Proc. of the Second Intl. Conf. on Advances In Computing, Communication and Information Technology- CCIT 2014.

ISBN: 978-1-63248-051-4 doi: 10.15224/ 978-1-63248-051-4-31

Probabilistic synthesis of KDP satisfying mutually complementary correctness conditions

Alexander B. Frolov and Alexander V. Zatey

***Abstract*— On the basis of probabilistic estimates and computer experiments with application of probabilistic algorithms of synthesis of key distribution patterns in a computer network, it is shown that a combination of two well-known correctness conditions KDP, Key Distribution Pattern and HARPS, Hashed Random Preloaded Subset Key Distribution may increase the information rate of the combined scheme HAKDP, Hashed Key Distribution Pattern compared with data rate of schemes based on separate conditions.**

***Keywords*—computer network, system key, key distribution patterns, probabilistic synthesis, probabilistic algorithm, probabilistic estimate, key distribution scheme, cryptographic hash function, correctness condition, information rate**

I. Introduction

Key pre-distribution schemes in the computer network provide the formation by a trusted center packets of secret key information for each network participant and sending these packets to eligible participants via secure channels. These packets are computed on the basis of source key information generated securely by the trusted center. The composition of these packages is published on a public server. A packet secret key information received by each participant should be sufficient for the calculation of working keys for communication with members of the groups it belong to. The composition of the groups is also known and published. Such groups are called *privileged*. On the other hand, there are so-called *forbidden* groups of participants. In a well-designed scheme, all members of such a group using packages received by each of its members should not be able to compute the working key of any privileged group. The correctness of the scheme is guaranteed by a certain condition (correctness condition) which it has to satisfy. Key distribution schemes are characterized by information rate, i.e., the inverse to the total volume of secret packets sent to participants via secure channels. The less secret information is transmitted over secure channels, the greater the information rate. Information rate schemes is the main parameter of its efficiency, the larger it is, the more efficient the scheme. There are known many approaches to key pre-distribution. R. Blom and D. Stinson [1, 2, 3, 4] have proposed algebraic methods.

Alexander B. Frolov and Alexander V. Zatey

National Research University "Moscow Power Engineering Institute", Moscow
Russia

This work has been supported financially by Russian Foundation for Basic Research, project 14-01-00671a.

P. Erdös et al. [5, 6] have studied so-called Key Distribution Pattern, i.e., subset families with pairwise or more generally *r*-wise intersections being Sperner families. Probabilistic algorithms for KDP (Key Distribution Patterns) deriving were proposed in [7]. All those methods are unconditionally secure. Some efficient ad-hoc methods for key pre-distribution were proposed in articles [8, 9, 10, 11, 12]. Due to essential decreasing of secret information distributed in network and scaling property those methods are the most appropriate for networks with mobile devices.

In this paper, it is shown a possibility of constructing a key distribution patterns which correctness condition is disjunction of correctness conditions of two other schemes. The combined scheme is correct if it satisfies at least one of these conditions. Thies means that these conditions are mutually complementary. At the same time, using probabilistic estimates and computer simulations based on probabilistic algorithms of synthesis of key distribution schemes there is shown a possibility of increasing the information rate of key distribution schemes with combined correctness condition.

II. HAKDP satisfying mutually complementary correctness conditions

In this section, as example of schemes with mutually complementary correctness conditions, we study HAKDP(**P**,**F**,*L*)(*n*,*q*)-scheme (Hashed Key Distribution Pattern) using *q* initial secret system keys (binary vectors of a fixed length *k*) for computing of *n* secret packets, one for each of *n* participants, which allow coalitions *F* of participants from the set **F** of forbidden coalitions and groups *P* of participants from the set **P** of privileged groups of participants. Parameter *L* will be explained below. Below we will interpret such coalitions and groups as sets of their participants numbers, i.e., as subsets of the set **U** = {1,2, .., *n*}. To obtain such a scheme there is used the source set **K** of *q* numbered system keys, There are formed *n* its subsets K_i, *i* = 1, ..., *n*, the systems of keys assigned to the *i*-th participant. They correspond to the

"…the positive effect of using two mutually complementary conditions of schemes correctness, reflected in increased their information rate …"

Proc. of the Second Intl. Conf. on Advances In Computing, Communication and Information Technology- CCIT 2014.

ISBN: 978-1-63248-051-4 doi: 10.15224/ 978-1-63248-051-4-31

items of secret packets that will be sent to each of n participant. For each participant, there is determined and published on the server a pair of numerical sets (S_i, D_i). Sets S_i contain the numbers s of system keys from subsets K_i, and sets D_i contain the numbers $D_i(s)$, $0 \le D_i(s) \le L$, defining how many times a keyless cryptographic hash function $h:\{0,1\}^k \to \{0,1\}^k$ has to be implemented to obtain the image of corresponding system key s for including in the secret packet of an i-th participant.

The information rate of the considered key pre-distribution scheme is defined as the value $\rho = 1 \setminus \sum_{i=1}^{n} |K_i|$, i.e., the inverse of the total number of system keys which images sent over secure channels. This definition corresponds to [3].

To compute common key of privileged group P each of its members (i-th network participant) should apply a hash function to the received image of an s-th system key $\max_{j \in P} D_j(s) - D_i(s)$ times. The exploitation key, which is computed by each member of the group P by the image of the system of keys with numbers from the set available to each such member shall not be computed by participants from any forbidden groups on the basis of association of keys images received by them, i.e., using the hash images from the set of keys.

Thus these numerical sets have to satisfy the predicate

$$\begin{aligned} &\forall P \in \mathbf{P}, F \in \mathbf{F}, P \cap F = \varnothing : \cap_{i \in P} S_i \neq \varnothing \wedge \\ &\wedge \{ [\cap_{i \in P} S_i \not\subseteq \cup_{j \in F} S_j] \vee \\ &\vee [\exists s \in \cap_{j \in P} S_j : \max_{j \in P} D_j(s) < \min_{i \in F} D_i(s)] \}. \end{aligned} \quad (1)$$

Then, if there is used a cryptographic hash function, members of any forbidden coalition cannot compute a key shared by participants of any preferred coalition. On the one hand, described HAKDP(**P**,**F**,L)(n,q)-schemes, are a generalization of KDP(**P**,**F**)(n,q)-schemes (Key Distribution Pattern) [14] that do not use hashing, and which are described by sets of sets S_i satisfying the predicate

$$\begin{aligned} &\forall P \in \mathbf{P}, F \in \mathbf{F}, P \cap F = \varnothing : \cap_{i \in P} S_i \neq \varnothing \wedge \\ &\wedge [\cap_{i \in P} S_i \not\subseteq \cup_{j \in F} S_j]. \end{aligned} \quad (2)$$

On the other hand, they are a special subclass of the so-called HARPS(**P**,**F**,L)(n,q)-schemes (HARPS, Hashed Random Preloaded Subset Key Distribution) [6] in which each participant recieves all system keys from the set **K** ($\forall i \in P \cup F : S_i = \{1,...,q\}$) and has a matching predicate of the simple form:

$$\begin{aligned} &\forall P \in \mathbf{P}, F \in \mathbf{F}, P \cap F = \varnothing : \cap_{i \in P} S_i \neq \varnothing \wedge \\ &\wedge [\exists s \in \cap_{j \in P} S_j : \max_{j \in P} D_j(s) < \min_{i \in F} D_i(s)], \end{aligned} \quad (3)$$

Schemes satisfying the predicate (2) were first described in [13]. In that paper, as in [7] they are called set intersection systems.

The advantage of KDP(**P**,**F**)(n,q)-schemes and their particular case of KDP (n,q)-schemes (set **P** includes all two-members subsets, and the set **F** includes all singleton subsets) is their unconditional secrecy, while HAKDP(**P**,**F**,L)(n,q)-schemes and HARPS(n,q)-schemes assume limitation of computational capabilities of network participants since they use the hash function.

The notion of HAKDP(**P**,**F**,L)(n,q)-scheme was introduced in [14]. Let as define formally this concept informally explained above.

Definition [15]. HAKDP (**P**,**F**,L)(n,q)-scheme, where **P** and **F** are families of subsets of **U**={1,...,n}, is a pair ($\tilde{\mathbf{K}}$,**D**) of families $\tilde{\mathbf{K}}$ = {K_1, ...,K_n} of subsets of a finite numbered set **K** of q elements (system keys) and **D** = {D_1, ...,D_n} of subsets of the set {0,1, ..., L} with the elements of the sets D_i being in one-to-one correspondence with the elements of the sets K_i, i = 1, ...,n, satisfying the condition (1) where S_i (or S_j) are the sets of numbers of the elements of **K**, forming the set K_i (or K_j).

Correctness conditions for HAKDP(**P**,**F**,L)(n,q)-scheme

1) [$\cap_{i \in P} S_i \not\subseteq \cup_{j \in F} S_j$],
2) [$\exists s \in \cap_{j \in P} S_j : \max_{j \in P} D_j(s) < \min_{i \in F} D_i(s)$]

in (1) are mutually complementary: performence of any of them is sufficient to check the correctness of the scheme (matching predicate (1)). Below we will mention the first of these conditions as KDP-condition, and the second one as HASH-condition. It provides the possibility of reducing the number q=|**K**| of source system keys, and the total number of their hash images sent from a trusted center to network participants via secure channels, that is, the possibility of increasing of the information rate of key distribution patterns.

For the synthesis of the key distribution patterns along with deterministic algorithms probabilistic algorithms are used.

A probabilistic method for the synthesis of KDP(**P**,**F**)(n, q)-schemes was first proposed in [7].

In this paper, for the synthesis of HAKDP(**P**,**F**,L)(n,q)-schemes there is used a probabilistic algorithm with preliminary evaluation of a number q of system keys in the source set **K** that is sufficient for successful termination of algorithm

The input for the algorithm are the numbers n, q, p, $0,5 \le p \le 1, L, 0 \le L, L \in Z,$, as well as the descriptions of sets **P** and **F** of privileged groups P and forbidden coalitions F. Output is the pair of families, calculated via randomized procedures for the choice of sets K_i, i = 1, ..., n. Each element of **K** is included in any subset K_i with probability p. Elements of D_i, i = 1, ... n, are taken from the set {0, ..., L} with uniform probability 1\(L+1). A chosen pair of families ($\tilde{\mathbf{K}}$,**D**) is checked to obey the predicate (1). In the case of the positive result of verification a computed scheme is returned, otherwise, the algorithm fails. A natural extension of this algorithm is to implement it in a loop with a repetition cycle at failure. This algorithm is characterized by the probability of successful synthesis of circuits in a single iteration.

Proc. of the Second Intl. Conf. on Advances In Computing, Communication and Information Technology- CCIT 2014.

ISBN: 978-1-63248-051-4 doi: 10.15224/ 978-1-63248-051-4-31

Denote $c=npq$ an everage value of $\sum_1^n K_i$ and $\rho=1\backslash c$ an average value of information rate of probabilistically synthesized HAKDP(**P**,**F**,*L*)(*n*,*q*)-schemes.

Note that in the case $p = 1$ the synthesized scheme does not correspond to the KDP-condition (i.e. predicate (2)), and the family **D** is HARPS(**P**,**F**,*L*)(*n*,*q*)–scheme. On the other hand for $L = 0$, it does not correspond to the HASH-condition (i.e. predicate (3)), and the family is KDP(**P**,**F**)(*n*,*q*)–scheme. For other choices of parameters *p* and *L* it is enough to match any of these conditions (predicates) to synthesize a scheme successfully.. Therefore, it becomes possible to increase the information rate of a key distribution scheme.

III. Estimation of the number of source system keys

By definition, the pairs of sets ($\tilde{\mathbf{K}}$,**D**) are in one-to-one correspondence with the pairs of families (**S**,**D**), where **S** = $\{S_1, ..., S_n\}$. If the cardinalities of the elements of **P** are equal to *g*, and the cardinalities of the elements of **F** are equal to *w*, then HAKDP(**P**,**F**,*L*)(*n*,*k*)-scheme is denoted HAKDP(*g*,*w*,*L*)(*n*,*k*).

Clearly, there is a certain value *q*, wherein HAKDP(**P**,**F**,*L*)(*n*,*k*)-scheme with $|\mathbf{K}|=q$ exists but it does not exist when $|\mathbf{K}|<q$. It is almost impossible to determine *q* exactly and it is yet more difficalt to build a corresponding scheme. Nevertheless one can find some upper estimate. The latter can be obtained by assuming that all sets in **P** contain the same number *g* of elements (minimum cardinality of elements of this set). Similarly, the sets in **F** contain the same number *w* of elements (maximum cardinality of elements of this set). Further, in the calculation of the upper estimate, we suppose the inequality in (1) to hold not for some element only, but for all elements. That is, an upper bound will be calculated satisfying the predicate

$$\begin{aligned}&\forall P\in \mathrm{P}, F\in \mathrm{F}, P\bigcap F=\varnothing : \bigcap_{i\in P} S_i \neq \varnothing \wedge \\ &\wedge\{[\bigcap_{i\in P} S_i \not\subseteq \cup_{j\in F} S_j]\vee \\ &\vee[\forall s\in \bigcap_{j\in P} S_j : \max_{j\in P} D_j(s) < \min_{i\in F} D_i(s)]\}.\end{aligned} \quad (4)$$

Let **P** be a family of all cardinality *g* subsets of **U** and **F** be the family of all cardinality *w* subsets of **U**, and $g+w\le n$. Let us estimate the probability $P_{L,g,w}$ that the inequality $\max_{i\in P} D_i(s) < \min_{i\in F} D_i(s)$ in the expression (4) holds for all $s\in \bigcap_{i\in P} S_i$.

Take a set $D_{i\in F}$. The probability of the event $D_{i\in F}(s) = t$ is $\frac{1}{L+1}$.

The probability that for a particular set $D_{i\in P}$ the value $D_{i\in P}(s)$ is less than *t*, is $(L-t)\backslash(L+1)$.

The joint probability of the events $D_{i\in F}(s)=t$ and $\forall i D_{i\in P}(s) < t$ is $\frac{1}{L+1}\left(\frac{L-t}{L+1}\right)^g$.

The probability that these events occur at the same time, for some *t*, is $\sum_{i=0}^{L}\frac{1}{L+1}\left(\frac{L-t}{L+1}\right)^g$.

Finally, the probability $P_{L,g,w}$ that these events occur for some certain *t* and the indicated specific value $D_{i\in F}(s)$ is minimal is not less than $P'_{L,g,w}=\sum_{i=0}^{L} w^{-1}\frac{1}{L+1}\left(\frac{L-t}{L+1}\right)^{g+w-1}$.

The expected number of pairs of sets (**P**,**F**) for which the predicate (2) is not satisfied is defined by the formula [16]:

$$E(q,p)=\sum_{P\in\mathbf{P}}\sum_{\substack{F\in\mathbf{F}\\ P\bigcap F=\varnothing}}\left(1-p^g(1-p)^w\right)^q$$

The expected number *X* of pairs of subsets (**P**,**F**) with inequality $\max_{j\in P} D_j(s) < \min_{i\in F} D_i(s)$ in (3) being violated for each *s* is

$$\begin{aligned}&E'[X](q,p,g,w)= \\ &=\sum_{P\in\mathbf{P}}\sum_{\substack{F\in\mathbf{F}\\ P\bigcap F=\varnothing}}(1-p^g(1-p)^w-p^g(1-(1-p)^w)P'_{l,g,w})^q= \\ &=C_n^g C_{n-g}^w(1-p^g(1-p)^w-p^g(1-(1-p)^w)P'_{l,g,w})^q.\end{aligned}$$

In this formula,

$$(1-p^g(1-p)^w)-p^g(1-p)^w)P'_{L,g,w}$$

is the probability of collision, i.e., violation of the inequality for a particular pair of sets (**P**,**F**).

The number $q=|\mathbf{K}|$ of source system keys that is sufficient for a synthesis scheme in single iteration of probabilistic algorithm with success probability *E* can be obtained by taking the logarithm in the inequality $E'(q,p,g,w)<(1-E)$:

$$q<\frac{\log\left((1-\mathrm{E})\cdot\frac{g!w!}{(n-g-w+1)\cdot\ldots\cdot n}\right)}{\log\left(1-\left(p^g((1-p)^w+p^wP_{L,g}\right)\right)}. \quad (5)$$

It is clear that if the number of source system keys is less than *q* then one has to execute more iterations of the probabilistic algorithm to synthesize a scheme.

IV. Computer experiments

The aim of the section is experimental confirmation of the above estimate along with the positive effect of using two mutually complementary correctness conditions in a probabilistic algorithm for synthesis of HAKDP-scheme.

Proc. of the Second Intl. Conf. on Advances In Computing, Communication and Information Technology- CCIT 2014.

ISBN: 978-1-63248-051-4 doi: 10.15224/ 978-1-63248-051-4-31

Let us fix the parameters n =16 (the number of participants in the network), and E = 0.5 (the probability of successful synthesis of circuits in a single iteration of the probabilistic algorithm).

Compare the results of estimation and the computer experiments for two series of schemes

1) HAKDP (3, w, 20) (16, q), w = 2,3 and

2) HAKDP (3, w, 0) (16, q), w = 2,3

at varying parameters p of the probabilistic algorithm. In

With p <1, the schemes of the first series satisfy predicate (2) or predicate (3), i.e., in the aggregation they satisfy predicate (1). With p=1 they satisfy only predicate (3). Schemes of the second series satisfy only predicate (2).

In Table 1, for the first series of schemes there are presented the values q, obtained by the formula (5) and the values q' that have been achieved experimentally, in terms of allowable time t<100 sec. In Table 2 there are presented similar data for the second series of schemes. The data table show that the analytically obtained estimates are confirmed in practice, namely, we can build schemes when the number q' of used system keys is less than the number q sufficient for the construction of the scheme in the single iteration of the probabilistic algorithm. In this case, it is clear that the use of HASH-condition in addition to the KDP-condition implies a decrease in sufficient q and experimentally achieved q' numbers of source system keys.

In Table 3 for the first series of schemes (L=20) and for the second series (L=0), there are presented the average values c'=pnq' corresponding to values q' achieved experimentally.

In Table 4 there are presented the values c'' obtained experimentally upon successful completion of computer experiments on the synthesis of these two series schemes.

The data in Table 4 correspond to the expected data in Table 3: the actual data in Table 4 differ from the expected no more than ten units. The data in the lowest rows are the same, i.e., in the respective schemes all q' units of the source key information are assigned to each participant.

Comparison of the italicized data in the columns of the first series schemes (L = 20), with the data in the bottom line indicates a positive effect (increase in the information rate that is inverse of c') of using KDP- conditions (in addition to HASH-condition). Comparison of the italicized data in adjacent columns of the first (L = 20) and second (L = 0) series of schemes indicates a positive effect of using HASH-condition (in addition to the KDP-condition). The results of this analysis are depicted in Fig.1 and Fig.2.

In this paper, the estimate of number of system keys q whose hash images are distributed network participants, sufficient for the synthesis of HAKDP(**P**,**F**,L)(n,q)-schemes for practically reasonable number of iterations of the probabilistic algorithm has been obtained and confirmed by computer simulation experiments. Taking this estimate and the probabilistic algorithm for synthesizing such schemes, the positive effect of using two mutually complementary conditions of scheme correctness, reflected in increased their information rate with respect to information rate of schemes satisfies separate conditions has been confirmed experimentally by computer simulation.

TABLE I.

	w			
	2		3	
p	q	q'	q	q'
0,5	289	145	609	290
0,6	226	110	541	*230*
0,7	196	94	503	210
0,8	178	*80*	447	205
0,9	160	76	357	205
0,95	148	75	308	205
0,99	134	75	274	205
1	130	75	266	205

TABLE II.

	w			
	2		3	
p	q	q'	q	q'
0,5	365	235	768	640
0,6	331	220	868	720
0,7	370	240	1295	1010
0,8	556	325	2927	2350
0,9	1562	790	16440	-
0,95	5309	2560	111800	-
0,99	117300	-	-	-
1	-	-	-	-

TABLE III.

	w			
	2		3	
p	c', (L=20)	c', (L=0)	c', (L=20)	c', (L=0)
0,5	1160	*1880*	2320	*5120*
0,6	1056	2112	*2208*	6912
0,7	1053	2688	2352	11312
0,8	*1024*	4160	2624	30080
0,9	1095	11376	2952	-
0,95	1140	38912	3116	-
0,99	1188	-	3247	-
1	1200	-	3280	-

Proc. of the Second Intl. Conf. on Advances In Computing, Communication and Information Technology- CCIT 2014.

ISBN: 978-1-63248-051-4 doi: 10.15224/ 978-1-63248-051-4-31

TABLE IV.

	w			
	2		3	
p	*c', (L=20)*	*c', (L=0)*	*c', (L=20)*	*c', (L=0)*
0,5	1199	*1917*	2372	*5076*
0,6	1077	2100	*2198*	6809
0,7	1058	2654	2334	11306
0,8	*1028*	4153	2662	22519
0,9	1103	11299	2969	-
0,95	1120	38835	3135	-
0,99	1143	-	3245	-
1	1200	-	3280	-

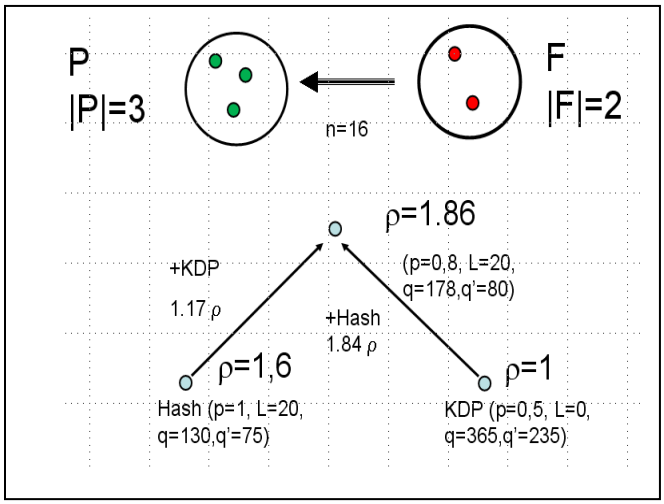

Figure 1. The results of computer experiments with HAKDP(3,2)-(16,*q*) schemes.

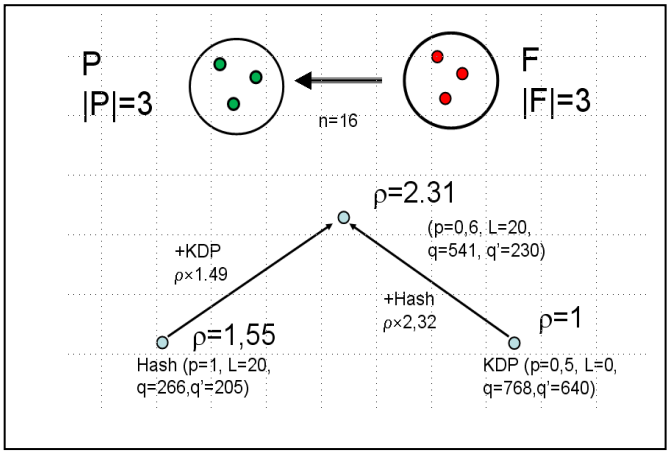

Figure 2. The results of computer experiments with HAKDP(3,3)-(16, *q*) schemes.

Acknowledgment

The authors are grateful to Igor Sergeev for helpful comments.

References

[1] R.Blom, "Nopublic key distribution." Advances in Cryptology. Proceedinge of EURUCRYPT'82. Plenum. New York, 1983, pp. 231--236.

[2] R.Blom, "An optimal Class of Symmetric key Generation Systems." Advances in Cryptology: Proc. of Eurocrypt 84, Lecture notes in Computer Science, 209, Springer-Verlag, 1984, pp. 335-338.

[3] D. R. Stinson. "On Some Methods for Unconditionally Secure Key. Distribution and Broadcast Encryption." Designs, Codes and Cryptography, Kluwer Academic Publishers, Norwell, MA, USA, 1997.

[4] Stinson D.R. "Cryptography: Theory and practice." Third Edition, CRC Press, Boca Raton, Florida, 2006.

[5] P. Erdös , P.Francl , Z.Füredi. "Families of Finite Sets in which no Set is Covered by the Unuon of 2 Others". Journal of Combinatorial Theory. Series A. 33, 1982, pp. 158-166.

[6] P. Erdös, P.Francl , Z. Füredi. "Families of Finite Sets in which no Set is Covered by the Unuon of *r* Others". Israel Journal of Mathematics. 51, 1985, pp. 79-89.

[7] M.Dyer , T.Fenner , A.Frieze , A.Thomason. "On key storage in secure networks." Journal of Cryptology, vol. 8, 1995, pp. 189--200.

[8] M.Ramkumar , N.Memon , R.Simha. Pre-Loaded Key Based Multicast and Broadcast Authentication in Mobile ad-Hoc Networks. Globecom-2003.

[9] L.Leighton , S.Micali. "Secret-Key Agreement with out Public-Key Cryptography". Advances in Cryptology-CRYPTO-1993}, 1994, pp. 456-478.

[10] M.Ramkumar , N.Memon. "An efficient key predistribution scheme for ad hoc network security". Selected Areas in Communications, IEEE Journal on, vol. 23, Issue 3, March 2005, pp. 611 - 621.

[11] M.Ramkumar. "Broadcast Encryption Using Probablistic Key Distribution and Applications." Journal of Computers, vol. 1, No3, June 2006, pp. 1-12.

[12] M.Ramkumar. "I-HARPS: an Efficient Key Pre-Distribution Scheme." E-print Archive, Rep 138, 2005, pp.1-13.

[13] C.J. Mitchell, F.C. Piper. "Key storage in secure networks". Discrete Applied Mathematics. 21., 1988, pp. 215─228.

[14] A.B. Frolov, I.I. Shchurov. "Non-Centralized Key Pre-Distribution in Computer Networks". IEEE Proceedings of International Conference on Dependability of Computer Systems DepCos-RELCOMEX 2008, Szklarska Poreba, Poland, Computer Society Conference Publishing Services. Los Alamitos, California, Washington, Tokyo, 2008, pp. 179-188.

[15] A.B. Frolov, A.V. Zatey. "Hashed key pre-distribution schemes allowing coalitions." MPEI Bulletin, 6, 2013, pp. 166-172. (In Russian).

[16] I.I, Shchurov "Key material minimazation for safe network construction." MPEI Bulletin, 6, 2006, pp. 112-118. (In Russian).