An Authenticated Self-Healing Key Distribution Scheme Based on Bilinear Pairings

Biming Tian, Elizabeth Chang, Tharam S. Dillon, Song Han, and Farookh K. Hussain
DEBI Institute Curtin University of Technology, Australia
Biming.Tian@cbs.curtin.edu.au

Abstract— **Self-healing key distribution mechanism can be utilized for distributing session keys over an unreliable network. A self-healing key distribution scheme using bilinear pairings is proposed in this paper. As far as we know, it is the first pairing-based authenticated self-healing key distribution scheme. The scheme achieves a number of excellent properties. Firstly, the users can check the integrity and correctness of the ciphertext before carrying out more complex key recovery operations thus fruitless work can be avoided. Secondly, the scheme is collusion-free for any coalition of non-authorized users. Thirdly, the private key has nothing to do with the number of revoked users and can be reused as long as it is not disclosed. Finally, the storage overhead for each user is a constant.**

I. INTRODUCTION

One of the significant issues in wireless networks is how to securely distribute session keys for group communication. There have been two mainstream ways on addressing the above issue. One is aiming at the design of key distribution for reliable networks. The other is aiming at the design of key distribution for non-reliable networks. Most of existing schemes suppose that underlying networks are reliable. However, how to distribute session keys for unreliable wireless networks, in a manner that is resistant to packet loss, is an issue that has not been addressed deeply.

In an unreliable network, the key distribution broadcast for a particular session might never reach some users. Requiring re-transmissions would contribute to the traffic on the network which might already be heavily burdened. Especially, when communication group size is large, such re-transmissions could potentially exhaust the group manager. In addition, in some high security environments, it is suggested that only sending essential messages lest they make themselves vulnerable by revealing their location. Self-healing key distribution schemes enable large and dynamic groups of users over an unreliable network to establish group keys for secure communication. The goal of self-healing key distribution schemes is that even if in a certain session the broadcast is lost, the group users are still able to recover the session key from the broadcasts received before and after the session. Hence, non-interactive self-healing key distribution solutions are not only favorable but also necessary.

Self-healing key distribution appears to be quite useful in several settings in which session keys need to be used for a short time-period, due to frequent changes in the group structure. Military-oriented applications as well as Internet application [1], such as broadcast transmissions, pay-per-view TV, are some important examples which can benefit from such approaches. In addition, the self-healing method may be useful in commercial content distribution applications or electronic services in which the contents are highly sensitive.

In this paper, we will propose an authenticated self-healing key distribution scheme based on bilinear pairings. The main contribution of this paper is highlighted by the following properties:

- It is the first time to deal with self-healing key distribution scheme using pairing-based cryptology.
- It is the first time to address the authentication on self-healing key distribution scheme using efficient short signature.
- The scheme is collusion-free for any coalition of non-authorized users.
- The private key has nothing to do with the number of revoked users and can be reused as long as it is not disclosed.
- The storage overhead for users is a constant.

The rest of the paper is organized as follows: In section II, we present an overview of earlier works in the area of self-healing key distribution, ID-based cryptography and bilinear pairing, and short signature. In section III, we briefly introduce the preliminaries to be used in the design of self-healing key distribution protocol. In section IV, we give system parameters firstly and present concrete construction secondly. In section V, we analysis the security of the proposed scheme and make efficiency comparison with previous protocols. We conclude the paper in the last section.

II. RELATED WORKS

A. Self-healing Key Distribution Schemes

The notion of self-healing key distribution was introduced by Staddon et al. in [1]. Formal definitions, lower bounds on the resources as well as some constructions of self-healing key distribution scheme were proposed in it. Since then, self-healing key distribution has been one of the hot research topics. Liu et al. generalized the definitions in [1] and gave some constructions in [2]. The scheme reduced communication overhead and storage overhead by introducing a novel personal key distribution technique.

Subsequently, many works on self-healing key distribution were done in terms of improving efficiency or entitling some special features. More et al. in [3] used a sliding window

978-1-4244-2309-5/09/$25.00 ©2009 IEEE

to address the three problems in [1]. The three problems were inconsistent robustness, high overhead and expensive maintenance costs. Sáez in [4] considered the possibility that a coalition of users sponsor a user outside the group for one session. Muhammad et al. in [5] considered the possibility of idea of mutual-healing.

All of these schemes ([1]-[5]) took it for granted that the broadcast messages arrive the destination without any change. However, broadcast messages delivered over low-cost broadcast channels easily suffer from substitution and distortion attacks. This results in the additional requirement that the members must authenticate the integrity and correctness of the received broadcast messages.

Jiang et al. in [6] used TEK (Traffic Encryption Key) to prevent non-legitimate nodes from having access to the secret broadcast contents. TEK is re-keyed periodically instead of every node topology change thus there exists time delay. In dynamic communication group, session key must be updated on each membership change. Time delay will violate the forward and backward security of the scheme. Han et al. considered encrypting broadcast messages by TEK thus the integrity of broadcast messages can be kept. Two constructions of TEK were proposed in [13]. While both of them have shortcomings. The first construction introduces too much computation overhead for the group manager. The second construction does not fit for the new users.

B. Identity-based Cryptography and Bilinear Pairing

In 1984, Shamir [7] introduced the notion of ID-based cryptography to alleviate many of the problems inherent with managing certificates. Since then, many ID-based cryptographic schemes have been proposed using the bilinear pairing. In 2001, Boneh and Franklin in [8] proposed the first practical identity-based encryption scheme. Inspired by the idea of [8], Du et al. proposed a broadcast encryption scheme for key distribution in [9]. In this paper, we extend the broadcast encryption scheme for key distribution to a self-healing key distribution scheme.

C. Short Digital Signature

Short digital signature are essential to ensure the authenticity of messages in low-bandwidth communication and low-storage and less computation networks. Many short digital signature scheme have been proposed so far. One of the famous short signature scheme is BLS scheme which is introduced by Boneh et al. in [10]. This scheme is based on the CDHP (Computational Diffie-Hellman Problem) on elliptic curves and can be acquired from the private key extraction process of Boneh-Franklin's ID-based encryption scheme [8]. Shortly after that, Boneh et al. in [11] proposed another short signature scheme where signatures are almost as short as the former without random oracle model under a strong Diffie-Hellman problem assumption. Zhang et al. in [12] improved BLS scheme by substituting special hash functions with general cryptography hash functions. The security of this scheme relies on Inv-CDHP (Inverse Computational Diffie-Hellman Problem), which is a variation of CDHP, based on bilinear pairing. This scheme requires less pairing operation than BLS scheme thus more efficient. Our authenticated self-healing key distribution scheme adopts Zhang's short signature.

III. PRELIMINARIES

In this section, we briefly describe the bilinear pairing, Bilinear Diffie-Hellman (BDH) assumption and ID-based Public Key Infrastructure (PKI).

A. Bilinear Pairing and Related Assumption

Let G_1 and G_2 be two cyclic groups of order q for some large prime q. G_1 is a cyclic additive group and G_2 is a cyclic multiplicative group. We assume that the discrete logarithm problems in both G_1 and G_2 are hard. Let $e : G_1 \times G_1 \rightarrow G_2$ be a pairing which satisfies the following conditions:

- Bilinearity: $e(aP, bQ) = e(P, Q)^{ab}$, for $\forall\ P, Q \in G_1$ and $\forall\ a, b \in \mathbb{Z}_q^*$;
- Non-degeneracy: There exists $P \in G_1$ and $Q \in G_1$, such that $e(P, Q) \neq 1$;
- Computability: There exists an efficient algorithm to compute $e(P, Q)$ for any $P, Q \in G_1$.

1) BDH Parameter Generator: A BDH parameter generator $\mathcal{IG}$ is a probabilistic algorithm that takes a security parameter $0 < k \in \mathbb{Z}$, runs in polynomial time, and outputs the description of two groups G_1 and G_2 of the same order q and the description of an admissible bilinear map $e : G_1 \times G_1 \rightarrow G_2$.

DLP, CDHP, and Inv-CDHP are defined in the additive group G_1. According to **Theorem 1** in [12], CDHP and Inv-CDHP are polynomial time equivalent.

1) Discrete Logarithm Problem (DLP): Given two group elements P and Q, to find an integer $n \in \mathbb{Z}_q^*$, such that $Q = nP$ when such an integer exists.
2) CDHP: For $a, b \in \mathbb{Z}_q^*$, given P, aP, bP, to compute abP.
3) Inv-CDHP: For $a \in \mathbb{Z}_q^*$, given P, aP, to compute $a^{-1}P$.
4) BDHP (Bilinear Diffie-Hellman Problem): Given $\langle P, aP, bP, cP \rangle$ for some $a, b, c \in \mathbb{Z}_q^*$, computes $e(P, P)^{abc} \in G_2$.
5) BDH Assumption: There is no polynomial time algorithm to solve the BDH problem.

B. ID-Based Public Key Infrastructure

ID-based PKI (Public Key Infrastructure) involves a trusted KGC (Key Generation Center) and users. Users' private keys are calculated by KGC and sent to them privately. The basic operations consist of **Set up** and **Private Key Extraction**. When we use bilinear pairings to construct ID-based private/public keys, the operations can be implemented as follows: KGC runs BDH parameter generator to generate two groups G_1, G_2 and a bilinear pairing $e : G_1 \times G_1 \rightarrow G_2$. It chooses an arbitrary generator $P \in G_1$ and defines two cryptographic hash functions: $H_1 : \{0, 1\}^* \rightarrow G_1$, $H_2 : G_2 \rightarrow \{0, 1\}^*$.

- **Set Up:** KGC chooses a random number $s \in \mathbb{Z}_q^*$ and sets $P_{pub} = sP$. Then KGC publishes system parameters

$params = \{G_1, G_2, q, P, P_{pub}, H_1, H_2\}$, and keeps s as master-key, which is only known by it.

- **Private Key Extraction:** A user submits its identity information ID to KGC. KGC computes the user's public/private keys as $Q_{ID} = H_1(ID)$ and $S_{ID} = sQ_{ID}$, then returns the public/private keys to the user.

C. Zhang's Short Signature Scheme

Zhang's short signature scheme includes the following four steps:

1) ParamGen. The system parameters are $\{G_1, G_2, e, q, P, H\}$ where H is a hash function and the other parameters are defined as aforementioned.
2) KeyGen. Randomly chooses a random number $s \in \mathbb{Z}_q^*$ and sets $P_{pub} = sP$. The public key is P_{Pub}. The secret key is s.
3) Sign. Given the secret key s, and a message m, computes $S = \frac{1}{H(m)+s}P$. The signature is S.
4) Ver. Given the public key P_{Pub}, a message m, and a signature S, verify if

$$e(H(m)P + P_{pub}, S) = e(P, P). \tag{1}$$

The process of verification is as following:

$$\begin{aligned} & e(H(m)P + P_{pub}, S) \\ & \quad = e((H(m)+s)P, (H(m)P+s)^{-1}P) \\ & \quad = e(P,P)^{(H(m)+s)\cdot(H(m)+s)^{-1}} \\ & \quad = e(P,P). \end{aligned} \tag{2}$$

IV. THE PROPOSED SCHEME

A. Parameters

Let $U = \{u_1, \ldots, u_n\}$ be the finite universe of users. Each user u_i has a unique identifier ID_i. A broadcast unreliable channel is available, and time is defined by a global clock. GM (Group Manager) sets up and manages, by means of joining and revoking operations, a communication group which is a dynamic subset of users of U. GM has public key P_{pub} and private key s as aforementioned. m denotes the number of sessions. Let $G_j \subseteq U$ be the communication group established by the group manager in session j. Each node is preloaded with a public/private key pair (Q_i, S_i) before the deployment of networks. The public/private key pair is used to recover the session keys as long as u_i is not removed by GM from the group. Let $R_j \subseteq G_{j-1}$ denotes the set of revoked group users in session j and $J_j \subset U \setminus G_{j-1}$ denotes the set of users who join the group in session j with $R_j \cap J_j = \phi$. Hence, $G_j = (G_{j-1} \cup J_j) \setminus R_j$ for $j \geq 2$ and by definition $G_1 = U$. Moreover, for $j \in \{1, \ldots, m\}$, the session key K_j is randomly chosen by GM and according to uniform distribution. For any non-revoked user $u_i \in G_j$, the j-th session key K_j is determined by broadcast information B_j and its personal pbulic/private key pair (Q_i, S_i).

B. Construction

The authenticated self-healing key distribution scheme proposed in this paper is a computational security scheme. It includes several procedures. In the procedure of *Broadcast*, GM will sign the ciphertext which is used to recover session keys. Subsequently, at the beginning of *Key Recovery*, the users check the integrity and correctness of the ciphertext first. If the ciphertext is changed during the process of delivering, the group users will discard it.

1) Setup: GM obtains both public system parameters and all the public keys of possible users from ID-based PKI. GM chooses m session keys $K_1, \cdots, K_m$ from $\mathbb{Z}_q^*$. The session keys are independent to each other and according to uniform distribution.

2) Broadcast: Suppose $|G_j|$ denotes the number of users in session j. For each session $1 \leq j \leq m$, according to the public keys of users in the session group G_j, GM computes $Q_{V_1} = \sum_{i=1}^{n} Q_i$ and a $(|G_j|-1) \times |G_j|$ matrix is defined as follows:

$$\begin{pmatrix} a_2 \\ a_3 \\ \vdots \\ a_{|G_j|} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & \ldots & 0 \\ 1 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & 0 \\ 1 & 0 & 0 & \ldots & 1 \end{pmatrix} \tag{3}$$

Let $a_i^{'}$ represents the transpose of a_i. GM also constructers $|G_j| - 1$ auxiliary keys

$$Q_{V_i} = (Q_1, Q_2, \ldots, Q_{|G_j|}) \times a_i^{'} \quad 2 \leq i \leq |G_j| \tag{4}$$

which means $Q_{V_2} = Q_1 + Q_2$, $Q_{V_3} = Q_1 + Q_3$, $\ldots$, $Q_{V_{|G_j|}} = Q_1 + Q_{|G_j|}$. The broadcast message is then formed by computing, for a random $r_j \in \mathbb{Z}_q^*$,

$$U_1 = r_j P, \quad U_i = r_j Q_{V_i} \quad 2 \leq i \leq |G_j|, \tag{5}$$

$$V_j = K_j \oplus H_2(e(P_{pub}, r_j Q_{V_1})) \tag{6}$$

Let $z_j = (U_i (1 \leq i \leq |G_j|), V_j)$. The ciphertext for j-th broadcast in the following form:

$$B_j = \{z_1, \ldots, z_j\}. \tag{7}$$

GM signs the broadcast message as $Sign_j = \frac{1}{H(B_j)+s}P$. The signature is $Sign_j$. Finally, GM broadcasts the ciphertext together with the signature to the set of users G_j.

3) Key Recovery: When a user $u_i \in G_j$ receives the ciphertext B_j and signature $Sign_j$, it verifies the signature by computing $e(H(m)P + P_{pub}, Sign_j)$ like the following step:

$$\begin{aligned} & e(H(B_j)P + P_{pub}, Sign_j) \\ & \quad = e((H(B_j)+s)P, (H(B_j)+s)^{-1}P) \\ & \quad = e(P,P)^{(H(B_j)+s)\cdot(H(B_j)+s)^{-1}} \\ & \quad = e(P,P). \end{aligned} \tag{8}$$

If $e(H(m)P + P_{pub}, Sign_j) \neq e(P, P)$, it discards the incorrect message. Otherwise, it sets a vector $a_1 =$

$(0, \ldots, 0, 1, 0, \ldots, 0)$ with $|G_j|$ elements, and only the i-th element is 1. Then A_j is a $|G_j| \times |G_j|$ matrix

$$A_j = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_{|G_j|} \end{pmatrix}. \quad (9)$$

The user u_i can solve the following system of equations using Cramer's Rule or other algebraic methods.

$$(x_1, x_2, \ldots, x_{|G_j|}) \times A_j = (1, 1, \ldots, 1). \quad (10)$$

With $(x_1, x_2, \ldots, x_{|G_j|})$, u_i gets

$$(x_1, x_2, \ldots, x_{|G_j|}) \times \begin{pmatrix} Q_i \\ Q_{V_2} \\ \vdots \\ Q_{V_{|G_j|}} \end{pmatrix} = Q_{V_1}. \quad (11)$$

In order to decrypt the ciphertext, user u_i needs to compute $e(P_{pub}, r_j Q_{V_1})$, which with knowledge the private key S_i it can do via:

$$\begin{aligned} & e(P_{pub}, r_j Q_{V_1}) \\ &= e(P_{pub}, r_j(x_1 Q_i + x_2 Q_{V_2} + \ldots + x_{|G_j|} Q_{V_{|G_j|}})) \\ &= e(P_{pub}, r_j x_1 Q_i) \cdot e(P_{pub}, r_j(x_2 Q_{V_2} + \ldots + x_{|G_j|} Q_{V_{|G_j|}})) \\ &= e(r_j P, x_1 s Q_i) \cdot e(P_{pub}, x_2 r_j Q_{V_2} + \ldots + x_{|G_j|} r_j Q_{V_{|G_j|}}) \\ &= e(U_1, x_1 S_i) \cdot e(P_{pub}, x_2 U_2 + \ldots + x_{|G_j|} U_{|G_j|}). \end{aligned} \quad (12)$$

Then, u_i can recover the session key

$$K_j = V_j \oplus H_2(e(U_1, x_1 S_i) \cdot e(P_{pub}, \sum_{i=2}^{|G_j|} x_i U_i)). \quad (13)$$

4) Self-healing: Without loss of generality, suppose u_i lost the broadcast message for a session $t < j$. As far as it belongs to the session group G_t, it picks up the polynomial z_t from broadcast message B_j and forms the $|G_t| \times |G_t|$ matrix A_t as operations in the procedure of *Key Recovery*. Then, u_i solves the following system of equations.

$$(x_1, x_2, \ldots, x_{|G_t|}) \times A_t = (1, 1, \ldots, 1). \quad (14)$$

With $(x_1, x_2, \ldots, x_{|G_t|})$, u_i gets

$$(x_1, x_2, \ldots, x_{|G_t|}) \times \begin{pmatrix} Q_i \\ Q_{V_2} \\ \vdots \\ Q_{V_{|G_t|}} \end{pmatrix} = Q_{V_1}. \quad (15)$$

After that, with the knowledge of its effective private key S_i, u_i computes $e(P_{pub}, r_t Q_{V_1})$.

$$\begin{aligned} & e(P_{pub}, r_t Q_{V_1}) \\ &= e(P_{pub}, r_t(x_1 Q_i + x_2 Q_{V_2} + \ldots + x_{|G_t|} Q_{V_{|G_t|}})) \\ &= e(P_{pub}, r_t x_1 Q_i) \cdot e(P_{pub}, r_t(x_2 Q_{V_2} + \ldots + x_{|G_t|} Q_{V_{|G_t|}})) \\ &= e(r_t P, x_1 s Q_i) \cdot e(P_{pub}, x_2 r_t Q_{V_2} + \ldots + x_{|G_t|} r_t Q_{V_{|G_t|}}) \\ &= e(U_1, x_1 S_i) \cdot e(P_{pub}, x_2 U_2 + \ldots + x_{|G_t|} U_{|G_t|}). \end{aligned} \quad (16)$$

Finally, u_i recovers the lost session key:

$$K_t = V_t \oplus H_2(e(U_1, x_1 S_i) \cdot e(P_{pub}, \sum_{i=2}^{|G_t|} x_i U_i)) \quad (17)$$

If more than one broadcast messages get lost, the operations of session keys recovery is the same as aforementioned.

5) Adding and Revoking User: If GM wants to add a new user u_{new} to session j, in the procedure of *Broadcast*, GM constructs a new $(|G_j| - 1) \times |G_j|$ matrix and computes new $Q_{V_i} (1 \leq i \leq |G_j|)$ which includes Q_{new}.

If GM wants to revoke a user u_{rov} in session j, what GM should do is constructing a new $(|G_j| - 1) \times |G_j|$ matrix and computing new $Q_{V_i} (1 \leq i \leq |G_j|)$ which excludes Q_{rov}.

The adding and revoking operations are very efficient in our scheme. There is no interaction between the GM and other group members. For the condition that more than one user joining or revoking, the operations preform as aforementioned.

V. ANALYSIS OF PERFORMANCE

In this section, we analyze the security of the proposed scheme firstly. Then we analyze the efficiency of the proposed scheme in terms of storage overhead, computation overhead and communication overhead.

A. Analysis of Security

According to the *Construction* described in Section IV, we can say that our construction realizes an authenticated self-healing key distribution scheme using bilinear pairings. It is the first time to address the authentication on broadcast messages in self-healing key distribution scheme using short signature. This scheme is simple and avoid the deficiencies that incurred by [6] and [13]. According to the exact security proofs for the signature scheme in [12], the signature is secure under the random oracle model. In the procedure of *Key Recovery*, the receivers will first check the validity of the signature. If the verification fails, the broadcast message must be changed during the transmission. The receivers will not waste time on the useless broadcast message.

While in general self-healing key distrusting scheme without augmentation, the users do not know whether the recovered session keys are correct or not.

The scheme is collusion-free for any coalition of non-authorized users. In this scheme, if a user wants to obtain session keys, it should compute $e(U_1, x_1 S_i)$ in the procedure of *Key Recovery*. Therefore, only the authorized users can recover the session key. In addition, due to the difficulty of DLP, any coalition of non-authorized users can not derive the private keys of authorized users from their public keys. Furthermore, session keys are independent to each other and according to uniform distribution, which subsumes forward security and backward security of the scheme.

In previous secret sharing-based self-healing key distribution schemes, the personal key could be reused on the condition that less than the threshold number of users were revoked. In this paper, private key has nothing to do with the number of revoked users and can be reused as long as it is not

disclosed. In addition, our scheme enables a user to recover from a single broadcast message all the session keys for which it belongs to the associated session groups.

B. Analysis of Efficiency

Different from the previous papers, we take advantage of a broadcast encryption and short signature to design a self-healing key distribution scheme. As far as we know, it is the first paper of pairing-based authenticated self-healing key distribution scheme. In this section, we analyze the efficiency of the scheme.

There is a reasonable assumption that the group manager takes up more resource than ordinary users thus can store more information and perform more complex computation as well as communication. This is the reason that in the process of efficiency analysis, we only elaborate on analyzing the various overheads for ordinary users.

In terms of storage overhead, each user only stores its public/private key pair. Therefore, the storage overhead for each user is a constant. Because H_1 is a mapping from $\{0,1\}^*$ to G_1 and the order of G_1 is q, so the length of all the public keys is $logq$. The private keys are computed from the master key $s \in \mathbb{Z}_q^*$ and the public key, so the size of private keys is $logq$. Therefore, the storage overhead for each group user is $2logq$, which is a constant number.

All the computation in the procedure of *Key Recovery* is as follows: (1) Solving a set of linear equations with $|G_j|$ variables; (2) $|G_j|+1$ scalar multiplications in the group G_1; (3) $|G_j|$ additions in the group G_1; (4) Three pairings computation. One is for the verification of signature and the other two for recovering the session key; (5) One hashing computation; (6) One XOR operation. Generally speaking, bilinear pairing computation is more time-consuming than scalar multiplication, let alone addition, hash and XOR operation. Therefore, the main computation overhead comes form (4).

The communication overhead comes from ciphertext $B_j = \{z_1, \ldots, z_j\}$ and the signature $Sign_j$. z_j is composed of $U_i (1 \le i \le |G_j|)$ and V_j. The size of $U_i (1 \le i \le |G_j|)$ is $2logq$ and the size of V_j is $logq$ bits. Therefore, the length of z_j equals to $(2|G_j|+1)logq$, which is increases in direct proportion to $|G_j|$. The signature $Sign_j = \frac{1}{H(B_j)+s}P$ is a point in G_1, so the bit size of the signature is $2logq$. Consequently, the bit size of broadcast message is $[\sum_{i=1}^{j} 2|G_i| + (j+2)]logq$, which is related to the total number of users in all the communication group $\sum_{i=1}^{j}|G_i|$ and increases in direct proportion to the sequence of session j. In fact, this is the shortcoming of this scheme. In future works, we will address this problem and find ways to shorten the length of broadcast messages.

VI. Conclusion

An authenticated pairing-based self-healing key distribution scheme is proposed in this paper. The new scheme achieves good features. Above all, the short signature keeps the integrity and correctness of the ciphertext without introducing too much computation overhead. Secondly, the scheme is collusion-free for any coalition of non-authorized users, private key has nothing to do with the number of revoked users and can be reused as long as it is not disclosed. While in secret sharing-based self-healing key distribution schemes, the personal key can be reused on the condition that less than threshold number users are revoked. At the same time, the constant storage overhead is kept in this scheme. Furthermore, session keys are independent to each other and according to uniform distribution and thus forward security and backward security are kept. In addition, our scheme enables a user to recover from a single broadcast message all session keys for the corresponding session groups which it belongs to.

References

[1] J. Staddon, S. Miner, M. Franklin, D. Balfanz, M. Malkin, and D. Dean, *Self-healing Key Distribution with Revocation*, Proceedings of IEEE Symposium on Security and Privacy, pp.224-240, 2002.

[2] D. Liu, P. Ning, and K. Sun, *Efficient Self-healing Key Distribution with Revocation Capability*, Proceedings of the **10**th ACM, 2003.

[3] S. M. More, M. Malkin, J. Staddon, and D. Balfanz, *Sliding Window Self-healing Key Distribution with Revocation*, ACM Workshop on Survivable and Self-Regenerative Systems, pp.82-90, 2003.

[4] G. Sáez, *Self-healing Key Distribution Schemes with Sponsorization*, International Federation for Information Processing IFIP**'05**, LNCS, Vol.3677, pp.22-31, 2005.

[5] J. B. Muhammad and and M. Ali, *Self-healing Group Key Distribution*, International Journal of Network Security, Vol.1, No 2, pp.110-117, 2005.

[6] Y. Jiang, C. Lin, M. Shi, and X. shen, *Self-healing Group Key Distribution with Time-limited Node Revocation for Wireless Sensor Networks*, Ad hoc Networks 5, pp.14-23, 2007.

[7] A. Shamir, *Identity-Based Cryptosystems and Signature Scheme*, Proceedings of Cryptology**'84**, pp.47-53, 1984.

[8] D. Boneh and M. Franklin, *Identity Based Encryption From the Weil Pairing*, Advanced in Cryptology-CRYPTO**'01**, pp.213-229, 2001.

[9] X. Du, Y. Wang, J. Ge, and Y. Wang, *An ID-Based Broadcast Encryption Scheme for Key Distribution*, IEEE Transactions on Broadcasting, Vol.51, No.2, pp.264-266, June 2005.

[10] D. Boneh, B. Lynn, H. Shacham, *Short signature from the Weil pairing*, Proceeding of Asiacrypt**'01**, LNCS, Vol.2248, pp.514-532, 2001.

[11] D. Boneh, X. Boyen, *Short signature without random oracles*, In Proceedings of EUROCrypto**'04**, LNCS, Vol.3027, pp.56-73, 2004.

[12] F. Zhang, R. Safavi-Naini, W. Susilo, *An efficient signature scheme from Bilinear pairings and Its application*, Proceedings of PKC 2004, LNCS, Vol.2947, pp.277-290, 2004.

[13] S. Han, B. Tian, M. He, and E. Chang, *Efficient Threshold Self-healing Key Distribution with Sponsorization for Infrastructureless Wireless Networks*, IEEE Transactions on Wireless Communications, Accepted, 2008.