Information-Theoretically Secret Key Generation for Fading Wireless Channels

Chunxuan Ye, Suhas Mathur, Alex Reznik, Yogendra Shah, Wade Trappe, and Narayan B. Mandayam, *Fellow, IEEE*

***Abstract*—The multipath-rich wireless environment associated with typical wireless usage scenarios is characterized by a fading channel response that is time-varying, location-sensitive, and uniquely shared by a given transmitter–receiver pair. The complexity associated with a richly scattering environment implies that the short-term fading process is inherently hard to predict and best modeled stochastically, with rapid decorrelation properties in space, time, and frequency. In this paper, we demonstrate how the channel state between a wireless transmitter and receiver can be used as the basis for building practical secret key generation protocols between two entities. We begin by presenting a scheme based on level crossings of the fading process, which is well-suited for the Rayleigh and Rician fading models associated with a richly scattering environment. Our level crossing algorithm is simple, and incorporates a self-authenticating mechanism to prevent adversarial manipulation of message exchanges during the protocol. Since the level crossing algorithm is best suited for fading processes that exhibit symmetry in their underlying distribution, we present a second and more powerful approach that is suited for more general channel state distributions. This second approach is motivated by observations from quantizing jointly Gaussian processes, but exploits empirical measurements to set quantization boundaries and a heuristic log likelihood ratio estimate to achieve an improved secret key generation rate. We validate both proposed protocols through experimentations using a customized 802.11a platform, and show for the typical WiFi channel that reliable secret key establishment can be accomplished at rates on the order of 10 b/s.**

***Index Terms*—Information-theoretic security, key generation, PHY layer security.**

I. Introduction

THE problem of secret key generation from correlated information was first studied by Maurer [39], and Ahlswede and Csiszár [4]. In a basic secret key generation problem, called the *basic source model*, two legitimate terminals (Alice and Bob)[1] observe a common random source that is inaccessible to an eavesdropper. Modeling the observations as memoryless, we can define the model as follows: Alice and Bob respectively observe n independent and identically distributed (i.i.d.) repetitions of the dependent random variables X and Y, denoted by $X^n = (X_1, \ldots, X_n)$ and $Y^n = (Y_1, \ldots, Y_n)$. In any given time instance, the observation pair (X_i, Y_i) is highly statistically dependent. Based on their dependent observations, Alice and Bob generate a common secret key by communicating over a public error-free channel, with the communication denoted collectively by $\mathbf{V}$.

A random variable K with finite range $\mathcal{K}$ represents an ε-*secret key* for Alice and Bob, achievable with communication $\mathbf{V}$, if there exist two functions f_A, f_B such that $K_A = f_A(X^n, \mathbf{V})$, $K_B = f_B(Y^n, \mathbf{V})$, and for any $\varepsilon > 0$

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

$$I(K; \mathbf{V}) \leq \varepsilon \tag{2}$$

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

Here, condition (1) ensures that Alice and Bob generate the same secret key with high probability; condition (2) ensures such secret key is effectively concealed from the eavesdropper observing the public communication $\mathbf{V}$; and condition (3) ensures such a secret key is nearly uniformly distributed.

An achievable secret key rate R is defined [4], [39] to be a value such that for every $\varepsilon > 0$ and sufficiently large n, an ε-secret key K is achievable with suitable communication such that $1/nH(K) \geq R - \varepsilon$. The supremum of all achievable secret key rates is the *secret key capacity* denoted by C_{SK}. For the model presented above, this is given by [4], [39], [40], [42]

$$C_{\mathrm{SK}} = I(X; Y). \tag{4}$$

This result holds for both discrete and continuous random variables X and Y, as long as $I(X; Y)$ is finite (cf., [47], [62]).

The model defined above assumes the eavesdropper (i.e., Eve) may observe the transmissions on the public channel, but is unable to tamper with them and has no access to any other useful side information. The case of an eavesdropper with access to side information has received significant attention (see, e.g., [4], [19], [39], [53]); unfortunately the capacity problem remains open in this case. The case of an eavesdropper with the ability to tamper with the transmissions on the public channel has been addressed in a comprehensive analysis by Maurer and Wolf [41], [43]–[45].

[1]Unless otherwise specified, all the terminals in this paper refer to legitimate terminals, and hence the term "legitimate" will be omitted henceforth.

Manuscript received February 23, 2009; revised January 02, 2010; accepted January 04, 2010. Date of publication March 01, 2010; date of current version May 14, 2010. The work of S. Mathur, W. Trappe, and N. B. Mandayam was supported in part by the National Science Foundation (NSF) Grant CNS-0626439 and in part by Defense Advanced Research Projects Agency (DARPA) Grant W31P4Q-07-1-002. Portions of this work were presented at the IEEE International Symposium on Information Theory, Seattle, WA, July 2006 and the ACM Conference on Mobile Computing and Networking, San Francisco, CA, Sep. 2008. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Christian Cachin.

C. Ye, A. Reznik, and Y. Shah are with InterDigital Communications, LLC, King of Prussia, PA 19406 USA (e-mail: chunxuan.ye@interdigital.com; alex.reznik@interdigital.com; yogendra.shah@interdigital.com).

S. Mathur, W. Trappe, and N. B. Mandayam are with WINLAB, Rutgers University, North Brunswick, NJ 08902 USA (e-mail: suhas@winlab.rutgers.edu; trappe@winlab.rutgers.edu; narayan@winlab.rutgers.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2010.2043187

A practical implementation of secret-key agreement schemes follows a basic three-phase protocol defined by Maurer *et al.*. The first phase, *advantage distillation* [39],[15], is aimed at providing two terminals an advantage over the eavesdropper when the eavesdropper has access to side information. We do not consider this scenario (as we shall see shortly, it is not necessary for secrecy generation from wireless channels) and, therefore, do not address *advantage distillation*.

The second phase, *information reconciliation* [7], [8], [14], is aimed at generating an identical random sequence between the two terminals by exploiting the public channel. For a better secret key rate, the entropy of this random sequence should be maximized, while the amount of information transmitted on the public channel should be minimized. This suggests an innate connection between the information reconciliation phase of the secrecy agreement protocol and Slepian–Wolf data compression. This connection was formalized by [23] in the general setting of multiterminal secrecy generation.

The connection between secrecy generation and data compression is of significant practical, as well as theoretical interest. Considering the duality between Slepian–Wolf data compression and channel coding (e.g., [17], [20], [27], [35], [49], etc.), the relationship between secrecy generation and data compression allows capacity-achieving channel codes, like Turbo codes or low-density parity check (LDPC) codes, to be used for the information reconciliation phase. Moreover, the capacity-achieving capabilities of such codes in the channel coding sense carry over to the secrecy generation problem. A comprehensive treatment of the application and optimality of such codes to the secrecy generation problem can be found in [12] and [13].

The last phase of Maurer's protocol, *privacy amplification* [9], [11], extracts a secret key from the identical random sequence agreed to by two terminals in the information reconciliation phase. This can be implemented by linear mapping and universal hashing [11], [16], [45], [57], or by an extractor [22], [24], [25], [45], [52]. The combination of the information reconciliation phase and the privacy amplification phase has been considered in [15] and [61].

Perhaps the first practical application of the basic source model is quantum cryptography (cf. e.g., [10], [46]), where nonorthogonal states of a quantum system provide two terminals correlated observations of randomness which are at least partially secret from a potential eavesdropper. Quantum key distribution schemes based on continuous random variables have been discussed in [13], [28], [36], and [55]. Less realized is the fact that the wireless fading channel provides another source [12], [30], [62] of secrecy which can be used to generate information-theoretically secure keys. Because the source model for secrecy establishment essentially requires *a priori* existence of a "dirty secret" which is then just cleaned up, such sources of secrecy are hard to find. To our knowledge, no such sources other than quantum entanglement and wireless channel reciprocity have been identified to date. Further, we note that although there have been several implementations of quantum cryptographic key establishment, little work has been done to provide a system validation of this process for wireless channels. This paper examines both theoretical and practical aspects of key establishment using wireless channels and represents one of the first validation efforts to this effect.

An alternative approach to secrecy generation from wireless channels is based on the wiretap channel models, see e.g., [12]. However, this approach suffers from a need to make certain assumptions as part of the security model that are hard to satisfy in practice and has not, to date, led to a practical implementation.

A (narrowband) wireless channel is well modeled as a flat fading channel. The fading coefficient changes in time, but the change is rather slow (on the order of 1 ms to 1 s, depending on terminal velocities and other factors). For simplicity, let us consider frequency flat fading. Roughly speaking, for a fixed time and location, the transmitted signal t and the received signal r are related via $r = Ft+Z$, where F is the channel fading coefficient and Z is the additive independent noise. If the transmitted signal t is known at the receiver beforehand (e.g., it is a training sequence), then the receiver is able to obtain a noisy estimate of the fading coefficient F. Furthermore, if both terminals send the training sequence at approximately the same time (more precisely, well within one channel coherence time of each other), then they can obtain channel estimates that are highly correlated due to channel reciprocity. This suggests the following model: let the random variables X and Y be defined by $X = F + Z_A$, $Y = F + Z_B$, where F, Z_A, Z_B are three independent random variables.

In data communications application, it is common to model the channel as Rayleigh or Rician, in which case, F, Z_A, and Z_B are Gaussian. Let these be distributed as $\mathcal{N}(0, P)$, $\mathcal{N}(0, N_A)$, and $\mathcal{N}(0, N_B)$, respectively. A simple calculation shows that the secret key capacity [62] of this jointly Gaussian model is

$$C_{\mathrm{SK}} = \log_2 \left(1 + \frac{P}{N_A + N_B + \frac{N_A N_B}{P}} \right) \frac{\text{bits}}{\text{sample}}. \qquad (5)$$

If we let $N_A = N_B = N$ in this setting, then we get a natural definition of signal-to-noise ratio (SNR) as $\mathsf{SNR} = P/N$, and the above secret key capacity reduces to $\log_2 (1 + (\mathrm{SNR}/2 + 1/\mathrm{SNR}))$ bits/sample.

As noted, the above calculation is relevant for the traditional Rayleigh or Rician fading model, and serves as an upper bound on the secret key establishment rate, but does not provide insight into how one can practically extract such secret bits from the underlying fading process. In this paper, we examine two different approaches for secrecy extraction from the channel state between a transmitter and receiver in a richly scattering wireless environment. Our first approach, which is based on level-crossings, is a simple algorithm that is well-suited for environments that can be characterized as Rayleigh or Rician. However, we recognize that such a method might not apply to other, general fading cases. One way to address this problem is to consider more complex fading distribution models, such as those appropriate for ultrawideband channels. This has been addressed in a previous work by Wilson *et al.* [58] (see also [5], [6], and [31]). However, we take a different approach in this paper. Inspired by our prior work on Gaussian-based approaches, we propose a *universal* reconciliation approach for wireless channels. This second, and more powerful method, only assumes that the channel impulse responses (CIRs) measured at both terminals are highly correlated, and their measurement noise is very low. Whereas the first of our two approaches was simple, and able

to achieve a limited secret key establishment rate, our second approach is more complex, but is able to take better advantage of the secrecy capabilities offered by CIR measurements, which tend to have high SNR (due to a high processing gain associated with such measurements in modern communication systems).

In both of these cases, our goal is to come up with a practical approach to secrecy generation from wireless channel measurements. In particular, because the statistics of the real channel sources we utilize are not known (and that is the major challenge we believe addressed by our work), it is impossible to make any quantitative statements about optimality of our approaches. Nevertheless, we do want to make sure that our solution is based on solid theoretical foundation. To do so, we include discussion of the motivating algorithms and their performance in idealized models when necessary.

Several previous attempts to use wireless channels for encrypting communications have been proposed. Notably, reference [34] exploited reciprocity of a wireless channel for secure data transformation; reference [29] discussed a secrecy extraction scheme based on the phase information of received signals; the application of the reciprocity of a wireless channel for terminal authentication purpose was studied in [48], [59], and [60], etc. Unlike these and other approaches, our approach for direct secrecy generation allows the key generation component to become a "black box" within a larger communication system. Its output (a secret bit stream) can then be used within the communication system for various purposes. This is important, as the key generation rate is likely to be quite low, and thus direct encryption of data will either severely limit throughput (to less than 1 kb/s in indoor channels) or result in extremely weak secrecy.

The adversary model assumed in this paper focuses mainly on passive attacks. We do not consider authentication attacks, such as the man-in-the-middle attack, since these require an explicit authentication mechanism between Alice and Bob and cannot be addressed by key-extraction alone. The starting point for algorithms presented in this paper is the successive probing of the wireless channel by the terminals that wish to extract a secret key. Implicitly, we assume that the adversary is not engaging in an active attack against the probing process, though we note that physical layer authentication techniques, such as presented in [60], might be applicable in such an adversarial setting. The infeasibility of passive eavesdropping attacks on the key generation procedures is based on the rapid spatial decorrelation of the wireless channel. We demonstrate this using empirically computed mutual information from the channel-probing stage, between the signals received at Bob and Eve and comparing it with the mutual information between the signals received at Alice and Bob. Beyond the basic eavesdropping attack, we do consider a particular type of active attack in our level-crossing algorithm in Section II, where the adversary attempts to disrupt the key extraction protocol by replacing or altering the protocol messages. In this case, we provide a method to deal with this type of active attack by cleverly using the shared fading process between Alice and Bob.

One of the goals of our work is to demonstrate that secrecy generation can be accomplished in real-time over real channels (and not simulation models) and in real communication systems. To that end, results based on implementations on actual wireless platforms (a modified commercial 802.11 a/g implementation platform) and using over-the-air protocols are presented. To accomplish this, we had to work with several severe limitations of the *experimental system* at our disposal. Consequently, certain parameters (e.g., code block length) had to be selected to be somewhat below what they should be for a well-designed system. This, however, does not reflect on the feasibility of proper implementation in a system with these features designed in. For example, nothing would prevent a design with the code block length sufficiently long to guarantee desired performance. On the contrary, we believe the demonstration of a practical implementation to be one of the major contributions of our work.

The rest of this paper is organized as follows. Section II discusses the simpler of our algorithms based on level crossings. Section III presents a more complex and more powerful approach to extracting secret bits from the channel response, as well as some new results on secrecy generation for Gaussian sources which motivate our solution. We conclude the paper with some final remarks in Section IV.

II. Level Crossing Secret Key Generation System

In this section, we describe a simple and lightweight algorithm in [38] for extracting secret bits from the wireless channel that does not explicitly involve the use of coding techniques. While this comes at the expense of a lower secret key rate, it reduces the complexity of the system and it still provides a sufficiently good rate in typical indoor environments. The algorithm uses excursions in the fading channel for generating bits and the timing of excursions for reconciliation. Further, the system does not require i.i.d. inputs and, therefore, does not require knowledge of the channel coherence time *a priori*. We refer to this secret key generation system as the *level crossing system*. We evaluate the performance of the level crossing system and test it using customized 802.11 hardware.

A. System and Algorithm Description

Let $F(t)$ be a stochastic process corresponding to a time-varying parameter F that describes the wireless channel shared by, and unique to Alice and Bob. Alice and Bob transmit a known signal (a probe) to one another in quick succession in order to derive correlated estimates of the parameter F, using the received signal by exploiting reciprocity of the wireless link. Let X and Y denote the (noisy) estimates of the parameter F obtained by Alice and Bob, respectively.

Alice and Bob generate a sequence of n correlated estimates $\hat{X}^n = (\hat{X}_1, \hat{X}_2, \ldots, \hat{X}_n)$ and $\hat{Y}^n = (\hat{Y}_1, \hat{Y}_2, \ldots, \hat{Y}_n)$, respectively, by probing the channel repeatedly in a time-division duplex (TDD) manner. Note, however, that $\hat{X}_i$ (and $\hat{Y}_i$) are no longer i.i.d. for $i = 1, \ldots, n$ since the channel may be strongly correlated between successive channel estimates.

Alice and Bob first low-pass filter their sequence of channel estimates, $\hat{X}^n$ and $\hat{Y}^n$, respectively, by subtracting a windowed moving average. This removes the dependence of the channel estimates on large-scale shadow fading changes and leaves only the small scale fading variations (see Fig. 6). The resulting sequences, X^n and Y^n, have approximately zero mean and contain excursions in positive and negative directions with respect to the mean. The subtraction of the windowed mean ensures that

the level-crossing algorithm below does not output long strings of ones or zeros and that the bias towards one type of bit is removed. The filtered sequences are then used by Alice and Bob to build a 1-bit quantizer $\psi^u(\cdot)$ quantizer based on the scalars q_+^u and q_-^u that serve as threshold levels for the quantizer

$$q_+^u = \text{mean}(U^n) + \alpha \cdot \sigma(U^n) \tag{6}$$

$$q_-^u = \text{mean}(U^n) - \alpha \cdot \sigma(U^n) \tag{7}$$

where the sequence $U^n = X^n$ for Alice and $U^n = Y^n$ for Bob. $\sigma(\cdot)$ is the standard deviation and the factor α can be selected to control the quantizer thresholds. The sequences X^n and Y^n are then fed into the following locally computed quantizer at Alice and Bob, respectively:

$$\psi^u(x) = \begin{cases} 1, & \text{if } x > q_+^u \\ 0, & \text{if } x < q_-^u \\ e, & \text{otherwise} \end{cases}$$

where e represents an undefined state. The superscript u stands for *user* and may refer to either Alice, in which case the quantizer function is $\psi^A(\cdot)$, or to Bob, for which the quantizer is $\psi^B(\cdot)$. This quantizer forms the basis for quantizing positive and negative excursions. Values between q_-^u and q_+^u are not assigned a bit.

It is assumed that the number n of channel observations is sufficiently large before using the level crossing system, and that the ith element X_i and Y_i correspond to successive probes sent by Bob and Alice respectively, for each $i = 1, \ldots, n$. The level crossing algorithm consists of the following steps:

1) Alice parses the vector X^n containing her filtered channel estimates to find instances where m or more successive estimates lie in an excursion above q_+ or below q_-. Here, m is a parameter used to denote the minimum number of channel estimates in an excursion.
2) Alice selects a random subset of the excursions found in step 1 and, for each selected excursion, she sends Bob the index of the channel estimate lying in the center of the excursion, as a list L. Therefore, if $X_i > q_+$ or $< q_-$ for some $i = i_{\text{start}}, \ldots, i_{\text{end}}$, then she sends Bob the index $i_{\text{center}} = \lfloor i_{\text{start}} + i_{\text{end}}/2 \rfloor$.
3) To make sure the L-message received is from Alice, Bob computes the fraction of indices in L, where Y^n lies in an excursion spanning $(m-1)$ or more estimates. If this fraction is less than $1/2 + \epsilon$, for some fixed parameter $0 < \epsilon < 1/2$, Bob concludes that the message was not sent by Alice, implying an adversary has injected a fake L-message.
4) If the check above passes, Bob replies to Alice with a message $\tilde{L}$ containing those indices in L at which Y^n lies in an excursion. Bob computes $K_B = \psi^B(Y_i; i \in \tilde{L})$ to obtain N bits. The first N_{au} bits are used as an authentication key to compute a message authentication code (MAC) of $\tilde{L}$. The remaining $N - N_{\text{au}}$ bits are kept as the extracted secret key. The overall message sent by Bob is $\left\{\tilde{L}, \text{MAC}\left(K_{\text{au}}, \tilde{L}\right)\right\}$. Practical implementations, for example, one could use CBC-MAC as the implementation for MAC, and use a key K_{au} of length $N_{\text{au}} = 128$ bits.
5) Upon receiving this message from Bob, Alice uses $\tilde{L}$ to form the sequence of bits $K_A = \psi^A(X_i; i \in \tilde{L})$. She uses the first N_{au} bits of K_A as the authentication key $K_{\text{au}} = K_A(1, \ldots, N_{\text{au}})$, and, using K_{au}, she verifies the MAC to confirm that the package was indeed sent by Bob. Since Eve does not know the bits in K_{au} generated by Bob, she cannot modify the $\tilde{L}$-message without failing the MAC verification at Alice.

Fig. 1 shows the system-level operation of the level crossing algorithm. We show later that provided the levels q_+, q_- and the parameter m are properly chosen, the bits generated by the two users are identical with very high probability. In this case, both Alice and Bob are able to compute identical key bits and identical authentication key bits K_{au}, thereby allowing Alice to verify that the protocol message $\tilde{L}$ did indeed come from Bob. Since Eve's observations from the channel probing do not provide her with any useful information about X^n and Y^n, the messages L and $\tilde{L}$ do not provide her any useful information either. This is because they contain time indices only, whereas the generated bits depend upon the values of the channel estimates at those indices.

B. Security Discussion for the Level-Crossing Algorithm

The secrecy of our key establishment method is based on the assumption that Alice and Bob have confidence that there is no eavesdropper Eve located near either Alice or Bob. Or equivalently, any eavesdropper is located a sufficient distance away from both Alice and Bob. In particular, the fading process associated with a wireless channel in a richly scattering environment decorrelates rapidly with distance and, for two receivers located at a distance of roughly the carrier wavelength from each other, the fading processes they each witness with respect to a transmitter will be nearly independent of each other[32]. For a Rayleigh fading channel model, if h_{ba} and h_{be} are the jointly Gaussian channels observed by Alice and Eve due to a probe transmitted by Bob, then the correlation between h_{ba} and h_{be} can be expressed as a function of the distance d between Alice and Eve, and is given by $J_0(2\pi d/\lambda)$, where $J_0(x)$ is the zeroth-order Bessel function of the first kind, d is the distance between Alice and Eve, and λ is the carrier wavelength. Hence, because of the decay of $J_0(x)$ versus the argument x, if we are given any $\epsilon > 0$, it is possible to find the minimum distance d that Eve must be from both Alice and Bob such that the mutual information $I(h_{\text{ba}}; h_{\text{be}}) \leq \epsilon$.

Further, we note that the statistical uniformity of the bit sequences that are extracted by Alice and Bob using our level-crossing algorithm is based on the statistical uniformity of positive and negative excursions in the distribution of the common stochastic channel between them. This inherently requires that the channel state representation for the fading process be symmetrically distributed about the distribution's mean. Many well-accepted fading models satisfy this property. Notably, Rayleigh and Rician fading channels[33], which result from the multiple paths in a rich scattering environment adding up at the receiver with random phases, fall into this category. Consequently, we believe that the reliance of level-crossing algorithm on the underlying distribution symmetry, suggests that the level-crossing algorithm is best suited for Rayleigh or Rician fading environments. The independence of successive extracted bits follows from the fact that the excursions used for each bit are naturally separated by a coherence time interval or more, allowing

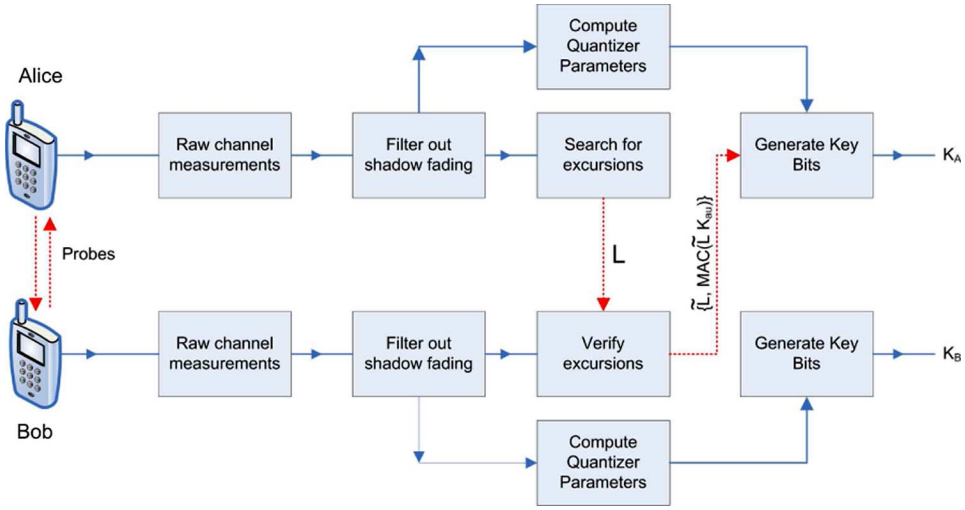

Fig. 1. System level description of the level crossing algorithm. Messages exchanged over the air are shown in dotted lines.

the channel to decorrelate in time. Finally, we note that our approach should be followed by a final privacy amplification step. Application of such a postprocessing step is straightforward and makes sure that no information is gleaned by an eavesdropper.

C. Performance Evaluation and Experimental Validation

The central quantities of interest in our protocol are the rate of generation of secret bits and the probability of error. The controls available to us are the parameters: q_+^u, q_-^u, m and the rate at which Alice and Bob probe the channel between themselves, f_s. We assume the channel is not under our control and the rate at which the channel varies can be represented by the maximum Doppler frequency f_d. The typical Doppler frequency for indoor wireless environments at the carrier frequency of 2.4 GHz is $f_d = v/\lambda \sim 2.4 \times 10^9/3 \times 10^8 = 8$ Hz, assuming a velocity v of 1 m/s. We thus expect typical Doppler frequencies in indoor environments in the 2.4-GHz range to be roughly 10 Hz. For automobile scenarios, we can expect a Doppler of ~200 Hz in the 2.4-GHz range. We assume, for the sake of discussion, that the parameter of interest F is a Gaussian random variable and the underlying stochastic process $F(t)$ is a stationary Gaussian process. A Gaussian distribution for F may be obtained, for example, by taking F to be the magnitude of the in-phase component of a Rayleigh fading process between Alice and Bob [51]. We note that the assumption of a Gaussian distribution on F is for ease of discussion and performance analysis, and our algorithm is valid in the general case where the distribution is symmetric about the mean.

The probability of error p_e is critical to our protocol. In order to achieve a robust key-mismatch probability p_k, the bit-error probability p_e must be much lower than p_k. A bit-error probability of $p_e = 10^{-7} \sim 10^{-8}$ is desirable for keys of length $N = 128$ bits. The probability of bit-error, p_e is the probability that a single bit generated by Alice and Bob is different at the two users. Consider the probability that the ith bit generated by Bob is "$K_B^i = 0$" at some index given that Alice has chosen this index, but she has generated the bit "$K_A^i = 1$." As per our Gaussian assumption on the parameter F and estimates X and Y, this probability can be expanded as shown in equation (8), at the bottom of the page, where K_m is the covariance matrix of m successive Gaussian channel estimates of Alice and K_{2m-1} is the covariance matrix of the Gaussian vector $(X_1, Y_1, X_2, \ldots, Y_{m-1}, X_m)$ formed by combining the m channel estimates of Alice and the $m-1$ estimates of Bob in chronological order. The numerator in (8) is the probability that of $2m-1$ successive channel estimates (m belonging to Alice, and $m-1$ for Bob), all m of Alice's estimates lie in an excursion above q_+ while all $m-1$ of Bob's estimates lie in an excursion below q_-. The denominator is simply the probability that all of Alice's m estimates lie in an excursion above q_+.

We compute these probabilities for various values of m and present the results of the probability of error computations in Fig. 2. The results confirm that a larger value of m will result in a lower probability of error, as a larger m makes it less likely that Alice's and Bob's estimates lie in opposite types of excursions.

$$\Pr(K_B^i = 0 | K_A^i = 1) = \frac{\Pr(K_B^i = 0, K_A^i = 1)}{\Pr(K_A^i = 1)} = \frac{\underbrace{\int_{q_+^X}^{\infty} \int_{-\infty}^{q_-^Y} \cdots \int_{q_+^X}^{\infty}}_{(2m-1) \text{ terms}} \frac{(2\pi)^{(1-2m)/2}}{|K_{2m-1}|^{1/2}} e^{-\left\{1/2 x^T K_{2m-1}^{-1} x\right\}} d^{(2m-1)}x}{\underbrace{\int_{q_+^X}^{\infty} \cdots \int_{q_+^X}^{\infty}}_{(m) \text{ terms}} \frac{(2\pi)^{-m/2}}{|K_m|^{1/2}} e^{-\left\{1/2 x^T K_m^{-1} x\right\}} d^{(m)}x} \tag{8}$$

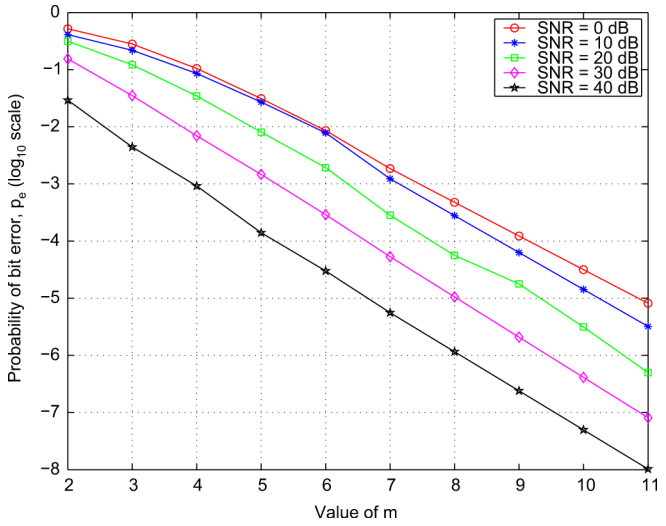

Fig. 2. Probability of bit error p_e for various values of m at different SNR levels [$\alpha = 0.8$ in (6), (7)].

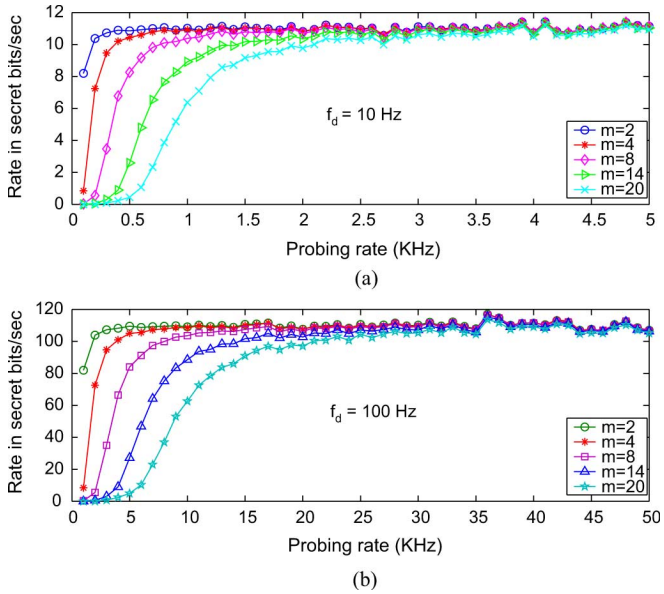

Fig. 3. Rate in secret bits per second for various values of m, against probing rate for a channel with Doppler frequency (a) $f_d = 10$ Hz and (b) $f_d = 100$ Hz [$\alpha = 0.8$ in (6), (7)].

Note that if either user's estimates do not lie in an excursion at a given index, a bit error is avoided because that index is discarded by both users.

How many secret bits per second (b/s) can we expect to derive from a fading channel using level crossings? An approximate analysis can be done using the level-crossing rate for a Rayleigh fading process, given by $\mathrm{LCR} = \sqrt{2\pi} f_d \rho e^{-\rho^2}$ [51], where f_d is the maximum Doppler frequency and ρ is the threshold level, normalized to the root mean square signal level. Setting $\rho = 1$ gives $\mathrm{LCR} \sim f_d$. This tells us that we cannot expect to obtain more secret bits per second than the order of f_d. In Fig. 3(a) and (b), we plot the rate in secret-bits/s as a function of the channel probing rate for a Rayleigh fading channel with maximum Doppler frequencies of $f_d = 10$ Hz and $f_d = 100$ Hz, respectively. As expected, the number of secret-bits the channel yields increases with the probing rate, but saturates at a value on the order of f_d.

In order for successive bits to be statistically independent, they must be separated in time by more than one coherence time interval. While the precise relationship between coherence time and Doppler frequency is only empirical, they are inversely related and it is generally agreed that the coherence time is smaller in magnitude (coherence time T_c is sometimes expressed in terms of f_d as $T_c \approx \sqrt{9/16\pi f_d^2}$) than $1/f_d$. Therefore, on average, if successive bits are separated by a time interval of $1/f_d$, then they should be statistically independent.

More precisely, the number of secret b/s is the number of secret bits per observation times the probing rate. Therefore,

$$\begin{aligned} R_k &= H(\text{bins}) \times \Pr(K_A^i = K_B^i) \times \frac{f_s}{m} \\ &= 2\frac{f_s}{m} \times \Pr(K_A^i = 1, K_B^i = 1) \\ &= 2\frac{f_s}{m} \cdot \underbrace{\int_{q_+^X}^{\infty} \cdots \int_{q_+^X}^{\infty}}_{(2m-1)\text{ terms}} \frac{(2\pi)^{1-2m/2}}{|K_{2m-1}|^{1/2}} e^{\left\{-1/2 x^T K_{2m-1}^{-1} x\right\}} d^{2m-1}x \end{aligned} \tag{9}$$

where $H(\text{bins})$ is the entropy of the random variable that determines which bin ($> q_+$ or $< q_-$) of the quantizer the observation lies in, which in our case equals 1 assuming that the two bins are equally likely.[2] The probing rate f_s is normalized by a factor of m because a single "observation" in our algorithm is a sequence of m channel estimates.

Fig. 3 confirms the intuition that the secret bit rate must fall with increasing m, since the longer duration excursions required by a larger value of m are less frequent. In Fig. 4(a), we investigate how the secret-bit rate R_k varies with the maximum Doppler frequency f_d, i.e., the channel time-variation. We found that for a fixed channel probing rate (in this case, $f_s = 4000$ probes/s), increasing f_d results in a greater rate but only up to a point, after which the secret-bit rate begins to fall. Thus, "running faster" does not necessarily help unless we can increase the probing rate f_s proportionally. Fig. 4(b) shows the expected decrease in secret-bit rate as the quantizer levels the value of α is varied to move q_+^u and q_-^u further apart. Here, α denotes the number of standard deviations from the mean at which the quantizer levels are placed. It should be noted that these rates are not the achievable rates in the sense defined in Section I.

We examined the performance of the secrecy generation system through experiments. The experiments involved three terminals, Alice, Bob, and Eve, each equipped with an 802.11a development board.

In the experiments, Alice was configured to be an access point (AP), and Bob was configured to be a station (STA). Bob sends Probe Request messages to Alice, who replies with Probe Response messages as quickly as possible. Both terminals used the long preamble segment [2] of their received Probe Request or Probe Response messages to compute 64-point CIRs. The tallest peak in each CIR (the dominant multipath) was used as

[2]The levels q_+ and q_- are chosen so as to maintain equal probabilities for the two bins.

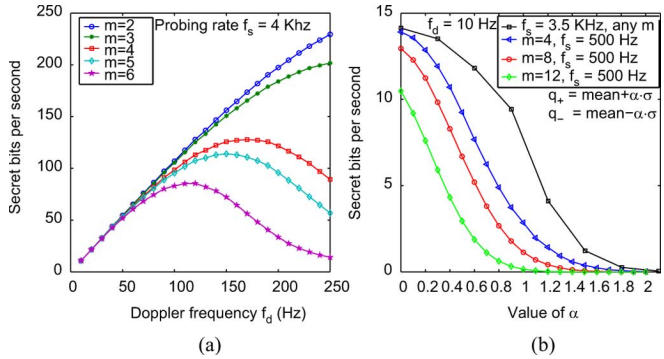

Fig. 4. (a) Secret-bit rate for varying Doppler f_d and fixed f_s for various values of m. (b) Rate as a function of function of quantizer levels q_+ and q_- parametrized by α.

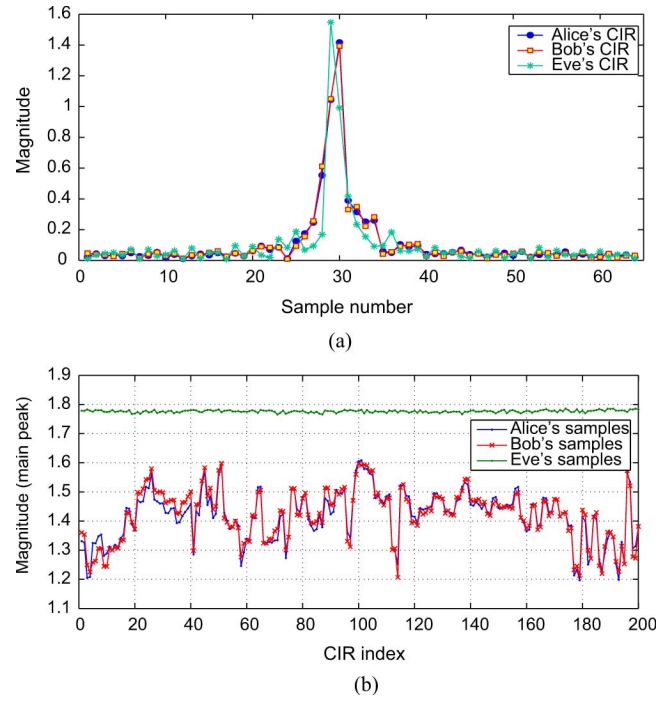

Fig. 5. (a) Alice, Bob, and Eve's 64-point CIRs from a common pair of Probe Request, Probe Response messages. (b) Traces of the magnitudes resulting from 200 Alice, Bob, and Eve's CIRs.

the channel parameter of interest, i.e., the X and Y sample inputs to the secret key generation system. To access such peak data, field-programmable gate array (FPGA)-based customized logic was added to the 802.11 development platform. Eve was configured to capture the Probe Response messages sent from Alice in the experiments.

Two experiments were conducted. In the first experiment, Alice and Eve were placed in a laboratory. In a second experiment, Alice and Eve remained in the same positions while Bob circled the cubicle area of the office.

Fig. 5(a) shows an example of Alice's, Bob's, and Eve's 64-point CIRs obtained through a single common pair of Probe Request and Probe Response messages. It is seen from the figure that Alice's and Bob's CIRs look similar, while they both look different from Eve's CIR. We show the traces for Alice and Bob resulting from 200 consecutive CIRs in Fig. 5(b). The similarity of Alice's and Bob's samples, as well as their difference from Eve's samples, are evident from the figure.

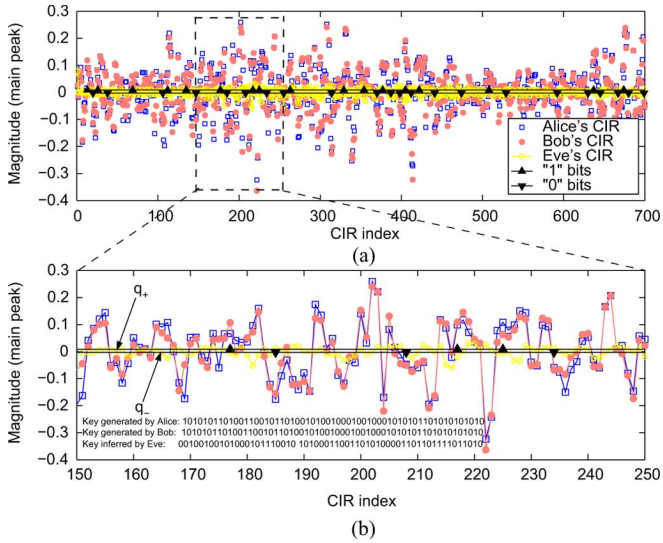

Fig. 6. (a) Traces of Alice and Bob after subtracting average signal power. Using $m = 5$, $N = 59$ bits were generated in 110 s ($R_k = 0.54$ s-b/s) while $m = 4$ gives $N = 125$ bits ($R_k = 1.13$ s-b/s.) with no errors in each case. (b) A magnified portion of (a).

While our experiments ran for ∼22 min, in the interest of space and clarity we show only 700 CIRs collected over a duration of ∼77 s. Each user locally computes q_+ and q_- as in (6) and (7). We chose $\alpha = 1/8$ for our experiments.

Fig. 6 shows the traces collected by Alice and Bob after removal of slow shadow fading components using a simple local windowed mean. This is to prevent long strings of 1s and 0s, and to prevent the predictable component of the average signal power from affecting our key generation process. Using the small scale fading traces, our algorithm generates $N = 125$ bits in 110 s ($m = 4$), yielding a key rate of about 1.13 b/s. Fig. 6 shows the bits that Eve would generate if she carried through with the key-generation procedure. The results from our second experiment with a moving Bob are very similar to the ones shown for the first experiment, producing 1.17 b/s with $m = 4$ and $\alpha = 1/8$. Note that while Figs. 3 and 4 depict the secret bit rate that can be achieved for the specified values of Doppler frequency, our experimental setup does not allow us to measureably control the precise Doppler frequency and the secret bits rates we report from our experiments correspond only the indoor channel described.

In order to verify the assumption that Eve does not gain any useful information by passive observation of the probes transmitted by Alice and Bob, we empirically computed the mutual information using the method in [56] between the signals received at the legitimate users and compare this with that between the signals received by Eve and a legitimate user. The results of this computation, summarized in Table I, serve as an upper bound to confirm that Eve does not gather any significant information about the signals received at Alice and Bob. Although this information leakage is minimal relative to the mutual information shared between Alice and Bob, privacy amplification must be employed as a postprocessing step to be sure that Eve has learned no information about the key established between Alice and Bob. Finally, we note that with suitable values of the parameters chosen for the level crossing algorithm, the bits

TABLE I
MUTUAL INFORMATION (M.I.) $I(u_1; u_2)$ BETWEEN THE MEASUREMENTS OF USERS u_1 AND u_2

Value of m used	4
Choice of q_+, q_-	mean $\pm 0.125\sigma$
Duration of experiments	1326 sec ($\sim$ 22 min.)
Inter-probe duration	110 msec.
Static case:	
I(Alice; Bob)	$3.294\ bits$
I(Bob; Eve)	$0.047\ bits$
Mobile case:	
I(Alice; Bob)	$1.218\ bits$
I(Bob; Eve)	$0.000\ bits$

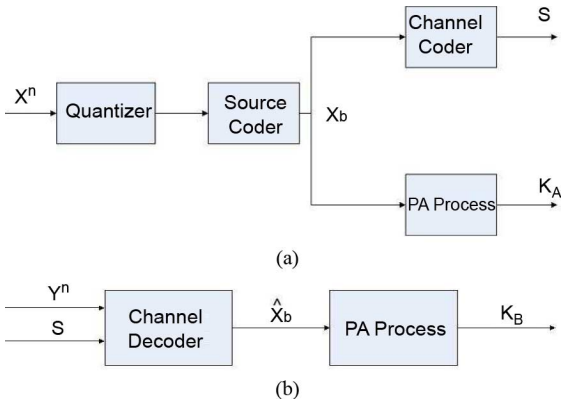

Fig. 7. Block diagrams of the basic system.

extracted by Alice and Bob are statistically random and have high-entropy per bit. This has been tested for and previously reported in [38] using a suite of statistical randomness tests provided by NIST [3].

III. QUANTIZATION-BASED SECRET KEY GENERATION FOR WIRELESS CHANNELS

We now present a more powerful and general approach than the level-crossing approach discussed in Section II for obtaining secret keys from the underlying fading phenomena associated with a richly scattering wireless environment. Whereas the level-crossing algorithm was best suited for extracting keys from channel states whose distributions are inherently symmetric, our second approach is applicable to more general channel state distributions. Further, this second approach is capable of generating significantly more than a single bit per independent channel realization, especially when the channel estimation SNRs are high.

To accomplish this, we propose a new approach for the quantization of sources whose statistics are not known, but are believed to be similar in the sense of having "high SNR"—a notion we shall define more precisely below. Our quantization approach is motivated by considering a simpler setting of a Gaussian source model and addressing certain deficiencies which can be observed in that model. This problem has been addressed by [62] using a simple "BICM-like" approach [13] to the problem. A more general treatment which introduces multilevel coding can be found in [13] and also [12]; however, for our purposes, the simple "BICM-like" approach of [62] and [13] is sufficient. To motivate our approach to "universal" quantization, we need to take this solution and improve on it—the process which we describe next.

A. Over-Quantized Gaussian Key Generation System

We begin our discussion of the over-quantized Gaussian Key Generation System by reviewing the simple approach to the problem described in [62]. A block diagram of a basic secret key generation system is shown in Fig. 7. Alice's secrecy processing consists of four blocks: Quantizer, Source Coder, Channel Coder, and the Privacy Amplification (PA) process. The Quantizer quantizes Alice's Gaussian samples X^n. The Source Coder converts the quantized samples to a bit string $\mathbf{X}_b$. The Channel Coder computes the syndrome $\mathbf{S}$ of the bit string $\mathbf{X}_b$. A rate $1/2$ LDPC code is used in [62]. This syndrome is sent to Bob for his decoding of $\mathbf{X}_b$. As discussed in Section I, the transmission of the syndrome is assumed to take place through an error-free public channel; in practice, this can be accomplished through the wireless channel with the use of standard reliability techniques (e.g., CRC error control and ARQ). Finally, privacy amplification is implemented in the PA block.

Fig. 8(a) presents the results obtained by using various algorithm options discussed in [62]. We observe from this figure that at high SNR (>15 dB), the secret key rates resulting from Gray coding are within 1.1 bits of the secret key capacity (5). However, the gap between the achieved secret key rates and the secret key capacity is larger at low SNR. In this subsection, we demonstrate how the basic system can be improved such that the gap at low SNR is reduced. We restrict ourselves to Gray coding, as this is clearly the better source coding approach.

We start with the observation that the quantization performed by Alice involves some information loss. To compensate for this, Alice could quantize her samples at a higher level than the one apparently required for the basic secret key generation purpose. Suppose that quantization to v bits is required by the baseline secrecy generation scheme. Alice then quantizes to $v+m$ bits using Gray coding as a source coder. We refer to the v most significant bits as the *regularly quantized bits* and the m least significant bits as the *over-quantized bits*. The over-quantized bits $\mathbf{B}$ are sent directly to Bob through the error-free public channel.

The Channel Decoder (at Bob) uses the syndrome $\mathbf{S}$ of the regularly quantized bits $\mathbf{X}_b$, the over-quantized bits $\mathbf{B}$, and Bob's Gaussian samples Y^n to decode $\mathbf{X}_b$. Again, it applies the modified belief-propagation algorithm (cf. [35]), which requires the per-bit log likelihood ratio (LLR). The LLR calculation is based on both Y^n and $\mathbf{B}$.

Suppose one of Alice's Gaussian samples X is quantized and Gray coded to bits $(X_{b,1}, \ldots, X_{b,v+m})$. With Bob's corresponding Gaussian sample Y and Alice's over-quantized bits $(X_{b,v+1}, \ldots, X_{b,v+m}) = (a_{v+1}, \ldots, a_{v+m})$, the probability of $X_{b,i}$, $1 \le i \le v$, being 0 is derived below

$$\Pr\left(\begin{array}{c} X_{b,i}=0 | Y=y, X_{b,v+1}=a_{v+1}, \ldots \\ \ldots, X_{b,v+m}=a_{v+m} \end{array}\right) = \frac{\Pr\left(\begin{array}{c} X_{b,i}=0, X_{b,v+1}=a_{v+1}, \ldots \\ \ldots, X_{b,v_m}=a_{v+m} | Y=y \end{array}\right)}{\Pr(X_{b,v+1}=a_{v+1}, \ldots, X_{b,v_m}=a_{v+m} | Y=y)} \tag{10}$$

$$= \frac{\left(\begin{array}{c} \sum_{j=1}^{2^{v+m}} \Pr(\bar{q}_{j-1} \le X < \bar{q}_j | Y=y) \cdot \\ \cdot \mathbf{1}_{G^i_{v+m}(j-1)=0} \cdot \mathbf{1}_{G^{v+1}_{v+m}(j-1)=a_{v+1}} \\ \cdots \mathbf{1}_{G^{v+m}_{v+m}(j-1)=a_{v+m}} \end{array} \right)}{\left(\begin{array}{c} \sum_{j=1}^{2^{v+m}} \Pr(\bar{q}_{j-1} \le X < \bar{q}_j | Y=y) \times \\ \mathbf{1}_{G^{v+1}_{v+m}(j-1)=a_{v+1}} \cdots \times \mathbf{1}_{G^{v+m}_{v+m}(j-1)=a_{v+m}} \end{array} \right)} \quad (11)$$

where $\mathbf{1}$ is an indicator function and the function $G^i_k(j)$, $1 \le i \le k$, $0 \le j \le 2^k - 1$, denotes the ith bit of the k-bit Gray codeword representing the integer j. The quantization boundaries $\bar{q}_0 < \cdots < \bar{q}_{2^{v+m}}$ depend on the quantization scheme used. For instance, the quantization boundaries of the *equiprobable quantizer* satisfy

$$\int_{\bar{q}_{j-1}}^{\bar{q}_j} \frac{1}{\sqrt{2\pi N}} e^{-x^2/2N} dx = \frac{1}{2^{v+m}}, \quad j = 1, \ldots, 2^{v+m}. \quad (12)$$

Now,

$$\begin{aligned} &\Pr(\bar{q}_{j-1} \le X < \bar{q}_j | Y=y) \\ &= \Pr(\bar{q}_{j-1} \le \frac{P}{P+N} Y + Z_0 < \bar{q}_j | Y=y) \\ &= \Pr(\bar{q}_{j-1} - \frac{P}{P+N} y \le Z_0 < \bar{q}_j - \frac{P}{P+N} y) \\ &= Q\left(\frac{\bar{q}_{j-1} - \frac{P}{P+N} y}{\sqrt{\frac{2PN+N^2}{P+N}}} \right) - Q\left(\frac{\bar{q}_j - \frac{P}{P+N} y}{\sqrt{\frac{2PN+N^2}{P+N}}} \right) \\ &= g(j-1, y) - g(j, y) \end{aligned} \quad (13)$$

where the function $g(k, y)$, $0 \le k \le 2^{v+m}$, is defined as

$$g(k, y) = Q\left(\frac{\bar{q}_k - \frac{P}{P+N} y}{\sqrt{\frac{(2PN+N^2)}{(P+N)}}} \right) \quad (14)$$

and Q is the usual Gaussian tail function [50]. Hence, the probability of (11) is given by

$$\frac{\left(\begin{array}{c} \sum_{j=1}^{2^{v+m}} [g(j-1, y) - g(j, y)] \times \mathbf{1}_{G^i_{v+m}(j-1)=0} \\ \times \mathbf{1}_{G^{v+1}_{v+m}(j-1)=a_{v+1}} \cdots \mathbf{1}_{G^{v+m}_{v+m}(j-1)=a_{v+m}} \end{array} \right)}{\left(\begin{array}{c} \sum_{j=1}^{2^{v+m}} [g(j-1, y) - g(j, y)] \times \mathbf{1}_{G^{v+1}_{v+m}(j-1)=a_{v+1}} \\ \cdots \times \mathbf{1}_{G^{v+m}_{v+m}(j-1)=a_{v+m}} \end{array} \right)}. \quad (15)$$

It should be noted that when equiprobable quantization is used, the over-quantized bits $\mathbf{B}$ and the regularly quantized bits $\mathbf{X}_b$ are independent as shown below. Suppose a sample X is equiprobably quantized and source coded to t bits $(X_{b,1}, \ldots, X_{b,t})$. For an arbitrary bit sequence $(a_1, \ldots, a_t)$ and a set $\mathcal{S} \subseteq \mathcal{T} = \{1, \ldots, t\}$, we have

$$\begin{aligned} &\Pr\left(\{X_{b,i} = a_i : i \in \mathcal{S}\} | \{X_{b,i} = a_i : i \in \mathcal{T} \setminus \mathcal{S}\}\right) \\ &= \frac{\Pr\left(\{X_{b,i} = a_i : i \in \mathcal{T}\}\right)}{\Pr\left(\{X_{b,i} = a_i : i \in \mathcal{T} \setminus \mathcal{S}\}\right)} \\ &= \frac{2^{-t}}{2^{-(t-|\mathcal{S}|)}} = 2^{-|\mathcal{S}|} = \Pr\left(\{X_{b,i} = a_i : i \in \mathcal{S}\}\right) \end{aligned} \quad (16)$$

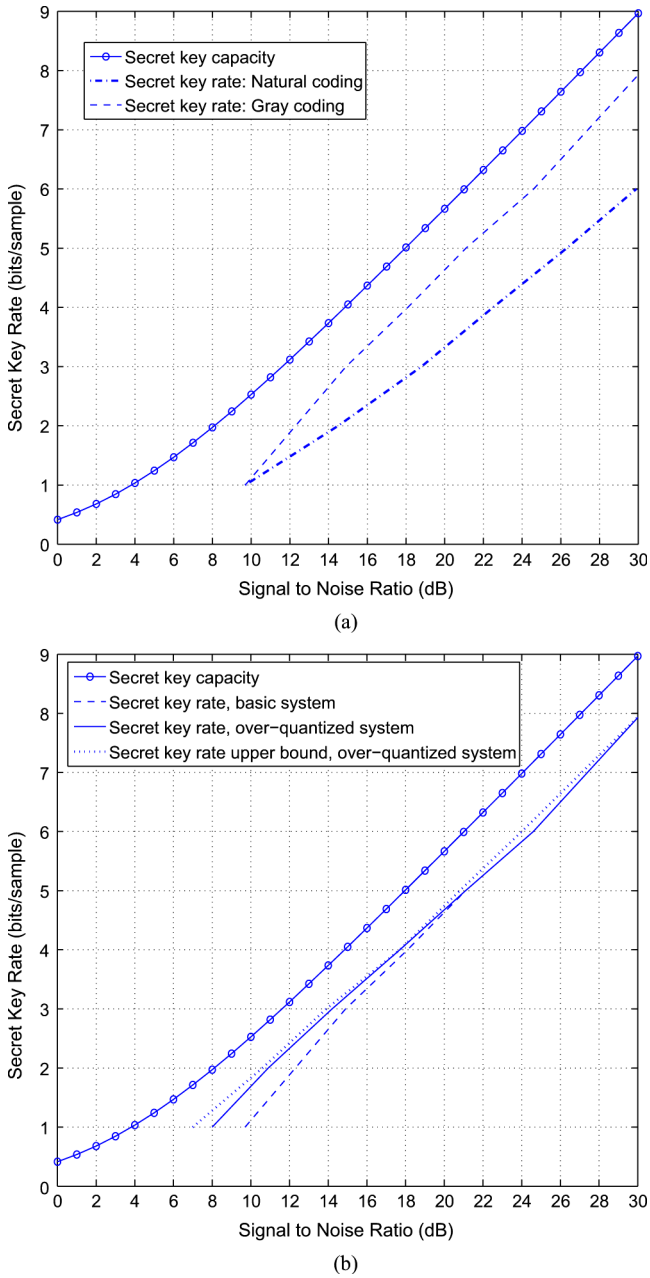

Fig. 8. (a) Secret key rates achieved by the basic system. (b) Secret key rates achieved by the improved system.

which implies the amount of secrecy information remaining in $\mathbf{X}_b$ after the public transmission is at least $|\mathbf{X}_b| - |\mathbf{S}|$ bits.[3] Note that this conclusion does not hold for other quantization approaches (e.g., minimum mean square error (MMSE) quantization) and, therefore, equiprobable quantization should be used if over-quantization is applied.

On the other hand, it is implied by (15) that the over-quantized bits $\mathbf{B}$ and the regularly quantized bits $\mathbf{X}_b$ are dependent given Bob's samples Y^n. Hence, $I(\mathbf{X}_b; \mathbf{B} | Y^n) > 0$. It follows from the Slepian–Wolf theorem (cf. [21]) that with the

[3]Relying on hash functions for privacy amplification requires the use of Rényi entropy. However, we can use [11, Th. 3] to translate between Rényi and Shannon entropies.

availability of the over-quantized bits $\mathbf{B}$, the number of syndrome bits $|\mathbf{S}|$ required by Bob to successfully decode $\mathbf{X}_b$ is approximately $H(\mathbf{X}_b|Y^n,\mathbf{B})$, which is less than $H(\mathbf{X}_b|Y^n)$, the number of syndrome bits transmitted in the basic system. In other words, the secret key rate achieved by the over-quantized system is approximated by $1/nI(\mathbf{X}_b;Y^n,\mathbf{B})$, which is larger than $1/nI(\mathbf{X}_b;Y^n)$, the secret key rate achieved by the basic system. Here, we adapt the code rate in the Channel Coder for the over-quantized system to achieve a higher secret key rate than the basic system. This could be implemented either by lower rate channel codes or by rate-matching algorithms.

To obtain an upper limit on the performance improvement that over-quantization may provide us, we can imagine sending the entire (real-valued) quantization error as a side information. There are a number of issues with this approach. Clearly, distortion-free transmission of real-valued quantities is not practically feasible. However, as we are looking for a bound, we can ignore this. More importantly, the transmission of raw quantization errors may reveal information about $\mathbf{X}_b$. For example, to equiprobably quantize a zero mean, unit variance Gaussian random variable with 1 bit per sample, the quantization intervals are $(-\infty,0]$ and $(0,\infty)$, with respective representative value -0.6745 and 0.6745. Suppose a sample X is of value 2, then its quantization error is $2-0.6745=1.3255$. This implies that X must be in the interval $(0,\infty)$, since otherwise, the quantization error does not exceed 0.6745. Thereby, it is necessary to process the raw quantization errors such that the processed quantization errors do not contain any information about $\mathbf{X}_b$. For this purpose, it is desirable to transform quantization errors to uniform distribution. To do so, we first process an input sample X with the cumulative distribution function (CDF) of its distribution and then quantize. The transformed quantization error is then given by $E=\phi(X)-\phi(q(X))$, where $\phi(x)$ is the CDF for X and $q(X)$ is the representative value of the interval to which X belongs. The quantization errors $E^n=(E_1,\ldots,E_n)$, which are then uniformly distributed on $\left[-2^{-(v+1)},2^{-(v+1)}\right]$, are sent to Bob through the error-free public channel.

The rest of the process (encoding/decoding and PA) proceeds as before. However, the LLR computation must be modified to use probability density functions, rather than probabilities

$$\ln\frac{\Pr(X_{b,i}=0|Y=y,E=e)}{\Pr(X_{b,i}=1|Y=y,E=e)}=\sum_{j=1}^{2^v}(-1)^{\mathbf{1}_{G_v^i(j-1)=0}}\cdot h(e,j,y) \quad (17)$$

where the function $G_k^i(j)$ is defined in (11) and the function $h(e,j,y)$ is defined as

$$h(e,j,y)=\frac{P+N}{2(2PN+N^2)}\left(\phi^{-1}\left(e+\frac{j-0.5}{2^v}\right)-\frac{P}{P+N}y\right)^2$$

for $-2^{-(v+1)}\le e\le 2^{-(v+1)}$, $1\le j\le 2^v$, with the function ϕ being the CDF for X. The derivation of (17) is similar to that of (15), which is omitted here.

Fig. 8(b) shows simulation results for 2-bit over-quantization and the upper bound. We note, as expected, that the overall gap to capacity has been reduced to about 1.1 dB at the low-SNR.

B. Universal Secret Key Generation System

In the previous subsection, we discussed secret key generation for a jointly Gaussian model. The random variables X and Y in the model are jointly Gaussian distributed and the distribution parameter SNR is known at both terminals. However, in many practical conditions, the correlated random variables at the two terminals may not be subject to a jointly Gaussian distribution, and the distribution parameters are usually unknown or estimated inaccurately.

We address this problem by describing a method for LLR generation and subsequent secrecy generation that makes very few assumptions on the underlying distribution. As we shall see this method is largely based on the over-quantization idea we introduced above.

1) System Description: Compared to the basic system (Fig. 7) developed for the Gaussian model, the universal system includes two additional Data Converter blocks (one at Alice; the other at Bob), and modified Quantizer and Channel Decoder blocks. The inputs to Alice's Data Converter blocks are X^n and the outputs of Alice's Data Converter block are sent to the modified Quantizer block. The inputs to Bob's Data Converter blocks are Y^n and the outputs of Bob's Data Converter block are sent to the modified Channel Decoder block.

The purpose of the Data Converter is to convert the input samples X^n, Y^n to uniformly distributed samples U^n, V^n, where $U_i,V_i\in[0,1)$. The conversion is based on the empirical distribution of input samples. Given the ith sample X_i of input samples X^n, denote by $K_n(X_i)$ the number of samples in X^n which are strictly less than X_i plus the number of samples in X^n which are equal to X_i but their indices are less than i. The output of the Data conversion block corresponding to X_i is given by $U_i=K_n(X_i)/n$.

To justify the use of this approach, we show that U^n asymptotically tends to an i.i.d. sequence, each uniformly distributed between 0 and 1. Thus, while for any finite block length the sequence U^n is not comprised of independent variables, it is asymtotically i.i.d. uniform. Consider an i.i.d. sequence $X^n=(X_1,\ldots,X_n)$. Denote by ϕ the actual CDF of X_i. Let $W_i=\phi(X_i)$, $i=1,\ldots,n$. Then $W_1,\ldots,W_n$ is an i.i.d. sequence, each uniformly distributed between 0 and 1. Hence, it suffices to show that the sequence U^n converges to the sequence W^n.

Convergence of the empirical distribution to the true distribution is a well-established fact in probability known as the Glivenko–Cantelli Theorem [54]. However, we need a stronger statement which gives the rate of such convergence. This is known as the Dvoretzky–Kiefer–Wolfowitz Theorem [26] and is stated in the following lemma.

Lemma 1: Let $X_1,\ldots,X_n$ be real-valued, i.i.d. random variables with distribution function F [26]. Let F_n denote the associate empirical distribution function defined by

$$F_n(x)=\frac{1}{n}\sum_{i=1}^{n}1_{(-\infty,x]}(X_i),\quad x\in\mathcal{R}.$$

For any $\varepsilon>0$,

$$\Pr\left(\sup_{x\in\mathcal{R}}|F_n(x)-F(x)|>\varepsilon\right)\le 2e^{-2n\varepsilon^2}. \quad (18)$$

□

We will also need the notion of a L^p convergence of random sequences [18]. The L^p-norm of a sequence X^n,

$p \geq 1$, is defined by $||X^n||_p = (\sum_i^n |X_i|^p)^{1/p}$. A sequence X^n is said to converge in L^p to Y^n, $0 \leq p \leq \infty$, if $\lim_{n\rightarrow\infty} \mathcal{E}\left[||X^n - Y^n||_p\right] = 0$. We then have the following lemma [18, Th. 4.1.4].

Lemma 2: If a sequence X^n converges to another sequence Y^n in $L^p, 0 \leq p \leq \infty$, then X^n converges to Y^n in probability. □

We can now show the desired statement.

Theorem 1: The sequence U^n converges to the sequence W^n in probability.

Proof: According to Lemma 2, we only need to show $\lim_{n\rightarrow\infty} \mathcal{E}[||U^n - W^n||_4] = 0$. Here,

$$\mathcal{E}[||U^n - W^n||_4] \tag{19}$$

$$= \mathcal{E}\left[\left(\sum_{i=1}^n |U_i - W_i|^4\right)^{1/4}\right] \leq \left(\mathcal{E}\left[\sum_i^n |U_i - W_i|^4\right]\right)^{1/4}$$

$$= \left(\sum_i^n \mathcal{E}[|U_i - W_i|^4]\right)^{1/4}. \tag{20}$$

For any $i = 1, \ldots, n$, we have

$$\mathcal{E}[|U_i - W_i|^4] = \int_0^1 \Pr(|U_i - W_i|^4 > u)du \tag{21}$$

$$= \int_0^1 \Pr(|U_i - W_i| > u^{1/4})du$$

$$\leq \int_0^1 2e^{-2nu^{1/2}}du \tag{22}$$

where (22) follows from (18). By letting $t = \sqrt{u}$ and integrating by parts, we show

$$\mathcal{E}\left[|U_i - W_i|^4\right] \leq 4\int_0^1 te^{-2nt}dt$$

$$= \frac{1}{n^2} - \frac{e^{-2n}}{n}\left(2 + \frac{1}{n}\right) \leq \frac{1}{n^2}. \tag{23}$$

Combining (20) and (23), we obtain

$$\mathcal{E}\left[||U^n - W^n||_4\right] \leq \left(\sum_{i=1}^n \frac{1}{n^2}\right)^{1/4} = n^{-1/4}$$

which tends to 0 as $n \rightarrow \infty$. This completes the proof of the theorem. □

The conversion from X^n (or Y^n) to U^n (or V^n) can be accomplished using a procedure that requires no computation and relies only on a sorting algorithm. It has the important side benefit that the output is inherently fixed-point, which is critical in the implementation of most modern communication systems. Let A be the number of bits to be used for each output sample U_i. This implies that U_i is of value $j/2^A$, $0 \leq j \leq 2^A - 1$. Denote by $C(j)$, $0 \leq j \leq 2^A$, the number of output samples of value $j - 1/2^A$. The values of $C(j)$ are determined by the following pseudocode:

$C(0) \leftarrow 0;$

for $j = 1$ to 2^A;

$C(j) \leftarrow \lfloor j \cdot n/2^A \rfloor - \sum_{k=0}^{j-1} C(k)$

end

where $\lfloor x \rfloor$ is the largest integer less than x. For an input sample X_i with

$$\sum_{j=0}^{k} C(j) \leq K_n(X_i) < \sum_{j=0}^{k+1} C(j)$$

the corresponding output U_i is given by $k/2^A$.

To efficiently implement this process, we follow a three step process: 1) sort the input samples X^n in ascending order; 2) convert sorted samples to values $j/2^A, 0 \leq j \leq 2^A - 1$; 3) associate each input sample with its converted value.

Suppose input samples X^n are sorted to $\tilde{X}^n$, where $\tilde{X}_1 \leq \cdots \leq \tilde{X}_n$. The index mapping between X^n and $\tilde{X}^n$ is also recorded for the use in the association step.

The values of $\tilde{X}^n$ are converted to $\tilde{U}^n$ using the algorithm defined via the pseudocode below. The algorithm distributes n items among A bins in a "uniform" way even when A does not divide n. The process is based on the rate-matching algorithms used in modern cellular systems, e.g., [1], and is also similar to line-drawing algorithms in computer graphics.

$c \leftarrow 0; \quad k \leftarrow 0; \quad j \leftarrow 1;$

while $(j \leq n)$

$c \leftarrow c + n/2^A;$

while $(c \geq 1)$

$\tilde{U}_j \leftarrow k/2^A; \quad j \leftarrow j + 1; \quad c \leftarrow c - 1;$

end

$k \leftarrow k + 1;$

end

The last step rearranges $\tilde{U}^n$ to outputs U^n such that the ith output sample U_i is associated with the ith input sample X_i.

Although the above procedures use 2^A as the total number of possible values to be assigned, in general, any integer M may be substituted for 2^A, in which case the unit interval $[0, 1)$ is partitioned into M equal subintervals, with the data distributed among them as uniformly as possible.

To equiprobably quantize uniformly distributed samples U^n with v bits per sample, the Quantizer determines the quantization boundaries as

$$q_i = \frac{i}{2^v}, \quad 0 \leq i \leq 2^v.$$

For a simple decoding process, the quantization error E is defined as the difference between U and the lower bound of the interval to which U belongs. Hence, the quantization error E is uniformly distributed between 0 and $1/2^v$. The transmission of such quantization errors $E^n = (E_1, \ldots, E_n)$ over the public channel does not reveal any information about $\mathbf{X}_b$.

For the case of fixed point inputs U^n, if the number of bits per sample v in the Quantizer block used for generating $\mathbf{X}_b$ is less than the number A of bits used for U, then the Quantizer block obtains the quantized value and the quantization error for U simply from the first v bits and the last $A - v$ bits out of the A bits for U, respectively.

Bob's Data Converter performs the same operations as Alice's. The Channel Decoder calculates the per-bit LLR based on the outputs of Bob's Data Converter block V^n and the received quantization errors E^n. Unlike the jointly Gaussian model, the joint distribution of X and Y in this case is unknown and the accurate LLR is generally incomputable.

We provide an extremely simple but effective way of computing the LLR. Heuristically, the LLR is related to the distances from V to the possible U values that cause $X_{b,i} = 1$ and that cause $X_{b,i} = 0$. Suppose a uniform sample U is quantized and Gray coded to bits $(X_{b,1}, \ldots, X_{b,v})$ and the quantization error of U is E. The heuristic LLR L_i for $X_{b,i}, 1 \leq i \leq v$, is derived through the following pseudocode:

for $i = 1$ to v

$L_i \leftarrow 2E - 2V + 1 - 2^{-(v-i+1)}$;

if $V < 0.5$

$V \leftarrow 2V$;

$E \leftarrow 2E$;

else

$V \leftarrow 1 - 2V$;

$E \leftarrow 2^{-(v-i)} - 2E$;

end

end

Consider an example of $E = 0.2$ and $v = 1$. This quantization error indicates the two possible values of U are 0.2 and 0.7, which corresponds to $X_{b,1} = 0$ and $X_{b,1} = 1$, respectively. If $V = 0.3$, which is closer to the possible U value 0.2, then it is more likely that $X_{b,1}$ is equal to "0" and the LLR for $X_{b,1}$ should be positive. It follows from the pseudocode above that $L_1 = 0.3$. If $V = 0.5$, which is closer to the possible U value 0.7, then it is more likely that $X_{b,1}$ is equal to "1" and the LLR for $X_{b,1}$ should be negative. It follows from the codes above that $L_1 = -0.1$.

As the L_i obtained in the codes above is generally within the range of $[-1, 1]$, the likelihood probability of each bit is restricted to the range of $[0.27, 0.73]$. Hence, it is desirable to rescale L_i to the operational range of the modified belief-propagation algorithm by multiplying with a constant.

2) Simulation and Experimental Validation: We examine the performance of the proposed approach in a simulation environment with the jointly Gaussian channel model and with real channels.

In order to examine the performance of the universal system, we apply it to the jointly Gaussian model, though noting that the parameters P, N of the jointly Gaussian model are not utilized in the universal system. The secret key rates achieved by the universal system are shown in Fig. 9. For comparison, the secret key capacity and the upper bound for the secret key rates achieved by the over-quantized system are also plotted in the same figure. It is seen from the figure that the universal system performs well at low SNR, but deviates at high SNR. The deviation may be due to the trade-off made between the regularly quantized bits and the over-quantized bits. A different trade-off can push the deviation point higher at the expense of more communication (of over-quantized bits) and higher LDPC decoding complexity.

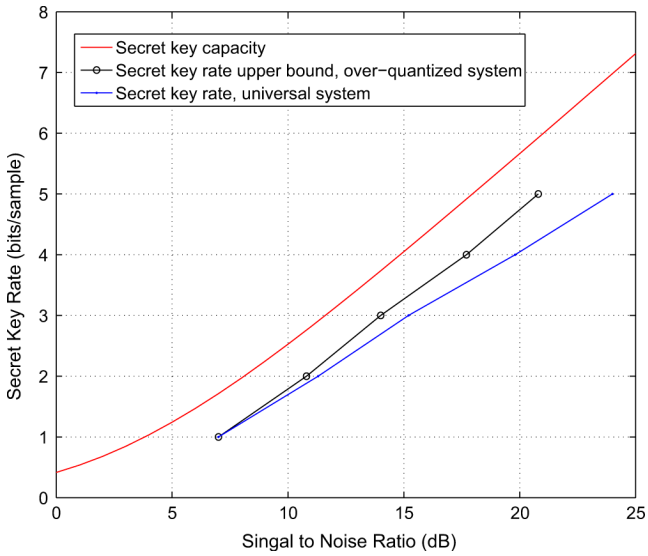

Fig. 9. Secret key rates achieved by the universal system.

We experimentally validated the feasibility of the above universal approach using 802.11 setup described earlier. In the two experiments stated in Section II, Bob sent Probe Request messages at an average rate of 110 ms.[4] Typically, Bob received the corresponding Probe Response message from Alice within 7 ms after a Probe Request message was sent. It is reported in Table I that in the first experiment, the mutual information between Alice's and Bob's samples is about 3.294 bits/sample, while the mutual information between Bob's and Eve's samples is about 0.047 bit/sample. In the second experiment, the mutual information between Alice's and Bob's samples is about 1.218 bits/sample, while the mutual information between Bob's and Eve's samples is 0 within the accuracy of the measurement. This suggests that the respective secret key capacities[5] of the first and the second experimental environments are about 30 ($\approx$ (3.294–0.047) bits/sample $\div$0.11 s/sample) b/s and 11 b/s, provided that the channel coherence time is around 110 ms.

Next, we check the secret key rates achieved by the universal system. For the purpose of generating keys in a short time duration, we apply an LDPC code with a shorter block length in the universal system. The code is a (3,6) regular LDPC code of codeword length 400 bits. The quantization parameter v is chosen as 3 for the first experiment and 2 for the second experiment. This implies that for each run of the system, a block of 134 ($\approx 400/3$) first experimental samples or 200-s experimental samples is sent to the universal system.

Our experimental results show that in both cases, Bob is able to successfully decode Alice's bit sequence $\mathbf{X}_b$ of 400 bits. With the reduction of 200 bits, revealed as syndrome bits over the public channel, both terminals remain with 200 secret bits. In

[4]Here, we assume the channel coherence time is less than or equal to 110 ms. Hence, two consecutive CIRs at either terminal are assumed to be mutually independent.

[5]We abuse the notion of capacity a bit as this "capacity" assumes i.i.d. channel samples.

order to remove the correlation between the 200 secret bits and Eve's samples in the first experiment, which shows nonzero mutual information, we may need to squash out an additional $7(\approx\ 0.047 * 134)$ bits from the 200 secret bits, resulting in 193 secret bits. Considering the period of collecting these 134 or 200 samples, we conclude that the secret key rate achieved by the universal system is about 13 b/s for the first experiment and 9 b/s for the second experiment.

IV. Conclusion

The wireless medium creates the unique opportunity to exploit location-specific and time-varying information present in the channel response to generate information-theoretically secret bits, which may be used as cryptographic keys in other security services. This ability follows from the property that in a multipath scattering environment, the CIR decorrelates in space over a distance that is of the order of the wavelength, and that it also decorrelates in time, providing a resource for fresh randomness. In this paper, we have studied secret key extraction, under the assumption of a Rayleigh or Rician fading channel, and under a more general setting where we do not make any assumption on the channel distribution. We have developed two techniques for producing identical secret bits at either end of a wireless communication link and have evaluated each technique using channel measurements made using a modified 802.11 system. The first technique is based on the observation of correlated excursions in the measurements at the two users while the second technique employs error-correction codes. The former method trades off the performance of the latter with a lower complexity and does not require knowledge of the channel coherence time. Since the time-varying nature of the channel acts as the source of randomness, it limits the number of random bits that can be extracted from the channel for the purpose of a cryptographic key. The second method applies to more general distributions for the shared channel information between a transmitter and receiver, and is able to achieve improved secret key rates at the tradeoff of increased complexity. Our evaluations indicate that typical indoor wireless channels allow us to extract secret bits at a practically useable rate, with minimal information about these secret bits being learned by an eavesdropper. Lastly, we note that as a final step, the legitimate participants in the protocol should employ PA to be assured that the eavesdropper cannot infer the bits being generated.

References

[1] *Technical Specification Group Radio Access Network; Multiplexing and Channel Coding (FDD) (Release 6), v. 6.5.0*, 3GPP TS 25.212, Jun. 2005 [Online]. Available: http://www.3GPP.org

[2] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High-Speed Physical Layer in the 5 GHz Band*, IEEE Standard 802.11a, Part 11, 1999 [Online]. Available: http://standards.ieee.org

[3] A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications National Institute of Standards and Technology, 2001.

[4] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography, Part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[5] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *IEEE Trans. Antennas Propag.*, vol. 53, no. 11, pp. 3776–3784, Nov. 2005.

[6] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *Proc. ACM Comput. Commun. Security*, Oct. 2007, pp. 401–410.

[7] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *J. Cryptology*, vol. 5, pp. 3–28, 1992.

[8] C. H. Bennett, G. Brassard, and J. M. Robert, "How to reduce your enemy's information," in *Advances in Cryptology—CRYPTO*, 1986, pp. 468–476.

[9] C. H. Bennett, G. Brassard, and J. M. Robert, "Privacy amplification by public discussion," *SIAM J. Comput.*, vol. 17, pp. 210–229, Apr. 1988.

[10] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," *Phys. Rev. Lett.*, vol. 68, pp. 557–559, Feb. 1992.

[11] C. H. Bennett, G. Brassard, C. Crepeau, and U. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pt. 2, pp. 1915–1923, Nov. 1995.

[12] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[13] M. Bloch, A. Thangaraj, S. W. McLaughlin, and J.-M. Merolla, "LDPC-based Gaussian key reconciliation," in *Proc. IEEE Inf. Th. Workshop arXiv:cs.IT/0509041*, Punta del Este, Uruguay, Mar. 2006, pp. 116–120.

[14] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in *Advances in Cryptology—EUROCRYPT*, 1994, pp. 410–423.

[15] C. Cachin and U. Maurer, "Linking information reconciliation and privacy amplification," *J. Cryptology*, vol. 10, pp. 97–110, 1997.

[16] J. L. Carter and M. N. Wegman, "Universal classes of hash functions," *J. Comput. Syst. Sci.*, vol. 18, pp. 143–154, 1979.

[17] J. Chen, D. He, and E. Yang, "On the codebook-level duality between Slepian-Wolf coding and channel coding," in *Proc. IEEE Inform. Theory Appl. Workshop*, Feb. 2007, pp. 84–93.

[18] K. L. Chung, *A Course in Probability Theory*, 3rd ed. San Diego: Academic, 2001.

[19] M. Christandl, R. Renner, and S. Wolf, "A property of the intrinsic mutual information," in *Proc. Int. Symp. Inform. Theory*, Jul. 2003, p. 258.

[20] T. P. Coleman, A. H. Lee, M. Médard, and M. Effros, "Low-complexity approaches to Slepian–Wolf near-lossless distributed data compression," *IEEE Trans. Inf. Theory*, vol. 52, no. 8, pp. 3546–3561, Aug. 2006.

[21] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York: Wiley, 1991.

[22] R. Cramer, Y. Dodis, S. Fehr, C. Padró, and D. Wichs, "Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors," in *Advances in Cryptology—EUROCRYPT*, 2008, pp. 471–488.

[23] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3047–3061, Dec. 2004.

[24] Y. Dodis, J. Katz, and L. Reyzin, "Robust fuzzy extractors and authenticated key agreement from close secrets," in *Advances in Cryptology—CRYTPO '06*, pp. 232–250.

[25] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM J. Comput.*, pp. 97–139, 2008.

[26] A. Dvoretzky, J. Kiefer, and J. Wolfowitz, "Asymptotic minimax character of the sample distribution function and of the classical multinomial estimator," *Ann. Math. Statist.*, vol. 27, no. 3, pp. 642–669, 1956.

[27] J. Garcia-Frias and Y. Zhao, "Compression of correlated binary sources using turbo codes," *IEEE Commun. Lett.*, vol. 5, no. 10, pp. 417–419, Oct. 2001.

[28] F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using gaussian-modulated coherent states," *Lett. Nature*, vol. 421, pp. 238–241, Jan. 2003.

[29] A. A. Hassan, W. E. Stark, J. E. Hershey, and S. Chennakeshu, "Cryptographic key agreement for mobile radio," *Digital Signal Process. Mag.*, vol. 6, pp. 207–212, 1996.

[30] J. E. Hershey, A. A. Hassan, and R. Yarlagadda, "Unconventional cryptographic keying variable management," *IEEE Trans. Commun.*, vol. 43, no. 1, pp. 3–6, Jan. 1995.

[31] H. Imai, K. Kobara, and K. Morozov, "On the possibility of key agreement using variable directional antenna," in *Proc. 1st Joint Workshop Information Security (JWIS 2006)*, Seoul, Korea, 2006, pp. 153–167.

[32] W. C. Jakes, *Microwave Mobile Communications*. Hoboken, NJ: Wiley, 1994.

[33] A. Goldsmith, *Wireless Communications*. Cambridge, U.K.: Cambridge University Press, 2005.
[34] H. Kooraparty, A. A. Hassan, and S. Chennakeshu, "Secure information transmission for mobile radio," *IEEE Commun. Lett.*, vol. 4, no. 2, pp. 52–55, Feb. 2000.
[35] A. D. Liveris, Z. Xiong, and C. N. Georghiades, "Compression of binary sources with side information at the decoding using LDPC codes," *IEEE Commun. Lett.*, vol. 6, no. 10, pp. 440–442, Oct. 2002.
[36] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, "Quantum key distribution over 25 km with an all-fiber continuous-variable system," *Phys. Rev. A*, vol. 76, pp. 042305/1–10, Oct. 2007.
[37] L. Lamport, "Password authentication with insecure communication," *Commun. ACM*, vol. 24, no. 11, pp. 770–772, 1981.
[38] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in *Proc. 14th ACM Int. Conf. Mobile Comput. Network. (MobiCom 2008)*, San Francisco, CA, pp. 128–139.
[39] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inform. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.
[40] U. M. Maurer, "The strong secret key rate of discrete random triples," in *Communications and Cryptography: Two Sides of One Tapestry*, R. E. Blahut, Ed. *et al.* Norwell, MA: Kluwer, 1994, ch. 26, pp. 271–285.
[41] U. M. Maurer, "Information-theoretically secure secret-key agreement by NOT authenticated public discussion," in *Advances in Cryptology—EUROCRYPT*, 1997, pp. 209–225.
[42] U. M. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Advances in Cryptology—EUROCRYPT*, May 2000, pp. 351–368.
[43] U. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels—Part I: Definitions and a completeness result," *IEEE Trans. Inform. Theory*, vol. 49, no. 4, pp. 822–831, Apr. 2003.
[44] U. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels—Part II: The simulatability condition," *IEEE Trans. Inform. Theory*, vol. 49, no. 4, pp. 832–838, Apr. 2003.
[45] U. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels—Part III: Privacy amplification," *IEEE Trans. Inform. Theory*, vol. 49, no. 4, pp. 839–851, Apr. 2003.
[46] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, U.K.: Cambridge Univ. Press, 2000.
[47] S. Nitinawarat, "Secret key generation for correlated Gaussian sources," in *Proc. Int. Symp. Inform. Theory*, Toronto, Canada, Jul. 2008.
[48] N. PatwariS and K. Kasera, "Robust location distinction using temporal link signatures," in *Proc. ACM Conf. Mobile Comput. Network*, Sep. 2007, pp. 111–122.
[49] S. S. Pradhan and K. Ramchandran, "Distributed source coding using syndromes (DISCUS): Design and construction," *IEEE Trans. Inf. Theory*, vol. 49, no. 3, pp. 626–643, Mar. 2003.
[50] J. G. Proakis, *Digital Communications*, 4th ed. New York: McGraw-Hill, 2000.
[51] T. S. Rappaport, *Wireless Communications: Principles and Practice*. Englewood Cliffs, NJ: Prentice-Hall, 2001.
[52] R. Raz, I. Reingold, and S. Vadhan, "Extracting all the randomness and reducing the error in trevisan's extractors," in *Proc. Symp. Theory Comput.*, 1999, pp. 149–158.
[53] R. Renner, J. Skripsky, and S. Wolf, "A new measure for conditional mutual information and its properties," in *Proc. Int. Symp. Inform. Theory*, Jul. 2003, p. 259.
[54] G. R. Shorak and J. A. Wellner, *Empirical Processes With Applications to Statistics*. Hoboken, NJ: Wiley, 1986.
[55] G. Van Assche, J. Cardinal, and N. J. Cerf, "Reconciliation of a quantum-distributed Gaussian key," *IEEE Trans. Inf. Theory*, vol. 50, no. 2, pp. 394–400, Feb. 2004.
[56] Q. Wang, S. R. Kulkarni, and S. Verdu, "A nearest-neighbor approach to estimating divergence between continuous random vectors," in *Proc. Int. Symp. Inform. Theory*, Jul. 2006, pp. 242–246.
[57] M. N. Wegman and J. Carter, "New hash functions and their use in authentication and set equality," *J. Comput. Syst. Sci.*, vol. 22, pp. 265–279, 1981.
[58] R. Wilson, D. Tse, and R. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 3, pp. 364–375, Sep. 2007.
[59] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Fingerprints in the ether: Using the physical layer for wireless authentication," in *Proc. Int. Conf. Commun.*, Jun. 2007, pp. 4646–4651.
[60] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication under time-variant channels," *IEEE Trans. Wireless Commun.*, vol. 7, no. 7, pp. 2571–2579, Jul. 2008.
[61] C. Ye and P. Narayan, "Secret key and private key constructions for simple multiterminal source models," in *Proc. Int. Symp. Inform. Theory*, Sep. 2005, pp. 2133–2137.
[62] C. Ye, A. Reznik, and Y. Shah, "Extracting secrecy from jointly Gaussian random variables," in *Proc. Int. Symp. Inform. Theory*, Jul. 2006, pp. 2593–2597.

Chunxuan Ye received the B.Eng. (Hons) degree in electrical engineering from Shanghai Jiao Tong University, China, the M.Phil. degree in information engineering from the Chinese University of Hong Kong, and the Ph.D. degree in electrical and computer engineering from the University of Maryland, College Park, in 1997, 2000, and 2005, respectively.

He has been working at InterDigital Communications, King of Prussia, PA, since 2005. His research interests are in the areas of information theory, communication theory, and wireless communication systems. These include physical layer security, cooperative and relayed networks, network coding and source coding, wireless system prototyping platform, and wireless communications networks. He has published more than 20 papers and book chapters. He has more than 12 pending U.S. patents.

Dr. Ye is a member of the technical program committee of 2010 IEEE Sarnoff Symposium. He received the 2006 President's awards at InterDigital.

Suhas Mathur received the B.Tech. degree in electrical engineering from the Indian Institute of Technology (IIT), Madras, in 2004, and the M.S. degree in electrical engineering from Rutgers University, New Brunswick, NJ, in 2006. He is currently working toward the Ph.D. degree at the Wireless Information Networking Laboratory (WINLAB), Rutgers University.

His reserch work spans mobile sensing, wireless networking, and information security. His doctoral research is focussed on building practical mechanisms for improving security and privacy in wireless systems. For his Masters thesis, he worked on studying cooperation in wireless networks using game theoretic tools. He spent the summer of 2006 working at the Corporate R&D division at Qualcomm Inc. and the summer of 2008 at the Chief Technology Office of InterDigital Inc. His research interests include wireless networks, mobile systems, and the security and privacy chellenges arising out of emerging mobile wireless systems.

Alex Reznik receive the BSEE degree from The Cooper Union, the SM degree in EECS from Massachusetts Institute of Technology, and the Ph.D. degree in electrical engineering from Princeton University in 1996, 1998, and 2005, respectively.

During 2000–2002, he held a MURI fellowship at Princeton University. He has been with InterDigital, King of Prussia, PA, since 1999, where he is currently a Principal Engineer in the Advanced Communication Networks Group, leading a number of activities in the area of cognitive radio. His past contributions at InterDigital included technical leadership positions on projects in physical layer security, cellular modem architecture, and advanced receiver design. He holds a visiting faculty appointment at Winlab, Rutgers University. His research interests are in information and communication theory and architecture and design of modern communication systems and devices.

Dr. Reznik is an inventor or coinventor on over 40 granted U.S. patents and has been awarded several President's and CTO innovation awards at InterDigital.

Yogendra Shah received the B.Sc. and Ph.D. degree in electrical engineering from The City University, London, in 1982 and 1985, respectively.

He has worked in the wireless industry developing consumer products incorporating wireless technologies from the early CT2 digital cordless telephony standard through to the current generation 3G systems. He has worked as a Systems Engineer and Product Developer at various organizations before joining InterDigital. He is currently an Manager in the R&D Department at InterDigital, King of Prussi, PA, with research interests in developing advanced communications modem technologies and wireless security technologies.

Dr. Shah is an inventor or coinventor on several U.S. patents and has been awarded the President's and CTO innovation awards at InterDigital.

Wade Trappe received the B.A. degree in mathematics from The University of Texas at Austin in 1994, and the Ph.D. degree in applied mathematics and scientific computing from the University of Maryland in 2002.

He is currently Associate Director at the Wireless Information Network Laboratory (WINLAB) and an associate professor in the Electrical and Computer Engineering Department at Rutgers University, North Brunswick, NJ. His research interests include wireless security, wireless networking, multimedia security, and network security. He has led projects involving security and privacy for sensor networks, physical layer security for wireless systems, a security framework for cognitive radios, the development of wireless testbed resources, and new RFID technologies. Recently, his research group has developed several cross-layer security mechanisms for wireless networks, has developed jamming detection and jamming defense mechanisms for wireless networks, and has investigated privacy-enhancing routing methods for wireless networks. He has published over 100 papers, including two best papers in media security, a best paper on the localization of cognitive radios, and several wireless security papers in premier conferences. His experience in network security and wireless systems spans 12 years, and he has coauthored a popular textbook in the field, *Introduction to Cryptography with Coding Theory*, as well as four other books on wireless systems and multimedia security.

Dr. Trappe is a member of the IEEE Signal Processing and Communications societies, and a member of the ACM.

Narayan B. Mandayam (S'90–M'95–SM'00–F'09) received the B.Tech. (Hons.) degree in 1989 from the Indian Institute of Technology, Kharagpur, and the M.S. and Ph.D. degrees in 1991 and 1994 from Rice University, all in electrical engineering.

From 1994 to 1996, he was a Research Associate at the Wireless Information Network Laboratory (WINLAB), Rutgers University, North Brunswick, NJ, before joining the faculty of the Electrical and Computer Engineering Department at Rutgers where he became Associate Professor in 2001 and Professor in 2003. Currently, he also serves as Associate Director at WINLAB. He was a visiting faculty fellow in the Department of Electrical Engineering, Princeton University, in 2002, and a visiting faculty at the Indian Institute of Science in 2003. His research interests are in various aspects of wireless data transmission including system modeling and performance, signal processing and radio resource management with emphasis on techniques for cognitive radio networks.

Dr. Mandayam is a recipient of the Fred W. Ellersick Prize from the IEEE Communications Society in 2009 along with O. Ileri for their work on dynamic spectrum access models and spectrum policy. He is also a recipient of the Institute Silver Medal from the Indian Institute of Technology in 1989 and the National Science Foundation CAREER Award in 1998. He is a coauthor with C. Comaniciu and H. V. Poor of the book *Wireless Networks: Multiuser Detection in Cross-Layer Design* (New York: Springer). He has served as an Editor for the journals IEEE COMMUNICATION LETTERS and IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS. He has also served as a guest editor of the SPECIAL ISSUE ON ADAPTIVE, SPECTRUM AGILE, AND COGNITIVE RADIO NETWORKS, IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS (2007) and SPECIAL ISSUE ON GAME THEORY IN COMMUNICATION SYSTEMS, IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS (2008).