Efficient Identity-Based Protocol for Fair Certified E-mail Delivery

Zhenfeng Zhang[1,2], Jing Xu[1,3], and Dengguo Feng[1,2]

[1] State Key Laboratory of Information Security
[2] Institute of Software, Chinese Academy of Sciences, Beijing 100080, P.R. China
[3] Graduate School of Chinese Academy of Sciences, Beijing 100039, P.R. China
zfzhang@is.iscas.ac.cn

Abstract. Certified e-mail delivery has become one of the basic requirement in performing business transactions over the Internet securely. How to construct efficient fair protocols for certified e-mail delivery is of great interest. The notion of identity based cryptosystem has attracted much interest since its introduction by Shamir in 1984, as it eliminates the need of certificates and simplifies the key management. In this paper, we propose a fair protocol for certified e-mail delivery based on identity-based signatures. A semi-trust third party (TTP) is involved in our protocol to ensure fairness, who does not need to store anything except its own private-key. There is no need for an additional registration between users and TTP. The proposed scheme is the first identity-based protocol with such a concise frame and is computation- and communication-efficient.

Keywords: Fair exchange, Certified E-mail, Security protocol, Identity-based signature.

1 Introduction

Communication by e-mail has become a vital part of everyday business and has replaced most of the conventional ways of communicating. The basic e-mail security services include the provision of privacy (only the intended recipient can read the message) and authentication (the recipient can be assured of the identity of the sender). Cryptographic mechanisms for providing these security services have been applied in Internet mail systems, such as S/MIME [24] and PGP [25]. In addition to sender authentication and message privacy, S/MIME can also provide a signed receipt service. A signed receipt from the recipient (requested by the sender) serves as a non-repudiable proof of receipt for a specific e-mail. However, the return of this receipt relies on the willingness of the recipient to honor the sender's request and provides no protection to the sender if the recipient chooses not to sign and return the acknowledgement after having read the message. In other words, this technique does not truly provide non-repudiation of the receipt security service.

Y.G. Desmedt et al. (Eds.): CANS 2005, LNCS 3810, pp. 200–210, 2005.

Important business correspondence may require certified e-mail delivery service, analogous to that provided by conventional mail service. For a viable certified e-mail service, the following security properties are needed:

- Non-repudiation of origin - the recipient must have a way of proving that a specific e-mail indeed originates from the sender;
- Non-repudiation of receipt - the sender must have a way of proving that the recipient has indeed received a specific e-mail;
- Strong fairness for the exchange - the recipient should obtain a specific e-mail if and only if the sender obtains a receipt for it.

By now, certified e-mail delivery (CEMD) has become one of the central problems in performing business transactions over the Internet securely and can be applied in numerous e-commerce transactions. Briefly speaking, this is the problems of how two mutually distrustful parties can fairly exchange a sender's valuable e-mail for a receiver's digital signature representing a proof of reception. A CEMD protocol [13, 17] shall provide strong fairness to ensure that the recipient receives the e-mail if and only if the sender receives the receipt.

The most practical and efficient approach to the fair exchange problems is to make use of an off-line trusted third party (TTP) to help the participants with the exchange. By this approach, the exchanging parties attempt to exchange their respective items themselves, i.e. without any involvement of the TTP. Should any dispute arise during the exchange process due to a party's misbehavior or a network failure, TTP is invoked to recover the disputed items and restore fairness.

Recently, a new category of off-line TTP-based fair exchange protocols has been proposed based on a cryptographic primitive called *verifiable and recoverable encryption of a signature* (VRES) [1, 2, 3, 4, 8, 10, 11, 14]. The VRES represents a digital signature encrypted in such a way that a receiver of the VRES can verify that it indeed contains the correct signature without obtaining any information about the signature itself (verifiability). The receiver can also verify that a designated TTP can help to recover the original signature from the VRES, in case the original signature sender refuses to do so (recoverability).

In SAC'04, Nenadic et al. [21] proposed a new RSA-CEMD protocol for the two communicating parties to fairly exchange an e-mail message for an RSA-based receipt. The main contribution of their work is a novel RSA-based method for the verifiable and recoverable encrypted signature, which is utilized as a crucial primitive to construct their RSA-CEMD protocol. The proposed protocols has been used as a main cryptographic primitive in the Fair Integrated Data Exchange Services (FIDES) project [22] provided for E-commerce transactions. However, as a building block, their VRES scheme was shown to be insecure recently by [23]: an adversary can easily generate a valid VRES which cannot be recovered by the designated TTP, and hence the proposed certified e-mail delivery protocol can not guarantee the claimed fairness.

As we know, in traditional public key cryptosystems, an entity's public-key is generated from some random information that is unrelated to his identity, and hence needs to be certified to provide users with confidence in the authenticity of the public keys they are using. PKI is an important infrastructure to manage these digital certificates and the trust relationships between entities in a hierarchical manner. Unfortunately, these certificate-based infrastructures turned out to be very heavy to deploy, cumbersome to use and non-transparent for the user.

In order to bypass the trust problems encountered in conventional Public Key Infrastructures, Shamir [18] introduced the concept of ID-based public-key cryptography (ID-PKC) in 1984, where an entity's public key can be a unique binary string identifying its owner non-ambiguously, such as an e-mail address, an IP address combined to a user-name, a social security number, et. al.. The motivation of ID-PKC was to simplify key management and remove the need of public key certificates as much as possible: since a key is the identity of its owner, there is no need to bind them by a digital certificates, and thus end users do not have to enquire for a certificate for their public key. A breakthrough work in the research of ID-PKC shall owe to Boneh and Franklin [7], who proposed the first efficient identity encryption scheme based on the bilinear pairings over elliptic curves. Since then, a great deal of research has been done about the ID-based cryptosystems. Moreover, the identity-based protocols constructed over elliptic curves are more suitable for ad hoc and sensor networks. However, as far as we know, no identity based protocol for certified e-mail delivery has been proposed.

In this paper, we proposed an efficient identity-based fair protocol for certified e-mail delivery, which work with an identity-based signature scheme constructed over elliptic curves. In our protocol, there is no registration between a party and TTP, which makes our protocol much concise and easy to implementation. In fact, TTP generates a trapdoor permutation as the system parameter, and does not need to store anything except the private-key of permutation. The trapdoor kept secret by TTP is only used in the recovery phase to ensure fairness.

The rest of the paper is organized as follows. In section 2, some notations and assumptions that will be used in this paper are given. Then we present our identity-based fair certified e-mail delivery protocol and analysis its security and efficiency in section 3. A conclusion is drawn in section 4.

2 Notations and Preliminaries

The following notations will be used in the remaining part of the paper.

- $E_{sk}(m)$ expresses a signature of an item m created with a private key sk.
- $h(\cdot)$ is a suitable collision-resistant one-way hash functions.
- $x \| y$ denotes the concatenation of data items x and y.

The following assumptions are used in the design of a certified e-mail delivery protocol.

- Alice wishes to send an e-mail message M to party Bob in exchange for Bob's receipt for M.
- Alice and Bob have agreed to employ an off-line TTP to help them with the exchange if they cannot reach a fair completion of the exchange themselves.

2.1 The Bilinear Pairing

Let $\mathcal{G}_1$ be a cyclic additive group generated by P, whose order is a prime q, and $\mathcal{G}_2$ be a cyclic multiplicative group of the same order. Let $e : \mathcal{G}_1 \times \mathcal{G}_1 \rightarrow \mathcal{G}_2$ be a pairing which satisfies the following conditions:

1. Bilinearity: For any $P, Q, R \in \mathcal{G}_1$, we have $e(P + Q, R) = e(P, R)e(Q, R)$ and $e(P, Q + R) = e(P, Q)e(P, R)$. In particular, for any $a, b \in \mathbf{Z}_q$,

$$e(aP, bP) = e(P, P)^{ab} = e(P, abP) = e(abP, P).$$

2. Non-degeneracy: There exists $P, Q \in \mathcal{G}_1$, such that $e(P, Q) \neq 1$.

3. Computability: There is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in \mathcal{G}_1$.

The typical way of obtaining such pairings is by deriving them from the weil-pairing or the tate-pairing on an elliptic curve over a finite field. We refer to [6, 7] for a more comprehensive description on how these groups, pairings and other parameters should be selected for efficiency and security. The interested reader is also referred to [16] for a complete bibliography of cryptographic works based on pairings.

Computation Diffie-Hellman (CDH) Problem: Given P, aP, $bP \in \mathcal{G}_1$ for randomly chosen $a, b \in_{\mathcal{R}} \mathbf{Z}_q^*$, to compute abP.

2.2 The Identity-Based Setting

In an identity-based cryptosystem, there is a trusted authority called the private key generator (PKG) who holds a master key and issues private keys for all users in the system domain. The public-key of a user can be derived publicly and directly from his unique identifier information. The following is a brief overview of the identity-based setting. We refer to [7] for a detailed description.

- **Setup.** Given a security parameter k, the PKG chooses groups $\mathcal{G}_1$ and $\mathcal{G}_2$ of prime order $q > 2^k$, a generator P of $\mathcal{G}_1$, a bilinear map $e : \mathcal{G}_1 \times \mathcal{G}_1 \rightarrow \mathcal{G}_2$, a randomly chosen master key $s \in \mathbf{Z}_q^*$ and the associated public key $P_{pub} = sP$. It also picks cryptographic hash functions of same domain and range $H_1, H_2 : \{0, 1\}^* \rightarrow \mathcal{G}_1$. The system's public parameters are

$$\texttt{params} = (\mathcal{G}_1, \mathcal{G}_2, e, P, P_{pub}, H_1, H_2).$$

- **Extract.** Suppose the identity of a user is ID. Given an identity ID, the PKG computes $Q_{ID} = H_1(ID) \in \mathcal{G}_1$ and $d_{ID} = sQ_{ID} \in \mathcal{G}_1$, and then transmits it to the user securely. The private key of the user is d_{ID}.

Now we briefly present the identity-based signature scheme proposed by Sakai, Ogishi and Kasahara [19], which has been commonly called SOK-IBS scheme in [5].

• **Sign:** In order to sign a message M, the signing algorithm takes as input the signer's private key d_{ID} and its identity ID, and performs as following:

1. Pick $r \in_{\mathcal{R}} \mathbf{Z}_q$, compute $U = rP \in \mathcal{G}_1$ and $H = H_2(ID, M, U) \in \mathcal{G}_1$.
2. Compute $V = d_{ID} + rH \in \mathcal{G}_1$.

The signature on M is the pair $\sigma = \langle U, V \rangle \in \mathcal{G}_1 \times \mathcal{G}_1$.

• **Ver:** To verify a SOK-IBS signature $\sigma = \langle U, V \rangle \in \mathcal{G}_1 \times \mathcal{G}_1$ on a message M for an identity ID, a verifier first takes $Q_{ID} = H_1(ID) \in \mathcal{G}_1$ and $H = H_2(ID, M, U) \in \mathcal{G}_1$, and then accepts the signature if and only if

$$e(P, V) = e(P_{pub}, Q_{ID}) \cdot e(U, H). \qquad (1)$$

In [5, 15], the SOK-IBS signature scheme has been shown to be non-existential forgeable under adaptive chosen message attacks in the random oracle model, assuming the computational Diffie-Hellman problem in $\mathcal{G}_1$ is hard.

3 Our ID-CEMD Protocol

Let the system parameter `params` $= (\mathcal{G}_1, \mathcal{G}_2, e, P, P_{pub}, H_1, H_2)$ be defined as in the **Setup** algorithm of section 2.2.

System Setup. Suppose the identity of user Alice is ID_A, and the corresponding private key is $d_A = sQ_A \in \mathcal{G}_1$, which is generated by PKG and is transmitted to Alice via a secure channel, where $Q_A = H_1(ID_A) \in \mathcal{G}_1$. Similarly, assume the identity of Bob is ID_B. The private key of Bob is then $d_B = sQ_B \in \mathcal{G}_1$, which is also computed by PKG and transmitted to him via a secure channel, where $Q_B = H_1(ID_B) \in \mathcal{G}_1$.

In our protocol, a designated TTP chooses $x \in \mathbf{Z}_q^*$ at random, generates a public key $PK = xP \in \mathcal{G}_1$ and publishes it as a system parameter, while keeps $SK = x$ secret.

Bob's receipt for a message M, denoted as $receipt_B = (U, V)$, is represented by Bob's SOK-IBS signature on M.

The ID-CEMD protocol consists of two protocols: the exchange protocol and the receipt recovery protocol.

3.1 The Exchange Protocol

In the exchange protocol, Alice and Bob attempt to exchange a message M for its receipt, without any involvement of the TTP. The exchange protocol comprises steps (E1)-(E4), as shown in Table 1.

Table 1. The ID-CEMD Protocol

(E1): Alice → Bob : $h(M), E_{d_A}(h(M))$
(E2): Bob → Alice : U, V'
(E3): Alice → Bob : M
(E4): Bob → Alice : V

(E1): Alice first transfers to Bob the hash value $h(M)$ and her digital signature $E_{d_A}(h(M))$ on M. This signature is optional. If this option is selected, it will serve as a non-repudiable proof of origin of M.

(E2): Upon receipt of the two items, Bob verifies Alice's signature $E_{d_A}(h(M))$ with Alice's public key $Q_A = H_1(ID_A)$. If the verification is negative, Bob may either ask Alice to re-send message (E1) or terminate the protocol execution. Otherwise, Bob produces a *verifiable and recoverable encryption* of its receipt for message M, denoted as (U, V'). To do so, Bob performs as following:

- 1. First choose $r \in \mathbf{Z}_q$ at random and compute $U = rP \in \mathcal{G}_1$, and then let

$$H = H_2(ID_B, h(M), U) \in \mathcal{G}_1.$$

- 2. Compute $V' = d_B + rH + rPK \in \mathcal{G}_1$.

Now $\sigma' = \langle U, V' \rangle \in \mathcal{G}_1 \times \mathcal{G}_1$ is Bob's VRES on M and is delivered to Alice.

Remark: Similar to that in [5, 15], the above VRES scheme can also be shown to be non-existential forgeable under adaptive chosen message attacks in the random oracle model, assuming the CDH problem in $\mathcal{G}_1$ is hard.

(E3): Upon receipt of this item, Alice performs the following verification to check the correctness of Bob's VRES (U, V'). First compute $Q_B = H_1(ID_B) \in \mathcal{G}_1$ and $H = H_2(ID_B, h(M), U) \in \mathcal{G}_1$, and then accept the VRES if

$$e(P, V') = e(P_{pub}, Q_B) \cdot e(U, H + PK), \tag{2}$$

and reject it otherwise. If this verification is negative, Alice may either ask Bob to re-send message (E2) or terminate the protocol execution. Otherwise, Alice transfers the message M to Bob.

(E4): Upon receipt of M, Bob performs the following verification to ensure the correct message M was received. Confirm that the message M received generates the hash value identical to that received in step (E1), i.e. calculate the fresh hash value $h(M)''$ of the received message M and compare it with the hash value $h(M)$ received from Alice in step (E1).

If the verification is negative, Bob may either ask Alice to re-send message (E3) or terminate the protocol execution. Otherwise, Bob computes $V = V' - rPK$ and transfers it to Alice.

Upon receipt of V, Alice uses it to check that

$$e(P, V) = e(P_{pub}, Q_B) \cdot e(U, H). \tag{3}$$

If this verification is positive, the certified e-mail delivery is completed successfully, i.e. Alice has obtained Bob's $receipt_B = (U, V)$ and Bob has obtained Alice's message M together with its proof of origin $E_{d_A}(h(M))$.

3.2 The Receipt Recovery Protocol

In case when Alice fails to obtain Bob's correct $receipt_B$ after handing over M to Bob, Alice may request TTP for the receipt recovery by invoking the recovery protocol.

Table 2. The Recovery Protocol

(R1): Alice → TTP : M, U, V'
(R2): TTP → Alice : V
(R3): TTP → Bob : M

(R1): Alice transfers the items M and (U, V') to TTP, which performs the following verification. Compute $Q_B = H_1(ID) \in \mathcal{G}_1$ and $H = H_2(ID_B, h(M), U) \in \mathcal{G}_1$, and then check

$$e(P, V') = e(P_{pub}, Q_B) \cdot e(U, H + PK). \tag{4}$$

If the verification is negative, TTP rejects Alice's request. Otherwise, TTP uses his knowledge of the trapdoor x to compute

$$V = V' - xU, \tag{5}$$

and returns V.

(R2): TTP sends V to Alice, who checks that

$$e(P, V) = e(P_{pub}, Q_B) \cdot e(U, H).$$

(R3): TTP forwards M to Bob.

Note that, the TTP's public key PK is used for the generation and verification of a VRES, while the private-key SK is sufficient for TTP to extract a SOK-IBS signature from a valid VRES in the recovery protocol. The TTP does not need to maintain an additional state, such as secret-public key pair, for each user via a special registration phase so as to resolve a dispute. What the TTP needs to store is only his own private-key SK.

3.3 Security and Efficiency Analysis

We shall show that the proposed protocol is secure against various attempts of cheating by either Alice or Bob.

For a malicious Bob, he attempts to cheat by generating a VRES (U, V') on $h(M)$ in (E2), which will pass Alice's verification, but the corresponding V cannot be recovered correctly by the designated TTP in (R2). After getting the message M in (E3), Bob refuses to send V to Alice, or just send a wrong V. However, this is always not the case. In fact, for any VRES (U, V') satisfying

$$e(P, V') = e(P_{pub}, Q_B) \cdot e(U, H + PK),$$

and $V = V' - xU$, we have

$$\begin{aligned} e(P, V) &= e(P, V')e(P, -xU) \\ &= e(P, V')e(PK, U)^{-1} \\ &= e(P_{pub}, Q_B) \cdot e(U, H). \end{aligned}$$

Thus, for the V extracted by TTP, the (U, V) is definitely a valid SOK-IBS signature on M, and the signer Bob cannot deny it. Therefore, a malicious Bob cannot gain any advantage over Alice in our ID-CEMD protocol.

Alice may attempt to cheat by refusing to send M or sending an incorrect M' in step (E3). If Bob does not receive M before a timeout or detects the incorrect message M' through the verification in step (E3), Bob will consequently terminate the protocol. Note that it is computationally infeasible for Alice to compute V from (U, V') by himself, without the knowledge of $SK = x$. In fact, since $V' - V = xU = xrP$, to compute V from (U, V') is equivalent to solve the computational Diffie-Hellman problem for the instance of $(P, U = rP, PK = xP)$. This means that Alice will not receive Bob's receipt $receipt_B$, so Alice gains no benefit from this misbehavior.

Alice attempts to cheat by requesting TTP to recover Bob's receipt after step (E2) without sending M to Bob in step (E3). One of the conditions for TTP to accept Alice's request is that Alice must provide message M that can pass the verification in step (R1). If the verification is positive, TTP forwards Alice's message M to Bob while passing V to Alice. Thus, Alice cannot benefit from this misbehavior, as message M will ultimately be delivered to Bob by TTP.

There is another attack we must take into consideration: colluding attack. That is, Alice may attempt to collude with another user, and try to have TTP recover V from (U, V'). However, the signer's identity ID is explicitly included in the signature as $H = H_2(ID_B, h(M), U)$, thus the colluding attacks proposed by Bao [4] will not work here.

Finally, we remark that our trust on TTP is minimal: it is only semi-trusted, which means that TTP cannot generate a valid receipt (U, V) without getting the corresponding VRES (U, V'). From TTP's point of view, a VRES is actually equivalent to a receipt since he has the trapdoor of the permutation $V = V' - xU$.

Noting the underlying receipt (U, V) is a SOK-IBS signature, which is non-existential forgeable under adaptive chosen-message attacks, a malicious TTP cannot generate a valid receipt (U, V) by himself, without the corresponding VRES (U, V'). So, our protocol is also secure against a malicious TTP.

Efficiency Analysis: In [21], it is shown that their protocol requires less computation and communication overhead, and places less security and storage requirements on the TTP. It seems appropriate to compare our protocol with [21]. The following analysis shows that our protocol is more efficient and concise.

In Nenadic et al.'s CEMD protocol, it requires an initialization phase for a party and a TTP to agree on a shared secret, which is then used by the TTP for possible receipt recovery. In our protocol, there is no need for such a registration between a user and TTP. This feature will greatly reduce the communication overhead and managing cost. And the time-consuming computations arise from (2) and (3) for verifying a VRES and a signature respectively. The corresponding computational cost is the same to that of a SOK-IBS scheme, which is roughly two pairing operations, as the term (P_{pub}, Q_B) can be pre-computed and stored before the exchange procedure.

In our ID-CEMD protocol, the end-users Alice and Bob need not to have their own certificates. Of course, as all the identity-based cryptosystems, the system parameters and the public key of TTP need to be certified by a certificate. Moreover, the designated TTP can be anyone different from the only PKG of an identity-based system. In fact, if we let PKG be the designated TTP, then we must have full trust in it since each user's private key is escrowed by PKG.

4 Conclusions

Certified e-mail delivery over Internet is an important e-commerce application that will proliferate in the coming years. This paper proposed a novel and efficient scheme enabling the *verifiable and recoverable encrypted signature* (VRES) for an identity-based signature scheme. Based upon the identity-based VRES, we presented an efficient identity-based fair protocol for certified e-mail delivery, which provides strong fairness to ensure that the recipient receives the e-mail if and only if the sender receives the receipt, and is more efficient in computation and communication. Moreover, there is no registration between a party and TTP, which makes our protocol much concise and easy to implementation.

Acknowledgement

The work is supported by National Natural Science Foundation of China under Granted No.60373039, and National Grand Fundamental Research Project of China under Granted No.G1999035802.

References

1. N. Asokan, V. Shoup and M. Waidner. Optimistic fair exchange of digital signatures. IEEE Journal on Selected Areas in Communications, 18(4): 593-610, 2000.
2. G. Ateniese. Verifiable encryption of digital signatures and applications, ACM Transactions on Information and System Security, 7, 1 (2004), 1-20.
3. G. Ateniese, C. Nita-Rotaru. Stateless-recipient certified E-mail system based on verifiable encryption. Proc. of 2002 RSA Conference-Topics in Cryptology, volume 2271 of Lecture Notes in Computer Science, pages 182-199, Springer-Verlag, 2002.
4. F. Bao, R. Deng and W. Mao. Efficient and practical fair exchange protocols with off-line TTP. Proc. IEEE Symposium on Security and Privacy, pages 77-85, 1998.
5. M. Bellare, C. Namprempre and G. Neven. Security Proofs for Identity-Based Identification and Signature Schemes, Proc. of Advances in Cryptology-Eurocrypt 2004, volume 3027 of Lecture Notes in Computer Science, pages 268-286, Springer-Verlag, 2004.
6. D. Boneh, B. Lynn, H. Shacham. Short signatures from the weil pairing. Proc. of Advances in Cryptology-ASIACRYPT 2001, volume 2248 of Lecture Notes in Computer Science, pages 514-532, Springer-Verlag, 2001.
7. D. Boneh and M. Franklin. Identity-based encryption from the Weil Pairing. Proc. of Advances in Cryptology-Crypto 2001, volume 2139 of Lecture Notes in Computer Science, pages 213-229, Springer-Verlag, 2001.
8. C. Boyd and E. Foo. Off-line fair payment protocols using convertible signatures. Proc. of Advances in Cryptology-ASIACRYPT 1998, volume 1514 of Lecture Notes in Computer Science, pages 271-285, Springer-Verlag, 1998.
9. J. Camenisch and M. Michels. Separability and efficiency for generic group signature schemes. Proc. of Advances in Cryptology-Crypto 1999, volume 1666 of Lecture Notes in Computer Science, pages 106-121, Springer-Verlag, 1999.
10. L. Chen. Efficient Fair Exchange with Verifiable Confirmation of Signatures. Proc. of Advances in Cryptology-ASIACRYPT 1998, volume 1514 of Lecture Notes in Computer Science, pages 286-299, Springer-Verlag, Berlin, Germany, 1998.
11. R. H. Deng, L. Gong, A. A. Lazar, and W. Wang. Practical Protocols for Certified Electronic Mail. J. of Network and System Management, 4(3): 279-297, 1996.
12. S. Even and Y. Yacobi. Relations among public key signature schemes. Technical Report 175, Computer Science Dept., Technion, Israel, 1980.
13. M. Franklin, M. Reiter. Fair exchange with a semi-trusted third party. Proc. ACM Conference on Computer and Communications Security, Zurich, Switzerland, pages 1-5, 1997.
14. J. A. Garay, M. Jakobsson, and P. MacKenzie. Abuse-free optimistic contract signing. Proc. of Advances in Cryptology-CRYPTO 1999, volume 1666 of Lecture Notes in Computer Science, pages 449-466, Springer-Verlag, Berlin, Germany, 1999.
15. B. Libert, J.-J. Quisquater. The Exact Security of an Identity Based Signature and its Applications, IACR Cryptology ePrint Archive, Report 2004/102, 2004.
16. The Pairing-Based Crypto Lounge. Web page maintained by Paulo Barreto: http://planeta.terra.com.br/informatica/paulobarreto/pblounge.html
17. B. Schneier and J. Riordan. A certified E-mail protocol. Proc. of 13th Computer Security Applications Conference, pages 347-352. ACM Press, 1998.
18. A. Shamir, Identity based cryptosystems and signature schemes, Proc. of Advances in Cryptology-Crypto 1984, volume 196 of Lecture Notes in Computer Science, Springer-Verlag, pages 47-53.

19. R. Sakai, K. Ohgishi, M. Kasahara. Cryptosystems based on pairing, In 2000 Sympoium on Cryptography and Information Security, Okinawa, Japan, 2000.
20. I. Ray and I. Ray. An optimistic fair exchange E-commerce protocol with automated dispute resolution, Proc. International Conference on E-Commerce and Web Technologies (EC-Web), volume 1875 of Lecture Notes in Computer Science, pages 84-93, Springer-Verlag, 2000.
21. A. Nenadic, N.Zhang and S.Barton. Fair certified E-mail delivery, Proc. ACM Symposium on Applied Computing (SAC 2004) - Computer Security Track, Nicosia, Cyprus, pages 391-396, 2004.
22. A. Nenadic, N. Zhang, S. Barton. FIDES-A middleware E-commerce security solution, Proc. of 3rd European Conference on Information Warfare and Security (ECIW 2004), London, UK, pages 295-304, 2004.
23. Z. F. Zhang, D. G. Feng, Efficient Fair Certified E-Mail Delivery Based on RSA, Proc. First International workshop on Information Assurance in Distributed Systems, ISPA Workshops 2005, volume 3759 of Lecture Notes in Computer Science, pages 368-377, Springer-Verlag, 2005.
24. S/MIME. *Secure Multipurpose Internet Mail Extensions.* Available at http://www.rsasecurity.com/standards/smime/.
25. The Internet Engineering Task Force (IETF). OpenPGP, *An Open Specification for Pretty Good Privacy.* Available at http://www.ietf.org/html.charters/openpgp-charter.html.