Certificate-Based Encryption Scheme with General Access Structure

Tomasz Hyla[1] and Jerzy Pejaś[1]

West Pomeranian University of Technology in Szczecin
Faculty of Computer Science and Information Technology, Poland
{thyla, jpejas}@wi.zut.edu.pl

Abstract. The protection of sensitive information is very important, but also a difficult task. It usually requires a centralised access policy management and control system. However, such solution is often not acceptable in the era of users' mobility. In the paper we propose a certificate-based group-oriented encryption scheme with an effective secret sharing scheme based on general access structure. The special design of the scheme ensures that the shared secret (encryption key information), a collection of shareholders, and the access structure can be dynamically changed without the need to update the long-term keys and shares owned by shareholders. It is also possible to delegate the access rights to another member of the qualified subgroup or to a new entity from outside the current access structure.

Keywords: information protection, general access structure, cryptographic access control, certificate-based cryptosystems.

1 Introduction

The user and information mobility is an important feature of IT systems, which have to be considered during the design of the mechanisms for protection of sensitive information. The mobility enables creation of many new and exciting applications, and makes life much easier for mobile workers as well. Mobile devices, i.e. laptops, tablets and smartphones, often contain sensitive information, e.g. personal data, address books, files with valuable information (e.g. contracts, orders, projects). The information is usually downloaded from the network, where it can be stored by third parties.

The ability to download information from the network is crucial for the working comfort of the mobile user: regardless of where the user is, the information is always at hand. On the other hand the information stored in network by third parties subject to the risks and vulnerabilities associated with information security, i.e. anonymity, information retrieval, loss, theft and interception.

One method to reduce some of these risks is to store the information in an encrypted form. However, such solution limits the users' ability to selectively share their encrypted information at a fine-grained level. We need to control the access to

the information, but the access control mechanisms should allow granting access according to a number of different constraints depending on the user privileges.

The most effective solution of the user and information mobility problem can be achieved by using cryptographic access control mechanisms. These mechanisms allow to store the information in the network in an encrypted form and to be decrypted only by authorised users.

Cryptographic access control mechanisms are typically implemented in two stages. At the first stage the information is encrypted (according to some pre-defined access control policy) and is made available on a public server. At the second stage the encrypted information can be collected by any entity. However, the information can be read only by an entity that meets the requirements specified in the access policy related to the encrypted information. A group-oriented cryptosystem, where a group of participants cooperatively decrypt the ciphertext, is the solution to this kind of task.

1.1 Related Works

The concept of a group-oriented cryptosystem was first introduced by Y. Desmedt in [1] and is based on cooperation of designated authorized subsets of participants (an access structure). In group-oriented cryptography a sender firstly determines an access structure suitable to a receiving group of users and then sends an encrypted information or stores it in some localisation. Only authorized subsets of users in the group can cooperatively recover the message.

Many group-oriented decryption schemes are based on a traditional certificate-based PKI, on an identity-based public key cryptography (ID-PKC) or on a certificateless public key cryptography (CL-PKC). However, the need for PKI supporting certificates is considered as the main drawback for deployment and management of the traditional PKI. On other hand, the main disadvantages of ID-PKC and CL-PKC are the lack of authentication of TAs and end users. C. Gentry in [2] introduced the solution that comes naturally. This solution combines the merits of traditional public key infrastructure (PKI) and identity-based cryptography. Primarily it was used for encryption and was called certificate-based encryption, but it was quickly generalised for certificate-based signature schemes [3].

There are many works on ID-based threshold decryption scheme [4, 5] that combines ID-based cryptography with threshold decryption. Considerable less effort is devoted to ID-based group-oriented decryption scheme with general access structure [6-8]. This is due to the greater popularity of threshold secret sharing methods and their simplicity in the case of a large number of subgroups belonging to the access structure. However, to realise the selective access control to information, i.e. to solve the problem of the user and information mobility, the ID-based group-oriented decryption schemes with general access structure are more suitable.

1.2 Our Contributions

In this work we firstly contribute the definition, formalization and generic feasibility of group encryption. Next, we construct a new certificate and ID-based group-oriented decryption scheme with general access structure (CIBE-GAS), and investigate its related practical and theoretical properties. The CIBE-GAS scheme is more suitable, comparing to threshold secret sharing methods, when the same access rights to decrypt data should be selectively assigned to all participants belonging to the same well defined group of users.

The proposed certificate-based encryption scheme with general access structure (CIBE-GAS, Section 3) combines three different ideas: the secret sharing scheme [9], publicly available evidence of being a member of a particular group [10] and Sakai-Kasahara IBE (SK-IBE) scheme [11] with technique introduced by Fujisaki and Okamoto [12]. Such approach allows to achieve the new group encryption scheme with following features:

(a) the originator is not required to know the structure of qualified subsets, members of which are authorised to decrypt the information; he simply encrypts it, no designated group having in mind, and then decides who should be able to decrypt it (the value C_5 by Eq. (14) can be calculated at any time);
(b) there is no need to designate a specific recipient of encrypted information - each member within a qualified subset can decrypt it (Section 3, Decryption algorithm); moreover, a sender can temporarily remove some subgroups from having access rights to encrypted information, i.e. a sender can arbitrarily select the recipients by overlaying the appropriate filter on the access structure;
(c) the CIBE-GAS scheme is the certificate and ID-based encryption scheme (Section 3); it means, compared to the certificateless schemes, that partial key created by TA is published as a certificate and allows simplifying the user's identity verification.

Furthermore, the CIBE-GAS scheme has special construction of the public component $k_{i,j}$ (Section 3, Eq. (7)), which (a) protects the scheme against dishonest shareholders and unauthorised changes of the secret values being in possession of all users, and (b) allows any shareholder $u_i \in U$ to check if he is a member of an authorised group A_j. This component allows also any member of qualified subset to delegate his rights to any entity, which belongs or doesn't belong to the set of all users (Section 4).

We proved that the CIBE-GAS scheme is correct and secure against chosen-plaintext attacks IND-CID-GO-CPA (Section 5). The proposed encryption scheme was implemented and tested using a freely available PBC library written by Ben Lynn [13].

1.3 Paper Organisation

The paper is organized as follows. In Section 2, the bilinear maps and their properties are reviewed. Then, we present the Discrete Logarithm problem and its variations, on which our scheme is based. This Section introduces also some basic definitions of

secret sharing schemes with general access structures, which works under certificate and ID-based scenarios. In Section 3 we present the group-oriented encryption scheme CIBE-GAS with general access structures. Section 4 presents an extension to the CIBE-GAS scheme allowing delegations to be specified from an authorized user to any another user. The analyses and discussions concerning the proposed scheme are given in Section 5. Section 6 shows a practical implementation of the group-oriented decryption scheme and summarizes the results of tests. Finally, conclusions are presented.

2 Preliminaries

2.1 Bilinear Groups and Security Assumptions

Below, we summarise some concepts of bilinear pairings using notations similar to those presented by Al-Riyami, S., et al. [14].

Definition 1. Let $(G_1, +)$ and $(G_2, \cdot)$ be two cyclic groups of some prime order $q>2^k$ for security parameter $k \in N$. The bilinear pairing is given as $\hat{e}: G_1 \times G_1 \to G_2$ and must satisfy the following three properties:

1. **Bilinearity**: $\hat{e}(aP, bQ) = \hat{e}(abP, Q) = \hat{e}(P, abQ) = \hat{e}(P, Q)^{ab}$ for all $P, Q \in G_1$ and all $a, b \in Z_q^*$; this can be restated in the following way: for $P, Q, R \in G_1$, $\hat{e}(P+Q, R) = \hat{e}(P, R)\hat{e}(Q, R)$ and $\hat{e}(P, Q+R) = \hat{e}(P, Q)\hat{e}(P, R)$.
2. **Non-degeneracy**: some $P, Q \in G_1$ exists such that $\hat{e}(P, Q) \neq I_{G_2}$; in other words, if P and Q are two generators of G_1, then $\hat{e}(P, Q)$ is a generator of G_2.
3. **Computability**: given P, Q$\in G_1$, an efficient algorithm computing $\hat{e}(P, Q)$ exists.

To construct the bilinear pairing we can use, for example, the Weil or Tate pairings associated with an elliptic curve over a finite field.

2.2 Security Assumptions and Hard Problems

A few definitions presented below are important for security reduction techniques used to design the CIBE-GAS scheme and prove its security. We start from three classical hard problems: the DL (Discrete Logarithm) and BDH (Bilinear Diffie–Hellman) problems. Then we describe a problem presented in [15], called the *k*-BDHI (Bilinear Diffie-Hellman Inversion) problem.

Assumption 1 (DL problem). For $P, Q \in G_1^*$ finding an integer k, which satisfies $Q = kP$ is hard.

Assumption 2 (BDH problem [16]). For $P, Q \in G_1^*$ and given (P, aQ, bQ, cQ), where $a, b, c \in Z_q^*$, computing $\hat{e}(P, Q)^{abc}$ is hard.

Assumption 3 (k-BDHI problem [15]). For an integer k, $x \in_R Z_q^*$, $P, Q \in G_1^*$ and given $(P, xQ, x^2Q, \ldots, x^kQ)$, computing $\hat{e}(P, Q)^{1/x}$ is hard.

Obviously, if it is possible to solve DL problem then it is also possible to solve BDH problem (given Q, aQ, bQ and cQ we can take discrete logarithms to obtain a, b and b, which allows computing $\hat{e}(P, Q)^{abc}$). It is not known whether the k-BDHI problem, for $k > 1$, is equivalent to BDH [15]. However, solving the k-BDHI problem is no more difficult than calculating discrete logarithms in G_1.

2.3 General Access Structure

An access structure is a rule that defines how to share a secret, or more widely, who has an access to particular assets in IT system. Access structures can be classified into structures with and without threshold [17]. Although threshold access structures are frequently used (e.g. the most familiar examples are (n, n) and (t, n) secret sharing schemes given by Shamir or by Asmuth-Bloom), the non-threshold structures are more versatile. It is especially visible when the sender of the information defines special decryption rules that have to be met by the document recipient (e.g., the recipient should belong to a specific users' group).

Let us assume that $U = \{u_1, u_2, \ldots, u_n\}$ is a set of n participants. The set $\Gamma = \{ A \in 2^U : \textit{a set of shareholders, which are designated to reconstruct the secret}\}$ is an access structure of U, if the secret can be reconstructed by any set $A \in \Gamma$. All sets in access structure Γ are called authorized or qualified subsets. A desirable feature of each access structure is its monotonicity. It means that every set containing a subset of privileged entities is also a collection of the privileged entities. The set of all minimal subsets $C \in \Gamma$ is called the access structure basis Γ_0 (or alternatively, the minimal access structure) and is expressed mathematically by the following relation:

$$\Gamma \supseteq \Gamma_0 = \left\{ C \in \Gamma : \forall_{B \subset C}\ B \notin \Gamma \right\} \tag{1}$$

Due to the monotonicity of the set Γ, the access structure basis Γ_0 may be always extended to the set Γ by including all supersets generated from the sets of Γ_0.

The access structure $\Gamma_{(t,n)}$ of the threshold scheme (t, n) is defined as follows:

$$\Gamma_{(t,n)} = \left\{ A \in 2^U : |A| \geq t \right\} \tag{2}$$

It is easy to notice, that in case of the access structure $\Gamma_{(t,n)}$ of the threshold scheme (t, n), all users have the same privileges and credentials. G.J. Simmons in [18] generalized a secret threshold sharing scheme (t, n) and gave the definition of hierarchical (multilevel) and compartmented threshold secret sharing. In such approach, in contrast to the classical threshold secret sharing, trust is not uniformly distributed among the members of the qualified subsets. It means that participants are divided

into several subsets and only participants belonging to the same subset play the equivalent roles.

We say that the structure is useful, when it is possible to implement the access structure Γ. An example of the access structures realization is the approach proposed by Benaloh-Leichter [19]. However, the application of access structures for the construction of group-oriented decryption scheme is effective only when it is possible to reuse shares being in possession of participants. The discussion how to meet this requirement is presented in the work [9, 10, 20, 21].

3 Full Certificate-Based Encryption Scheme with General Access Structure

Assume that there are given: n–element set containing all shareholders $U = \{u_1, u_2, ..., u_n\}$, m–element access structure $\Gamma = \{A_1, A_2, ..., A_m\}$, dealer $D \notin U$ and combiner $Com \in U$. Then proposed Certificate-Based Encryption scheme with General Access Structure (CIBE-GAS) consists of eight algorithms: **Setup**, **SetSecretValue**, **CertGen**, **SetPublicKey**, **ShareDistribution**, **Encryption**, **SubDecrytpion** and **Decryption**.

The **ShareDistribution** algorithm is based on ideas taken from [9, 10] and allows to generate shares and evidences used during a message decryption (the **SubDecrytpion** and **Decryption** algorithms). In turn, group **Encryption** and **Decryption** algorithms with general access structure are built on basis of the non-group SK-IBE scheme [11]. A detailed description of all algorithms of CIBE-GAS scheme is presented below.

Setup. For cyclic additive group $(G_1, +)$ and cyclic multiplicative group $(G_2, \times)$ of the same prime order q a trusted authority TA chooses randomly its main key $s \in_R Z_q^*$, defines a bilinear pairing $\hat{e}$ and generates encryption scheme parameters *params*:

$$\hat{e} : G_1 \times G_1 \to G_2 \tag{3}$$

$$params = \{G_1, G_2, \hat{e}, q, P, P_0, H_1, H_2, H_3, H_4, H_5, H_6\} \tag{4}$$

where P is a primitive element of G_1, $P_0 = sP$ is a public key, $H_1 : \{0,1\}^* \times G_1 \times G_1 \to G_1^*$, $H_2 : \{0,1\}^* \times G_1 \times G_1 \to Z_q^*$, $H_3 : G_2 \times \{0,1\}^* \to Z_q^*$, $H_4 : \{0,1\}^p \times \{0,1\}^p \to Z_q^*$, $H_5 : G_2 \to \{0,1\}^p$ and $H_6 : \{0,1\}^p \to \{0,1\}^p$ are secure hash functions. Last two hash functions are used to transform a message M of p bits: a cryptographic hash function H_5 hashes elements of G_2 into a form that can be combined with the plaintext message M, which is a bit string of length p.

SetSecretValue. Every shareholder $u_i \in U$ with an identity ID_i chooses a random number $s_i \in_R Z_q^*$ ($i=1, ..., n$), calculates $X_i = s_i P$, $Y_i = s_i P_0$ and sends them to TA. The dealer $D \notin U$ performs similar actions: chooses secret $s_d \in_R Z_q^*$, calculates $X_d = s_d P$ and $Y_d = s_d P_0$.

CertGen. TA checks equation $\hat{e}(X_i, P) = \hat{e}(Y_i, P_0)$ for every shareholder identity ID_i ($i=1, ..., n$). If test results are positive, then TA calculates iteratively for $i=1, ..., n$ hash values $Q_i = H_1(ID_i, Pk_i)$, where $Pk_i = (X_i, Y_i)$, and participant's certificate $Cert_i = sQ_i$. In similar way dealer's certificate $Cert_d = sQ_d$ is calculated, where $Q_d = H_1(ID_d, Pk_d)$ and $Pk_d = (X_d, Y_d)$. TA publishes all issued certificates.

SetPublicKey. Every shareholder with an identity ID_i tests authenticity of received certificate $Cert_i$ using equation $\hat{e}(Cert_i, P) = \hat{e}(Q_i, P_0)$. If the verification passes, then the shareholder $u_i \in U$ ($i=1, ..., n$) publishes his or her public keys $Pk_i = (X_i, Y_i)$. The dealer proceeds similarly and publishes his or her public key $Pk_d = (X_d, Y_d)$.

ShareDistribution. The dealer $D \notin U$ tests public keys of all shareholders $u_i \in U$, verifying equations $\hat{e}(Cert_i, X_i) = \hat{e}(Q_i, Y_i)$ ($i=1, ..., n$). If test results are positive, then the dealer:

(a) for $i=1, ..., n$ calculates values

$$h_i' = \hat{e}(Cert_d + Cert_i, Y_i)^{s_d} = \hat{e}(Cert_d + Cert_i, Y_d)^{s_i} \tag{5}$$

$$h_i'' = \hat{e}(Cert_i, Y_i)^{s_d} = \hat{e}(Cert_i, Y_d)^{s_i} \tag{6}$$

(b) chooses $m = |\Gamma|$ different values $d_j \in_R Z_q \setminus \{1\}$, ($i=1, ..., m$); these values should unambiguously identify qualified subsets of an access structure $\Gamma = \{A_1, A_2, ..., A_m\}$;

(c) chooses secret $y \in_R Z_q^*$ and two random numbers $\alpha, \beta \in_R Z_q^*$; keeps the number α secret and then constructs first-degree polynomial $f(x) = y + \alpha x$;

(d) calculates $f(1)$ and

$$\gamma_j = f(d_j) - \sum_{u_{i_j} \in A_j} H_3(h_{i_j}', d_j \beta) \tag{7}$$

for each subset $A_j = \{u_{1_j}, u_{2_j}, \ldots\} \in \Gamma$, $j=1, ..., m$;

(e) for every shareholder $u_i \in A_j$ ($i=1, ..., n$; $j=1, ..., m$) calculates the evidence in the form:

$$k_{i,j} = \frac{\left(H_3\left(h_i', d_j\beta\right) - y^{-1}H_3\left(h_i'', d_j\beta\right)\right)}{s_d + H_2\left(ID_d, Pk_d\right)}X \tag{8}$$

(f) publishes β, $f(1)$, $Y = yP$, $Y_{-1} = y^{-1}P$, $\left(d_j, \gamma_j, k_{i,j}\right)$ for *j=1, ..., m* and *i=1, ..., n*; it should be noted that every shareholder $u_i \in U$ might verify whether his secret value s_i is related with parameters published by *TA* and the dealer:

$$\begin{aligned}&\hat{e}\left(H_2\left(ID_d, Pk_d\right)P + X_d, s_i^{-1}k_{i,j}\right) = \\ &\hat{e}(P, H_3\left(\hat{e}\left(Cert_d + Cert_i, Y_d\right)^{s_i}, d_j\beta\right)P - \\ &- H_3\left(\hat{e}\left(Cert_i, Y_d\right)^{s_i}, d_j\beta\right)Y_{-1})\end{aligned} \tag{9}$$

This verification can be repeated for each qualified group, in which a shareholder $u_i \in U$ is a member. Moreover, special construction of the evidence $k_{i,j}$ protects from dishonest shareholders, preventing from unauthorised changes of the secret value s_i as well as value of $k_{i,j}$.

Encryption. To encrypt the message $M \in \{0,1\}^p$ the dealer *D* selects a random value $\sigma \in \{0,1\}^p$ and:

(a) calculates $r = H_4\left(\sigma, M\right)$;

(b) sets the ciphertext $C = \left(C_1, C_2, C_3, C_4, C_5, C_6\right)$ as follows:

$$C_1 = r\left(H_2\left(ID_d, Pk_d\right)P + X_d\right) \tag{10}$$

$$C_2 = \sigma \oplus H_5\left(\hat{e}\left(P, Y\right)^r\right) \tag{11}$$

$$C_3 = M \oplus H_6\left(\sigma\right) \tag{12}$$

$$C_4 = \hat{e}\left(P, f\left(1\right)P\right)^r \tag{13}$$

$$C_5 = \left\{v_k = \hat{e}\left(P, \gamma_k P\right)^r, \forall k \in F \subseteq 2^m\right\} \tag{14}$$

$$C_6 = rY_{-1} \tag{15}$$

The set F in C_5 plays the role of the filter, which superimposed on the access structure Γ allows decrypting information only by privileged groups, which indexes belong to F.

SubDecryption. Every shareholder from the privileged subset $u_{i_j} \in A_j \in \Gamma$ ($j \in F$) partially decrypts ciphertext $C = \left(C_1, C_2, C_3, C_4, C_5, C_6\right)$ using his share s_{i_j} and returns to the combiner the following value:

$$\delta_{i_j,j} = \hat{e}\left(C_1, s_{i_j}^{-1} k_{i_j,j}\right)\hat{e}\left(P, H_3\left(\hat{e}\left(Cert_{i_j}, Y_d\right)^{s_{i_j}}, d_j\beta\right)C_6\right) \tag{16}$$

Decryption. Let us assume further that one of privileged shareholders, e.g. $u_{k_j} \in A_j, k \in \{1,\ldots,|A_j|\}$, will play the combiner role. To decrypt the ciphertext $C = (C_1, C_2, C_3, C_4, C_5, C_6)$, the combiner $Com = u_{k_j} \in A_j$ from (belonging to?) any authorised group performs the following steps:

(a) gathers all partial values $\delta_{1_j,j},\ldots,\delta_{Com-1,j},\delta_{Com,j},\delta_{Com+1,j},\ldots,\delta_{|A_j|_j,j}$ and calculates

$$\Delta = \Delta_1^{\frac{d_j}{d_j-1}} \cdot \Delta_2^{\frac{-1}{d_j-1}} \tag{17}$$

where $v_j \in C_5$ and

$$\begin{aligned} \Delta_1 &= C_4 \\ \Delta_2 &= v_j \cdot \delta_{Com,j} \prod_{u_{i_j} \in A_j \setminus Com} \delta_{i_j,j} \end{aligned} \tag{18}$$

(b) calculates

$$\sigma = C_2 \oplus H_5(\Delta) \tag{19}$$

(c) calculates

$$M = C_3 \oplus H_6(\sigma) \tag{20}$$

(d) recovers $r = H_4(\sigma, M)$;

(e) if $C_1 \neq r\left(H_2(ID_d, Pk_d)P + X_d\right)$, then raises an error condition and exits; otherwise sets the plaintext to *M*.

Thus the plaintext *M* can be obtained from the ciphertext $C = (C_1, C_2, C_3, C_4, C_5, C_6)$ and the combiner can decide if the decrypted ciphertext is correct.

4 Rights delegation

The CIBE-GAS scheme allows to decide who can have access to the information (i.e. allows to describe each member of the access structure, who is able to gather enough number of partial values $\delta_{1_j,j},\ldots,\delta_{|A_j|_j,j}$ (*j=1, ..., m*)). Moreover, we can easily introduce delegation operation to the proposed scheme.

Assume that delegation rule is implemented as follows: (a) the user $u_i \in U$ requests the dealer to delegate his right to any entity u_p (belonging or not belonging to

set *U*) to be a member of a group A_j; the entity u_p cannot forward this right further, (b) dealer issues to the entity u_p evidence $k_{p,j}$ and publish it. The evidence $k_{p,j}$ has the following form:

$$k_{p,j} = \frac{\left(H_3\left(h_i', d_j\beta\right) - y^{-1}H_3\left(h_p'', d_j\beta\right)\right)}{s_d + H_2\left(ID_d, Pk_d\right)} X_p \tag{21}$$

where $h_p'' = \hat{e}\left(Cert_p, Y_p\right)^{s_d} = \hat{e}\left(Cert_p, Y_d\right)^{s_p}$, and $Cert_p$ is the certificate of entity u_p.

The entity u_p can calculate his partial share using owned by himself evidence $k_{p,j}$ and the ciphertext $C = \left(C_1, C_2, C_3, C_4, C_5, C_6\right)$:

$$\begin{aligned}\delta_{p,j} = \hat{e}\left(C_1, s_p^{-1}k_{p,j}\right)\hat{e}\left(P, H_3\left(\hat{e}\left(Cert_p, Y_d\right)^{s_p}, d_j\beta\right)C_5\right) = \\ \hat{e}\left(rP, H_3\left(\hat{e}\left(Cert_d + Cert_i, Y_d\right)^{s_i}, d_j\beta\right)P\right) = \delta_{i,j}\end{aligned} \tag{22}$$

which is equal to the share $\delta_{i,j}$ of entity $u_i \in U$ (compare the proof of Theorem 1). It follows, that the entity u_p indeed represents the entity $u_i \in U$. Hence, the entity can not only be a provider (on behalf of the entity $u_i \in U$) of the share $\delta_{i,j}$, but might play a combiner role and decipher encrypted message.

5 Analysis and Discussion

5.1 Correctness

Assume that the ciphertext $C = \left(C_1, C_2, C_3, C_4, C_5, C_6\right)$ was generated using the **Encryption** algorithm. Then, according to properties of bilinear parings, the following theorem shows that the users in some access instance A_j can cooperate to recover the message *M*.

Theorem 1. Any user $u_{k_j} = Com \in A_j, k \in \left\{1, \ldots, \left|A_j\right|\right\}$ (i.e. the combiner), which is the member of authorised subgroup A_j referenced by index *j* belonging to the set *F* (see Eq. (14)) can decrypt the message *M* encrypted in the equation (12).

Proof. From Eq. (16), for each $u_{i_j} \in A_j, i \in \left\{1, \ldots, \left|A_j\right|\right\}$ we have:

$$\begin{aligned}\delta_{i_j,j} &= \hat{e}\left(C_1, s_{i_j}^{-1}k_{i_j,j}\right)\hat{e}\left(P, H_3\left(\hat{e}\left(Cert_{i_j}, Y_d\right)^{s_{ij}}, d_j\beta\right)C_6\right) = \\ &= \hat{e}\left(r\left(H_2\left(ID_d, Pk_d\right)P + X_d\right), s_{ij}^{-1}\frac{\left(H_3\left(h_{ij}', d_j\beta\right) - y^{-1}H_3\left(h_{ij}'', d_j\beta\right)\right)}{s_d + H_2\left(ID_d, Pk_d\right)}X_i\right) \cdot \\ &\quad \cdot \hat{e}\left(P, H_3\left(h_{ij}'', d_j\beta\right)C_6\right), \qquad \text{by Eqs.(8) and (10)} \\ &= \hat{e}\left(rP, \left(H_3\left(h_i', d_j\beta\right) - y^{-1}H_3\left(h_i'', d_j\beta\right)\right)P\right)\hat{e}\left(P, H_3\left(h_{ij}'', d_j\beta\right)ry^{-1}P\right), \text{ by Eq.(15)}\end{aligned}$$

$$= \hat{e}\left(rP, H_3\left(\hat{e}\left(Cert_d + Cert_{i_j}, Y_d\right)^{s_{i_j}}, d_j\beta\right)P\right) \qquad \text{by Eq. (5).}$$

With this partially decrypted ciphertext $\delta_{i_j,j}, i \in \{1,\ldots,|A_j|\}$ from all participants of authorised subset A_j the combiner $Com \in A_j, k \in \{1,\ldots,|A_j|\}$ can get:

$$\Delta_2 = v_j \cdot \delta_{Com,j} \prod_{u_{i_j} \in A_j \setminus \{Com\}} \delta_{i_j,j},$$

$$= \hat{e}(P, \gamma_j P)^r \cdot \prod_{u_{i_j} \in A_j} \hat{e}\left(rP, H_3\left(h'_{u_{i_j}}, d_j\beta\right)P\right) \quad \text{by Eq. (14) and calculated } \delta_{i_j,j}$$

$$= \hat{e}\left(rP, \left(\gamma_j + \prod_{u_{i_j} \in A_j} H_3\left(h'_{u_{i_j}}, d_j\beta\right)\right)P\right) = \hat{e}(P, rf(d_j)P), \qquad \text{by Eq. (7)}$$

The obtained value of $\Delta_1 = C_4$ and the reconstructed value Δ_2 are related with two points on line $f(x) = y + \alpha x$, and allow to make an implicit interpolation (using Langrange's polynomial interpolation) of the secret *y*:

$$\begin{aligned} \Delta &= \Delta_1^{\frac{d_j}{d_j - 1}} \cdot \Delta_2^{\frac{-1}{d_j - 1}} = \\ &= \hat{e}(P, rP)^{\frac{d_j}{d_j - 1} f(1) + \frac{-1}{d_j - 1} f(d_j)} = \hat{e}(P, rP)^y = \hat{e}(P, Y)^r \end{aligned} \tag{23}$$

Thus the plaintext *M* can be obtained from Eqs (11) and (12) as follows:

$$\sigma' = C_2 \oplus H_5(\Delta) = \sigma \oplus H_5\left(\hat{e}(P, Y)^r\right) \oplus H_5(\Delta), \qquad \text{by Eq. (11)}$$

$$= \sigma \oplus H_5(\Delta) \oplus H_5(\Delta) = \sigma, \qquad \text{by Eq. (23)}$$

$$M' = C_3 \oplus H_6(\sigma'),$$

$$= M_3 \oplus H_6(\sigma) \oplus H_6(\sigma') = M \qquad \text{by Eq. (12).}$$

If $C_1 \neq r\left(H_2(ID_d, Pk_d)P + X_d\right)$, the message M' calculated by (20) is the message *M*.

This ends the proof. □

5.2 Security analysis

The CIBE-GAS is the secret sharing group-oriented decryption scheme based on Sakai and Kasahara non-group IBE (SK-IBE) scheme [11]. L. Chen and Z. Cheng prove in [16] that the SK-IBE scheme is secure against chosen-plaintext attacks (IND-ID-CCA) in the random oracle model. They prove also that the security of SK-IBE can be reduced to the hardness of the *k*-BDHI problem.

In CIBE-GAS scheme an adversary can obtain public information related to all participants, i.e. $k_{i,j}$, $Pk_i = (X_i, Y_i)$, $Cert_i$ (*i=1, …, n; j=1, …, m*). In notice board service are also available other parameters like β, $f(1)$, $Y = yP$, $Y_{-1} = y^{-1}P$ and (d_j, γ_j) for each group of participants (*j=1, …, m*). However, this information doesn't

affect the security of the scheme, while the hardness of the CIBE-GAS scheme is reduced from the *k*-BDHI problem to the DL problem.

Theorem 2. The proposed CIBE-GAS scheme is secure against chosen-plaintext attacks IND-CID-GO-CPA in the standard model, assuming that (1) the hash function H_3 is collision-resistant and (2) the DL assumption holds in group G_1.

Proof (sketch). A group-oriented certificate and ID-based cryptosystem is secure against chosen-plaintext attacks IND-CID-GO-CPA if no polynomially bounded adversary has a non-negligible advantage against the cryptosystem in the game like this defined in [12]. In this game "*an adversary makes an attack on an authorised subset* A_j, *which the member number is* $|A_j|$. *We allow the adversary to possess the most advantageous conditions that he could obtain the private keys of any* $|A_j|-1$ *participants in the authorised subset, and furthermore, he could also obtain the private keys of any number of participants other than those in the authorised subset* A_j" [8].

Assume that the participant $u_{k_j} \in A_j$ and his secret key s_{k_j} are the adversary's targets of attacks. Then for the key $\bar{s}_{k_j}$ chosen by the adversary and from (18) follows:

$$\Delta_2 = v_j \cdot \delta_{u_{k_j},j} \prod_{u_{i_j} \in A_j \setminus \{u_{k_j}\}} \delta_{i_j,j} = \hat{e}\left(rP, \left(\gamma_j + \sum_{u_{i_j} \in A_j \setminus \{u_{k_j}\}} H_3\left(h'_{u_{i_j}}, d_j\beta \right) \right) P \right) \cdot$$

$$\cdot \hat{e}\begin{pmatrix} rP, \bar{s}_{k_j}^{-1} s_{k_j} H_3\left(h'_{u_{i_j}}, d_j\beta \right) P + \\ y^{-1}\left(H_3\left(\hat{e}\left(Cert_{k_j}, \bar{s}_{k_j} Y_d \right), d_j\beta \right) - \bar{s}_{k_j}^{-1} s_{k_j} H_3\left(\hat{e}\left(Cert_{k_j}, s_{k_j} Y_d \right), d_j\beta \right) \right) P \end{pmatrix}$$

The value of Δ_2 will be valid only if $\bar{s}_{k_j}^{-1} s_{k_j} = 1 \in Z_q^*$. This means that the adversary will succeed in solving the DL problem for $P, X_{k_j} \in G_1^*$. Hence, if the CIBE-GAS scheme is not secure against an IND-CID-GO-CPA adversary, then the corresponding DL assumption is flawed.

6 Implementation and practical performance

The scheme was implemented using the PBC library created and maintained by Benn Lynn [13]. The library consists of API, which is abstract enough, so only basic understanding of bilinear pairings is required from a programmer. The test operating system was Ubuntu 11.04 running on a virtual machine on Windows 7 host system. The host system machine was Intel Xeon W3520@2,67 GHz with 4GBRAM. We have run several tests that confirmed that our scheme is correct (the decrypted message was equal to the original message). In our tests we have used "Type A" pairing which are constructed on the curve $y^2 = x^3 + x$ over the field F_q for a 512- bit prime $q = 3 \bmod 4$, and thus the pairing result are in F_{q^2} (see details on PBC library specification [10]).

The second purpose of the tests was to verify algorithms' performance. The primary code analysis has shown that the most time consuming are encryption and decryption algorithms. The encryption time depends on the number of shareholders and on the cardinality *#A* of the qualified subset A. The encryption time of a sample case ($\Gamma = \{A_1, ..., A_{14}\}$ with six shareholders and average cardinality *#A* of the *A* equals three) is around 168ms.

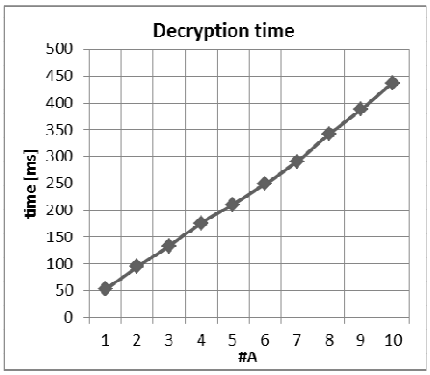

Fig. 1. Decryption time

The decryption time depends on the cardinality *#A* of the set *A*. The tests results for decryption for the different cardinality *#A* of the qualified subsets *A* are presented in the Fig.1. The results show that decryption time increases linearly with increasing the cardinality *#A* of the set *A*. It is also noteworthy that the most time consuming operation is paring calculation. The time for pairing calculation without pre-processing is around 4ms.

7 Summary

The proposed encryption scheme CIBE-GAS provides sensitive information protection in accordance with any general access structure. In this scheme we use the idea of a secret sharing scheme with general access structure given by Sang, Y., et al. [9] and the idea of a dynamic encryption scheme presented by Long, Y, et al. [10] (with modifications by Kitae, K., et al [21]).

We proved that our group-oriented certificate and ID-based cryptosystem is secure against chosen-plaintext attacks IND-CID-GO-CPA. Furthermore, the scheme allows sending the message to any authorised subsets with prior knowledge of theirs structure. This fine-grained access control mechanism allows a dealer alone (without the cooperation with other members of the subgroup) or each member of an authorised subgroup (in cooperation with other members of this subgroup) to decrypt sensitive information.

The access control to encrypted sensitive information is under the dealer's sole control (the dealer plays the role of an originator, which has the power to determine

who is able to access the information). Especially, this means that the dealer can define different subsets of the access structure, can add members to authorised subgroups or remove members from these subgroups, and may delegate the access rights to another member of the subgroup or to a new entity not belonging to the current access structure. These properties make the scheme a suitable choice for practical applications and make it more flexible and well applied in the field of sensitive information security.

Finally, we provided an implementation of our system using the Pairing Based Cryptography (PBC) library. The test results obtained for different authorized subgroups are promising and show that our system performs well in practice.

8 Acknowledgment

This scientific research work is supported by NCBiR of Poland (grant No O N206 001340) in 2011-2012.

References

1. Desmedt, Y.: Society and group oriented cryptography: a new concept. In Advances in Cryptology, CRYPTO'87, pp. 120–127, 1987
2. Gentry C.: Certificate-based Encryption and the Certificate Revocation Problem. In Biham, E. (ed.): Advances in Cryptology-Eurorypt'03, Lecture Notes in Computer Science, Vol. 2656. Springer-Verlag, pp. 272–293, 2003
3. Kang, B. G., Park, J. H., Hahn, S. G.: A Certificate-based Signature Scheme. In: Okamoto, T. (ed.): CT-RSA 2004, Lecture Notes in Computer Science, vol. 2964, Springer-Verlag, pp.99–111, 2004
4. Baek, J., Zheng, Y.: Identity-based threshold decryption. In: Proceedings of PKC'04, Lecture Notes in Computer Science, vol. 2947, pp. 262–276, 2004
5. Y. Long, K. Chen, S. Liu, ID-based threshold decryption secure against adaptive chosen-ciphertext attaca. Computers and Electrical Engineering, Vol. 33, No 3, 2007 166–176.
6. Ting-Yi Chang: An ID-based group-oriented decryption scheme secure against adaptive chosen-ciphertext attacks. Computer Communications, Vol. 32, No 17, pp. 1829–1836, 2009
7. Hongwei Liu, Weixin Xie, Jianping Yu, Peng Zhang, Sisi Liu: A general threshold encryption scheme based on new secret sharing measure. 6th IEEE Conference on Industrial Electronics and Applications (ICIEA), 21-23 June 2011, pp: 2235 – 2239
8. Xu, Ch., Zhou, J., Xiao, G.: General Group Oriented ID-Based Cryptosystems with Chosen Plaintext Security. International Journal of Network Security, Vol.6, No.1, pp.1–5, January 2008
9. Sang, Y., Zeng, J., Li, Z., You, L.: A Secret Sharing Scheme with General Access Structures and its Applications. International Journal of Advancements in Computing Technology, Vol. 3, No. 4, pp. 121-128, May 2011
10. Long Y., Chen Ke-Fei: Construction of Dynamic Threshold Decryption Scheme from Pairing. International Journal of Network Security, Vol.2, No.2, pp. 111–113, March 2006
11. Sakai, R., Kasahara, M.: ID based cryptosystems with pairing on elliptic curve. Cryptology ePrint Archive, Report 2003/054

12. Fujisaki, E., Okamoto, T.: Secure Integration of Asymmetric and Symmetric Encryption Schemes. In Proceedings of CRYPTO ’99, Santa Barbara, CA, August 20–24, 1999, pp. 537–554
13. Lynn, B.: PBC Library Specification, available online at http://crypto.stanford.edu/pbc/ , retrieved 2012
14. Al-Riyami, S., Paterson, K.: Certificateless public key cryptography. In Advances in Cryptology - AsiaCrypt, LNCS, vol. 2894, pp. 452–473, Springer-Verlag, 2003
15. Boneh, D., Boyen, X.: Efficient selective-ID secure identity-based encryption without random oracles. In Proceedings of Advances in Cryptology – Eurocrypt 2004, LNCS, Vol. 3027, pp. 223-238, Springer-Verlag, 2004
16. Chen, L., Cheng, Z.: Security proof of Sakai-Kasahar's identity-based encryption scheme. In Proceedings of Cryptography and Coding 2005, LNCS, Vol. 3796, pp. 442-459. Springer-Verlag, 2005
17. Daza, V., Herranz, J., Morillo, P., Ràfols, C.: Extensions of access structures and their cryptographic applications. Applicable Algebra in Engineering, Communication and Computing, Vol. 21, No. 4, pp. 257-284, 2010
18. Simmons, G. J.: How to (really) share a secret. In Advances in Cryptology - CRYPTO 88, LNCS 403, 1990, pp. 390-448
19. Benaloh J., Leichter J.: Generalized secret sharing and monotone functions. In S. Goldwasser (ed.) Advances in Cryptology - CRYPTO '88, LCNS No 403, Springer-Verlag, London, 1990, pp. 27-35
20. Zheng, Y., Hardjono, T., Seberry, J.: Reusing shares in secret sharing schemes. Computer Journal, Vol. 37, No 3, pp. 199–205, 1994
21. Kitae, K., Lim, S., Yie, I., Kim, K.: Cryptanalysis of a Dynamic Threshold Decryption Scheme. Communications of the Korean Mathematical Society, Vol. 24, No. 1, pp. 153-159, 2009