Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 7 – No. 13, February 2018 – www.caeaccess.org

PUF-based Privacy-Preserving RFID Protocol

Ali M. Allam
Associated Professor
Department of Applied Natural Sciences, UCC, Qassim University, Unaizah, 51911, PO box 4394, Saudi Arabia
Department of Electronic, Communication and Computer Engineering, Faculty of Engineering, Helwan University, PO box 11792, Cairo, Egypt

ABSTRACT
The limitation of RFID tag resources plays a great challenge for the researchers to implement an applied RFID scheme which is privacy-preserving, efficient and suitable for a low-cost tag. In this paper, we suggest a privacy-preserving mutual authenticated key establishment protocol for RFID systems with no computational or storage consumption. Our scheme is based on the utilization of the fading channel features and the use of Physically Unclonable Functions (PUFs). Firstly, we exploit the resources provided by the time-varying channel gains to share a common randomization source between RFID reader and its tags, for key establishment. Secondly, we use PUF for tags authentication and improving the key generation rate of our suggested protocol. We determine the upper bound for the generation rate of a secret key shared among reader and tag, and give numerical examples to reveal the performance of our suggested technique.

General Terms
Wireless Communication, Security.

Keywords
Information-theoretic security; key generation; Channel reciprocity; RFID system; PUF

1. INTRODUCTION
Lately, Radio Frequency Identification (RFID) [1-12] has attract a great attention as a new spotlight technology for assisting the computing systems everywhere. In the existing open network situation, RFID recognizes an entity via radio frequency technique which is a type of non-contact automatic identification method. It can spontaneously get the information from a lot of tags immediately. Consequently, RFID technology has been commonly used by manufacturing management, care monitoring, supervision of people and good tracking, organization of books at bookstores, etc.

The information security is the vital issue in the current RFID schemes. It implies that those present RFID frameworks bring a few security issues and challenges. In the regular RFID schemes, the communication network among the reader and the backend database is considered to be secure. On the other hand, since the communication channel between the RFID tag and the reader is not secure channel, it can be straightforwardly attacked by passive or active opponents. Therefore, protected RFID schemes must be able to counterattack any type of attack, such as eavesdrop, modification, tracing etc., and also provides the three basic security services including privacy, identification and non-traceability [1-4].

Overall, RFID tags have very inadequate computing recourses, memory and stored energy. Due to these features and a lot of limitations, it is a challenge to design the security structure of the RFID scheme. Presently, the most frequent design technique is to use secure one-way hash function, bit-wise exclusive-or (XOR) operation, PRNG (pseudo-random number generator) etc. Up to now, most RFID authentication protocols are based on these cryptographic mechanisms. Therefore, in the RFID scheme, it is an important challenge to design an efficient and secure protocol which can be used in the low-cost tag [1-4].

In 2007, He et al. [12] suggested an authentication and key agreement (AKA) protocol which is used in the operation of communication between the low-cost tag and reader. They also verified the security of the protocol through the extended strand space model [13-15]. In [16], the authors offered a more efficient authentication and key agreement (AKA) protocol which is used in the operation of communication between the low-cost tag and reader for RFID scheme than He et al.'s AKA protocol. Compare with He et al.'s AKAP protocol, the proposed AKA protocol reduces the computational costs as well as protocol communication rounds to agree a shared session key between the reader and the tag.

Most of the suggested solution for authentication and key agreement for RFID systems [17-18] based on cryptographic tools which consume the energy and computation recourses of the limited capabilities tags. In this paper we suggest a solution based on non-cryptographic mechanisms. More precisely, we use physical unclonable functions (PUFs) as challenge-response authentication technique, beside the channel-based key generation technique for shared secret key generation. In the following points, our contribution will be summarized:

- Figure out the secret key generation between reader and tag based on the reciprocity feature of wireless communication channel in time division duplex (TDD) mode.
- Calculate the key rate of the suggested protocol, and try to improve the generated rate using the PUF technique.
- Suggest a mutual authentication between the reader and the tag based on challenge-response mechanism.

The rest of the paper is organized as follows. Section 2 describes the system model under investigation and provides the assumption necessary for our suggested schemes. We discuss the authenticated key generation protocol and derive its secret key rate in sections 3. Numerical results are presented in section 4; finally, concluding notes are given in section 5.

Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 7 – No. 13, February 2018 – www.caeaccess.org

2. SYSTEM MODEL

Our suggested protocol provides two security services, privacy preserving by exchanging a secret key between entities, and mutual authentication. The system model for the mutual authenticated key generation scheme and its associated system assumption demonstrated as follows.

2.1 Physically Unclonable Function

Physically unclonable functions or PUFs are innovative physical security primitives which produce unclonable and inherent instance-specific measurements of physical objects. PUFs are one-way functions that are embodied in, a physical structure [19]. The main security properties of PUFs are uncloneability and unpredictability. A PUF feeds with an input challenge $C_i \in C$, where C the set of all possible challenges is, and its output is a response $R_i \in R$, where R is the set of all possible responses. A PUF depends on the random variations during the fabrication of its corresponding circuit, even two PUFs with the same design results in two different functions. In other words, it is physically difficult to make two PUFs perform identically.

2.2 Channel-Based Key Generation

During a fading block duration, two authentic terminals tries to establish a shared secret key depending on the common observation for the channel status of link between them in wireless communication system. We assume that all the parties in the system are half-duplex terminals. If RFID reader A sends a training sequence X_A in a given channel use, then tag B gets

$$Y_B = h_{AB}X_A + N_B \qquad (1)$$

in which h_{AB} is the channel status between reader A and tag B, N_B is zero mean univariate normal distribution noise with variance σ^2. Similarly, if tag B sends X_B in a given channel use, then reader A gets

$$Y_A = h_{BA}X_B + N_A \qquad (2)$$

in which h_{BA} is the channel status between tag B and reader A, due to the reciprocity feature for time division duplex system (TDD), $h_{AB} = h_{BA}$, N_A is zero mean univariate normal distribution noise with variance σ^2. We assume that the univariate normal distribution noise at the terminals are uncorrelated of each other.

Due to TDD mode, we assume the channel gains for a link is reciprocal, i.e. $h_{AB} = h_{BA}$. Furthermore, we suppose that no terminal has any information about the channel properties of the communication links before communicating with the other terminal; however, channel state information statistical distributions presented at each party. For clarification, we suppose that all channel gains are univariate normal distribution with zero means. In addition, we consider that the fading coefficient of the wireless channel remains unchangeable for a duration T, after that it switches randomly to another independent quantity at the start of each cycle of T, which is recognized as slow block fading type in the literature. Note that these assumptions are regularly utilized in most of the current associated research for the generation of shared secret key in wireless communication in TDD mode [20–22].

For each terminal, let $X_n = [x_n(1), \dots, x_n(L_n)]^T$ represent the signals sent by terminal $n \in \{A, B\}$ in L_n channel uses. As in [23], we suppose that the transmitted power constraint for each terminal is equal for simplicity, i.e.

$$\frac{1}{L_n}\mathbb{E}\{X_n^T X_n\} \le P, \forall\, n \in \{A, B\}. \qquad (3)$$

All the authentic terminals in the network desire to have a common secret key among them, by exchanging messages through wireless channels. We denote the pairwise key generation function associated with terminal n as f_n, i.e., $K_n = f_n(S_n, Y_n)$, where Y_n is the signals received by terminal n, and S_n is the probe signal transmitted by terminal n. A secret key rate R_L is said to be *feasible* if, for any $\epsilon > 0$, there occurs an algorithm and a random variable K such that

$$Pr(K_n \ne K) \le \epsilon, n = 1,2, \qquad (4)$$

$$\frac{1}{N}H(K) \ge R_L - \epsilon. \qquad (5)$$

Here (4) denotes that the secret key K generated at all the terminals depending on the using the function is equal with high probability. Finally, (5) insure that the rate of the generated key is at least equal to the normalized entropy of the generated key.

3. PROPOSED PROTOCOL

In this section, we suggest the scheme of mutual authenticated key establishment between a reader A and a tag B in RFID scheme. We then calculate the key rate that can be established.

Our suggested key generation scheme is composed of two stages. The first stage is establishing a shared secret key between reader and the tag based on the common observation of the channel status of the channel between them. Then, the second stage uses the PUF technique to compute the final key off-line beside the mutual authentication between the two terminals. The details of the protocol is discussed as follow.

Stage 1: Generation of a shared secret pre-key.

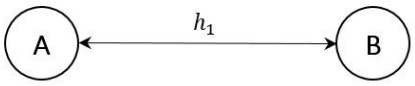

Fig. 1: System model.

The system model for the suggested scheme is shown in figure1, where the two terminals attempt to establish a secret pre-key from the common observation of the channel gain h_1 of the link between them. The corresponding resource element of the scheme is shown in figure 2, where the coherence time T is split to two training allocation sequence, so that both terminals can estimate the channel status h_1, channel training sequence αT in which tag B estimates h_1 and training sequence $(1-\alpha)\,T$ in which reader A realizes common randomness source h_1. Table 1 summarized the notations used in this paper.

Each of reader A and tag B first gets an estimation of the channel status through training. That is, at the start of each coherence time, reader A transmits an identified probe signal S_A to the wireless channel, tag B gets an estimation of the channel status h_1, and then tag B transmits an identified probe signal S_B to the wireless channel from which reader A gets an estimation of the channel status h_1.

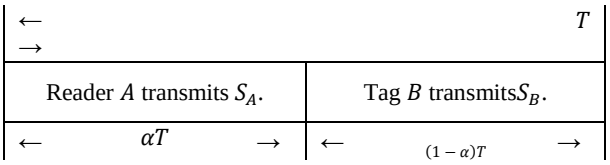

Fig. 2: Time Frame

Table 1: Notations

$\tilde{Y}_A$	Common observation at reader ***A*** for the TDD link status.
$\tilde{Y}_B$	Common observation at tag *B* for the TDD link status.
h_1	Channel status for the path between *A* to *B*, $\sim\mathcal{N}(0,\sigma_1^2)$.
S	Signal Prob.
N_A	Noise at reader *A*, $\sim\mathcal{N}(0,\sigma^2)$.
N_B	Noise at tag *B*, $\sim\mathcal{N}(0,\sigma^2)$.

After that, they can observe a common composed channel gains h_1.These two observation will not be similar, but will be correlated. In our scheme, reader *A* and tag *B* will establish a key from these correlated observations. We will explore the details of the procedure as follows.

Suppose reader *A* transmits an identified probe signal S_A of size $1 \times \alpha T$. Tag *B* receives

$$Y_B = h_1 S_A + N_B \quad (6)$$

where $N_B = [N_B(1), \dots, N_B(\alpha T)]^T$. Similarly, tag *B* transmits an identified probe signal S_B of same size $1 \times (1 - \alpha T$ through the wireless channel, and reader *A* gets

$$Y_A = h_1 S_B + N_A \quad (7)$$

where $N_A = \left[N_A(1), \dots, N_A\big((1-\alpha)T\big)\right]^T$.

Reader *A* and tag *B* use Y_A and Y_B respectively, to establish a shared secret key from these two correlated observations based on the source model technique [24].

In our scheme, reader *A* figure out $\tilde{Y}_A$ from Y_A through

$$\tilde{Y}_A = \frac{S_B^T}{\|S_B\|^2} Y_A,$$

$$\tilde{Y}_A = h_1 + \frac{S_B^T}{\|S_B\|^2} N_A \quad (8)$$

in which $\|\cdot\|$ signifies the norm of its argument. Also, tag *B* figure out $\tilde{Y}_B$ from Y_B through

$$\tilde{Y}_B = \frac{S_A^T}{\|S_A\|^2} Y_B$$

$$\tilde{Y}_B = h_1 + \frac{S_A^T}{\|S_A\|^2} N_B \quad (9)$$

As shown, the channel gain h_1 will play the role of the common randomness source used to generate a secret key from it.

The secret key capacity generated between reader *A* and tag *B*, denoted by $S(\tilde{Y}_A; \tilde{Y}_B)$, is defined as the maximum of all possible secret key rates. In [25], the secret key capacity between two nodes is specified as follow

$$S(\tilde{Y}_A; \tilde{Y}_B) = I(\tilde{Y}_A; \tilde{Y}_B) \quad (10)$$

This means that, the generated secret key capacity depends on the mutual information of the common observation between reader *A* and tag .

Reader *A* and tag *B* will establish a key from these two correlated observations. As will be express in consequence, our scheme will establish a key from $(\tilde{Y}_A, \tilde{Y}_B)$ with a rate

$$R_L = \frac{1}{T} I(\tilde{Y}_A; \tilde{Y}_B) \quad (11)$$

The normalization factor $\frac{1}{T}$ is due to the changing of channel characteristics every T sequences times, i.e., the path gain between parties remain consists only for a block of T sequences times. Generally, $I(\tilde{Y}_A; \tilde{Y}_B)$ is the common randomness that both reader *A* and tag *B* share.

Assuming that reader *A* and tag *B* transmit with power P_A and P_B respectively, throughout the training phase, we have $\|S_A\|^2 = \alpha T P_A$ or $\|S_B\|^2 = (1-\alpha) T P_B$ according to the transmitted terminal.

We can rewrite R_L as follows:

$$TR_L = I(\tilde{Y}_A; \tilde{Y}_B) \quad (12)$$

$$= H(\tilde{Y}_A) - H(\tilde{Y}_A|\tilde{Y}_B) \quad (13)$$

$$= H(h_1 + \mathrm{N}_1) - H(\tilde{Y}_A|\tilde{Y}_B) \quad (14)$$

According to [26], we have

$$H(\tilde{Y}_A|\tilde{Y}_B) = H(\tilde{Y}_A - c\tilde{Y}_B|\tilde{Y}_B) \quad (15)$$

$$\leq H(\tilde{Y}_A - c\tilde{Y}_B) \quad (16),$$

Since, $(\tilde{Y}_A, \tilde{Y}_B)$ are jointly Gaussian and if we choose

$$c = cov(\tilde{Y}_A, \tilde{Y}_B) / var(\tilde{Y}_B) \quad (17).$$

Then, $(\tilde{Y}_A - c\tilde{Y}_B)$ and $\tilde{Y}_B$ are independent, and the upper bound for $H(\tilde{Y}_A|\tilde{Y}_B)$ is

$$H(\tilde{Y}_A|\tilde{Y}_B) = H(\tilde{Y}_A - c\tilde{Y}_B) \quad (18).$$

Since,

$$c\tilde{Y}_B = \mathcal{N}\big(0, c^2 var(\tilde{Y}_B)\big) \quad (19)$$

$$= \mathcal{N}\left(0, \Big(cov(\tilde{Y}_A, \tilde{Y}_B)\Big)^2 / var(\tilde{Y}_B)\right) \quad (20)$$

$$R_L = \frac{1}{T}\left[H(h_1 + \mathrm{N}_1) - H(\tilde{Y}_A - c\tilde{Y}_B)\right]^+ \quad (21)$$

Since, $\tilde{Y}_A$ is a zero mean Gaussian random variable, with variance

$$\sigma_1^2 + \frac{\sigma^2}{\|S_B\|^2} \quad (22),$$

and similarly, $\tilde{Y}_B$ is a zero mean Gaussian random variable, with variance

$$\sigma_1^2 + \frac{\sigma^2}{\|S_A\|^2}. \quad (23)$$

The resultant rate from the common observation $(\tilde{Y}_A, \tilde{Y}_B)$ is:

$$R_L = \frac{1}{T}\left[H(h_L + \mathrm{N}_1) - H(\tilde{Y}_A - c\tilde{Y}_B)\right]^+ \quad (24)$$

$$R_L = \frac{1}{2T} log\left[\frac{var(\mathrm{h}_1) + var(\mathrm{N}_1)}{var(\tilde{Y}_A) - \frac{\left(var(\mathrm{h}_1)\right)^2}{var(\tilde{Y}_B)}}\right]^+ \quad (25)$$

$$R_L = \frac{1}{2T} log\left(\frac{\sigma_1^2 + \frac{\sigma^2}{\|S_B\|^2}}{\sigma_1^2 + \frac{\sigma^2}{\|S_B\|^2} - \frac{\sigma_1^4}{\sigma_1^2 + \frac{\sigma^2}{\|S_A\|^2}}}\right) \quad (26)$$

Stage 2: Mutual Authentication.

The reader selects randomly challenge response pair CRP and sends C_i with length n bits to the tag. The tag feeds the challenge to its embedded PUF device and gets the corresponding R_i with length n bits according to PUF design. The resultant key is bit-wise exclusive–or operation between the key generated from the first stage and the response of the PUF with final rate $R_L + n$. Of course the final generated key

is established off-line which increase privacy level of the protocol.

At the same time, the authentication is done due to the correction of the final key depending to the response R_i of the challenge C_i.

4. NUMERICAL RESULTS

From the secret key rate formulate that dreived in the privous section, we can deduce the parameters affect the rate as follow:

- Coherence duration.
- Training sequence allocation, which is managed by alpha (allocation coefficent).
- Transmitted power consterint.
- Channle gains.

In this section, we present various simulation results to illustrate the performance of our suggested scheme, and show the effect of each parameter on the secret key rate, so that we can get the suitable condition for non-zero rate key generation.

We follow the same values of the parameters for all the papers in this field [20-22].

The value of the simulation parameters is summarized in table 2.

Table 2. Value of the simulayion paramters

Parameter	T	σ_1^2	σ^2
Value	99	0.3	0.1

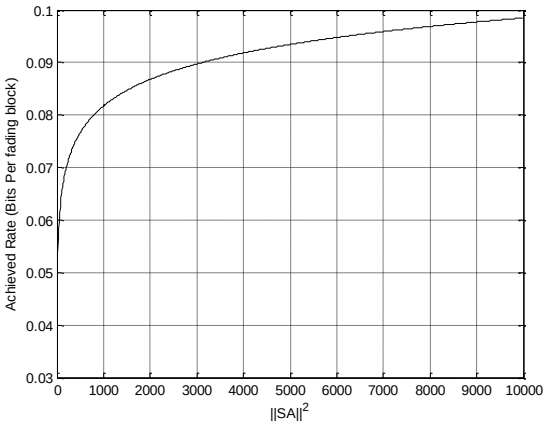

Fig. 3: Secret key rate vs transmitted power.

First, we consider the influence of the transmitted power on the secret key rate as shown in fig. 3. The figure shows that as the transmitted power with equal power allocation for reader A and tag B increase the generation rate of the secret key per channel use increase.

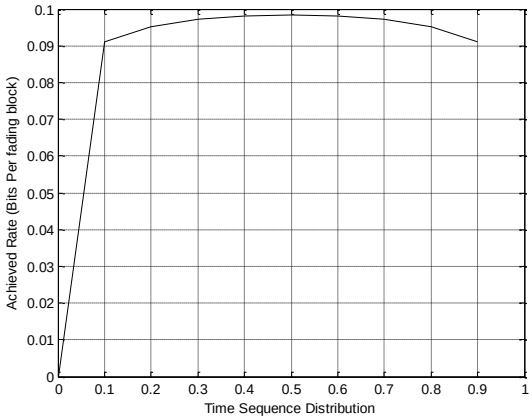

Fig. 4: Secret key rate vs Time sequence allocation distribution

In figure 4, we consider the influence of the distribution of the training sequence allocation for both terminals on the secret key rate. The figure shows that the maximum key rate under the suggested parameters values presented at $\alpha \in [0.4,0.6]$. i.e., equal time allocation distribution between both terminals training time allocation give maximum key rate. This because that the information about the channel is distribute during this two periods.

5. CONCLUSION

In this paper, we propose an efficient mutual authenticated key establishment protocol which is tolerated for the communication between the low-cost tag and reader for RFID system. Our protocol is based on the channel reciprocity of the fading channel for wireless communication to share a common randomness source between entities. Furthermore, our proposed scheme provides mutual authentication between the reader and the tag by using PUFs. The proposed protocol does not require non-volatile memory or cryptographic primitives on both the reader and the tag. Also, we improve the key generation rate of our protocol by using the response bit string of PUF to increase the bit length of the generated key from the channel-based scheme.

6. ACKNOWLEDGMENTS

The author gratefully acknowledge Qassim University represented by the Deanship of Scientific Research for the material support for this research under the number (2040-ucc-2016-1-12-S) during the academic year 1437 AH/2016AD.

7. REFERENCES

[1] Yang, A., Liang, K., Zhuang, Y., Wong, D. and Jia, X. (2015). A new unpredictability-based radio frequency identification forward privacy model and a provably secure construction. *Security and Communication Networks*, 8(16), pp.2836-2849.

[2] Zhang, Y.-L., & Guo, H. (2010). An Improved RFID Privacy Protection Scheme Based on Hash-Chain. *2010 International Conference on Logistics Engineering and Intelligent Transportation Systems*.

[3] Avoine, G., & Oechslin, P (2005). A Scalable and Provably Secure Hash-Based RFID Protocol. *Third IEEE International Conference on Pervasive Computing and Communications Workshops*, pp. 110-114.

[4] Xiao, M., Shen, X., Wang, J., & Crop, J. (2011). Design of a UHF RFID tag baseband with the hummingbird cryptographic engine. *2011 9th IEEE International Conference on ASIC*.

[5] Kaiser, U (2005). UICE: a low-power high-speed cryptographic module for RFID and embedded systems. *Proceedings of the 2005 European Conference on Circuit Theory and Design, 2005*.

[6] Narayanaswamy, J., Sampangi, R. V., & Sampalli, S. (2014). SCARS: Simplified cryptographic algorithm for RFID systems. *2014 IEEE RFID Technology and Applications Conference (RFID-TA)*.

[7] Alagheband, M. R., & Aref, M. R. (2012). Unified privacy analysis of new-found RFID authentication protocols. *Security and Communication Networks*, *6*(8), 999–1009.

[8] Chabanne, H., & Fumaroli, G. (2006). Noisy Cryptographic Protocols for Low-Cost RFID Tags. *IEEE Transactions on Information Theory*, *52*(8), 3562–3566.

[9] eris-Lopez, P., Hernandez-Castro, J. C., Tapiador, J. M. E., Palomar, E., & Lubbe, J. C. V. D. (2010). Cryptographic puzzles and distance-bounding protocols: Practical tools for RFID security. *2010 IEEE International Conference on RFID (IEEE RFID 2010)*.

[10] YANG, C. and ZHANG, H. (2013). RFID authentication protocol based on secret-sharing scheme. *Journal of Computer Applications*, 32(12), pp.3458-3461.

[11] Mustapha, B., Djeddou, M. and Drouiche, K. (2016). An ultralightweight RFID authentication protocol based on Feistel cipher structure. *Security and Communication Networks*, 9(18), pp.6017-6033.

[12] He, L., Gan, Y., LI, N.N., Cai, Z.Y. (2007). A Security-provable Authentication and Key Agreement Protocol in RFID System. *International Conference on Wireless Communications, Networking and Mobile Computing, 2007*, 1(1), pp. 2078-2080.

[13] Benssalah, M., Djeddou, M. and Drouiche, K. (2016). Dual cooperative RFID-telecare medicine information system authentication protocol for healthcare environments. *Security and Communication Networks*, 9(18), pp.4924-4948.

[14] XIE, C. (2011). RFID authentication protocol based on Hash function and key array. *Journal of Computer Applications*, 31(3), pp.805-807.

[15] LIU, P., ZHANG, C. and OU, Q. (2013). Authentication protocol of mobile RFID based on Hash function. *Journal of Computer Applications*, 33(5), pp.1350-1352.

[16] Yoon, E. and Yoo, K. (2008). An Efficient Authentication and Key Agreement Protocol in RFID System. *Lecture Notes in Computer Science*, pp.320-326.

[17] ZHANG, X., CAI, W. and WANG, Y. (2013). Enhanced minimalist mutual-authentication protocol for RFID system. *Journal of Computer Applications*, 32(9), pp.2395-2399.

[18] LI, H. and LIU, D. (2013). Matrix-based authentication protocol for RFID and BAN logic analysis. *Journal of Computer Applications*, 33(7), pp.1854-1857.

[19] Katzenbeisser, S. and Schaller, A. (2012). Physical Unclonable Functions. *Datenschutz und Datensicherheit - DuD*, 36(12), pp.881-885.

[20] Zhou, H., Huie, L. and Lai, L. (2014). Secret Key Generation in the Two-Way Relay Channel With Active Attackers. *IEEE Transactions on Information Forensics and Security*, 9(3), pp.476-488.

[21] Khisti, A. (2016). Secret-Key Agreement Over Non-Coherent Block-Fading Channels With Public Discussion. *IEEE Transactions on Information Theory*, 62(12), pp.7164-7178.

[22] Lai, L., Liang, Y. and Poor, H. (2012). A Unified Framework for Key Agreement Over Wireless Fading Channels. *IEEE Transactions on Information Forensics and Security*, 7(2), pp.480-490.

[23] Zeinali, V. and Khaleghi Bizaki, H. (2016). Shared Secret Key Generation Protocol in Wireless Networks Based on the Phase of MIMO Fading Channels. *Wireless Personal Communications*, 89(4), pp.1315-1334.

[24] Ren, K., Su, H. and Wang, Q. (2011). Secret key generation exploiting channel characteristics in wireless communications. *IEEE Wireless Communications*, 18(4), pp.6-12.

[25] Csiszar, I. and Narayan, P. (2000). Common randomness and secret key generation with a helper. *IEEE Transactions on Information Theory*, 46(2), pp.344-366.

[26] Médard, M. (1997). Capacity of correlated jamming channels. *in Proc. Allerton Conf. Communication, Control, and Computing*, Monticello, IL.