THE ASSURANCE OF SECURITY OF ELECTRONIC VOTING THROUGH THE USE OF SECRETS SHARING SCHEMES AND BENALOH ELECTRONIC VOTING SCHEME

Alexandru-Mihnea SPIRIDONICĂ[1], Marius PISLARU[1]

[1] Technical University „Gheorghe Asache” of Iasi

Abstract

Information security, in the context of using computers to perform electronic operations, electronic voting, electronic voting, electronic payment, electronic auctions, taken on major importance. There is only one way to ensure information security in such situations, through implementation of a proper software. Mainly, such a software is based directly on cryptographic primitives. In this paper we will make a general description of secrets sharing schemes and then we will concentrate at one of the most important electronic vote scheme, namely Benaloh scheme based on homomorphic secrets compose. The schemes are presented in a uniform manner, in order to highlight the differences between then. The operation mode of the schemes that assure a protection and a good functioning of the electronic voting is materialized through the exemplification of implementation of the Benaloh electronic voting scheme.

Key words: electronic voting, sharing secrets schemes, cryptographic primitives, Benaloh scheme, homomorphic secrets compose

Using electronic computers in performing various electronic payments, in implementation of electronic voting schemes or in realization of electronic auctions raises fundamental problems of information security. For a proper functioning of the electronic voting, it is crucial to meet some security requirements (for more details, the reader can consult (Gritzalis D. 2003 and Rivest R.L., Shamir A., Adleman L.M., 1978).

Accuracy requires that the announced result exactly matches with the output of the electrion. This means that nobody can change another vote, all valid votes are taken into account, while invalid votes are not included. A system is considered to be *democratic* if only eligible voters participate, and each eligible voter can vote only once. An additional feature is that nobody would be allowed to duplicate the vote of someone else. In addition, each vote should have the same weight. *Confidentiality in terms of information theory* is stronger and harder to achieve, ensuring that no ballot can be linked to a particular voter as long as the principles of information theory remains valid. *Robustness* ensures that no reasonable sized coalition of voters or authorities cannot disturb the elections. This includes the permission of absence for some of the registered voters without causing problems or avoid the situations in which some entities issues legitimate votes in the name of those absents, and the prevention of fraudulent conduct of voters and of authorities. *Checking* assumes the existence of some mechanisms to verify the elections in order to ensure that it was conducted properly. Can be performed in three different forms: *public or universal checking*, meaning that everyone (voters, authorities, external auditors) can check the partial or final results, *individual checking without opening*, and this is a weaker requirement in which each voter can verify if his vote was take into account without expose his vote and *individual checking with opening*, that is even weaker that the precedent, allowing individual checking by the voter, but forces the voters to uncovering the ballots in order to report a complaint. *Fairness* ensures that nobody can determine the election results before the announcements of final results. The delayed voters could be influenced when reading some results before the official announcement of final results and thus could be produce a significant and unfair advantage to an candidate or to a group. Due to this property, this form of fraud is eliminated. *Checking of participation* ensures that is possible to know if a voter participated to elections by introducing a ballot or not. This measure is neccesary in the countries when voting is compulsory by law (such Australia, Belgium or Greece) or in social context (e.g. elections at a medium or small scale) where the absenteeism is considered a great shame, or even a offense. *Mobility of the voters* is another important requirement. Should be no restriction regarding the location in which the voter can participate to elections. *Flexibility* requires that a system would have allowed a variety of ballots in various languages and adapted to different types of voting processes. The ability to handle ad-hoc situations can also be claimed by this property.

MATERIAL AND METHOD

In the rows below we present some of the most important notions related to sharing secrets. *A sharing secrets scheme* divides a secret in a number of subsecrets. These subsecrets are distributed to users, so that only certain groups can reconstruct the secret. In the first sharing secrets schemes that were proposed in literature, only the number of participants was take into account (it was not important which participant restored the secret, but only their number). These are so-called *threshold-schemes* (Obana S., Kurosawa K., 1996).

Let $n \geq 2$ and $A \subseteq P(\{1,2,...,n\} \setminus \{\phi\})$. A secrets sharing scheme relative to *A* is an (*n*+1) – uple $(S, I_1, ..., I_n)$ so that:

- $\forall A$, the problem of finding the secret *S*, given by the set $\{I_1 \mid i \in A\}$ is „easy”;
- $\forall A \in P(\{1,2,...,n\}) \setminus A$, the problem of finding the secret *S*, given by the set $\{I_i \mid i \in A\}$ is intractable.

A is authorized acces structure (the total acces groups), *S* is secret, $I_1, ..., I_n$ are subsecrets of secret *S* (Shamir A., 1979).

A natural condition that should satisfy the acces structure is property of monotone:

$\forall B \in P(\{1,2,\dots,n\}))\ ((\exists A \in A)\ (A \subseteq B) \Rightarrow B \in A\ )$ (1)

Intuitively, this means that if a group can recover the secret, then a larger group (in the sense of inclusion) may do this. There are some papers that consider non-monotone access structures. In this schemes there are positive and negative subsecrets leading to *veto capability*. Conform to Obana and Kurosawa (Obana S., Kurosawa K., 1996), the easiest solution for veto capability is that, that participants who oppose to offer a wrong subsecret in the subsecret reconstruction phase and this leads to an incorrect secret.

In our paper we consider only monotone access structures *A* that satisfy the condition $(\forall i \in \{1,2,\dots,n\})(\exists A \in A: i \in A)$ because, if there is an *i* so that the mentioned property to be invalid, we can consider the set {1,2,..,*n*}\ {*i*}. In this case, *n* will be named as *structure grad*. Each monotone access structure *A* is complete specified by the set of authorized access minimal groups, i.e:

$$A_{\min} = \{A \in A \mid (\forall B \in A \setminus \{A\})\}(\neg\, B \subseteq A)\} \qquad (2)$$

Also, $\bar{A}$ =P({1,2,..,*n*}) \ A is fully specified by the unauthorized maximal groups, i.e:

$$\bar{A} = \{A \in \bar{A} \mid (\forall B \in \bar{A}) \setminus \{A\})(\neg A \subseteq B) \qquad (3)$$

A special and important class of secrets sharing schemes is the class of *threshold secrets sharing schemes* (Mignotte M., 1983). In these schemes only the cardinality of these groups is important in order to find the secret. More exactly, if the threshold is *k*, 2 ≤ *n* ≤ *k*, the minimal access structure is $A_{\min}$ = {*A*∈P({1,2,…,*n*}) | |*A*| = *k*}. In this case a secret sharing scheme *A* will be named an (*k*, *n*) – threshold secrets sharing scheme.

In the rows below we present the Benaloh electronic voting scheme and then we will use them to illustrate a practical example. The *Benaloh scheme* (Benaloh J., Leichter J., 1989 and Benaloh J., 1987) is based on homomorphic secrets compose. We consider two secrets:

- *S* that decomposes in $I_1, I_2, ..., I_n$ (that are subsecrets of *S*);
- *S*’ that decomposes $I_1^{'}, I_2^{'}, ..., I_n^{'}$ (that are subsecrets of *S*’)

and two operations, ⊕ on secrets set and ⊗ on subsecrets set.

A (*k*, *n*) secrets sharing scheme is (⊕,⊗)-*homomorphic* if:

$$S \oplus S' = (I_1 \otimes I_1^{'}, ..., I_n^{'} \otimes I_n^{'}) \qquad (4)$$

Usually, ⊕ and ⊗ operations are standard operations in Z_p^*, with *p* a prime number. We consider a function *f*(*x*) = $a_{k-1} x^{k-1}$ + …+ $a_1 x$+ a_0 (coefficients in Z_p^*), when a_0 is the secret (*S*). The recovery of the secret from a set $\{I_i / i \in J\}$, where *J* ⊆ {1,…*n*} and |*J*| = *k* is made through Lagrange interpolation:

$$S = \sum_{i \in J} I_i \prod_{i \in J \setminus \{i\}} \frac{j}{j-1} \qquad (5)$$

Indeed, if *f*(*x*) = $a_{k-1} x^{k-1}$ + …+ $a_1 x$+ a_0 and $f^{'}(x)$ = $a^{'}_{k-1}$ x^{k-1} + …+ $a_1{}^{'}$ *x*+ $a^{'}_{0}$ then we can calculate *f* + $f^{'}(x)$ = x^{k-1} (a_{k-1}+ $a^{'}_{k-1}$) + ….+ *x* (a_1+ $a_1{}^{'}$) + (*S*+ $S^{'}$).

$$S = \sum_{i \in J} I_i \prod \frac{j}{j-i} \qquad (6)$$

$$S' = \sum_{i \in J} I_i{}' \prod \frac{j}{j-i} \qquad (7)$$

So, we can make the sum $S + S^{'} = \sum (I_i + I_i{}') \prod \frac{j}{j-i}$.

The voting scheme is as follows:

- A_1,...,A_n sub(authorities) of which at least *k* are reliable;
- each voter *V* elect his vote (0 or 1) and constructs subsecrets $I_1, I_2, ..., I_n$ and send it to sub(authorities) $A_1, ..., A_n$, respectively;

- each sub(authorities) A_i calculates S_i = $\sum_{V voters} I_i^v$;
- at the ending of voting period, sub(authorities) send the partial results to the central authority *A*;
- if even *k* authorities are correct, the sume of the votes can be obtain as *S* = $\sum_{i\in J} S_i \prod_{j\in J, j\neq i} \frac{j}{j-i}$, *S* = the final result, i.e. the sum of votes.

RESULTS AND DISCUSSIONS

The utility and proper functioning of the Benaloh electronic voting scheme are exposed through a practical example.

We consider a number of 4 voters (V_1, V_2, V_3, V_4) and 5 authorities (A_1, A_2, A_3, A_4, A_5) and threshold 3. We consider one function for each voter, and all calculations are made in Z_{11}. So, we realize following calculations:

- for V_1: $f(x) = 2x^2 + 3x + 1$, and $I_1 = f(1) = 6$, $I_2 = f(2) = 4$, $I_3 = f(3) = 6$, $I_4 = f(4) = 1$ and $I_5 = f(5) = 0$;

- for V_2: $f(x) = 3x^2 + x + 1$, and $I_1 = f(1) = 5$, $I_2 = f(2) = 4$, $I_3 = f(3) = 9$, $I_4 = f(4) = 9$, $I_5 = f(5) = 4$;

- for V_3: $f(x) = x^2 + 5x + 0$, and $I_1 = f(1) = 6$, $I_2 = f(2) = 3$, $I_3 = f(3) = 2$, $I_4 = f(4) = 3$, $I_5 = f(5) = 6$;

- for V_4: $f(x) = x^2 + 2x + 1$, and $I_1 = f(1) = 4$, $I_2 = f(2) = 9$, $I_3 = f(3) = 5$, $I_4 = f(4) = 3$, $I_5 = f(5) = 3$;

Table of values

	*A*1	*A*2	*A*3	*A*4	*A*5
*V*1	6	4	6	1	0
*V*2	5	4	9	9	4
*V*3	6	3	2	3	6
*V*4	4	9	5	3	3
Sum	10	9	Not interest	5	Not interest

Applying Lagrange formula $S = \sum_{i\in J} I_i \prod_{j\in J\setminus\{i\}} \frac{j}{j-i}$ we will have the following result:

$$10*\frac{2}{2-1}*\frac{4}{4-1} + 9*\frac{1}{1-2}*\frac{4}{4-2} + 5*\frac{1}{1-4}*\frac{2}{2-4} = 10*2*\frac{4}{3} - 9*2 + 5*\frac{1}{3} = 3.$$

This scheme has the following properties:

- to attack succesfully the scheme, even *k* sub(authorities) must behave dishonestly (resistance at coalition of order $\le k-1$);
- if even *k* authorities are honest, the result is correct (robustness at coalition of order ≤ *n*-*k*).

The presented scheme has three major problems:

- it is not shown that vote $v_i \in \{0,1\}$;
- it is not shown that subvotes $I_1, \ldots, I_n$ are correct, i.e. are subsecrets of the secret v_i and any set *k* of such information leads to the same vote;
- it is not shown that partial results $S_1, \ldots, S_n$ are calculated correct.

CONCLUSIONS

In this paper we presented in a unified way some of the most important elements of secrets sharing, through a compendium based on several such schemes that are known so far. Then, in the second part of the paper we have concentrated on one of the most electronic vote scheme, the Benaloh scheme. Also, we have exemplified the operation mode of this scheme through the presentation of a practical example.

As we seen, the Benaloh scheme has some disadvantages. Principally, it is not demonstrated the correctness of certain steps or entity of the scheme. These disadvantages are somewhat resolved through other electronic voting schemes like CFSY (Cramer, Franklin, Schoenmakers and Yung), by using masks and also by FOO (Fujioka, Okamoto and Ohta) scheme that use blind digital signatures. However, in most applications from this field is used Benaloh scheme, mainly for simplicity and for low number of steps to be achieved.

The demonstration of the accuracy of an electronic voting scheme or that it provides fairness among voters is one of the fundamental problem in the theory of electronic voting schemes, an issue on which we will focus on the future.

Acknowledgement

The present paper was developed with financial support from both ANCS – NACOPAN and PNII 51-015 projects.

BIBLIOGRAPHY

Gritzalis, D., 2003 - *Secure Electronic Voting*. Kluwer Academic Publishers.

Rivest, R.L., Shamir, A., Adleman, L.M., 1978 - *A method for obtaining digital signatures and public-key cryptosystems*, Commun.ACM 21(2).

Obana, S., Kurosawa, K., 1996 - *Veto is Imposible in Secret Sharing Schemes*. Inf. Process. Lett. 58(6), pp.293-295.

Shamir, A., 1979 - *How to share a secret*. Communications of the ACM, 22(11), pp.612-613.

Mignotte, M., 1983 - *How to share a secret*. Proceedings of the Workshop on Cryptography, Burg Feuerstein, volume 149 of Lecture Notes in Computer Science, pp.371-375.

Benaloh, J., Leichter, J., 1989 - *Generalized secret sharing and monotone functions* , in „Advances in Cryptology – CRYPTO ’88” , GoldWasser Ed., Lecture Notes in Computer Science 403, pp.27-35.

Benaloh, J., 1987 - *Secret sharing homomorphisms*: *keeping shares of a secret* , in „Advances in Cryptology – CRYPTO ‘86”, Lecture Notes in Computer Science 236, pp.251-260.