Proceedings of the Federated Conference on Computer Science and Information Systems pp. 823–830
DOI: 10.15439/2016F85
ACSIS, Vol. 8. ISSN 2300-5963

Secret key agreement based on a communication through wireless MIMO fading channels

Victor Yakovlev and Valery Korzhik
State University of Telecommunications
Saint-Petersburg, Russia
Email: viyak@bk.ru, val-korzhik@yandex.ru

Pavel Mylnikov
Research & Design Institute
for Information Technology,
Signaling and Telecommunications
on Railway Transport (JSC NIIAS)
Saint-Petersburg, Russia
Email: paul.mylnikov@gmail.com

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

***Abstract*—The method of key sharing between a mobile unit and a base station through a wireless MIMO-based fading channel is investigated. The description of a key distribution protocol is given. The expression to estimate the correct key bit agreement based on the use of guard interval is proved. Statistical properties of the key string are tested using the NIST criteria. Impossibility of key string eavesdropping by illegal users is guaranteed due to small values of correlation between legal and eavesdropper carrier phases. Numerical examples show that the MIMO system with 8 antennas is able to agree 256 bits with a reliability value 0.99 for SNR equal to 35 dB. This experiment confirms that the MIMO scenario is especially effective for secret key distribution.**

***Index Terms*—MIMO fading channel, key distribution, multi-phase detection, correlation, NIST tests.**

I. Introduction

SECURE transmission is still a concern for wireless mobile devices due to broadcast nature of signals. Although traditional secure systems employ private or public-key cryptography independently of physical transmission, there is a growing interest in *physical layer security* methods that exploit noisy telecommunication channels and channels with multi-path wave propagation.

In a pioneered paper [1], Wyner introduced the *wire-tap channel concept* with two types of channels: the main channel (less noisy) and the wire-tap channel (more noisy). Wyner's theorem states that under some (not very strong conditions) there exist such encoding and decoding procedures that reliable transmission on the main channel and zero information leakage on the wire-tap channel can be provided with an increasing of the block lengths if the transmission rate is less than the so called *secrecy capacity Cs.* In the post-Wyner's period there appear a lot of paper devoted to a generalization of wire-tap channel models [2], [3], [4], [5], [6] and to a specification of the amount of information leaking to eavesdropper [7]. But unfortunately it is still unknown constructive encoding and decoding procedures providing a transmission rate close to secrecy capacity. Next advance in the physical security area occurs due to Maurer's paper [8] at the cost of public discussion between legitimate users. Such approach allows to share secret keys between legitimate users even in the case when the wire tapper observes a "better" channel than one used by the legitimate user but only if the wire tapper is passive (that is in another words if legal channel is authenticated). After a common key sharing the legitimate correspondents can use ideal Shannon's one-time pad cipher [9].

The idea of a common key sharing and the execution of an ideal cipher is very positive especially in the so called *post-quantum* period when it is assumed that many cryptographic algorithms can be broken by a quantum computer [10]. But such approach requires to share a very long secret key string before ideal encryption. Moreover, in order to provide a secure key sharing that means to get a negligible amount of Shannon information leaking to an eavesdropper about this key, it is necessary to be sure that signal-to-noise ratio at the input of wire tapper receiver is fixed and known for legitimate users. In order to avoid such strong requirement it has been proposed to execute (for mobile users) a multipath wave propagation in some wireless channels [11], [12]. Unfortunately if mobile unit stops it may result in a very slow and small channel fluctuation. In order to take for granted some given randomness level it would be better to create this randomness artificially by means of legitimate users. In [13] it has been proposed a method using smart antenna excited randomly by electronic means. More detail investigation of such approach was undertaken in [14]. But such approach requires a special construction of a *Variable Directional Antenna.*

The explosion of interest to multiple-input multiple-output (MIMO) systems soon led to a realisation that exploiting the available spatial dimensions can also enhance the secrecy capabilities of wireless channels [15].

One of advantage of MIMO system for key sharing is its property that a presence of many antennas results in a better randomisation even for very small transfer of mobile units. It is worth to note that in contrast to communication system where a presence of MIMO devices results in interference of signals at the receiving antennas, key sharing occurs avoidable of such interference because in that case it is necessary to form any but only coinciding key bits. The last property is provided thanks to the *Reciprocity Theorem of radio wave propagation* between

978-83-60810-90-3/$25.00

transmitting and receiving sides of MIMO-based link. Further investigation of MIMO-based *key distribution protocols (KDP)* was undertaken by authors of the papers [16], [17]. But a final solution of this problem is very far from a termination. First of all it is requested to increase the key generation rate providing simultaneously high secrecy and good statistical properties of the shared keys that should be close to truly random data. Namely these questions form the main subject of our investigations undertaken in the current paper.

The reminder of the article is organised as follows. Section II describes the model of MIMO channel with point of view key sharing protocol. In Section III algorithm of key distribution is presented jointly with estimation of key bits reliability and key rate generation. Section IV discusses system parameters optimisation. Section V concludes the paper and formulates open problems for further investigations. The appendix presents the proof of the relation for the error probability given in Section III.

II. Mathematical model of MIMO-based channel

We assume that a key distribution protocol (KDP) is performed between a mobile unit A and a base station B that have the same number of antennas N_A and that the signal power radiated of each antenna is equal to P_S/N_A.

For a *frequency-flat fading MIMO channel*, the commonly used discrete-time input-output relation for test-signal is given by

$$y = Hs + z \tag{1}$$

where H is a square $(N_A \times N_A)$-matrix, s is a transmitted test-signal $(N_A \times 1)$-vector, y is a received signal $(N_A \times 1)$-vector, and z is an additive noise $(N_A \times 1)$-vector of the MIMO channel output.

Due to the Reciprocity Theorem the relation for back channel is

$$y' = H^T s + z'.$$

However the elements of the matrix H can change during the test signal transmission, generally speaking, and therefore in order to provide approximated equally channel matrices in direct and back channels it is necessary that the following inequalities hold [18]:

$$\Delta t << T_c \quad , \quad \Delta f << B_c$$

where Δt is the delay in transmission between direct and back test signals, Δf is the frequency (Doppler) shift, T_c is the coherent time and B_c is the coherent band width for the MIMO channel.

In order to specify the values of the matrix H, it is necessary to describe the channel model in detail.

Let us consider the multi-path MIMO channel model with Raleigh fading according to [19] and presented in Fig. 1.

We denote the number of rays as L and denote by β_l the attenuation in the l-th ray, by ϕ_l, ψ_l the transmitted and received angles, respectively, by Φ, Ψ the antenna diagram angles, and by ω_l the frequency shift due to mobile units transfer (Doppler effect).

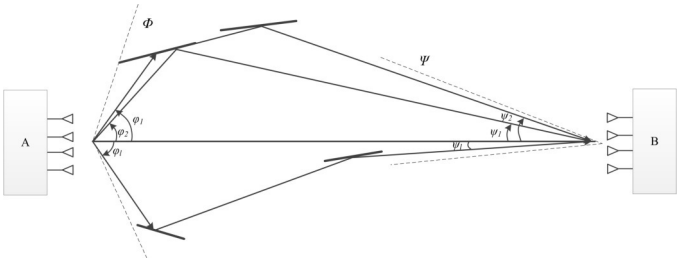


Fig. 1. General model of MIMO channel between mobile unit and base station.

Then the matrix $H(t)$ of the test signal at time t can be presented as

$$H(t) = \sum_{l=1}^{L} \beta_l \left(\mathbf{a}_{Rl}\mathbf{a}_{Tl}^T\right) e^{-j\omega_l t}$$

being

- $\beta_l = a_l e^{j\theta_l}$: signal attenuation resulting by reflection,
- $\mathbf{a}_{Rl}, \mathbf{a}_{Tl}$: response vectors at the receiver and at the transmitter respectively.

$$\begin{aligned} \mathbf{a}_{Rl} &= \left[1 \;\; e^{-j\Omega_{Rl}} \;\; \dots \;\; e^{-j(N_A-1)\Omega_{Rl}}\right]^T, \\ \mathbf{a}_{Tl} &= \left[1 \;\; e^{-j\Omega_{Tl}} \;\; \dots \;\; e^{-j(N_A-1)\Omega_{Tl}}\right]^T, \end{aligned}$$

- $\Omega_{Rl} = \frac{2\pi}{\lambda} d_R \sin\phi_l$: angular receiver frequency,
- $\Omega_{Tl} = \frac{2\pi}{\lambda} d_T \sin\psi_l$: angular transmission frequency,
- λ: wave length corresponding to carrier frequency,
- d_R: diversity interval for receiving antennas, and
- d_T: diversity interval for transmission antennas.

A typical example of the above channel model is the octal-rays model of the railway telecommunication system having 8 antennas with distances $\frac{\lambda}{2}$, between them, mobile object speed 100 km/h, $\Phi = 28°$, $\Psi = 180°$, and carrier frequency 2.6 GHz.

Investigation of such model has been undertaken in many papers (e.g. [20], [21] and others) and results of our investigations show that the entries of matrix H can be correctly approximated by zero mean Gaussian distribution with equal variances.

The space correlation is determined only by mutual antenna locations. Then space-time correlation can be presented following to the results of [22], [18] as

$$R_H(t) = R_H \cdot \rho(t),$$

where R_H is the matrix of space correlation between antennas, and ρ is the time correlation function of antenna location. For Jakes fading model [20], the function ρ can be determined as

$$\forall t: \;\; \rho(t) = J_0(2\pi f_D(t)),$$

where f_D is the Doppler spread and J_0 is the Bessel function of zero order.

III. KDP BASED ON MIMO CHANNEL MODEL

The KPD is described in the following steps:

1) User B (base station) sends the test signal to the mobile unit A executing all antennas.
2) A calculates some parameter of the received signals.
3) Just after step 2, A sends the same test signal to B.
4) B calculates the same (selected in advance by both users) parameters of the received signals.
5) Both users A and B form the key bits from the found parameters using a quantisation procedure.

It is worth to note that the knowledge of MIMO-based channel model parameters can be ignored in KDP design if during the time of its execution these parameters are approximately constant. But this knowledge it is necessary to estimate a reliability of KDP (the probability of key bits coincidence for both correspondents), the statistical properties of key strings and its security (in terms of information leakage about this key to eavesdropper who can be located in some vicinity of users A and B).

We can see from relation (1) that each coordinate y_i of the vector $\mathbf{y}$ is a complex Gaussian random value with amplitude $\mu_i = \sqrt{\Re(y_i)^2 + \Im(y_i)^2}$ (here $\Re$ and $\Im$ are the maps that take the real and the imaginary parts of a complex number) and phase $\theta_i = \tan^{-1}\left(\frac{\Im(y_i)}{\Re(y_i)}\right)$, and these variables have Rayleigh distribution and uniform distribution, respectively. It has been proved in [23] that phases are less correlated versus distance between legal users and eavesdroppers than amplitude. Therefore our selection as parameter for the key bit generation, namely the phase quantisation procedure into q integers, is determined as:

$$\begin{array}{rl} \text{if} & \theta_i \in \left[\frac{2\pi(q-1)}{Q}, \frac{2\pi q}{Q}\right) \text{ with } 1 \le q \le Q \\ \text{then} & f_Q(\theta_i) = q, \end{array} \tag{2}$$

where Q is the number of quantisation levels. Then the probability of an integer q equals $\frac{1}{Q}$. Since the channel noise results in a transition of q to $q' \neq q$ and it is more likely closer to the bounds of the decision areas in (2), we propose to introduce guard intervals between decision areas as key symbols may be erased. Then the decision function (2) can be modified as:

$$\begin{array}{rl} \text{if} & \theta_i \in \left((q-1)\Omega - \frac{\gamma}{2}, (q-1)\Omega + \frac{\gamma}{2}\right) \cup \\ & \left(q\Omega - \frac{\gamma}{2}, q\Omega + \frac{\gamma}{2}\right) \\ \text{then} & f_{QG}(\theta_i) = \textit{erasure}; \end{array}$$

$$\begin{array}{rl} \text{if} & \theta_i \in \left[(q-1)\Omega + \frac{\gamma}{2}, q\Omega - \frac{\gamma}{2}\right) \\ \text{then} & f_{QG}(\theta_i) = q; \end{array}$$

with $1 \le q \le Q$, $\Omega = \frac{2\pi}{Q}$ and γ a threshold, $\gamma \in \left[0, \frac{1}{2}\Omega\right)$.

Let us consider one of the decision areas (or *sector*) in Fig. 2, determined by $\mathbf{y}_i = (\mu_i, \theta_i)$, $\mathbf{x}_i = Hs = (a_i, \phi_i)$, $\mathbf{z}_i = (b_i, \psi_i)$. Under the decision taken about the phase ϕ_i when $\mathbf{y}_i$ is received, the following events may occur:

- $\mathbf{y}_i$ is in the same area that the vector $\mathbf{x}_i$ (correct decision area with angle $\Omega - \gamma$),

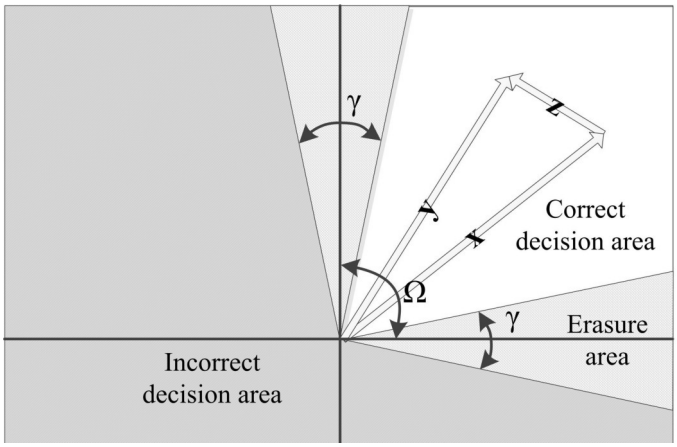


Fig. 2. Sectors of decision area.

- $\mathbf{y}_i$ belongs to the guard interval (erasure area with angle γ),
- $\mathbf{y}_i$ appears outside of both previous areas (incorrect decision).

Let us denote the probabilities of previous events by P_{cor}, P_{er}, P_{error}, respectively.

It is proved in the Appendix that

$$\begin{aligned} P_{error} &= \frac{1}{2\pi\Omega}\int_0^{\Omega} F(\phi)\, d\phi \\ F(\phi) &= \int_{\phi+\frac{\gamma}{2}}^{2\pi-(\phi+\frac{\gamma}{2})} \left[1 + \left[\frac{h\tan\left(\phi+\frac{\gamma}{2}\right)}{\sin\psi}\right]^2\right]^{-1} d\psi \\ P_{er} &= 1 - P_{cor} - P_{error} \end{aligned} \tag{3}$$

where P_{cor} is given by eq. (16) in the Appendix after combining (11)–(15).

In Fig. 3 there are plotted the dependences of P_{cor}, P_{er}, P_{error} with respect to signal to noise ratio for $Q = 8$ and different *guard intervals* (GI) that were calculated after numerical computations of corresponding integrals. We observe that it is possible to trade off P_{error} to the value of the guard interval but it affects also on P_{er}. Hence there appears the problem of KDP parameters optimisation, given some final requirements, as key generation rate maximisation for given SNR and the number of antennas N_A in MIMO system. (We remark that it is not obtained a precise expression for the corresponding probabilities but some bounds, namely an upper bound for P_{error}, a lower bound for P_{er} and lower bound for P_{cor} because it was not taken into account that correct key bits can be obtained sometimes even if both legal users got incorrect phase. But such incorrectness is acceptable).

From Fig. 3, it can be seen that a guard interval (GI) allows to decrease the error probability but simultaneously the probability of erasure increases. In reality a final decision about key bit has to be taken no by the single user B but by

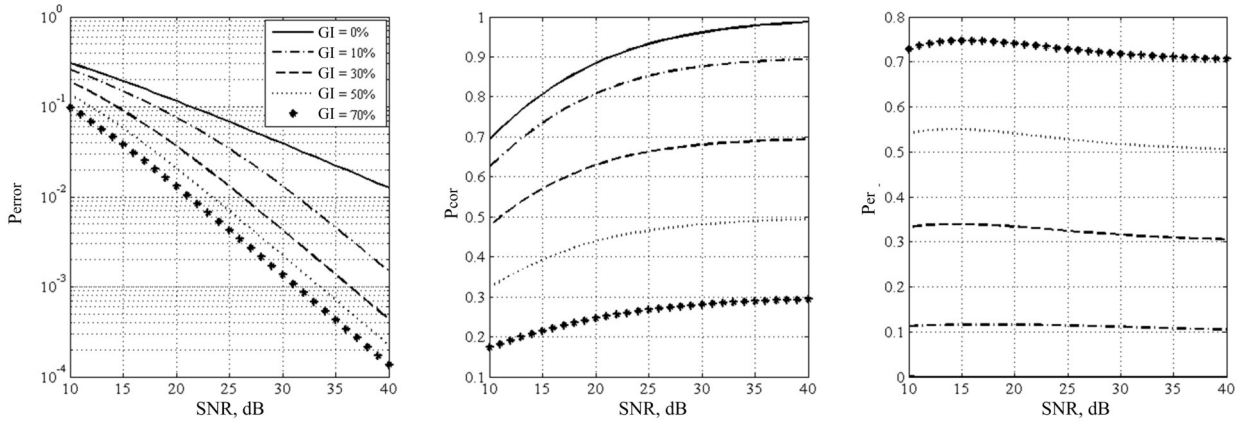


Fig. 3. Curves of P_{error}, P_{cor}, P_{er} against the values of SNR for $Q = 8$.

both users A and B. Thus the final probabilities P_{cor}, P_{er}, P_{error} should be changed as follows:

$$\begin{aligned} P^*_{cor} &= P_{cor}(A) \cdot P_{cor}(B) \\ P^*_{error} &= P_{error}(A) \cdot P_{cor}(B) + \\ &\quad P_{error}(B) \cdot P_{cor}(A) + \\ &\quad P_{error}(A) \cdot P_{error}(B) \\ P^*_{er} &= 1 - P^*_{cor} - P^*_{error} \end{aligned}$$

The KDP should be also slightly corrected under the condition of symbol erasures. Namely the numbers of the erased symbols have to be transmitted from both users to opposite ones in addition and next it is transmitted extra signal if it is necessary.

A relation for the probability $P_{n_0}(k)$ of the key bit string sharing of length n_0 is:

$$P_{n_0}(k) = \left(\frac{P^*_{cor}}{1 - P^*_{er}} \right)^{\frac{n_0}{\log Q}} \tag{4}$$

where Q is the number of quantisation levels. The key bit stream rate for the use of all N_A antennas is

$$R = N_A \log_2 Q (1 - P^*_{er}) \frac{bit}{sample}. \tag{5}$$

Then the following optimisation problem arises:

$$(\gamma^*, Q^*, N^*_A, (h^2)^*) = \underset{\gamma, Q, N_A, h^2}{\arg\max}\ R \tag{6}$$

subject to the restrictions

$$\begin{gathered} P_{n_0}(k) \geq P_{n_0}(k)_{\text{requested}}; \\ \gamma \in \left[0, \tfrac{\pi}{Q}\right); \\ Q \in [2, Q_{\max}]; \\ N_A \in [1, (N_A)_{\max}]; \\ h^2 \in [1, (h^2)_{\max}]; \end{gathered}$$

where the values $P_{n_0}(k)_{\text{requested}}$, $Q_{\max}$, $(N_A)_{\max}$, $(h^2)_{\max}$ have to be conditioned by the general requirements of the MIMO system design.

The solution of problem (6) has been found by the *branch and bound algorithm* [24].

In Fig. 4 there are presented the dependences R from SNR under the conditions $n_0 = 256$, $P_{n_0}(k)_{\text{requested}} = 0.9$ and 0.99, and $N_A = 1, 2, 4, 8, 16$.

In Table I the optimal values for $a = \frac{\gamma}{\Omega}$ and Q are displayed maximising the rate R for a given SNR.

An analysis of the curves in Fig. 4 shows that the key generation rate R increases with an increasing of the number of antennas in MIMO massive. Key generation rate increases obviously as SNR increases. For every SNR value there exist optimal number of phase quantisation levels and value of guard interval providing the requested probability of correct key sharing for both legal users.

IV. Investigation of Key Stream Statistic and Information Leaking to Eavesdropper

The statistics of the key stream distributed due to KDP is very important because if it is very far from uniform distribution it may result in effective attacks for cipher breaking. In order to investigate the key stream statistic after phase quantisation from different antennas they will be combined in a serial sequence containing bits from all antennas and this sequence investigated by statistical tests. In Fig. 5 there are presented the empirical density distributions for the length of binary strings equal to 1 and 16.

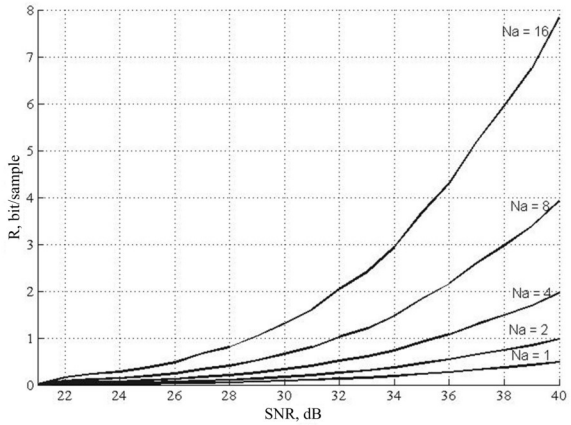
We see there that also a balance of zeros and ones (as follows from Fig. 5 a) is good, but the multi-variate distribution (Fig. 5 b) has anomalous peaks. In order to improve the statistics of the key string it was undertaken some deterministic transforms of two types recommended in [25]. The first type is so called *transposition of symbols* and the second transform is *adjacent bit XOR-ing*. The results of testing after such transforms are presented in Table II in which were used some NIST STS tests [26].

We see that after both transforms the key bit sequence passes the most of NIST tests.

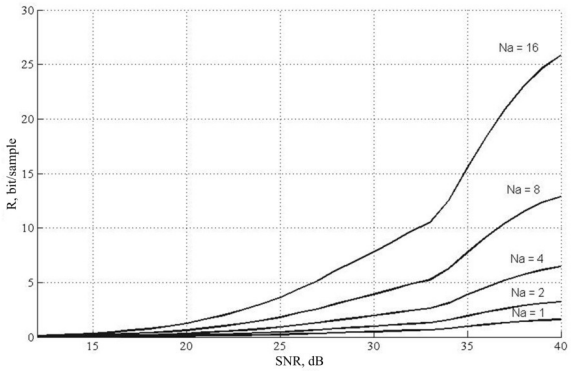
Now let us face with eavesdropping problem and assume that the following parameters hold [21]:

TABLE I
OPTIMAL PARAMETERS γ AND Q PROVIDING THE MAXIMUM RATE R FOR A GIVEN SNR.

$P_{n_0}(k)_{\text{requested}}$		SNR (dB)															
		10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40
0.9	Q^*	–	2	2	2	2	2	2	2	2	2	2	2	4	4	4	4
	a^*	–	0.89	0.86	0.82	0.77	0.71	0.64	0.56	0.47	0.38	0.30	0.22	0.37	0.24	0.15	0.10
0.99	Q^*	–	–	–	–	–	–	2	2	2	2	2	2	2	2	2	2
	a^*	–	–	–	–	–	–	0.89	0.86	0.82	0.77	0.71	0.64	0.57	0.48	0.39	0.30

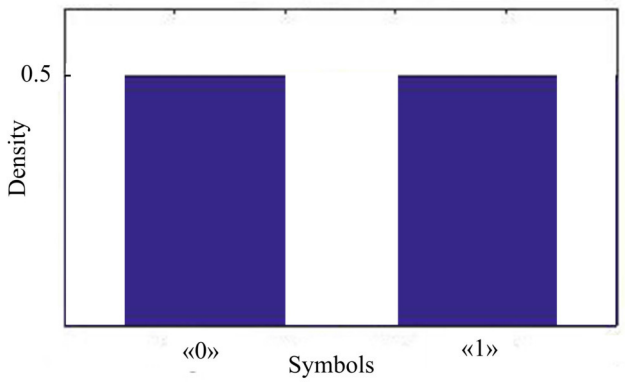


a) $P_{n_0}(k)_{\text{requested}} = 0.9$

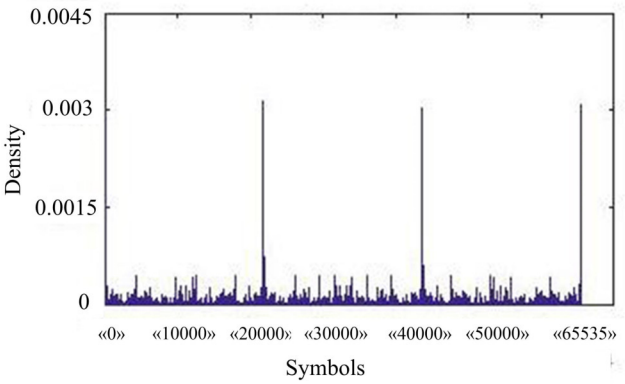


b) $P_{n_0}(k)_{\text{requested}} = 0.99$

Fig. 4. The key sharing bit rate of the length 256 bits with $P_{n_0}(k)_{\text{requested}} \in \{0.9, 0.99\}$ for optimisation of the system parameters.



a) String length 1



b) String length 16

Fig. 5. Empirical probability density distributions for two string lengths.

- frequency carrier: 2600 MHz;
- MIMO massive: 8×8;
- distance between MIMO antennas at the departure unit: 0.5λ
- distance between MIMO antennas at the arrival unit: 0.5λ
- number of rays: 8;
- departure ray angle: 28°;
- arrive ray angle: 180°;
- speed of mobile unit motion: 50 km/h;
- number of simulated channel matrices: 1000.

The mutual correlation between the phases of legal user B and an eavesdropper located at a distance d from B (in terms of wave length factors) is presented in Fig. 6.

We see from this figure that in line with similar results presented in [14] the correlation has not a monotonically decreasing dependence from d but it has a randomly-looking dependence. But in contrast to [14] it has significantly less values from all distances between $(0.1\lambda, \ldots, 20\lambda)$. This is a consequence of the multi-phase functional used for key bit generation and another channel model. Thus, we can believe that it can be neglected an opportunity of key eavesdropping

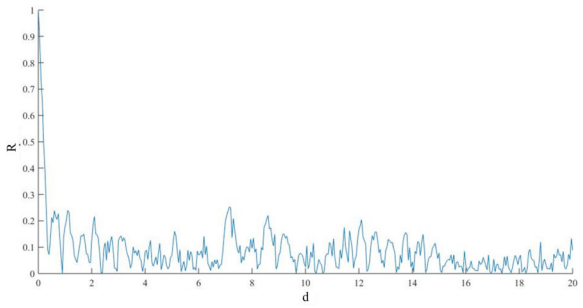


Fig. 6. Mutual correlation between phases of legal user and eavesdropper against distance between them in terms of wave length factors.

TABLE II
EXPERIMENTAL TESTING BASED ON NIST STS OF THE KEY SEQUENCES AFTER TWO TYPES OF TRANSFORMS.

Nr.	Name of test	Transposition	TXOR
1	The Frequency (Monobit) Test	10/10	10/10
2	Frequency Test within a Block	10/10	10/10
3	The Runs Test	9/10	10/10
4	Tests for the Longest-Run-of-Ones in a Block,	0/10	10/10
5	The Binary Matrix Rank Test	10/10	10/10
6	The Discrete Fourier Transform (Spectral) Test	0/10	9/10
7	The Non-overlapping Template Matching Test	1/10	8/10
8	The Overlapping Template Matching Test	0/10	10/10
9	Maurer's "Universal Statistical" Test	10/10	10/10
10	The Linear Complexity Test	5/5	7/7
11	The Serial Test	5/5	7/7
12	The Approximate Entropy Test	0/10	10/10
13	The Cumulative Sums (Cusums) Test	3/10	10/10
14	The Random Excursions Test	1/10	10/10
15	The Random Excursions Variant Test	10/10	10/10

TXOR: Transposition plus XOR of adjacent bits.
The numerators of fractions are number of "passed" tests and the denominators are the total number of tests.

in large area of eavesdropper locations.

(It is worth to note that if phase had Gaussian distribution and even for binary quantisation values it would be results in the error probability for eavesdropper about one key bit near 0.47 [14] that it is very close to "break of eavesdropper channel".)

V. CONCLUSION

We considered a method of key sharing for wireless secret communication based on MIMO concept with the use of multi-phase functionals that seems to be especial effective for mobile unit and multi-path fading channels.

It has been proved that following to the proposed key distribution protocol it can be provided a key sharing of size 256 bits and with probability of its reliable performance about 0.99 for SNR equal to 35 dB, and 16 antennas after execution of about 74 test signals on average. It was also shown that the key sequence after simple transforms is very close to i.i.d. practically satisfying all NIST tests. Interception of key stream by eavesdropper is prevented by a very small correlation between phases at legal users and eavesdropper if distance between them is not lesser than 0.1λ.

We believe that a future work that can be undertaken is in the use of error correcting codes in order to maximise the key distribution rate and to short a delay in key delivering.

REFERENCES

[1] A. Wyner, "Wire-tap channel concept," *Bell System Technical Journal*, vol. 54, pp. 1355–1387, 1975.
[2] A. B. Carleial and M. E. Hellman, "A note on Wyner's wiretap channel (corresp.)," *IEEE Trans. Information Theory*, vol. 23, no. 3, pp. 387–390, 1977. [Online]. Available: http://dx.doi.org/10.1109/TIT.1977.1055721
[3] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Information Theory*, vol. 24, no. 4, pp. 451–456, 1978. [Online]. Available: http://dx.doi.org/10.1109/TIT.1978.1055917
[4] I. Csiszár and J. Körner, "Broadcast channel with confidential messages." *IEEE Transactions on Information Theory*, vol. 24, no. 2, pp. 339–348, 1978.
[5] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," 1985, pp. 33–50.
[6] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *IEEE International Symposium on Information Theory*. IEEE, 2006, pp. 356–360.
[7] V. I. Korzhik and V. Yakovlev, "Nonasymptotic estimation for efficiency of code jamming for the wire-tape channel concept (In Russian)," *IEEE Transactions on Information Theory*, vol. 17, no. 4, pp. 223–228, 1981.
[8] U. Maurer, "Secret key agreement by public discussion from common information." *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, 1993.
[9] C. E. Shannon, "Communication theory of secrecy systems," *Bell Systems Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.
[10] D. Micciancio and O. Regev, "Lattice-based cryptography," in *Post-quantum Cryptography*, D. J. Bernstein and J. Buchmann, Eds. Springer, 2008.
[11] A. M. Sayeed and A. Perrig, "Secure wireless communications: Secret keys through multipath," in *ICASSP*, 2008, pp. 3013–3016.
[12] Y. Liu, S. C. Draper, and A. M. Sayeed, "Secret key generation through ofdm multipath channel," in *CISS*, 2011, pp. 1–6.
[13] 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.
[14] 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.
[15] 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
[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, pp. 905–910.
[17] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *International Symposium on Information Theory, 2007. ISIT 07.*, June 2007.
[18] E. Biglieri, R. Calderbank, A. Constantinides, A. Goldsmith, A. Paulraj, and H. V. Poor, *MIMO Wireless Communications*. New York, NY, USA: Cambridge University Press, 2007.
[19] H. Yigit and A. Kavak, "Analytical derivation of 2×2 MIMO channel capacity in terms of multipath angle spread and signal strength," *Frequenz*, vol. 66, no. 1, pp. 97–100, 2012.
[20] W. C. Jakes and D. C. Cox, *Microwave Mobile Communications*. Wiley-IEEE Press, 1994.

[21] K. Guan, Z. Zhong, and B. Ai, "Assessment of LTE-R using high speed railway channel model." in *CMC*, D. Yuan, M. Cao, C.-X. Wang, and H. Huang, Eds. IEEE Computer Society, 2011, pp. 461–464. [Online]. Available: http://dblp.uni-trier.de/db/conf/ieeecmc/ieeecmc2011.html#GuanZA11

[22] M. Bakulin, L. Varukina, and V. Krejdelin, *Tehnologija MIMO: principy i algoritmy*. Gorjachaja linija–Telekom, 2014.

[23] V. Yakovlev, V. Korzhik, and Y. Kovajkin, "Key sharing protocol for wireless local area networks based on the use of randomly excited antenna with variable diagram under the condition of multipath wave propagation. part 1. channel model for key sharing based on the use of smart antenna," in *Problemy informacionnoi bezopasnosti. Komp'juternye sistemy, SPb.: SPbGTU*, June 2011.

[24] A. H. Land and A. G. Doig, "An automatic method of solving discrete programming problems," *Econometrica*, vol. 28, no. 3, pp. 497–520, 1960. [Online]. Available: http://jmvidal.cse.sc.edu/library/land60a.pdf

[25] B. Schneier, *Applied Cryptography (2Nd Ed.): Protocols, Algorithms, and Source Code in C*. New York, NY, USA: John Wiley & Sons, Inc., 1995.

[26] 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.

[27] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products*, 7th ed. Elsevier/Academic Press, Amsterdam, 2007, translated from the Russian, Translation edited and with a preface by Alan Jeffrey and Daniel Zwillinger, With one CD-ROM (Windows, Macintosh and UNIX).

APPENDIX

Proof of the formula (3)

Let us consider one of the decision areas, namely $\angle\text{TOL} = \Omega$ (see Fig. 7). Assume that the vector $\mathbf{y}$ is in the sector $\angle\text{SOX}$ (area D_1') and that it is a sum of the vectors $\mathbf{x}$ and $\mathbf{z}$. Then the error for taking a decision on the phase of $\mathbf{y}$ occurs if $\mathbf{y}$ lays on the axis OS or at left to it. This event will occur if and only if:

$$\angle\text{BOA} \geq \angle\text{SOA} = \Omega - \phi + \frac{\gamma}{2}. \tag{7}$$

Let us draw the perpendicular from the point B on the axis OX. Then $\text{BC} = b\sin(\pi - \psi) = b\sin\psi$, $\text{AC} = -b\cos\psi$. We have

$$\angle\text{BOA} = \tan^{-1}\left(\frac{\text{BC}}{a - \text{AC}}\right) = \tan^{-1}\left(\frac{b\sin\psi}{a + b\cos\psi}\right). \tag{8}$$

where a is the amplitude of vector $\mathbf{x}$, and b is the amplitude of vector $\mathbf{z}$. By substituting (8) into (7) we get

$$\frac{b\sin\psi}{a + b\cos\psi} \geq \tan\left(\Omega - \phi + \frac{\gamma}{2}\right).$$

If $a >> b$ (which is very likely) then the term $b\cos\psi$ can be neglected and it results in the following condition to produce error:

$$u := \frac{b}{a} \geq \frac{\tan\left(\Omega - \phi + \frac{\gamma}{2}\right)}{\sin\psi} =: \ell_{\Omega-\phi,\psi}.$$

Let us denote by $P(u)$ the probability density of the random variable u. Then the error probability (P_{error}), provided that the received vector $\mathbf{y}$ lies at the left of OS, can be expressed by the following formula, on the assumption that phases ϕ and ψ are distributed uniformly:

$$P^{I}_{error} = \frac{1}{\Omega}\int_0^{\Omega} d\phi\,\frac{1}{2\pi}\int_{\Omega-\phi+\frac{\gamma}{2}}^{\pi} d\psi \int_{\ell_{\Omega-\phi,\psi}}^{+\infty} f(u)\,du \tag{9}$$

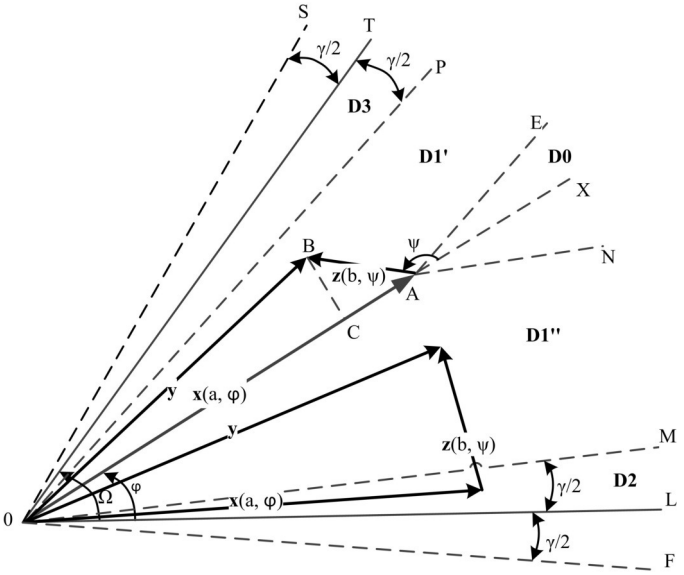


Fig. 7. Areas for taken of decision after quantisation.

(the superindex I emphasises that it is true whenever the received vector occurs to the left of line OS).

For the area $\text{D1}'' = \angle\text{LOX}$, we can repeat the derivation of (9) in order to get

$$P^{II}_{error} = \frac{1}{\Omega}\int_0^{\Omega} d\phi\,\frac{1}{2\pi}\int_{\pi}^{2\pi-\phi-\frac{\gamma}{2}} d\psi \int_{\ell_{\phi,\psi}}^{+\infty} f(u)\,du \tag{10}$$

Let us specify the formula for the probability of correct decision after quantisation and introducing of guard interval. We can see such areas at Fig. 7. Having received the vector $\mathbf{y}$ we get the following cases:

1) $\mathbf{x} \in \text{D1}, \mathbf{y} \in \text{D1}$, with $\text{D1} = \text{D1}' \cup \text{D1}''$. After repeating the procedure to obtain (9) and (10), we get

$$P_{cor\,\text{D1}} = \frac{1}{\Omega}\int_{\frac{\gamma}{2}}^{\Omega-\frac{\gamma}{2}} d\phi\,\frac{1}{2\pi}\int_{\phi-\frac{\gamma}{2}}^{2\pi-\phi+\frac{\gamma}{2}} d\psi \cdot \int_0^{\ell_{\phi,-\psi}} f(u)\,du \tag{11}$$

2) $\mathbf{x} \in \text{D2} \cup \text{D3}, \mathbf{y} \in \text{D1}$, with $\text{D1} = \text{D1}' \cup \text{D1}''$. After repeating the procedure to obtain (9) and (10), we get

$$P_{cor\,\text{D2}\cup\text{D3}} = \frac{1}{\Omega}\int_{\Omega-\frac{\gamma}{2}}^{\frac{\gamma}{2}} d\phi\,\frac{1}{2\pi}\int_{\phi-\frac{\gamma}{2}}^{2\pi-\phi+\frac{\gamma}{2}} d\psi \cdot \int_{\ell_{-(\Omega-\phi),\psi}}^{\ell_{\phi,-\psi}} f(u)\,du \tag{12}$$

3) $\mathbf{x} \in \text{D1}, \mathbf{y} \in \text{D0}$. In such situation the vector $\mathbf{x}$ transfers to the area of correct decision from the area of erasure due to noise.

$$P_{cor\,\text{D0}} = \frac{1}{\Omega}\int_{\frac{\gamma}{2}}^{\Omega-\frac{\gamma}{2}} d\phi\,\frac{1}{2\pi}\int_0^{\Omega-\gamma} d\psi \int_0^{+\infty} f(u)\,du = \frac{(\Omega-\gamma)^2}{2\pi\Omega} \tag{13}$$

4) $\mathbf{x} \in$ D2, $\mathbf{y} \in$ D0 (in this case, D2 and D0 are intersected)

$$P_{cor\,\mathrm{D2}\to\mathrm{D0}} = \frac{1}{\Omega}\int_0^{\frac{\gamma}{2}} d\phi\,\frac{1}{2\pi}\int_{\frac{\gamma}{2}}^{\Omega-\frac{\gamma}{2}} d\psi\,\cdot \int_{\ell_{-\phi,\psi}}^{+\infty} f(u)\,du \tag{14}$$

5) $\mathbf{x} \in$ D3, $\mathbf{y} \in$ D0. It is easy to see that

$$P_{cor\,\mathrm{D3}\to\mathrm{D0}} = P_{cor\,\mathrm{D2}\to\mathrm{D0}} \tag{15}$$

Combining (11)–(15) we get:

$$P_{cor} = P_{cor\,\mathrm{D1}} + P_{cor\,\mathrm{D2}\cup\mathrm{D3}} + P_{cor\,\mathrm{D0}} + 2\,P_{cor\,\mathrm{D2}\to\mathrm{D0}} \tag{16}$$

It is very easy to see that

$$P_{erasure} = 1 - P_{cor} - P_{error}.$$

In order to prove the relations (9)–(14) in a closed form it is necessary to derive the probability density function of the random variable $u = \frac{b}{a}$, where a and b have the Rayleigh distribution and they are mutually independent. This means that

$$f(a) = \begin{cases} \frac{a}{\sigma_a^2} e^{-\frac{a^2}{2\sigma_a^2}} & \text{if } a \geq 0 \\ 0 & \text{if } a < 0 \end{cases}$$

$$f(b) = \begin{cases} \frac{b}{\sigma_b^2} e^{-\frac{b^2}{2\sigma_b^2}} & \text{if } b \geq 0 \\ 0 & \text{if } b < 0 \end{cases}$$

After a simple transform, we get the following relation

$$f(u) = \frac{u}{\sigma_a^2\sigma_b^2}\int_0^{+\infty} a^3 e^{-ra^2}\,da, \tag{17}$$

where $r = \frac{1}{2\sigma_a^2} + \frac{u^2}{2\sigma_b^2}$.

The integral (17) can be expressed in a closed form [27]. Then for the definite integral (17) we get

$$f(u) = \frac{2\sigma_a^2\sigma_b^2\,u}{(u\sigma_a^2 + \sigma_b^2)^2}. \tag{18}$$

By denoting $\delta^2 = \frac{\sigma_b^2}{\sigma_a^2}$ then we get from (18)

$$f(u) = \frac{2\delta^2\,u}{(\delta^2 + u^2)^2}. \tag{19}$$

Substituting (19) into (9) and (10) we obtain

$$P_{error} = \frac{1}{2\pi\Omega}\int_0^{\Omega} d\phi\int_{\phi+\frac{\gamma}{2}}^{2\pi-\phi-\frac{\gamma}{2}} d\psi\,\cdot \int_{\ell_{\phi,\psi}}^{+\infty} \frac{2\delta^2\,u}{(\delta^2+u^2)^2}\,du \tag{20}$$

Last integral in (20) can be expressed in a closed form:

$$\int \frac{2\delta^2\,u}{(\delta^2+u^2)^2}\,du = -\frac{\delta^2\,u}{\delta^2+u^2}.$$

Then we get for the definite integral

$$\int_V^W \frac{2\delta^2\,u}{(\delta^2+u^2)^2}\,du = \left[\frac{1}{1+(hV)^2} - \frac{1}{1+(hW)^2}\right] \tag{21}$$

where $h = \frac{1}{\delta}$ is the signal-to-noise ratio.

Substituting (21) into (20) we get finally

$$P_{error} = \frac{1}{2\pi\Omega}\int_0^{\Omega} d\phi\,\cdot \int_{\phi+\frac{\gamma}{2}}^{2\pi-\phi-\frac{\gamma}{2}} \left[1 + \left[\frac{h\tan\left(\phi+\frac{\gamma}{2}\right)}{\sin\psi}\right]^2\right]^{-1} d\psi$$

Q.E.D