International Journal of Computer Science and Applications,
©Technomathematics Research Foundation
Vol. 16, No. 1, pp. 1 – 16, 2019

KEY GENERATION PROTOCOL EXECUTING THROUGH NON-RECIPROCAL FADING CHANNELS

VLADIMIR STAROSTIN, VALERY KORZHIK,
MUAED KABARDOV, ALEKSANDER GERASIMOVICH, VICTOR YAKOVLEV

The Bonch-Bruevich Saint Petersburg State University of Telecommunications,
Saint-Petersburg, Russia.
Email: val-korzhik@yandex.ru, star_vs_47@mail.ru

GUILLERMO MORALES-LUNA

Computer Science Department
CINVESTAV-IPIV,
Mexico City, Mexico.
gmorales@cs.cinvestav.mx

We consider key generation protocol published recently by D.Qin and Z.Ding and called by them EVSKey scheme. This protocol is based on extraction by legitimate users of eigenvalues, which are invariant by matrix commutation and it does not require reciprocal channels connecting the users. We extend this protocol to extraction of matrix traces and we consider quantization procedure in more detail. On the contrary, to a statement of D.Qin and Z.Ding we prove that their sharing protocol occurs insecure for any distances between eavesdropper and legitimate users. In order to provide reliability and security of the shared key we propose to add artificial noises in channels and to use error correction codes and privacy amplification methods.

Keywords: Physical layer security, key sharing protocol, MIMO transmission system, characteristic polynomials, privacy amplification.

1. 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 known well that security of this protocol rests on the intractability of the Diffie-Hellman Problem or simply on the related discrete logarithm-computing problem.

There is also a class of keyless cryptography (KC), where encryption of messages can be provided secure even without any prior secret key sharing [2]. One protocol of such KC can be implemented if we have an encryption algorithm satisfying 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. The encryption/decryption protocol between users A and B is performed as shown in Table 1. 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 identity of the message originator.

In [4] an extension to the previous scheme was suggested, called semi-anonymous channel. Although the last scheme seems to be more realistic than the previous one, both

scenarios require serious restrictions regarding communication networks between users sharing secret keys.

Table 1. Encryption/decryption protocol

M: $A(K_A)B(K_B)$

1. $C_A = f_{K_A}(M) \longrightarrow$
2. $\longleftarrow C_B = f_{K_B}(C_A)$
3. $C'_A = f_{K_A}^{-1}(C_B)\ ;\ f_{K_B}^{-1}(C'_A) = M \longrightarrow$

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 to 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].

Table 2. 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 antennas 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]

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 2 jointly with a 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 2, we conclude that none of the keyless cryptosystems satisfy the natural requirements: to be secure independently on eavesdropper channel or the equipment states. In fact, legal users cannot provide noise that SNR in the eavesdropper channel is not larger than some 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, recently some of the above-mentioned problems seemed to be solved [24].

In Section 2 we describe one of key sharing schemes presented in [24] that is on our opinion very interesting from a practical point of view. We extend this protocol [24] and examine theoretically how to optimize its parameters. We prove that the original EVSKey protocol is insecure and we show how it can be modified to provide security. In Section 3 we present experimental results obtained by simulation. Section 4isdevoted to error correction and privacy amplification of key string shared by legitimate units after performance of the protocol. Section 5 concludes the paper and proposes some open problems for further investigations.

2. Extension of EVSKey Scheme

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

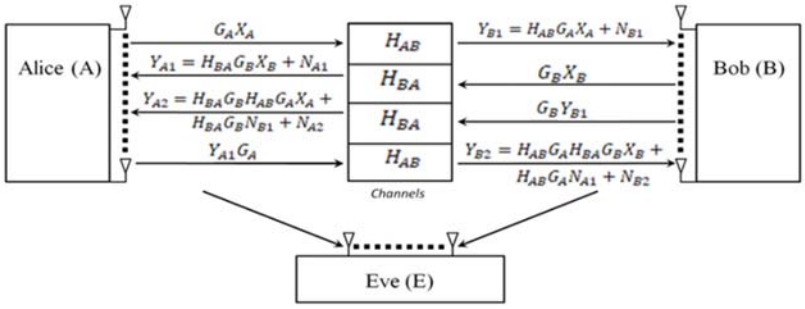

Fig. 1. The scenario corresponding to EVSKey scheme.

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 × 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:

$$\text{Alice:} Y_{A2} = PQX_A + PN_{B1} + N_{A2} \tag{2}$$

$$\text{Bob:} Y_{B2} = QPX_B + QN_{A1} + N_{B2} \tag{3}$$

with

$$P = H_{BA}G_B, \quad Q = H_{AB}G_A \tag{4}$$

For small enough noisesN_{B1},N_{A1}, N_{B2},N_{A2} we get a good estimation for the matrices PQ and QP respectively as$PQ \approx Y_{A2}X_A^{-1}$, $QP \approx Y_{B2}X_B^{-1}$

Since Alice knows Y_{A2},X_A and Bob knows Y_{B2},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 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 characteristicpolynomials.*

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

$$\det(PQ - \lambda I) = 0 \tag{5}$$

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

$$0 = \det(PQ - \lambda I) = \det Q \cdot \det(PQ - \lambda I) = \det(QPQ - \lambda Q)$$
$$= \det(QPQ - \lambda Q)\det Q^{-1} = \det(QP - \lambda I)$$

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.

2.1. Using quantized matrix traces as shared key bits

Since the traces of matrices are complex, 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 providing equal probabilities of their occurrence should be chosen as follows:

$$r_{k-1} \le |Z| \le r_k, k = 1, 2, \dots, N \quad (6)$$

where Z is the trace of the matrices, $r_k = \sigma_z \sqrt{-\ln\left(1 - \frac{k}{N}\right)}$ and N is the number of intervals. Then the probabilities that quantized trace amplitudes coincide for users Alice and Bob will be determined by

$$P' = \sum_{k=1}^{N} (1 - (k-1)p)^{1/\gamma^2} - (1 - kp)), \quad (7)$$

where $\gamma = \frac{1}{1+\alpha}$, $p = \frac{1}{N}$.

In Table 3 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 = 64 if $\sigma^2 \le 0.0001$.$\sigma^2 = \frac{\sigma_e^2}{\sigma_w^2}$ NSRwith $\sigma_w = 1$.

Table 3.The probabilities of key coinciding by (7) after a performance of key sharing protocol based on quantization by (6) the matrix traces on amplitude.

σ2 / **N**	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

2.2. 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 $g_1,g_2,\dots,g_i$, 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 $g_i,\dots g_i$. 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 $N \gg n$ (n is the number of antennas), approximately computed [25] as:

$$\log_2\left[\binom{N+n-1}{n}\right] = \log_2\left[\frac{(N+n-1)(N+n-2)\dots N}{n!}\right]. \quad (8)$$

2.3. 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_AX_A, G_BX_B, Y_{A1}, Y_{B1}, Y_{A2}, Y_{B2}. 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 2. Unfortunately, this statement is wrong.

In fact, let us assume that eavesdropper is able to receive signals (matrices) $\widetilde{Y}_{A1}$, $\widetilde{Y}_{A2}$, $\widetilde{Y}_{B1}$, $\widetilde{Y}_{B2}$ (see Fig. 1) but over channels described by matrices H_{AE}, H_{BE} that do not coincide with matrices H_{AB}, H_{BA}, respectively. Moreover matrices H_{AE}, H_{BE} be even not correlated with corresponding matrices H_{AB}, H_{BA}. Consider firstly a scenario when both legitimate and eavesdropper channels are noiseless. Then we get the following relations (see Fig. 1):

$$\widetilde{Y}_{A1} = H_{BE}G_BX_B, \quad \widetilde{Y}_{A2} = H_{BE}G_BH_{AB}G_AX_A,$$
$$\widetilde{Y}_{B1} = H_{AE}G_AX_A, \quad \widetilde{Y}_{B2} = H_{AE}G_AH_{BA}G_BX_B\ . \tag{9}$$

Let the eavesdropper E, given matrices$\widetilde{Y}_{A1}$, $\widetilde{Y}_{A2}$,$\widetilde{Y}_{B1}$,$\widetilde{Y}_{B2}$, compute the matrix:

$$\Lambda = \widetilde{Y}_{A2}\left(\widetilde{Y}_{B1}\right)^{-1}\widetilde{Y}_{B2}(\widetilde{Y}_{A1})^{-1} \tag{10}$$

Substituting (9) into (10) she gets:

$$\Lambda = H_{BE}G_BH_{AB}G_AX_AX_A^{-1}G_A^{-1}H_{AE}^{-1}H_{AE}G_AH_{BA}G_BX_BX_B^{-1}G_B^{-1}H_{BE}^{-1} \tag{11}$$

After a simple transforms (11) can be expressed as the following:

$$\Lambda = H_{BE}G_BH_{AB}G_AH_{BA}G_B(H_{BE}G_B)^{-1} \tag{12}$$

Substituting (4) into (12):

$$\Lambda = (H_{BE}G_B)QP(H_{BE}G_B)^{-1} \tag{13}$$

We can see from (13) that matrix Λ is similar to matrix QP and then they have the same characteristic polynomial (in a particular case the same eigenvalues and traces).

Because in [24] there were considered not necessary squared matrices it would be appropriate to prove "breaking of EVSKey Scheme" also for the case of n x m rectangular matrices H_{AB}, H_{BA}, H_{AE}, H_{BE}. Then first of all let us define inverse matrix to rectangular matrix D following Penrouse [26]:

$$D_P^{-1} = D^{\dagger}(DD^{\dagger})^{-1} \tag{14}$$

Then Eve computes the "attack" matrix:

$$\Lambda' = \widetilde{Y}_{A2}\left(\tilde{Y}_{B1}\right)_P^{-1}\widetilde{Y}_{B2}\left(\tilde{Y}_{A1}\right)_P^{-1},$$

where $\widetilde{Y}_{A1}$, $\widetilde{Y}_{A2}$, $\widetilde{Y}_{B1}$, $\widetilde{Y}_{B2}$ are rectangular matrices. Then substituting (9) into $\Lambda'$and taking into account (14) she gets the relation similar to (13) where inverse matrix can be found by (14).

Thus, we get the same "striking" confusion for rectangular matrices as for square ones.

The last statement results immediately in a conclusion that for noiseless channels EVSKey Scheme can be broken for any correlation between legitimate and eavesdropper channels!

But for noisy channels such conclusion is valid only partly because depends on SNR in eavesdropper channels. But we can see from Fig. 1 that noises in eavesdropper channels are determined not only by ones at the receiver side but also by noises N_{A1}, N_{B1} of legitimate users which may an opportunity to increase artificially noise power forming its lower bound for eavesdropper. Experiment with different SNR will be presented in the next section but so far let us face to key sharing procedures for legitimate users.

In order to provide a good key bit agreement between legitimate users it is very important strong correlation between channel matrices in the first and in the second steps of 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:

$$Y'_{A2} = H'_{BA}G_BH_{AB}G_AX_A, \qquad Y'_{B2} = H'_{AB}G_AH_{BA}G_BX_B \tag{15}$$

From the second equation in (15), there is no a matrix permutation of the first one and hence the matrices Y'_{A2} and Y'_{B2}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 cellular communication (LTE, 56) lies in a range of several hundreds meters. Coherence time for channels used in mobile unit communication is in range (1-10 ms) [27] 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_{A2}, Y_{B2} with matrices Y'_{A2}, Y'_{B2}.

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 [28].

3. Simulation results

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 4, where is presented also the number of key bits for different number of antennas n calculated by (8).

Table 4. Simulation results of the bit error probabilities (in percent) for extraction them from eigenvalues. Both numbers of phase and amplitude quantization intervals equal to8.

n / **SNR 1/α (dB)**	4	8	16
20	21.6	22	24
30	7.7	10	12
40	2.7	3.5	4
The number of extracted bits	19	33	52

n is the number of antennas.

We see from Table 4 that the acceptable SNR is at least 30 dB even for the case when we mean to use the 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 4.)

The generated key bits were investigated by NIST tests on pseudo randomness [29]. The list of NIST tests is presented in Table 5, while the results of testing on pseudo randomness in Table 6 with their numbering taken from Table 5.

In the same Table 6 there are presented also the results of NIST-based testing after a shifting right on the 20 bits and addition mod 2 with the original sequence.

Table 5. Listof NIST tests on pseudo-randomness

№	**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

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 7, 8. Comparing the results in Table 4 and Tables 7, 8 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.

Table 6. Results of NIST-based testing for the key bits sequence extracted from matrix eigenvalues under condition of 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 mod2**
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 7. 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

The key bits extracted from traces were investigated by the NIST tests given in Table 5. The results of testing are shown in Table 9 jointly with "shift and addition" transformation. We can

see from this Table that now an additional transform is not necessary. This means that this case is superior to extraction from eigenvalues with point of key statistic view. By comparing the results of Table 3 and Table 7, we conclude that the quantization procedure based on (6) is acceptable. This is valid also for the case of 4 and 8 antennas.

Table 8. Simulation results of the bit error probabilities P'(in percent) for extraction them from matrix eigenvalues with different sizes of quantization levels and antenna numbers

The number of antennas	**The number of sectors**	**The number of rings**	**The 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

Because it was demonstrated before that EVSKey Scheme cannot provide security against its interception by eavesdropper who is placed not necessary nearby to legitimate users there exists only one opportunity to provide security – to fix a lower bound on power of noise σ^2 at eavesdropper side. It can be achieved only by an artificially noise generation by legitimate users because such noises cannot be cancelled by eavesdroppers.

Let us consider a scenario where eavesdropper has nothing her noises, and legitimate users also haveN_{A2}=N_{B2}=0 but N_{B1}, $N_{A1} \neq 0$ when the power of last noises can be artificially increased.

The results of bit error probabilities (in percent) both for legitimate users P_l and eavesdropper $P_e$for such scenario are presented in Table 10. (It is worth to note that in this Table is considered a general case for rectangular $n \times m$ matrices).

We can see from this Table that for all matrix sizes and σ^2 the probabilities P_l occur larger than the probabilities P_e. This is not "dramatic" fact but it requires to perform some additional protocol that is considered in the next section.

Table 9. Results of NIST-based testing for the key bits extracted from matrix traces under condition of SNR = 30 db and also after a shifting and summation procedure

Test number	**Original one**	**After shift and summation mod2**
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

4. 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 4 and Tables 7, 8).

As we can see from Table 10 the error probabilities P_l for legitimate users occur in all selection of the parameters larger than the probabilities for eavesdropper. But the main positive property of this protocol is that the probabilities P_e cannot be decreased by any measures of eavesdropper because noise is created by legitimate users.

In order to provide reliable key sharing between legitimate users and simultaneously as small as desired leakage of information to eavesdropper, it is necessary to perform the so called public discussion and privacy amplification procedures [11, 30]. The first transforms a pair of probabilities (P_l, P_e) to a new pair of probabilities $(P_l, P_e' = P_l + P_e - 2P_lP_e)$ without any leakage some information on the shared key to eavesdropper. Regarding the second procedure it has been proved in [11, 30] that there exist such algorithms that provides as small as desired leakage of Shannon's information about the

key to eavesdropper and the key sharing rate (key capacity) be equal to the following value:

$$R = h(P_e') - h(P_l) \tag{16}$$

where $h(P) = -Plog_2P - (1-P)log_2(1-P)$.

It follows from (16) that parameters P_l, $P_e$should be selected in such a way to maximize R. For example, we can easy to compute using Table 10, that it we select matrix 8x10, σ^2 = 0.001, then R = 0.137. Unfortunately value R by (16) gives only capacity (e.g. potential upper bound) but in order to achieve this bound is unknown presently some constructive algorithm. The use of effective error corrective codes (like LDPC[31]) and hash function (or extractors) do not allow to get key rate very near to its capacity. Optimization of error correcting codes and calculation of achievable key rates requires further investigation.

5. 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.

Table 10. Simulation results of the bit error probabilities pl for legitimate users and eavesdropper (pe) (in percent) with different $n \times m$matrix sizes and different power (σ2) of noises na1, nb1

nx / m / σ2	4x4		4x6		4x12		8x8		8x10		8x24		16x16		16x24		16x48	
	Pl	Pe	Pl	Pe	Pl	Pe	Pl	Pe	Pl	Pe	Pl	Pe	Pl	Pe	Pl	Pe	Pl	Pe
1	40	36	39	34	33	26	37	34	37	33	31	27	34	33	31	31	27	24
10^{-1}	35	29	27	19	20	14	36	31	30	23	15	10	32	30	22	19	16	12
10^{-2}	21	15	10	8	6	3	26	18	15	11	5	3	26	21	11	9	6	4
10^{-3}	8	5	4	2	3	1	14	9	5	4	3.2	2	16	11	4	2.8	1.6	1.5
10^{-4}	3.0	1.8	1.1	0.7	0.5	0.3	3.2	1.8	1.3	0.8	1.5	0.7	7.7	5.1	1.0	0.8	0.5	0.3

We investigated how affect the parameters of key sharing protocol as the number of antennas, SNR in the legitimate channel and the method of quantization.

We have proved that EVSKey Scheme is in fact insecure for noiseless channels and any location of eavesdroppers even nearby to legitimate users where they have the same channel matrices. We proposed to generate artificial noise for eavesdropper that cannot be cancel. Then there exist protocol that provides both security and reliability of the shared key but selection of error correcting codes requires further investigation.

It is worth to note that the considered protocol does not require at all wireless fading channels and MIMO-based devices. Channel matrices H_{AB}, H_{BA} can be generated randomly by legitimate users and signals can be transmitted over noiseless channels with

constant parameter, say on Internet. This is also interesting area that requires further investigations.

Appendix

Proof of relation (7).

Let us consider an extraction of the key based on matrix traces. Assume that the entries of both channel matrices$P = \{p_{ij}\}, Q = \{q_{ij}\}$arerandom, mutual independent and identically distributed:$p_{ij}, q_{ij} \sim CN(0, \sigma_w^2)$, $i, j = 1,2, \dots k$. Similarly, these conditions hold and for noises:

$$N_1 = \left\{n_{ij}^{(1)}\right\}, N_2 = \left\{n_{ij}^{(2)}\right\}, n_{ij}^{(1)}, n_{ij}^{(2)} \sim CN(0, \sigma_e^2).$$

We admit also that channel matrices and noisy are mutual independent. Formula (3) entails

$$YX^{-1} = PQ + PN_1X^{-1} + N_2X^{-1}, \text{ and}$$
$$tr(YX^{-1}) = tr(PQ) + tr(PN_1X^{-1}) + tr(N_2X^{-1}).$$

It is easy to show that for large number of antennas ($n^2 \gg 1$) due to Central Limit Theorem, the random variables $Z_A = tr(Y_{A2}X_A^{-1})$, $Z_B = tr(Y_{B2}X_B^{-1})$are Gaussian distributed:

$$f_A(z) = f_B(z) = \frac{1}{\pi\sigma_z^2} e^{-\frac{|z|^2}{\sigma_z^2}}, \tag{A1}$$

where$\sigma_z^2 = DZ_A = DZ_{\mathrm{B}} = n^2\sigma_w^2(\sigma_w^2 + \sigma_e^2) + n\sigma_e^2$.

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

$$Z_B - E(Z_B) = \gamma\frac{\sigma_B}{\sigma_A}(Z_A - E(Z_A)), \tag{A2}$$

where

$$\gamma = \frac{cov(Z_A, Z_B)}{\sqrt{DZ_A DZ_{\mathrm{B}}}} \tag{A3}$$

is a correlation coefficient. Since $Z_A, Z_B$are centered random variables with equal variances, the equation of linear regression $Z_B$onto$Z_A$has a form

$$Z_B = \gamma Z_A. \tag{A4}$$

It is easy to show that$cov(Z_A, Z_B) = n^2\sigma_w^4$. Thus, we get

$$\gamma = \frac{n^2\sigma_w^4}{n^2\sigma_w^2(\sigma_w^2+\sigma_e^2)+n\sigma_e^2} = \frac{1}{1+\frac{\sigma_e^2}{\sigma_w^2}(1+\frac{1}{n\sigma_w^2})} \tag{A5}$$

Since the correlation coefficient γ is real-valued, it results that the random values Z_A, Z_Bdiffer by modulus only.If$n\sigma_w^2 \gg 1$ and a noise-to-signal ratio$\sigma_e^2/\sigma_w^2$is small then we get by(A5)

$$\gamma = \frac{1}{1+\alpha} \approx 1 - \alpha, \alpha = \frac{\sigma_e^2}{\sigma_w^2}(1 + \frac{1}{n\sigma_w^2}) \approx \frac{\sigma_e^2}{\sigma_w^2} \ll 1 \tag{A6}$$

Thus the dependence (A4) between Z_B and Z_A is almost linear.

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

$$P(r_{k-1} \le |z| < r_k) = p = \frac{1}{N}, k = 1,2, \dots, N. \quad \text{(A7)}$$

Using (A1) we are able to find radial distribution function of Z_A:

$$F(r) = P(|z| < r) = 1 - e^{-r^2/\sigma_z^2}.$$

Thus, we can see that (A7) holds if and only if

$$P(r_{k-1} \le |z| < r_k) = F(r_k) - F(r_{k-1}) = e^{-r_{k-1}^2/\sigma_z^2} - e^{-r_k^2/\sigma_z^2} = p.$$

It results the relation

$$F(r_k) = kp = 1 - e^{-r_k^2/\sigma_z^2}. \quad \text{(A8)}$$

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

Let us estimate now the key coincidence probability 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 dependence (A4) is almost linear $z_B \approx \gamma z_A$, where $0 < \gamma \le 1$, we get $|z_B| = \gamma|z_A|$. Hence

$$p_k = P\big((Z_A \in R_k)(Z_B \in R_k)\big) = P\left(\begin{cases} r_{k-1} \le |z_A| < r_k \\ r_{k-1} \le |z_B| < r_k \end{cases}\right).$$

$$\begin{aligned} p_k &\approx P\left(\begin{cases} r_{k-1} \le |z_A| < r_k \\ r_{k-1} \le \gamma|z_A| < r_k \end{cases}\right) \\ &= P\left(\begin{cases} r_{k-1} \le |z_A| < r_k \\ r_{k-1}/\gamma \le |z_A| < r_k/\gamma \end{cases}\right) = P(r_{k-1}/\gamma \le |z_A| < r_k). \end{aligned}$$

Using (A8), we find that

$$p_k = F(r_k) - F(r_{k-1}/\gamma) = e^{-\frac{r_{k-1}^2}{\gamma^2\sigma_z^2}} - e^{-\frac{r_k^2}{\sigma_z^2}} = (1-(k-1)p)^{1/\gamma^2} - (1-kp).$$

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

$$P' = \sum_{k=1}^{N} p_k = \sum_{k=1}^{N}\Big((1-(k-1)p)^{1/\gamma^2} - (1-kp)\Big). \quad \text{(A9)}$$

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 distribution (A1) is independent of "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.

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

[8] 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.

[9] 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

[10] 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.

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

[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.

[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. 41stAnnual 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,", International Journal of Computer Science and Application, 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. NewYork, Chichester, Brisbane: John Wiley & sons, 1968. ISBN 0-471-25711-7. [Online]. Available: http://opac.inria.fr/record=b1122219

[26] Ben-Israel, Adi; Greville, Thomas N.E. (2003), p. 7. Generalized inverses: theory and applications (2nded.). NY: Springer.
ISBN 0-387-00293-6

[27] T. Rappaport, Wireless Communications: Principles and Practice, 2nd ed. Upper Saddle River, NJ, USA: Prentice Hall PTR, 2001. ISBN0130422320

[28] D. Dasgupta, A. Roy, and A. Nag, Advances in User Authentication, 1st ed. Springer Publishing Company, Incorporated, 2017. ISBN 3319588060,9783319588063

[29] 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.

[30] 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.

[31] K. Shalkoska, Implementation of LDPC Algorithm: In C Programming Language. LAP LAMBERT Academic Publishing, 2017. ISBN 9783330026049.