSize ->
Tiny},
 {{p, 4.1, "Predecesor Cells"}, 4.1, 20., Appearance -> "Labeled", ImageSize ->
Tiny},
 {{s, 2.5, "Cell Stimulating Rate"}, 2.5, 5,Appearance->"Labeled", ImageSize ->
Tiny},
 SaveDefinitions -> True, ControlPlacement -> Top, TrackedSymbols :> {dose1, r, k, p,
s},
 Initialization :> {t2 = 3; dose2 = 6; f[t_, p_] := p cT[t]^2/(1 + cT[t]^2);
   g[t_, s_] := s cE[t]^2/(1 + cE[t]^2)}]
```

The initialization contains the crucial computation of conditions for f(T) and g(E), implemented as:

f[t_,p_]:=p cT[t]^2/(1+cT[t]^2)

g[t_,s_]:=s cE[t]^2/(1+cE[t]^2)

Then, two standard differential equations are solved using NDSolve, where NDSolve[*eqns*,*f*,{*x*,*xmin*,*xmax*}] catches a mathematical solution to the normal differential equations given by *eqns* for the function f with the independent variable x in the range x_{min} to x_{max}.

Finally, *ParametricPlot*[{f_x, f_y},{u, u_{min}, u_{max}}] is used to generate a parametric plot of a curvature with x and y coordinates Subscript[f, x] and Subscript[f, y] as a function of u.

Numerical examples

Example 1. Function manipulate generates a version of expr with controls added to allow interactive manipulation of the value of parameters. Therefore, we get the below depicted controls, which are used to manipulate the results based on the input values.

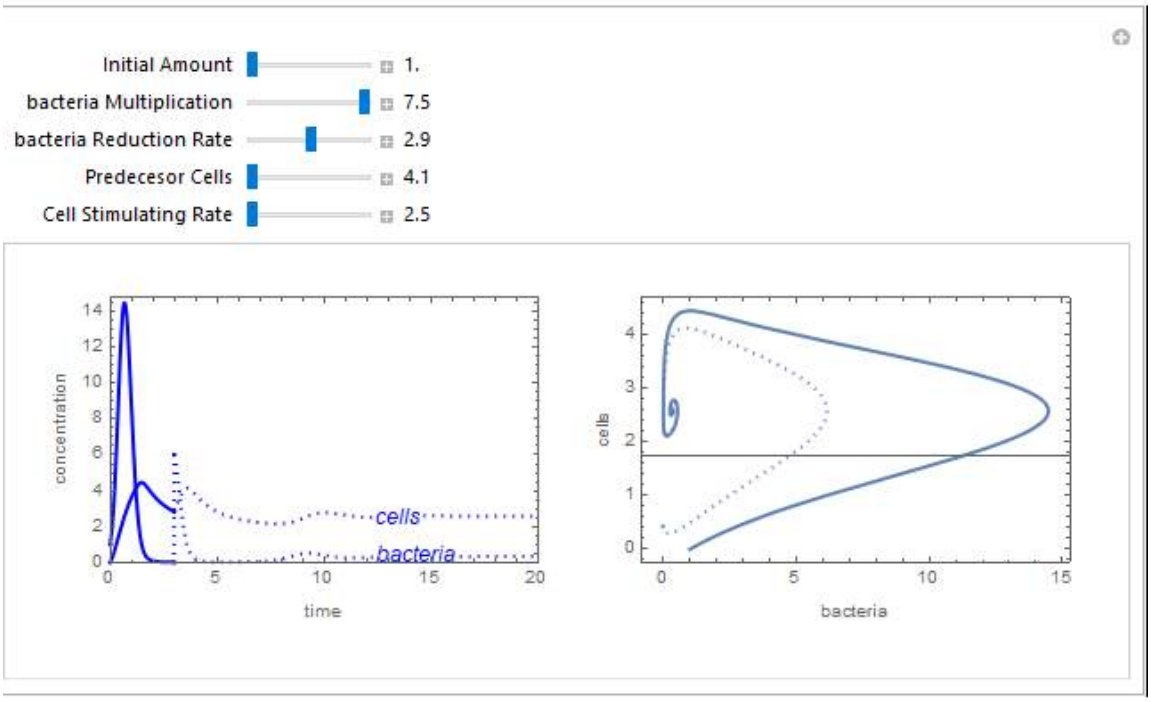


Figure 1. *Controls and the results based on the specific input values.*

In this example, we have set the initial amount to be the largest possible, the predecessor cells amount and the cell stimulating rate to the smallest amounts. By considering the bacteria multiplication rate to be equal to 7.5 and the bacteria reduction rate to be equal to 2.9, we have obtained the concentration-time-bacteria parametric plot as given in Figure 1.

Example 2. Here, we have set the initial amount, the predecessor cells amount and the cell stimulating rate to the smallest amounts. By considering the bacteria multiplication rate to be equal to 4.3 and the bacteria reduction rate to be equal to 3.98, we have obtained the concentration-time-bacteria parametric plot as given in Figure 2.

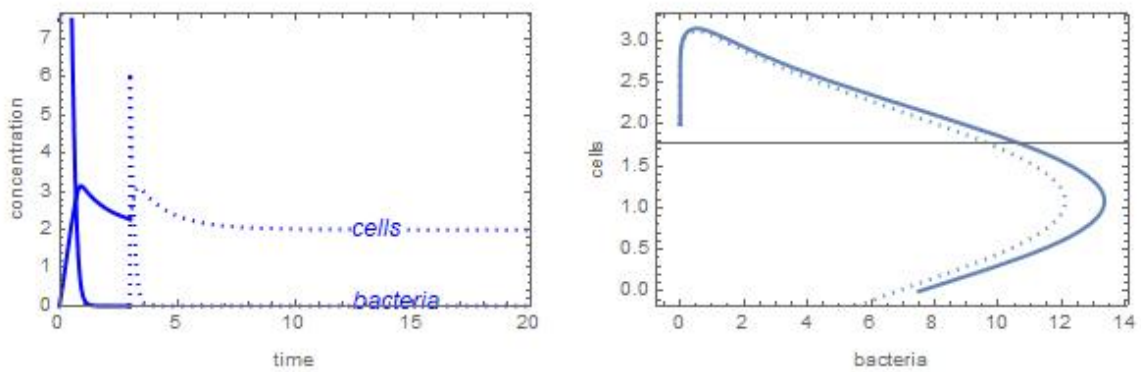


Figure 2. *Results based on the specific input values.*

Conclusions and Future work

We have performed a simulation of immune system response using a cellular automata approach. Therefore, a standard scheme of the resistant reaction is labeled by a structure of the conventional differential equations.

Obviously the utilization of the technique depends essentially on the yield of the model as opposed to on the multifaceted nature of the model. Other expansion of the two-dimensional CA model of tumor– insusceptible connecting can without much of a stretch be dealt with. For instance, one can ponder the varieties in the supplement utilization rates which may prompt changes in the morphologies of the developing tumor [16], the impact of the tissue oxygen focus on the development of strong tumor [14], the impact of mechanical weight on the development procedure [12], the impact of various cytotoxic effectors (macrophages, NK cells, tumor cell demolition by immune response subordinate cell cytotoxicity) on the development examples of the malignancy tumors [1], and so on.

At long last, the likelihood of future improvement of the present strategy includes the genuine application with three stages system. Rather than utilizing the reenacted information, one can conclude the model condition from the information produced by CA display that recreated by utilizing the parameter evaluate from the genuine informational index.

For future work, one could incorporate more parameters to the model in order to make more realistic simulation; for example, incorporate parameters such as age, gender, socioeconomic status and other factors. Also for future simulations could investigate the effects over time of initiation of therapy, discontinuation and periodicity should be applied.

References

[1] Dewdney, A. K. (1989). A cellular universe of debris, droplets, defects and demons. *Scientific American*, *261*(2), 102-105.

[2] Bezzi, M., Celada, F., Ruffo, S., & Seiden, P. E. (1997). The transition between immune and disease states in a cellular automaton model of clonal immune response. *Physica A: Statistical Mechanics and its Applications*, *245*(1-2), 145-163.

[3] Boondirek, A., Lenbury, Y., Wong-Ekkabut, J., Triampo, W., Tang, I. M., & Picha, P. (2006). A stochastic model of cancer growth with immune response. *JOURNAL-KOREAN PHYSICAL SOCIETY*, *49*(4), 1652.

[4] Castiglione, F., Mannella, G., Motta, S., & Nicosia, G. (1999). A network of cellular automata for the simulation of the immune system. *International Journal of Modern Physics C*, *10*(04), 677-686.

[5] de Pillis, L. G., Mallet, D. G., & Radunskaya, A. E. (2006). Spatial tumor-immune modeling. *Computational and Mathematical Methods in medicine*, *7*(2-3), 159-176.

[6] Puzone, R., Kohler, B., Seiden, P., & Celada, F. (2002). IMMSIM, a flexible model for in machina experiments on immune system responses. *Future Generation Computer Systems*, *18*(7), 961-972.

[7] Celada, F., & Seiden, P. E. (1996). Affinity maturation and hypermutation in a simulation of the immune immune response. *European journal of immunology*, *26*(6), 1350-1358.

[8] Farmer, J. D., Packard, N. H., & Perelson, A. S. (1986). The immune system, adaptation, and machine learning. *Physica D: Nonlinear Phenomena*, *22*(1-3), 187-204.

[9] Celada, F., & Seiden, P. E. (1992). A computer model of cellular interactions in the immune system. *Immunology today*, *13*(2), 56-62.

[10] Mayer, H., Zaenker, K. S., & An Der Heiden, U. (1995). A basic mathematical model of the immune response. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, *5*(1), 155-161.

[11] Kleinstein, S. H., & Seiden, P. E. (2000). Simulating the immune system. *Computing in Science & Engineering*, *2*(4), 69-77.

[12] Owen, M. R., & Sherratt, J. A. (1997). Pattern formation and spatiotemporal irregularity in a model for macrophage–tumour interactions. *Journal of theoretical biology*, *189*(1), 63-80.

[13] Perelson, A. S., & Weisbuch, G. (1997). Immunology for physicists. *Reviews of modern physics*, *69*(4), 1219.

[14] Perelson, A. S. (2018). *Theoretical Immunology, Part One*. CRC Press.

[15] Santoni, D., Pedicini, M., & Castiglione, F. (2008). Implementation of a regulatory gene network to simulate the TH1/2 differentiation in an agent-based model of hypersensitivity reactions. *Bioinformatics*, *24*(11), 1374-1380.

[16] Seiden, P. E., & Celada, F. (1992). A model for simulating cognate recognition and response in the immune system. *Journal of theoretical biology*, *158*(3), 329-357.

[17] Wodarz, D. (2003). Evolution of immunological memory and the regulation of competition between pathogens. *Current biology*, *13*(18), 1648-1652.

[18] Wolfram, S. (1984). Universality and complexity in cellular automata. *Physica D: Nonlinear Phenomena*, *10*(1-2), 1-35.

[19] Wolfram, S. (1986). *Theory and applications of cellular automata: including selected papers 1983-1986*. World scientific