Creation of Secrets Sharing Protocols Resistible Against Disloyal Participants

Petar T. Antonov[1] and Valentina R. Antonova[2]

***Abstract* – This paper reviews a perfected variant of the secrets sharing protocol, bearing in mind the loyalty level of the separate participants. A classification of the possibilities for the grouping of the participants in the protocol is offered, and recommendations are brought out about creation of resistible against disloyal participants secrets sharing protocol.**

***Keywords* – Secret, security, secrets sharing protocol, grouping of the participants, loyalty.**

I. INTRODUCTION

It is well known that the approach to dividing a secret to parts and giving these parts to chosen separate participants is used for a long time in order to increase the security during preserving and subsequent usage of this secret [1,2 etc.]. The security in this case is expressed by the level of prevention against eventual abuse of secrets, for example, independent access and subjective disposition of a common bank account, independent access and illegal consumption of common resources, personal activation of military destructive capacities, etc.

For the practical realization of the approach, mentioned above, it is necessary to have a corresponding *secrets sharing protocol* (SSP) among the participants, in which two interconnected components are differentiated: *secrets sharing scheme* (SSS) and *secrets restoring scheme* (SRS). In SSP it is supposed that all or at least a certain minimum number of the participants of the protocol will be if loyal behaviour and will be able to restore successfully the secret when that occurs to be necessary.

To designate such a scheme of realization the term *threshold structure of restoration* (n, k) is proposed in [1]. In [1] is also offered a perfection of the considered protocol SSP, taking account of the introduced for that purpose *loyalty level of the participants* and using on that basis a *secrets restoring probability scheme* (SRS).

Furthermore, in [1] an analysis is carried out concerning the *probability for successful restoration of secrets* at a threshold structure (n, k), which supposes loyal behaviour of a minimum of *k* out of the included in the protocol *n* participants.

It should be mentioned, however, that the *threshold structure of restoration* introduced above might be considered also as a *structure for grouping of the participants* in SSP by a *parameter of grouping (threshold of restoration) k.* This means that for the completeness of study upon SSP, it is necessary to determine and consider all possibilities of such a grouping. In this connection, in the present report, which is an extension and a development of [1], a *classification of the possibilities for grouping of the participants* in SSP is offered and recommendations are brought out about the choice of parameters of grouping that would guarantee some preliminary given resistibility against disloyal behaviour of the participants in the protocol.

For the purposes of the further consideration we shall introduce and determine the following designations:

- n - number of participants in SSP;
- A_i - i-th participant in SSP;
- k - threshold of restoration;
- S - secret;
- s_i - one i-th part of the secret, that is given to participant A_i;
- R - dealer (distributor);
- p_i - probability for loyal behaviour of the participant A_i;
- q_i - probability for disloyal behaviour of the participant Ai (q_i=1- p_i);
- P - probability for successful restoration of the secret.

II. CLASSIFICATION OF THE POSSIBILITIES FOR GROUPING OF THE PARTICIPANTS

The possibilities for grouping of the participants in SSP or, in other words, the varieties of the threshold structure of restoration (*n, k*), can be classified as follows:

- **arbitrary grouping** (*threshold structure with arbitrary grouping*);
- **orderly grouping** (*threshold structure with arranged grouping*);
- **consecutive – parallel grouping** (*threshold structure with consecutive – parallel grouping*);
- **parallel – consecutive grouping** (*threshold structure with parallel – consecutive grouping*);
- **combined grouping** *(threshold structure with combined grouping*).

In the case of *arbitrary grouping* the separate participants Ai are not interconnected among themselves and an arbitrary

[1]Petar T. Antonov is with the Department of Computer Science and Engineering, Technical University of Varna, 1 Studentska str., 9010 Varna, Bulgaria, E-mail: peter.antonov@ieee.org

[2]Valentina R. Antonova is with the Department of Computer Science and Engineering, Technical University of Varna, 1 Studentska str.,9010 Varna, Bulgaria, E-mail:valyvarna@yahoo.com

subset of them with dimension $l \geq k$ is in position to restore successfully the secretes.

The analysis carried out in [1] concerns this variant of the threshold structure, where ($k \leq l \leq n$) and ($1 \leq k \leq n$). In this case the location of the chosen subset of loyal participants in SSP, respectively, of the parts s_i of the secret granted by these participants, in the *chain of restoration of the secret* is accidental and does not reflect in any way upon the result of the restoration.

Under *orderly grouping* not only the threshold *k* should be taken into account, but also the successive order and the exact location of the separate participants in the *chain of restoration of the secret*. For the case in consideration this chain might be schematically represented as in Fig.1, where the dark squares depict the participants with loyal behaviour, whose number l must not be less than k, and the contents of these squares corresponds to the granted by these participants parts of the secret (s_1, s_3 , … , s_l). It is possible for the chain restoration to be with dimension *n*, as shown in Fig.1, but it might be with reduced dimension *l* as well, if the empty squares, corresponding to the disloyal participants, drop off and the location of the loyal participants, respectively of their parts of the secret, moves forward, keeping their succession.

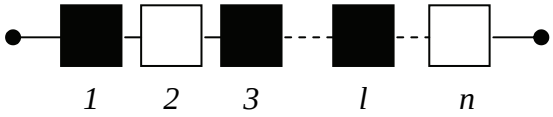

Fig. 1

The scheme for *consecutive – parallel grouping* of the participants in SSP is given in Fig.2, where *m* consecutive groups are shown, connected in parallel, and in each of the consecutive groups there are included *n* participants. At that, the first part s_1 of the secret *S* is given to all the first participants in the consecutive groups, the second part s_2 – to all the second participants and so on, up to the last part s_n, which is given to the last of the participants in each group. The participants in the separate consecutive groups are not interconnected among themselves and can assist in the restoration of the secret only within their own group.

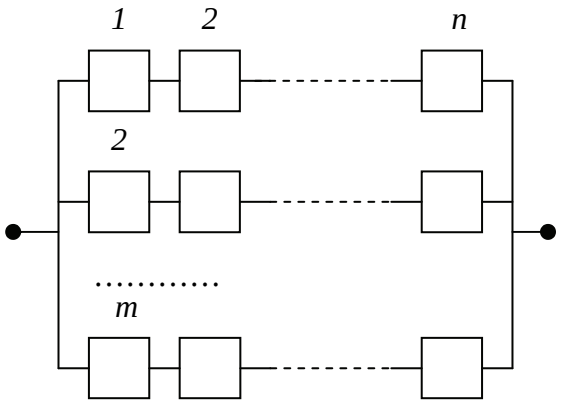

Fig. 2

In this case the total number of the participants is $N = n.m$, and for the successful restoration of the secret it is necessary to have loyal behaviour of not less than *k* participants in at least one of the consecutive groups, connected in parallel. As in each of the consecutive groups there might be included either arbitrary or orderly grouping, we should distinguish *consecutive – parallel arbitrary*, and respectively *consecutive – parallel orderly grouping*.

Parallel – consecutive grouping might be represented as in Fig.3, where *n* parallel groups are consecutively connected, and in each of the parallel groups there are included *m* participants. All the participants in the i-th parallel group receive from the dealer the corresponding part of the secret s_i, so for the successful restoring back the secret are necessary the parts of not less than *k* parallel groups.

It is evident that if the arrangement of the parallel groups in the process of restoration of the secret can be accidental, then the parallel – consecutive grouping will be *arbitrary*, otherwise – *orderly*.

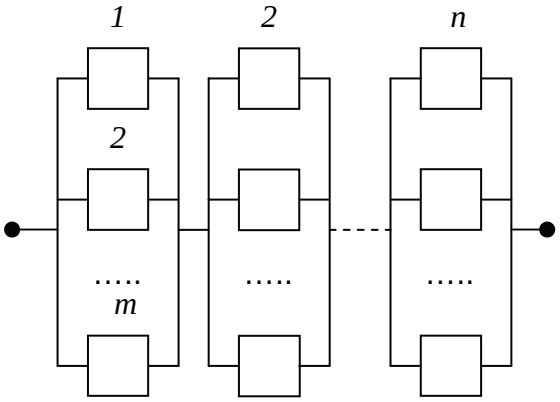

Fig. 3

Combined grouping represents combined usage of the mentioned above possibilities of basic grouping of the participants in SSP. It is evident that the possible variants for such a grouping are many, which gives the opportunity of finding an optimum solution for every particular case in practice.

III. Analysis of the Probability for Successful Restoration of the Secret

In the case of *arbitrary* and *orderly* grouping and provided the separate participants A_i can be considered equally loyal, i.e.

$$\forall i,\ p_i = p = const = 1 - q, \tag{1}$$

then the probability P can be determined using one of the following two equivalent correlations:

$$P = \sum_{i=k}^{n} C_n^i p^i (1-p)^{n-i} = \sum_{i=0}^{n-k} C_n^i q^i (1-q)^{n-i}. \tag{2}$$

In Fig.4 there are given exemplary curves of the changes of *P*, depending on *p*, for different values of *n* and *k*.

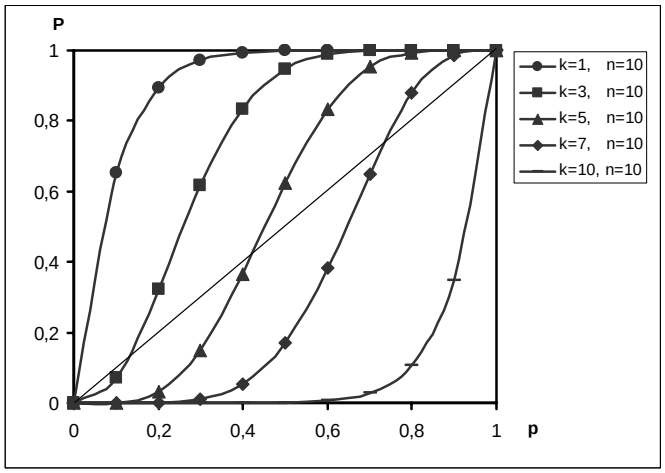

Fig. 4

On the basis of the introduced definitions, in the cases of *consecutive – parallel* and *parallel – consecutive grouping*, the following correlations can be deduced for the probability *P*:

$$P = 1 - [1 - \sum_{i=k}^{n} C_n^i p^i (1-p)^{n-i}]^m \quad \text{and} \tag{3}$$

$$P = \sum_{i=k}^{n} C_n^i [1-(1-p)^m]^i [(1-p)^m]^{n-i} \tag{4}$$

The correlations (2), (3) and (4) given above allow a comparative analysis to be made for the varieties of threshold structure for restoration and recommendations to be given about optimum choice of the *scheme of grouping*, depending on the specific conditions and requirements for resistibility against disloyal behaviour of the participants.

In case a minimum admissible value of *P* is assigned as P_{min} , and using the correlations (2), (3) and (4), analysis can be carried out and can be chosen optimum for the case (with respect to the expenses) scheme of grouping with determination of the parameters *n*, *k* and *m*. Here we ought to mention that in some cases the threshold k and/or the number of the participants *n* will be predetermined by the specific conditions and will not be possible to be decreased.

For example, if we suppose that the threshold $k = n$, then the correlations (2), (3) and (4) will be written respectively in the following form:

$$P = p^n = P_* \tag{5}$$

$$P = 1 - (1 - p^n)^m = P_{**} \tag{6}$$

$$P = [1 - (1-p)^m]^n = P_{***} \tag{7}$$

Let $n = 3$, $p = 0.8$ and $P_{min} = 0.92$. It can be seen that the *arbitrary* and *orderly* grouping in this case are misplaced, as

$$P_* = p^n = 0.512 < P_{\min} \tag{8}$$

For *consecutive – parallel* and respectively, *parallel – consecutive grouping*, we get:

$$P_{**} = 1 - (1 - p^3)^m \geq P_{\min} = 0.92 \tag{9}$$

$$P_{***} = [1 - (1-p)^m]^3 \geq P_{\min} = 0.92 \tag{10}$$

The solutions of the inequalities (9) and (10) are respectively $m = 4$ and $m = 3$, so $P_{**} = 0.9433$ and $P_{***} = 0.9762$.

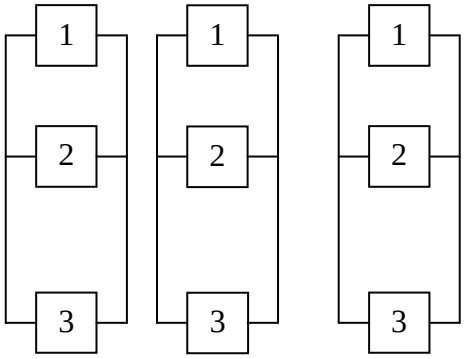

Fig. 5

Therefore in this case it is more expedient to use *parallel – consecutive grouping* with parameter $m = 3$, as at that the expenses on realization will be smaller and the probability $P = 0.9762$ for successful restoration of the secret – considerably bigger. The scheme of this case is given in Fig. 5.

In conclusion, the presented approach can be used to creation a secrets sharing protocols with different resistible level against disloyal participants.

REFERENCES

[1] П. Антонов, В. Антонова, "Подход за усъвършенстване на протокола за разпределяне на секрети", Компютърни науки и технологии, бр. 1, с. 4 – 8, изд. ТУ-Варна, 2005.

[2] В. В. Ященко, Введение в криптографию, СПб.: Питер, 2001. – 288 с.