Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Engineering 29 (2012) 2214 – 2218

Procedia Engineering

www.elsevier.com/locate/procedia

2012 International Workshop on Information and Electronics Engineering (IWIEE)

Online/Offline Blind Signature

JIANG Hua[a]*, HU Ran-dong[b]

[a]*Network Information Center, Guilin University of Electronic Technology, Guilin, 541004, China*
[b]*School of Computer Science and Engineering, Guilin University of Electronic Technology, Guilin, 541004,China*

Abstract

The processing ablity and response speed of the wireless communication terminals are limited, common signatures become the bottleneck to the development of the wireless networks. For that problem, based on the characteristics of the blind signature, the online/offline blind signature is given in this paper which incorporates with the optimal online/offline signature. Most computations are finished before the blind message is given, after that, only a few operations are needed. The performance analysis is also given in this paper, the new signature scheme can be applied to the security of wireless network, it protect the users' privacy efficiently.

Keywords: bilinear map; online/offline signature; blind signature

1 Introduction

Digital signature schemes play an important role in information security and have exhibited many applications. However, the computation of signature requires a private computer with a reasonable computation power. In practice, there could be a situation, where such a computer is not availabe.

In order to further reduce the computational cost of signature generation, online/offline signature is preferable in wireless network. Even, Goldreich and Micali proposed a general method for converting any signature scheme into an online/offline signature scheme.The signature can divided into two parts which are the offline signatre and the online signatre. In the process of the offline signature, almost all of the calculations are done before the blind message is given. And in the following process of the online signature, only small quantities of computations are needed after the blind message is available. However, the method is impratical since it increases the size of the signature by a quadratic factor. Later, Shamire[1] proposed a new method called 'hash-sign-swich' for designing more efficient schemes.The calculation of

* JIANG Hua. *E-mail address*: jianghua0773@126.com

doi:10.1016/j.proeng.2012.01.290

online phase is one tenth of the modular multiplication. The scheme can resist the chosen message attack but has a problem of the trapdoor leak. Chen[2] proposed a online/offline scheme with double trapdoor hash functions, which can solve the problem of trapdoor leak. Harm[3] introduce the trapdoor function of multi collision in online/offline signature which can sign a variety of message. Gao[4] proposed a scheme which can directly convert the trapdoor hash functions into online/offline signatures. The whole computation in Gao's scheme is half of the computation in Shamir's scheme. Girault proposed GPS scheme[5] in which the length of secret key is short and the operation in online phase is on the integers not the modular calculation, so its efficiency is more efficient than Shamir's scheme. Chevallier-Mames and Joye respectly put forward their schemes in[6][7], which efficiency is the same to the GPS. Guo[8] proposed the optimal online/offline signature which is more efficient than GPS's scheme.

Blind signature[10][11][12] is a special digital signature for the signer doesn't know the specific content of the document. The technology of blind signature has been used widely(e.g. the electronic voting system, electronic cash system, etc.). The blind signature was first proposed by Chaum ,which is to make the signature to sign for the blind messsage. The blind signature can protect the uers' privacy for the signer doesn't know the original message and the signer cannot link up the signature with the original message.

Based on the opimal online/offline signature in Guo's scheme, a new scheme proposed in this paper which can convert blind signature into online/offline blind signature that can effectly protect the users' and the merchants' privacy.

2 Related works

2.1 Bilinear Map

Let G and G_T be two cyclic groups of prime order p. Let g be a generator of G. A map e: $G\times G\rightarrow G_T$ is called a bilinear map if this map satisfies the following properties:

(1) Bilinear: for all u, v$\in$G, a,b$\in Z_q$, we have $e(u^a,v^b)=e(u,v)^{ab}$.

(2) Non-degeneracy: g is the generator of G, then $e(g,g)\neq 1$.

(3) Computability: It is efficient to compute e(u,v) for all $u,v\in G$.

2.2 Blind message

User dispose the original message M into $\overline{M}$ called blind message and give it to the signer. For example, randomly choose an integer d, set $\overline{M}$ =dM, the integer d is called blind factor. As the signer does not know the blind factor, the message is blind to signer.

2.3 basic online/offline signature

Definiton 1: Guo proposed basic online/offline signature which based on Water's scheme of signature[9].The security of Guo's signature is attributed to the GDH problem. Here we call it on/offline-w scheme which can be described as follows:

Initialize: Run the system and output q,e,G,G_T and bilinear map $e:G\times G\rightarrow G_T$, the prime order of G is q and the generator is g. And u_0, (u_{10},u_{11}), (u_{20},u_{21}), ⋯ , (u_{n0},u_{n1}) are the other random generators. The public params are defined as the following tuple:

params={e, q, G, G_T, u_0, (u_{10},u_{11}), (u_{20},u_{21}), ⋯ , (u_{n0},u_{n1})}.

KeyGen: Randomly choose an integer $\beta\in Z_q$, and compute the secret key SK = g^β, the public key PK= $e(g^\beta,g)$.

Sign: The signing is divided into the offline phase for pre-computation and the online phase . Compute most computations in offline phase and store the offline datas which are as the outputs of online phase.

Offline phase: Signer input the secret key and params.

(1)Randomly choose two n-length vectors ($\mu_1,\cdots,\mu_n$) and ($\nu_1,\cdots,\nu_n$), such that

（$\mu_1+\cdots+\mu_n$）=($\nu_1+\cdots+\nu_n$)=1(mod q)

(2)Randomly choose $r \in Z_q$, compute $\tau = g^r$ and the following 2n values:

$$(s_{i0}, s_{i1}) = (g^{\mu_i\beta}(u_0^{\nu_i}u_{i0})^r, g^{\mu_i\beta}(u_0^{\nu_i}u_{i1})^r \text{ , for i=1,2,}\cdots\text{,n;}$$

(3)Store the following 2n+1 elements:

$$w=((s_{10},s_{11}),\cdots,(s_{i0},s_{i1}),\tau)$$

Online phase:Given the message $M \in \{0,1\}^n$, let M[i] be the ith bit of M, the signature is generated as follows:

(1)compute $s = \prod_{i=1}^{n} s_{iM[i]} = \prod_{i=1}^{n} g^{\mu_i\beta}(u_0^{\nu_i}u_{iM[i]})^r = g^{\beta}(u_0\prod_{i=1}^{n}u_{iM[i]})^r$

(2)output the last signature (s,τ).

Verify: input (M,s,τ), accept the signature if the following equation holds

$$e(s,g) = e(g^{\beta}, g)e(u_0\prod_{i=1}^{n}u_{iM[i]}, \tau)$$

3 Our scheme

3.1 Model of the scheme

Definitions 2: The model of our scheme contains the following several parts: Setup, KeyGen, Blind, Sign, Verify. Here the signature that we construct is called online/offline-b-s scheme which can be described as the following.

Initialize: Output public params.

KeyGen: Input public params, and output public key and the secret key.

Blind: User converts the original message M into the blind message $\tilde{M}$ and then transfer it to the signer.

Sign: This algorithem is divided into two phases:

Offline phase: Input the secret key and public params, output the offline-datas and strore them.

Online phase: Input the blind message $\tilde{M}$ and the datas in offline phase, after some simple computations, output the signature on the blind message. And the last signature is a set of the signature and some related coefficients.

Verify: Input the original message M and the last signature, if the equation holds and then accept the signatue.

3.2 Scheme construction

Setup: run the system, h is a strong hash function without collision, h: $\{0,1\}^* \times Z_q \to \{0,1\}^n$ .G and G_T are cyclic groups of prime order q, g and u_0 are the generators of G, randomly choose n different pairs of generators of G : $(u_{10},u_{11}),(u_{20},u_{21}),\cdots,(u_{n0},u_{n1})$. Output the public params:

params={e,q,G,G_T,g,u_0,$(u_{10},u_{11}),\cdots,(u_{n0},u_{n1})$}

KeyGen: Randomly choose integer $\beta \in Z_q$, compute the secret key g^{β} , and $e(g^{\beta}, g)$ as the public key.

Blind: User randomly choose integer $d \in Z_q$, compute $\tilde{M} = h(M, d)$.

Sign: The two phases are the offline phase and the online phase.

Offline phase: the blind message is not given.

(1) Randomly choose two n-length vectors $(\mu_1,...,\mu_n) \in Z_q$ and $(\nu_1,...,\nu_n) \in Z_q$,such that $(\mu_1 + ... + \mu_n) = (\nu_1 + ... + \nu_n) = 1 (\mathrm{mod}\, q)$

(2) Randomly integer $r \in Z_q$, compute $\tau = g^r$ and the other 2n values of offline phase $(s_{i0}, s_{i1}) = (g^{\mu_i \beta} (u_0^{\nu_i} u_{i0})^r, g^{\mu_i \beta} (u_0^{\nu_i} u_{i1})^r)$, for i=1,2,⋯,n.

(3) Store the offline-datas w=((s10,s11),⋯,(sn0,sn1), τ)

Online phase: after the blind message $\overline{M}$ is given, $\overline{M} \in \{0,1\}^n$, $\overline{M}[i]$ is the ith bit of $\overline{M}$.

(1) In accordance with $\overline{M}[i]$, choose $s_{i\overline{M}[i]}$ from w, and then compute signature $s = \prod_{i=1}^{n} s_{i\overline{M}[i]}$

(2) Output the last signature (M,τ,d,s).

Verify: Input (M,τ,d,s), and check the equation.

(1) Compute $M_0 = h(M,d)$, $M_0[i]$ is the ith bit of M_0 .

(2) Accept the signature if the equation holds: $e(s,g) = e(g^{\beta}, g) e(u_0 \prod_{i=1}^{n} u_{iM_0[i]}, \tau)$

4 Performance analysis and application

4.1 Performance analysis

Blind: The message that signer receives is the blind message $\overline{M}$ not the original message M, so the message is blind to him. It is impossible to regain the original message M from the blind message $\overline{M}$ for $\overline{M} = h(M,d)$, and not only the blind factor d is unknown to the signer but also the hash function is irreversible. Even if the original message M is published, the signer cannot make association with M and $\overline{M}$, and then cannot make association the signature with M.

Verifiability: Given the message M and (τ,d,s), and compute e(s,g) whose expansions are as the following:

$$e(s,g) = e(\prod_{i=1}^{n} s_{i\overline{M}[i]}, g) = e(\prod_{i=1}^{n} g^{\mu_i \beta} (u_0^{\nu_i} u_{i\overline{M}[i]})^r, g)$$

$$= e(g^{(\mu_1 + ... + \mu_n)\beta} (u_0^{(\nu_1 + ... + \nu_n)} \prod_{i=1}^{n} u_{i\overline{M}[i]})^r, g)$$

$$= e(g^{\beta} (u_0 \prod_{i=1}^{n} u_{i\overline{M}[i]})^r, g) = e(g^{\beta}, g) e((u_0 \prod_{i=1}^{n} u_{i\overline{M}[i]})^r, g)$$

$$= e(g^{\beta}, g) e(u_0 \prod_{i=1}^{n} u_{i\overline{M}[i]}, g^r) = e(g^{\beta}, g) e(u_0 \prod_{i=1}^{n} u_{i\overline{M}[i]}, \tau)$$

after neaten the expansions, we get that: $e(s,g) = e(g^{\beta}, g) e(u_0 \prod_{i=1}^{n} u_{i\overline{M}[i]}, \tau)$.

Compute $M_0 = h(M,d)$, if the signature is effective, M_0 and $\overline{M}$ are same, the M[i] and $M_0[i]$ are same. Then we have the following equation:

$$e(s,g)=e(g^{\beta},g)e(\mathrm{u}_0\prod_{i=1}^{n}u_{i\,M[i]},\tau)=e(g^{\beta},g)e(\mathrm{u}_0\prod_{i=1}^{n}u_{i\,M_0[\mathrm{i}]},\tau)$$

4.2 Efficiency and application

In our online/offline-b-s scheme, as most computations have been done in offline phase, so we only analysis the efficiency in online phase. Different from other online/offline signatures, the computation is only the simple multiplication not the exponentiation.

Our online/offline-b-s can be applied to the wireless network with that the computational capabilities are limited, the scheme can effectively solve the drawback of the wireless terminals in communication. In the offline phase, the computations are done on the terminals with strong processing capacity or in the time when the terminals are vacant. Only a few simple computations are needed after message is given. And online/offline-b-s is also a kind of blind signature, the signer cannot know the content in ocument, so the secret information is protected, for which reason the scheme can applied to the Wireless Mobile Internet(e.g. the wireless e-voting system and e-cash system,etc.).

5 Conclusion

The online/offline-b-s is high-efficiency, and the essence of blind signature is that the signer doesn't know the original content of the message. In the fields where the time of message-signing is limited and the computational capability is weak(e.g. wireless sensor network), the scheme is practicable. The future work is to design more secure and more efficient online/offline signature.

References

[1]A.Shamir and Y.Tauman. Improved online/offline signature schemes. In CRYPTO,pages:47-53,2001

[2]X. Chen, F. Zhang, W. Susilo, and Y. Mu.Efficient generic on-line/off-line signatures Without key exposure. In ACNS, pages:18-30,2007.

[3]L.Harm, W.-J. Hsin, and C.Lin. Efficient On-line/Off-line Signature Schemes Based on Multiple-Collision Trapdoor Hash Families.The Computer Journal, 2009.

[4]C. zhi Gao and Z. an Yao. A further Improved online/offline signature schemes.In CRYPTO, pages:47-53,2009.

[5]M. Girault, G. Poupard, and J.Stern. On the fly authentication and signature schemes Based on Multiple-Collision Trapdoor Hash Families. The Computer Journal, 2009

[6]B. Chevallier-Mames and M. Joye. A Pratical and tightly secure signature scheme without hash function. In CT-RSA, pages:339-356,2007.

[7]M. Joye. An efficient on-line/off-line signature scheme without random oracles. In CANS, pages 98-107,2008

[8]GUO Fu-chun, MU Yi. Optimal online/offline signature: how to sign message without online computation[C]. Proc of the 2nd International Conference on Provable Security. Berlin/Heidelberg: Springer Verlag,2008:98-111.

[9]WATERS B. Efficient identity-based encryption without random oracles.[C]. Proc of ROCRYPT.[s.l.]: Springer verlag,2005:114-127.

[10]Masayuki Abe and Eiichiro Fujisaki. How to date blind signatures.[C].Lecture Notes in Computer Science,1996:244-251

[11]Hyung-Woo Lee and Tai-Yun Kim. Message Recovery Fair Blind Signature.[C].Lecture Notes in Computer Science,1999:632

[12]Sanjam Garg, Vanishree Rao, Amit Sahai. Round Optimal Blind Signature.[C].Lecture Notes in Computer Science.2011,pages: 630-648