NEW ID BASED FAIR BLIND SIGNATURES

Girraj Kumar Verma[1], B. B. Singh[2]
[1]Department of Mathematics, SMS Govt. Model Science College, Gwalior, India
[2]Department of Mathematics, Govt. K.R.G. (PG) College, Gwalior, India
Email: girrajv@gmail.com[1], bbsinghkrg@gmail.com[2]

Abstract

A blind signature scheme is cryptographic primitive in which an user can obtain a valid signature from the signer, without revealing any information about message signature pair. Blind signatures are used in electronic payment systems, electronic voting machines, DRM systems etc. But, the anonymity of these signature schemes can be misused by criminals by money laundering or by dubious money. To prevent these crimes, the idea of fair blind signature was given by Stadler et al. In a fair blind signature scheme, there is a trusted third party judge who can provide a linking protocol to the signer to link his view to the resulting message signature pair. In this paper, we propose two identity based fair blind signature schemes one based on cut and choose method and another based on oblivious transfer protocol. The proposed schemes can be a good alternative for removing misuse of cryptographic protocols and key management problem in public key cryptographic protocols.

I. INTRODUCTION

The idea given by Diffey and Hillman [14] in their seminal paper “New Directions in Cryptography”, in 1976 has played a critical role in Cryptography. This article developed the notion of public key cryptography (PKC) and this new development inspired the generation of digital signature schemes for authenticity of source and the sender. In 1978, Rivest et al. [29] designed a first fully functional public key cryptography system based on factorization problem. In this article, they have designed a public key encryption as well as a digital signature scheme. Later, these signatures were used widely in several modified versions [2], [4], [6], [7].

In 1983 [8] D. Chaum gave the idea of blind signature schemes for electronic payment systems. A blind signature scheme is cryptographic primitive in which an user can obtain a valid signature from the signer, without revealing any information about message signature pair. The blind signatures are used in electronic payment systems, electronic voting machines, DRM systems etc [9]-[13], [16], [17], [27]. But, the anonymity of these signature schemes can be misused by criminals [31], [32] by money laundering or by dubious money. In 1993[26] Micali introduced the concept of fair cryptosystems to prevent the misuse of strong cryptographic protocols by criminals. In 1995[31] Stadler et al., designed two fair blind signature schemes, using cut and choose and oblivious transfer protocol [5]. In these schemes a trusted third party (known as judge) was also involved and who provides a linking of signer’s view to the resulting message signature pair to remove anonymity. Later in 2004, Lin et al. [25], presented new development of fair cryptosystems and in recent years, some more applications of fair cryptosystems [19], [20], [22]-[25], [33] have been reported by cryptographers.

The applications of public key cryptography, created a new problem of key management of public keys. In 1984[30] Shamir introduced the idea of identity based cryptosystems for removing the key management problem in public key cryptography. The first fully functional identity based cryptosystem was proposed in 2003[3] by Boneh and Franklin using bilinear pairing. In 2002[1], Barreto et al., designed some algorithms for pairing based cryptography and this development enhanced the interest of cryptographer community to design new identity based primitives [15], [21], [28]. In identity based cryptosystems, the public keys are derived from the identity of the user, such as their email, phone numbers etc.

In this article, we propose two identity based fair blind signature schemes, which are actually the identity based version of Stadler et al.'s [31] schemes.

The rest of the paper is organized as follows:

In section II, we have defined the identity based fair blind signatures and bilinear pairings which are creating a base for our signatures. In section III, we are considering fair blind signature by Stadler et al. and then we describe our proposed schemes and their analysis. Finally in section IV, we have concluded our discussion.

II. Identity Based Fair blind signatures and bilinear pairing

In this section, we are giving some brief discussion about fair blind signature and bilinear pairing.

A. Defining Identity Based Fair Blind Signature

An identity based fair blind signature scheme consist of several users, one signer and one trusted party known as judge and the following polynomial time algorithms:

(a)-Setup: This algorithm takes as input the security parameter k and outputs the key generation center KGC's master key, global public key and system parameter $params$.

(b)-Extract: An algorithm, which takes as input an identity $ID_U \in \{0, 1\}^*$ of any user U and master key of KGC and then outputs the public key and private key pair of the user U.

(c)-Signing: This algorithm is executed between user and signer and by executing the signing protocol, the user obtains a valid blind signature on a message of its choice such that the signer cannot link his view of the protocol to the resulting message signature pair.

(d)-Verification: By running this algorithm, the verifier defines the accept or reject the signature.

(e)-Correctness: This algorithm shows the correctness of the signature verification proof.

(f)- Blindness and Link Recovery: By running the link recovery or linking algorithm, the signer obtains the information from the judge that enables him to recognize the corresponding protocol view and the message signature pair.

There are two types of fair blind signatures, depending on the information provided by the judge during link recovery protocol.

Type-1: Given signer's view of the protocol, the judge delivers information that enables the signer (or to every body) to efficiently recognize the corresponding message signature pair(e.g. judge can also extract the message signature pair).

Type-2: Given the message signature pair, the judge delivers information that enables the signer to efficiently identify the sender of the message or to find the corresponding view of the signing protocol.

B. Bilinear Pairing

Let G_1, G_2 be two groups of same order q. We view G_1 as additive group (group of pints on elliptic curves) and G_2 as multiplicative group. Let P be an arbitrary generator of G_1. Assume that discrete log problem (DLP) is hard, in both G_1 and G_2. A mapping $e: G_1 \times G_1 \to G_2$, satisfying the following properties is called bilinear pairing:

Bilinearity:

$e(aP, bQ) = e(P, Q)^{ab} \quad \forall P, Q \in G_1, \forall a, b \in Z_n^*$

Or it can also be represented as follows:

$\forall P, Q, R \in G_1, e(P+Q, R) = e(P, R)e(Q, R)$ and $e(P, Q+R) = e(P, Q)e(P, R)$

Non-degeneracy: There exist $P,\ Q \in G_1$, such that $e(P,\ Q) \neq 1$.

Computability: There is an efficient algorithm to compute $e(P,\ Q)$ for all $P,\ Q \in G_1$.

III. PROPOSED IDENTITY BASED FAIR BLIND SIGNATURES

In this section first we discuss fair blind signature scheme by Stadler et al [31] and then we propose our two identity based fair blind signature schemes one using cut and choose and another using oblivious transfer protocol.

A. Fair Blind Signature by Stadler et al.[31]

These signatures are based on Chaum's blind [8] signatures and on cut and choose method. The system parameters are as follows:

- (n, e), the signer's public key and (p, q, d) is master key as used in RSA signature.
- $E_j(.)$,the enciphering function of a judge's public key cryptosystems.
- $H : \{0, 1\}^* \to Z_n^*$ is a one way cryptographic hash function.
- k is a security parameter.

The Protocol:

Signature Generation:

(a) User first chooses $r_i \in_R Z_n$ For $i = 1, 2, 3, ...2k$, and strings $\alpha_i, \beta_i \in_R \{0, 1\}^*$ and computes $u_i = E_j(m \| \alpha_i), v_i = E_j(ID \| \beta_i),\ m_i = r_i^e H(u_i \| v_i) \bmod n$ and sends m_i to the signer.

(b) Signer, chooses a subset $S \subset \{1, 2, 3, ...2k\}$ randomly of size k and sends to the sender.

(c) User then sends $r_i, u_i,\ \beta_i \quad \forall i \in S$ to the signer.

(d) Signer then checks $m_i = r_i^e H(u_i \| E_j(ID \| \beta_i)) \bmod n$ for every $i \in S$ and hence computes $b = \left(\prod_{i \notin S} m_i\right)^d \bmod n$ and sends it to sender.

(e) The User computes $s = \dfrac{b}{\left(\prod_{i \notin S} r_i\right) \bmod n}$ and display $\{s, T\}$ as signature , where $T = \{(\alpha_i,\ v_i) \mid i \notin S\}$.

Signature Verification: The signatures can be verified by $s^e = \prod_{(\alpha_i,\ v_i) \in T} H\left(E_j(m \| \alpha_i) \| v_i\right) \bmod n$.

At the end of the execution of signing protocol, the signer is convinced that with overwhelming probability, each v_i has been formed correctly. Since every v_i depends on ID, it is impossible for a dishonest signer to use information received during different sessions to generate a signature following the signing protocol.

B. Proposed Fair Blind Signatures using Cut and Choose

In this subsection, we are introducing our identity based fair blind signature scheme using cut and choose method used in [31]. This scheme is based on ID based signature scheme by K. G. Peterson [28].

(a)Setup: Let G_1 be an additive group of prime order q and G_2 be a multiplicative group of same order q. We assume the existence of a bilinear map $e : G_1 \times G_1 \to G_2$ with the property that discrete logarithm problem in both G_1 and G_2 is hard. Typically G_1, will be a subgroup of the group of points on elliptic curve over a finite field and G_2 will be a subgroup of associated finite field and map e may be derived from the Weil or Tate pairing over elliptic curves. We also assume that an element $P \in G_2$ satisfying $e(P, P) \neq 1_{G_2}$ is known. Let ID_s , be a string denoting the identity of the signer and ID is the string denoting session identifies of a user with signer. We consider, $H_1 : \{0, 1\}^* \to G_1,\ H_2 : \{0, 1\}^* \to Z_q$ and $H_3 : G_1 \to Z_q$ as three cryptographic hash functions. Hence system parameters are $param = (G_1, G_2, e, H_1, H_2, H_3, P, P_{pub}, q, k)$

(b)Extract: In our scheme a signer's public key is derived from his identity and is defined as $Q_{ID} = H_1(ID_s)$ and secret key as $D_{ID} = sQ_{ID}$, where $s \in_R Z_n^*$ is chosen by TA as his master key. We also assume $P_{pub} = sP$ is known to all.

(c)Signing: This algorithm is executed between user and the signer and at the end of this, a valid blind signature is generated. The user and the signer do the following steps:

1.Let the user wants to obtain a signature from the signer on the message $m \in \{0, 1\}^*$. For doing so, both of them agreed upon $ID \in \{0, 1\}^*$ as session identifier and user chooses

$\alpha_i, \beta_i \in_R \{0, 1\}^{|l|}$ for $i = 1, 2, ...2k$ where k is a security parameter.

2. Then user computes $u_i = E_j(\alpha_i \| m), v_i = E_j(\beta_i \| ID),\ m_i = H(u_i \| v_i) \bmod n$ and sends m_i to the signer.

3. Signer, chooses a subset $S \subset \{1, 2, 3, ...2k\}$ randomly of size k and sends to the user.

4. User then sends $u_i,\ \beta_i \quad \forall i \in S$ to the signer.

5.Signer then computes and checks $m_i = H(u_i \| E_j(\beta_i \| ID)) \bmod n\ \forall i \in S$ and then computes $R = rP, b = \prod_{i \notin s} m_i$ and $S_1 = r^{-1}(bP + H_3(R)D_{ID})$ where $r \in_R Z_n^*$ and sends (R, S_1) to the user.

6. User display (R, S_1, T) as signature, where $T = \{(\alpha_i,\ v_i) \mid i \notin S\}$.

(d)Verification: Verifier runs the following algorithm for checking validity of the signature:

1. Verifier computes $Q_{ID} = H_1(ID_s)$ and $b = \prod_{i \notin s} H_2(E_j(\alpha_i \| m) \| v_i)$ and $H_3(R)$.

2. Accepts the signature iff $e(P, P)^b e(P_{pub}, Q_{ID})^{H_3(R)} = e(R, S_1)$.

(e)Correctness: :

$$\begin{aligned} e(R, S_1) &= e(rP, r^{-1}(bP + H_3(R)D_{ID})) = e(P, bP + H_3(R)D_{ID}) \\ &= e(P, bP)e(P, H_3(R)D_{ID}) \quad = e(P,\ P)^b e(P, D_{ID})^{H_3(R)} \\ &= e(P,\ P)^b e(P, sQ_{ID})^{H_3(R)} \quad = e(P,\ P)^b e(sP, Q_{ID})^{H_3(R)} \\ &= e(P,\ P)^b e(P_{pub}, Q_{ID})^{H_3(R)} \end{aligned}$$

(f)Blindness and Link Recovery by Judge: Since user sends the value of $u_i = E_j(\alpha_i \| m)$ and β_i to the signer, so signer cannot link his view of the protocol to the resulting message signature pair. Since signer can verify the m_i ,s randomly, so user cannot obtain signature on a wrong message.

When the signer wants to check m or ID (session identifier), he requests to the judge. The judge takes $u_i = E_j(\alpha_i \| m)$ and $v_i = E_j(\beta_i \| ID)$, and after decryption of these he does the following steps:

*Given the values $u_i, i \in S$, the judge can disclose the message m as in [31]. Therefore, the scheme is of type-I

*Given the signature (R, S_1, T) , the judge can easily compute the identification string ID as in [31]. Therefore, the scheme is of type-II.

C. *Fair Blind Signature Using Oblivious transfer*

In this subsection, we are giving a new identity based fair blind signature scheme using oblivious transfer [5],[31]. We are developing this scheme on a variation of Fiat-Shamir signature scheme as described in [31]. In [31] Stadler et al. have explained the variation but they have not discussed the identity based version of this variation. We are first giving the identity based version of this variation and then use this variation to design our new protocol.

Fiat-Shamir Signature[18]:

Extraction: Signer generates his keys using RSA [30] and selects a cryptographic hash function $H : Z_n^* \times \{0, 1\}^* \to \{0, 1\}^k$ and defines $param = (n,\ e, H)$ and $(p, q,\ d)$ as is master key.

Signing: Let ID be the user's identity such that $g = ID^d \bmod n$, signer then executes the following steps:

1.Chooses $r \in_R Z_n^*$ and computes $t = r^e \bmod n$ and $s = gr^{H(t,m)}$.

2. Display (s, t) as a signature on message m .

Verification: Verifier accepts the signature iff $s^e = IDt^{H(t,m)} \bmod n$.

ID-Based Variation of Fiat-Shamir Signature:

Extraction: Signer generates his keys using RSA [29] and selects two cryptographic hash function $H_1 : Z_n^* \to Z_n^*,\ H_2 : Z_n^* \times \{0, 1\}^* \to \{0, 1\}^k$ and defines $param = (n,\ e, H_1, H_2)$ and $(p, q,\ d)$ as is master key.

Signing: Let $ID \in Z_n^*$ be the user's identity such that $g = ID^d \bmod n$. For a security parameter k $(k > 80)$, we define $y_i = H_1(ID + i) \bmod n$ and $x_i = y_i^d \bmod n$ for $i = 1, 2......k$. Then signer performs the following algorithm:

1.Chooses $r \in_R Z_n^*$ and computes $t = r^e \bmod n$.

2.Computes $C = H(t, m)$ and let c_i be the *i* th bit of *C*.

3.Computes $s = g\prod_{i=1}^{k} x_i^{c_i} \bmod n$ and display (s,t) as a signature.

Verification: Verifier computes $C = H_2(t, m)$ and let c_i be the *i* th bit of *C* and accepts the signature iff

$$s^e = ID\prod_{i=1}^{k} H_1(ID+i)^{c_i} \bmod n.$$

Correctness:

$$s^e = g^e\prod_{i=1}^{k} (x_i^{c_i})^e \bmod n = ID\prod_{i=1}^{k} (H_1(ID+i))^{c_i} \bmod n$$

Proposed Fair Blind Signature using oblivious transfer:

The *params* and secret keys are same as described in variation of Fiat-Shamir signature and let message to be signed is *m*. Then the user and signer participate in the following way:

Signing:

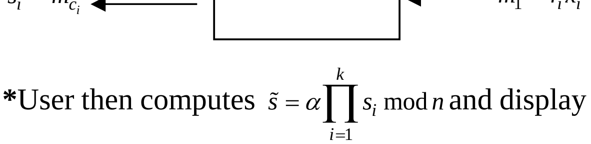
1.Signer Chooses $r_1, r_2, \ldots\ldots\ldots r_k \in_R Z_n^*$ and computes $t = \prod_{i=1}^{k} r_i^e \bmod n$ and sends t to the user.

2.User chooses $\alpha \in_R Z_n^*$ and computes $\tilde{t} = t\alpha^e \bmod n$ and $C = H_2(\tilde{t}, m)$ and let c_i be the *i*th bit of *C*.

Then they use the following oblivious transfer protocol:

User **Signer**

For $i = 1, 2, \ldots\ldots k$



*****User then computes $\tilde{s} = \alpha\prod_{i=1}^{k} s_i \bmod n$ and display $n(\tilde{s}, \tilde{t})$ as a valid signature.

Verification: Verifier accepts the signature iff

$$\tilde{s}^e = \tilde{t}\prod_{i=1}^{k} (H_1(ID+i))^{c_i} \bmod n.$$

Correctness:

$$\tilde{s}^e = \alpha^e\prod_{i=1}^{k} s_i^e = \alpha^e\prod_{i=1}^{k} r_i^e (x_i^e)^{c_i} = \tilde{t}\prod_{i=1}^{k} (x_i^e)^{c_i} = \tilde{t}\prod_{i=1}^{k} (H_1(ID+i))^{c_i}$$

Blindness and link recovery by Judge: Now, let us analyze the blindness of our scheme. We assume that the signer cannot determine the selection bit c_i (because of the $f - OT_2^1$). Therefore, *t* is the only value known to signer to use for linking his view to the resulting message signature pair. But for each valid signature $(\tilde{s}, \tilde{t})$ of a message m there is exactly one α with $\tilde{t} = t\alpha^e \bmod n$ and therefore, $\tilde{s} = \alpha\prod_{i=1}^{k} r_i x_i^{c_i} \bmod n$, where c_i be the *i*th bit of $C = H_2(\tilde{t}, m)$. So, the resulting signature is independent of the signing protocol and the signature scheme is perfectly blind signature scheme.

On the other hand considering the fairness of the scheme, if the signer sends the view of the protocol to the judge, the selection bit c_i can be determined and therefore the challenge C is known. This value could then be put onto a black list, so that everybody can recognize the message signature pair later.

Applications: There are several applications of fair blind signatures. One is to provide a tool to prevent money laundering in anonymous payment systems. In a payment system based on type-2 fair blind signature scheme the authorities can determine the origin of dubious money, while in typre-1 they can find out the destination of suspicious withdrawals.

Another application is the perfect crime scenario described in [32]: a customer is black mailed and forced to anonymously withdraw digital money from his account, acting as an intermediary between the blackmailer and the bank. In a perfectly anonymous payment system, the ransom could not be recognized later, but if a (type-1) fair blind signature scheme had been used, the judge, when the bank's view of the withdrawal protocol, can trace the blackmailed coin.

IV. Conclusion

In this research article, we have proposed two new identity based fair blind signatures for removing key management problem in public key cryptographic protocols. These signature schemes can be used for controlling the misuse of anonymity of cryptographic protocols. Although, these signature schemes are not much efficient non the less, they provides a practical solution for removing misuse of anonymity.

V. Acknowledgement

The authors would like to thank Prof. Sunder Lal, Ex. Vice-Chancellor, Poorvanchal University, Jaunpur, India for their valuable co operation and motivation.

References

[1] P.S.L. M. Barreto, H. Y. Kim and M. Scott, Efficient algorithms for pairing based cryptosystems, in proc. Of CRYPTO-2002, LNCS-2442, Springer Verlag, pp. 354-369, 2002.

[2] M. Ben-Or, O. Goldreich,, S. Micali and R. L. Rivest, A fair protocol for signing contracts, Transaction on Information theory, IEEE, 36(1), pp. 40-46, 1990.

[3] D. Boneh and M. Franklin, Identity based encryption from Weil pairing, SIAM J. of computing, pp.585-615, extended abstract in Crypto-2001.

[4] S. Brands, Untraceable off-line cash in wallet with observers, In proc. Of CRYPTO-93, LNCS-773, Springer Verlag, pp. 302-318, 1993.

[5] G. Brassard, C. Crepeau and M. Santha, Oblivious transfer and interesting codes, Transaction on Information Theory, IEEE, 42(6), pp. 1769-1780, 1996.

[6] J. Camenisch, J. M. Piveteau and M. Stadler, Blind Signature based on discrete logarithm problem, in proc. of EUROCRYPT-94, LNCS-950, Springer Verlag, pp. 428-432, 1994.

[7] J. Camenisch, J. M. Piveteau and M. Stadler, An efficient payment system protecting privacy, in Proc. Of ESORICS-94, LNCS-875, Springer Verlag, pp. 207-215, 1994.

[8] D. Chaum, Blind Signature systems, in proc. Of CRYPTO-83, LNCS-, Springer Verlag, pp.153-158, 1983.

[9] D. Chaum, Blind signatures for untraceable payments, in: Advances in cryptology, pp. 199-203. Springer US (1983). [10] D. Chaum, A. Fiat and M. Naor, Untraceable electronic cash, in proc. Of CRYPTO-88, LNCS-403, Springer Verlag, pp. 319-327, 1988.

[11] D. Chaum, Privacy protected systems, in proc. Of SMART CARDS-2000, Elseveir Science, B. V. North Holland, pp.69-93.

[12] D. Chaum, B. DenBoer, E. Van Heyst, S. Mj Flnse and A. Steenbeek, Efficient offline electronic checks, in proc. Of EUROCRYPT-89, LNCS-434, Springer Verlag, pp.294-301, 1989.

[13] D. Chaum and T. Pedersen, Wallet database with Observers, in proc. Of CRYPTO-92, LNCS-740, Springer Verlag, pp.89-105, 1992.

[14] W. Diffey and M. E. Hillman, New directions in cryptography, Transaction of Information Theory, IEEE, 22(6), pp.74-84, 1977.

[15] R. Dutta, R. Barua and P. Sarkar, Pairing based cryptographic protocols: A Survey, available at http://eprint.iacr.org/2004/064.

[16] S. Even, O. Goldreich and A. Lempel, A randomized protocol for signing contracts, Communications of ACM, 28, p.637-647, 1985.

[17] N. Ferguson, Single term offline coins, in proc. Of EUROCRYPT-93, LNCS-765, Springer Verlag, pp.318-328, 1993.

[18] A. Fiat and A. Shamir, How to prove yourself: Practical solution to identification and signature problems, in proc. Of CRYPTO-86, LNCS-263, Springer Verlag, pp.186-194, 1986.

[19] G. Fucshbaurer and D. Vergaurd, Fair blind signatures without random oracles, in proc. Of AFRICACRYPT- 2010, Springer Verlag, pp. 16-33, 2010.

[20] S. Han, E. Chang, X. Deng, L. Gao and W. Yeung, Practical fair anonymous undeniable signatures, Int. J. of Signal processing, 1(4), pp. 291-296, 2004.

[21] F. Hess, Efficient identity based signature schemes, in proc. Of SAC-2003, LNCS-2595, Springer Verlag, pp.310-324, 2003.

[22] X. Hou and C. H. tan, On fair traceable electronic cash, in proc. Of CNSR-05, IEEE, pp. 2005.

[23] E. Hufschmitt and J. Traore, Fair blind signatures revisited, in proc. Of PAIRING-2007, LNCS-4575, Springer Verlag, pp. 268-292, 2007.

[24] M. Jacobson, Blackmailing using undeniable signatures, in proc. Of

EUROCRYPT-94, LNCS-950, Springer Verlag, pp. 425-427, 1994.
[25] M. H. Lin, C. C. Chang and Y. R. Yen, A fair and secure mobile agent environment based on a blind signature and proxy host, Computers and Security, 23, pp.199-212, 2004.
[26] S. Micali, Fair Cryptosystems, Technical Report MIT/ LCS/ TR -579, 1993.
[27] T. Okamoto and K. Otha, Universal electronic cash, in proc. Of CRYPTO-91, LNCS-576, Springer Verlag, pp. 324-337, 1991.
[28] K. G. Peterson, Identity based signatures from pairing on elliptic curves, available at http://eprint.iacr.org/2002/004.
[29] R. L. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public key cryptosystems, Communica- tion of the ACM 21, pp.120-126, 1978.
[30] A. Shamir, Identity based cryptosystems and signature schemes, in proc. Of CRYPTO-84, LNCS-196, Springer Verlag, pp.47-53, 1984.
[31] M. stadler, M. Piveteau and J. Camenisch, Fair blind signatures, in proc. Of EUROCRYPT-95, LNCS-921,Springer Verlag, pp.209-219, 1995.
[32] S. Von, Solms and D. Naccache, On blind signatures and perfect crimes, Computers and Security-11, pp.581-583, 1992.
[33] W. T. Yin and W. Q. Yan, Fair quantum blind signatures, Chinese Physics B, 19(6), pp…, 2010.