ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

Physical-Layer Cryptography through Massive MIMO

Prof. Jyoti Raghatwan, Alka Taur,

RMD Sinhgad School of Engineering, Pune, India

Student, RMD Sinhgad School of Engineering, Pune, India

ABSTRACT: We propose the new technique of physical-layer cryptography based on using a massive MIMO channel as a key between the sender and desired receiver, which need not be secret. The goal is for low-complexity encoding and decoding by the desired transmitter-receiver pair, whereas decoding by an eavesdropper is hard in terms of prohibitive complexity. The decoding complexity is analysed by mapping the massive MIMO system to a lattice. We show that the eavesdropper's decoderfor the MIMO system with M-PAM modulation is equivalent to solving standard lattice problems that are conjectured to be of exponential complexity for both classical and quantum computers. Hence, under the widely-held conjecture that standard lattice problems are hard to solve, the proposed encryption scheme has a more robust notion of security than that of the most common encryption methods used today such as RSA and Diffie-Hellman. Additionally, we show that this scheme could be used to securely communicate without a pre-shared secret and little computational overhead. Thus, by exploiting the physical layer properties of the radio channel, the massive MIMO system provides for low complexity encryption commensurate with the most sophisticated forms of application-layer encryption that are currently known.

KEYWORDS: Cryptography, Lattices, MIMO, Quantum Computing

I. INTRODUCTION

Due to the advancement in multimedia technologies used in communication. Wireless networks channels are more vulnerable to attack. The security architectures provide security mechanism to prevent from attacks. OSI models architecture used seven layers such that physical layer, data link layer, network layer, transport layer, session layer, presentation layer and application layer as shown in Fig.1. There are different security mechanisms which are used according to the type of layer and protocols, In upper layers its essential requirement for data security correction level and mask pattern.

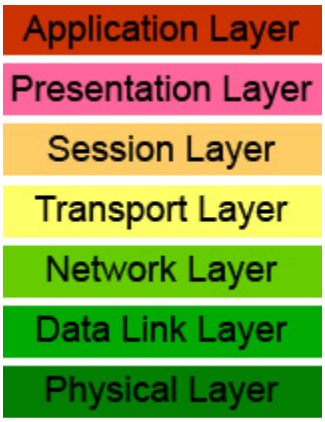

Figure 1.1 Open Systems Interconnection (OSI) model

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

In the fourth generation mobile networks security techniques like substitution and confusion methods, end to end encryption and light weight cryptography used. The encryption of data occurs at the upper layers (application layer, presentation layer) by using the cryptography. While at the physical layer there is also need for data security. For the security of physical links provided by the results of cryptography, signal processing and transmission of information, authentication, confidentiality and integrity are controlled at the upper layers of OSI model by different types of symmetric and asymmetric cryptosystem.

Background

Security is a vital issue in wireless networks due to the broadcast nature of themedium.Traditionally, security has been achieved through cryptographic encryptionimplemented at the application layer, which requires a certain form of information (e.g., key) shared between the legitimate entities. This approach ignores thebehaviour of the communication channels and relies on the theoretical assumption that communication between the legitimate entities is error free. More importantly,all cryptographic measures assume that it is computationally infeasible for them tobe deciphered without knowledge of the secret key, which remains mathematically unproven. Ciphers that were considered potentially unbreakable in the past are continuallydefeated due to the increasingly growth of computational power. Moreover,error free communication cannot be always guaranteed in non-deterministic wireless channels. A novel approach for wireless security taking advantage of the characteristicsof physical layer communication channels was proposed by Wyner in and is referred to as physical layer security. The concept was originally developed forthe classical wire-tap channel. Fig.1.2. Wyner showed that a source(Alice)-destination (Bob) pair can exchange perfectly secure messages with a positiverate if the desired receiver enjoys better channel conditions than the eavesdropper(Eve). However, this condition cannot always hold in practice, especially in wirelessfading channels. To make things worse, Eve enjoys a better average channel gainthan Bob as long as he/she is located closer to Alice than Bob. Therefore, perfectlysecure communication seems impossible, and techniques to enhance Bob's channelcondition while degrading Eve's are needed. One option is to utilize artificial noise(AN) to perturb Eve's reception, as shown in Fig. 1.2. Eves are typicallypassive so as to hide their existence, and thus their CSI cannot be obtainedby Alice. In this case, multiple transmit antennas can be exploited to enhance secrecyby simultaneously transmitting both the information bearing signal and AN.Specifically, precoding is used to make the AN invisible to Bob while degrading thedecoding performance of possibly present Eves. In, authors investigated the secrecy outage probability for the AN-aided secrecy system, where only Alice has multiple antennas. When Eve is also equipped with multiple antennas, the work in employs AN precoder to achieve a near-optimal performance in high signal-to noise(SNR) regime. The contribution extends to a secrecy system where all nodes have multiple antennas in. More recent studies have considered physical layer security provisioning in multiuser networks. Although the secrecy capacity region for multiuser networks remains an open problem, it is interesting to investigate the achievable secrecy rates of such networks for certain practical transmission strategies. All aforementioned work generally assumed that Alice can acquire perfect CSI of Bob, which seems too ideal. Robust beam forming designs with estimated CSI were reported.

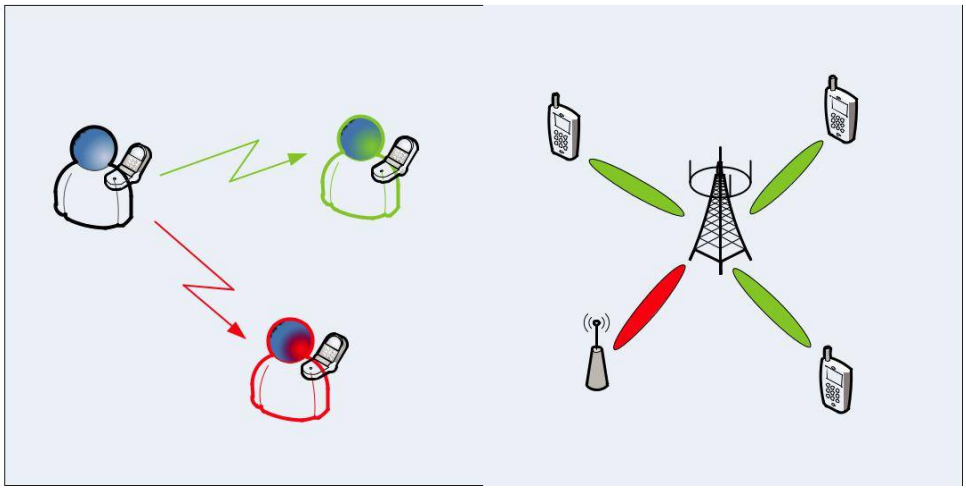

Figure 1.1.1: Physical layer security model.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

1.2 What is Massive MIMO?

MIMO stands for Multiple-input multiple-output. While it involves multiple technologies, MIMO can essentially be boiled down to this single principle: a wireless network that allows the transmitting and receiving of more than one data signal simultaneously over the same radio channel.Standard MIMO networks tend to use two or four antennas. Massive MIMO, on the other hand, is a MIMO system with an especially high number of antennas.

There's no set figure for what constitutes a Massive MIMO set-up, but the description tends to be applied to systems with tens or even hundreds of antennas. For example, Huawei, ZTE, and Facebook have demonstrated Massive MIMO systems with as many as 96 to 128 antennas.

Because MIMO systems need to physically pack more antennas into a small area, they require the use of higher frequencies (and hence shorter wavelengths) than current mobile network standards.

Advantages of Massive MIMO:-

The advantage of a MIMO network over a regular one is that it can multiply the capacity of a wireless connection without requiring more spectrums. Early reports point to considerable capacity improvements, and could potentially yield as much as a 50-fold increase in future.

The more antennas the transmitter/receiver is equipped with, the more the possible signal paths and the better the performance in terms of data rate and link reliability.

A Massive MIMO network will also be more responsive to devices transmitting in higher frequency bands, which will improve coverage. In particular, this will have considerable benefits for obtaining a strong signal indoors.

The greater number of antennas in a Massive MIMO network will also make it far more resistant to interference and intentional jamming than current systems that only utilise a handful of antennas.

1.3 Physical Layer Security in Massive MIMOSystems:

The emerging massive MIMO architecture overs tremendous performance gains interms of network throughput and energy efficiency by employing simple coherent processing on the large-scale antenna array. However, very little attention has beengiven to the security issue in massive MIMO systems. In order to address this concern,we need first to consider two fundamental questions: 1) Is massive MIMO secure? 2)If not, how can we improve security in massive MIMO systems? In this section, weillustrate the main motivation of this thesis by providing brief and general responsesto the two questions.

1. Is Massive MIMO Secure?

Compared with conventional MIMO, massive MIMO is inherently more secure, as the large scale antenna array equipped at the transmitter (Alice) can accurately focus a narrow and directional information beam on the intended terminal (Bob), such that the received signal power at Bob is several orders of magnitude higher than that at any incoherent passive eavesdropper (Eve). Unfortunately, this benefit mayvanish if Eve also employs a massive antenna array for eavesdropping. The followingscenarios further deteriorate the security of the massive MIMO system:

- As Eve is passive, it is able to move arbitrarily close to Alice without beingdetected by either Alice or Bob. In this case, the signal received by Eve can bestrong.
- In a ultra-dense multi-cell network, Bob supers from severe multiuser interference(both pilot contaminated and uncontaminated), while Eve may have access to the information of all other MTs, e.g., by collaborating with them, and remove their interference when decoding Bob's information.
- In practice, both Alice and Bob are equipped with low-cost transceivers toreduce the total expenditure, which are prone to hardware imperfections, whileEve has ideal hardware.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

In the aforementioned scenarios, unless additional measures to secure the communicationare taken by Alice, even a single passive Eve is able to intercept the signalintended for Bob. Furthermore, we note that Eve could emit its own pilot symbolsto impair the channel estimates obtained at Alice to improve his ability to decodeBob's signals during downlink transmission. However, this would also increase the chance that the presence of the eavesdropper is detected by Alice. Therefore, in this thesis, we limit ourselves to passive eavesdropping.

2. How to Improve Security for Massive MIMO?

Massive MIMO systems over an abundance of BS antennas, while multiple transmitantennas can be exploited for secrecy enhancement, e.g., by emitting AN. Therefore,the combination of both concepts seems natural and promising. There arise several challenges and open problems for physical layer security provisioning in massive MIMO systems that are not present for conventional MIMO systems. We summarize them as follows.

- In a conventional massive MIMO system (without security), pilot contaminationconstitutes a limit on performance in terms of data throughput. However, itseffects on the AN design, as well as wireless security have not been considered.
- One of the tremendous advantages of massive MIMO in the physical layer is thesimple processing, e.g., MF precoding. It remains unknown if more advancedand sophisticated signal processing techniques, e.g., ZF/RCI precoding and BScollaboration are beneficial in terms of data throughput and security, in a pilotcontaminated environment.
- In conventional MIMO systems, AN is transmitted in the null space (NS) of thechannel matrix. The complexity associated with computing the NS may not be affordable in case of massive MIMO and thus simpler AN precodingmethods are essential.
- When deployed in practice, low-cost transceivers are equipped to reduce thetotal expenditure. Such components are usually prone to hardware imperfections. The effects of the imperfections on the AN design, as well as the resulting security performance remains an open problem.

II. LITERATURE SURVEY

2.1 Introduction

Zhou, Xiangyun, Lingyang Song, and Yan Zhang [1]Physical layer security has recently become an emerging technique to complement and significantly improve the communication security of wireless networks. Compared to cryptographic approaches, physical layer security is a fundamentally different paradigm where secrecy is achieved by exploiting the physical layer properties of the communication system, such as thermal noise, interference, and the time-varying nature of fading channels.

Mukherjee, Amitav, et al.[2] Author have proposed in the paper provides a comprehensive review of the domain of physical layer security in multiuser wireless networks. The essential premise of physical-layer security is to enable the exchange of confidential messages over a wireless medium in the presence of unauthorized eavesdroppers without relying on higher-layer encryption. This can be achieved primarily in two ways: without the need for a secret key by intelligently designing transmit coding strategies, or by exploiting the wireless communication medium to develop secret keys over public channels.

HienQuoc. Massive MIMO [3] future wireless systems have to satisfy three main requirements: i) having a high throughput; ii) simultaneously serving many users; and iii) having less energy consumption. Massive multiple-input multiple-output (MIMO) technology, where a base station (BS) equipped with very large number of antennas (collocated or distributed) serves many users in the same time-frequency resource, can meet the above requirements, and hence, it is a promising candidate technology for next generations of wireless systems. With massive antenna arrays at the BS, for most propagation environments, the channels become favorable, i.e., the channel vectors between the users and the BS are (nearly) pairwisely orthogonal, and hence, linear processing is nearly optimal. A huge throughput and energy efficiency can be achieved due to the multiplexing gain and the array gain. In particular, with a simple power control scheme, Massive MIMO can offer uniformly good service for all users.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

Rawat, Danda B.[4] Author proposes In this paper, we present an iterative algorithm that adapts transmit signal vector and power of the user using game theory to enhance the physical-layer security (achievable secrecy rate) of massive MIMO system in the presence of eavesdropper and jammers. The proposed algorithm takes account of impact of jammers while meeting the target Signal-to-Interference-plus-Noise Ratio (SINR) and the impact of both eavesdropper and jammers while evaluating the secrecy rate of the users.

Chen, Xiaoming, Jian Chen [5] Author proposes the secrecy transmission with the aid of a large-scale multi-antenna amplify-and-forward (AF) relay wireless powered by the source. Specifically, the wireless energy harvesting (WEH)-enabled relay devices a hybrid receiver architecture, in which the received power at each individual antenna is split for energy harvesting (EH) and information receiving (IR) in the first transmission phase; the aggregate of the total harvested power is further split for cooperative jamming (CJ) to confound the eavesdroppers, and AF for information transmission in the second transmission phase.

2.2 Existing system

As an emerging network security solution, physical layer security (PLS) takes advantage of the intrinsic characteristics of wireless channels, such as noise, interference, and fading, to degrade the received signal qualities at the malicious users, and achieves keyless secure transmission via signal design and signal processing approaches.Comparedwith the traditional cryptographicmethods at upper layers of the protocol stack, PLS has the following technical advantages.
First, PLS does not depend on encryption/decryption operations, thus avoiding the di.culty of distributing and managing secret keys in large-scale heterogeneous 5Gnetworks.
Second, by using PLS approaches, adaptive signal design and resourceallocation can be implemented based on the varying channel conditions, therebyproviding .exible security levels and realizing user-centric security guarantees.
Third, PLS often requires relatively simple signal processing operations, whichtranslates into minor additional overheads.In the past few years, the research on PLS has generated a large body of literature,with the topics ranging from information-theoretical studies to practical schemedesign.
However, it is still challenging to develop innovative PLS solutions that wellmatch the unique features of 5G networks. First, most of the existing PLS schemesonly exploit the characteristics of wireless channels (i.e., link-level propertiesincluding noise, fading, and interference) but underappreciate the significance ofcharacteristics of wireless networks (i.e., network-level properties such as feedback, cooperation, competition, and cognition among users) in security enhancement.Second, the PLS techniques developed so far mainly focus on the optimizationof the secrecy rate or secrecy outage performance.
Yet, 5G is expected to supportvarious application scenarios and diverse wireless services. Different types ofservices have totally different quality-of-service (QoS) requirements, which implies that the PLS protocols should jointly consider various aspects of user demands,including reliability, delay, throughput, and secrecy as well. Third, the existing PLSsolutions often unilaterally pursue the system performance optimization withouttaking into account the limitations in the available resources of practical devices.In 5G-enabled IoT communications, low-cost machine-type devices have verysimple functionalities and very limited power, storage, and processing capabilities.Therefore, most of the existing PLS solutions cannot be directly applied in IoTapplications.The aim of this special issue is to provide a venue to publish innovative PLS solutionsthat address the aforementioned challenges faced by 5G security.
Original research articles as well as review articles from both academia and industry are welcome.Potential topics include but are not limited to the following:Information-theoretic fundamentals for PLSAdvanced signal design and coding techniques for enhanced securityPHY authentication techniques in 5G CSI-based key generation and PHY encryption algorithm designsecure transmission techniques in massive MIMO

III. PROBLEM STATEMENT AND OBJECTIVE

a. Problem Statement

The decoding of massive MIMO systems forms a complex computational problem.Given these distributions, we now precisely define MIMO decoding for the eavesdropper in the MIMO wiretap channel, which we denote as the MIMO-Search problem. The search problem asks us to recover the transmitted vector x without error. We loosely use the term

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

"MIMO decoding problem" to refer to the search problem. In Section V, we discuss how to use the hardness of the problem to construct cryptographically secure systems, and provide a comparison between cryptographer's notions of security with ones used by information theorists.

b. Objective

The main objective of this is for low-complexity encoding and decoding by the desired transmitter-receiver pair, whereas decoding by an eavesdropper is hard in terms of prohibitive complexity. The decoding complexity is analyzed by mapping the massive MIMO system to a lattice. We show that the eavesdropper's decoder for the MIMO system with M-PAM modulation is equivalent to solving standard lattice problems that are conjectured to be of exponential complexity for both classical and quantum computers. Thus, by exploiting the physical layer properties of the radio channel, the massive MIMO system provides for lowcomplexity encryption commensurate with the most sophisticated forms of application-layer encryption that are currently known.
The premise of physical-layer cryptography is to allow the transmission of confidential messages over a wireless channel in the presence of an eavesdropper. We present a model where a given transmitter-receiver pair is able to efficiently encode and decode messages, but an eavesdropper who has a physically different channel must perform an exponential number of operations in order to decode. This allows for confidential messages to be exchanged without a shared key or key agreement scheme. Rather, the encryption exploits physical properties of the massive MIMO channel.

IV. METHODOLOGY

This paper is organized as follows. Section II outlines our system model and the underlying assumptions upon which the security of our system is based. In Section III we discuss lattices, lattice problems, and lattice-based cryptography in order to provide the background for our main result, which is stated in Section IV and proved in Appendix A. In Section V we discuss additional notions of security for our model, including how to achieve security under adversarialmodels commonly considered by cryptographers.

4.1PROBLEM FORMULATION

A. The Wiretap Model
Consider an n×mreal-valued MIMO system consisting of n transmits antennas and m receive antennas:

$$y = Ax + e; \text{ ----------} \quad (1)$$

where x € R^n, and A € $R^{n\times m}$ is the channel gain matrix. Each entry of the channel gain matrix is drawn i.i.d. from theGaussian distribution with zero mean and standard deviation $k/\sqrt{2\pi}$.

We consider real-valued MIMO systems with real-valued channel coefficients and the transmitted signal constellation, X, defined as the set of integers [0;M]. Lattices can easily be scaled and shifted, so we use this constellation without loss of generality over all possible M-PAM constellations.

Let the vector ai €R^n denote the gains between the transmitter and the ith receive antenna, let e_i denote the noise sample at this antenna, and let x represent the transmitted vector which is drawn from X^n. The ith receive antenna gets a noisy, random inner-product of the form

$$yi = \langle a_i, x\rangle + e_i \text{----------} \quad (2)$$

If the noise power is below the required level, efficient decoding methods such as the zero-forcing decoder could be applied to our system. In other words, if these conditions are not met, then our results provide no insight on the complexity of decoding, and hence on the security of the MIMO wiretap channel. Specifically, for some arbitrary m > 0, we require the following constraints on the transmission from user A to user B:

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

Minimum Noise: $m\alpha/k^2>\sqrt{n}$ ---------- (3)

Constellation Size: $M > m2^{n\log\log n / \log n}$ ---------- (4)

where the parameter m may be chosen by a user or system designer in order to trade off the SNR requirement for the size of the constellation.
Now consider an eavesdropper, εVε, which has poly(n) receive antennas, and receives message x with channel represented by B. Now consider the message received by εVε:

$\tilde{y} = BVx + \tilde{e}$ ---------- (5)

B. MIMO Signal Distributions
In this subsection, we define various distributions that are used in our problem. Specifically, we discuss distributions of lattice points and distributions that can be empirically related to received MIMO signals. Below, we define two distributions: AM , α, k, which is continuous and DA, α which is discrete. Both of these distributions assume that x is drawn uniformly at random over X^n. For other distributions on x; AM , α, k, and DA, αare entirely determined by the second moment of the distribution of x.

C. The MIMO Decoding Problem
Given these distributions, we now precisely define MIMO decoding for the eavesdropper in the MIMO wiretap channel,which we denote as the MIMO-Search problem. The search problem asks us to recover the transmitted vector x withouterror. We loosely use the term "MIMO decoding problem" torefer to the search problem. In Section V, we discuss how touse the hardness of the problem to construct cryptographicallysecure systems, and provide a comparison between cryptographer'snotions of security with ones used by informationtheorists. In Appendix A, we prove that the search problem isas hard as solving certain lattice problems.We wish to show that the MIMO decoding problem, definedbelow, is hard to solve, i.e., that this decoding is of exponential complexity in the number of transmit antennas. We say that analgorithm solves this problem if it returns the correct answerwith a probability greater than $1 - n^{-c}$, for some $c > 0$.

4.2 LATTICES
We now provide an overview of lattices and lattice-based cryptography. This section contains all of the concepts usedin the cryptography literature that are required in the proof of our main result. We first define several problems on lattices that are all conjectured to be hard to solve and are all used in the proof of our main result to show that MIMO decoding is at least as hard as solving standard lattice problems. Wenext provide a discussion on the complexity of solving theselattice problems, followed by a discussion on the Learning With Errors (LWE) problem. The Learning With Errors problem has a striking similarity to the problem of MIMO decoding. We follow a very similar approach to show the hardness of MIMO decoding as is used to show the hardness of LWE decoding.

A. Lattice-Based Cryptography
In recent years, lattice-based cryptography has becomea very attractive field for cryptographers for a number ofreasons. The security guarantees provided by many latticebased schemes far exceeds that of many modern schemes suchas RSA and Diffie-Hellman, since lattice problems enjoy an average to-worst case connection, as discussed in AppendixB. Lattice problems also appear to be resistant to quantumcomputers. The creation of such computers poses a significant challenge to the state of modern cryptography, since a quantumcomputer could break most modern number-theoretic schemes.
Lattice-based cryptography provides a wide variety of tools to create many different cryptographic constructions. We here reference some of these constructions as it is possible that some of them could be applied to the MIMO decoding problem or even that the MIMO decoding construction could inspire entirely new cryptographic constructions.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

V. ALGORITHMS

1. Algorithm 1 MIMO-OAEP+
2. Algorithm 2 Key-Agreement Scheme.

1. Algorithm 1 MIMO-OAEP+:

Let K = n logM be the number of bits transmitted per MIMOchannel use. Alice wishes to send Bob a message, m, that isη = K - 2n bits. Assume Alice and Bob both have access to three random oracle functions: G:{0, 1}^{n}→{0, 1}^{n} , H':{0,1}$^{n+n}$→{0, 1}^{n}, H:{0,1}$^{n+n}$ →{0, 1}^{n}. Alicedraws r uniformly at random over {0,1}$^{n+n}$ and computess€{0,1}$^{n+n}$; t €{0, 1}^{n}, x € {0, 1}^{k} as shown underEncryptbelow. Alice then multiplies x by the right singularvectors of Bob's channel and transmits the message to Bob.Bob recovers x through his channel and then recovers m using the procedure shown under Decrypt. Bob verifiesthat c = H'(r‖m). If these quantities are not equal then Bobhas not properly received Alice's message and he rejects.

Encrypt
s = (G(r) + m) ‖H'(r‖m)
t = H(s) +r
x = s‖t

Decrypt
s = x[0,....,η+n-1]
t = x[η+ n,...,k]
r = H(s) +t
m = G(r) + s[0,...,η- 1]
c = s[η,...,η+ n -1]
c = H' (r‖m)

2. Algorithm 2 Key-Agreement Scheme:

Alice wishes to send Bob η secret bits. Alice generates some number c = c(n), such that 2c $\sqrt{n}\log M\ log1.005$>η,of random messages m €(0;M)^n and sends them to Bob over the MIMO channel with channel parameters meeting the constraints in Theorem 1. Alice and Bob ensure that the message is exchanged without error for example through channel coding. Alice and Bob then hash the message (after decoding if channel coding is used), using a universal hash which outputs ηbits and use the result as their secret.

VI. CONCLUSION

We have demonstrated that the complexity of an eavesdropper decoding a large-scale MIMO systems with M-PAMmodulation can be related to solving certain lattice problems which are widely conjectured to be hard. This suggests thatthe complexity of solving these problems grows exponentiallywith the number of transmitter antennas.
Unlike the computationally hard problems underlying many of the most commonencryption methods used today, such as RSA and Diffie-Hellman, it is believed that the underlying lattice problems are hard to solve using a quantum computer, and thus this schemepresents a practical solution to post-quantum cryptography. It is not new to exploit properties of a communicationchannel to achieve security; however, to our knowledge, thisis the first scheme which uses physical properties of thechannel to achieve security based on computational complexityarguments. Indeed, the notion of the channel is not typically considered by cryptographers.
We thus describe our system asa way of achieving physical-layer cryptography.Further novel to our scheme is the role that the channel gainmatrix plays in decoding. A transmitted message can only bedecoded by a user with the corresponding channel gain matrix. The channel gain matrix, or more specifically the precodingof the message using the right-singular vectors of the channelgain matrix, essentially plays the role of a secret key in thatit allows for efficient decoding at the receiver.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

However, thisvalue does not need to be kept secret, nor does it play the traditional role of a public key. We term this type of key asthe Channel State Information- or CSI-key. In cryptographyterminology, this system is a trapdoor function, for which the trapdoor varies both spatially and temporally. The fact thatthis is a new type of cryptographic primitive suggests thepossibility of entirely new cryptographic constructions.

We have used the hardness result, in conjunction with anew notion of computational secrecy capacity, to construct a method in which two users can perform a key-agreementscheme, without a pre-shared secret. In addition, we give ascheme that allows Alice and Bob to securely communicatein the presence of an eavesdropper. We relate the parametersrequired to maintain security to SNR requirements and constellation size and show that they are practical to achieveassuming a system with enough transmitter antennas andthe corresponding number of receivers, and relatively largeconstellation sizes.

REFERENCES

[1] J.Katz, and Y. Lindell, Introduction to Modern Cryptography. New York: Chapman & Hall/CRC, 2007.
[2] M. O. Damen, H. El Gamal, and G. Caire, "On maximum likelihood detection and the search for the closest lattice point", IEEE Trans. Inf.Theory, vol. 49, no. 10, pp.2389–2402, 2003.
[3] D. Micciancio and O. Regev, "Lattice-based Cryptography," in Post- Quantum Cryptography, Berlin, German: Springer Berlin/Heidelberg,pp. 147–191, 2009.
[4] D. Micciancio and S. Goldwasser, Complexity of Lattice Problems: ACryptographic Perspective. Boston, MA: Kluwer Academic Publishers,Mar. 2002.
[5] M. Ajtai, "Generating hard instances of lattice problems", Complexity of computations and proofs, vol. 13 of Quad. Mat., pp. 1–32, 2004.Preliminary version in STOC 1996.
[6] O. Goldreich and S. Goldwasser. On the limits of nonapproximability of lattice problems. Journal of Computer and System Sciences, 60(3):540-563, 2000. Preliminary version in STOC 1998.
[7] D. Aharonov and O. Regev. Lattice problems in NP intersect coNP. J. of the ACM, 52(5):749–765, 2005. Preliminary version in FOCS 2004.
[8] S. Khot. Hardness of approximating the shortest vector problem inlattices. InProc. 45th Annual IEEE Symp. on Foundations of ComputerScience (FOCS), pages 126–135, 2004.
[9] I. Haviv and O. Regev. Tensor-based hardness of the shortest vector problem to within almost polynomial factors. In Proc. 39th ACM Symp. on Theory of Computing (STOC), pp. 469–477, 2007.
[10] D. Micciancio. The shortest vector in a lattice is hard to approximate to within some constant. SIAM J. on Computing, 30(6): 2008–2035, 2001.
[11] D. Boneh, E. Goh, and X. Boyen, "Hierarchical Identity Based Encryption with Constant Size Ciphertext", Proc. of Eurocrypt '05, LNCS 3493, pages 440–456, 2005.
[12] C. Peikert, V. Vaikuntanathan, and B. Waters, "A framework for efficient and composable oblivious transfer", in Proc. of CRYPTO '08, 2008, pp. 554–571.
[13] D. Micciancio, and S. P. Vadhan. "Statistical zero-knowledge proofs with efficient provers: Lattice problems and more". In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 282–298. Springer, Heidelberg (2003).
[14] A. Banerjee, C. Peikert, and A. Rosen. "Pseudorandom functions and lattices", Proc. of CRYPTO '12: 719-737.
[15] C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, Dept. of Comp. Sci., Stanford Univ., Stanford, CA, 2009.
[16] V. Shoup. "OAEP Reconsidered." Annual International Cryptology Conf. Springer Berlin Heidelberg, 2001.
[17] M. Bellare and P. Rogaway. Optimal asymmetric encryption. In Advances in Cryptology—Eurocrypt '94, pgs. 92–111, 1994.