SECURE PAIRING-FREE TWO-PARTY CERTIFICATELESS AUTHENTICATED KEY AGREEMENT PROTOCOL WITH MINIMAL COMPUTATIONAL COMPLEXITY

SEYEDMOHSEN GHOREISHI

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Doctor of Philosophy (Computer Science)

School of Computing
Faculty of Engineering
Universiti Teknologi Malaysia

AUGUST 2019

ACKNOWLEDGEMENT

First and foremost, I would like to give my immense appreciation to **Dr. Ismail Fauzi bin Isnin**, who has served as the main supervisor throughout the doctoral program for his guidance and outstanding scientific support during my study at UTM. Thanks is also due to him helpful comments on the text. I would like also to express my special appreciation and thanks to my co-supervisors **Assoc. Prof. Dr. Shukor Abd Razak** and **Dr. Hassan Chizari** for being supportive and also for encouraging my research. I consider myself very fortunate for being able to work with such very considerate and encouraging supervisors like them. Besides, I would like to thank the authority of Universiti Teknologi Malaysia (UTM) for providing me with a good environment and facilities to complete this project.

ABSTRACT

Key agreement protocols play a vital role in maintaining security in many critical applications due to the importance of the secret key. Bilinear pairing was commonly used in designing secure protocols for the last several years; however, high computational complexity of this operation has been the main obstacle towards its practicality. Therefore, implementation of Elliptic-curve based operations, instead of bilinear pairings, has become popular recently, and pairing-free key agreement protocols have been explored in many studies. A considerable amount of literatures has been published on pairing-free key agreement protocols in the context of Public Key Cryptography (PKC). Simpler key management and non-existence of key escrow problem make certificateless PKC more appealing in practice. However, achieving certificateless pairing-free two-party authenticated key agreement protocols (CL-AKA) that provide high level of security with low computational complexity, remains a challenge in the research area. This research presents a secure and lightweight pairing-free CL-AKA protocol named CL2AKA (CertificateLess 2-party Authenticated Key Agreement). The properties of CL2AKA protocol is that, it is computationally lightweight while communication overhead remains the same as existing protocols of related works. The results indicate that CL2AKA protocol is 21% computationally less complex than the most efficient pairing-free CL-AKA protocol (KKC-13) and 53% less in comparison with the pairing-free CL-AKA protocol with highest level of security guarantee (SWZ-13). Security of CL2AKA protocol is evaluated based on provable security evaluation method under the strong eCK model. It is also proven that the CL2AKA supports all of the security requirements which are necessary for authenticated key agreement protocols. Besides the CL2AKA as the main finding of this research work, there are six pairing-free CL-AKA protocols presented as CL2AKA basic version protocols, which were the outcomes of several attempts in designing the CL2AKA.

ABSTRAK

Protokol perjanjian kekunci memainkan peranan penting dalam mengekalkan keselamatan dalam banyak aplikasi kritikal berikutan pentingnya kerahsiaan sesuatu kekunci. Pasangan-Bilinear telah biasa digunakan dalam merekabentuk protokol keselamatan sebelum ini. Namun, kerumitan dan kompleksiti dalam komputasi operasinya menjadi penghalang ke arah penggunaannya secara praktikal. Maka, pengunaan operasi berasaskan Lengkungan-Eliptik menjadi popular pada masa kini. Maka, protokol perjanjian kekunci awam bebas-pasangan banyak diteroka dalam banyak kajian semasa. Sejumlah besar kajian diterbitkan berkenaan penggunaan protokol perjanjian kekunci awam bebas-pasangan dalam konteks Kriptografi Kekunci Awam (PKC). Pengurusan kekunci yang lebih mudah serta tiada masalah key-escrow menjadikan PKC tanpa sijil lebih menarik secara praktikalnya. Walau bagaimanapun, menghasilkan protokol perjanjian kekunci berpasangan tanpa sijil (CL-AKA), yang memastikan tahap keselamatan yang tinggi, beserta kerumitan komputasi yang rendah, masih kekal merupakan satu cabaran dalam bidang penyelidikan ini. Kerja penyelidikan ini membentangkan satu protokol CL-AKA yang selamat dan ringan dari aspek komputasi operasinya, yang dinamakan CL2AKA. Ciri-ciri protokol CL2AKA ini ialah, ianya mempunyai komplesiti komputasi yang ringan disamping overhed komunikasi dapat dikekalkan sama seperti protokol sediaada dari kerja penyelidikan yang berkaitan. Hasil dari perbandingan menunjukkan protokol CL2AKA adalah kira-kira 21% lebih rendah kompleksiti komputasinya berbanding protokol CL-AKA bebas-pasangan yang paling efisien iaitu (KKC-13), dan 53% lebih rendah komplesiti komputasinya berbanding protokol CL-AKA bebas-pasangan dengan jaminan tertinggi iaitu (SWZ-13). Tahap keselamatan protokol CL2AKA dinilai berdasarkan kaedah Provable yang dibuktikan menggunakan model eCK. Selain itu, Ia juga terbukti bahawa protokol CL2AKA menyokong semua keperluan keselamatan sesuatu protokol perjanjian kunci yang sah. Selain CL2AKA merupakan penemuan utama kerja penyelidikan ini, terdapat enam protokol CL-AKA bebas-pasangan dibentangkan sebagai protokol versi asas protokol CL2AKA. Enam protokol ini merupakan dapatan yang terhasil dari beberapa cubaan dalam merekabentuk CL2AKA.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ADV	–	Adversary
AKA	–	Authenticated Key Agreement
CA	–	Certificate Authority
CCA	–	Chosen Ciphertext Attack
CDH	–	Computational Deffie Hellman
CL-AKA	–	Certificateless Authenticated Key Agreement
Cless	–	Certificateless (AKA protocol)
CL2AKA	–	Certificateless two-party Authenticated Key Agreement (the proposed protocol)
CL-PKC	–	Certificateless Public Key Cryptography
CPA	–	Chosen Plaintext Attack
DDH	–	Decisional Deffie Hellman
ECC	–	Elliptic Curve Cryptography
eCK	–	extended Canetti-Krawczyk
EP	–	Exponent Problem
FS	–	Forward Secrecy
HP	–	Hard Problem
HPC	–	Hard Problem Challenger
IND	–	Indistinguishability
KA	–	Key Agreement
KC	–	Key Control
KCI	–	Key-Compromise Impersonation
KGC	–	Key Generation Center
KKS	–	Known-Key Security
KSSTI	–	Known Session-Specific Temporary Information
NM	–	Non-Malleability
ORA	–	Oracle
PFS	–	Perfect Forward Secrecy
PKC	–	Public Key Cryptography

PKG	–	Private Key Generator
PUB	–	a subset of publics and openly transferred parameters
SIM	–	Simulator
TPP	–	Trusted Third Party
UKSR	–	Unknown Key-Share Resilience

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

Cryptography plays an important role in this age of digital information and telecommunications, from applications used on a daily basis such as emails and Internet banking to highly sensitive military platforms. Cryptography enables secure communication over a public channel. That is, by sharing a secret among the communicating parties they would be able to communicate securely even in the presence of third parties such as adversaries. A cryptographic protocol that enables two or more entities to generate such a shared secret cooperatively over an open channel, named Key Agreement (KA) protocol [1, 2]. In general, KA protocol does nothing about authentication which makes it prone to impersonation and thus man-in-the-middle attack.

"A key agreement protocol which provides implicit key authentication to both participating entities is called an *authenticated key agreement (AKA)* protocol" [3].

AKA protocols are one of the fundamental cryptographic primitives due to the importance of the security of the shared secret in an open channel. It is worth to note that in an AKA protocol, two parties are not sharing information during the key agreement but they generate a shared key together. The focus of this research is on two-party AKA protocols in the context of Certificateless Public Key Cryptography (CL-PKC).

To avoid complex management of Public Key Infrastructure (PKI), Identity-based PKC (ID-PKC) was introduced by Shamir in 1984. That is, to generate the public keys from users' identifiers (e.g. email, photo, name). Afterwards, the users can obtain the corresponding private key by referring to a Private Key Generator (PKG), who is a Trusted Third Party (TTP). Although this simplifies key management, it has key escrow problem; access to all users' private keys by PKG. To overcome the mentioned problem CL-PKC was introduced by Al-Riyami and Paterson in 2003. CL-PKC is a combination of PKI based PKC and ID-PKC where the advantages of both are preserved. More precisely, CL-PKC avoids the key escrow problem of ID-PKC and the complex certificate management of the traditional PKC.

After the entrance of bilinear pairings to make ID-PKC applicable, many ID-PKC and CL-PKC protocols based on pairing maps have been proposed including Certificateless AKA (CL-AKA) protocols. However, the complexity of pairing operations, made these protocols computationally expensive. That is, to achieve the same security level, the operation time of computing bilinear pairing is much longer in compare with computing scalar multiplication over elliptic curves [4–7]. To address this issue several pairing-free CL-AKA protocols have been proposed. However, designing a pairing-free CL-AKA protocol with a balanced security and performance is still challenging.

This research proposes secure and computationally lightweight pairing-free AKA protocol in the context of certificateless PKC.

1.2 Problem Background

A traditional public key cryptosystem relies on digital certificates provided by a trusted party named Certification Authority (CA) to ensure that the issued public keys are authenticated [8, 9]. However, the need to the authenticated CAs makes the management of PKI complex [10, 11]. Thus, to eliminate the need to public key certificates, Shamir in [12] introduced a powerful theory named Identity-based cryptography; replacing the users' public key with their identity. Joux [13] beside of Boneh and Franklin [14] played a significant role in opening a window to a large variety of applicable cryptographic protocols in the area of ID-PKC (including identity-based key agreements). An impressive tool in making ID-PKC applicable was a cryptographic map named bilinear pairing [15–18]. Bilinear pairing is a cryptographic function, which maps two elements of elliptic curve based algebraic groups to an element of a determined finite field [15]. Pioneered by the proposed three-party key agreement scheme by Joux [13] as the first pairing-based key agreement scheme, Sakai *et al.* in [19] proposed the first identity-based key construction protocol by the use of bilinear pairings. Boneh and Franklin in [14] proposed a fully functional pairing-based encryption protocol as the first formally secure ID-PKC. Later, many ID-PKC protocols based on bilinear pairings were proposed in different primitives such as encryption [20–24], digital signature [25,26], authentication [27,28], and key agreement [29–34].

In an ID-PKC scheme, the users' private keys are generated by Private Key Generator (PKG). This makes PKG able to compromise individuals and confidential channels [35]. This inherent problem of ID-PKC is named "Key Escrow". To avoid this drawback of identity-based cryptosystems, several research have been done [36–39].

Al-Riyami and Paterson in [9] proposed a novel cryptosystem named Certificateless Public Key Cryptography (CL-PKC) to overcome key escrow problem. In a CL-PKC there is a trusted third party named Key Generation Center (KGC) who is responsible to generate users' partial private key. That is, using the partial private key, each entity is able to generate its private key.

The use of bilinear pairings became attractive in designing various formally secure ID-PKC and CL-PKC protocols including key agreement ones. Similar to the role of the ID-PKC scheme of Boneh and Franklin [14], which had a significant effect on proposing a large variety of ID-AKA protocols [40–44], introducing the idea of CL-PKC by Al-Riyami and Paterson led to proposing a large variety of Certificateless Authenticated Key Agreement protocols (CL-AKA) using bilinear pairings [45–51].

Bilinear pairing is expensive from computational complexity viewpoint [4–7]. Thus, to make the pairing-based cryptosystems applicable in resource-constrained devices some works studied lightweight design or efficient implementation of this cryptographic map [52–58]. In the context of ID-AKA and CL-AKA protocols, various researchers designed protocols based on the other lightweight cryptographic operations instead of expensive bilinear pairings. Computation of bilinear pairings is much more time-consuming than ECC based scalar multiplication [4]. Hence, a large proportion of the recently proposed ID-PKC and CL-PKC authenticated key agreement protocols are pairing-free and utilize ECC-based group operations [4, 59–65].

However, even in the area of pairing-free AKA protocol it is still challenging to have a computationally efficient protocol while maintaining the balanced security. Section 1.2.1 briefly reviews the state-of-the-art of CL-AKA protocols and then Section 1.2.2 presents the challenges in the current CL-AKA protocols.

1.2.1 Narrative review of CL-AKA protocols

AKA protocols can be presented in traditional PKC, ID-PKC, and CL-PKC settings. Among these settings CL-PKC is more appealing as it does not suffer from complex certificate management of PKI-based PKC and key escrow problem of ID-PKC. Pioneered by the first CL-PKC of Alriyami and Paterson [9], various CL-AKA protocols have been proposed that were relied on bilinear pairings. However, pairing-based cryptosystems are hard to be implemented especially in low power devices due to high operation time. More precisely, the computation time of pairing operation is much longer than an ECC-based scalar multiplication [4–7]. Therefore, many CL-AKA protocols have been proposed that utilize ECC-based operations instead of pairings [51, 60–62, 66–68].

According to the strength level of security (which is determined by the number of attacks and adversarial models covered in a security model) from low to high, the security models for AKA protocols are BR (Bellare and Rogaway [69]), mBR (modified BR [70]), CK (Canetti and Krawczyk [71]), and eCK (extended CK [72]).

In 2009, Hou and Xu in [51] proposed a pairing-free CL-AKA protocol which was not provably secure. In the same year, Geng et al. [67] presented a pairing-free CL-AKA protocol with the security proof in mBR model. Later, in 2011 Yang and Tan [66] found security flaws in Geng's proof and thus they proposed a secure pairing-free CL-AKA protocol. However, as shown by He et al. in [62] Yang's protocol is not computationally efficient. Hence, He et al. in [62] proposed an efficient pairing-free CL-AKA protocol which later shown by He et al. in [60] to be vulnerable against type-1 adversary. To avoid such vulnerability He et al. [60] presented a CL-AKA protocol without bilinear pairings. Although He's protocol [60] has the same performance as the He's protocol in [62], it is proven under a very weak security model; mBR [61]. He et al. in [61] tried to present a pairing-free CL-AKA protocol that can perform as efficient as the previous works while providing security in a strong security model; eCK. Sun et al. in [64] found several security flaws in the security proof of He's protocol [61] and presented a concrete attack to prove that He's protocol is not secure in eCK model. Sun et al. proposed an enhanced version of He's protocol to be secure in eCK model. However, as indicated in [64] their proposed protocol is computationally more complex than He's protocol [61], thus they failed to maintain the same level of efficiency. As a result, proposing a lightweight pairing-free CL-AKA protocol (from computational complexity viewpoint) which is secure in eCK model remained as an open challenge.

1.2.2 Issues and challenges in pairing-free CL-AKA protocols

This section introduces the issues and challenges in pairing-free CL-AKA protocols from security and efficiency viewpoints. As mentioned earlier, the main motivation for moving from pairing-based cryptosystems to the pairing-free ones is to reduce the computational complexity. However, it should be noted that utilizing many ECC-based group operations may also result in inefficiency and hence making the protocols hard to be implemented in practice. As stressed by Blake et al. in [73], four performance attributes must be considered in an AKA protocol which are

1. Minimal number of passes (the number of messages exchanged).
2. Low communication overhead (total number of bits transmitted).
3. Low computation overhead (total number of arithmetical operations required).
4. Possibility of precomputation (to minimize on-line computational overhead).

Most of the current related works have similar communication overhead. Thus, it is important to minimize the computational complexity. Each agreed shared session secret contains several group operations, hence the smaller number of utilized group operations can lead to the lower computational cost. However, supporting all of the AKA security requirements and provable security simultaneously, with minimum agreed shared session secret is challenging. Using less complex group operation is another way to decrease the computational cost. It can be done by utilizing lighter ECC-based operations such as modular multiplication and point addition instead of heavier ones like scalar multiplication can result in the lower computational complexity. That is, the computational complexity of one scalar multiplication is 29 times more than a modular multiplication and the computational complexity of point addition in compare with scalar multiplication is negligible. Another possible approach is to pre-compute some of the values. That is, in the design of the protocol some combination of the values can be reused after the first computation without the need to recompute them. However, it is challenging to provide all of the above mentioned performance considerations while maintaining security at the high level. For instance, He et al. [61] could improve the efficiency of Yang's protocol [66] by nearly fifty percent (from 8 scalar multiplications and 2 point additions to 4 scalar multiplications and 2 point additions). But they failed to provide a secure scheme as their scheme is vulnerable against both adversary type-1 and type-2 [64].

On the other hand, provable security is known to be as good as a practical analysis technique as exists [74]. Provable security is a paradigm that ensures the security of a scheme via a *reduction* to a mathematical hard problem. The reduction shows that the only way to defeat the protocol is to break the considered mathematical hard problem [75]. Moreover, as stated by Blake et al. [73]:

> *"There are two primary drawbacks of protocols which provide heuristic security. First, their security attributes are typically unclear or not completely specified. Second, they offer no assurances that new attacks will not be discovered in the future. These drawbacks make a notion of provable security desirable".*

Although provable security may appear to be the highest possible level of security for a key agreement protocol, it has some limitations [73]. Therefore, it is not a surprise that provable security evaluation method might not cover all of the AKA security requirements. For instance, [66] provided the security proof in a very strong model, eCK, however Zhang et al. in [76] showed that this protocol does not support "key compromise impersonation" security requirement. Similarly, Bala et al. in [77] indicated that the proposed provably secure CL-AKA protocol by Kim et al. [78] is vulnerable against key compromise impersonation attack. Thus, in order to ensure about the security of an AKA protocol by a comprehensive security, both provable security and the support of AKA protocols' security requirements are essential. The following statement from [75] clarify this issue.

> *"Practitioners typically think only about concrete attacks; theoreticians ignore them, since they prove the security. Under the practice oriented provable security approach, attacks and security emerge as opposite sides of the same coin, and complement each other. Attacks measure the degree of insecurity; our quantitative bounds measure the degree of security. When the two meet, we have completely characterized the security of the protocol".*

1.3 Problem statement

Heavy computational complexity is a hindrance in many cryptographic protocols towards their practical applications. This holds true also in the context of AKA protocols, where cryptographic protocols are used to fulfill multiple security requirements. The complexity of pairing operations, made pairing-based certificateless AKA protocols computationally expensive. Thus, it is not a surprise that a number of pairing-free CL-AKA protocols over elliptic curves have been proposed. However, a pairing-free CL-AKA protocol with a balanced security and efficiency is still desirable.

1.4 Research questions

The problem statements of this research are supported by the following questions:

i How to design a secure two-party certificateless authenticated key agreement protocol with minimal computational complexity?

ii How to evaluate the performance of the proposed protocol?

iii How to validate the security of the proposed protocol in accordance to the security requirements of authenticated key agreement protocols?

iv How to prove the security of the proposed protocol formally based on a strong security model?

1.5 Research aim

The output of this research is an efficient two-party pairing-free certificateless authenticated key agreement protocol over elliptic curves. That is, the proposed protocol has the minimal computational complexity while its communication overhead remained the same as the existing related works. According to what mentioned in section 1.2.2, to mitigate possible attacks against CL-AKA protocols, it must be validated that the proposed protocol supports the security requirements of AKA protocols. Moreover, to ensure that the proposed CL-AKA protocol is formally secure in the simulated attack environment which is similar to real world condition, the security is proven under a strong security model; the extended Canetti-Krawczyk (eCK) model.

1.6 Research Objectives

The objectives of this research are as follows;

i To design a minimal computationally complex and secure two-party certificateless authenticated key agreement protocol.

ii To evaluate the performance of the proposed protocol in terms of computational complexity.

iii To evaluate security of the proposed protocol in accordance to the security requirements of AKA protocols and provable security based on the extended Canetti-Krawczyk (eCK) model.

1.7 Research Scope

The scope of this research is defined as follows:

1. This research emphasizes on two-party key agreement protocols.
2. AKA protocols are considered under public key cryptography.
3. The scope of this research, emphasizes on certificateless key agreement protocols which are implicitly authenticated.
4. The communication channel is assumed to be open and accessible by the adversary.
5. Investigation of an AKA protocol limits to cryptographic function part of the protocol from both design and security analysis viewpoint.
6. To investigate existing cryptographic functions, this research considers pairing-free protocols over elliptic curves.

1.8 The significance of study

Nowadays, widely usage of collaborative and distributed applications made the security and cryptography as one of the major concerns of scientific research. However, the trade-off between security and efficiency is always challenging. Key agreement is remained as one of the hot topics of cryptography for many years. The reason is deducible; security of a cryptographic scheme is dependent on the secrecy of the used keys rather than the secrecy of used cryptographic algorithms or protocols. The importance of key agreement is more observed in selection between the use of

Symmetric or Public Key Cryptography (PKC), especially over encryption schemes [79, 80].

To keep the transferred messages in an open channel confidential, the use of symmetric encryption generally has significant advantages in compare with PKC from performance perspective due to the inherent use of more lightweight cryptographic operations. However, the use of pure symmetric cryptographic schemes, inherently imposes challenges in management and distribution of the shared keys [79]. Confidential distribution of the pre-shared keys between each pair of entities before the entrance to an environment can be a possible solution to make the communications secure. However, this solution limits the scalability of the environment. In addition, it can lead to increase the complexity of management of the shared keys, especially by the growth of the number of communicating participants [80]. For instance, if n participants are in the system each user has to manage and maintain $n(n-1)/2$ shared keys securely [80]. Therefore, symmetric cryptographic protocols are more efficient than PKC, however the simpler organization and management of PKC cannot be ignored [80].

Key agreement protocols follow a hybrid setting by their nature. That is, existing entities rely on their own long-term public/private keys, hence the key management is less complex than symmetric cryptosystems. On the other hand, when the communicating participants generate the short-term session key they can perform more efficient symmetric cryptographic protocols temporary during the life cycle of the session key. Among the different types of AKA protocols, certificateless pairing-free AKA protocols are more appealing in practice due to their efficiency and avoiding key escrow problem of ID-PKC. This research presents a computationally lightweight two-party CL-AKA protocol in the context of elliptic curve cryptography.

1.9 Thesis organization

This research consists of six chapters.

Chapter One: This chapter provides a quick view over the considered problem in this research. To reach this goal, this chapter talks about the background of the research, problem statements, research questions, research aim, research objectives, research scopes, significance of study and the organization of the research.

Chapter Two: This chapter gives some information about preliminary topics such as bilinear pairings, elliptic curves, key management and various aspects of security models. Then, the existing AKA protocols are investigated from security and computational complexity viewpoint.

Chapter Three: This chapter discusses the utilized methodologies in this research. Operational framework and Research framework are investigated in detail. For each phase of the research, several figures are provided to clarify the utilized research methodologies and how they help to fulfill the research objectives.

Chapter Four: This chapter presents the motivations, tools, techniques, and actions taken in the design of the proposed protocol. The design goal is to propose a CL-AKA protocol which achieves the high performance while the high level of security is guaranteed. The initial results are presented in the form of six computationally lightweight CL-AKA protocols. Then, the main result which is the proposed pairing-free two-party CL-AKA protocol, named CL2AKA is given. Moreover, this chapter provides discussions about the security and performance of CL2AKA protocol.

Chapter Five: In this chapter, a comprehensive discussion on the security and the performance of the considered pairing-free authenticated key agreement protocols is given. Moreover, this chapter provides a security proof based on the extended Canetti-Krawczyk (eCK) model in order to simulate attack environment the same as real world condition and prove that the proposed cryptographic protocol, CL2AKA, is formally secure.

Chapter Six: This chapter draws the summary of what has been presented and reached in this research. Moreover, the contributions of this research are reviewed and directions for future works are given.

REFERENCES

1. Dutta, R., Barua, R. and Sarkar, P. Pairing-Based Cryptographic Protocols: A Survey. *IACR Cryptology ePrint Archive*, 2004. 2004: 64.

2. Chen, L., Cheng, Z. and Smart, N. P. Identity-based key agreement protocols from pairings. *International Journal of Information Security*, 2007. 6(4): 213–241.

3. Law, L., Menezes, A., Qu, M., Solinas, J. and Vanstone, S. An efficient protocol for authenticated key agreement. *Designs, Codes and Cryptography*, 2003. 28(2): 119–134.

4. Cao, X., Kou, W. and Du, X. A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges. *Information Sciences*, 2010. 180(15): 2895–2903.

5. He, D., Chen, C., Chan, S. and Bu, J. Secure and efficient handover authentication based on bilinear pairing functions. *IEEE Transactions on Wireless Communications*, 2012. 11(1): 48–53.

6. Aranha, D. F., Faz-Hernández, A., López, J. and Rodríguez-Henríquez, F. Faster implementation of scalar multiplication on Koblitz curves. *International Conference on Cryptology and Information Security in Latin America*. Springer. 2012. 177–193.

7. Aranha, D. F., Karabina, K., Longa, P., Gebotys, C. H. and López, J. Faster explicit formulas for computing pairings over ordinary curves. *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2011. 48–68.

8. Baek, J., Safavi-Naini, R. and Susilo, W. Certificateless public key encryption without pairing. *International Conference on Information Security*. Springer. 2005. 134–148.

9. Al-Riyami, S. S. and Paterson, K. G. Certificateless public key cryptography. *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2003. 452–473.

10. Adams, C. and Lloyd, S. *Understanding public-key infrastructure: concepts,*

standards, and deployment considerations. Sams Publishing. 1999.

11. Gutmann, P. PKI: it's not dead, just resting. *Computer*, 2002. 35(8): 41–49.

12. Shamir, A. Identity-based cryptosystems and signature schemes. *Workshop on the theory and application of cryptographic techniques*. Springer. 1984. 47–53.

13. Joux, A. A one round protocol for tripartite Diffie–Hellman. *International algorithmic number theory symposium*. Springer. 2000. 385–393.

14. Boneh, D. and Franklin, M. Identity-based encryption from the Weil pairing. *Annual international cryptology conference*. Springer. 2001. 213–229.

15. Galbraith, S. D., Paterson, K. G. and Smart, N. P. Pairings for cryptographers. *Discrete Applied Mathematics*, 2008. 156(16): 3113–3121.

16. Miller, V. *et al.* Short programs for functions on curves. *Unpublished manuscript*, 1986. 97(101-102): 44.

17. Capco, J. Weil Pairings On Elliptic Curves. 2003.

18. Tate, J. Duality theorems in Galois cohomology over number fields. *Proc. Internat. Congr. Mathematicians (Stockholm, 1962)*. 1962. 288–295.

19. Sakai, R. Cryptosystems based on pairing. *Proc. of SCIS2000, Jan.*, 2000.

20. Boneh, D. and Franklin, M. Identity-based encryption from the Weil pairing. *SIAM journal on computing*, 2003. 32(3): 586–615.

21. Gentry, C. and Silverberg, A. Hierarchical ID-based cryptography. *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2002. 548–566.

22. Boneh, D. and Boyen, X. Efficient selective-ID secure identity-based encryption without random oracles. *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2004. 223–238.

23. Boneh, D., Raghunathan, A. and Segev, G. Function-private identity-based encryption: Hiding the function in functional encryption. In: *Advances in Cryptology–CRYPTO 2013*. Springer. 461–478. 2013.

24. Seo, J. H. and Emura, K. Revocable identity-based encryption revisited: Security model and construction. In: *Public-Key Cryptography–PKC 2013*. Springer. 216–234. 2013.

25. Hess, F. Efficient identity based signature schemes based on pairings. *International Workshop on Selected Areas in Cryptography*. Springer. 2002. 310–324.

26. Zhang, F. and Kim, K. ID-based blind signature and ring signature from pairings. *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2002. 533–547.

27. Li, H., Dai, Y., Tian, L. and Yang, H. Identity-based authentication for cloud computing. *IEEE International Conference on Cloud Computing*. Springer. 2009. 157–166.

28. Amin, R. and Biswas, G. Design and analysis of bilinear pairing based mutual authentication and key agreement protocol usable in multi-server environment. *Wireless Personal Communications*, 2015. 84(1): 439–462.

29. Chen, L. and Kudla, C. Identity based authenticated key agreement protocols from pairings. *Computer Security Foundations Workshop, 2003. Proceedings. 16th IEEE*. IEEE. 2003. 219–233.

30. Shim, K. Efficient ID-based authenticated key agreement protocol based on Weil pairing. *Electronics Letters*, 2003. 39(8): 653–654.

31. McCullagh, N. and Barreto, P. S. A new two-party identity-based authenticated key agreement. *Cryptographers Track at the RSA Conference*. Springer. 2005. 262–274.

32. Smart, N. P. Identity-based authenticated key agreement protocol based on Weil pairing. *Electronics letters*, 2002. 38(13): 630–632.

33. Wang, Y. Efficient Identity-Based and Authenticated Key Agreement Protocol.

34. Ni, L., Chen, G., Li, J. and Hao, Y. Strongly secure identity-based authenticated key agreement protocols in the escrow mode. *Science China Information Sciences*, 2013. 56(8): 1–14.

35. Paterson, K. G. and Price, G. A comparison between traditional public key infrastructures and identity-based cryptography. *Information Security Technical Report*, 2003. 8(3): 57–72.

36. Chow, S. S. Removing escrow from identity-based encryption. *International Workshop on Public Key Cryptography*. Springer. 2009. 256–276.

37. Cheng, Z., Comley, R. and Vasiu, L. Remove key escrow from the identity-based encryption system. In: *Exploring New Frontiers of Theoretical Informatics*. Springer. 37–50. 2004.

38. Oh, J., Lee, K. and Moon, S. How to solve key escrow and identity revocation in identity-based encryption schemes. *International Conference on Information Systems Security*. Springer. 2005. 290–303.

39. Yuen, T. H., Susilo, W. and Mu, Y. How to construct identity-based signatures without the key escrow problem. *International Journal of Information Security*, 2010. 9(4): 297–311.

40. Yuan, Q. and Li, S. A New Efficient ID-Based Authenticated Key Agreement Protocol. *IACR Cryptology ePrint Archive*, 2005. 2005: 309.

41. Choie, Y. J., Jeong, E. and Lee, E. Efficient identity-based authenticated key agreement protocol from pairings. *Applied Mathematics and Computation*, 2005. 162(1): 179–188.

42. Ryu, E.-K., Yoon, E.-J. and Yoo, K.-Y. An efficient ID-based authenticated key agreement protocol from pairings. *International conference on research in networking*. Springer. 2004. 1458–1463.

43. Scott, M. Authenticated ID-based Key Exchange and remote log-in with simple token and PIN number. *IACR Cryptology ePrint Archive*, 2002. 2002: 164.

44. Wang, Y. Efficient identity-based and authenticated key agreement protocol. In: *Transactions on Computational Science Xvii*. Springer. 172–197. 2013.

45. Zhang, L. Certificateless one-pass and two-party authenticated key agreement protocol and its extensions. *Information Sciences*, 2015. 293: 182–195.

46. Lu, Y., Zhang, Q., Li, J. and Shen, J. Comment on a certificateless one-pass and two-party authenticated key agreement protocol. *Information Sciences*, 2016. 369: 184–187.

47. Wang, S., Cao, Z. and Dong, X. Certificateless authenticated key agreement based on the MTI/CO protocol. *Journal of Information and computational science*, 2006. 3(3): 575–581.

48. Mandt, T. K. and Tan, C. H. Certificateless authenticated two-party key agreement protocols. *Annual Asian Computing Science Conference*. Springer. 2006. 37–44.

49. Shi, Y. and Li, J. Two-party authenticated key agreement in certificateless public key cryptography. *Wuhan University Journal of Natural Sciences*, 2007. 12(1): 71–74.

50. Lippold, G., Boyd, C. and Nieto, J. G. Strongly secure certificateless key agreement. *International Conference on Pairing-Based Cryptography*. Springer. 2009. 206–230.

51. Hou, M. and Xu, Q. A two-party certificateless authenticated key agreement protocol without pairing. 2009.

52. Oliveira, L. B., Aranha, D. F., Gouvêa, C. P., Scott, M., Câmara, D. F., López, J. and Dahab, R. TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks. *Computer communications*, 2011. 34(3): 485–493.

53. Shirase, M., Miyazaki, Y., Takagi, T., Han, D.-G. and Choi, D. Efficient implementation of pairing-based cryptography on a sensor node. *IEICE transactions on information and systems*, 2009. 92(5): 909–917.

54. Xiong, X., Wong, D. S. and Deng, X. TinyPairing: computing tate pairing on sensor nodes with higher speed and less memory. *Network Computing and Applications, 2009. NCA 2009. Eighth IEEE International Symposium on*. IEEE. 2009. 187–194.

55. Barreto, P. S., Kim, H. Y., Lynn, B. and Scott, M. Efficient algorithms for pairing-based cryptosystems. *Annual international cryptology conference*. Springer. 2002. 354–369.

56. Ramachandran, A., Zhou, Z. and Huang, D. Computing cryptographic algorithms in portable and embedded devices. *Portable Information Devices, 2007. PORTABLE07. IEEE International Conference on*. IEEE. 2007. 1–7.

57. Bertoni, G., Chen, L., Fragneto, P., Harrison, K. and Pelosi, G. Computing tate pairing on smartcards. *White Paper STMicroelectronics*, 2005.

58. Zhou, Z. and Huang, D. Computing cryptographic pairing in sensors. *ACM SIGBED Review*, 2008. 5(1): 27.

59. Cao, X., Kou, W., Yu, Y. and Sun, R. Identity-based authenticated key agreement protocols without bilinear pairings. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 2008. 91(12): 3833–3836.

60. He, D., Chen, Y., Chen, J., Zhang, R. and Han, W. A new two-round certificateless authenticated key agreement protocol without bilinear pairings. *Mathematical and Computer Modelling*, 2011. 54(11-12): 3143–3152.

61. He, D., Padhye, S. and Chen, J. An efficient certificateless two-party authenticated key agreement protocol. *Computers & Mathematics with Applications*, 2012. 64(6): 1914–1926.

62. He, D., Chen, J. and Hu, J. A pairing-free certificateless authenticated key agreement protocol. *International Journal of Communication Systems*, 2012. 25(2): 221–230.

63. Islam, S. H. and Biswas, G. An improved pairing-free identity-based

authenticated key agreement protocol based on ECC. *Procedia Engineering*, 2012. 30: 499–507.

64. Sun, H., Wen, Q., Zhang, H. and Jin, Z. A novel pairing-free certificateless authenticated key agreement protocol with provable security. *Frontiers of Computer Science*, 2013. 7(4): 544–557.

65. Farash, M. S. and Ahmadian-Attari, M. A Pairing-free ID-based Key Agreement Protocol with Different PKGs. *IJ Network Security*, 2014. 16(2): 143–148.

66. Yang, G. and Tan, C.-H. Strongly secure certificateless key exchange without pairing. *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*. ACM. 2011. 71–79.

67. Geng, M. and Zhang, F. Provably secure certificateless two-party authenticated key agreement protocol without pairing. *Computational Intelligence and Security, 2009. CIS'09. International Conference on*. IEEE. 2009, vol. 2. 208–212.

68. Xiong, H., Wu, Q. and Chen, Z. Toward pairing-free certificateless authenticated key exchanges. *International Conference on Information Security*. Springer. 2011. 79–94.

69. Bellare, M. and Rogaway, P. Entity authentication and key distribution. *Annual international cryptology conference*. Springer. 1993. 232–249.

70. Kudla, C. and Paterson, K. G. Modular security proofs for key agreement protocols. *International conference on the theory and application of cryptology and information security*. Springer. 2005. 549–565.

71. Canetti, R. and Krawczyk, H. Analysis of key-exchange protocols and their use for building secure channels. *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2001. 453–474.

72. LaMacchia, B., Lauter, K. and Mityagin, A. Stronger security of authenticated key exchange. *International conference on provable security*. Springer. 2007. 1–16.

73. Blake-Wilson, S. and Menezes, A. Authenticated Diffe-Hellman key agreement protocols. *International Workshop on Selected Areas in Cryptography*. Springer. 1998. 339–361.

74. Menezes, A. J., van Oorschot, P. C. and Vanstone, S. A. Handbook of applied cryptography, 1997.

75. Bellare, M. Practice-oriented provable-security. *International Workshop on*

Information Security. Springer. 1997. 221–231.

76. Zhang, M., Zhang, J., Wen, Q.-Y., Jin, Z.-P. and Zhang, H. Analysis and improvement of a strongly secure certificateless key exchange protocol without pairing. *Systems and Informatics (ICSAI), 2012 International Conference on*. IEEE. 2012. 1512–1516.

77. Bala, S., Sharma, G. and Verma, A. K. Impersonation attack on CertificateLess key agreement protocol. *International Journal of Ad Hoc and Ubiquitous Computing*, 2018. 27(2): 108–120.

78. Kim, Y.-J., Kim, Y.-M., Choe, Y.-J. *et al.* An efficient bilinear pairing-free certificateless two-party authenticated key agreement protocol in the eCK model. *arXiv preprint arXiv:1304.0383*, 2013.

79. Buchmann, J. *Introduction to cryptography*. Springer Science & Business Media. 2013.

80. William, S. Cryptography and network security: principles and practice. *Prentice-Hall, Inc*, 1999: 23–50.

81. Schneier, B. Applied Cryptography, 1996 John Wiley & Sons. *Inc, USA*.

82. Hankerson, D., Menezes, A. J. and Vanstone, S. *Guide to elliptic curve cryptography*. Springer Science & Business Media. 2006.

83. NIST Recommendation for Key Management Part 1, 2005. URL `http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=36F335B4824C134E0D17BAD9F2A851C8doi=10.1.1.106.307&rep=rep1&type=pdf`.

84. ECRYPT Yearly Report on Algorithms and Keysizes (2004), 2004. URL `http://www.ecrypt.eu.org/ecrypt1/documents/D.SPA.10-1.1.pdf`.

85. Du, X., Xiao, Y., Guizani, M. and Chen, H.-H. An effective key management scheme for heterogeneous sensor networks. *Ad Hoc Networks*, 2007. 5(1): 24–34.

86. Younis, M. F., Ghumman, K. and Eltoweissy, M. Location-aware combinatorial key management scheme for clustered sensor networks. *IEEE transactions on parallel and distributed systems*, 2006. 17(8): 865–882.

87. Zhou, J., Cao, Z., Dong, X., Xiong, N. and Vasilakos, A. V. 4S: A secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks. *Information Sciences*, 2015. 314: 255–276.

88. Boloorchi, A. T., Samadzadeh, M. and Chen, T. Symmetric Threshold Multipath (STM): An online symmetric key management scheme. *Information Sciences*, 2014. 268: 489–504.

89. Anita, E. M., Geetha, R. and Kannan, E. A novel hybrid key management scheme for establishing secure communication in wireless sensor networks. *Wireless Personal Communications*, 2015. 82(3): 1419–1433.

90. Saied, Y. B., Olivereau, A., Zeghlache, D. and Laurent, M. Lightweight collaborative key establishment scheme for the Internet of Things. *Computer Networks*, 2014. 64: 273–295.

91. Liu, D., Ning, P. and Li, R. Establishing pairwise keys in distributed sensor networks. *ACM Transactions on Information and System Security (TISSEC)*, 2005. 8(1): 41–77.

92. Du, W., Deng, J., Han, Y. S., Varshney, P. K., Katz, J. and Khalili, A. A pairwise key predistribution scheme for wireless sensor networks. *ACM Transactions on Information and System Security (TISSEC)*, 2005. 8(2): 228–258.

93. Zhu, S., Xu, S., Setia, S. and Jajodia, S. Establishing pairwise keys for secure communication in ad hoc networks: A probabilistic approach. *Network Protocols, 2003. Proceedings. 11th IEEE International Conference on*. IEEE. 2003. 326–335.

94. Zhou, L., Ni, J. and Ravishankar, C. V. Efficient key establishment for group-based wireless sensor deployments. *Proceedings of the 4th ACM workshop on Wireless security*. ACM. 2005. 1–10.

95. Das, A. K. and Sengupta, I. An effective group-based key establishment scheme for large-scale wireless sensor networks using bivariate polynomials. *Communication Systems Software and Middleware and Workshops, 2008. COMSWARE 2008. 3rd International Conference on*. IEEE. 2008. 9–16.

96. Bao, F., Deng, R. H. and Zhu, H. Variations of diffie-hellman problem. *International conference on information and communications security*. Springer. 2003. 301–312.

97. Bellare, M., Desai, A., Pointcheval, D. and Rogaway, P. Relations among notions of security for public-key encryption schemes. *Annual International Cryptology Conference*. Springer. 1998. 26–45.

98. Feige, U., Fiat, A. and Shamir, A. Zero-knowledge proofs of identity. *Journal of cryptology*, 1988. 1(2): 77–94.

99. Bellare, M. and Rogaway, P. Random oracles are practical: A paradigm for designing efficient protocols. *Proceedings of the 1st ACM conference on Computer and communications security*. ACM. 1993. 62–73.

100. Blake-Wilson, S., Johnson, D. and Menezes, A. Key agreement protocols and their security analysis. *IMA international conference on cryptography and coding*. Springer. 1997. 30–45.

101. Cheng, Z., Nistazakis, M., Comley, R. and Vasiu, L. On The Indistinguishability-Based Security Model of Key Agreement Protocols-Simple Cases. *IACR Cryptology ePrint Archive*, 2005. 2005: 129.

102. Bellare, M. and Rogaway, P. Entity Authentication and Key Distribution. *Lecture Notes in Computer Science*, 1994. 773: 0232–0232.

103. Huang, H. and Cao, Z. Strongly Secure Authenticated Key Exchange Protocol Based on Computational Diffie-Hellman Problem. *IACR Cryptology ePrint Archive*, 2008. 2008: 500.

104. Yang, Z. Efficient eck-secure authenticated key exchange protocols in the standard model. *International Conference on Information and Communications Security*. Springer. 2013. 185–193.

105. Li, S., Yuan, Q. and Li, J. Towards Security Two-part Authenticated Key Agreement Protocols. *IACR Cryptology ePrint Archive*, 2005. 2005: 300.

106. Cremers, C. J. Formally and Practically Relating the CK, CK-HMQV, and eCK Security Models for Authenticated Key Exchange. *IACR Cryptology ePrint Archive*, 2009. 2009: 253.

107. Fujioka, A., Suzuki, K. and Yoneyama, K. Strongly secure predicate-based authenticated key exchange: Definition and constructions. *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*, 2012. 95(1): 40–56.

108. Zhang, F., Safavi-Naini, R. and Susilo, W. An efficient signature scheme from bilinear pairings and its applications. *International Workshop on Public Key Cryptography*. Springer. 2004. 277–290.

109. Fiore, D. and Gennaro, R. Identity-based key exchange protocols without pairings. In: *Transactions on computational science X*. Springer. 42–77. 2010.

110. Islam, S. H. and Biswas, G. A pairing-free identity-based authenticated group key agreement protocol for imbalanced mobile networks. *Annals of télécommunications-annales des telecommunications*, 2012. 67(11-12): 547–558.

111. Islam, S. H. and Biswas, G. Design of two-party authenticated key agreement protocol based on ECC and self-certified public keys. *Wireless Personal Communications*, 2015. 82(4): 2727–2750.

112. Koblitz, N., Menezes, A. and Vanstone, S. The state of elliptic curve cryptography. *Designs, codes and cryptography*, 2000. 19(2-3): 173–193.

113. Joux, A. and Nguyen, K. Separating decision Diffie–Hellman from computational Diffie–Hellman in cryptographic groups. *Journal of cryptology*, 2003. 16(4): 239–247.

114. Niven, I. *Maxima and minima without calculus*. 6. Cambridge University Press. 1981.

115. Diffie, W. and Hellman, M. New directions in cryptography. *IEEE transactions on Information Theory*, 1976. 22(6): 644–654.