Security Evaluation Over Lightweight Cryptographic Protocols

Seyed-Mohsen Ghoreishi, Shukor Abd Razak, Ismail Fauzi Isnin, Hassan Chizari
Faculty of Computing, Universiti Teknologi Malaysia (UTM), 81310 Johor, Malaysia
mohsen.gh100@gmail.com, {shukorar, ismailfauzi, chizari}@utm.my

Abstract—Due to the applicability of a wide range of cryptosystems in recently proposed applications, large variety of cryptographic schemes have been developed. It can be claimed that proposing a cryptographic protocol to satisfy security and efficiency requirements is one of the significant challenging issues. Nevertheless, cryptographic research community suffers from non-existence of an integrated pattern to categorize and standardize possible challenges of mentioned concerns. These drawbacks could in turn lead to much confusion for the researchers who are not expert in this research area. Therefore, we paid particular attention to assemble a powerful document to fill this gap between the beginners and the experts. Our final goal is to make other researchers able to classify the challenges over Provably Secure cryptosystems or lightweight ones, analyze the proposed scheme based on the determined components and help them to find better solutions for the future researches.

Keywords—Provable Security, lightweight, Security Evaluation, Attack Model

I. INTRODUCTION

The widely usage of collaborative and distributed applications in the resource constrained devices, recently led to developing a large variety of lightweight security mechanisms in such environments. Moreover, the natural vulnerability of such communicating links made the security field one of the most interesting challenges especially in resource constraints platforms. In this way, many researchers have been tried to propose appropriate solutions to make such environments more reliable than ever before. From the security viewpoint, a subset of mentioned solutions have been tried to prevent the considered environment from some categories of external attacks [1-3], while some others tried to detect possible threats and proposed some solutions to resist against [4-6]. If roughly speaking, it is possible to claim that the level of proposed secure protocols can be emphasizing on cryptographic protocols or as a higher level they can use other cryptographic functions as a building block to make the considered protocol.

From the security perspective, the objective of this research is to focus on those categories of cryptosystems, which are provably secure. Being provably secure emphasizes on this fact that breaking the considered scheme would lead to solve one of the mathematical hard problems. Beside of what mentioned above, it is necessary to point out that the limitations of resources such as memory usage, computation capacity, energy consuming, etc., made the majority of the proposed schemes inappropriate for resource-constrained devices. The importance of efficiency in mentioned cryptographic schemes motivated us to pay particular attention to the efficiency of cryptosystems beside of the security scientific area.

The final goal of this research is based on three dimensions. As the first dimension, we have tried to trace the way that a subset of researchers made their proposed cryptosystems lightweight. The outline of this part is to clarify what investigated in [7]. As the second dimension, we have tried to introduce the boundary of well-known standard attacks against the main cryptographic primitives, Encryption, Digital Signature and key Agreement. Finally, the last dimension introduces possible challenges for the future researches over cryptosystems especially lightweight and/or provably secure ones by expanding what investigated in [7] to cover more variety of cryptographic protocols.

The rest of this paper is organized as follows: the second section is related to tracing a sequence of researches to make cryptosystems lightweight for resource-constrained platforms. The third section provides an extensive presentation of the standard attacks for three main cryptographic primitives, Encryption, Digital Signature and Key Agreement. Then, in the fourth section, we outlined the possible challenges of lightweight and/or provably secure cryptosystems to cover a wide range of possible open problems in these scientific areas. Finally, the last section concludes the contents of this document.

II. A PROGRESSIVE HISTORY OF MAKING CRYPTOGRAPHIC SCHEMES LIGHTWEIGHT

As it is pointed out before, the limitations of resources is one of the most significant challenging issues in the variety of proposed cryptographic schemes. To solve this problem many proposed schemes have tried to use symmetric cryptosystems such as RC5 [8] and Skip-Jack [9] to make the proposed scheme lightweight. Although symmetric cryptographic schemes were more efficient than public-key ones, they suffer from a subset of significant problems especially from key management perspective. In contrast with symmetric cryptosystems, the use of public-key cryptographic schemes could make key management security services easier and reduces the overhead of transmitting processes [10,11].

Mentioned reasons above were sufficient to persuade a large group of developers to find a solution to make public key cryptosystems feasible in resource-constrained platforms [7]. To make the use of public key cryptosystems feasible in such resource constrained environments, it is possible to refer to what Gaubatz et al. proposed in [10]. In this document, the authors could reduce the traffic overhead by simplifying the implementation of a public-key cryptographic scheme, therefore reducing the amount of

transmission power. Beside of this, Baek et al. could propose a lightweight public-key encryption scheme from computation time and communication overhead viewpoints [12].

Motivated by what pointed above, cryptography research community have concluded that the use of Elliptic Curve Cryptography (ECC) is the golden key to make public key cryptosystems lightweight in order to make them appropriate for resource constrained platforms [7]. As an example, we can refer to the result of what studied by Tan et al. [13] who compared the energy cost of two popular Public-Key cryptosystems, RSA and ECC. The last result of this study indicated that the use of ECC instead of RSA based cryptosystems leads to obtaining smaller key size, decreasing the expense of computation power and communication capacity and reduces the amount of transmitted or stored data. The TABLE I and TABLE II demonstrate the used key sizes for ECC based cryptosystems and RSA based ones as a function of considered security levels based on two standard documents, NIST [14] and ECRYPT [15], respectively.

TABLE I. KEY SIZES OF NIST STANDARD DOCUMENT [14]

Security level (bits) / Category of cryptosystems	80	128	256
ECC-based	160	256	512
Finite field	1024	3072	15360

TABLE II. KEY SIZES OF ECRYPT STANDARD DOCUMENT [15]

Security level (bits) / Category of cryptosystems	80	128	256
ECC-based	160	256	512
Finite field	1248	3248	15424

It is worth noting that the "Security Level" parameter in the TABLE I and TABLE II refers to the size of required cryptographic field to attain a given level of security against the Discrete Logarithm mathematical hard problem. The outcome of mentioned results above, emphasizes on the fact that the use of ECC based cryptosystems leads to implementing more efficient public-key cryptographic schemes. Accordingly, a large variety of lightweight ECC based cryptosystems have been proposed to fulfill the requirements of a subset of resource constrained environments. The use of bilinear pairings over algebraic elliptic curves is the basis of a large category of mentioned ECC based cryptosystems [7]. Therefore, pairing based cryptography has had a significant role in the most proposed lightweight cryptosystems especially in resource-constrained ones [16]. Generally, bilinear pairings are one of the significant categories of algebraic maps, which most of them are constructed based on Miller algorithm [17]. Since, the use of these maps is the basis of many recently proposed lightweight cryptosystems, various researches have been done to make bilinear pairings more efficient in order to make them perfect for lightweight pairing based cryptographic schemes in resource-constrained platforms [7].

It is necessary to point out to deploy public key cryptosystems by the use of bilinear pairings, existing entities must be able to validate the public-key of the other side authorized ones. Although this concern can be settled by the use of Public Key Infrastructures (PKI), the high expense of PKI seems to make this method impractical in resource- constrained environments. To eliminate this drawback, identity based cryptosystems came into the mentioned scientific area. The idea of identity based cryptosystems in the context of public key ones was first suggested by Adi Shamir [18], in order to use the user's identifier instead of their public key, therefore eliminating the need to digital certificates. Then, implementing this idea remained an open problem for seventeen years, until Boneh et al. could propose the first applicable Provably-Secure identity based cryptosystem under the Bilinear Diffie Hellman (BDH) assumption [19]. The next section provides an overview for the boundary of standard attacks against the provably secure main cryptographic primitives, which most of them are defined in the context of identity-based cryptosystems.

III. BOUNDARY OF ATTACKS IN MAIN PRIMITIVES

This section assigns to a review over the boundary of attacks in Provably Secure schemes for three main primitives, Encryption, Digital Signature, and Key Agreement. The considered model for the determined attacker is an essential component in Provable Security evaluation method. To prove the security of an evaluated scheme, this model, named Attack Model, aimed to identify the boundaries of possible attacks that the evaluated scheme must be secure against. Hence, based on the considered primitive (e.g. Encryption, Digital Signature, Key Agreement, etc.) this model should be defined. More precisely, the model of queries that an imaginary adversary can issue within a polynomial time complexity before attempting to break the scheme, shapes the model of mentioned boundary of possible attacks. Clearly, considering the ability of issuing wide and various queries for the imaginary adversary brings a much more powerful model than a limited one.

Another essential component of Provable Security evaluation method is the Attacker Goal. In fact, the Attacker Goal determines the form of the challenge between the security evaluator and the determined imaginary adversary. It is necessary to

point out that this goal is a probability distribution and could be "computational" or "decisional". It is noteworthy that easier goal from the adversary entity's viewpoint can make the Attacker Goal stronger.

The Attack Models for fundamental cryptographic primitives "Encryption," "Digital signature," and "Key Agreement" are discussed in the next subsections.

A. Attack Model of Encryption schemes

There are two main classes of Attack Models for Encryption schemes named Chosen Plaintext Attack(CPA) and Chosen Ciphertext Attack(CCA) that have been introduced by Bellare et al. in [19]. In the first class, the adversary might be challenged through one of the encryptions of the plaintexts of her choice while in the second one the decryption oracle is also accessible. Beside of these two classes, it is possible to define adaptive Chosen Ciphertext Attack which is more powerful than normal CCA. In this kind of attack model, the decryption oracle is accessible for the adversary even after obtaining the challenge ciphertext[19].

Moreover, two Attacker Goals have been considered for Encryption schemes by the same authors named Indistinguishability (IND) and Non-Malleability (NM). In the first one, the considered adversary cannot obtain any knowledge about plaintext relevant to the challenging ciphertext. In Non-Malleability, the adversary who obtained two plaintexts P1 and P2 (meaningfully related) and the ciphertext C1 (the ciphertext of P1) is incapable to produce C2 (the ciphertext of P2).

Similar to this subsection, following subsection focuses on the boundary of adversary in another important security primitive which is Digital Signature.

B. Attack Model of Digital Signature schemes

Attack Model for Digital Signature can be categorized in two main groups called "key-only attacks" and "message attacks" based on the discussions in [20]. The first one covers those attacks that adversary assumed to have just the signer's public-key whereas in the other one, the corresponding signature for a group of known or chosen messages can be taken from an oracle which is accessible by the adversary. Hence, the message attacks are more powerful than the key-only attacks.

In general, message attacks can be categorized into three groups [20]:

a. **Known-Message Attack (KMA).** Valid signatures of a set of messages are given to the adversary by the oracle. The adversary has knowledge about the messages but they are not selected based on the adversary's interest.
b. **Chosen-Message Attack (CMA).** The adversary can obtain valid signatures of a set of messages selectively but before the challenge phase.
c. **Adaptive Chosen-Message Attack (ACMA).** The adversary is able to communicate with the oracle as a signer and request signatures for desired messages adaptively even after the challenge phase.

Attacker Goal for an attacker against Digital Signature schemes can be defined in three main classes [20]:

d. Total Break. The adversary aimed to compute the signer's private-key or to find an efficient algorithm to forge all valid signatures.
e. Selective Forgery. The adversary must be able to generate valid signatures for a set of chosen messages.
f. Existential Forgery. The adversary must be able to forge a signature for at least one of the messages.

It is noteworthy that, although the last goal is the easiest goal for the adversary, it brings stronger model for defense than two others.

C. Attack Model of Key Agreement schemes

In continue to what pointed out before, the Attack Model of a Key Agreement protocol can be considered from two dimensions. Based on this, the only well-defined model for the notion of security in Key Agreement protocols is based on Bellare and Rogaway Model (BRM) [21]. In this Attack Model, the adversary can access the oracle from the first party's viewpoint to issue three followed queries:

$Send(\Pi_{ij}^{s}, x)$: This query lets the considered adversary to send her chosen message as a "material exchange" sub-phase message to the ID_j entity in the session "s" of the protocol.

$Reveal(\Pi_{ij}^{s})$: This query lets the adversary to obtain the shared key that can be established between ID_i and ID_j in the session "s" of the protocol.

$Corrupt(t)$: In this query the adversary can issue the first party's long-term private key.

It is worth mentioning that an oracle at any time can be in one of the following possible states:

Accepted: in this case, the adversary issues allowed queries.
Rejected: in this condition, the adversary issues not- allowed queries.
Opened: an oracle is opened if the adversary has answered it in one of the reveal queries.

Like the notion of security in other primitives, the adversary at some time decides to be challenged. At this time, the adversary asks a Test query on a Fresh oracle.

An accepted oracle such as Π_{ij}^{s} named Fresh if the adversary did not issue the Reveal (Π_{ij}^{s}) query, the query Corrupt (i) have not been asked by the adversary, and the oracle Π_{jl}^{t} is not opened. However if the adversary asked a Test (Π_{ij}^{s}) query in the challenge phase, the oracle randomly chooses $b \in_r \{0,1\}^*$ if b=0 the oracle gives the adversary the corresponding session key, but otherwise it gives her a random sample instead. Finally, the adversary outputs her guess for b.

Based on what pointed out before, the model of adversary's guess is decisional. So, the function of guess probability distribution for an adversary such as "A" against the key agreement scheme "KA" can be obtained from following equation:

$$Adv_{A}^{KA} = 2 \times |Pr(Correct\ Distinguish) - \frac{1}{2}| \quad (1)$$

In continue to what mentioned before, the TABLE III, introduces six provably secure cryptographic schemes of three main primitives.

TABLE III. CONSIDERED ATTACK MODEL FOR A SUBSET OF PROPOSED SCHEMES

Category of protocol	Author(s)	Attack Model	
		Model	Goal
Encryption	Boneh, Franklin [23]	CPA	IND
Encryption	Boneh, Boyen [24]	CCA	IND
Digital Signature	Boneh et al. [25]	CMA	SF
Digital Signature	Boldyreva [26]	CMA	EF
Key Agreement	Wang [27]	BRM	BRM
Key Agreement	Chen, Kudla [28]	BRM	BRM

It is worth to note that although it is possible to compare two provably secure schemes from the reduced mathematical hard problem [22], this paper excludes this scientific topic. The next section issues possible challenges of lightweight and/or provably secure cryptographic protocols.

IV. Future Challenges Around Lightweight And/Or Provably Secure Cryptosystems

In continue to what investigated in the previous sections, this section assigns to a subset of possible issues and challenges, which can be considered as future researches in the area of lightweight and provably secure schemes over the use of bilinear pairings in the context of identity based cryptosystems. Some findings of this research, are as follows:

1) Proving the security of a novel proposed cryptographic scheme

The main significance of a novel research in this category is to prove that the proposed scheme is more reliable than other existing ones. This group of developers would be able to reach this goal by doing a combination of followed methods:

a) To reduce the security of the proposed scheme to a new mathematical hard problem. It is necessary to point out that in this case, the developer must claim and prove that the determined mathematical hard problem is more powerful than other reduced ones in the considered comparable provably secure scheme

b) To consider stronger notion of security by assuming a stronger Attack Model or stronger Attacker Goal based on what mentioned in the third section.

2) Improving an existing cryptographic scheme from efficiency or performance viewpoint

The main focus of this group of researches is to focus on a considered cryptosystem or a subset of them, instead of proposing a novel one. This group of developers are able to improve a determined scheme by doing a combination of followed ways:

a) To decrease the expense of the determined scheme by considering some criterions such as computational cost, communicational capacity, memory or energy usage, etc.
b) To improve the functionality of a considered secure protocol by eliminating the number of involving entities such as Trusted Third Party
c) To transform one of the provably secure cryptographic scheme to the another one to obtain the advantages of the first primitive

3) Comparing various cryptographic schemes to analyze their functionality

One of the possible challenges in the area of provably secure cryptosystems is to compare the efficiency or performance of a group of schemes from security or expense viewpoints, based on what mentioned in the last item. This comparison would be beneficial due to make future researchers able to categorize the existing schemes based on new benchmarks. In addition, this comparison would be a useful way to find out the advantages of the proposed schemes in the mentioned scientific area.

4) Attacking on a known cryptographic scheme or a subclass of them

The other possible challenge in the area of provably secure cryptosystems is to find a subset of vulnerabilities of a subset of schemes to prove that they are not resistant enough against the claimed attacks.

5) Finding appropriate applications for a determined cryptographic scheme

In addition to the mentioned challenges above, it is possible to use a considered cryptographic scheme as a building block of another protocol or application.

V. CONCLUSION

Due to the importance of reliability and efficiency of the existing cryptographic schemes, many researchers have tried to propose provably secure and/or lightweight cryptographic schemes. In order to contribute further researches in these fields, this paper issues possible challenges beside of required backgrounds of these two scientific areas.

REFERENCES

[1] Capkun, S., Buttyan, L. and Hubaux, J.-P. (2003). "Self-organized public-key management for mobile ad hoc networks". IEEE Transactions on Mobile Computing. 2(1), 52 – 64. ISSN 1536-1233.

[2] Douceur, J. R. (2002). "The Sybil Attack". In IPTPS '01: Revised Papers from the First International Workshop on Peer-to-Peer Systems. London, UK: Springer-Verlag. ISBN 3540441794, 251– 260.

[3] Yi, S. and Kravets, R. (2003). "MOCA: Mobile Certificate Authority for Wireless Ad Hoc Networks". In 2nd Annual PKI Research Workshop Program.65–79.

[4] Anjum, F. and Talpade, R. (2004). "LiPaD: lightweight packet drop detection for ad hoc networks". Vehicular Technology Conference, 2004.VTC2004-Fall.2004 IEEE 60th. 2, 1233–1237. ISSN 1090-3038.

[5] Subhadrabandhu, D., Sarkar, S. and Anjum, F. (2004). "Efficacy of misuse detection in ad hoc networks". Sensor and Ad Hoc Communications and Networks. IEEE SECON 2004. 2004 First Annual IEEE Communications Society Conference on, 97–107. doi:10.1109/SAHCN.2004.1381907.

[6] Vigna, G., Gwalani, S., Srinivasan, K., Belding-Royer, E. M. and Kemmerer, R. A.(2004). "An intrusion detection tool for AODV- based ad hoc wireless networks". In Proceedings - Annual Computer Security Applications Conference, ACSAC. Los Alamitos, CA 90720-1314, United States. ISSN 1063-9527, 16 – 27.

[7] SM Ghoreishi, IF Isnin. (2013). "Secure Lightweight Pairing-Based Key-Agreement Cryptosystems: Issues and Challenges". IACSIT International Journal of Engineering and Technology, Vol. 5, No. 2.

[8] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, . (2002). "SPINS: Security protocols for sensor networks," in Proc. Conf. Wireless Networks, pp. 521-534.

[9] C. Karlof, N. Sastry, and D. Wagner. (2004). "Tinysec: A link layer security architecture for wireless sensor networks," in 2nd ACM Sens Sys, pp.162-175, Nov.

[10] G. Gaubatz, J.-P. Kaps, E. Oztruk, and B. Sunar. (2005). "State of the art in ultra-low power public key cryptography for wireless sensor networks", In Proc. PerSec '05, pages 146–150. IEEE.

[11] J. K. Liu, J. Baek, J. Zhou, Y. Yang, and J. W. Wong. (2010). "Efficient online/offline identity-based signature for WSN" , In IJIS 9(4): 287-296.

[12] J. Baek, H. Tan, J. Zhou, and J. Wong. (2008). "Realizing stateful public key encryption in wireless sensor Network", In Proc. IFIP-SEC '08, pages 95–108. Springer-Verlag.

[13] C. Tan, H. Wang, S. Zhong, and Q. Li. (2008). "Body sensor network security: an identity-based cryptography approach", In Proc. 1st ACM conference on Wireless Network Security, pages 148–153. ACM.

[14] NIST Recommendation For Key Management Part 1: General, NistSpecialpublication 800-57. August,(2005).

[15] ECRYPT Yearly Report On Algorithms And Keysizes (2004).

[16] L.B. Oliveira and R.Dahab. (2006). "Pairing-based cryptography for sensor networks" ,In 5th IEEE International Symposium on Network Computing and Applications, Cambridge,MA, July.

[17] V. Miller. (1986). "Short programs for functions on curves", Unpublished manuscript.

[18] Adi Shamir. (1985). "Identity-based cryptosystems and signature schemes" , Advances in Cryptology - CRYPTO '84, LNCS 0196, pp. 47-53, Springer-Verlag.

[19] Mihir Bellare , Anand Desai , David Pointcheval , And Phillip Rogaway. (1998). "Relations Among Notions Of Security For Public- Key Encryption Schemes". Crypto '98.

[20] A. Menezes, P. V. (1996). "Handbook Of Applied Cryptography". Crc Press.

[21] Bellare, M., Rogaway,P. (1993). "Entity Authentication And Key Distribution". Advances In Cryptology—Crypto '93.

[22] Chen, L., Cheng, Z. (2005). "Security proof of the Sakai- Kasahara'sidentity-based encryption scheme". In: Cryptography and Coding, pp.442–459. Springer, Heidlberg, LNCS 3706.

[23] D. Boneh, M. Franklin. (2003). "Identity Based Encryption from the Weil Pairing". SIAM J. of Computing, Vol. 32, No. 3, pp. 586-615.

[24] D. Boneh, X. Boyen. (2004). "Efficient Selective-ID Secure Identity Based Encryption Without Random Oracles". In Proceedings of Eurocrypt.

[25] D. Boneh, B. Lynn, H. Shacham. (2001). "Short Signatures from the Weil Pairing". In Proceedings of Asiacrypt.

[26] A. Boldyreva. (2003). "Efficient Threshold Signature, Multisignature and Blind Signature Schemes Based on the Gap-Diffie-Hellman- Group Signature Scheme". PKC 2003, LNCS 2139, pp. 31-46, Springer-Verlag.

[27] Wang, Y. (2013). "Efficient Identity-Based And Authenticated Key Agreement Protocols". Transactions On Computational Science Xvii.

[28] Chen, L., Kudla, C. (2003). "Identity Based Authenticated Key Agreement From Pairings". Ieee Computer Security Foundations Workshop.