Proceedings of the Federated Conference on Computer Science and Information Systems pp. 569–576
DOI: 10.15439/2018F66
ISSN 2300-5963 ACSIS, Vol. 15

Secret Key Sharing Protocol between Units Connected by Wireless MIMO Fading Channels

Valery Korzhik, Aleksandr Gerasimovich,
Cuong Nguyen, Vladimir Starostin,
Victor Yakovlev, Muaed Kabardov

The Bonch-Bruevich Saint-Petersburg
State University of Telecommunication
Saint-Petersburg, Russia
Email: val-korzhik@yandex.ru, star_vs47@mail.ru

Guillermo Morales-Luna
Computer Science
CINVESTAV-IPN
Mexico City, Mexico
Email: gmorales@cs.cinvestav.mx

***Abstract*—The method of secret key sharing between units that did not possess any secret keys in advance is considered. It is assumed that between these units there are duplex wireless MIMO fading channels. In a recent paper published by D. Qin and Z. Dingh a new key sharing protocol has been proposed between legitimate users based on eigenvalues which are invariant under permutation of two matrices in their product. We extend this statement to a characteristic polynomial and by the way to matrix trace. Methods of key bits extraction are optimized both theoretically and experimentally. On the contrary to a statement of D. Qin and Z. Ding we prove that their key sharing protocol occurs insecure if eavesdroppers have the same channels as legitimate users. In order to provide reliability and security of the shared keys both error correction codes and privacy amplification methods can be used.**

***Index Terms*—Physical layer security, key sharing protocol, MIMO transmission system, characteristic polynomial, privacy amplification, error correction codes**

I. Introduction

THE pioneered paper devoted to key sharing protocol for users that did not have any secret keys in advance belongs to Diffie and Hellman [1]. It is well known that security of this protocol rests on the intractability of the *Diffie-Hellman Problem* or simply the related *discrete logarithm computing problem* [2].

There is also a class of keyless cryptography (KC), where encryption of messages can be provided secure even without any prior secret key sharing. One of such KC can be implemented by some protocol if we have encryption algorithm satisfied to the following relation for any different keys K_A, K_B and any plaintext M:

$$f_{K_A}(f_{K_B}(M)) = f_{K_B}(f_{K_A}(M)) \quad (1)$$

where f_K is the encryption algorithm for plaintexts given a key K. Then the encryption/decryption protocol between users A and B can be performed as shown in Table I. But unfortunately the condition (1) is not valid for strong symmetric block ciphers.

Alpern and Schneier [3] proposed a cryptographic technique in which the security lies in hiding the identify of the message ordinator.

TABLE I
Encryption/decryption protocol.

M: $A(K_A)$		$B(K_B)$
1.	$C_A = f_{K_A}(M)$	
2.	$\rightarrow C_B = f_{K_B}(C_A)$	
3.	$\leftarrow C'_A = f_{K_A}^{-1}(C_B); f_{K_B}^{-1}(C'_A) = M$	

In [4] some extensions to the previous scheme was suggested that was called as *semi-anonymous channel*. Although the last scheme seems to be more realistic than the previous one but both scenarios require serious restrictions regarding communication network between users that want to share secret keys.

On the other hand it was developed in recent years a new domain known as *physical layer security* (PHY) *in multiuser wireless networks*. In this setting it is assumed that users are connected by some communication (mostly continuous) channels and the properties of these channels allow either implement directly secure information transmission between users or to share secret keys for their further usage with conventional encryption/decryption. It is worth to note that such keyless cryptosystem was based firstly on Wyner's *wire-tap channel concept* proposed in 1975 [5]. This approach has been developed later in fundamental papers [6]–[8].

But we should emphasize that in order to provide information theoretic security in wireless networks it is necessary to have in any case some advantages in legitimate communication channels against eavesdropper's channels. Such advantages are presented in Table II jointly with list of references where they were used in order to provide information security of messages or key string sharing in frames of given conditions.

Summarizing the content of Table II, we can conclude that no one of the keyless cryptosystems satisfy the natural requirements: to be secure independently on eavesdropper channel or equipment states. In fact, legal user cannot provide that SNR in eavesdropper channel is not larger than some

TABLE II
POSSIBLE ADVANTAGES OF THE LEGITIMATE CHANNELS AGAINST EAVESDROPPER CHANNELS.

Nr.	Advantages of the legitimate channels	Defect of such setting	References
1.	SNR in legitimate channels is superior to SNR in eavesdropper channel	SNR as a rule is unknown in eavesdropper channel	[5], [6], [8], [9]
2.	Not all symbols of legally transmitted blocks can be intercepted by eavesdropper	It is very specific and rare case	[10], [11]
3.	Legal users have authenticated channel for public discussion	Even so authenticated channel is provided by additional measures it is unknown SNR in the eavesdropper channel in order to optimize parameters of legal transmission	[7], [12], [13]
4.	Legal channels are sensitive to any adversary intervention. (Quantum cryptography)	Special legal channels and devices are required	[14], [15]
5.	Legal users are mobile and communication channels have multipath wave propagation. (MIMO technology can be used also for security enhancing)	Mobile units can stop sometimes. Eavesdropping is still possible on very short distance from legitimate units. Reciprocity theorem of radio wave propagation can be invalid in some cases.	[16], [17], [18]
6.	Smart antennais excited randomly by electronic means and a presence of multipath communication channels is requested. (It is not required that units can be nonstop; and eavesdropper channel can be even noiseless)	Eavesdropping is possible on very short distance from legitimate units. Reciprocity theorem of radio wave propagation can be invalid in some cases.	[19], [20]
7.	The number of antennas in legitimate MIMO system is not less than the number of eavesdropper antennas	Cryptosystem can be broken if the number of eavesdropper antennas is larger than the number of legitimate antennas	[21], [22], [23]

given value, that the number of antennas in eavesdropper MIMO system is not larger than the number of legitimate antennas and finally that reciprocity of channels is always valid.

But fortunately, it has been published recently the paper [24] in that some of mentioned above problems can be removed.

In Section II we describe one of key sharing schemes presented in [24] that is on our opinion very interesting from a practical point of view. Later we extend the protocol in [24] and examine theoretically how to optimize its parameters. In Section III we present experimental results obtained by simulation. Section IV devoted to error correction and privacy amplification of key string shared by legitimate units after performing of protocol. Section V concludes the paper and proposes some open problems for further investigations.

II. EXTENSION OF EVSKEY SCHEME

Let us remind the key sharing protocol proposed in [24] and called there *EVSkey scheme*. The scenario corresponding to this scheme is presented in Figure 1.

For simplicity reasons we restricted our consideration by the condition of equality for the numbers of antennas of the legitimate users Alice (A) and Bob (B), both at the transmitter and at the receiver are n.

Before transmission, Alice and Bob generate their own reference matrices $X_A, X_B \in \mathbb{C}^{n\times n}$, as well as randomly generated unitary matrices $G_A, G_B \in \mathbb{C}^{n\times n}$. In line with our previous assumption all matrices are square of order $n \times n$.

Let the noise matrices $N_{B1}, N_{A1}N_{B2}, N_{A2}$ have *additive white Gaussian numbers* (AWGN) as random values. After the postmultiplication of the channel matrices H_{AB} and H_{BA} by G_B and G_A, respectively and sending the resulting matrices back, users Alice and Bob get the following matrices:

$$\text{Alice:} \quad Y_A = PQX_A + PN_{B1} + N_{A2} \quad (2)$$

$$\text{Bob:} \quad Y_B = QPX_B + QN_{A1} + N_{B2} \quad (3)$$

$$\text{with } P = H_{BA}G_B \quad , \quad Q = H_{AB}G_A \quad (4)$$

For small enough noises $N_{B1}, N_{A2}, N_{A1}, N_{B2}$ we get a good estimation for the matrices PQ and QP respectively as

$$PQ \approx Y_A X_A^{-1} \quad , \quad QP \approx Y_B X_B^{-1}.$$

Since Alice knows Y_A, X_A and Bob knows Y_B, X_B, they are able to compute the matrices PQ and QP although with some errors due to the presence of noises.

In [24] it is suggested to extract a common key as the quantized complex eigenvalues of matrices PQ and QP since those eigenvalues coincide one to another although these matrices may be completely different. We extend their statement and prove the following:

Lemma 1: Given two non-singular complex matrices $P, Q \in \mathbb{C}^{n\times n}$, the matrices PQ and QP have the same *characteristic polynomials*.

Proof. By definition, the characteristic polynomial of PQ is $\pi(\lambda) = \det(PQ - \lambda I)$, where I is the identity matrix.

Then the roots λ of the characteristic polynomials satisfy the equation

$$\det(PQ - \lambda I) = 0. \quad (5)$$

It follows from (5), being Q a unitary matrix,

$$\begin{aligned} 0 &= \det(PQ - \lambda I) \\ &= \det Q \det(PQ - \lambda I) \\ &= \det(QPQ - \lambda Q) \\ &= \det(QPQ - \lambda Q)\det Q^{-1} \\ &= \det(QP - \lambda I) \end{aligned}$$

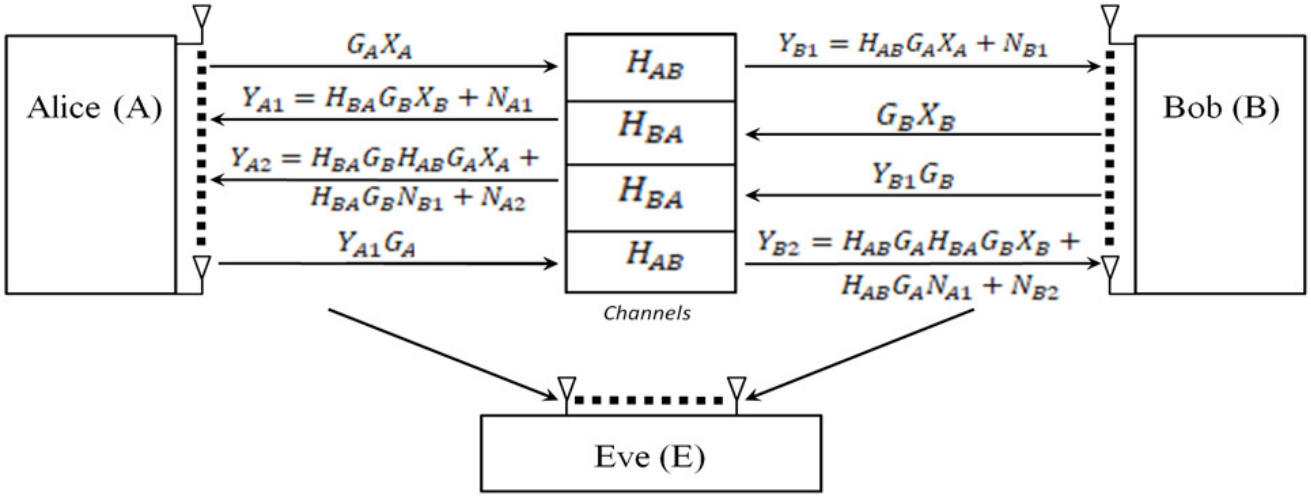

Fig. 1. The scenario corresponding to EVSKey scheme.

Then the roots of the characteristic polynomials of matrices PQ and QP coincide one to another and hence these matrices have the same characteristic polynomials. □

Thus we can calculate for the key bit generation not only the eigenvalues but also all coefficients of the characteristic polynomial and in particular case the traces of matrices PQ and QP or their determinants. Let us investigate, at first theoretically, which of the main invariants-eigenvalues or traces are less sensitive to channel noises, more closer to uniform distribution and give the most number of reliable key bits for legitimate users.

A. Using quantized matrix traces as shared key bits

Since the traces of matrices are complex values they can be quantized both on amplitude and on phase. It is proved in the Appendix that the quantization intervals on amplitude of the traces in order to provide equal probabilities of their occurrence should be chosen as follows:

$$r_{k-1} \le |Z| \le r_k \quad , \quad k = 1, 2, \ldots, N \tag{6}$$

where Z is the trace of the matrices, $r_k = \sigma\sqrt{-\ln\left(1 - \frac{k}{N}\right)}$ and N is the number of intervals.

Then the probabilities that quantized trace amplitudes coincide for users Alice and Bob will be determined by

$$p' = \sum_{k=1}^{N} \left((1 - (k-1)p)^{\frac{1}{\gamma^2}} - (1 - kp) \right) \tag{7}$$

where $\gamma = \frac{1}{1+\alpha}$, $\alpha = \sigma^2\left(1 + \frac{1}{N}\right)$, $p = \frac{1}{N}$.

In Table III there are presented the results of calculations by (7) for some parameters. We see from this table that the probability of errors are still acceptable for $N = 16$ if $\sigma^2 \le 0.001$ and for $N = 32$ if $\sigma^2 \le 0.0001$.

TABLE III
THE PROBABILITIES OF KEY COINCIDING BY (7) AFTER A PERFORMANCE OF KEY SHARING PROTOCOL BASED ON QUANTIZATION BY (6) THE MATRIX TRACES ON AMPLITUDE.

$N \setminus \sigma^2$	0.01	0.001	0.0001
4	0.98	0.998	0.9998
8	0.96	0.996	0.9996
16	0.92	0.992	0.9992
32	0.84	0.984	0.998
64	0.68	0.968	0.9968

σ^2: SNR N: Number of quantization intervals

B. Using quantized matrix eigenvalues as the shared key bits

Then every eigenvalue can be quantized on phase and amplitude intervals. Unfortunately there appears one problem: how to compare the numbering of eigenvalues adopted by the users?

Let us denote by N_P, N_A the numbers of quantization intervals on phase and amplitude, respectively. Then total number of quantization intervals is $N = N_A \cdot N_P$. We will fix the number of eigenvalues that hit in each of the N intervals (cells). After a completion of eigenvalues extraction, we get a string of integers $g_1, g_2, \ldots, g_i$, where g_i is the number of the i-th cell containing at least one eigenvalue. If several eigenvalues occur in the same cell, then the cell number is repeated as $g_i, \ldots g_i$. Next each number g_i is presented as a string of bits and such strings are connected in a consecutive binary manner. The final binary string forms a part of the shared key. It is easy to see that the total number of bits for each session of protocol can be, if $N \gg n$, approximately computed [25] as:

$$\log_2 \binom{N+n-1}{n} = \log_2 \left[\frac{1}{n!} \prod_{i=N}^{N+n-1} i \right] \tag{8}$$

C. Security of the proposed key sharing protocol

As it is shown in Figure 1, the eavesdropper Eve is able to receive only the matrices $G_A X_A, G_B X_B, Y_{A1}, Y_{B1}, Y_{A2}, Y_{B2}$ even for the ideal case when eavesdropping channels are noiseless. It is claimed in [24] that even in the very unrealistic case when Eve's receivers are located very close to the locations of Alice and Bob, and hence she is able to estimate correctly the channel matrices H_{AB}, H_{BA} of legitimate users, she is unable to compute the matrices P and Q (see eq (4)) because they are "randomized" by the unitary matrices G_B and G_A. The last matrices cannot in turn be estimated by Eve because they are "randomized" by the reference matrices X_A and X_B.

In [24] it is concluded that such key sharing system is *ideal secure* and its security is regardless of the state of the channels and the SNR in the eavesdropper channel, in contrast to all key distribution protocols described actually in Table II. *Unfortunately this statement is wrong.* In fact, following the steps below, Eve for sure is able to receive the key shared by the legitimate users:

1. $H_{BA}G_B = H_{BA}G_B H_{AB}G_A X_A \left(H_{AB}G_A X_A\right)^{-1}$
2. $X_B = \left(H_{BA}G_B\right)^{-1} H_{BA}G_B X_B$
3. $QP = Y_B X_B^{-1}$
4. $QP \rightarrow$ characteristic polynomial (equivalent to the shared key)

The key bit string should have good statistical properties as it is common for all secret cryptographic keys. (Such property is verified in the next Section using the NIST tests on pseudorandomness.)

On the other hand in order to provide a good key bit agreement between legitimate users it is very important a strong correlation between channel matrices in the first and in the second steps of the key sharing protocol.

In fact, if they would be different, say H_{AB}, H_{BA} at the first step and H'_{AB}, H'_{BA} at the second step, we would get (even in noiseless channels) instead of relations (2-4) the following ones:

$$\begin{array}{rcccl} Y'_A & = & Y'_{A2} & = & H'_{BA}G_B H_{AB}G_A X_A \\ Y'_B & = & Y'_{B2} & = & H'_{AB}G_A H_{BA}G_B X_B \end{array} \quad (9)$$

From the second equation in (9), there is no a matrix permutaition of the first one and hence the matrices Y'_A and Y'_B have not necessarily equal characteristic polynomials.

In order to provide a strong correlation between channel matrices in the first and in the second steps of the key sharing protocol (channel coherence property – in other words) it is necessary to agree physical channel properties with the rate of communication.

Typical data rates for Wi-Fi network or celular communication (LTE, 56) lies in a range of several hundreds ms. Coherence time for channels used in mobile unit communication is in range (1-10 ms) [26] and then during coherence time a number between 103 and 106 of bits can be transmitted which is sufficient to provide practical coincidence of Y_A, Y_B with matrices Y'_A, Y'_B.

TABLE IV
SIMULATION RESULTS OF THE BIT ERROR PROBABILITIES (IN PERCENT) FOR EXTRACTION THEM FROM EIGENVALUES. BOTH NUMBERS OF PHASE QUANTIZATION INTERVALS AND AMPLITUDE ONE ARE 8.

SNR $\frac{1}{\alpha}$ (dB) $\setminus$ n	4	8	16
20	21.6	22	24
30	7.7	10	12
40	2.7	3.5	4
Number of extracted bits	19	33	52

n is the number of antennas

TABLE V
LIST OF NIST TESTS ON PSEUDO RANDOMNESS.

Nr.	Title of test
1	The frequency test
2	Frequency test within a block
3	The runs test
4	Tests for the longest-run-of-ones in a block
5	The binary matrix rank test
6	The discrete Fourier transform (spectral) test
7	The non-overlapping template matching test
8	The overlapping template matching test
9	Maurer's "Universal Statistical" test
10	The linear complexity test
11	The serial test
12	The approximate entropy test
13	The cumulative sums (cusums) test
14	The random excursion test
15	The random excursions variant test

Unfortunately the considered system (as well as all PHY-based systems) is vulnerable against active adversary. It is a scenario where an adversary, say Mallet, is presented by Alice or Bob as legitimate users and performs with any of them the above mentioned protocol. It is obvious that then he is able to share reliable key after completing the protocol. Such problem has to be solved by some additional activity of legitimate users, in order to reject falsely shared key before its implementation for encryption of secure messages [27].

III. SIMULATION RESULTS FOR THE PROPOSED KEY SHARING PROTOCOL

In order to verify our theoretical discussion it was undertaken a simulation of the EVSkey protocol. The results of simulation for extraction of key bits from matrix eigenvalues are presented in Table IV, where is presented also the number of key bits for different number of antennas n calculated by (8).

We see from Table IV that the acceptable SNR is at least 30 dB even for the case when we mean to use later error correcting codes (see Section IV). As far as the lengths of share key string they are too small for implementation even for block ciphers like 3DES or AES. Thus one can be recommended to repeat key sharing session several times. (Such approach is also presented in Section IV.)

The generated key bits were investigated by NIST tests on pseudo randomness [28]. The list of NIST tests is presented in Table V, while the results of testing on pseudo randomness in Table VI with their numbering taken from Table V.

TABLE VI
RESULTS OF THE NIST-BASED TESTING FOR THE KEY BITS SEQUENCE EXTRACTED FROM THE MATRIX EIGENVALUES UNDER THE CONDITION SNR = 30 DB AND ALSO AFTER A SHIFTING AND SUMMATION PROCEDURE.

("1" – means that test is passed, "0" – that test is not passed).

Test number	Original one	After shift and addition mod 2
1	1	1
2	1	1
3	1	1
4	0	1
5	1	1
6	0	0
7	1	1
8	1	1
9	1	1
10	1	1
11	0	0
12	0	0
13	1	1
14	0	0
15	0	0

TABLE VII
SIMULATION RESULTS FOR PROBABILITY OF KEY (TRACE) COINCIDING AFTER A PERFORMANCE OF KEY SHARING PROTOCOL BASED ON QUANTIZATION BY (6) THE MATRIX TRACES ON AMPLITUDE (16 ANTENNAS).

The number of rings	Number of key bits	σ^2	P_{tr}
4	2	0.01	0.88
		0.001	0.90
		0.0001	0.98
8	3	0.01	0.82
		0.001	0.94
		0.0001	0.99
16	4	0.01	0.74
		0.001	0.90
		0.0001	0.98
32	5	0.01	0.68
		0.001	0.83
		0.0001	0.97
64	6	0.01	0.67
		0.001	0.78
		0.0001	0.92

In the same Table VI there are presented also the results of NIST-based testing after a shifting right on the 20 bits and addition $\mathrm{mod}\ 2$ with the original sequence.

We see that after the transformation procedure the key sequence occurs slightly better. The results of simulation for extraction of key bits from matrix traces are presented in Tables VII, VIII. Comparing the results in Table IV and Tables VII, VIII we see that extraction of the key bits from the matrix eigenvalues results in larger errors than for the trace-based extraction but the number of extracted bits is significantly less for the case of extraction from the traces than for the extraction from eigenvalues.

The key bits extracted from traces were investigated by the NIST tests given in Table V. The results of testing are shown in Table IX jointly with "shift and addition" transformation. We can see from this Table that now an additional transform is not

TABLE VIII
SIMULATION RESULTS OF THE BIT ERROR PROBABILITIES P' (IN PERCENTS) FOR EXTRACTION THEM FROM MATRIX TRACES WITH DIFFERENT SIZES OF QUANTIZATION LEVELS AND ANTENNA NUMBERS.

The number of antennas	The number of sectors	The number of rings	Number of key bits	σ^2	P'
4	8	8	6	0.01	14.7
				0.001	4.7
				0.0001	2.1
	16	4	6	0.01	14
				0.001	4
				0.0001	1.5
	32	4	7	0.01	21
				0.001	11
				0.0001	3
	16	8	7	0.01	18
				0.001	7
				0.0001	2
	8	16	7	0.01	19
				0.001	10
				0.0001	2
	32	8	8	0.01	19
				0.001	10
				0.0001	2
8	8	8	6	0.01	14.3
				0.001	4.4
				0.0001	1.1
16	8	8	6	0.01	12.3
				0.001	6.7
				0.0001	0.7

TABLE IX
RESULTS OF NIST-BASED TESTING FOR THE KEY BITS EXTRACTED FROM MATRIX TRACES UNDER CONDITION OF SNR = 30 DBAND ALSO AFTER A SHIFTING AND SUMMATION PROCEDURE.

Test number	Original one	After shift and addition mod 2
1	1	1
2	1	1
3	1	1
4	1	1
5	1	1
6	1	1
7	1	1
8	1	1
9	1	1
10	1	1
11	1	1
12	1	1
13	1	1
14	0	0
15	0	0

necessary. This means that this case is superior to extraction from eigenvalues with point of key statistic view.

By comparing the results of Table III and Table VII we conclude that the quantization procedure based on (6) is acceptable. This is valid also for the case of 4 and 8 antennas.

IV. ERROR CORRECTION AND PRIVACY AMPLIFICATION

We assume that the length of the shared key should be at least 256 bits, taken into account for example that the length of key string for AES is 128 bits. This means that in order to provide the requested key length it is necessary to arrange

several sessions of key sharing protocol. Moreover in order to provide a good statistic of shared key bits it is necessary that states of channel matrices between sessions should be statistically independent. In order to short the number of such sessions the method of key bit extraction from matrix eigenvalues occurs preferential because it allows to extract more bits than matrix trace extraction during a single session (see Table IV and Tables VII, VIII). But anyway the values of bit error probabilities are too much for a good key agreement between legitimate users. This fact requires to correct errors by sending over public noiseless channel the check symbols of some good error correction code. But on the other hand a sending of check symbols over public (open) channel results in a leaking to Eve some information about key string. In order to guarantee that such leakage is limited by some value of Shannon information it is necessary to use so called *privacy amplification*. It can be provided by hashing of raw key string to more shorter final key string. It has been proved in [29] the enhanced *privacy amplification theorem.* This theorem says that using special two-stage hashing procedure the eavesdropper's expected Shannon information I_o about the final key shared by legitimate parties, satisfies the inequality:

$$I_o < \frac{1}{\gamma \ln 2} 2^{-(k-t_c-\ell-r)} \tag{10}$$

where k is the length of the raw key string shared by legitimate users after a completing of protocol, t_c is the Renyi (collision) information obtained by Eve, r is the number of check symbols sent from Alice to Bob in order to reconcile their key strings, ℓ is the length of the final key string after hashing, γ is a coefficient that approaches 0.42 for any fixed r, as k, ℓ and $k - \ell$ increase.

Since we assume that Eve is not nearby legal users, she has no eavesdropping at all, hence t_c can be removed ($t_c = 0$).

The probability P_d of error after decoding by some linear binary error correcting code with the number of information bits k, the number of check symbols r and for the probability of bit error after a completing at protocol *P'* has the following upper bound [29]

$$P_d \leq 2^{-k(1-R)} \left(1 + 2\sqrt{P'(1-P')}\right)^k \tag{11}$$

where $R = \frac{k}{k+r}$.

Using the formulas (10), (11) we can optimize the parameter r to provide the requested values I_o and P_d.

But of course for practical implementation it is necessary to use some constructive methods of encoding and decoding, say for the thing, the LDPC codes [30].

V. Conclusion

In the current paper we considered some extension of key sharing protocol proposed in [24]. It has been proved that key extraction can be performed not only from matrix eigenvalues but from matrix traces also. Moreover the extracted key bits occur for the last case even closer to pseudo random sequence in terms of NIST tests. But unfortunately the length of key strings is significantly less in the last case in comparison with extraction the key from matrix eigenvalues. Therefore this method is superior for practical implementation against matrix trace-based extraction.

We investigated how affect such parameters of key sharing protocol as the number of antennas, SNR in the legitimate channel and method of quantization. It was striked that key sharing protocol does not work if eavesdroppers has the same communication channels as legitimate users!

In fact it would be very strange to be the case because then legitimate users could share secret key without a presence of any fading channels and they could simply communicate through any channels with constant parameters.

We believe that key sharing between mobile unit is a promising approach because nothing restrictions on eavesdropping channels are suggested except of nearby locations of eavesdroppers against legal users.

The future work can be devoted to a modification of quantization procedures for the case of extraction from eigenvalues and investigation of constructive encoding and decoding for the most effective error correction in the shared key string.

References

[1] W. Diffie and M. E. Hellman, "New directions in cryptography," vol. 22, no. 6, pp. 644–654, 1976.

[2] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, ser. The CRC Press series on discrete mathematics and its applications. 2000 N.W. Corporate Blvd., Boca Raton, FL 33431-9868, USA: CRC Press, 1997. ISBN 0-8493-8523-7

[3] B. Alpern and F. B. Schneider, "Key exchange using 'keyless cryptography'." *Inf. Process. Lett.*, vol. 16, no. 2, pp. 79–81, 1983. [Online]. Available: http://dblp.uni-trier.de/db/journals/ipl/ipl16.html#AlpernS83

[4] M. M. Yung, "A secure and useful "keyless cryptosystem"," vol. 21, no. 1, pp. 35–38, Jul. 1985.

[5] A. Wyner, "Wire-tap channel concept," *Bell System Technical Journal*, vol. 54, pp. 1355–1387, 1975.

[6] A. Carleial and M. Hellman, "A note on wyner's wiretap channel (corresp.)," *IEEE Transactions on Information Theory*, vol. 23, no. 3, pp. 387–390, May 1977. doi: 10.1109/TIT.1977.1055721

[7] U. Maurer, "Secret key agreement by public discussion from common information." *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, 1993.

[8] I. Csiszár and J. Körner, "Broadcast channel with confidential messages." *IEEE Transactions on Information Theory*, vol. 24, no. 2, pp. 339–348, 1978.

[9] V. Korjik and V. Yakovlev, "Non-asymptotic estimates for efficiency of code jamming in a wire-tap channel," *Problems of Information Transmission*, vol. 17, pp. 223–22, 1981.

[10] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," in *Advances in Cryptology: Proceedings of EUROCRYPT 84, A Workshop on the Theory and Application of of Cryptographic Techniques, Paris, France, April 9-11, 1984, Proceedings*, 1984. doi: 10.1007/3-540-39757-4_5 pp. 33–50. [Online]. Available: https://doi.org/10.1007/3-540-39757-4_5

[11] V. Korjik and D. Kushnir, "Key sharing based on the wire-tap channel type ii concept with noisy main channel," in *Proc. Asiacrypt96*. Springer Lecture Notes in Computer Science 1163, 1996, pp. 210–217.

[12] V. Yakovlev, V. I. Korzhik, and 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*, vol. 54, no. 6, pp. 2535–2549, 2008.

[13] V. Korjik and M. Bakin, "Information-theoretically secure keyless authentication," in *Proc. IEEE Symp. on IT'2000*. IEEE, 2000, p. 20.

[14] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *J. Cryptol.*, vol. 5, no. 1, pp. 3–28, Jan. 1992. [Online]. Available: http://dl.acm.org/citation.cfm?id=146395.146396

[15] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of International Conference on Computers, Systems and Signal Processing*, December 1984.
[16] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *Information Sciences and Systems, 2007. CISS '07. 41st Annual Conference on*, March 2007. doi: 10.1109/CISS.2007.4298439 pp. 905–910.
[17] J. W. Wallace and R. K. Sharma, "Automatic secret keys from reciprocal MIMO wireless channels: measurement and analysis." *IEEE Trans. Information Forensics and Security*, vol. 5, no. 3, pp. 381–392, 2010. [Online]. Available: http://dblp.uni-trier.de/db/journals/tifs/tifs5.html#WallaceS10
[18] V. Yakovlev, V. Korzhik, P. Mylnikov, and G. Morales-Luna, "Outdoor secret key agreement scenarios using wireless MIMO fading channels," vol. 14, pp. 1–25, 01 2017.
[19] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *IEEE Transactions on Antennas and Propagation*, vol. 53, no. 11, pp. 3776–3784, 2005.
[20] V. Yakovlev, V. I. Korzhik, Y. Kovajkin, and G. Morales-Luna, "Secret key agreement over multipath channels exploiting a variable-directional antenna," *Int. Jour. Adv. Computer Science & Applications*, vol. 3, no. 1, pp. 172–178, 2012.
[21] T. Dean and A. Goldsmith, "Physical-layer cryptography through massive MIMO," in *2013 IEEE Information Theory Workshop, ITW 2013, Sevilla, Spain, September 9-13, 2013*, 2013. doi: 10.1109/ITW.2013.6691222 pp. 1–5. [Online]. Available: http://dx.doi.org/10.1109/ITW.2013.6691222
[22] R. Steinfeld and A. Sakzad, "On massive mimo physical layer cryptosystem," in *2015 IEEE Information Theory Workshop - Fall (ITW)*, Oct 2015. doi: 10.1109/ITWF.2015.7360782 pp. 292–296.
[23] V. Korzhik, V. Starostin, and K. Akhrameeva, "Investigation of keyless cryptosystem proposed by Dean and Goldsmith," in *2017 21st Conference of Open Innovations Association (FRUCT)*, Nov 2017. doi: 10.23919/FRUCT.2017.8250182 pp. 194–201.
[24] D. Qin and Z. Ding, "Exploiting multi-antenna non-reciprocal channels for shared secret key generation," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 12, pp. 2693–2705, Dec 2016. doi: 10.1109/TIFS.2016.2594143
[25] W. Feller, *An introduction to probability theory and its applications. Volume 1*, ser. Wiley series in probability and mathematical statistics. New York, Chichester, Brisbane: John Wiley & sons, 1968. ISBN 0-471-25711-7. [Online]. Available: http://opac.inria.fr/record=b1122219
[26] T. Rappaport, *Wireless Communications: Principles and Practice*, 2nd ed. Upper Saddle River, NJ, USA: Prentice Hall PTR, 2001. ISBN 0130422320
[27] D. Dasgupta, A. Roy, and A. Nag, *Advances in User Authentication*, 1st ed. Springer Publishing Company, Incorporated, 2017. ISBN 3319588060, 9783319588063
[28] L. E. Bassham, III, A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, E. B. Barker, S. D. Leigh, M. Levenson, M. Vangel, D. L. Banks, N. A. Heckert, J. F. Dray, and S. Vo, "Sp 800-22 rev. 1a. a statistical test suite for random and pseudorandom number generators for cryptographic applications," Gaithersburg, MD, USA, Tech. Rep., 2010.
[29] V. Korjik, G. Morales-Luna, and V. Balakirsky, "Privacy amplification theorem for noisy main channel," *Lecture Notes in Computer Science*, vol. 2200, pp. 18–26, 2001.
[30] K. Shalkoska, *Implementation of LDPC Algorithm: In C Programming Language*. LAP LAMBERT Academic Publishing, 2017. ISBN 9783330026049. [Online]. Available: https://books.google.com.mx/books?id=1yNcMQAACAAJ

APPENDIX

Proof of relation (7)

Let us consider an extraction of the key based on matrix traces. Assume that the elements of both channel matrices $P = [p_{ij}]_{1\le i,j\le n}$, $Q = [q_{ij}]_{1\le i,j\le n}$ are random, mutually independent and identically distributed: $p_{ij}, q_{ij} \sim \mathrm{CN}(0, \sigma_w^2)$. Similarly these conditions hold and for the noise matrices $N_1 = [n_{ij1}]_{1\le i,j\le n}$, $N_2 = [n_{ij2}]_{1\le i,j\le n}$: $n_{ij1}, n_{ij2} \sim \mathrm{CN}(0, \sigma_e^2)$. We admit also that channel matrices and noisy are mutual independent. The relation (3) entails

$$\begin{aligned} YX^{-1} &= PQ + PN_1X^{-1} + N_2X^{-1} \quad \text{and} \\ \mathrm{Tr}(YX^{-1}) &= \mathrm{Tr}(PQ) + \mathrm{Tr}(PN_1X^{-1}) + \mathrm{Tr}(N_2X^{-1}). \end{aligned}$$

It is easy to show that for large number of antennas ($n \gg 1$) due to Central Limit Theorem, the random variables

$$Z_A = \mathrm{Tr}(Y_{A2}X_A^{-1}) \quad , \quad Z_B = \mathrm{Tr}(Y_{B2}X_B^{-1})$$

have Gaussian distributions:

$$f_A(z) = f_B(z) = \frac{1}{\pi\sigma^2} e^{-\frac{|z|^2}{\sigma^2}} \tag{12}$$

where $\sigma^2 = DZ_A = DZ_B = n^2\sigma_w^2(\sigma_w^2 + \sigma_e^2)$.

Let us estimate the dependence of the random variables Z_A, Z_B using the notion of linear regression Z_A onto Z_B:

$$Z_B - E(Z_B) = \gamma \frac{\sigma_A}{\sigma_B} (Z_A - E(Z_A))$$

where

$$\gamma = \frac{1}{\sqrt{(DZ_A)(DZ_B)}} \mathrm{cov}\,(Z_A, Z_B)$$

is a correlation coefficient.

Since Z_A, Z_B are centered random variables with equal variances, the equation of linear regression Z_A onto Z_B has the form

$$Z_B = \gamma Z_A. \tag{13}$$

It is easy to show that $\mathrm{cov}\,(Z_A, Z_B) = n^2\sigma_w^2$. Thus we get

$$\begin{aligned} \gamma &= \frac{n^2\sigma_w^2}{n^2\sigma_w^2(\sigma_w^2 + \sigma_e^2) + n\sigma_e^2} \\ &= \left(1 + \frac{\sigma_e^2}{\sigma_w^2}\left(1 + \frac{1}{n\sigma_w^2}\right)\right)^{-1} \end{aligned} \tag{14}$$

Since the correlation coefficient γ is real-valued, it results that the random values Z_A, Z_B differ by modulus only.

If $n\sigma_w^2 \gg 1$ and the noise-to- signal ratio $\frac{\sigma_e^2}{\sigma_w^2}$ is small, then we get by (14)

$$\gamma = \frac{1}{1+\alpha} \approx 1 - \alpha \ , \ \alpha = \frac{\sigma_e^2}{\sigma_w^2}\left(1 + \frac{1}{n\sigma_w^2}\right) \approx \frac{\sigma_e^2}{\sigma_w^2} \ll 1.$$

Thus the dependence (13) between Z_A, Z_B is almost linear.

In order to get a uniformly distributed key, let us quantize the range of values Z_A (on the complex plane) in radial direction in such a way that the probability to hit Z_A into each of N rings $R_k = \{z \in \mathbb{C} |\ r_{k-1} \le |z| < r_k\}$, $r_0 = 0$, $r_N = +\infty$, occurs equally likely:

$$\Pr\,(r_{k-1} \le |z| < r_k) = \frac{1}{N} =: p \text{ for } k = 1, \ldots, N \tag{15}$$

Using (12) we are able to find the radial distribution function of Z_A:

$$F(r) = \Pr\,(|z| < r) = 1 - e^{-\frac{r^2}{\sigma^2}}$$

Thus (15) holds if and only if

$$\begin{aligned}\Pr\left(r_{k-1} \le |z| < r_k\right) &= F(r_k) - F(r_{k-1}) \\ &= e^{-\frac{r_{k-1}^2}{\sigma^2}} - e^{-\frac{r_k^2}{\sigma^2}} \\ &= p\end{aligned}$$

It results the relation

$$F(r_k) = kp = 1 - e^{-\frac{r_k^2}{\sigma^2}} \tag{16}$$

Eventually we get $r_k = \sigma\sqrt{-\ln(1-kp)}$.

Let us estimate now the probability of key coincidence for both legitimate users A and B. First we estimate the probability p_k to get Z_A and Z_B in the ring R_k. Taken into account that the dependence (13) is almost linear $Z_B \approx \gamma Z_A$, where $0 < \gamma \le 1$, we get $|Z_B| = \gamma|Z_A|$. Hence

$$\begin{aligned}p_k &= \Pr\left(Z_A \in R_k \ \&\ Z_B \in R_k\right) \\ &= \Pr\left(r_{k-1} \le |Z_A| < r_k \ \&\ r_{k-1} \le |Z_B| < r_k\right) \\ &= \Pr\left(r_{k-1} \le |Z_A| < r_k \ \&\ r_{k-1} \le \gamma|Z_A| < r_k\right) \\ &= \Pr\left(r_{k-1} \le |Z_A| < r_k \ \&\ \frac{r_{k-1}}{\gamma} \le |Z_A| < \frac{r_k}{\gamma}\right) \\ &= \Pr\left(\frac{r_{k-1}}{\gamma} \le |Z_A| < r_k\right).\end{aligned}$$

Using (16), we find that

$$\begin{aligned}p_k &= F(r_k) - F\left((\frac{r_{k-1}}{\gamma}\right) \\ &= e^{-\frac{r_{k-1}^2}{\gamma^2\sigma^2}} - e^{-\frac{r_k^2}{\sigma^2}} \\ &= (1-(k-1)p)^{\frac{1}{\gamma^2}} - (1-kp)\end{aligned}$$

Then the probability that even legal users get the same key (trace) under the condition $\gamma > \gamma_{cr} = \frac{r_{k-1}}{r_k}$ is equal to

$$\begin{aligned}p' &= \sum_{k=1}^{N} p_k \\ &= \sum_{k=1}^{N} \left((1-(k-1)p)^{\frac{1}{\gamma^2}} - (1-kp)\right).\end{aligned}$$

It is worth to note that a quantization problem of the matrix trace (in the case when legal users extract the key namely from it) can be solved trivially because the distribution (12) is independent of the "angle variable". This is valid also for all coefficients of characteristic polynomial including matrix eigenvalues. In fact, it is a consequence of circular symmetry of channel matrices and matrices of noises.