Robust Key Agreement From Received Signal Strength in Stationary Wireless Networks

Aiqing Zhang[1,2], Xinrong Ye [1] , Jianxin Chen [1,3], Liang Zhou*[1,3], and Xiaodong Lin [4]

[1] The Key Lab of Broadband Wireless Communication and Sensor Network Technology, NJUPT, Ministry of Education, China.
[e-mail:aqzhang2006@163.com,chenjx@njupt.edu.cn,liang.zhou@njupt.edu.cn]
[2] College of Physics and Electronic Information Engineering, Anhui Normal University, China.
[e-mail:yaya_ye@126.com]
[3]Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, NJUPT, China.
[4]Faulty of Business and Information Technology, University of Ontario Institute of Technology, Canada
{e-mail:Xiaodong.Lin@uoit.ca}
*Corresponding author: Liang Zhou

Received March 17, 2016; revised April 20, 2016; accepted May 8, 2016; published May 31, 2016

Abstract

Key agreement is paramount in secure wireless communications. A promising approach to address key agreement schemes is to extract secure keys from channel characteristics. However, because channels lack randomness, it is difficult for wireless networks with stationary communicating terminals to generate robust keys. In this paper, we propose a Robust Secure Key Agreement (RSKA) scheme from Received Signal Strength (RSS) in stationary wireless networks. In order to mitigate the asymmetry in RSS measurements for communicating parties, the sender and receiver normalize RSS measurements and quantize them into q-bit sequences. They then reshape bit sequences into new l-bit sequences. These bit sequences work as key sources. Rather than extracting the key from the key sources directly, the sender randomly generates a bit sequence as a key and hides it in a promise. This is created from a polynomial constructed on the sender's key source and key. The receiver recovers the key by reconstructing a polynomial from its key source and the promise. Our analysis shows that the shared key generated by our proposed RSKA scheme has features of high randomness and a high bit rate compared to traditional RSS-based key agreement schemes.

Keywords: Key agreement, received signal strength, stationary wireless networks, polynomial

This work is partly supported by the National Natural Science Foundation of China (Grants No. 61322104, No. 61571240, No.61401228), The Priority Academic Program Development of Jiangsu Higher Education Institutions, University Natural Science Foundation of Anhui Province (KJ2015A105, KJ2015A092), Natural Science Foundation of Anhui Province (1608085QF138), Key Projects of the Outstanding Young Talents Program in Universities of Anhui Province (gxyqZD2016027).

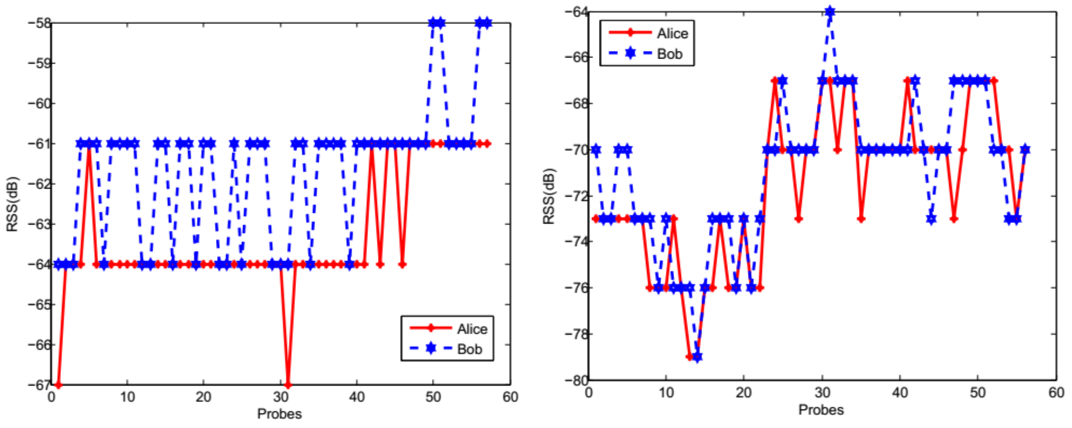
http://dx.doi.org/10.3837/tiis.2016.05.023 **ISSN : 1976-7277**

1. Introduction

Wireless networks are more vulnerable to attacks over contemporary networks due to their broadcast nature. To protect wireless networks, a number of security protocols have been proposed and established [1-3]. Secret keys play a critical role in these security [4,5]. Traditional key generation schemes are based on public key infrastructures and cryptographic algorithms. Recent studies have been proposed to generate the shared secret keys by exploring physical (PHY)-layer information in wireless networks [6-10]. PHY-layer based key agreement schemes are constructed on wireless channel characteristics. These include channel randomness, channel reciprocity and independent channel variation over space [11]. Compared to the traditional schemes, the PHY-layer based key exchange protocols do not rely on computational hardness. Rather, they utilize random channel measurements and can achieve information-theoretical security [12].

Generally, channel measurements may range from Channel State Information (CSI), channel phase to Receive Signal Strength (RSS). CSI information is usually extracted from Orthogonal Frequency-Division Multiplexing (OFDM) sub-carriers for achieving high bit-rate key generation [7]. However, it is only efficient in OFDM systems. Channel phase [8,9] may be extracted for key generation but their implementations require an analog-to-digital converter (ADC) working with the Nyquist frequencies of single-tone carriers [11]. This introduces hardware constraints. RSS is an attractive means for generating secret keys. It is available in most affordable off-the-shelf wireless cards without any modification [7].

A number of RSS-based key agreement schemes generate high bit-rate secret keys through optimal quantization strategies such as ranking for quantization or multi-level quantization [10,13-18]. These schemes enhance information reconciliation efficiency for key robustness [19]. The above approaches require that the RSS has large variations to produce randomly changing measurements for robust key generation. However, there are many wireless application scenarios where channel coherence time is long and where channel have limited variations. These include wireless body area networks, wireless sensor networks or device-to-device communications with stationary nodes or terminals. We define these networks as stationary wireless networks.



(a) Scenario 1 (b) Scenario 2

Fig. 1. Rss measurements of stationary wireless networks.

To study fluctuations in the channel characteristics of stationary wireless networks, we conducted practical experiments[1] and collected the channel measurements from both transmitters and receivers. These are denoted by Alice and Bob, respectively. **Fig. 1** shows the RSS measurements. From these figures we observed the following features of RSS measurements in stationary wireless networks:

- The RSS measurements have slow variations. As shown in **Fig. 1** (a) and **Fig. 1** (b), RSS measurements may remain stable for several probes in stationary wireless networks. This results in low randomness for keys if keys are extracted from measurements directly. Additionally, if RSS measurements are quantized according to thresholds [16], most of the measurements may be discarded, which reduces the key generation rate.
- The RSS measurements at both endpoints are not symmetric. Measurements collected at Alice and Bob are not identical due to non-ideal conditions such as hardware differences and noise.

Stationary wireless channel measurements lack variations and randomness. It is thus, difficult to generate high bit-rate and high-entropy secret keys from their channels. Bits extracted by traditional RSS-based key agreement schemes are less suitable for secret keys as their rate and entropy are low [18]. These problems are extensively discussed in [20,21]. Specifically, [20] integrates opportunistic beamforming and frequency diversity for key generation. However, it requires an additional antenna at transmitter to introduce channel fluctuations. [21] introduces iJam to ensure that eavesdroppers are unable to demodulate wireless signals. The scheme is channel-independent but is only effective for an OFDM based systems. Furthermore, secrecy depends on the statistical characteristics of transmitted data.

Despite the aforementioned efforts, secret key agreement from RSS in stationary wireless channel continues to face the following challenges: i) How to improve secret key bit-rates from channel measurements with slow variation in general wireless networks except for specific OFDM systems? and ii) How can we increase the entropy of RSS-based secret keys from stationary wireless channel without additional hardware or system modifications?

To address the above issues, we propose a fuzzy-vault-based key agreement scheme from the RSS of the stationary wireless channels. We refer to this scheme as the Robust Secure Key Agreement (RSKA). In RSKA, the RSS measurements are quantized with normalization through maximal measurements to mitigate the non-reciprocity of the channel characteristics. The normalized quantization bit sequences are then reshaped into sequences with different levels. These methods alter the original repeated sequences into new variations, and can generate high bit-rate keys. The reshaped sequences function as key sources to produce a promise to hide key information. A promise is a fuzzy-vault, which is generated from a polynomial constructed on the key. The key is randomly generated by the transmitter. Upon receiving the promise sent by the transmitter, the receiver is able to reconstruct the polynomial with its key source and recover the secret key. In summary, the main contributions are threefold.

- We propose normalized quantization and bit reshaping techniques to generate high bit-rate secret keys. By normalizing quantization, the channel measurements of both communicating parties are translated into more matching sequences. Moreover, the bit reshaping process transforms the repeated sequences into more diverse ones. Therefore, the reshaped sequences may provide high bit-rate key source.
- We propose an RSS-based high bit-rate high-entropy secure key agreement for stationary wireless networks. In the proposed RSKA scheme, a polynomial is constructed on the key

which is randomly generated by the transmitter. A modified fuzzy-vault is used to generate a promise for key information concealment. Promises are then transmitted to the receiver for key recovery. Rather than generating keys directly from the channel measurements, the fuzzy-vault scheme uses a randomly generated bit sequence as the key, thus providing high-entropy.

- We formally discuss the parameter settings for the proposed RSKA scheme and analyze its performance, security level, bit rate, and key entropy. Additionally, we conduct practical experiments to collect channel measurements of stationary wireless networks and validate the effectiveness of our proposed RSKA scheme.

The remainder of the paper is organized as follows. Section 2 presents the proposed RSKA scheme and discusses the parameter settings. This is followed by a performance analysis in Section 3. Section 4 evaluates the performance of the proposed protocol through practical experiments and extensive simulations. Finally, Section 5 concludes this work.

2. The Proposed RSKA

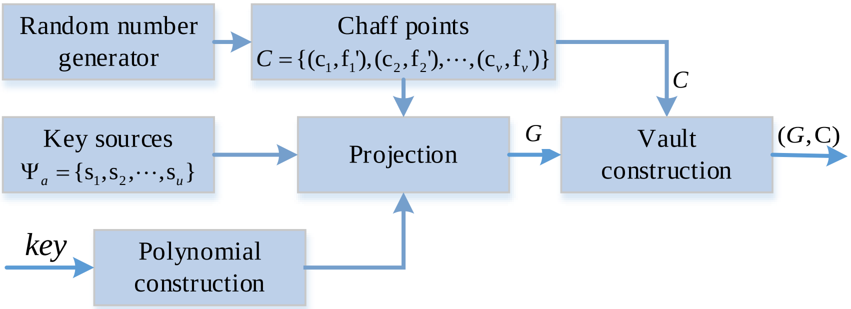
In contrast to existing RSS-based key extraction approaches, which focus on error-correcting bits, our proposed RSKA scheme generates shared keys based on a fuzzy-vault, which will be presented in the first subsection. The RSKA scheme is described in detail with the corresponding parameters.

2.1 Preliminary

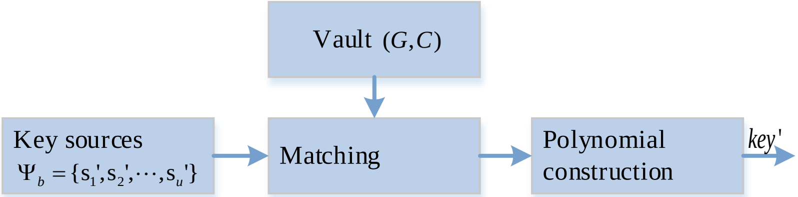
Fuzzy-vault. The intent of the fuzzy-vault-based key agreement scheme is to hide keys in a construction called vault using a set of key sources [22,23]. As shown in **Fig. 2** (a), the transmitter Alice generates an *m*th order polynomial

$$f(x) = c_{m-1}x^{m-1} + c_{m-2}x^{m-2} + \ldots + c_1 x + c_0$$

over the variable *x*. Alice keeps $key = c_{m-1} \mid c_{m-2} \mid \ldots c_1 \mid c_0$ as the shared key. Then Alice projects each real point s_i in its source Ψ_a onto the polynomial to generate a set of real points $G = \{(s_1, f(s_1)), (s_2, f(s_2)), \ldots (s_z, f(s_z))\}$ and randomly creates chaff points $C = \{(c_1, f_1), (c_2, f_2), \ldots (c_v, f_v)\}$, where $f_i \neq f(c_i)$. The fuzzy-vault is constructed by combing *G* and *C* in a random order. Upon receiving the vault (*G*,*C*), the receiver Bob matches the vault with its key source Ψ_b, and reconstructs the polynomial using Lagrange theorem, as shown in **Fig. 2** (b).



(a) Fuzzy-vault at transmitter



(b) Fuzzy-vault at receiver

Fig. 2. The traditional fuzzy-vault scheme at (a) transmitter and (b) receiver.

In the proposed RSKA scheme, the RSS measurements perform as the key sources. We modify the fuzzy-vault to improve the performance of key agreement scheme in stationary wireless networks.

2.2 The RSKA Scheme

The proposed RSKA scheme consists of three steps: Normalized quantization, bit reshape, and modified fuzzy-vault based key extraction.

Step 1 RSS Normalization and Quantization. In order to mitigate the asymmetry of RSS measurements, we normalize the RSS with maximal measurements received by the terminal[1]. The normalized value is then quantized by a predefined level, denoted by q. Without loss of generality, we assume that Alice stores its s RSS measurements in array $A = [a]_{1\times s}$ and that the maximal element in A is s_m. All the elements of A, denoted by s_i, are then normalized and quantized as

$$\overline{s_i} = \frac{s_i}{s_m + \alpha s_m} \times 2^q, \tag{1}$$

where $\overline{s_i}$ is represented by a q-bit binary sequence[2], and $\alpha \in (0,1)$ is a modification factor.

Remark 1 *i) Due to unideal conditions, Alice and Bob may fail to achieve absolutely identical RSS measurements. Yet they may get similar variation trends due to channel reciprocity. By normalization and quantization, the measurements may be translated into more matching bits. ii) The modification factor α is introduced in Eq. 1 to limit the quantized bit sequence at some level which is not predicable for the eavesdroppers.*

We denote Alice's RSS measurements A=[55, 55, 56, 56, 57] and Bob's RSS measurements B=[56, 56, 56, 57, 58]. By normalization and quantization with level q=8 and $\alpha = 0.5$. For Alice's measurement 55, receives a normalized value $\frac{55}{55+57/2} \times 2^8 = 164.67$. With rounding, the value is quantized into sequence $165_{10}=10100101_2$. In this way, Alice gets sequences

$$\Phi_a = \{10100101,10100101,10101000,10101000,10101011\}.$$

Similarly, for Bob's measurement 56, it gets normalized value $\frac{56}{56+58/2} \times 2^8 = 164.78$ and the value is quantized into sequence $165_{10}=10100101_2$. Thus, Bob receives sequences

$$\Phi_b = \{10100101,10100101,10101001,10101000,10101011\}.$$

[1] For the simplification of computation, we extract the absolute value of RSS for quantization.

[2] The numerator is a little larger than s_m, thus avoiding full ones of the sequence when the measurement reaches s_m.

As a result, the two different measurements A and B are quantized into two high matching bits. We will discuss the prerequisites of high matching normalization in subsection 2.3.

Step 2 Bit reshaping. As there is only little variations in stationary wireless networks, the entropy of the quantized bits is slow and they are not suitable for extracting keys directly. We propose to reshape the bit sequence Φ_a and Φ_b with a different level *l*, where $l \neq q$. In the above example, with *l*=10, Φ_a and Φ_b may be reshaped as

$$\Psi_a = \{1010010110,1001011010,1000101010,0010101011\}$$

And

$$\Psi_b = \{1010010110,1001011010,1001101010,0010101011\},$$

which have noticeable variations. The reshaped bit sequences Ψ_a and Ψ_b work as the key sources for the generation of shared keys with modified fuzzy-vault.

Step 3 Modified fuzzy-vault-based key extraction. In the traditional fuzzy-vault schemes, the fuzzy-vault includes the points on the polynomial. This may result information leakage to eavesdropper [22,23]. Additionally, security relies on the computational complexity of constructing polynomial from the fuzzy-vault. Thus it is conditionally secure. We propose to send only partial point information to the receiver. This is inconsequelntial to the eavesdropper, thus reaching higher security level. Specifically, Alice generates a random *k*-bit sequence *key* and splits it into the form of a $key = c_{m-1} \mid c_{m-2} \mid ...c_1 \mid c_0$. The *m*th order polynomial

$$f(x) = c_{m-1}x^{m-1} + c_{m-2}x^{m-2} + ... + c_1 x + c_0$$

is constructed. For each element $a_i \in \Psi_a$, Alice computes $f_i = f(a_i)$ and creates a set $N = \{(a_1, f_1), (a_2, f_2), ...(a_n, f_n)\}$, where *n* denotes the amount of elements in key source Ψ_a. Instead of sending all the values $\{f_1, f_2, ...f_n\}$ in order, Alice chooses *v*, *m*<*v*<*n* elements from *N* denoted by $T = \{f_{i_1}, f_{i_2}, ...f_{i_v}\}$, where $i_1<i_2<\ldots<i_v$. Here $i_j, j \in [1, v]$ is computed by the following equation:

$$i_j = n * \frac{a_{l_1}+a_{l_2}+...+a_{l_j}}{a_{l_1}+a_{l_2}+...+a_{l_{v+1}}} \tag{2}$$

where $L = \{l_1, l_2, ...l_{v+1}\}$ specifies the position of $a_{l_1}, a_{l_2}, ..., a_{l_{v+1}}$ in the set Ψ_a. If the first *v+1* elements are selected, $L = \{1, 2, ...v+1\}$. Additionally, Alice selects a secure hash function *Hash* and calculates $Hash(RSS) = Hash(a_{l_1} \mid a_{l_2} \mid ... \mid a_{l_{v+1}})$ and *Hash*(*key*) for the verification of the RSS value and the key. Consequently, Alice formulates the promise in the format *T*|*Hash*(*RSS*)|*L*|*Hash*(*key*) and sends it to Bob.

Remark 2 *Eq. 2 is an example of calculating the sequence number i_j from the RSS. Other methods may be explored under the condition that Alice and Bob can derive the sequence number without interaction such that Eve gathers no information from it.*

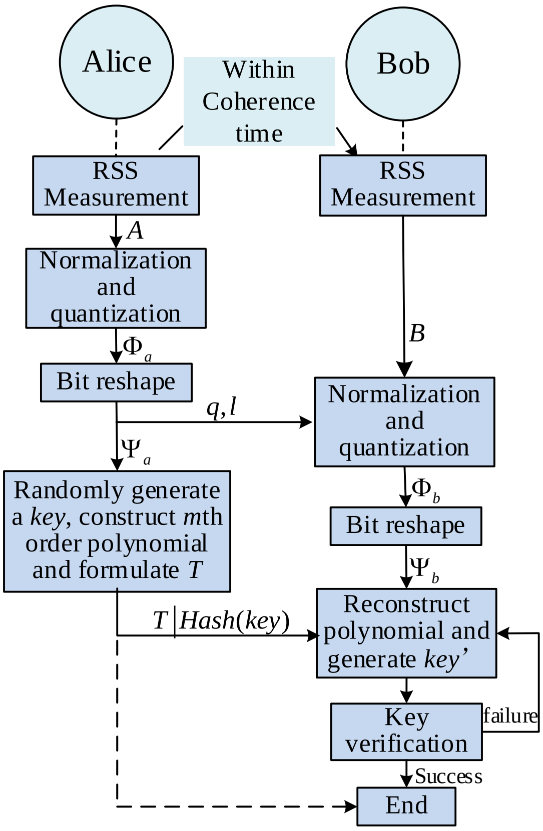

Alice
Within Coherence time
Bob
RSS Measurement
RSS Measurement
A
Normalization and quantization
Φ_a
Bit reshape
q, l
B
Normalization and quantization
Ψ_a
Randomly generate a *key*, construct *m*th order polynomial and formulate *T*
Φ_b
Bit reshape
Ψ_b
$T | Hash(key)$
Reconstruct polynomial and generate *key'*
failure
Key verification
Success
End

Fig. 3. The proposed RSKA scheme.

After receiving the promise, Bob checks whether $Hash(RSS) = Hash(b_{l_1} | b_{l_2} | ... | b_{l_{v+1}})$. If the equation does not hold, Bob will notify Alice to reselect the RSS value until the equation holds. Later, Bob computes the sequence number as follows:

$$i_j = n * \frac{b_{l_1} + b_{l_2} + ... + b_{l_j}}{b_{l_1} + b_{l_2} + ... + b_{l_{v+1}}} \tag{3}$$

and constructs the set $H = \{(b_{l_1}, f_{l_1}), (b_{l_2}, f_{l_2}), ...(b_{l_v}, f_{l_v})\}$ with *T*. By choosing *m* elements from *H*, represented by $\{(x_1, y_1), (x_2, y_2), ...(x_m, y_m)\}$, Bob reconstructs the polynomial using Lagrange theorem. The polynomial is reconstructed as

$$f'(x) = \sum_{j=1}^{m} y_j d_j(x) \quad ,$$

where $d_j(x) = \prod_{i \neq j, i=1}^{i=m} (x - x_i) / (x_j - x_i)$. Rewrite $f'(x)$ as

$$f'(x) = c'_{m-1} x_{m-1} + c'_{m-2} x_{m-2} + ... + c'_1 x + c_0$$

Bob gets the shared key $key' = c'_{m-1} | c'_{m-2} | ... c'_1 | c'_0$ and checks

$$Hash(key)\underset{=}{?}Hash(key') \tag{4}$$

If Eq. 4 holds, the key agreement scheme successes. Otherwise, Bob reselects *m* elements from *H* and reconstructs the polynomial until the equation holds. The protocol of the proposed RSKA scheme is shown in **Fig. 3**.

2.3 Discussion

In this subsection, we discuss the prerequisite of high matching normalization in *Step 1*. We later clarify the relationship between reshaping level *l* and quantization level *q* for high variations of key sources in *Step 2*.

Recall that in the experiment of section 1, the RSS measurements of stationary wireless networks at Alice and Bob have almost the same variation trends and range despite their asymmetry. Furthermore, they acheive the maximal or minimal values almost at the same probe. In other words, by adjusting Alice's measurements along the vertical axis in **Fig. 1**, we can match Bob's value with minor differences. Thus we have the following assumptions.

Assumption 1 *i) We sort Alice and Bob's measurements according to ascending order, denoted by* $X_a=\{a_1,a_2,...a_m\}$ *and* $X_b=\{b_1,b_2,...b_m\}$ *, respectively. Without loss of generality, we suppose the measurements at Alice and Bob have the same variation range and the same interval, i.e.,* $b_m-b_1=a_m-a_1\underline{\underline{\Delta}}\ r$ *and* $a_1-b_1=a_2-b_2...=a_m-b_m\underline{\underline{\Delta}}\ d$ *.ii) The measurements* $a_i\in X_a$ *and* $b_i\in X_b$ *are normalized by Eq. 1 and transformed into integer by rounding.*

Under the *Assumption 1*, we have the following theorem.

Theorem 1 *The prerequisite of* X_a *and* X_b *have the same quantization bits is*

$$x_m>\frac{\sqrt{d^2+\dfrac{d\times r\times 2^{q+2}}{1+\alpha}}-d}{2} \tag{5}$$

where d and r are defined in Assumption 1, q is the quantization level, x_m *denotes the minimal maximal RSS measurements of Alice and Bob, i.e.* $x_m=min\{a_m,b_m\}$*.*

Proof. According to Eq. 1, for all $a_i\in X_a$ and $b_i\in X_b$, they are normalize as $\frac{a_i}{a_m(1+\alpha)}\times 2^q$ and $\frac{b_i}{b_m(1+\alpha)}\times 2^q$, respectively. In order to acheive the same quantized bits by rounding, they should satisfy

$$|\frac{a_i}{a_m(1+\alpha)}\times 2^q - \frac{b_i}{b_m(1+\alpha)}\times 2^q|<1 \tag{6}$$

Without loss of generality, we suppose

$$a_i-b_i=a_m-b_m=d>0 \text{ and } b_m-b_1=a_m-a_1=r_i.$$

Then Eq. 6 turns to

$$|\frac{b_i+d}{(b_m+d)(1+\alpha)}\times 2^q - \frac{b_i}{b_m(1+\alpha)}\times 2^q|<1$$

We let $x_m\underline{\underline{\Delta}}\min(a_m,b_m)=b_m$. It can be further simplified as

$$x_m{}^2 + d \times x_m - \frac{d \times r_i \times 2^q}{1+\alpha} > 0 \tag{7}$$

Since $x_m > 0$, we can have

$$x_m > \frac{\sqrt{d^2 + \frac{d \times r_i \times 2^{q+2}}{1+\alpha}} - d}{2} \tag{8}$$

For all $a_i \in X_a$ and $b_i \in X_b$, $r_i \le r \triangleq a_m - a_1$. Substitute r_i in Eq. 8 by *r*, we get the prerequisite of X_a and X_b possessing the same quantization bits, as shown in Eq. 5.

Remark 3 *i) Under the condition that Alice and Bob do not have the same RSS variation range, i.e.,* $b_m - b_1 \ne a_m - a_1$, *we define* $r \triangleq \max\{b_m - b_1, a_m - a_1\}$ *for redundancy. ii) Eq. 8 is the solution of Eq. 7 over variable* x_m*. If another parameter, supposing q, is the variable, the solution of Eq. 7 becomes*

$$q < \log_2 \frac{(x_m{}^2 + d \times x_m)(1+\alpha)}{d \times \alpha} \tag{9}$$

By reshaping, the repeated bit sequences may be transformed into varied ones. Next, we provide definitions of repetition and variation characteristics for sequence sets and the relationship between these parameters.

Definition 1 *(q,t)-repetition sequence set. A q-bit sequence is repeated by t times and the t repeated sequences consist of a (q,t)-repetition sequence set.*

Definition 2 *(l,w)-variation sequence set. An (l,w)-variation sequence set is composed by w different sequences with the same length l bits.*

The relationship between the quantization level *q* and the reshaping level *l* is given in the following theorem.

Theorem2 *An RSS measurement's (q,t)-repetition sequence set may be reshaped into a new sequence set which includes an (l,w)-variation sequence set. The parameters satisfy* $w = \left\lfloor \frac{z}{l} \right\rfloor$, *where* $z = \min\{q \times t, e\}$*. Here, e is the least common multiple of q and l.*

Proof. Please see Appendix A.

From *Theorem 2*, we learn when *l* and *q* are relatively-prime, the reshaped sequence set has the largest size. This theorem provides a guide for selecting a proper *l* for the variations of the key sources Ψ_a and Ψ_b. Whereafter, the determination of *l* is not only affected by *q*, but also related with the order of the polynomial *m* and the security level of the key. Their relationship will be analyzed in Section 3.

3. Performance Analysis

In this section, we analyze the secureness of the proposed RSKA scheme. We also show how the scheme achieves high entropy and high bit-rate performance.

3.1 Security Level

The security of RSKA is based on the computational difficulty of polynomial reconstruction. As Alice only sends the function value of the polynomial, an adversary who does not know any information about the variable value has to try out $2^l \times (2^l - 1) \times (2^l - 2) \times ....(2^l - m)$ times to arrive at the correct polynomial. Generally, *l* is large enough to satisfy $2^l > m$, then the term $2^l \times (2^l - 1) \times (2^l - 2) \times ....(2^l - m) \cong 2^{l \times m}$. Further, the adversary may derive the secret key by a brute-force attack, making 2^k attempts, where *k* is the length of the key. Consequently, the security level is determined by $\min\{2^{l \times m}, 2^k\}$.

In order to protect the key, the parameters (*l*,*m*,*k*) should satisfy $l \times m \geq k$. Usually, we set $m < l$ for reducing the computational complexity. Additionally, as key sources come from the RSS samples, the amount of samples *s* should meet the requirement of generating enough bit sequences, i.e., $s \times q \geq l \times m$.

Remark 4 *Eve may deduce the key by guessing the RSS values instead of directly reconstructing the polynomial with Lagrange theorem. In order to resist this kind of attack, the parameters should satisfy*

$$\mathrm{P}_n^m \times (r)^{m \times \lceil l/q \rceil} \times G > 2^{l \times m} \tag{10}$$

where *G* denotes the maximal variability on the range of the RSS measurements. P_n^m denotes the permutation amounts for choosing *m* numbers from *n* numbers. The left side of Eq. 10 denotes that the adversary has to make $\mathrm{P}_n^m \times (r)^{m \times \lceil l/q \rceil} \times G$ attempts to guess the values of RSS in order to obtain $(x_1, x_2 ... x_m)$ such that it can reconstruct the polynomial from $\{(x_1, y_1), (x_2, y_2), ...(x_m, y_m)\}$. The right side of Eq. 10 denotes that the adversary has to make $2^{l \times m}$ attempts in order to guess the key via a brute-force attack. To resist brute-force attacks the parameters should satisfy Eq. 10. Generally, parameters satisfy Eq. 10 in most cases.

3.2 Secure Bit Rate

Secure bit rate is defined as the average number of secret bits extracted per collected measurement [18]. As $l \times n \cong s \times q$, we have the secure bit rate[3]

$$R = \frac{l \times m}{s} = \frac{m}{n} q \tag{11}$$

Given the *s* RSS measurements, the maximal secure bit rate may be obtained by selecting proper parameters *q*,*m*,*l*. Specifically, the problem may be explicitly expressed as:

[3] Under the condition that the parameters (*l*,*m*,*k*) should satisfy $l \times m \geq k$, the secure bit rate is *k/s*. Whereas, in order to analyze the maximal secure bit rate, we assume that the security level $k = l \times m$.

$$\begin{aligned} \max \quad & \frac{m}{n} q \\ s.t. \quad & (C1) n = \left\lfloor \frac{s \times q}{l} \right\rfloor, \\ & (C2) s \times q > m \times l > k, \\ & (C3) q < \log 2 \frac{(x_m{}^2 + d \times x_m)(1+\alpha)}{d \times r}, \\ & (C4) q, l \in \mathrm{N}^+. \end{aligned}$$

Constraint (C2) is established to guarantee the security level. Constraint (C3) is the solution of Eq. 6, for guaranteeing the validity of bit reshaping. In constraint (C4), N^+ denotes a positive integer set. Additionally, *q,l* may satisfy *gcd(q,l)*=1, denoting that *q* and *l* are relative-prime. Where *gcd(q,l)* presents the greatest common divisor of *q* and *l*. Consequently, there is a tradeoff between the security level and the key generation rate.

3.3 Key Entropy and First-try-success Probability

In the proposed RSKA scheme, the key is generated randomly by Alice, with a high level of randomness. Provided that the random generator performs well, the entropy of a *k*-bit key may reach the upper bound. In Section 4, we estimate the entropy of the key generated by RSKA, which shows that the proposed RSKA scheme has the characteristic of high entropy.

First-try-success probability is defined as the probability of successful key agreement for the first turn. We denote *h* the amount of mismatching elements from Alice and Bob's key sources. Only when all the *m* elements are selected from the *n*-*h* matching ones, can the reconstructed polynomial correctly extract matching bits. The first-try-success probability P_s is

$$P_s = \binom{n-h}{m} \Big/ \binom{n}{m}.$$

If Bob fails to recover the shared key in the first turn, he may try again. We define *u* as the average times that Bob tries befores a successful agreement. We have $u = \lceil 1/P_s \rceil$. Next, we draw the relationship between *u* and *n*, *m*, *h* in **Fig. 4**. The figure shows that a higher *n* may increase the probability of key matching while a larger *m* causes more attempts for obtaining the correct key. Additionally, the higher the key sources mismatching ratio is, the more efforts Bob makes for a key agreement.

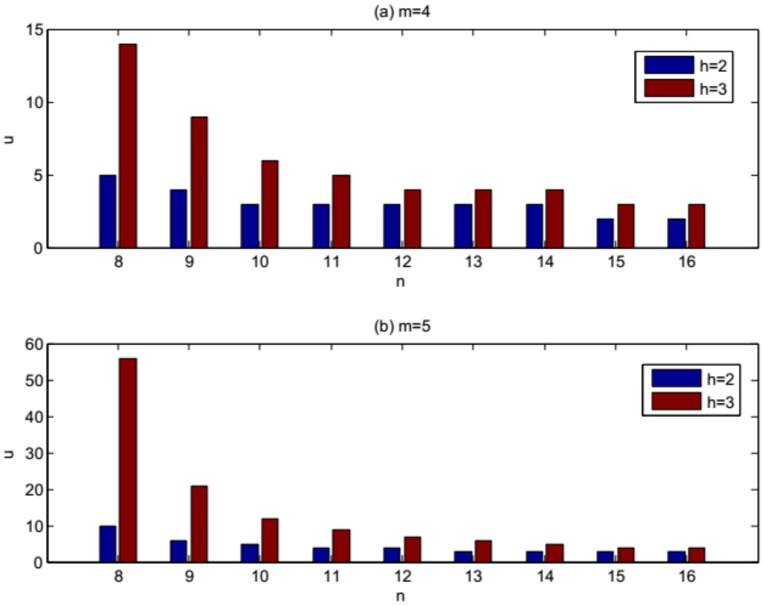


Fig. 4. The relationship between *u* and *n*, *m*, *h*.

4. Experimental Evaluation

In this section, we evaluate the performances of the proposed RSKA scheme and compare it with the traditional RSS-based key agreement from wireless channel [18].

4.1 Experimental Settings

We set up a wireless channel using an IRIS wireless sensor motes operating at 2.4*GHz*. There are three motes located within the communication radius of each other. Two motes, Alice and Bob, function as the communicating parties. The other mote works as a sink and connects to a laptop. Specifically, the initiator Alice sends a probe message to Bob. Upon receiving the packet, Bob conducts two tasks: i) Measuring the RSS and transmitting the value to the sink; and ii) Sending a probe message back to Alice. Alice repeats the processes, i.e., measuring the RSS, transmitting it to the sink, and sending a probe message back to Bob. In this way, the sink obtains all the RSS measures on the channel between Alice and Bob. It is worth noting that Alice may wait τ millisecond in order to fully control the rate and interval between packets.

Alice and Bob are stationary and are located at two corners of the room. They send probe messages to each other at the interval of τ =100*ms*. We collect the RSS measurements in two scenarios.

- *Scenario 1*. There are intermediate objects between the communicating terminals and all of the objects are stationary.
- *Scenario 2*. There are intermediate objects between the communication terminals and one intermediate object (i.e., a person) moves at a regular gait [26], i.e., 1*m/s*.

After receiving *s* probe messages, Alice randomly generate an $m \times l$ bit sequences for the key and constructs an *m*th order polynomial. Simultaneously, she produces a promise and sends it to Bob. Based on RSS measurements and promise, Bob can reconstruct the polynomial for the key recovery.

Firstly, we estimate the range of *q* according to Eq. 9. The receiving sensitivity of IRIS motes is -101*dBm*, while the RSS measurements vary from -55*dBm* to -70*dBm*. Consequently, we set x_m=70 in Eq. 9. Additionally, the other parameters are estimated as $d = 3, r = 5, \alpha = 0.5$. Thus *q* is estimated by

$$q < \log 2 \frac{(70^2 + 3 \times 70)(1 + 0.5)}{3 \times 5} < \log_2 511.$$

In our experiments, we set *q=7, q=8*. Generally, *l* is larger than *q* for higher security while *m* is relatively small for low computational complexity, i.e., *m=5,m=6*.

In the traditional RSS-based key agreement as described in [18], named TRKA, the upper threshold and the lower threshold are represented by θ^+ and θ^-, respectively. The RSS measurement are quantized as

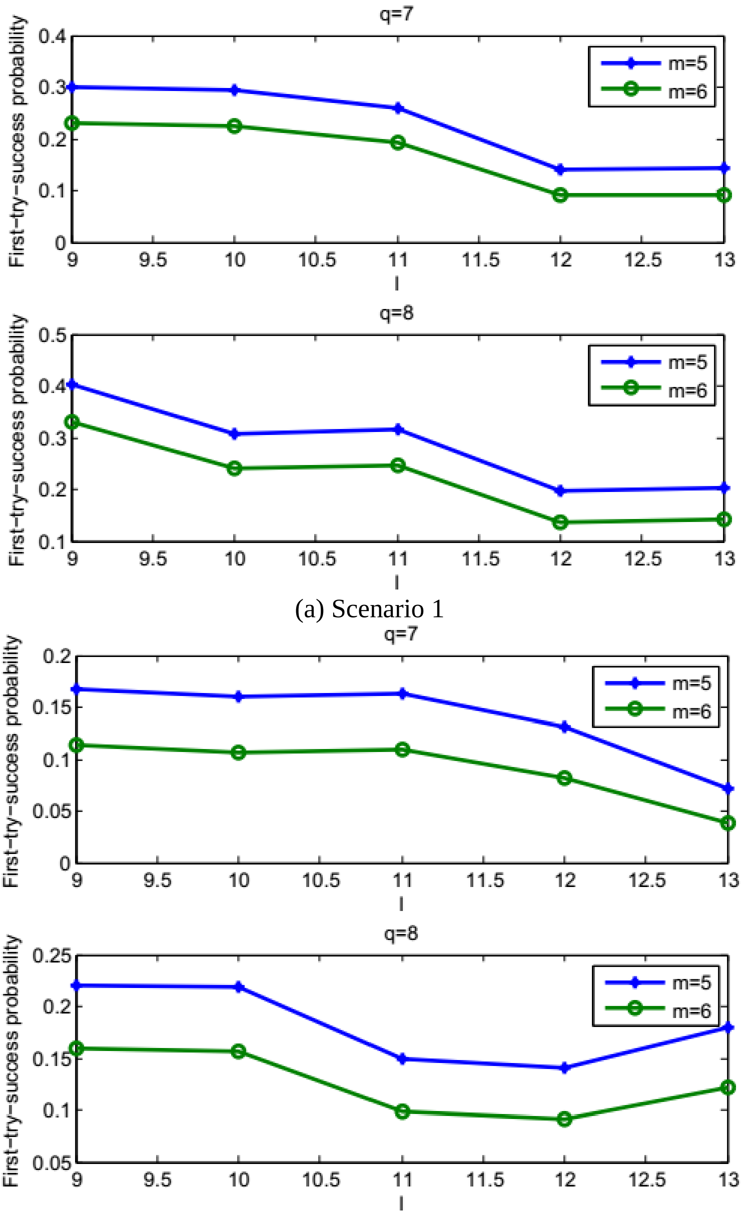
$$x = \begin{cases} 1, & RSS > \theta^+ \\ 0, & RSS < \theta^- \end{cases}$$

The values between the lower and the upper threshold are dropped. Cascade protocol [27] is adopted for information reconciliation. For the uniformity of our benchmark, both of the schemes compare the entropy of the keys before privacy amplification.

4.2 Performance Evaluation

First-try-success probability P_s *of RSKA*. **Fig. 5** shows the affecting factors of first-try-success probability in RSKA. With *l* increasing from 9 to 13, P_s may decrease slightly both at *q*=7 and *q*=8. However as an exception, the probabilty increases at *l*=13 and *q*=8. This is due to *q*=8 and *l*=13 being relatively-prime for more various key sources. Generally, Bob has a high probability for a successful key agreement when *q* increases from 7 to 8. The result is encouraging because the secure bit rate is higher when *q* is larger according to Eq. 11. Note that *q* should not exceed the solution of Eq. 9. Whereafter, Bob has to try more times for key agreement when *m* increases, as shown in both **Fig. 5** (a) and (b). Consequently, it is better to set *m* at a low level for fast key agreement. However, *m* should satisfy (C2) for the optimization problem in Eq. 12 for security guarantee.

In *Scenario 2*, as there are mobile objects between the communicating parties causing asymmetrical channel characteristics, there may be a larger disparity of bits in the key sources comparing to *Scenario 1*. As a result, the receiver has low probability of success in the first attempt of the key agreement implementation, as demonstrated in **Fig. 5** (b).

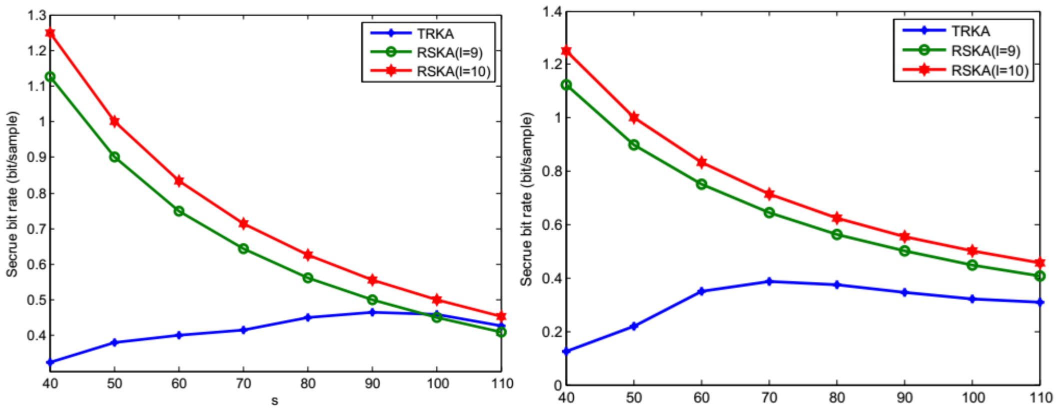


(a) Scenario 1

(b) Scenario 2

Fig. 5. First-try-success probability varies with *l,q,m* (*s*=60)

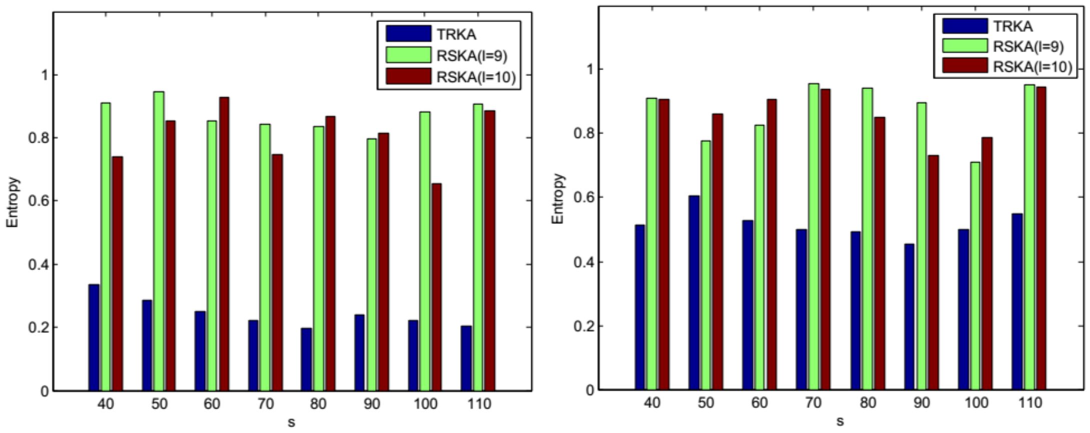
Secure bit rate. As shown in **Fig. 6**, the secure bit rate of RSKA decreases with increasing *s* in both *Scenario 1* and *Scenario 2*. This is not surprising, the secure bit rate is an inverse ratio to sample amounts while proportional to reshaping level as analyzed in *Section 3*. In this figure, the secure bit rate of TRKA does not change distinctly with increasing *s*. The figure also demonstrates that RSKA has higher key generation bit-rate than TRKA in most cases. However, it is predicable; the bit rate of RSKA may fall below TRKA if *s* continues increasing. Therefore, it is not necessary to collect too many RSS measurements in RSKA. Nonetheless, it is required that *s* satisfies constraint (C2) of the optimization problem Eq. 12. Furthermore, *s* is proportional to *n* and higher *n* may increase the first-try-success probability as shown in **Fig. 4.** Thereby, optimal *s* is a tradeoff between security level and secure bit rate.



(a) Scenario 1 (b) Scenario 2

Fig. 6. Comparisons of secure bit rate varying with *s* (*m*=5, *q*=8).

Entropy. In order to compare the key entropy of the proposed scheme with the benckmark, we use NIST test suit [28] to estimate the approximate entropy of the key. From **Fig. 7** we found that the key generated by RSKA has much higher randomness than that of TRKA. Bear in mind that the key is randomly generated by the transmitter in RSKA. Thus the entropy may almost reach as high as 1, which is the upper bound of the entropy in NIST test suit. The figure also depicts that the entropy is not related with *s* and *l* in both *Scenario 1* and *Scenario 2*. It is worthy noting that TRKA extracts keys with higher randomness in *Scenario 2* than in *Scenario 1* due to the fact that mobility increases uncertainty of channel characteristics. The result shows that our proposed protocol has much higher entropy and is immune to the parameter variations.



(a) Scenario 1 (b) Scenario 2

Fig. 7. Comparisons of entropy varying with *s* (*m*=5, *q*=8).

5. Conclusion

In this paper, a novel RSS-based robust key agreement scheme is proposed for stationary wireless networks. By introducing normalized quantization and bit reshaping, the channel measurements are transformed into matching bits with high variations. Transmitter and receivers achieve key agreement by using a modified fuzzy-vault. As the key is randomly generated by the transmitter, it produces high entropy, almost reaching the upper bound of a sequence according to the NIST test. Furthermore, when the parameters are properly selected, RSKA has the characteristic of higher key generation rate compared to traditional RSS-based key agreements. Additionally, the proposed approach does not require any modification to hardware and is applicable in both stationary and mobile environments.

Note that in this study, we mainly focus on resisting passive attacks, i.e., eavesdropping. In our future work, we will consider other attacks such as predicable channel attacks and stalking attacks [7].

Appendix A: Proof of Theorem 2

Without loss of generality, we assume that part of Alice's RSS measurements, denoted by $\Phi_a = \{s_1, s_2,...s_t\}$, is a (*q*,*t*)- *repetition sequence set.* We construct a new sequence Φ_a', which is formulated by combining the elements in Φ_a one by one. For simplification of expression, we list the bit amount of the sequence s_i in Φ_a', as shown in the middle line of Fig. A1. The figure shows the processes of transforming Φ_a into key source Ψ_a. We assume that $q<l=q+p<2q$. From the figure, we find that the first element of Ψ_a, a_1, is composed by s_1 and the first p bits of s_2. Similarly, a_2 is composed by the rest q-p bits of s_2 and the first l-$(q$-$p)$ bits of s_3 (when l-$(q$-$p)<q$). If l-$(q$-$p)>q$, a_2 is composed by the rest q-p bits of s_2, s_3 and the first l-$(2q$-$p)$ bits of s_4. According to this method, $a_1,a_2,...,a_w$ are constructed by different arrangements of the q-bit sequence thus formulating (*l*,*w*)-*variation sequence set*. Actually, there are two cases.

If $t > t'$, the first repetition of a_1 appears after a_w, where $l \times w = q \times t'$ and the product $l \times w$ is the least common multiple of q and l. If t is large enough, $a_1,a_2,\ldots,a_w$ will circularly appear.

If $t < t'$, Φ_a is not large enough to construct a repetition of a_1 while constructing an (*l*,*w*) -*variation sequence set*, where $w = \left\lfloor \dfrac{q \times t}{l} \right\rfloor$.

Combining the above two cases, the result follows.

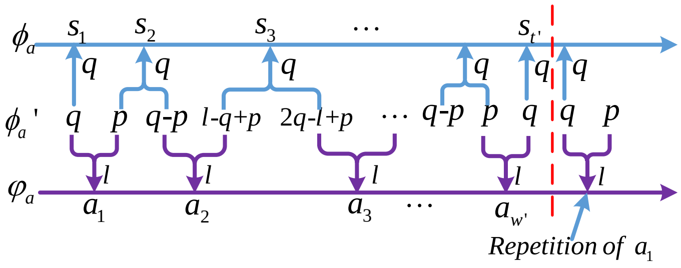


Fig. A1. The reshaping processes of key source.

References

[1] H. Nguyen Thi Thanh, J. Minho, N. Tien-Dung, and H. Eui-Nam, "A Beneficial Analysis of Deployment Knowledge for Key Distribution in Wireless Sensor Networks," *Security and Communication Networks*, vol. 5, no. 5, pp. 485-495, May 2012. Article (CrossRef Link)

[2] L. Guo, C. Zhang, J. Sun, and Y. Fang, "A privacy-preserving attribute-based authentication system for mobile health networks," *IEEE Transactions on Mobile Computing*, vol. 13, no. 9, pp. 1927-1941, September, 2014. Article (CrossRef Link)

[3] L. Zhou, D. Wu, B. Zheng, and M. Guizani, "Joint physical-application layer security for wireless multimedia delivery," *IEEE Communications Magazine*, vol. 52, no. 3, pp. 66-72, March 2014. Article (CrossRef Link)

[4] C. Yu, C. Lu, and S. Kuo, "Non-interactive pairwise key establishment for sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 3, pp. 556-569, May 2010. Article (CrossRef Link)

[5] Y. Hao, Y. Cheng, C. Zhou, and W. Song, "A distributed key management framework with cooperative message authentication in VANETs," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 3, pp. 616-629, March 2011. Article (CrossRef Link)

[6] N. Wang, N. Zhang, and T. Aaron Gulliver, "Cooperative key agreement for wireless networking: Key rates and practical protocol design," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 2, pp. 272-284, February 2014. Article (CrossRef Link)

[7] H. Liu, Y. Wang, J. Yang, and Y. Chen, "Fast and practical secret key extraction by exploiting channel response," in *Proc. of IEEE International Conference on Computer Communications (INFOCOM)*, Turin, Italy, pp. 3048-3056, April 14-19, 2013. Article (CrossRef Link)

[8] A. Sayeed and A. Perrig, "Secure wireless communications: Secret keys through multipath," in *Proc. of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Las Vegas, Nevada, USA, pp. 3013-3016, March 31-April 4, 2008. Article (CrossRef Link)

[9] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *Proc. of IEEE International Conference on Computer Communications (INFOCOM)*, Shanghai, China, pp. 1422-1430, April 10-15, 2011. Article (CrossRef Link)

[10] N. Patwari, J. Croft, S. Jana, and S. Kasera, "High bit-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Transactions on Mobile Computing*, vol. 9, no. 1, pp. 17-30, January 2010. Article (CrossRef Link)

[11] K. Ren, H. Su, and Q. Wang, "Secret Key Generation exploiting channel characteristics in wireless communications," *IEEE Wireless Communications*, vol. 18, no. 8, pp. 6-12, August 2011. Article (CrossRef Link)

[12] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, no. 28, pp. 656-715, 1949. Article (CrossRef Link)

[13] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks," in *Proc. of IEEE International Conference on Computer Communications (INFOCOM)*, San Diego, USA, pp. 1-9, March 15-19, 2010. Article (CrossRef Link)

[14] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radiotelepathy: extracting a secret key from an unauthenticated wireless channel," in *Proc. of ACM International Conference on Mobile Computing and Networking (MobiCom)*, San Francisco, CA, USA, pp. 128-139, September 14-19, 2008. Article (CrossRef Link)

[15] X. Zhu, F. Xu, E. Novak, C. C. Tan, Q. Li, and G. Chen, "Extracting Secret Key from Wireless Link Dynamics in Vehicular Environments," in *Proc. of IEEE International Conference on Computer Communications (INFOCOM)*, Turin, Italy, pp. 2283-2291, April 14-19, 2013. Article (CrossRef Link)

[16] H. Liu, J. Yang, Y. Wang, and Y. Chen, "Collaborative Secret Key Extraction Leveraging Received Signal Strength in Mobile Wireless Networks," in *Proc. of IEEE International Conference on Computer Communications (INFOCOM)*, Orlando, Florida, USA, pp. 927-935,

March 25-30, 2012. Article (CrossRef Link)

[17] B. Zan, M. Gruteser, and F. Hu, "Improving Robustness of Key Extraction from Wireless Channels with Differential Techniques," in *Proc. of International Conference on Computing, Networking and Communications, Wireless Ad Hoc and Sensor Networks Symposium (WiMob)*, Barcelona, Spain, October 8-10, pp. 980-984, 2012. Article (CrossRef Link)

[18] S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K.r Kasera, N. Patwari, and S. V. Krishnamurthy, "Secret key extraction from wireless signal strength in real environments," *IEEE Transactions on Mobile Computing*, pp. 917-930, vol. 12, no. 5, May 2013. Article (CrossRef Link)

[19] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, et al., "Robust key generation from signal envelopes in wireless networks," in *Proc. of ACM Conference on Computer and Communications Security (CCS)*, Alexandria, Virginia, USA, pp. 401-410, October 28-31, 2007. Article (CrossRef Link)

[20] P. Huang, and X. Wang, "Fast Secret Key Generation in Stationary Wireless Networks: A Virtual Channel Approach," in *Proc. of IEEE International Conference on Computer Communications (INFOCOM)*, Turin, Italy, pp. 2292-2300, April 14-19, 2013. Article (CrossRef Link)

[21] S. Gollakota and D. Katabi, "Physical layer wireless security made fast and channel independent," in *Proc. of IEEE International Conference on Computer Communications (INFOCOM)*, Shanghai, China, pp. 1125-1133, April 10-15, 2011. Article (CrossRef Link)

[22] A. Juels, M. Sudan, "A fuzzy-vault scheme," *Design Codes and Cryptography*, vol. 38, no. 6, pp. 237-257, June 2006. Article (CrossRef Link)

[23] F. Miao, S. Bao, and Y. Li, "A Modified fuzzy vault scheme for biometrics-based body sensor networks security," in *Proc. of IEEE Global Communications Conference (GLOBCOM)*, Miami, Florida, USA, pp. 1-5, December 6-10, 2010. Article (CrossRef Link)

[24] M. Zafer, D. Agrawal, and M. Srivatsa, "Limitations of generating a secret key using wireless fading under active adversary," *IEEE/ACM Transactions on Networking*, vol. 20, no. 5, pp. 1440-1451, May 2012. Article (CrossRef Link)

[25] G. D. Durgin, "Space-time wireless channels," *Prentice Hall PTR*, 2002. http://dl.acm.org/citation.cfm?id=1405684.

[26] K. Lee, S. Hong, S. Kim, et al., "SLAW: A mobility model for human walks," in *Proc. of IEEE International Conference on Computer Communications (INFOCOM)*, Rio de, Janeiro, Brazil, pp. 855-863, April 20-25, 2009. Article (CrossRef Link)

[27] G. Brassard, and L. Salvail, "Secret key reconciliation by public discussion," in *Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology*, pp. 410-423, 1994. Article (CrossRef Link)

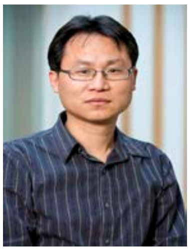
[28] NIST, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Article (CrossRef Link).

Aiqing Zhang received the Master's degree in circuit and system from Xiamen University, China in 2006. Currently, she is working toward a Ph.D degree with the Department of Telecommunications and Information Engineering, Nanjing University of Posts and Telecommunications, China. She is also an associated professor of Anhui Normal University, China. Her research interests include wireless network security and Device-to-Device communications.

Xinrong Ye is an associate professor of the College of Physics and Electronic Information at the Anhui Normal University, Wuhu, Anhui, P. R. China. He received a B.E. degree from Anhui Normal University, and an M. E. degree and a Ph. D. degree from Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu, P. R. China. His research interests include channel estimation, compressed sensing, and massive MIMO.

Jianxin Chen received Ph.D degree with major on Electronics Engineering from Shanghai Jiaotong University in 2007. From May 2008 to July of 2009, Mr. Chen worked as a postdoctoral in IPP Hurray Research Group, and researcher in a Spainish research center during 2009-2010. He worked as a visiting scholar in Nebraska-Lincoln University during 2013 and in Umea University in 2015. Currently he is an associate professor in the information and telecommunication engineering school of Nanjing University of Posts and Telecommunications. Mr. Chen's research interests include body sensor network and e-health, etc.

Liang Zhou is a professor in Key Lab of Broadband Wireless Communications and Sensor Network Technology (NJUPT), Ministry of Education, China. His research interests are in the areas of multimedia networks and wireless communications.



Xiaodong Lin received the Ph.D. degree in information engineering from Beijing University of Posts and Telecommunications, Beijing, China, in 1998 and the Ph.D. degree in electrical and computer engineering (with Outstanding Achievement in Graduate Studies Award) from the University of Waterloo, Waterloo, ON, Canada, in 2008. He is currently an Associate Professor of information security with the Faculty of Business and Information Technology, University of Ontario Institute of Technology (UOIT), Oshawa, ON. His research interests include wireless network security, applied cryptography, computer forensics, software security, and wireless networking and mobile computing. Dr. Lin received a Canada Graduate Scholarship for Doctoral Award from the Natural Sciences and Engineering Research Council of Canada and the Best Paper Awards of the 18th International Conference on Computer Communications and Networks (2009), the Fifth International Conference on Body Area Networks (2010), and IEEE International Conference on Communications (2007). He is a senior member of the IEEE.

.