# Secret Key Generation from Common Randomness over Ultra-wideband Wireless Channels

**Jing jing Huang, Ting Jiang**
Key Laboratory of Universal Wireless Communication, Ministry of Education
Beijing University of Posts and Telecommunications, Beijing, China
[e-mail: jingjinghuangbupt@gmail.com]
*Corresponding author: Ting Jiang

*Received May 4, 2014; revised July 22, 2014; accepted August 20, 2014; published October 31, 2014*

## Abstract

We develop a secret key generation scheme using phase estimation in ultra-wideband (UWB) wireless fading channels. Based on the reciprocity theorem, two terminals extract the phase of the channel as a common random source to generate secret bits. Moreover, we study the secret key rate by a pair of nodes observing correlated sources and communicating to achieve secret key agreement over public communication channels. As our main results, we establish a more practical upper bound from Cramer-Rao bound (CRB) and compare it with a universally theoretical upper bound on the shared maximum key rate from mutual information of correlated random sources. Derivation and numerical examples are presented to demonstrate the bound. Simulation studies are also provided to validate feasibility and efficiency of the proposed scheme.

***Keywords:*** UWB, secret key generation, Cramer-Rao bound, reciprocity, secret key capacity, mutual information

The research was supported by National Science Foundation of China under grant no.61171176. We express our thanks to the anonymous reviewers for their thoughtful and constructive remarks that are helpful to improve the quality of this paper.

**http://dx.doi.org/10.3837/tiis.2014.10.016**

## 1. Introduction

Recent developments in physical layer security have led to growing interest in secret key generation exploiting fading channel characteristics. The research on secret key generation encompasses the study of key generation algorithm, key capacity, some applications with existing communication techniques, such as orthogonal frequency division multiplexing (OFDM), multiple-input-multiple output (MIMO) and so on. In this paper, we focus on key generation mechanism and key capacity.

The problem of secret key generation from correlated random sources was firstly studied by Maurer [1], Ahlswede and Csiszar [2]. They derived some fundamental bounds on the secret key rate of system models. We will give details about their related contributions later in Section 2. Note that the eavesdropper in their system models can neither jam the channel nor tamper with any message over the public channel. The case of an adversary with the ability to modify the transmissions over the public channel has been discussed in [3-6]. Due to their work, a great deal of extensions explore the secret key generation capacity of some complex models. In [7, 8], secret key agreement was accomplished through wiretap channel [9] with no access to public channel. In [10-13], a wiretap channel influenced by a random channel state was pondered. In such models, channel state information can be viewed as a correlated source shared by two terminals of a wireless link, which affects secret key capacity as well. Chou considered key generation from a discrete memoryless multiple source (DMMS) using external source excitation [14, 15], and ergodic capacity of key generation from sparse wireless channels [16].

In respect of practical implementation of secret key generation, there have been many papers on key generation schemes. In the earliest work [17], Hershey sent two unmodulated signals through a radio link, measured the phase and quantized the differential phase values to generate secret key. Phase differences between multiple channels have been further investigated in [18-20]. Amplitude or received signal strength (RSS) is the most reciprocal common channel characteristic exploited for key generation in [21-25] because it can be easily acquired on most off-the-shelf radio devices. In addition, time delay and angle-of-arrival (AOA) can also be used for key generation. Note that AOA is unable to be used directly to generate key, steerable directional antennas should be employed as in [24] to obtain reciprocal channel gains. Besides, Madiseh et al. [26, 27] and Wilson et al. [28] utilize UWB radios to get channel feature. Huang et al. [29, 30] use multipath relative delay to generate key in UWB channels.

Although all the previous works [29-32] are interesting and have significantly contributed to this domain, there are still some limitations. For instance, probability of secret key match is not high in UWB channel using existing mechanisms. Secret key capacity over UWB channel has been neglected to deeply consider. Consequently, we will concentrate on the investigation of facilitating secret key match and establishing upper bounds on secret key rate in condition of UWB channel. Our main contribution are： We first develop a key generation mechanism using the phase characteristic of UWB channel. We then establish a practical upper bound on secret key rate using CRB. Finally, we perform numerical illustration to exemplify the practical bound and compare the practical bound with universal bound from mutual information. In addition, we implement simulation studies to validate that the mechanism is feasible and efficient.

The remainder of this paper is organized as follows. Section 2 gives problem formulation and preliminaries. Section 3 is devoted to an overview of the proposed secret key generation scheme. Section 4 describes the establishing process of the upper bound on secret key rate. Section 5 discusses numerical examples and simulation studies. In Section 6, conclusions and some possibilities for future work are presented.

## 2. Problem Formulation and Preliminaries

In this section, we first illustrate a secret key generation problem, introducing some basic concepts. We then specify our system model - UWB channel model [33] that is closely related to the proposed secret key generation scheme.

### 2.1 Problem Formulation

The inherent feature in wireless channel is considered to be the random source for secret key generation due to the following three aspects [30]:

1. Reciprocity of radio wave propagation: The multipath characteristics of the radio channel are theoretically identical on both directions of a link. A transmitter-receiver pair can obtain these characteristics from the received signal.
2. Spatial variations: The property of the radio channel is unique to the location of the two endpoints of the link. Receivers at different locations cannot observe the same channel response information. This uniqueness offers potential security guarantee. Generally, an entity that is at least $\lambda/2$ ($\lambda$ is the wavelength) away from the transmitter-receiver pair experiences uncorrelated fading.
3. Temporal variations in the radio channel: The movements of the communication parties as well as other objects near the transmitter-receiver pair in the environment will make the channel change over time. Apparently, channel variations are beneficial for increasing the randomness of secret keys.

Considering that two terminals A and B want to share common key in the presence of a passive adversary E, we suppose the system works in a time-division (TDD) mode. E is more than $\lambda/2$ ($\lambda$ is the wavelength of the radio waves being used) away from either A or B. Within the coherence time (i.e. the maximum time duration that the wireless channel impulse response is stable), A transmits a signal to B, and E can listen to it on the public channel. Afterwards, B transmits a signal to A, and E can also hear the signal. Legitimate terminals A and B measure the channel gain from the received signals, respectively, and generate secret key based on their observation. The adversary E knows the key generation algorithm and can eavesdrop all the transmissions between A and B. However, E can not make active attacks, which means E can only listen to the communication between legitimate terminals, not modifying it. E can not cause a man-in-the-middle attack, either. The above can be regarded as the essential element of a secret key generation problem in wireless networks. In this paper, we would like to leverage phase randomness to extract secret key and provide a practical upper bound on secret key rate.

In the end of this subsection, we introduce bounds on secret key rate discoved by Maurer [1], Ahlswede and Csiszar [2]. Considering a fundamental secret key generation problem as mentioned above, A and B observe a sequence of $n$ random variables $X^n=[X_1,X_2,...,X_n]$ and $Y^n=[Y_1,Y_2,...,Y_n]$, respectively, and an eavesdropper observes the sequence $Z^n$. For any given time case, the pair $(X_i,Y_i)$ is greatly statistically dependent. According to their observed

results, A and B generate secret key via exchanging a collection of message denoted by $C$ over public channel observable by an eavesdropper. If $f_A$ and $f_B$ are two functions, let $K_A = f_A(X^n, C)$, $K_B = f_B(Y^n, C)$, $R$ be an achieveable secret key rate and $K$ be secret key. For any $\varepsilon > 0$, $R$ is the maximum rate satisfying

$$P(K_A = K_B) \geq 1 - \varepsilon \tag{1}$$

$$I(K; C, Z^n)/n \leq \varepsilon \tag{2}$$

$$H(K) \geq \log|K| - \varepsilon \tag{3}$$

$$H(K)/n \geq R - \varepsilon \tag{4}$$

where $I$ means mutual information, $H$ stands for entropy. Condition (1) guarantees that A and B obtain common secret key with a low error probability; condition (2) ensures secret key is well unavailable to an eavesdropper; and condition (3) means that the distribution of the secret key is nearly uniform. Secret key capacity is the supremum of achievable secret key rates.

**Table 1.** A summary of important notation

| Notation | Definition |
|---|---|
| $T_c$ | channel coherence time |
| $t_o$ | observation time |
| $h(t)$ | channel gain |
| $f_s$ | sampling rate |
| $q$ | the number of quantization levels |
| $N_s$ | the number of samples in the observation time |
| $R_{\max}$ | key rate from mutual information |
| $R_{\max}^{CRB}$ | key rate from CRB |

## 2.2 System Model

We focus on a UWB wireless system while the proposed scheme can also be applicable to other communication systems. Assume that the frequency spectrums of transmitted and received signals are nonzero only over a bandwidth $B$ centered at frequency $f_c$. Then, the transmitted signal can be written as

$$x(t) = \Re\{\tilde{x}(t) e^{j2\pi f_c t}\} \tag{5}$$

where $\tilde{x}(t)$ is the complex valued random process with bandwidth extent $-B/2$ to $B/2$. The UWB channel impulse response is

$$h(t) = \sum_{l=0}^{L} \sum_{k=0}^{K} \alpha_{k,l} \exp(j\phi_{k,l}) \delta(t - T_l - \tau_{k,l}) \tag{6}$$

where $L$ is the number of clusters, $K$ is the number of rays within a cluster, $\alpha_{k,l}$ is the tap weight of the $k-th$ path in the $l-th$ cluster, $T_l$ is the delay of the $l-th$ cluster, $\tau_{k,l}$ is the delay of the $k-th$ path of the $l-th$ cluster relative to $T_l$, and phase $\phi_{k,l}$ is uniformly distributed in $[0, 2\pi]$.

In order to ease the analysis, we simplify the derivation, considering only one cluster. That means we do not analyze the influence of clusters. So the channel impulse response can be given by

$$h(t)=\sum_{k=0}^{K}\alpha_k \exp(j\phi_k)\delta(t-\tau_k) \tag{7}$$

The received signal can be written as

$$y(t)=\Re\left\{\left[\int_{-\infty}^{+\infty}h(\tau)\tilde{x}(t-\tau)\exp(-j2\pi f_c\tau)d\tau+n(t)\right]\exp(j2\pi f_c t)\right\}$$

$$=\sum_{k=0}^{K}\alpha_k x(t-\tau_k)\cos\phi_k\cos(2\pi f_c t)+\sum_{k=0}^{K}\alpha_k x(t-\tau_k)\sin\phi_k\sin(2\pi f_c t)+n(t)\exp(j2\pi f_c t)$$

$$=y_I(t)\cos(2\pi f_c t)+y_Q(t)\sin(2\pi f_c t)+n(t)\exp(j2\pi f_c t) \tag{8}$$

where $y_I(t)=\sum_{k=0}^{K}\alpha_k x(t)\cos\phi_k$, $y_Q(t)=\sum_{k=0}^{K}\alpha_k x(t)\sin\phi_k$, $n(t)$ is additive white Gaussian noise with mean power of $\sigma^2=N_0/2$. Note that equation (8) is derived based on the assumption that the delay associated with $\tau_k$ is lower than the delay spread. The complex equivalent signal for $y_I(t)\cos(2\pi f_c t)+y_Q(t)\sin(2\pi f_c t)$ is given by $y_I(t)+jy_Q(t)$ which has phase $\theta=\arctan\left(y_Q(t)/y_I(t)\right)$. $\theta$ is uniformly distributed in $[0,2\pi]$. Then, $y_I(t)+jy_Q(t)$ can be written as $y_I(t)+jy_Q(t)=|y|e^{j\theta}$, where $|y|=\sqrt{y_I(t)^2+y_Q(t)^2}$. Therefore, we get

$$y(t)=|y|\cos\theta\cos(2\pi f_c t)+|y|\sin\theta\sin(2\pi f_c t)+n(t)=|y|\cos(2\pi f_c t-\theta)+n(t) \tag{9}$$

We will make parameter estimation in $y(t)$ and use multipath channel phase to generate secret key. **Table 1** gives a list of important notation.

## 3. Secret Key Generation Scheme

In this section, we describe our key generation mechanism of extracting secret bits from phase randomness of UWB wireless channel, which is modified based on the approach in [20]. The difference is that we use the method in UWB environment and we consider the problem of time unsynchronization. **Fig.1** shows the key generation scheme.

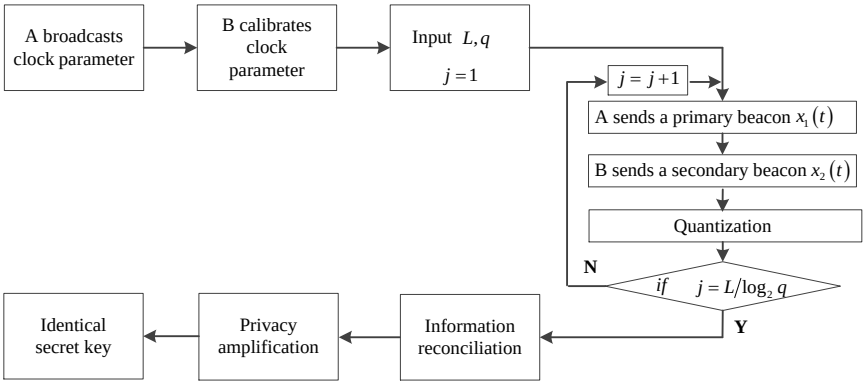


**Fig. 1.** A flow diagram of secret key generation mechanism from channel phase characteristic

We now detail our algorithm as follows:

1. Suppose terminal A is the primary node. A broadcasts its clock parameter to B. Then B calibrates its clock parameter based on A's clock information and sends an acknowledge character (ACK) to A. In this case, two terminals can have a common time reference to generate absolute phase estimators, which makes preparation for the following channel probing step.

2. Channel probing: For easy exposition, we assume the scheme starts at time zero point. In the first slot, terminal A sends a primary beacon $x_1(t)=\cos\left(w_c(t-0)\right)$, where $t\in[0,T_1)$, and $T_1$ means the duration of the primary beacon. Terminal B observes the response of the multipath channel over the interval $t\in[\tau_{AB},\tau_{AB}+\upsilon_{mAB})$. Here, $\tau_{AB}$ is the delay of the shortest path and $\upsilon_{mAB}$ is the delay spread of the channel $h_{AB}(t)$. Suppose $T_1>\max\upsilon_{mAB}$, the received signal at B can be expressed by

$$y_{AB}(t)=\alpha_{AB}\cos\left(w_c t+\theta_{AB}\right)+n_{AB}(t),t\in[\tau_{AB}+\upsilon_{mAB},\tau_{AB}+T_1) \tag{10}$$

where $n_{AB}(t)$ denotes the additive white Gaussian noise. $\alpha_{AB}$ and $\theta_{AB}$ denote the steady state gain and the phase response of channel $h_{AB}(t)$. At the end of primary beacon, a final response of the multipath channel is also received by B over the interval $t\in[\tau_{AB}+T_1,\tau_{AB}+\upsilon_{mAB}+T_1)$. With the noisy observation, B performs Maximum Likelihood Estimation (MLE) of the received phase and frequency, which are designated by $\hat{\theta}_{AB}$ and $\hat{w}_{AB}$ respectively. The MLE is implemented in three phases which are rough frenquency search, fine frequency search and phase estimation. $\hat{w}_{AB}$ and $\hat{\theta}_{AB}$ can be cauculated by [20]

$$\hat{w}_{AB}=\arg\max_w\left|Y(w)\right| \tag{11}$$

$$\hat{\theta}_{AB}=-\tan^{-1}\frac{\sum_{m=0}^{N_s-1}y[m]\sin(wm)}{\sum_{m=0}^{N_s-1}y[m]\cos(wm)} \tag{12}$$

where $y[m]$ is sample sequence of $y_{AB}(t)$, and $Y(w)$ is the continous discrete fourier transform of $y[m]$. We substitute $\hat{w}_{AB}$ for $w$ to compute $\hat{\theta}_{AB}$ in equation (12).

3. In the second slot, B transmits a secondary beacon $x_2(t)=\cos\left(w_c(t-t_2)\right)$ at the instant $t_2=\tau_{AB}+\upsilon_{mAB}+T_1$, where $t\in[t_2,t_2+T_2)$ and $T_2$ means the duration of the secondary beacon. Terminal A observes the response of the multipath channel over the interval $t\in[t_2+\tau_{BA},t_2+\tau_{BA}+\upsilon_{mBA})$. Owing to channel reciprocity, we have $\upsilon_{mAB}=\upsilon_{mBA}$. Similarly, suppose $T_2>\upsilon_{mBA}$, the received signal at A can be expressed by

$$y_{BA}(t)=\alpha_{BA}\cos\left(w_c t+\theta_{BA}\right)+n_{BA}(t)t\in[t_2+\tau_{BA}+\upsilon_{mBA},t_2+\tau_{BA}+T_2) \tag{13}$$

where $n_{BA}(t)$ represents the additive white Gaussian noise. $\alpha_{BA}$ and $\theta_{BA}$ denote the steady state gain and the phase response of channel $h_{BA}(t)$. At the end of this beacon, a final response of the multipath channel is also received by A over the interval $t\in[t_2+\tau_{BA}+T_2,t_2+\tau_{BA}+\upsilon_{mBA}+T_2)$. Through noisy observation, A uses the same method as B does to compute MLE of the received phase and frequency, which are designated by $\hat{\theta}_{BA}$ and $\hat{w}_{BA}$ respectively.

$$\hat{w}_{BA}=\arg\max_w\left|Y(w)\right| \tag{14}$$

$$\hat{\theta}_{BA} = -\tan^{-1}\frac{\sum_{m=0}^{N_s-1} y[m]\sin(wm)}{\sum_{m=0}^{N_s-1} y[m]\cos(wm)} \tag{15}$$

where $y[m]$ is sample sequence of $y_{BA}(t)$, and $Y(w)$ is the continous discrete fourier transform of $y[m]$. We substitute $\hat{w}_{BA}$ for $w$ to compute $\hat{\theta}_{BA}$ in equation (15).

4. Quantization: For the sake of generation of high-entropy secret bits, we assume only one round of channel probing (i.e. the former three steps) should be run by A and B during each coherence time. After one round, each terminal gets a phase estimation value for quantization.

$$\text{A: } \hat{\theta}_{BA} \bmod 2\pi, \text{ B: } \hat{\theta}_{AB} \bmod 2\pi$$

Both the two terminals uniformly map their phase estimation values into the quantization sector (index) according to the following rule:

$$Q(\theta) = i,\ \theta \in \left[2\pi i/q, 2\pi(i+1)/q\right),\ i \in 0,1,...,q-1$$

Hence, in the first round, after $i$ is encoded into bit vectors, each phase value generates $\log_2 q$ secret bits. On account of channel reciprocity theorem, A and B share $\log_2 q$ bits generated from $\hat{\theta}_{BA}$ and $\hat{\theta}_{AB}$.

Suppose the anticipated key size is $L$. For $j = 2,3,...,L/\log_2 q$, A and B repeat the steps as in the first round to extract phase estimation values and convert them into secret bits. After $L/\log_2 q$ rounds, A and B share the key $K_1$, whose size is $L$.

5. In accordance with channel reciprocity principle, the generated bits at A and B should be same. However, due to noise, estimation error and half-duplex transmission, some minor bit discrepancies may exist. We can correct these error bits using error correcting codes [34] or the Cascade Protocol [35]. Because the reconciliation information is transmitted in the public channel, some information might be revealed and an eavesdropper might guess portions of the key. To address these problems, Hash functions are leveraged by A and B to perform privacy amplification to increase entropy of secret key.

## 4. Upper Bounds on Secret Key Rate

In this section, we analyze the performance of the proposed key generation scheme in terms of the maximum key rate that the system can achieve. In the light of information theory, the mutual information of two random variables or sequences is a quantity that measures the mutual dependence of the two variables or sequences. Thus the secret key generation rate can be upper bounded by the mutual information between the observation of two terminals. We have established the upper bound on key rate from mutual information in [36]. Nonetheless, this bound does not depend on the specific estimation method, and is commonly loose. Hence, we plan to compute a more practical and tight upper bound on key rate using CRB in estimation theory. This is because CRB for unbiased parametric estimation offers a lower bound on the variance of estimator error.

We sample $y(t)$ at sampling rate $f_s$ with the first sample taken at $t_0 = 0$ to obtain discrete-time values. If we rewrite equation (9) as $y(t) = b\cos(wt+\theta)+n(t)$, and then

$$y[m] = b_0\cos\left[w(t_0+mT_s)+\theta_0\right]+n[m], 0 \le m \le N_s-1 \tag{16}$$

Let $s[m] = b_0\sin\left[w(t_0+mT_s)+\theta_0\right]+\check{n}[m], 0 \le m \le N_s-1$, where $s[m]$ is the Hilbert tranform of $y[m]$, $\check{n}[m]$ is the Hilbert transform of $n[m]$.

If we write $Z = y[m] + js[m]$, the probability density function (pdf) of $Z$ is [37]

$$f(Z;\alpha) = \left(\frac{1}{\sigma^2 2\pi}\right)^{N_s} \exp\left\{-\frac{1}{2\sigma^2}\sum_{m=0}^{N_s-1}\left[\left(y[m]-u_m\right)^2 + \left(s[m]-v_m\right)^2\right]\right\} \tag{17}$$

where, if $w$, $b$, $\theta$ are all unknown, $u_m$ and $v_m$ are functions of $\theta$,

$$\alpha = [w, b, \theta] \tag{18}$$

$$u_m = b\cos(wt_m + \theta) \tag{19}$$

$$v_m = b\sin(wt_m + \theta) \tag{20}$$

The unbiased CR bounds are the diagonal elements of the inverse of the Fisher information matrix $\mathbf{J}$, whose typical element is given by

$$J_{ij} = E\left\{\frac{\partial}{\partial\alpha_i}\ln f(Z;\alpha)\frac{\partial}{\partial\alpha_j}\ln f(Z;\alpha)\right\} \tag{21}$$

The bounds are given by

$$\mathrm{var}\{\hat{\alpha}_i\} \geq J_{ii} \tag{22}$$

where $\hat{\alpha}_i$ is the estimation of $\alpha_i$ and $J_{ii}$ is the $i\,th$ diagonal element of $\mathbf{J}^{-1}$.

When $f(Z;\alpha)$ is assumed by equation (17), the elements of $\mathbf{J}$ are

$$J_{ij} = \frac{1}{\sigma^2}\sum_{m=0}^{N_s-1}\left[\frac{\partial u_m}{\partial\alpha_i}\frac{\partial u_m}{\partial\alpha_j} + \frac{\partial v_m}{\partial\alpha_i}\frac{\partial v_m}{\partial\alpha_j}\right] \tag{23}$$

The subscripts $i$ and $j$ in equation (23) refer to the unknown elements in $\alpha$. In general instance, all elements of $\alpha$ are unknown. According to equation (21), the matrix $\mathbf{J}$ is

$$\mathbf{J} = \frac{1}{\sigma^2}\begin{bmatrix} b_0^2 T_s^2 N_s(N_s-1)(2N_s-1)/6 & 0 & b_0^2 T_s N_s(N_s-1)/2 \\ 0 & N_s & 0 \\ b_0^2 T_s N_s(N_s-1)/2 & 0 & b_0^2 N_s \end{bmatrix} \tag{24}$$

After computing the determinant of $\mathbf{J}$ and $\mathbf{J}$ 'adjoint matrix, we get $|\mathbf{J}| = b_0^4 T_s^2 N_s^3\left(N_s^2-1\right)/\left(12\sigma^6\right)$. Finally,

$$\mathrm{var}\{\theta\} \geq \frac{1}{|\mathbf{J}|}\mathbf{J}_{33}^{*} = \frac{2\sigma^2(2N_s-1)}{b_0^2 N_s(N_s+1)} \tag{25}$$

We rewrite equation (25) as

$$\mathrm{var}\{\theta\} = \sigma_{\hat{\theta}}^2 \geq \frac{2}{\left(b_0^2/\sigma^2\right)\left[N_s(N_s+1)/(2N_s-1)\right]} \tag{26}$$

where CRB can be expressed as a function of signal noise ratio (SNR) and $N_s$.

Assume $[\,0, 2\pi\,]$ is divided into $q = 2^n$ levels. Next we explore the probability that estimations of terminal A and B are in the same interval when conducting quantization. Suppose $P_A$ represents the average probability of quantization index agreement. Without loss of generality, assume that $\theta$ falls into the $i\,th$ section $\left[2\pi i/q, 2\pi(i+1)/q\right)$, $(i \in 0,1,...,q-1)$. According to equation (26), phase estimation errors are independent and Gaussian distributed [20], the probability of $\hat{\theta} = \theta + \tilde{\theta} \in \left[2\pi i'/q, 2\pi(i'+1)/q\right)$ is

$$P_{Ai'}(\theta) = \int_{2\pi i'/q}^{2\pi(i'+1)/q}\frac{1}{\sqrt{2\pi}\sigma_{\tilde{\theta}}}\exp\left\{-\frac{(x-\theta)^2}{2\sigma_{\tilde{\theta}}^2}\right\}dx \tag{27}$$

where $i^{'} \in (0,1,...,q-1)$ and $\tilde{\theta}$ is the estimation error.

As a result, $P_A$ can be computed by $P_A(\theta) = \sum_{i^{'}=0}^{q-1} P_{Ai^{'}}(\theta)^2$. Here, if the true $\theta$ approximates the center of a interval, then $P_{Ai^{'}}(\theta)$ rises, and vice versa. $P_{Ai^{'}}(\theta)$ is symmetric to the center of a interval and the variance of phase is much smaller than one. Thus, concerning $\theta \in \left[2\pi i/q, 2\pi(i+1)/q\right)$, $P_{Ai^{'}}(\theta)$ is primarily determined by $P_{Ai}(\theta)$ ($i^{'} = i$). On the basis of the above analysis, the average probability of quantization index agreement can be computed as

$$P_A = \int_{2\pi i/q}^{2\pi(i+1)/q} P_A(\theta)\frac{q}{2\pi}d\theta \approx \int_{2\pi i/q}^{2\pi(i+1)/q} P_{Ai}(\theta)^2\frac{q}{2\pi}d\theta \tag{28}$$

When terminal A and B's estimations lie in the same section, they agree on the secret bits, whose size is $\log_2 q$. Therefore, the key rate is

$$R_{\max}^{CRB} = \frac{P_A \log_2 q}{T_c} \tag{29}$$

## 5. Numerical Examples and Simulation Studies

In this section, numerical examples of upper bounds on secret key rate are presented. Additionally, the proposed key generation scheme using phase randomness is verified through simulation from three evaluation metrics, which are key generation rate, key-mismatch probability and key randomness.

### 5.1 Numerical Illustration on Upper Bounds

Assume $T_c$=33.3ms, $q$=16, $t_o \approx T_c/2$=16.65ms, then $N_s = t_o f_s$. This example considers the two upper bounds on secret key rate between two terminals as the observation time $t_o$ rises. **Fig.2** shows R-MI is higher than R-CRB, which suggests that the upper bound from mutual information R-MI servers as the universal upper bound and the upper bound from Cramer-Rao bound R-CRB is tighter on secret key rate. The bounds grow rapidly when $t_o$ varies from 0 to 5.55ms, while increase slowly from 5.55 to 16.65ms. Because the growth of $N_s$ leads to the decline of $\sigma_{\tilde{\theta}}^2$ according to equation (26), $P_A$ will increase according to equation (27) and (28), then the secret key rate will rise. However, $P_A$ seldom increases fast during the observation interval 8.325 to 16.65ms. Note that the key rate can also be increased by enhancing SNR.

In order to explore how the CR bound on secret key rate changes with $N_s$, referring to the equation of CR bound on key rate

$$R_{\max}^{CRB} = P_A(\log_2 q) f_s \tag{30}$$

we present its numerical results (the curves R-CRB) in Fig.3. We use the same value of $P_A$ as equation (29) and the same value of $t_o$ as Fig.2. Here, we assume $f_s$=20GHz. The curve R-MAX is $f_s(\log_2 q)$, which serves the upper bound of $R_{\max}^{CRB}$. It can be seen that R-MAX can be approached when SNR or $N_s$ become very large. Therefore, we can increase secret key rate by enhancing SNR or $N_s$.

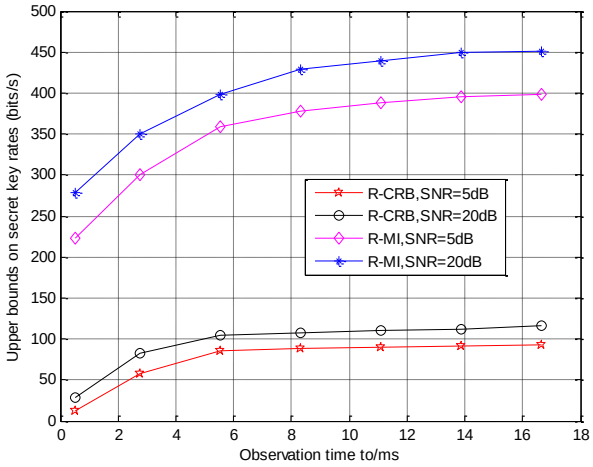


**Fig. 2.** Key rate versus observation time $t_o$ under different SNR

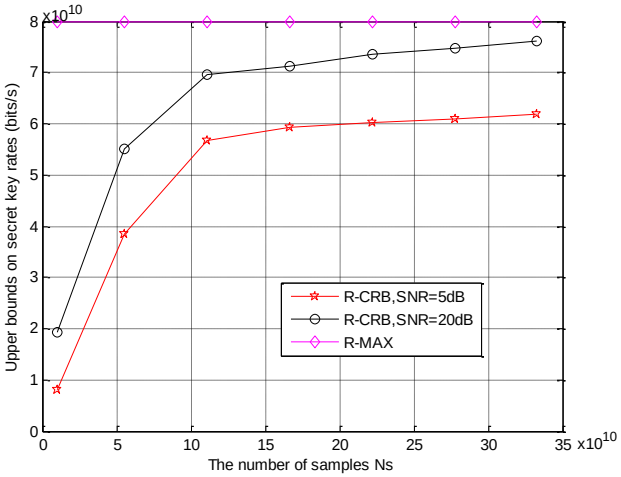


**Fig. 3.** Key rate versus $N_s$ under different SNR

## 5.2 Simulation Studies

The simulated channel model is the UWB channel model [33] in subsection 2.2. We utilize full MLE and approximate analytical prediction using CRB to estimate the variance of the phase estimation error. Additionally, some other parameters are:

1) Carrier frequency of 4.5GHz
2) Bandwidth of 600MHz
3) Sampling rate of 20GHz
4) Average moving speed of 2m/s, Doppler shift of 30Hz
5) Coherence time of 33.3ms
6) Number of quantization levels of 16

### 5.2.1 Key Generation Rate

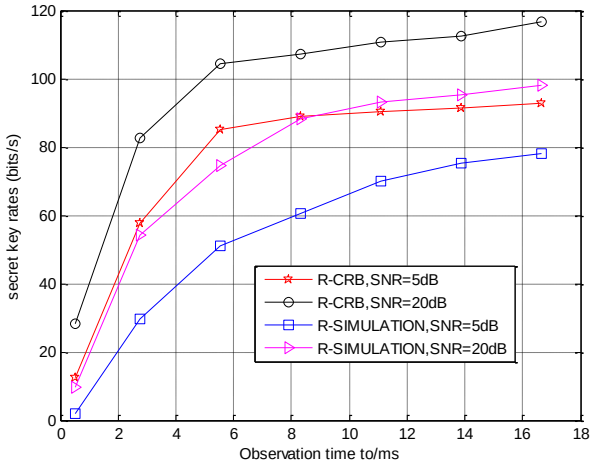


**Fig. 4.** Key rate comparison between using CRB and simulation under different SNR

**Fig. 4** diplays key rates under different SNR versus observation time given $q$=16 using CRB analytical prediction and simulation. As we mentioned before, CRB is a lower bound on the variance of estimation error and can provide a more practical bound on key rate. The curves indicate that key rate from simulation is more close to the CRB at high SNR as well as large $t_o$, which proves that the proposed method can approximate CRB on secret key rate. Here, if $q$ is a variable, key rate will increase as $q$ increases. This is because $q$ stands for the number of quantization levels, the increase of $q$ leads to the increase of $\log_2 q$, and finally the increase of key rate.

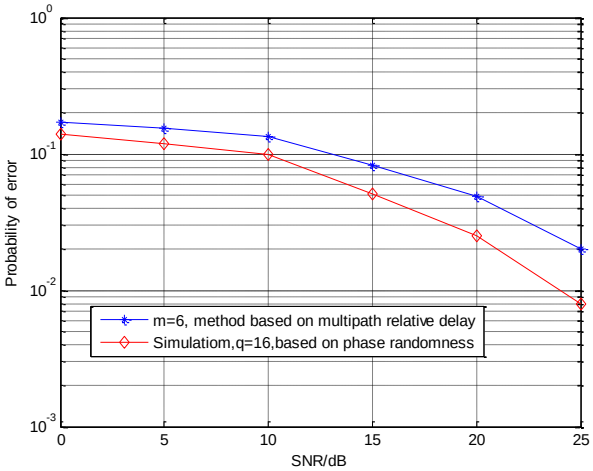


**Fig. 5.** Probability of error based on different scheme

### 5.2.2 Key-mismatch Probability

In order to evaluate key-mismatch probability, which means the probability that two terminals fail to agree on the same key bits, **Fig. 5** plots the error probability (i.e., key-mismatch probability) as a function of SNR. It can be observed that error probability decreases when SNR increases. For better comparison, we also give the error probability using our former method (see Fig.9 in [30]), the results illustrate that the proposed approach using phase randomness outperforms the method exploiting multipath relative delay in terms of key match. Note that the error probability will increase as $q$ increases. The reason is that when $q$ increases, the interval $\left[2\pi i/q, 2\pi(i+1)/q\right)$ becomes smaller and, hence the probability that terminal A and terminal B falls into the same interval decreases.

### 5.2.3 Key Randomness

**Table 2.** Results of NIST

| Test | P-value |
|---|---|
| Frequency | 0.11 |
| BlockFrequency | 0.15 |
| Cumulative sum(Fwd) | 0.29 |
| Cumulative sum(Rev) | 0.17 |
| Runs | 0.31 |
| Longest run | 0.5 |
| Approximate Entropy | 0.54 |
| Serial | 0.37, 0.41 |

We employ a widely used randomness test suit NIST [38] to verify the randomness of our generated secret key bits. 80 key sequences generated from our simulation are randomly selected and their p-values are calculated. To pass the test, all p-values must be greater than 0.01. Due to the limitation of bit length, we run eight tests from 16 different statistical tests in Linux. The results listed in **Table 2** show that the generated key bit streams pass the test, which can ensure the randomness of the secret keys.

## 6. Conclusions

In this paper, we have proposed a secret key generation mechanism using phase characteristic in UWB channels. Simulation studies have been conducted and the results demonstrate that the mechanism is feasible, and achieves better performance in key match. Furthermore, we establish a practical upper bound on secret key rate, also comparing it with the theoretical bound from mutual information. Numerical examples are employed to exemplify the bounds. For further study, we would like to optimize secret key generation algorithm to find a solution to achieve a better balance between key rate and key-match probability and explore the lower bound on secret key rate.

## References


[1] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inform. Theory*, vol. 39, no. 3, pp. 733-742,May 1993. Article (CrossRef Link).

[2] R. Ahlswede, and I. Csiszar, "Common randomness in information theory and cryptography. I. secret sharing," *IEEE Trans. on Information Theory*, vol.39, no.4, pp. 1121-1132, 1993. Article (CrossRef Link).

[3] U. M. Maurer, "Information-theoretically secure secret-key agreement by NOT authenticated public discussion," in *Advances in Cryptology-Eurocrypt*, pp. 209-225, 1997. Article (CrossRef Link).

[4] U. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels-Part I: Definitions and a completeness result," *IEEE Trans. on Information Theory*, vol. 49, no. 4, pp. 822-831, Apr. 2003. Article (CrossRef Link).

[5] U. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels-Part II: The simulatability condition," *IEEE Trans. on Information Theory*, vol. 49, no. 4, pp. 832-838, Apr. 2003. Article (CrossRef Link).

[6] U. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels-Part III: Privacy amplification," *IEEE Trans. on Information Theory*, vol. 49, no. 4, pp. 839-851, Apr. 2003. Article (CrossRef Link).

[7] A. Khisti, S. Diggavi, and G. Wornell, "Secret-key generation with correlated sources and noisy channels," in *Proc. Int. Symp. Inform. Theory*, pp. 1005–1009, July 2008. Article (CrossRef Link).

[8] V. Prabhakaran, K. E swaran, and K. Ramchandran, "Secrecy via sources and channels-a secret key-secret message rate tradeoff region," in *Proc. of Int. Symp. Inform. Theory*, pp. 1010-1014, July 2008. Article (CrossRef Link).

[9] A. Wyner, "The wire-tap channel," *The Bell Systems Technical J.*, vol. 54, pp. 1355-1387, 1975. Article (CrossRef Link).

[10] Y. Chen and A. Han Vinck, "Wiretap channel with side information," *IEEE Trans. on Information Theory*, vol. 54, pp. 395-402, Jan. 2008. Article (CrossRef Link).

[11] W. Liu and B. Chen, "Wiretap channel with two-sided channel state information," in *Proc. of Asilomar Conf. Signals, Systems and Computers*, pp. 893-897, Nov. 2007. Article (CrossRef Link).

[12] A. Khisti, S. Diggavi, and G. Wornell, "Secret key agreement using a symmetry in channel state knowledge," in *Proc. of Int. Symp. Inform. Theory*, pp. 2286-2290, 2009. Article (CrossRef Link).

[13] A. Khisti, S. Diggavi, and G. Wornell, "Secret-key agreement with channel state information at the transmitter," *IEEE Trans on Information Forensics and Security*, vol. 6, no. 3, pp. 672-681, 2011. Article (CrossRef Link).

[14] T. Chou, S. Draper, and A. Sayeed, "Key generation using external source excitation: Capacity, reliability, and secrecy exponent," *IEEE Trans. on Information Theory*, vol. 58, pp. 2455-2474, Apr. 2012. Article (CrossRef Link).

[15] T. Chou, V. Tan, and S. Draper, "The sender-excited secret key agreement model: Capacity theorems," in *Proc. of Allerton Conference on Communication, Control, and Computing*, pp. 928-935, 2011. Article (CrossRef Link).

[16] T. Chou, S. Draper, and A. Sayeed, "Secret Key Generation from Sparse Wireless Channels: Ergodic Capacity and Secrecy Outage," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1751-1764, Sep. 2013. Article (CrossRef Link).

[17] J. E. Hershey, A. A. Hassan, and R. Yarlagadda, "Unconventional Cryptographic Keying Variable Management," *IEEE Trans. Comm.*,vol. 43, no. 1, pp. 3-6, Jan. 1995. Article (CrossRef Link).

[18] A. A. Hassan, W. E. Stark, and J. E. Hershey, "Cryptographic key agreement for mobile radio," *Digital Signal Processing*, vol. 6, pp. 207-212, 1996. Article (CrossRef Link).

[19] A. Sayeed and A. Perrig, "Secure Wireless Communications: Secret Keys through Multipath," in *Proc. of IEEE Int'l Conf. Acoustic, Speech & Signal Processing*, pp. 3013-3016, Apr. 2008. Article (CrossRef Link).

[20] Q. Wang, K. Xu, and K. Ren, "Cooperative secret key generation from phase estimation in narrow band fading channels," *IEEE Journal on selected areas in communications*, vol. 30, no. 9, pp.1666-1674, Oct. 2012. Article (CrossRef Link).

[21] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *Proc. ACM CCS'07*, Alexandria, USA, pp. 401-410, Oct. 2007. Article (CrossRef Link).
[22] S. Mathur, W. Trappe, N. Mandayam, and C.Ye, "Radio telepathy: extracting a secret key from an unauthenticated wireless channel," in *Proc. ACM MobiCom'08*, San Francisco, USA, pp. 128-139, Sept. 2008. Article (CrossRef Link).
[23] S. Jana, S. N. Premnath, M. Clark, S. Kasera, N. Patwari, and S. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," in *Proc. of ACM MobiCom'09*, pp. 321-332, Sept. 2009. Article (CrossRef Link).
[24] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation for fading wireless channels," *IEEE Trans on Antennas and Propagation*, vol. 53, no. 11, pp. 3776-3784, Nov. 2005. Article (CrossRef Link).
[25] C. Ye, S. Mathur, A. Reznik, Y. Shah, W.Trappe, and N.Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Trans on Information Forensics and Security*, vol. 5, no. 2, pp. 240-254, Jun. 2010. Article (CrossRef Link).
[26] M. G. Madiseh, M. L. McGuire, S. S. Neville, L. Cai, and M. Horie, "Secret key generation and agreement in UWB communication channels," *IEEE GLOBECOM'08*, New Orleans, USA, pp. 1-5, Nov. 2008. Article (CrossRef Link).
[27] M. G. Madiseh, S. He, M. L. McGuire, S. Neville, and X. Dong, "Verification of secret key generation from UWB channel observations," in *Proc. of IEEE Int. Conf. Communications*, Dresden, Germany, pp. 1-5, Jun. 2009. Article (CrossRef Link).
[28] R.Wilson, D. Tse, and R. Scholtz, "Channel identification: secret sharing using reciprocity in UWB channels," *IEEE Trans on Information Forensics and Security*, vol. 2, no. 3, pp. 364-375, 2007. Article (CrossRef Link).
[29] J. J. Huang, and T. Jiang, "Secret key generation exploiting Ultra-wideband indoor wireless channel characteristics," *IEEE MILCOM'13*, San Diego, USA, Nov. 2013. Article (CrossRef Link).
[30] J. J. Huang, and T. Jiang, "Secret key generation using reciprocity in Ultra-wideband outdoor wireless channels," *KSII Trans on Internet and Information Systems*, vol. 8, no. 2, pp. 524-539, Feb. 2014. Article (CrossRef Link).
[31] Lih-Chyau Wuu, Chi-Hsiang Hung and Wen-Chung Kuo, "Group Key Management based on (2, 2) Secret Sharing," *KSII Trans on Internet and Information Systems*, vol. 8, no. 3, pp. 1144-1156, Mar. 2014. Article (CrossRef Link).
[32] P.Vijayakumar, S.Bose, A.Kannan and L.Jegatha Deborah, "Computation and Communication Efficient Key Distribution Protocol for Secure Multicast Communication," *KSII Trans on Internet and Information Systems*, vol. 7, no. 4, pp. 878-894, Apr. 2013. Article (CrossRef Link).
[33] J. Foerster, *Channel modeling sub-committee report (final)*, Feb. 2003.
[34] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM Journal of Computing*, vol. 38, no.1, pp. 97-139, 2008. Article (CrossRef Link).
[35] G. Brassard, and L. Salvail, "Secret key reconciliation by public discussion," *Lecture notes in Computer Science*, 765: 410-423, 1994. Article (CrossRef Link).
[36] J. J. Huang, and T. Jiang, "Information-theoretically adaptive PHY-based secret key generation in Ultra-wideband channel," submitted to *Ad Hoc & SensorWireless Networks.*
[37] David C. Rife and Robert R. Boorstyn. "Single tone parameter estimation from discrete-time observations," *IEEE Transactions on Information Theory*, vol. 20, no. 5, pp. 591-598, Sep. 1974. Article (CrossRef Link).
[38] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Hechert, J. Dray, and S. Vo, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," 800th ed., *National Institute of Standards and Technology*, May. 2001.

**Jing jing Huang** received her B.E and M.S degree in communication engineering from Nan Chang University of Aeronautics, Jiang Xi province, China in 2007 and 2010 respectively. From 2010 to 2012, she was a teacher in communication department at An Hui University of Technology. Now, she is a Ph.D. student, majoring in communication and information system, at Beijing University of Posts and Telecommunications. Her research interests are primarily in Internet of things and wireless network security.

**Ting Jiang** is currently a professor of Key Laboratory of Universal Wireless Communication, Ministry of Education at Beijing University of Posts and Telecommunications. His research interests include short range communication, wireless sensor network, information security and signal processing.