I.J. Mathematical Sciences and Computing, **2018, 2, 12-21**
Published Online April 2018 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijmsc.2018.02.02

***Available online at** http://www.mecs-press.net/ijmsc*

A Systematic Expository Review of Schmidt-Samoa Cryptosystem

Qasem Abu Al-Haija [a*], Mohamad M.Asad [b], Ibrahim Marouf [a,b,]

[a,b c] *Department of Electrical Engineering, King Faisal University, Hufof 31982, Saudi Arabia*

Received: 21 November 2017; Accepted: 13 February 2018; Published: 08 April 2018

Abstract

Public key cryptographic schemes are vastly used to ensure confidentiality, integrity, authentication and non-repudiation. Schmidt-Samoa cryptosystem (SSC) is a public key cryptosystem, which depends on the difficulty of large integer factorization problem. The implementation of SSC to secure different recent communication technologies such as cloud and fog computing is on demand due to the assorted security services offered by SSC such as data encryption/decryption, digital signature and data integrity. In this paper, we provide a systematic review of SSC public key cryptosystem to help crypto-designers to implement SSC efficiently and adopt it in hardware or software-based applications. According to the literature, the effective utilization and design SSC can place it as a viable alternative of RSA cryptosystems and many others.

Index Terms: Information Security, Public Key Cryptography, Schmidt-Samoa Cryptosystem, Integer Factorization.

© 2018 Published by MECS Publisher. Selection and/or peer review under responsibility of the Research Association of Modern Education and Computer Science

1. Introduction

In the last decades, the communication system over the world has been extremely enlarged where millions of computers were connected to networks and internet to exchange a huge amount of information. This information is vulnerable to interrupt, change, or even seen by unwanted people (i.e. unauthorized). Because of that, secure communication channels were introduced to prevent any third party from reading or changing information. Such prevention is accomplished by setting rules for accessing the confidential data known collectively as Cryptography. Cryptography is the science that concern with encrypting and decrypting data to provide secure transactions between communication parties. Cryptography provides the secure communication networks by a means of cryptographic primitives [1] (listed in table 1) which contributed along with the crypto-

* Corresponding author. Tel.: +966-13-589-5400; fax: +966-13-581-7068
E-mail address: Qalhaija@kfu.edu.sa

algorithms to provide many services such as: confidentiality: To help protect a user's identity or data from being read, data integrity: To help protect data from being changed, authentication: To ensure that data is originated from a certain user, and non-repudiation: To prevent a certain party from being denied of sending messages [1].

Table 1. Cryptographic Primitive and Their Use

Cryptographic primitive	Use
Secret-key encryption (symmetric cryptography)	Performs a transformation on data to keep it from being read by third parties. This type of encryption uses a single shared, secret key to encrypt and decrypt data.
Public-key encryption (asymmetric cryptography)	Performs a transformation on data to keep it from being read by third parties. This type of encryption uses a public/private key pair to encrypt and decrypt data.
Cryptographic signing (Digital Signatures)	Helps verify that data originates from a specific party by creating a digital signature that is unique to that party. This process also uses hash functions.
Cryptographic hashes (Fixed Size Digesting)	Maps data from any length to a fixed-length byte sequence. Hashes are statistically unique; a different two-byte sequence will not hash to the same value.

Based on encryption/decryption process, cryptographic algorithms are categorized as Symmetric key algorithms and Public key algorithms (Asymmetric key). Symmetric Key Cryptography (SKC) is a field of cryptography where the same key is shared between both sender and receiver to be used for encryption and decryption processes. SKC ciphers can either be stream cipher which encrypt and decrypts data as bit-by-bit process using bit operations (such as XOR) or block cipher which deals with blocks of fixed length of bits encrypted/decrypted with a key. An examples of stream cipher is LFSR encryption [2] and examples of block cipher are DES, 3DES, Blowfish, and AES. Modern symmetric algorithms such as AES or 3DES are very secure. However, there are several drawbacks associated with symmetric-key scheme like key distribution problem, number of keys or the lack of protection against cheating [3]. In symmetric key algorithms, the key must be established in a secure channel which does not exist in communication channels. Even if this problem solved, substantial number of keys will be needed when each pair needs a separate key in a network. Moreover, any party can cheat and accuse the other party. Hence, asymmetric key algorithms are needed to solve these problems.

Public Key Cryptography (PKC) where the two parties (sender and receiver) have two different keys; one public shared key for encryption and one private key for decryption. Public-key algorithms are used mainly for Key Establishment, Identification and Encryption. Diffie-Hellman Key Exchange (DHKE) [4] is an example of an asymmetric key algorithm used for key exchange and RSA is an encryption public-key algorithm [5]. PKC algorithms are fundamental security component in many cryptosystems, applications and such as Transport Layer Security (TLS) protocol [6]. Public key algorithms provide data encryption, key exchange, and digital signatures [7].

PCK algorithms can be categorized based on the mathematical problem used in the scheme into [4]: Integer-factorization based schemes such RSA and McEliece [8] algorithms and discrete logarithm-based schemes such as Diffie–Hellman key exchange and ELGamal encryption scheme [4]. Integer factorization is the process where an integer is decomposed to the product of smaller numbers. If these numbers are prime numbers, then it is called prime factorization. The complexity in this method arises when factoring a very large number because there no such known efficient algorithm. However, not all number with the same length are equal in complexity. When the number is the product of two coprime numbers, it is infeasible to factor this kind of numbers using the current technology [9]. Most non-RSA public-key algorithms with practical relevance are based on another one-way function, the discrete logarithm problem [3]. The security of many cryptographic schemes relies on the computational intractability of finding solutions to the Discrete Logarithm Problem (DLP). The discrete logarithm problem is defined in what are called cyclic groups. However, there are four families of alternative public key schemes [10] that are potentially interesting for use in practice: hash based, code-based, lattice-based and multivariate quadratic (MQ) public-key algorithms.

Practically, public key schemes are preferred to use due to many reasons such as the non-exitance of the secure communication channels. Therefore, the efficient implementation of public key cryptosystems is on demand especially if its implemented with appropriate technology with high precision design. In this paper, Schmidt-Samoa Cryptosystem (SSC) [11] will be used analyzed as efficient and comparable alternative to RSA which is a well-known secure and practicable public key scheme that can be used to protect information during the transmission over the insecure channels. SSC Cryptosystem is heavily based on modular arithmetic involving large prime numbers.

The remaining of this paper is organized as follows: Section 2 discusses the Schmidt-Samoa Cryptosystem (SSC) in details including SSC crypto-algorithm, the SSC factoring, numerical example of how SSC works, some possible attacks of SSC, and the underlying design issues and requirements followed by conclusions.

2. Schmidt-Samoa Cryptosystem (SSC)

Schmidt-Samoa Cryptosystem (SSC) is an asymmetric cryptographic technique (public key algorithm) in which security depends on the difficulty of integer factorization problem used for data encryption and decryption. Just like RSA, SSC uses very large prime numbers and modular arithmetic to provide different security services such as conditionality, integrity, and non-repudiation.

2.1. SSC Algorithm

To start the secure communication session, the receiver, who is Alice in this case, starts by choosing two large prime numbers *(p, q)* and then compute her public key $N = p^2 q$. Alice then share the public key (*N*) with Bob (and even other senders) who will use it to encrypt the plaintext messages communicated with Alice. Again, Alice computes her private key (*d*) to be used for decryption processes $d = N^{-1}$. Next, using the private key, Alice decrypts the ciphertext.

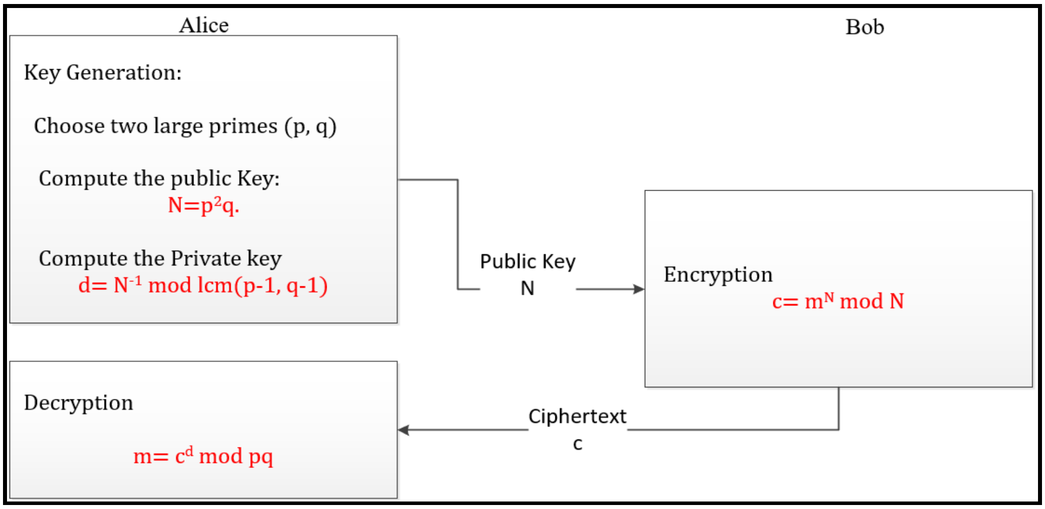

Fig.1. Complete Diagram of Schmidt-Samoa Algorithm.

Fig.1, shows the complete SSC algorithm diagram which is divided into three stages: key generation stage, Encryption stage, and Decryption stage. The challenge in SSC is the ability to factor out the public key which is the product of two very large primes. As the size of the key is increases, the factorization problem becomes even more complicated [9]. Factoring a number means defining that number as a product of prime numbers. In

SSC, factoring the public key (*N*) means as breaking the cryptosystem. If an attacker can factor out the public key, he can easily calculate the private key (*d*) and decrypt any data. As public key $N = p^2q$, is known to everyone, therefore factoring (*N*) leads to compute *p* and *q*. Then the private key can be computed using congruent (1) (where LCM is the least common multiple of two numbers):

$$d \equiv N^{-1} \bmod LCM(p-1, q-1) \tag{1}$$

For better understanding, we provide the following simplified numerical example. Let's assume that the plaintext message *m = 2* and the domain parameters *(p = 11, q = 17, m = 2)*, then we run *SSC (11,17,2)* as follows:

$$\begin{aligned}
&N = p^2q = 2057 \\
&d \equiv N^{-1} \bmod LCM(10,16) = 2057^{-1} \bmod 80 = 73 \\
&c = m^{2057} \bmod 2057 = 1855 \\
&m = 1855^{73} \bmod 187 = 2
\end{aligned}$$

2.2. Possible Attacks of SSC

Reasonably, there is no such a perfect system, but there are systems hard to be attacked. SSC is proved to be very secure [11], however, it is vulnerable to some known attacks such as Brute-force attack, Man-in-the-Middle attack, and Side Channel attack. Generally, all public key cryptography algorithms suffer from these attacks [3].

- Exhaustive search of SSC: In computer science, brute-force search or exhaustive search, also known as generate and test, is a very general problem-solving technique that consists of systematically generating all possible candidates for the solution and checking whether each candidate satisfies the problem's statement. For instance, finding the factorization of a very large number by trying all the numbers less than the asked number. In cryptography, an exhaustive search attack involves checking all possible keys until the correct key is found [12]. This strategy theoretically can be used against any cryptosystem by an attacker who is unable to take advantage of any weakness in the system that would make breaking the system easier. The length of the used key in the encryption process determines the practical feasibility of performing a brute force attack, with larger keys exponentially more difficult to break than smaller ones. One of the measures of the strength of an encryption system is how long it would theoretically take an attacker to successfully mount a brute force attack against it. In Schmidt-Samoa cryptosystem, as the bit size of the key is increased, the time needed to perform an exhaustive search would increase exponentially. It is believed that a 1024-bit key can be factored in period of 10-15 years, where it is possible for some intelligence agencies to compute the key earlier [12]. However, for 2048- bit or more, it is not feasible to factor out SSC key relying on the current technology (computers). Sample example of exhaustive search algorithm (brute force) is illustrated in figure 2 as it shows the possible trial values of simple 4-bit key.

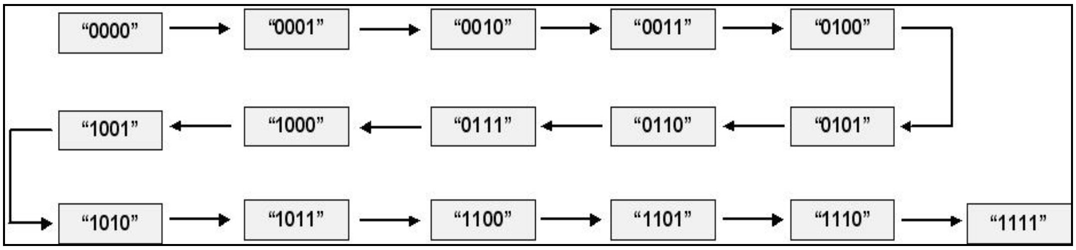

Fig.2. Example of Brute Force Attack of 4 bit Key

- Man-in-the-Middle Attack [13]: it is a type of cyberattack where a malicious actor inserts him/herself into a conversation between two parties, impersonates both parties and gains access to information that the two parties were trying to send to each other. It allows a malicious actor to intercept, send and receive data meant for someone else, or not meant to be sent at all, without either outside party knowing until it is too late. Man-in-the-middle attacks can be abbreviated in many ways, including MITM, MitM, MiM or MIM. An example of MITM by using SSC scheme is shown in Fig.3 where Alice generates her public and private keys and sends the public key over unsecure channel. However, Trudy interrupts the communication and generates new public key then sends it to Bob. Bob now encrypts data and sends it back to Alice on the unsecure channel, however, only Trudy who can decrypt the message. Trudy can generate new false message and send it to Alice, pass the original message, or just block it where Alice and Bob thinking they are communicating with each other securely.

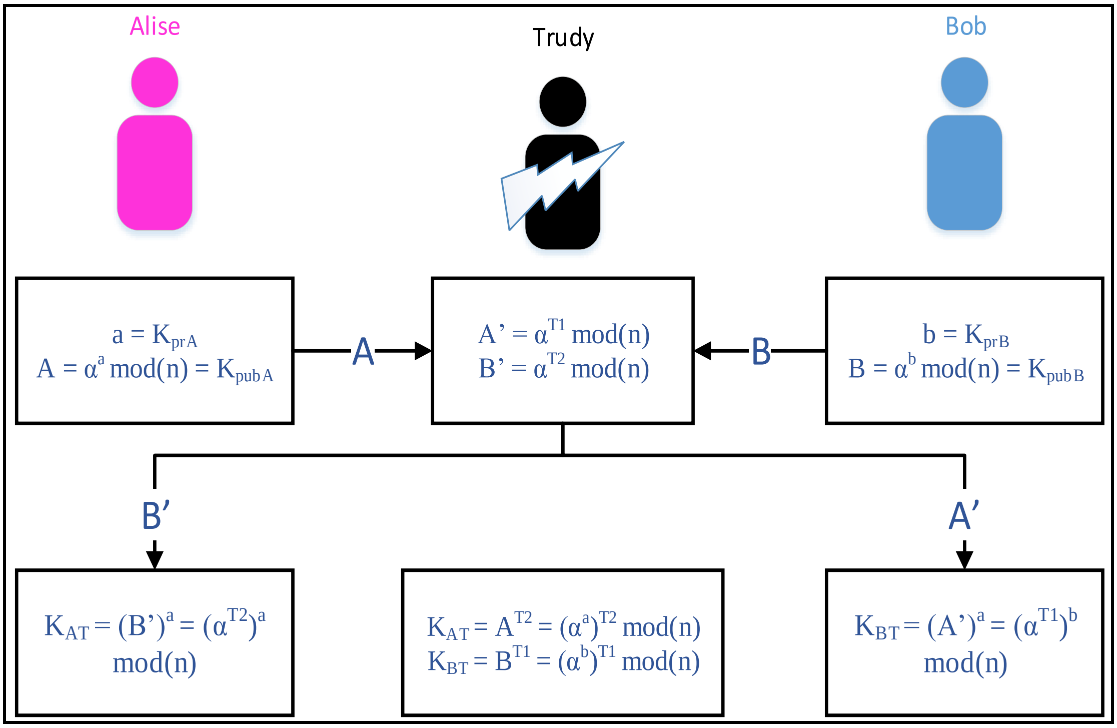
Alise
Trudy
Bob
$a = K_{prA}$
$A = \alpha^{a} \bmod(n) = K_{pubA}$
A
$A' = \alpha^{T1} \bmod(n)$
$B' = \alpha^{T2} \bmod(n)$
B
$b = K_{prB}$
$B = \alpha^{b} \bmod(n) = K_{pubB}$
B'
A'
$K_{AT} = (B')^{a} = (\alpha^{T2})^{a} \bmod(n)$
$K_{AT} = A^{T2} = (\alpha^{a})^{T2} \bmod(n)$
$K_{BT} = B^{T1} = (\alpha^{b})^{T1} \bmod(n)$
$K_{BT} = (A')^{a} = (\alpha^{T1})^{b} \bmod(n)$

Fig.3. MITM Attack Scheme for SSC.

- Side Channel Attack: In cryptography, a side-channel attack is an attack based on analyzing the physical implementation gained information of a cryptosystem, rather than a brute-force of any theoretical weakness [12]. They exploit information about the private key which is leaked through physical channels such as the power consumption or the timing behavior. However, to observes such channels, an attacker must have access to the cipher implementation, e.g., in cell phones or smart card. Fig.4 shows the power trace of an RSA implementation on a microprocessor [12], or the drown electric power by the processor to be more precise. The attacker goal is to extract the private key d which is used during the RSA decryption. It can be differentiated between the high and low activity from the graph, this behavior is explained by the square-and-multiply algorithm. If an exponent bit has the value 0, only a squaring is per formed. If an exponent bit has the value 1, a squaring together with a multiplication is computed.

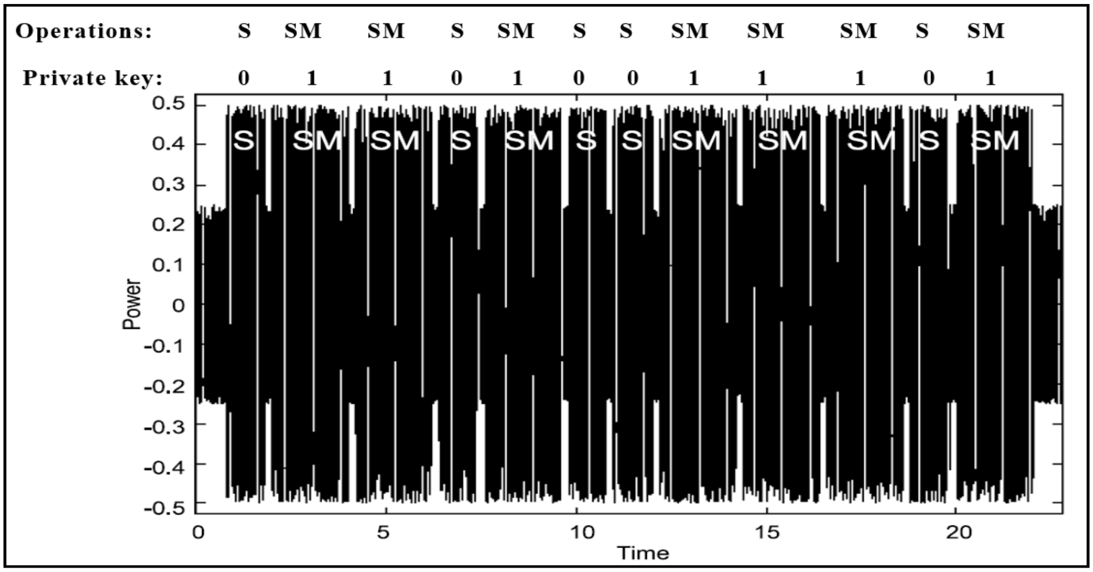

Fig.4. The Power Trace of an RSA Implementation.

2.3. SSC Services

SSC is very flexible and can provide the four main cryptographic services: confidentiality, integrity, authentication, and non-repudiation. As for RSA algorithm, SSC algorithm can be used to encrypt and decrypt private message providing, confidentiality and non-repudiation. Also, SSC can be implemented to be used as digital signature (DSA-SSC) as shown in Fig.5, providing integrity. PKI and alternative schemes; hashed-based, coded-based, etc., can be implemented using SSC.

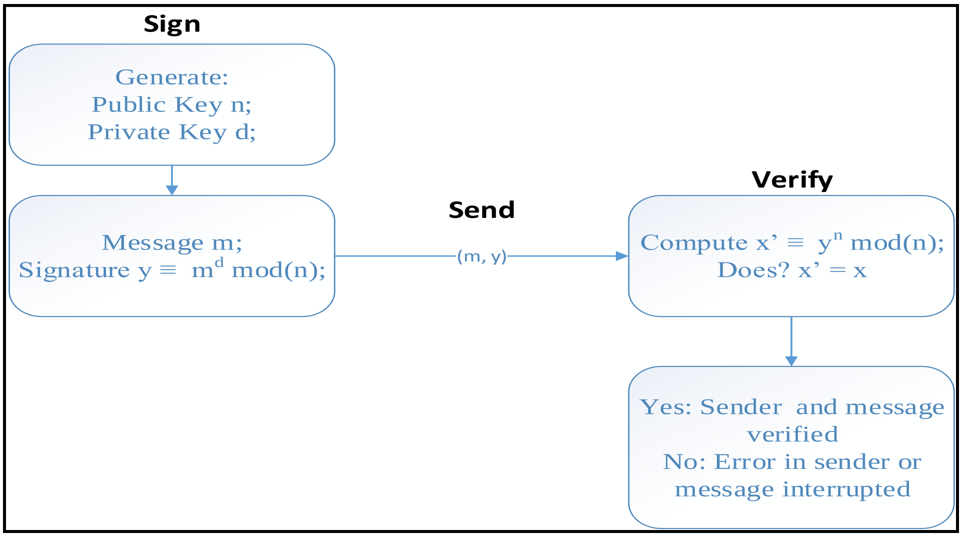

Fig.5. Digital Signature using Schmidt-Samoa Scheme.

2.4. SSC Underlying Design

As alluded earlier, SSC is a public key cryptosystem that its computations significantly based on the use of several digital arithmetic and modular arithmetic algorithms as well as different number theory schemes. It employs the properties of prime numbers alongside the congruent to produce a very secure hard to break cryptosystem. Arithmetic operation like multiplication and squaring, and modular exponentiation and modular inverse are involved in the algorithm to add complexity to the cipher. Thus, implementing a SSC coprocessor requires the contribution of many design components as seen in the diagram of figure 6.

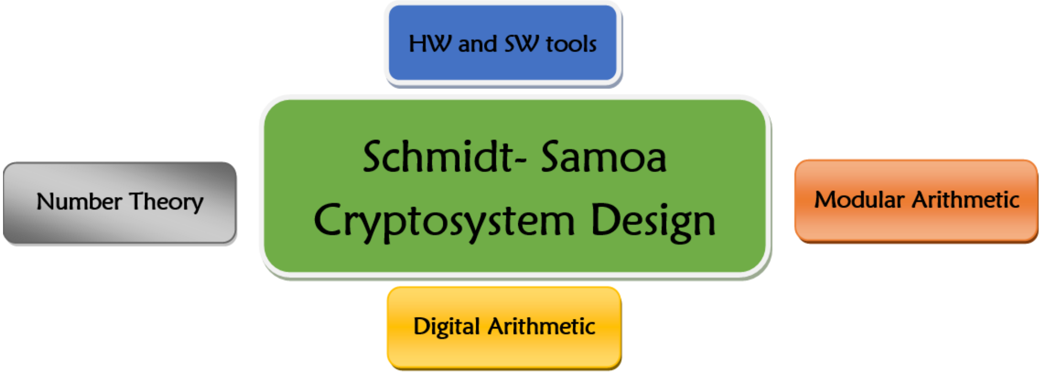

Fig.6. SSC Underlying Design Requirements Diagram.

- Number Theory Algorithms: Because of the modular factors (p, q) must be prime, therefore, two components are contributing here generate test a prime number with desired length: a random number generator (RNG) [2] and a prime number tester PNT) [14]. Also, to test the co-prime relativity, a greatest common devisor (GCD) unit [15] is required in Schmidt-Samoa. In addition, to generate the private key modulus, a Least common multiple (LCM) [15] unit is needed.

- Digital Arithmetic Algorithms: in order to compute the public key (N) which is also used as the encryption algorithm modulus, efficient arithmetic digital multiplier (used for squaring as well) unit is required to generate N, such as Karatsuba multiplier [16]. The multiplier is built from fast two operand adder units such as Kogge Stone adder (KSA) [17] as an efficient Parallel prefix adder [18], fast three operand adder such as Carry save adder [18] and multi-operand addition trees such as Wallace trees [18].
- Modular Arithmetic Algorithms: As for SSC encryption and decryption processes, an efficient modular expatiation such as [19] should be carefully selected as this operation consumes most of the time in the SSC system. Similarly, another costly operation is needed in the generation of decryption key which is the modular inverse (division by modulus) operation [9] which is well known to be one of the long-time operations performed by the Cryptoprocessor.
- Hardware/Software design tools: SSC Cryptoprocessor can be implemented either in software environment or in hardware platform. However, it's noted that building Cryptoprocessor via hardware is more secure and efficient than in software [20]. Nowadays, reconfigurable hardware devices are commonly spread to implement various digital applications such as cryptographic coprocessor and embedded systems design. It's largely recommended to implement SSC using the field programmable gate arrays (FPGA) [21] which provide wide range of flexibility and dynamic control of several design factors such as delay, area and power consumption. The reconfigurability feature of FPGA devices attracted many cryptographic researchers to implement their designs using FPGA devices benefiting from the spacious libraries and modules offered by Computer Aided Design (CAD) [22] tools as well as the flexibility of Hardware description languages (HDLs) [23].

Eventually, the adequate adoption of the efficient accelerated built-in units and component along with affordable high technology design platform will result in undoubtedly robust SSC cryptosystem that is comparable and competitive with RSA and many other well-known secure cryptosystems. It can replace RSA Cryptosystem in many applications such as in design of the cryptography system with multi-level crypto-algorithms [24], in the design an effective parallel digital signature algorithm for GPUs [25], in the design of robust image Steganography [26], in the design of an alternative equations for Guillou-Quisquater Signature scheme which is based originally on RSA [27], or many other valid applications.

3. Conclusions and Remarks

Schmidt-Samoa cryptosystem public key cryptosystem (SSC) with numerical example and sample possible attacks as well as the cryptosystem's design issues has been methodologically analysed and investigated in this paper. Thus, even if you use the best possible random number generators to create candidates for the primes that are needed to make SSC secure, the security of SSC encryption/decryption depends critically on the difficulty of factoring large integers which become easier for shorter key sizes due the existence of powerful computers. Therefore, SSC cryptography has had to rely on increasingly larger values for the integer modulus and, Hence increasingly longer encryption keys. As for RSA, these days you are unlikely to use a key whose length is shorter than 1024 bits for SSC as many people recommended to use 2048 or even 4096-bit keys.

References

[1] Denning, D.E.R.E, "Cryptography and data security", Reading, MA: Addison-Welsey.

[2] Q. A. Al-Haija, N. A. Jebril, and A. AlShua'ibi. (2015). Implementing variable length Pseudo Random Number Generator (PRNG) with fixed high frequency (1.44 GHZ) via Vertix-7 FPGA family. Network Security and Communication Engineering, CRC press, Pp. 105 -108.

[3] C. Paar, J. Pelzl, (2010) 'Understanding Cryptography'. Springer-Verlag Berlin Heidelberg Publisher. https://doi.org/10.1007/978-3-642-04101-3.

[4] Menezes, A.J., van Oorschot, P.C. and Vanstone, S.A., (1996), 'Handbook of applied cryptography', CRC Press, http://cacr.uwaterloo.ca/hac/

[5] Q. Abu Al-Haija, et. al, (2014) 'Efficient FPGA Implementation of RSA Coprocessor using Scalable Modules', 9th International Conference on Future Networks & Communications (FNC), Elsevier, Canada. https://doi.org/10.1016/j.procs.2014.07.092

[6] Dierks and Rescorla, (2008), Standards Track: The Transport Layer Security (TLS) Protocol Version 1.2', The IETF Trust, RFC 5246.

[7] Developer Network (2017). 'Cryptographic Services', Microsoft. https://docs.microsoft.com/en-us/dotnet/standard/security/

[8] H. Sun. Enhancing the Security of the McEliece Public-Key Cryptosystem. Journal of Information Science and Engineering 16, pages 799-812, 2000.

[9] W. Trappe and L. C. Washington, (2002) 'Introduction to Cryptography with Coding Theory', Prentice Hall, vol. 1: p.p. 1-176, http://dl.acm.org/citation.cfm?id=560133

[10] Daniel J. Bernstein, Johannes Buchmann, Erik Dahmen, (2009), 'Post-Quantum Cryptography', Springer-Verlag Berlin Heidelberg, DOI: 10.1007/978-3-540-88702-7

[11] Katja Schmidt-Samoa, (2006) ‘A New Rabin-type Trapdoor Permutation Equivalent to Factoring’, Electronic Notes in Theoretical Computer Science, Elsevier, vol.157, issue 3, p.p.79-94. https://eprint.iacr.org/2005/278.pdf

[12] Mark Burnett, (2007), ‘Blocking Brute Force Attacks', UVA Computer Science, University of Virginia (UVA). http://www.cs.virginia.edu/~csadmin/gen_support/brute_force.php

[13] Desmedt, Y. Man in the middle attack. In: van Tilborg, H.C.A. (ed.) Encyclopedia of Cryptography and Security, p. 368. Springer, Heidelberg (2005) Xx

[14] M. M. Asad, I. Marouf, Q. Abu Al-Haija, " Investigation Study of Feasible Prime Number Testing Algorithms", Acta Technica Napocensis Electronics and Telecommunications, 58 (3), Pp. 11– 15, 2017

[15] I. Marouf, M. M. Asad, Q. Abu Al-Haija, " Reviewing and Analyzing Efficient GCD/LCM Algorithms for Cryptographic Design", International Journal of New Computer Architectures and their Applications (IJNCAA), By Society of Digital Information and Wireless Communications (SDIWC), 7(1), Pp. 1-7, 2017.

[16] M. M. Asad, I. Marouf, Q. Abu Al-Haija, Qasem Abu Al-Haija, " Review of Fast Multiplication Algorithms for Embedded Systems Design ", International Journal of Scientific & Technology Research (IJSTR), 6 (8), Pp., 238 – 242, 2017.

[17] Kogge, P. & Stone, H. "A Parallel Algorithm for the Efficient Solution of a General Class of Recurrence Equations". IEEE Transactions on Computers, 1973, C-22, 783-791Xx

[18] M. D. Ercegovac and T. Lang, “Digital Arithmetic," Morgan Kaufmann Publishers, Elsevier, Vol1, Ch2, pages (51-136), 2004.

[19] I. Marouf, M. M. Asad, Q. Abu Al-Haija, "Comparative Study of Efficient Modular Exponentiation Algorithms", COMPUSOFT, An international journal of advanced computer technology, 6 (8), Pp. 2381– 2389, 2017

[20] L. Tawalbeh and Q. Abu Al-Haija," Enhanced FPGA Implementations for Doubling Oriented and Jacobi-Quartics Elliptic Curves Cryptography,” Journal of Information Assurance and Security (JIAS), By Dynamic Publishers Inc., Vol 6 (3), Pp. 167-175, 2010

[21] C. Maxfield, " The Design Warrior’s Guide to FPGAs: Devices, Tools and Flows", Mentor Graphics Corporation and Xilinx, Elsevier, 2004.

[22] Nicos Bilalis, (2000), 'Computer Aided Design CAD', INNOREGIO Project: dissemination of innovation and knowledge management techniques, Technical University of Crete.

[23] David Harris Sarah Harris, (2012), ‘Digital Design and Computer Architecture’, Imprint: Morgan Kaufmann, ISBN: 9780123944245, Elsevier.

[24] Surinder Kaur, Pooja Bharadwaj, Shivani Mankotia,"Study of Multi-Level Cryptography Algorithm: Multi-Prime RSA and DES", International Journal of Computer Network and Information Security(IJCNIS), Vol.9, No.9, pp.22-29, 2017.DOI: 10.5815/ijcnis.2017.09.03.

[25] Sapna Saxena, Neha Kishore," PRDSA: Effective Parallel Digital Signature Algorithm for GPUs ", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.7, No.5, pp. 14-21, 2017.DOI: 10.5815/ijwmt.2017.05.02.

[26] M.I.Khalil,"Medical Image Steganography: Study of Medical Image Quality Degradation when Embedding Data in the Frequency Domain", International Journal of Computer Network and Information Security(IJCNIS), Vol.9, No.2, pp.22-28, 2017.DOI: 10.5815/ijcnis.2017.02.03

[27] J. Ettanfouhi, O. Khadir," Alternative Equations for Guillou-Quisquater Signature Scheme ", International Journal of Computer Network and Information Security, 2016, 9, 27-33, DOI: 10.5815/ijcnis.2016.09.04/

Authors' Profiles

Qasem Abu Al-Haija is a senior lecturer of Electrical and Computer Engineering at King Faisal University. Eng. Abu Al-Haija received his B.Sc. in ECE from Mu'tah University in Feb-2005 and M.Sc. in computer engineering from Jordan University of Science & Technology in Dec-2009. His current research Interests: Information Security & Cryptography, Coprocessor & FPGA design, Computer Arithmetic, Wireless Sensor Networks.

Muhammad M. Asad is a senior student of Electrical Engineering Department at King Faisal University. He is a Syrian resident born on Jan-01-1994 and excellent in both languages Arabic and English. His research interests include (but not limited to): Public Key Cryptography, FPGA Design, Digital Arithmetic, Microcontroller Design, Electronic Design.

Ibrahim A. Marouf is a senior student of Electrical Engineering Department at King Faisal University. He is a Syrian resident born on Aug -15-1995 and excellent in both languages Arabic and English. His research interests include (but not limited to): Public Key Cryptography, FPGA Design, Digital Arithmetic, Microcontroller Design, Electronic Design.

How to cite this paper: Qasem Abu Al-Haija, Mohamad M.Asad, Ibrahim Marouf,"A Systematic Expository Review of Schmidt-Samoa Cryptosystem", International Journal of Mathematical Sciences and Computing(IJMSC), Vol.4, No.2, pp.12-21, 2018.DOI: 10.5815/ijmsc.2018.02.02