International Journal of Multimedia and Ubiquitous Engineering
Vol.12, No.3 (2017), pp.75-80
http://dx.doi.org/10.14257/ijmue.2017.12.3.08

Efficient ID-based Rabin Signature without Pairings

Chaoyang Li[1], Xiangjun Xin[2*] and Xiaolin Hua[3]

[1, 2 ,3]*School of Mathematics and Information Science, Zhengzhou University of Light Industry, Zhengzhou 450002, PR China*
E-mail: [1]lichaoyang2013@163.com; [2]xin_xiang_jun@126.com; [3]xl_hua@126.com

Abstract

ID-based signatures can greatly simplify the key management procedures of certificate-based public key infrastructures. In this paper, based on Rabin's cryptosystem, an efficient ID-based signature scheme without pairings is proposed. In our scheme, the hash value of the user's identity is used as his/her public key, while its square root is used as the user's secret key. During either the signing phase or the verification phase of the proposed scheme, only one exponential operation under modular is used. Then, compared with the similar schemes of this kind, our scheme is more efficient. On the other hand, our scheme can be proved to be secure against existential forgery under adaptively chosen identity and message attacks in the random oracle model.

Keywords*: ID-based signature, exponential operation, random oracle*

1. Introduction

In the past few decades, the identity-based public key cryptosystem (ID-PKC) [1] has been researched by many cryptographers. In the ID-PKC, the private key is generated by a trusted authority, while the user's identity is taken as the corresponding public key. For example, the user's name or email can be used as his/her public key, and the system doesn't need any public key certificate. Therefore, ID-PKC can greatly simplify the key management procedures of certificate-based public key infrastructures.

For all the identity-based public key cryptosystems, their security and efficiency are very important. It is desirable to construct a secure and efficient ID-based signature scheme. The first ID-based signature [1] is constructed by RSA problem [2]. In 1991, Chang and Lin [3] proposed an ID-based signature scheme based on Rabin's public key cryptosystem. Unfortunately, their scheme has been proved not secure [4]. In 1989, Lath *et al.* proposed an ID-based signature based on ElGamal signature [5]. But his scheme is inefficient with many exponential operations under modular. Fiat-Shamir signature [6] is very efficient, since it needs less exponential operations under modular. But the size of his signature and the private key are linear with the parameter t or k, where t and k are security parameters, and n is the RSA modular. Recently, many ID-based signature schemes from pairings were proposed [7-13]. Although these schemes were proved to be secure, many pairing operations had to be used in their schemes. It should be noted that the bilinear pairing is regarded as the most expensive cryptography primitive. According to the result in [14], one pairing operation is about 11110 multiplications in finite field F_3^{163}. The relative computation cost of a pairing is approximately twenty times higher than that of the scalar multiplication over elliptic curve group [15, 16]. Therefore, ID-based signature schemes without bilinear pairings would be more appealing in terms of efficiency.

* Corresponding Author

ISSN: 1975-0080 IJMUE

In this paper, based on Rabin's cryptosystem [17], an efficient ID-based signature scheme is proposed. In our scheme, there is not any pairing operation. In fact, in our scheme, during either the signing phase or the signature verification phase, only one exponential operation under modular is used. Comparing with the similar schemes of this kind, our scheme has less exponential operations, so our scheme is more efficient. In addition, by using the forking lemma theorem, we can prove that our scheme is secure against existential forgery under adaptively chosen identity and message attacks in the random oracle model.

The rest of our paper is organized as follows. In Section 2, we propose our ID-based Rabin signature scheme. In Section 3, the security analysis of our scheme is discussed. In Section 4, we make the efficiency comparison among the similar schemes of this kind. In Section 5, we make a conclusion.

2. Our ID-Based Rabin Signature Scheme

In this section, we present our identity-based Rabin signature. The scheme contains four algorithms: Setup, Key Extract, Sign and Verify.

Setup: Let p and q be two large primes, and $p=2p'+1$, $q=2q'+1$, where p' and q' are both large primes, too. Let $N=p\cdot q$ be the RSA modular. Assume it is hard to factor N. On the other hand, $H:\{0, 1\}^* \rightarrow \boldsymbol{Q}_N^*$ and $H_1:\{0, 1\}^*\times\{0, 1\}^*\rightarrow Z_N$ are two secure hash functions, where the $\boldsymbol{Q}_N^*$ is the quadratic residue set under modular N. The public system parameters are N, H, H_1, while the pair (p, q) is used as the master key, which is only mastered by the private key generator (PKG).

Key Extract: Given the user's identity ID, PKG computes $h=H(ID)$ and $S_{ID}=\sqrt{h} \bmod N$. The square root of h can be computed by using Rabin algorithm [18]. Let $g=S_{ID}$. Then, PKG secretly sends g to the user. And g is used as the user's private key.

Sign: Given a message m, the user randomly chooses a number $r\in Z_N$, and computes $t=r^2 \bmod N$, $l=H_1(t, m)$, and

$$s=r\cdot g^l \bmod N \tag{1}$$

Then, the pair (s, t) is the signature of the message m.

Verify: Given the message m and the signature $\sigma=(s, t)$ of the user with identity ID, the verifier computes $h=H(ID)$ and $l=H_1(t, m)$. Then, he/she verifies whether the equation holds. If it holds, the verifier accepts the signature, or he/she refuses it.

$$s^2=t\cdot h^l \bmod N \tag{2}$$

3. Security Analysis

In this section, we prove the security of our ID-based signature scheme in the random oracle model. Here, we adopt the security model for ID-based signature schemes in reference [19]. An ID-based signature scheme is secure against existential forgery on adaptively chosen message and ID attacks, if no polynomial time algorithm A has a non-negligible advantage against a challenger C in the following query-respond game:

(1) C runs Setup algorithm of the scheme. Then, the system parameters are sent to A.

(2) A issues the following queries by his decision:

(a) A queries the hash function. C computes the value of the hash function, and sends it to A.

(b) A queries the Extract algorithm. Given the identity ID, C runs the Extract algorithm to obtain the private key corresponding to the ID, and sends it to A.

(c) A queries the Sign algorithm. Given the identity ID and a message m, C sends a signature obtained by running Sign to A.

(3) *A* outputs (*ID*, *m*, σ), where *ID* is an identity, *m* is a message, and σ is a signature, such that *ID* and (*ID*, *m*) are not equal to the inputs of any query to Extract and Sign, respectively. *A* wins the query-respond game if σ is a valid signature on *m* for identity *ID*.

Suppose the adversary has a polynomial-time algorithm α that can break our scheme with non-negligible advantage ε, and H, H_1 are two random oracles. Let *C* be the challenger. Then, we prove our signature scheme is secure against existential forgery under adaptively chosen identity and message attacks in the random oracle model.

Definition 1 A forger α (t, q_s, q_h, ε)-breaks a signature scheme if α runs in time at most t, and makes at most q_s signature queries, and at most q_h queries to the hash functions, and the probability that α wins the query-respond game is at least ε. A signature scheme is (t, q_s, q_h, ε)-existentially unforgeable under an adaptively chosen identity and message attacks if there exists no forger that can (t, q_s, q_h, ε)-break it.

On the other hand, in our security proof, the forking lemma [18] is used. In a generic signature scheme, the signature on *m* can be seemed as a triple (σ_1, h, σ_2), where σ_1 randomly takes its values in a large set, and h is the hash value of (m, σ_1). σ_2 is dependent on the values of σ_1, m and h.

Lemma 1. [Forking Lemma] [18] In the random oracle mode, for a generic signature scheme, let *F* be a Turing machine whose input only consists of public data. Assume that *F* can produce a valid signature (m, σ_1, h, σ_2) within a time bound T by un-negligible probability $\varepsilon \geq 10(n_s+1)(n_h+n_s)/q$, where n_h and n_s are the numbers of queries that *F* can ask to the random oracle and the signing oracle respectively. If the triple (σ_1, h, σ_2) can be simulated without knowing the secret key, with an indistinguishable distribution probability, then there is another machine which has control over the machine obtained form *F* replacing the signing oracle by simulation, and produces two valid signatures (m, σ_1, h, σ_2) and (m, σ_1, h', σ'_2) such that $h \neq h'$ in the expected time less than $120686 \cdot n_h \cdot T/\varepsilon$.

Theorem 1. In the random oracle model, for our identity based signature scheme, let the adversary have a polynomial-time algorithm α that can produce a valid signature (s, t, *ID*) within a time bound T by un-negligible probability $\varepsilon \geq 10(q_s+1)(q_H+q_{H1}+q_s)/q$, where q_H and q_{H1} are the numbers of queries that α can ask to the random oracles H and H_1, respectively, and q_s is the number of queries that α can ask to the signing oracle. If the signature (s, t, *ID*) can be simulated without knowing the private key, with an indistinguishable distribution probability, then there is another machine which can solve the factoring problem in the expected time less than $120686 \cdot (q_H+q_{H1}) \cdot T/\varepsilon$.

Proof. First, *PKG* setups the system parameters {p, q, N, H, H_1,} as those described in the Setup phase in Section 2. The factors p and q of modular N are only mastered by *PKG*. The hash functions H and H_1 can be seemed as two random oracles. The challenger *C* doses not know any factor of the modular N. But, the goal of the challenger *C* is to factor the modular N. In the following query-respond game, the polynomial-time algorithm α can query all the oracles adaptively. Each query is unique.

***H* Query:** Upon receiving an H query for the identity ID_i from α, *C* checks the list $list_H$ maintained by him/her. If (S_{ID_i}, h_i, ID_i) already exists in the list $list_H$, *C* directly returns h_i to α. Otherwise, *C* randomly chooses a number $S_{ID_i} \in Z_N$, computes $h_i = S_{ID_i}^2 \bmod N$, and returns h_i to α. After that, the triple (S_{ID_i}, h_i, ID_i) is added into the list $list_H$.

***H*$_1$ Query:** Upon receiving a H_1 query for the pair (m_i, t_i) from α, *C* checks the list list_{H_1} maintained by him/her. If (l_i, m_i, t_i) already exists in the list list_{H_1}, *C* directly returns l_i to α. Otherwise, *C* randomly chooses a number $l_i \in Z_N$, and returns it to α. After that, *C* adds (l_i, m_i, t_i) into the list list_{H_1}.

Key-Extract Query: Upon receiving the key-extraction query for ID_i, C executes the H Query, and checks the list $list_H$ to obtain S_{ID_i} corresponding to identity ID_i. Then, C returns it to α.

Signing Query: Upon receiving a signing query for a user with identity ID_i on some message m_i, C executes the Key Extract Query for ID_i to obtain the triple (S_{ID_i}, h_i, ID_i). Then, he/she randomly chooses a number $r_i \in Z_N$, and computes $t_i = r_i^2 \bmod N$. Next, C executes the algorithm H_1 Query for m_i, and obtains the triple (l_i, m_i, t_i). So, he/she computes $s_i = rg^{l_i} \bmod N$, where $g=S_{ID_i}$. Last, C returns the signature $\sigma_i=(s_i, t_i)$ to α. It is easy to know that σ_i can pass the signature verification.

From the simulation game, the challenger can successfully answer all the queries without being detected. α cannot distinguish the simulation from real life because the hash functions behave as random oracles. Then, α believes that he/she has attacked our scheme as he/she wished, and will forge a valid signature with non-negligible advantage ε. Note that l is the hash value of (t, m), and l only depends on t and m. Then, from lemma 1, we know that there is another machine which has control over the machine obtained form α replacing the signing oracle, and produces two valid signatures (s, t) and (s*, t) for the target user with identity ID such that $l \neq l$*, where

$$s^2 = t \cdot h^l \bmod N \tag{3}$$

$$s^{*2} = t \cdot h^{l^*} \bmod N \tag{4}$$

and $h=H(ID)$. Note $h=g^2 \bmod N$. Then, from the equations (3) and (4), we can get

$$\left(\frac{s}{s^*}\right)^2 = \left(g^{l-l^*}\right)^2 \bmod N \tag{5}$$

Then, we can derive $\left(\frac{s}{s^*} - g^{l-l^*}\right)\left(\frac{s}{s^*} + g^{l-l^*}\right) = 0 \bmod N$. Therefore, the integer N can be factored.

From Theorem 1, we can get Theorem 2 as follow.

Theorem 2. Under the hardness assumption of factoring problem, our signature scheme can achieve existential unforgeability against adaptively chosen identity and message attacks.

4. Efficiency Comparison

In an ID-based signature scheme under modular, the exponential operation is the most time-consuming compared with the other operations. Then, to compare the efficiency among different ID-based signature schemes under modular, we mainly choose the exponential operation. In this part, to compare with the similar schemes, we consider the exponential operations in the signing phase and signature verification phase as the main indexes. The results are shown in the following table.

Table 1. Efficiency Comparison of the Similar Schemes

Schemes	Exponential operations	
	Signing phase	Signature verification phase
[1]	2	2
[3]	2	1
[5]	1	3
Our scheme	1	1

As shown in the **Table 1**, compared with the schemes in [1, 3], our scheme has less exponential operations in the signing phase. Comparing with the schemes in [1, 5], our scheme has less exponential operations in the signature verification phase. Therefore, our scheme will need less time consuming, and our scheme is more efficient than the other schemes of this kind.

On the other hand, Fiat and Shamir [6] proposed an ID-based signature scheme without any exponential operations. But in [6], during both of the signing phase and signature verification phase, $(k+1)t$ multiplication operations are used, where k and t are security parameters. The sizes of the Fiat-Shamir signature and its private key is about $t(k+\log n)$ and $k\log n$ bits, respectively, where n is the RSA modular. Then, the sizes of Fiat-Shamir signature and its private key are linear with the parameter t or k. Hence, comparing with the scheme of [6], our signature has the fixed and shorter length.

5. Conclusion

We have presented an efficient pairing-free ID-based signature scheme based on Rabin's cryptosystem. And we have proved that our scheme is secure against existential forgery under adaptively chosen identity and message attacks in random oracle model. The security of our scheme is based on factoring problem. Additionally, during either the signing phase or the verification phase of the proposed scheme, only one exponential operation under modular is used. Therefore, comparing with the previous similar schemes, our scheme is more efficient.

Acknowledgements

This work is supported by the Natural Science Foundation of China (Grant No. 61272525), the Foundation for Doctors of Zhengzhou University of Light Industry (NO. 20080014), and the Fundamental and Advanced Technology Research Project of Henan province (Grant No. 152300410129).

References

[1] A. Shamir. "Identity based cryptosystems and signature schemes", Advances in cryptology (Santa Barbara, Calif.), **(1984)**, pp. 47-53.
[2] R. L. Rivest, A. Shamir, and L. Adleman. "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, 21, no.2, **(1978)**, pp. 120–126.
[3] C. C. Chang, C. H Lin. "An ID-based signature scheme based upon Rabin's public key cryptosystem", Proceedings. 25th Annual 1991 IEEE International Carnahan Conference on Security Technology, **(1991)**, pp. 139-141.
[4] M. Y. Ko, T. Hwang and C. C. Chang. "Attacks on ID-based Signature Scheme Based upon Rabin's Public Key Cryptosystem", Computer communications, vol. 17, **(1994)**, pp.674-676.
[5] C. S. Lath, J. Y. Lee, L. Harn, C. H. Chen. "A new scheme for ID-based cryptosystem and signature", Proceedings of the Eighth Annual Joint Conference of the IEEE Computer and Communications Societies. Technology: Emerging or Converging, IEEE INFOCOM '89, **(1989)** April 23-27.
[6] A. Fiat, A. Shamir. "How to prove yourself: practical solutions to identification and signature problems", Advances in Cryptology-CRYPTO'86, (Santa Barbara, Calif.), **(1986)**, pp.186-194.
[7] C. J. Cha, J. H. Cheon. "An Identity-based Signature from Gap Diffie-Hellman Groups", Public Key Cryptography, **(2003)**, pp. 18-30.
[8] J Xu, Z. Zhang, and D. Feng. "ID-based Proxy Signature Using Bilinear Pairings", ISPA Workshops 2005. Berlin: Springer-Verlag, **(2005)**, pp. 359-367.
[9] F. Hess. "Efficient Identity Based Signature Schemes Based on Pairings", SAC 2002. Berlin: Springer-Verlag, **(2003)**, pp. 310-324.
[10] K. G. Paterson. "ID-based Signatures From Pairings on Elliptic Curves", Electronics Letters, 38(1), **(2002)**, pp. 1025-1026.
[11] Z. Huang, K. Chen and Y. Wang. "Efficient Identity-based Signatures and Blind signatures", CANS 2005. Berlin: Springer-Verlag, **(2005)**, pp. 120-133.
[12] K. A. Shim. "An ID-based aggregate signature scheme with constant pairing computations", Journal of Systems and Software, 83(10), **(2010)**, pp. 1873–1880.

[13] S. H. Islam and G. P. Biswas. "Provably Secure and Pairing-Based Strong Designated Verifier Signature Scheme with Message Recovery', Arabian Journal for Science and Engineering, 40(4), **(2015)**, pp. 1069-1080.
[14] F. Zhang, R. Safavi-Naini, W. Susilo. "An efficient signature scheme from bilinear pairings and its applications", Public Key Cryptography, **(2004)**, pp. 277-290.
[15] L. Chen, Z. Cheng, N. P. Smart. "Identity-based key agreement protocols from pairings", International Journal of Information Security, 6(4), **(2007)**, pp. 213–241.
[16] D. He, J. Chen and J. Hu. "An ID-based proxy signature schemes without bilinear pairings", Annals of Telecommunications, 66(11), **(2011)**, pp.657–662.
[17] M. O. Rabin, "Digitalized signatures and public key cryptosystems as intractable as factorization", Technical Report MIT/LCS/TR-212, MIT, Cambridge, MA**(1979)**.
[18] D. Pointcheval and J. Stern. "Security arguments for digital signatures and blind signatures", Journal of Cryptology, vol. 13, no. 3, **(2000)**, pp. 361−369.
[19] J. C. Cha, J. H. Cheon. "An identity-based signature from gap Diffie-Hellman groups", Public Key Cryptography, **(2003)**, pp. 18-30.

Authors

Chaoyang Li, He is now a postgraduate in the School of Mathematics and Information Science, Zhengzhou University of Light Industry, Zhengzhou, China. His recent research interests include cryptography and network security.

Xiangjun Xin, he received his Ph.D. degree in Cryptography from Xidian University in 2007. He is now an associate professor in the School of Mathematics and Information Science, Zhengzhou University of Light Industry, Zhengzhou, China. His recent research interests include cryptography and network security.

Xiaolin Hua, She is now a postgraduate in the School of Mathematics and Information Science, Zhengzhou University of Light Industry, Zhengzhou, China. Her recent research interests include cryptography and network security.

