VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

School of Computer Science and Engineering

Quantum Cryptography to secure Cyber Physical Systems

Information Security Analysis and Audit
J-Component Review - 3

` **Team members:**

Moitrish Sinha 18BCE0617

Abhinav 18BCE0641

Shaik Haseeb Ur Rahman 18BCE0646

Lakshit Dua 18BCE0824

Performed Under:
Dr. Sendhil Kumar K.S
Associate Professor Grade 1 (SCOPE)
October – 2020

ABSTRACT

Cyber-physical systems (CPSs) refers to the tight conjoining of and coordination between computational and physical resources. Some of the CPSs are smart grid, autonomous automobile systems, medical monitoring, process control systems, robotics systems, and automatic pilot avionics. CPSs will be deployed for decades, thus they should be secure against malicious cyberattacks. Quantum cryptography is one of the emerging topics in the field of the computer industry. Quantum Computers have made it easier to crack existing cryptography techniques. Rather than depending on the complexity of factoring large numbers, quantum cryptography is based on the fundamental and unchanging principles of quantum mechanics. Thus, on this project we will try to apply Quantum cryptography on the Cyber-physical systems in order to make them more secure.

INTRODUCTION

A cyber-physical system (CPS) is a mechanism controlled or monitored by computer-based algorithms, tightly integrated with the internet and its users. In cyber-physical systems, physical and software components are deeply intertwined, each operating on different spatial and temporal scales, exhibiting multiple and distinct behavioral modalities, and interacting with each other in a myriad of ways that change with context. Examples of CPS include smart grid, autonomous automobile systems, medical monitoring, process control systems, robotics systems, and automatic pilot avionics.

CPS involves transdisciplinary approaches, merging theory of cybernetics, mechatronics, design, and process science. The process control is often referred to as embedded systems. In embedded systems, the emphasis tends to be more on the computational elements, and less on an intense link between the computational and physical elements. CPS is also similar to the Internet of Things (IoT) sharing the same basic architecture, nevertheless, CPS presents a higher combination and coordination between physical and computational elements.

Precursors of cyber-physical systems can be found in areas as diverse as aerospace, automotive, chemical processes, civil infrastructure, energy, healthcare, manufacturing, transportation, entertainment, and consumer appliances.

Unlike more traditional embedded systems, a full-fledged CPS is typically designed as a network of interacting elements with physical input and output instead of as standalone devices. The notion is closely tied to concepts of robotics and sensor networks with intelligence mechanisms proper of computational intelligence leading the pathway. Ongoing advances in science and engineering will improve the link between computational and physical elements by means of intelligent mechanisms, dramatically increasing the adaptability, autonomy, efficiency, functionality, reliability, safety, and usability of cyber-physical systems. This will broaden the potential of cyber-physical systems in several dimensions, including intervention (e.g., collision avoidance); precision (e.g., robotic surgery and nano-level manufacturing); operation in dangerous or inaccessible environments (e.g., search and rescue, firefighting, and deep-sea exploration); coordination (e.g., air traffic control, war fighting); efficiency (e.g., zero-net energy buildings); and augmentation of human capabilities (e.g., healthcare monitoring and delivery).

LITERATURE SURVEY

1) Cyber Physical Systems: Design Challenges

Cyber-Physical Systems (CPS) are integrations of computation and physical processes. Embedded computers and networks monitor and control the physical processes, usually with feedback loops where physical processes affect computations and vice versa. The economic and societal potential of such systems is vastly greater than what has been realized, and major investments are being made worldwide to develop the technology. There are considerable challenges, particularly because the physical components of such systems introduce safety and reliability requirements qualitatively different from those in general-purpose computing. Moreover, physical components are qualitatively different from object-oriented software components. Standard abstractions based on method calls and threads do not work. This paper examines the challenges in designing such systems, and in particular, raises the question of whether today's computing and networking technologies provide an adequate foundation for CPS. It concludes that it will not be sufficient to improve design processes, raise the level of abstraction, or verify (formally or otherwise) designs that are built on today's abstractions. To realize the full potential of CPS, we will have to rebuild computing and networking abstractions. These abstractions will have to embrace physical dynamics and computation in a unified way.[1]

2) Cyber-physical systems: The next computing revolution

Cyber-physical systems (CPS) are physical and engineered systems whose operations are monitored, coordinated, controlled, and integrated by a computing and communication core. Just as the internet transformed how humans interact with one another, cyber-physical systems will transform how we interact with the physical world around us. Many grand challenges await in the economically vital domains of transportation, health-care, manufacturing, agriculture, energy, defense, aerospace, and buildings. The design, construction, and verification of cyber-physical systems pose a multitude of technical challenges that must be addressed by a cross-disciplinary community of researchers and educators. Cyber-physical systems (CPS) will transform how humans interact with and control the physical world. Zero-energy buildings and cities, extreme-yield agriculture, near-zero automotive fatalities, perpetual life assistants, location-independent access to medical care, situation-aware physical critical infrastructure, blackout-free electricity, and safe evacuation from hazardous areas are but some of the many societal benefits that CPS will deliver. CPS must operate dependably, safely, securely, efficiently, and in real-time. CPS represents a confluence of technologies in embedded systems, distributed systems, dependable systems, real-time systems with advances in energy-efficient networking, microcontrollers, sensors, and actuators. Correct, affordable, and flexible deployment of CPS can only be made possible by fundamental advances in science, engineering, and education. CPS technologies must be scalable across time and space and must deal with multiple time-scales, uncertainty, privacy concerns, and security issues. A new CPS science will define new mathematical foundations with formalisms to specify, analyze, verify, and validate systems that monitor and control physical objects and entities. The new infrastructure will benefit different economic and industrial sectors. Sophisticated design tools will capture both cyber abstractions and the dynamics of physical/engineered systems. CPS scientists and engineers must be educated and trained to have a common knowledge framework that bridges the discrete world of computing and communications with the continuous world of physics.[2]

3) A Cyber-Physical Systems architecture for Industry 4 - based manufacturing systems

Recent advances in the manufacturing industry has paved way for a systematically deployment of Cyber-Physical Systems (CPS), within which information from all related perspectives is closely monitored and synchronized between the physical factory floor and the cyber computational space. Moreover, by utilizing advanced information analytics, networked machines will be able to perform more efficiently, collaboratively, and resiliently.

Such a trend is transforming the manufacturing industry to the next generation, namely Industry 4.0. At this early development phase, there is an urgent need for a clear definition of CPS. In this paper, a unified 5-level architecture is proposed as a guideline for the implementation of CPS.[3]

4) Cyber-physical Systems

The term cyber-physical systems (CPS) refers to a new generation of systems with integrated computational and physical capabilities that can interact with humans through many new modalities. The ability to interact with, and expand the capabilities of, the physical world through computation, communication, and control is a key enabler for future technology developments. Opportunities and research challenges include the design and development of next-generation airplanes and space vehicles, hybrid gas-electric vehicles, fully autonomous urban driving, and prostheses that allow brain signals to control physical objects. Cyber-physical systems are expected to play a major role in the design and development of future engineering systems with new capabilities that far exceed today’s levels of autonomy, functionality, usability, reliability, and cyber security. Advances in CPS research can be accelerated by close collaborations between academic disciplines in computation, communication, control, and other engineering and computer science disciplines, coupled with grand challenge applications.[4]

5) Attack Detection and Identification in Cyber-Physical Systems

Cyber-physical systems are ubiquitous in power systems, transportation networks, industrial control processes, and critical infrastructures. These systems need to operate reliably in the face of unforeseen failures and external malicious attacks. In this paper:

i) we propose a mathematical framework for cyber-physical systems, attacks, and monitors;

ii) we characterize fundamental monitoring limitations from system-theoretic and graph-theoretic perspectives; and

iii) we design centralized and distributed attack detection and identification monitors. Finally, we validate our findings through compelling examples. CYBER-PHYSICAL systems integrate physical processes, computational resources, and communication capabilities. Examples of cyber-physical systems include transportation networks, power generation and distribution networks, water and gas distribution networks, and advanced communication systems.[5]

6) Secure Control: Towards Survivable Cyber-Physical Systems

Cyber-Physical Systems (CPS) integrate computing and communication capabilities with monitoring and control of entities in the physical world. These systems are usually composed by a set of networked agents, including sensors, actuators, control processing units, and communication devices; see Fig. While some forms of CPS are already in use, the widespread growth of wireless embedded sensors and actuators is creating several new applications –in areas such as medical devices, autonomous vehicles, and smart structures– and increasing the role of existing ones –such as Supervisory Control and Data Acquisition (SCADA) systems.[6]

7) Quantum cryptography

Quantum cryptography could well be the first application of quantum mechanics at the individual quanta level. The very fast progress in both theory and experiments over the recent years are reviewed, with emphasis on open questions and technological issues. The most peculiar characteristics of quantum mechanics are the existence of indivisible quanta and of entangled systems. Both of these are at the root of Quantum Cryptography (QC) which could very well be the first commercial application of quantum physics at the individual quantum level. In addition to quantum mechanics, the 20th century has been marked by two other major scientific revolutions: the theory of information and relativity. The status of the latter is well recognized. It is less known that the concept of information, nowadays measured in bits, and the formalization of probabilities is quite recent1, although they have a tremendous impact on our daily life. It is fascinating to realize that QC lies at the intersection of quantum mechanics and information theory and that, moreover, the tension between quantum mechanics and relativity – the famous EPR paradox (Einstein al.1935) – is closely connected to the security of QC. Let us add a further point for the young physicists. Contrary to laser and semiconductor physics, which are manifestations of quantum physics at the ensemble level and can thus be described by semi-classical models, QC, and even much more quantum computers, require a full quantum mechanical description (this may offer interesting jobs for physicists well trained in the subtleties of their science). Quantum cryptography is a fascinating illustration of the dialog between basic and applied physics. It is based on a beautiful combination of concepts from quantum physics and information theory and made possible thanks to the tremendous progress in quantum optics and in the technology of optical fibers and of free-space optical communication. Its security principle relies on deep theorems in classical information theory and on a profound understanding of the Heisenberg's uncertainty principle, as illustrated by theorems 1 and 2 in section VI G (the only mathematically involved theorems in this review!).

Let us also emphasize the important contributions of QC to classical cryptography: privacy amplification and classical bound information (paragraphs II C 4 and II C 5) are examples of concepts in classical information whose discovery was much inspired by QC. Moreover, the fascinating tension between quantum physics and relativity, as illustrated by Bell’s inequality, is not far away, as discussed in section VI F. Now, despite the huge progress over the recent years, many open questions and technological challenges remain[7].

8) Experimental quantum cryptography

We describe results from an apparatus and protocol designed to implement quantum key distribution, by which two users, who share no secret information initially: (1) exchange a random quantum transmission, consisting of very faint flashes of polarized light; (2) by subsequent public discussion of the sent and received versions of this transmission estimate the extent of eavesdropping that might have taken place on it, and finally (3) if this estimate is small enough, distil from the sent and received versions a smaller body of shared random information, which is certifiably secret in the sense that any third party's expected information on it is an exponentially small fraction of one bit. Because the system depends on the uncertainty principle of quantum physics, instead of the usual mathematical assumptions such as the difficulty of factoring, it remains secure against an adversary with unlimited computing power[8].

9) Quantum cryptography: Public key distribution and coin tossing

When elementary quantum systems, such as polarized photons, are used to transmit digital information, the uncertainty principle gives rise to novel cryptographic phenomena unachievable with traditional transmission media, e.g. a communications channel on which it is impossible in principle to eavesdrop without a high probability of disturbing the transmission in such a way as to be detected. Such a quantum channel can be used in conjunction with ordinary insecure classical channels to distribute random key information between two users with the assurance that it remains unknown to anyone else, even when the users share no secret information initially. We also present a protocol for coin-tossing by the exchange of quantum messages, which is secure against traditional kinds of cheating, even by an opponent with unlimited computing power, but ironically can be subverted by the use of a still subtler quantum phenomenon, the Einstein-Podolsky-Rosen paradox[9].

10) Quantum Cryptography with Entangled Photons

By realizing a quantum cryptography system based on polarization-entangled photon pairs we establish highly secure keys because a single photon source is approximated and the inherent randomness of quantum measurements is exploited. We implement a novel key distribution scheme using Wigner’s inequality to test the security of the quantum channel, and, alternatively, realize a variant of the BB84 protocol. Our system has two completely independent users separated by 360 m and generates raw keys at rates of 400 – 800 bits/second with bit error rates around 3%. The primary task of cryptography is to enable two parties (commonly called Alice and Bob) to mask confidential messages such, that the transmitted data are illegible to any unauthorized third party (called Eve). Usually, this is done using shared secret keys. However, in principle, it is always possible to intercept classical key distribution undoubtedly. The recent development of quantum key distribution1 can cover this major loophole of classical cryptography. It allows Alice and Bob to establish two completely secure keys by transmitting single quanta (qubits) along a quantum channel. The underlying principle of quantum key distribution is that nature prohibits to gain information on the state of a quantum system without disturbing it. Therefore, in appropriately designed schemes, no tapping of the qubits is possible without showing up to Alice and Bob. These secure keys can be used in a One-Time-Pad protocol, which makes the entire communication absolutely secure. A range of experiments has demonstrated the feasibility of quantum key distribution, including realizations using the polarization of photons 9 or the phase of photons in long interferometers10. These experiments have a common problem: the sources of the photons are attenuated laser pulses that have a non-vanishing probability to contain two or more photons, leaving such systems prone to the so-called beam splitter attack11. Using photon pairs as produced by parametric down conversion allows us to approximate a conditional single photon source12 with a very low probability for generating two pairs simultaneously and a high bit rate13. Moreover, when utilizing entangled photon pairs one immediately profits from the inherent randomness of quantum mechanical observations leading to purely random keys. Various experiments with entangled photon pairs have already demonstrated that entanglement can be preserved over distances as large as 10 km14, yet none of these experiments was a full quantum cryptography system. We present in this paper a complete implementation of quantum cryptography with two users, separated and independent of each other in terms of Einstein locality and exploiting the features of entangled photon pairs for generating highly secure keys.[10]

11) Unconditional security in quantum cryptography

Basic techniques to prove the unconditional security of quantum cryptography are described. They are applied to a quantum key distribution protocol proposed by Bennett and Brassard [1984]. The proof considers a practical variation on the protocol in which the channel is noisy and photons may be lost during the transmission. Each individual signal sent into the channel must contain a single photon or any two-dimensional system in the exact state described in the protocol. No restriction is imposed on the detector used at the receiving side of the channel, except that whether or not the received system is detected must be independent of the basis used to measure this system. This paper proves the unconditional security of quantum key distribution and reviews basic notions and principles which apply to any quantum key distribution protocol, and in fact to other kinds of quantum protocols as well. The techniques that we have described here, some of them taken in Yao [1995], were proven to be efficient to analyze the security of quantum key distribution. However, these techniques were first used in Mayers [1996] to analyze a quantum protocol for a different application, a quantum string oblivious transfer protocol [Bennett et al. 1992]. For some time this quantum string oblivious transfer was ignored because it was built on top of a task called bit commitment. This was proven to be unsecure given that the participants, potential cheaters, have unlimited computational power [Mayers 1997]. However, recently a quantum protocol was proposed [Dumais et al. 2000] for bit commitment under some computational assumption and this raises the important question of the security of the quantum string oblivious transfer protocol on top of a computationally secure quantum bit commitment. We hope that the technique described here would be useful to address this question. There is also the serious issue of defective and unreliable quantum apparatus. A more practical protocol was the encoding must still respect the exact polarization angle specified in the protocol, but not necessarily for a single photon, was proven secure in Inamori et al. [1999] using the techniques described Unconditional Security in Quantum Cryptography 393 here. The most powerful and global approach to address this problem is proposed in Mayers and Yao [1998] and Mayers [2001a]. However, the results in Mayers and Yao [1998] and Mayers [2001a] are general and their applicability to a given protocol is still an open question. Again, we hope that the techniques provided here will be useful to establish the connection.[11]

12) One-time pad Encryption key Distribution

Some of these problems with digital information protection Systems may be overcome by providing a mechanism that allows a content provider to encrypt digital information without requiring either a hardware or platform manufacturer or a content consumer to provide Support for the Specific form of corresponding decryption. This mechanism can be provided in a manner that allows the digital information to be copied easily for back-up purposes and to be transferred easily for distribution, but which should not permit copying of the digital information in decrypted form. In particular, the encrypted digital information is stored as an executable computer program that includes a decryption program that decrypts the encrypted information to provide the desired digital information, upon successful completion of an authorization procedure by the user. In combination with other mechanisms that track distribution, enforce royalty payments, and control access to decryption keys, the present invention provides an improved method for identifying and detecting Sources of unauthorized copies. Suitable authorization procedures also enable the digital information to be distributed for a limited number of uses and/or users, thus enabling per-use fees to be charged for the digital information.[12]

13) System and method for synchronizing one-time pad encryption keys for secure communication and access control

A method for generating an identical electronic one-time pad at a first location and a second location, the method comprising the steps of: (a) providing a first electronic device at the first location and a second electronic device at the second location, each of the first and the second electronic devices having: (i) a non-volatile memory; (ii) a processor; (iii) at least one table of true random numbers being stored on the non-volatile memory, the table being identical for the first and the second electronic devices; and (iv) at least one software program for obtaining a true random number from the table, the software program being stored on the non-volatile memory and the at least one software program being operated by the processor; (b) providing a communication channel for communication between the first electronic device and the second electronic device; (c) selecting a selected true random number from the table at the first and the second electronic devices according to a selection procedure, the selection procedure being identical for the first and the second electronic devices, the selection procedure including exchanging at least a portion of a key between the first and the second electronic devices over the communication channel, such that the selected true random number is identical for the first and the second electronic devices; and (d) forming at least a portion of the identical electronic one-time pad at the first and the second locations with the selected true random number. The present invention relates to a system, a device, and a method of providing secure communication between two parties, and in particular for providing Such Secure communication over a communication network. Secure communication between two parties has always been an important but difficult task. The moment information is shared between two parties, a third, unauthorized party may be able to access this information as well. The problem is magnified when the two authorized parties are Separated by a distance, So that information must be passed in the form of messages rather than by direct communication. Historically, the content of messages has Sometimes been protected by cryptography, in which the content is altered by transformation into another form which is understandable only by the intended recipient or recipients of the message. AS the technology for transferring information has become increasingly complex and Sophisticated, So has the technology of cryptography. Currently, cryptography may be performed by encoding the original message into an incomprehensible protected message according to mathematical algorithms using a particular key. Only the correct recipient should have both the same algorithm and the particular key needed to decode the protected message into the original message. Thus, the incomprehensible encoded message can be freely transmitted over a relatively insecure communication channel Such as a telephone network, while remaining. Secure to all but the correct recipient.[13]

14) Emerging Embedded and Cyber Physical System Security Challenges and Innovations

DEEPLY-EMBEDDED systems (deployed in the human body, with computer programs sending and receiving sensitive data and performing data mining for the decisions) are increasingly popular, but the security and privacy issues are not fully understood and studied. For example, issues relating to the confidentiality/integrity/availability/privacy of implantable and wearable medical devices, secure and private big data analytics, acquisition, and storage, privacy-preserving data mining, secure machine learning, cyber physical systems security, and security of hardware and software systems used for databases (with diverse societal contexts) are critical and can be challenging to address due to their unique constraints and usage model. Existing systems for such computations would need to be transparently integrated into sensitive environments-the consequent size and energy constraints imposed on any security solutions are demanding. Thus, unique challenges arise due to the sensitivity of computation processing, the need for security in implementations, and assurance "gaps." This special issue is dedicated to the identification of techniques designed for embedded systems and cyber physical systems, such as emerging cryptographic solutions applicable to extremely-constrained, sensitive infrastructures. We received 35 submissions for this special issue, of which 4 have been accepted (acceptance rate 11.45 percent). Each paper went through a rigorous peer-review process, in addition to multiple follow-up rounds with the authors. A summary of the papers is provided below.[14]

15) Overview of Cyber Physical Systems in Future Production

Surrounded by the various recent technologies, cyber-physical systems (CPS) are a booming terminology symbolizing the combination of computation and physical capabilities which has an immense area of application in process control, medical devices, energy control, traffic control, advanced automated systems, and smart structures. Businesses or rather, manufacturers of diverse sizes and industry segments progressively cooperate with each other and with the service providers, the telecommunication suppliers, and the software producers, in order to combine their competencies, which are finally going to be needed to construct and operate cross-industry product innovation.

MOTIVATION

Surrounded by the various recent technologies, cyber-physical systems (CPS) are a booming terminology symbolizing the combination of computation and physical capabilities which has an immense area of application in process control, medical devices, energy control, traffic control, advanced automated systems, and smart structures. Businesses or rather, manufacturers of diverse sizes and industry segments progressively cooperate with each other and with the service providers, the telecommunication suppliers, and the software producers, in order to combine their competencies, which are finally going to be needed to construct and operate cross-industry product innovation. Cyber-physical systems donate a lot to finding answers to key problems of our society and are highly suitable for countless industries and fields of application. Cyber-physical systems supply companies with assistance in process optimization and consequently also in being cost-effective and time-saving, and they provide help in energy saving, thus reducing CO2 emissions at a high rate.

In the CPS study, the following four fields of application were investigated in elaborate scenarios for the period up to 2025:

1. Energy – CPS for the smart grid
2. Mobility – CPS for networked mobility
3. Health – CPS for telemedicine and remote diagnosis
4. Industry – CPS for industry and automated production.[15]

INFORMATION SECURITY CONCEPTS USED IN THE PROJECT

The concept of information security in the context of Cyber physical Systems has be brought under light in this project. As described earlier, Cyber physical Systems are large-scale contraptions that maybe a part of smart-grid, military and defence, medical research etc. They are systems which include a cyber interaction side and a physical interaction side. Cyber physical systems are generally deployed as an aid to a huge number of individuals and any compromise in the data may lead to large-scale failure and losses.

The project applies and takes care of three major information security concepts of:

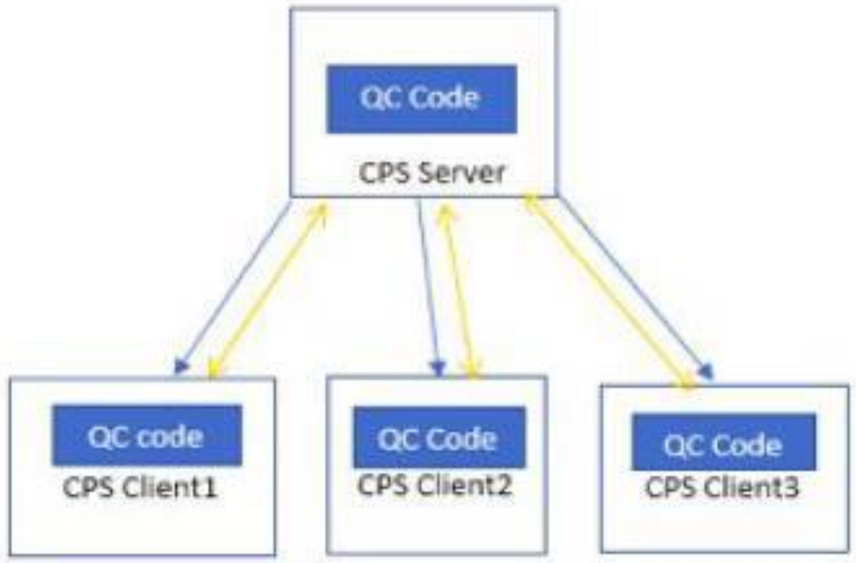
1. Confidentiality: This is described by the fact that information is transmitted in a confidential manner and is not made available in a useful form to everybody. Confidentiality in the project has been achieved by the use of encryption and decryption modules that make the information in an unreadable form and make is useless unless and until a key is found to decrypt it. It defines the very basic protection of data from intruders and acts as protection from data theft.
2. Integrity: Any system that ensures integrity of its data ensures that nobody without the required permissions can tamper or change the data. In our system, if a data breach occurs, some of the mechanisms included such as the tampering detector that will detect data breach and shut down system.
3. Availability: Data is available when it is smoothly accessed by the right individuals and is protected from unforeseen incidents. Data is made available to each and every deserving client by providing key value and sending through the data in an encrypted manner such that it cannot be tampered with while the communication happens.

METODOLOGY

In this project, we will apply Quantum cryptography on the Cyber-physical systems in order to make them more secure. Using Quantum Key Exchange, the keys can be exchanged over a network and connection can be secured. Since Cyber-Physical Systems require hardware implementation, in this project we will be proposing only a certain architecture. This architecture will explore how to provide security or how to create a secure communication channel for a Cyber-Physical System or between multiple systems.

Quantum Cryptography involves sending photons from where according to the spin or the configuration, the procedure is further carried on. This also cannot be practically carried out so instead of that, we will be including an algorithm for demonstration purposes. To illustrate the application of Quantum Cryptography on the Cyber-Physical System, firstly we will create an algorithm for Quantum Cryptography in python.

Next, for a dummy Cyber Physical System, which can either be one to one or one to many, we can create a client-server system. For one to one system, we can have one client and one server. Similarly, for one to many, one server and multiple clients. So, when the client(s) request the server for any data, it can be sent directly. But for the communication to be secure we will import the Quantum Cryptography code for the servers as well as the clients. Using the imported code, we will encrypt the data that the server is sending and decrypt it at the client end. Likewise, if the client wishes to send data to the server, the same encryption will be applied.



MODULES

1) Client Module:

Emulation of a CPS device that is to be connected to server and in network to other similar devices. Basically, a node in the network grid of multiple CPS devices communicating with server.

2) Server Module:

Responsible for supplying instructions (in real-time applications) to CPS devices. Here, the server will act as a hub for communication between the devices.

3) Encryption/Decryption Module:

Algorithm that will act as middle-ware between the server and client device (and vice-versa) and encrypt/decrypt outgoing/incoming messages with quantum algorithm.

IMPLEMENTATION

The implementation of the program has been done in a manner as to simulate the real life scenario where the cyber physical system's information may have been compromised and the algorithm needs to detect this and abort the operation.

Server/Sender Module:

```
#on sender's side the four orientations of the electron are vertical(v)
, horizon
#tal(h), 45 degrees left(l)and 45 degrees right(r)
#on receiver's side splitters being used are diagonal beamsplitter(lr)
and horiz
#ontal/vertical beamsplitter(vh)

from random import random

def get_key(sending_stream):
    key=''

    print("Enter bit value for each orientation: ")
    for_v=input('for vertical: ')
    for_h=input('for horizontal: ')
    for_l=input('for left diagonal: ')
    for_r=input('for right diagonal: ')

    for i in sending_stream:
        if(i=='v'):
            key+=for_v
        elif(i=='h'):
            key+=for_h
        elif(i=='l'):
            key+=for_l
        elif(i=='r'):
            key+=for_r
    return(key)

def create_key(key_size,c,orientations):
    sending_stream=''

    for i in range(0,key_size):
        random_number=int(random()*1000000)
        sending_choice=random_number%c
        sending_stream+=orientations[sending_choice]

    return(sending_stream)

orientations=['v','h','r','l']
splitter_type=['lr','vh']
lr=['l','r']
vh=['v','h']
splitters_used=''
received_key=''
Final_Key=''

key_size=500

#connecting to the cyber physical system
#final_key=get_key(received_key)
#print(final_key)

for i in range(0,key_size):
    if(sending_stream[i] in splitters_used[i:i+2]):
        Final_Key+=key[i]

key = Final_Key + "a"

print(key)
print(len(key))
def send_key():
    return(key)
```

```
print('The Key has been generated and now enter the text to be encrypted and decrypted later..\n\n')
```

Receiver/Client Module:

```
key = key[:-1]  #function only known to the reciever

print(key)
print(len(key))

if(key[len(key)-1] == 'a'):
  print('Key has been compromised!! Exiting')

msg=input('Enter message to be sent')
key=key[0:5*len(msg)]
list1=[]
newword=''
last=''
for i in range(0,len(key),5):
    b=0
    c=0
    k=key[i:5+i]
    while(b<len(k)):
        c+=int(k[b])*(2**(len(k)-b-1))
        list1.append(c)
        b=b+1
for i in range(len(msg)):
    msg=msg.upper()
    n2=ord(msg[i])
    newword+=chr(n2^list1[i])
print('Message after encryption : \n')
print(newword)
for i in range(len(newword)):
    last+=chr(ord(newword[i])^list1[i])
print("Now on the reciever's side\n")
done = False
t = threading.Thread(target=animate)
t.start()

#long process here
time.sleep(10)
done = True
print('Message after decryption : ')
print(last)
```

Encrypt Module:

```
msg=input('Enter message to be sent')
key=key[0:5*len(msg)]
list1=[]
newword=''
last=''
for i in range(0,len(key),5):
    b=0
    c=0
    k=key[i:5+i]
    while(b<len(k)):
        c+=int(k[b])*(2**(len(k)-b-1))
        list1.append(c)
        b=b+1
for i in range(len(msg)):
    msg=msg.upper()
    n2=ord(msg[i])
    newword+=chr(n2^list1[i])
```

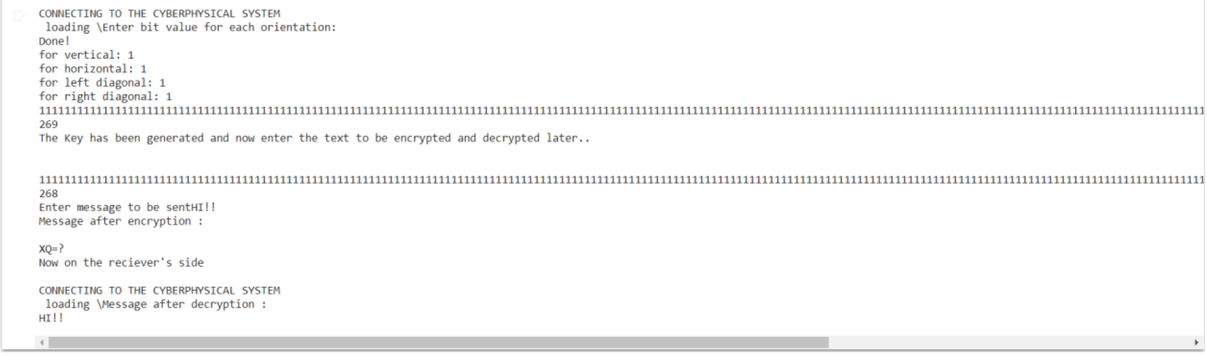
Decrypt Module:

```
for i in range(len(newword)):
    last+=chr(ord(newword[i])^list1[i])
print("Now on the reciever's side\n")
done = False
t = threading.Thread(target=animate)
t.start()

#long process here
time.sleep(10)
done = True
print('Message after decryption : ')
print(last)
```

OUTPUT

1) Encryption and Decryption



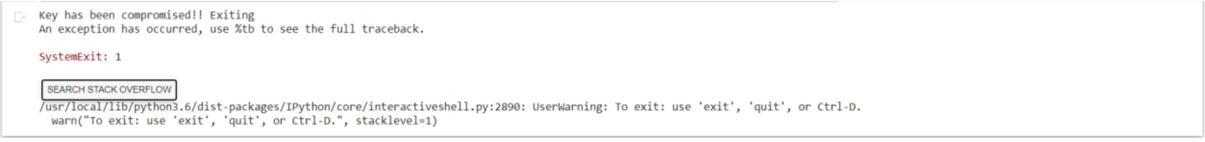
```
CONNECTING TO THE CYBERPHYSICAL SYSTEM
 loading \Enter bit value for each orientation:
Done!
for vertical: 1
for horizontal: 1
for left diagonal: 1
for right diagonal: 1
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
269
The Key has been generated and now enter the text to be encrypted and decrypted later..


1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
268
Enter message to be sentHI!!
Message after encryption :

XQ=?
Now on the reciever's side

CONNECTING TO THE CYBERPHYSICAL SYSTEM
 loading \Message after decryption :
HI!!
```

2) Intruder attack



```
Key has been compromised!! Exiting
An exception has occurred, use %tb to see the full traceback.

SystemExit: 1
```

```
/usr/local/lib/python3.6/dist-packages/IPython/core/interactiveshell.py:2890: UserWarning: To exit: use 'exit', 'quit', or Ctrl-D.
  warn("To exit: use 'exit', 'quit', or Ctrl-D.", stacklevel=1)
```

CONCLUSION

CPS is an important driver of major industries such as aero-space, defence and medical. This project aims to and is successful in finding and implementing a way to protect and secure data transfer to and from the CPS. This is made possible by application of Quantum Cryptography. The project asserts these results from a simulation of a client server system where the data transfer between the two parties is encrypted by Quantum Cryptography algorithm. Finally, the results of simulation are found to be applicable to all scales of CPSs and in many other applications as well.

REFERENCES

Journals :

[1] Edward A. Lee, “Cyber Physical Systems: Design Challenges”, Electrical Engineering and Computer Sciences University of California at Berkeley, January 23, 2008
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.156.9348&rep=rep1&type=pdf

[2] Ragunathan (Raj) Rajkumar, Insup Lee, Lui Sha, John Stankovic, “Cyber-Physical Systems: The Next Computing Revolution”
https://dl.acm.org/doi/pdf/10.1145/1837274.1837461

[3] Jay Lee, Hung-An Kao, Behrad Bagheri, “ A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems”, December 2014
https://www.researchgate.net/profile/Jay_Lee10/publication/269709304_A_Cyber-Physical_Systems_architecture_for_Industry_40based_manufacturing_systems/links/59e4f5670f7e9b0e1aa8805f/A-Cyber-Physical-Systems-architecture-for-Industry-40-based manufacturing-systems.pdf

[4] Radhakisan Baheti, Helen Gill, “Cyber- Physical systems”, The Impact of Control Technology, T. Samad and A.M. Annaswamy (eds.), 2011.
https://www.researchgate.net/profile/Mohamed_Mourad_Lafifi/post/What_is_the_difference_between_Cyber_Physical_Systems_and_Networked_Control_Systems/attachment/59d6407379197b807799caa6/AS:431158354812928@1479807570298/download/IoCT-Part3-02CyberphysicalSystems.pdf

[5] Fabio Pasqualetti, “Attack Detection and Identification in Cyber-Physical Systems”, November 2013
http://www.fabiopas.it/papers/FP-FD-FB-12a.pdf

[6] Alvaro A. Cardenas, Saurabh Amin, Shankar Sastry, “Secure Control: Towards Survivable Cyber-Physical Systems”, University of California, Berkeley
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.475.8230&rep=rep1&type

[7] Nicolas Gisin, Gregoire Ribordy, Wolfgang Tittel, Hugo Zbinden, “Quantum cryptography”,University of Geneva, February 1, 2008.
https://arxiv.org/pdf/quant-ph/0101098.pdf

[8] Charles H. Bennett, Francois Bessette, Gilles Brassard, Louis Salvail, John Smolin, “Experimental Quantum Cryptography”, 1992.
https://eclass.uoa.gr/modules/document/file.php/PHYS253/Bennett1992_Article_Exp

erimentalQuantumCryptograph.pdf

[9] Charles H. Bennett, Gilles Brassard, “QUANTUM CRYPTOGRAPHY: PUBLIC KEY DISTRIBUTION AND COIN TOSSING “, 1984
https://arxiv.org/ftp/arxiv/papers/2003/2003.06557.pdf

[10] Thomas Jennewein, Christoph Simon, Gregor Weihs, Harald Weinfurter †, and Anton Zeilinger ,”Quantum Cryptography with Entangled Photons”, Universit¨at M¨unchen, Schellingstr, February 1, 2008
https://arxiv.org/pdf/quant-ph/9912117.pdf

[11] Dominic Mayers, “Unconditional Security in Quantum Cryptography”, NEC Research Institute, Princeton, New Jersey, May 2001.
https://dl.acm.org/doi/pdf/10.1145/382780.382781

[12] John J. Glover, “ONE-TIME PAD ENCRYPTION KEY DISTRIBUTION”, July 21, 2000
https://patentimages.storage.googleapis.com/78/e1/e7/b67853b4b3d2cb/US6868495.pdf

[13] Adam Shefi, Ramat Gan, “SYSTEM AND METHOD FOR SYNCHRONIZING ONE TIME PAD ENCRYPTION KEYS FOR SECURE COMMUNICATION AND ACCESS CONTROL “, May 11, 1999.
https://patentimages.storage.googleapis.com/fc/bb/e3/7f190ea8d7b119/US6266413.pdf

[14] Kim-Kwang Raymond Choo, “Emerging Embedded and Cyber Physical System Security Challenges and Innovations”, IEEE, May/June 2017.
https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7926472

[15] Melih Soner Celiktas, Engin Deniz, “ Overview of Cyber Physical Systems In Future Production”, Ege University, September 2015.
https://www.researchgate.net/publication/282242701