ZETANET: Blockchain 5.0 & Internet 2.0

Professor Dr Lord Jack Rahman

Zetanet Abstract — A real secure communication has long been an import issue in recent years. To protect ones privacy, encryption was invented to help owners encrypt the data into meaningless information to non-receiver in order to prevent leakage. Since zeta series encryption in Jack's Law provides more flexibility in information protection as it grows more attention, but effective methods are rare in this new research domain. In this blockchain 5.0 project, a multi-layered and authentication-enhanced scheme for information encryption based on Jack's Law was created and its application focuses on encryption and autonomous storage. The scheme encrypts the whole or parts of the data according to its owners' authorization by cryptography. Owners of the data can also specify their own permissions encrypted by hashing data based on their own private key as a signature in the data by embedding the corresponding authentication codes into the encrypted data. Later, the receivers can extract the hidden authentication codes to judge whether the decrypted data is authentic. The design applied in Zetanet is to demonstrate the effectiveness of the proposed Jack's Law encryption scheme, and the conceptual framework for autonomous storage that can also be applied to other applications requiring information encryption especially in the new Internet 2.0 for blockchain.

In digital word security is a most important issue and data hiding with image cryptography is one of the possible ways to ensure the security of the important message from outer world. In this paper we proposed a novel technique that encrypted the message such a ways that the message encoded as well as hidden in an image. The proposed solution is to use image cryptography to hide textual message. The proposed technique use of an encryption technique that is based on Fibonacci series & image encryption and a secret key generated from the image.

The objective of cryptography is to make it feasible for two persons to exchange a message in such a way that other persons cannot understand. There is no end to the number of ways this can be done, but here the proposed method will be more concerned with a technique of encoding the text in such a way that the recipient can only discover the original message. The original message usually called plain text is converted into cipher text by finding each character in the message and replacing it with another character based on the Fibonacci number generated. Further cipher text is converted into Unicode symbols, which avoid suspicion from the third party when send through an unsecured communication channel. There are two levels in the proposed method; (i) converting plain text to cipher text and (ii) converting cipher text to Unicode symbols. In each level, security key is used to encode the original message which provides two levels of security from intruders. On the other end, the extraction algorithm is designed in such a way that the process converts the Unicode symbols into cipher text and then cipher text to plain text. This encoding and decoding scheme of the proposed method is significantly different as compared to the traditional methods. With the increase in the use of electronic transactions in everyday life, secure communications and data storage to withstand any kind of attack is warranted. The golden ratio, being the most irrational among irrational numbers, can be used in elliptic curve cryptosystems, power analysis security, and other applications. However, in such applications, cryptographic operations should take place very quickly before the keys are extracted or decoded by the attackers. This paper proposes an efficient method of golden ratio computation in cryptography to resist information security breaches. We compare our new golden ratio method with the well-known Fibonacci sequence method. The experimental results show that our proposed method is more efficient than the Fibonacci sequence method. Our golden ratio method with infinite precision provides reliable counter measure strategy to address the escalating security attacks.

Index Terms— Cipher text, Decryption, Encryption, Fibonacci Number, Key, Plain text, Unicode Symbols security, image cryptography, encryption technique, Fibonacci series, image encryption, secret key, Secret Sharing; Double layered Image Encryption; Tag Image; Access control, Skipjack, Encrypblock, Encrypcurrency, Zetanet, Jack's Law.

INTRODUCTION

Zetanet project is a Blockchain 5.0 project lead by Skipjack Technology and the partners and in future may include a consortium of leading universities working in partnership with industry and the government's. This Next Generation Internet (NGI) initiative is for developing a faster, more reliable Internet 2.0 for blockchain technology and communities including all over the world.

The Internet 2.0 Blockchain Initiative enables a new generation of emerging new applications whose architecture and development have been restricted by or are beyond the constraints of traditional Internet environments. These initiatives facilitate a variety of activities to foster the development and deployment of emerging applications that meet the requirements throughout the public sector.

Blockchain applications that work with high performance networks and supercomputing capabilities offer exciting new solutions for the internet industry. Internet 2.0 strive to combine the expertise of their constituents to establish a decentralised knowledge system for achieving innovation in research, teaching, learning, and commercialization. Zetanet as Internet 2.0 is an effort by Skipjack Technology to develop advanced Internet 2.0 technology and applications vital to the research and commercialization blockchain technology . Zetanet in partnership with blockchain industry and government, to provide leadership and direction for advanced Internet development. The "community" of Zetanet also includes international participation through agreements with similar groups worldwide.

HISTORY

Skipjack Technology leadership drives Zetanet Internet 2.0 with the demand for advanced applications and valuable expertise to implement initiatives. The combination of requirements and resources provides a perfect setting for developing the next generation of Internet capabilities. By accelerating the blockchain technology necessary to move the appropriate blockchain technologies into the commercial sector, Internet 2.0 provides both a next generation network and the applications that run on high performance decentralized networks.

Skipjack Technology invented **Jacks Law** and started the advanced application technology development has led to the introduction of Zetanet to be as Internet 2.0 initiatives by first released the **Encrypblock 1.0** technology in 2018. The Zetanet Initiative was created in January 2018 and allows members of Encrypblock 1.0 to find peers, work collaboratively, and share tools and other resources. Its goals include facilitating the creation and enhancement of blockchain applications whose development and deployment have been hampered or prevented by traditional Internet technology. Through the Zetanet Initiative the project work closely together to catalyze the development and deployment of advanced applications in the blockchain domain.

The internet, designed more than 40 years ago, has grown from little more than a research project to something that touches almost all digital interactions in the world. Although the core, lower-layer internet protocols have remained somewhat consistent since the 1990s, the internet's application layer and server infrastructure have evolved tremendously to support the massive growth of internet applications.The primary model for building internet applications is the client/server model , popularized in the 90s. This model was a short-term blessing with long-term negative consequences. It enabled the Web to take off but caused Web services to become increasingly dependent on remote servers. Cloud computing is an evolution of the basic client/server model. Today, cloud providers stores private user data, run application logic and computations, manage access credentials, and so on.

Zetanet is an open-source effort to design, develop, and grow a zetanet network by integrating decentralized computing network that provides an alternative to traditional cloud computing. Zetanet is reimagining the transport layer of the traditional internet and provides a new network for decentralized applications; transport and applications layers built on Zetanet enable users to own and control their data directly into new internet. Zetanet creating new internet transport layer and underlying communication protocols while removing points of centralization in the application layer.

We follow the end-to-end design principle to keep the core of the network simple while pushing complexity to the clients. To scale the applications, we minimize global change and provide a reliable non decentralized storage system that gives comparable performance than to cloud storage. Further, our approach gives default options for all developer stack components necessary to build decentralized applications. Zetanet is modular, and developers can easily customize it and integrate alternative technologies.

This paper is a major revision of our earlier 2018 whitepaper and will incorporate the evolution of our design as to be design in production deployments and future feedback from application developers. This paper introduces the design of our new *Zetanet* blockchain, which is designed to enable blockchain run on top over zetanet , scale up decentralized applications and provide incentives to developers for building high-quality applications .We created a new smart contracting language where developers would be able to call and reuse function that are generic running on top of zetanet, this layers gives flexibility and standardization for developers while creating their blockchain or app on top of zetanet called *Blowfish,* that will optimize security in Zetanet (Section 3). We outline the design of the *Zetanet Autonomous Data* decentralized storage system (Section 4), our authentication protocol (Section 5), developer tools (Section 6), and highlight some ways in which application developers are currently using Zetanet (Section 7).

BACKGROUND ON ZETANET

In recent years, blockchain systems and their applications have expanded the boundaries of the crypto space and resulted in deeper decentralized application development. Bitcoin, Ethereum, Hyperledger Fabric, Corda, and other public and consortium chains have continued to emerge, creating a highly competitive environment. The research community required more functionality than existed in the Internet of the mid-90s. Responding to this need, in mid 2015, Skipjack started the research on fundamental of creating Internet 2.0. How we design the Zetanet to be a new Internet 2 is based on the encrypblock protocol that we created in 2017. EncrypBlock is a technology that has many application. One of which is through Financial Technology, Encrypblock can act as a Real-Time Gross Settlement and Security technology that allows a more secure and fast transaction that also scales up to more than 1,000,000 transactions per second. EncrypBlock Technology is built upon a zeta series internet protocol, and supports a new digital currency (encrypcurrency) that will represent fiat currency, cryptocurrency, commodities, or other units of value such as frequent flier miles or mobile minutes. Released in 2018, EncrypBlock Technology purports to enable "secure, instant, and almost free global financial transactions of any size with no chargebacks."

The Zetanet protocol suite provides an end-to-end data communication specifying how data should be packed, addressed, transmitted, routed, and received in the network topology of Zeta Series. This functionality is organized into abstract layers, which classify all related protocols according to the scope of networking involved. Encrypblock plans to be the core of all kinds of transactions especially in Financial institutions. With the development of blockchain technology and its applications, various problems have gradually been exposed. Issues such as the inability to scale for large-scale performance, the inability to support diverse business use cases, and the inability to exchange information and share assets across different blockchain networks have become more prominent.

In response to these problems, we are going back to the core values of blockchain technology. We want to solve blockchain's current problems by improving some of the base-level issues – consensus algorithms, adding the new encryption protocol, ecological topologies, cross-chain agreements, underlying new network communication protocols, collaborative convergence computing, application ecosystems, and more, to promote the wider application of blockchain and Internet of Value technology.

VISION

The following major technological solutions:

- A novel Zetanet Algorithm Protocol to improve speed, security and new concept autonomous data (zero storage) and transaction per second, With the new consensus agreement which will remove the Byzantine Agreement (BA) algorithm.
- A Zeta Series Network (ZSN) architecture is a new network concept for nodes with high scalability and speed for use in a wide variety of application scenarios. This network will be secure, include resource isolation, and can be customizable for any demand.
- Zetanet Protocol (ZP) and Zetanet Crypto Algorithm (ZCA) to aid in the naming, discovery, and addressing of Value Zetanet assets and entities. These seamlessly integrate with internet resources to build underlying protocols and infrastructure services for blockchain ecosystems.
- A new protocol design TCP/UDP-based low-latency Zetanet Protocol (ZP) to better adapt to and meet the requirements of blockchain network interactions compared to the traditional internet.

There are many different types of decentralized systems in production today. The primary goal of Bitcoin, the first and currently the largest blockchain network, is to track and resolve the ownership of the Bitcoin digital currency. The goal of Ethereum is more general purpose: to construct a "world computer" to enable smart contracts and decentralized applications. Filecoin is an attempt to construct a network for decentralized file hosting and storage. In contrast, Zetanet attempts to realize *a blockchain internet* for decentralized computing, focus on enabling secure, private applications where the blockchain layer handles minimal state and logic because of Zetanets' protocol layer for reusable codes and function standards.

Design Goals

The design of Zetanet optimizes for the following properties:

1. **Easy to Use. Zetanet Internet 2.0** decentralized applications should be easy to use for end users in internet 2.0 applications. Decentralized applications should be as easy to develop as developing on Zetanet.

2. **Scalability**. Zetanet should support users at internet-scale, i.e., hundreds of millions to billions of users. The network blockchain 5.0 must scale with the number of users and applications it runs.

3. **Autonomous Data and User Control**. Applications that use zetanet should put users in control by default. No dependent on servers operated by applications, users should be able to provide their computation and storage resources in autonomous data.

4. **Minimal logic and state at the blockchain layer**: To achieve scalability, Zetanet minimizes application logic and data at our "zetanet" blockchain layer. Using blockchain operations for application logic and storage is inherently slower than "off-chain" approaches; the need to synchronize and validate state across a wide range of networks and devices imposes significant limits on the throughput of such operations. The limiting factor is underlying bandwidth for global connectivity and memory/storage available at typical network nodes, i.e., physical limitations (vs. any protocol limits).

5. **Autonomous data storage changes**: The Zetanet network uses an approach to ensure that applications built on top are scalable: interactions in applications result in local state changes vs. global state changes whenever possible. Autonomous data to reduce storage system and new encryption authentication protocol are fundamental components of our network— they enable applications to interact with a user's private data and authenticate a user without ever issuing a blockchain transaction. The zetanet blockchain is only used to coordinate global state transitions in a consistent way (such as registering a globally-unique credentials) in a decentralized fashion.

6. **Reliable cloud-like storage vs. peer storage**: Applications built on Zetanet store data with the user (using their private data lockers) and don't need to store any user data or access credentials at the server side. This approach not only puts users in control of their data but also reduces complexity for developers: developers no longer need to run servers and databases and pay cloud infrastructure bills on behalf of their users. Moreover, we avoid reliability and performance issues inherent with peer-to- peer storage and repurpose existing cloud storage providers in a decentralized wide-area file system — the blockchain layer only stores pointers to user's data lockers. **SDKs for developers**: Zetanet provides default options for all the layers required to develop decentralized applications. Developer SDKs abstract away the complexity of the blockchain and other technologies at work; application developers can build their applications with ease using interfaces of SDKs .Various layers of the developer stack are modular and can be used with other technologies as needed.

In addition to these differences from contemporary decentralized computing approaches, our smart contract language also makes unique design decisions to optimize for security and predictability of smart contracts.

A NEW MODEL

A New Model for Applications

Zetanet provides developers with a new model for constructing applications, ensuring that the applications are decentralized and put the users in control by default:

1. **No opaque databases**: In the client/server model, databases are a core part of any application because the server-side needs to store and query large amounts of user data. In decentralized computing, developers don't need to worry about maintaining and securing databases since they do not host data in the first place. Developers mostly focus on their app logic; users download the apps and plug- in their private data lockers. Databases, if used, are functionally equivalent to "search indexers" on the old internet— services which index public data. Anyone can create these indexes using the underlying (decentralized) data.

2. **No servers:** In the client/server model, apps scale by adding more servers as computations for all users execute on the server side. In decentralized computing, apps run client-side, and each new user brings their computation and storage capacity to the network (rather than relying on the app developers). Developers only need to supply minimal infrastructure for hosting the application code, since each user brings the storage and computing resources they need to use the app.

3. **Smart contracts:** In the client/server model, global state changes are coordinated by a central server which functions as the sole authority of truth in the network. In decentralized computing, these state changes occur through smart contracts executing on an open blockchain.

4. **Decentralized authentication**: In the traditional internet, users authenticate using some trusted authentication process. If an application maintains a user database, the application authenticates the user with a password and sometimes a second factor. If an application relies on a third-party identity service, like Google or Facebook and other federated identity, uses OAuth 2.0 to obtain an assertion from that identity service. Of course, all these approaches remove control of the process from the users themselves. In comparison, decentralized computing authentication is performed using OIDC mechanism by cryptographically signing a statement proving control over a particular credentials anchored to the blockchain. Any application can independently verify these proofs.

5. **Native tokens**: In traditional internet applications, payment activities are usually performed using third-party services like credit cards. Digital tokens are a native asset of decentralized computing platforms like Zetanet and Ethereum. Users have direct ownership of these tokens and can use them directly to register digital assets and smart contracts, as well as pay for executing smart contracts. Use of such native tokens can be programmed through smart contracts to build subscription services and automate other app functionality. Such programmable tokens were traditionally not available to developers of traditional internet apps.

Layers of Decentralized Computing

The Zetanet decentralized computing network logically exists at the "application layer" in the traditional internet design. However, the Zetanet network itself is composed of multiple systems which together provide the necessary components for implementing decentralized applications:

1. Zetanet Blockchain: The foundation for the Zetanet network is the Zetanet blockchain which enables users to register and control digital assets like universal credential and register/execute smart contracts. Digital assets like universal credential, in turn, allow users to control their data storage and more—users link their access credentials for private data lockers with their universal credential.

2. Autonomous Data: The Autonomous Data storage system is a user-controlled storage system that enables applications to interact with private data lockers. Users can host these encrypted data lockers on a cloud-provider, local disk, or remote storage. Importantly, the user controls the choice of the underlying provider. Data on Autonomous is encrypted and signed client-side by the user's cryptographic keys. Data lockers for users are discovered by looking up information on the Zetanet blockchain.

3. Zetanet Authentication: The Zetanet Authentication protocol is a protocol for decentralized authentication with applications. This protocol enables users to authenticate using identities that they own and provide information about which Zetanet location should be used to store that user's application data.

4. Zetanet Libraries and SDKs: At the top of the software stack are the developer libraries and SDKs through which application developers and users interact with the various components of the zetanet network. For example, Zetanet client software allows users to register and manage their own identities. Zetanet's developer libraries make it as easy for developers to build Zetanet applications as it is to create traditional web applications.

Zetanet as a Blockchain

The foundation of Zetanet is its own blockchain network. The Zetanet blockchain provides the global consensus and coordination layer for the network and implements the native token of the Zetanet called the *Zetanet coin*. Zetanet coin are consumed as "fuel" when users register digital assets like universal credential, software licenses, pointers to storage lockers, etc. They are also used to pay miners for registering/executing smart contracts.

We present the high-level design of the Zetanet blockchain, for more details on how these designs are being implemented and are evolving, we recommend reading the Zetanet Blockchain Improvement Proposals (ZBIPs) for these various component as well as Zetanet Resquest for Comments (ZRC). We plan to update this paper as more ZBIPs or ZRC are accepted through the Zetanet improvement process.

PROBLEM STATEMENT

The airwaves, telephone circuits, and computer cables are buzzing. Digital information surrounds us. We see digital bits on our new HDTVs, listen to them over the Internet, and create new ones ourselves every time we take a picture with our digital cameras. Then we email them to friends and family and create more digital bits.

There's no secret here. YouTube, a company that didn't exist just a few years ago, hosts 100 million video streams a day.

[i]Experts say more than a billion songs a day are shared over the Internet in MP3 format.[ii] Digital bits. London's 200 traffic surveillance cameras send 64 trillion bits a day to the command data center.[iii] Chevron's CIO says his company accumulates data at the rate of 2 terabytes – 17,592,000,000,000 bits – a day.[iv] TV broadcasting is going all-digital by the end of the decade in most countries. More digital bits.

What is a secret – one staring us in the face – is how much all these bits add up to, how fast they are multiplying, and what their proliferation imply.

This White Paper, is forecast of the digital universe – all the 1s and 0s created, captured, and replicated – and the implications for those who take the photos, share the music, and generate the digital bits and those who organize, secure, and manage the access to and storage of the information.

When it comes to disruption in the tech world, there are only few that made a huge impact in more than just one industry. An example of this is blockchain technology.[1] Blockchain was predicted to fundamentally change the way things are done[2] as well as create new opportunities for different industries to maximize its potential without huge cost implications.

However, like any new technology, it comes with its own limitations and issues[3]. Below are some of the issues associated with blockchain technology and its applications:

- **Environmental Implications**. Blockchain uses encryption to validate transactions over a distributed network as well as keeping it secure. This means complex algorithms and large computing power are required for every transaction, which in turn would consume large amounts of energy. A study 4conducted in 2017 showed that the computing power needed to run Bitcoin required the same amount of energy used by 159 of the world's nations.

- **Complexity**. Blockchain technology requires a lot of reading to fully understand the concept of distributed ledgers and encryption. The popularity of blockchain-based payment systems are built upon the unreliability of traditional systems employed by banks and financial institutions.

- **Slow Transaction Speed**. Due to the complexity and distributed nature of old blockchain networks, transactions can sometimes take several hours to finalize. In addition, since these chains are basically data that needs processing, there is a tendency for it to become slow and unwieldy as it grows in size and the number of computers accessing the network.

[1] https://www.cardozo.yu.edu/sites/default/files/SSRN-id2580664.pdf

[2] https://www.bernardmarr.com/default.asp?contentID=1302

[3] https://www.forbes.com/sites/bernardmarr/2018/02/19/the-5-big-problems-with-blockchain-everyone-should-be-aware-of/#7d5104ee1670

[4] https://futurism.com/mining-bitcoin-costs-more-energy-159-countries-consume-year/

Skipjack Preface

There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files.
If I take a letter, lock it in a safe, hide the safe somewhere in New York, then tell you to read the letter, that's not security. That's obscurity. On the other hand, if I take a letter and lock it in a safe, and then give you the safe along with the design specifications of the safe and a hundred identical safes with their combinations so that you and the world's best safecrackers can study the locking mechanism—and you still can't open the safe and read the letter—that's security.For many years, this sort of cryptography was the exclusive domain of the military. The United States' National Security Agency (NSA), and its counterparts in the former Soviet Union, England, France, Israel, and elsewhere, have spent billions of dollars in the very serious game of securing their own communications while trying to break everyone else's. Private individuals, with far less expertise and budget, have been powerless to protect their own privacy against these governments.

During the last 20 years, public academic research in cryptography has exploded. While classical cryptography has been long used by ordinary citizens, computer cryptography was the exclusive domain of the world's militaries since World War II. Today, state–of–the–art computer cryptography is practiced outside the secured walls of the military agencies. The layperson can now employ security practices that can protect against the most powerful of adversaries—security that may protect against military agencies for years to come.

Do average people really need this kind of security? Yes. They may be planning a political campaign, discussing taxes, or having an illicit affair. They may be designing a new product, discussing a marketing strategy, or planning a hostile business takeover. Or they may be living in a country that does not respect the rights of privacy of its citizens. They may be doing something that they feel shouldn't be illegal, but for whatever reason, the data and communications are personal, private, and no one else's business.

In 1994, the Clinton administration approved the Escrowed Encryption Standard (including the Clipper chip and Fortezza card) and signed the Digital Telephony bill into law. Both of these initiatives try to ensure the government's ability to conduct electronic surveillance.Some dangerously Orwellian assumptions are at work here: that the government has the right to listen to private communications, and that there is something wrong with a private citizen trying to keep a secret from the government. Law enforcement has always been able to conduct court–authorized surveillance if possible, but this is the first time that the people have been forced to take active measures to *make themselves available* for surveillance. These initiatives are not simply government proposals in some obscure area; they are preemptive and unilateral attempts to usurp powers that previously belonged to the people.

Clipper and Digital Telephony do not protect privacy; they force individuals to unconditionally trust that the government will respect their privacy. The same law enforcement authorities who illegally tapped Martin Luther King Jr.'s phones can easily tap a phone protected with Clipper. In the recent past, local police authorities have either been charged criminally or sued civilly in numerous jurisdictions—Maryland, Connecticut, Vermont, Georgia, Missouri, and Nevada—for conducting illegal wiretaps. It's a poor idea to deploy a technology that could some day facilitate a police state.
The lesson here is that it is insufficient to protect ourselves with laws; we need to protect ourselves with mathematics. Encryption is too important to be left solely to governments.

Let have a look in the other part of the digital world problem. What will we do when the world's data hits 163 Zettabytes in 2025? Zettabytes **Now Needed to Describe Global Data Overload**

In less than a decade from now, total worldwide data will swell to 163 zettabytes, which is equivalent to watching the entire Netflix catalog 489 million times. Most of this data will be created by enterprises and only about half will be be fully secured, says a Seagate study. We — humanity, that is — created 4.4 zettabytes of data last year. This is expected to rise to 44 zettabytes by 2020. And no, I didn't make up the word "zettabytes." For scale, it is estimated that 42 zettabytes could store all human speech ever spoken. One zettabyte is around 250 billion DVDs — almost enough fit the whole *Friends* series.All that data wouldn't be any use to us if we couldn't move it around quickly and reliably. We are constantly sending, receiving and streaming. We live in an age where anyone with a smart handheld device — and there are about 2.6 billion — can instantly become a video streamer. This large count doesn't even include big businesses and governments, most of which now do the majority of their communication digitally, adding to a prodigious amount of bits and bytes.

As connectivity continues to skyrocket, will we be able to move this data fast enough? Are we willing to pay the price to keep moving it faster and more reliably?

To c or Not To c

Current technology/wires are very fast, but our data creation and consumption is quickly catching up. Google Fiber, offering one of the fastest speeds available to regular consumers, has a transfer rate of one gigabit per second, and the Hibernia Express, a transatlantic fiber optic cable currently under construction for use in financial markets, will have a rate of 8.8 terabits per second (8800x faster than Google Fiber). So why not just go faster?

We are running up against the universal speed limit.

There are rules to the universe. Unfortunately, we don't know all of them. What we do know is that information has a speed limit: namely, c, the speed of light. Light travels about 300,000,000 meters per second. The two cables mentioned above, Google Fiber and the Hibernia Express, are both moving data at about 2/3 c (two-thirds the speed of light), limited by the refractive properties of the glass fiber. Basically, light bounces around and slows down inside the cable.

The Need for Speed

Outside of business, milliseconds may not mean millions of dollars, but today's consumer expectations are higher than ever. Viewers now consider instantaneous; on-demand access the norm. In this ecosystem, the word "buffering" means something has gone wrong. Slow load times for images while online shopping can mean clicking on the next site and never returning. And for the streaming service provider or the online retailer, this means dents in the bottom line.

Are we willing to pay the price to keep moving data faster and more reliably?

The rate at which we create data is not going to slow down anytime soon. The advent of the Internet of Things looms on the horizon — a predicted 25 billion devices (three per person on Earth) each producing, sending and receiving data. Is our infrastructure ready for that cascade of data?

The Age of The Plateau

Notice how the line on the infographic below flattens out over the last few decades? We've made huge advances in previous decades, but now the rate of progress is affected by very different struggles. The most advanced technologies are only a few percentage points away from the speed of light — but the technology to reliably utilize that speed may be many years and many millions of dollars away.

An increase of a small percentage in speed requires intensive resources. The Hibernia Express will shave off 6 milliseconds of latency for transatlantic transmission. It is estimated that the project will cost more than $300 million, and firms will pay millions for access to the line. The secret behind the Hibernia's speed is quite simple: They laid the cable in a straighter line across the Atlantic.

For the average consumer, and even those with intense speed needs, like financial markets, the faster transfer doesn't make that much of a difference. But when we consider the sheer volume of data that will need to be moved constantly, reliably and without issue, the importance of these incremental steps toward better infrastructure is clear. Every tenth of a percentage point will be hugely impactful.

Faster, Better, Stronger

Luckily, breakthroughs are coming quickly, albeit often at great price. Researchers in the U.K. have created fiber cables that move data at 99.73 percent the speed light, and combined them with technologies that allow for incredible 73.7 terabits per second — that's a 5GB HD movie downloaded in 1 second. These cables, however, are so far only efficient for very short distances, so further work is needed.

A good way to avoid losing speed to the physical media you are sending the light through is to avoid it altogether. Microwave relays, which are sent through (mostly) empty air, are able to travel much faster. Relays must be built as a series of stationary towers, so the viability of crossing an ocean in such a manner would make for some serious construction challenges. Some have proposed a series of stationary barges holding towers and, in a truly sci-fi twist, a network of hovering drones that would transfer the signal over short distances using lasers.

All this progress will come at great cost. The financial sector has typically led the charge because of their reliance on absolute top speeds, and those technologies, proven in the fire of the international markets, eventually make their way into general business use.

We are spending billions on this development; progress is slow compared to the increase in speeds in previous decades. Every fraction of the speed of light matters if we expect to keep up with the incredible amount of data we will be capable of producing in the coming years.

Milliseconds don't matter until there are millions of them, and millions upon millions of people expecting to consume at speeds close to the speed of light.

ZTN ISSUANCE AND DISTRIBUTION

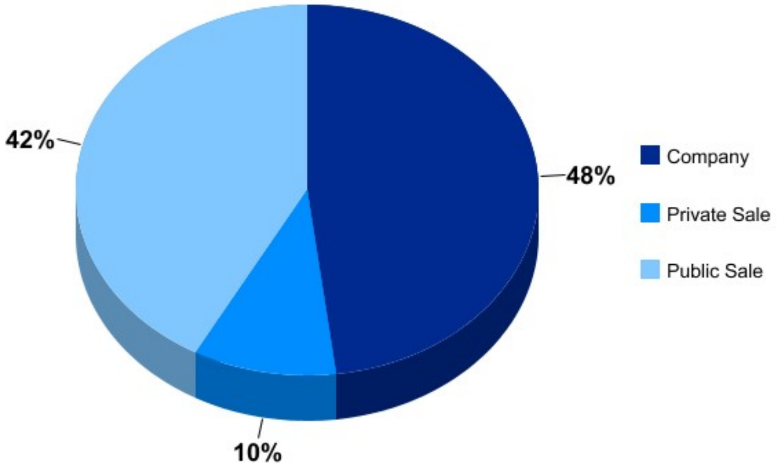
A. Token Distribution

A total of 5 billion ZTN will be issued, from which 2,100,000,000 will be offered to the market during public ICO.

Skipjack ZTN Token will be distributed as shown in the graph below:
(graph)

B. Token Sale Period

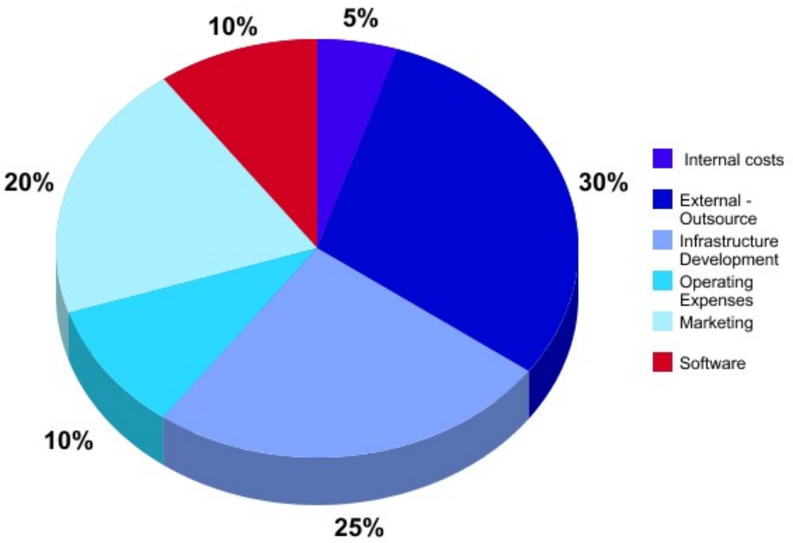
i. Private sale – Ongoing
ii. Public sale – 1 September 2019 to 1 September 2020



A total of 5 billion **ZTN** will be issued, from which 42% or 2,100,000,000 ZTN will be offered to the market in during **public ICO** with 10% 500,000,000 for **Private sale**. A limited amount of 1 million token is available for bounty and rewards. Each Token is priced at **0.002544529 ETH** with a minimum purchase of **1 ETH**.

USE OF FUNDS

The funds raised during the ICO will be used in the continuous development of Zetanet protocol including but not limited to @DOI, Encrypblock and blockchain-based Blowfish technology. It will also be used to promote these innovations for massive adoption. All funds usage are audited and accessible through etherscan.io



Summarized Description	USD (M)	Percentage
Legal and other Internal Costs	50	5.0%
External - Outsource	300	30.0%
Infrastructure Development	250	25.0%
Operating Expense	100	10.0%
Marketing	200	20.0%
Software	100	10.0%
	1000.0	100.00%

ENCRYPBLOCK AS REFERENCE

In this whitepaper we will discuss the invention of the new law of digital encryption and it is name as Jack's Law. The building blocks of Zetanet protocol architecture is base on the previous development in Encrypblock (Superencrypblock) protocol to be used in this project. Encrypblock was launched back in December 17, 2018 in the hope to help solve the problem on speed and data security in the financial industry. But, encrypblock is much more than that. It is the baseline of Zetanet protocol and all of Skipjack products such as skipjackfcn and Adoi. Both of which are available in public to try and use.

Jack's *law* *is the observation that the number of network computing in a dense of data doubles about every two years. The observation is named after the scientist of Skipjack Technology, who's in the Encrypcurrency paper described a doubling every year in the number of network connected per data network, and projected this rate of growth would continue for at least another decade. The period is often quoted as 18 months because of we predicted that network performance and efficiency protocols would double every 18 months (being a combination of the effect of more data and the network connectivity be more efficient and faster based on protocols and hardware improvement). This will be a problem solver of the increase of internet traffic that forecasts surge in IP traffic driven by number of factors, including growth of the Internet of Things.*

More Internet users, more connected devices, faster broadband speeds and more video all add up to one thing: a heck of a lot of IP traffic. Latest Visual Networking Index (VNI) shows global Internet traffic growing at an eye-popping rate, reaching 2 zettabytes per year by 2019.Two zettabytes is 12 times more than all the IP traffic generated in 2009.While it took 32 years -- from 1984 to 2016 -- to reach the first zettabyte mark, it will take only three more years to reach 2 zettabytes.Global IP traffic will grow at a compound annual growth rate of 23% between 2014 and 2019, reaching 168 exabytes per month in four years VNI forecast.

Jack's prediction will be use in the future internet industry to guide long-term planning and to set targets for research and development. Advancements in digital economy are strongly linked to Jack's law: Jack's law describes that the connectivity, the storage and the speed shall improve from the change of split protocol in the algorithm in the encryption of data technology. It is a factor to driving force of technological and social change, productivity, and economic growth.

Jack's law is an observation and projection of a trend and not a physical or natural law. In general, it is not logically sound to extrapolate from the historical growth rate into the indefinite future. When Jack's law applied in internet 2.0 in the form internet of value financial technology it will increase the store value of currency, improvement design in protocols efficiency and connectivity .The theory is solving the issue of speed of data, storage and connectivity. Superencryp block or Encrypblock had increase the efficiency in zeta series ledger that was developed before ledger in financial transaction to transfer the virtual currency more efficient where to the speed more than 1 million transactions per second.

What's the previous BIG IDEA?

Skipjacks' encrypcurrency is the virtual money that was birth based on the Jack's Law. It was designed to use under principle of Jack's law as Superencryp Block with Key Exchange Algorithm.

A **superencrypblock**, originally **superencryp block**, is a zeta series ledger called *superencryp*, which are linked using cryptography and encryption technology. Superencrypblock which are readable by the public are widely used by encrypcurrency. Each superencryp contains a cryptographic hash and encryption key exchange algorithm of the previous superencryp, double HMAC, a timestamp, and transaction data. By design, a superencrypblock is resistant to modification of the data. It is "a centralized ledger controlled by a system called ***Fiestel Core Network (FCN)*** that can record transactions between two parties efficiently and in a verifiable and permanent way. For use as a centralized ledger a superencrypblock is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new superencryp by FCN. Once recorded, the data in any given superencryp cannot be altered retroactively without alteration of all subsequent superencryp, which requires consensus of the network majority and FCN. Though superencrypblock records are not unalterable, superencryp may be considered secure by design and exemplify a centralized computing system with high double HMAC protocol verification method.

Superencrypblock was invented by Lord Jack in 2018 to serve as the public transaction ledger of the encrypcurrency skipjack dime. The invention of the superencryp block made it the first digital currency to develop highly encrypted application of new internet including to solve the transaction speed, security on the central server. The skipjack design has inspired other applications such as the Internet 2.0 in the Skipjack Zetanet project.

The rise of virtual currency represents a radical transformation of how people store and transfer value. But despite the growth of the cryptocurrency market, the underlying blockchain technology is far from mass market adoption due to its complexity, usability and scalability issues.

ENCRYPBLOCK

Encrypblock technology is a way to structure data without the need for a central authority but using the Skipjack Fiestel Core Network (FCN) and advanced blockchain 5.0. An encrypblock is a distributed database that hosts a continuously growing number of records. The database stores records in encrypblock rather than collating them in a single file. Each encrypblock is then "chiper" to the next encrypblock, in linear, chronological order, using a HMAC (hash message authentication code) cryptographic signature and Key Exchange Algorithm by Skipjack; as a result, records cannot be revised, and any attempted changes are visible to all participants. This process allows encrypblock to be used as ledgers, which can be shared and corroborated by anyone with the appropriate permissions. These zeta centralised ledgers can be spread across multiple sites, countries or institutions. Encrypblock technology is the foundation for financial transaction but there are a variety of telecommunications (Voice over Zetanet) and internet 2.0 technology (Zetanet protocol) financial and accounting applications beyond the realm of encrypblock own currency (encrypcurrency).

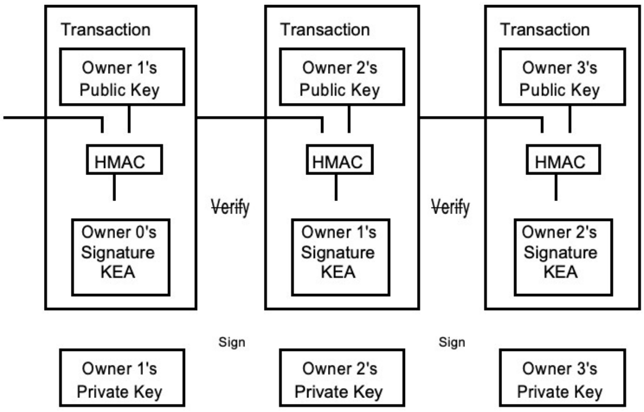


Figure : Encrypblock Protocol

TYPES OF ENCRYPBLOCK

Based on the participants, encrypblock are categorized as public, private or hybrid. This is similar to comparing the public internet and a company's intranet.

- Public and permission-less: Public and permission-less encrypblock resemble skipjack dime [encrypcurrency].All transactions in these encrypblock are public, and no permissions are required to join these distributed entities.
- Private and permissioned: These encrypblock are limited to designated members, transactions are private, and permission from an owner or manager entity is required to join this network. These are often used by private consortia to manage industry value chain opportunities.
- Hybrid encrypblock: An additional area is the emerging concept of blockchain, which allows for different blockchains (public or private) to communicate with each other in encrypblock, enabling transactions between participants across blockchain and encrypblock networks

ENCRYPBLOCK TODAY

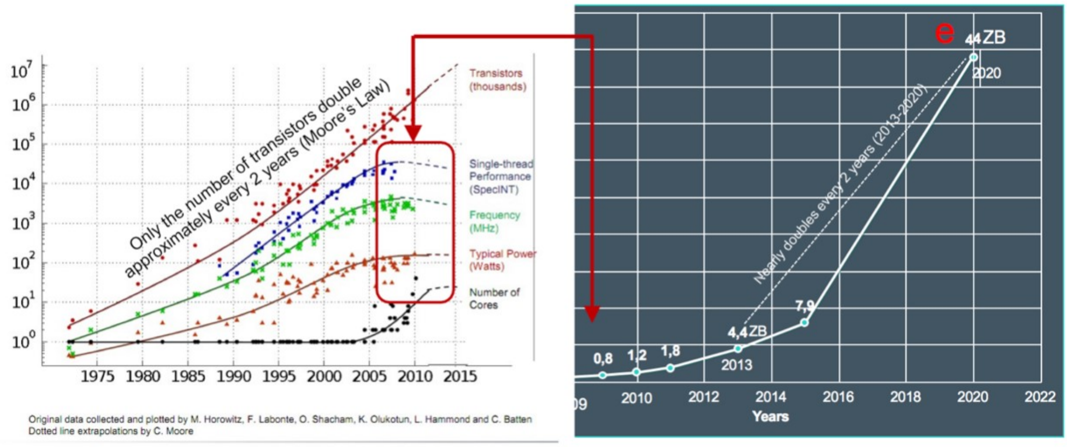
Encrypblock is at an inflection point, with momentum shifting and exploration to the building of practical business applications. This is particularly true among "digital enterprise" organizations [see enterprise vs. "emerging disruptors"], rather than in more traditional enterprises that are still working on how to incorporate digital into their existing operations and protocols. While our survey shows that these "enterprise digital" organizations may be lagging their fully digital brethren in this endeavor, the fact is, traditional enterprises are putting more resources behind encrypblock than they had been in an effort to achieve greater efficiency and to develop new business models and revenue sources.

Compare in the blockchain industry, despite enterprise digital respondents' interest in blockchain's capabilities, nearly 39 percent of the broad global sample said they believe blockchain is "overhyped." In the United States, this number is higher: 44 percent of respondents view blockchain as overhyped, up from 34 percent in a 2016 survey by Deloitte. This perception may be driven by the steep increase in token values over the last 18 months, and survey members conflating blockchain with the incentive layer of public blockchains, namely tokens.

On their own, these numbers seem to indicate that blockchain is moving in the wrong direction. However, we believe this change in attitude is more reflective of the shift toward the pragmatists in the blockchain community.

Because we are still early in encrypblock development, these fits and starts in its maturation are not surprising. While executives in the financial services sector, for example, are leading the way in using encrypblock to reexamine processes and functions that have remained static for decades, their counterparts in other sectors remain more reserved as they work to develop appropriate use cases for encrypblock. At the same time, there are a growing number of emerging technology disruptors across each sector in encrypblock, challenging traditional business models with the use of encrypblock protocol.

The Jack's Law



Original data collected and plotted by M. Horowitz, F. Labonte, O. Shacham, K. Olukotun, L. Hammond and C. Batten
Dotted line extrapolations by C. Moore

JACK'S LAW

Jack's law is the observation that the number of network computing in a dense of data doubles about every two years. The observation published Encrypcurrency paper described a doubling every year in the number of network connected per data network, and projected this rate of growth would continue for at least another decade. The period is often quoted as 18 months because of we predicted that network performance and efficiency protocols would double every 18 months (being a combination of the effect of more data and the network connectivity be more efficient and faster based on protocols and hardware improvement). This will be a problem solver of the increase of internet traffic that forecasts surge in IP traffic driven by number of factors, including growth of the Internet of Things.

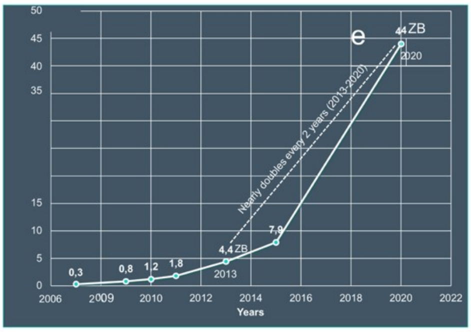
Based on the fundamentals of Jack's law, the superencrypblock is developed to the application for financial technology and the next Internet 2.0 as we described here as Zetanet. Zetanet is described as a new internet protocols to be released and demonstrate in year 2020 for the application of the next Internet 2.0.

Under Zetanet project by Skipjack Technology it will be used to solve the problem when the world's data hits 163 Zettabytes in 2025. Zettabytes now needed to describe global data overload and will be solved by the new Jack's law theorem

The Jack's Law

The invention states the data in computer network computing nodes is increasing nearly doubles every year and a split protocol is solving by increasing 10 times within the communication network.

Mr. Skipjack, Chief Scientist



Encrypcurrency protocols: Skipjack Protocol Building Blocks

Introduction to Protocols

The whole point of encrypcurrency is to solve financial transactions problems. (Actually, that's the whole point of computers—something many people tend to forget.) Encrypcurrency solves problems that involve secrecy, authentication, integrity, and dishonest people when do the transactions.
A **protocol** is a series of steps, involving two or more parties, designed to accomplish a task. This is an important definition. A "series of steps" means that the protocol has a sequence, from start to finish. Every step must be executed in turn, and no step can be taken before the previous step is finished. "Involving two or more parties" means that at least two people are required to complete the protocol; one person alone does not make a protocol. A person alone can perform a series of steps to accomplish a task (like baking a cake), but this is not a protocol. (Someone else must eat the cake to make it a protocol.) Finally, "designed to accomplish a task" means that the protocol must achieve something. Something that looks like a protocol but does not accomplish a task is not a protocol—it's a waste of time.
Protocols have other characteristics as well:

- Everyone involved in the protocol must know the protocol and all of the steps to follow in advance.
- Everyone involved in the protocol must agree to follow it.
- The protocol must be unambiguous; each step must be well defined and there must be no chance of a misunderstanding
- The protocol must be complete; there must be a specified action for every possible situation.

The protocols in this encrypcurrency design are organized as a series of steps. Execution of the protocol proceeds linearly through the steps, unless there are instructions to branch to another step. Each step involves at least one of two things: computations by one or more of the parties, or messages sent among the parties.

An **encrypcurrency protocol** is a protocol that uses cryptography. The parties can be friends and trust each other implicitly or they can be adversaries and not trust one another to give the correct time of day. An encrypcurrency protocol involves some cryptographic algorithm, but generally the goal of the protocol is something beyond simple secrecy. The parties participating in the protocol might want to share parts of their secrets to compute a value, jointly generate a random sequence, convince one another of their identity, or simultaneously sign a contract. The whole point of using cryptography in a protocol is to prevent or detect eavesdropping and cheating. If we have never seen these protocols before, they will radically change our ideas of what mutually distrustful parties can accomplish over a computer network. In general, this can be stated as:

- It should not be possible to do more or learn more than what is specified in the protocol.

This is a lot harder than it looks. In some of them it is possible for one of the participants to cheat the other. In others, it is possible for an eavesdropper to subvert the protocol or learn secret information. **Some protocols fail because the designers weren't thorough enough in their requirements definitions. Others fail because their designers weren't thorough enough in their analysis. Like algorithms, it is much easier to prove insecurity than it is to prove security.**

The Skipjack Encrypcurrency Protocol

Skipjack mission is to create a verified and centralized distributed platform for value exchange, a global currency protocol that enables a payment system that is easier, safer, and faster to use than paper money or cryptocurrency. In addition, Skipjack will ensure that the majority of the economic value generated by the platform is fairly distributed to the community through accounts created, to create a more balanced distribution of resources.

Skipjack seeks to address three issues within digital currencies: verification of speed transactions, usability of applications, and efficiency of transactions. Skipjack makes significant improvements by *1) forming a matching block superencryp to verify network 2) increasing overall skipjack dime supply, and creating multiple efficiency platform and mobile encryptrade apps, and 3) designing a centralized system managed by Fiestel Core Network (FCN) as central bank with less human interface. 4) Improving security breach by designing a hybrid protocol and multi layer encryption.*

Skipjack is a new currency that the new term as **encrypcurrency**. Skipjack is a general purpose encrypt digital currency. It is design for **programmable money backed with asset**. An **encrypcurrency** (or **encryp currency**) is a digital asset designed to work as a medium of exchange that uses encryption algorithm to secure its transactions, to control the creation of additional units, and to verify the transfer of assets. Encrypcurrency are classified as a subset of digital currencies and are also classified as a subset of alternative currencies and virtual currencies.The new skipjack algorithm will develop to overcome the existing traditional digital currency which currently having a lot of weakness.

Skipjack, created in 2018, is the **first zeta series encrypcurrency**. Skipjack and its derivatives use **Feistel Core Network (FCN) designed with Artificial Intelligence (AI) Superencryp Block** that control as same to centralized electronic money and central banking systems. The centralized control is related to the use of skipjack's **superencryp blockchiper** transaction database in the role of a distributed ledger.

Encrypcurrency (encryp money) or called as Skipjack Dime is a type of currency available only in digital form, not in physical (such as banknotes and coins). It exhibits properties similar to physical currencies, but allows for instantaneous transactions and borderless transfer-of-ownership. Examples include virtual currencies and cryptocurrencies or even central bank issued "digital base money". Like traditional money, these currencies may be used to buy physical goods and services, but may also be restricted to certain communities such as for use inside an on-line game or social network. Encryp currency is a money balance recorded electronically on a stored-value card or other device. Another form of electronic money is network money, allowing the transfer of value on computer networks, particularly the Internet. Encryp money is also a claim on a private bank or other financial institution such as bank deposits.

Skipjack Basic Protocols

Encryption Algorithms Contained in Skipjack

Skipjack may contain one or more of the following encryption algorithms.
Accordingly, Skipjack containing encryption are subject to the U.S. Export Administration Regulations and may be controlled for National Security (NS), Anti Terrorism (AT), and/or Encryption (EI) reasons.

The primary function of encryption in Skipjack falls into two categories:

1. Data Privacy (confidentiality - encrypting user data)

2. Administrative - OAM&P (secure network management - administrative network functions)

Data Hashing/Authentication
MD4
MD5 SHA-1 RIPEMD160 MICHAEL HMAC MMH CRC32

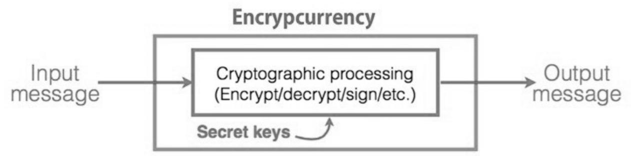
Key Exchange/ Asymmetric Algorithm Strength
DSA 1024, 1024/1536
Elliptic Curve Diffie-Hellman (ECDH) 163
RSA 1024, 2048, 4096
DSA 1024,2048 Diffie Hellman 1024, 1536 ElGamal 384

Data Security Encryption
Blowfish 128 CAST 128 DES-56 56, 64 Triple DES 112, 168, 192 DESX 56/64 RC2 40, 64, 128 RC4—128 40, 128 RC5 128 AES-128/l92/256 ARCFOUR 128 SEAL 160 IDEA 128 Skipjack

Message Authentication Codes

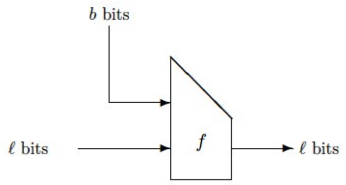
A **message authentication code** (MAC), also known as a data authentication code (DAC) use in Encrypblock protocol, is a one-way hash function with the addition of a secret key. The hash value is a function of both the pre-image and the key. The theory is exactly the same as hash functions, except only someone with the key can verify the hash value. Skipjack can create a MAC out of a hash function or a block encryption algorithm; there are also dedicated MACs.

A message authentication code, or MAC, is a key-dependent one-way hash function. MACs have the same properties as the one-way hash functions, but they also include a key. Only someone with the identical key can verify the hash. They are very useful to provide authenticity without secrecy. MACs can be used to authenticate files between users. They can also be used by a single user to determine if his files have been altered, perhaps by a virus. A user could compute the MAC of his files and store that value in a table. If the user used instead a one-way hash function, then the virus could compute the new hash value after infection and replace the table entry. A virus could not do that with a MAC, because the virus does not know the key.



Key Exchange

A common encrypcurrency technique is to encrypt each individual transaction with a separate key. This is called a session key, because it is used for only one particular communications session. Session keys are useful because they only exist for the duration of the communication.



A compression function. $(b = 512, \ell = 128$ *in MD5.).*

JACK'S LAW PRINCIPLE OF MATHEMATICS

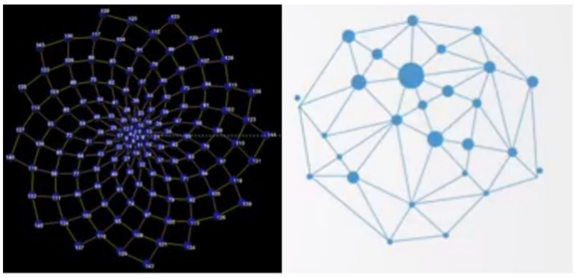
The Theory of Jack's Law – Definitions and Propositions

1. We define a new Jack's Law is a kind of cryptosystem using k -Fibonacci number. The invention of Jack's Law The Golden cryptosystem was introduced by Fibonacci but was proven to be exist in the series that the long integer exist in the series for use in public-key encryption with the RSA algorithm. We will show that this new cryptosystem, which is a modification of the golden cryptosystem, is secure against chosen plaintext attack. The pervasive appearance of phi throughout the series we name as Zeta Series is define by some to be the signature of encryption,K , a universal constant of design used to assure the infinite.

$$Z(\mathrm{n})\ \Xi\ K^{ab}$$

Jack's Law is the observation that the encryption or secret key is exist in every Fibonacci series that we name now as Zeta Series. *Jack's Law observed that the act of "part of the whole adding the whole onto itself" can be thought of as a "mathematical way of describing secret key recognition of being part of the quantum series." In application, this would suggest that "when any zeta series as part of the network in quantum, and stays firmly in that perspective, then it will also become into a harmonic relationship with the quantum network. As the golden ratio define become in Phi relationship with the nature in the quantum series it represents the secret key or private key as encryption to infinite. This could suggest as a new encryption series for long integers."*

2. The Jack's Law scheme encrypts the whole or parts of the data according to its owners' authorization by cryptography. Each node in the zeta series can also be use as a blockchain node that will be built on top of the zeta network. Owners of the data can also specify their own permissions encrypted by hashing data based on their own private key as a signature in the data by embedding the corresponding authentication codes into the encrypted data. Later, the receivers can extract the hidden authentication codes to judge whether the decrypted data is authentic. The design applied in Zetanet is to demonstrate the effectiveness of the proposed Jack's Law encryption scheme, and the conceptual framework for autonomous storage that can also be applied to other applications requiring information encryption especially in the new Internet 2.0 for blockchain.



ZETANET ENCRYP BLOCK BLOCKCHAIN

3. The number of network computing in a dense data doubles every two years. It also states that the connectivity, storage, speed and security will improve from the change of the protocol because of its algorithm and encryption. **Jack's *law*** *is the observation that the number of network computing in a dense of data doubles about every two years. The observation is named after the scientist of Skipjack Technology, who's in the Encrypcurrency paper described a doubling every year in the number of network connected per data network, and projected this rate of growth would continue for at least another decade. The period is often quoted as 18 months because of we predicted that network performance and efficiency protocols would double every 18 months (being a combination of the effect of more data and the network connectivity be more efficient and faster based on protocols and hardware improvement). This will be a problem solver of the increase of internet traffic that forecasts surge in IP traffic driven by number of factors, including growth of the Internet of Things*

In Jack's Law, the series of Fibonacci now define as

ZETA SERIES

where every **Zeta numbers** or **Zeta series** are **binary sequence** named after the mathematician Professor Dr Lord Jack Rahman who studied both that sequence and the closely related Fibonacci numbers. Zeta numbers and Fibonacci numbers form complementary instances of Zeta binary sequences.

The Zeta binary sequence has the same recursive relationship as the Fibonacci sequence, where each term is the sum of the two previous terms, but with different interpretation of k constant in the series. This produces a sequence where the ratios of successive terms approach the golden ratio, and in fact the terms themselves are roundings of integer powers of the golden ratio. The sequence also has a variety of relationships with the Fibonacci numbers, like the fact that adding any two Fibonacci numbers two terms apart in the Fibonacci sequence results in the Lucas number in between.

Similar to the Fibonacci numbers, each Zeta number is defined to be the sum of its two immediate previous terms, thereby forming a Fibonacci integer sequence .The first two Zeta numbers are $Z_0 = 00$ and $Z_1 = 01$ as opposed to the first two Fibonacci numbers $F_0 = 0$ and $F_1 = 1$. Though closely related in definition, Lucas and Fibonacci numbers exhibit distinct properties.

In mathematics and computing, **Zeta coding** is a universal code which encodes positive integers into binary code words. It is one example of representations of integers based on Fibonacci numbers. Each code word ends with "11" and contains no other instances of "11" before the end.

The Zeta code is closely related to the *Zeckendorf representation*, a positional numeral system that uses Zeckendorf's theorem and has the property that no number has a representation with consecutive 1s. The Fibonacci code word for a particular integer is exactly the integer's Zeckendorf representation with the order of its digits reversed and an additional "1" appended to the end.

The Zeta numbers may thus be defined as follows:

For a number N , if d (0),d(1),….., d(k-1), d(k) represent the digits of the code word representing N then we have:

$$N = \sum_{i=0}^{k} \mathrm{Z}_{r}$$

It is based on the Zeta sequence which now includes the initial 0.

The pattern in column one (the right-hand column) is derived from the rabbit sequence where *every "1" in the rabbit sequence has been replaced by "10"*:-

The zeta sequence:
010110101101101011010...
becomes:
0 1 0 1 1 0 1 0 1 1 0 1 1 0 1 0 1 1 0 1 0 ...
0 10 0 10 10 0 10 0 10 10 0 10 10 0 10 0 10 10 0 10 0 ...
which is **column 1** above, read downwards.
[N.B. This is exactly the same as if we flipped the bits (1 changes to 0 and 0 to 1) in the Zeta sequence (without its initial zero).However, there is a pattern in the other columns which is better seen with the description above.]

every "1" in the zeta sequence is replaced by "100" and every "0" is replaced by "00".

0 1 0 1 1 0 1 0 1 1 0 1 1 0 ... Zeta Sequence
00 100 00 100 100 00 100 00 100 100 00 100 100 00 ... Column 2

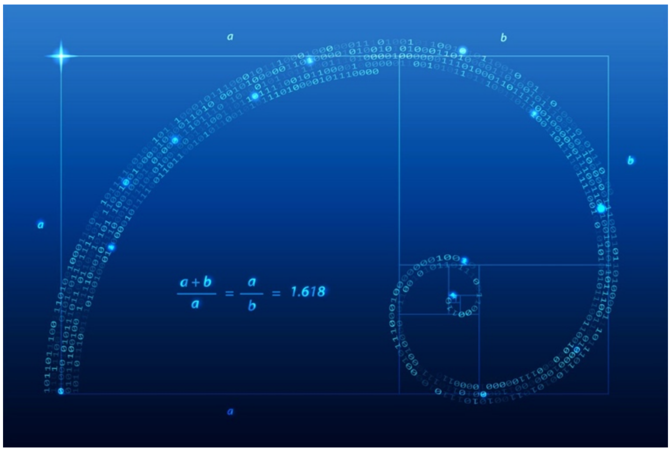
where column 2 in the Table of Fibonacci representations is read downwards.

For column 3, replace "0" by "000" and "1" by "11000"
For column 4, replace "0" by "00000" and "1" by "11100000"
For column 5, replace "0" by "00000000" and "1" by "1111100000000"

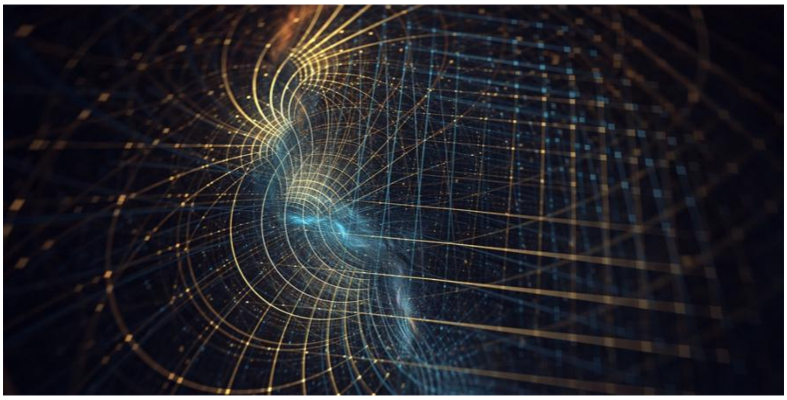
It can be shown that such a coding is unique, and the only occurrence of "11" in any code word is at the end i.e. $d(k-1)$ and $d(k)$. The penultimate bit is the most significant bit and the first bit is the least significant bit. Also leading zeros cannot be omitted as they can in e.g. decimal numbers.

The first few Fibonacci codes are shown below, and also the so-called implied probability distribution, the distribution of values for which Fibonacci coding gives a minimum-size code.

The sequence of Zeta numbers is:



All Fibonacci-like integer sequences appear in shifted form as a row of the wythoff array ; the Fibonacci sequence itself is the first row and the Zeta sequence is the first row. Also like all Fibonacci-like integer sequences, the ratio between two consecutive Lucas numbers converges to the golden ratio

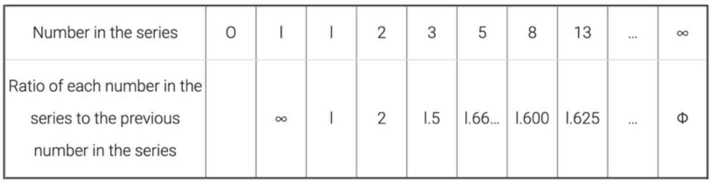


Meaning hidden in Phi, the symbol for the Golden Number?

The use of the Greek letter Phi to represent the golden number 1.618 … is generally said to acknowledge Phidias, a 5th century B.C. sculptor and mathematician of ancient Greece, who studied phi and created sculptures for the Parthenon and Olympus. Today we understand the universe to consist of positive and negative atomic and subatomic particles and charges, matter and anti-matter, all coming from a singularity in what we term the "Big Bang. "Curiously, the mathematical constant of 1.618 … that is found throughout creation is represented by the symbol Phi, which is the symbol 0 for nothing split in two by the symbol 1 for unity and one". In the Jack's Law the Phi is represent K constant number for encryption in the series.

Adding Unity to nothingness produces the Zeta series, which converges on Phi

In other words, add 0 plus 1 to get 1, and then follow this pattern to the Infinite. This is the Zeta series. The ratio of each number in the series to the one before it converges on Phi as you move towards infinity, ∞!

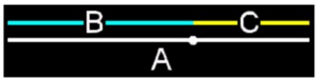


Number in the series	0	I	I	2	3	5	8	13	...	∞
Ratio of each number in the series to the previous number in the series		∞	I	2	I.5	I.66...	I.600	I.625	...	Φ

The Golden Proportion is analogous to encryption

The Golden Section, or Phi, or K constant found throughout nature, also applies in understanding the relationship to nature. In the golden section, we see that there is only one way to divide a line so that its parts are in proportion to, or in the image of, the whole:

The ratio of the larger section (B) to the whole line (A) is the same as the ratio as the smaller section (C) to the large section (B):



The K constant in Jack's Law Golden Section as a universal constant of design

The pervasive appearance of phi throughout the series is believed to be the encryption, a universal constant of design used to encrypt in the quantum network

Phi can be calculated in an iterative process, such as those shown in the equations below:

$$\Phi = 1 + (1/Xn), \text{e.g.,}$$

$$1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\ldots}}}}$$

or

$$\phi = \sqrt{1+\sqrt{1+\sqrt{1+\sqrt{1+\ldots}}}}$$

Jack's Law Key Exchange

Jack's Law observed that the act of "part of the whole adding the whole onto itself" can be thought of as a "mathematical way of describing secret key recognition of being part of the quantum series." In application, this would suggest that "when any zeta series as part of the network in quantum, and stays firmly in that perspective, then it will also become into a harmonic relationship with the quantum network. As the golden ratio define become in Phi relationship with the nature in the quantum series it represents the secret key or private key as encryption to infinite. This could suggest as a new encryption series for long integers."

The public-key encryption schemes that are mostly used today are RSA and ElGamal . Their security are based on the problems of factoring large composite integers or computing discrete logarithms. However, in [Sho97], Shor published an algorithm that quantum computers can use to solve both discrete logarithms and factoring in polynomial time. Therefore, it is important to construct new encryption schemes which are to remain secure even after the advent of quantum computers.

Given a Jack's prime $p = 2^n - 1$ (where n is prime), samples of the Zeta (Z) distribution are constructed as (a, b) , where $a \in_R Z_p$, the secret or private key and the error e are chosen uniformly at random from the elements in Z_p .The decisional version of the Zeta assumption states that no efficient adversary can distinguish the Z distribution from a uniform distribution over Z^2_p.

Figure: The K constant

Despite the efficiency benefit of its reliance on Z primes. The new encryption here is still in the development for the zetanet quantum encryption.

In this paper, we present new Jack's Law Key Exchange schemes for enhancing the information rate, this improvement is nonetheless significant in practice.

There exist groups for which computing discrete logarithms is apparently difficult. In some cases (e.g. large prime order subgroups of groups ($(\mathbf{Z}_p)^\times$) there is not only no efficient algorithm known for the worst case, but the average case complexity can be shown to be about as hard as the worst case using random self reducibility.

At the same time, the inverse problem of discrete exponentiation is not difficult (it can be computed efficiently using exponentiation by squaring ,for example). This asymmetry is analogous to the one between integer factorization and integer multiplication. Both asymmetries (and other possibly one way functions) have been exploited in the construction of cryptographic systems.

Popular choices for the group *G* in discrete logarithm cryptography (DLC) are the cyclic groups $(\mathbf{Z}_p)^\times$ .While there is no publicly known algorithm for solving the discrete logarithm problem in general, the first three steps of the number field sieve algorithm only depend on the group *G*, not on the specific elements of *G* whose finite log is desired. By precomputing these three steps for a specific group, one need only carry out the last step, which is much less computationally expensive than the first three, to obtain a specific logarithm in that group.

This is the concept of Jack's Law Key Exchange algorithm. It is based on mathematics on binary Jack Encryption works by having two parties agree on two prime numbers: G and P. Each party individually selects a secret number: a for one party, b for another. They then raise G to the power of their given number, multiply it times the modulus of P, and transmit that result.

When each party gets the result of their transaction, they raise that result to their selected secret number, multiply it against times the modulus of P, and suddenly now each is working with the same selected key thanks to the Laws of Exponents.

In zeta series to breaking KEA is hard. Even if know P and G, finding the keypair for a,b requires to calculate a discrete logarithm. Without a quantum computer, we don't know how to efficiently compute a discrete logarithm. We layer KEA in extra steps multiplication algorithm that authenticate each party and make sure that nobody is intercepting your traffic and shuttling traffic between you and your partner, it's basically uncrackable.

Multiplication algorithm

A **multiplication algorithm** is an algorithm (or method) to multiply two numbers. Depending on the size of the numbers, different algorithms are in use. Efficient multiplication algorithms have existed since the advent of the decimal system.The basic idea is to use fast polynomial multiplication to perform fast integer multiplication. The algorithm was made practical and theoretical guarantees were provided in 1971 by Schönhage and Strassen resulting in the Schönhage–Strassen algorithm. The details are the following: We choose the largest integer w that will not cause overflow during the process outlined below. Then we split the two numbers into m groups of w bits as follows:

$$a=\sum_{i=0}^{m-1} a_i 2^{wi} \text{ and } b=\sum_{j=0}^{m-1} b_j 2^{wj}.$$

We look at these numbers as polynomials in *x*, where $x = 2^w$, to get,

$$a=\sum_{i=0}^{m-1} a_i x^{i} \text{ and } b=\sum_{j=0}^{m-1} b_j x^{j}.$$

Then we can then say that,

$$ab=\sum_{i=0}^{m-1}\sum_{j=0}^{m-1} a_i b_j x^{(i+j)} = \sum_{k=0}^{2m-2} c_k x^k$$

Clearly the above setting is realized by polynomial multiplication, of two polynomials a and b. The crucial step now is to use Fast Fourier multiplication of polynomials to realize the multiplications above faster than in naive O(m2) time.To remain in the modular setting of Fourier transforms, we look for a ring with a 2mth root of unity. Hence we do multiplication modulo N (and thus in the Z/NZ ring). Further, N must be chosen so that there is no 'wrap around', essentially, no reductions modulo N occur. Thus, the choice of N is crucial. For example, it could be done as,

N = 2 3 w + 1 {\displaystyle N=2^{3w}+1} N=2^{3w}+1

The ring Z/NZ would thus have a 2mth root of unity, namely 8. Also, it can be checked that ck < N, and thus no wrap around will occur.

The algorithm has a time complexity of $\Theta(n \log(n) \log(\log(n)))$ and is used in practice for numbers with more than 10,000 to 40,000 decimal digits. To give a time complexity of $n \log(n)\ 2^{\Theta(\log^*(n))}$ using Fourier transforms over complex numbers. a similar algorithm using modular arithmetic achieving the same running time. In context of the above material, what these latter authors have achieved is to find N much less than $2^{3k} + 1$, so that Z/NZ has a $2m^{th}$ root of unity. This speeds up computation and reduces the time complexity.

Using number theoretic transforms instead of discrete Fourier transforms avoids rounding error problems by using modular arithmetic instead of floating point arithmetic. In order to apply the factoring which enables the FFT to work, the length of the transform must be factorable to small primes and must be a factor of N-1, where N is the field size.

Large Integer Arithmetic

An integer in C is typically 32 bits, of which 31 can be used for positive integer arithmetic. This is good for representing numbers up to about two billion (2 times 10^9).

Some compilers, such as GCC, offer a "long long" type, giving 64 bits capable of representing about 9 quintillion (9 times 10^{18})

This is good for most purposes, but some applications require many more digits than this. For example, public-key encryption with the RSA algorithm typically requires 300 digit numbers. Computing the probabilities of certain real events often involves very large numbers; although the result might fit in a typical C type, the intermediate computations require very large numbers.

- It turns out that, using a divide and conquer algorithm, one can obtain an algorithm that works in time Θ (Nlg 3) = O(N1.59), much better than the quadratic time above. However, this technique only becomes efficient for very large values of N. There is another technique using the Fast Fourier Transform that multiples numbers in O(N log N log log N) time, which is even better, but still only becomes efficient for large values of N(e.g. > 10,000 decimal digits).
- A practical way to get more out of this algorithm is to increase BASE; this way, the same number of bits can be represented with less storage (i.e., lower value of N). The reason for choosing 10, other than the fact that it makes doing examples easy, is that it makes printing the numbers out a matter of traversing the array; other bases require complex conversions of bases. If we keep BASE as a power of 10 (e.g. 10,000), we can still easily print the numbers (fixing up leading zeros when we find them), and still improve performance.
- If we let BASE=2, then we are doing binary arithmetic. Multiplying by a single digit then becomes trivial: the partial product of n * A[0..N-1] is either all zeros (if the n=0) or A[0..N-1] itself (if n=1). This fact is not lost on computer architects, who implement multiplication algorithms in binary all the time :-)
- These are some simple arithmetic algorithms. There are other algorithms for integer division, subtraction (requiring a representation of negative numbers), exponentiation, modulus, etc. that are somewhat more complex but are basically the same idea. When we look at RSA encryption, we will assume a full implementation of large number arithmetic, being careful to take into account the various asymptotic complexities.
- If you would like to play with very large numbers, the Unix command bc implements "arbitrary" precision arithmetic; type bc at the command prompt and then type something ridiculously large like 2^1000 (2 to the 1000 power). The result will quickly come back.

I. ZETANET CONCEPT AND ARCHITECTURE

The Internet has the potential to greatly boost the convenience in our daily lives, but also increased the risk on privacy violation or secret leakage by hashing and rehashing the data and creating a hashed data based on the header. Data will be addressed and accessed by its name and there will be no need for IP. For example, the interconnect cameras in a smart home can improve context-awareness and remote monitoring but at the risk of privacy violation. In this regard, secret communication has become an important issue in recent years, particularly for the upcoming era of IoTs (the Internet of Things). Among all possible exchanging information, image related data is more privacy sensitive, and that is why steganography is widely used to hide a secret into cover multimedia, such as images, audios, videos, etc. To protect the secret, encryption is another general way to help the owners encrypt a secret into meaningless noises and only the person who owns the private key can decrypt the data. Information encryption was widely used in ensuring the quality of services in wireless communication as well. The resolution of a video service can be determined by how much a user is willing to pay . Also, the access control of resolution on a video can be used to prevent from plagiarism. However, the prior encryption schemes cannot be easily applied on some embedded devices because they needs powerful computation ability. In this regard, Jack's Law based encryption schemes for image encryption were proposed in concept of Zetanet design

In a social network, the owner of an image or data may need to share different parts of then image or data with different receivers. This is, the owner need to have the ability to authorize different receivers to access different contents on the same image, thus leading to so-called fine-grained access control. Fine- grained access control schemes are widely in current business models, such as publishing , authoring, E-services,etc. However, the prior image encryption schemes focused more on how to encrypt a whole image, but did not support partial authorization.

A fine-grained encryption scheme is required in some domains, such as e-Papers, e-Books, collaborative design, and so on. More specifically, the policy of authorizing an image for children and adults should be different. Those images related to violence or pornography should be encrypted for children. People have no rights to see the contents without legitimate copyrights. Thus, a fine-grained access control scheme is desirable for image encryption, and it allows owners to encrypt different parts of an image according different authorizations. The fine-grained encryption scheme proposed by was achieved by modeling the sensitive regions using a tree structure. Next, the tree structure was transformed into a serial bit of compression codes. The compression codes in turn were hidden into the digital images and then shuffled the sensitive regions into noise pads. They protects the sensitive regions; however, the image needs to keep a huge amount of compression codes for identifying whereabouts of the sensitive regions.

To authenticate whether the received encrypted image was a fake one, new image authentication schemes were proposed. Note that the challenge of such authentication schemes is that the encrypted contents are changed after embedding authentication codes; thus, they may fail in an attempt to decrypt the contents. Therefore, these schemes require a reversible embedding or hiding technique to guarantee that the encrypted contents can be completely decrypted. However, the hiding capacity of the reversible hiding schemes is still limited and often with the underflow or overflow problems in the current studies. To resolve this problem, we proposed a multilayer and fine-grained image encryption scheme with the authentication ability to ensure the authenticity of a received image. The scheme adopts the method from Lin et al. to design a reversible embedding approach for image encryption without suffering from the underflow or overflow problems. Also, the hiding capacity of Lin et al.'s scheme is greater than others. In addition, the fine- grained image encryption scheme is provided to allow the owners to encrypt any partial contents of an image in accordance with to their concerns in access control.

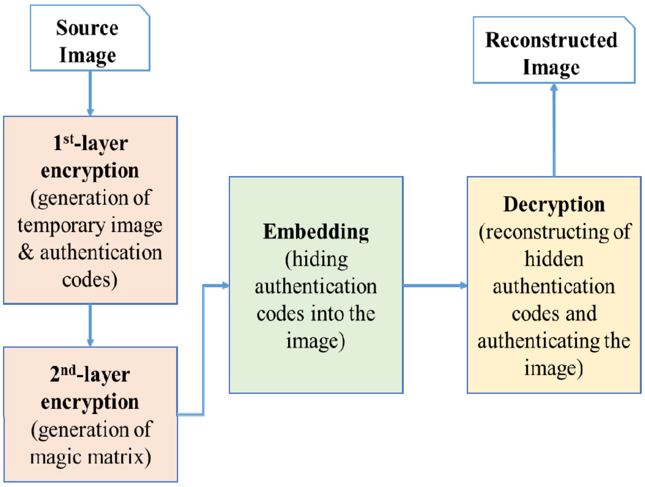

Source Image
1st-layer encryption (generation of temporary image & authentication codes)
2nd-layer encryption (generation of magic matrix)
Embedding (hiding authentication codes into the image)
Decryption (reconstructing of hidden authentication codes and authenticating the image)
Reconstructed Image

Fig. 1. The flowchart

THE STEGANOGRAPHY SCHEME

Lin et al. proposed a steganography scheme based on the concept of Sudoku. First, the secret bitstream s is transformed into a secret sequence of digits ss by using a 3^n-base notational system, and denoted as a pixel unit $x = (\beta_1, \beta_2, ..., \beta_n)_{3n}$.

Next, each digit of x is hidden into the cover image by a pixel pair using an extracting function f, which is defined as:

$$f(\lambda_1, \lambda_2, ..., \lambda_n) = \sum_{i=1}^{n} 3^{i-1} \lambda_i \mod 3^n. \qquad (1)$$

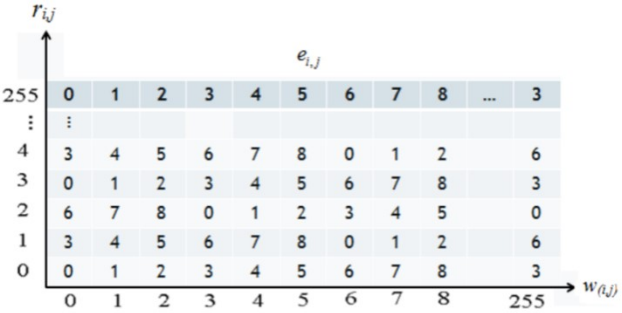
Here, n pixels be a group as input data depicted as

$(\lambda_1, \lambda_2, ..., \lambda_n)$ in Equation (1). Suppose that a digit r, obtained by x, is to embed into the cover image. A temporary value y is generated with equation (2).

$$y = (r - f(\lambda_1, \lambda_2, ..., \lambda_n) + \left\lfloor \frac{3^n - 1}{2} \right\rfloor) \mod 3^n. \qquad (2)$$

Next, the value of y is transformed into a sequence yy by using a 3^n-base notational system as $yy = s_1 s_2 ... s_n$, where $s_i \in [0, 1, ..., n-1]$ and $1 \leq i \leq n$. Subsequently, the sequence of each digit in yy is changed and subtracted by 1 to generate a new sequence as $z = e_n e_{n-1} ... e_1$, where $e_j \in [-1, 0, ..., n-2]$, $e_j = s_i - 1$, and $j = n-i+1$. Finally, each digit in x is added to a corresponding digit in z with equation (3) to create a new pixel unit $w = (p_1, p_2, ..., p_n)$.

$$p_i = \lambda_i + e_i, \text{ where } i = 1 \text{ to } n. \qquad (3)$$



255	0	1	2	3	4	5	6	7	8	...	3
⋮	⋮										
4	3	4	5	6	7	8	0	1	2		6
3	0	1	2	3	4	5	6	7	8		3
2	6	7	8	0	1	2	3	4	5		0
1	3	4	5	6	7	8	0	1	2		6
0	0	1	2	3	4	5	6	7	8		3
	0	1	2	3	4	5	6	7	8		255

Fig. 2. Example of magic matrix

When a receiver receives the $(p_1, p_2, ..., p_n)$, the decoder can extract the hidden secrets *ss* with equation (1), which replaces （$\lambda_1, \lambda_2, ..., \lambda_n$） with $(p_1, p_2, ..., p_n)$. The secret *s* can be recovered by transforming *ss* with the 2-base notational system.

I. PROPOSED SCHEME

There are totally three procedures including encryption, embedding, and decryption, where a multilayered encryption method is proposed, and the first version has two layers, as illustrated in Fig. 1.

In the first layer of the encryption procedure, a secret image *S* is divided into several blocks with *w*×*w* pixels. Note that the *q*-th block is denoted as B_q, and (i, j) refers to the position of a pixel in B_q and its pixel value is denoted as $p_{i,j}$. A mask is used to indicate whether pixels $p_{i,j}$ in B_q is authorized. If authorized, $m_{i,j}$ equals to 1; otherwise, 0. The temporary image is generated with equation (4), where *rnd_seed* is a random integer ranging from 0 to 255, and is the XOR (Exclusive- OR) operation. This is used to make the un-authorized regions as random pads, which are meaningless to users; otherwise, keep intact. After that, the pixels after first encryption phase, the pixel located at (*i*,*j*)-position is denoted as $t_{i,j}$.

$$t_{i,j} = \begin{cases} p_{i,j}, & \text{if } m_{i,j} = 1, \\ rnd\_seed \oplus p_{i,j}, & \text{otherwise.} \end{cases} \quad (4)$$

Next, the 2LSB (Least Significant Bit) of $t_{i,j}$ are replaced with 00, denoted as S'. The image S' is hashed to generate authentication codes *A*. Later, receivers can extract the hidden authentication codes to authenticate whether the image is not a fake.

Generally, the MSBs (Most Significant Bits) are the most important bits for a pixel. That is, if the MSB is changed, the original content cannot easily be recognized. On the contrast, the LSB is not important and if it is changed, the content still can be recognized. Thus, in the second layer of the encryption procedure, pixels $t_{i,j}$ are transformed into a binary stream and only the 3MSBs are used to encrypt. Note that the one who owns the secret key can decrypt the second layered encryption. For example, if the pixel value, denoted as $s_{i,j}$, is 201, the corresponding 3MSBs are 110. The 3MSBs are transformed into a decimal digit and denoted as $w_{i,j}$. In this example, $w_{i,j}$ is 6. The random number $r_{i,j}$ is generated and its interval is [0, 255]. A magic matrix is calculated with equation (1).

In Fig. 2, we can use $r_{i,j}$ and $w_{i,j}$ to obtain $e_{i,j}$ with the magic matrix. If $e_{i,j}$ equals 8, it requires four MSBs; however, three MSBs are enough for this case. Thus, we can adjust $e_{i,j}$ value with equation (5). If $e_{i,j}$ equals 8, let $w_{i,j}$ be 8; then, use $r_{i,j}$ and $w_{i,j}$ to obtain $e_{i,j}$ with the magic matrix again to complete the encryption procedure. For example, if $w_{i,j}$ and $r_{i,j}$ are 5 and 1, respectively, the mapping $e_{i,j}$ is equal to 8. Thus, let $w_{i,j}$ equal 8. The new $e_{i,j}$ (equals to 2) is obtained by mapping $w_{i,j}$ and $r_{i,j}$ (8 and 1, respectively) to magic matrix.

$$\begin{cases} \text{intact}, & \text{if } e_{i,j} \neq 8, \\ w_{i,j} = e_{i,j}, & \text{if } e_{i,j} = 8. \end{cases} \quad (5)$$

To avoid the authentication codes are easily extracted, encrypted results are used to shuffle the authentication codes as shown in equation (6), where every two bits of the authentication codes *A* are treated as a bit pair, denoted as $h_{i,j}$ and use equation (6) to calculate L_S value. Next, L_S is transformed into a two binary bits B_S. In the embedding procedure, the 2LSBs of the original pixel value are replaced with B_S.

$$L_s = (e_{i,j} + h_{i,j}) \bmod 4. \tag{6}$$

In the decryption procedure, the 2LSBs and 3MSBs are extracted and denoted as B'_S and $e'_{i,j}$, and the secret key is used to generate the $r'_{i,j}$. Later on, the mapping value, de- picted as $w'_{i,j}$, can be extracted with the magic matrix according to $e'_{i,j}$ and $r'_{i,j}$ to reconstruct the secret image. Note that if $w'_{i,j}$ equals 8, we replace the value of $e_{i,j}$ with 8 to extract $w'_{i,j}$

$w'_{i,j}$ is then mapped as 8. Again, let $e'_{i,j}$ and $r'_{i,j}$ equal 8 and 1;

$w'_{i,j}$ is identical to 5.

The hidden authentication codes $h_{i,j}$ are obtained by equation (6), where L_S and $e_{i,j}$ are the decimal value of B'_S and $e'_{i,j}$, respectively. The next step is concatenating all $h_{i,j}$ to reconstruct the authentication codes A' .

The 2LSBs of the reconstructed image are substituted with 00 to create a new image W. The A hash codes A $\sim$ are obtained by hashing W. Compare A' with A to check whether it is authentic. If A' equals to A , it is judged as authentic; otherwise, inauthentic.

Zetanet for Autonomous Data (Mathematics Derivation)

I. INTRODUCTION

Security is a most important issue in communication and encryption is one of the ways to ensure security of the communicated message. Encoding is the transformation of data into some unreadable form. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it is not intended. Decoding is the reverse of encoding; it is the transformation of encrypted data back into some intelligible form. Cryptography is popularly known as the study of encoding and decoding private massages. In cryptography, encryption processes are used in transforming information using an algorithm to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted information. The reverse process is referred to as decryption .

Steganography, which literally means “covered writing", Steganography is the more conservative technology to hide any secret information within an image. Cryptography and steganography are well known and widely used techniques that manipulate information (messages) in order to cipher or hide their existence. These techniques have many applications in their Computer science and other related fields: they are used to protect e-mail messages, credit card information and etc. Cryptography and steganography are well known and widely used techniques that manipulate information (messages) in order to cipher or hide their existence. These techniques have many applications in their Computer science and other related fields: they are used to protect e-mail messages, credit card information and etc. The proposed solution is to use image cryptography for disguising encrypted or normal textual information. This is a hybrid technique that inherits features from steganography and cryptography. Data hiding is a method used for hide information within computer code. By hiding the data, it's much harder to crack the code, because the data will appear invisible to the objects and the hacker.

A. Image Processing

It generally refers to processing of a two-dimensional picture by a digital computer. A digital image is a representation of a two-dimensional image as a finite set of digital values, called picture elements or pixels. Pixel values typically represent gray levels, colours, heights, opacities etc. Then the image processing focuses on two major tasks

- Improvement of pictorial information for human interpretation
- Processing of image data for storage, transmission and representation for autonomous machine perception. Where image processing ends and fields such as image analysis and computer vision start. Our proposed method is one of the techniques used to encrypt the images by dividing the original image into transparencies. The transparencies can be sent to the intended person, and at the other end the transparencies received person can decrypt the transparencies using our decryption method and key image, thus gets the original message.

B. Image Stenography

Steganography is the art and science of invisible communication. This is the hiding information in other information, thus hiding the existence of the communicated information. Steganography is derived from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing” defining it as “covered writing”. In image steganography the information is hidden exclusively in images.Extremely difficult to detect, a normal cover message was sent over an insecure channel with one of the periods on the paper containing hidden information.

To ensure the security of the important message in communication, by the data hiding with image cryptography. We proposed a novel technique that encrypted the message such a ways that the message encoded as well as hidden in an image. The proposed solution is to use image cryptography to hide textual message. The proposed technique use of an encryption technique that is based on Fibonacci series & image encryption and a secret key generated from the image.

II. RELATED WORK

A. Visual Cryptography

Visual Cryptography is a secret sharing scheme which uses the human visual system to perform computations. The basic principle behind visual cryptography is the use of superimposed images to reveal the secret. Each individual image can be considered as a cipher, and the corresponding image may be regarded as a key. It can also be interpreted as a graphical form of one time pad. Xiao *et al.* (2000) present a novel way to hide information with the aid of visual cryptography. They concealed a secret message using two innocent looking images .Once the two images were superimposed the secret text was revealed. They used a hybrid technique, which is a combination of visual cryptography and steganography to hide information. But Xiao *et al.* (2000) did not offer a disguising component to conceal the use of cryptography.

B. Image Cryptography

Image cryptography hasn't been widely studied as normal cryptography or visual cryptography. It was used by Zenon *et al.* (1997), to encode digital media (images and video) to provide confidentiality and intellectual property protection against unauthorized access. They proposed a version of digital image cryptography by using random phase mask for encrypting image. Here the authors consider image encoding as a new form of image encryption .They accomplish this using a transformation technique based on random phase masks. Their technique of encryption consists of four major steps. Fourier transform of initial image, phase modification, inverse Fourier transform and finally image conversion. Zenon *et al.* (1997) used image cryptography and steganography to increase security, but they have not considered the use of image cryptography to disguise text cryptography, which would provide enhanced privacy and confidentiality in cryptographic communication.

C. Image Steganography

Image steganography has been widely studied by researchers. There are a variety of methods used in which information can be hidden in images. Some of them are described here .

- Replacing least significant bit: In image steganography almost all data hiding techniques try to alter insignificant information in the cover image. For instance, a simple scheme proposed by Chen, is to place the embedding data at the least significant bit(LSB)of each pixel in the cover image [Lee et al. 2000]. The altered image is called stego-image. Altering LSB doesn't change the quality of image to human perception but this scheme is sensitive a variety of image processing attacks like compression, cropping etc.

- Replacing moderate significant bit: Chan and Chang showed how to use the moderate significant bits of each pixel in the cover image to embed the secret message. This method improves sensitivity to modification, but it degrades the quality of stego-image.

- Transformation domain techniques: Other familiar data hiding techniques use the transformation domain of digital media to hide information [Chang et al. 2002, and Hsu et al. 1999]. Functions suchas the Discrete Cosine transform (DCT) and the discrete wavelet transform (DWT) are widely applied [Fabien et al. 1999, Chang et al. 2002, and Hsu et al. 1999]. These methods hide the messages in the significant areas of the cover image which makes them robust against compression, cropping and other image processing attacks.

III. METHODOLOGY

A. Read Image and Text

First, user given a secret message and choice a covered image.

```
>> user_entry = input('Enter a String?:', 's');
```

The response to the input prompt can be any MATLAB expression, which is evaluated using the variables in the current workspace.

user_entry = input('prompt') displays prompt as a prompt on the screen, waits for input from the keyboard, and returns the value entered in user_entry.

user_entry = input('prompt', 's') returns the entered string as a text variable rather than as a variable name or numerical value.

```
>> A = imread('circuit.tif');
```

A = imread(filename, fmt) reads a grayscale or color image from the file specified by the string filename. If the file is not in the current directory, or in a directory on the MATLAB path, specify the full path name.The text string fmt specifies the format of the file by its standard file extension.

Encryption Process

ASCII Convert: a=double(r);

B. Zeta Series Generate

In mathematics based on Jack's Law , the Zeta Series numbers or Zeta Series sequence are the numbers in the following integers sequence

$$0,\ 1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ 34,\ 55,\ 89,\ 144,\ \ldots$$

By definition, the first two numbers in the Zeta Series sequence are 0 and 1, and each subsequent number is the sum of the previous two. In mathematical terms, the sequence Zn of Zeta Series numbers is defined by the recurrence relation

$$Z_n = Z_{n-1} + Z_{n-2} \qquad (1)$$

With seed values

$$Z_0 = 0, \qquad Z_1 = 1 \qquad (2)$$

C. Random Number Matrix

out = randint(n,n,[1,100]);

out = randint generates a random scalar that is either 0 or 1,
with equal probability.
out = randint(m) generates an m-by-m binary matrix, each of whose entries independently takes the value 0 with probability 1/2.
out = randint(m,n) generates an m-by-n binary matrix, each of whose entries independently takes the value 0 with probability 1/2.
out = randint(m,n,rg) generates an m-by-n integer matrix. If rg is zero, out is a zero matrix. Otherwise, the entries are uniformly distributed and independently chosen from the range

- [0, rg-1] if rg is a positive integer
- [rg+1, 0] if rg is a negative integer
- Between min and max, inclusive, if rg = [min,max] or[max,min]

D. Key and Encrypted Image

Key:
y = imcrop(x,[0 0 n n]);
Retrieving the coordinates of the crop rectangle.
Imcrop copies a four element position vector ([xminyminwidth height]) to the clipboard. imwrite(y,'d:\b.tif');
imwrite(A,filename,fmt) writes the image A to the filespecified by filename in the format specified by fmt.

Encrypted image:
imwrite(r1,'d:\a.tif');
imwrite(A,filename,fmt) writes the image A to the file specified by filename in the format specified by fmt.

Read Key and Encrypted image

x2 = double(imread('d:\a.tif')); x1 = double(imread('d:\b.tif'));

double(x) returns the double-precision value for X. If X is already a double-precision array, double has no effect. imread(filename, fmt) reads a grayscale or color

E. Decryption Process

Result = Encrypted image – Key image Read the Diagonal value of Result
Retrieve the left to right diagonal values of Z matrix If i == j

M(i) = Z(i,j)

F. Zeta Series Generate

In mathematics based on Jack's Law , the Zeta Series numbers or Zeta Series sequence are the numbers in the following integers sequence

$$0,\ 1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ 34,\ 55,\ 89,\ 144,\ \ldots$$

By definition, the first two numbers in the Zeta Series sequence are 0 and 1, and each subsequent number is the sum of the previous two. In mathematical terms, the sequence Zn of Zeta Series numbers is defined by the recurrence relation

$$Z_n = Z_{n-1} + Z_{n-2} \qquad (3)$$

With seed values

$Z_0 = 0$, $Z_1 = 1$ (4)

Image from the file specified by the string filename. If the file is not in the current directory, or in a directory on the MATLAB path, specify the full pathname.

A. Convert ASCII to string:

char(X);

char(X) can be used to convert an array that contains positive integers representing numeric codes into a MATLAB character array.

FLOW OF WORK

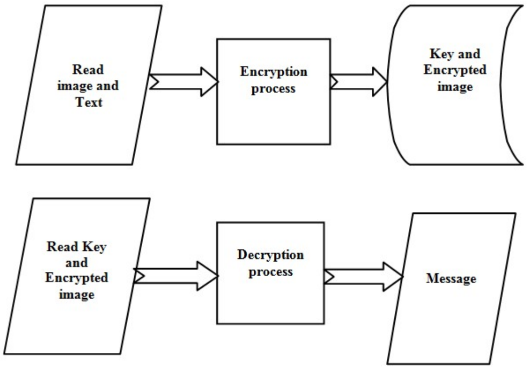


Figure 1: Diagram of flow of work

ALGORITHM

A. Encryption

1. START
2. M →Read a text message from user.
3. C →Convert Message to ASCII code using double function in Matlab
4. N →Calculate the length of the message
5. F →Generate the Fibonacci series up to N
6. T→Transpose the F matrix
7. S →Addition of C and T matrix
8. R →Generate Random number 1 to 100 by randint( ) and store it N X N matrix
9. Generate a (N x N) matrix

```
If i==j
A(i,j) →S(i)
Else
A(i,j) →R(i,j)
```

10. X →Read a Image by imread function
11. Y →Crop the image by imcrop(X,[0 0 N N])
12. G →Change the data type of Y to double by double()
13. Write the matrix G as image format in the memory by imwrite()
14. E →Adding two Matrix of A and G
15. Write the matrix E as image format in the memory by imwrite()
16. STOP

B. Decryption

1. START
2. D →Read The Encrypted image from memory

```
3.    B →Read the Key image from memory
4.    Z →Subtraction of D and B matrix
5.    N1 →Calculate the length of Z
6.    M →Retrieve the left to right diagonal values of  Z matrix

       If i==j
       M(i) →Z(i,j)
7.    M1 →Transpose the M matrix
8.    E →Generate the Fibonacci series up to N1
9.    E1→Transpose the E matrix
10.   P →Subtraction of M1 and E1
11.   Result →Convert ASCII to String and show the  message.
12.   STOP
```

CONCLUSION

In this paper we proposed a novel technique that encrypted the message such a ways that the message encoded as well as hidden in an image. The proposed solution is to use image cryptography to hide textual message. The proposed technique use of an encryption technique that is based on Fibonacci series & image encryption and a secret key generated from the image. From these mathematical concept, Skipjack will create and develop zetanet.

Jack's Law K constant - An Efficient Golden Ratio Method for Secure Cryptographic Applications

Abstract: With the increase in the use of electronic transactions in everyday life, secure communications and data storage to withstand any kind of attack is warranted. The golden ratio, being the most irrational among irrational numbers, can be used in elliptic curve cryptosystems, power analysis security, and other applications. However, in such applications, cryptographic operations should take place very quickly before the keys are extracted or decoded by the attackers. This paper proposes an efficient method of golden ratio computation in cryptography to resist information security breaches. We compare our new golden ratio method with the well-known Fibonacci sequence method. The experimental results show that our proposed method is more efficient than the Fibonacci sequence method. Our golden ratio method with infinite precision provides reliable counter measure strategy to address the escalating security attacks.

Introduction

With technological advancements, electronic communications have evolved to be in various forms and media. Since the early theories of digital communication and secrecy, there have been rapid advancements in information communication technologies . However, security threats have also increased rapidly, affecting businesses and individuals worldwide . Hence, secured communication with appropriate cryptographic techniques plays a key role in this networked society. Cryptography, the art and science of secret writing, is being used by many security systems to securely communicate information over the Internet. It uses patterns and algorithms to encrypt all forms of communication messages, including text, images, and signals. Encryption is a process of applying cryptography to encode a message or information in such a way that it becomes unreadable to unauthorized users. In encryption, the original message or plaintext for communication is encoded using an encryption algorithm (cipher) to generate a ciphertext that can only be read if decrypted . The encryption algorithm generates a pseudo-random encryption key or secret key, which is used to decrypt the ciphertext for the authorized access of the message. Organizations use cryptography for secure data transmission and storage. Typically, a cryptosystem consists of a set of cryptographic techniques for key generation, encryption, and decryption of the information to preserve its confidentiality, privacy and integrity .

Many cryptographic techniques are adopted by various businesses and governments to communicate sensitive information to their stakeholders over the Internet. However, cyber-attacks are still on the rise. Hence, many advanced encryption algorithms have emerged to help uphold the security of communication. The size and randomness of the secret key plays a role in addressing security attacks. The golden ratio, defined as the ratio of the hypotenuse of an isosceles triangle to its base, has interesting properties. A golden rectangle with a longer side a and shorter side b, when placed adjacent to a square with sides of length a, will produce a similar golden rectangle with longer side $a + b$ and shorter side a. While researchers have been deriving connections between the golden ratio, resulting in many applications in physics, including Lorentz transformation recently , the motivation of our work lies in its application to cryptography. Calculating a precise golden ratio with a higher decimal place of accuracy is of interest in generating more secure keys . There is a need for an innovative and efficient method to look beyond the popular Fibonacci method. The aim of this paper is to propose a golden ratio method which is more efficient than the Fibonacci method to develop a faster cryptosystem. By enhancing the cryptographic techniques, this work plays an important role in arriving at a security solution that forms an improved counter measure for cyber-attacks, which are on the rise.

We organize the remainder of the paper as follows. We gives a literature review of related work. We provide a background theory about the golden ratio and its various properties. We derive the key mathematical relationships of the golden ratio with right-angled triangles and a Fibonacci sequence. These relationships aid in proposing a new faster method for golden ratio computation The experimental results of our proposed method as compared to the commonly used Fibonacci method are summarized. Finally, conclusions and future work are given.

Literature Review

The most popular commercial application of the golden ratio is in RSA cryptography, where primes of about 150 digits are required .Even though there are many prime number generation algorithms, data breaches and security attacks are still escalating, since attackers are using advanced technologies to decipher these algorithms. In another security context, an interesting example is power analysis, where the attacker uses the patterns of power consumption of a cryptographic hardware device for gaining secret information .In other words, devices such as a smart card, integrated circuit chips, microprocessors, or other hardware can be non-invasively attacked by extracting cryptographic keys and other secret information from the device. While simple power analysis (SPA) involves visual interpretation of power signals over a period of time, differential power analysis (DPA) is a more advanced power analysis, where the intermediate values between any two cryptographic operations are statistically analyzed. The attackers study and perform pattern analysis of power signals whenever operations using secret keys are performed that vary the power consumption of such devices.

The most common methods of encryption use Fibonacci numbers generated to convert the plaintext into ciphertext. Stakhov introduces the concept of the golden matrix and its application in cryptography .However, subsequent studies proved that this method in cryptosystems was insecure against certain plaintext attacks .In another set of research work, we found that cryptosystems using golden ratio methods were gaining importance by modifying the golden cryptosystem using a k-Fibonacci number .While some new proposals of cryptosystem based on k-Fibonacci numbers are shown to be more secure than the original golden cryptography against a plaintext attack, there are still many cyber-attacks taking place .

We argue that a method based on the golden ratio can be used to achieve secure cryptography based on the work by De Castro with respect to realizing it as one-way function .This can be further strengthened by other research work which has provided similar mathematical representations. According to Levin , one-way functions are the most important problems in computer theory, and his work provides a unified approach to define this problem including its computational complexity. It is well known that the golden ratio is the most irrational of the irrational numbers. The irrational property of the golden ratio is consistent with Levin's one-way functions, and hence is the most difficult to resolve when used through a one-way function. By introducing an efficient method to calculate the golden ratio, the cycle time would be hastened so that intruders will not have sufficient time to probe or penetrate between two operations with the secret key. Hence, in this work, we explore the mathematical properties of the golden ratio to arrive at a much faster and efficient method for its computation. We compare our method in terms of its efficiency and precision with the popular Fibonacci method.

Theory and New Derivations of the Golden Ratio and its Properties

In this section, we define and summarize the theory behind the golden ratio and derive certain key relationships it has with right-angled triangles and the Fibonacci sequence. The relationships we establish here would be used in proposing our new method of golden ratio computation in the next section.

Definition of the Golden Ratio

The first mathematical definition of the golden ratio traces back to the famous Greek mathematician Euclid who, in the third century B.C., introduced it to solve a geometrical problem called the problem of division of a line segment in an extreme and mean ratio . The essence of the problem is the following:

A line segment AB must be divided with a point C into two parts so that the ratio between the longer part CB and the shorter one AC is equal to the ratio between the whole line segment AB and the longer part CB, i.e.;

$$\frac{AB}{CB} = \frac{CB}{AC}$$

Let us consider a rectangle with dimensions as shown in Figure 1. Then, we can express the golden ratio based on its definition as follows:

$$\varphi = \frac{1}{\varphi - 1} \qquad (1)$$

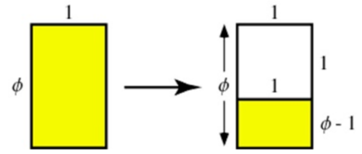


Figure 1. Pictorial representation of the golden ratio.

We determine the value of the golden ratio by undergoing various mathematical transformations as given below. Performing a multiplication operation on both sides of Equation (1) with $(\phi-1)$, we get:

$$\phi(\phi-1)=\frac{\phi-1}{\phi-1}=1$$

$$\phi^2-\phi-1=0$$

Completing the square we get

$$(\varphi-1)^2=\varphi^2-\varphi+\frac{1}{4}\Rightarrow-\frac{5}{4}\Rightarrow-1$$

$$(\varphi-\frac{1}{2})^2-\frac{5}{4}=0$$

$$(\varphi-\frac{1}{2})^2-\left(\frac{\sqrt{5}}{2}\right)^2=0$$

$$(\varphi-\frac{1}{2}-\frac{\sqrt{5}}{2})(\varphi-\frac{1}{2}+\frac{\sqrt{5}}{2})=0$$

$$(\varphi-\frac{1+\sqrt{5}}{2})(\varphi-\frac{1-\sqrt{5}}{2})=0$$

$$\varphi=\frac{1+\sqrt{5}}{2},\frac{1-\sqrt{5}}{2} \qquad (2)$$

In order to arrive at a fast method to calculate the golden ratio, we consider the various properties of the golden ratio in the next sections. We derive mathematical relationships between these properties to propose a new efficient method for golden ratio computations. Such an efficient method is desired since the order of computational complexity plays a major role in cryptosystems . The method and results of this paper advance previous work on the methods used for estimating the golden ratio and silver ratio .

The Golden Ratio and Right-Angled Triangles

We establish the first property of the golden ratio, where it can be expressed as the ratio of the sides of a right-angled triangle (Figure 2), as follows:

$$\varphi=\frac{a+c}{b}=\frac{1+\sqrt{5}}{2} \qquad (3)$$

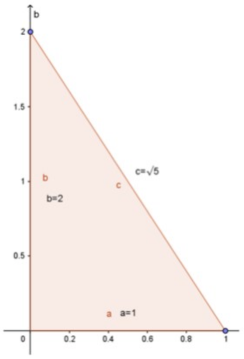


Figure 2. Right-angled triangle representation of the golden ratio.

The sides of a right-angled triangle can be expressed in terms of a, as shown below:

$$b=2a,\ c=\sqrt{a^2+b^2}=\sqrt{a^2+4a^2}=\sqrt{5a^2}=a\sqrt{5}$$

$$\varphi=\frac{1+\sqrt{5}}{2},\frac{1-\sqrt{5}}{2} \qquad (4)$$

Consider the following four propositions as shown in Figure 3:

(1)

$c^2 = a^2 + (2a-1)^2 = 5a^2 - 4a + 1$ (2) c^2
$= a^2 + (2a+1)^2 = 5a^2 + 4a + 1$ (3) $c^2 =$
$(a+1)^2 + (2a)^2 = 5a^2 + 2a + 1$ (4) $c^2 =$
$(a-1)^2 + (2a)^2 = 5a^2 - 2a + 1$

We observe that proposition (2) given above increases more rapidly than that of the other three propositions because of the $+4a$ term.

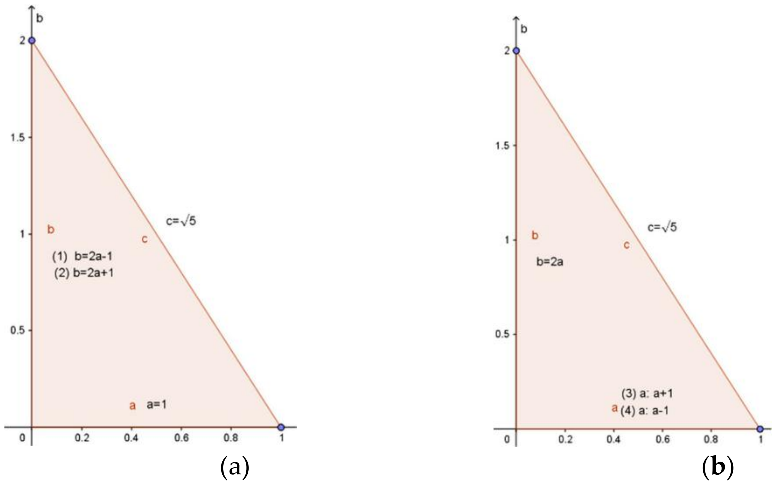


Figure 3. The triangle forms of the golden ratio: (**a**) $b = 2a - 1$; (**b**) $b = 2a$.

Let us now express the sides of the triangle as :

$$a = a,\ b = \lim_{a\to\infty} 2a + 1 = 2a,$$
$$c = \lim_{a\to\infty} \sqrt{5a^2 + 4a + 1} = a\sqrt{5}$$

From previous work it can be shown that the sides (a, b, c) can be expressed as three Diophantine equations (an equation that allows only integer solutions) in terms of (m, n) :

$$P(a,b,c) = P(m,n)$$

where

$$a = 2n^2 + 2n(2m-1) \tag{5}$$

$$b = 2n(2m-1) + (2m-1)^2 \tag{6}$$

$$c = 2n^2 + 2n(2m-1) + (2m-1)^2 \tag{7}$$

It is worth noting the special condition that we had specified in proposition (2): $b = 2a + 1$. By substituting this in the above Equations (5) and (6), and by bringing a and b in terms of m and n, we get:

$$2n(2m-1) + (2m-1)^2 = 2\left[2n^2 + 2n(2m-1)\right] + 1$$

This gives us the special condition, a Diophantine equation, given below:

$$4n^2 + 2n(2m-1) - (2m-1)^2 + 1 = 0 \tag{8}$$

Solving this Diophantine Equation (8) given above, we get $m = 7, n = 4$.
By substituting $P(m,\ n) = P(7,\ 4)$ into Equations (5)–(7), we derive $\Rightarrow P(a,b,c) = (136,\ 273,\ 305)$. Next, substituting $P(a,\ b,$

c) = (136, 273, 305) into Equation (3), we get:

$$\frac{\phi\, a \pm c}{b} - \frac{136 + 305}{273} - \frac{441}{273} - \frac{21}{13} \approx 1.61$$

It is noted that the numbers in the quotients above, namely 13 and 21, are both sequential Fibonacci numbers. It is well known that the golden ratio can be expressed as the ratio of two sequential Fibonacci sequence numbers. A brief explanation and simple proof are given in the next section.

1.2. *The Golden Ratio and Fibonacci Sequence*

We establish the second property of the golden ratio by expressing it as a ratio of the terms in the Fibonacci sequence. The Fibonacci sequence is an infinite series of integers, where each term is the sum of the two previous terms. It is defined by the following mathematical function:

$$F(i) = F(i-1) + F(i-2) \text{ with } F(0) = 0 \text{ and } F(1) = 1$$

i	0	1	2	3	4	5	6	7	8	9	10	11
F_i	0	1	1	2	3	5	8	13	21	34	55	89

As i takes large values when we go farther and farther to the right of the Fibonacci sequence, the ratio of a term to the one before it will be approximately equal to the golden ratio.

The golden ratio as defined earlier is given by: $\varphi = \frac{1}{\varphi - 1} = \frac{1+\sqrt{5}}{2} = 1.618$

$$\varphi = \lim_{i\to\infty} \frac{F_{i+1}}{F_i} \Rightarrow \frac{F_{11}}{F_{10}} = \frac{89}{55} \approx 1.618 \qquad (9)$$

The golden ratio as a ratio of the Fibonacci number sequence can be pictorially visualized as the golden rectangle, as shown in Figure 4. We start with a square and, by placing another square of the same size adjacent to it, we can form a new rectangle. As we continue to place adjacent squares, the longer side of the rectangle formed will always be a successive Fibonacci number. The larger rectangle formed becomes a golden rectangle, as shown in Figure 4.

In this section, we have shown that for higher terms in the Fibonacci sequence, i.e., when we go farther and farther to the right of the Fibonacci sequence, the ratio of a term (n) to the one before it ($n - 1$) approximates to the golden ratio. Since the Fibonacci sequence is an infinite series of numbers, the time/space complexity grows with larger terms and varies according to various implementations already reported in literature [34]. Some implementations have the space/time complexity to have exponential dependence on n. Certain others, using the constant-time arithmetic, have the space/time complexity to be O(n). These analytical proofs assume infinite precision. However, from the software-based computational aspects, there are limitations on the precision due to hardware or software constraints and this has a major impact on the space/time complexity. Hence, our purpose in this paper is not to provide an analytical proof in general. Rather, the purpose of our paper is to propose the golden ratio using Diophantine equations for its use in cryptographic software solutions. In this context, we compare its space/time complexity to the commonly used Fibonacci sequence method experimentally up to a certain computing precision that is feasible and applicable for secure cryptography. We make use of a few more properties of the golden ratio as described below before we provide our proposed method to compute the golden ratio in Section 4 and the experimental comparison results of our experiments in Section 5

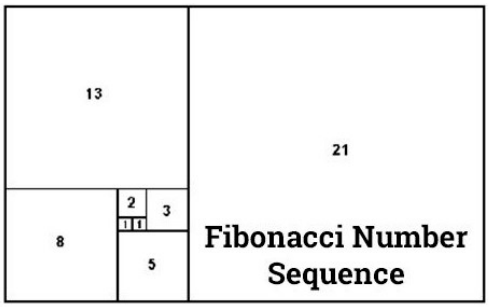


Figure . Representation of the golden ratio as the Fibonacci sequence.

1.3. *The Golden Ratio as a Ratio in Terms of* (m, n) : $\phi(m, n)$

Having established the basic forms of the golden ratio, we are now in a position to explore some more advanced properties, which lay the foundation of our proposed new method for computing the Golden Ratio. In Section 3.2, we solved the special condition Equation (8):

$$4n^2 + 2n(2m-1) - (2m-1)^2 + 1 = 0$$

Let us now express a general equation for ϕ in terms of m, n : $\phi(m, n)$ from Equation (3):

$$\varphi = \frac{a+c}{b}$$

Equations (5)–(7) become as follows:

$$a = 2n^2 + 2n(2m-1),\ \ b = 2n(2m-1) + (2m-1)^2$$
$$c = 2n^2 + 2n(2m-1) + (2m-1)^2$$

Substituting these into Equation (3), we get

$$\begin{aligned}\varphi &= \tfrac{a+c}{b} = \frac{4n^2+4n(2m-1)+(2m-1)^2}{2n(2m-1)+(2m-1)^2}\\ &= \frac{4n^2+2n(2m-1)+2n(2m-1)+(2m-1)^2}{2n(2m-1)+(2m-1)^2}\\ &= \frac{4n^2+2n(2m-1)}{2n(2m-1)+(2m-1)^2}+1\\ &= \frac{(2n)(2n)+2n(2m-1)}{2n(2m-1)+(2m-1)^2}+1\\ &= \frac{2n(2n+2m-1)}{(2m-1)(2n+2m-1)}+1\\ \varphi &= \frac{2n}{2m-1}+1\end{aligned}$$

From Equation (1):

$$\varphi = \frac{1}{\varphi - 1} \Rightarrow \frac{1}{\varphi} = \varphi - 1 = \frac{2n}{2m-1}$$

We note the following:

$$\varphi = \frac{2m-1}{2n} \tag{10}$$

$$\lim_{m\to\infty} 2m - 1 = 2m$$

$$\varphi = \frac{m}{n} \tag{11}$$

It should be noted that, for the special condition in Equation (8), there are multiple solutions

The Golden Ratio and the Infinite Series for (m:n)

We establish another advanced property of the golden ratio by deriving the infinite series for m, n so that any resolution for $\phi(m, n)$ can now be arrived at. We had previously solved the special condition Equation (8) given below:

$$4n^2 + 2n(2m-1) - (2m-1)^2 + 1 = 0$$

Next, we derive the general expression for n in terms of m:

$$\begin{gathered}4n^2 + 2n(2m-1) - (2m-1)^2 + 1 = 0\\ n^2 + \tfrac{n(2m-1)}{2} = \tfrac{(2m-1)^2-1}{4}\\ \Rightarrow n^2 + \tfrac{n(2m-1)}{2} + \tfrac{(2m-1)^2}{16} = \tfrac{(2m-1)^2}{16} + \tfrac{(2m-1)^2-1}{4}\\ \left(n + \tfrac{2m-1}{4}\right)^2 = \tfrac{(2m-1)^2}{16} + \tfrac{(2m-1)^2-1}{4} \Rightarrow\\ n + \tfrac{2m-1}{4} = \sqrt{\tfrac{(2m-1)^2}{16} + \tfrac{(2m-1)^2-1}{4}} \Rightarrow\\ n = \sqrt{\tfrac{(2m-1)^2}{16} + \tfrac{(2m-1)^2-1}{4}} - \tfrac{2m-1}{4} \Rightarrow\end{gathered}$$

$$n = \frac{\sqrt{20m^2 - 20m + 1} - 2m + 1}{4} \tag{12}$$

The above set of mathematical derivations lead us towards the proposal of our new efficient golden ratio method with infinite precision.

Proposed Method for Golden Ratio Computations

We propose a new method to solve the Diophantine Equation (8)—$4n^2 + 2n(2m-1) - (2m-1)^2 + 1 = 0$—by finding solutions to Equation (12) for values of m which provide integer values of n. The results of these solutions are shown in Table 1. The first two values of i_1 and i_2 determine the series.

Table 1. Recursive solutions to the Diophantine equations.

i	1	2	3	4	5	6
m	7	117	2,091	37,513	673,135	12,078,909
n	4	72	1,292	23,184	416,020	746,5176

Now, using Equation (10), we get:

$$\varphi(6) = \frac{2m_6-1}{2n_6} = \frac{2(12{,}078{,}909)-1}{2(7{,}465{,}176)} = 1.618033988749894 \mid 08$$

$$\mathit{Actual}\ \phi = 1.6180339887498948482 04\ldots$$

From Table 1, the following infinite series for m, n can now be derived.

$$m_i = 18m_{i-1} - m_{i-2} - 8 \tag{13}$$

$$n_i = 18n_{i-1} - n_{i-2} \tag{14}$$

From the above Equations (13) and (14), given that the 5th and 6th values are known, we determine the 7th value, $i = 7$ as follows:

$$m_7 = 18(12,078,909) - 673,135 - 8 = 216,747,219$$

$$n_7 = 18(7,465,176) - 416,020 = 133,957,148$$

$$\phi(7) = \frac{2m_7-1}{2n_7} = \frac{2(216{,}747{,}219)-1}{2(133{,}957{,}148)}$$

$$= 1.61803398874989485 \mid 4,435.$$

From the above, we can easily see that there is an improvement of two places between the values of $\phi(6)$ and $\phi(7)$. The accuracy of $\phi(8)$ is 19 places, as derived below:

$$m_8 = 18(216,747,219) - 12,078,909 - 8 = 3,889,371,025$$

$$n_8 = 18(133,957,148) - 7,465,176 = 2,403,763,488$$

$$\phi(8) = \frac{2m_8-1}{2n_8} = \frac{2(3{,}889{,}371{,}025)-1}{2(2{,}403{,}763{,}488)}$$

$$= 1.6180339887498948482 \mid 2$$

Results

We demonstrate the efficiency of our proposed method for determining the golden ratio by performing experiments to compare our proposed method with the commonly used Fibonacci sequence method.

We consider Equation (9): $\varphi = \lim\limits_{n\to\infty} \frac{F_{i+1}}{F_i}$ and Equation (10): $\varphi = \frac{2m-1}{2n}$. We can make the $2n$ following observations:

$$F_{i+1} = 2m - 1 \text{ and } F_i = 2n$$

Consider $m_8 = 3,889,371,025$, $n_8 = 2,403,763,488$

$$F_{48} = 2n_8 = 2(2,403,763,488) = 4,807,526,976$$
$$F_{49} = 2m_8 - 1 = 2(3,889,371,025) - 1 = 7,778,742,049$$

Hence, to calculate ϕ to 19 decimal places requires 49 Fibonacci loops, which are essentially additions and one division.Solving the Diophantine Equation (12) is tedious. However, once the first two values of the each of the sequences m_i and n_i are known, the series Equations (13) and (14) very quickly determine the desired values for m_i and n_i. Doubling these and one subtraction elegantly places values in the Fibonacci sequence. We revise Table 1 to include the number of computations performed in our proposed method to calculate the golden ratio using Diophantine equations as compared to Fibonacci sequence method. These comparisons are summarized in Table 2.

Table 2. Comparison of the proposed method vs. Fibonacci sequence method.

i	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
m	7	117	2,091	37,513	673,135	12,078,909	216,747,219	3,889,371,025
n	4	72	1,292	23,184	416,020	7,465,176	133,957,148	2,403,763,488
$2m - 1$	13	233	4,181	75,025	1,346,269	24,157,817	433,494,437	7,778,742,049
F_i	7	13	19	25	31	37	43	49
$2n$	8	144	2,584	46,368	832,040	14,930,352	267,914,296	4,807,526,976
F_{i-1}	6	12	18	24	30	36	42	48

From Table 2, it can be observed that once our initial m_i and n_i are known, each succeeding value for each sequence requires a multiplication (×18) and a subtraction of the previous sequence value, and for m_i, a minor subtraction of a constant (8). This essentially results in four operations versus six additions in the Fibonacci sequence to obtain the same value. Equations (9)–(11) require a division. Now, we reconsider the following equations:

$$\varphi = \lim_{i \to \infty} \frac{F_{i+1}}{F_i} \ (9) \quad \varphi = \frac{2m-1}{2n} \ (10) \quad \varphi = \frac{m}{n} \ (11)$$

Let us now consider eight iterations of our new method, which is essentially 32 operations. We compare our proposed method and Fibonacci sequence method of computations for the golden ratio by considering 32 operations in each method.

$$\varphi = \frac{F_{32}}{F_{31}} = \frac{2,178,309}{1,346,269} = 1.6180339887496$$
$$\varphi = \frac{m_8}{n_8} = \frac{3,889,371,025}{2,403,763,488} = 1.618034$$

If we allow three addition calculations, we get:

$$\varphi = \frac{F_{35}}{F_{34}} = \frac{9,227,465}{5,702,887}$$
$$= 1.6180339887499 \text{ (13 decimal places)}$$
$$\varphi = \frac{2m_8-1}{2n_8} = \frac{2(3,889,371,025)-1}{2(2,403,763,488)} = \frac{7,778,742,049}{4,807,526,976}$$

$$= 1.618033988749894848 \text{ (18 decimal places)}$$

This would require 49 cycles in the Fibonacci sequence method to obtain the same accuracy.Overall, it is observed that 35 calculations of our new proposed method provide the golden ratio with an accuracy to 19 decimal places, while 35 calculations of the Fibonacci sequence method provide the golden ratio with only 13 decimal places of accuracy. In other words, 49 calculations in the Fibonacci sequence method are required to arrive at the same level of accuracy as the proposed new method. We note that Equation (10) provides a much better result than Equation (11) with very little performance penalty.
Next, let us consider 48 operations + 3 addition calculations, totaling 51 operations altogether.

$$\varphi = \frac{F_{51}}{F_{50}} = \frac{20,365,011,074}{12,586,269,025}$$
$$= 1.6180339887498948482 07 \text{ (20 decimal places)}$$
$$\varphi = \frac{2m_{12}-1}{2n_{12}}$$
$$= \frac{2(403,257,766,524,697)-1}{2(249,227,005,939,632)} = \frac{806,515,533,049,393}{498,454,011,879,264}$$

$$= 1.61803398874989484820458683436 7 \text{ (29 decimal places)}$$

$$\phi = 1.618033988749894848204586834365$$

These results clearly indicate the trend that with more iterations performed, our new method far outperforms that of Fibonacci sequence method in terms of precision for the same number of arithmetic operations. Hence, the computations of our proposed method for the golden ratio are much faster than the existing well-known methods using the Fibonacci sequence, meeting the need of faster cryptosystems with high precision.

Conclusions and Future Work

In this paper, we presented an efficient method to compute the k golden ratio, which has wide applications in secret key generations and in secure cryptographic applications. While simple to very complex cipher-based cryptography are available, these methods have failed to counter the rising security attacks due to the lack of speed in their computations. More recently a new cryptography called golden cryptography is studied, where golden ratio computations are used. Compared with previous methods where the well-known Fibonacci sequence method is used to compute the golden ratio, our proposed method adopts the advanced properties of applying the Diophantine equations in the computations. Firstly, we established these properties and the proposed method mathematically. Then, we experimentally computed the golden ratio using the proposed method with infinite precision. Finally, we evaluated our method by comparing the computational results with the well-known Fibonacci sequence method. We established the efficiency of our proposed golden ratio method in terms of both speed of calculation and precision.

This research has applications in faster cryptographic algorithms, and future work would study their impact in preventing security attacks. It would be of interest to explore how our faster method for K , golden ratio computations would facilitate cryptographic protection by establishing efficient secret keys for the timely combating of any possible information security penetration.

PROJECT CONCLUSION

Zetanet is a blockchain 5.0 generation for decentralized computing network that provides high compatibility to developers for building decentralized internet applications. This decentralized autonomous data storage system gives comparable performance to traditional cloud storage and only introduces a small overhead for encryption/decryption. Our authentication protocol removes the need for password-based logins which are known to be less secure than cryptographic authentication. Users are able to use a single account across services and applications, removing the need to continuously create new accounts for new services. Our future developer libraries make the development of decentralized apps on this platform as easy as building traditional internet applications. With this it will be much faster because we don't have to go through the Content Delivery Network (CDN) and more secure than encrypting via SSL we are already encrypting the data using our jack's law encryption algorithm prior to releasing the data to zeta network

In this paper, we presented the latest design of Zetanet. Since earlier production implementation in 2017 from first concept protocol of encrypblock, the core design of Zetanet has evolved and incorporates lessons learned from production deployments and feedback from developers of decentralized applications. The main changes from the earlier (2017) whitepaper include (a) description of the encrypblock into blockchain which uses a new Zetanet mechanism to design protocol on top of a new blockchain, and (b) description of a new smart contract language that focuses on security and predictability of smart contracts.

ACKNOWLEDGMENT

Over the years many people have contributed to the design and implementation of Zetanet idea. We would like to thank John Moses Ventura, Adriel Artiza, Jomer Pangilinan and Jeffrey Lim for their early contributions, ideas and for their work on developers' libraries and SDKs. For product designs and development docs; For infrastructure development; Neil Francis Portugal, Paulius Stankevicius for their helpful comments and feedback. More Zetanet contributors can be found at https://github.com/Zetanet-dev but in general we hope many people will contribute to this project that it's not realistic to explicitly thank them – we're grateful for your support to the entire Zetanet Blockchain 5.0 project.

DISCLAIMER

Every effort is made to ensure accurate, current and complete information on this whitepaper but Skipjack Technology cannot and does not guarantee accuracy or timeliness of materials or information written on this. This Document is always being updated.