Journal of King Saud University – Computer and Information Sciences xxx (xxxx) xxx

Contents lists available at ScienceDirect

Journal of King Saud University – Computer and Information Sciences

journal homepage: www.sciencedirect.com

The recent trends in cyber security: A review

Jagpreet Kaur, K .R. Ramkumar *

Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India

ARTICLE INFO

Article history:
Received 5 October 2020
Revised 4 January 2021
Accepted 24 January 2021
Available online xxxx

Keywords:
Cyber security
DES
RSA
Key management
Quantum cryptography
Prime factorization
Side channel attacks

ABSTRACT

During recent years, many researchers and professionals have revealed the endangerment of wireless communication technologies and systems from various *cyberattacks*, these attacks cause detriment and harm not only to private enterprises but to the government organizations as well. The attackers endeavor new techniques to challenge the security frameworks, use powerful tools and tricks to break any sized keys, security of private and sensitive data is in the stale mark. There are many advancements are being developed to mitigate these attacks. In this conjunction, this paper gives a complete account of survey and review of the various exiting advanced cyber security standards along with challenges faced by the cyber security domain. The new generation attacks are discussed and documented in detail, the advanced key management schemes are also depicted. The quantum cryptography is discussed with its merits and future scope of the same. Overall, the paper would be a kind of technical report to the new researchers to get acquainted with the recent advancements in Cyber security domain.

Contents

* Corresponding author.
E-mail addresses: jagpreet.kaur@chitkara.edu.in (J. Kaur), k.ramkumar@chitkara.edu.in (K .R. Ramkumar).
Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

https://doi.org/10.1016/j.jksuci.2021.01.018
1319-1578/

Please cite this article as: J. Kaur and K .R. Ramkumar, The recent trends in cyber security: A review, Journal of King Saud University – Computer and Information Sciences, https://doi.org/10.1016/j.jksuci.2021.01.018

1. Introduction

The world is experiencing rapid growth in cyberspace today (Arora, 2016). Such an extraordinary growth in information- access gives opportunities to those with malicious intentions. It is the need of the hour (Arora, 2016) and the act of protecting the systems and technologies from unusual activities. Cyber security means maintaining the Integrity, Confidentiality, and Availability (ICA) of computing assets belonging to an organization or connecting to another organization's network. Due to the evolution and increase of cyber threats, many researchers believed and urged to educate the new generation about the concepts of cyber-security (Lunt et al., 2011). Cyber-crimes occur due to negligence in cyber-security and awareness among the clients (Schneier, 2018; Albrechtsen, 2007). As stated in the recent research (Jasper, 2017; Abdallah et al., 2018), the US has introduced the threat intelligence frameworks. This framework works on the principle of gathering information from various sources which have been carefully examined by human security experts. Besides, researcher also taking aid of machine learning techniques to analyze threats which in advanced way respond to attack incidents (Emmanuel et al., 2020). The United Kingdom has introduced its own National Cyber Security Strategy 2016–2021 that resembles the ideas to that of the 2011 version (Niekerk and Solms, 2013) and has allocated a budget of £1.9bn for the Cyber Security Programme (UKCyber Security Strategy. National Cyber Security Strategy, 2016). As close as to 70 nations have addressed this issue through national cyber/information security strategies and significant legal acts in some type of strategy document describing their national security and defense strategies (Apostolopoulos et al., 2018). In fact, under the cyber network guide, the preplanning of vulnerabilities which includes the timely information exchange regarding threats which may lead to protect various entities such as environment, business, infrastructure and is capable of understanding the situational incidents accordingly (Fiedelholtz, 2021).

In most recent studies, Cybersecurity is defined as a comprehensive term (ISO, 2018). ITU-T X.1205 also defines cybersecurity in their draft (International Telecommunications Union (ITU), 1205). Hence, in generalized term cyber security which helps prevent cyber attacks, data breaches and can aid in risk management. The Security architecture defines some characteristics of security which include security attacks consists of two types: active and passive attacks and security objectives (Stallings, 2006).

In general, the threats include various scenarios such as Cyberbullying (Smit, 2015), Identity theft (Michel et al., 2015), Digital devices (Smit, 2015) Autonomous systems (Miller et al., 2017), Wireless Sensor Networks (WSN) and Wireless body area Networks (WBAN) (Aslam et al., 2020), Cyber terrorism (Smit, 2015), and can approach us from unforeseen sources and directions. With the advancements in science, more sophisticated cyber-crimes and malicious activities are evident in today's world which is targeted and extremely dangerous. One such example was detected earlier in 2018; a ransomware attack was harming the government of Atlanta City (Conti et al., 2018) and other recent cyber breaches (Ruohonen, 2019).

This paper is structured to start with the common attacks in section 1.1 to have a glimpse of various attacks in general. Section 1.2 starts with the historical background of cryptographic standards and gives an overview of the same. The recent advancements of asymmetric algorithms are discussed in Section 2 that is continued with the advancements of key management schemes, as a summary, Table 2 gives a list of attacks mitigated because of recent advancements. Quantum cryptography is a term that brings a new dimension to cryptographic algorithms; Section 2.2 gives a succinct of quantum key distribution and management with proper examples. In section 3, a predominant attack called side-channel attack is scheduled to know the real and future attacks that are quantum-resistant even; these attacks still exist as a big threat to the cybersecurity world. In Section 4 we have given the summary of this paper. This paper will be an avenue for new researchers and covers the major issues and advancements of cybersecurity.

1.1. Attacks classification

This section introduces multifarious types of attacks in different domains and is further categorized as shown in Fig. 1.

1.1.1. Cryptographic attack

Type of attack in which the adversary breaks the cryptography, pragmatically, to discover the shortcoming in an exceeding protocol, code, or ciphers to retrieve the plaintext without the key.

1.1.2. Access attack

Type of attack where the perpetrator procures ingress to the host's machine where they have no right to use with the intent to manipulate information. Web application services and File Transfer services are being compromised where attackers able to access e-accounts, databases, and other private information.

1.1.3. Reconnaissance attack

An attack in which the perpetrator maps with targeted systems to scan any vulnerability in the machine to gather information. This is a kind of scenario similar to stealing for instance in the house which is vulnerable to break locks, doors, and windows that are not strong and are joined.

1.1.4. Active attack

An attack, while transmission of data alters the content and affects the operations thereby serve as an intercessor, leads to severe damage.

1.1.5. Passive attack

The database is neither intrudes nor amends by the attacker; however, only monitors the target to access the information throughout the transmission. In other words, the attacker's main aim is to collect the information by listening to a conversation between hosts through several means.

1.1.6. Phishing attack

An act of sending fallacious messages via many ways such as emails, text messages, etc. that tends to become from the legitimate resource, thereby, deceive users and obtain sensitive and confidential information such as login passwords, card numbers.

1.1.7. Malware attack

An attack where a perpetrator deliberately installed malicious software on the host's computer intending to not only proliferate

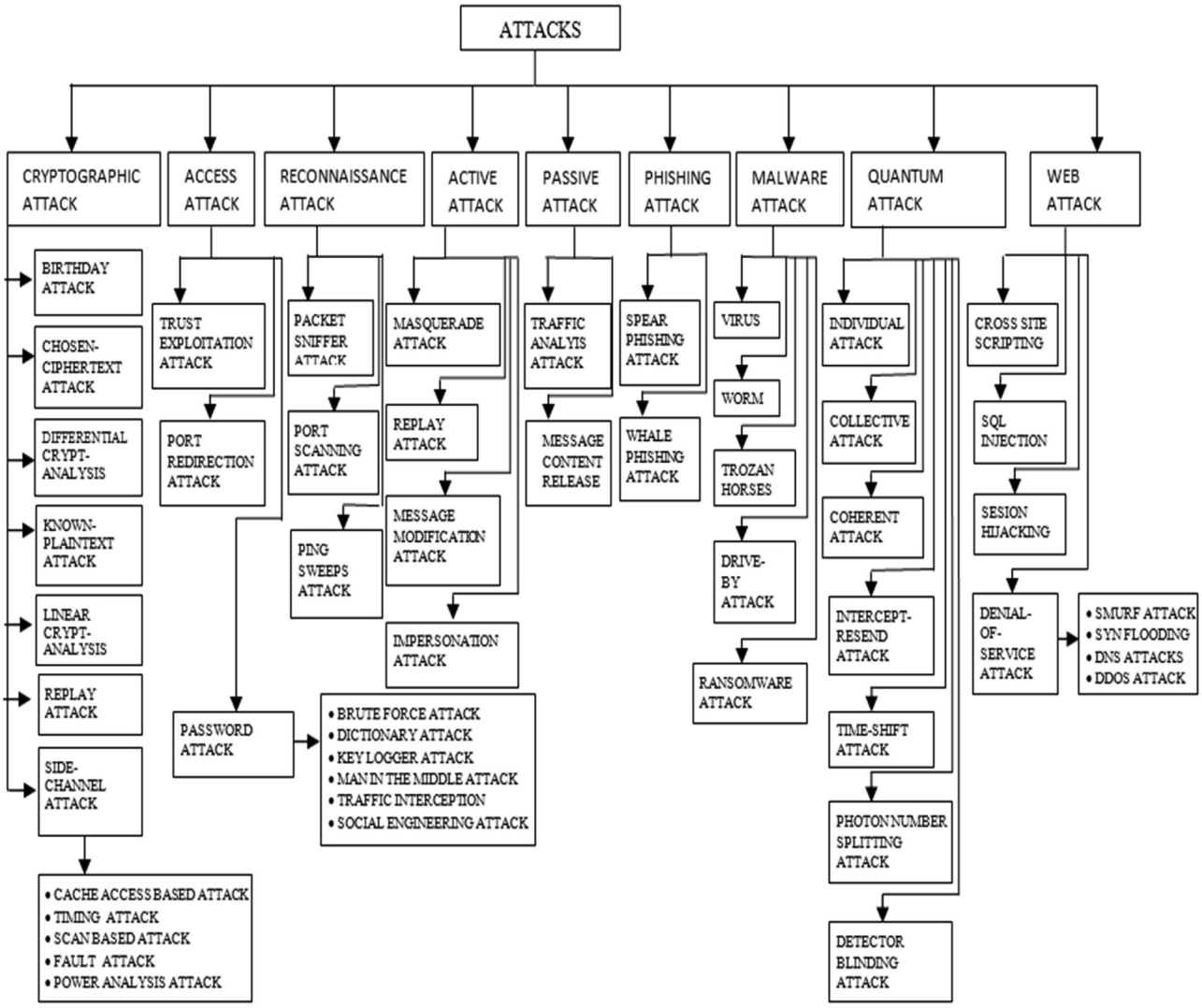

Fig. 1. Different attack types.

virus, nonetheless but also infect and harm the computer, thereby, gain private data.

1.1.8. Attack on quantum key distribution

An attack has done while transmitting any data through a quantum channel either by forge a single photon, multiple photons, or by time elapsing of pulses.

1.2. Standard security frameworks

1.2.1. Historical background

Data security is the main challenge of any network communication; hence there exist many algorithms to solve the security issues. The history of cryptography and the encryption algorithms are discussed in the section below (Dagmar et al., 2007). Cryptography was first invented by Spartans (Djekic, 2013) in some 400BCE for transmitting data securely between militants. They named their tool as scytale to encrypt their messages. Earlier times substitution method is used to encrypt the data. It replaces each letter of the plain text with another letter which is shifted with some fixed number between 0 and 25. The ciphertext can be decoded only if one knows the secret shift. For example, the string "modern" will become "oqftp" and can be decoded if one knows the secret shift is two. The message becomes more secure if the secret shift of each letter is different. For example, the string "modern" will become "rqekut" having a secret shift "421636". If the plain text is combined with some key with random values having the same keyword length as that of plaintext, we would call it a one-time pad and ensure the security of the message at that time.

Modern security techniques as shown in Fig. 1 are complex but the basics remain the same. The security algorithms are categorized into symmetric and asymmetric algorithms (Simmons, 1979) having the same basic functionality of XOR-ing, confusion and diffusion of data (Stallings, 2006).

1.2.2. Early generation of cyber security algorithms

DES was once a primary symmetric-key algorithm (Standard, 2018) published in 1977. Initially, DES works with a 64-bit block size with a 56-bit key. DES works on equal block size and uses both confusion and diffusion in the algorithm. However, due to its small key length, DES is considered to be unsafe. In 1999, Electronic Frontier Foundation in collaboration with distributed.net had broken the DES key in less than 24 h using a brute force attack (Dhole and Verma, 2012). Hence, in 2005 DES with other FIPS is withdrawn (NIST, 2018). There are various other attacks (Biham and Shamir, 2012; Matsui, 1993; Biham, 1994; Biham and Biryukov, 1997) that can break the DES with less time complexity than brute force. Accordingly, Triple DES was expanded with Encrypt-

Table 1
Modified algorithm – RSA.

GENERATING KEY	
Choose a, b, c	a, b, c are prime, a≠b≠c.
Compute s= a * b * c	
Compute Ø(s)= (a-1) * (b-1) * (c-1)	
Choose e	√s<e<Ø(s) ; GCD(Ø (s),e) =1
To replace s select Y such that	
▯ Take Y in order that s- a < Y < n and GCD(Y , s) = 1 if a>b	
▯ Take Y in order that s - b < Y < n and GCD(Y , s) = 1 if a<b	
Compute d	
Public Key	PU={e,Y}
Private Key	PK={d,Y}
ENCRYPTION	
Plain Text	P < s
Cipher Text	CT = P^e mod Y
DECRYPTION	
Cipher Text	CT
Plain Text	P=CT^d (mod Y)

Decrypt- Encrypt (EDE) mode, and hence the size of the key is 168 bits (Bhanot and Hans, 2015).

But there was a new attack that introduced is a meet-in-the-middle attack that challenged 3 DES. Therefore, in 2001, NIST (Diehl and Laws, 2016) declared and choose a new cipher, AES, invented by Rijmen and Daemen. AES works with distinct length keys – 128, 192, and 256 bits. Larger the key bits, the safer the transmission. Despite of many attacks (recovery attack and side-channel attack) on AES, till now it has not been broken and considered safe. In 1993, Blowfish (Bhanot and Hans, 2015; Schneier, 1993) was designed by Bruce Schneier having key length varies between 32 bits ranges up to 448 bits with a 64-bit block size. This algorithm is vulnerable to birthday attacks due to its block size.

One of the earliest key exchange methods in cryptography was published in 1976 and is known asDiffie–Hellman key exchange (Diffie and Hellman, 1976). It is an algorithm in which two parties evaluate the shared secret which can be used as an encryption key, over an unprotected same communication channel; the problem is also called the discrete logarithm problem. The sender and receiver computation is based on exponentiation performed over a modulus. Since using modulus this becomes a one-way function which makes it difficult for the illegitimate user to get the secret key. However, the man-in-the-middle attack also jeopardizes its security. In 1978, Rivest–Shamir–Adleman (Rivest, 1978; Mohapatra and Cryptography, 2000) proposed a public-key algorithm based on the factoring problem (Vaudenay, 2006).

2. Recent developments and emerging trends of cyber security

There are many recent developments in cyber security with the help of new algorithms, procedures and frameworks. This section discusses in detail about imperative mathematical equations, worked out samples, flow diagrams, overcome attacks along with their vulnerabilities and the various improvements over the existing standards over the years.

2.1. Advancements in s

The world is moving towards a new phase of security for asymmetric schemes that promised to provide security to prevailing security problems. Instead of using the predetermined matrix properties, problems are resolved using polynomials. Marcin (Kapczynski and Lawnik, 2019) proposed two cryptosystems based on the chebyshev theorem and that proves the less time and space complexity. However, performance analysis and security challenges still to be overcome. On the same hand, Gomez (Gómez, 2009) proposed a scheme based on the concepts of multivariate cryptography using the concept of hidden irreducible polynomials having some issues related to this design that it lets the perpetrator discover the private key directly from the public key.

Chowhan and Jaju (2015) introduced a modified RSA the public-key encryption algorithm and performs a comparison based on security and time complexity by operating data of distinct sizes. According to the author, the algorithm works as follows with three prime numbers and two more constraints to make the system more stable as delineated in Table 1.

The algorithm becomes more efficient with the increase in Security levels and key generation speed. Nevertheless, findings say that in terms of speed of encrypting and decrypting text and overall execution time RSA is still better.

Aggarwal and Maurer (2016) has outlined the factoring problem of RSA and demonstrates that the issue of factoring N can be effectively mitigated by Generic Ring Algorithm (GRA) which executes ring operations namely add and multiply, inverse ring operations namely subtract and divide, and equality test that specifies which two results need to be compared. According to this paper, RSA presumes that message m ∈ Zn, it is encrypted as mx (mod n), where x > 1 and gcd (x, Ø (N)) = 1. The security of this algorithm is based on the fact that, given r, selected randomly from Zn, it is difficult to find m such that mx - r≡ 0 (mod n). This paper shows that under the factoring scheme RSA and digital signature algorithms are not vulnerable to several attacks and is hard to break RSA by using ring operations.

Hwang et al. (2016) has outlined an essential form of public-key cryptography known as Identity Based Encryption (IBE). Employing this scheme author proposed a new certificate-based encryption technique based on pair less cryptography, which provides security against in distinguishability under Chosen Ciphertext Attack (IND-CCA) and is used in many applications like resource-constrained node networks. The algorithm works in the way in which the sender encrypts the data by performing the mentioned steps as:

Step1: Selects the random integer σ ∈ {0, 1} n and evaluate:
(a) n = HS_3 (MS, σ)
(b) QC_{id} = HS_1 (id, US_{id}, PC_{id})
(c) HS_{id} = HS_5 (QC_{id}, US_{id}, PC_{id}, g1)

Table 2
Methods with their Attacks and vulnerabilities.

Paper	Method detail	Mitigated attacks	Vulnerabilities/Limitation
(Kapczynski and Lawnik, 2019)	Ciphering utilizing variable key length	Resistant against various attacks such as side channel attacks , related key attack, chosen plain text attack	Space and Execution time increases enormously.
(Aggarwal and Maurer, 2016)	Utilizing Generic Ring Algorithm for RSA factoring problem	Mitigated factoring issue of RSA	Vulnerable to various cryptanalytic attacks.
(Hwang et al., 2016)	Certificate-based encryption based on pairless cryptography	Mitigates Chosen Cipher text Attack	Vulnerable to Denial-of –Service attack, inefficacious for limited bandwidth.
(Fujisaki, 2018)	Involves public key encryption based upon a binary string with apt length.	Mitigates Man –in the middle attack	Vulnerable to Denial-of –Service attack.
(Dwivedi, 2011)	Message recovery through distribution-transforming encoder	Secure against Brute force attack	Vulnerable to known-Plaintext attacks.
(Biswas and Mohit, 2016)	Integrating RSA within DES	Secure from different attacks	Vulnerable to known-cipher text attack, brute force attack
(Hazay et al., 2018)	Resolve factoring problem using two party distributed.	Secure from malicious attacks	Space and Execution time increases enormously.
(Chie, 2018)	Generate session keys using key agreement scheme	Models against active and passive attacks	Vulnerable to Third-Party attack.
(Thangarasu and Selvakumar, 2018)	Securing session keys using modified ECC	Mitigate Intruder attacks	Suffers from traditional Attacks
(Barbulescu and Duquesne, 2017)	Propose novel key sizes using NFS variant	Mitigate dos, impersonation attacks and replay attacks	Not accessible by the multi-server environment

(d) Key1 = $(US_{id}^{HS_{id}})^{n}$
(e) Key2 = $(PC_{id}\ g1^{\ HS\ (QC\ PC}_{2\ \ \ id\ \ id})^{n}$
Step2:
(a) Evaluate $CT_0 = g^{n}$
Step3:
(a) Evaluate $CT_1 = HS_4$ (Key1, Key2) (MS || σ).

where MS = message to be encrypted, HS_1 – HS_5 = generated hash functions, QC_{id} = certification query, HS_{id} = hash id, US_{id} = user public key id, PC_{id} = public certifier random generated id, g and g1 are ring generators calculated over prime numbers, CT_0 and CT_1 are the cipher texts.

Sender sends the encrypted text to Receiver as CT = (CT_0, CT_1). The receiver also computes the Q_{ID} and H_{ID} same as the sender and also computes MS || σ with the following equation:

Step 4:
(a) $HS_4\ (CT_o^{(a_{id})(H_{id})}, CT_o^{C_{id}})\ CT_1$

If the abovementioned equation gives a result equivalent to MS || σ then the decrypted text is correct, and it returns M by discarding σ; otherwise, returns null. Certainly, security increases but with the increase in the cipher size communication overhead increases for the bandwidth-limited networks. Moreover, clients put requests for the key management server concurrently leads to obstruction in the system.

Fujisaki (Fujisaki, 2018) presents an encryption scheme called an all-but-many encryption scheme which involves public- key encryption based upon a binary string with apt length. According to this theme, to unlock the message with stable haphazardness, the sender stated the confidential key which initiates a forgery cipher text. However, any person not possessing the private key can neither perceive a fake cipher text from a genuine one nor produce a fake one. They proposed a framework for erecting an all-but-many encryption scheme with expansion factor O(1), which brings the first fully equipped universally configurable commitment scheme.

Dwivedi (2011) and Maheswara and Valluri (2012) along with many other researchers work with polynomials to give a new direction to security algorithms. However, Jia et al. (2017) proves that their algorithm based upon Polynomial symmetrical decomposition (PSD) problem, the main objective is to provide security owing to the fact the algorithms based upon factorization or logarithmic problems are under threat of breaking soon due to the availability of quantum computers. The author proves that these algorithms are vulnerable to a multitude of attacks as they require rendering a similar secret for multiple given public keys. Thus, in this algorithm, an improved polynomial scheme is proposed based on two operations as a b, and a b.

Fujisaki and Okamoto (2013) designed a secure integration of symmetric and asymmetric strategy. They introduced a new hybrid technique the converts a frail symmetric and asymmetric strategy to an asymmetric strategy that is chosen-cipher text secure. Their hybrid scheme works in a sense such that encrypted message MS is defined as:

$$\varepsilon_{P_k}^{H}(MS;\sigma) = \varepsilon_{P_k}^{AS}(\sigma; H(\sigma,e)||\varepsilon_{G(\sigma)}^{S}(\mathrm{MS}) \quad (1)$$

where

$\varepsilon_{P_k}^{AS}$ (Message; bits) represents message encryption using asymmetric algorithm using randomized bits.

ε_{a}^{S} (Message): represents message encryption using symmetric algorithm utilizing the private key a.

σ is an arbitrary string selected over a proper domain.

e= $\varepsilon_{G(\sigma)}^{S}$(MS)

G and H indicate hash functions.

Biswas and Mohit (2016) proposed a novel asymmetric algorithm by integrating RSA and DES. To make DES more secure authors modified the structure by encrypting the plain text with RSA and the receiver's public key to acquire the cipher text. In this technique, 64-bit plain text is divided into parts left and right and performs the computation as shown in Fig. 2.

The equation carried out for encrypting the plain text is as described below:

$$Li = EN_{RSA}(R_{i-1}) \quad (2)$$

$$Ri = L_{i-1} \oplus F(R_{i-1}, k) \quad (3)$$

In the similar way, Digital signatures are also implemented in asymmetric DES. Apart from security, the algorithm works under the RSA cryptosystem that increases the complexity and computation cost and is endangered to brute force attack which makes the system weaker.

Jianghua Liu along with other researchers (Huang et al., 2019) worked upon data authentication to preserve data online. With

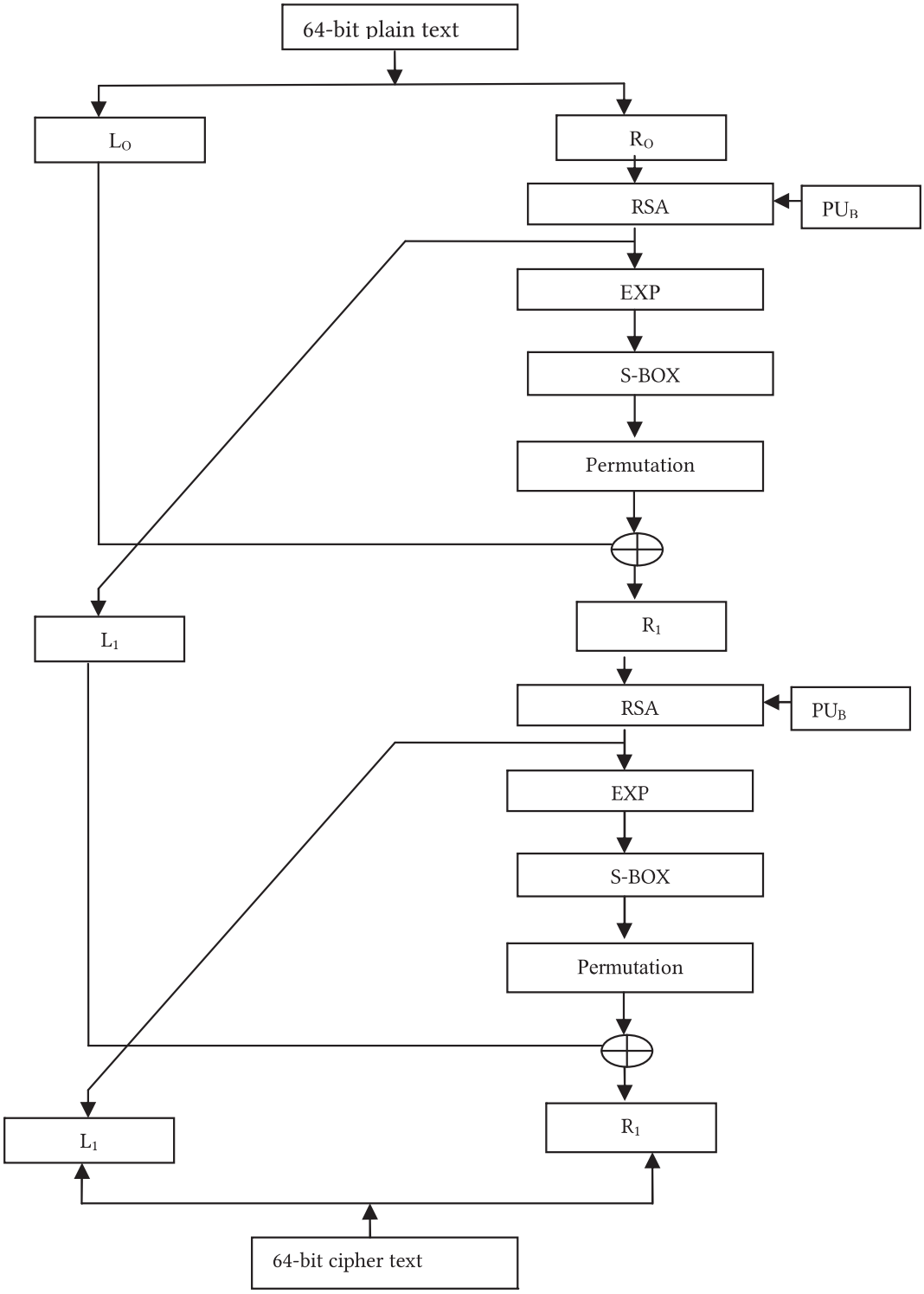

Fig. 2. Encryption using DES asymmetric-key algorithm, Mohit et al. (Biswas and Mohit, 2016).

the emergence of cloud computing increasingly number of data in this day and age is being shifted to the servers in order to manage large system management costs and for easy access. However, it comes with its own disadvantages of editing of text by intruders also known as data Redaction. Therefore, researchers worked upon redactable signature schemes and hence extended it to three authenticated data reduction scheme. These schemes are more efficacious and secure, nonetheless; still face some challenges which makes it unstable.

2.2. Advanced key management schemes

On one side the algorithm complexities are getting increased, however; most of the time, the strength of an algorithm majorly depends on key sizes and key management schemes; this section describes the various advanced key management schemes for providing better authentication and data integrity.

Babamir and Davahli (2016) extended the block cipher with variable-length key selected randomly. The keys generation is in

a randomized fashion and the key size increases dynamically; hence, hard to recover the plain text without the knowledge of the key. The proposed algorithm is discussed with the following mathematical relations for encryption (Babamir and Davahli, 2016):

$$MS_{j+1} = CT_j - r_{j+1}/K_{j+1} \quad (4)$$

$$CT_j = MS_{j+1}/K_{j+1} \quad (5)$$

$$R_{j+1} = CT_j \% \; MS_{j+1} \quad (6)$$

$$CT_{j+1} = MS_{j+1/2} || \; R_{j+1} \quad (7)$$

For decryptions the mentioned equations are as follows:

$$CT_{j+1} = MS_{j+1} * Kj_{+1} + R_{j+1} \quad (8)$$

$$MS_{j+1} = R_{j+1}/CT_{j+1} \quad (9)$$

where MS_{j+1}= (j + 1) the message block, CT_j = jth Cipher Text, R_{j+1} = remaining of jth cipher text block, K_{j+1}= (j + 1) th key block, r_j = initial random number.

In this method, the key size is of variable length and starts with some random bits and increased step by step. The approach is based on randomization hence after calculating the last cipher text i.e. C_{j+1}, authors generate a random value and the random place. The random values are generated to be positioned somewhere in C_{j+1} and the random place specifies where C_{j+1} random value is positioned. Hence, the procured key has: random bits + random value + random place + key [1…j + 1], [MS_{j+1}/2]. Thus, this approach is more resistant against various attacks, and hence, security increases more due to randomization which produces confusion among the encrypted text. However, increased execution time and usage of extra memory space are some of the main limitations of the approach.

Hazay et al. (2018) proposed a key generation protocol that comprises sub-protocols: first they present a fully simulated protocol for producing a distributive RSA composite with no factorization problem. Authors also implement a two-party setting (Gilboa, 1999) under this sub-protocol by adopting a novel technique of using two unique additively homomorphism encryption strategy that empowers to guarantee dynamic security easily. Secondly, they adopt the bi-Primality test for confirming the legitimacy of the produced composite and then generate the secret share keys in the form of $d \equiv 1 \bmod N \equiv 0 \bmod \varphi(N)$. Lastly, they proposed a two-party distributed decryption protocol.

Chie (2018) proposed a technique called a three-party authenticated key agreement (3PAKA) that allows a couple of registered users to create the session keys employing authentic server. The user formerly shared its secret key with the server. The author described the technique in which U wants to create a session with V and perform the following steps as shown in Fig. 3:

Step1: In this scheme, U sends the message to V and upon receiving V sends its encrypted message along with U's message to the server shows that Fig. 3a below:
Step 2: When server receives a request from V client, it uses the private key of U and V for encrypting the message and use the public keys to produce a short-time public key gx and gy and return the following encryption to the clients as shown in Fig. 3b below:
Step 3: When U receives the response from the server then decrypt the message and compute session key and (gy) x. After computing it sends the key, and the encoded message to V as shown in Fig. 3c below:
Step 4: When V receives the response from the server then decrypt the message and compute session key and (gy) x. After computing, it sends the key, and the encoded message to U as shown in Fig. 3d below:

Hence, to decode the message both use the session key and achieve the best computational speed by reducing the several rounds with limited resources and enhance the security proofs. However, sending encrypted messages to the server increases complexity and cost. Furthermore, if the third-party is not loyal then it may jeopardize the security.

Thangarasu and Selvakumar (2018) proposed an enhanced encryption technique over sensor-cloud architecture for securing the session keys between hosts while utilizing a reliable service. To enhance the validation of sensor nodes in the network modified Elliptical Curve Cryptography (ECC) algorithm and to remove the complexity related to the finding of invaders in the network theory of the Abelian group is used by this technique.

Chen and Qi (2018) proposed an advanced biometric-based mutual authentication technique with the key agreement. To use other public-key cryptography, this technique uses the Elliptical Curve Cryptography with a small key size. The scheme is based on the certainty that every key for a particular session is enclosed within two haphazard integers that vary every time. Regardless of whether an opponent obtains the private key of the server, to infer past keys for that session, they are required to extricate the associating two haphazard integers by solving the elliptic curve discrete logarithm (ECDLP) problem which seems to be impossible. To proof the authentication, Burrows-Abadi-Needham (BAN) logic has been used. However, the proposed technique is secure and efficient, but may not accessible by the multi-server environment.

Barbulescu and Duquesne (2017) works with attacks against the pairings and proposes a new key size. In this paper, they estimate the complexity of the Special extended Tower Number Field Sieve (SexTNFS) algorithm. For this author works the Number Field Sieve (NFS) variant and explains the NFS with the help of Fig. 4 below where α_m and α_n are roots of m and n in the field number and where O_m and O_n are the ring integers of the same fields. Then m & n are two polynomials such that m, $n \in Z_i[y]$, having a common factor ϕ modulo S, where S = N for a factor and $S = p^r$ for discrete logarithms.

From this they find the complexity of the classical variant of NFS:

$$LS\,[64]1 + o\,(1)\; where\; S = N \quad (10)$$

$$LS[c] = exp\left((c/9)^{1/3}(log\; S)^{1/3}(log\; log\; S)^{2/3}\right) \quad (11)$$

By using these complexities they generate new pairing parameters which are 255-bit security levels. Finally, to ensure the bit security level they work with the various curves like Barreto-Naehrig (BN), BLS12, and KSS16. The authors also evaluated the optimal ate pairing complexity for each and every proposed curves to assure the 128 bits of security. Hence, concluded, that BLS12 is a more systematic option.

Katz and Vaikuntanathan (2013) introduced a system for building password-based protocols that empower customers to reboot the frail shared key into a cryptographic key and authenticated key exchange protocols that enable parties to share a secret key safely over the uncertain network. This novel system is processed where clients concurrently send messages to each other. To make a protected protocol for key exchange, the protocol applies a hash function and secure encryption scheme (Gen, Enc, Dec) as shown in Fig. 5 below.

In the aforementioned Fig. 5, pwd represents the shared password, U and W are the clients; key1 and key2 are hash keys. In the above scenario, U selects a random hash key key1 and generates S1 and CT1 and sends it to W. Similarly, W produces S2 and

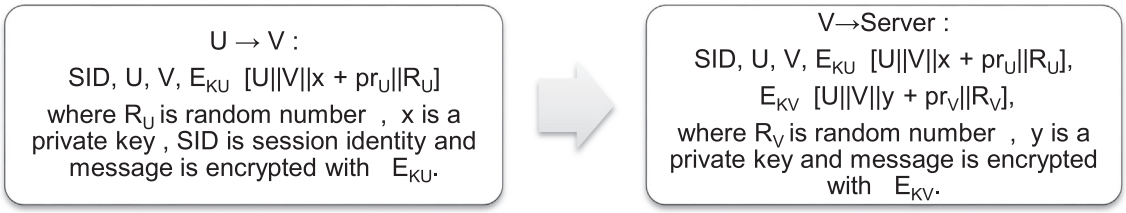

Fig. 3a. Client send encrypted message to Server.

Fig. 3b. Server returns Encrypted Message to Clients.

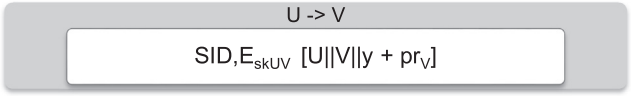

Fig. 3c. Send Key and message to Client V.

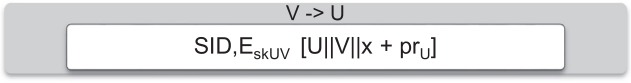

Fig. 3d. Send Key and message to Client U.

CT2 and sends it to U. Upon receiving, U checks the validity of S2 and CT2. If invalid, U simply rejects; otherwise, compute L2 and SKU. However, this scheme builds a secure protocol for key exchange but the system depends upon non-interactive zero-knowledge (NIZK) proof which is computationally inefficient.

2.3. Tradeoff of recent algorithms

The standards such as RSA and AES are being used in several applications, although, the recent advancements in computing facilities make these algorithms vulnerable to various attacks. The researchers are working to mitigate the new types of attacks and finding the best possible ways to counter-attack them to provide a complete security framework for futuristic communications. In this paper, we have discussed some important new generation security algorithms and their improvements; besides, this section gives a glimpse of the most important algorithms discussed in previous sections along with the attacks they can able to mitigate. The limitations and vulnerabilities are also mentioned in Table 2.

2.4. Quantum cryptography

Quantum is a new technology, which is generating an abundance of opportunities to develop an entirely a new generation of cyber security algorithms. A normal quantum computer will be 10,000 times faster than classical computers, hence, the researchers are working in-depth to bring out the best possibilities of smart, intelligent and quantum safe cyber security algorithms

This section discusses the Quantum based cryptography method and schemes, in this quantum era and the pertaining advantages.

2.4.1. Quantum key distribution

Shen et al. (2018) enlighten the biggest endanger which Quantum cryptography brings to the security of existing cyberspace. Classical cryptosystems work with a secret key; if the key is fragile, then the entire framework will be disintegrated. Exploiting Quantum Mechanical properties (Gisin et al., 2002) perform cryptographic tasks. Chen (2015) worked on Quantum, which can be

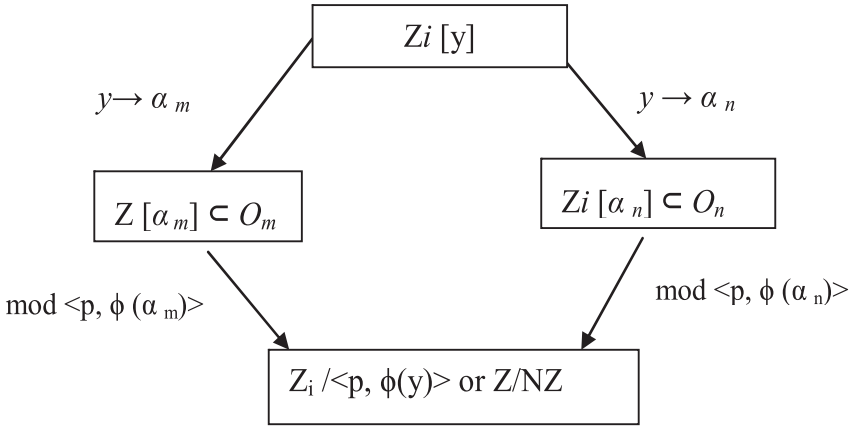

Fig. 4. Number Field Sieve Variant, extended from Barbulescu and Duquesne (2017).

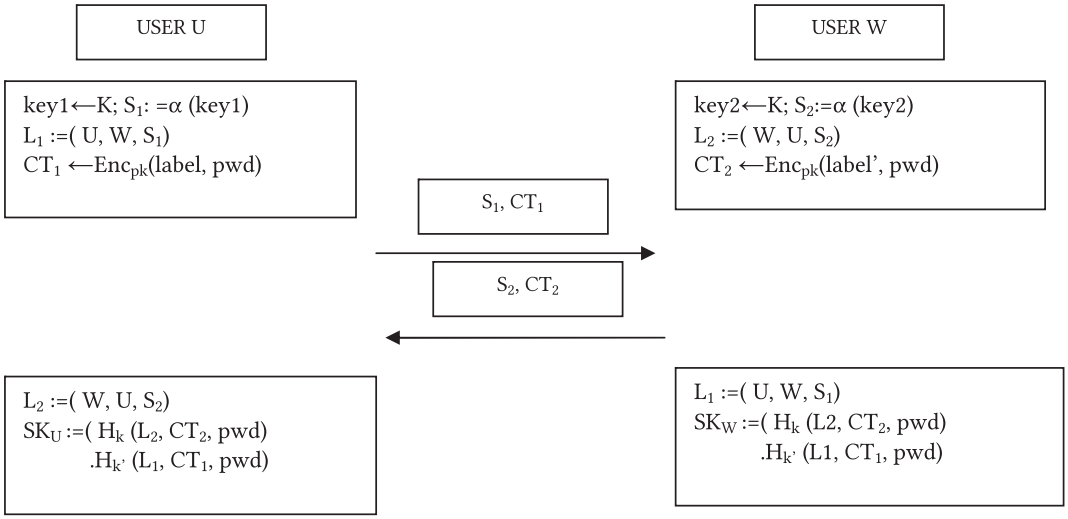

Fig. 5. Key exchange protocol.

used in sharing secret messages, computing securely, and secures communication among two parties. According to the author, quantum cryptography utilizes quantum physics to make the communication secure over the network between the users. To defeat this; a new key distribution technique based on quantum physics is introduced called quantum key exchange-clients can do key sharing along with preventing an illegitimate user from procuring the key.

Brassard and Bennett (2014) describe the Public Key Distribution (PKD) that uses a quantum channel that is not only utilized for sending messages, yet is legally used to transmit arbitrary bits between two clients who share no secret data initially. If the transmission has not been aggravated, they consent to utilize these shared secret bits in the notable route as a one-time pad (Chen, 2015) to disguise the importance of consequent significant correspondences, or for other cryptographic applications requiring shared secret random data else they dispose of it.

Quantum Key Distribution (QKD), instead of relying on the concepts of mathematics, is based upon the laws of quantum physics to create the symmetric key (Ardehali et al., 2005). The first practical QKD protocol (Brassard and Bennett, 2014), wherein two parties communicate by the usage of both classical and quantum communication channels as delineated in Fig. 6. Classical channel (Chen et al., 2018) allows individual bits of information back and forth to pass through the channel just as same as they use the internet and this channel uses classical bits which can be either 0 or 1. Hence, no privacy holds here and the eavesdropper easily get the bits and send the false data to a receiver. On the other hand, the quantum channel acts differently. Instead of transforming bits, it transforms QUBITS (Quantum bits) (Nitaj, 2012; Moizuddin et al., 2017). Qubits can be 0 or 1 at the same time. In physics, the number of physical objects that can be used as Qubits: a single photon or electron.

Qubits represent bits and incorporate some special properties:

- Qubits cannot be copied.
- It is impossible to determine whether a qubit can be processed through which filter.

BB84 uses a photon having a property spin which can be changed when passes through any of the Rectilinear or diagonal filter as shown in Table 3 below:

In the first stage, Ellie starts sending the photons over a quantum channel while switching between the filters at random to communicate with Clark. Although, Clark doesn't know which filter to use and he also uses random filters to compute the photon's polarization.

In the second phase, Clark apprise Ellie over the classical channel neither the spin nor (0 or 1) just the filter he used. Ellie will reply and keep the digits if both use the same filter else discard the digits. Clark and Ellie should now both have similar bits which are called a shift key as shown in Fig. 7. Since, Clark chooses the correct filter half the time on average 50% of the measures will be correct. However, the remaining Qubits for which Clark use the wrong filter accidentally end up with the correct bit half the time just by chance. This means 75% of Clark's measurement will be correct.

Without any computation fault, if any of the comparable bits would be rejected, indicates the appearance of malicious intender on the secured-quantum channel (Elliott, 2004). This is on account of the malicious intender, Eve, endeavoring to acquire the key. Apart from measuring the photon spin by passing them through filters, she would have no other option. This is because of the quantum no-cloning theorem (Wootters and Zurek, 1982). Now, suppose Ellie pass the photon from rectilinear filter show guess correctly that it has vertical spin and note down 0, but if eve uses the diagonal filter the photon spin will be altered as passes through and incorrectly raises 0 and vice versa as shown in Fig. 8a and Fig. 8bs. Given that (Polak and Rieffel, 2000), as switching between the filters at random, Eve will select the basis falsely about half of the time. On the off chance that Eve has listened in on every one of the bits then after n bit correlations by Ellie and Clark, they will decrease the likelihood that Eve will go unseen to ¾n (Lomonaco, 1999). That's how quantum physics protects from her knowing the key.

In 1991, Ekert proposed the protocol (Ekert, 1991) that is based on Bell's theorem. Note that (Ekert, 1991) employs a pair of quantum bits (i.e., an EPR pair), which is essentially the same as (Brassard and Bennett, 2014). Subsequently, in 1992, the improvement (Bennett, 1992) of the scheme (Brassard and Bennett, 2014) was put forward by Bennett. Instead of using two orthogonal states, they go for single non-orthogonal states. Subsequently, many QKD protocols, (Gisin et al., 1995; Bruß, 1998; Christensen, 2004; Inoue et al., 2002; Brunner et al., 2005; Liu et al., 2013) have been proposed with the same basic principles of quantum mechanics.

3. Security threats and challenges

This section discusses the various threats and challenges faced by most of the researchers. Jelezko et al. (2010) on one hand

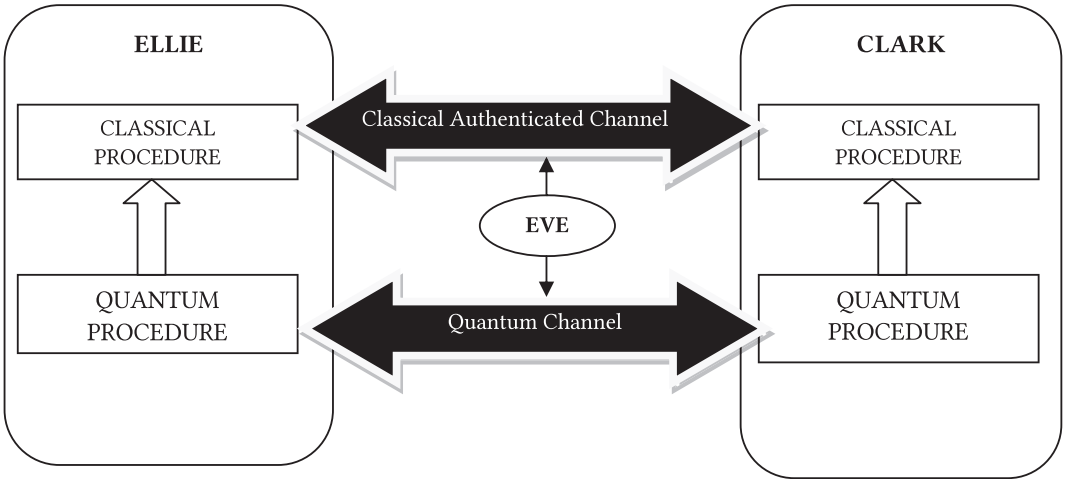

Fig. 6. Quantum Communication Model.

Table 3
BB84 encoding.

BASICS	0	1
+ (Rectilinear Basics)	↑	→
X (Diagonal Basics)	↖	↗

describes a fact that quantum computing is a novel kind of figuring machine which permits calculations represented by quantum–mechanical procedures to permit "enormous parallelism at the physical level". They have given the superposition rule of quantum states which would accelerate the classical algorithms. Despite its infancy, Shen et al. (2018) apprise the challenges that Quantum computers bring to the classical cryptography algorithms, for instance: RSA with key length 2048-bits (Rivest, 1978; Chen et al., 2018), ElGamal (1985), ECC (Tseng, 2007), and many more that can easily be broken. Classical algorithms facing the two main problems effectively known as the: factorization problem (Integer factorization, 2018), elliptic-curve discrete logarithm problem (Elliptic-curve cryptography, 2018). Many researchers (Gilboa, 1999; William and Woodward, 2017; Chen et al., 2016) in their paper unfolds the truth and describes the algorithm proposed by Shor (1994), Lov and Grover (1996) which in polynomial time solves these problems efficiently. However, in many surveys (Brandl et al., 2016; Sullivan and Forget, 2018; IBM, 2018; EPSRC, 2018) it has been revealed that till now quantum computers do not exist but they will come into reality by 2025.

Another biggest threat to cybersecurity is the WannaCry ransomware attack. Mustaca (Mustaca, 2014) and Brewer (2016) describe the ransomware attack, which was initially happened in

Ellie's bits	1	0	0	1	1	0	0	0	1
Ellie's basis	+	X	+	+	X	X	X	+	+
Ellie's Polarization	→	↖	↑	→	↗	↖	↖	↑	→
Clark's Basis	+	X	X	+	+	X	+	+	X
Clark's measurement	→	↖	↗	→	→	↖	↑	↑	↖
Clark's bits	1	0	1	1	1	0	0	0	0
Comparison of Basis	=	=	≠	=	≠	=	≠	=	≠
Shared secret bits	1	0		1		0		0	

Fig. 7. BB84 simulation.

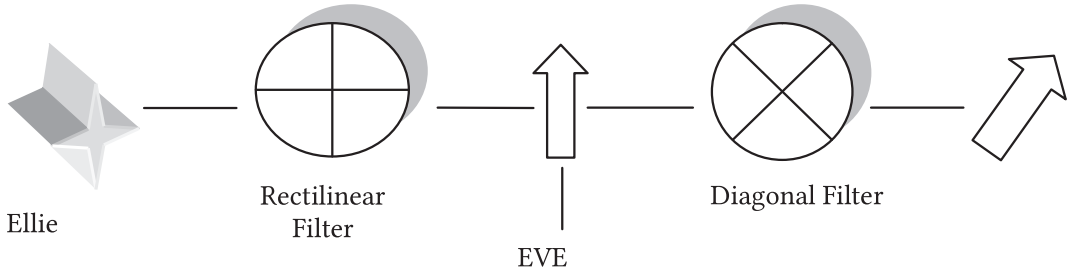

Fig. 8a. Eve Intercepts and random guess for qubits.

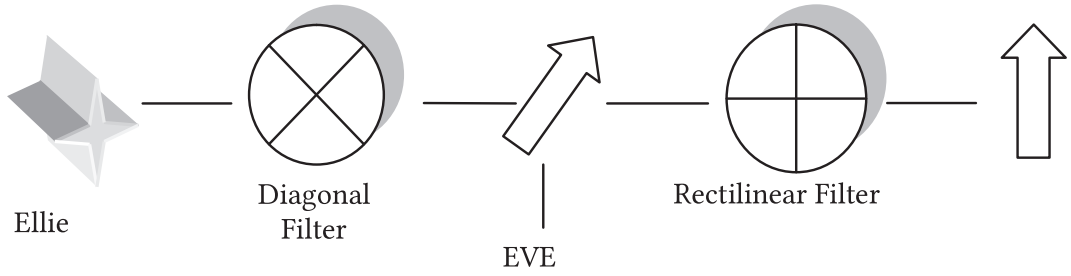

Fig. 8b. Eve intercepts and random Guess for Qubits.

2013. They presented a new variant of ransomware that encrypts the files on the client's system and then demands a ransom to decrypt the files. Nanded and Pathak (2016) describe different types of ransomware attacks and their functions. WannaCry is also one of the forms of ransomware worm, and a recent security alert occurred in May 2017. Many authors examined the concepts, characteristics, exponential growth of WannaCry, and different measurements to resolve this attack (Hsiao and Kao, 2018; Mohurle and Patil, 2017; Tabone, 1988; Sabharwal, 2020).

Wang et al. (2018) introduced a novel quantum algorithm that breaks the RSA cryptosystem within the polynomial-time using quantum inverse Fourier transform and phase estimation by computing the order g of M of the RSA public-key (x, s = pq) ∈ Mxg≡ M (mod s). Since, when g is found, the plaintext P of RSA can easily be procured by computing P ≡ Mxg-1 (mod s). Hence, a cipher text-only attack is proposed to attack RSA whereas Ariffin et al. (2014) proposed an attack on RSA, in which decryption exponents p1 and p2 share their most significant bits in relation with prime numbers x and y, which share their information of the least significant bits. The scheme performs in a way that makes by improving the bounds of previous attacks and make RSA insecure.

Bar-On et al. (2018) presented efficient slide attacks. Due to slid pairs, these slide attacks perform better than the standard slide attacks and complexity is not more than 2n. These attacks decrease the time complexity from 291 to 240 on the same 128-bit variant of the GOST block cipher.

Rather than focusing on mathematical properties of the cryptographic system i.e., mapping amongst a plaintext and ciphertext, some algorithms focus on implementation in hardware on physical devices that communicate with each other. These physical communications can be actuated and checked by attackers and may bring about data valuable in the cryptanalysis.

Attacking a Physical channel is very dangerous; they need to be analyzed in detail. This kind of data is called side-channel data, and the attacks abusing side-channel data are called side-channel attacks (SCA) (Badrignans et al., 2011). By exploiting various techniques and analyzing non-functional behaviors, these attacks extricate the key and confidential data from the devices such as Time details, consumption of the power, and getting clues from the leakages of electromagnetic or even sound (Standaert, 2010). In this, the cryptographic algorithm is modeled as a grey box i.e., the attacker gains or leaks the intermediate information as shown in Fig. 9. Side channels are described to be the unplanned result of the system.

Hall et al. (2000) and Kocher (1996) presented the leakage of abstract information about the key. However, it ought to be stressed that a specific side-channel attack may not be a practical risk in a few situations.

According to the observation, Standaert (2010) categorized these attacks between two orthogonal axes: Active vs. Passive attacks and Invasive vs. Non-Invasive attacks. An invasive attack may abstain from aggravating the device's behavior, whereas a passive attack may require a fundamental indispensable data to be perceptible. There are different important methods and techniques applied in SCA attacks as shown in Table 4:

Bernstein (2005), Keller et al. (2007), Cock et al. (2018) described cache timing attacks as the attacks in which the attacker measures the execution time it takes to execute cryptographic operations for extracting the sensitive data. The reason behind the attack is that the execution time differs from the input. Consequently, the attacker extricates keys by measuring the time taken to run each operation. Whereas, in Cache-Access Based Attacks, an attacker monitors the security operations which includes data cache such as AES lookup table entries or AES T-table entry (Osvik et al., 2010; Bangerter et al., 2011; Percival, 2005; Luo et al., 2018), instruction cache (Aciiçmez, 2007), etc. Whenever access is made by the user from the memory, the attacker monitors the time it takes and; hence, extracts the encryption key. It has effectively broken AES, DES, Camellia (Tsunoo, 2002), and many cryptographic algorithms successfully. To implement cache side-channel attacks there are many methods which include Evict + Time (Osvik et al., 2006), Prime + Probe (Percival, 2005), Flush + Reload (Bangerter et al., 2011). Osvik et al. (2006) introduce Evict + Time and Prime + Probe methods in which intruders overflow the cache with his/her information called as Eviction and Prime step. In the former method, when the process was implemented by the victim, the attacker learned the data from its execution time. Another yet important method to implement cache

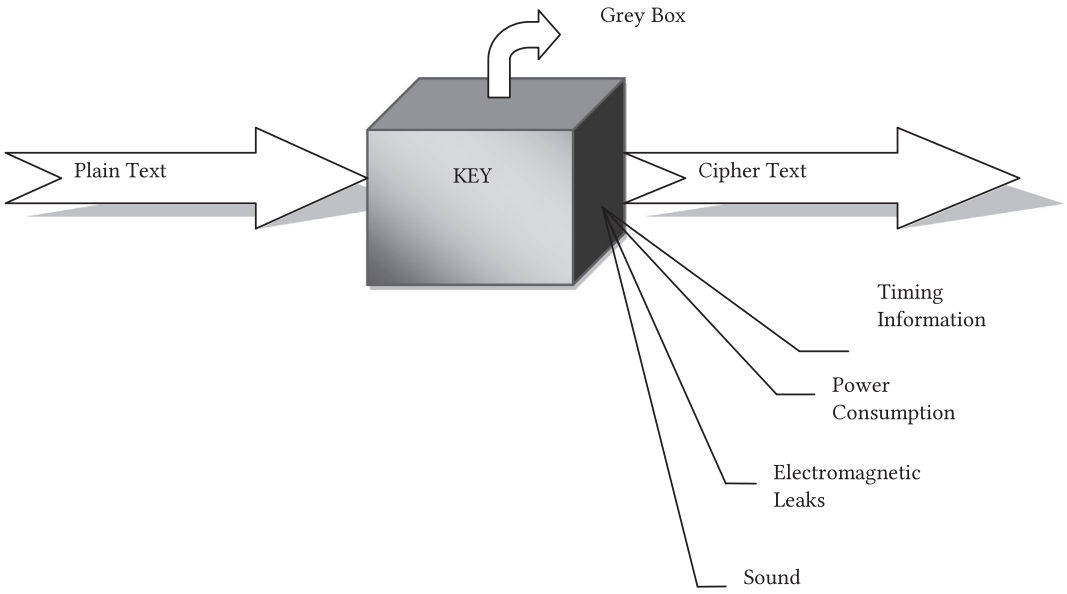

Fig. 9. Side channel attacks.

based attack is Flush + Reload which was initially proposed by Bangerter et al. (2011) and they attacked AES L1- cache which was further extended L3-cache by Falkner and Yarom (2014) for cross-core attacks. Eisenbarth et al. (2015) initially presented the idea of mounting a cross-VM AES key recovery attack and increased the performance by flushing the memory lines between the rounds.

A scan-based side-channel attack is yet another tough test technique as well as the tool to fetch the key in the cryptosystem by examines the scanned data. To retrieve the keys of DES, Karri et al. (2004) in 2004 came up with the idea to utilize scan chains and implement it on hardware. While performing the hardware implementations of NTRUEncrypt for retrieving the key, Kamal and Youssef (2012) utilizes Design-For –Test (DFT) technique in which the cryptanalyst recovers the keys using polynomial based multipliers of scan chain used in the decryption algorithm wherein 2013 Flottes (2013) presented a new novel technique targeted against DFT structure using scan chains. This novel attack is adopted by all the cryptographic algorithms including AES, DES, RSA, ElGamal, and ECC. Scan-based attacks can also be implemented using scan signatures, these are used to retrieve data from the entire stream as well as block ciphers (Fujishiro et al., 2014a, 2014b, 2015). This technique is also useful in retrieving data from many cryptosystems including RSA, HMAC-SHA-256 (Nara et al., 2010; Oku et al., 2018).

A fault attack is a deliberate manipulating of the integrated circuit or an electronic device (e.g., smartcard, HSM) with the intent to incite or induce errors by putting the device in abnormal conditions such as light, high and low voltage, temperature, clock, etc. the end goal to induce errors in such a way that it leads to the ingress of indispensable data such as PIN code recovery, accepting false signatures, key recover.). To carry out a fault attack on integrated circuits successfully, Fault Injection, and Fault Exploitation are required (Benot, 2011). Kim et al. (2012) developed new attacks that deal with all directions on Differential fault analysis (DFA) by finding the key based on differential knowledge between precise and erroneous cipher text achieved by urging the faults. The author works with random byte fault of the 1-byte model by reducing the pair of precise and wrong cipher text whereas Fan et al. (2017) proposed DFA on LBlock and impart that to retrieve all information of key, least 13.3 faults are needed.

4. Conclusions

Cybersecurity pertains to the practices that prevent cyber attacks, data breaches, and security threats. In general, the term cybersecurity is left with many questions such as what types of challenged and threats faced by organizations? How to mitigate those attacks? Who is at the highest risk? What steps need to be taken to reduce the cyber-attacks and risks? Still, many more questions are unanswered. This article describes the taxonomy of various existing standards for encryption and decryption of data with the recent emerging trends and the challenges faced by these standards in cybersecurity.

The commonly used security standards have been discussed with their strengths and weaknesses. In recent times, cybersecurity reached a new level, being transformed into a pre-eminence for digital business. However, some new approaches and methods are getting introduced based on the digital growth rate and on the other side, the hackers try new tools and technologies to challenge the security frameworks. Thenceforward, numerous other endeavors emanate. This paper provided a detailed review of the new advancements of the security standards of symmetric and asymmetric algorithms developed by various researchers over the period of time with the help of new algorithms, procedures, and frameworks. The RSA started with a one-way function along with a factoring problem. Adversely, instead of using a one-way function to secure the data, researchers instead of employing prime numbers develop an improved RSA algorithm with the help of ring integers to solve the factoring problems. The authors also proposed the technique of merging DES and RSA to achieve good confidentiality along with minimal overhead. Likewise, all the other recent advancements of the RSA algorithm are well documented in this paper, the various key management schemes with their pros & cons are also discussed well. Further, the symmetric encryption standards use XOR as their main function for transferring the bits on to the classical and perilous channel, but in recent days, another interesting cryptography is prominently getting developed called quantum cryptography based on the law of physics. This technology uses Qubits to provide more security with the new set of algorithms, where cryptanalysis is not an easy task with respect to Qubits. The quantum computers bring challenges and have a destructive result on classical asymmetric cryptography

Table 4
Summary of side channel attacks.

Type of Attacks	Paper	Experiment System	Target	Algorithm/Method	Knowledge extracted	Performance
Cache-Timing Attack	(Adve et al., 2013)	Intel i7-870	Address space layout randomization (ASLR)	Cache Probing	Extract the Physical address of system call Handler	Probing attack 180 times
	(Jia and Xie, 2016)	high-precision oscilloscope, smartcard reader, fi1lter devices	RSA-SPA	L2R AND R2L using Montgomery's algorithm modular multiplier	Extracted 1024 bits key	1536 modular multiplications
	(Genkin et al., 2017)	Intel Xeon E5-2430	RSA (OpenSSL 1.0.2f)	Cache-Bank Conflicts- Variant of Cache Bleed	Extracted 4096 bits key	16,000 decryptions
	(Heinz et al., 2012)	Cortex-A8	AES	Barreto's implementation (T-Tables implementation)	Per key byte it bound to 4 choices	1,600,000 samples
	(Aldaya et al., 2018)	Sandy Bridge 3.10 GHz, Intel Core i5-2400	RSA (OpenSSL)	Non constant-time binary GCD algorithm	Key recovered 28%	10 K trials
Cache-Access Based Attacks	(Osvik et al., 2010)	Athlon 64	AES (OpenSS, Linux 2.6.11 dm-crypt)	Prime + Probe with relevant information about lookup tables of Physical and Virtual addresses	Full 128-bit AES	300 Encryptions
	(Bangerter et al., 2011)	Pentium M, Linux 2.6.33.4	AES (OpenSSL 0.9.8n)	Flush + Reload with The Completely Fair Scheduler (CFS)	Full 128-bit AES secret Key.	Instruct the machine for 2 samples from 1,68,000 Encryptions, to recover the key it need 100 encryptions
	(Eisenbarth et al., 2015)	Pentium 4E	AES (OpenSSL 1.0.1f)	Prime + Probe technique with L1 cache	Full 128-bit AES secret Key.	16.000 encryptions.
	(Adve et al., 2015)	Xen 4.4 (Intel Xeon E5 2690), VMware ESXi 5.1	ElGamal	Prime + Probe technique	Full breakage of key between 12 and 27 min	79,900 experimentalexponentiations
	(Genkin et al., 2018)	Chrome OS 58.0.3029.112, HP Elite Book 8760w laptop	ElGamal and ECDH	Portable Native Client (PNaCl) or WebAssembly with the variant Prime + Probe	Full extraction of RSA and ElGamal keys	8192 eviction sets with 22 ms with sample time 3 min.
Scan-Based Attacks	(Nara et al., 2010)	Window XP SP3, Intel Atom 1.2 GHz	RSA LSI	Scan Signature	RSA 1024-Bit secret key extracted	Minimum 29 messages required.
	(Fujishiro et al., 2014)	Intel(R) Core(TM) i7-2620 M 2.70GHZ X4	Trivium Stream Cipher	Scan Chains- a Design-for-test technique.	512-bit plain text from cipher text generated by Trivium	Required 30 cycles for maximum 4096 scan chain length.
	(Fujishiro et al., 2014)	Intel(R) Core(TM) i7-2620 M 2.70GHZ X4	LED Block Cipher	Scan Chains- a Design-for-test technique.	Retrieved 64-Bit key	100 trials with 79 plain Texts.

algorithms includes RSA, ECC, ElGamal, and symmetric cryptography algorithms such as DES, AES, RC5, and Blowfish. Over the years, immense research is going on quantum computing, the quantum computers can break the existing standards completely when they come into real time implementations. Furthermore, the hardware implementations of security algorithms are being developed by various researchers along with the software implementations to achieve the goal of speed, complexity, and correctness, but researchers need to be cautious to avoid side-channel attacks that incorporate timing attack, cache attack, scan-based attack, fault and differential based attacks. There are many practical trials to break the AES and RSA by timing attacks and symmetric ciphers such as a stream, block, or Trivium ciphers are prone to scan-based attacks.

Our main aim is to provide an aspect of interesting advancements and challenges that cybersecurity brings to researchers. The prominent methods and algorithms that are available to solve all security-related problems, their challenges, and new technologies such as Quantum computing and Quantum mechanics all are discussed in detail. This paper is a complete survey that covers all aspects of cybersecurity and will create an avenue for the new researchers to carry over the further steps to enrich this domain with advanced techniques for future applications. The next generation of security algorithm could be based on polynomials, in literature, there is a limited availability of polynomial based encryption. We found it has a very good scope to include polynomials in the array of security algorithms.

References

Abdallah, A.E., Mahbub, K., Palomar, E., Wagner, T.D., 2018. A novel trust taxonomy for shared cyber threat intelligence. Sec. Commun. Netw. https://doi.org/10.1155/2018/9634507. Article 9634507.

Aciiçmez, O., Yet another Microarchitectural Attack: Exploiting I-Cache. In Proceedings of the 2007 ACM workshop on Computer security architecture. ACM, Fairfax, Virginia, USA .11-18. (2007). doi: 10.1145/1314466.1314469.

Adve, V., Criswell, J., Dautenhahn, N., Practical timing side channel attacks against kernel space ASLR. In 2013 IEEE Symposium on Security and Privacy. IEEE, Berkeley, CA, USA. 191-205.(2013).DOI: http://doi.ieeecomputersociety.org/10.1109/SP.2013.23.

Adve, V., Criswell, J., Dautenhahn, N., Last-Level Cache Side-Channel Attacks are Practical. In Proceedings of 2015 IEEE Symposium on Security and Privacy.IEEE, San Jose, CA, USA . 605-622. (2015). doi: 10.1109/SP.2015.43.

Aggarwal, D., Maurer, U., 2016. Breaking RSA generically is equivalent to factoring. IEEE Trans. Inform. Theory 62 (11), 6251–6259. https://doi.org/10.1109/TIT.2016.2594197.

Albrechtsen, Eirik, 2007. Qualitative study of users' view on information security. Comput. Sec. 26 (4), 276–289. https://doi.org/10.1016/j.cose.2006.11.004.

Aldaya, A.C., Brumley, B.B., García, C.P., Tapia, L.M.A., 2018. Cache-timing attacks on RSA Key generation. IACR Cryptol. ePrint Archives 367, 4.

Apostolopoulos, T., Gritzalis, D., Mitrou, L., Pipyros, K., Thraskias, C., 2018. A new strategy for improving cyber-attacks evaluation in the context of tallinn manual. Comput. Sec. 74 (3), 371–383. https://doi.org/10.1016/j.cose.2017.04.007.

Ardehali, M., Ardehali, M., Lo, H.K., 2005. Efficient quantum key distribution scheme and a proof of its unconditional security. J. Cryptol. 18 (2), 133–165. https://doi.org/10.1007/s00145-004-0142-y.

Ariffin, M. R. K., Bahig, H. M., Nitaj, A., Nassr, D.I., New attacks on the RSA Cryptosystem. In Proceedings of the International Conference on Cryptology in Africa. Springer, Africa.178-198.(2014)DOI:https://doi.org/10.1007/978-3-319-06734-6_12.

Arora, Bhavna, 2016. Exploring and analyzing Internet crimes and their behaviours. Perspect. Sci. 8 (7), 540–542. https://doi.org/10.1016/j.pisc.2016.06.014.

Aslam N., Chowdhury C., Roy M, 2020. Security and privacy issues in wireless sensor and body area networks. Gupta B., Perez G., Agrawal D., Gupta D. (eds) Handbook of Computer Networks and Cyber Security.173-200.2020.Springer, Cham.doi: 10.1007/978-3-030-22277-2_7.

Babamir, S.M., Davahli, A., 2016. Indefinite block ciphering based on variable and great length key. Sec. Commun. Netw. 9 (18), 5533–5546. https://doi.org/10.1002/sec.1715.

Badrignans, B., Danger, J. L., Fischer, V., Gogniat, G., Torres, L. (Eds.).:Security trends for FPGAS: From secured to secure reconfigurable systems. Springer Science & Business Media.(2011).s

Bangerter, E., Gullasch, D., Krenn, S., Cache games–Bringing Access-Based Cache Attacks on AES to Practice. InProceedings of 2011 IEEE Symposium on Security and Privacy. IEEE, Berkeley, CA, USA. 490-505. (2011). doi: 10.1109/SP.2011.22.

Barbulescu, R., Duquesne, S., 2017. Updating key size estimations for pairings. J. Cryptol. 1–39. https://doi.org/10.1007/s00145-018-9280-5.

Bar-On, A., Biham, E., Dunkelman, O., Keller, N., 2018. Efficient slide attacks. J. Cryptol. 31 (3), 641–670. https://doi.org/10.1007/s00145-017-9266-8.

Bennett, C.H., 1992. Quantum cryptography using any two non-orthogonal states. Phys. Rev. Lett. 68 (21), 3121. https://doi.org/10.1103/PhysRevLett.68.3121.

Benot, O.: Fault attack. In Encyclopedia of Cryptography and Security. Springer, Boston, ssss 452-453. (2011). doi: 10.1007/978-1-4419-5906-5.

Bernstein, D. J.: Cache-timing Attacks on AES. http://cr.yp.to/papers.html#cachetiming. (2005).

Bhanot, R., Hans, R., 2015. A review and comparative analysis of various encryption algorithms. Int. J. Sec. Its Appl. 9 (4), 289–306. https://doi.org/10.14257/ijsia.2015.9.4.27.

Biham, E., 1994. New types of cryptanalytic attacks using related keys. J. Cryptols. 7 (4), 229–246. https://doi.org/10.1007/BF00203965.

Biham, E., Biryukov, A., 1997. An improvement of davies' attack on DES. J. Cryptol. 10 (3), 195–205. https://doi.org/10.1007/s001459900027.

Biham, E., Shamir, A., 2012. Differential Cryptanalysis of the Data Encryption Standard. Springer, New York.

Biswas, G. P., Mohit, P., Modification of Symmetric-Key DES into Efficient Asymmetric-Key DES using RSA. In Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies. ACM,New York, NY, USA .136. (2016). doi: 10.1145/2905055.2905352.UKI

Brandl, M.F., Martinez, E.A., Monz, T., Nigg, D., Rines, R., Schindler, P., Blatt, R., 2016. Realization of a scalable shor algorithm. Science 351 (6277), 1068–1070. https://doi.org/10.1126/science.aad9480.

Brassard, C.H.B.G., Bennett, C.H., 2014. Quantum cryptography: public key distribution and coin tossing. Theor. Comput. Sci. 560 (P1), 7–11. https://doi.org/10.1016/j.tcs.2014.05.025.

Brewer, R., 2016. Ransomware attacks: detection, prevention and cure. Netw. Sec. 2016 (9), 5–9. https://doi.org/10.1016/S1353-4858(16)30086-1.

Brunner, N., Gisin, N., Stucki, D., Scarani, V., Zbinden, H., 2005. Fastsnd simple one-way quantum key distribution. Appl. Phys. Lett. 87 (19). https://doi.org/10.1063/1.2126792.

Bruß, D., 1998. Optimal eavesdropping in quantum cryptography with six states. Phys. Rev. Lett. 81 (14), 3018–3021. https://doi.org/10.1103/PhysRevLett.81.3018.

Chen, C.Y., 2015. Quantum cryptography and its applications over the internet. IEEE Netw. 29 (5), 64–69. https://doi.org/10.1109/MNET.2015.7293307.

Chen, W., Du, W., Ma, W., Li, J., Li, N., Zhang, Y., 2018. A survey on quantum cryptography. Chin. J. Electron. 27 (2), 223–228. https://doi.org/10.1049/cje.2018.01.017.

Chen, X., Li, J., Shen, J., Susilo, W., Zhou, T., 2018. Anonymous and traceable group data sharing in cloud computing. IEEE Trans. Inform. Foren. Sec. 13 (4), 912–925. https://doi.org/10.1109/TIFS.2017.2774439.

Chen, J., Qi, M., 2018. New robust biometrics-based mutual authentication scheme with key agreement using elliptic curve cryptography. Multimedia Tools Appl. 77 (18), 23335–23351. https://doi.org/10.1007/s11042-018-5683-4.

Chie, H., 2018. Using the modified Diffie-Hellman problem to enhance client computational performance in a three-party authenticated key agreement. Arab. J. Sci. Eng. 43 (2), 637–644. https://doi.org/10.1007/s13369-017-2725-6.

Chowhan, S. S, Jaju, S. A.: A Modified RSA Algorithm to Enhance Security for Digital Signature. In Proceedings of International Conference and Workshop on Computing and Communication. IEEE, Vancouver, BC, Canada. 1-5. (2015). DOI: https://doi.org/10.1109/IEMCON.2015.7344493.

Christensen, Iversen, B. B., M., Toberer, E. S., Snyder, G. J.:Quantum Cryptography Protocols Robust Against Photon Number Splitting Attacks for Weak Laser Pulse Implementations. Phys. Rev. Lett. 92(5). (2004). doi: 10.1103/PhysRevLett.92.057901.

Cock, D., Heiser, G., Ge, Q., Yarom, Y., 2018. A survey of microarchitectural timing attacks and countermeasures on contemporary hardware. J. Cryptogr. Eng. 8 (1), 1–27. https://doi.org/10.1007/s13389-016-0141-6.

Conti, M., Dargahi, T., Dehghantanha, A., 2018. Cyber Threat Intelligence. Springer International Publishing, Switzerland. ISBN: 978-3-319-73950-2.

Dagmar, B., Gabor, E., Jorg, R., Tim, M., Tobias, R., 2007. Quantum cryptography: a survey. ACM Comput. Surv 39 (2), 6. https://doi.org/10.1145/1242471.1242474.

Dhole, A., Verma, V., 2012. Analysis of comparison between single encryption (Advance Encryption Scheme (AES)) and Multicrypt Encryption Scheme. Int. J. Sci. Res. Publ. 2 (4), 90–94.

Diehl, E., Ten Laws for Security. Springer, Cham. (2016).ISBN: 978-3-319-42641-9.

Diffie, W., Hellman, H., New directions in cryptography.IEEE Transactions on Information Theory. 22(6).644–654. (1976). doi: 10.1109/TIT.1976.1055638.

Djekic, A Scytale – Cryptography of the Ancient Sparta. Australian Science.(2013) Retrieved Jun 30, 2018 from http://www.australianscience.com.au/technology/a-scytale-cryptography-of-the-ancient-sparta/.AccessedJun 30, 2018.

Dwivedi, A., 2011. A model of key agreement protocol using polynomials over non-cummutative division semirings. J. Global Res. Comput. Sci. 2 (3).

Eisenbarth, T., Irazoqui, G., Sunar, B., A Shared Cache Attack that Works Across Cores and Defies VM Sandboxing–and its Application to AES. In Proceedings of 2015 IEEE Symposium on Security and Privacy.IEEE, San Jose, CA, USA . 591-604. (2015). doi: 10.1109/SP.2015.42.

Eisenbarth, T., Inci, M. S., Irazoqui, G., Gülmezoğlu, B., Sunar, B.: A Faster and More Realistic Flush+ Reload Attack on AES. Springer, Cham. 111-126. (2015).DOI: https://doi.org/10.1007/978-3-319-21476-4_8.

Ekert, Artur K., 1991. Quantum cryptography based on bell's theorem. Phys. Rev. Lett. 67 (6), 661. https://doi.org/10.1103/PhysRevLett.67.661.
ElGamal, T., 1985. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. Inform. Theory 31 (4), 469–472. https://doi.org/10.1109/TIT.1985.1057074.
Elliott, C., 2004. Quantum cryptography. IEEE Sec. Privacy 2 (4), 57–61. https://doi.org/10.1109/MSP.2004.54.
Elliptic-curve cryptography. https://en.wikipedia.org/wiki/Elliptic-curve_cryptography. Accessed August 25, 2018.
Emmanuel, S., Thomas, T., Vijayaraghavan, A.P., 2020. Machine learning and cybersecurity. In: Machine Learning Approaches in Cyber Security Analytics. Springer, Singapore, pp. 37–47. https://doi.org/10.1007/978-981-15-1706-8_3.
EPSRC.: Quantum Technologies. https://www.epsrc.ac.uk/research/ourportfolio/themes/quantumtech/. Accessed August 28, 2018.
Falkner, K., Yarom, Y., FLUSH+ RELOAD: A High Resolution, Low Noise, L3 Cache Side-Channel Attack. In Proceedings of the 23rd USENIX Security Symposium. USENIX, San Diego, CA, US. 22-25. (2014). ISBN:978-1-931971-15-7.
Fan, C., Rong, Y ., Wei, Y.: Differential Fault Attacks on Lightweight Cipher LBlock. FundamentaInformaticae. 157(1-2).125-139.(2018). doi: 10.3233/FI-2018-1621.
Fiedelholtz: Incident Response and Recovery. The Cyber Security Network Guide. Studies in Systems, Decision and Control, vol 274. 2021.Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-61591-8_4.
Flottes, Natale, G. D., M. L., Rolt, J. D., Rouzeyre, B.: A Novel Differential Scan Attack on Advanced DFT Structures. ACM Transactions on Design Automation of Electronic System.18 (4).58. (2013). doi: 10.1145/2505014.
Fujisaki, E., 2018. All-but-many encryption. J. Cryptol. 31 (1), 226–275. https://doi.org/10.1007/s00145-017-9256-x.
Fujisaki, E., Okamoto, T., 2013. Secure integration of asymmetric and symmetric encryption schemes. J. Cryptol. 26 (1), 80–101. https://doi.org/10.1007/s00145-011-9114-1.
Fujishiro, M., Togawa, N., Yanagisawa, M., 2014a. Scan-based attack against trivium stream cipher using scan signatures. IEICE Trans. Fundament. Electron. Commun. Comput. Sci. 97 (7), 1444–1451. https://doi.org/10.1587/transfun.E97.A.1444.
Fujishiro, M., Togawa, N., Yanagisawa, M., 2014b. Scan-based side-channel attack on the LED block cipher using scan signatures. IEICE Trans. Fundament. Electron. Commun. Comput. Sci. 97 (12), 2434–2442. https://doi.org/10.1587/transfun.E97.A.2434.
Fujishiro, M., Jiang, H., Kodera, H., Togawa, N., Yanagisawa, M.: Scan-Based Side-Channel Attack on the Camellia Block Cipher Using Scan Signatures. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences. 98(12).2547-2555.(2015).DOI:https://doi.org/10.1587/transfun.E98.A.2547.
Genkin, D., Pachmanov, L., Tromer, E., Yarom, Y., sDrive-By Key-Extraction Cache Attacks from Portable Code. In Proceedings of the International Conference on Applied Cryptography and Network Security. Springer. 83-102.(2018). doi: 10.1007/978-3-319-93387-0_5.
Genkin, D., Heninger, N., Yarom, Y., 2017. CacheBleed: a timing attack on OpenSSL constant-time RSA. J. Cryptogr. Eng. 7 (2), 99–112. https://doi.org/10.1007/s13389-017-0152-y.
Gilboa, N., Two party RSA key generation. In Proceedings of Annual International Cryptology Conference. Springer, Berlin, Heidelberg.116-129. (1999). doi: 10.1007/3-540-48405-1_8.
Gisin, N., Huttner, B., Imoto, N., Mor, T., 1995. Quantum cryptography with coherent states. Phys. Rev. A Atom. Mol. Opt. Phys. 51 (3), 1863–1869. https://doi.org/10.1103/PhysRevA.51.1863.
Gisin, N., Ribordy, G., Tittel, W., 2002. Quantum cryptography. Rev. Modern Phys. 74 (1), 145. https://doi.org/10.1103/RevModPhys.74.145.
Gómez, B., 2009. Hidden Irreducible Polynomials: A Cryptosystem Based on Multivariate Public Key Cryptography. Cryptology ePrint Archive, Report.
Hall, C., Kelsey, J., Schneier, B., Wagner, D., 2000. Side channel cryptanalysis of product ciphers. J. Comput. Sec. 8 (2–3), 141–158. https://doi.org/10.3233/JCS-2000-82-304.
Hazay, C., Mikkelsen, G.L., Rabin, T., Toft, T., Nicolosi, A.A., 2018. Efficient RSA key generation and threshold paillier in the two-party setting. J. Cryptol. 1–59. https://doi.org/10.1007/s00145-017-9275-7.
Heinz, B., Stumpf, F., Weiß, M., A cache timing attack on AES in Virtualization Environments.In Proceedings of the International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg.314-328.(2012). doi: 10.1007/978-3-642-32946-3_23.
Hsiao, S. C., Kao, D.Y., The Dynamic Analysis of WannacryRansomware. In Proceedings of the 20th International Conference on Advanced Communication Technology (ICACT) . IEEE, Chuncheon-siGangwon-do, Korea.159-166.(2018). (2018). doi: 10.23919/ICACT.2018.8323682.
Huang, X., Liu, J., Ma, J., Xiang, Y., Zhou, W., Data Authentication with Privacy Protection. In Advances in Cyber Security: Principles, Techniques, and Applications.115-142. 2019. Springer, Singapore. doi: 10.1007/978-981-13-1483-4_6.
Hwang, S.O., Le, M.H., Kim, I., 2016. Efficient certificate-based encryption schemes without pairing. Sec. Commun. Netw. 9 (18), 5376–5391. https://doi.org/10.1002/sec.1703.
IBM, Quantum Computing Primer. https://www.research.ibm.com/quantum/expertise.html. Accessed August 28, 2018.
Inoue, K., Waks, E., Yamamoto, Y., 2002. Differential phase shift quantum key distribution. Phys. Rev. Lett. 89 (3). https://doi.org/10.1103/PhysRevLett.89.037902.
Integer factorization. https://en.wikipedia.org/wiki/Integer_factorization. Accessed August 25, 2018.
International Telecommunications Union (ITU).X. 1205: Overview of Cyber Security. https://www.itu.int/rec/T-REC-X.1205-200804-I. AccessedAugust 20, 2018.
ISO. Guidelines for Cyber Security. http://www.iso27001security.com/html/27032.html. Accessed August 18, 2018.
Jasper, Scott E., 2017. US cyber threat intelligence sharing frameworks. Int. J. Intell. Count. Intell. 30 (1), 53–65. https://doi.org/10.1080/08850607.2016.1230701.
Jelezko, F., Ladd, T.D., Laflamme, R., Monroe, C., Nakamura, Y., O'Brien, J.L., 2010. Quantum computers. Nature 464 (7285), 45–53. https://doi.org/10.1038/nature08812.
Jia, J., Liu, J., Zhang, H., 2017. Cryptanalysis of schemes based on polynomial symmetrical decomposition. Chin. J. Electron. 26 (6), 1139–1146. https://doi.org/10.1049/cje.2017.05.005.
Jia, F., Xie, D., 2016. A unified method based on SPA and timing attacks on the improved RSA. China Commun. 13 (4), 89–96. https://doi.org/10.1109/CC.2016.7464126.
Kamal, A. A., Youssef, A.M., A Scan-Based Side Channel Attack on the NTRUEncrypt Cryptosystem. In Proceedings of the 2012 Seventh International Conference on Availability, Reliability and Security. IEEE, Prague, Czech Republic. 402-409. (2012). doi: 10.1109/ARES.2012.14.
Kapczynski, A., Lawnik, M., 2019. The application of modified Chebyshev polynomials in asymmetric cryptography. Comput. Sci. 20 (3). https://doi.org/10.7494/csci.2019.20.3.3307.
Karri, R., Yang, B., Wu, K., Scan based side channel attack on dedicated hardware implementations of data encryption standard. In Proceedings of the 2004 International Conference on Test. IEEE, Charlotte, NC, USA .339-344.(2004). (2004). doi: 10.1109/TEST.2004.1386969.
Katz, J., Vaikuntanathan, V., 2013. Round-optimal password-based authenticated key exchange. J. Cryptol. 26 (4), 714–743. https://doi.org/10.1007/s00145-012-9133-6.
Keller, N., Miller, S. D., Mironov, I., Venkatesan, R., Cache Based Remote Timing Attack on the AES. In Proceedings of Cryptographer's Track at the RSA Conference. Springer, Berlin, Heidelberg. 271-286. (2007). doi: 10.1007/11967668_18.
Kim, C.: Improved Differential Fault Analysis on AES Key Schedule. IEEE Transactions on Information Forensics and Security. 7(1). 41-50.(2012). doi: 10.1109/TIFS.2011.2161289.
Kocher, P. C., Timing Attacks on Implementations of Diffie- Hellman, RSA, DSS, and other Systems.InProceedings of the Annual International Cryptology Conference. Springer, Berlin, Heidelberg.104–113.(1996).DOI:https://doi.org/10.1007/3-540-68697-5_9.
Lily Chen, Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner, Daniel Smith-Tone, Report on Post-Quantum Cryptography. US Department of Commerce, National Institute of Standards and Technology. (2016). doi: 10.6028/NIST.IR.8105.
Liu, Y.T.Y., Chen, L.J., Wang, H., Liang, G.L., Shentu, J., Wang, X., 2013. Ma Experimental measurement-device-independent quantum key distribution. Phys. Rev. Lett. 111 (13), 130502. https://doi.org/10.1103/PhysRevLett.111.130502.
Lomonaco, S.J., 1999. A quick glance at quantum cryptography. Cryptologia 23 (1), 1–41. https://doi.org/10.1080/0161-119991887739.
Lov, K., Grover, L.K., A Fast Quantum Mechanical Algorithm for Database Search. In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing. ACM, Philadelphia, Pennsylvania, USA 212-219. (1996).DOI: http://dx.doi.org/10.1145/237814.237866.
Lunt, Barry M., Rowe, Dale C., Ekstrom, Joseph J., 2011. In: The Role of Cyber-Security in Information Technology Education. Information Technology Education, ACM, New York, NY, USA, pp. 113–122.
Luo, X., Qi, Y., He, J., Wang, Q., Wan, Y., 2018. Access-driven cache attack resistant and fast AES Implementation. Int. J. Embedded Syst. 10 (1), 32–40. https://doi.org/10.1504/IJES.2018.089429.
Maheswara, R., Valluri, 2012. Authentication schemes using polynomials over non-commutative rings. Int. J. Cryptogr. Inform. Sec. 2 (4), 51–57. https://doi.org/10.5121/ijcis.2012.2406.
Mitsuru Matsui, Linear Cryptanalysis Method for DES Cipher. In Proceedings of International Workshop on the Theory and Application of Cryptographic Techniques. Springer, Berlin, Heidelberg. 386-397. (1993). doi: 10.1007/3-540-48285-7_33.
Michel E. Kabay ME, Eric Salveggio, Robert Guess, Russell D. Rosco. Computer Security Handbook (6th. ed.). Wiley Online Library. (2015).ISBN: 9781118134115.
Miller, J., Parkinson, S., Ward, P., Ward, P., 2017. Cyber threats facing autonomous and connected vehicles: future challenges. IEEE Trans. Intell. Transport. Syst. 8 (11), 2898–2915. https://doi.org/10.1109/TITS.2017.2665968.
Pradosh K. Mohapatra, Public Key Cryptography. Crossroads. 7(1). 14-22.(2000). doi: 10.1145/351092.351098.
Mohurle, S., Patil, M., 2017. A Brief study of wannacry threat: ransomware attack 2017. Int. J. Adv. Res. Comput. Sci. 8 (5).
Moizuddin, M.,Qayyum, M., Winston, J.: A Comprehensive Survey: Quantum Cryptography. In Proceedings of 2nd International Conference on Anti-Cyber

Crimes. IEEE, Abha, Saudi Arabia. 98-102. (2017). DOI: https://doi.org/10.1109/Anti-Cybercrime.2017.7905271.

Mustaca, S., 2014. Are your IT professionals prepared for the challenges to come?. Comput. Fraud Sec. 2014 (3), 18–20. https://doi.org/10.1016/S1361-3723(14)70472-5.

Nanded, Y Mss, Pathak, P.B., 2016. A dangerous trend of cybercrime: ransomware growing challenge. Int. J. Adv. Res. Comput. Eng. Technol. 5 (2), 371–373.

Nara, R., Ohtsuki, T., Satoh, K., Togawa, N., Yanagisawa, M., 2010. Scan-based side-channel attack against RSA cryptosystems using scan signatures. IEICE Trans. Fundament. Electron. Commun. Comput. Sci. 93 (12), 2481–2489. https://doi.org/10.1587/transfun.E93.A.2481.

Niekerk, Johan V., Solms, Rossouw V., 2013. From information security to cyber security. Comput. Sec. 38 (7), 97–102. https://doi.org/10.1016/j.cose.2013.04.004.

NIST. Withdrawal of FIPS 46-3 FIPS 74 and FIPS 81. https://csrc.nist.gov/news/2005/withdrawal-of-fips-46-3-fips-74-and-fips-81. Accessed June 14, 2018

Abderrahmane Nitaj, Quantum and post quantum cryptography, (2012), Available at: https://pdfs.semanticscholar.org/25d9/82dfdaa93976dda7fd8dfdae8e12c7b28bb4.pdf.

Oku, D., Togawa, N.,Yanagisawa, M.: Scan-Based Side-Channel Attack against HMAC-SHA-256 Circuits Based on Isolating Bit-Transition groups using Scan Signatures. IPSJ Transactions on System LSI Design Methodology. 11.16-28. (2018). doi: 10.2197/ipsjtsldm.11.16.

Osvik, D. A., Shamir, A., Tromer, E.:Cache Attacks and Countermeasures: The Case of AES. In Proceedings of Cryptographer's Track at the RSA Conference. Springer, Berlin, Heidelberg. 1-20. (2006). doi: 10.1007/11605805_1.

Osvik, D.A., Shamir, A., Tromer, E., 2010. Efficient cache attacks on AES, and countermeasures. J. Cryptol. 23 (1), 37–71. https://doi.org/10.1007/s00145-009-9049-y.

Percival, C., Cache missing for Fun and Profit. BSDCan, Ottawa. http://www.daemonology.net/hyperthreading-considered-harmful/. (2005).

Polak, W., Rieffel, E., 2000. An introduction to quantum computing for non-physicists. ACM Comput. Surv. 32 (3), 300–335. https://doi.org/10.1145/367701.367709.

Rivest, R.L., 1978. A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM 21 (2), 120–126. https://doi.org/10.1145/359340.359342.

Ruohonen, J., 2019. An acid test for europeanization: public cyber security procurement in the European union. Eur. J. Sec. Res., 1–29 https://doi.org/10.1007/s41125-019-00053-w.

Sabharwal, S., & Sharma, S.: Ransomware Attack: India Issues Red Alert. Emerging Technology in Modelling and Graphics. Springer, Singapore. 471-484. (2020). DOI:https://doi.org/10.1007/978-981-13-7403-6_42.

Schneier, B, Description of a New Variable-Length Key, 64-bit Block Cipher (Blowfish). In Proceedings of the International Workshop on Fast Software Encryption. Springer, Berlin, Heidelberg. (1993). doi: 10.1007/3-540-58108-1_24.

Bruce Schneier. 2018. Crypto- Gram. https://www.schneier.com/crypto-gram/archives/2018/0615.html#1. AccessedAugust 18, 2018

Shen, J., Shen, J., Wang, C., Zhou, T., 2018. Quantum cryptography for the future internet and the security analysis. Sec. Commun. Netw.. https://doi.org/10.1155/2018/8214619. Article 8214619.

Shor, P. W., Algorithms for Quantum Computation: Discrete Logarithms and Factoring. In Proceedings 35th Annual Symposium on Foundations of Computer Science. IEEE, Santa Fe, NM, USA.124-134. (1994).DOI: http://dx.doi.org/10.1109/SFCS.1994.365700.

Simmons, Gustavus J., 1979. Symmetric and asymmetric encryption. ACM Comput. Surv. 11 (4), 305–330. https://doi.org/10.1145/356789.356793.

Smit, D.M., 2015. Cyber bullying in south african and american schools: a legal comparative study. S. Afr. J. Educ. 35 (2), 1076–1087. https://doi.org/10.15700/saje.v35n2a1076.

William Stallings. Cryptography and Network Security(4/E). Pearson Education, India. (2006). ISBN: 9788177587746.

Standaert, F. X. .: Secure Integrated Circuits and Systems. Springer, Boston, MA, USA. (2010).ISBN: 978-0-387-71827-9.

Federal Information Processing Standard. https://en.wikipedia.org/wiki/Federal_Information_Processing_Standard. Accessed August 25, 2018.

Sullivan, B., Forget AI, Real quantum computers By 2025 Are Truly Achievable. https://www.silicon.co.uk/e-innovation/microsoft-quantum-computers-2025-179064?inf_by=5bcd6ff1671db87b368b4de0. Accessed August 28, 2018.

Tabone, S. R., Cyber Security 51 Handy Things To Know About Cyber Attacks: From the first Cyber Attack in 1988 to the WannaCryransomware 2017 (1st. ed.).ACM, USA .(2017).ISBN:1546841164 9781546841166.

Thangarasu, N., Selvakumar, A.A.L., 2018. Improved elliptical curve cryptography and abelian group theory to resolve linear system problem in sensor-cloud cluster computing. Cluster Comput. 1. https://doi.org/10.1007/s10586-017-1573-1.

Tseng, Yuh-Min, 2007. An efficient two-party identity-based key exchange protocol. Informatica 18 (1), 125–136.

Tsunoo, Y.S. Crypt-Analysis of Block Ciphers Implemented on Computers with Cache. In preproceedings of ISITA. Article10026863967. (2002), [online] Available: https://ci.nii.ac.jp/naid/10026863967/.

UKCyber Security Strategy. National Cyber Security Strategy 2016 to 2021. https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021. Accessed July 10, 2018

Vaudenay, S.A., Classical introduction to cryptography: applications for communications security. Springer, US. (2006).ISBN: 978-0-387-25464-7.

Wang, Y., Wang, H., Zhang, H., 2018. Quantum sfor RSA. China Commun. 15 (2), 25–32. https://doi.org/10.1109/CC.2018.8300269.

William, B., Woodward, A., 2017. Will quantum computers be the end of public key encryption. J. Cyber Sec. Technol. 1 (1), 1–22. https://doi.org/10.1080/23742917.2016.1226650.

Wootters, William K., Zurek, Wojciech H., 1982. A single quantum cannot be cloned. Nature 299 (5886), 802–803. https://doi.org/10.1234/12345678.