Tomasz HYLA, Jerzy PEJAŚ

West Pomeranian University of Technology in Szczecin, Faculty of Computer Science and Information Technology

Classified information protection requirements and their implementation method

Abstract. *Protection of classified information is very important, but also a difficult task. It usually requires a centralized access policy management and control system. However, such solution is often difficult to accept in the era of users' mobility. Protection of mobile and portable classified information using only encryption techniques is inefficient and precludes its protection in accordance with an approved access policy. In the paper (based on the Polish Classified Information Act from 5 August 2010) we present the basic requirements for access structures, which reflect access policies applicable to protect specific classified information. Subsequently, five different scenarios for access to classified information are listed and described. The scenarios can be implemented using general access structures. Finally, one of dynamic encryption schemes is described and analysed. The scheme can be used to encrypt classified information using general access structures describing access scenarios.*

Streszczenie. *Ochrona informacji niejawnej jest bardzo istotnym, ale jednocześnie trudnym zadaniem. Zastosowanie do ochrony przemieszczającej się informacji niejawnej tylko technik szyfrowania jest nieefektywne oraz uniemożliwia jej ochronę zgodnie z przyjętą polityką dostępu. W artykule, na podstawie Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, sformułowano podstawowe wymagania nakładane na struktury dostępu, które są odzwierciedleniem polityk dostępu mających zastosowanie do ochrony określonej informacji niejawnej. Następnie zostało wymienionych i opisanych pięć różnych scenariuszy dostępu do informacji niejawnych. Scenariusze te mogą zostać zaimplementowane z użyciem ogólnych struktur dostępu. W pracy przedstawiono także i przeanalizowano dynamiczny schemat szyfrowania. Pokazano także, że schemat ten może być używany do szyfrowania informacji niejawnych za pomocą ogólnych struktur dostępu, które mogą opisywać każdy z wymienionych pięciu scenariuszy dostępu. (**Wymagania nakładane na ochronę informacji niejawnej i metoda ich implementacji.)***

Keywords: protection of classified information, general access structure, cryptographic access control, certificate-based cryptosystems
Słowa kluczowe: ochrona informacji niejawnej, ogólna struktura dostępu, kryptograficzna kontrola dostępu, kryptosystemy oparte na certyfikatach

doi:10.12915/pe.2014.02.22

Introduction

According to the Polish Act of 5 August 2010 on Protection of Classified Information [2], the classified information is defined as information, which disclosure would or could cause damage for Poland or would be disadvantageous from Poland's point of view. The Act applies to public authorities, organizational units of the Ministry of National Defence, National Bank of Poland, public units subordinated to the public authorities as well as private contractors, who work with classified information. Processing of classified information is considered as any operations proceeded on this information, i.e. creation, modification, copying, classification, collection, transfer and sharing.

Information can be classified into one of four levels: top secret, secret, confidential and restricted. Classification clauses are given by a person entitled to sign the document. This person is able to determine characteristic date or event, followed by abolition or modification of the clearance level, what may happen after written approval given by the classification issuer or his/her supervisor. In addition, the manager of an organization, in which information is stored, must take the decision of abolition of the „top secret" level. After modification of the security level, document recipients have to be informed, that the clause has changed.

Classified information can be distributed to persons who have to meet two basic conditions. Firstly, the information recipients must guarantee to keep it in secret, i.e. any recipient should have the appropriate security clearance and, secondly, the information should be necessary to perform their duties. Classified information has to be processed under restrictions which prevent their disclosure, in the particular case – prevent to send it to another person.

Compliance with above requirements (related to any information in electronic form) requires the creation of a centralized access policy management system, acting in accordance with the approved access control model. The most basic access control models include MAC (Mandatory Access Control), DAC (Discretionary Access Control) and RBAC (Role Based Access Control). The paper of Pejaś J., et al [3] presents the analysis of these models in terms of their application in IT systems processing classified information The analysis shows that these models do not meet directly all the requirements imposed on access rules related to classified information. It is possible only using rules of the ORCON model (ORiginator CONtrolled) (M. Bishop [4]).

ORCON assumes that each resource (document) has its owner (an originator). The originators of documents retain control over them even after those documents are disseminated. The owner may give another user rights to his/her document. However, user who received such rights can pass them further only with the approval of the document creator.

Access control models, including ORCON, can be build based on any (including dynamic) access structure (see [5 - 10]). However, not every access structure is suitable for implementation of decentralized access control and rights delegation to other entities (see Table 1). Although DAC model has such features (decentralization and delegation), only ORCON is proper for protecting classified information. The reason is simple - in the DAC model each information owner may also give (delegate) his rights to other user, but without the ability to control whether those rights are given to other entities.

Table 1 – Decentralization and delegation in the access control models

	Requirements	MAC	DAC	RBAC	ORCON
1.	Decentralization	no	yes	yes	yes
2.	Delegation	no	yes	no	yes

This paper contains the basic information about the access structures, their properties and implementation approaches. We formulate the requirements imposed on access structures used in access control scenarios that are necessary to protect classified information. Next, we describe and analyse a dynamic group encryption scheme based on the general access structure [1] that can be used to implement described access control scenarios.

Related works

Access structures can be classified into structures with and without threshold (e.g., Daza V., et al. [11]). Although threshold access structures are frequently used (Shamir secret sharing scheme [12] or Asmuth-Bloom scheme [13]), the non-threshold structures are more versatile. It is especially visible when the sender of confidential information defines special rules for its decryption, that have to be met by the document recipient (e.g., the recipient should belong to a specific users' group or have certain attributes).

In practice, dynamic access structures should meet the following conditions (see Delerablee C., et al. [14] Y. Long, et al. [15], W. Bagga [16]):

1) adding a new shareholder or removing existing one should not require changes of other shareholders' shares and should not cause any leakage of information about the encryption key;
2) the encryption entity can dynamically define the threshold values, which have to be exceeded for decrypting the ciphertext;
3) the renewal of the key used in encryption or decryption procedures should be possible without changing the secret shares held by participants;
4) the renewal of a single share should not require renewal of any shares belonging to other shareholders and should not cause any leakage of information about the encryption key.

An interesting example of a dynamic scheme that meets these requirements is an encryption scheme presented by Y. Long, et al. [15] (with modifications by Kitae Kim, et al [17]). This scheme is based on the typical threshold structure *(t, n)*, which significantly limits its possible application. More suitable threshold schemes for general access structure are presented by V. Daza et al. [11], Yongxuan Sang, et al. [18] C. Cachin [19] and Liao-Jun Pang, et al. [20].

Access structure as a way of privileges controlling

The access structure defines a set of users who have access to the particular resources in the system. The users belonging to such set need not to have the same rights - some of them may be more privileged than others. Dependencies between privileges can form different topographies of such structures, e.g. monotonic and hierarchical access structure. The access to a resource is defined as the right to read it using decryption. This right means that if any user possesses the proper decryption cryptographic key, then he/she can get access to protected information. Of course, the key should be also treated as secret information. In order to formalize the discussion on the access structure it is worth to introduce its mathematical model. Assume the following notations:

- $U=\{u_1,u_2,...,u_n\}$ - a set of n shareholders,
- K - a set of secrets,
- S - a set of shares (shadows),
- $P(U)=2^U$ - a set of all subsets of U (so called power set of the set U),
- s - a secret (a private key), which gives access right to the resource,
- A - an authorized set of shareholders,
- Γ - a set of subsets of U, which can reconstruct the secret s (the access structure in short), i.e. the set of all authorized sets of shareholders.
- $\overline{\Gamma}=P(U)\setminus\Gamma$ - a set of user subsets; each user belonging to such subsets is not authorized to reconstruct the secret - these users form the unprivileged subsets.

The elements of the access structure will be referred to as the authorized groups/sets and the rest are called unauthorized groups/sets.

Next, we will say that the scheme is a perfect secret sharing scheme implementing the access structure, if it provides the following two properties (see, e.g., [21]):

1) if shareholders of an authorized subset $A\in\Gamma$ pool together their shares, then they should be able to reconstruct the secret value $s\in K$;
2) if shareholders of an unauthorized subset $B\in\overline{\Gamma}$ pool together their shares, then they are not able to determine nothing about the secret value $s\in K$;

A desirable feature of each access structure is its monotonicity. It means that every set containing a subset of privileged entities also is a collection of the privileged entities.

Definition 1. *Access structure $\Gamma=\{A\in P(U)$: a set of shareholders, which are designated to reconstruct the secret$\}$ is monotone, if for any subset $A\in\Gamma$ all its supersets $B\supseteq A$ are contained in Γ, that is:*

$$A\subseteq B\Rightarrow\forall A\in\Gamma,B\in\Gamma \tag{1}$$

Definition 2. The set of all *minimal* subsets $C\in\Gamma$ is called the access structure basis Γ_0 (or alternatively, the minimum access structure) and is expressed mathematically by the following relation:

$$\Gamma\supseteq\Gamma_0=\left\{C\in\Gamma:\forall_{B\subset C}\ B\notin\Gamma\right\} \tag{2}$$

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:

$$\Gamma=cl(\Gamma_0)=\{A: A\supseteq C\wedge C\in\Gamma_0\} \tag{3}$$

where $cl(\Gamma_0)$ is the closure of Γ_0.

When is possible to implement the access structure Γ, we say that the structure is useful. An example of the access structures realization is the approach proposed by Benaloh-Leichter (see [6, 22]). A specific access structure Γ can be implemented using the logical operations AND ($\wedge$) and OR ($\vee$). The AND operator is used to combine the entities belonging to a particular privileged subset, while the OR operator is useful to combine privileged subsets. This model can be implemented using various cryptographic methods (e.g. using the encryption scheme [1] presented below in Section *Certificate-Based Encryption Scheme with General Access Structure*).

Requirements for access structures

In order to meet the requirements specified in the Polish Act on Protection of Classified Information (see [2]), the access structures have to fulfil the general conditions specified in Article 8 of the Act. The confidential information with classification clause:

- may be made available only to the person entitled to access to information with specific security clause;
- must be processed in accordance with the security clause assigned to information and under conditions which prevent their unauthorized disclosure;
- have to be protected in accordance with the security clause assigned to information, using appropriate security measures specified in the Act and regulations issued under it.

Implicitly, there is usually the need to use the access structure supporting the ORCON model with two extending

rules, which allow to: (a) share information by various entities (e.g., different government agencies) and (b) delegate (transfer) access to information (in exceptional cases) to another entity by entity that such access has already received from the originator. Introduction of the extending rules results from the criticism after the attack on the WTC towers on September 11, 2001 (see [23]).

Table 2. Proposed requirements for access structure

No.	Name	Description
1	Classification	The originator have to classify the document using one of *n* clearance levels, on the first level documents are public, while on the subsequent levels - classified.
2	Decentralization	Many organizational units exist and it is not necessary to have one point containing information on all documents.
3	Access	To gain access to the document, it is necessary to meet, among others, the following conditions divided into two categories: • conditions related to the user, • conditions related to the workstation.
4	Flexibility	The access to the newly created document has its creator and optionally his manager. Over time, a set of users who have access to the document may change according to the access policy. The set of authorized users and their assertions can form hierarchical relations or belong to the known in advance number of disjoint classes.
5	Delegation[1]	The creator of the document can delegate his permissions to the manager or manager can himself take the permissions to the document
6	Propagation of the document I	User (excluding the person providing the access to a specific document) cannot make an electronic copy of the document and save it as plaintext - even if he/she has the permission to read.
7	Propagation of the document II	Making electronic copies of the document saved in plaintext is technically not possible.
8	Dynamicity	The security clause can be decreased or increased by the author (with the approval of the manager) for the clearance levels $i \geq p$, where p is the level that requires approval of the manager (e.g. the "top secret" level, according to the Act).
9	Offline work	After verification of user's permission to read the document, she/he has access to it for a *t* period.
10	Online work	User permission to read the document is verified at each access to the document.
11	Audit	It is required to store the access record, which collect information about users who had permission to access in the past and who can currently access the document.
12	Untrusted data storage	The document can be stored in the data warehouse without any security certificates (e.g. in encrypted form).
13	Trusted data storage	The document can be stored in a data warehouse in plaintext; the confidence to the data warehouse relies on the security certificate.
14	Business continuity	In the case of death of the creator and manager, or their dismissal, access to the document may be given to a new manager after obtaining certification supported by *n* of *m* groups of designated users.
15	Export to SAML and XACML	Access structures, assertions and policies should be easily exported to SAML and XACML languages.

[1] Delegation is a method of temporarily assigning permissions to the user.

General access structures should allow the implementation of the following scenarios for access to classified information:

1. **broad Information Sharing Mode** - information is available to all entities, as long as they have the appropriate security clearance or access authorization issued by the authorized entity;
2. **addressed Information Sharing Mode** - information is available only to individual members of the group, as long as they have the appropriate security clearance or access authorization issued by the authorized entity;
3. **threshold Information Sharing Mode** - information is available to the entity only, if it shares information with any of *t* from *n* entities; each of *t* entities must have the appropriate security clearance or access authorization issued by the authorized entity;
4. **hierarchical Information Sharing Mode** – information is available only to those entities that belong to different groups forming the hierarchy, each entity taking part in the scenario must have the appropriate security clearance or access authorization issued by the authorized entity;
5. **compartment Information Sharing Mode** - information is available only to those entities that belong to different groups of entities forming a separable compartments; each entity taking part in the scenario must have the appropriate security clearance or access authorization issued by the authorized entity.

It is required to design corresponding access structures to realize these scenarios. The access control system can support all of the scenarios, but in practice, depending on the required tasks, only selected scenarios are going to be implemented. Access structures must be dynamic, i.e. must allow to change the number of entities (adding and deleting entities, changing the entities threshold *t* required to reproduce the information, rights delegation).

Figure 1 presents a general access control scheme to classified information with use of the access policies and structures that satisfy the requirements from Table 2. This diagram shows that the entity can obtain access to information, if it belongs to an authorized subset of users (it is a part of the access structure) and fulfils the predefined number of assertions.

Information sharing rules are formulated in the form of access policies, and these in turn are mapped to the access structure. Access structures received as a result might be implemented using different mechanisms. One of the most commonly used mechanisms are standard threshold secret sharing schemes (*t, n*). They may be used only when access to information is determined by the presence of at least *t* of *n* players (see, e.g. A. Shamir scheme [11] and Asmuth-Bloom scheme [12]). The standard threshold schemes may be used to implement the second scenario -

Addressed *Information Sharing Mode*. Implementation of the remaining four scenarios require the use of general access structures (see, e.g.[4], [5], [9]).

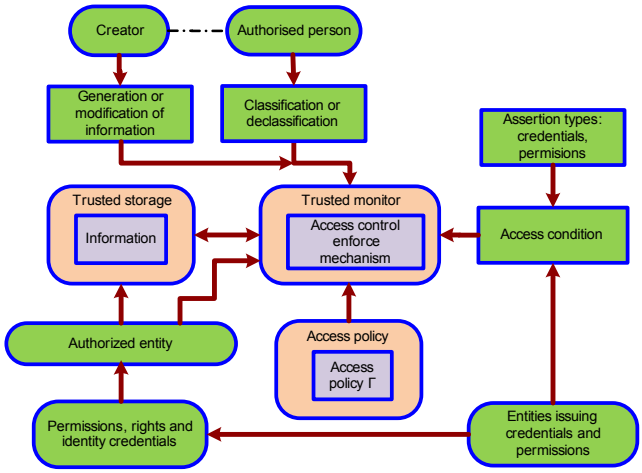

Fig. 1 General scheme for classified information access

Certificate-Based Encryption Scheme with General Access Structure

The access scenarios can be implemented using our CIBE-GAS scheme [1]. The scheme consists of eight algorithms: **Setup**, **SetSecretValue**, **CertGen**, **SetPublicKey**, **ShareDistribution**, **Encryption**, **SubDecrytpion** and **Decryption**:

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*:

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

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

where P is a primitive element of G_1, $P_0 = sP$ is a public key and H are different secure hash functions.

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 the TA. 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 authority verifies 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 for each *i=1, ..., n* TA calculates hash value $Q_i = H_1(ID_i, Pk_i)$, where $Pk_i = (X_i, Y_i)$, and then participant's certificate $Cert_i = sQ_i$. In similar way dealer's certificate is calculated. TA authority 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 pass, then shareholder $u_i \in U$ (*i=1, ..., n*) publishes his or her public key $Pk_i = (X_i, Y_i)$. Dealer proceeds similarly and publishes his or her public key $Pk_d = (X_d, Y_d)$.

ShareDistribution. 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) calculates values $h_i' = \hat{e}(Cert_d + Cert_i, Y_i)^{s_d} = \hat{e}(Cert_d + Cert_i, Y_d)^{s_i}$ and $h_i'' = \hat{e}(Cert_i, Y_i)^{s_d} = \hat{e}(Cert_i, Y_d)^{s_i}$, for *i=1, ..., n*;

(b) chooses $m = |\Gamma|$ different values $d_j \in_R Z_q^*$, (*i=1, ..., m*); each from the values unambiguously identifies qualified subsets of an access structure $\Gamma_0 = \{A_1, A_2, ..., A_m\}$;

(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 $\gamma_j = f(d_j) - \sum_{u_{i_j} \in A_j} H_3(h_{i_j}', d_j \beta)$ for each subset $A_j = \{u_{1_j}, u_{2_j}, \ldots\} \in \Gamma_0$, *j=1, ..., m* and next the value $f(1)$;

(e) for every shareholder $u_{i_j} \in A_j$, (*j=1, ..., m; i=1, ..., $|A_j|$*) calculates the evidences in the form:

$$k_{i_j, j} = \frac{\left(H_3(h_{i_j}', d_j \beta) - y^{-1} H_3(h_{i_j}'', d_j \beta)\right)}{s_d + H_2(ID_d, Pk_d)} X_i;$$

(f) publishes β, $f(1)$, $Y = yP$, $Y_{-1} = y^{-1}P$, $(d_j, \gamma_j, k_{i_j, j})$, for *j=1, ..., m* and *i=1, ..., $|A_j|$*; it is worth to note that every shareholder $u_{i_j} \in A_j$ might verify, if his secret value s_i is related with parameters published by TA and the dealer:

$$\hat{e}(H_2(ID_d, Pk_d)P + X_d, s_i^{-1} k_{i,j}) =$$

$$\hat{e}(P, H_3(\hat{e}(Cert_d + Cert_i, Y_d)^{s_i}, d_j \beta) P -$$

$$- H_3(\hat{e}(Cert_i, Y_d)^{s_i}, d_j \beta) Y_{-1})$$

Moreover, the special construction of the evidence $k_{i,j}$ protects from dishonest shareholders, preventing from unauthorized changes of secret values s_i and $k_{i,j}$.

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

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

(b) sets the ciphertext $C = (C_1, C_2, C_3, C_4, C_5, C_6)$, where:

$$C_1 = r(H_2(ID_d, Pk_d) P + X_d)$$

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

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

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

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

$$C_6 = rY_{-1}$$

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 form the privileged subset $u_{i_j} \in A_j \in \Gamma$ ($j \in F$) partially decrypts ciphertext $C = (C_1, C_2, C_3, C_4, C_5, C_6)$, using his/her share s_{i_j}, the following value:

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

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 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

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

where $v_j \in C_5$ and

$$\Delta_1 = C_4$$

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

(b) calculates

$$\sigma = C_2 \oplus H_5(\Delta)$$

(c) calculates

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

(e) recovers

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

(d) 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 combiner can decide if the decrypted ciphertext is corrected.

CIBE-GAS scheme with dynamic access structure

CIBE-GAS encryption scheme allows to update keys and shares and by that to change dynamically access structure:

(a) The secret $y \in_R Z_q^*$ renewal. Assume, that value $y' \in_R Z_q^*$ is a new secret chosen by the dealer. Thedealer chooses another first degree polynomial: $f'(x) = y' + \alpha' x$, $\alpha' \in_R Z_q^*$, and public random numbers $\beta' \in_R Z_q^*$, and next renew and publishes public information β', $Y' = y'P$, $Y'_{-1} = (y')^{-1} P$, $\left(d'_j, \gamma'_j, k'_{i,j}\right)$ for *j=1, ..., m* and *i=1, ..., $|A_j|$* (see **ShareDistribution** algorithm).

(b) Adding the new shareholder u_{n+1}, i.e. $U' = U \cup \{u_{n+1}\}$. The shareholder u_{n+1} with an identity ID_{n+1} chooses a secret key $s_{n+1} \in_R Z_q^*$ and calculates a corresponding public key $Pk_{n+1} = (X_{n+1}, Y_{n+1})$. The TA issues certificate $Cert_{n+1} = sQ_{n+1}$ to the shareholder u_{n+1}, where $Q_{n+1} = H_1(ID_{n+1}, Pk_{n+1})$. Next, the dealer sets a new *m'*-element minimal access structure $\Gamma'_0 = \{A'_1, A'_2, \ldots, A'_{m'}\}$ (e.g. like in the method presented by Daza V., et al. in [11]) and executes the **ShareDistribution** algorithm for a new polynomial $f(x) = y' + \alpha' x$ and the value $\beta' \in_R Z_q^*$.

(c) The shareholder $u_i \in U$ removal, i.e. $U' = U \setminus \{u_i\}$. The dealer, when it is necessary, sets new m'-element minimal access structure $\Gamma'_0 = \{A'_1, A'_2, \ldots, A'_{m'}\}$. Next, dealer executes the **ShareDistribution** algorithm (without the necessity to change the polynomial $f(x) = y + \alpha x$ and values $\beta \in_R Z_q^*$) and renews public information (the values $k_{i,j}$, for *j=1, ..., m* are set to NULL and cannot be used in the encryption and decryption procedures).

(d) The secret $s_j \in Z_q^*$ renewal. Assume that it is necessary to renew the secret $s_j \in Z_q^*$, which belong to the shareholder $u_j \in U$ who chooses a new secret share $s'_j \in Z_q^*$ and calculates a new public key $Pk'_j = (X'_j, Y'_j)$. TA authority issues to shareholder u_j a new certificate $Cert'_j = sQ'_j = sH_1(ID_j, Pk'_j)$. Dealer executes **ShareDistribution** algorithm (without the necessity to change the polynomial $f(x) = y + \alpha x$ and the value $\beta \in_R Z_q^*$), and next renews public information.

Execution of the **ShareDistribution** algorithm might be optimized and limited only to calculations which are necessary to fulfil requirements in one of the cases (a), (b), (c) or (d).

CIBE-GAS scheme allows to fulfil basic ORCON requirement: the dealer who is information owner, decides who can have access to the information (it is each member of minimal access structure, who is able to gather enough number of partial values $\delta_{1_j}, \ldots, \delta_{|A_j|}$ (*j=1, ..., m*)). It is possible to introduce delegation operation to the proposed scheme in easy way. The delegation allows implementing one of the ORCON model extending rules (see Section *Requirements distinguished to access structures*).

Summary

Any information generated on the device or downloaded from external information systems should be protected in accordance with the access policy associated with the information generated or downloaded. This provides a cost effective solution of essential dilemma of every user of classified information - whether the information that was

necessary to me while performing my duties were effectively removed from my mobile device (e.g. laptop) before leaving work?

The article shows that security requirements imposed on classified information should be transferred to the access structure, which reflects the information access policy. Such defined access structures, in turn, allow solving the presented above dilemma. In fact you can use them to construct a corresponding encryption scheme.

The CIBE-GAS encryption scheme provides information protection in accordance with any minimum access structure. It also has the feature of dynamicity, i.e. it allows adopting access structures to the needs by adding or removing the shareholders, and by reconfiguring the access structure itself, without the need to involve the shareholders. Thus, the scheme allows meeting most requirements formulated in Table 2, i.e. decentralization, flexibility, delegation (see [1]), working on- and off-line, classified information storage in untrusted data warehouse and business continuity.

Acknowledgment

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

REFERENCES

[1] Hyla T., Pejaś J., *Certificate-Based Encryption Scheme with General Access Structure*, A. Cortesi et al. (Eds.): CISIM 2012, LNCS 7564, pp. 41–55, 2012.

[2] Act of 5 August 2010 *on Protection of Classified Information* (in polish), Low Diary, Dz.U. 2010, No. 182, pos. 1228

[3] Pejaś J., Hyla T., Kryński J., *ORCON: Originator Controlled Access Control - Theoretical and Practical Methods of Implementation* (in polish), in *Cybercrime and Information Security*, B. Hołyst, J. Pomykała (Eds.), Oficyna Wydawnicza WSM, Warszawa 2012, pp. 277-310

[4] Bishop M., *Computer Security: Art and Science*, Addison Wesley, 2002

[5] Ito M., Nishizei T., Saito A., *Secret sharing schemes realizing general access structure*, Proc. IEEE Globecom'87, IEEE, 1987, p. 99-102

[6] Benaloh J., Leichter J., *Generalized secret sharing and monotone functions*, in Advances in Cryptology - CRYPTO '88, Springer-Verlag, London, 1990, pp. 27-35

[7] Stinson D. R., *An Explication of Secret Sharing Scheme*, Designs, Codes and Cryptography, Vol. 2, No 4, pp. 357-390, 1992

[8] K. Kaşkaloğlu Some Generalized Multipartite Access Structures, PhD Thesis, Middle East Technical University, May 2010

[9] Tassa T., *Hierarchical threshold secret* sharing, Journal of Cryptology, Vol. 20, pp. 237-264, 2007

[10] Bozkurt I. N., Kaya K., Selcuk A. A., *Secret Sharing for General Access Structures*, 4th International Conference on Information Security and Cryptology, Ankara, Turkey, May 6-7, 2010

[11] 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

[12] Shamir A., *How to share a secret*, Communication of the ACM, Vol. 22, pp. 612–613, 1979

[13] Asmuth, C., Bloom, J., *A modular approach to key safeguarding*, IEEE Trans. on Information Theory, Vol. 29, Issue 2, pp. 208–211, 1983

[14] Delerablee C., Pointcheval D., *Dynamic Threshold Public-Key Encryption*, in Advances in Cryptology – Proceedings of CRYPTO 2008 (17–21 August 2008, California, USA), D. Wagner (Ed.), Springer-Verlag, LNCS 5157, pp. 317–334, 2008

[15] 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

[16] Bagga W., *Policy-Based Cryptography: Theory and Applications*, PhD Thesis, Ecole Nationale Supérieure des Télécommunications, Computer Science and Networks, December, 8th 2006

[17] Kitae Kim, Seongan Lim, Ikkwon Yie, Kyunghee Kim *Cryptanalysis of a Dynamic Threshold Decryption Scheme*, Commun. Korean Math. Soc. 24 (2009), No. 1, pp. 153-159

[18] Yongxuan Sang, Jiwen Zeng, Zhongwen Li, Lin You, *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

[19] Cachin C., *On-line Secret Sharing*, in Cryptography and Coding: 5th IMA Conference, Cirencester, UK, (C. Boyd, ed.), Lecture Notes in Computer Science, Vol. 1025, pp. 190-198, Springer, 1995.

[20] Liao-Jun Pang, Hui-Xian Li and Yu-Min Wang, *A Secure and Efficient Secret Sharing Scheme with General Access Structures*, in Proceedings of the Fuzzy Systems and Knowledge Discovery Conference, Berlin: Springer-Verlag, LNAI 4223, pp. 646-649, 2006.

[21] Stinson D. R., *An Explication of Secret Sharing Scheme*, Designs, Codes and Cryptography, Vol. 2, No 4, pp. 357-390, 1992

[22] Pieprzyk J., Hardjono T., Seberry J., *Fundamentals of Computer Security*, Springer-Verlag, Berlin, Heidelberg, New York, 2003

[23] Roberts A., *ORCON Creep: Networked Governance, Information Sharing, and the Threat to Government Accountability*, Campbell Public Affairs Institute, The Maxwell School of Syracuse University, October 2, 2003,

***Authors**:*
Tomasz Hyla, PhD, West Pomeranian University of Technology in Szczecin, Faculty of Computer Science and Information Technology, 52 Żołnierska St., 71-210 Szczecin, e-mail: thyla@wi.zut.edu.pl; *Jerzy Pejaś, PhD eng., West Pomeranian University of Technology in Szczecin, Faculty of Computer Science and Information Technology, 52 Żołnierska St., 71-210 Szczecin, e-mail: jpejas@wi.zut.edu.pl.*