An efficient and provably secure certificateless short signature scheme

Shu-Rong Feng, Jiao Mo
School of Science
Beijing University of Posts and Telecommunication
Beijing, China
e-mail: fengshurongbupt@163.com

Shu-Rong Feng, Jiao Mo, Hua Zhang, Zheng-Ping Jin
State Key Laboratory of Networking and Switching Technology
Beijing University of Posts and Telecommunication
Beijing, China

Abstract—**Certificateless short signature can not only have the advantage of certificateless signature, but also provide a short signature size in communication. However , all existing certificateless short signature scheme only proven secure against a normal adversary which can only obtain the valid signatures for the original public key rather than a super adversary which can obtain the valid signatures for the replaced public key. In order to solve the problem, so in this paper, we proposed an efficient and provably secure certificateless short signature scheme which can be proved that it is secure against super adversaries in the random oracle model under the computational Diffie-Hellman (CDH) assumption. Furthermore, our scheme can provide both the strongest security level and the shortest signature size compared the existed provably secure certificateless short signature scheme.**

Keywords-Random oracle; Certificateless signature; Short signature; Bilinear pairing.

I. INTRODUCTION

Short signatures have a great advantage in applications where the bandwidth of a communication channel is limited. Since Boneh et al. [1] proposed the first short signature in traditional PKC which called BLS signature where the signature size are about half the size of DSA signatures while with the similar level of security, many concrete short signature schemes have been proposed in different public key cryptosystems [2-6]. Due to certificateless signature can not only avoid the inherent key escrow problem in identity-based public key cryptosystems, and do not need expensive certificates management in the public key infrastructure, it's a highlight to extend the notion of short signatures into certificateless cryptography and design certificateless signatures with short signature size. However, to construct an efficient and secure certificateless short signature is not an easy work for the adversaries who can be allowed to obtain valid signatures under the replaced public key [2] .

The first certificateless short signature was proposed by Huang et al. [2]. In their scheme, Huang et al. revised the security models of certificateless signature scheme, they classified type I/II adversaries into normal, strong and super type I/II adversaries according to their attack power. A normal adversary can only obtain the valid signatures for the original public key, a strong adversary can obtain the valid signatures for the replaced public key if additionally submits the correspond secret key, a super adversary can obtain the valid signatures for the current public key. In 2009 Du et al. [3] proposed a short CLS scheme, they claimed that their short certificateless signature scheme is provably secure against the strong type I normal type II adversaries in the random oracle model. Choi et al. [4] demonstrated the short CLS scheme is insecure against the strong type I adversary. They also proposed a short CLS scheme and proved their scheme is provably secure against the super type I/II adversary in the random oracle model under the CDH assumption. Recently, Tian et al. [5] show the scheme is insecure against a strong type I adversary. To enhance the security of short signatures, in 2012 Raylin Tso et al. [6] presented a strongly secure certificateless short signatures based on bilinear pairing, their scheme is strongly secure in the random oracle model. But all the existing certificateless short signature scheme only proven secure against a normal adversary which can only obtain the valid signatures for the original public key rather than a super adversary which can obtain the valid signatures for the replaced public key.

A. Contributions and organization

Our contributions: In this paper, we present an efficient certificateless short signature scheme that is proved to be secure in the random oracle model under the hardness assumption of CDH. The signature size of our scheme is as short as BLS short signature [1]. Compared with all other certificateless short signature [2-6], our scheme is the only one with provable security against super adversaries. Moreover signing a message requires only one exponentiation and one multiplication in a multiplicative cyclic group G_1 , and signature verification requires only one pairing (on-line) operation.

Organization: The rest of this paper is organized as follows. section II, we describe some fundamental backgrounds and define the certificateless signature scheme and its security model. section III and section IV, we propose a new efficient and provable secure short CLS scheme which is secure against the super type I/II adversary. section V, we compare our scheme with existing certificateless short signatures scheme, and we conclude the paper in section VI.

II. PRELIMINARIES

A. Bilinear Map

A bilinear map satisfying the three properties of bilinear, non-degenerate, computable is said to be an admissible

Published by Atlantis Press, Paris, France.

bilinear map[7]. We can make this map using the Weil pairing [8].

B. Complexity assumption

The proof of our scheme is under computational Diffie-Hellman (CDH) assumption in the random oracle model [7].

C. Certificateless signature scheme

A certificateless short signature scheme is specified by six polynomial time algorithms which is very similarly to the algorithms defined in Al-Riyami and Paterson[7]. The only difference in our scheme is that the user's public key pk_{ID} needed in the Set-Partial-Private-Key algorithm in order to against the super adversary.

D. Security models

For certificateless cryptosystems, there are two types of adversaries which called type I/II adversary with different capabilities according to the widely accepted notion of security defined by Al-Riyami and Paterson [7].

Generally, five oracles can be accessed by adversaries according to game, specifications will be given shortly.

Create-User：Input identity $ID \in \{0,1\}^*$ and check if the ID has been created. If not, the oracle generates the public key pk_{ID} and the private key which includes secret value x_{ID} and partial private key D_{ID}, After that, the oracle returns secret value x_{ID}, public key pk_{ID}, and partial private key D_{ID}. In both cases ID is returned.

Public-Key-Replace-Query: Input an identity ID and a user public key pk_{ID}' which is used to replace the original public key pk_{ID} of the user with identity ID. If ID has not been created, ignore this request.

Secret-Value-Query: Input an identity ID and check if ID has been created or not. If yes, return x_{ID} of ID. Otherwise, a symbol $\perp$ meaning invalid is returned. Note that, the secret value x_{ID} is used to generate the original public key, if ID has been replaced earlier, adversary cannot receive any response.

Partial-Private-Key-Query: Input an identity ID, pk_{ID} and check if ID has been created or not. If true, return D_{ID} of ID. Otherwise, a symbol $\perp$ meaning invalid is returned. Note that pk_{ID} is the current public key of the user with identity ID, so D_{ID} is the current partial private key.

Sign-Query: A signature is requested for an identity ID, pk_{ID} and a message $m \in \{0,1\}^*$. If ID has been created, the oracle returns a valid signature σ signed by the current private key of the user with identity ID. Otherwise, a symbol $\perp$ is returned. Note that pk_{ID} is the current public key of the user with identity ID.

In our scheme we will let A_1 be a type I adversary and A_2 be a type II adversary. Two games (Game 1 and Game 2) will be consider in here where A_1 and A_2 will respectively interact with its challenger C in these two games. If the success probability of both A_1 and A_2 is negligible, then we say that a CLS scheme is existentially unforgeable against adaptive chosen message and identity attackers.

Game 1: This game is executed between A_1 and a challenger C.

Setup: Taken a security parameter k as input, C runs the Setup algorithm to obtain a master key s and the system parameters $params$. C sends $params$ to A_1, keeps s secret.

Queries: A_1 makes a polynomial bounded number of all queries defined above in an adaptive manner.

Forgery: Eventually A_1 outputs a forgery $(ID^*, pk_{ID}{}^*, m^*, \sigma^*)$, and wins the game if σ^* is a valid signature, (ID^*, m^*) has never been submitted to the Sign-Query and ID^* has never been submit to the Partial-Private-Key-Query or the Secret-Value-Query.

Definition 1. Define Adv_{A_1} be the probability that A_1 succeeds in the above Game 1. If for all probability polynomial time (PPT) adversary A_1, the success probability Adv_{A_1} is negligible, we say a certificateless signature scheme is secure against type I adversary.

Game 2: This game is executed between A_2 and a challenger C.

Setup: Taken a security parameter k as input, A_2 runs the Setup algorithm to obtain a master key s and the system parameters $params$. Then A_2 sends both $params$ and s to C. It is noted that the system parameters are chosen by A_2.

Queries: A_2 makes a polynomial bounded number of all queries (except the Partial-Private-Key-Query) defined above in an adaptive manner.

Forgery: Eventually A_2 outputs a forgery $(ID^*, pk_{ID}{}^*, m^*, \sigma^*)$, wins the game if σ^* is a valid signature, (ID^*, m^*) has never been submitted to the Sign-Query and ID^* has not been submitted to the Secret-Value-Query.

Definition 2. Define Adv_{A_2} be the probability that A_2 succeeds in the above Game 2. If for all probability polynomial time (PPT) adversary A_2, the success probability Adv_{A_2} is negligible, we will say a certificateless signature scheme is secure against type II adversary.

Definition 3. If the certificateless signature scheme is secure against both type I and type II attacks defined above, we said the scheme is existentially unforgettably against adaptive chosen message and chosen identity attack.

As we see, adversaries defined above are very similar to the super adversaries defined in Huang et al. [8], namely adversaries are allowed to obtain valid signature under any public keys chosen by itself in the public key space.

III. OUR CERTIFICATELESS SHORT SIGNATURE SCHEME

In this section, we describe a new construction of certificateless short signature scheme. It consists of the following algorithms:

Setup: Let (G_1, G_2) be bilinear groups of a prime order p, where k is the security parameter of the scheme, Let $e: G_1 \times G_1 \to G_2$ be an admissible bilinear. Let H_0 : $\{0,1\}^* \to G_1^*, H_1: \{0,1\}^* \to G_1^*$ be two secure cryptographic hash functions. In system initialization, KGC chooses a random number $s \in Z_p^*$ and an arbitrary generator $g \in G_1^*$. It then calculates $P_{pub} = g^s$, and publishes $params = \{G_1, G_2, g, e, H_0, H_1, P_{pub}\}$. The master secret key s is kept as secret by KGC.

Set-Secret-Value: The entity ID chooses a random number $x_{ID} \in Z_p^*$, which is set as the secret value of ID.

Set-Public-Key: Given sk_{ID}, the entity ID computes the public key $pk_{ID} = (pk_{(ID,1)}, pk_{(ID,2)}) = (g^{x_{ID}}, P_{pub}{}^{x_{ID}}) = (g^{x_{ID}}, g^{s x_{ID}})$.

Set-Partial-Private-Key: Given user's identity $ID \in \{0,1\}^*$, public key pk_{ID}, KGC sets $Q_{ID} = H_0(ID \| pk_{ID})$, computes user's partial private key $D_{ID} = Q_{ID}{}^s$, the partial private key D_{ID} is sent to ID over a confidential and authentic channel.

Set-Private-Key: The entity ID sets his private key as $sk_{ID} = (D_{ID}, x_{ID})$

Sign: To sign a message $m \in \{0,1\}^*$, the entity ID computes the signature $\sigma = D_{ID}{}^{x_{ID}} \cdot H_1(m \| ID \| pk_{ID})^{x_{ID}}$.

Verify: Given a message/signature pair (m, σ) and ID's public key pk_{ID}, σ is verified by checking the following equations: $e(\sigma, g) = e(H_1(m \| ID \| pk_{ID}), pk_{(ID,1)}) e(Q_{ID}, pk_{(ID,2)})$

If the equation is satisfied, this algorithm outputs true. Otherwise, it outputs false.

IV. SECURITY ANALYSIS

In this section, a formal security analysis of our proposed scheme in the random oracle model will be given by us. In our model, the adversary has the power to obtain the valid signature under the replaced public key, which is similar to the super adversary defined in Huang et al.[2].

Theorem1 (Unforgettability against type I adversary): If there exists a type I adaptively chosen message and identity adversary A_1 who can make at most q_{cu} Create-User queries, q_{pke} Partial-Private-Key queries, q_{sve} Secret- value queries and q_s Sign queries, and can break the unforgettability of the proposed scheme via type I attack in polynomial time t with success probability ε. Then we show that there exists an algorithm ζ that can solve CDH problem with probability $Adv_{\varsigma}^{CDH} \geq 1/q_{cu} + q_s + 1(1 - 1/q_{cu} + q_s + 1)^{q_{cu} + q_s} \varepsilon$.

Proof: If there exists an adversary A_1 who can break the unforgettability of the proposed scheme via type I attack, then we can construct a algorism ς, such at ς can use A_1 as a black-box and solve the CDH problem.

Let (g, g^a, g^b) be a random instance of CDH problem taken as input by ζ. ζ first sets the system's master public key as $P_{pub} = g^a$ and generates params according to the Setup algorithm, then initializes A_1 with P_{pub} and $parames$. Then ζ simulates the oracles and answers A_1's queries as follows.

1. Random Oracles: In order to respond A_1's queries to random oracles, two lists: H_0 - list and H_1 - list will be maintained by ζ.

2. H_0 Queries: Let $\psi = ID \| pk_{ID}$, A_1 can issue H_0 Query on an identity ψ whenever. ζ will maintain a H_0 - list which stores his responses to such queries. If ψ has not be queried, ζ chooses $u_{ID} \in \{0,1\}$ with the probability that $\Pr[u_{ID} = 1] = \delta$ and $\Pr[u_{ID} = 0] = 1 - \delta$ (the value of δ will be determined later). if $u_{ID} = 1$ ζ chooses $k \in_R Z_p^*$ and sets $H_0(ID \| pk_{ID}) = (g^b)^k$. Otherwise, ζ sets $H_0(\psi) = g^k$. Then ζ adds $(ID, H_0(\psi), k, u_{ID})$ into the H_0 -list and returns $H_0(\psi)$ as the answer.

3. H_1 Queries: Let $w = m \| ID \| pk_{ID}$, A_1 can issue a H_1 Query when input w whenever. ζ will maintain a H_1 - list which stores his responses to such queries. If w has not be queried, ζ chooses $s \in_R Z_p^*$ and sets $H_1(w) = g^s$. Then ζ adds $(H_1(w), g^s, s)$ into the H_1 -list and returns g^s as the answer. Otherwise, nothing will be taken.

4. Create-User Oracle: We assume that before A_1 makes a Create-User query on an identity ID, it has already made the corresponding H_0 query on ψ. At any time, A_1 can make a Create-User query on an identity ID, if ID has already been created, nothing is to be carried out by ζ. Otherwise, ζ checks the H_0 - list.

1) If $u_{ID} = 1$, $\mathrm{H}_0(\psi) = (\mathrm{g}^{\mathrm{b}})^k$, In this situation, ζ sets $D_{ID} = \perp$, which means it can not compute the partial private key of ID. Then ζ chooses $t \in_R Z_p^*$, and sets the secret value of ID as $x_{ID} = t$ and the public key of ID as $pk_{ID} = (pk_{(ID,1)}, pk_{(ID,2)}) = (g^t, g^{at})$.

2) If $u_{ID} = 0$, $H_0(\psi) = g^k$ in this situation, ζ first computes the partial private key of ID as $D_{ID} = P_{pub}{}^k$. Then it chooses $t \in_R Z_p^*$, and sets the secret value of ID as $x_{ID} = t$ and the public key of ID as $pk_{ID} = (pk_{(ID,1)}, pk_{(ID,2)}) = (g^t, g^{at})$. Finally, ζ adds $(ID, D_{ID}, x_{ID}, pk_{ID})$ into the list L.

5. Public-Key-Replace-Query Oracle: When ζ makes a query on $(ID, pk_{ID}{}^*)$, where $pk_{ID}{}^*$ is a public key chosen by ζ. If ID has been created, ζ replaces ID's original public key with $pk_{ID}{}^* = (pk^*{}_{(ID,1)}, pk^*{}_{(ID,2)})$, updates the correspond information in the list L. Otherwise, outputs a symbol $\perp$.

6. Secret-Value-Extract-Query Oracle: When ζ makes a query on an identity ID, if ID has not been created, ζ outputs a symbol $\perp$. Otherwise, ζ browses the list L and returns the secret values x_{ID}.

7. Partial-Private-Key--Query Oracle: When ζ makes a query on an identity ID, if ID has not been created, ζ

outputs a symbol $\perp$. Otherwise, ζ browses the list L and returns the partial private key D_{ID}.

8. Sign-Query Oracle: We assume that when ζ requests a signature on (m,ID) where ID denotes the identity which has been created, it has already made the corresponding H_0 query on ($ID \| pk_{ID}$) and H_1 query on ($m \| ID \| pk_{ID}$) and the list L contains an item $(ID, D_{ID}, x_{ID}, pk_{ID})$. At any time, ζ can submit a Sign-Query on (m,ID), if $u_{ID}=1$, ζ halts and fails to solve CDH problem. Otherwise, ζ compute $\sigma = P_{pub}{}^{kt} g^{st}$. Then ζ adds (ID, m, pk_{ID}, σ) into the Sign- list L_{sign} and returns short signature σ to A_1.

After all queries, A_1 outputs a valid forgery σ^* on m^*, for an identity ID^* with public key pk_{ID^*}. If $u_{ID^*}=1$, then $\mathrm{H}_0(ID^* \| pk_{ID^*}) = (\mathrm{g}^{\mathrm{b}})^{k^*}$, so $\sigma^* = (g^b)^{k^* at} g^{s^* t^*} = (g^{ba})^{k^* t^*} g^{s^* t^*}$. Consequently, ζ outputs $g^{ab} = (\sigma^*)^{(k^* t^*)^{-1}} / (g^{s^*})^{(k^*)^{-1}}$ and thus solves CDH problem.

To complete the proof, we need to calculate the probability that ζ succeeds and the time ζ runs. If ζ does not halt in the simulation and $u_{ID}{}^* = 1$, then A_1 can forge a valid signature with advantage ε. The probability that ζ does not halt in the simulation is $(1-\sigma)^{q_{cu}}(1-\sigma)^{q_s}$. Therefore, the success probability ε' that ζ solves CDH problem is $\sigma(1-\sigma)^{q_{cu}}(1-\sigma)^{q_s}\varepsilon = \sigma(1-\sigma)^{q_{cu}+q_s}\varepsilon$ when $\sigma = 1/q_{cu}+q_s+1$, this probability is maximized at $1/q_{cu}+q_s+1(1-1/q_{cu}+q_s+1)^{q_{cu}+q_s}\varepsilon$. The time t' is at most $t+Qt_q+c$ where t_q is the maximum time for simulating one oracle query, Q denotes the max oracle queries and c denotes some constant time of system setup.

Theorem2 (unforgettability against type II adversary). The kinds and times of queries maked by type II adversary are similar to the type I adversary excepted it can not make Partial-Private-Key queries. Then we show that there exists an algorithm ζ that can solve CDH problem with probability $Adv_{\varsigma}^{CDH} \geq 1/q_{cu}+q_s+1(1-1/q_{cu}+q_s+1)^{q_{cu}+q_s}\varepsilon$.

Proof: The proof is very similar to the proof procedure of unforgettability against type I adversary, it's given in http://blog.sina.com.cn/u/2120716550 in detailed.

V. PERFORMANCE COMPARISON

In this section, we compare our certificateless short signature scheme with other existing certificateless short signature schemes from the aspects of communication and computation cost in sign and verification phase and type of against adversary respectively. In the comparison, the operations of $e(H_1(m \| \mathrm{ID} \| pk_{ID}), pk_{(ID,1)})$ and $e(Q_{ID}, pk_{(ID,2)})$ are precomputable or only need to be computed once. Therefore, these computations are neglected in comparison.

TABLE I.

Schemes	**Hardness**	**Cost**	**Cost verify**	**Strong**
	assumption	**sign**		**adversary**
Ours	CDH	1 E_{G_1}	1 $\hat{e}$	secure
R. Tso et al. 2012[6]	CDH, InvCDH	1 E_{G_1}	2 $\hat{e}$ +1 E_{G_1}	insecure
Choi et al. 2011[4]	CDH	3 E_{G_1}	3 $\hat{e}$ +2 E_{G_1}	insecure

Figure 1. performance evaluation

As shown in Fig. 1, signature generation in our scheme only needs one E_{G_1} computation and one e computation (e is a pairing computation and E_{G_1} is an exponentiation in G_1). Moreover our certificateless short signature scheme is the only one which can achieve secure against super adversary.

VI. CONCLUSION

In this paper, we proposed a new short CLS scheme and proved its security in the random oracle model under the CDH assumption. The proposed scheme has the shortest signature length compared with other CLS schemes with same level of security. Most of the CLS schemes including the proposed scheme are proven secure in the random oracle model. Therefore, designing the CLS scheme without random oracles needs to be studied as further work.

ACKNOWLEDGEMENTS

This work is supported by NSFC (Grant Nos. 61202434, 61170270, 61121061), the Fundamental Research Funds for the Central Universities (Grant Nos. 2011RC0505, 2011RCZJ15, 2012RC0612, 2011YB01).

REFERENCES

[1] D. Boneh, B. Lynn, H. Shacham, Short signatures from the Weil pairing, in: C.Boyd(Ed.), Advances in Cryptology-Asiacrypt 2001, LNCS, vol. 2248, Springer-Verlag,2001, pp. 514–532.

[2] Huang, X., Mu, Y., Susilo, W., Wong, D.S., Wu, W., 2007. Certificateless signature revisited. Proceedings of ACISP'07.Lecture Notes in Computer Science 4586, 308–322.

[3] H. Du and Q. Wen, "Efficient and provably-secure certificateless short signature scheme from bilinear pairings," Computer Standards and Interfaces 31(2009)390–394.

[4] K. Choi, J. Park, D. Lee, A new provably secure certificateless short signature scheme, Computers and Mathematics with Applications 61(2011)1760-1768.

[5] Miaomiao Tian□, Liusheng Huang, and Wei Yang, "On the security of a certificateless short signature scheme".

[6] Raylin Tso, Xinyi Huang, Willy Susilo , Strongly secure certificateless short signatures, The Journal of Systems and Software 85 (2012) 1409– 1417.

[7] S. Al-Riyami, K. Paterson, Certificateless public key cryptography, in: Proceedings of the Asiacrypt 2003, Taipei, Taiwan, 2003, pp. 452–473.

[8] D. Boneh, B. Lynn, H. Shacham, Short signatures from the Weil pairing, in: C.Boyd(Ed.), Advances in Cryptology-Asiacrypt 2001, LNCS, vol. 2248, Springer-Verlag,2001, pp. 514–532.