ELSEVIER

Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Engineering 15 (2011) 2103 – 2107

Procedia Engineering

www.elsevier.com/locate/procedia

Advanced in Control Engineering and Information Science

A Kind of Message-recoverable Fairness Blind Digital Signature Scheme

Jian-shi Zhang a*

College of Computer Science and Technolog, Jilin University, Changchun, China

Abstract

Blind digital signature indeed protects interests of the participants to some extent, but the anonymity of blind digital signature present exploit opportunities to attackers. Aiming at problems of current fairness blind digital signature schemes can not simultaneously guarantee completely fairness and can not recover message, the paper proposed a kind of message-recoverable fairness blind signature scheme and analyzed its correctness, security and fairness. The analysis results show that the just can authorize user's identity and correspond it to original signature message with this scheme, and the user can not forge fairness information of just.

Selection and/or peer-review under responsibility of [CEIS 2011]

Keywords: blind digital signature; fairness; message recoverable

1. Introduction

With widespread use of computer network, electronic mail, electronic payment systems and automation system, the digital signature problem become more prominent. In general sense, public key cryptography and private key cryptography can all build digital signature scheme. Early digital signature was completed with traditional keys, which is very complicated and difficult to achieve same effect with

* Corresponding author. Tel.:+8613341593377
E-mail address: cindazjs@sina.com.

doi:10.1016/j.proeng.2011.08.393

hand signature. Since the advent of public key cryptography, digital signature technology has matured and has been applied. In a written signature, the signature and file contents are separated from each other. While in digital signature, digital signature and signature file content can be separated from each other, or be separated. In other words, the signature file content and signature formed a whole. According to whether message can be recoverable of digital signature scheme, the digital signature can be divided into digital signature without recoverable message and that with recoverable message.

Blind signature is a new signature system introduced by Chaum in Crypto' 83 [1]. It has two characteristics, one is that the message content is blind to signer; the other is that after signature was leaked by receiver, the signer can not track signature. In case of signature, the receiver firstly blind message with blind transformation. The signer signed blinded message and sent back to receiver. The receiver then transformed the signed information with verse transformation of blind transformation to obtain signed information of original message. In order to prevent abuse of anonymity of blind signature, [2] introduced concept of fairness blind digital signature, which means the signature is still blind to signer, but it can be tracked through trusted third party. Three kinds of fairness blind signature schema were proposed in [2]. The first scheme achieved fairness of blind signature with the method of segmentation selection, which has large computation but not relatively high practical value. The second scheme constructed fairness blind signature with forgetful transportation protocol. Ref. [3] referred that the scheme can not completely guarantee fairness in some cases. The third scheme did not provide message recovery function. Aiming at this, we presented a kind of message-recoverable fairness blind signature scheme. The paper is organized as follows: Section 2 provides fairness blind digital model to guide message-recoverable blind signature scheme design; Section 3 designs message-recoverable fairness blind digital signature scheme and analyzes on its correctness, fairness and security; Section 4 concludes our work.

2. Fairness Blind Digital Signature Model

The fairness blind digital signature scheme of Stadler includes algorithms (*RKG*, *SKG*, *IP*, *Ver*, *R*).

-*RKG* is undo key generation algorithm, which is used to generate undo key randomly.

-*SKG*, *IP*, *Ver* are blind signature algorithm. If there is no corresponding undo key, it is general blind signature algorithm.

-$R(x_R, \ldots)$ is undo algorithm.

The algorithm has the following one or two characteristics:

(1) If information of signer was given, the just enable signer connecting blind signature message and original signature message.

(2) If the message to sender and received was given, the just can enable signer recognize message pair. The just can connect blind signature and original signed message through undo protocol, so as to track signed message if necessary and effectively prevent payment and secondary consuming of illegal users [4, 5]. The fait blind signature model is shown in Fig. 1.

3. Message-recoverable Fairness Blind Signature Scheme

3.1. Scheme Description

The message-recoverable fairness blind digital signature scheme can be described through the following process as parameter setting, registering, sign and others.

(1) System parameters

The system parameters include finite field F_q, elliptic curve E defined on F_q, $\#E(F_q)$ to represent order of elliptic curve, large prime number *p*, base point $G \in E(F_q)$ and $|G| = p$. Then we can represent $D = (q, FR, E, G, p, h)$. H is hash function with strong collision.

(2) System composition

The system consists of (*Reg*, *Sig*, *Ver*), where *Reg* is the register algorithm of user to just; *Sig* is the signature algorithm and *Ver* is the verification algorithm. If there is no undo algorithm, the *Sig* algorithm is a general blind signature.

(3) System users

Just *TC*, the public key and private key of which are x_{TC} and $Q_{TC} = x_{TC}G$.

Signer *Alice*, the public key and private key of which are x_A and $Q_A = x_A G$.

User *Bob*.

(4) Registration process

Step 1: The *TC* randomly select $a, b, c \in [1, p-1]$ and compute:

$R_1 = aG + bG$, $R_2 = cG$; $r_0 = H(R_1, R_2)$ and $s_0 = c + rx_{TC}$.

Then *TC* send (a, b, s_0, r_0) to *Bob* in secrete way.

Step 2: After *Bob* received (a, b, s_0, r_0), he immediately compute $R' = s_0 G - r_0 Q_{TC}$ and $R'' = aG + bG$, and then to verify $r_0 = H(R'', R')$. If the equation is satisfied, store (a, b, s_0, r_0). The *TC* stores (ID_B, a, b, s_0, r_0).

(5) Signature process

Step 1: *Bob* computes $Q_1' = aG$ and $Q_2' = bG$, and then sends (Q_1', Q_2', s_0, r_0) to the signer *Alice*.

Step 2: After *Alice* received (Q_1', Q_2', s_0, r_0), she computes $Q_0 = s_0 G - r_0 Q_{TC}$ and verify $r_0 = H(Q_1' + Q_2', Q_0)$. After verification, she will send r_0 to *TC* to verify whether r_0 comes from *TC*.

After verification of *TC*, *Alice* randomly selects $k \in [1, p-1]$ and computes $Q_1 = kaQ_1'$ and $Q_2 = x_A b Q_2'$. Then she will send (Q_1, Q_2) to *Bob*.

Step 3: After *Bob* received (Q_1, Q_2), he computes:

$Q = Q_1 + aQ_2 + abG = (x, y)$

$r' = x \bmod p$

$r = r' + m \bmod p$

$m^* = ra^{-1} + b \bmod p$

Then he sends *m** to *Alice*.

Step 4: After Alice received *m**, she computes $s' = k + m^* x_A \bmod p$ and sends *s*' to *Bob*.

Step 5: After Bob received *s*', he computes $s = (s' + b)a \bmod p$.

So (*r*, *s*) is the signed message about *m*.

(6) Verification

$sG - rQ_A = (x, y)$

$r' = x \bmod p$

$m = r - r' \bmod p$

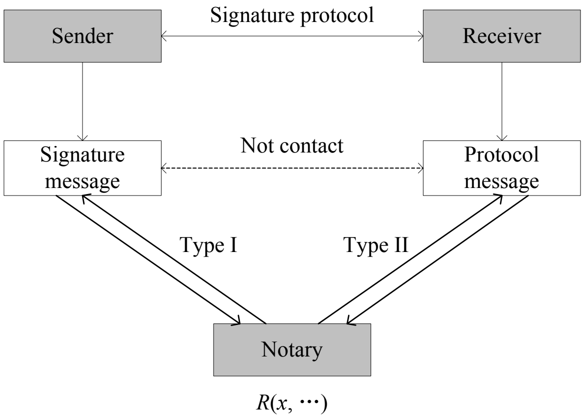

Fig. 1. Fairness blind signature model.

3.2. Scheme Analysis

(1) Correctness analysis

$$
\begin{aligned}
sG - rQ_A &= (s'+b)aG - rQ_A \\
&= (k + (ra^{-1} + b)x_A + b)aG - rQ_A \\
&= (ka + rx_A + abx_A + ab)G - rQ_A \\
&= kaG + abQ_A + abG = (x, y)
\end{aligned}
$$

$r' = x \bmod p$

$m = r - r' \bmod p$

(2) Fairness analysis

In the scheme, the just can connect (m^*, s^*) and (m, s) through obtained information and owned temporary key.

Firstly, $m = (m^* - b)a - r'$, $r' = (sG - rQ_A)_x \bmod p$.

Then $s^* = (s + b)a = (k + (ra^{-1} + b)x_A + b)a = ka + rx_A + abx_A + ab$.

With private key *x* of signer, temporary private key *k* and undo key *a*, *b* of *TC*, the just publicly verify the correctness of *s**. Therefore, as soon as illegal behavior was found, the just can immediately authorize user and correspond it with original signed messages.

(3) Security analysis

The security of scheme registration is based on the security of Hash function. It is difficult for user to find $R_1^{'}$ and $R_2^{'}$ to meet $r = H(R_1^{'}, R_2^{'})$. So the user can not forge just information of *TC*.

In the first step of signature, it requires user to show just information of *TC* so that unregistered users can not pass the verification of *TC*. It is obviously the security of signature scheme depends on that of *EIGamal* digital signature.

4. Conclusion

Aiming at problems of current fairness blind digital signature schemes that can not guarantee completely fairness simultaneously and can not recover messages, the paper proposed a message-recoverable fairness blind signature scheme. The correctness, security and fairness were analyzed.

Analysis results show that the just can authorize user’s identity and correspond it to original signature message with this scheme, and the user can not forge fairness information of just.

References

[1] D. Chaum: Blind Signature Systems. Proceedings of Crypto’83, Plenum, 1983.

[2] M.stadler, J-M. Piveteau, J and Camenisch: Fair Blind Signatures. Advances in Cryptology-EUROCRYPT’95, LANCS 921, 1995, pp. 209-219.

[3]N-Y. Lee and T.Hwang: On the Security of Blind Signature Using Oblivious Transfer. Computer Communications, 1999(22), pp. 287-290.

[4]Feng Deng-guo: Blind Signature Schemes Based on DLP Problem. Privacy of Communication (China), 1997 (1), pp. 31-34.

[5]Teo Chun Yew, Hailiza Kamarul Haili and Putra Sumari. Message Recovery Signature Scheme Using Complementary Elliptic Curves, 2003 IEEE, GMAG'03, 2003.