SECURE COMMUNICATION IN MOBILE AD HOC NETWORK USING EFFICIENT CERTIFICATELESS ENCRYPTION

Peter Hyun-Jeen Lee, Shivaramakrishnan Narayan and Parampalli Udaya
Department of Computer Science and Software Engineering, University of Melbourne, Victoria, 3010, Australia

Keywords: CLE, MANET, Bilinear Pairing, IBE.

Abstract: Establishing secure communication in a wireless network such as Mobile Ad Hoc Network (MANET) is particularly challenging because: (i) the network is self-organizing; (ii) messages are broadcasted; (iii) messages travel in a hop-by-hop manner; (iv) nodes are constrained in terms of computation and battery power. We propose a flexible and efficient Certificateless Encryption scheme which is optimized for MANET environment. Further, we couple the idea of Resurrecting Duckling with the scheme to achieve efficient key establishment and demonstrate the use of the transparent policy encoder which facilitates the authentication. We also show the security of the scheme in random oracle model assuming k-Bilinear Diffie-Hellman Inversion problem is hard.

1 INTRODUCTION

Wireless network is gaining increasing attention due to its freedom in connectivity. Mobile Ad Hoc Network (MANET) is one such a network where it is particularly challenging to enforce security. This is because MANET is a self-organizing wireless network where messages are broadcasted to travel hop-by-hop and nodes are limited in terms of computational power and battery. These characteristics make MANET vulnerable to various kind of attacks ranging from passive attacks (eg. eavesdropping on broadcasted messages) to active attacks (eg. compromising nodes).

Identity Based Encryption (BF-IBE) by Boneh and Franklin (Boneh and Franklin, 2001) has been a popular choice as a cryptographic primitive in MANET due to its low infrastructural cost and convenience in deriving the authentic public key. One disadvantage of IBE however, is the forced unconditional trust towards the Private Key Generator (PKG). This limits the use of IBE to a closed environment where key escrow is acceptable.

Thus majority of previous attempts involved the use of threshold cryptography (Bohio and Miri, 2004; Luo et al., 2002; Pan et al., 2007; Zhang et al., 2005) in order to provide secure communication in MANET. While threshold public key cryptography helps establishing escrow free secure communication without the presence of a central authority, it is not a favorable choice due to the following reasons: (i) n number of nodes need to be online and reachable at a given time for key establishment; (ii) incurs a high overhead during the decryption.

On the other hand, Al-Riyami and Paterson proposed Certificateless Encryption (CLE) (Al-Riyami and Paterson, 2003) in an effort to overcome the key escrow problem of IBE. CLE does this successfully while remaining non-directory based by incorporating positive aspects from both IBE (implicit authentication of a public key via its associated identity) and conventional PKC (user contributed secret in private key generation). Yet, their CLE carries over similar computational burden including map-to-point hash function and pairings involved in both encryption and decryption due to its close resemblance to BF-IBE.

Another IBE scheme proposed by Sakai and Kasahara (SK-IBE) (Sakai and Kasahara, 2003) in 2003 has not received much attention due to the lack of security proof which was not available until Chen and Cheng (Chen and Cheng, 2005) proved its security under k-Bilinear Diffie-Hellman Inversion (BDHI) assumption. SK-IBE presents better efficiency by avoiding map-to-point hash function and reducing the number of pairing operations required to one.

In 2006, Libert and Quisquater (Libert and Quisquater, 2006) gave a construction of CLE which is computationally more efficient than previously pro-

Hyun-Jeen Lee P., Narayan S. and Udaya P. (2008).
SECURE COMMUNICATION IN MOBILE AD HOC NETWORK USING EFFICIENT CERTIFICATELESS ENCRYPTION.
In *Proceedings of the International Conference on Security and Cryptography*, pages 306-311
DOI: 10.5220/0001921703060311

posed CLE schemes from the above observation. However, their public key size is too big as it is an element in the extension field (typical size of 1024 bits). Although they suggest the use of two special types of curves which can reduce the size of public key by a considerable amount, it adds extra complexity.

While the consequence of these drawbacks may be subtle in a desktop environment, its effect can be significant in a resource constrained environment such as Mobile Ad Hoc Network (MANET). With this motivation we propose a CLE scheme optimized for efficient computation, storage and communication.

1.1 Contribution

We propose a CLE scheme which is optimized for efficiency, targeting the resource constrained environment such as MANET. Specifically, our scheme is more efficient than the scheme by Libert and Quisquater by two field exponentiations in computation-wise and up to 40% in public key size-wise when MNT curves (Miyaji et al., 2001) are used.

Our scheme facilitates secure communication in MANET with efficient key establishment which can readily be initiated due to the virtue of key escrow freeness. Further, the use of the transparent policy encoder eases authentication process.

Our scheme is secure against adaptive chosen-ciphertext-attack in the random oracle model assuming k-BDHI assumption holds. We show the reduction by closely modeling the adversary model in (Al-Riyami and Paterson, 2003) and applying the result in (Chen and Cheng, 2005). We also show that our scheme is resistant to the recent attack by Au et al. (Au et al., 2007). Due to space limitation, we omit the security proof (available in the full version of the paper).

The rest of the paper is organized as follows. Section 2 gives the necessary background for the Basic and Full Scheme presented in Section 3. In Section 4, we show key establishment followed by performance analysis in Section 5. Finally we show the conclusion and future works in Section 6.

2 PRELIMINARIES

In this section, we describe the necessary mathematical background required.

2.1 Bilinear Groups

$\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{G}_T$ are cyclic groups of prime order q. P_1 is a generator of $\mathbb{G}_1$ and P_2 is a generator of $\mathbb{G}_2$. ψ is an isomorphism from $\mathbb{G}_2$ to $\mathbb{G}_1$ with $\psi(P_2) = P_1$. $\hat{e}$ is a bilinear map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$.

Necessary requirements for the bilinear map $\hat{e}$ are:

Bilinear. For all $P \in \mathbb{G}_1$ and all $Q \in \mathbb{G}_2$ and all $a, b \in \mathbb{Z}$ we have $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$.

Non-degenerate: $\hat{e}(P_1, P_2) \neq 1$.

Computable: There is an efficient algorithm to compute $\hat{e}(P, Q)$ for all P and Q.

2.2 Assumptions

Assumption 1 (Bilinear Diffie-Hellman (BDH).)**.** *Given (P_2, aP_2, bP_2, cP_2) where $P_2 \in \mathbb{G}_2$ and $a, b, c \in_R \mathbb{Z}_q^*$, computing $\hat{e}(P_1, P_2)^{abc}$ is hard.*

Assumption 2 (k-Bilinear Diffie-Hellman Inversion (k-BDHI).)**.** *For an integer k, and $x \in \mathbb{Z}_q^*, P_1 = \psi(P_2)$, $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$, given $(P_1, P_2, xP_2, x^2P_2, \ldots, x^kP_2)$, computing $\hat{e}(P_1, P_2)^{1/x}$ is hard.*

2.3 Security Model

Let $\mathcal{K}$ be a security parameter, and $\mathbb{M}$ and $\mathbb{C}$ denote the plaintext and ciphertext spaces respectively. A CLE system consists of the following polynomially bounded algorithms.

Setup. Given security parameter $\mathcal{K}$, returns a master public key M_{pk} and a master secret key M_{sk}.

Partial-Private-Key-Extract: Given M_{pk}, M_{sk} and $ID_A \in \{0,1\}^*$, which is an identifier string for entity A, returns the corresponding partial private key ∂d_A.

Extract. Given $M_{pk}, \partial d_A$ and the user chosen secret k, returns the corresponding full private key d_A.

Set-Public-Key : Given M_{pk} and the user chosen secret k, returns the randomly generated public key K_{pub}.

Encrypt. Given M_{pk}, ID_A, K_{pub} and a message $m \in \mathbb{M}$, returns the ciphertext $C \in \mathbb{C}$.

Decrypt. Given M_{pk}, ID_A, d_A and C, returns the plaintext m or a failure symbol $\perp$.

Next, we define the security of our scheme using the following game model.

Setup. The challenger $\mathcal{C}$ takes a security parameter $\mathcal{K}$ and runs the Setup algorithm. $\mathcal{C}$ gives M_{pk} to the adversary $\mathcal{A}$ and keeps M_{sk} secret to himself.

Phase 1. $\mathcal{A}$ issues any of the following queries.

1. Partial private key extraction on ID_i: $\mathcal{C}$ runs the Partial-Private-Key-Extract algorithm to generate ∂d_i.

2. Extraction query on ID_i: $\mathcal{C}$ runs the Extract algorithm to generate d_i and passes it to $\mathcal{A}$.
3. Decryption query on (ID_i, C_i): $\mathcal{C}$ decrypts by searching for the corresponding d_i in H_1^{list}.
4. Request public key on (ID_i): $\mathcal{C}$ returns the public key generated by running Set-Public-Key.
5. Replace public key for (ID_i): $\mathcal{A}$ is free to make any valid change to the given public key and request to replace its given public key to the modified public key.

Challenge. Once $\mathcal{A}$ decides that Phase 1 is over, $\mathcal{A}$ outputs two equal length plaintexts $m_0, m_1 \in \mathbb{M}$, and an identity ID_{ch} on which $\mathcal{A}$ wishes to be challenged. The only constraint is that $\mathcal{A}$ must not have queried the extraction oracle on ID_{ch} in Phase 1. $\mathcal{C}$ picks a bit $b \in_R \{0,1\}$ and sets $C_{ch} = \text{Encrypt}(M_{pk}, ID_{ch}, m_b) \in \mathbb{C}$. $\mathcal{C}$ sends C_{ch} as the challenge to $\mathcal{A}$.

Phase 2. $\mathcal{A}$ issues more queries as in Phase 1 but with two restrictions: (1) Extraction queries cannot be issued on ID_{ch}; (2) Decryption queries cannot be issued on (ID_{ch}, C_{ch}).

Guess. Finally, $\mathcal{A}$ outputs a guess $b' \in \{0,1\}$ and wins the game if $b' = b$.

Next we define two different types of adversaries Type 1 and 2.

Type 1. Type I adversary $\mathcal{A}_1$ does not have access to the master secret s. However, is given the partial private key component k and is allowed to request for the public key replacement. Restrictions are:

1. $\mathcal{A}_1$ cannot extract the private key for ID_{ch} at any time.
2. $\mathcal{A}_1$ request the private key for any identity if the corresponding public key has been replaced.
3. $\mathcal{A}_1$ cannot both replace the public key for the challenge identity ID_{ch} before the challenge phase and extract the partial private key for ID_{ch} in some phase.
4. In Phase 2, $\mathcal{A}_1$ cannot make a decryption query on the challenge ciphertext C_{ch} for the combination of identity ID_{ch} and the public key P_{ch} that was used to encrypt m_b.
5. When requesting for a public key replacement, δ applied to the public key needs to be informed to the simulator.

Type 2. Type II adversary $\mathcal{A}_2$ does have access to the master secret s. However, $\mathcal{A}_2$ is not allowed to replace public keys.

1. $\mathcal{A}_2$ cannot replace public keys.
2. $\mathcal{A}_2$ cannot extract the private key for ID_{ch}.
3. In Phase 2, $\mathcal{A}_2$ cannot make a decryption query on the challenge ciphertext C_{ch} for the combination of identity ID_{ch} and public key P_{ch} that was used to encrypt m_b.

Definition 2.1. A CLE scheme is secure against adaptive-chosen-plaintext-attack (IND-CPA) if no polynomially bounded adversary $\mathcal{A}$ (Type 1 or Type 2) has a non-negligible advantage against the challenger in the described game model (excluding the decryption oracle).

Definition 2.2. A CLE scheme is secure against adaptive-chosen-ciphertext-attack (IND-CCA) if no polynomially bounded adversary $\mathcal{A}$ (Type 1 or Type 2) has a non-negligible advantage against the challenger in the described game model.

3 EFFICIENT CLE SCHEMES

3.1 Basic Scheme

Setup. Given a security parameter $\mathcal{K} \in \mathbb{Z}^+$, generate the following:

1. Three groups $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{G}_T$ of prime order q and a bilinear map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$.
2. Random generators $P_1 \in \mathbb{G}_1$, $P_2 \in \mathbb{G}_2$ and a random master secret $s \in \mathbb{Z}_q^*$ then set $P_{pub} = sP_2$.
3. Cryptographic hash functions $H_1 : \{0,1\}^* \to \mathbb{Z}_q^*$, $H_2 : \mathbb{G}_\mathbb{T} \to \{0,1\}^n$ for some integer $n > 0$.

Finally publish $M_{pk} = \langle q, \mathbb{G}_1, \mathbb{G}_2, \hat{e}, \psi, P_1, P_2, P_{pub}, H_1, H_2, n \rangle$ as the master public key and $M_{sk} = s$ as the master private key. The plaintext space is $\mathbb{M} = \{0,1\}^n$ and the ciphertext space is $\mathbb{C} = \mathbb{G}_1 \times \{0,1\}^n$.

Partial-Private-Key-Extract. Given a string identifier for an entity A $ID_A \in \{0,1\}^n, \bar{k}, M_{pk}$ and M_{sk}, do the following:

1. Compute $h_A = H_1(ID_A || \bar{k})$.
2. Compute the partial private key as $\partial d_A = (h_A + s)^{-1} P_2$.

Extract. Given M_{pk}, a partial private key ∂d_A and user's chosen secret k, do the following:

1. Compute k^{-1}.
2. Set the private key as $d_A = k^{-1} \partial d_A$.

Set-Public-Key. Given M_{pk} and the user chosen secret k, generate the public key K_{pub} as follows.

1. Compute kP_1 and kP_{pub}.
2. Set the public key as $K_{pub} = (kP_1, kP_{pub}, \bar{k})$.

Encrypt. A plaintext message $m \in \mathbb{M}, ID_A, K_{pub}$ and M_{pk} results in a ciphertext C as follows:

1. Check that $\hat{e}(kP_1, P_{pub}) = \hat{e}(P_1, kP_{pub})$. If not, output $\perp$ and abort.
2. Pick $r \in_R \mathbb{Z}_q^*$.
3. Compute h_A and g^r. Note that $g = \hat{e}(P_1, P_2)$ needs only be computed once.
4. Then encrypt as $C = (U,V) = (r(h_A kP_1 + k\psi(P_{pub})), M \oplus H_2(g^r))$.

Decrypt. Given C, d_A and M_{pk}:

1. Compute $g' = \hat{e}(U, d_A)$ and $\sigma' = V \oplus H_2(g')$.
2. Compute $m' = V \oplus H_2(g')$ and return m' as the plaintext.

Above is true since,
$g' = \hat{e}(U, d_A) = \hat{e}(r(h_A kP_1 + k\psi(P_{pub})), k^{-1}(h_A + s)^{-1}P_2) = \hat{e}(P_1, P_2)^r = g^r$

3.2 Full Scheme

This scheme is constructed by applying FO transformation (Fujisaki and Okamoto, 1999) to Basic Scheme.

Setup. Given a security parameter $\mathcal{K} \in \mathbb{Z}^+$, generate the following:

1. Follows the Steps 1-3 of Basic Scheme's **Setup**.
2. Two additional cryptographic hash functions $H_3 : \{0,1\}^n \times \{0,1\}^n \rightarrow \mathbb{Z}_q^*$ and $H_4 : \{0,1\}^n \rightarrow \{0,1\}^n$ for some integer $n > 0$.

Finally publish $M_{pk} = \langle q, \mathbb{G}_1, \mathbb{G}_2, \hat{e}, \psi, P_1, P_2, P_{pub}, H_1, H_2, H_3, H_4, n \rangle$ as the master public key and $M_{sk} = s$ as the master private key. The plaintext space is the same as in Basic Scheme. The ciphertext space is $\mathbb{C} = \mathbb{G}_1 \times \{0,1\}^{2n}$.

Partial-Private-Key-Extract. Follows Basic Scheme's **Extract**.

Extract. Follows Basic Scheme's **Extract**.

Set-Public-Key. Follows Basic Scheme's **Set-Public-Key**.

Encrypt. A plaintext message $m \in \mathbb{M}, ID_A, K_{pub}$ and M_{pk} results in a ciphertext C as follows:

1. Check that $\hat{e}(kP_1, P_{pub}) = \hat{e}(P_1, kP_{pub})$. If not, output $\perp$ and abort.
2. Pick a $\sigma \in_R \{0,1\}^n$ and compute $r = H_3(\sigma, m)$.
3. Compute h_A and g^r as in Basic Scheme's **Encrypt**.
4. Then encrypt as $C = (U,V,W) = (r(h_A kP_1 + k\psi(P_{pub})), \sigma \oplus H_2(g^r), m \oplus H_4(\sigma)$.

Decrypt. Given C, d_A and M_{pk}:

1. Compute $g' = \hat{e}(U, d_A)$ and $\sigma' = V \oplus H_2(g')$.
2. Compute $m' = W \oplus H_4(\sigma')$ and $r' = H_3(\sigma', m')$.
3. If $U \neq r'(h_A kP_1 + k\psi(P_{pub}))$, output $\perp$, else return m' as the plaintext.

4 KEY ESTABLISHMENT

The characteristics of MANET demand an efficient, escrow-free and self-configuring encryption scheme in order to establish secure communication between the participating nodes. Many threshold-based cryptographic approaches proposed so far are not adequate for MANET for at least two reasons: (i) n number of nodes need to be online and reachable at a given time for key establishment; (ii) incurs a high overhead during the decryption.

Resurrecting Duckling is a novel approach by Stajano and Anderson (Stajano and Anderson, 2000) for key establishment in MANET. The idea is simple, a node A will recognize another node B as its master if B sends A a secret key before any other node does (known as *imprinting*). This allows the network to readily begin secure communication instead of having to wait until a certain number of nodes become available in the network. However, such a master-slave relationship between nodes are not suitable where every node is autonomous and compromising a master node can significantly endanger the security of its slave nodes.

We propose the use of our scheme combined with Resurrecting Duckling idea to leverage the vulnerable master-slave relationship to facilitator-benefitor relationship. Due to the escrow free property of CLE, a node A acting as a PKG does not have the full control over the other node B which obtains its partial private key from A. Instead, A merely facilitates the secure communication (by setting up the public parameters and generating the partial private key) and B benefits from A's service. By using the blinding technique, the secure channel (such as SSL) between A and B need not be established when transferring the partial private key. We now describe how the key establishment can readily start in the absence of any online central authority (N is the number of existing nodes).

N = 2: Node A and B come in contact of each other.

- A and B starts negotiating on the public parameter selection for their secure communication. Note that each node will choose its master secret independently as s_A and s_B.
- Once the negotiation is done, A chooses a blinding factor $x \in_R \mathbb{Z}_q^*$ and sends (ID_A, k, xP_2) to B.
- Upon successful authentication of A, B performs Partial-Private-Key-Extract and com-

putes the blinded partial private key $\partial d_A = (h_A + s_B)^{-1} x P_2$ where $h_A = H_1(ID_A||k)$, then sends the key to A.

- A obtains its unblinded partial private key = $x^{-1}(h_A+s_B)^{-1}xP_2 = (h_A+s_B)^{-1}P_2$ as required.
- B follows the same procedure to obtain its partial private key from A.

Notice that even if an adversary eavesdrops on the communication and catches $(h_A + s_B)^{-1} x P_2$, he cannot use this to impersonate as A since x is unknown to him nor can he become a valid member of the network.

$N > 2$: Another node C joins the network.

- C broadcasts the request that it wishes to join the network.
- Nodes willing to provide PKG service will reply to the request.
- C randomly selects one among the replied nodes.
- The rest follows the same procedure as in $N = 2$ case.

4.1 $\bar{k}$ as the Transparent Policy Encoder

In this subsection, we demonstrate how to use $\bar{k}$ as the policy encoder and show how its transparency can ease the task of authentication. Recall that in our Basic and Full Scheme, we have used k as a simple random element in $\mathbb{Z}_q^*$. Instead, we can use k as the policy encoder (eg. validity period, location info, etc) which can be determined during the negotiation phase. For example, one may define $k = sP_2 \oplus policy$.

Then, nodes C and D each of which have been issued its partial private key from different PKG nodes A and B respectively, can easily authenticate each other in the following way.

- C sends its public key $(k_C P_1, k_C P_{pub}, \bar{k_C})$ and $s_A P_2$ to D
- D obtains $policy = \bar{k_C} \oplus s_A P_2$ and checks if the policy is valid.
- D follows the same procedure to be authenticated by C.
- If both C and D are satisfied with each other's policy, they can start secure communication.

5 PERFORMANCE

In the Table 1 and 2, we compare the efficiency of different CLE schemes with respect to the number of operations required and their public key sizes. Although encryption schemes presented in (Al-Riyami and Paterson, 2003; Libert and Quisquater, 2006) imply the use of supersingular curves, for a fair efficiency comparison, we assume MNT curves are used. Also it is assumed that point compression techniques are applied. (+160) in the Table 2 denotes the additional bits needed when k is used separately as the policy encoder. Note that in Table 1, we have not included the computation required for the public key check since this only needs to be done once for each new user.

(Libert and Quisquater, 2006) outperforms (Al-Riyami and Paterson, 2003) by 1 pairing in encryption. Since pairing is the cost-dominant operation, this gain outweighs the performance loss due to some other extra computations. Our scheme makes further performance improvement by reducing one element exponentiation in each encryption and decryption.

While we are aware of the recently proposed CLE without pairing by Sun et al. (Y. Sun and Baek, 2007), it is not included in our comparison. This is because although this scheme requires less computation, its public key size is bigger hence making a straightforward comparison difficult. To conduct a comparison, the difference between significance of reducing computational cost and reducing communication cost in MANET needs to be studied and is beyond the scope of this paper.

6 CONCLUSIONS AND FUTURE WORKS

In this paper, we have presented a provably secure efficient certificateless encryption scheme. We have shown that our scheme is an ideal choice for key establishment in MANET when coupled with Resurrecting Duckling idea. Further, we have shown how the use of transparent policy encoder eases the authentication task. The security of our scheme has been proven against adaptive-chosen-ciphertext-attack in the random oracle model assuming k-BDHI holds. To further enhance our proposal we suggest PGP's web of trust concept (Abdul-Rahman, 1997) to manage the trust level of each node in the network for determining the potential candidate to take the PKG's role. This will aid in avoiding or detecting dishonest node behaviours (eg. node impersonation).

ACKNOWLEDGEMENTS

We would like to thank the anonymous reviewers for their helpful comments.

Table 1: Performance Comparison (No. required in encryption/decryption).

	Map to point	Point addition	Scalar multiplication	Element exponentiation	Pairing
(Al-Riyami and Paterson, 2003)	1/0	0/0	1/1	1/0	1/1
(Libert and Quisquater, 2006)	0/0	1/1	2/2	2/1	0/1
Our Scheme	0/0	1/1	2/2	1/0	0/1

Table 2: Public Key Size Comparison (in bits).

	Supersingular Curve	MNT Curve	BN Curve
(Al-Riyami and Paterson, 2003)	320	320	320
(Libert and Quisquater, 2006)	1024	512	320
Our Scheme	320 (+ 160)	320 (+ 160)	320 (+ 160)

REFERENCES

Abdul-Rahman, A. (1997). The pgp trust model. edi- forum, april 1997. http://www.cs.ucl.ac.uk/staff/F.AbdulRahman/docs/.

Al-Riyami, S. and Paterson, K. (2003). Certificateless public key cryptography. In *Advances in Cryptology - ASIACRYPT 2003*, pages 452–473. Springer-Verlag.

Au, M. H., Mu, Y., Chen, J., Wong, D. S., Liu, J. K., and Yang, G. (2007). Malicious kgc attacks in certificateless cryptography. In *ASIACCS '07: Proceedings of the 2nd ACM symposium on Information, computer and communications security*, pages 302–311. ACM.

Bohio, M. and Miri, A. (2004). Efficient identity-based security schemes for ad hoc network routing protocols. *Journal of Ad Hoc Networks*.

Boneh, D. and Franklin, M. K. (2001). Identity-based encryption from the weil pairing. In *CRYPTO '01: Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology*, pages 213–229. Springer-Verlag.

Chen, L. and Cheng, Z. (2005). Security proof of the sakai-kasahara's identity-based encryption scheme. In *Cryptography and Coding*, pages 442–459. Springer-Verlag.

Fujisaki, E. and Okamoto, T. (1999). Secure integration of asymmetric and symmetric encryption schemes. In *CRYPTO '99: Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology*, pages 537–554. Springer-Verlag.

Libert, B. and Quisquater, J. J. (2006). On constructing certificateless cryptosystems from identity based encryption. In *Public Key Cryptography - PKC 2006*, volume 3958 of *Lecture Notes in Computer Science*, pages 474–490. Springer-Verlag.

Luo, H., Zerfos, P., Kong, J., Lu, S., and Zhang, L. (2002). Self-securing ad hoc wireless networks. In *ISCC '02: Proceedings of the Seventh International Symposium on Computers and Communications (ISCC'02)*, page 567. IEEE Computer Society.

Miyaji, A., Nakabayashi, M., and Takano, S. (2001). New explicit conditions of elliptic curve traces for fr-reduction. In *IEICE Transactions on Fundamentals*, volume E84-A, pages 1234–1243.

Pan, J., Cai, L., Shen, X. S., and Mark, J. W. (2007). Identity-based secure collaboration in wireless ad hoc networks. *Comput. Networks*, 51(3):853–865.

Sakai, R. and Kasahara, M. (2003). Id based cryptosystems with pairing on elliptic curve. In 2003 Symposium on Cryptography and Information Security – SCIS'2003, Hamamatsu, Japan, 2003. http://eprint.iacr.org/2003/054.

Stajano, F. and Anderson, R. J. (2000). The resurrecting duckling: Security issues for ad-hoc wireless networks. In *Proceedings of the 7th International Workshop on Security Protocols*, pages 172–194. Springer-Verlag.

Y. Sun, F. Z. and Baek, J. (2007). Strongly secure certificateless public key encryption without pairing. In *Cryptology and Network Security*, volume 4856, pages 194–208. Springer-Verlag.

Zhang, Y., Liu, W., Lou, W., Fang, Y., and Kwon, Y. (2005). Ac-pki: anonymous and certificateless public-key infrastructure for mobile ad hoc networks. In *ICC 2005: 2005 IEEE International Conference on Communications*, pages 3515–3519. IEEE.