Analysis of Keyless Massive MIMO-based Cryptosystem Security

Valery Korzhik[1], Guillermo Morales-Luna[2], Sergei Tikhonov[1], and Victor Yakovlev[1]

[1] State University of Telecommunications, St. Petersburg, Russia,
val-korzhik@yandex.ru
[2] Computer Science, CINVESTAV-IPN, Mexico City, Mexico,
gmorales@cs.cinvestav.mx

Abstract. A cryptosystem for wireless communications, recently proposed by T. Dean and A. Goldsmith, is considered. That system can be regarded as a second revolution in cryptography because the confidentiality of the messages transmitted over a wireless massive MIMO-based channel is provided by the difference in the space locations of legal and illegal users and it does not require any secret key distribution. However our investigation shows that there is a chance of eavesdropping the cipher texts by using a suboptimal algorithm. Therefore we investigate some additional conditions for channel matrices and additive noises in order to provide a desired security. A combination of wiretap channel coding with a MIMO-based cryptosystem is also considered.
Keywords. Cryptosystem, wireless channel, massive MIMO, lattice hard problems.

1 Introduction

The invention of public key cryptography by W. Diffie and M. Hellman [1] can be thought as a real "revolution in cryptography of the 20-th century". The authors proposed an asymmetric cryptosystem for which encryption and decryption keys were different and, moreover, the decryption key cannot be computationally derived from the encryption key. This approach simplified the problem of key distribution among legitimate users in the presence of eavesdroppers. The use of a *public key algorithm* (PKA) solved the problem for a digital signature scenario and allowed the creation of many multiparty cryptographic protocols [2]. However, the PKA's have several drawbacks:

- the encryption or the decryption procedure, even for legitimate users, may be enough complex,
- it is necessary to check the integrity and authenticity of public keys within their storing or distribution,
- although some PKA's are "provable secure", i. e. breaking the cipher can be equivalent to solve strong mathematical problem (say integer factorisation or discrete logarithm calculation), typically this assert holds on the average but not for the worst cases, and

– private keys can be extracted from tamper resistant modules over side attack channels (say, electrical power or electromagnetic radiation in the environment).

In a recent paper [3], a cryptosystem has been proposed to avoid generic drawbacks belonging to PKA. Although this cryptosystem cannot be used in all situation requiring confidentiality, it is adequate for the case when transmission of secret messages over wireless multipath channels supplied by massive MIMO technology is necessary. On the other hand such wireless channel model was very popular in recent years both as object for theoretical investigations and for practical implementations [4]. Thus, at least for wireless multipath channels, our proposal approach is rather relevant. The main restrictions on the channel model assumed at [3] are:

1. The channel between legitimate users (say Alice (A) and Bob (B)) is described by an $m \times n$-matrix $A = (a_{ij})_{1 \leq i \leq m}^{1 \leq j \leq n}$ of i.i.d. Gaussian random values with zero mean and a given variance σ^2, where each a_{ij} is the gain of the i-th antenna at A to the j-th antenna at B.
2. The eavesdropper channel between A and Eve (E) is properly an $n \times m$-matrix $B = (b_{ij})_{1 \leq i \leq m}^{1 \leq j \leq n}$ of i.i.d Gaussian random values with zero mean and a given variance σ_w^2, where each b_{ij} is the gain of the i-th antenna at A to the j-th antenna at E.
3. All elements of the matrix A are statistically independent of all elements of B if the legitimate user B is replaced by the eavesdropper E, at least with respect to some reasonable distance (of order about the wave-length).
4. The gain matrices are known exactly by all parties of communications including the eavesdropper.
5. The entries of the matrices A and B do not depend statistically on the elements at these matrices on other communication sessions.

These requirements are in line with the experimental results for some wireless channels [5]. At [3] it is claimed that under these conditions, there exists a cryptosystem having the following properties:

1. No secret keys are required to be shared in advance between legitimate users.
2. The *proposed cryptosystem* (PCS) is provably secure, and it is associated with a well known hard problem on lattices [6] for the worst case.
3. Encryption and decryption operations are relatively simple and they require just a matrix multiplication over the field of reals.

The above properties (and especially the first one) may assert that PCS is indeed "the next revolution in cryptography" (at least in the case of MIMO-based channels).

The goal of the current paper is to analyse the PCS security (or, in other words, its unbreakability). For simplicity reason we consider further just the particular case $m = n$, namely, that the number of receiving antennas equals the number of transmitting antennas. By using an error-correcting code, it would be

possible to reduce the complexity of deciphering for legitimate users [7]. However this facility may be also of help for potential eavesdroppers, hence we avoid in the current approach the use of any error-correcting code.

2 Description of the encryption/decryption algorithms for PCS

Following [3], let us recall the mathematical model of a legitimate channel:

$$z = Ay + e \tag{1}$$

where $y \in \mathbb{Z}^n$ represents the transmitted vector, $A \in \mathbb{Z}^{n\times n}$ characterises the channel among legitimate users, and $e \in \mathbb{Z}^n$ represents the legitimate channel noise. Instead, the eavesdropper's channel is:

$$z' = By + e'$$

where $B \in \mathbb{Z}^{n\times n}$ characterises the channel between a legitimate user and an intruder user, and $e' \in \mathbb{Z}^n$ represents the eavesdropper's channel noise.

Alice, A, encrypts a message $x \in \mathbb{Z}_M^n$, $x = [x_1 \ \cdots \ x_n]^T$, with $0 \leq x_k < M$ and $x_k \in \mathbb{N}$, for all $k = 1, \ldots, n$, as:

$$y = Vx \tag{2}$$

where V is a matrix appearing at the calculation of the *singular value decomposition* (SVD) of the matrix A, given as $A = USV^T$, with orthogonal matrices U and V, and diagonal matrix S (the superindex "T" denotes matrix transposition). By combining (1) with (2) and taking into account the orthogonality of V, the following version of the ciphertext is obtained

$$z = Ay + e = USx + e.$$

In order to decrypt the ciphertext, the legitimate user B, knowing the SVD form of A (see the restriction 4 above), computes

$$z'' = U^T z = U^T USx + U^T e = Sx + \hat{e} \tag{3}$$

where $\hat{e} = U^T e$. On the assumption of Gaussian distribution for $\hat{e}$, from (3), the optimal estimation (that is the decryption indeed) of x as x' given z'', is:

$$x' = \arg\min_x \|z'' - Sx\| \tag{4}$$

($\|\cdot\|$ denotes the Euclidean norm on $\mathbb{R}^n$). Since the matrix S is diagonal, say $S = \mathrm{diag}[s_1 \ \cdots \ s_n]$, the relation (4) is transformed into:

$$\forall i \in \{1, \ldots, n\} : \quad x'_i = \arg\min_{x_i} \|z''_i - s_i x_i\| \tag{5}$$

From (5) it follows immediately that the decryption of the message x has linear complexity (proportional to n) because it is provided by the calculation of all the n coordinates of x. As a matter of fact, no keys are used for decryption or encryption. Of course, it is possible to call "key" the matrix A but since the eavesdropper E may know this matrix, it is not a secret key at all.

Let us cryptanalyse the case when an eavesdropper tries to follow the strategy of a legitimate user. Eve, E, receives the vector

$$z' = By + e' = BVx + e' = U'S'(V')^T Vx + e' = Cx + e' \tag{6}$$

where $C = U'S'(V')^T V$ and $U'S'(V')^T = B$ is the SVD of the matrix B. The eavesdropper E then computes (see (3))

$$z''' = (U')^T z' = (U')^T Cx + (U')^T e' = C'x + \hat{e}'$$

where $\hat{e}' = (U')^T e'$ and $C' = S'(V')^T V$. Since the matrix C' is not diagonal, finding an optimal estimation for the vector x in the case of a Gaussian i.i.d. noise vector $\hat{e}'$, given the vector z''', is reduced to:

$$x'' = \arg\min_x \|z''' - C'x\|. \tag{7}$$

The problem (7) is known to be a hard problem on lattices [6]. It is shown in [3] (see its main theorem), that it is NP-hard problem under the following condition:

$$M\sqrt{\sigma^2 \tilde{\sigma}_e^2} \geq \sqrt{n}, \tag{8}$$

where M is the size of the message alphabet, σ is the standard deviation of the channel gains in B, $\tilde{\sigma}_e$ is the standard deviation of the eavesdropper's channel noise, and n is the number of antennas in the MIMO system. Indeed, the condition (8) entails a larger noise at the attacker side, thus the bounded distant decoding algorithm [8] is not suitable in this context.

We may claim, however, that due to the NP-hardness of the problem (7), this cryptanalysis of PCS renders impractical an attack for $n \geq 100$.

In summary, at [3] it is claimed that under the assumptions of

- separated locations of legal users and eavesdroppers, and
- the existence of multipath channels with fading combined with massive MIMO technology,

it is possible to build a cryptosystem which, under the condition (8), guarantees a polynomial deciphering complexity by the legitimate users and exponential complexity of cipher breaking by any eavesdropper. However, at [3] it is not considered to break PCS (even under the assumption (8)) for the case when suboptimal deciphering algorithms are used. We consider these algorithms in the next section.

3 Suboptimal cipher breaking algorithms

Consider the suboptimal decryption algorithm under the not so strong condition that the matrix C in (6) is non-singular, i.e. there exists its inverse C^{-1}. Multiplication of both sides of (6) by the inverse matrix gives:

$$\hat{z}' = C^{-1}z' = x + C^{-1}e'$$

C^{-1} is not necessarily an orthogonal matrix, hence $C^{-1}e'$ is not necessarily an i.i.d. Gaussian vector. Then

$$\forall i \in \{1, \ldots, n\}: \quad x_i''' = \arg\min_{x_i} \|\hat{z}_i' - x_i\| \tag{9}$$

where $\hat{z}' = [\hat{z}_1' \ \cdots \ \hat{z}_n']^T$ is not necessarily an optimal estimation algorithm. Clearly, (9) entails a linear complexity.

The quality of the cryptanalysis given by (9) can be determined by the *error probability* ($x_i''' \neq x$). This probability depends on the parameters σ_w, $\tilde{\sigma}_e$ and n.

The simulations for both the error probabilities of the legitimate user and the eavesdropper, calculated by (5) and (9), respectively, are presented in Table 1. We consider that the message alphabet is $\{-1, +1\}$, thus $M = 2$, and $n = 100$.

It can be can seen at Table 1, that for the case of equal legitimate and wiretap channels qualities ($\sigma^2 = \sigma_w^2$ and $\sigma_e^2 = \tilde{\sigma}_e^2$) the error probabilities at a legitimate channel is much lesser than the error probabilities at a wiretap channel. Moreover, the error probabilities for a wiretap channel may occur sufficiently large such that it is not possible to recover any meaningful text in some natural language. In fact, if we assume (for ease of simplicity) that the symbols of some natural language are coded into 5-bits combinations and each bit is transformed independently into an erroneous bit with probability p' in line with a binary symmetric channel model, then the capacity of such 32-ary symmetric channel without memory can be calculated as follows [9]:

$$\begin{aligned} C = 5 + & \quad (1-p')^5 \log_2 \left[(1-p')^5\right] \\ & + \quad 5p'(1-p')^4 \log_2 \left[p'(1-p')^4\right] \\ & + 10(p')^2(1-p')^3 \log_2 \left[(p')^2(1-p')^3\right] \\ & + 10(p')^3(1-p')^2 \log_2 \left[(p')^3(1-p')^2\right] \\ & + \quad 5(p')^4(1-p') \log_2 \left[(p')^4(1-p')\right] \\ & + \quad (p')^5 \log_2 \left[(p')^5\right] \end{aligned} \tag{10}$$

In Table 2 there are presented the results of some calculations by (10) for different values of p'.

Let us suppose that the entropy of a natural language with 32-letter alphabet is approximately 1.5 bit/letter [10], then for $p' > 0.19$ it is impossible to recognise the meaningful text correctly by Shannon theorem [10].

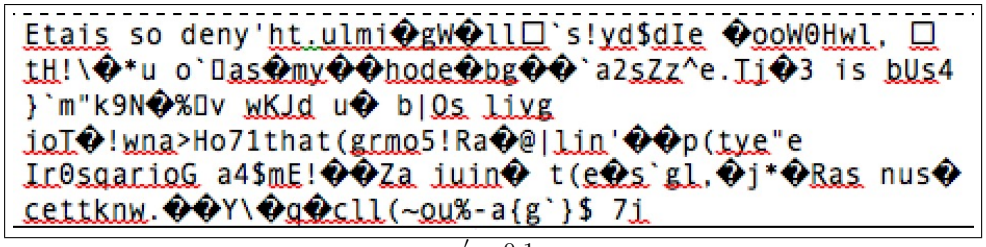
In order to confirm this fact, we simulate a corruption of a meaningful text in English using a BSC model with different error probabilities p'. The results are presented in Table 3.

Channel parameters		p	p'	$M\sqrt{\sigma_w^2\,\tilde{\sigma}_e^2}$
σ^2	$\tilde{\sigma}_e^2$			
7	4	0.0207	0.2119	10.58
8	4	0.0187	0.2024	11.31
9	4	0.0190	0.1927	12.00
6	5	0.0243	0.2398	10.95
7	5	0.0224	0.2240	11.83
8	5	0.0214	0.2182	12.64
5	6	0.0290	0.2657	10.95
6	6	0.0267	0.2530	11.99
7	6	0.0248	0.2382	12.96
8	6	0.0240	0.2207	13.85
4	7	0.0345	0.2915	10.58
5	7	0.0314	0.2836	11.83
6	7	0.0287	0.2721	12.96
7	7	0.0261	0.2569	14.00
4	8	0.0374	0.3008	11.31
5	8	0.0327	0.2817	12.64
6	8	0.0305	0.2791	13.85
7	8	0.0281	0.2639	14.96

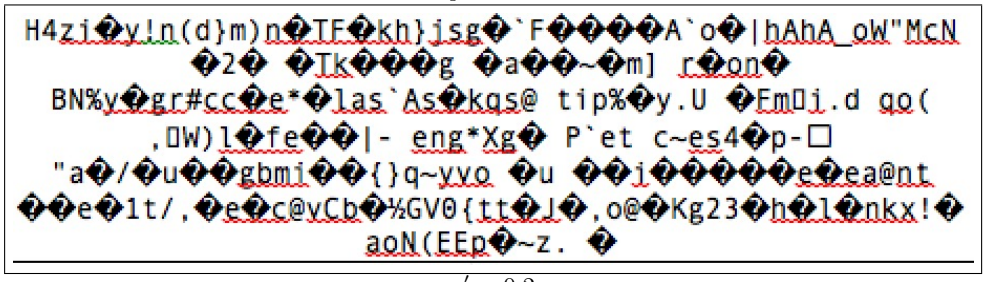
Table 1. The error probabilities for the legitimate user (p) and for eavesdropper (p'). We assume $\sigma^2 = \sigma_w^2$ and $\sigma_e^2 = \tilde{\sigma}_e^2$ and $n = 100$.

p'	0.1	0.19	0.4	0.49
C	2.655	1.4926	0.1452	0.0014

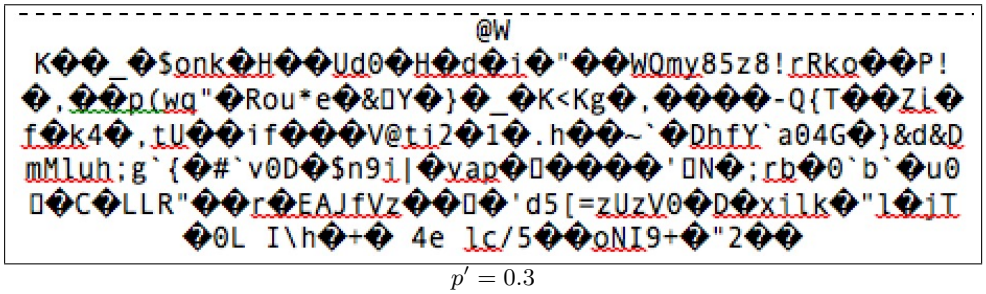
Table 2. Capacity of a 32-ary symmetric noisy channel without memory for 5-bit representation and transmitting bits over binary symmetric channel (BSC) without memory against the error probability p'.



$p' = 0.1$



$p' = 0.2$



$p' = 0.3$

Table 3. The results of simulation English meaningful text that passes over BSC with error probabilities p' (many non-printable characters appear).

From this experiment it can be seen that, for $p' > 0.2$, it is practically impossible to recover correctly the text. But if it is encrypted, more redundant material (say multiple repetition of the same symbols or words) may appear, thus it could be possible to recover this text even for the error probability $p' > 0.2$. Moreover, Table 1 shows that, for chosen channel parameters, the error probability for a legitimate channel is insufficiently small.

In order to decrease this probability we propose to increase the variance σ^2, say at the cost of increasing the transmitted signal power. The results of such simulation of both channels (legitimate and wiretap, for $n = 100$) are presented in Table 4. It follows that although the error probabilities for legitimate users can be acceptable, the error probabilities for wiretapper are not sufficiently large. (We stress that this result is valid even under the condition (8)!)

It is possible to decrease the error probability at the legitimate channel keeping almost the same error probability for wiretap channel by increasing the number n of antennas. So, taking $n = 1000$, $\sigma^2 = \sigma_w^2 = 8$ and $\sigma_e^2 = \tilde{\sigma}_e^2 = 5$ then necessarily $p = 0.00642$, $p' = 0.2175$ (compare with Table 1, $N = 6$). However such a large number of antennas obviously creates a technological problem within a MIMO system.

4 A combination of PCS with wiretap channel coding

From Table 1, we find that PCS entails a significant increasing of the error probability for wiretap channel. This fact paves the way for additional application of wiretap coding [11]. It is well known that the so called *secret capacity* of wiretap channel is (in our notation) [12]:

$$C = h(p) - h(p')$$

where $H : x \mapsto h(x) = x \log_2 x + (1 - x) \log_2(1 - x)$.

This means that there exist encoding/decoding procedures with code rate $R < C$ providing a probability of incorrect decoding, by a legitimate channel, as small as desired and simultaneously an amount of Shannon's information leaking to eavesdropper as small as desired when the length of code blocks approaches to infinity.

In Table 5 there are presented the values of C calculated for some values p and p' appearing partly at Table 1.

We see from this table that it is possible to reach sufficiently large code rate in order to provide close to zero eavesdropping and reliable legitimate information transmission. Moreover, changing additive noise variation we can maximise the value of capacity C. The control of additive noise power can be done by sending additive noise with desired power from transmitting side as it was described in [3].

Of course it is possible to share a secret key initially using the so called public discussion [13, 14] which does not require complex encoding/decoding methods but in this way one may lost the main feature of PKS, namely, the absence of any key distribution in advance.

Channel parameters				
σ^2	$\tilde{\sigma}_e^2$	p	p'	$M\sqrt{\sigma^2\,\tilde{\sigma}_e^2}$
20	4	0.0122	0.1320	17.88
50	4	0.0081	0.0838	28.28
70	4	0.0069	0.0742	33.46
100	4	0.0059	0.0625	40.00
20	5	0.0137	0.1496	20.00
50	5	0.0090	0.0974	31.62
70	5	0.0075	0.0854	37.41
100	5	0.0067	0.0693	44.72
20	6	0.0149	0.1605	21.90
50	6	0.0097	0.1040	34.64
70	6	0.0084	0.0905	40.98
100	6	0.0072	0.0742	48.98
20	7	0.0162	0.1692	23.66
50	7	0.0106	0.1117	37.41
70	7	0.0089	0.0990	44.27
100	7	0.0077	0.0815	52.91
20	8	0.0171	0.1793	25.29
50	8	0.0112	0.1210	40.00
70	8	0.0095	0.1062	47.32
100	8	0.0081	0.0869	56.56

Table 4. The error probabilities for the legitimate user (p) and for eavesdropper (p'). We assume $\sigma^2 = \sigma_w^2$ and $\sigma_e^2 = \tilde{\sigma}_e^2$ and $n = 100$, with increased variances of channel matrices.

p	0.0207	0.0224	0.0248	0.0261	0.0281
p'	0.2119	0.2240	0.2382	0.2569	0.2639
C	0.5997	0.6127	0.6244	0.6476	0.6478

Table 5. The values of secret capacity C for wiretap channel with different bit error probabilities of legitimate (p) and wiretap channel (p').

5 Conclusion

We have considered the keyless cryptosystem proposed in [3] and intended for the use in wireless multipath channels based on massive MIMO technology. It seems to be very novel approach to build a provable (for the worst case) secure cryptosystem based on lattice hard problem. We remark that if the condition (8) holds it is sufficient to provide an exponential complexity for the optimal decryption algorithm (7) but it is not enough to exclude suboptimal cipher breaking algorithm (9). Although even so this algorithm is used, it provides in significant degradation of the eavesdropper's channel but not for all cases it results in impossibility of plaintext reading. It depends on the parameters of the channel model $(\sigma^2, \sigma_w^2, \sigma_e^2, \tilde{\sigma}_e^2)$, which in turn can be unknown exactly for a designer of cryptosystem. The use of wiretap coding in a combination with PCS allows to provide both security and reliability but constructive encoding method that provides the code rate close to channel capacity is still unknown. In order to put PCS into practice, it is also necessary to arrange a procedure of channel matrices estimation based on a sending of testing signals in real time.

And then the first question arises how affects incorrectness of channel matrices estimation on the error probability in the legitimate channel?

Thus we can conclude that the proposed cryptosystem is very interesting from the theoretical point of view but its practical implementation requires further investigations.

References

1. Diffie, W., Hellman, M.: New directions in cryptography. IEEE Trans. Inf. Theor. **22**(6) (September 2006) 644–654
2. Menezes, A.J., van Oorschot, P.C., Vanstone, S.A.: Handbook of Applied Cryptography. The CRC Press series on discrete mathematics and its applications. CRC Press, 2000 N.W. Corporate Blvd., Boca Raton, FL 33431-9868, USA (1997)
3. Dean, T., Goldsmith, A.: Physical-layer cryptography through massive MIMO. In: 2013 IEEE Information Theory Workshop, ITW 2013, Sevilla, Spain, September 9-13, 2013, IEEE (2013) 1–5
4. Mukherjee, A., Fakoorian, S.A.A., Huang, J., Swindlehurst, A.L.: Principles of physical layer security in multiuser wireless networks: A survey. CoRR **abs/1011.3754** (2010)
5. Clarke, R.H.: A statistical theory of mobile radio reception. Bell Systems Technical Journal **47** (1968) 957–1000
6. Micciancio, D., Regev, O.: Lattice-based cryptography. In Bernstein, D.J., Buchmann, J., eds.: Post-quantum Cryptography. Springer (2008)
7. Bellare, M., Tessaro, S., Vardy, A.: Semantic security for the wiretap channel. In Safavi-Naini, R., Canetti, R., eds.: Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings. Volume 7417 of Lecture Notes in Computer Science., Springer (2012) 294–311
8. Klein, P.: Finding the closest lattice vector when it's unusually close. In: Proceedings of the Eleventh Annual ACM-SIAM Symposium on Discrete Algorithms.

SODA '00, Philadelphia, PA, USA, Society for Industrial and Applied Mathematics (2000) 937–941
9. Gallager, R.G.: Information Theory and Reliable Communication. Wiley (January 1968)
10. Shannon, C.E.: A mathematical theory of communication. Volume 27. (1948)
11. Wyner, A.: Wire-tap channel concept. Bell System Technical Journal **54** (1975) 1355–1387
12. Csiszar, I., Korner, J.: Broadcast channels with confidential messages. Information Theory, IEEE Transactions on **24**(3) (May 1978) 339–348
13. Maurer, U.: Secret key agreement by public discussion from common information. IEEE Transactions on Information Theory **39**(3) (1993) 733–742
14. Yakovlev, V., Korzhik, V.I., Morales-Luna, G.: Key distribution protocols based on noisy channels in presence of an active adversary: Conventional and new versions with parameter optimization. IEEE Transactions on Information Theory **54**(6) (2008) 2535–2549