SCIENCE CHINA
Information Sciences

• LETTER •

November 2017, Vol. 60 119102:1–119102:3
doi: 10.1007/s11432-015-0367-6

An efficient pairing-free certificateless signature scheme for resource-limited systems

Liangliang WANG[1,3], Kefei CHEN[2,3*], Yu LONG[4] & Huige WANG[4]

[1] *College of Computer Science and Technology, Shanghai University of Electric Power, Shanghai* 200090*, China;*
[2] *School of Science, Hangzhou Normal University, Hangzhou* 310036*, China;*
[3] *Laboratory of Science and Technology on Communication Security, Chengdu* 610041*, China;*
[4] *Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai* 200240*, China*

Received June 30, 2016; accepted August 12, 2016; published online December 14, 2016

Citation Wang L L, Chen K F, Long Y, et al. An efficient pairing-free certificateless signature scheme for resource-limited systems. Sci China Inf Sci, 2017, 60(11): 119102, doi: 10.1007/s11432-015-0367-6

Dear editor,

As certificateless public key cryptography (CL-PKC) [1] is proposed, a number of certificateless public key signature (CL-PKS) schemes [2–6] have been proposed. According to various construction methods, we divide them into three types: pairing-based CL-PKS schemes, elliptic curve cryptography-based (ECC-based) pairing-free CL-PKS schemes and general pairing-free CL-PKS schemes (see Appendix A in the supporting information). On account of the high cost of bilinear pairings operations, pairing-based CL-PKS schemes are not good choices for resource-limited systems. These systems cannot execute complex applications very well due to the limitations of computing resource, storage space and communication bandwidth. Nevertheless, the majority of pairing-free CL-PKS schemes that are more appropriate for resource-limited systems cannot achieve expected security levels, in particular, general pairing-free CL-PKS schemes seem to be rare. In recent years, a general pairing-free CL-PKS scheme was respectively proposed by Harn et al. [2] and Zhang and Mao [3]. Three kinds of adversaries were informally defined in [2] for CL-PKS and a loose security analysis was given for their scheme. He et al. [7] pointed out that the scheme proposed in [3] was insecure against Type I adversary. These two general pairing-free CL-PKS schemes are efficient, but both of them have weaknesses in the aspect of security. Therefore, it remains to be an open problem to construct a general pairing-free CL-PKS scheme, for which a formal security proof can be given under a formal adversary model.

Contribution. In this article, the existing CL-PKS schemes are divided into three types: pairing-based CL-PKS schemes, ECC-based pairing-free CL-PKS schemes and general pairing-free CL-PKS schemes. In addition, an efficient general pairing-free CL-PKS scheme is proposed, which can satisfy the requirements of resource-limited systems and has the following features: (1) When compared with the known general pairing-free CL-PKS schemes, our scheme enjoys a lower computation cost and a shorter signature size (see Appendix C in the supporting information). (2) Our scheme is the only one that possesses provable security against Type I adversary and Type II adversary when compared with the known general pairing-free CL-PKS schemes. (3) The security of our scheme is based on discrete logarithm assumption

* Corresponding author (email: kfchen@hznu.edu.cn)
The authors declare that they have no conflict of interest.

and it is discussed in the random oracle model (ROM) (see Appendix B in the supporting information).

Hard problem. The Discrete Logarithm Problem (DLP) is described as that, a polynomial-time adversary $\mathcal{A}$ tries to find an integer α such that $g^{\alpha} = \beta \bmod p$ for a known element $\beta \in Z_p^*$, where p is a prime and g is a generator of Z_p^*.

We state that the Discrete Logarithm Assumption (DL Assumption) holds, if the success probability of a polynomial-time adversary $\mathcal{A}$ in solving DLP $\mathrm{Succ}_{\mathcal{A}}^{\mathrm{DLP}}$ is negligible, where $\mathrm{Succ}_{\mathcal{A}}^{\mathrm{DLP}} = \Pr[\mathcal{A}(p, g, \beta) \rightarrow \alpha]$.

Certificateless signature scheme. A certificateless signature scheme includes seven probabilistic polynomial-time algorithms.

Setup. This algorithm is a probabilistic algorithm and it is ran by KGC. Given a security parameter l, it returns a list of system parameter params, a master secret key masterkey and a master public key P_{pub}.

Partial-Private-Key-Extract. This algorithm is a deterministic algorithm and it is ran by KGC. Given params, masterkey and a user's identity $\mathrm{ID} \in \{0,1\}^*$, it returns the user's partial private key PS_{ID} and partial public key $\mathrm{PP}_{\mathrm{ID}}$ over a confidential channel.

Set-Secret-Value. This algorithm is a probabilistic algorithm and it is ran by a signer. Given params and the signer's identity ID, it returns the signer's secret value s_{ID}.

Set-Private-Key. This algorithm is a probabilistic algorithm and it is ran by a signer. Given params, the signer's $\mathrm{PS}_{\mathrm{ID}}$ and s_{ID}, it returns the signer's full private key $\mathrm{SK}_{\mathrm{ID}}$.

Set-Public-Key. This algorithm is a deterministic algorithm and it is ran by a signer. Given params and the signer's s_{ID}, it returns the signer's public key $\mathrm{PK}_{\mathrm{ID}}$.

Sign. This algorithm is a probabilistic algorithm and it is ran by a signer. Given params, a message m, the signer's ID and $\mathrm{SK}_{\mathrm{ID}}$, it returns a certificateless signature σ.

Verify. This algorithm is a deterministic algorithm and it is ran by a verifier. Given params, m, σ, the signer's identity ID and $\mathrm{PK}_{\mathrm{ID}}$, it returns 1 or 0. The signature σ is correct if and only if this algorithm returns 1.

Security models of certificateless signature. For construction of CL-PKS schemes, we almost follow Zhang et al.'s security model [6] in which two adversaries interact with a challenger $\mathcal{B}$ in the form of two games to represent the capabilities of adversaries. The concrete interaction games are detailed as follows.

Type I adversary. $\mathcal{A}_{\mathrm{I}}$ serves as an external third party who is not able to possess the master secret key, but is allowed to perform public keys replacement with values chosen by itself.

Type II adversary. $\mathcal{A}_{\mathrm{II}}$ serves as an inner malicious KGC who is allowed to possess the master secret key, but is not able to perform public keys replacement.

Game I. This is the game between $\mathcal{A}_{\mathrm{I}}$ and $\mathcal{B}$.

Setup. $\mathcal{B}$ first takes l as input and runs Setup to obtain masterkey and params, then $\mathcal{B}$ gives params to $\mathcal{A}_{\mathrm{I}}$ and keeps masterkey secret.

Partial private key queries. On receiving ID, $\mathcal{B}$ runs Partial-Private-Key-Extract to obtain PS_{ID} and returns it to $\mathcal{A}_{\mathrm{I}}$.

Private key queries. On receiving an identity ID, the challenger $\mathcal{B}$ first runs the two algorithms Partial-Private-Key-Extract and Set-Secret-Value to obtain PS_{ID} and s_{ID}, then $\mathcal{B}$ runs Set-Private-Key to obtain $\mathrm{SK}_{\mathrm{ID}}$ and returns it to $\mathcal{A}_{\mathrm{I}}$.

Public key queries. On receiving an identity ID, the challenger $\mathcal{B}$ first consecutively runs the algorithms Set-Secret-Value and Partial-Private-Key-Extract to obtain s_{ID} and $\mathrm{PS}_{\mathrm{ID}}$, then $\mathcal{B}$ runs Set-Public-Key to obtain $\mathrm{PK}_{\mathrm{ID}}$ and returns it to $\mathcal{A}_{\mathrm{I}}$.

Public key replacement. For any ID, $\mathcal{A}_{\mathrm{I}}$ is able to replace the original $\mathrm{PK}_{\mathrm{ID}}$ with the new $\widetilde{\mathrm{PK}_{\mathrm{ID}}}$ of its choice.

Signing queries. On receiving ID and m, $\mathcal{B}$ runs Sign to obtain a correct σ with respect to $\mathrm{PK}_{\mathrm{ID}}$ and m and returns it to $\mathcal{A}_{\mathrm{I}}$. Note that $\mathrm{PK}_{\mathrm{ID}}$ may have been replaced in this case.

Output. Finally, $\mathcal{A}_{\mathrm{I}}$ outputs $(\widehat{m}, \widehat{\sigma})$ with respect to $\mathrm{PK}_{\widehat{\mathrm{ID}}}$ for a target $\widehat{\mathrm{ID}}$. Here the identity $\widehat{\mathrm{ID}}$ should fulfill the following requirements: (1) $\widehat{\mathrm{ID}}$ cannot be submitted to the private key oracle. (2) $\widehat{\mathrm{ID}}$ cannot be an identity that is both submitted to the public key replacement oracle and partial private key oracle. (3) $(\widehat{\mathrm{ID}}, \widehat{m})$ cannot be submitted to the signing oracle. (4) $\mathsf{Verify}(\mathrm{params}, \mathrm{PK}_{\widehat{\mathrm{ID}}}, \widehat{m}, \widehat{\mathrm{ID}}, \widehat{\sigma}) = 1$. Note that $\mathrm{PK}_{\widehat{\mathrm{ID}}}$ may have been replaced.

Definition 1. A CL-PKS scheme is existentially unforgeable under Type I adaptively chosen message attacks (EUF-CMA), if $\mathrm{Succ}_{\mathcal{A}_{\mathrm{I}}}^{\text{EUF-CMA}}$ is negligible, where $\mathrm{Succ}_{\mathcal{A}_{\mathrm{I}}}^{\text{EUF-CMA}}$ denotes the success probability of $\mathcal{A}_{\mathrm{I}}$ to win game I.

Game II. This is the game between $\mathcal{A}_{\mathrm{II}}$ and $\mathcal{B}$.

Setup. $\mathcal{B}$ first takes l as input and runs Setup to obtain masterkey and params, then $\mathcal{B}$ gives masterkey and params to $\mathcal{A}_{\mathrm{II}}$.

Private key queries. On receiving an identity ID, the challenger $\mathcal{B}$ first runs the two algorithms Partial-Private-Key-Extract and Set-Secret-Value to obtain $\mathrm{PS}_{\mathrm{ID}}$ and s_{ID}, then $\mathcal{B}$ runs Set-Private-Key to obtain $\mathrm{SK}_{\mathrm{ID}}$ and returns it to $\mathcal{A}_{\mathrm{II}}$.

Public key queries. On receiving an identity ID, the challenger $\mathcal{B}$ first consecutively runs the algorithms Set-Secret-Value and Partial-Private-Key-Extract to obtain s_{ID} and $\mathrm{PS}_{\mathrm{ID}}$, then $\mathcal{B}$ runs Set-Public-Key to obtain $\mathrm{PK}_{\mathrm{ID}}$ and returns it to $\mathcal{A}_{\mathrm{II}}$.

Signing queries. On receiving ID and m, $\mathcal{B}$ runs Sign to obtain a correct σ with respect to $\mathrm{PK}_{\mathrm{ID}}$ and m and returns it to $\mathcal{A}_{\mathrm{II}}$.

Output. Finally, $\mathcal{A}_{\mathrm{II}}$ outputs $(\widehat{m}, \widehat{\sigma})$ with respect to $\mathrm{PK}_{\widehat{\mathrm{ID}}}$ for a target $\widehat{\mathrm{ID}}$. Here the identity $\widehat{\mathrm{ID}}$ should fulfill the following requirements: (1) $\widehat{\mathrm{ID}}$ cannot be submitted to the private key oracle. (2) $(\widehat{\mathrm{ID}}, \widehat{m})$ cannot be submitted to the signing oracle. (3) Verify$(\mathrm{params}, \mathrm{PK}_{\widehat{\mathrm{ID}}}, \widehat{m}, \widehat{\mathrm{ID}}, \widehat{\sigma}) = 1$.

Definition 2. A CL-PKS scheme is existentially unforgeable under Type II adaptively chosen message attacks (EUF-CMA), if $\mathrm{Succ}_{\mathcal{A}_{\mathrm{II}}}^{\text{EUF-CMA}}$ is negligible, where $\mathrm{Succ}_{\mathcal{A}_{\mathrm{II}}}^{\text{EUF-CMA}}$ denotes the success probability of $\mathcal{A}_{\mathrm{II}}$ to win game II.

Our proposed scheme. Our proposed scheme is constructed by the following seven polynomial-time algorithms.

Setup. This algorithm is performed by KGC. Given a security parameter l, randomly pick two different primes p and q which satisfy $q|p-1$. Then randomly pick $g \in Z_p^*$ and $x \in Z_q^*$, and compute $y = g^x \bmod p$, where $g^q = 1 \bmod p$ and $g \neq 1$. Define the master secret key and master public key of KGC as masterkey $= x$ and $P_{\mathrm{pub}} = y$, respectively. Define two hash functions H_1 and H_2 as $H_1 : \{0,1\}^* \times Z_p^* \times Z_p^* \to Z_q^*$ and $H_2 : \{0,1\}^* \times Z_p^* \to Z_q^*$. The system parameters are defined as params $= (p, q, g, P_{\mathrm{pub}}, H_1, H_2)$ and they are considered public known.

Set-Secret-Value. This algorithm is performed by a signer. Given the signer's identity ID, randomly pick $v \in Z_q^*$ as the secret value. Assign $s_{\mathrm{ID}} = v$ and compute $R_{\mathrm{ID}} = g^v \bmod p$. ID and R_{ID} are sent to the KGC.

Partial-Private-Key-Extract. This algorithm is performed by KGC. Given a user's identity ID $\in \{0,1\}^*$ and masterkey, first randomly pick $t \in Z_q^*$ and compute the partial public key as $\mathrm{PP}_{\mathrm{ID}} = g^t \bmod p$. Then use H_1 to compute $e = H_1(\mathrm{ID}, R_{\mathrm{ID}}, \mathrm{PP}_{\mathrm{ID}})$. Continue to compute the partial private key as $\mathrm{PS}_{\mathrm{ID}} = t - xe \bmod q$. Thereafter, $\mathrm{PS}_{\mathrm{ID}}$ and $\mathrm{PP}_{\mathrm{ID}}$ are sent to the user with ID.

Remark. Once the user has received $\mathrm{PS}_{\mathrm{ID}}$ and $\mathrm{PP}_{\mathrm{ID}}$, the user must check whether the equation $g^{\mathrm{PS}_{\mathrm{ID}}} {P_{\mathrm{pub}}}^{H_1(\mathrm{ID}, R_{\mathrm{ID}}, \mathrm{PP}_{\mathrm{ID}})} = \mathrm{PP}_{\mathrm{ID}} \bmod p$ holds. If the equation holds, the user continues to perform the following steps.

Set-Private-Key. This algorithm is performed by a signer. Given $\mathrm{PS}_{\mathrm{ID}}$ and s_{ID}, compute $\mathrm{SK}_{\mathrm{ID}} = s_{\mathrm{ID}} - \mathrm{PS}_{\mathrm{ID}}$. Define $\mathrm{SK}_{\mathrm{ID}}$ as the signer's private key.

Set-Public-key. This algorithm is performed by a signer. Assign $\mathrm{PK}_{1\mathrm{ID}} = R_{\mathrm{ID}}$ and $\mathrm{PK}_{2\mathrm{ID}} = \mathrm{PP}_{\mathrm{ID}}$. Define the signer's public key as $\mathrm{PK}_{\mathrm{ID}} = (\mathrm{PK}_{1\mathrm{ID}}, \mathrm{PK}_{2\mathrm{ID}})$.

Sign. This algorithm is performed by a signer. Given the signer's identity ID, a message m and the signer's private key $\mathrm{SK}_{\mathrm{ID}}$, randomly pick $k \in Z_q^*$ and compute $u = g^k \bmod p$, then use H_2 to compute $h = H_2(\mathrm{ID}, m, u)$, continue to compute $s = k - \mathrm{SK}_{\mathrm{ID}} h \bmod q$. Return (u, h, s) as the signature σ on m and it is sent to a user who potentially is a verifier.

Verify. This algorithm is performed by a verifier. Given the signer's identity ID, m and $\mathrm{PK}_{\mathrm{ID}}$ which are corresponding to σ, use H_1 and H_2 to compute $e' = H_1(\mathrm{ID}, \mathrm{PK}_{1\mathrm{ID}}, \mathrm{PK}_{2\mathrm{ID}})$ and $h' = H_2(\mathrm{ID}, m, u)$. σ is considered as a correct signature corresponding to the signer with identity ID if the equation $g^s {\mathrm{PK}_{1\mathrm{ID}}}^{h'} {P_{\mathrm{pub}}}^{e'h'} = u {\mathrm{PK}_{2\mathrm{ID}}}^{h'} \bmod p$ holds.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61133014, 61572318, 61472114), and Science and Technology on Communication Security Laboratory (Grant No. 9140C110203140C11049).

Supporting information Appendixes A–C. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Al-Riyami S S, Paterson K G. Certificateless public key cryptography. In: Advances in Cryptology-ASIACRYPT 2003. Berlin: Springer, 2003. 452–473

2 Harn L, Ren J, Lin C. Design of dl-based certificateless digital signatures. J Syst Softw, 2009, 82: 789–793

3 Zhang J, Mao J. An efficient rsa-based certificateless signature scheme. J Syst Softw, 2012, 85: 638–642

4 Huang X, Mu Y, Susilo W, et al. Certificateless signature revisited. In: Information Security and Privacy. Berlin: Springer, 2007. 308–322

5 Yap W-S, Heng S-H, Goi B-M. An efficient certificateless signature scheme. In: Emerging Directions in Embedded and Ubiquitous Computing. Berlin: Springer, 2006. 322–331

6 Zhang Z, Wong D S, Xu J, et al. Certificateless public-key signature: security model and efficient construction. In: Applied Cryptography and Network Security. Berlin: Springer, 2006. 293–308

7 He D, Khan M K, Wu S. On the security of a rsa-based certificateless signature scheme. Int J Netw Secur, 2014, 16: 78–80