Authentication of Diffie-Hellman Protocol for Mobile Units Executing a Secure Device Pairing Procedure in Advance

Viktor Yakovlev, Valery Korzhik
The Bonch-Bruevich Saint-Petersburg State University of Telecommunication
Saint-Petersburg, Russia
viyak@bk.ru, val-korzhik@yandex.ru

Sergey Adadurov
JSC "VNIIZHT"
Moscow, Russia
Adadurov.Sergey@vniizht.ru

***Abstract*—It is well known that Diffie-Hellman key distribution protocol is vulnerable to a man-in-the-middle attack for which an adversary manages to share the key with the legitimate users. In order to protect the protocol against such attack it is necessary to authenticate so called Diffie-Hellman values using some additional secret information shared by the legitimate users in advance. For mobile units using for a communication between portable devices, it is very appropriate to extract an authenticating information executing the secret device pairing process. But the drawback of this method is a little disagreement between authenticating strings of different users. The mathematical model of the described scenario is a binary symmetric channel without memory. An authentication method based on the use of such additional strings slightly corrupted by errors and followed by executing the hash functions chosen from strongly universal$_2$ hash function class is considered. The formulas for probabilities of the undetected deception and the false alarm are proved. In addition, the methods of parameter optimization, i.e. the number of blocks and the full authenticator length, are proposed.**

I. INTRODUCTION

Let us consider a scenario when a pair of mobile users Alice (A) and Bob (B) need to communicate securely with each other, but they do not have a secret key for the encryption/decryption procedures. The way out is to apply so called Diffie-Hellman key sharing protocol (DHP) in order to generate a common key. Let us remind briefly DHP in line with its description in [1] and presented in Fig.1.

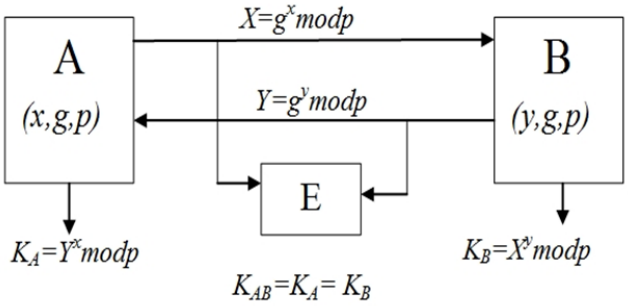

Fig.1. Diffie-Hellman key sharing protocol

We can see from Fig.1 that initially A and B agree about the prime number p and element $g \in GF(p)$ of the high order. Then, users forward the values X and Y to one another over the noiseless public channels. Finally, A and B compute the values K_A and K_B respectively in such a way, so they must be equal one to another (K_{AB}) as it is showed in Fig.1.

If an eavesdropper Eve (E) is passive, she can intercept DH-values with her knowledge of the values g and p only. In order to find the secret key K_{AB}, Eve has either to find the value x (or y) calculating discrete $\log_g X (mod\ p)$ or at least to solve *Diffie-Hellman problem*, i.e. compute $g^{xy} (\mathrm{mod}\ p)$ given $g^x (\mathrm{mod}\ p)$ and $g^y (\mathrm{mod}\ p)$. It is well known [2] that solution for such problems belongs to so called *hard problems class* and it can be computationally unsolvable for an appropriated selection of the parameter p. But unfortunately, the *man-in-the-middle* attack takes place when an eavesdropper is exchanging the false DH-values with the legitimate users and therefore shares the common secret with them.

The way to prevent such an attack is to authenticate DH-values, namely, to prove to the legitimate users that they have received X and Y transmitted from one to another but not from eavesdropper. The straightforward solution for this problem would be to use the digital signature with public key certified by some authority or by legitimate users themself, for DH-values. However, such approach is not that convenient, especially for the case when a couple of communicating mobile users do not know each other initially. In this paper another way known as the *secure device pairing* is suggested. Following to the mentioned above strategy, mobile units must arrange a personal meeting in advance. During this meeting users produce *authenticating strings* (AS) ***a*** and ***b*** without direct electrical contact of one unit with another because it can be impossible sometimes [3-5]. The simplest example of such a string generation is the pairing of two or more smartphones as it shown in [6] (see also Fig. 2).

It worth to note that eavesdropper is as a rule on some large distance from the legitimate users during this meeting. Hence, he (or she) is unable to intercept either ***a*** or ***b.*** But on the other hand, the legitimate users can receive ***a*** and ***b*** only

with some small errors introduced between them. We approximate the authenticating channel by *binary symmetric channel* without memory (BSC) with some known *bit error rate* (BER). Namely, such arrangement creates a special condition for the further investigations of authentication procedure.

Fig.2. An example of device pairing

In Section II the scenario of authentication procedure is specified and described briefly using different methods of authenticating strings generation.

Section III describes the proposed authentication algorithms with use of the hash functions taken from strongly universal$_2$ class.

Section IV presents a proof of the formulas for probabilities of undetected deception and the false alarm probabilities for DH-values.

Section V is devoted to parameter optimizing in order to choose the appropriate authenticated block and authenticator lengths.

Section VI concludes the main results and proposes the directions for the further investigations.

II. Scenario of Authentication Procedure and Different Approaches for Authenticating String Generation Design

In order to provide a reliable authentication of DH-values during the key sharing between mobile unities based on the use of DHP, firstly, it is necessary to arrange a generation of the authenticating strings for both units. Let us call the last procedure performed by the mobile unit devices by *conjugation.* This means that the mobile units arrange a personal meetings in advance, as soon as injection of AS into mobile units is performed on a base of additional communication channel (out of band) like visual, acoustic, vibration, magnetometer etc. It is usually called by *secure device pairing method* [8].

A comparative review of this kind of methods is given in papers [7-14]. The main features of the approach are the following:

– it is assumed that eavesdropper is unable to intercept AS during a conjugation,
– since the users' devices differ to one another, such disagreement can be modeled by BSC without memory and given BER,
– capacity of the channel is quite low and hence the requested length of AS should be minimized.

Let us consider examples of the two most common AS sources only, the vibration and magnetometers. The first approach requires mobile device to have accelerometer sensors inside. Then one of the users must shake two devices in one hand for about 5 s [12]. The both devices shaken together compute their location in space and transform these data into digital authentication strings.

The second magnetometer-based method executes an extraction from the both devices data and exchange by them between units [7]. Users need to hold the devices close to each other for a few seconds without a performing any additional operations. This method is superior against the previous one in terms of the data injection rate. Moreover, it provides a lower BER between units. Therefore, we will consider further the magnetometer-based method only, although all our proofs are valid also for the other pairing methods.

In Fig.3 the scenario of the authenticated key sharing protocol based on DHP in presence of active eavesdropper E is given.

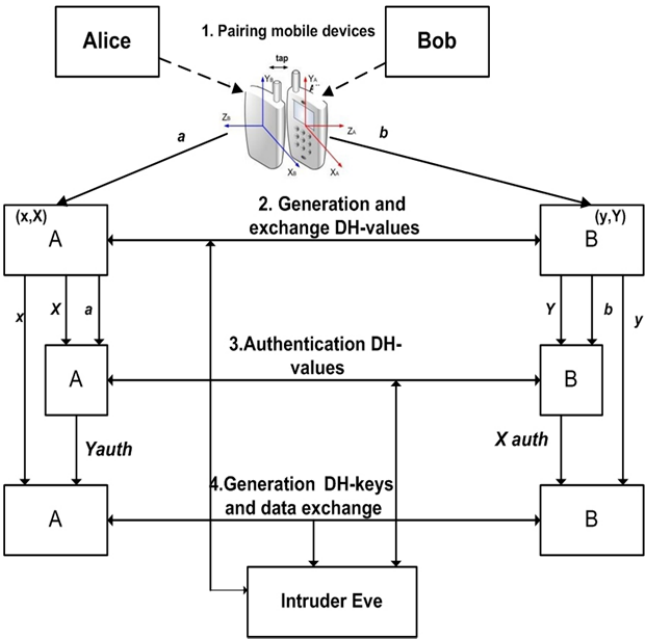

Fig.3. Scenario of the authenticated key sharing protocol based on DHP

We can see from Fig.3 that initially A and B execute mobile unit conjugation placing devices sufficiently close one to another. They can correct data something based on the measurement.

Our experiments show that BER between the users' binary strings obtained by magnetometer-based method are about 0.06. More detail investigation of this approach can be found in [15].

But an eavesdropper is located typically about 1m away from the legitimate users' devices. Therefore he (or she) cannot agree on the bases and provides the probability smaller than 0.5.

Next, the legitimate users exchange their DH-values, authenticate them by strings ***a*** and ***b,*** and if authentication is successful in the both directions, A and B calculate the common key. Now they can transmit a confidential information encrypted by an authenticated shared key over the public channel.

In the paper [16] a method of an authentication based on the use of *forward error correction* (FEC) [17,18] was proposed. However, it requires considerably long sequences ***a*** and ***b*** that is inconvenient in our case**.**

In this paper we suggest to apply the hash functions taken from universal$_2$ class hash for authentication of DH-values with authenticating strings ***a***, ***b*** jointly. This approach is presented in the next Section.

III. An authentication method for DH-values based on the use of Wegman-Carter's algorithm and initially distributed random bit strings

Let us remind definition of hash functions belonging to strongly universal$_2$ class H [19]. It is a set of the mappings $X \to Y$ such that:

- for any $x \epsilon X$ and $y \epsilon Y$ the following condition holds
  - $\#\{hmH : y = h(x)\} = \frac{|H|}{|Y|}$,
- for any x_1, $x_2 \epsilon X$ and y_1, $y_2 \epsilon Y$, $x_1 \neq x_2$ the following condition holds
  - $\#\{hmH : y_1 = h(x_1), y_2 = h(x_2)\} = \frac{|H|}{|Y|^2}$,

where $|H|$ is the total number of hash functions in H, the $|Y|$ is the total number of authenticators and $\#\{*\}$ is the number of hash functions, satisfying to the condition in brackets.

Having received authenticating string ***a*** and ***b,*** A and B perform the following steps for authentication of DH-protocol providing a common key sharing:

Let us denote the length of DH-value by n_{DH}.

1) Both A and B receive DH-values X and Y after exchanging of the information over the channel $A \to B$ and $B \to A$, respectively, in line with Fig.3.
2) A divides her DH-value X on $N = \frac{n_{DH}}{m}$ blocks $u_1, u_2, ..., u_N$ of the length m each, whereas B does the same procedure to get N blocks $s_1, s_2, ..., s_N$ for DH-value Y.
3) Both A and B compute authenticators $w_1, w_2, ..., w_N$ and $z_1, z_2, ..., z_N$, respectively for each of the blocks DH-values based on strongly universal$_2$ class H of hash functions,
   It is naturally to use the disjoint blocks of the length $2m$, taken from the sequences a and ***b*** for authenticators' calculations.
4) Both A and B send authenticators w_i, z_i, $i = 1, 2, ..., N$ over the public channel to the opposite users.
5) Both A and B compute proper authenticators w_i', z_i', $i = 1, 2, ..., N$ as the functions of $(u_i, b_i), (s_i, a_i)$, respectively.
6) Both A and B compare authenticators w_i with w'_i and z_i with z'_i respectively.
7) If the following inequalities hold
   $\#\{i : z_i = z_i'\} \geq \Delta$, $\#\{i : w_i = w_i'\} \geq \Delta$,

where Δ is some chosen threshold, then DH-protocol is assumed to be verified in the both directions.

Then A and B extract common key K_{AB} (see Fig3.) and start the secret communication using some symmetric encryption/decryption algorithm with the shared common key K_{AB}.

Let us specify authentications procedure executing strongly universal$_2$ class of the hash functions and authentication sequences ***a*** and ***b*** shared by the legitimate users in advance. We will use Wegman-Carter algorithm in order to compute the authenticators [19].

Every block u_i of the length m is presented as an element of Galois field $GF(2^m)$. Then authenticator w_i, (similary z_i) can be calculated as follows

$$w_i = [u_i \times k_{0i} + k_{1i}]_v,$$

where k_{0i}, $k_{1i} \in GF(2^m)$, $i = 1, 2, \cdots, N$ are authentication keys, with notations $\times, +$ meaning operations of addition and multiplication in Galois field $GF(2^m)$. $\lfloor w \rfloor_v$ means a choice of the left or right v digits among the m digit of the whole block w. It is obviously that in our case blocks $k_{0i}, k_{1i} \in GF(2^m)$ are taken as sequential blocks of the length m each from the string ***a*** (or ***b*** for authenticator z_i).

The probability of the false block $(u_i' \neq u_i)$ deception for the given blocks $\boldsymbol{u_i}$, $\boldsymbol{w_i}$ and unknown k_{0i}, k_{1i}, will be the following [19]:

$$P_s(block) = \frac{1}{2^v}. \quad (1)$$

Because for the each block authentication requires the separate key of the length $2m$ bits, hence for the authentication of the whole DH-value the sequences ***a*** (***b***) of the length $L = 2mN$ are needed.

Eavesdropper Eve can perform three main versions of attacks in order to break authenticity of the DH-protocol:

Impersonation attack, when a forge DH-value $X' = g^{x'}$ is created by E without the knowledge of values X,w or Y,z.

Reflection attack, when E intercepts DH-value $X = g^x$ jointly with authenticators w_i, $i = 1, 2, ..., N$ and resends them back to A.

Substitution attack, when E intercepts DH-value $X = g^x$ jointly with authenticators $w_i, i = 1,2,...,N$ and generates a false value $X' = g^{x'}$, adding for each of blocks u_i' included in *X'* authenticators w_i' following to the rule:

if $u_i' = u_i$ then select $w_i' = w_i$,

if $u_i' \neq u_i$ then select w' as truly randomly generating values.

Next Eve sends to Bob both $u_i(u_i'), w_i(w_i')\ i = 1,2,...,N$ impersonating as Alice.

IV. ESTIMATIONS OF AUTHENTICATION PROTOCOL EFFICIENCY

Let us introduce the following probabilities that can be taken jointly as the quantitative estimation of authentication protocol efficiently:

P_f is the probability of false rejection of DH-value that occurs when the number of non-authenticated blocks u_i is at least Δ+1 under the condition that no attacks were performed by E. (This event can be appeared due to a disagreement of strings ***a*** and ***b.***)

P_i is the probability of successful impersonating attack.

P_{ref} is the probability of successful reflection attack.

P_s is the probability of successful substitution attack.

P_d is the probability of false DH-value deception. It is equal to $P_d = \max(P_i, P_{ref}, P_s)$ by definition.

Since these probabilities are obviously connected with one to another, we select the requirements that should be provided as $P_d \le \tilde{P}_d$, $P_d \le \tilde{P}_d$, where $\tilde{P}_f, \tilde{P}_d$ are some given values initially.

Then, our problem is to select the parameters *m* (authenticator block length) and *v* (authenticator block length) for which the following inequalities hold $P_d \le \tilde{P}_d$, $P_d \le \tilde{P}_d$). If these inequalities hold for several pairs (*m*, *v*), then optimal parameters be such ones for which the total length of all authenticators $W = vN$ is minimal. (Remember that, the total key length for any variant must be equal to $L = 2mN = n_{DH}$).

It is important to prove the new formulas for the probabilities given above because secure DH-protocol authentication is based on the different authenticating sequences ***a*** and ***b*** and simultaneously on Wegman-Carter authentication algorithms [19].

P_f can be found as the probability of at least Δ+1 breaking authentication among ***u*** blocks, that is in turn equal to the follow value

$$P_f(\Delta) = \sum_{i=\Delta+1}^{N} \binom{N}{i} p_b^i (1-p_b)^{N-i}, \quad (2)$$

where p_b is the probability of bit disagreement for the authentication keys (k_0, k_1) chosen from AS ***a*** or ***b:***

$p_b = 1-(1-p_m)^{2m}$.

Taking into account that the probability of the single block successful deception given unknown strings $\boldsymbol{u_i}$, $\boldsymbol{w_i}$ is equivalent to the probability of guessing the authenticator, i.e. to $1/2^v$. Hence, we get the probability of successful impersonate attack:

$$P_i(\Delta) = \sum_{i=0}^{\Delta} \binom{N}{i} (\frac{1}{2^v})^{(N-i)} (1-\frac{1}{2^v})^i \ . \quad (3)$$

As far as the reflection attack it is possible to note that A substitutes for authentication of reflected blocks another authenticating keys are requested. Therefore, we can let that $P_{ref} = P_i$ (see above).

In order to estimate the probability of the successful substitution attack, let us present this attack as a consecutive occurrence of the two events:

- creation of false DH-value, that differs from the valid one in *D* blocks of the length *m* each (we denote the probability of this event by $P_g(D)$,
- occurrence of a deception event by creation of authenticators for *D* blocks, that differ in false DH-values from blocks of valid DH-values. (denote the corresponding probability by $P_r(D)$.

Then, the probability of DH-value substitution by the false one can be expressed as the product of two probabilities

$P_s = P_g(D)P_r(D)$.

It is worth to note that the parameter *D* is controlled by eavesdropper and, hence, from key sharing system designer's point of view, it is necessary to provide the requirements for probability for any *D* -value substitution.

Obviously, the less is the number of blocks *D* which are different *X* and *X'*, the easy for eavesdropper to perform an attack «a man-in-the-middle». It is necessary to remark that eavesdropper cannot select the value *X'* itself. In fact, he (or she) selects *x'* initially and then, finds the value $X' = g^{x'} \bmod p$. If *x'* had taken randomly on the set of integers (0 , *p-1)*, then the value of *X'* would have been also random on the set (0 , *p-1)*. For the large modulo *p* (let's say $p \approx 2^{256}$) a mapping of $x' \Leftrightarrow X'$ requires infeasible number of computations. Therefore, a reasonable strategy of eavesdropper could be take a truly random choice of *x'* which is equivalent to a random choice of integer *X'* that differs from the valid integer in *D* blocks.

We can let the number *D* be a random value with the probability

$$P_g(D) = \binom{N}{D} \left(\frac{1}{2^m}\right)^{N-D} \left(1-\frac{1}{2^m}\right)^D. \quad (4)$$

(We note that the proof of (4) can be based on the model with falling out of equal results during a tossing of two dies with 2^m sides each.)

Next E creates authenticators for these *D* blocks. The upper

bound of the false deception DH-values which differ from the valid ones in D blocks given threshold Δ will be the following:

$$P_r(D,\Delta) \le \sum_{i=0}^{\Delta} \binom{D}{i} (\frac{1}{2^v})^{(D-i)} (1-\frac{1}{2^v})^i \sum_{j=0}^{t} \binom{N-D}{j} p_b^j (1-p_b)^{(N-D-j)}, \quad (5)$$

where $t = \begin{cases} N-D, if\ \Delta - i \ge N-D, \\ \Delta - i, if\ \Delta - i < N-D \end{cases}$.

The first sum in (5) describes the probability of occurrence i ($0 \le i \le \Delta$) of false authenticators that are not detected. The second sum is the probability of disagreement j $(0 \le j \le t)$ from N-D authenticators of original message that have been sent by Eve without a change. This disagreement is a consequence of disagreement among authenticating keys ***a*** and ***b.*** (It is worth to note that inequality in (5) appears owing the fact under the checking of D authenticators that were chosen by Eve randomly. The errors in authenticating sequences were not considered. Hence, these probabilities can be neglected).

Because the parameter D is controlled by E and hence, it is necessary to provide the requested value of $P_S(D)$ for any D. Thus, eventually we have to define the substitution probability for any strategy of attack as follows

$$P_s' = \max_D P_s(D).$$

V. Examples of the Parameters Estimation for Authentication Systems

Let us assume that we need to authenticate DH-values of the length n_0=256 bits which is according to many encryption standards. As it was mentioned before we fix the BER between AS ***a*** and ***b*** to be equal about 0.05. We are interested in the estimation of the probabilities P_f, P_i, P_{ref} and P_s. For some definiteness we let $\tilde{P}_f = \tilde{P}_d = 10^{-6}$ that can be considered as the appropriated values in practice. In Fig.4 the curves $P_f = g(\Delta, p_m)$ calculated by (2) for different block lengths m and different BER p_m against threshold values Δ are presented. We can see from Fig.4 that the probability P_f is decreasing for all block length m and for all BER values p_m with an increasing of threshold values Δ. The probability P_f is increasing with increasing of BER p_m that is obviously because a disagreement between authenticating sequences ***a*** and ***b*** results in an increasing of the incorrect receiving of authenticators. But such behavior results in an increasing of the probability P_f. Hence, if we want to keep P_f the same as before we have to increase the threshold value Δ.

That means, by a selection of the threshold Δ as block length m the one can provide the value $\tilde{P}_f < 10^{-6}$ as small as required, even for a significant probability up to p_m equal to 0.1.

In Fig.5 the substitution probabilities $P_r(\Delta, m, D)$ of the valid DH-values calculated by (5) with false values depending from the threshold Δ, block lengths m=2,4,8 and a pair of values D (the number of disagreement blocks between valid and false DH-values) at $p_m = 0.05$ are shown. It is worth to note that the first D corresponds to the case when $D = M\{D\}$, where $M\{D\}$ is an expectation of the random value D under a random generating of the false DH-value. The second D is 4-6 blocks less than the average one. Also, it is assumed that $v = m$, i.e. the authenticator lengths are equal to the lengths of the authenticating blocks. We consider in the sequel how the authenticator length affects the substitution probability.

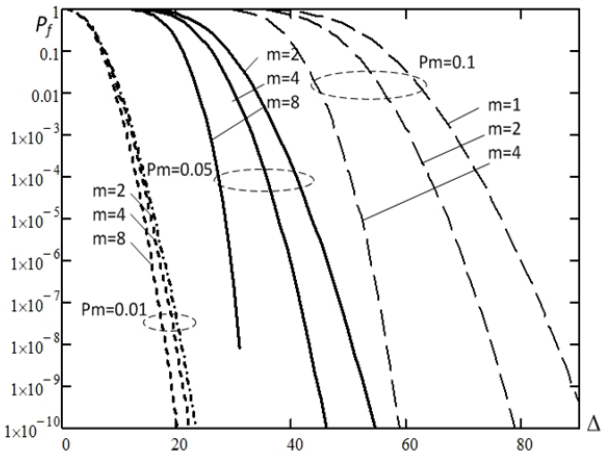

Fig.4. The dependence of the DH-value false rejection probability P_f against threshold values Δ under different block length m and the probability ***a*** and ***b*** disagreement- p_m

For the comparison purposes the dependences $P_f(\Delta, m)$ similar to presented in Fig 4 are shown in Fig.5.

We note that a choice of D which is equal to an average of $M\{D\}$ (e.g. $M\{D\}$=128 for m=1; 96 for m=2; 60 for m=4; 32 for m=8), corresponds to the cases when the DH-value is false. It is created by random sampling of the sequence X' from the set of sequences with the length n_0. At the second case an attacker can improve his (her) choice by selecting X' with the number of distinctions D against X less than the average one.

We can see that the probability P_r is rapidly increasing against Δ given the fixed value m. An increasing of the block length m increases P_r also. Decreasing the number of the distinct blocks D in the deception message, on the contrary, results in increasing of the successful substitution attacks by replacing DH-value with the false one.

A joint consideration of the dependences P_r and P_f shows that they are changing in the opposite directions depending on Δ.

Realization of the both conditions $P_f \le \tilde{P}_f$ and $P_r \le \tilde{P}_d$ simultaneously occurs possible only if some given parameters Δ, m, D have been selected before. For example if m=4 and

Δ=40, *D*=60, we get $P_f = P_r = 10^{-8}$ or if *m*=2 and Δ=46, *D*=96, we get $P_f = P_r = 10^{-6}$. However if *m*=8, then there is no Δ for which $P_f = P_r \le 10^{-6}$.

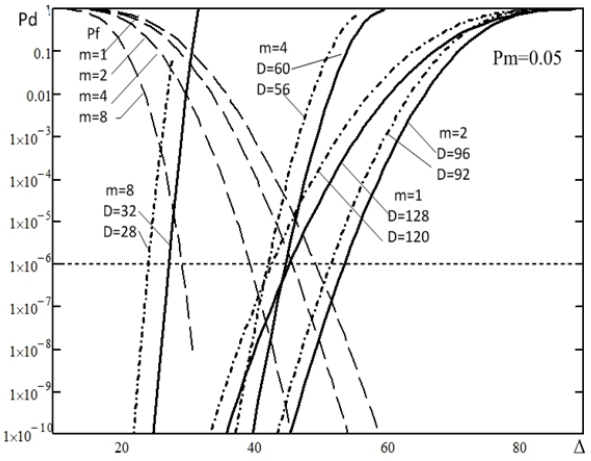

Fig. 5. The dependence of the DH-value substitution probability P_r against threshold values Δ for different authenticating block length (*m*=2,4,8) and a pair of values *D* (distinctions between valid and false DH-values)

In order to answer to the question about a possibility to select optimal parameters *m* and *v* for which the conditions $P_f \le \tilde{P}_f$, $P_r \le \tilde{P}_d$, $\tilde{P}_f = \tilde{P}_d = 10^{-6}$ are fulfilled together, let us plot a dependence of the probabilities: P_g - the probability of creation by an attack false DH-values that differ from valid ones in *D* blocks; P_r - the probability of DH-value substitution by false value that differs from valid ones in D blocks; $P_s = P_g \cdot P_r$ the probability of substitution for block length *m* =1,2,4,8 (See Fig. 6). The threshold values Δ were selected in order every *m* to fulfill the condition $\tilde{P}_f \approx 10^{-6}$ (Δ=50, 46, 40, 30 for *m*=1, 2, 4, 8 respectively, see Fig.4).

We can see from Fig.6 that the probability P_r decreases with a growing of *D*. It is naturally because for a large difference between valid and false DH-values it is harder to pass an authentication. We note that the dependence of P_g on *D* is determined by binominal coefficient distribution in equation (4) and is similar to the substitution probability $P_s = P_g \cdot P_r$. As far as we can see from Fig. 6 there exist values *D* for which the requirement $P_s = 10^{-6}$ is not realized with the block length *m*=1 and *m*=8. On the contrary, for *m*=2 and *m*=4 for any *D* probability $P_s = 10^{-8} < \tilde{P}_d = 10^{-6}$. This says that any attempts of attacker to pick up an appropriated false DH-value in terms of choice *D* would be useless.

In Fig. 7 the impersonation probability $P_i(\Delta, m)$ against threshold values Δ in line with equation (3) for different block lengths v (solid lines) are given. The substitution probabilities P_r according to the relation (5) under $D = M\{D\}$ (dotted lines) are presented as well. By comparing these curves one can make a conclusion that the impersonating probability P_i is less than the substitution probability P_r. The probability of successful attack is $P_{ref} = P_i$ as it was mentioned above.

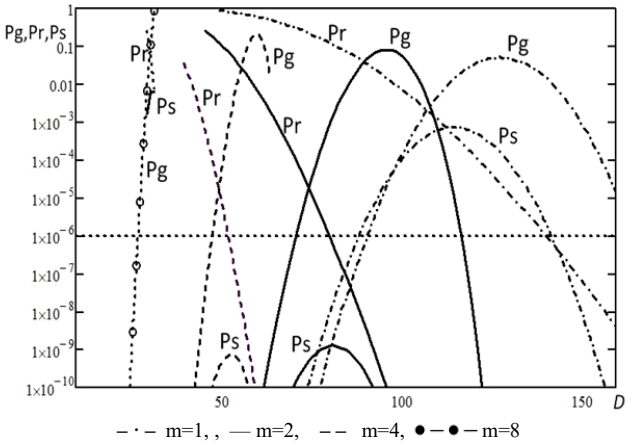

Fig. 6. The probability of creation by an attack false DH-value that differs from valid one in *D* blocks P_g -; the probability of DH-value substitution by false value that differs from valid one in D blocks - P_r; the probability of substitution - $P_s = P_g \cdot P_r$ for different block lengths *m* =1,2,4,8

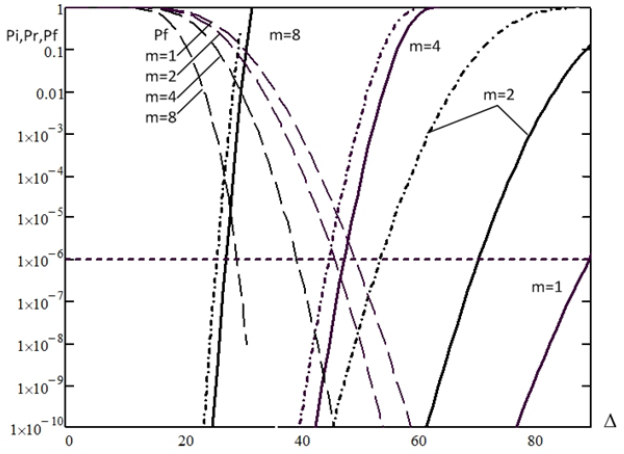

Fig.7. The impersonation probability P_i and the substitution probability P_r against threshold values Δ for different authenticating block lengths

We believed until now that authenticator length is equal to the length of authenticating block, e.g. $m = v$. Let us investigate now how a choice of authentication length affects on the main characteristics of the authentication procedure.

It follows from relation (1), (4) that P_f and P_g do not depend on *v*. Hence, let us investigate how authentication

length affects on P_r. In Fig. 8 the dependences $P_r(\Delta,m,v)$ against Δ for m =2 и 4 and all values $v \le m$ are presented. For the comparison purposes the dependences of $P_f(\Delta,m)$ on the same values m are given by the same Figure also.

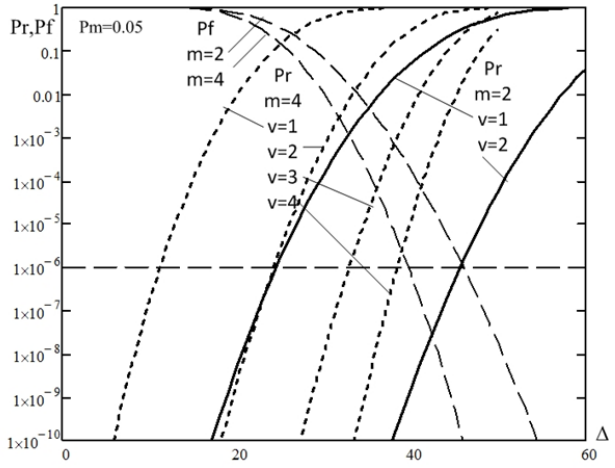

Fig. 8. Curves $P_r(\Delta,m)$, $P_f(D,m)$ for m=2,4 and different authenticator lengths against threshold values Δ.

We can see from Fig.8 that the probability of substitution decreases with a growing of authenticator length.

Let us denote $\Delta_{min} = min\Delta$ for that $P_f \le \tilde{P}_f$ and given values *(m,v)*.

In Table I the probabilities P_f, P_i, P_s', P_d for some parameters *m,v* under a selection on threshold values $\Delta = \Delta_{min}$ given $P_f \le 10^{-6}$ are presented. Realization of the requirements $(P_i, P_s', P_d) \le 10^{-6}$ is marked by the symbol (+), whereas non-realization of them by symbol (-).

We can see from Table I that requirements $P_i \le 10^{-6}$, $P_d \le 10^{-6}$ are realized only for the two pairs of parameters *(m,v):* (4,4) and (2,2). A decreasing of summarized authenticator length *W* (for all partial blocks of authenticators) is possible in m/v times if *v<m,* given the requirements $P_f \le \tilde{P}_f$. $P_r \le \tilde{P}_d$ are realized. But in the example above a decreasing of authenticator length is impossible and therefore summarized authenticator length is always equal to the length DH-value W=256 bits.

Thus, we can formulate the following deduction. Authenticator design is based on the Wegman-Carter construction and authenticating strings ***a*** and ***b*** distributed in advance, allowing one to provide sufficiently high requirements on the deception probability of false DH-values and false alarm deception probability $\tilde{P}_f = \tilde{P}_d = 10^{-6}$ under the condition relatively large disagreement probability between AS equal to p_m=0.05.

TABLE I. THE PROBABILITIES OF FALSE REJECTION P_f, SUBSTITUTION P_s', IMPERSONATION P_i AND DECEPTION P_d OF DH-VALUES FOR DIFFERENT PAIRS *(m,v)*

(m,v)	P_f	P_s'	P_i	$P_d = \max(P_s', P_i)$
(1,1)	7.1×10^{-7} (+)	6.2×10^{-6} (-)	5.7×10^{-24} (+)	6.2×10^{-6} (-)
(2,2)	1×10^{-6} (+)	8.1×10^{-10} (+)	1.4×10^{-20} (+)	8.1×10^{-10} (+)
(2,1)	1×10^{-6} (+)	7.4×10^{-3} (-)	9.3×10^{-4} (-)	7.4×10^{-3} (-)
(4,4)	6.5×10^{-7} (+)	6.8×10^{-10} (+)	2.7×10^{-13} (+)	6.8×10^{-10} (+)
(4,3)	6.5×10^{-7} (+)	3.8×10^{-6} (-)	3.3×10^{-7} (+)	3.8×10^{-6} (-)
(4,2)	6.5×10^{-7} (+)	1×10^{-2} (-)	1.8×10^{-2} (-)	1×10^{-2} (-)
(4,1)	6.5×10^{-7} (+)	1.4×10^{-1} (-)	9.8×10^{-1} (-)	1.4×10^{-1} (-)

It is very important to select authenticating block length *m* and authenticator length *v* correctly.

The key-consumption for this method authenticating DH-value of the length n_0=256 bits is equal to $L = 2mN = 512$ bits.

It is worth to note that in [16] there was a solving the of similar problem with authentication length 256 bits that was based on the use of error correction codes (FEC) mentioned in [17,18] and authenticating strings distributed by the legitimate users in advance. In that paper the disagreement probability was taken as p_m=0.01 and the length of authenticating sequences was chosen as 768 bit given the probabilities of errors are $P_d \le 10^{-6}$, $P_f \le 10^{-6}$. But if p_m=0.05 then the final probabilities $P_d \le 10^{-6}$, $P_f \le 10^{-6}$ cannot be provided for any authentication system parameters. Thus, we can see that the authentication system proposed in the current paper seems to be superior to the system considered in [16].

VI. CONCLUSION

The widespread use of different mobile wireless devices (like smartphones, notebooks, tablets, etc) poses the question about a cryptographic protection of the messages transmitting or saving by these devices. But this problem requires to provision them with the secret keys executing by means of cryptographic algorithms. Under the condition of possible interception and active intervention by unauthorized persons, it is required to provision with so called authenticated keys by ordinary users in the Internet.

In the current paper the problem of key distributing using Diffie-Hellman protocol is solved but without assistance of any authority. But in order to provide authentication of the shared key, namely a protection against so called a man-in-the-middle attack, an approach to share initially random authenticating key strings was proposed. This procedure can be done by different methods but the simplest one for mobile units is so called pairing process during the previous face to face meeting. Unfortunately, such a solution has one

significant defect, namely a presence of slight disagreement in the strings shared by a pair of users. This disagreement can be modeled by binary symmetric channel without a memory given by BER p_m. Developing of such approach jointly with the central idea of unconditionally secure Wegman-Carter authentication algorithm was the main goal of our investigation. To be more precisely, we divide DH-values on the blocks of equal lengths m and then, apply the hashing procedure to them chosen from strongly universal$_2$ class and in line with shared authentication keys. Eventually the number of blocks passing the authentication is compared with some threshold value given in advance and if it was exceeded then the shared DH-values are accepted, otherwise are rejected (the last case requires a repetition of such procedure one or more time later). The main result of our paper is the proof of formulas which allow to estimate the following probabilities:

- P_f is the probability of false rejection DH-value under absence of attack;
- P_d is the probability of false DH-value deception.

It is worth to note that the approach how attacker can create false DH-values with given number of blocks different to valid ones is proposed in the proof of the probability P_d. In addition, we proposed the methods of parameter optimization (the number of blocks and full authenticator's length).

An example was presented for DH-value of the length equal to 256 bits and it was shown that the probabilities of false rejection and false deception can be provided sufficiently small and hence practically acceptable.

In the future, authors hope to consider other methods of authenticating block design that could improve an efficiency of authentication procedure for the Diffie-Hellman key sharing protocol.

REFERANCES

[1] W. Diffie, M. Hellman, "New Directions in Cryptography", *IEEE Trans. Inf. Theory,* vol. 22, no. 6, 1976, pp. 644-654.

[2] A.J. Menezes. *Handbook of Applied Cryptography.* New-York, London, Tokio: CRC Press,1977.

[3] S. Mirzadeh, H. Cruickshan, R. Tafazolli, "Secure Device Pairing: A Survey". *IEEE Communications Surveys & Tutorials*, vol. 16, 2014, pp. 17– 40.

[4] K. Zeng, "Physical Layer Key Generation in Wireless Networks. Challenges and Opportunities ", *IEEE Commun. Magazin*, vol. 53, no. 4, 2015, pp. 20-27.

[5] J. Zhang, T.Q. Duong, Marshall, R. Woods, "Key Generation from Wireless Channels: a Review", *IEEE Access,* vol. 4, 2016, pp. 614-626.

[6] T., Jokela, M.K., Chong, A., Lucero, H. Gellersen, "Connecting devices for collaborative interactions". 22(4), 3943 (2015). doi:10.1145/2776887.

[7] R. Jin, L. Shi, K. Zeng, A. Pande, P. Mohapatra, "MagPairing: Pairing Smartphones in Close Proximity Using Magnetometer", *IEEE Transactions on Information Forensics and Security,* no. 6, 2016, pp. 1304–1319.

[8] N. Saxena et al. "Secure Device Pairing Based on a Visual Channel", *Security and Privacy*, IEEE Symposium, 2006, pp.57-68.

[9] R. Prasad, N. Saxena, "Efficient Device Pairing Using Human-Comparablel Synchronized Audiovisual Patterns", *Conf. of Applied cryptography and Network Security (ACNS) 2008*. LNCS Springer, Heidelber, vol. 5037, 2008, pp. 328-345.

[10] M. T. Goodrich, M. Sirivianos, J. Solis, C. Soriente, G. Tsudik and E. Uzun, "Using Audio in Secure Device Pairing", *International Journal of Security and Networks,* vol. 4, no. 1, 2009, pp. 57–68.

[11] C. Soriente, G. Tsudik, E. Uzun, "HAPADEP: Human-Assisted Pure Audio Device Pairing", *ISC,* 2008, pp. 385–400.

[12] R. Mayrhofer, H. Gellersen, "Shake Well Before Use: Intuitive and Secure Pairing of Mobile Devices". *IEEE Transactions on Mobile Computing,* vol. 8, no. 6, 2009, pp. 792–806.

[13] C. Soriente, G. Tsudik, E. Uzun, "BEDA: Button-Enabled Device Association". *International Workshop on Security for Spontaneous Interaction (IWSSI),* 2007, pp.443-449.

[14] A. Kumar, N. Saxena, G. Tsudik, E. Uzun, "Caveat emptor: A Comparative Study of Secure Device Pairing Methods", *IEEE International Conference on. IEEE*, 2009, pp. 1–10.

[15] V.Yakovlev, O. Ol'hovoj, V. Korpusov, "Magnetometer based random number sensor analysis", *VIII Int. Conf. of advanced Infotelecommunication (ICAIT-2018), Collected papers.* SPb.: 2018, pp. 488-493. (in Russ.).

[16] V. A. Yakovlev, "Authentication of keys that are distributed by the Diffie-Hellman method for mobile devices based on authentication codes and magnetometric data" *SPIIRAS Proc.,* issue 18, N 3, 2019, pp.705-740. (in Russ.)

[17] U. Maurer, "Information-Theoretically Secure Secret-Key Agreement by not Authenticated Public Discussion" *Lecture Notes in Computer Science*, 1233, 1997. pp. 209-223.

[18] V.Korzhik, V. Yakovlev, G, Morales-Luna, R. Chesnokov, "Perfomance Evaluation of Keyless Authentication Based on Noisy Channel", *MMM-ACNC 2007.* CCIS 2007, no.1. pp.115-126.

[19] M. Wegman, L. Carter, "New Hash Functions and their Use in Authentication and Set Equality", *Journal of Computer and System Sciences,* vol. 22, 1981, pp. 265-279.