Secret Key Agreement Over Multipath Channels Exploiting a Variable-Directional Antenna

Valery Korzhik, Viktor Yakovlev,Yuri Kovajkin
State University of Telecommunication
St. Petersburg, Russia

Guillermo Morales-Luna
Computer Science Department
CINVESTAV-IPN
Mexico City, Mexico

***Abstract*—We develop an approach of key distribution protocol(KDP) proposed recently by T.Aono et al., where the security of KDP is only partly estimated in terms of eavesdropper's key bit errors. Instead we calculate the Shannon's information leaking to a wire tapper and we also apply the privacy amplification procedure from the side of the legal users. A more general mathematical model based on the use of Variable-Directional Antenna (VDA) under the condition of multipath wave propagation is proposed. The new method can effectively be used even in noiseless interception channels providing thus a widened area with respect to practical applications. Statistical characteristics of the VDA are investigated by simulation, allowing to specify the model parameters. We prove that the proposed KDP provides both security and reliability of the shared keys even for very short distances between legal users and eavesdroppers. Antenna diversity is proposed as a mean to enhance the KDP security. In order to provide a better performance evaluation of the KDP, it is investigated the use of error correcting codes.**

Keywords-wireless communication; wave propagation; cryptography; key distribution.

I. Introduction

The problem of key distribution is still in focus of research activity especially for wireless LAN systems. This is due to the severe restriction of asymmetric (public key) cryptography WLAN implementation entailing a lower processing speed.

In order to solve this problem, quantum cryptography [1] which allows eavesdropping detection within the key sharing procedure seems useful. However, this approach does not reach a practical level due to many technical problems, such as the requirement of special quantum devices. There are well known key distribution protocols (KDP) based on the presence of noise in both legal and illegal channels [2], [3], [4]. But even though the eavesdropper's channel is less noisy than the legal ones and the eavesdroppers is passive, it is necessary to have the knowledge of the eavesdropper's noisy power in order to guarantee a fixed level of key security. Unfortunately this condition cannot be taken for granted because an eavesdropper may be able to get some advantage at the cost of better receiver sensitivity or a shorter distance of interception that it was considered by legal parties in the design of the secure KDP.

The most basic assumption on the executed KDP is that the legal and illegal users have different locations, and this fact has to be verified by physical means. (For that matter, an existing special zone surrounding each legal user shall be assumed where the presence of an eavesdropper is not allowed.)

This assumption is sufficient for secure key distribution if either the communication channel between the legal users and the eavesdropper have random parameters or one legal user generates some randomness, under the condition that this randomness is transmitted to other legal users over multipath channels and any eavesdropper is able to receive this information only on a multipath channel, but with some other parameters, due to different locations of the legal users and the eavesdropper.

The first approach is considered in [5], [6] for multipath channels with random parameters and in [7], [8] for ultra-wide band channels with random pulse responses. But the randomness exploiting of the fluctuation of channel parameters is very questionable because there may be such channel states in which a temporal variation of propagation characteristics is slow and small. In order to take for granted some given randomness level it would be better to create artificially this randomness by means of legal users.

Let us consider the following mathematical model of the channels between a source of randomness (the first legal user) and both the second legal user and the eavesdropper:

$\eta = \sum_{i=1}^{m} x_i \xi_i, \quad \zeta = \sum_{i=1}^{m} y_i \xi_i,$ where $\xi = (\xi_i)_{i=1}^{m}$ is the vector randomness, $x = (x_i)_{i=1}^{m}$ is the coefficient vector of the multipath propagation to the second legal user, and $y = (y_i)_{i=1}^{m}$ is the coefficient vector of multipath propagation to the eavesdropper. Let us assume for simplicity E(ξ)=0, then the following relation for the correlation coefficient between η and ζ results:

$$\rho(\eta, \zeta) = \frac{x^T R_\xi y}{\sqrt{(x^T R_\xi x)(y^T R_\xi y)}},$$

where R_ξ is correlation matrix of the random vector ξ. In a general case $\rho(\eta,\zeta) \leq 1$. Moreover if x and y are orthogonal, (e.g.$\langle x, y \rangle = 0$) and $R_\xi = \mathrm{Id}_m$ is the $(m \times m)$-identity matrix, then $\rho(\eta, \zeta) = 0$.

The key bits of the second legal user can be generated after multiple repetition of the random independent vector (ξ) and the binary quantization of the random values (η). The first legal user can form key bits in a similar manner after a signal reception from the second user over the same multipath channel with the same randomness. If the variables η and ζ are Gaussian and non-correlated, then the shared key is provided secure due to the statistical independence of the variables. (A more general situation with non-zero correlation is considered in Section II.)

Common randomness can result from fluctuation of the cannel characteristics due to communicating object motion. Such approach has been proposed in [9], [10], [11]. But it still entails another problem: it is easy to break the secret key under an environment with small fluctuation of the channel characteristics or in the case when the communicating objects are stopped. In order to overcome these defects, a more sophisticated method, using smart antenna excited randomly by electronic means [12], has been proposed (although their results were obtained experimentally without an estimation of information-theoretic security of the shared keys).

This direction has been developed in many papers, [13], [14], [15], [16] are among the most important. In [14] some additional interference signals are simultaneously transmitted from the auxiliary antenna at legitimate access point. The authors of [13] change slightly the KDP based on Variable Directional Antenna (VDA) at the cost of a special selection of appropriate RSSI values in order to improve the key distribution security. In [15], an experimental scheme with the execution of dipole antennas was introduced. Such criterion of KDP security as Information Mutual Anti-tapping Condition (IMac) has been proposed in [16] but it was not proved that the IMac correctly estimates the security of KDP.

It is worth to note that in all above mentioned papers, there has not been considered the use of Privacy Amplification (PA) of the raw key bit strings and the application of the Privacy Amplification Theorem in order to correctly estimate the amount of Shannon's information leaking to an eavesdropper, although it is a very common technique used in the execution of different KDP [2], [3], [4], [17], [18], [19].

Our contribution consists first of all in an application of PA to VDA-based KDP that allows restricting reasonably the values of the required correlations between samples of legal users and eavesdroppers which are used for key bit generation. But in order to come closer to this main problem we have to solve a number of particular problems. The first attempt of such approach has been presented in [20].

In Section II, we describe the conditions of the physical channel and we introduce an exact mathematical model of the KDP. The results of the VDA simulation are presented in Section III. Section IV contains an optimization of the KDP in order to provide both reliability and security. Finally we conclude the main results and present some open problems in Section V.

II. KDP Based On Multipatch Wave Propagation And Randomly Excited VDA

The scheme of the communication system corresponding to the KDP is presented in Fig. 1.

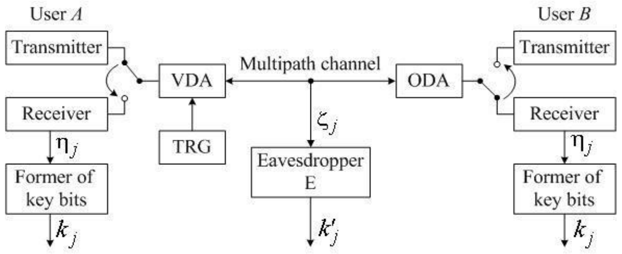


Figure 1. Scheme of communication system corresponding KDP

The KDP is described in the following steps:

1) The legal user A forms the random antenna diagram by exciting the VDA with output of *truly random generator* (TRG) and fix this diagram for some given time interval $[0,T_j]$ of the j-th key bit generation, $j=1,2,..., n$.

2) *A* transmits to *B* a harmonic signal $S_j(t) = \cos\omega_0 t$, $0 \le t \le T_j/2$, with the beam pattern obtained at step 1 over the multipath channel.

3) *B* receives a harmonic signal by an omni directional antenna (ODA) and forms the j-th key bit by comparing some functional η_j computed with the received signal on the time interval $[0, T_j/2]$ with a given threshold, forming the j-th key bit k_j.

4) The user *B* switches its ODA in a regime of radiation and transmits the same harmonic signal $S_j(t)=cos\omega_0 t$ within the time interval $T_j/2 \le t \le T_j$.

5) The user *A* switches its VDA to a receiver and processes the received signal in the same manner as *B* did, forming the j-th key bit k_j.

6) *A* and *B* repeat n times the steps 1-5 with new and independent outputs of TRG in order to create the desired number of key bits.

Thanks to the *Reciprocity Theorem* of radio wave propagation between uplink and downlink, the key sequences of *A* and *B* should be identical up to a random noise of receivers. Then the signal received by *B* at the time interval $T_j/2\le t \le T_j$ can be expressed as:

$$y_j(t) = \sum_{i=1}^{m} \upsilon_{ij}\beta_{ij} \cos(\omega_0 t + \theta_{ij}), \qquad (1)$$

where with respect to the i-th ray at the j-th time interval, β_{ij} is the channel attenuation coefficient, υ_{ij} is the VDA amplitude gain, θ_{ij} is the phase shift, including both phases in antenna diagram and phase shift in i-th ray, and m is the number of paths (rays).

The signal received by E at time interval $T_j/2\le t\le T_j$ is:

where the primed parameters have the same meaning as the

$$z_j(t) = \sum_{i=1}^{m} \upsilon'_{ij}\beta'_{ij}\cos(\omega_0 t + \theta'_{ij}), \qquad (2)$$

corresponding parameters in (1) but in possession of E. (We neglect initially the noise at the legal receivers, and we assume at this moment a noise absence at the eavesdropper E, in advantage with the illegal users.)

Later we will show that the probability distributions of the random values η_j and ζ_j, which are produced by executing some functionals from both $y_j(t)$ and $z_j(t)$ can have a good approximation by a zero mean Gaussian law.

It is easy to prove by a series of simple but tedious transforms that the probability of a bit disagreement between the j-th bit of the legal users and the eavesdropper key bits is:

$$p_e = 2\int_{-\infty}^{0} dy \int_{0}^{\infty} \frac{\exp\left(-\frac{x^2-2\rho xy+y^2}{2\sigma^2(1-\rho^2)}\right)}{2\pi\sigma^2\sqrt{1-\rho^2}}dx = \frac{1}{\pi}\arctan\left(\frac{\sqrt{1-\rho^2}}{\rho}\right) \qquad (3)$$

where ρ is the correlation coefficient between η_j and ζ_j, σ^2=Var(η_j)=Var(ζ_j).The dependence of p_e versus ρ is presented in Fig. 2. We can see that in contrast to our intuition, the probability p_e = 0.1 can be provided even when the correlation coefficient ρ has a significant value 0.95.

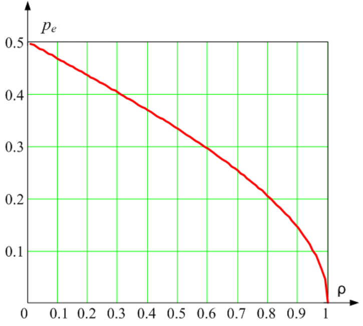


Figure 2. The probability of the key bit disagreement between legal and illegal users depending on the correlation coefficient ρ

In order to enhance the security of the legal user key string k shared after completion of the KDP it should be performed a privacy amplification [3], [17], [18], [19], or more specifically a mapping of the raw key string k to a shorter key string ǩ of length l<n, using the so called hashing procedure ǩ =h(k) taken from the universal class of hash functions [21]. Then the amount of Shannon's information leaking to E given her knowledge of the string k′ satisfies

$$I(\breve{\mathbf{k}};\mathbf{k}') \le \frac{l}{2^{n-l-t}\ln(2)} \qquad (4)$$

where $t = n+n\log_2(p_e^2+(1-p_e)^2)$ is the Renyi information under the assumption that the errors in the eavesdropper's key bits occur independently due to the independently generated VDA on each of the j-th time intervals. Hence in order to select the parameter l we should calculate the correlation coefficient ρ depending on the mutual location of the legal user and the eavesdropper, the properties of VDA and the characteristics of the multipath cannel. A solution for this problem will be presented in the next Section.

It is worth to remark that the quantized string k' has no redundancy and it is senseless to perform its soft decoding. As far as the use of a list decoding with the cipher text encrypted through the known key k, it looks as an completely intractable problem due to its large length (see Tables I and II at the end of Section IV below).

III. Correlation Between the Values η and ζ

Let us consider as VDA the so called ring antenna (RA) shown in Fig. 3 having N identical isotropic radiators excited by their random phases. Then the complex instant antenna diagram can be presented by the well-known formula [22]:

$$f(\varphi,\theta) = \sum_{i=1}^{m}\exp\left[ik_0R\sin\left(\varphi - \frac{2\pi s}{N}\right) - i\psi_s\right] \qquad (5)$$

where ψ_s is a phase in the s-th radiator; $k_0=2\pi/\lambda$, λ is the length of the wave; R the radius of the RA; φ is the angle in the azimuthally plane; and θ is the angle in the vertical plane.

Both instant amplitude and the phase antenna diagrams can be obtained from (5) and they are random values providing random exciting to the RA. It would be possible to find different statistical characteristics of $f(\varphi,\theta)$ theoretically but it is rather more easy to solve the same problem by simulation. Since the current paper is limited in space, we present only the main conclusions based on the simulations for the case of independent and uniformly distributed phases ψ_s on (0, 2π):

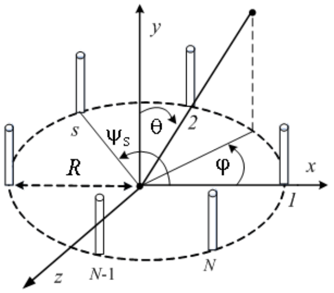


Figure 3. Ring antenna with N identical radiators

- the probability distribution of the amplitude antenna diagram has a good approximation through the Rice law which can be approximated in its turn by a Gaussian non-zero mean law;
- the probability distribution of the phase antenna diagram has a good approximation by an uniform law on the interval (0,2π).

Next it is possible to compute theoretically the correlation coefficients between η_j and ζ_j for different functionals producing them and to find their probability distributions by simulation. However, it is necessary to specify the channel model and thereafter the functional description. To be more specific, let us consider a 3-ray channel model and a location of eavesdropper on the line connecting legal users (Fig. 4).

We select two functionals of $y_j(t)$ and $z_j(t)$ producing η_j and ζ_j respectively. Henceforth the functionals are compared with some thresholds in order to obtain the key bit k_j. The functionals are (see eq. (1)):

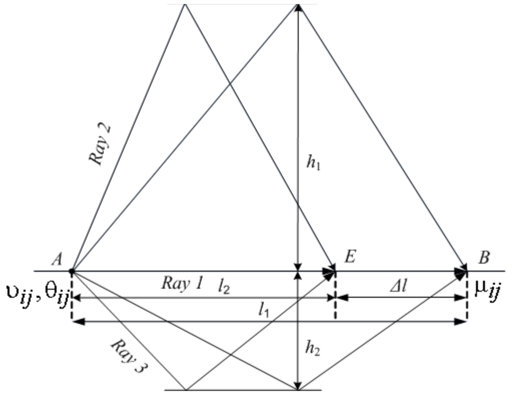


Figure 4. Channel model with 3-ray wave propagation

- envelope: $\mu_j = \sqrt{\mu_{cj}^2 + \mu_{sj}^2}$,

where

$$\mu_{cj} = \sum_{i=1}^{m} A_{ij} \cos\theta_{ij}, \quad \mu_{sj} = \sum_{i=1}^{m} A_{ij} \sin\theta_{ij}, \quad A_{ij} = \upsilon_{ij}\beta_{ij},$$

- phase difference

$$\Delta\psi_j = \Delta\psi_{j+1} - \Delta\psi_j = \arctan\frac{\mu_{s_{j+1}}}{\mu_{c_{j+1}}} - \arctan\frac{\mu_{s_j}}{\mu_{c_j}}.$$

In a similar manner, there can be presented the corresponding functionals for eavesdropper: μ'_j, μ'_{cj}, μ'_{sj}, $\Delta\psi'_j$.

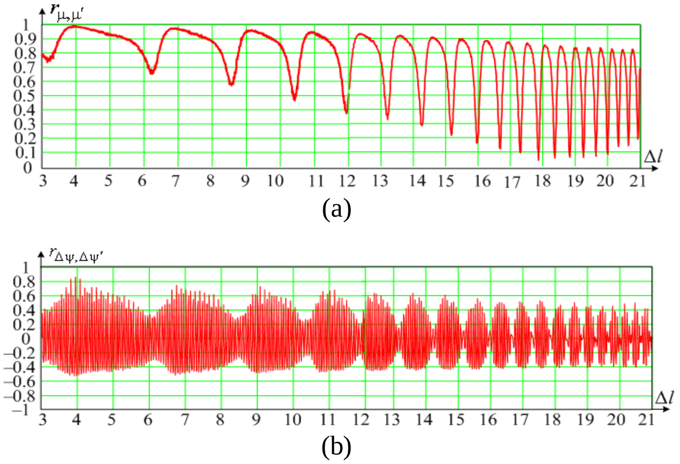
We will be interested in a procedure to find the probability distributions of all functionals and correlations between similar functionals of any legal user *B* and the eavesdropper *E*. Because it is very hard to compute these values theoretically, we will find them by simulation for some given channel parameters.

Let us take distance between *AB* l_1=25m; distances to the first and to the second reflecting surfaces, respectively h_1=3m, h_2=3m, *N*=6, λ=12.5cm, *R*=λ/2 (see Fig's. 3 and 4). Assume that *E* is placed between legal users *A* and *B* within the interval Δ*l*=3-22m. The dependences of the correlation coefficients $r_{\mu,\mu'}$ and $r_{\Delta\psi,\Delta\psi'}$ versus distance Δ*l* between the eavesdropper *E* and the legal user *B* are shown in Fig. 5(a) and Fig. 5(b) respectively.

Similar dependences versus distance l_1 between legal users *A* and *B* where Δ*l*=4m, h_1=h_2=3m are presented in Fig.6 (a) and 6(b). In Fig 7 (a) and 7(b) are shown the same dependences but versus distances to the first reflecting surface and for other parameters: l_1=25m, Δ*l*=4m, h_2=3m.

As we can see from these figures, these dependences are looking very strange because if, for the thing, in some points on the line connecting *A* and *B* the correlation of amplitude is small enough, nevertheless a small shift of the eavesdropper location with respect to the locations of legal users results in strong correlation. Similar property holds also for the correlation of phase differences but the absolute values of this correlation are at most 0.8 for any conditions. Since the correlation between the values $\Delta\psi_j$ and $\Delta\psi'_j$ occurs less than the correlation between μ_j and μ'_j (see Fig. 5, 6, 7), it is reasonable to select the phase difference functional in order to form η_j and compare it with zero threshold for the k_j key- bit generation. (In order to coincide phases of support generators at users *A* and *B*, it is possible to transmit a special pilot signal and to tune phases of both users at the initial stage of KDP.)

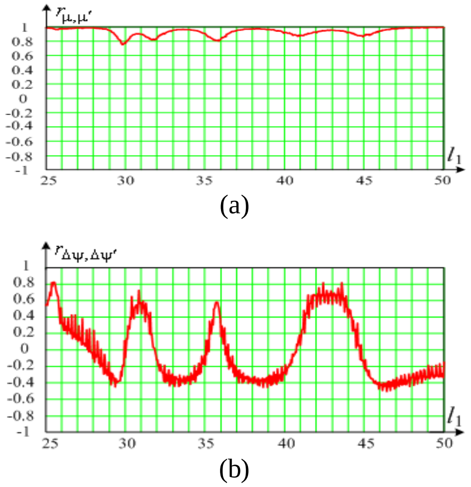
In Fig. 8 there are presented empirical probability distributions for these functionals. It is evident that both cases can be approximated by appropriated Gaussian distributions (see solid curves). Therefore the relation (3) can be used to find the probability of disagreement between the key bits of the legal users and the eavesdropper. But before we address to eq. (4) in order to calculate security of KDP, it should be taken into account an opportunity for the presence of noise at the receivers of the legal users.



(a)

(b)

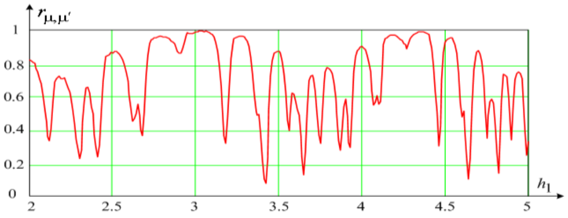
Figure 5. The dependence of correlation coefficients versus distances between legal use and eavesdropper.
a) for envelope, b) for phase difference



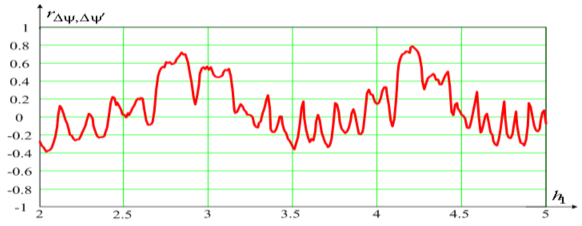
(a)

(b)

Figure 6. The dependence of correlation coefficients versus distances l1 between legal users for Δl=4m, h1=h2=3m.
a) for envelope, b) for phase difference

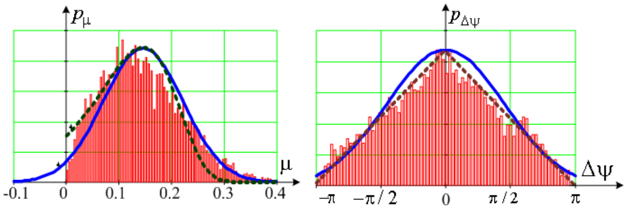


(a)



(b)

Figure 7. The dependence of correlation coefficients versus distances to the first reflecting surface and parameters: l1=25m, Δl=4m, h2=3m. a) for envelope, b) for phase difference



(a) envelope (b) phase difference

Figure 8. Empirical probability distribution for chosen functionals

IV. KDP Optimization Under Noisy Legal Channel

From now on we remove our previous assumption that the multipath channel among legal users *A* and *B* is noiseless but keep such condition for eavesdropper's channel. (Obviously, the last assumption cannot degrade the security of KDP.)

In this setting it is necessary to use some methods in order to correct disagreements in key bits of legal users. It is very reasonable to use firstly a selection of the most reliable key bits with a public discussion over a noiseless channel between legal users, and then to apply *forward error correction codes* (FEC) by sending of the check bits over the same but noiseless channel. (It is worth to note that a noiseless public channel among legal users can be arranged by the choice of special regime, namely large signal power or omni directional antenna of the user A that we were unable to use for the execution of KDP.)

The first method of the most reliable key bit selection is to take the decision according to the rule:

$$k_j = \begin{cases} 1, \text{ if } \eta_j \geq \alpha, \\ 0, \text{ if } \eta_j \leq -\alpha, \\ \text{erase otherwise,} \end{cases}$$

where η_j is the output of $\Delta\psi_j$, and α a threshold.

After a completion of the KDP including a production of the erased bits for both legal users it is necessary to mutually announce the numbers of these bits over public noiseless channels. In this case, the probability of a key bit disagreement between legal users and eavesdropper, given by (3), has to be corrected because an eavesdropper is able to intercept information about the numbers of accepted key bits over the public channel. We will take into account this fact later for the simulation procedure. The second method is to keep only the most reliable key bits, say *M*, and to remove the others. This means that the legal users form variation series of the values $|\eta_j|$ on a decreasing order and next to keep (after mutual public discussion) the first *M* members of this series to generate the key bits. Of course in this case the probability of key bit disagreement p_e is changed also against (3).

Let us denote by p1 and p2 the probability of legal key bit errors after the first and the second method, respectively. Next we use an error-correcting code (n_0+*r*, n_0) sending a sequence of *r* check symbols over public noiseless channel in order to correct eventually errors in the key sequence.

Then the probability of erroneous decoding P_{ed} by the modified Gallager's theorem is [19]: $P_{ed} \leq 2^{-n_0E(R_C)}$, where

$$E(R_C) = \max_{\rho_0 \in (0,1)} \left[E_0(\rho_0) - \frac{\rho_0(2R_C - 1)}{R_C} \right].$$

$$E_0(\rho_0) = \rho_0 - (1-\rho_0)\log_2 \left[p^{\frac{1}{1+\rho_0}} + (1-p)^{\frac{1}{1+\rho_0}} \right],$$

$R_C = n_0/(n_0+r)$, and no is the number of bits k_j which have been kept by legal users after erasing the unreliable bits following the first or the second procedures, and *p* is the error probability for the kept bits. In the case of check symbol sending, the Privacy Amplification Theorem against (4) becomes [19]:

$$I(\breve{\mathbf{k}};\mathbf{k}') \leq \frac{l}{2^{n_0-l-t-r}\ln(2)}.$$

KDP optimization problem is to get the maximum key rate

$$R_C = \frac{l}{n_0 + n_{er}} = \frac{l}{n},$$

where n_{er} is the number of erased symbols after the use of the method 1 or 2 and given the values $I(\breve{\mathbf{k}};\mathbf{k}')$, P_{ed}, *l*, and different signal-to-noise ratio (*S*/*N*) at the receivers of the legal users. We solve this problem by simulation for the case of Gaussian noise at the legal receivers.

In Tables I and II there are presented the results of such optimization for typical conditions for the first and the second method of unreliable bits removal, respectively, where P_{er} is the probability of key bit erasing.

We can see from these tables that the second method is for large correlation a little bit better than the first one. However both methods provide sufficiently reliable and secure key sharing if eavesdropper is placed on 3-21m away from legal user *B* and phase difference is used as key generating method (see Fig. 5(b)).

A similar conclusion is drawn also for multipath channels with a greater number of rays and with other reasonable parameters and eavesdropper locations. In order to enhance the security of the KDP, antenna diversity can be used when *B* has m omni directional antennas and he selects randomly one of them at each time period T_j to receive and transmit signal. Then the relation finding the Renyi information used in (4) changes for:

$$t = n + \frac{n}{m}\log_2(\tilde{p}_e^2 + (1-\tilde{p}_e)^2). \tag{5}$$

TABLE 1. KEY RATE MAXIMIZATION FOR THE FIRST METHOD GIVEN $I(\check{\mathbf{K}};\mathrm{K}')=10^{-9}$, $P_{ED}=10^{-5}$, S/N=10 AND DEFFERENT P

ρ	αopt	pe	Per	p1	l	n0	Rk
0.8	0.18	0.263	0.194	0.0087	128	539	0.243
			0.191	0.0083	256	940	0.272
			0.189	0.0082	512	1685	0.303
0.95	0.14	0.152	0.189	0.0083	128	1528	0.084
			0.188	0.0082	256	2484	0.103
			0.187	0.0082	512	4195	0.122
0.99	0.11	0.051	0.183	0.0078	128	7405	0.017
			0.181	0.0075	256	10977	0.023
			0.18	0.0075	512	15234	0.033

TABLE 2. KEY RATE MAXIMIZATION FOR THE SECOND METHOD GIVEN $I(\check{\mathbf{K}};\mathrm{K}')=10^{-9}$, $P_{ED}=10^{-5}$, S/N=10 AND DEFFERENT P

ρ	Mopt	pe	Per	p2	l	Rk
0.8	539	0.222	0.24	0.0075	128	0.245
	940		0.238		256	0.277
	1685		0.236		512	0.306
0.95	1528	0.115	0.236	0.0072	128	0.095
	2484		0.235		256	0.105
	4195		0.233		512	0.123
0.99	7405	0.049	0.23	0.0069	128	0.017
	10977		0.29		256	0.023
	15234		0.29		512	0.033

The relation (6) holds with the probability equal to the probability of the event in which with at least of one of antennas mutual location of the legal user and the eavesdropper is got such that ρ≤ρ*, where ρ* is found by (3) given p_e.

We considered so far a scenario when an eavesdropper uses the same omni directional antenna as the legal user *B*. But *E* can execute directional antenna to separate all rays and to process the best of them or even apply joint processing to all of them. We have performed a simulation of the case with single ray separation and it has been shown that the correlation coefficient even decreases in comparison with one presented before. The case of joint processing of separated rays is noteworthy. But we can remark that even under the very strong condition in which the eavesdropper knows exactly all channel parameters both for *E* and *B*, there is still uncertainty about VDA gains in the direction of *E* and *B*. Therefore, generally speaking, the correlation coefficient occurs even in this case with a value less than one.

V. CONCLUSION AND FUTURE WORK

We considered a method of key sharing based on the concept of a VDA under the condition of multipath channel and we showed that sufficient security and reliability of the shared keys can be provided even when the eavesdropper's channel is noiseless. (It is worth to remark that in order to get such result, the following two conditions are necessary: to create truly randomness with the help of a VDA and to have multipath channels.) The results of investigations show that the security of the KDP (in terms of Shannon's information leaking to eavesdropper) does not depend only on the distance between legal users and eavesdropper but also on the eavesdropper's location. This result somewhat contradicts to a very optimistic conclusion in [12].

We propose to use the difference-phase functional instead of either quadrature components or envelope in order to form key bits. This approach results in less mutual correlation between legal user and eavesdropper and simplifies a choice of threshold. The key sequence k is i.i.d if VDA is excited by independent random phases and threshold is chosen in an appropriate manner. (This fact has been confirmed by simulation using statistical tests.) Our contribution consists also in the proof of relation (3) which allows to connect the probability of disagreement between the key bits of legal users and eavesdropper with the correlation of corresponding values. Unfortunately, a limited space of the paper does not allow us to show all simulation results for different multipath channels and mutual location of legal users and eavesdroppers, which we have got at our disposition. It is pertinent to note that although some results were obtained by the use of computer simulation, it does not lead to a loss of generality because this is only an approach to reach the same goal by a simpler way. As far as the limitation due to the parameter selection (number of rays, position of eavesdropper, *S*/*N*, etc) it can be explained only by the space paper limitations. Indeed, following our theory, one can get the results corresponding to arbitrary parameters.

In the future we are going to investigate: *i*) the use of multitone signals in the KDP, ii) the optimal processing of the eavesdropper rays separation in order to provide the greatest correlation, iii) the use of real FEC and effective decoding algorithms with KDP (instead of extended Gallager's bounds);and, iv) the use of other types of VDA (like ESPAR or others).

REFERENCES

[1] 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.

[2] U. Maurer, "Protocols for secret key agreement by public discussion based on common information." in CRYPTO, ser. Lecture Notes in Computer Science, E. F. Brickell, Ed., vol. 740. Springer, 1992, pp.461-470.

[3] U. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels II: the simulatability condition." IEEE Transactions onInformation Theory, vol. 49, no. 4, pp. 832-838, 2003.

[4] V. Yakovlev, V. 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.

[5] A. M. Sayeed and A. Perrig, "Secure wireless communications: Secret keys through multipath," in ICASSP. IEEE, 2008, pp. 3013-3016.

[6] Y. Liu, S. C. Draper, and A. M. Sayeed, "Secret key generation through ofdm multipath channel," in CISS. IEEE, 2011, pp. 1-6.

[7] M. G. Madiseh, M. L. McGuire, S. S. Neville, L. Cai, and M. Horie, "Secret key generation and agreement in uwbcommuniction channels," in GLOBECOM 2008.IEEE, 2008.

[8] M. G. Madiseh, S. W. Neville, and M. L. McGuire, "Time correlation analysis of secret key generation via uwb channels," in GLOBECOM. IEEE, 2010, pp. 1-6.

[9] A. A. Hassan, W. E. Stark, J. E. Hershey, and S. Chennakeshu, "Cryptographic key agreement for mobile radio," Digital Signal Processing, vol. 6, pp. 207-212, 1996.

[10] J. Hershey, A. Hassan, and R. Yarlagadda, "Unconventional cryptographic keying variable management," Communications, IEEE Transactions on, vol. 43, no. 1, pp. 3 -6, Jan. 1995.

[11] Ch.Ye, S. Mathur, AReznik, W. Trappe and N.B. Mandayam. "Information-Theoretically Secrete Key Generation for Fading Wireless Channels, IEEE Transactions on Information Forensics and Security , vol.5, No.2,June 2010,pp.240-254.

[12] T. Aono, K. Higuchi, T. Ohira, B. Komiyam, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," IEEE Trans. Antennas &ropagation,vol. 53, pp. 3776-3784, Nov. 2005.

[13] T. Shimizu, H. Iwai, and H. Sasaoka, "Improvement of key agreement scheme using espar antenna," in Proc. 2008 Int. Symp. Antennas Propag.(ISAP2008). Taipei, Taiwan, 2008, pp. 1-4.

[14] M. Onishi, T. Kitano, H. Iwai, and H. Sasaoka, "Improvement of tolerance for eavesdropping in wireless key agreement scheme using espar antenna based on interference transmission," in The 2009 International Symposium on Antennas and Propagation (ISAP 2009).Bangkok, Thailand: ISAP, October 20-23 2009.

[15] T. Shimizu, N. Otani, T. Kitano, H. Iwai, and H. Sasaoka, "Experimental validation of wireless secret key agreement using array antennas," in XXX URSI General Assembly and Scientific Symposium. Istambul, Turkey: URSI, August 11-20 2011.

[16] T. Yoshida, T. Saito, K. Fujiki, K. Uematsu, and H. U. T. Ohira, "Impact of direct-path wave on imac in secret key agreement system using espar antennas," in XXX URSI General Assembly and Scientific Symposium. Istambul, Turkey: URSI, August 11-20 2011.

[17] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, "Generalized privacy amplification," IEEE Transactions on Information Theory, vol. 41, no. 6, pp. 1915-1923, 1995.

[18] U. Maurer and S. Wolf, "Privacy amplification secure against active adversaries," Lecture Notes in Computer Science, vol. 1294, pp. 307-321,1997.

[19] 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.

[20] V.Korzhik V. Yakovlev,,G. Morales-Luna, Yu. Kovajkin. "Wireless Secrete Key Sharing Based on on the Use of Variable-directional Antenna over Multipath Channels", in Proc.ELMAR' 2010 ,pp.277-280.

[21] L. Carter and M. N. Wegman, "Universal classes of hash functions," J. Comput. Syst. Sci., vol. 18, no. 2, pp. 143-154, 1979.

[22] R. E. Collin and F. J. Zucker, Antenna Theory - Part 1.McGraw-Hill,1969.