Comments

On the Security of a Ticket-Based Anonymity System with Traceability Property in Wireless Mesh Networks

Huaqun Wang and Yuqing Zhang, *Member*, *IEEE*

Abstract—In 2011, Sun et al. [5] proposed a security architecture to ensure unconditional anonymity for honest users and traceability of misbehaving users for network authorities in wireless mesh networks (WMNs). It strives to resolve the conflicts between the anonymity and traceability objectives. In this paper, we attacked Sun et al. scheme's traceability. Our analysis showed that trusted authority (TA) cannot trace the misbehavior client (CL) even if it double-time deposits the same ticket.

Index Terms—WMNs, cryptanalysis, anonymity, traceability.

1 Introduction

Anonymity and privacy issues have gained considerable research efforts in the literature [1], [2], [3], which have focused on investigating anonymity in different context or application scenarios. Nevertheless, unconditional anonymity may incur insider attacks since misbehaving users are no longer traceable. Therefore, traceability is highly desirable, such as in e-cash systems, where it is used for detecting and tracing double-spenders.

Motivated by resolving the security conflicts of anonymity and traceability in the emerging WMNs communication systems, Sun et al. have proposed the initial design of a security architecture achieving anonymity and traceability in WMNs in [4], [5]. Their system borrows the restrictive partially blind signature technique from payment systems [6], [7], [8] and hence can achieve the anonymity of unlinking user identities from activities, as well as the traceability of misbehaving users. Furthermore, the proposed pseudonym technique renders user location information unexposed. Unfortunately, we found that their scheme is not as secure as they claimed. In this paper, we demonstrate that Sun et al.'s scheme cannot trace the misbehavior clien (CL) even if it double-time deposits the same ticket.

The rest of this paper is organized as follows: Section 2 introduces some preliminaries. In Section 3, an overview of the ticket-based anonymity system with traceability property in WMNs is presented. An attack method to the ticket-based anonymity system is proposed in Section 4. We conclude in Section 5.

2 Preliminaries

2.1 IBC from Bilinear Pairings

ID-based cryptography (IBC) allows the public key of an entity to be derived from its public identity information such as name and e-mail address, which avoids the use of certificates for public key verification in the conventional PKI (public key infrastructure) [9]. Boneh and Franklin [10] introduced the first functional and efficient ID-based encryption scheme based on bilinear pairings on elliptic curves. Specifically, let $\mathbb{G}_1$ and $\mathbb{G}_2$ be an additive group and a multiplicative group, respectively, of the same prime order p. The Discrete Logarithm Problem (DLP) is assumed to be hard in both $\mathbb{G}_1$ and $\mathbb{G}_2$. Let P denote a random generator of $\mathbb{G}_1$ and $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ denote a bilinear map constructed by modified Weil or Tate pairing with the following properties:

1. Bilinear: $e(aP, bQ) = e(P, Q)^{ab}$, $\forall P, Q \in \mathbb{G}_1$ and $\forall a, b \in \mathbb{Z}_p^*$, where $\mathbb{Z}_p^*$ denotes the multiplicative group of $\mathbb{Z}_p$, the integers modulo p. In particular, $\mathbb{Z}_p^* = \{x | 1 \leq x \leq p-1\}$ since p is prime.
2. Nondegenerate: $\exists P, Q \in \mathbb{G}_1$ such that $e(P, Q) \neq 1$.
3. Computable: There exists an efficient algorithm to compute $e(P, Q), \forall P, Q \in \mathbb{G}_1$.

2.2 Security Definitions

We give the security concepts that are used in Sun et al.'s scheme as follows:

- Anonymity (Untraceability): The anonymity of a legitimate client refers to the untraceability of the client's network access activities. The client is said to be anonymous if the TA, the gateway, and even the collusion of the two cannot link the client's network access activities to his real identity.
- Traceability: A legitimate client is said to be traceable if the TA is able to link the client's network access activities to the client's real identity if and only if the client misbehaves, i.e., one or both of the following occurs: ticket-reuse and multiple-deposit.
- Ticket-reuse: One type of misbehavior of a legitimate client that refers to the client's use of a depleted ticket (val = 0).
- Multiple-deposit: One type of misbehavior of a legitimate client that refers to the client's disclosure of his valid ticket and associated secrets to unauthorized entities or clients with misbehavior history so that these coalescing clients can gain network access from different gateways simultaneously.
- Collusion: The colluding of malicious TA and gateway to trace a legitimate client's network access activities in the TA's domain (i.e., to compromise the client's anonymity).
- Framing: A type of attack mounted by a malicious TA in order to revoke a legitimate client's network access privilege. In this attack, the TA can generate a false account number and associate it with the client's identity. The TA can then create valid tickets based on the false account number and commit fraud (i.e., misbehave). By doing so, the TA is able to falsely accuse the client of misbehaving and thus revoke his access right.

2.3 Network Architecture

The wireless mesh backbone consists of mesh routers (MRs) and gateways (GWs) interconnected by ordinary wireless links. Mesh routers and gateways serve as the access points of the WMN and the last resorts to the Internet, respectively. Each WMN domain or trust domain (to be used interchangeably) is managed by a domain administrator that serves as a trusted authority (TA), e.g., the central server of a campus WMN. The TA and associated gateways are connected by high speed wired or wireless links, displayed as solid and bold dashed lines, respectively. TAs and gateways are

- *H. Wang is with the School of Information Engineering, Dalian Ocean University, No. 52 Heishijiao Street, Shahekou District, Dalian, Liaoning, China, P.C. 116023. E-mail: wanghuaqun@yahoo.com.cn.*
- *Y. Zhang is with the National Computer Network Intrusion Protection Center, GUCAS, Beijing, China, P.C. 100049. E-mail: zhangyg@gucas.ac.cn.*

Manuscript received 18 Aug. 2010; accepted 4 Oct. 2011; published online 26 Oct. 2011.
Recommended for acceptance by R. Sandhu.
For information on obtaining reprints of this article, please send e-mail to: tdsc@computer.org, and reference IEEECS Log Number TDSC-2010-08-0145. Digital Object Identifier no. 10.1109/TDSC.2011.53.

assumed to be capable of handling computationally intensive tasks. In addition, they are assumed to be protected in private places and cannot be easily compromised due to their important roles in the WMN. The WMNs of interest here are those where the TA provides free Internet access but requires the clients (CLs) to be authorized and affiliated members, generally for a long term, as the employees or students in the case of enterprise and hospital WMNs or campus WMNs. Such individual WMN domains can be building blocks of an even larger metropolitan WMN domain.

3 Reviewing Sun et al.'s Ticket-Based Scheme

We only restrict Sun et al.'s scheme within the home domain. The ticket-based security architecture consists of ticket issuance, ticket deposit, fraud detection, and ticket revocation protocols. Our paper designed the attack methods on the ticket issuance, ticket deposit, and fraud detection. So, we omit the ticket revocation protocol in the section. Some notations are used in Sun.'s scheme. We list them as follows:

$\rightarrow$: single-hop communications;

$\rightarrow\!\!\rightarrow$: multi-hop communications;

$||$: concatenation;

ID_x: the real identity of an entity x;

PS_x: the pseudonym self-generated by a client x by using his real identity ID_x;

$H_1(ID_x)/\Gamma_x$: public/private key of the entity x;

$PS_x/\widetilde{\Gamma_x}$: the self-generated pseudonym/private key pairs based on the above public/private key pairs;

$SIG_{\Gamma_x}(m)$: signature on a message m using Γ_x;

$VER(SIG)$: verification process;

$SKE_k(D)$: symmetric encryption on plaintext D using the shared secret key k;

$HMAC_k(m)$: keyed-hash message authentication code on a message m using k.

3.1 Ticket Issuance

The TA (i.e., Trusted Authority) publishes the parameters within its trust domain as $(p, \mathbb{G}_1, \mathbb{G}_2, e, P, P_1, P_2, H_1, H_2, H_3, P_{pub})$ using the standard IBC (i.e., identity based cryptography) domain initialization, where (P, P_1, P_2) are random generators of $\mathbb{G}_1$, and

$$\begin{aligned} &P_{pub} = \pi P \\ &e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2 \\ &H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1 \\ &H_2 : \mathbb{G}_1^3 \times \mathbb{G}_2^5 \rightarrow \mathbb{Z}_p^* \\ &H_3 : \mathbb{G}_2 \times \mathbb{G}_2 \times ID_{GW} \times time \rightarrow \mathbb{Z}_p^*, \end{aligned}$$

the order of $\mathbb{G}_1$ and $\mathbb{G}_2$ is p, $\mathbb{G}_1$ is a Gap Diffie-Hellman group. TA chooses $r \in_R \mathbb{Z}_p^*$ and $Q \in_R \mathbb{G}_1$, and the client chooses $\alpha, \beta, \gamma, \tau, \lambda, \mu, \rho \in_R \mathbb{Z}_p^*$. The ticket issuance protocol is demonstrated as:

1. $CL \rightarrow\!\!\rightarrow TA$:
   $ID_{CL}, m, t_1, HMAC_k(m||t_1)$;
2. $TA \rightarrow\!\!\rightarrow CL$:
   $ID_{TA}, X = e(m, \Gamma_{TA}), Y = e(P, Q), Z = e(m, Q)$,
   $U = rH_1(ID_{TA}), V = rP, t_2, HMAC_k(X||Y||Z||U||V||t_2)$;
3. $CL \rightarrow\!\!\rightarrow TA$:
   $ID_{CL}, t_3, HMAC_k(B||t_3)$,
   $B = \lambda^{-1}H_2(m'||U'||V'||R||W||X'||Y'||Z') + \mu$;
4. $TA \rightarrow\!\!\rightarrow CL$:
   $ID_{TA}, \sigma_1 = Q + B\Gamma_{TA}$,
   $\sigma_2 = (r+B)\Gamma_{TA} + rH_1(c), t_4, HMAC_k(\sigma_1||\sigma_2||t_4)$

At the end, the client checks if the following equalities hold: $e(P, \sigma_1) = y^B Y$ and $e(m, \sigma_1) = X^B Z$, where $y = e(P_{pub}, H_1(ID_{TA}))$. If the verification succeeds, the client calculates $\sigma_1' = \gamma\sigma_1 + \tau H_1(ID_{TA})$, $\sigma_2' = \lambda\sigma_2, \rho = \gamma B$, and outputs the signature $(U', V', X', \rho, \sigma_1', \sigma_2')$ on (TN, W, c), where $TN = m'$. In Step 3 above, $m = u_1 P_1 + u_2 P_2 = \Omega + u_2 P_2 \neq 0$, where $u_1 \in_R \mathbb{Z}_p^*$ and $u_2 = 1$, $m' = \alpha m$, $U' = \lambda U + \lambda\mu H_1(ID_{TA}) - \beta H_1(c)$, $V' = \lambda V + \beta P_{pub}$, $R = e(m', H_1(ID_{TA}))$, $W = g_1^{v_1} g_2^{v_2}$, where $g_1 = e(P_1, H_1(ID_{TA}))$, $g_2 = e(P_2, H_1(ID_{TA}))$, and $v_1, v_2 \in_R \mathbb{Z}_p^*$, $X' = X^\alpha, Y' = Y^\gamma g^\tau$, where $g = e(P, H_1(ID_{TA}))$, $Z' = Z^{\alpha\gamma} R^\tau$. Given m', W, the shared information c, and the tuple $(U', V', X', \rho, \sigma_1', \sigma_2')$, the verifier computes:

$$\begin{aligned} Y' &= e(P, \sigma_1')e(P_{pub}, H_1(ID_{TA}))^{-\rho} \\ Z' &= e(m', \sigma_1')X'^{-\rho} \end{aligned}$$

and accepts the signature if

$$\begin{aligned} &e(\sigma_2', P) \\ &= e(U' + H_2(m'||U'||V'||R||W||X'||Y'||Z')H_1(ID_{TA}), \\ &\quad P_{pub})e(H_1(c), V') \end{aligned}$$

holds. c is defined as $(val, exp, misb)$, where val, exp, and $misb$ denote the ticket value, expiry date/time, and the client's misbehavior level, respectively. c is the commonly agreed information negotiated at the beginning of the ticket generation algorithm. The valid ticket is $ticket = \{TN, W, c, (U', V', X', \rho, \sigma_1', \sigma_2')\}$ at the output, where T_N is the unique serial number of the ticket which can be computed from the client's account number Ω. $(U', V', X', \rho, \sigma_1, \sigma_2)$ is the signature on (TN, W, c), where W is necessary for verifying the validity of the signature in the ticket deposit protocol.

3.2 Ticket Deposit

After obtaining a valid ticket, the client may deposit it anytime the network service is desired before the ticket expires, using the ticket deposit protocol shown below. Sun et al.'s scheme restricts the ticket to being deposited only once at the first gateway according to val before exp.

1. $CL \rightarrow\!\!\rightarrow GW$:
   $PS_{CL}, m', W, c, \sigma = (U', V', X', \rho, \sigma_1', \sigma_2'), t_5$,
   $SIG_{\widetilde{\Gamma_{CL}}}(m'||W||c||\sigma||t_5)$;
2. $GW \rightarrow\!\!\rightarrow CL$:
   $ID_{GW}, d = H_3(R||W||ID_{GW}||T), t_6, HMAC_{k'}(d||t_6)$;
3. $CL \rightarrow\!\!\rightarrow GW$:
   $PS_{CL}, r_1 = d(u_1\alpha) + v_1$,
   $r_2 = d\alpha + v_2, t_7, HMAC_{k'}(r_1||r_2||t_7)$; and
4. $GW \rightarrow\!\!\rightarrow CL$:
   $ID_{GW}, misb, exp, t_8$,
   $SIG_{\Gamma_{GW}}(PS_{CL}||ID_{GW}||misb||exp||t_8)$.

At the end, the gateway checks if the equality $g_1^{r_1} g_2^{r_2} = R^d W$ holds. At the end of Step 1, the gateway will perform $VER(\sigma)$ before Steps 2 and 3 can proceed, and R can be derived as $R = e(m', H_1(ID_{TA}))$ from the received information. T is the date/time the ticket is deposited. A symmetric key k' can be derived locally by the gateway and the client as $k' = e(\Gamma_{GW}, PS_{CL})$, and $k' = e(H_1(ID_{GW}), \widetilde{\Gamma_{CL}})$, respectively, after learning each other's ID (or pseudonym). The deposited ticket record is $record = (ticket, r_1, r_2, T, rem, log)$, where rem and log denote the remaining value of the ticket and the logged data of the client's noncompliant behavior, respectively. The value of rem is initially set to val.

3.3 Fraud Detection

When the TA detects duplicate deposits using the ticket records reported by gateways, the TA will have the view of at least two

different challenges from gateways and two corresponding sets of responses from the same client. By solving the equation sets below based on these challenges and responses, the TA is able to obtain the identity information encoded in the message and hence the real identity of the misbehaving client. The fraud detection protocol is shown as:

$GW \rightarrow TA$: $ID_{GW}, m', W, c, \sigma = (U', V', X', \rho, \sigma'_1, \sigma'_2), r_1, r_2, T, t_9$, $HMAC_{k''}(m'||W||c||\sigma||r_1||r_2||T||t_9)$, where k'' is the preshared symmetric key between the gateway and the TA. The TA performs $VER(\sigma)$. If the signature is verified, the TA checks if m' (or TN) has been stored. If m' is not stored, the TA will store the following information: m', c, T, r_1, r_2 for future fraud detection. If m' has been stored, TA will compute the challenge $d = H_3(R||W||ID_{GW}||T)$ and accuse the gateway if d is the same as the stored one. If d is different, the TA can conclude that misbehavior has occurred and will reveal the identity information by the two sets of equations: $r_1 = d(u_1\alpha) + v_1, r_2 = d\alpha + v_2,\ r'_1 = d'(u_1\alpha) + v_1, r'_2 = d'\alpha + v_2$. TA solves for $u_1 = \frac{r_1 - r'_1}{r_2 - r'_2}$ and obtains the account number $\Omega = u_1 P_1$ to reveal the associated identity ID_{CL}.

4 Cryptanalysis of the Ticket-Based Scheme

In this section, we propose an attack on Sun et al.'s ticket-based anonymity scheme. We show that any CL can impersonate the TA to issue a ticket that cannot satisfy the message constraints. This means that the scheme's fraud detection cannot hold. We give the details as follows.

4.1 Forge Attack on the Ticket Issuance Protocol

Let c be the negotiated information. To obtain a ticket that cannot satisfy the restrictive $m' = \alpha m$, the CL performs the following protocol with TA as follows:

1. $CL \rightarrow\rightarrow TA$:
   $\{ID_{CL}, m, t_1, HMAC_k(m||t_1)\}$;
2. $TA \rightarrow\rightarrow CL$:
   - TA computes: $X = e(m, \Gamma_{TA}), Y = e(P, Q)$,
     $Z = e(m, Q), U = rH_1(ID_{TA}), V = rP$
   - TA sends to CL:

     $\{ID_{TA}, X, Y, Z, U, V, t_2, HMAC_k(X||Y||Z||U||V||t_2)\}$
3. $CL \rightarrow\rightarrow TA$:
   - CL computes: $\forall \sigma'_1, X', m' \in \mathbb{G}_1, \forall \rho, \lambda, \mu, \beta \in \mathbb{Z}_p^*$,
     $Y' = e(P, \sigma'_1)e(P_{pub}, H_1(ID_{TA}))^{-\rho}$,
     $Z' = e(m', \sigma'_1)X'^{-\rho}$,
     $U' = \lambda U + \lambda\mu H_1(ID_{TA}) - \beta H_1(c)$,
     $V' = \lambda V + \beta P_{pub}$,
     $R = e(m', H_1(ID_{TA}))$,
     $W = g_1^{v_1} g_2^{v_2}$,
     $B = \lambda^{-1} H_2(m'||U'||V'||R||W||X'||Y'||Z') + \mu$,
     where $g_1 = e(P_1, H_1(ID_{TA})), g_2 = e(P_2, H_1(ID_{TA}))$,
     $v_1, v_2 \in_R \mathbb{Z}_p^*$.
   - CL sends to TA: $\{ID_{CL}, B, t_3, HMAC_k(B||t_3)\}$
4. $TA \rightarrow\rightarrow CL$:
   - TA computes: $\sigma_1 = Q + B\Gamma_{TA}, \sigma_2 = (r + B)\Gamma_{TA} + rH_1(c)$
   - TA sends to CL: $\{ID_{TA}, \sigma_1, \sigma_2, t_4, HMAC_k(\sigma_1||\sigma_2||t_4)\}$
     CL computes $\sigma'_2 = \lambda\sigma_2$, and outputs the signature $(U', V', X', \rho, \sigma'_1, \sigma'_2)$ on (TN, W, c), where $TN = m'$.

The forged signature can pass the verification as follows:
According to the verification procedures, the verifier computes

$$\overline{Y'} = e(P, \sigma'_1)e(P_{pub}, H_1(ID_{TA}))^{-\rho}, \overline{Z'} = e(m', \sigma'_1)X'^{-\rho}.$$

Based on the forge procedures, $\overline{Y'} = Y', \overline{Z'} = Z'$. Thus,

$$H_2(m'||U'||V'||R||W||X'||\overline{Y'}||\overline{Z'}) = H_2(m'||U'||V'||R||W||X'||Y'||Z').$$

So,

$$\begin{aligned}
&e(\sigma'_2, P)\\
&= e(\lambda\sigma_2, P)\\
&= e(\lambda(r + B)\Gamma_{TA} + \lambda r H_1(c), P)\\
&= e(V', H_1(c))e(\lambda(r + B)\Gamma_{TA} - \beta P_{pub}, P)\\
&= e(U' + H_2(m'||U'||V'||R||W||X'||Y'||Z')H_1(ID_{TA}),\\
&\quad P_{pub})e(H_1(c), V')\\
&= e(U' + H_2(m'||U'||V'||R||W||X'||\overline{Y'}||\overline{Z'})H_1(ID_{TA}),\\
&\quad P_{pub})e(H_1(c), V').
\end{aligned}$$

Thus, the verifier accepts the forged signature $(U', V',\ X', \rho, \sigma'_1, \sigma'_2)$ on (TN, W, c), where $TN = m'$. As $m' \in_R \mathbb{G}_1$, it cannot satisfy the restrictive $m' = \alpha m$.

4.2 Attack on the Traceability

CL computes the unique account number $\Omega = u_1 P_1$, where $u_1 \in_R \mathbb{Z}_p^*$, and transmits Ω to TA and keeps u_1 secret. When CL wants to deposit a coin, CL first proves ownership of his account $\Omega = u_1 P_1$ and negotiates a common information c. According to our designed forge method, CL and TA perform the ticket issuance protocol, and CL can get a signed ticket $M' = \alpha u P_1 + \alpha P_2$ instead of $M' = \alpha u_1 P_1 + \alpha P_2$, where $u_1 \neq u \in_R \mathbb{Z}_p^*$. When CL and TA perform the deposit protocol twice with the same ticket $\{M', W, c\}$, TA can get the values:

$$\begin{aligned}
ticket &= \{M', W, c, (U', V', X', \rho, \sigma'_1, \sigma'_2)\},\\
record &= (ticket, r_1, r_2, T, rem, log),\\
record' &= (ticket, r'_1, r'_2, T', rem, log),\\
d &= H_3(R||W||ID_{GW}||T),\\
d' &= H_3(R||W||ID_{GW}||T'),
\end{aligned}$$

where $R = e(m', H_1(ID_{TA}))$, and $r_1 = d(u\alpha) + v_1, r_2 = d\alpha + v_2$, $r'_1 = d'(u\alpha) + v_1,\ r'_2 = d'\alpha + v_2$. TA can solve for $u = \frac{r_1 - r'_1}{r_2 - r'_2}$. As u has no any relationship with u_1, the information u cannot serve as a proof to trace the dishonest double-deposit, i.e., the traceability cannot be satisfied. Fraud detection fails.

5 Conclusion

We analyzed a ticket-based anonymity scheme in Sun et al.'s security architecture. Our attack showed that the client can impersonate the TA to sign some tickets that cannot satisfy the restrictivity. Based on the forge attack, we analyzed the fraud detection. Our analysis showed that Sun et al.'s ticket-based anonymity scheme cannot satisfy the traceability.

Acknowledgments

The authors sincerely thank the editor for allocating qualified and valuable referees. The authors sincerely thank the anonymous referees for their very valuable comments. This research is supported in part by the Natural Science Foundation of Liaoning Province (No.20102042), by the China Post-doctor Science Fund (No.20110490061), by the Program for Liaoning Excellent Talents in University (No.LJQ2011078), and by the Spanish government through project CONSOLIDER INGENIO 2010 CSD2007-0004 "ARES."

REFERENCES

[1] M. Raya and J-P. Hubaux, "Securing Vehicular Ad Hoc Networks," *J. Computer Security,* special issue on security of ad hoc and sensor networks, vol. 15, no. 1, pp. 39-68, 2007.
[2] S. Brands, "Untraceable Off-Line Cash in Wallets with Observers," *Proc. CRYPTO '93,* pp. 302-318, 1993.
[3] K. Wei, Y.R. Chen, A.J. Smith, and B. Vo, "Whopay: A Scalable and Anonymous Payment System for Peer-to-Peer Environments," *Proc. IEEE Intl'l Conf. Distributed Computing Systems,* 2006.
[4] J. Sun, C. Zhang, and Y. Fang, "A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks," *Proc. IEEE Conf. Computer Comm.,* pp. 1687-1695, 2008.
[5] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "SAT: A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks," *IEEE Trans. Dependable and Secure Computing,* vol. 8, no. 2, pp. 295-307, 2011.
[6] X. Chen, F. Zhang, Y. Mu, and W. Susilo, "Efficient Provably Secure Restrictive Partially Blind Signatures from Bilinear Pairings," *Proc. Financial Cryptography 2006,* pp. 251-265, 2006.
[7] X. Chen, F. Zhang, and S. Liu, "ID-Based Restrictive Partially Blind Signatures and Applications," *J. Systems and Software,* vol. 80, no. 2, pp. 164-171, 2007.
[8] X. Hu and S. Huang, "Analysis of ID-Based Restrictive Partially Blind Signatures and Applications," *J. Systems and Software,* vol. 81, no. 11, pp. 1951-1954, 2008.
[9] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Securing Mobile Ad Hoc Networks with Certificateless Public Keys," *IEEE Trans. Dependable and Secure Computing,* vol. 3, no. 4, pp. 386-399, Oct. 2006.
[10] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairings, *Advances in Cryptology-Asiacrypt 2001,* pp. 514-532, 2001.