Vulnerability of the Key Sharing Protocol Executing over the Noiseless Public Channels with Feedback

Valery Korzhik, Viktor Yakovlev
korzhikvalery@gmail.com, viyakovlev4@gmail.com

Vladimir Starostin, Alexey Lapshin, Aleksei Zhuvikin
star.vs.47@gmail.com, SCodeC.LA@gmail.com,
mail@zhuvikin.com.

Abstract — **It has been proven that several recently published protocols for exchanging by keys over noiseless channels of the same authors as in the current paper, have real vulnerability to eavesdropping rooted in the attacker's receiver optimization procedure. Moreover, we have proved that binary bits and real-valued numbers exchange protocols have zero secret capacity and are therefore unpromising in their applications. Protocols of exchanging by real-valued vectors and by matrices have nonzero secret capacity under the condition of hard decoding by eavesdroppers. The use of optimal soft decoding results in a compromise of such protocols. Thus, a problem is still open about an existence or non-existence for reliable key sharing protocols executed over noiseless public channels.**

I. Introduction

It is well known that the use of strong ciphers is the main way to ensure information security both when storing data and when transmitting it through public channels accessible to eavesdropping. But every strong cipher based on symmetric (single-key) standards (like 3DES, AES etc.) requires a prior key distribution to their correspondents. Although after the real cryptographic revolution (1978), thanks to the invention of the so-called public key cryptosystems by M. Hellman and W. Diffie [1], the problem seemed to be solved, because then legitimate users can keep the secret decryption key only. But such approach has several problems. First of all, it requires for legitimate users to collaborate with third party (certification centers of public keys) in order to avoid impersonalization's attack. Secondly, the most of popular public key cryptosystem (like El-Gamal, RSA, Rabin etc.) can be broken if so-called quantum computers [2] be put into practice which is still in question (See [3] for detail). However, some cryptographic algorithms (for example McEliece or based on digital lattice) cannot be broken even on quantum computers but they require more complex hardware or they results in more slowly software. Therefore "old fashioned" methods of key sharing over regular channels between users are still in demand. Of course, they must be resistant to eavesdropping attacks.

At the end of the last century, such a strange (at first glance) term as *keyless cryptography* was introduced in the field of applied cryptography. It has two characteristic features. In one case, it is assumed that the key is not actually needed at all, since security can be provided through certain properties of the channel. In the second one, a key is needed, but it can be secure distributed over the channel before due to the fact that the natural properties of the channel differ for legitimate and illegitimate users. In such situation, one usually says that we have *physical layer security* [4]. The following properties can be considered as natural ones of a channel: noise, multi ray wave propagation, smart antennas, presence of feedback, quantum channels (both over space and over optical fiber). Papers [5,6] are devoted to the first case. Example of information security based on noisy channels is presented also in [7]. Multi ray channels was investigated in [8]. The smart antenna is used as it is demonstrated in [9]. Quantum channels are implemented in the so-called *quantum cryptography*, which has been intensively developing in recent years, both theoretically and practically [10].

Unfortunately, all approaches mentioned above based on physical layer security have significant drawbacks. Thus, the noise power level in the eavesdropping channel can greatly interfere with the correct prediction of information leakage. The same situation occurs with parameters in multi-ray channels. The use of smart antennas and quantum channels, requires quite complex and expensive devices. In this case, it seems easiest to distribute cryptographic keys using noiseless public channels with constant parameters like Internet. Such channels are very popular and does not require any additional devices or any assistance from third parties. This is especially convenient for ordinary individual users, since such approach has only one constraint, namely feedback between users. By the way, it is worth noting that such feedback may not be needed immediately. Namely, such scenario was investigated in the series of our paper published over the last four years [11-13]. The main difference between the models of these papers lies in the prime key sharing protocols (users exchange bits, real numbers, vectors and matrices). Unfortunately, we have found later that some of them have "holes" for information leakage.

The current paper is devoted to specification of this "holes" and correct formulation of the problem, which is very important for ensuring information security.

The paper is structured as follows: charter II is devoted to brief description of two protocols (bits, real numbers and vector exchange). We show that for the first two cases the secret capacity equals to zero. For vector basic protocol it is only very likely too. In charter III matrix exchange protocol is investigated and the hard key sharing protocol (KSP) is shown to work well with this scenario. However, for the soft decoding by eavesdropper, KSP can be broken. Charter IV summarized the main results and put the problem for future investigations.

II. Breaking of KSP with Exchanging of Bits, Real Numbers and Vectors

2.1. Let's start with a basic protocol that uses bitwise exchange. This protocol described in the paper [13] and presented in Fig 1 below.

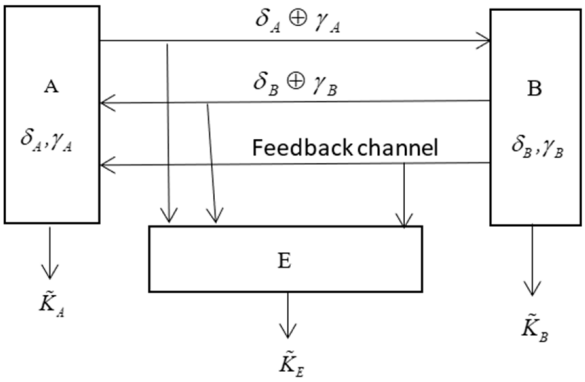

Fig. 1. Basic protocol with exchange by random bits between legitimate users A and B over public noiseless channel and in a presence of eavesdropper

For brevity, we will abbreviate the main protocol as BEC (bit exchange channel).

We assume (as in [13]) that $\delta_A, \delta_B, \gamma_A, \gamma_B \in \{0,1\}$; $P(\delta_A = 1) = P(\delta_B = 1) = 0.5; P(\gamma_A = 1) = P(\gamma_B = 1) = p$ and all random bits are mutual independent (in other words, we can call the bits γ_A, γ_B by random binary noise).

After exchange by sequences of bits both A and B be able to form bits of primary keys:

$$\tilde{K}_A = \delta_A \oplus \delta_B \oplus \gamma_B, \tilde{K}_B = \delta_B \oplus \delta_A \oplus \gamma_A, \quad (1)$$

where "$\oplus$" is bitwise addition modulo two.

Eavesdropper E should also form primary key as follows:

$$\tilde{K}_E = \delta_A \oplus \gamma_A \oplus \delta_B \oplus \gamma_B. \quad (2)$$

Then additive noises between A and B, A and E can be found, respectively, as:

$$\begin{aligned} \varepsilon_{AB} &= \tilde{K}_A \oplus \tilde{K}_B = \delta_A \oplus \delta_B \oplus \gamma_B \oplus \delta_B \oplus \delta_A \oplus \delta_A \oplus \gamma_A = \gamma_B \oplus \gamma_A \\ \varepsilon_{AE} &= \tilde{K}_A \oplus \tilde{K}_E = \delta_A \oplus \delta_B \oplus \gamma_B \oplus \delta_A \oplus \gamma_A \oplus \delta_B \oplus \gamma_B = \gamma_B \end{aligned} \quad (3)$$

In order to provide a good statistic for final key, legal users A and B have to exploit hardware sequence key γ generator and additional final key distribution scheme (similar to scheme shown in Fig. 2 [13] and presented here:

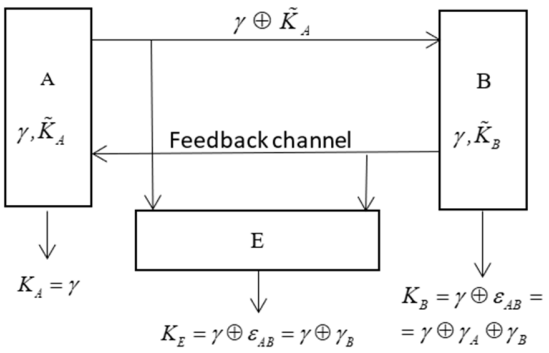

Fig. 2. Additional final key distribution scheme

After a completion of protocol by Fig 2, legitimate user B receives the final key γ with additive noise $\gamma_A \oplus \gamma_B$, whereas E gets an additive noise γ_B. Since it follows that the bit error rate (BER) in the main channel (A→B) can be greater than that in the eavesdropping channel (A→E), another sub-protocol, named in [13] "*predominant improvement of the main channel*" (PIMC), was used. The goal of this protocol was to provide such channel transformation to diverse BER's between main and wire-tap channels.

It was proved by both theoretically and by simulation in [13], that such problem can be solved after several iterations of PIMC (See Tables V and VI in [13]).

We remember that IPMC protocol is determined as:

- Legitimate user A generates random bit $\gamma = \{0,1\}$, $p(\gamma = 0) = p(\gamma = 0) = 1/2$.
- He forms the block $\bar{u} = \bar{\gamma} \oplus \bar{\tilde{K}}_A$, where $\bar{\gamma}$ is the vector consisting of s-fold repetitions of bit γ, $\bar{\tilde{K}}_A = \tilde{K}_{A1}, \tilde{K}_{A2}, ..., \tilde{K}_{As}$
- User A sends the block $\bar{u}$ to user B. The last one receives block $\bar{u}$ and computes block $\bar{w} = \bar{u} \oplus \bar{\tilde{K}}_B = \bar{\gamma} \oplus \bar{\tilde{K}}_A \oplus \bar{\tilde{K}}_B$,

  where $\bar{\tilde{K}}_B = \tilde{K}_{B1}, \tilde{K}_{B2}, ..., \tilde{K}_{Bs}$
- User B decodes $\bar{w} \to \tilde{\gamma}$, $\tilde{\gamma} = (0,1)$ in line with relation:

$$\tilde{\gamma} = \begin{cases} 0, \textit{ if } \bar{w} = 0^s, \\ 1, \textit{ if } \bar{w} = 1^s, \\ *, \textit{ otherwise} \end{cases}$$

- If B erases this s-block he informs A about such event using feedback channel (send symbol*). Eavesdropper E is able to intercept all erasing signals without errors.

But unfortunately, after additional investigations we have established that multi-iterative approach of PIMC protocol is not optimal from the point of view of the eavesdropper. Execution of optimal decoding results in a breaking of BEC protocol.

Let's now prove that once the basic BEC protocol works, no other protocol can solve our problem of providing reliable and secure key distribution between legitimate users in the presence of an eavesdropper.

For this purpose let us transform scheme presented in Fig 2 to its equivalent scheme presented in Fig 3.

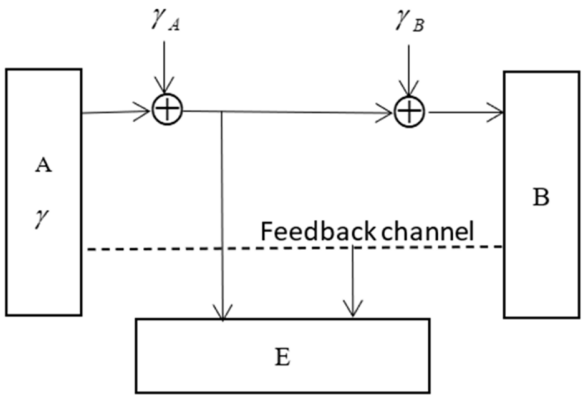

Fig. 3. Key distribution scheme that is equivalent to the scheme presented in Fig. 2

On the other hand, we can see from Fig. 3 that channel presented in that figure is namely *wire-tap channel with feedback and degradation of the main channel* (in line with terminology given in [14]). But for such model has been proven strictly that its secret capacity is zero.(Let's remember that in line with definition given in [14], secret capacity Cs is main channel capacity providing arbitrarily small leakage to eavesdropper over wire-tap channel.) This means that there is no reliable KSP for noiseless channels with feedback, at least for BEC model.

2.2. Let us consider now basic protocol using exchanging by real numbers. This protocol was described in the paper [12] and presented in Fig. 4 below.

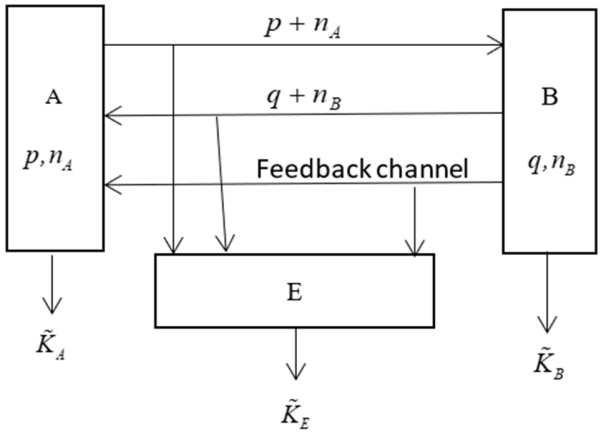

Fig. 4. Basic protocol with exchange by random real numbers between legitimate users A and B over public noiseless channel and with a presence of eavesdropper

Let us denote such scheme for a simplicity by abbreviation RNEC (real numbers exchange channel). We assume that all random real values p, q, n_A, n_B are Gaussian ones, mutual independent, with zero mean and variances $Var(p) = Var(q) = 1$, $Var(n_A) = Var(n_B) = \sigma^2$. Thus, the values n_A, n_B form Gaussian white noise. After exchange by real-valued sequences both A and B be able to form binary primary keys:

$$\tilde{K}_A = rect\left(p\left(q+n_B\right)\right), \tilde{K}_B = rect\left(q\left(p+n_A\right)\right), \tag{4}$$

where "+" is ordinary arithmetic addition,

$$rect(x) = \begin{cases} 0, x \geq 0 \\ 1, x < 0 \end{cases}.$$

Eavesdropper E should also to form primary key bit as follows:

$$\tilde{K}_E = rect\left(\left(p+n_A\right)\left(q+n_B\right)\right). \tag{5}$$

Using easy provable equality

$$rect\left(a \cdot b\right) = rect\left(a\right) \oplus rect\left(b\right), \tag{6}$$

we can replace scheme shown in Fig. 4 to the scheme shown in Fig. 5.

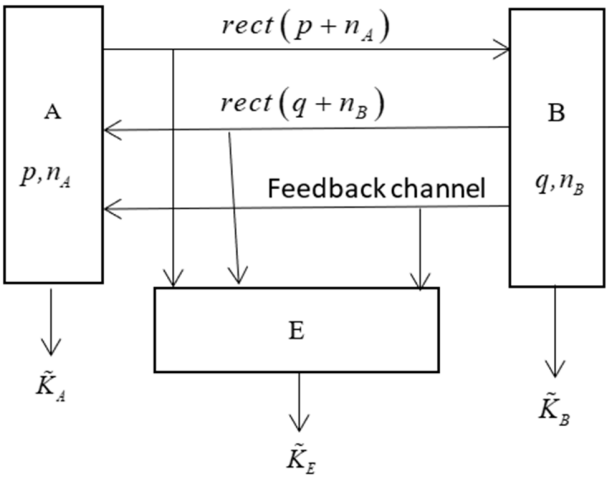

Fig. 5. Scheme equivalent to the basic protocol shown in Fig. 4.

Then the primary key bits obtained from the scheme shown in Fig. 5 are:

$$\begin{aligned} \tilde{K}_B &= rect\left(p+n_A\right) \oplus rect\left(q\right), \\ \tilde{K}_A &= rect\left(p\right) \oplus rect\left(q+n_B\right), \\ \tilde{K}_E &= rect\left(p+n_A\right) \oplus rect\left(q+n_B\right). \end{aligned} \tag{7}$$

It is easy to find noises between A, B and A, E:

$$\begin{aligned} \varepsilon_{AB} = \tilde{K}_A \oplus \tilde{K}_B = rect\left(p\right) \oplus rect\left(q+n_B\right) \oplus \\ \oplus rect\left(p+n_A\right) \oplus rect\left(q\right) \\ \varepsilon_{AE} = \tilde{K}_A \oplus \tilde{K}_E = rect\left(p\right) \oplus rect\left(q+n_B\right) \oplus \\ \oplus rect\left(p+n_A\right) \oplus rect\left(q+n_B\right) = rect\left(p\right) \oplus rect\left(p+n_A\right) \end{aligned} \tag{8}$$

We can see from relations (7) and (8) that scheme for an execution of PIMC protocol after basic protocol in this case, is similar to scheme, presented in Fig. 3, if to replace in the last one γ_B to $rect\left(p\right) \oplus rect\left(p+n_A\right)$ and γ_A to $rect\left(q\right) \oplus rect\left(q+n_B\right)$.

But this means that we obtain wire-tap channel with feedback model and with a degradation of the main channel.

Hence, referring to the paper [14], we get $C_S = 0$ and execution of such KSP is useless.

2.3. Let us consider protocol based on the use of basic protocol with exchange by n-dimension vectors.

The scheme of such basic protocol is shown in Fig. 6.

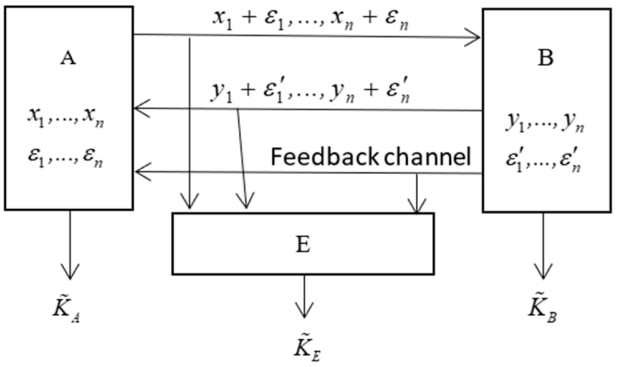

Fig. 6. Basic protocol with exchange by n-dimension vectors with real valued coordinates, between legitimate users A and B over public noiseless channel and in a presence of eavesdropper E

Let us denote this basic protocol (for brevity) by CGVE (channel with Gaussian vector exchange). We assume that all random real numbers $x_1,\ldots,x_n,\varepsilon_1,\ldots,\varepsilon_n,\ y_1,\ldots,y_n,\varepsilon_1',\ldots,\varepsilon_n'$ are Gaussian, mutually independent, with zero mean and with variances

$$Var(x_i)=Var(y_i)=1,$$
$$Var(\varepsilon_i)=Var(\varepsilon_i')=\sigma^2<1,$$

After a completion of CGVE protocol, both legitimate users A and B and eavesdropper E be able to form one bit of primary key as follows:

$$\tilde{K}_A=rect\left(\sum_{i=1}^{n}x_i(y_i+\varepsilon_i')\right),\tilde{K}_B=rect\left(\sum_{i=1}^{n}y_i(x_i+\varepsilon_i)\right), \quad (9)$$

$$\tilde{K}_E=rect\left(\sum_{i=1}^{n}(x_i+\varepsilon_i)(y_i+\varepsilon_i')\right). \quad (10)$$

Let us find additive continuous noises between $\tilde{K}_A$ and $\tilde{K}_B$ as well as between $\tilde{K}_A$ and $\tilde{K}_E$:

$$\varepsilon_{AB}=\tilde{K}_A-\tilde{K}_B=\sum_{i=1}^{n}(y_ix_i+\varepsilon_i'x_i-x_iy_i-\varepsilon_iy_i)= \quad (11)$$
$$=\sum_{i=1}^{n}(\varepsilon_i'x_i-\varepsilon_iy_i)$$

$$\varepsilon_{AE}=\tilde{K}_A-\tilde{K}_E=\sum_{i=1}^{n}(y_ix_i+\varepsilon_i'x_i-x_iy_i-\varepsilon_iy_i-x_i\varepsilon_i'-\varepsilon_i\varepsilon_i')= \quad (12)$$
$$=\sum_{i=1}^{n}(-\varepsilon_iy_i-\varepsilon_i\varepsilon')=\sum_{i=1}^{n}(-\varepsilon_i(y_i+\varepsilon_i'))$$

Let us estimate noise powers ε_{AB} and ε_{AB}

$$Var(\varepsilon_{AB})=2n\sigma^2,Var(\varepsilon_{AE})=n(\sigma^2+\sigma^4).$$

Since $\sigma^4<\sigma^2$ if $\sigma^2<1$,then $Var(\varepsilon_{AB})>Var(\varepsilon_{AE})$. This leads to an equality $P_m>P_e$, where P_m is *BER* in the main channel and P_e is *BER* in the wire-tap channel.

Thus PIMC protocol is unable to diverse P_m and P_e as it was noted in Section [12].

Moreover, if we neglect by product noise $\varepsilon_i\cdot\varepsilon_i'$, then protocol, which is presented in Fig. 6, can be considered as a degradation of the main channel.

Therefore, although it is not proved in [14] for continuous Gaussian model, but *very likely,* that for such scenario C_S=0 also and hence key distribution problem cannot be solved for primary protocol shown in Fig. 6.

III. INVESTIGATION OF THE BASIC MATRIX EXCHANGE

IV. PROTOCOL

Let us consider finally protocol based on channel with square matrices exchange (SME) investigated in [11] (but with slightly different notations) and showed below in Fig. 7.

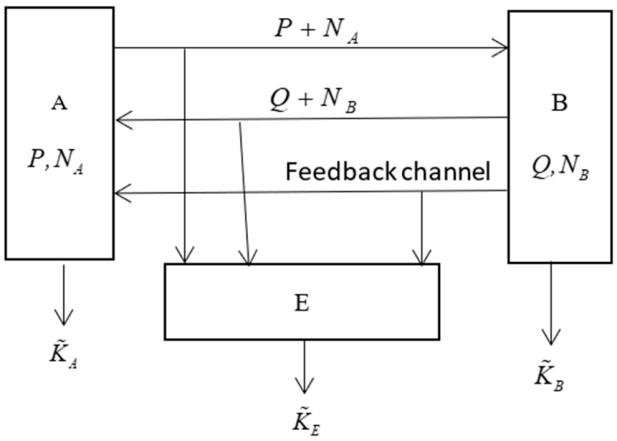

Fig. 7. Basic protocol with exchanging by square matrices between legitimate users A and B over public noiseless channel and with a presence of eavesdropper.

Elements of matrices P, Q, N_A, N_B are believed Gaussian zero mean random values with variances 1 for matrices P, Q and σ^2 for matrices N_A, N_B. All matrix elements are mutual independent.

After exchange by matrices legitimate users A and B form primary key bits as follows:

$$\tilde{K}_A=rect(tr(P(Q+N_B))),$$
$$\tilde{K}_B=rect(tr(Q(P+N_A))).$$

Eavesdropper E be able to form her key bits after hard decoding as follows:

$$\tilde{K}_E=rect(tr((P+N_A)(Q+N_B))),$$

where "*tr*" means matrix trace operation.

We remind that in our paper [11] was investigated similar matrix basic protocol but with "*EV*" – operation (calculation of matrix eigenvalues) instead of "*tr*". It was shown in that paper that after application of PIMC protocol with parameter s = *5*, LPDC codes for error correction and privacy amplification procedure [15], we have got after a hard decoding

$P_{ed} = 2.5 \cdot 10^{-3}$ for key bit block of the length k = 24039 and information leakage to eavesdropper $I = 1.4 \cdot 10^{-3}$ bits.

This means that KSP with basic matrix protocol "works" because changing of $EV(\bullet)$ operation to $tr(\bullet)$ operation is not important and was used for algorithm simplification only.

But our task now is to check if an eavesdropper can significantly improve its decoding algorithm due to soft decoding?

We believe that eavesdropper E knows exactly algorithm PIMC and receives erasing signals correctly. Therefore, E be able to perform before of basic protocol the following preprocessing:

-simulation of SME protocol with false legitimate users A and B and repetition of this protocol N times.

In order to perform the simplest decoding procedure it is necessary

- to quantize $\tilde{K}_e = tr\left(\left(\tilde{P} + \tilde{N}_A\right)\left(\tilde{Q} + \tilde{N}_B\right)\right)$ on several levels. (More general method require to quantize diagonal elements of the matrix $\left(\tilde{P} + \tilde{N}_A\right)\left(\tilde{Q} + \tilde{N}_B\right)$)
- to form the vector $\bar{v} = \tilde{K}_{e1}, \tilde{K}_{e2}, \ldots, \tilde{K}_{es}$,
- simulate receiving of the block $\bar{u} = \bar{\gamma} \oplus \tilde{\tilde{K}}_A$ corresponding to the vector $\bar{v}$ on protocol IMCP.

After simulation SME protocol by E, she be able to arrange the Table I in line with general form, for the case of 3-level quantizing: "0", "1" or "erasing" (designated below as "er") and s = 3.

Quantization on 3 levels was performed in line with the following relations:

$$\tilde{K}_{ei} = \begin{cases} -1, if\ tr\left[P + N_A)(Q + N_B)\right] \le -d \\ 0, if\ -d < tr\left[P + N_A)(Q + N_B)\right] \le d \\ +1,\ if\ tr\left[P + N_A)(Q + N_B)\right] > d \end{cases}$$

where d – is some threshold chosen by eavesdropper

TABLE I. RESULTS OF SME PROTOCOL SIMULATION BY E (EXAMPLE FORM)

Number of seams	Observed results		Number of observation		
	Quantized traces	$\bar{u}$	$N = N_0 + N_1$	N_0	N_1
1	111	111	5000	5000	0
2	111	110	5050	4900	150
3	111	101	4820	4770	50
			…		
i	1er0	111	5010	2510	2500
i+1	1er0	110	4900	2450	2450
i+2	1er0	101	5120	3740	1380
			…		
$3^s \cdot 2^s$	er er er	000	4600	2400	2200

After a construction of the Table 1, it can be rearranged in such a way to group results corresponding to γ = 0 and γ = 1. Using this Table it is possible to find the probability of incorrect receiving of key bit as follows: $p_e = P(\gamma \neq \hat{\gamma})$

$$p_e = \frac{\sum_{\bar{u}\|\bar{v}} \min(N_0, N_1)}{M}$$

where " ‖ " is concatenation of vectors.

Next the modified Table I can be used as *soft decoding Table*.

For this purpose, E performs the following operations:

- Intercept matrices $P + N_A$, $Q + N_B$ and signal of erasing (taking into account only non-erased s-blocks),
- Calculate values of quantized traces as observation vector and find corresponding to it row in the second column.
- Take decision on $\hat{\gamma}$ (soft decoding) following to the rule:
$$\hat{\gamma} = \begin{cases} 0, N_0 \ge N_1 \\ 1, N_0 < N_1 \end{cases},$$
where N_0, N_1 are values in columns 5, 6 of the chosen row.
- If the desired row cannot be found, then decision should be taken randomly with equal probabilities for $\hat{\gamma} = 1$ and $\hat{\gamma} = 0$.

In Table II is shown only small part of the whole Table as an example of decoding procedure on the results of protocol simulation (See Fig. 7) given the following parameters: matrix sizes – 16x16; the number of primary key quantization levels – 3; threshold of quantizing – 3; the length of blocks (s_ in protocol IPMC – 5; $\sigma^2 = 1$. We note that the full Table II has 7776 rows and the number of Séances is $12 \cdot 10^6$.

TABLE II. DECODING TABLE FOR SME PROTOCOL SIMULATION BY E

Number of seams	Observed results		Number of observation		
	Quantized traces	$\bar{u}$	$N = N_0 + N_1$	N_0	N_1
1	++---	00111	118853	0	118853
2	++-+-	00101	118845	0	118845
3	+--++	10011	118834	118834	0
			…		
100	-++*-	10011	10979	0	11979
160	*+-+-	10101	10906	10906	0
227	*++-+	11100	105	104	1
305	**-**	11101	11	2	9
			…		
503	++++-	11111	1082	1082	0
638	+++-+	11000	12	1	11
932	++*-+	10110	102	0	102
			…		
1078	++-+*	00101	10872	0	10872
1119	++-*+	11110	1	1	0
1463	+*+**	00110	8	4	4
			…		

We recall (following definition given in [11]) that PIMC protocol is determined as generation of s-times repetitions for symbol γ and sending them to B. User B receives bit equals to "0" if and only if all s symbols of the received block are zeros and bits equal to "1", if and only if all symbols of the received block are ones. Otherwise B erasures this s-block and informs A about such event using feedback channel.(Remember that eavesdropper E is able to intercept all erasing signals without errors.)

In Fig. 8 are presented experimental curves of dependences $P_m = f_1(d)$ and $P_e = f_2(d)$, where d is the value of threshold for a choice of 3-level quantization channel with ***erasing***, obtained by simulation.

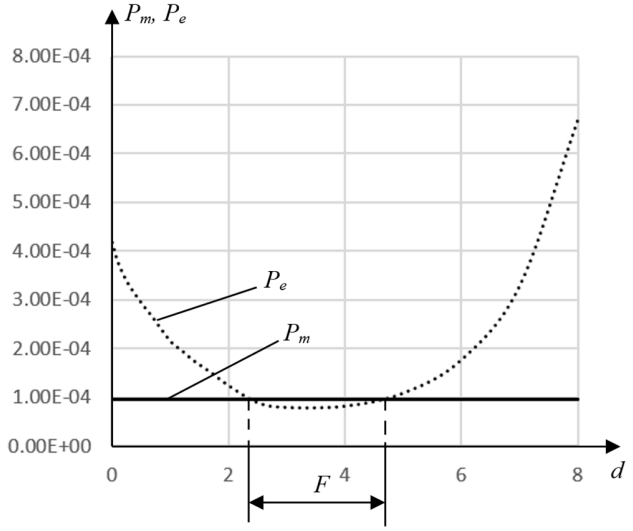

Fig. 8. Experimental dependences P_m and P_e against value of threshold d chosen for parameters s = 5, sizes of matrices 16x16 and variance $\sigma^2 = 0.1$.

We can see from Fig. 8 that E is free to select such threshold d to get $P_m, P_e \in F$, where $P_m > P_e$ and hence legitimate users A and B be unable to provide a protection against leakage of some information on the key to eavesdropper.

Of course, the parameters of SME and PIMC protocols, such as matrix sizes n, variance of noise σ^2, lengths of blocks "s" and the values of quantization thresholds d have to be optimized. Thus, only after such optimization, final conclusion about vulnerability of SME protocol can be given. But this problem requires further investigations. Another problem is to estimate the complexity of decoding Table II design, that also depends on the chosen protocol parameters.

V. Conclusion

Unfortunately, we obliged to accept that protocols of key sharing with the use of constant, public and noiseless channel without any cryptographic assumption in the presence of passive eavesdropper, presented in our papers [12], [13], are vulnerable to compromise attacks. If say more specifically, protocol BEC and RNEC can be broken with E by relatively simple hard decoding procedure of low complexity. And therefore, for such protocols $C_S = 0$

Hence such basic protocol cannot be used with any other PIMC protocols to improve such bad situation for legitimate users. The CGVE procedure may be considered acceptable one for legitimate users but only on the condition of hard decoding for eavesdropper. But it occurs still vulnerable against attacks based on soft decoding. SME protocol is secure for sure if eavesdropper is able to perform only hard decoding. As for the eavesdropper's ability to perform soft decoding, it is limited only by the complexity of decoding. Therefore, such a protocol requires further research towards assessing its complexity.

The author of the current paper would like to strike that according to our mind, the problem of secure key distribution over constant, public and noiseless channels (like Internet) is still actual for ordinary users. Hence attempts to prove or to reject its solution for CGVE and SME basic protocol is still important for information security.

References

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

[2] P. Shor. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". *SIAM Journal on Scienticand Statistical Computing.* 1997;5(26), pp.1484–1509.

[3] Dyakonov M.I. "Is Fault Tolerant Quantum Computation Really Possible? In Luryi S.,Xu J,Zaslavsky A. *Future Trends in Microelectronics*. John Wiley and Sons 2007, p.4-18.

[4] A. Mukherjee, et al., "Principles of Physical Layer Security in Multiuser Wireless Network": A Survey, 2014, arXiv:1011.3754.3 [cs. IP].

[5] U. Maurer "Secret key agreement by public discussion from common information". *IEEE Trans. on Inf. Theory*, n 3,1993, p.733-742.

[6] T. Dean and and A. Goldsmith, "Physical layer cryptography through massive MIMO" Proc. of 2013 IEEE IT Workshop,p.1-5.

[7] V. Yakovlev, V. Korzhik, G. Morales-Luna. "Key distribution protocols based on noisy channels in presence of an active adversary: Conventional and new versions with parameter optimization", *IEEE Transactions on Information Theory*, 54:6 (2008), pp. 2535-2549.

[8] V. Starostin et al., "Key generation protocol executing through non-reciprocal fading channels", LNCS vol. 16, N1, p1-16, 2019.

[9] V. Korzhik et al., "Secret Key Agreement over Multipass Channel Exploiting a Variable-Directional Antenna", *Int. Conf. of Advance Comp. Science and Application*s, vol.3,N 1,pp.172-178,2012.

[10] C. H. Bennett, et al., "Experimental quantum cryptography", *Journal of. Cryptol*., vol. 5, N1 (1992), pp. 3-28.

[11] V. Korzhik, V. Starostin, V. Yakovlev, M. Kabardov, A. Gerasimovich, A. Zhuvikin. "Information Theoretically Secure Key Sharing Protocol Executing with Constant Noiseless Public Channels". *Mathematical problems of cryptography*, 2021, T.12, N 3 pp. 31-47.

[12] V. Yakovlev, V. Korzhik, M. Akhmetsina, A. Zhuvikin. "Key Sharing Protocol Using Exchange by Integers over Public Noiseless Channels Between Users that Provides Security executing without Cryptographic Assumption", *The 31th Conference of Open Innovations Association FRUCT*, Helsinki Finland, 27-29 April 2022, pp. 363-379.

[13] V. Yakovlev, V. Korzhik, V. Starostin, A. Lapshin, A. Zhuvikin. "Channel Traffic Minimizing Key Sharing Protocol Intended for the Use over the Internet and Secure without any Cryptographic Assumption", *The 32th Conference of Open Innovations Association FRUCT*, Helsinki Finland, 2023.

[14] L. Lal. Et al, "The Wiretap Channel with Feedback Encryption over the Channel", arXiv:0704.2259v1[csIT 18Apr. 2007.

[15] V. Korjik, G. Morales-Luna, and V. Balakirsky. "Privacy amplification theorem for noisy main channel", *Lecture Notes in Computer Science*, 2200 (2001), pp. 18-26.