CRYPTOGRAPHY

A DISSERTATION

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE AWARD OF DEGREE

OF

MASTER OF SCIENCE

IN

APPLIED MATHEMATICS

Submitted By:

JOSHUA NAHUM GIDEON

(2K21/MSCMAT/24)

Under the Supervision of:

Dr. Dhirendra Kumar

DEPARTMENT OF APPLIED MATHEMATICS

DELHI TECHNOLOGICAL UNIVERSITY

(Formerly Delhi College of Engineering)

Bawana Road, Delhi – 110042.

MAY, 2023

CANDIDATE'S DECLARATION

I, JOSHUA NAHUM GIDEON (2K21/MSCMAT/24) of M.Sc. (MATHEMATICS), hereby declare that the project Dissertation titled "CRYPTOGRAPHY" which is submitted by Me to the Department of APPLIED MATHEMATICS, DELHI TECHNOLOGICAL UNIVERSITY, DELHI in partial fulfillment of the requirement for the award of the degree of Master of Science, is original and not copied from any source without project citation. This work has not previously formed the basis for the award of any Degree, Diploma Associateship, Fellowship or other similar title or recognition.

Place: DELHI **JOSHUA NAHUM GIDEON**
Date: **(2K21/MSCMAT/24)**

DEPARTMENT OF APPLIED MATHEMATICS

DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi – 110042.

CERTIFICATE

I hereby certify that the Project Dissertation titled "CRYPTOGRAPHY" which is submitted by JOSHUA NAHUM GIDEON (2K21/MSCMAT/24) of APPLIED MATHEMATICS, DELHI TECHNOLOGICAL UNIVERSITY, DELHI in partial fulfillment of the requirement for the award of the degree of Master of Science, is a record of the project work carried out by the students under my supervision. To the best of my knowledge this work has not been submitted in part or full for any Degree or Diploma to this University or elsewhere.

Place: DELHI **Dr. Dhirendra Kumar**
Date: **(SUPERVISOR)**

Assistant Professor
DELHI TECHNOLOGICAL UNIVERSITY

ACKNOWLEDGEMENT

I want to express My Appreciation to **Dr. Dhirendra Kumar**, Assistant Professor, Department of Applied MATHEMATICS, **DELHI TECHNOLOGICAL UNIVERSITY**, for his careful and knowledgeable guidance, constructive critism, patience hearing and kind demeanor throughout our ordeal of the present report. I will always be appreciative of his kind, helpful demeanor and his insightful advice, which served as a catalyst for the effective completion of My Project.

Biocryptography
The Future of User Authentication?

Abstract

Traditional cryptography requires shared information for authentication, typically in the form of a secret token or password. These password authentication schemes are widely used in today's wired society, but they have a number of fundamental flaws, the most important of which is their inability to discriminate between legitimate users and hackers using stolen credentials. Biometric solutions address these issues by using bodily traits to distinguish legitimate users from imposters. These systems do, however, have a special set of weaknesses.

The study of cryptographic techniques for safeguarding biometric systems is known as biocryptography, and it sits at the nexus of biometrics and conventional cryptography. This study investigates cutting-edge biocryptographical techniques to develop systems that are accurate and resistant to intrusions.

1. Introduction

Traditional cryptography requires shared information for authentication, typically in the form of a secret token or password. These password authentication schemes are widely used in today's wired society, but they have a number of fundamental flaws, the most important of which is their inability to discriminate between legitimate users and hackers using stolen credentials. Users are also need to keep track of several accounts with different passwords.

Biometric solutions address these issues by employing features such as fingerprints, irises, and even the shape of the ear to distinguish legitimate users from imposters. These systems do, however, have a special set of weaknesses, such as what happens if a user's biometric information is stolen. A fingerprint cannot readily be changed, unlike a password. Bio cryptography, the study of specialised cryptographic techniques for safeguarding biometrics systems, lies at the interface between biometrics and conventional cryptography. This study examines cutting-edge biocryptography techniques to develop systems that accurately identify real users and are resistant to conventional biometric attacks.

2. To the Community

A 2012 survey on online registration and passwords by Janrain found that 30% of people had more than ten different passwords they need to remember, and 58 percent of adults have at least one unique password for each online login. Additionally, 2 out of 5 people (37%) at least once a month need help with their user name or password

The current models for user authentication have resulted in a ridiculous situation: on the one hand, experts advise us to use lengthy, random, and unique passwords to make them difficult to crack; on the other hand, we must create, keep track of, and occasionally change credentials for each service we sign up for. According to anecdotal evidence, most people put convenience ahead of security and frequently use (and reuse) weak passwords. The fact that the organisations we rely on to protect our credentials are not safe themselves makes the situation worse; in fact, it seems

like we are hearing about significant security breaches more frequently lately (like those at LinkedIn, Target, and Sony). Hackers obtained access to 6.5 million user credentials from the LinkedIn breach on June 5, 2012 alone. More than 60% of the unique passwords had been decrypted and made public by the next day. My own dissatisfaction with how user authentication systems are currently implemented served as the primary inspiration for this project. It is incredibly frustrating that the user is required to manage and secure her own credentials to such an extent. Therefore, this study investigates biometric systems and the biocrytographic techniques employed to protect them as an alternative to a password-based authentication system. I was interested in learning if biometric systems are actually feasible and, if so, how feasible they would be how they would differ from the present systems used for traditional authentication.

3. Cryptography

The fundamental goal of cryptography is to let two parties to communicate safely and confidentially with one another when a third person, or adversary, is present. Data encryption is used to do this, rendering the communication unintelligible to those who lack the necessary decryption skills. An initial message in plaintext is typically converted into a jumbled, unintelligible message, or in crypto-text, using an encryption technique and a cryptographic key.

3.1 Algorithms for Encryption

There are two primary types of encryption algorithms used in modern cryptography: symmetric, or private-key encryption, and asymmetric, or public-key encryption. The same cryptographic key and technique are used by symmetric-key encryption methods the process of converting plaintext into cyphertext and then back into plaintext. The Data Encryption Standard (DES) is one of the symmetric-key algorithms that is most frequently employed. In asymmetric-key systems, a public key for encryption and a private key for decryption are jointly established. The public key, as its name implies, is distributed widely and can be used by another person to encrypt data before sending it to you. Only the private key, which you keep private, can be used to decrypt data encrypted with this public key. The RSA algorithm, so called because developers Rivest, Shamir, and Adleman, is a popular symmetric-key algorithm.

4. Authentication Systems

The four primary objectives of contemporary cryptography are as follows: Confidentiality, data integrity, non-repudiation, and authentication are listed in that order [Xi and Hu, 2010]. The final objective, authentication, is concerned with confirming identity claims. It should be possible for sender and receiver to confirm one other's identities and the message's source when sending a message. Authentication is different from authorization, which is the process of providing a party access to a system or data based on the verification of their identity. A user's identity is verified in knowledge-based authentication systems using some sort of piece of information, such as a password, passphrase, or personal identification number (PIN). However, this approach has a number of drawbacks:

Passwords and PINs can be guessed through social engineering, as was shown above. 1) Knowledge like passwords and PINs can be quickly forgotten.

3) Wordlist or brute-force assaults can readily crack even encrypted passwords. 4) Plaintext passwords and PINs are simple to share and disseminate, and 5) A system relying on passwords cannot tell the difference between a legitimate the attacker and the user using stolen or counterfeit credentials.

4.1 Biometric Authentication Systems

In biometric systems, authentication is based on a person's physiological or behavioural traits rather than a shared secret or key. Angerprints, irises, or even ear shape can be used to identify genuine users [Xi and Hu, 2010].

Biometric systems typically consist of two distinct components. A biometric sensor, such as a fingerprint reader, reads the biometric data and typically performs some quality control on the sample. This raw biometric data is consumed by the feature ex- tractor, which then extracts an appropriate feature set (or template) to represent the data. These characteristics would include minute particulars that define a ngerprint system. The matcher, also known as the matching model, compares this sample template to a previously saved template and generates a score, indicating how well the sample matches the previously stored template. And last, it's typical for systems to keep known templates in a database.

Biometric systems have the potential to be more dependable than traditional password-based systems since biometric features cannot be lost or forgotten and are challenging to imitate, fabricate, exchange, or distribute. However, they come with their own set of problems, such as those with accuracy (false positive and negative matches), security (because, unlike a password, stolen biometric data cannot be replaced), and privacy. Additionally, biometric systems have their own unique set of weaknesses; they are not immune to attack.

4.2 Biometric System Attacks

According to Ratha et al., there are eight different categories that can be used to categorize the attack vectors that are specific to biometric systems.

1. phone biometric: An attacker impersonates a biometric, such as a phone fingerprint
2. Replay attack: The attacker plays back a previously captured signal, for as by showing the system an outdated version of a fingerprint image.
3. By inserting a Trojan horse inside the feature extractor, the attacker can override it and force it to produce the feature set that the attack chose.
4. Override matcher: The attacker tricks the matcher into faking higher or lower match rates.
5. Change the feature representation: The attacker substitutes the retrieved feature set with a different, synthesized one.
6. Modification of stored templates: An attacker modifies a template to provide someone a false authorization by altering the database that contains the templates.

Attack tampers with the templates as they are being transported from the storage database to the matcher through the attack's communication channel.

8. Overriding the choice: The recognition system performs as predicted, but the attacker modifies the final authentication decision.

5. Biocryptographic Methods and Applications

Xi and Hu assert that among the assaults against biometric systems, those targeting templates have the potential to be the most damaging and difficult to identify. 2010's [Xi and Hu] Therefore, biometric templates must always be encrypted both during storage and during matching for a system to be secure. Traditional approaches that use non-smooth functions, such DES and RSA, cannot be used for encryption because of the properties of biometric data [Fengling Han, 2007]. For instance, even minor changes in a feature set obtained from a ngerprint will result in dramatically different encrypted feature sets, making it difficult to perform feature matching with encrypted templates.

5.1. Template Encryption

A secret key, KE, and an encryption method, E, are typically used to encrypt a template, T, so that the encrypted form, C, is given by: C = E (T, KE).
Then, to decrypt, we use the formula T = D (C, KD), which applies a decryption method, D to C, and a decryption key, KD, to recover the template.
Key binding is a biocryptographic method in which the secret key and the biometric information (i.e., the template) are coupled to create an artefact that conceals both the template and the key. Since it is computationally impossible to directly decrypt the artefact, it can then be disseminated openly [Xi and Hu, 2010].

5.1.1 Fingerprint Fuzzy Vault

The fuzzy vault algorithm is a key-binding design suggested by Juels and Sudan [Juels and Sudan, 2006]. The fact that this technique is error-tolerant and order-invariant makes it particularly suitable for use with biometric data. In other words, as long as there is a certain amount of overlap between the sets, data can be encoded using one set of values (such as a biometric feature set) and then unlocked using an other set of values. It doesn't matter which of the sets is used for locking and which is used for unlocking because of order invariance. Given a secret key and a template (i.e., feature set), the basic method operates as follows: first, encode the key as the coecients of a polynomial function, p(x). To create a set of points that accurately depicts the polynomial, apply p(x) to each value in the feature set. Create a "cha" set of points next, which are inside the domain and range but do not lie on the polynomial, to mask the template data. The final collection of points is the "fuzzy vault" and it is created by combining the two sets and rearranging the order. Utilise the user-provided feature set to unlock the fuzzy vault. The polynomial can be rebuilt and the secret key exposed if sufficient numbers of the points within a specific mistake match the set used to encode the data [Xi and Hu, 2010, Juels and Sudan, 2006].
As a proof of concept, I created a straightforward "biometric" authentication system that encrypts identity/fingerprint pairings using the fuzzy vault algorithm.

6. Conclusion

Although widely used, password-based authentication methods are problematic because users must manage numerous sets of credentials, which encourages the use of weak, easily cracked passwords. A password-based system also is unable to discriminate between a legitimate user and an attacker using credentials that have been stolen. Biometric systems, which employ physiological traits to identify authentic users just once, offer a solution to these issues but are not without their own set of difficulties and risks. The field of biocryptography investigates specialised cryptographic approaches for safeguarding biometric systems because many conventional cryptographic techniques are inappropriate for biometric data.

References

[buf,] Fuzzy vault. https://wiki.cse.buffalo.edu/cse545/content/

fuzzy-vault.

[Das, 2013] Das, R. (2013). An Introduction to Biocryptography.

http://www.nationalhomelandsecurityknowledgebase.com/cln/

news/2013/11221.aspx.

[Das, 2014] Das, R. (2014). Biometric Technology: Authentication, Biocryp-

tography, and Cloud-Based Architecture. CRC Press.

[Fengling Han, 2007] Fengling Han, Jiankun Hu, X. Y. Y. W. (2007). Fin-

gerprint images encryption via multi-scroll chaotic attractors. Applied

Mathematics and Computation.

[Janrain, 2012] Janrain (2012). Online Americans Fa-

tigued by Password Overload Janrain Study Finds.

http://janrain.com/about/newsroom/press-releases/

online-americans-fatigued-by-password-overload-janrain-study-finds/.

[Juels and Sudan, 2006] Juels, A. and Sudan, M. (2006). A fuzzy vault

scheme. Des. Codes Cryptography, 38(2):237{257.

[Ratha et al., 2001] Ratha, N. K., Connell, J. H., and Bolle, R. M. (2001).

An analysis of minutiae matching strength. In Proc. 3rd AVBPA, pages

223{228.

[Vijayan, 2012] Vijayan, J. (2012). Hackers crack more
than 60% of breached LinkedIn passwords. http://www.
computerworld.com/article/2504078/cybercrime-hacking/
hackers-crack-more-than-60--of-breached-linkedin-passwords.
html.

[Xi and Hu, 2010] Xi, K. and Hu, J. (2010). Bio-cryptography. In Handbook
of Information and Communication Security, pages 129-157.

DNA Cryptography

Keywords: DNA Biological conundrum, algorithm, DNA chip, cryptography.

Abstract.

Applying DNA computing to the subject of DNA cryptography still faces several theoretical and practical challenges. The most popular DNA cryptography methods in use today combine conventional encryption with DNA technology, whose practicality has not yet been fully proved. We chose the biological conundrum that "DNA sequencing is difficult under the conditions of not knowing the correct sequencing primers and probes" through research and analysis. We create a fresh DNA-based cryptography algorithm biological technology and DNA chips. The method's viability and safety are verified through simulation, which is offered. The findings demonstrate that this technology, while ensuring viability, provides higher security compared to conventional encryption techniques.

Introduction

A ground-breaking academic study area called DNA computing has recently emerged. It includes a novel calculating technique in which a biological DNA molecule serves as the calculation medium and biochemical reactions serve as the calculation means. DNA computing has the following benefits over current computer technology: a high level of parallelism, minimal energy consumption, and a significant storage capacity for information. These features give DNA encryption a distinct edge in applications such as data encryption in huge parallel with reduced real-time demand, information, digital signatures, and safe data storage concealment, etc. Along with the study field of DNA computing, a new branch of cryptography called DNA cryptography [1] has evolved recently. The DNA code's information carrier is a DNA molecule, and contemporary biotechnologies provide the means of implementation. It completes cryptographic operations including encryption, authentication, and signatures by fully using the DNA computing and DNA cryptography's inherent high storage density and high parallelism advantages.

Associated Technologies and Complex Biological Issues

Two distinct encryption techniques based on a DNA binary string were introduced by Andre' L, et al. [1]. The techniques are applied under specific presumptions. The method's viability is constrained, but it can provide a guide for further research.

Sivan S. et al.'s [2] use of the molecular automaton and DNA chip allows for picture encryption. The system described in this study has the advantages of utilising molecular automaton techniques and DNA chip technology, but it also has several drawbacks, including the fact that it can only be used for image encryption and that its operational viability has not been thoroughly proven. However, the authors' findings suggest that we can investigate and examine DNA

encryption techniques in greater detail. In paper[5], The authors suggested an encryption approach by fusing challenging biological issues with traditional cryptography theory. A doubly secure version is provided by challenging biological problems and computer challenges in encryption. The method has a high level of security strength, as demonstrated by the validation studies. Luming X,et. al,[6] used computational complexity theory of cryptography in conjunction with Technologies for DNA synthesis, DNA cloning, PCR amplification, and DNA chips to propose a biotechnology-based encryption approach. Without the necessary decryption keys, Decrypting the plaintext that has been encrypted using this is challenging approach, which ensures the method's security due to the limitations of current biological and computational capabilities.

Designing PCR primers and DNA coding

Encoding DNA

The three primary types of DNA encoding techniques are as follows:

1) The 10, 01, 11, and 00 are represented, respectively, by A, T, G, and C, in a base representing two binary digits;[5]

2) Depicting 0 and 1 using two DNA short chain molecules, respectively;[2]

3) DNA encoding as quaternary, where a letter or number is represented by three nucleotides.[7] We opt for the first encoding method, which uses the letters A/T/G/C to represent two binary values, or 0123/CTAG, respectively, stand in for 10/01/11/00.

Primer PCR

Currently, Oligo 6.0, Primer premier 4.11, and other programmes are used often for primer design. Using the Oligo Analyzer programme, we created the proper primers for this study based on the template DNA strand. The DNA vector's DNA fragments are each placed in a separate place. In order to discover the appropriate DNA fragments for decryption, We initially amplify the lengthy strands of DNA using PCR. using the chosen primer. Long DNA chain with (P1, P2, P3).

Because the original DNA template has a significant impact on primer design and the characteristics of the DNA sequences converted from plaintext through a series of steps have difficulty meeting the PCR primer design principles, the designed encryption method adds a pair of encryption keys at the beginning and end of each DNA sequence. The encryption key pairs are chosen based on the DNA sequences that match the PCR primers that can be utilised for amplification. By doing this, we can prevent a situation where the DNA sequences obtained from the encrypted plaintext cannot be used to create PCR primers. The additional outcome of this is that the decryption key and the encryption key are compatible. For the encryption procedure, There are three necessary pairs of encryption keys (si, ei), where i = 1, 2, and 3. Twenty characters make up the encryption key.The start and end of each DNA segment include the matching encryption keys. Using the Oligo Analyzer application, matching primers for the encryption keys can be created. The DNA sequences that can be utilised to create the proper PCR primers and perform PCR

amplification in a biological laboratory can be used to obtain the encryption keys. The DNA segments are shown in Fig. 1 after having appropriate encryption key pairs inserted to both ends.

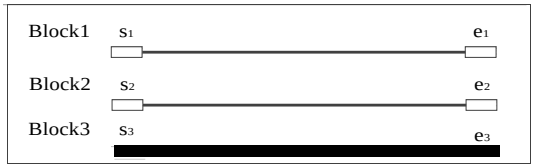


Fig 1.The schematic of DNA fragments after adding corresponding encryption primers at both ends

According to the designed encryption primer pairs (s_i, e_i), using the Oligo Analyzer to design corresponding decrypt primers (decode_s_i, decode_e_i), i=1,2,3.The schematic diagram of the combination of PCR primers and the template is shown in Fig 2.

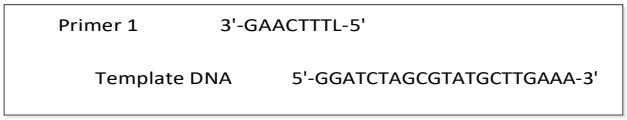


Fig 2. The illustration of the PCR primers and template combination

In Fig. 3, a long DNA chain with the appropriate DNA pieces is depicted schematically.

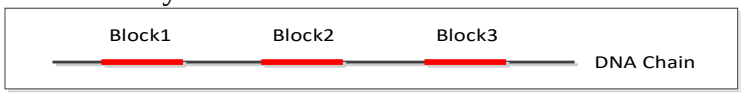


Fig 3. the conceptual representation of the long DNA chain containing the desired DNA pieces

Based on the generation of biological puzzle keys, the DNA Encryption Method

In this situation, all of the decryption keys can be used to generate signals that meet specified criteria and hybridise with the encryption keys used to produce DNA chips. When the hybridization signals mix the decryption keys with other encryption keys. can be created. All encryption keys produce the same hybridization signals when they mix with different decoding keys. The approach is a form of asymmetric encryption because the encryption keys and the decryption keys are different. The complementary sequence of each encryption key is contained in the decryption key in this instance.

There are many possible probes in both encryption and decryption keys. These probes are often classified into two types: probe 0 and probe 1. One type of probe is placed on the position where the value is 1, and another type is placed on the spot where 0 is the value, we place one type of probe. for the simple binary matrix. We can create the desired DNA chips in this method. By employing the decryption key to hybridise with the DNA microarray, the receiving party is able to get the plaintext. The contrasting order of each 0 and 1 probe in the encryption keys is contained in the decryption keys. A category of meaningless information, a category of probes

that corresponds to the two different types of bases, and a category of probes are used to categorise both the encryption and decryption keys in this study. It is necessary to create two DNA chips because the plaintext is split into two matrices, and these two DNA chips correspond two separate encryption and decryption keys. For a matrix made out of the nucleotide bases A and C, we need three different kinds of keys. Probe_A, Probe_T, and Probe_ATK are the three probes (ATK indicates the position of the nucleotide base, not both A and T). Among all encryption keys, one type of probe A and one type of probe T are both put in the nucleotide base A position and location, respectively. The regions without any information have one sort of ATK probe added in the middle of all the encryption keys. This is how we can make a DNA chip. We additionally require three extra types of keys: probe_C, probe_G, and probe_CGK for a matrix composed of the nucleotide bases C and G. CGK refers to the region of a nucleotide base that is neither A nor T. For the nucleotide base C position and the nucleotide base G position, each encryption key uses a specific kind of probe_C and a specific type of probe_G. In the areas with no data, one type of probe_CGK is spread among all encryption keys. In this way, we can produce another DNA chip. The receiver can get the plaintext by using the DNA microarray along with the decryption keys. If the encrypted ciphertext consists of a mixture rather than DNA chips, the DNA probe that corresponds to each bit of the plaintext binary matrix must be placed in the test tube. Because you are unaware of the hybridization signal intensity of each bit, each DNA probe must therefore correspond to a distinct bit of the matrix. If the cypher text is a DNA chip, the probe on each bit can be the same. The text that we encrypt in the paper is stored on a DNA chip. A DNA chip is the text that we encrypt in the paper. In order to completely use the DNA's plentiful resources and increase the critical space, each probe that is positioned on the chip is distinct. It is possible to use all of the stable substances present in biological materials as encryption keys, including DNA, PNA [8], and protein. The only difference is the various experimental approaches.

Encryption Method

1) Fig. 4 depicts the flowchart for the method's encryption procedure. 1) The binary sequence (N bits) from the plain text is converted before being processed in the subsequent steps. (1) Find the DNA sequence Q in the online gene pool and mark its path as Path_ Q; (2) (3) Separate the binary streams of plaintext and the one derived from the DNA sequence Q into 8-bit chunks. From the DNA sequence Q, generate the binary stream Q2. We execute an XOR operation between the binary sequence created if the number of 1 in the binary sequence is odd, given the correct DNA sequence Q and the 8-bit plaintext binary sequence. In all other cases, the binary sequence created from the appropriate DNA sequence Q is combined with the 8-bit plaintext binary sequence using the XOR approach. Alternately, we can find a DNA sequence X in the online gene pool that contains N/16 or (N + 1)/16 nucleotides, and then we can track X's path through the online gene pool using the name Path_X. The binary sequence X2 is then created by converting X into an 8-bit binary block for each bit in the original sequence. XO If one bit's value is 1, then Q is completed. If not, then the appropriate 8-bit plaintext binary sequence should be rung with the binary sequence produced from the matching DNA sequence. The appropriate 8-bit plaintext binary sequence is then XO Red, Additionally, the related DNA sequence Q was used to generate the complement binary stream of binary sequence. It functions precisely like plaintext stream encryption.

2) The DNA sequence from step one is designated as W, and it is subsequently divided into n segments with lengths of N/n each. These n fragments of the DNA sequence go by the labels P1, P2,..., Pn. In order to prepare the sequence Pi, where i=1, 2,..., n, for the creation of primers for PCR amplification, si and ei are added to both ends. Each of the new sequences is then placed into a challenging area of the bio-genetic DNA. The vector DNA can be chosen using either the network's gene pool or the biological experiments section. The subsequent block-encryption of each DNA fragment creates new DNA blocks S1, S2,..., Sn. Then, a long DNA strand is created by rearranging and connecting these DNA building blocks.

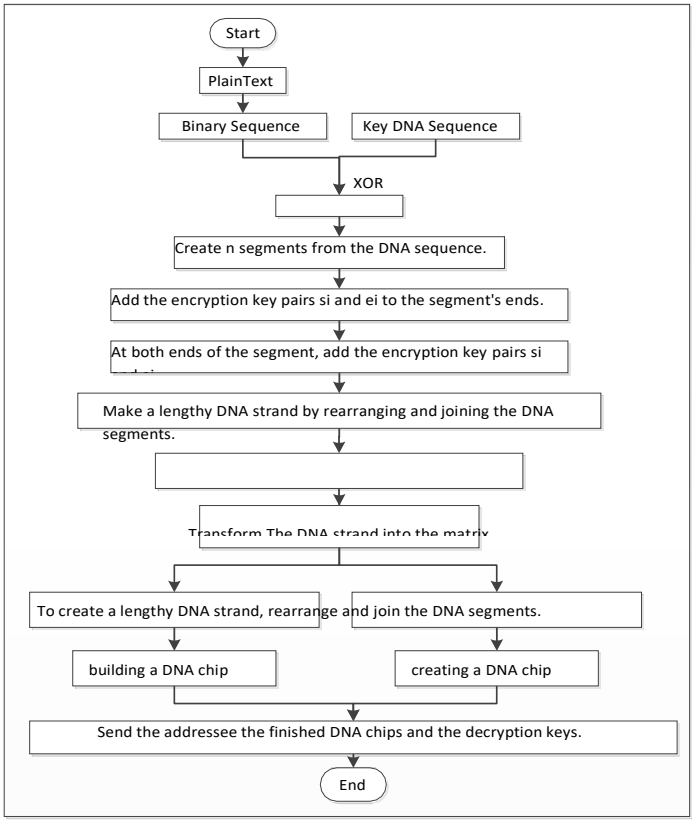


Fig 4. Flowchart for encryption

1) 3 The lengthy DNA The strand from step two is transformed into the matrix form (p*q) in accordance with a preset compositional arrangement. The matrix form is then encrypted using the newly developed encryption algorithm to produce the cypher text. The matrix is initially split into two separate matrices, one of which only contains the letters A and T and the other of which only contains the letters G and C. Then, for each point on the encryption DNA chip, we produce two distinct DNA sequences—two different sequences for A and T for the matrix that only contains A and T, and two different sequences for C and G for the matrix that only contains Using the two distinct DNA sequence keys produced in step 3, C and G create a DNA chip. The DNA chip size in this instance is p*2q. The matrix with just the characters A and T is represented by the left side of the p*q matrix. C and G use the two distinct DNA sequence keys that were produced in step 3 to create a DNA chip. The DNA chip in this instance is p*2q in size. The matrix that just has A and T is shown on the left side of the p*q matrix. We choose the DNA sequence that corresponds to base position A on the DNA chip and put it there as the DNA

probe. The DNA probe corresponding to that base is chosen and inserted into the appropriate location on the DNA chip if the nucleotide at that location on the chip is T.

Simulation

Using VC ++ 6.0, the cryptography technique is simulated in this study. We practise encrypting and decrypting data. The decryption was successful because the recovered plaintext matched the original data exactly.

Conclusions

Here, we describe a unique encryption technique that fully exploits the benefits of the biological riddle. Two major contributions are made by this study: (1) an analysis of the viability of developing a fresh approach to encryption based on the biological riddle, which provides a theoretical underpinning for the safety and viability of the suggested approach; and (2) a fresh approach to DNA cryptography based on DNA chip technology and the biological conundrum.

Through this research, we have created a helpful cryptography system, and the simulation results demonstrate its viability and security. This algorithm can serve as a guide for future work on DNA encryption techniques.

References

[1] Jiang J, Yin Z. The Advantages and Disadvantages of DNA Password in the Contrast to the Traditional Cryptography and Quantum Cryptography[C],the Eighth International Conference on Bio-Inspired Computing: Theories and Applications (BIC-TA), 2013. Springer Berlin Heidelberg, 2013:307-316.

[2] Andre´ L, Christoph R, Wolfgang B, Hilmar R. Cryptography with DNA binary strands [J].BIOSYSTEMS,2000,57(1): 13-22.

[3] Sivan S, Ron P, Yoav A, Ehud K. A Molecular Cryptosystem for Images by DNA Computing [J]. AngewandteChemie, 2012, 124(12): 2937-2941.

[4] Zhang Z, Shi X, Liu J. A method to encrypt information with DNA computing[C]// Bio-Inspired Computing: Theories and Applications, 2008. BICTA 2008. 3rd International Conference on. IEEE, 2008:155-160.

[5] Guangzhao C, LiminQ, YanfengW. An Encryption Scheme Using DNA Technology[J]. 3rd International Conference on Bio-Inspired Computing - Theories and Applications,2008:37-41

[6] Xin L M, Yuan C, Lei Q, et al. An encryption scheme based on DNA [J]. Journal of Xidian University, 2006, 33(6):939-942.

[7] Morford L. A theoretical application of selectable markers in bacterial episomes for a DNA cryptosystem[J]. Journal of Theoretical Biology, 2011, 273(1): 100-102.

Nielsen P E, Egholm M, Berg R H, et al. Sequence-selective recognition of DNA by strand displacement with a thymine-substituted polyamide[J]. Science, 1991, 254(5037): 1497-1500

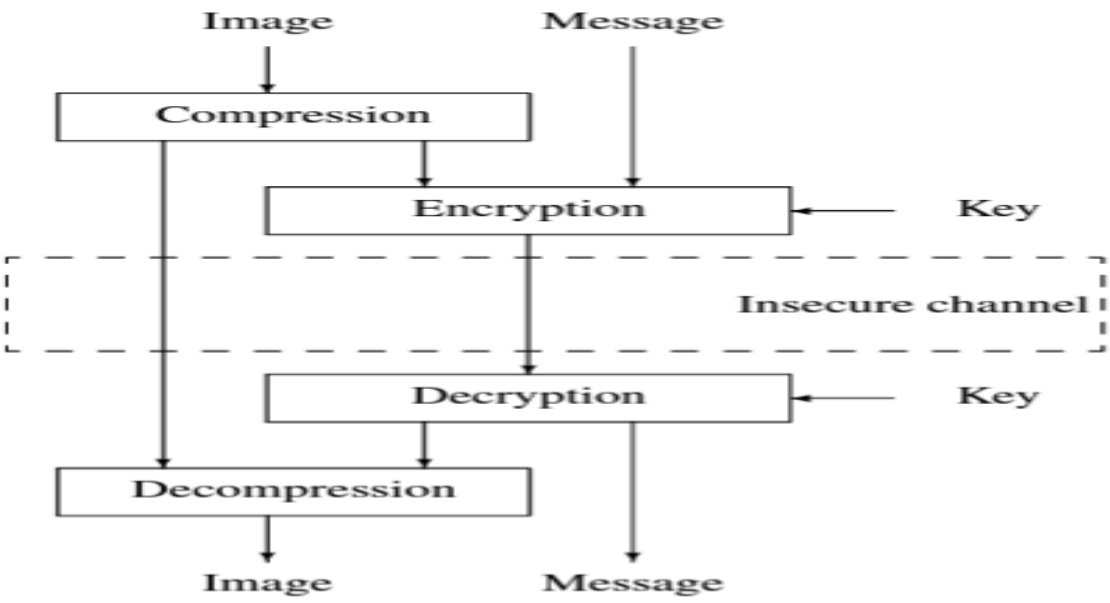
ENCRYPTION OF IMAGES IN PART FOR REAL-TIME USE

ABSTRACT

Most multimedia systems build their security on limiting access to services. This paradigm has a number of limitations when used in real-time imaging applications. Applications become open to password attacks, and if they are revealed, attackers can access every piece of information. The systematic encoding of every data is an alternative. This approach is problematic when working with photos because the data must be processed thoroughly before users can obtain any insight. Decryption demands a lot of computing power as well. With less overhead than complete encryption, this presentation demonstrates how partial encryption can satisfy application needs. The paper analyses a number of techniques combining picture encoding and encryption first. Then, we concentrate on a method that uses JPEG-based images to partially encrypt data. The method aims to satisfy two crucial requirements: maintaining the overall bit rate and maintaining compliance with the JPEG file format. As our final project, we propose and develop a news scheme that combines flexibility, multiple encryption, spatial selectivity, self-sufficiency, and format compliance. We provide examples of how it might satisfy the needs of real-time applications.

1. INTRODUCTION

When a communication enters an insecure channel, it should be standard procedure to conceal its content. Unfortunately, there is no way to convert a portion of the bit stream into cypher text before transmission in any of the audio-visual compression standards. An encryption algorithm and a key are needed for the encryption process. Decryption is the technique used to extract plaintext from encrypted data. Most cryptographers concur that the key should be kept private while the encryption method should be made public (KERKHOFF's law). It can be difficult to distribute keys in practise because they should only be exchanged after a rusted channel has been made. Speed, compression efficiency, and adaptability are additional concerns for real-time video systems that need to be addressed. Speed is dependent on both the processing type of the information and the encryption algorithm. Since compression and encryption are both presumed to be inevitable, there are practically only two options for real-time video transmission, depending on whether compression whether it does or not. First-pass compression lowers the bit stream but provides less confidentiality. However, compression is useless if encryption is applied first. Thankfully, there is a different option termed selective encryption, which operates as shown in Figure 1 and is the major theme of this research. Only some of the bit stream is encrypted once the image has been first compressed. The flexibility to employ Any decoder is a fascinating additional capability for real-time applications, even if the bit stream contains some encrypted portions. In order to achieve bit stream compatibility, the bit stream should only be modified in places where it doesn't compromise adherence to the original format. Numerous Selective encryption techniques have been developed, however they typically call for a specialized decoder that is inappropriate for video transmission, as ISO standards dominate the industry.



specialised encoding mechanism

2. ENCRYPTION OF CHOICE OF CONTENSIONED IMAGES

2.1. Brief review

Around the middle of the 1990s, there were various papers on the selective encryption of MPEG streams. The MAPPELSet et al.[2] put out a technique that solely encrypts an MPEG stream's Intra (I) frames. But AGI et al. The inclusion of blocks encoded in intra mode in the POR B frames as well as the high correlation of P and B frames when they relate to the same I frame, according to [3,] make selective encryption of the I frames only offer a small amount of security. This method is susceptible to cryptanalysis, which is a common problem when compression comes before encryption. Alternative encryption techniques have been created by others. Numerous techniques have been proposed in particular for the encryption of DCT-based coded pictures. Zig-zag permutation is a method that TANG created. [4].Despite the fact that this method increases security, overall bit rate actually increases. The frequency distribution of adjacent pairs of two-byte bytes within an MPEG bit stream is the foundation of a different strategy developed by QIAO and NAHRSTEDT.[5].The authors show that while this method offers overall security and size preservation, it falls short when it comes to visual acceptability and bit stream compliance. Other methods have recently been published (see [6] for a contemporary perspective), however they do not meet the following criteria:

[**Visual approval**] Even if some information is viewable, the encrypted image should appear noisy.

[**Selective cryptography**] After compression, encryption takes place, leaving some portions of the bit stream unencrypted.

The size of the bit stream should be preserved by [**constant bit rate**] encryption.

[**Compliance with bit streams**] The finished bit stream from the encryption procedure must match the format description provided.

Researchers have demonstrated that MPEG-encoded images are not the only ones that may use selective encryption. Examples include the approaches given by For the selective encryption of JPEG 2000 and wavelet packet sub band structures, see POMMER et al. [7] and NORCEN et al. [8].

2.2. A technique for selective JPEG picture encryption

MPEG was the main target for selective encryption due to its extensive use. However, because video transmission was a consideration when developing MPEG-2, the ability to selectively encrypt MPEG streams will be reliant on a reliable key distribution scheme. The significant correlation between frames causes an extra challenge. A video stream's redundancies are greatly reduced by MPEG-2, but a residual correlation caused by the encoder's error makes cryptanalysis impossible. We focus on the JPEG specification because it is used for point-to-point communication more frequently. The following theme was first suggested in [1]. Extensions will be covered in Section 3.

2.2.1. *A succinct explanation of compatible JPEG image specific encoding*

Runs of zeros are created by the HUFFMAN coder in JPEG by combining zero coefficients. It also uses symbols that pair magnitude categories that finish in zeros with non-zero coefficients to determine entropy. These symbols are given 8-bit code words by the HUFFMAN coder. Annexe bits that fully indicate the magnitude and sign of non-zero coefficients come after these keywords. We made the decision to preserve the codes but encrypt the extra bits. This is due to the necessity of code words in synchronisation and the illogical substitution of non-zero coefficients for zero coefficients. Therefore, it's important to store away objects that have little worth. Additionally, since DC coefficients contain significant The HUFFMAN coder gives These characters are 8-bit code words. The annexe bits that follow these keywords fully reveal the magnitude and sign of the non-zero coefficients. We decided to preserve the codes while encrypting the extra bits. The reasons for this include the necessity of code words in synchronisation and the illogic of replacing zero coefficients with non-zero coefficients. Setting away objects with no worth is therefore essential.

3. 3. SELECTIVE ENCRYPTION EXTENSIONS

3.1. Multiple Elective Encryption, Section 3.

If there is only one copyright holder—hereafter referred to as owner—he will use key K1 to perform selective DCT encryption on a subset C1 of the JPEG picture coefficients. The final picture is g=Ek1(f). To avoid having to recalculate f at the receiver end of the decryption process, f= Dk1(Ek1(f)) and only if k1 is known. Since our method can handle any encryption method, we might have instead utilised an encryption strategy based on a public key and a private key. The second owner must be permitted to pick a portion of the DCT coefficients and encrypt them with his own key if there is a second owner. The formula for the image sent over the network is h= Ek 2 (Ek1(f)).When C1 and C2 are selected separately, we called this approach "multiple selective encryption."

3.2. Over-encryption

It is recommended to use the over-encryption technique, which is equivalent to Ek1(Dk2(Ek1(f))), as described by TUCHMAN [9], where C1 crosses with C2 (C1C2=), as double-encrypted coefficients are more vulnerable to attacks. Over encryption delivers superior results than Ek2(Ek1(f)), according to SCHNEIER [10].

3.3. Scheme for generalised selective encryption

In a wide context, we might offer:

1. Flexibility. The subset of DCT coefficients, or the encryption level, should be adjustable by the user.

2. Multiplicity. Assume that Information C1 and C2 will be encrypted by Owners 1 and 2. While C1 and C2 are preferably over-encrypted, they are independently encrypted. Figure 2 shows a photo that has been encrypted by Owner 1 (b) and Owner 2 (c), respectively. Remember that parallelization is nothing more than multiplicity if C1C2=. (b) C1 and C2 do not need to be fixed during the entire encryption procedure. To increase secrecy, these coefficient sets could fluctuate at random over time.

3. conformity and independence. Side coder also needs the data C1, C2, and selection maps in order to decrypt the image. As stated by FRIDRICH [11], it is conceivable to integrate them within an image, however doing so will raise the bit rate.

TheschemedrawninFigure3implementsalltheseproperties. Data is divided into many segments. Some slices are left unmodified (this is referred to as part (1) on Figure3) while other slices(2) are processed by encryption blocks ordered into a sequence S. Slices are encrypted by known algorithms (RSA, Rijndael, etc) with different keys. Keep in mind that every encryption block

could be unique. A slice should be over-encrypted if it is encrypted twice using the same technique. The selection map, which specifies which slice is encoded, and the encryption sequence S the decoder or otherwise described into an information stream I 1, which is subsequently encrypted into I 2, must be used by each encryptor or known to the decoder. It is necessary to know or supply the type of algorithms into a stream I3aswell. Then, all data—encrypted or not—are put back together to create a stream that complies with the format. The number of bits before and after encryption are equal in terms of merging. Since the original data is replaced with encrypted slices and there are few encrypted bits, substitution happens quickly to meet the demands of real-time processing. Two embedding steps come after merging.

1. 1. All of the encryptor-related data, such as methods and keys in the case of public key cryptography, is embedded in the first step. There are numerous strategies Regardless of the data formats, the bit stream size is typically increased for embedding. Loss less data embedding techniques are utilised. Therefore, the header might need to be modified to account for changes.

2. The selection map and related data, such as used parameters, are embedded in the second phase. The embedding method is comparable to the earlier method.

Because the format is changed multiple times (it is not merely a substitute), both embedding procedures are difficult and time-consuming. But if the recipient has adequate information, embedding can be skipped without exposing more security flaws.

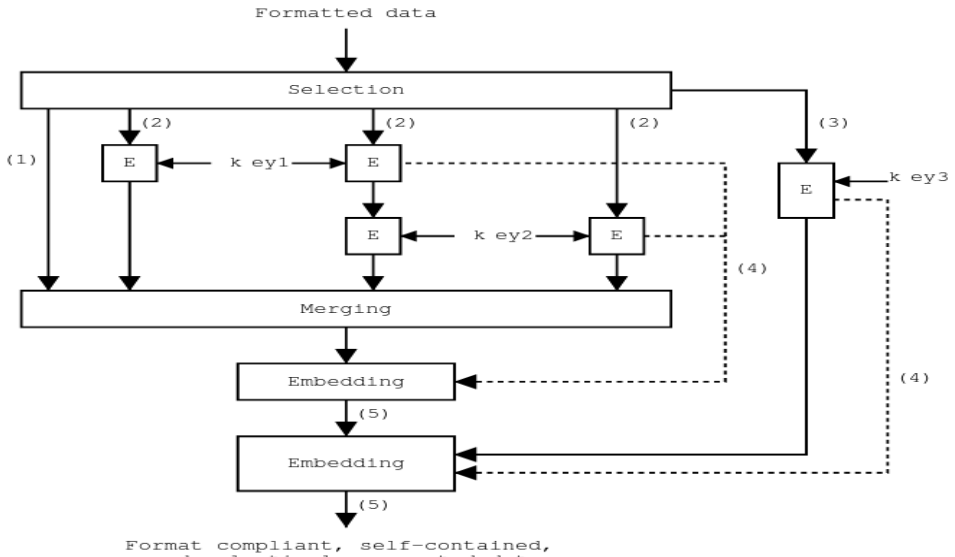
4. CONCLUSIONS

Here, we suggest a broad method for selectively encrypting images. Flexibility, multiplicity, spatial electivity, and format conformity are only a few benefits the scheme offers. The trade-off between processing speed and power leads to secrecy, but real-time processing is possible.

(a) Original image (b) Encrypted by owner 1

(c) Encrypted by owner 1 and owner 2 (d) Locally encrypted image

Flexible multiple encryption and spatial selectivity.



Self-sufficient selective encryption unit.

5. REFERENCES

[1]M.VanDroogenbroeckandR.Benedett,“Techniquesforaselectiveencryptionofuncompressed andcompressedimages,”inACIVSAdvancedConceptsforIntelligentVisionSystems,Ghent,Belgium, September2002,pp.90–97.

[2] T. Maples and G. Spanos, “Performance study of a selectiveencryptionschemeforthesecurityofnetworked,real-timevideo,”inProceedingsofthe4th InternationalConferenceonComputerCommunicationsandNetworks,LasVegas,Nevada,September 1995.

[3] I. Agiand L. Gong, “An empirical study of secure MPEGvideotransmission,”inSymposiumonNetworkandDistributedSystemsSecurity,1996.

[4] Lei Tang, “Methods for encrypting and decrypting MPEG video data efficiently, ”in ACM Multimedia, 1996,pp.219–229.

[5] Lintian Qiao and Klara Nahrstedt, “Comparison of MPEG encryption algorithms, ”Computers and Graphics,vol.22,no.4,pp.437–448,1998.

[6] A. Eskicioglu, “Multimedia content protection in digital distribution networks, ”Document available ontheInternet,2003.

[7] A. Pommer and A. Uhl, “Selective encryption of wavelet packet sub band structures for obscured transmission of visual data, ”in Proceedings of the 3rd IEEEB enelux Signal Processing Symposium (SPS2002),Leuven,Belgium,2002,pp.25–28.

[8] R. Norcenand A. Uhl, “Selective encryption of the JPEG2000bitstream,”inProc.IFIPTC6/TC117th Joint Working Conference on Communications and Multimedia Security(CMS2003),Lecture Notes in ComputerScience,volume2828,2003,pp.194–204.

[9]W.Tuchman,“HellmanpresentsnoshortcutsolutionstoDES,”IEEESpectrum,vol.16,no.7,pp. 40–41,July1979.

[10] B. Schneier, Applied cryptography, John Wiley& Sons,secondedition,1996.

[11]J.Fridrich,M.Goljan,andR.Du,“Loss less data embedding for all image formats,”in Proc.SPIE PhotonicWest,Vol.4675,ElectronicImaging2002, Security and Watermarking of Multimedia Contents, SanJose,California,January2002,pp.572–583.

Quantum Cryptography

ABSTRACT

Modern encryption Methods are constructed upon the basic, so-called "INTRACTABLE," factoring large integers into their prime factors. However, if mathematics and computing power improve, one-way operations like factoring enormous integers can be quickly reversed, making the security of the existing encryption vulnerable. A quantum physics-based evaluation of cryptography is the answer. One of the most recent topics in the computer industry is quantum cryptography. In this research, we focus on how quantum cryptography contributes to a defense-in-depth strategy for completely secure key distribution. This essay examines the problems with current digital cryptosystems, the theoretical foundations of quantum cryptography, the practical uses of this technology and its shortcomings, and finally the future prospects of quantum cryptography. The quantum key distribution approach, in which two users exchange a random quantum transmission made up of exceedingly small flashes of polarised light before exchanging private or public keys, is implemented using an apparatus and protocol that we present in this work.

Keywords

Quantum physics, large-scale distributed computing, cryptosystems, and quantum cryptography systems.

1. INTRODUCTION

Recent news about European Union members' plans received a lot of attention for its decision to invest $13 million in the research and development of a secure communications system based on quantum cryptography. The system will function as a tactical deterrent to the US, Australia, Britain, Canada, and New Zealand's Echelon intelligence gathering system. SECOQC (Secure Communication based on Quantum Cryptography) is the name of the system. In addition, a small number of quantum information processing firms, such as MagiQ Technologies and ID Quantique, are putting quantum cryptography solutions into practise in order to satisfy the needs of organisations like businesses, governments, and other institutions where preventing the unauthorised disclosure of information has become essential to maintaining an advantage over rivals. Why is spending so much money on developing a new cryptosystem,

quantum cryptography, when it is claimed that existing cryptosystems are extremely effective or "INTRACTABLE"

2. Modern cryptosystem limitations

Instead of encrypting huge amounts of data, public key cryptography is used to exchange keys because It requires lengthy, intricate calculations. For instance, well-known methods like the RSA and Diffie-Hellman key negotiation algorithms are routinely used to distribute symmetric keys across distant partiesFor the initial exchange of the symmetric key, both the speed of a shared key system and the security of a public key system can be used. Because asymmetric encryption is more slower than symmetric encryption, many organisations instead choose a hybrid strategy. As a result, this strategy makes use of both the public key infrastructure's scalability and the symmetric key system's performance and speed. However, it is not known what the mathematical underpinnings of public key cryptosystems like RSA and Diffie-Hellman are. Instead, after years of open examination of the fundamental operation of factoring huge integers into their primes—which is considered to be "intractable"—it has been found that these techniques are adequately secure. In other words, the information it was protecting had already lost all of its value by the time the encryption mechanism was broken. The power of these algorithms hinges on the fact that there is no known mathematical method for factoring enormously big integers efficiently. Even while the public key cryptosystems currently in use may be "good enough" to provide a respectably high level of confidentiality, there are still a number of issues. Public key cryptosystems might become outdated if processing power advances, such as those brought about by quantum computing, fast surpass systems like RSA. Another example is the DES algorithm, which had a 56-bit key in the past and was regarded as secure but is no longer so due to advancements in technology that have made it simple to defeat. The successor Advanced Encryption Standard was created as a result of the fact that DES may be broken by sophisticated computers in a matter of hours. Therefore, there is a concern the possibility exists that future advancements in computer processing capability could make public key cryptography vulnerable. Secondly, it's ambiguous if there is or will ever be a theory that quickly factors big numbers into their primes. The assertion that it is impossible to establish such a factoring theorem is currently unsupported by any evidence. This makes public key systems susceptible to it and substantially increases the likelihood that the algorithm cannot be theoretically solved, as the likelihood of such a theorem forming is unpredictable. Areas of national security and intellectual property that need to be completely protected could be at risk due to this ambiguity. Current encryption is susceptible because of the ease with which mathematics can readily reverse one-way processes like factoring huge integers and because of advancements in processor power. Businesses, governments, militaries, and other affected institutions would need to spend a lot of money researching the risk of harm and possibly quickly deploying a new and

pricey cryptography system if a factoring theorem was found or if computers were to advance to the point where it could beat public cryptography.

3. Theory of Quantum cryptanalysis

Instead of being constrained by the difficulties of factoring extremely large numbers, quantum encryption is based on the fundamental and constant laws of quantum mechanics. In fact, the two pillars of twentieth-century quantum physics upon which quantum cryptography is based are the Heisenberg Uncertainty theory and the photon polarisation theory. Heisenberg's Uncertainty principle states that no system's quantum state can be measured without altering it. As a result, the polarisation of a photon or other light particle can only be determined at the time of measurement. This concept is essential for preventing hackers from breaching an encryption system based on quantum cryptography. On the other hand, the photon polarisation principle explains how light photons can be polarised or directed in specific directions. A photon filter is also necessary to detect polarised photons in order to prevent photon damage. Quantum encryption is the recommended technique for safeguarding data privacy and discouraging prying eyes because of the "one-way-ness" of photons and the Heisenberg Uncertainty principle. As part of a physics and information investigation, Charles H. Bennet and Gilles Brassard developed the concept of quantum cryptography in 1984. Bennet and Brassad assert that the quantity and mode of photons received by a recipient can be used to construct an encryption key. The discovery that light can function as both a wave and a particle is compatible with their theory. Due to the vast variety of polarisation angles that these photons possess, they can be utilised to represent bits like ones and zeros. By securely exchanging keys, these bits enable PKI systems and can be used to produce one-time pads. The polarised photon encoding of bits serves as the foundation for quantum cryptography, which in turn serves as the foundation for quantum key distribution. Therefore, quantum cryptography simply depends on the rules of physics and is independent of the processing power of present computing systems, whereas modern digital encryption exclusively rely on the computational difficulties of factoring very big numbers. The principle of physics will always hold true, thus it is no longer essential to make assumptions about the computer capacity of hostile attackers or the creation of a theory to quickly solve the massive integer factorization problem. The uncertainty issue with conventional cryptography is addressed by quantum cryptography.

4. An Example of Quantum Key Transmission

Here is an example of a secure key distribution method using quantum cryptography. In this illustration, "Alice" is the sender, "Bob" is the receiver, and "Eve" is the perverse listener. Alice first sends a message to Bob by firing a stream of photons from a photon gun in one of four polarisations (0, 45, 90, or 135) that stand for opposing vertical,

horizontal, or diagonal directions. Using a photon receiver to count and measure each individual photon's polarisation, Bob will select a filter at random, which can be either rectilinear (0 or 90 degrees) or diagonal (45 or 135 degrees), record the results depending on which measurements were accurate in relation to the polarisations that Alice selected, and then select which measurements to repeat. Even if some of the photon stream splits up during the link, just a specified portion of the photon stream is necessary to generate a key sequence for a one-time pad. Then, Without releasing the actual results, Bob will use an out-of-band communication technique to advise Alice of the measurement type that was carried out and which measurements were the appropriate ones. The polarisation of the photons that were measured correctly will be utilised to transform them into bits once the improperly measured photons have been deleted. The basic building blocks of a one-time pad used to send encrypted data are these photons. The key is the result of both Alice and Bob's arbitrary choices, so it's crucial to emphasise that neither Alice nor Bob can predict the key in advance. As a result, quantum cryptography makes it possible to reliably distribute one-time keys.

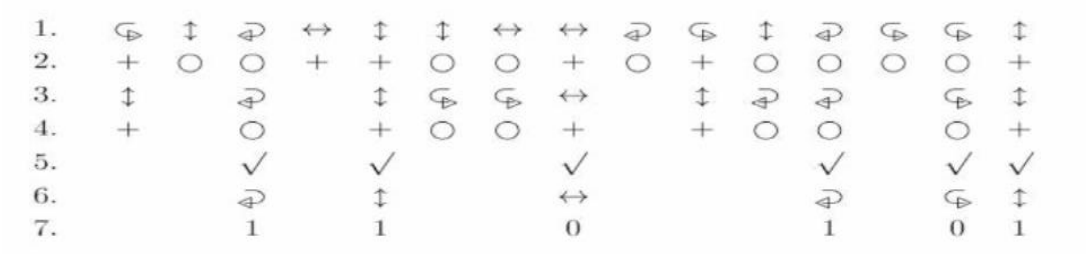


Figure 1: Basic quantum key distribution protocol.

1. Alice sends a random sequence of photons polarized horizontal (↔), vertical (↕), right-circular (↻) and left-circular (↺);
2. Bob measures the photons' polarization in a random sequence of bases, rectilinear (+) and circular (○).
3. Results of Bob's measurements (some photons may not be received at all).
4. Bob tells Alice which basis he used for each photon he received;
5. Alice tells him which bases were correct;
6. Alice and Bob keep only the data from these correctly-measured photons, discarding all the rest.
7. This data is interpreted as a binary sequence according to the coding scheme ↔ = ↺ = 0 and ↕ = ↻ = 1.

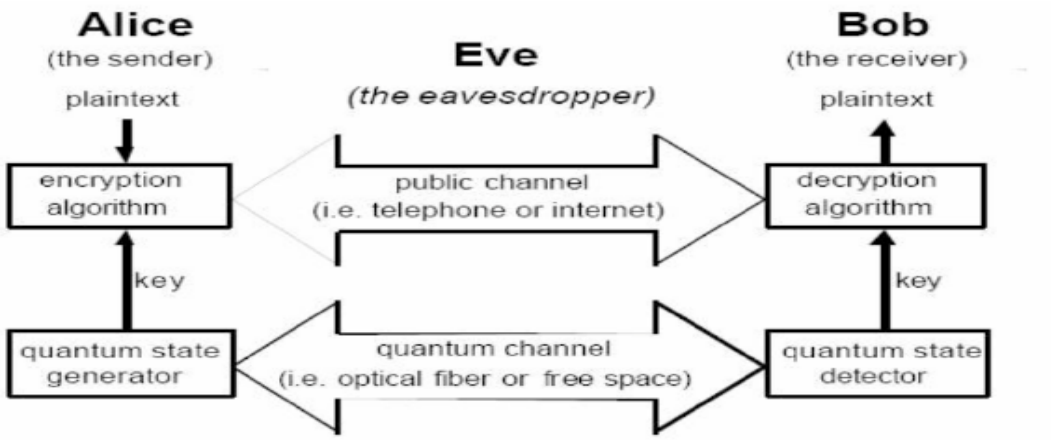


Figure 2. Quantum Key Distribution Example

Now consider the scenario when an adversary with malicious intent tries to hack the cryptosystem and undermine the quantum key distribution algorithms. The evil attacker Eave will also need to pick a rectilinear or diagonal filter at random in order to measure each of Alice's photons.

Eve won't have the option of asking Alice to validate the type of the filter, She will consequently have an equal chance of choosing the correct or incorrect filter. Even if Eve is successful in overhearing Bob and Alice verifying the protons they received, she won't be able to use this knowledge much unless she understands the correct polarisation of each individual photon. Because of this, Eve's attempts to render a meaningful key and accurately interpret the photons that make up the final key would be unsuccessful. This strategy offers a total of three notable advantages. It is firstly impossible to duplicate information about photons because doing so would lead to their destruction, according to the Heisenberg Uncertainty principle. Photons are unbreakable, therefore when they come into contact with a detector, they disappearThe length of the one-time pad must match the length of the message, therefore Alice and Bob must know in advance how many photons are required to create the encryption key. Given that Bob should, in theory, get 25% of the photons being delivered, a departure from the expected proportion may indicate that traffic is being sniffed or that there is a systemic issue. If Eve sees a photon, Bob won't be able to detect it since Eve can't reproduce an unidentified quantum state. Eve would be forced to pick a photon's orientation at random and would frequently be off by about 50%. This mistake rate would be sufficient to inform Bob of Eve's existence.

5. Desirable QKD Attributes

In general, QKD provides a means for two independent devices to concur on a shared random sequence of bits with a very low probability that other devices (eavesdroppers) will be successful in determining the values of those bits. These sequences are then

utilised as secret keys for message encoding and decoding between the two devices according to a particular technique. It is clear from this background that QKD is a crucial distribution strategy, and the sections that follow list the major distribution objectives where QKD excels.

5.1 Confidentiality of Keys

The primary motivation for interest in QKD is confidentiality. The persistent misconception that decryption is technically impossible harms public key systems. Thus, key agreement primitives frequently employed in the current Internet security architecture, such as Diffie-Hellman, may eventually be broken. This could reveal past traffic in addition to impairing communication in the future. Traditional secret key systems have been plagued by a variety of issues, considering the practical challenges of distributing keying material and insider threats. When QKD techniques are successfully incorporated into a system that is completely safe, they can produce automatic key distribution that may offer higher security than its competitors.

5.2 Authentication

QKD does not provide authentication by itself. Current approaches to Prepositioning secret keys at device pairs for use with hash-based authentication methods or hybrid QKD-public key approaches is one method of authentication in QKD systems. Neither strategy really appeals to me. Prepositioned secret keys must be sent in some way, such as by human courier, before QKD really starts, which could be expensive and logistically difficult. In the case that an adversary party forces a QKD system to run out of key material, at which point it is unable to finish authentication, this method also looks to be vulnerable to denial of service assaults. However, hybrid QKD-public key methods run the danger of having their public key infrastructure vulnerable to attack from quantum computers or unanticipated mathematical developments.

5.3 Rapid Key Delivery Enough

In order to prevent the supply of key bits in encryption devices from running out, key distribution systems must distribute keys as rapidly as possible. There is competition between the rates at which keying material is produced and consumed in encryption and decoding processes. In real-world scenarios, modern QKD systems frequently run at much lower rates and have a throughput for keying material of about 1,000 bits per second. This is an undesirable low value if one employs these keys in specialised applications, one-time pads for high-speed traffic, for instance. However, if the keying information is used as input for less secure (but frequently secure enough)

methods like the Advanced Encryption Standard, it might very well be appropriate. But greatly outperforming the rates provided by the current QKD technology is both desirable and practicable.

5.4 Robustness

The QKD community has never previously given this much thought.

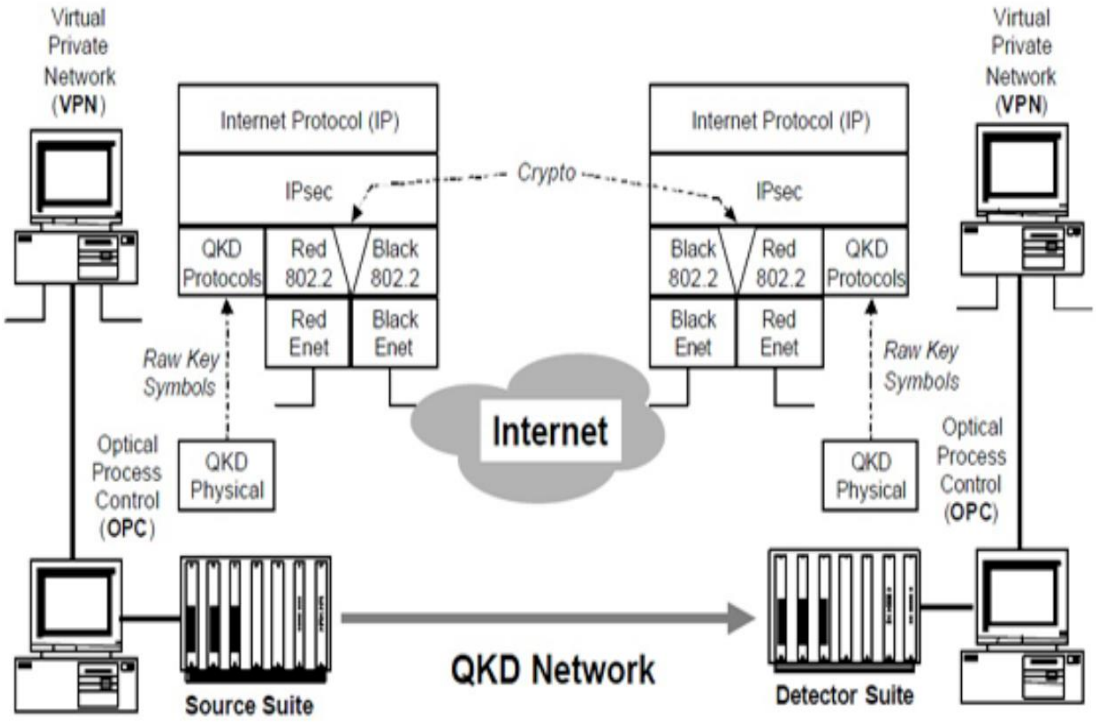
The flow of keying material must not be stopped, either by mistake or intentionally (via denial of service) by an opponent. This is essential because secure communications require keying material. This QKD service has been particularly susceptible up to this point given that just one point-to-point link has implicitly used QKD methods.

Any flow of keying material would stop if the link were to be broken, whether by active eavesdropping or simply a fibre cut. We claim that because a meshed QKD network provides several channels for key distribution, it is inherently more reliable than any single point-to-point link.

5.5 Distances and Location Independence

In a perfect world, any entity might come to an agreement on keying materials with any other (authorised) entity anywhere in the world. Surprisingly, the Internet's security design does have this feature: by selecting keys using the Internet IPsec protocols, any computer connected to the network can create a security relationship with any other computer.

This feature is conspicuously lacking in QKD, which can only operate over fibre for a short distance and necessitates a straight and obstruction-free path for photons to travel between the two entities.



5.5 Lack of Support for Traffic Analysis

A crucial distribution system may provide useful traffic analysis to adversaries. For instance, a considerable amount of private information may be moving between two locations or will do so in the future if there is a strong flow of keying material between them. It could be better to avoid such analysis as a result. QKD has typically taken a fairly poor approach in this area because Dedicated, point-to-point QKD links between communication entities have been assumed in the majority of configurations, which lays out the underlying key distribution relationships explicitly.

6. Making use of quantum cryptography

Here, we go over a number of systems that successfully used quantum cryptography.

6.1 QUANTUM NETWORK DARPA

The virtual private network (VPN) is a cryptographic security concept developed by DARPA. Traditional VPNs employ symmetric and public-key encryption to secure communications and provide authentication and integrity. Public-key techniques allow for key agreement or exchange and endpoint authentication.

Both traffic secrecy and integrity are provided by symmetric techniques, such as 3DES and SHA1. Because of this, VPN systems may provide confidentiality, authentication, and integrity without putting their faith on the public network that connects the VPN sites. In DARPA research, keys provided by quantum

cryptography are supplemented or entirely replaced by current VPN key agreement primitives. The VPN construct's remaining components are left unaltered; see Fig. 2. Therefore, normal Internet hosts, routers, firewalls, and other devices are fully compatible with the DARPA QKD-secured network.

6.2 Technologies MagiQ

MagiQ Technologies, a tech start-up with its headquarters in New York City, is one of the businesses creating solutions based on quantum cryptography. Among the target markets for MagiQ's solutions include academic and government labs, the financial services industry, and other industries. According to MagiQ's business strategy, current cryptography methods are supplemented by quantum cryptography rather than replacing existing encryption technologies like PKI in order to create a hybrid system that is more secure. The solution provided by MagiQ is called Navajo QPN Security Gateway. According to MagiQ, the first QKD system to be made commercially available is the quantum key distribution hardware box. Each unit costs around $50,000 and comes with a 40-pound chassis that fits in a conventional 19-inch rack. The system contains of the hardware and software necessary for distributing quantum keys, as well as a photon transmitter and receiver. The Brassard and Bennet-proposed BB84 quantum encryption technique is used to connect these "black boxes" that are used by remote parties. For the purpose of preventing unauthorised access to data travelling across fibre optic networks, the Navajo system is designed to switch randomly generated keys once per second.

7. QKD Protocols Implementation

We refer to the unexpectedly complex set of specialised protocols used in quantum cryptography as "QKD protocols." Many of these protocols' peculiar characteristics, Experts in communications protocols could be interested in their peculiar implementation and justification.

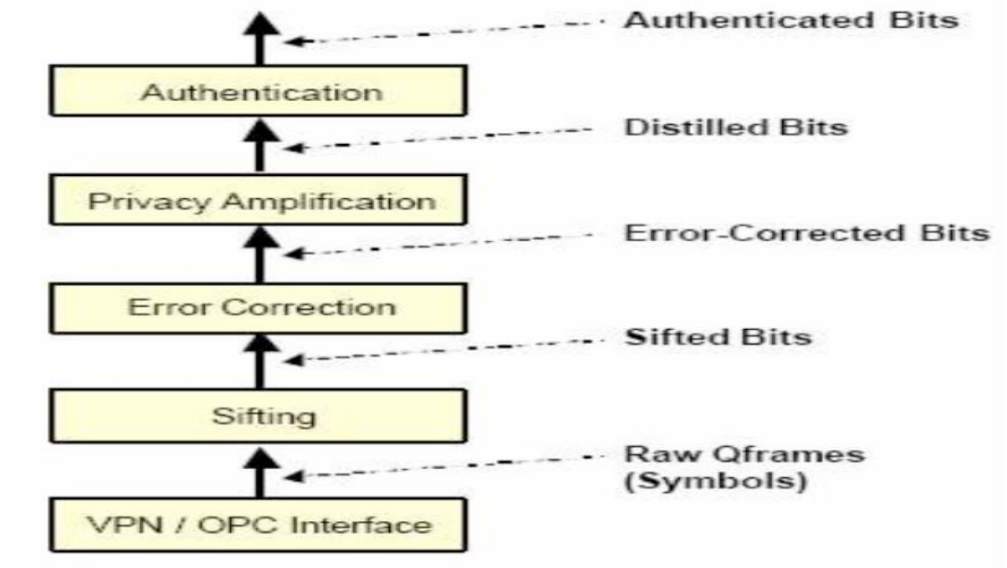


Figure 4. The QKD protocol Stack

This section provides a description of the protocols that are currently used in our C language implementation of the QKD protocol. DARPA built this engine to make "plugging in" new protocols straightforward, and they plan to spend a large amount of work in the next years developing and testing new QKD protocols. The easiest way to classify these protocols, as shown in Fig. 5, is as members of the QKD protocol family. But bear in mind that these layers don't necessarily correspond to the OSI layers or other tiers in a communications stack. As can be seen, they are actually approaching pipeline phases.

7.1 Sifting

Alice and Bob window all the obvious "failed q bits" from the pulses as they are being sorted out. As was said at the beginning of this section, examples of these failures include qubits where Alice's laser never sent, Bob's detectors weren't working, photons were lost during transmission, and so on. They also contain the symbols used when Bob chose one basis for receiving while Alice chose another. The useless symbols from Alice's and Bob's internal storage are eliminated following this protocol interaction, or a sift and sift response transaction, leaving just the symbols Bob was given, and Bob's justification is the same as Alice's.

7.2 Correction of Errors

The same sequence of error-corrected bits can be shared by Alice and Bob if they are able to identify and correct all of the "error bits" in their shared, filtered bits.

Bits that Alice sent as a 0 but Bob received as a 1, or vice versa, are known as error bits. These bit mistakes could be caused by eavesdropping or background noise. The amount of hidden entropy that can be used for key material decreases due to the extremely uncommon requirement for error correction in quantum cryptography, which assumes that evidence revealed in mistake detection and repair (such as parity bits) was known to Eve. Designing error detection and correction algorithms that reveal as little as possible in their public control communication between Alice and Bob is hence strongly motivated.

Increasing Privacy

Alice and Bob can restrict Eve's access to their shared bits to a tolerable amount by utilising privacy amplification. Advantage distillation is a another name for this technique.

The side that commences the privacy amplification process prefers a linear hash function to the Galois Field GF[2n] where n is the input bit count, rounded up to a multiple of 32. The next four pieces of information he transmits to the other end are the m bits of the reduced result, the basic polynomial of the sparse Galois field, an n-bit multiplier, and an m-bit polynomial to add (i.e., a bit string to exclusive-or) with the product. The relevant hash is then executed on each side, and the output is truncated to m bits for privacy amplification.

7.3 Authentication

Through the use of authentication, Alice and Bob may defend themselves against "man in the middle attacks," enabling both Alice and Bob to be certain that they are communicating with each other and not Eve. Continuous authentication is necessary used for all key management transactions because Eve could suddenly enter Alice and Bob's connection. The authenticating problem was covered in the original BB84 work [1], which also included a sketch of a solution utilising the universal families of hash functions Wegman and Carter had previously introduced [20]. To choose a hash function from the family and create an authentication hash of their public correspondence using this method, Alice and Bob must already have a little shared secret key. Even a malicious opponent with infinite computer power would have very little chance of producing the correspondence due to the nature of universal hashing if they lacked the secret key. The drawback is that even a single reuse of the secret key bits on unrelated data cannot be used to break the security.

Fortunately, many new shared secret bits from QKD can be verified by a complete authenticated discussion, they can be used to refresh the pool in tiny numbers. The numerous other elements in a practical system, such as symmetrically authenticating both parties, restricting Due of Eve's capacity to compel the shared secret key bits to exhaustion and her ability to adapt the system to network asynchrony and

retransmissions, will only be briefly touched upon. Another crucial point is that we also need to authenticate VPN data flow; utilising these techniques to merely validate the QKD protocols is not enough.

8. Discussion and Conclusion

DARPA is currently building a number of QKD links that are woven into a bigger QKD network that consists of a mesh of QKD relays or routers in order to connect its QKD endpoints. One point-to-point QKD link inside the relay mesh is abandoned and another is used in its place when that link has a failure, such as a fibre cut, excessive eavesdropping, or noise. The Even in the face of active eavesdropping or other kinds of denial-of-service assaults, the DARPA Quantum Network can be constructed to be resilient. One term for such a structure would be "key transport network." Quantum repeaters may be able to get over the fundamental problem of unreliable QKD networks—their constrained geographic reach—in the future of the DARPA Quantum Network. In order to enable QKD operations across much greater distances than are now possible, Such repeaters are the subject of extensive ongoing investigation. If useful devices are ever developed, they ought to integrate seamlessly into the overall structure of untrusted QKD networks. As a potential remedy for the distance problem, chaining quantum cryptography links with secure intermediary stations has been put forth.
Other options include transmission over void space or a low-orbiting spaceship.
The atmosphere attenuates less photons in this scenario because the satellite acts as the intermediary station. In order to transport quantum keys safely from satellites to another location, research and development are now underway in both the US and Europe. Even though quantum cryptography has advanced significantly There are still difficulties to be resolved before it may be used after the previous 10 years by businesses, governments, and common people as a standard key distribution system. The development of more advanced hardware to provide higher quality and longer transmission lengths for quantum key exchange is exactly one of these challenges.
However, the development of quantum cryptography will continue to be fueled by improvements in computer processing capacity and the fear of obsolescence for current encryption techniques. In fact, it is anticipated that during the following three years, almost $50 million in public and private funding will be invested in quantum cryptography technology3.
Although technology is still in its infancy, quantum cryptography appears to have a bright future. This technology has the potential to significantly improve personal security, government organisation security, and e-commerce and commercial security. Quantum cryptography will have a huge and revolutionary impact on all of our lives if it eventually proves to live up to even some of its expectations.

9. REFERENCES

[1] C. Bennett and G. Brassard, “Quantum Cryptography:Public Key Distribution and Coin Tossing,” International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 1984.

[2] A. Ekert, “Quantum Cryptography Based on Bell’s Theorem,” Phys. Rev. Lett. 67, 661 (5 August 1991).

[3] Ekert, Artur. "What is Quantum Cryptography?" Centre for Quantum Computation –Oxford University.Conger., S., and Loch, K.D. (eds.). Ethics and computer use. Commun. ACM 38, 12 (entire issue).

[4] Johnson, R. Colin. "MagiQ employs quantum technology for secure encryption." EE Times. 6 Nov. 2002..

[5] Mullins, Justin. "Quantum Cryptography's Reach Extended." IEEE Spectrum Online. 1 Aug. 2003.

[6] Petschinka, Julia. "European Scientists against Eavesdropping and Espionage." 1 April 2004. 7. Salkever, Alex. "A Quantum Leap in Cryptography." Business Week Online. 15 July 2003.

[7] Schenker, Jennifer L. "A quantum leap in codes for secure transmissions." The IHT Online. 28 January 2004..

[8] MagiQ Technologies Press Release. 23 November 2003.

[9] Schenker, Jennifer L. "A quantum leap in codes for secure transmissions." The IHT Online. 28 January 2004.

[10] C. Elliott, “Building the quantum network,” New J. Phys. 4

(July 2002) 46.

[11] Pearson, David. "High!speed QKD Reconciliation using Forward Error Correction." Quantum Communication, Measurement and Computing. Vol. 734. No. 1. AIP Publishing, 2004.

[12] Curcic, Tatjana, et al. "Quantum networks: from quantum cryptography to quantum architecture." ACM SIGCOMM Computer Communication Review 34.5 (2004): 3-8.

[13] Shor, Peter W., and John Preskill. "Simple proof of security of the BB84 quantum key distribution protocol." Physical

Review Letters 85.2 (2000): 441.

[14] Bienfang, J., et al. "Quantum key distribution with 1.25 Gbps clock synchronization." Optics Express 12.9 (2004): 2011-2016.

[15] Inoue, Kyo, Edo Waks, and Yoshihisa Yamamoto. "Differential phase-shift quantum key distribution." Photonics Asia 2002. International Society for Optics and Photonics, 2002.

[16] Barnum, Howard, et al. "Authentication of quantum messages." Foundations of Computer Science, 2002. Proceedings. The 43rd Annual IEEE Symposium on. IEEE, 2002.

[17] Elliott, Chip, David Pearson, and Gregory Troxel. "Quantum cryptography in practice." Proceedings of the 2003

conference on Applications, technologies, architectures, and protocols for computer communications. ACM, 2003.

[18] Buttler, W. T., et al. "Fast, efficient error reconciliation for quantum cryptography." Physical Review A 67.5 (2003): 052303.

[19] Poppe, A., et al. "Practical quantum key distribution with polarization entangled photons." Optics Express 12.16 (2004): 3865-3871.

[20] Lütkenhaus, Norbert. "Estimates for practical quantum cryptography." Physical Review A 59.5 (1999): 3301.

PAPER NAME

Biocryptography.pdf

WORD COUNT

11521 Words

CHARACTER COUNT

62855 Characters

PAGE COUNT

34 Pages

FILE SIZE

753.3KB

SUBMISSION DATE

May 27, 2023 7:41 AM GMT+5:30

REPORT DATE

May 27, 2023 7:42 AM GMT+5:30

18% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

- 14% Internet database
- 9% Publications database
- Crossref database
- Crossref Posted Content database
- 9% Submitted Works database

Excluded from Similarity Report

- Bibliographic material
- Quoted material
- Cited material
- Small Matches (Less then 9 words)

Biocryptography
The Future of User Authentication?

Abstract

Traditional cryptography requires shared information for authentication, typically in the form of a secret token or password. These password authentication schemes are widely used in today's wired society, but they have a number of fundamental flaws, the most important of which is their inability to discriminate between legitimate users and hackers using stolen credentials. Biometric solutions address these issues by using bodily traits to distinguish legitimate users from imposters. These systems do, however, have a special set of weaknesses.

The study of cryptographic techniques for safeguarding biometric systems is known as biocryptography, and it sits at the nexus of biometrics and conventional cryptography. This study investigates cutting-edge biocryptographical techniques to develop systems that are accurate and resistant to intrusions.

1. Introduction

Traditional cryptography requires shared information for authentication, typically in the form of a secret token or password. These password authentication schemes are widely used in today's wired society, but they have a number of fundamental flaws, the most important of which is their inability to discriminate between legitimate users and hackers using stolen credentials. Users are also need to keep track of several accounts with different passwords.
Biometric solutions address these issues by employing features such as fingerprints, irises, and even the shape of the ear to distinguish legitimate users from imposters. These systems do, however, have a special set of weaknesses, such as what happens if a user's biometric information is stolen. A fingerprint cannot readily be changed, unlike a password.
Biocryptography, the study of specialised cryptographic techniques for safeguarding biometrics systems, lies at the interface between biometrics and conventional cryptography. This study examines cutting-edge biocryptography techniques to develop systems that accurately identify real users and are resistant to conventional biometric attacks.

2. To the Community

A 2012 survey on online registration and passwords by Janrain found that 30% of people had more than ten different passwords they need to remember, and 58 percent of adults have at least one unique password for each online login. Additionally, 2 out of 5 people (37%) at least once a month need help with their user name or password
The current models for user authentication have resulted in a ridiculous situation: on the one hand, experts advise us to use lengthy, random, and unique passwords to make them difficult to crack; on the other hand, we must create, keep track of, and occasionally change credentials for

each service we sign up for. According to anecdotal evidence, most people put convenience ahead of security and frequently use (and reuse) weak passwords. The fact that the organisations we rely on to protect our credentials are not safe themselves makes the situation worse; in fact, it seems like we are hearing about significant security breaches more frequently lately (like those at LinkedIn, Target, and Sony). Hackers obtained access to 6.5 million user credentials from the LinkedIn breach on June 5, 2012 alone. More than 60% of the unique passwords had been decrypted and made public by the next day. My own dissatisfaction with how user authentication systems are currently implemented served as the primary inspiration for this project. It is incredibly frustrating that the user is required to manage and secure her own credentials to such an extent. Therefore, this study investigates biometric systems and the biocrytographic techniques employed to protect them as an alternative to a password-based authentication system. I was interested in learning if biometric systems are actually feasible and, if so, how feasible they would be how they would differ from the present systems used for traditional authentication.

3. Cryptography

The fundamental goal of cryptography is to let two parties to communicate safely and confidentially with one another when a third person, or adversary, is present. Data encryption is used to do this, rendering the communication unintelligible to those who lack the necessary decryption skills. An initial message in plaintext is typically converted into a jumbled, unintelligible message, or in crypto-text, using an encryption technique and a cryptographic key.

3.1 Algorithms for Encryption

There are two primary types of encryption algorithms used in modern cryptography: symmetric, or private-key encryption, and asymmetric, or public-key encryption. The same cryptographic key and technique are used by symmetric-key encryption methods the process of converting plaintext into cyphertext and then back into plaintext. The Data Encryption Standard (DES) is one of the symmetric-key algorithms that is most frequently employed. In asymmetric-key systems, a public key for encryption and a private key for decryption are jointly established. The public key, as its name implies, is distributed widely and can be used by another person to encrypt data before sending it to you. Only the private key, which you keep private, can be used to decrypt data encrypted with this public key. The RSA algorithm, so called because developers Rivest, Shamir, and Adleman, is a popular symmetric-key algorithm.

4. Authentication Systems

The four primary objectives of contemporary cryptography are as follows: Confidentiality, data integrity, non-repudiation, and authentication are listed in that order [Xi and Hu, 2010]. The final objective, authentication, is concerned with confirming identity claims. It should be possible for sender and receiver to confirm one other's identities and the message's source

when sending a message. Authentication is different from authorization, which is the process of providing a party access to a system or data based on the verification of their identity. A user's identity is verified in knowledge-based authentication systems using some sort of piece of information, such as a password, passphrase, or personal identification number (PIN). However, this approach has a number of drawbacks:

Passwords and PINs can be guessed through social engineering, as was shown above. 1) Knowledge like passwords and PINs can be quickly forgotten.

3) Wordlist or brute-force assaults can readily crack even encrypted passwords. 4) Plaintext passwords and PINs are simple to share and disseminate, and 5) A system relying on passwords cannot tell the difference between a legitimate the attacker and the user using stolen or counterfeit credentials.

4.1 Biometric Authentication Systems

In biometric systems, authentication is based on a person's physiological or behavioural traits rather than a shared secret or key. Angerprints, irises, or even ear shape can be used to identify genuine users [Xi and Hu, 2010].

Biometric systems typically consist of two distinct components. A biometric sensor, such as a fingerprint reader, reads the biometric data and typically performs some quality control on the sample. This raw biometric data is consumed by the feature ex- tractor, which then extracts an appropriate feature set (or template) to represent the data. These characteristics would include minute particulars that define a ngerprint system. The matcher, also known as the matching model, compares this sample template to a previously saved template and generates a score, indicating how well the sample matches the previously stored template. And last, it's typical for systems to keep known templates in a database.

Biometric systems have the potential to be more dependable than traditional password-based systems since biometric features cannot be lost or forgotten and are challenging to imitate, fabricate, exchange, or distribute. However, they come with their own set of problems, such as those with accuracy (false positive and negative matches), security (because, unlike a password, stolen biometric data cannot be replaced), and privacy. Additionally, biometric systems have their own unique set of weaknesses; they are not immune to attack.

4.2 Biometric System Attacks

According to Ratha et al., there are eight different categories that can be used to categorise the attack vectors that are specific to biometric systems.

1. phoney biometric: An attacker impersonates a biometric, such as a phoney ngerprint
2. Replay attack: The attacker plays back a previously captured signal, for as by showing the system an outdated version of a ngerprint image.
3. By inserting a Trojan horse inside the feature extractor, the attacker can override it and force it to produce the feature set that the attack chose.
4. Override matcher: The attacker tricks the matcher into faking higher or lower match rates.

5. Change the feature representation: The attacker substitutes the retrieved feature set with a different, synthesised one.
6. Modification of stored templates: An attacker modifies a template to provide someone a false authorization by altering the database that contains the templates.
Attack tampers with the templates as they are being transported from the storage database to the matcher through the attack's communication channel.
8. Overriding the choice: The recognition system performs as predicted, but the attacker modifies the final authentication decision.

5. Biocryptographic Methods and Applications

Xi and Hu assert that among the assaults against biometric systems, those targeting templates have the potential to be the most damaging and difficult to identify. 2010's [Xi and Hu] Therefore, biometric templates must always be encrypted both during storage and during matching for a system to be secure. Traditional approaches that use non-smooth functions, such DES and RSA, cannot be used for encryption because of the properties of biometric data [Fengling Han, 2007]. For instance, even minor changes in a feature set obtained from a ngerprint will result in dramatically different encrypted feature sets, making it difficult to perform feature matching with encrypted templates.

5.1. Template Encryption

A secret key, KE, and an encryption method, E, are typically used to encrypt a template, T, so that the encrypted form, C, is given by: C = E (T, KE).
Then, to decrypt, we use the formula T = D (C, KD), which applies a decryption method, D to C, and a decryption key, KD, to recover the template.
Key binding is a biocryptographic method in which the secret key and the biometric information (i.e., the template) are coupled to create an artefact that conceals both the template and the key. Since it is computationally impossible to directly decrypt the artefact, it can then be disseminated openly [Xi and Hu, 2010].

5.1.1 Fingerprint Fuzzy Vault

The fuzzy vault algorithm is a key-binding design suggested by Juels and Sudan [Juels and Sudan, 2006]. The fact that this technique is error-tolerant and order-invariant makes it particularly suitable for use with biometric data. In other words, as long as there is a certain amount of overlap between the sets, data can be encoded using one set of values (such as a biometric feature set) and then unlocked using an other set of values. It doesn't matter which of the sets is used for locking and which is used for unlocking because of order invariance. Given a secret key and a template (i.e., feature set), the basic method operates as follows: first, encode the key as the coecients of a polynomial function, p(x). To create a set of points that accurately depicts the

polynomial, apply p(x) to each value in the feature set. Create a "cha" set of points next, which are inside the domain and range but do not lie on the polynomial, to mask the template data. The final collection of points is the "fuzzy vault" and it is created by combining the two sets and rearranging the order. Utilise the user-provided feature set to unlock the fuzzy vault. The polynomial can be rebuilt and the secret key exposed if sufficient numbers of the points within a specific mistake match the set used to encode the data [Xi and Hu, 2010, Juels and Sudan, 2006]. As a proof of concept, I created a straightforward "biometric" authentication system that encrypts identity/fingerprint pairings using the fuzzy vault algorithm.

6. Conclusion

Although widely used, password-based authentication methods are problematic because users must manage numerous sets of credentials, which encourages the use of weak, easily cracked passwords. A password-based system also is unable to discriminate between a legitimate user and an attacker using credentials that have been stolen. Biometric systems, which employ physiological traits to identify authentic users just once, offer a solution to these issues but are not without their own set of difficulties and risks. The field of biocryptography investigates specialised cryptographic approaches for safeguarding biometric systems because many conventional cryptographic techniques are inappropriate for biometric data.

References

[buf,] Fuzzy vault. https://wiki.cse.buffalo.edu/cse545/content/

fuzzy-vault.

[Das, 2013] Das, R. (2013). An Introduction to Biocryptography.

http://www.nationalhomelandsecurityknowledgebase.com/cln/

news/2013/11221.aspx.

[Das, 2014] Das, R. (2014). Biometric Technology: Authentication, Biocryp-

tography, and Cloud-Based Architecture. CRC Press.

[Fengling Han, 2007] Fengling Han, Jiankun Hu, X. Y. Y. W. (2007). Fin-

gerprint images encryption via multi-scroll chaotic attractors. Applied

Mathematics and Computation.

[Janrain, 2012] Janrain (2012). Online Americans Fa-

tigued by Password Overload Janrain Study Finds.

http://janrain.com/about/newsroom/press-releases/

online-americans-fatigued-by-password-overload-janrain-study-finds/.

[Juels and Sudan, 2006] Juels, A. and Sudan, M. (2006). A fuzzy vault

scheme. Des. Codes Cryptography, 38(2):237{257.

[Ratha et al., 2001] Ratha, N. K., Connell, J. H., and Bolle, R. M. (2001).

An analysis of minutiae matching strength. In Proc. 3rd AVBPA, pages

223{228.

[Vijayan, 2012] Vijayan, J. (2012). Hackers crack more

than 60% of breached LinkedIn passwords. http://www.

computerworld.com/article/2504078/cybercrime-hacking/

hackers-crack-more-than-60--of-breached-linkedin-passwords.

html.

[Xi and Hu, 2010] Xi, K. and Hu, J. (2010). Bio-cryptography. In Handbook

of Information and Communication Security, pages 129-157.

DNA Cryptography

Keywords: DNA Biological conundrum, algorithm, DNA chip, cryptography.

Abstract.

Applying DNA computing to the subject of DNA cryptography still faces several theoretical and practical challenges. The most popular DNA cryptography methods in use today combine conventional encryption with DNA technology, whose practicality has not yet been fully

proved. We chose the biological conundrum that "DNA sequencing is difficult under the conditions of not knowing the correct sequencing primers and probes" through research and analysis. We create a fresh DNA-based cryptography algorithm biological technology and DNA chips. The method's viability and safety are verified through simulation, which is offered. The findings demonstrate that this technology, while ensuring viability, provides higher security compared to conventional encryption techniques.

Introduction

A ground-breaking academic study area called DNA computing has recently emerged. It includes a novel calculating technique in which a biological DNA molecule serves as the calculation medium and biochemical reactions serve as the calculation means. DNA computing has the following benefits over current computer technology: a high level of parallelism, minimal energy consumption, and a significant storage capacity for information. These features give DNA encryption a distinct edge in applications such as data encryption in huge parallel with reduced real-time demand, information, digital signatures, and safe data storage concealment, etc. Along with the study field of DNA computing, a new branch of cryptography called DNA cryptography [1] has evolved recently. The DNA code's information carrier is a DNA molecule, and contemporary biotechnologies provide the means of implementation. It completes cryptographic operations including encryption, authentication, and signatures by fully using the DNA computing and DNA cryptography's inherent high storage density and high parallelism advantages.

Associated Technologies and Complex Biological Issues

Two distinct encryption techniques based on a DNA binary string were introduced by Andre' L, et al. [1]. The techniques are applied under specific presumptions. The method's viability is constrained, but it can provide a guide for further research.

Sivan S. et al.'s [2] use of the molecular automaton and DNA chip allows for picture encryption. The system described in this study has the advantages of utilising molecular automaton techniques and DNA chip technology, but it also has several drawbacks, including the fact that it can only be used for image encryption and that its operational viability has not been thoroughly proven. However, the authors' findings suggest that we can investigate and examine DNA encryption techniques in greater detail. In paper[5], The authors suggested an encryption approach by fusing challenging biological issues with traditional cryptography theory. A doubly secure version is provided by challenging biological problems and computer challenges in encryption. The method has a high level of security strength, as demonstrated by the validation studies. Luming X,et. al,[6] used computational complexity theory of cryptography in conjunction with Technologies for DNA synthesis, DNA cloning, PCR amplification, and DNA chips to propose a biotechnology-based encryption approach. Without the necessary decryption keys, Decrypting the plaintext that has been encrypted using this is challenging approach, which ensures the method's security due to the limitations of current biological and computational capabilities.

Designing PCR primers and DNA coding

Encoding DNA

The three primary types of DNA encoding techniques are as follows:

1) The 10, 01, 11, and 00 are represented, respectively, by A, T, G, and C, in a base representing two binary digits;[5]

2) Depicting 0 and 1 using two DNA short chain molecules, respectively;[2]

3) DNA encoding as quaternary, where a letter or number is represented by three nucleotides.[7] We opt for the first encoding method, which uses the letters A/T/G/C to represent two binary values, or 0123/CTAG, respectively, stand in for 10/01/11/00.

Primer PCR

Currently, Oligo 6.0, Primer premier 4.11, and other programmes are used often for primer design. Using the Oligo Analyzer programme, we created the proper primers for this study based on the template DNA strand. The DNA vector's DNA fragments are each placed in a separate place. In order to discover the appropriate DNA fragments for decryption, We initially amplify the lengthy strands of DNA using PCR. using the chosen primer. Long DNA chain with (P1, P2, P3).

Because the original DNA template has a significant impact on primer design and the characteristics of the DNA sequences converted from plaintext through a series of steps have difficulty meeting the PCR primer design principles, the designed encryption method adds a pair of encryption keys at the beginning and end of each DNA sequence. The encryption key pairs are chosen based on the DNA sequences that match the PCR primers that can be utilised for amplification. By doing this, we can prevent a situation where the DNA sequences obtained from the encrypted plaintext cannot be used to create PCR primers. The additional outcome of this is that the decryption key and the encryption key are compatible. For the encryption procedure, There are three necessary pairs of encryption keys (si, ei), where i = 1, 2, and 3. Twenty characters make up the encryption key.The start and end of each DNA segment include the matching encryption keys. Using the Oligo Analyzer application, matching primers for the encryption keys can be created. The DNA sequences that can be utilised to create the proper PCR primers and perform PCR amplification in a biological laboratory can be used to obtain the encryption keys. The DNA segments are shown in Fig. 1 after having appropriate encryption key pairs inserted to both ends.

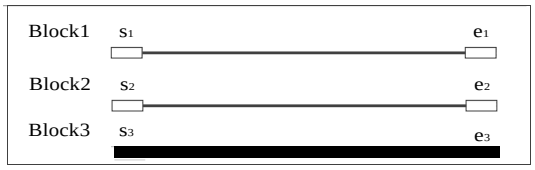
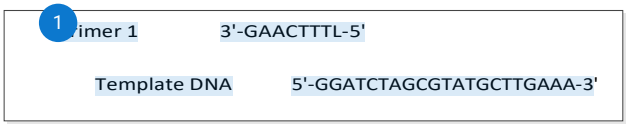


Fig 1.The schematic of DNA fragments after adding corresponding encryption primers at both ends

According to the designed encryption primer pairs (s_i, e_i), using the Oligo Analyzer to design corresponding decrypt primers (decode_s_i, decode_e_i), i=1,2,3.The schematic diagram of the combination of PCR primers and the template is shown in Fig 2.



g 2. The illustration of the PCR primers and template combination

In Fig. 3, a long DNA chain with the appropriate DNA pieces is depicted schematically.

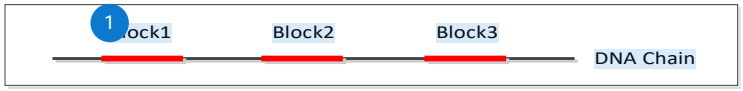


Fig 3. the conceptual representation of the long DNA chain containing the desired DNA pieces

Based on the generation of biological puzzle keys, the DNA Encryption Method

In this situation, all of the decryption keys can be used to generate signals that meet specified criteria and hybridise with the encryption keys used to produce DNA chips. When the hybridization signals mix the decryption keys with other encryption keys. can be created. All encryption keys produce the same hybridization signals when they mix with different decoding keys. The approach is a form of asymmetric encryption because the encryption keys and the decryption keys are different. The complementary sequence of each encryption key is contained in the decryption key in this instance.

There are many possible probes in both encryption and decryption keys. These probes are often classified into two types: probe 0 and probe 1. One type of probe is placed on the position where the value is 1, and another type is placed on the spot where 0 is the value, we place one type of probe. for the simple binary matrix. We can create the desired DNA chips in this method. By employing the decryption key to hybridise with the DNA microarray, the receiving party is able to get the plaintext. The contrasting order of each 0 and 1 probe in the encryption keys is contained in the decryption keys. A category of meaningless information, a category of probes that corresponds to the two different types of bases, and a category of probes are used to categorise both the encryption and decryption keys in this study. It is necessary to create two DNA chips because the plaintext is split into two matrices, and these

Two DNA chips correspond two separate encryption and decryption keys. For a matrix made out of the nucleotide bases A and C, we need three different kinds of keys. Probe_A, Probe_T, and Probe_ATK are the three probes (ATK indicates the position of the nucleotide base, not both A and T). Among all encryption keys, one type of probe A and one type of probe T are both put in the nucleotide base A position and location, respectively. The regions without any information have one sort of ATK probe added in the middle of all the encryption keys. This is how we can make a DNA chip. We additionally require three extra types of keys: probe_C, probe_G, and probe_CGK for a matrix composed of the nucleotide bases C and G. CGK refers to the region of a nucleotide base that is neither A nor T. For the nucleotide base C position and the nucleotide base G position, each encryption key uses a specific kind of probe_C and a specific type of probe_G. In the areas with no data, one type of probe_CGK is spread among all encryption keys. In this way, we can produce another DNA chip. The receiver can get the plaintext by using the DNA microarray along with the decryption keys. If the encrypted ciphertext consists of a mixture rather than DNA chips, the DNA probe that corresponds to each bit of the plaintext binary matrix must be placed in the test tube. Because you are unaware of the hybridization signal intensity of each bit, each DNA probe must therefore correspond to a distinct bit of the matrix. If the cypher text is a DNA chip, the probe on each bit can be the same. The text that we encrypt in the paper is stored on a DNA chip. A DNA chip is the text that we encrypt in the paper. In order to completely use the DNA's plentiful resources and increase the critical space, each probe that is positioned on the chip is distinct. It is possible to use all of the stable substances present in biological materials as encryption keys, including DNA, PNA [8], and protein. The only difference is the various experimental approaches.

Encryption Method

1) Fig. 4 depicts the flowchart for the method's encryption procedure. 1) The binary sequence (N bits) from the plain text is converted before being processed in the subsequent steps. (1) Find the DNA sequence Q in the online gene pool and mark its path as Path_Q; (2) (3) Separate the binary streams of plaintext and the one derived from the DNA sequence Q into 8-bit chunks. From the DNA sequence Q, generate the binary stream Q2. We execute an XOR operation between the binary sequence created if the number of 1 in the binary sequence is odd, given the correct DNA sequence Q and the 8-bit plaintext binary sequence. In all other cases, the binary sequence created from the appropriate DNA sequence Q is combined with the 8-bit plaintext binary sequence using the XOR approach. Alternately, we can find a DNA sequence X in the online gene pool that contains N/16 or (N + 1)/16 nucleotides, and then we can track X's path through the online gene pool using the name Path_X. The binary sequence X2 is then created by converting X into an 8-bit binary block for each bit in the original sequence. XO If one bit's value is 1, then Q is completed. If not, then the appropriate 8-bit plaintext binary sequence should be rung with the binary sequence produced from the matching DNA sequence. The appropriate 8-bit plaintext binary sequence is then XO Red, Additionally, the related DNA sequence Q was used to generate the complement binary stream of binary sequence. It functions precisely like plaintext stream encryption.

2) The DNA sequence from step one is designated as W, and it is subsequently divided into n segments with lengths of N/n each. These n fragments of the DNA sequence go by the labels P1, P2,..., Pn. In order to prepare the sequence Pi, where i=1, 2,..., n, for the creation of primers for PCR amplification, si and ei are added to both ends. Each of the new sequences is then placed into a challenging area of the bio-genetic DNA. The vector DNA can be chosen using either the network's gene pool or the biological experiments section. The subsequent block-encryption of each DNA fragment creates new DNA blocks S1, S2,..., Sn. Then, a long DNA strand is created by rearranging and connecting these DNA building blocks.

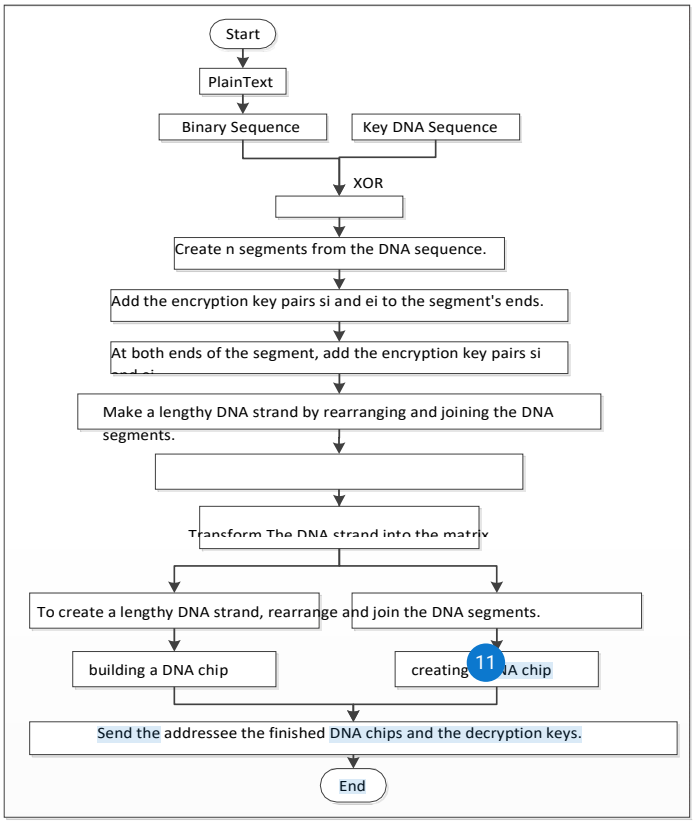


Fig 4. Flowchart for encryption

1) 3 The lengthy DNA The strand from step two is transformed into the matrix form (p*q) in accordance with a preset compositional arrangement. The matrix form is then encrypted using the newly developed encryption algorithm to produce the cypher text. The matrix is initially split into two separate matrices, one of which only contains the letters A and T and the other of which only contains the letters G and C. Then, for each point on the encryption DNA chip, we produce two distinct DNA sequences—two different sequences for A and T for the matrix that only contains A and T, and two different sequences for C and G for the matrix that only contains Using the two distinct DNA sequence keys produced in step 3, C and G create a DNA chip. The DNA chip size in this instance is p*2q. The matrix with just the characters A and T is represented by the left side of the p*q matrix. C and G use the two distinct DNA sequence keys that were produced in step 3 to create a DNA chip. The DNA chip in this instance is

p*2q in size. The matrix that just has A and T is shown on the left side of the p*q matrix. We choose the DNA sequence that corresponds to base position A on the DNA chip and put it there as the DNA probe. The DNA probe corresponding to that base is chosen and inserted into the appropriate location on the DNA chip if the nucleotide at that location on the chip is T.

Simulation

Using VC ++ 6.0, the cryptography technique is simulated in this study. We practise encrypting and decrypting data. The decryption was successful because the recovered plaintext matched the original data exactly.

Conclusions

Here, we describe a unique encryption technique that fully exploits the benefits of the biological riddle. Two major contributions are made by this study: (1) an analysis of the viability of developing a fresh approach to encryption based on the biological riddle, which provides a theoretical underpinning for the safety and viability of the suggested approach; and (2) a fresh approach to DNA cryptography based on DNA chip technology and the biological conundrum.

Through this research, we have created a helpful cryptography system, and the simulation results demonstrate its viability and security. This algorithm can serve as a guide for future work on DNA encryption techniques.

References

[1] Jiang J, Yin Z. The Advantages and Disadvantages of DNA Password in the Contrast to the Traditional Cryptography and Quantum Cryptography[C],the Eighth International Conference on Bio-Inspired Computing: Theories and Applications (BIC-TA), 2013. Springer Berlin Heidelberg, 2013:307-316.

[2] Andre´ L, Christoph R, Wolfgang B, Hilmar R. Cryptography with DNA binary strands [J].BIOSYSTEMS,2000,57(1): 13-22.

[3] Sivan S, Ron P, Yoav A, Ehud K. A Molecular Cryptosystem for Images by DNA Computing [J]. AngewandteChemie, 2012, 124(12): 2937-2941.

[4] Zhang Z, Shi X, Liu J. A method to encrypt information with DNA computing[C]// Bio-Inspired Computing: Theories and Applications, 2008. BICTA 2008. 3rd International Conference on. IEEE, 2008:155-160.

[5] Guangzhao C, LiminQ, YanfengW. An Encryption Scheme Using DNA Technology[J]. 3rd International Conference on Bio-Inspired Computing - Theories and Applications,2008:37-41

[6] Xin L M, Yuan C, Lei Q, et al. An encryption scheme based on DNA [J]. Journal of Xidian University, 2006, 33(6):939-942.

[7] Morford L. A theoretical application of selectable markers in bacterial episomes for a DNA cryptosystem[J]. Journal ofTheoretical Biology, 2011, 273(1): 100-102.

[8] Nielsen P E, Egholm M, Berg R H, et al. Sequence-selective recognition of DNA by strand displacement with a thymine-substituted polyamide[J]. Science, 1991, 254(5037): 1497-1500

ENCRYPTION OF IMAGES IN PART FOR REAL-TIME USE

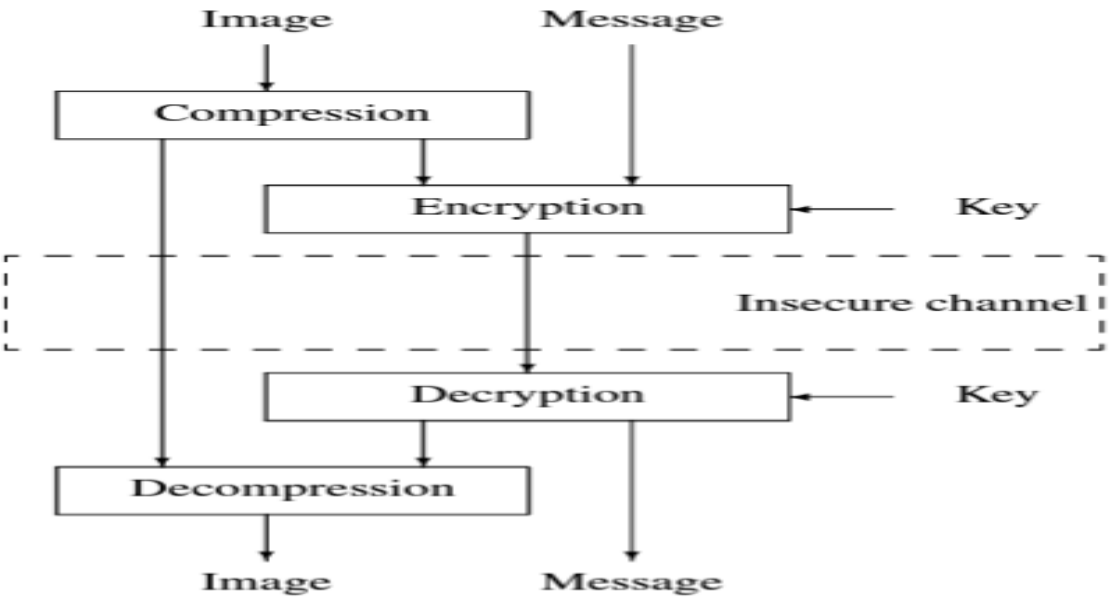
ABSTRACT

Most multimedia systems build their security on limiting access to services. This paradigm has a number of limitations when used in real-time imaging applications. Applications become open to password attacks, and if they are revealed, attackers can access every piece of information. The systematic encoding of every data is an alternative. This approach is problematic when working with photos because the data must be processed thoroughly before users can obtain any insight. Decryption demands a lot of computing power as well. With less overhead than complete encryption, this presentation demonstrates how partial encryption can satisfy application needs. The paper analyses a number of techniques combining picture encoding and encryption first. Then, we concentrate on a method that uses JPEG-based images to partially encrypt data. The method aims to satisfy two crucial requirements: maintaining the overall bit rate and maintaining compliance with the JPEG file format. As our final project, we propose and develop a news scheme that combines flexibility, multiple encryption, spatial selectivity, self-sufficiency, and format compliance. We provide examples of how it might satisfy the needs of real-time applications.

1. INTRODUCTION

When a communication enters an insecure channel, it should be standard procedure to conceal its content. Unfortunately, there is no way to convert a portion of the bit stream into cypher text before transmission in any of the audio-visual compression standards. An encryption algorithm and a key are needed for the encryption process. Decryption is the technique used to extract plaintext from encrypted data. Most cryptographers concur that the key should be kept private while the encryption method should be made public (KERKHOFF's law). It can be difficult to distribute keys in practise because they should only be exchanged after a rusted channel has been made. Speed, compression efficiency, and adaptability are additional concerns for real-time video systems that need to be addressed. Speed is dependent on both the processing type of the information and the encryption algorithm. Since compression and encryption are both presumed to be inevitable, there are practically only two options for real-time video transmission, depending on whether compression whether it does or not. First-pass compression lowers the bit stream but provides less confidentiality. However, compression is useless if encryption is applied first. Thankfully, there is a different option termed selective encryption, which operates as shown in Figure 1 and is the major theme of this research. Only some of the bit stream is

encrypted once the image has been first compressed. The flexibility to employ Any decoder is a fascinating additional capability for real-time applications, even if the bit stream contains some encrypted portions. In order to achieve bit stream compatibility, the bit stream should only be modified in places where it doesn't compromise adherence to the original format. Numerous Selective encryption techniques have been developed, however they typically call for a specialized decoder that is inappropriate for video transmission, as ISO standards dominate the industry.



specialised encoding mechanism

2. ENCRYPTION OF CHOICE OF CONTENSIONED IMAGES

2.1. Brief review

Around the middle of the 1990s, there were various papers on the selective encryption of MPEG streams. The MAPPELSet et al.[2] put out a technique that solely encrypts an MPEG stream's Intra (I) frames. But AGI et al. The inclusion of blocks encoded in intra mode in the POR B frames as well as the high correlation of P and B frames when they relate to the same I frame, according to [3,] make selective encryption of the I frames only offer a small amount of security. This method is susceptible to cryptanalysis, which is a common problem when compression comes before encryption. Alternative encryption techniques have been created by others. Numerous techniques have been proposed in particular for the encryption of DCT-based coded pictures. Zig-zag permutation is a method that TANG created. [4].Despite the fact that this method increases security, overall bit rate actually increases. The frequency distribution of adjacent pairs of two-byte bytes within an MPEG bit

stream is the foundation of a different strategy developed by QIAO and NAHRSTEDT.[5].The authors show that while this method offers overall security and size preservation, it falls short when it comes to visual acceptability and bit stream compliance. Other methods have recently been published (see [6] for a contemporary perspective), however they do not meet the following criteria:

[**Visual approval**] Even if some information is viewable, the encrypted image should appear noisy.

[**Selective cryptography**] After compression, encryption takes place, leaving some portions of the bit stream unencrypted.

The size of the bit stream should be preserved by [**constant bit rate**] encryption.

[**Compliance with bit streams**] The finished bit stream from the encryption procedure must match the format description provided.

Researchers have demonstrated that MPEG-encoded images are not the only ones that may use selective encryption. Examples include the approaches given by for the selective encryption of JPEG 2000 and wavelet packet sub band structures, see POMMER et al. [7] and NORCEN et al. [8].

2.2. A technique for selective JPEG picture encryption

MPEG was the main target for selective encryption due to its extensive use. However, because video transmission was a consideration when developing MPEG-2, the ability to selectively encrypt MPEG streams will be reliant on a reliable key distribution scheme. The significant correlation between frames causes an extra challenge. A video stream's redundancies are greatly reduced by MPEG-2, but a residual correlation caused by the encoder's error makes cryptanalysis impossible. We focus on the JPEG specification because it is used for point-to-point communication more frequently. The following theme was first suggested in [1]. Extensions will be covered in Section 3.

2.2.1. *A succinct explanation of compatible JPEG image specific encoding*

Runs of zeros are created by the HUFFMAN coder in JPEG by combining zero coefficients. It also uses symbols that pair magnitude categories that finish in zeros with non-zero coefficients to determine entropy. These symbols are given 8-bit code words by the HUFFMAN coder. Annexe bits that fully

indicate the magnitude and sign of non-zero coefficients come after these keywords. We made the decision to preserve the codes but encrypt the extra bits. This is due to the necessity of code words in synchronisation and the illogical substitution of non-zero coefficients for zero coefficients. Therefore, it's important to store away objects that have little worth. Additionally, since DC coefficients contain significant The HUFFMAN coder gives These characters are 8-bit code words. The annexe bits that follow these keywords fully reveal the magnitude and sign of the non-zero coefficients. We decided to preserve the codes while encrypting the extra bits. The reasons for this include the necessity of code words in synchronisation and the illogic of replacing zero coefficients with non-zero coefficients. Setting away objects with no worth is therefore essential.

3. 3. SELECTIVE ENCRYPTION EXTENSIONS

3.1. Multiple Elective Encryption, Section 3.
If there is only one copyright holder—hereafter referred to as owner—he will use key K1 to perform selective DCT encryption on a subset C1 of the JPEG picture coefficients. The final picture is g=Ek1(f). To avoid having to recalculate f at the receiver end of the decryption process, f= Dk1(Ek1(f)) and only if k1 is known. Since our method can handle any encryption method, we might have instead utilised an encryption strategy based on a public key and a private key. The second owner must be permitted to pick a portion of the DCT coefficients and encrypt them with his own key if there is a second owner. The formula for the image sent over the network is h= Ek 2 (Ek1(f)).When C1 and C2 are selected separately, we called this approach "multiple selective encryption."

3.2. Over-encryption

It is recommended to use the over-encryption technique, which is equivalent to Ek1(Dk2(Ek1(f))), as described by TUCHMAN [9], where C1 crosses with C2 (C1C2=), as double-encrypted coefficients are more vulnerable to attacks. Over encryption delivers superior results than Ek2(Ek1(f)), according to SCHNEIER [10].

3.3. Scheme for generalised selective encryption

In a wide context, we might offer:

1. Flexibility. The subset of DCT coefficients, or the encryption level, should be adjustable by the user.

2. Multiplicity. Assume that Information C1 and C2 will be encrypted by Owners 1 and 2. While C1 and C2 are preferably over-encrypted, they are independently encrypted. Figure 2 shows a photo that has been encrypted by Owner 1 (b) and Owner 2 (c), respectively. Remember that

parallelization is nothing more than multiplicity if C1C2=. (b) C1 and C2 do not need to be fixed during the entire encryption procedure. To increase secrecy, these coefficient sets could fluctuate at random over time.

3. conformity and independence. Side coder also needs the data C1, C2, and selection maps in order to decrypt the image. As stated by FRIDRICH [11], it is conceivable to integrate them within an image, however doing so will raise the bit rate.

TheschemedrawninFigure3implementsallthesepropertie. Data is divided into many segments. Some slices are left unmodified (this is referred to as part (1) on Figure3) while other slices(2) are processed by encryption blocks ordered into a sequence S. Slices are encrypted by known algorithms (RSA, Rijndael, etc) with different keys. Keep in mind that every encryption block could be unique. A slice should be over-encrypted if it is encrypted twice using the same technique. The selection map, which specifies which slice is encoded, and the encryption sequence S the decoder or otherwise described into an information stream I 1, which is subsequently encrypted into I 2, must be used by each encryptor or known to the decoder. It is necessary to know or supply the type of algorithms into a stream I3aswell. Then, all data—encrypted or not—are put back together to create a stream that complies with the format. The number of bits before and after encryption are equal in terms of merging. Since the original data is replaced with encrypted slices and there are few encrypted bits, substitution happens quickly to meet the demands of real-time processing. Two embedding steps come after merging.

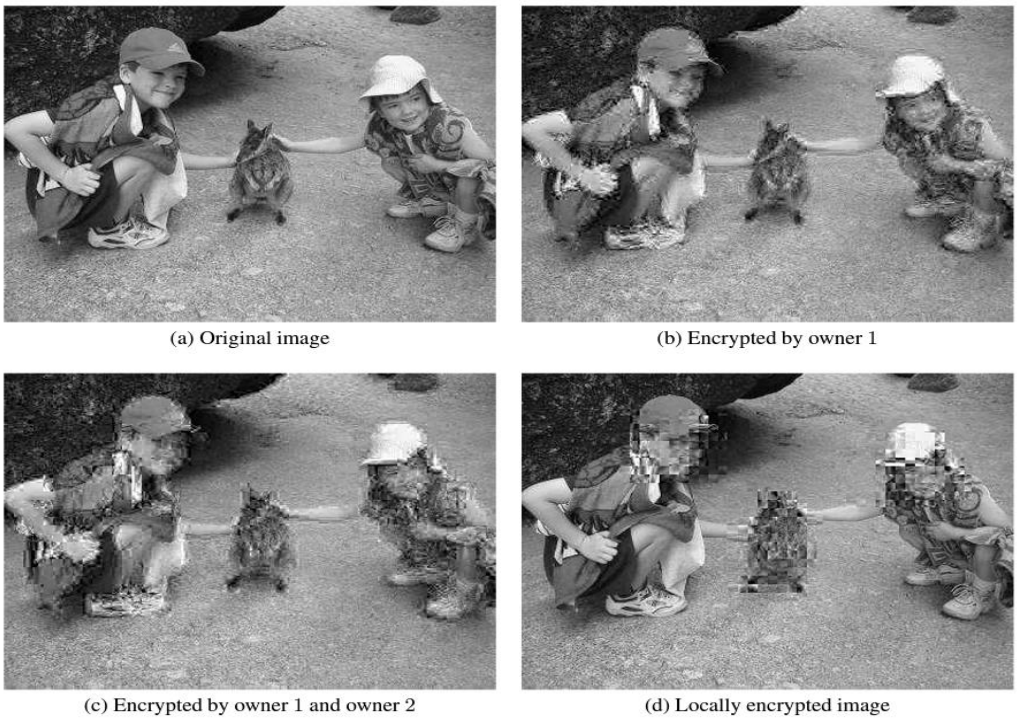
1. 1. All of the encryptor-related data, such as methods and keys in the case of public key cryptography, is embedded in the first step. There are numerous strategies Regardless of the data formats, the bit stream size is typically increased for embedding. Loss less data embedding techniques are utilised. Therefore, the header might need to be modified to account for changes.

2. The selection map and related data, such as used parameters, are embedded in the second phase. The embedding method is comparable to the earlier method.

Because the format is changed multiple times (it is not merely a substitute), both embedding procedures are difficult and time-consuming. But if the recipient has adequate information, embedding can be skipped without exposing more security flaws.

4. CONCLUSIONS

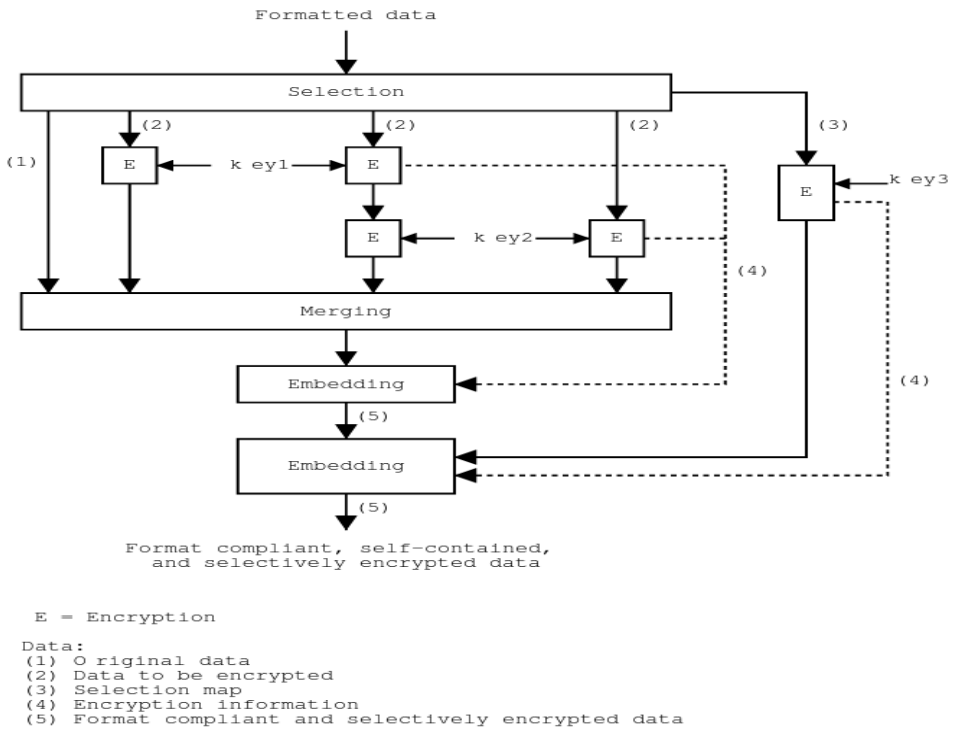
Here, we suggest a broad method for selectively encrypting images. Flexibility, multiplicity, spatial electivity, and format conformity are only a few benefits the scheme offers. The trade-off between processing speed and power leads to secrecy, but real-time processing is possible.



(a) Original image (b) Encrypted by owner 1

(c) Encrypted by owner 1 and owner 2 (d) Locally encrypted image

Flexible multiple encryption and spatial selectivity.



Self-sufficient selective encryption unit.

5. REFERENCES

[1]M.VanDroogenbroeckandR.Benedett,“Techniquesforaselectiveencryptionofuncompressed andcompressedimages,”inACIVSAdvancedConceptsforIntelligentVisionSystems,Ghent,Belgium, September2002,pp.90–97.

[2] T. Maples and G. Spanos, “Performance study of a selectiveencryptionschemeforthesecurityofnetworked,real-timevideo,”inProceedingsofthe4th InternationalConferenceonComputerCommunicationsandNetworks,LasVegas,Nevada,September 1995.

[3] I. Agiand L. Gong, “An empirical study of secure MPEGvideotransmission,”inSymposiumonNetworkandDistributedSystemsSecurity,1996.

[4] Lei Tang, “Methods for encrypting and decrypting MPEG video data efficiently, ”in ACM Multimedia, 1996,pp.219–229.

[5] Lintian Qiao and Klara Nahrstedt, “Comparison of MPEG encryption algorithms, ”Computers and Graphics,vol.22,no.4,pp.437–448,1998.
[6] A. Eskicioglu, “Multimedia content protection in digital distribution networks, ”Document available ontheInternet,2003.

[7] A. Pommer and A. Uhl, “Selective encryption of wavelet packet sub band structures for obscured transmission of visual data, ”in Proceedings of the 3rd IEEEB enelux Signal Processing Symposium (SPS2002),Leuven,Belgium,2002,pp.25–28.

[8] R. Norcenand A. Uhl, “Selective encryption of the JPEG2000bitstream,”inProc.IFIPTC6/TC117th Joint Working Conference on Communications and Multimedia Security(CMS2003),Lecture Notes in ComputerScience,volume2828,2003,pp.194–204.

[9]W.Tuchman,“HellmanpresentsnoshortcutsolutionstoDES,”IEEESpectrum,vol.16,no.7,pp. 40–41,July1979.

[10] B. Schneier, Applied cryptography, John Wiley& Sons,secondedition,1996.

[11]J.Fridrich,M.Goljan,andR.Du,“Loss less data embedding for all image formats,”in Proc.SPIE PhotonicWest,Vol.4675,ElectronicImaging2002, Security and Watermarking of Multimedia Contents, SanJose,California,January2002,pp.572–583.

Quantum Cryptography

ABSTRACT

Modern encryption Methods are constructed upon the basic, so-called "INTRACTABLE," factoring large integers into their prime factors. However, if mathematics and computing power improve, one-way operations like factoring enormous integers can be quickly reversed, making the security of the existing encryption vulnerable. A quantum physics-based evaluation of cryptography is the answer. One of the most recent topics in the computer industry is quantum cryptography. In this research, we focus on how quantum cryptography contributes to a defense-in-depth strategy for completely secure key distribution. This essay examines the

problems with current digital cryptosystems, the theoretical foundations of quantum cryptography, the practical uses of this technology and its shortcomings, and finally the future prospects of quantum cryptography. The quantum key distribution approach, in which two users exchange a random quantum transmission made up of exceedingly small flashes of polarised light before exchanging private or public keys, is implemented using an apparatus and protocol that we present in this work.

Keywords

Quantum physics, large-scale distributed computing, cryptosystems, and quantum cryptography systems.

1. INTRODUCTION

Recent news about European Union members' plans received a lot of attention for its decision to invest $13 million in the research and development of a secure communications system based on quantum cryptography. The system will function as a tactical deterrent to the US, Australia, Britain, Canada, and New Zealand's Echelon intelligence gathering system. SECOQC (Secure Communication based on Quantum Cryptography) is the name of the system. In addition, a small number of quantum information processing firms, such as MagiQ Technologies and ID Quantique, are putting quantum cryptography solutions into practise in order to satisfy the needs of organisations like businesses, governments, and other institutions where preventing the unauthorised disclosure of information has become essential to maintaining an advantage over rivals. Why is spending so much money on developing a new cryptosystem, quantum cryptography, when it is claimed that existing cryptosystems are extremely effective or "INTRACTABLE"

2. Modern cryptosystem limitations

Instead of encrypting huge amounts of data, public key cryptography is used to exchange keys because It requires lengthy, intricate calculations. For instance, well-known methods like the RSA and Diffie-Hellman key negotiation algorithms are routinely used to distribute symmetric keys across distant partiesFor the initial exchange of the symmetric key, both the speed of a shared key system and the security of a public key system can be used. Because asymmetric encryption is more slower than symmetric encryption, many organisations instead choose a hybrid strategy. As a result, this strategy makes use of both the public key infrastructure's scalability and the symmetric

key system's performance and speed. However, it is not known what the mathematical underpinnings of public key cryptosystems like RSA and Diffie-Hellman are. Instead, after years of open examination of the fundamental operation of factoring huge integers into their primes—which is considered to be "intractable"—it has been found that these techniques are adequately secure. In other words, the information it was protecting had already lost all of its value by the time the encryption mechanism was broken. The power of these algorithms hinges on the fact that there is no known mathematical method for factoring enormously big integers efficiently. Even while the public key cryptosystems currently in use may be "good enough" to provide a respectably high level of confidentiality, there are still a number of issues. Public key cryptosystems might become outdated if processing power advances, such as those brought about by quantum computing, fast surpass systems like RSA. Another example is the DES algorithm, which had a 56-bit key in the past and was regarded as secure but is no longer so due to advancements in technology that have made it simple to defeat. The successor Advanced Encryption Standard was created as a result of the fact that DES may be broken by sophisticated computers in a matter of hours. Therefore, there is a concern the possibility exists that future advancements in computer processing capability could make public key cryptography vulnerable. Secondly, it's ambiguous if there is or will ever be a theory that quickly factors big numbers into their primes. The assertion that it is impossible to establish such a factoring theorem is currently unsupported by any evidence. This makes public key systems susceptible to it and substantially increases the likelihood that the algorithm cannot be theoretically solved, as the likelihood of such a theorem forming is unpredictable. Areas of national security and intellectual property that need to be completely protected could be at risk due to this ambiguity. Current encryption is susceptible because of the ease with which mathematics can readily reverse one-way processes like factoring huge integers and because of advancements in processor power. Businesses, governments, militaries, and other affected institutions would need to spend a lot of money researching the risk of harm and possibly quickly deploying a new and pricey cryptography system if a factoring theorem was found or if computers were to advance to the point where it could beat public cryptography.

3. Theory of Quantum cryptanalysis

Instead of being constrained by the difficulties of factoring extremely large numbers, quantum encryption is based on the fundamental and constant laws of quantum mechanics. In fact, the two pillars of twentieth-century quantum physics upon which quantum cryptography is based are the Heisenberg Uncertainty theory and the photon

polarisation theory. Heisenberg's Uncertainty principle states that no system's quantum state can be measured without altering it. As a result, the polarisation of a photon or other light particle can only be determined at the time of measurement. This concept is essential for preventing hackers from breaching an encryption system based on quantum cryptography. On the other hand, the photon polarisation principle explains how light photons can be polarised or directed in specific directions. A photon filter is also necessary to detect polarised photons in order to prevent photon damage. Quantum encryption is the recommended technique for safeguarding data privacy and discouraging prying eyes because of the "one-way-ness" of photons and the Heisenberg Uncertainty principle. As part of a physics and information investigation, Charles H. Bennet and Gilles Brassard developed the concept of quantum cryptography in 1984. Bennet and Brassad assert that the quantity and mode of photons received by a recipient can be used to construct an encryption key. The discovery that light can function as both a wave and a particle is compatible with their theory. Due to the vast variety of polarisation angles that these photons possess, they can be utilised to represent bits like ones and zeros. By securely exchanging keys, these bits enable PKI systems and can be used to produce one-time pads. The polarised photon encoding of bits serves as the foundation for quantum cryptography, which in turn serves as the foundation for quantum key distribution. Therefore, quantum cryptography simply depends on the rules of physics and is independent of the processing power of present computing systems, whereas modern digital encryption exclusively rely on the computational difficulties of factoring very big numbers. The principle of physics will always hold true, thus it is no longer essential to make assumptions about the computer capacity of hostile attackers or the creation of a theory to quickly solve the massive integer factorization problem. The uncertainty issue with conventional cryptography is addressed by quantum cryptography.

4. An Example of Quantum Key Transmission

Here is an example of a secure key distribution method using quantum cryptography. In this illustration, "Alice" is the sender, "Bob" is the receiver, and "Eve" is the perverse listener. Alice first sends a message to Bob by firing a stream of photons from a photon gun in one of four polarisations (0, 45, 90, or 135) that stand for opposing vertical, horizontal, or diagonal directions. Using a photon receiver to count and measure each individual photon's polarisation, Bob will select a filter at random, which can be either rectilinear (0 or 90 degrees) or diagonal (45 or 135 degrees), record the results depending on which measurements were accurate in relation to the polarisations that Alice selected, and then select which measurements to repeat. Even if some of the photon stream splits up during the link, just a specified portion of the photon stream is

necessary to generate a key sequence for a one-time pad. Then, Without releasing the actual results, Bob will use an out-of-band communication technique to advise Alice of the measurement type that was carried out and which measurements were the appropriate ones. The polarisation of the photons that were measured correctly will be utilised to transform them into bits once the improperly measured photons have been deleted. The basic building blocks of a one-time pad used to send encrypted data are these photons. The key is the result of both Alice and Bob's arbitrary choices, so it's crucial to emphasise that neither Alice nor Bob can predict the key in advance. As a result, quantum cryptography makes it possible to reliably distribute one-time keys.

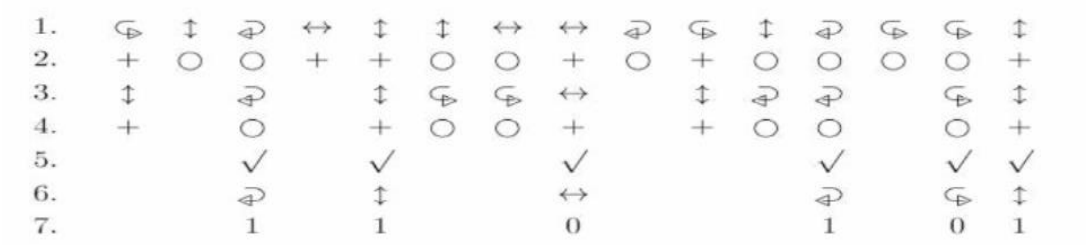


Figure 1: Basic quantum key distribution protocol.

1. Alice sends a random sequence of photons polarized horizontal (↔), vertical (↕), right-circular (↻) and left-circular (↺);
2. Bob measures the photons' polarization in a random sequence of bases, rectilinear (+) and circular (○).
3. Results of Bob's measurements (some photons may not be received at all).
4. Bob tells Alice which basis he used for each photon he received;
5. Alice tells him which bases were correct;
6. Alice and Bob keep only the data from these correctly-measured photons, discarding all the rest.
7. This data is interpreted as a binary sequence according to the coding scheme ↔ = ↺ = 0 and ↕ = ↻ = 1.

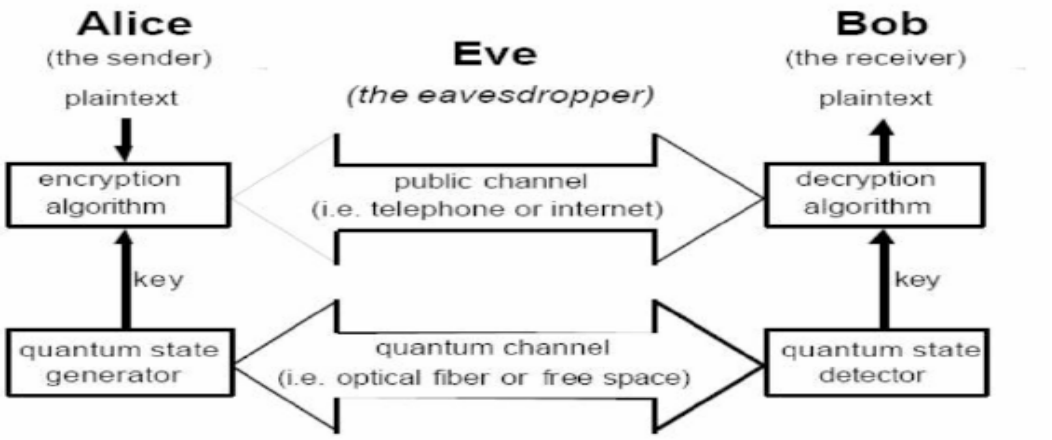


Figure 2. Quantum Key Distribution Example

Now consider the scenario when an adversary with malicious intent tries to hack the cryptosystem and undermine the quantum key distribution algorithms. The evil attacker Eave will also need to pick a rectilinear or diagonal filter at random in order to measure each of Alice's photons.

Eve won't have the option of asking Alice to validate the type of the filter, She will consequently have an equal chance of choosing the correct or incorrect filter. Even if Eve is successful in overhearing Bob and Alice verifying the protons they received, she won't be able to use this knowledge much unless she understands the correct polarisation of each individual photon. Because of this, Eve's attempts to render a meaningful key and accurately interpret the photons that make up the final key would be unsuccessful. This strategy offers a total of three notable advantages. It is firstly impossible to duplicate information about photons because doing so would lead to their destruction, according to the Heisenberg Uncertainty principle. Photons are unbreakable, therefore when they come into contact with a detector, they disappearThe length of the one-time pad must match the length of the message, therefore Alice and Bob must know in advance how many photons are required to create the encryption key. Given that Bob should, in theory, get 25% of the photons being delivered, a departure from the expected proportion may indicate that traffic is being sniffed or that there is a systemic issue. If Eve sees a photon, Bob won't be able to detect it since Eve can't reproduce an unidentified quantum state. Eve would be forced to pick a photon's orientation at random and would frequently be off by about 50%. This mistake rate would be sufficient to inform Bob of Eve's existence.

5. Desirable QKD Attributes

In general, QKD provides a means for two independent devices to concur on a shared random sequence of bits with a very low probability that other devices (eavesdroppers) will be successful in determining the values of those bits. These sequences are then utilised as secret keys for message encoding and decoding between the two devices according to a particular technique. It is clear from this background that QKD is a crucial distribution strategy, and the sections that follow list the major distribution objectives where QKD excels.

5.1 Confidentiality of Keys

The primary motivation for interest in QKD is confidentiality. The persistent misconception that decryption is technically impossible harms public key systems. Thus, key agreement primitives frequently employed in the current Internet security

architecture, such as Diffie-Hellman, may eventually be broken. This could reveal past traffic in addition to impairing communication in the future. Traditional secret key systems have been plagued by a variety of issues, considering the practical challenges of distributing keying material and insider threats. When QKD techniques are successfully incorporated into a system that is completely safe, they can produce automatic key distribution that may offer higher security than its competitors.

5.2 Authentication

QKD does not provide authentication by itself. Current approaches to Prepositioning secret keys at device pairs for use with hash-based authentication methods or hybrid QKD-public key approaches is one method of authentication in QKD systems. Neither strategy really appeals to me. Prepositioned secret keys must be sent in some way, such as by human courier, before QKD really starts, which could be expensive and logistically difficult. In the case that an adversary party forces a QKD system to run out of key material, at which point it is unable to finish authentication, this method also looks to be vulnerable to denial of service assaults. However, hybrid QKD-public key methods run the danger of having their public key infrastructure vulnerable to attack from quantum computers or unanticipated mathematical developments.

5.3 Rapid Key Delivery Enough

In order to prevent the supply of key bits in encryption devices from running out, key distribution systems must distribute keys as rapidly as possible. There is competition between the rates at which keying material is produced and consumed in encryption and decoding processes. In real-world scenarios, modern QKD systems frequently run at much lower rates and have a throughput for keying material of about 1,000 bits per second. This is an undesirable low value if one employs these keys in specialised applications, one-time pads for high-speed traffic, for instance. However, if the keying information is used as input for less secure (but frequently secure enough) methods like the Advanced Encryption Standard, it might very well be appropriate. But greatly outperforming the rates provided by the current QKD technology is both desirable and practicable.

5.4 Robustness

The QKD community has never previously given this much thought.

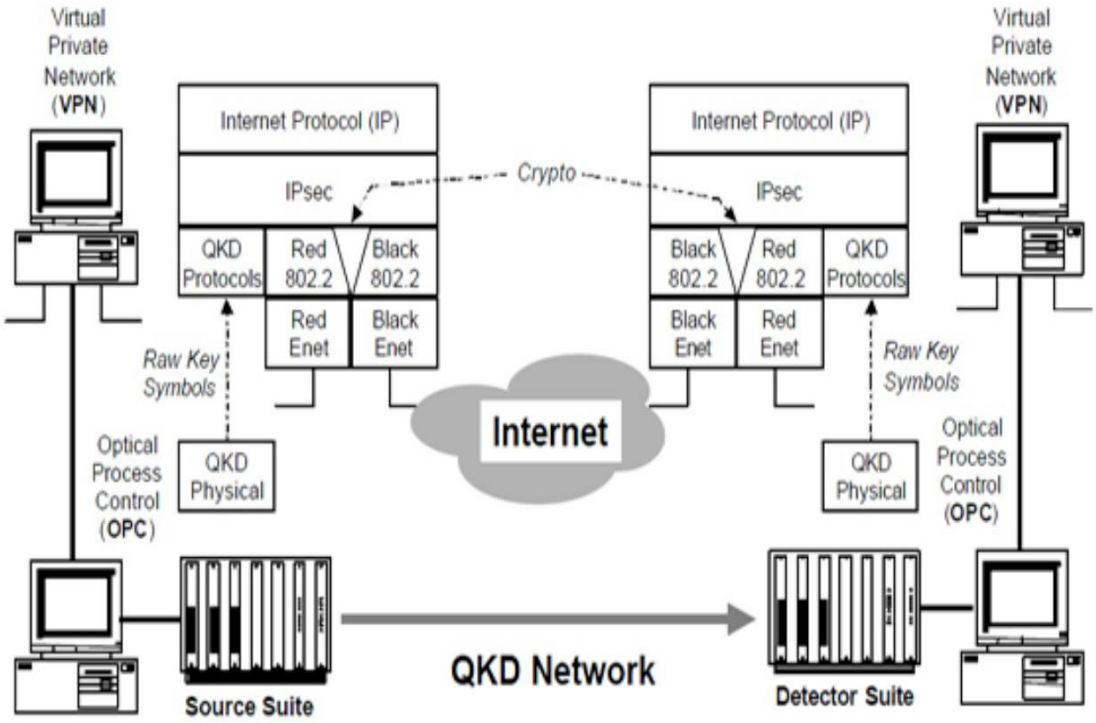
The flow of keying material must not be stopped, either by mistake or intentionally (via denial of service) by an opponent. This is essential because secure communications require keying material. This QKD service has been particularly susceptible up to this point given that just one point-to-point link has implicitly used QKD methods.

Any flow of keying material would stop if the link were to be broken, whether by active eavesdropping or simply a fibre cut. We claim that because a meshed QKD network provides several channels for key distribution, it is inherently more reliable than any single point-to-point link.

5.5 Distances and Location Independence

In a perfect world, any entity might come to an agreement on keying materials with any other (authorised) entity anywhere in the world. Surprisingly, the Internet's security design does have this feature: by selecting keys using the Internet IPsec protocols, any computer connected to the network can create a security relationship with any other computer.

This feature is conspicuously lacking in QKD, which can only operate over fibre for a short distance and necessitates a straight and obstruction-free path for photons to travel between the two entities.



5.5 Lack of Support for Traffic Analysis

A crucial distribution system may provide useful traffic analysis to adversaries. For instance, a considerable amount of private information may be moving between two locations or will do so in the future if there is a strong flow of keying material between them. It could be better to avoid such analysis as a result. QKD has typically taken a fairly poor approach in this area because dedicated, point-to-point QKD links between communication entities have been assumed in the majority of configurations, which lays out the underlying key distribution relationships explicitly.

6. Making use of quantum cryptography

Here, we go over a number of systems that successfully used quantum cryptography.

6.1 QUANTUM NETWORK DARPA

The virtual private network (VPN) is a cryptographic security concept developed by DARPA. Traditional VPNs employ symmetric and public-key encryption to secure communications and provide authentication and integrity. Public-key techniques allow for key agreement or exchange and endpoint authentication.

Both traffic secrecy and integrity are provided by symmetric techniques, such as 3DES and SHA1. Because of this, VPN systems may provide confidentiality, authentication, and integrity without putting their faith on the public network that connects the VPN sites. In DARPA research, keys provided by quantum cryptography are supplemented or entirely replaced by current VPN key agreement primitives. The VPN construct's remaining components are left unaltered; see Fig. 2. Therefore, normal Internet hosts, routers, firewalls, and other devices are fully compatible with the DARPA QKD-secured network.

6.2 Technologies MagiQ

MagiQ Technologies, a tech start-up with its headquarters in New York City, is one of the businesses creating solutions based on quantum cryptography. Among the target markets for MagiQ's solutions include academic and government labs, the financial services industry, and other industries. According to MagiQ's business strategy, current cryptography methods are supplemented by quantum cryptography rather than replacing existing encryption technologies like PKI in order to create a hybrid system that is more secure. The solution provided by MagiQ is called Navajo QPN Security Gateway. According to MagiQ, the first QKD system to be made commercially available is the quantum key distribution hardware box. Each unit costs around $50,000 and comes with a 40-pound chassis that fits in a conventional 19-inch rack. The system contains of the hardware and software

necessary for distributing quantum keys, as well as a photon transmitter and receiver. The Brassard and Bennet-proposed BB84 quantum encryption technique is used to connect these "black boxes" that are used by remote parties. For the purpose of preventing unauthorised access to data travelling across fibre optic networks, the Navajo system is designed to switch randomly generated keys once per second.

7. QKD Protocols Implementation

We refer to the unexpectedly complex set of specialised protocols used in quantum cryptography as "QKD protocols." Many of these protocols' peculiar characteristics, Experts in communications protocols could be interested in their peculiar implementation and justification.

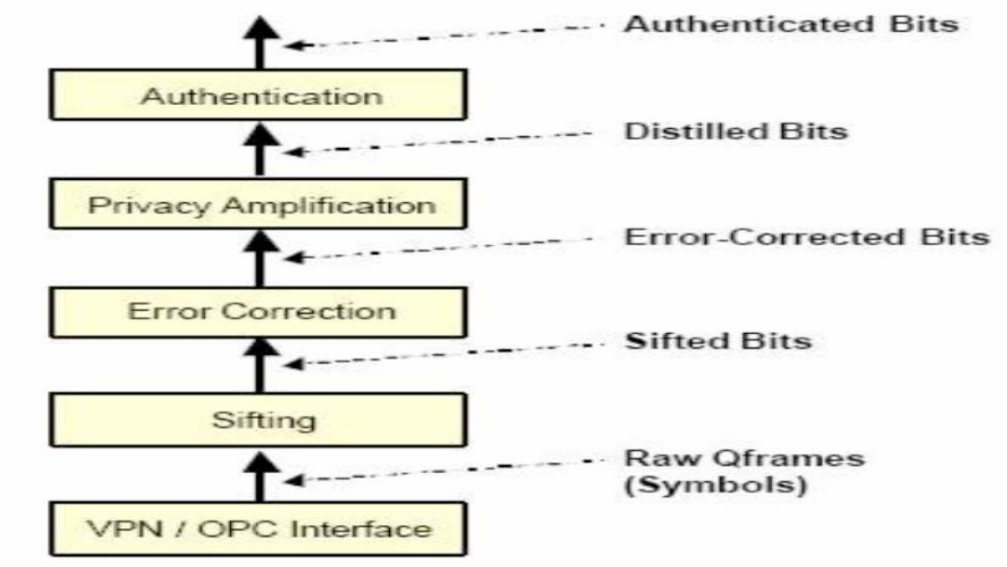


Figure 4. The QKD protocol Stack

This section provides a description of the protocols that are currently used in our C language implementation of the QKD protocol. DARPA built this engine to make "plugging in" new protocols straightforward, and they plan to spend a large amount of work in the next years developing and testing new QKD protocols. The easiest way to classify these protocols, as shown in Fig. 5, is as members of the QKD protocol family. But bear in mind that these layers don't necessarily correspond to the OSI layers or other tiers in a communications stack. As can be seen, they are actually approaching pipeline phases.

7.1 Sifting

Alice and Bob window all the obvious "failed q bits" from the pulses as they are being sorted out. As was said at the beginning of this section, examples of these failures include qubits where Alice's laser never sent, Bob's detectors weren't working, photons were lost during transmission, and so on. They also contain the symbols used when Bob chose one basis for receiving while Alice chose another. The useless symbols from Alice's and Bob's internal storage are eliminated following this protocol interaction, or a sift and sift response transaction, leaving just the symbols Bob was given, and Bob's justification is the same as Alice's.

7.2 Correction of Errors

The same sequence of error-corrected bits can be shared by Alice and Bob if they are able to identify and correct all of the "error bits" in their shared, filtered bits. Bits that Alice sent as a 0 but Bob received as a 1, or vice versa, are known as error bits. These bit mistakes could be caused by eavesdropping or background noise. The amount of hidden entropy that can be used for key material decreases due to the extremely uncommon requirement for error correction in quantum cryptography, which assumes that evidence revealed in mistake detection and repair (such as parity bits) was known to Eve. Designing error detection and correction algorithms that reveal as little as possible in their public control communication between Alice and Bob is hence strongly motivated.

Increasing Privacy

Alice and Bob can restrict Eve's access to their shared bits to a tolerable amount by utilising privacy amplification. Advantage distillation is a another name for this technique.

The side that commences the privacy amplification process prefers a linear hash function to the Galois Field GF[2n] where n is the input bit count, rounded up to a multiple of 32. The next four pieces of information he transmits to the other end are the m bits of the reduced result, the basic polynomial of the sparse Galois field, an n-bit multiplier, and an m-bit polynomial to add (i.e., a bit string to exclusive-or) with the product. The relevant hash is then executed on each side, and the output is truncated to m bits for privacy amplification.

7.3 Authentication

Through the use of authentication, Alice and Bob may defend themselves against "man in the middle attacks," enabling both Alice and Bob to be certain that they are

communicating with each other and not Eve. Continuous authentication is necessary used for all key management transactions because Eve could suddenly enter Alice and Bob's connection. The authenticating problem was covered in the original BB84 work [1], which also included a sketch of a solution utilising the universal families of hash functions Wegman and Carter had previously introduced [20]. To choose a hash function from the family and create an authentication hash of their public correspondence using this method, Alice and Bob must already have a little shared secret key. Even a malicious opponent with infinite computer power would have very little chance of producing the correspondence due to the nature of universal hashing if they lacked the secret key. The drawback is that even a single reuse of the secret key bits on unrelated data cannot be used to break the security.
Fortunately, many new shared secret bits from QKD can be verified by a complete authenticated discussion, they can be used to refresh the pool in tiny numbers. The numerous other elements in a practical system, such as symmetrically authenticating both parties, restricting Due of Eve's capacity to compel the shared secret key bits to exhaustion and her ability to adapt the system to network asynchrony and retransmissions, will only be briefly touched upon. Another crucial point is that we also need to authenticate VPN data flow; utilising these techniques to merely validate the QKD protocols is not enough.

8. Discussion and Conclusion

DARPA is currently building a number of QKD links that are woven into a bigger QKD network that consists of a mesh of QKD relays or routers in order to connect its QKD endpoints. One point-to-point QKD link inside the relay mesh is abandoned and another is used in its place when that link has a failure, such as a fibre cut, excessive eavesdropping, or noise. The Even in the face of active eavesdropping or other kinds of denial-of-service assaults, the DARPA Quantum Network can be constructed to be resilient. One term for such a structure would be "key transport network." Quantum repeaters may be able to get over the fundamental problem of unreliable QKD networks—their constrained geographic reach—in the future of the DARPA Quantum Network. In order to enable QKD operations across much greater distances than are now possible, Such repeaters are the subject of extensive ongoing investigation. If useful devices are ever developed, they ought to integrate seamlessly into the overall structure of untrusted QKD networks. As a potential remedy for the distance problem, chaining quantum cryptography links with secure intermediary stations has been put forth. Other options include transmission over void space or a low-orbiting spaceship.
The atmosphere attenuates less photons in this scenario because the satellite acts as the intermediary station. In order to transport quantum keys safely from satellites to

another location, research and development are now underway in both the US and Europe. Even though quantum cryptography has advanced significantly There are still difficulties to be resolved before it may be used after the previous 10 years by businesses, governments, and common people as a standard key distribution system. The development of more advanced hardware to provide higher quality and longer transmission lengths for quantum key exchange is exactly one of these challenges. However, the development of quantum cryptography will continue to be fueled by improvements in computer processing capacity and the fear of obsolescence for current encryption techniques. In fact, it is anticipated that during the following three years, almost $50 million in public and private funding will be invested in quantum cryptography technology3.

Although technology is still in its infancy, quantum cryptography appears to have a bright future. This technology has the potential to significantly improve personal security, government organisation security, and e-commerce and commercial security. Quantum cryptography will have a huge and revolutionary impact on all of our lives if it eventually proves to live up to even some of its expectations.

9. REFERENCES

[1] C. Bennett and G. Brassard, “Quantum Cryptography:Public Key Distribution and Coin Tossing,” International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 1984.

[2] A. Ekert, “Quantum Cryptography Based on Bell’s Theorem,” Phys. Rev. Lett. 67, 661 (5 August 1991).

[3] Ekert, Artur. "What is Quantum Cryptography?" Centre for Quantum Computation –Oxford University.Conger., S., and Loch, K.D. (eds.). Ethics and computer use. Commun. ACM 38, 12 (entire issue).

[4] Johnson, R. Colin. "MagiQ employs quantum technology for secure encryption." EE Times. 6 Nov. 2002..

[5] Mullins, Justin. "Quantum Cryptography's Reach Extended." IEEE Spectrum Online. 1 Aug. 2003.

[6] Petschinka, Julia. "European Scientists against Eavesdropping and Espionage." 1 April 2004. 7. Salkever, Alex. "A Quantum Leap in Cryptography." Business Week Online. 15 July 2003.

[7] Schenker, Jennifer L. "A quantum leap in codes for secure transmissions." The IHT Online. 28 January 2004..

[8] MagiQ Technologies Press Release. 23 November 2003.

[9] Schenker, Jennifer L. "A quantum leap in codes for secure transmissions." The IHT Online. 28 January 2004.

[10] C. Elliott, “Building the quantum network,” New J. Phys. 4 (July 2002) 46.

[11] Pearson, David. "High!speed QKD Reconciliation using Forward Error Correction." Quantum Communication, Measurement and Computing. Vol. 734. No. 1. AIP Publishing, 2004.

[12] Curcic, Tatjana, et al. "Quantum networks: from quantum cryptography to quantum architecture." ACM SIGCOMM Computer Communication Review 34.5 (2004): 3-8.

[13] Shor, Peter W., and John Preskill. "Simple proof of security of the BB84 quantum key distribution protocol." Physical Review Letters 85.2 (2000): 441.

[14] Bienfang, J., et al. "Quantum key distribution with 1.25 Gbps clock synchronization." Optics Express 12.9 (2004): 2011-2016.

[15] Inoue, Kyo, Edo Waks, and Yoshihisa Yamamoto. "Differential phase-shift quantum key distribution." Photonics Asia 2002. International Society for Optics and Photonics, 2002.

[16] Barnum, Howard, et al. "Authentication of quantum messages." Foundations of Computer Science, 2002. Proceedings. The 43rd Annual IEEE Symposium on. IEEE, 2002.

[17] Elliott, Chip, David Pearson, and Gregory Troxel. "Quantum cryptography in practice." Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications. ACM, 2003.

[18] Buttler, W. T., et al. "Fast, efficient error reconciliation for quantum cryptography." Physical Review A 67.5 (2003): 052303.

[19] Poppe, A., et al. "Practical quantum key distribution with polarization entangled photons." Optics Express 12.16 (2004): 3865-3871.

[20] Lütkenhaus, Norbert. "Estimates for practical quantum cryptography." Physical Review A 59.5 (1999): 3301.

18% Overall Similarity

Top sources found in the following databases:

- 14% Internet database
- Crossref database
- 9% Submitted Works database
- 9% Publications database
- Crossref Posted Content database

TOP SOURCES

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	atlantis-press.com Internet	3%
2	cs.stanford.edu Internet	3%
3	cs.tufts.edu Internet	2%
4	telecom.ulg.ac.be Internet	2%
5	Webster University on 2023-05-15 Submitted works	2%
6	Yunpeng Zhang, Zhiwen Wang, Zhenzhen Wang, Xin Liu, Xiaojing Yuan.... Crossref	1%
7	The University of the West of Scotland on 2022-05-06 Submitted works	<1%
8	R. Nagarajan, Kannadhasan S., Kanagaraj Venusamy. "chapter 3 Recen... Crossref	<1%

9	Shenzhen College of International Education on 2022-12-16 Submitted works	<1%
10	dtic.mil Internet	<1%
11	download.atlantis-press.com Internet	<1%
12	University of Melbourne on 2016-10-31 Submitted works	<1%
13	fdokumen.id Internet	<1%
14	CSU, Pomona on 2021-12-14 Submitted works	<1%
15	giac.org Internet	<1%
16	Leiden University on 2021-03-26 Submitted works	<1%
17	Shenzhen College of International Education on 2023-03-24 Submitted works	<1%
18	journal.uestc.edu.cn Internet	<1%
19	University of Bath on 2012-05-07 Submitted works	<1%
20	Manish Kumar, Shriniwas Patil, Keyur Parmar. "Secure Protocol for VA... Crossref	<1%

21	Sri Lanka Institute of Information Technology on 2022-11-28 Submitted works	<1%
22	Texas A&M University, College Station on 2007-04-17 Submitted works	<1%
23	Universiti Teknologi Malaysia on 2010-04-15 Submitted works	<1%
24	University of Maryland, University College on 2005-11-11 Submitted works	<1%
25	link.springer.com Internet	<1%
26	orbi.uliege.be Internet	<1%
27	"Quantum Computing:An Environment for Intelligent Large Scale Real ... Crossref	<1%
28	Chip Elliott. "Building the quantum network*", New Journal of Physics, ... Crossref	<1%
29	Sri Lanka Institute of Information Technology on 2021-10-21 Submitted works	<1%
30	University of Bath on 2008-03-13 Submitted works	<1%
31	University of Bath on 2012-05-09 Submitted works	<1%
32	ijsrset.com Internet	<1%

33 cc.gatech.edu

Internet

<1%