International Journal of Mechanical Engineering and Applications
2017; 5(4): 194-202
http://www.sciencepublishinggroup.com/j/ijmea
doi: 10.11648/j.ijmea.20170504.12
ISSN: 2330-023X (Print); ISSN: 2330-0248 (Online)

Leakage-Resilient Certificateless Short Signature Scheme

Chen Xiaokui

School of Mathematics and Big Data, An Hui University of Science & Technology, Huai Nan City, China

Email address:
xiaokuichen@126.com

To cite this article:
Chen Xiaokui. Leakage-Resilient Certificateless Short Signature Scheme. *International Journal of Mechanical Engineering and Applications*. Vol. 5, No. 4, 2017, pp. 194-202. doi: 10.11648/j.ijmea.20170504.12

Received: March 22, 2017; **Accepted**: May 10, 2017; **Published**: July 6, 2017

Abstract: For a certificateless short signature scheme to be applied in practical applications, it should without various leakage attacks. In this paper, we present a new leakage-resilient certificateless short signature scheme whose security is based on the classical decisional Diffie-Hellman (DDH) assumption. Our scheme is leakage-resilient signature scheme, and leaked information is a maximum value (upper bound). What is more, our scheme also enjoys a higher relative leaked information rate and still semantically secure against adaptive chosen message attack. Besides these good performance features, we have formally proved the security of our scheme in the random oracle model under the hardness of the DDH problem. With these import features, our proposal may have some significant value in the practical applications. Compared to existing schemes, our new scheme has two advantages: (1) Our scheme is leakage-resilient certificateless short signature scheme; (2) Our Scheme is leakage-resilient signature scheme, and leaked information is a maximum value (upper bound).

Keywords: Leakage Resilient, DDH Problem, Certificateless Short Signature Scheme

1. Introduction

Digital signatures, one of the most important components of cryptography, are the basic theory for protecting the integrity and authenticity of information. The digital signature is benefit from the development of the public key cryptography. The security of these schemes is based on factorization and discrete logarithms. It can provide many applications with all kinds of security service, such as authentication, confidentiality, information integrity and non-repudiation of transaction. The signature scheme has played an important role in the electronic commerce, electronic vote etc.

Digital signature is one of the important tools in information integrity and identity authentication. By the way of encryption, message authentication, the digital signature can defense the attacks and achieves security. On the one hand, digital signatures are used to verify that the message was actually sent by the sender. This includes identification and authentication, authorization, access control, and encryption. On the other hand, the signature information use in the process in the memory which and transmits, all has the possibility to interrupt, the interception, tampers with and fabricates. Therefore, digital signatures are very important means to guarantee authenticity of information.

In 1976, Diffie and Hellman [1] based on the ideas of public key cryptography, a digital signature is given. In the literature [1], although Diffie and Hellman proposed the digital signature, it is based on the public key cryptosystem. But they did not give the specific digital signature scheme. In 1978, the first digital signature scheme by Rivest, Shamir and Adleman is proposed [2]. The security is based on factoring representation problem. Then, early digital signature scheme is also proposed by Lamport [3], Merkle [4] and Rabin [5].

After the yearly development, Scholars have offered various efficient and secure digital signature schemes. Among them, there is a classic has based on elliptic curve discrete logarithm problem. Such as: ElGamal [6] digital signature scheme, Schnorr [7] digital signature scheme, DSA [8] digital signature scheme, Okamoto [9] digital signature scheme, Fiat-Shamir [10] signature scheme, and Nyberg-Ruppel [11] signature scheme, etc.

Then, Miller [12] and Koblitz [13] respectively independently establish the elliptic curve cryptosystem (ECC). Elliptic curve cryptosystem is a hot topic in public key cryptosystems. The security of the elliptic curve cryptography is built upon the difficulty of solving the elliptic curve discrete logarithm problem. Actually, Elliptic Curve Digital Signature is a simulation of the digital signature on the elliptic curve under this cryptosystem. Public Key Cryptosystems based on

the Elliptic Curve theory are divided into two types: elliptic curve digital signature and Hyperelliptic curve digital signature. Many previous signature algorithm based on discrete logarithm can be translated to elliptic curve cryptosystem. Such as, one of the most famous algorithm ECDSA signature schemes [14], that efficiency is superior to DSA signature scheme.

At present, public key cryptography system is based on public key cryptography infrastructure (PKI). PKI is a set of services that make use of public key cryptography to meet the needs of data confidentiality, integrity and non-repudiation function. However, with the extensive application of PKI, it reliability, security have been an obvious problem. Such as, in PKI system, people have to spend a lot of time and energy for certificate issuing and management work, especially management certificate authority (CA).

In order to simplify the traditional PKI system cost a lot of time in the transmission and validating the user public key certificate, Shamir [15] proposed the identity-based cryptography (IBC) by 1984. Soon, a large number of schemes [16-19] of identity-based signature are proposed based on identity-based cryptography. But these schemes are inefficient, thus cause to be not practical. Until 2000, Joux [20] proposed an identity-based of Diffie-Hellman key agreement protocol, using the characteristics of bilinear pairings on a super-elliptic curve. Bilinear pairings construct identity-based signature scheme [21-24] to become mainstream.

Since the appearance of identity-based signature scheme, much attention has been paid to identity-based public key cryptosystems to decrease the cost of certificates management. But it requires a trusted private key generator (PKG). PKG generate the private key of all users. However, there are some problems in identity-based signature scheme such as key escrow. Because PKG know the user's private key, a dishonest PKG can forge a warrant signature and proxy signing key, then the PKG can successfully counterfeit original signer, and make the proxy signer to sign message for him, and know how to decryption ciphertext by a certain user. Once the PKG security problems, the entire identity-based public key cryptosystems will be paralyzed. It will give business, society and even the whole country a huge economic loss. Therefore, solve the key escrow problem is urgent problems.

Threshold cryptography provides in which the secret key generation method [25-27]. It can resolve the key escrow problem. But none of the solutions was entirely satisfactory. In 2003, Al-Riyami and Paterson [28] has proposed a new cryptosystem ---- certificateless PKG, CLPKG). Similar to the identity-based cryptography, CLPKC also need a master key of Key Generation Center (KGC). In the certificateless public key cryptography, the user's private key is jointly produced by the user and KGC. Certificateless signature scheme solve the certificate management in traditional public key cryptography, and the key escrow in identity-based public key cryptography. Since CLPKG is invented, the research of CLPKG has been become one of the hotspots. Now, many CLPKG schemes had been provided [29-31].

A certificateless signature scheme is CLPKG's important cryptology primitive. The earliest certificateless signature scheme is given by scholars Al-Riyami and Paterson [28]. It consists of seven algorithms. It includes Setup, Extract-Partial-Private-key, Set-Secret-Value, Set-Private-Key, Set-Public-Key, Certificateless-Sign, and Certificateless-Verify. Then, Hu [32] also proposed certificateless signature scheme. It consists of five algorithms. It includes Setup, Extract-Partial-Private-key, Set-Private-Key, Certificateless-Sign, and Certificateless-Verify. In essence, Hu's scheme and Al-Riyami, Paterson is equivalent.

So it becomes a key problem how to build a better security protection scheme and key management system by making use of the cryptography algorithm in practice. Because of the large amount of calculation for pairing, a leakage resilient certificateless short signature scheme without pairing was proposed, which combined the new certificateless public key cryptosystem. In the new scheme, the digital signature can't be denied or forged, and the secret key update algorithm is fast, and the sizes of key and signature are small.

1.1. Our Motivation

In this paper, we mainly focus on constructing more efficient leakage resilient certificateless short signature scheme with a higher information leakage ration. As is known to all, both the leakage information length is significant elements that affect applications of signature scheme. When leakage-resilient attacks are taken into consideration, the relative information leakage ration is also an important concern in real applications. Hence, it is interesting and challenging to design leakage-resilient certificateless short signature scheme which enjoy a low computational cost, a short key length, as well as a high relative information leakage ratio.

1.2. Our Contribution

We pay close attention to leakage-resilient certificateless short signature scheme in this paper. To reach our goal, we simplify some parameters in our scheme which is based on random oracle model under the hardness of the DDH problem. The certificateless short signature is a special digital signature. Certificateless short signature scheme solves the certificate management in the tradition public key cryptography, and the key escrow in the identity-based public key cryptography. So, it is widely used in the certificateless short signature scheme.

As a result, we get a leakage-resilient certificateless short signature scheme, which can not only proves secure with leakage-resilient attacks under the hardness of the DDH problem but also enjoys a lower computational cost, shorter public key and secret key length, and a higher relative information leakage ratio. Nevertheless, our work gets a new way to obtain new and efficient leakage-resilient certificateless short signature scheme from non-homogeneous linear equation. We think it is interesting to show new ways of constructing more efficient leakage-resilient certificateless short signature scheme without sacrificing security.

Our scheme shows that the scheme is provably secure and leakage-resilient. We show that it is secure against existential

forgeable on adaptively chosen message in the random oracle model under the DDH assumption. Compared to existing schemes, our new scheme has two advantages: (1) Our scheme is leakage-resilient certificateless short signature scheme; (2) Our Scheme is leakage-resilient signature scheme, and leaked information is a maximum value (upper bound).

1.3. Organization

We organize the rest of the paper as follows. Firstly, i section 2, we review some preliminary knowledge that is non-homogeneous linear equations. We also give the security model for leakage-resilient certificateless short signature scheme against leakage attacks. Then, in Section 3, we present a new leakage-resilient certificateless short signature scheme. We prove the security and leakage-resilient of our scheme in Section 4. To demonstrate performances of scheme, a comparison with the existing scheme is made in Section 5. Finally, we give a conclusion in Section 6.

2. Preliminary

In this section, we firstly introduce some preliminary knowledge that is non-homogeneous linear equations. Then, we introduce the DDH assumption on which the security of our scheme is mainly based. Finally, we present the definitions which are important tools that will be used in our constructions and security analysis. For the security model under the DDH assumption is presented formally.

2.1. Computational Assumptions and Notations

Denote PPT as probability polynomial time. If $A(\cdot)$ is an algorithm, the $a \leftarrow A(\cdot)$ denotes running the algorithm $A(\cdot)$ and getting a as an output, which is distributed according to the internal randomness of $A(\cdot)$.

Definition 2.1 (DDH Assumption): Let $\mathbb{G}$ be a group of prime order q, which is determined by some security parameter n. Define two 4-tuples $\left(g, g^x, g^y, g^{xy}\right)$ and $\left(g, g^x, g^y, g^z\right)$, where $x, y, z \leftarrow \mathbb{Z}_q^*$. The DDH problem is to distinguish the two tuples.

A PPT adversary $\mathcal{A}$'s advantage is defined as

$$succ_{\mathbb{G},\mathcal{A}}^{DDH}(n) = \left|\Pr\left[\mathcal{A}\left(g, g^x, g^y, g^{xy}\right) = 1\right] - \Pr\left[\mathcal{A}\left(g, g^x, g^y, g^c\right) = 1\right]\right| \quad (1)$$

If the advantage of any adversary $\mathcal{A}$ is negligible in n, we say that the DDH assumption holds.

Next, we state the definition of traceable identity-based signature scheme used in the paper. A signature scheme with a plaintext space $\mathcal{M}$ is divided into five PPT algorithm.

Definition 2.2 (Certificateless Short Signature Scheme): A certificateless short signature scheme consists of the following 7 algorithms: *Setup*, *Extract-Partial-Private-Key*, *Set-Secret-Value*, *Set-Private-Key*, *Set-Public-Key*, *Certificateless-Sign* (*CL-Sign*), *Certificateless-Verify* (*CL-Verify*).

(1) *Setup* : This is an algorithm run by KGC which takes as input a security parameter l, and outputs system parameter *params*, and a master key s. Finally, KGC exposes system parameter *params*, and secrets master key s.

(2) $Extract-Partial-Private-Key$: This is an algorithm run by KGC which takes as input a system parameter *params*, a master key *params*, the user *ID*, and outputs the user *ID* 's part of the private key d_{ID}. KGC returns d_{ID} to the user *ID*.

(3) $Set-Secret-Value$: This is an algorithm run by the user which takes as input a system parameter *params*, the user *ID*, and outputs user *ID* 's secret value x_{ID}.

(4) $Set-Private-Key$: This is an algorithm run by the user which takes as input a system parameter *params*, the user *ID* 's part of the private key d_{ID}, the user *ID* 's secret value x_{ID}, and outputs user *ID* 's private key sk_{ID}.

(5) $Set-Public-Key$: This is an algorithm run by the user which takes an input a system parameter *params*, the user *ID* 's secret value x_{ID}, and outputs user *ID* 's public key pk_{ID}. Finally, the user *ID* exposes public key pk_{ID}.

(6) $Certificateless-Sign$ ($CL-Sign$): This is an algorithm run by the user which takes an input a system parameter *params*, message m, user's identity *ID*, private key sk_{ID} and public key pk_{ID}, outputs signature S.

(7) $Certificateless-Verify$ ($CL-Verify$): This is a deterministic algorithm which takes as input user's identity *ID*, public key pk_{ID}, system parameter *params*, message m and signature S. It outputs "1" if signature S is a valid signature on message m for the identity *ID*, otherwise outputs "0".

2.2. Security Model

When there is certificateless short signature scheme, the user's public key didn't get the authentication. In the security model, this article allows adversary have the right to use his own choice of illegal public key instead of the user's public key. On the side, KGC knows system's master key s, so that KGC can calculate all user's part of the private key. Therefore, in the security model, we also consider a malicious-but-passive KGC. We define that this adversary

can't the user's public key. Now we define the adversary model of certificateless short signature.

In the certificateless short signature scheme, adversaries can be divided into 2 categories based on PKG's behavior.

1. Type I: The adversary $\mathcal{A}_1$ plays a dishonest user. The adversary $\mathcal{A}_1$ does not know system master key s, and user's partial secret key. But, the adversary $\mathcal{A}_1$ can replace the user's public key. In the certificateless short signature scheme, there is no authentication between public key and the user.

2. Type II: The adversary $\mathcal{A}_2$ plays a malicious-but-passive KGC. The adversary $\mathcal{A}_2$ knows system master key s and user's partial secret key. But, the adversary $\mathcal{A}_2$ can't replace the user's public key.

Now we define the security model of certificateless short signature scheme.

Definition 2.3 (Security Model of Certificateless Short Signature Scheme):

A certificateless short signature scheme is existentially unforgeable under selective message and ID attacks if no probabilistic polynomial-time adversary $\mathcal{A}$ (type I or type II) can with the following game with non-negligible advantage ε.

Game I: The game is given below:

The challenger $\mathcal{C}$ randomly selects safety parameters l. The challenger $\mathcal{C}$ runs algorithm *Setup*, gets system parameter *params* and master key s. Then, the challenger $\mathcal{C}$ sends system parameter *params* to adversary $\mathcal{A}_1$. The adversary $\mathcal{A}_1$ adaptively queries as follows:

(1) $Hash-Queries$: The adversary $\mathcal{A}_1$ has the authority to access the signature scheme using all oracles. The challenger $\mathcal{C}$ returns the corresponding values to adversary $\mathcal{A}_1$.

(2) $Extract-Partial-Private-Key-Queries$: For queries of partial secret key d_{ID} of identity ID, the challenger $\mathcal{C}$ randomly choose value x_{ID} as the secret value of identity ID, generates corresponding partial secret key d_{ID}, and returns it to adversary $\mathcal{A}_1$.

(3) $Extract-Private-Key-Queries$: For queries of all of secret keys of identity ID (except ID^*), the challenger $\mathcal{C}$ returns the corresponding values to adversary $\mathcal{A}_1$. But, the user's public key has been replaced, then, the challenger $\mathcal{C}$ returns a null value to adversary $\mathcal{A}_1$.

(4) $Request-Public-Key-Queries$: For queries of public key pk_{ID}, the challenger $\mathcal{C}$ returns the corresponding values pk_{ID} to adversary $\mathcal{A}_1$.

(5) $Replace-Public-Key-Queries$: The adversary $\mathcal{A}_1$ can choose public key $pk_{ID'}$ replacements user's public key pk_{ID}.

(6) $Sign-Queries$: The adversary $\mathcal{A}_1$ can make a signature query on message/identity (m^*, ID^*), challenger $\mathcal{C}$ runs algorithm $Sign$ to generate corresponding signature S^*, and returns it to adversary $\mathcal{A}_1$. But, the user's public key has been replaced, then, the challenger $\mathcal{C}$ returns a null value to adversary $\mathcal{A}_1$.

The adversary $\mathcal{A}_1$ finally outputs a tuple $\left(m^*, S^*\right)$, where S^* is a signature signed by user with identity ID^* on message S^*. If signature S^* is a valid signature and satisfies the $CL-Verify\left(params, ID^*, m^*, pk_{ID^*}, S^*\right)=1$, and satisfies the following conditions, we say adversary $\mathcal{A}_1$ wins the game.

(i) For type I adversary $\mathcal{A}_1$, ID^* has never been used for $Extract-Private-Key-Queries$.

(ii) For type I adversary $\mathcal{A}_1$, ID^* has never been used for $Replace-Public-Key-Queries$, at the same time, ID^* has never been used for $Extract-Partial-Private-Key-Queries$.

(iii) For type I adversary $\mathcal{A}_1$, $\left(ID^*, m^*, pk_{ID^*}, S^*\right)$ has never been queried by algorithm $Sign$.

Game II: The game is given below:

The challenger $\mathcal{C}$ randomly selects safety parameters l. The challenger $\mathcal{C}$ runs algorithm *Setup*, gets system parameter *params* and master key s. Then, the challenger $\mathcal{C}$ sends system parameter *params* and master key s to adversary $\mathcal{A}_2$. The adversary $\mathcal{A}_2$ adaptively queries as follows:

(1) $Hash-Queries$: The adversary $\mathcal{A}_2$ has the authority to access the signature scheme using all oracles. The challenger $\mathcal{C}$ returns the corresponding values to adversary $\mathcal{A}_2$.

(2) $Extract-Private-Key-Queries$: For queries of all of secret keys of identity ID (except ID^*), the challenger $\mathcal{C}$ returns the corresponding values sk_{ID} to adversary $\mathcal{A}_2$. But, the user's public key has been replaced, then, the challenger $\mathcal{C}$ returns a null value to adversary $\mathcal{A}_2$.

(3) $Request-Public-Key-Queries$: For queries of public key pk_{ID}, the challenger $\mathcal{C}$ returns the corresponding values pk_{ID} to adversary $\mathcal{A}_2$.

(4) $Sign-Queries$: Adversary $\mathcal{A}_2$ can make a signature query on message/identity $\left(m^*, ID^*\right)$, challenger $\mathcal{C}$ runs algorithm $Sign$ to generate corresponding signature S^*, and returns it to adversary $\mathcal{A}_2$. But, the user's public key has been replaced, then, the challenger $\mathcal{C}$ returns a null value to adversary $\mathcal{A}_2$.

The adversary $\mathcal{A}_2$ finally outputs a tuple $\left(m^*, S^*\right)$, where S^* is a signature signed by user with identity ID^* on message S^*. If signature S^* is a valid signature and satisfies the $CL-Verify\left(params, ID^*, m^*, pk_{ID^*}, S^*\right)=1$, and satisfies the following conditions, we say adversary $\mathcal{A}_2$ wins the game.

(1) For type II adversary $\mathcal{A}_2$, ID^* has never been used for $Extract-Private-Key-Queries$.

(2) For type II adversary $\mathcal{A}_2$, $\left(ID^*, m^*, pk_{ID^*}, S^*\right)$ has never been queried by algorithm $Sign$.

And in general, it defines the certificateless short signature scheme's security, always gives the attacker's strongest attack ability, and minimum target of protection. In this model, if there is no any attacker can successfully complete the attack on the signature scheme, the scheme has the strongest security. In this article, we show that it is secure against existential forgeable on adaptively chosen message attack under the random oracle. In order to better describe the concept, related definition is given below.

Definition 2.4 (adaptive chosen-message attack [14]) We say that a signature scheme is ε-existentially forgeable if it is existentially forgeable with probability ε where the probability space include the random choices of the adaptive chosen-message attack, the random choices made by the legal signer in the creation of the public key, and the random choice made by the legal signer in producing signatures.

Definition 2.5 (Existentially unforgeable under chosen-message attack, EUF-CMA) Adversary $\mathcal{A}_1$ and Adversary $\mathcal{A}_2$ succeed in the above game if the following two conditions. Then, an existential unforgeable under chosen-message attack (EUF-CMA) is a security notion under a scenario of attack towards a signature scheme, where the forger can dynamically obtain signatures of message of his choice with a condition that is does not make any signature queries of the message it is going to output the valid forgery of. A valid forgery is a pair of a message and a valid signature of the message, where the signature was never retrieved by the forger.

Definition 2.6 (Existentially unforgeable under adaptive chosen-message attack, EUF-ACMA [15]) An existential unforgeability under an adaptive chosen message attack (EUF-ACMA) is a security notion under a scenario of attack towards a signature scheme, where the forger can dynamically obtain signatures of messages of his choice with a condition that is does not make any signature queries of the message it is going to output the valid forgery of. A valid forgery is a pair of a message and a valid signature of the message, where the signature was never retrieved by the forger.

Informally speaking, a certificateless short signature scheme is said resilient to leakage attacks if it is still semantically secure even when adversary $\mathcal{A}$ obtains some sensitive leakage information about the secret value. In the security model, leakage attacks are modeled by providing the adversary the chance to access a leakage oracle: the adversary could submit any efficient leakage function f to the oracle and receive the output of $f(s)$, where s denotes the input value.

We allow the when adversary $\mathcal{A}$ to query the leakage function f adaptively, with only one limitation: the total amount of output length of all the leakage functions f submitted to the leakage function f has to be bounded by a predetermined leakage parameter λ_{total}. Once leakage function output $f(s)$ more than λ_{total}, then the signature scheme is no longer safe, it need to update the related key parameters of signature scheme. Otherwise, the adversary $\mathcal{A}$ can decrypt the signature scheme.

Now, we give the following definition.

Definition 2.7 (Leakage-Resilient) If in the sense of traditional (black box), a cryptographic primitive (or protocol) is secure, and under the running condition of algorithm $\mathcal{C}$, the adversary $\mathcal{A}$ can get some information and the system is also secure, a cryptographic primitive (or protocol) is called leakage-resilient.

First of all, the adversary $\mathcal{A}$'s ability has the following restrictions:

Leakage-Resilient I (bounded leakage): In the whole running process of algorithm $\mathcal{C}$, the leaked information is unbounded. But, in every time invocation, the leaked information is bounded.

Leakage-Resilient II (only computation leaks): The algorithm $\mathcal{C}$, in the called process, the active state leaks information and the inactive state doesn't leak information. The state which is not used in one invocation is called passive state. The state which is used in one invocation is called active state. The adversary $\mathcal{A}$ has a leakage function $f(s)$ which gets the algorithm $\mathcal{C}$'s internal state information parameter as input.

The signature scheme is through the threshold thought, and uses leakage function $f(s)$ to limit the adversary $\mathcal{A}$'s attack ability. Leakage function $f(s)=s$ (among them, s is the algorithm $\mathcal{C}$ leaks out the amount of information). Domain: $\{0,1\}^{\lambda}$ (that is, bounded leakage range). Then, in the next algorithm $\mathcal{C}$ cycle, leakage function $f\left(s^+ \mid r\right)$(among them, s^+ is the algorithm $\mathcal{C}$ leaks out the amount of new information, r is the algorithm $\mathcal{C}$ random flip a coin to get the value). That is,

$$f(s)=\begin{cases} s & now \\ s^+ \mid r & next \end{cases} \tag{2}$$

In addition, define leakage function f, leaked information

amount no more than λ_{total} every time. The related literature [23-28].

Definition 2.8 (Security Model of Certificateless Short Signature Scheme): A certificateless short signature scheme is existentially unforgeable under selective message attacks if no probabilistic polynomial-time adversary $\mathcal{A}$ (type I or type II) can win the game with a non-negligible advantage ε.

Here, this paper generalized this concept; get the definition of leakage-resilient certificateless short signature scheme.

Definition 2.9 (Security Model of Leakage-Resilient Certificateless Short Signature Scheme) The adversary $\mathcal{A}$ gets a powerful oracle, it can output after choice message signature, and it can act as a leakage function. But, the adversary $\mathcal{A}$ can't forge a signature of any message.

Definition 3.0 By using oracle the adversary $\mathcal{A}$ gets the probability of correct results:

$$\Pr_{Oracel} = \frac{1}{2} \cdot (\alpha + \beta) \tag{3}$$

Among them, α is the type I error probability; β is the type II error probability.

Notice: If one uses the signature scheme to sign a lot of messages, that is, leaked information amount will exceed λ_{total}. Then, this signature scheme updates its internal state information.

The leakage-resilient traceable identity-based signature scheme security is defined using the following interactive game between the adversary $\mathcal{A}$ and the challenger $\mathcal{B}$:

1. Setup: The challenger $\mathcal{B}$ runs the key generation algorithm *Setup* and *Key-Extract* with a security parameter s as input and generates the public key pk and the secret key sk. Then, the challenger $\mathcal{B}$ gives the public key pk to the adversary $\mathcal{A}$ and keeps the secret key sk private to himself.

2. Phase I: The adversary $\mathcal{A}$ can make both $H_1 - Queries$ and $H_2 - Queries$ to the challenger $\mathcal{B}$. The challenger $\mathcal{B}$ operates the leakage function $f(s)$, gives the corresponding answers using the secret key sk. Notice that the total length of all returned $f(s)$ about the same secret key sk must less than a fixed λ in bits otherwise, the challenger $\mathcal{B}$ outputs the invalid answer $\perp$.

3. Phase II: The adversary $\mathcal{A}$ can make both $Partial - Private - Key - Extract - Queries$ and $Secret - Value - Queries$ to the challenger $\mathcal{B}$. The challenger $\mathcal{B}$ operates the leakage function $f(s)$, gives the corresponding answers using the secret key sk. Notice that the total length of all returned $f(s)$ about the same secret key sk must less than a fixed λ in bits otherwise, the challenger $\mathcal{B}$ outputs the invalid answer $\perp$.

4. Challenge: After receiving the secret key sk^* from the challenger $\mathcal{B}$, the adversary $\mathcal{A}$ continue to query the $Sign - Queries$ adaptively, gives the corresponding answers using the secret key sk^*.

5. Guess. The adversary $\mathcal{A}$ can make $Sign - Queries$ to the challenger $\mathcal{B}$. The challenger $\mathcal{B}$ operates the leakage function $f(s)$, gets the corresponding message signature v'. We say the adversary $\mathcal{A}$ succeeds if $v' = v$.

3. Leakage-Resilient Certificateless Short Signature Scheme

Based on the solution structure of the non-homogeneous linear equation system, this paper presents an efficient leakage-resilient certificateless short signature scheme. The signature scheme consists of eight primary algorithms, which is explained next.

(1) $Setup$: KGC randomly selects a random number $s \in \mathbb{Z}_q^*$, as a master private key s. KGC choose the two security cryptography hash function: $H_1, H_2 : (0,1)^* \to \mathbb{Z}_q^*$. Then, KGC calculates $a_{ij} = H_1(ID)$ (notice: ID is user identity.)

Then, KGC calculation of non-homogeneous linear equations $Ax = b$ (1), get the special solution η. Then, KGC calculates $P_{Pub} = s \cdot \eta$, (notice: it needs be secrecy.)

Finally, KGC public system parameters: $\{A, b, \eta, P_{Pub}, H_1, H_2\}$, and confidential s.

(2) $Extract$: First, user ID calculation of non-homogeneous linear equations $Ax = b$ (1), get the special solution d_{ID}, as the user ID's part of the private key d_{ID}.

(3) $Set - Secret - Value$: First, user ID calculation of non-homogeneous linear equations $Ax = b$ (1), get general solution $\xi = \{\xi_1, \xi_2, \cdots, \xi_n\}$. Then, user ID randomly selects a random value $\xi = \{\xi_1, \xi_2, \cdots, \xi_n\}$, as a secret value x_{ID}.

(4) $Set - Private - Key$: This is an algorithm run by user ID which takes as input a system parameter $params$, the user ID's part of the private key d_{ID}, the user ID's secret value x_{ID}, and outputs the user ID's private key $x = d_{ID} + x_{ID}$.

(5) $Set - Public - Key$: This is an algorithm run by user ID which takes as input a system parameter $params$, the user ID's part of the private key d_{ID}, and outputs the user ID's public key $pk_{ID} = s \cdot d_{ID}$.

(6) *Leaking compute*: in this phase, the user ID computing leakage message amount λ. When $\lambda \geq \lambda_{total}$ shows that the signature scheme is not security. That is, the adversary $\mathcal{A}$ can easily sign the message.

(7) $CL-Sign$: The user ID signs a message $m \in \{0,1\}^*$:

(i) Calculates: $h = H_1(m, pk_{ID})$;

(ii) Finally, the message signature is $S = h \cdot k \cdot x = h \cdot k \cdot (x_{ID} + d_{ID})$.

$Verify$: The verifier $\mathcal{B}$ who receives a signed message S . Then, the verifier $\mathcal{B}$:

(i) Calculates: $h = H_1(m, pk_{ID})$;

(ii) Calculates verifying formulas: $Ver(params, m, ID, PK_{ID}, S) = 1$. It outputs "1" if signature S is a valid signature on message m for the identity ID , and outputs "0" otherwise. A signed message S is valid only when its condition $Ax = h \cdot k \cdot b$ and $x = S$ is satisfied.

Now began to prove the validity of the formula.

Proof:

On the left:

$$Ax = A \cdot h \cdot k \cdot x = A \cdot h \cdot k \cdot (x_{ID} + d_{ID}) = h \cdot k \cdot A \cdot (\xi + \eta) \quad (4)$$
$$= h \cdot k \cdot A \cdot \xi + h \cdot k \cdot A \cdot \eta = 0 + h \cdot k \cdot b = h \cdot k \cdot b$$

on the right.

The right is equal to the left. Over.

4. Type I and Type II Adversary $\mathcal{A}$ of Security Proof

Nowadays, many certificateless signature schemes depend on the honesty of Key Generation Center (KGC) excessively, so they also lose security guarantees when the KGC is dishonest.

The formal security proof of this scheme is provided in the random oracle model (type I and type II adversary $\mathcal{A}$).

Theorem 4.1 Under the assumption that the DDH problem is hard, and the underlying hash function H is target collision-resistant, then our proposed leakage-resilient certificateless short signature scheme is semantically secure against adaptive chosen message attack for leakage message amount $\lambda \prec \lambda_{total}$, where λ denotes the signature scheme security parameter, λ_{total} denotes all leakage message amount.

And we have adversary $\mathcal{A}$ the probability of winning.

$$\Pr = \left[\frac{1}{2}\right]^{m \times n} \cdot \left[\frac{1}{2}\right]^{m \times n} \cdot \left[\frac{1}{2}\right]^{m \times n} = \left[\frac{1}{8}\right]^{m \times n} \quad (5)$$

Among them: m is the vector equations $Ax = b$ of solution space's dimensions; the total number of n is the element in the set $\{\xi_1, \xi_2, \cdots, \xi_n\}$.

And we have the advantage that the algorithm $\mathcal{C}$ wins in game.

$$\varepsilon' \geq \varepsilon - \left(\frac{1}{16}\right)^{m \times n} \quad (7)$$

The algorithm $\mathcal{C}$'s running time t' accords with $t' < t + 2(q_{pk} + q_S)t_e$, where t_e is computation time of $Ax = b$.

The security of our scheme follows by Theorem 4.1 which indicates that the above signature scheme is secure under the classical DDH assumption. To prove the Theorem 4.1, we show that any efficient adversary (type I and type II adversary $\mathcal{A}$) that breaks the security of the scheme can be used to break the security of the universal one-way hash function H .

Notation: the time of adversary $\mathcal{A}$'s access to $H_i (i = 1,2)$ is q_{H_i} , the adversary $\mathcal{A}$ access $Extract-Partial-Private-Key$ oracle's time is q_E , the adversary $\mathcal{A}$ access $Extract-Private-Key$ oracle's time is $q_{E'}$, the adversary $\mathcal{A}$ access $Request-Public-Key$ oracle's time is q_{pk} , the adversary $\mathcal{A}$ access $Sign$ oracle's time is q_S . Then, there is an algorithm $\mathcal{C}$ within the time t' with the advantages of ε' , solving non-homogeneous linear equation systems' correlation theory.

Proof:

Now, we are analysis the algorithm $\mathcal{C}$ in this game winning advantage ε .

(1) The adversary $\mathcal{A}$ cannot distinguish between $H_1-Queries$'s reply and $H_2-Queries$'s reply. Because every answer is independent uniform distribution in the $\mathbb{Z}_q^*$, and is a valid answer.

(2) If events E_1 and E_2 does not occur, then $Sign-Queries$'s reply and $Partial-Private-Key-Extract-Queries$'s reply is valid. If events E_1 , E_2 , and E_3 does not occur, the algorithm $\mathcal{C}$ stops the simulation, outputs "$FAILURE$".

Now we are calculating the probability of these events. There are clearly:

$$\Pr = \left[\frac{1}{2}\right]^{m \times n} \cdot \left[\frac{1}{2}\right]^{m \times n} \cdot \left[\frac{1}{2}\right]^{m \times n} = \left[\frac{1}{8}\right]^{m \times n} \quad (8)$$

Among them: m is the vector equations $Ax = b$ of solution space's dimensions; the total number of n is the element in the set $\{\xi_1, \xi_2, \cdots, \xi_n\}$.

In the end, we can calculate the algorithm $\mathcal{C}$ win in game advantage:

$$\varepsilon' \geq \varepsilon - \left(\frac{1}{16}\right)^{m \times n} \quad (9)$$

The algorithm $\mathcal{C}$ running time is $t' < t + 2(q_{pk} + q_S)t_e$,

and t_e is $Ax = b$ (1) computation time.

5. Efficiency Comparisons

Now we compare our scheme with other signature schemes in the following Table 1. E denotes one exponential in multiplicative group. $\Pr$ denotes one pairing operation. By A_d and Sm, A_d denotes one add operation. Sm denotes one multiplication operation in additive group. We denote a hash function which mapping to a point by H. $t_e(m,n)$ denotes the computing time of non-homogeneous linear equations $AX = b$.

Table 1. *The comparison of efficiency.*

Scheme	AP [1]	LCS [2]	YHG [4]	GS [29]	Our scheme
Sign	3*Sm*+1Pr	2*Sm*	2*Sm*	2*Sm*	$t_e(m, n)$
Verify	1*Exp*+4Pr	2*Sm*+4Pr	2Pr+2Sm	1*Sm*+3Pr	$t_e(m, n)$
|*pk*|	320*bits*	320*bits*	160*bits*	160*bits*	m
|*signature*|	320*bits*	320*bits*	320*bits*	320*bits*	h·k·m

This Table 1 shows that our certificateless short signature scheme is the most efficient. Since we remove the complicated pairing operation in our scheme, we acquire a secure scheme with small computation cost. Moreover, our signature scheme is leakage resilient signature scheme, and leaked information is a maximum value (upper bound).

6. Conclusion

In this paper we have introduced a new efficient leakage-resilient certificateless short signature scheme by simplifying some parameters of the certificateless short signature scheme. Our scheme is leakage-resilient signature scheme, and leaked information is a maximum value (upper bound). What is more, our scheme also enjoys a higher relative leaked information rate and still semantically secure against adaptive chosen message attack. Besides these good performance features, we have formally proved the security of our scheme in the random oracle model under the hardness of the decisional Diffie-Hellman problem. With these import features, our proposal may have some significant value in the practical applications.

In the process of scheme proof, the security model assumes tightly that the adversary does not know any of intermediate value which is produced during the signature generation. However, it is not always the case in real application environment. Therefore, it is an interesting and valuable future work that how to construct an efficient leakage-resilient certificateless short signature scheme in the standard model under the hardness of the computational Diffie-Hellman (CDH) problem.

Acknowledgments

The authors would like to thank the anonymous referees for their helpful comments.

References

[1] Al-Riyami, S. S., & Paterson, K. G. (2003). Certificateless public key cryptography. In *Advances in Cryptology-ASIACRYPT 2003* (pp. 452-473). Springer Berlin Heidelberg.

[2] Li, X. X., Chen, K. F., & Sun, L. (2005). Certificateless signature and proxy signature schemes from bilinear pairings. *Lithuanian Mathematical Journal*, *45* (1), 76-83.

[3] Zhang, Z., Wong, D. S., Xu, J., & Feng, D. (2006, January). Certificateless public-key signature: security model and efficient construction. In *Applied Cryptography and Network Security* (pp. 293-308). Springer Berlin Heidelberg.

[4] Yap, W. S., Heng, S. H., & Goi, B. M. (2006). An efficient certificateless signature scheme. In *Emerging Directions in Embedded and Ubiquitous Computing* (pp. 322-331). Springer Berlin Heidelberg.

[5] Zhang, Z., Wong, D. S., Xu, J., & Feng, D. (2006, January). Certificateless public-key signature: security model and efficient construction. In *Applied Cryptography and Network Security* (pp. 293-308). Springer Berlin Heidelberg.

[6] Liu, J. W., Sun, R., & Ma, W. P. (2008). Efficient ID-based certificateless signature scheme. *JOURNAL-CHINA INSTITUTE OF COMMUNICATIONS*, *29* (2), 87.

[7] Boneh, D., & Franklin, M. (2001, January). Identity-based encryption from the Weil pairing. In *Advances in Cryptology—CRYPTO 2001* (pp. 213-229). Springer Berlin Heidelberg.

[8] Goyal, V. (2007). Reducing trust in the PKG in identity based cryptosystems. In *Advances in Cryptology-CRYPTO 2007* (pp. 430-447). Springer Berlin Heidelberg.

[9] Chen, X., Zhang, F., & Kim, K. (2003). A New ID-based Group Signature Scheme from Bilinear Pairings. *IACR Cryptology ePrint Archive*, *2003*, 116.

[10] Liao, J., Xiao, J., Qi, Y., Huang, P., & Rong, M. (2005, January). ID-based signature scheme without trusted PKG. In *Information Security and Cryptology* (pp. 53-62). Springer Berlin Heidelberg.

[11] Bellare, M., & Neven, G. (2006, October). Multi-signatures in the plain public-key model and a general forking lemma. In *Proceedings of the 13th ACM conference on Computer and communications security* (pp. 390-399). ACM.

[12] Liu, J. K., Au, M. H., & Susilo, W. (2007, March). Self-generated-certificate public key cryptography and certificateless signature/encryption scheme in the standard model. In *Proceedings of the 2nd ACM symposium on Information, computer and communications security* (pp. 273-283). ACM.

[13] Zhang Hua, Wen Qiaoyan, Jin ZhengPing. (2012). Proven security algorithms and protocols (pp. 144). Bei Jing: Science Press.

[14] Goldwasser, S., Micali, S., & Rivest, R. L. (1988). A digital signature scheme secure against adaptive chosen-message attacks. *SIAM Journal on Computing*, *17* (2), 281-308.

[15] Bagus S., Kazuo O., Noboru K.. (2004). Optimal Security Proof for PFDH under Existential Unforgeability against Strong Adaptive Chosen Message Attack. (pp. 53-61). Information Processing Society of Japan.

[16] Ki, J., Hwang, J. Y., Nyang, D., Chang, B. H., Lee, D. H., & Lim, J. I. (2012). Constructing strong identity-based designated verifier signatures with self-unverifiability. *ETRI Journal*, *34* (2), 235-244.

[17] Chen, C. L., Lu, M. S., & Guo, Z. M. (2012). A non-repudiated and traceable authorization system based on electronic health insurance cards. *Journal of medical systems*, *36* (4), 2359-2370.

[18] Abe, M., Chow, S. S., Haralambiev, K., & Ohkubo, M. (2013). Double-trapdoor anonymous tags for traceable signatures. *International journal of information security*, *12* (1), 19-31.

[19] Shin, S., & Kwon, T. (2014). AAnA: Anonymous authentication and authorization based on short traceable signatures. *International Journal of Information Security*, *13* (5), 477-495.

[20] Taha, M., & Schaumont, P. (2015). Key Updating for Leakage Resiliency With Application to AES Modes of Operation. *Information Forensics and Security, IEEE Transactions on*, *10* (3), 519-528.

[21] Yan, Q., Han, J., Li, Y., Zhou, J., & Deng, R. H. (2015). Leakage-resilient password entry: challenges, design, and evaluation. *Computers & Security*, *48*, 196-211.

[22] Chen, D., Zhou, Y., Han, Y., Xue, R., & He, Q. (2014). On hardening leakage resilience of random extractors for instantiations of leakage-resilient cryptographic primitives. *Information Sciences*, *271*, 213-223.

[23] Kocher, P. C. (1996, January). Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In *Advances in Cryptology—CRYPTO'96* (pp. 104-113). Springer Berlin Heidelberg.

[24] Quisquater, J. J., & Samyde, D. (2001). Electromagnetic analysis (ema): Measures and counter-measures for smart cards. In *Smart Card Programming and Security* (pp. 200-210). Springer Berlin Heidelberg.

[25] Gandolfi, K., Mourtel, C., & Olivier, F. (2001, January). Electromagnetic analysis: Concrete results. In *Cryptographic Hardware and Embedded Systems—CHES 2001* (pp. 251-261). Springer Berlin Heidelberg.

[26] Kocher, P., Jaffe, J., & Jun, B. (1999, January). Differential power analysis. In *Advances in Cryptology—CRYPTO'99* (pp. 388-397). Springer Berlin Heidelberg.

[27] Boneh, D., DeMillo, R. A., & Lipton, R. J. (1997, January). On the importance of checking cryptographic protocols for faults. In *Advances in Cryptology—EUROCRYPT'97* (pp. 37-51). Springer Berlin Heidelberg.

[28] Biham, E., & Shamir, A. (1997). Differential fault analysis of secret key cryptosystems. In *Advances in Cryptology—CRYPTO'97* (pp. 513-525). Springer Berlin Heidelberg.

[29] Choi, K. Y., Park, J. H., Hwang, J. Y., & Lee, D. H. (2007, January). Efficient certificateless signature schemes. In *Applied Cryptography and Network Security* (pp. 443-458). Springer Berlin Heidelberg.

Biography

Chen Xiaokui (1978.10-) received the master's degree in safety engineering from Anhui University Of Science And Technology, Currently, he is a lecturer in Anhui University Of Science And Technology, engaging in computer security research.