ID- Based Multiuser Signature Schemes And Their Applications

Vandani Verma , Shivani Rawat

Abstract: Threshold signature scheme works on the principle that if a secret/shadow is divided into n shadows or parts such that this shadow can be recreated only if all the shadows are available. If any one of the shadow is unavailable then it cannot be recreated. Multiuser signatures have different variants like ring signatures, group signatures, threshold signature schemes and many more. The paper focuses on threshold signature schemes. The main aim of this paper is to formalize the concept of identity-based threshold signature and give the provably secure scheme based on the bilinear pairings. In this paper, we proposed a new ID-based threshold signature scheme from bilinear pairings which is provably secure in random oracle model. We also discussed how threshold signatures can be applied for security of data in cloud computing.

Keywords: Bilinear Pairings, General Phases of Threshold Signature Scheme, Key Generation, ID Based Threshold Signature Scheme, Threshold Signatures, Cloud Computing, Security Analysis.

1. INTRODUCTION

For decentralizing the power to sign a message, threshold signatures [5] can be considered as a useful tool. A major motivation for ID-based signature which was proposed by Shamir is authentication of messages in which exchange of public keys or keeping public key directories is not needed. ID-based signature has one major advantage i.e. signing of message is allowed by one person in such a way that verification of signature can be done by any user using the identifier of signer such as email address instead of using his/her digital certificate. A digital signature can be defined as a mathematical technique which is used to validate the authenticity and integrity of a message, digital document or a software. Digital signatures provide easy transportability, imitation cannot be done by anyone and can be time stamped automatically. Using various cryptographic primitives, many contributions have been done to this field. Several forms of digital signatures are proxy signatures, ring signatures, blind signatures and so on. In 1982, David Chaum introduced the notion of blind signatures. In 2001, Shamir et al.[4] formalized the ring signatures. Zhang and Kim proposed ID-based blind signature and ring signature using bilinear pairings for simplification of key management. The concept of threshold proxy signature was proposed by Kim et al.[1] and Zhang et al.[2] in 1997. Later on, in 2004, first threshold proxy signature scheme from bilinear pairings was proposed by Qian et al.[6]. Subsequently, many threshold proxy signature schemes were proposed. Hwang et al.[3] was first one to propose multi-proxy signature scheme which is a special case of threshold proxy signature scheme. In the year 1987, the concept of the threshold signature was introduced by Desmedt. Well, introduced an identity-based threshold signature scheme. Also, independently Zhang with nonrepudiability introduced the very first proxy threshold signature. In 2009, it was proved that the scheme by Zhang does not possess nonrepudiability. 2000 was the year in which M.S. Hwang showed that even the scheme by Sun was weak in context of the security. Hsu in year 2001 proved that the scheme by Sun can be easily attacked by conspiracy. Then, again in 2003 Hwang explained how the scheme by Hsu is vulnerable to the insider attack. A vigorous interest was quiet visible for the proxy threshold signature in the year 2004 by the publications. 2005 was year when the security for the threshold signature with the efficiency and the practicability were very much emphasized. Then some more interesting schemes were proposed in the year 2006. In 2007, it was proved the warrant attack can be easily made on the scheme by Yang by Shao . In 2009 again, the scheme by Yang is very much vulnerable to the public key substitution attack and the frame attack, this was explained by Jianghong.

2. BILINEAR PAIRINGS

Bilinear pairings or mappings can be defined as a function

\[ e : G_1 \times G_2 \rightarrow G_r \]

where \( G_1 \) and \( G_2 \) are cyclic groups under addition and \( G_r \) is cyclic group under multiplication of order p which satisfies following properties :-

- **Bilinearity**: \( e (cP, dQ) = e (P,Q)^{cd} \forall P \in G_1 \text{ and } Q \in G_2 \text{ and } c,d \in \mathbb{Z}_q^* \)
- **Non-degeneracy**: \( e (P,P) \neq 1 \)
- **Computability**: e (P,Q) can be calculated by using an efficient algorithm \( \forall P \in G_1 \text{ and } Q \in G_2 \).

2.1 Relationships between \( G_1, G_2 \) and \( G_r \)

- Since \( G_1, G_2, G_r \) are cyclic groups of same order so they are isomorphic to each other.
- \( G_1, G_2, G_r \) are different group because we represent the element and perform different operations.
Since $G_1$ and $G_2$ are isomorphic :: $G_1 = G_2$. Let us take $G_1 = G_2 = G$

- G and $G_2$ are groups of either prime or composite order.
- If $G = G_2$, then we call it a self-bilinear map.

### 3. GENERAL PHASES OF THRESHOLD SIGNATURE SCHEME

A general $(t, n)$ threshold signature scheme has the following phases:

#### 3.1 Setup
- Given security parameter ‘k’ it outputs the public parameters.

#### 3.2 Key Generation
- On inputting the master key, identity ID and public parameters- it outputs the public and secret key of the users.

#### 3.3 Secret Share Generation
- Given a message ‘m’, random numbers, a polynomial and public key of the signing group it generates the secret share of each group member.

#### 3.4 Signature Generation
- Given secret share of the group members, message ‘m’ and public parameters any ‘t’ out of ‘n’ members can generate the threshold signatures on message ‘m’.

#### 3.5 Signature Verification
- Given message signature pair and public key of the signing group, it verifies whether the signatures are accepted or rejected.

### 4. PROPOSED ID- BASED THRESHOLD SIGNATURE SCHEME USING BILINEAR PAIRINGS

#### 4.1 SIGNATURE ALGORITHM[10]

##### (A) Setup

Public parameters ‘params’ are generated by key generating centre (KGC). A master public – private key pair (MPK, MSK) is obtained by inputting the security parameter $k \in IN$. e: $G_1 \times G_1 \rightarrow G_2$ is bilinear mapping where $(G_1, +)$ is a cyclic group under addition with P as generator and $(G_2, .)$ is a cyclic group under multiplication. $P_{pubc} = sP$ is the public information that is provided by bilinear mapping where s is the master secret key (msk). Three hash functions are defined as $H_1 : \{0,1\}^* \rightarrow G_1$, $H_2 : G_2 \rightarrow \{0,1\}$, $H_3 : \{0,1\} \times \{0,1\} \rightarrow Z_q$. The message is $m = \{0,1\}$ and the cipher text is $C = Z_q \times \{0,1\} \times \{0,1\}$. < $G_1$, $G_2$, mpk, e, p, $H_1$, $H_2$, $H_3$ > are scheme parameters denoted by ‘params’.

##### (B) Key Generation

KGC executes it once for every user who has registered with him. In this, the secret/private key $S_{ID}$ is computed by taking identity $Q_{ID}$ of user U and msk as input i.e. $Q_{ID} = H_1(ID_U) \in G_1$ is computed by taking $ID_U$ as input where the string ID $\in \{0,1\}$, $S_{ID} = sQ_{ID}$.

##### (C) Signature Generation

Step1: arbitrary $\mu \in \{0,1\}^*$ is chosen by Alice.

Step2: calculates $r = H_2(\mu, m)$

Step3: calculates $Y = e(P_{ID}, P_{pubc})$

Step4: calculates $T_2 = rp$, $T_3 = r^*S_{ID}$

$< T_2, T_3 > = \sigma$ is the signature on message m.

##### (D) Signature Verification

Given a message me $\{0,1\}^*$ , a signature $\sigma = < T_2, T_3 >$, user verifies the signature and accepts iff $e(T_3, T_2) = e(r^{-1}S_{ID}, rP)$ holds $e(T_3, T_2) = e(r^{-1}S_{ID}, rP)$

$= e(sQ_{ID}, P)^{-1}$

$= e(Q_{ID}, sP)$

$= e(Q_{ID}, P_{pubc})$

### 4.2 ID-BASED THRESHOLD SIGNATURE SCHEME USING BILINEAR PAIRINGS

The two algorithms involved in the construction of ID-based threshold signature scheme are as follows :-

##### (A) Keyshare

The private key $S_{ID}$ with identity $Q_{ID}$ can be distributed among n parties $P_1, P_2, \ldots, P_n$ as follows:

(a) A random no. $r = H_3(\mu, m)$ is chosen by Alice and calculates $T_2 = rp$ and $T_3 = rS_{ID}$. To check the validity of public information $(T_2, T_3)$ each party $P_i$ checks equation

$e(T_3, T_2) = e(Q_{ID}, P_{pubc})$

(b) Alice selects an equation $X = S_{ID}S_1 \ldots S_nP$ where $X_1 = S_2P$, $X_2' = S_3X_1'$, $X_3' = S_4X_2' \ldots S_nP_{pubc}$. Figure the resulting signature by computing $D = e(T_3, T_2) = e(r^{-1}S_{ID}, rP)$.

##### (B) Tsign

Let m be an message to be signed. The signature is jointly created by n parties $P_1, P_2, \ldots, P_n$ as follows:

(a) The partial signature $D_i = \mu_i T_2$ is generated by each party $P_i$ and then broadcasts $D_i$. Verification of validity of signature share $D_i$ due to player $P_i$ can be done by checking equation

$e(D, P) = e(T_2, \sum_{\mu_i}(b)P_{\mu_i})$

(b) The full signature is reconstructed by each party locally as follows: Using the above verification equation, he first finds $t+1$ valid signature shares. Suppose $\omega$ is the set of $t+1$ players necessary for generation of valid signature share. $< T_2, T_3 > = \sigma$ is the resulting signature by computing $D = \sum_{\mu_i} L_{\omega_i} i(0) D_i$, where $L_{\omega_i}, i(0)$ is our lagrange coefficient such that $\mu_i \times \sum_{\mu_i} L_{\omega_i}, i(0) \mu_i$
Correctness of this threshold signature scheme can be easily seen. In fact:
\[ D = \sum_{i \in \omega} L \omega, \quad i(0) = \sum_{i=0}^{j} b^j (\mu, m) = \sum_{i \in \omega} L \omega, \quad i(0) \mu T_2 = \mu T_2 \]

5. APPLICATION OF THRESHOLD SIGNATURES IN CLOUD COMPUTING

For outsourced data in cloud computing [9], two basic things that are necessary for security are data confidentiality and access control. Sometimes, we forget about performance of systems (DO, CSP, users) when we emphasize more on security of data. For example, we sometimes use too many keys in order to secure data. As keys are confidential, security and maintenance of keys is needed which is an additional work. Performance of system is affected by these additional works. So, reduction in the number of keys is desirable. So, we need a scheme which provides data security and maintains performance.

Group – key scheme is proposed in [7]. In group – key scheme, there is a single key for decryption process for each group of users and key is known to all users of the group. Here, there is a reduction in no. of keys but a problem of collusion attack of CSP and a user is present because the whole data of the group can be leaked by a single malicious user to CSP. CSP cannot be trusted as it can use data of the data owner for its commercial benefits. Data secrecy and access control is achieved in [8]. In this scheme, symmetric keys are used for data encryption and only owner of data and corresponding users of data know the symmetric keys. CSP stores the encrypted data. As data is encrypted, data can’t be accessed by CSP. Whole data security is provided by this scheme but corresponding to each user there is associated a key and in some applications, number of users may increase. So, there is an increase in the no. of keys. Hence, maintenance and security concerns of keys increases. In the field of data storage and computation, cloud computing is a new and fast growing technology. It provides services such as computing and storage at very attractive cost. Services are provided according to three fundamental service models –

(a) IaaS-Infrastructure as a service
(b) PaaS-Platform as a service
(c) SaaS-Software as a service

Attributes of cloud computing are - self service, on-demand service, location independent, rapid elasticity and measured scale service. These characteristics of cloud computing are exploited by industries and institutions to increase their profit and revenue. So, businesses of industries are shifting towards cloud computing. However, one of the major obstacle in the way of cloud computing is data safety. It is believed by some people that cloud is not a safe place and once your data is send to the cloud, your control loses. They may be right or wrong. External servers stores and processes the data of data owners. So, confidentiality, integrity and access of data become more vulnerable. Since, commercial service providers operate external servers, data owners can’t trust on them as they can spoil businesses of data owners by using data for their benefits. Also, trust cannot be done on the users as they may be malicious. To ensure security requirements many schemes are given but they are suffering from collusion attack of malicious users and heavy computation (use of large no. of keys) and cloud service provider. A scheme is proposed to address these issues. Three entities are involved in this scheme: Data owner (DO), cloud service provider (CSP) and users. On the basis of location, project and department, users are divided in groups and each group has a single key for both encryption and decryption of data. Parts of key are shared by each user in the group. When atleast threshold no. of users will be present, data can be decrypted. Reduction of no. of keys and data confidentiality by all means is provided by this scheme. Authorised data and operations for a user are specified in capability list. In this paper, modified Diffe-Hellman algorithm is used for generation of one time shared session – key between CSP and user so that data can be protected from outsiders. In order to ensure data integrity MD5 (Hash algorithm) is used by the approach.
6. SECURITY ANALYSIS OF THRESHOLD SIGNATURE SCHEME

Following are the security requirements for threshold signature scheme:

6.1 Strong unforgeability- A valid threshold signature can be created for the original signer by the threshold signer. But neither the threshold signer nor the third party can create the threshold signature having the name of threshold signer.

6.2 Strong unrepudiability- Once valid threshold signature is generated by threshold signer for the original signer then the signature creation cannot be repudiated against anyone by him or her.

6.3 Strong identifiability- From the threshold signature the threshold signer’s identity can be determined by anyone.

6.4 Verifiability- If there is an agreement by the original signer from its corresponding threshold signature then any verifier can be very well convinced.

6.5 Prevention of misuse- There is a restriction on threshold signer to transfer the respective threshold key to anyone else. If by chance something like that happens that is the threshold signer does transfer the key to someone else then the threshold signer’s responsibility is well determined by the warrant itself.

7. CONCLUSION

In an age of explosive worldwide growth of electronic data storage and communications, there is a requirement of protecting vital information. Cryptography is a very powerful tool for protecting information. In this paper, we proposed a new ID-based threshold signature scheme which is provably secure in the random oracle model in the presence of t malicious players. Also, we have studied how threshold signatures can be used for data security in cloud computing. When we compare the performance of the schemes, the efficient one turns out to be the one having the bilinear pairings.

8. REFERENCES


Fig 2. Security and Privacy for Storage and Computation in Cloud Computing