

On the Secrecy Capabilities of ITU Channels

Chunxuan Ye, Alex Reznik, Gregory Sternberg and Yogendra Shah

InterDigital Communications Corporation

King of Prussia, PA 19406

Email: {Chunxuan.Ye, Alex.Reznik, Gregory.Sternberg, Yogendra.Shah}@interdigital.com

Abstract— We consider the secrecy inherent in the reciprocal nature of multipath fading channels and present a technique to generate a shared perfectly secret key by two terminals observing a multipath fading channel. Using this technique we quantify the secrecy that can be generated from ITU cellular channels for the 2GHz frequency range.

I. INTRODUCTION

In a source-type model for secrecy generation [2], [6], two terminals observe a common random source which is inaccessible to other terminals. Based on their dependent observations, these two terminals generate a common secret key by communicating with each other over a public channel. A potential eavesdropper may observe the transmissions on the public channel, but is unable to tamper with the transmissions. The secret key generated by these two terminals should be concealed from the eavesdropper. Specifically, the secret key is required to be nearly “statistically independent” of the public transmissions. Such a secret key is called a perfectly secret key or an information theoretic secret key. Various extensions of this source-type model have been investigated (see e.g., [3], [4], [7], [12], [13]).

The theoretic aspects of the source-type model are well understood and availability of even small-rate perfectly secret key sources could be used to significantly enhance the effectiveness of modern security systems. Nevertheless, there are few practical applications of this model. The main reason for this is the lack of a random source which is observable to the two terminals but is inaccessible to other terminals. One area where such a random source exists is quantum cryptography. In the field of quantum cryptography, a random source originates from quantum entanglement. Another area where such a random source exists is wireless communications [14]. Suppose that a pair of wireless terminals communicate with each other on the same frequency in a wireless communication environment. The mutual wireless channel between these two terminals can serve as a common random source: i) The commonality follows from the reciprocity of the wireless channel. ii) The randomness is well known to be inherent in wireless channels due to the constantly changing physical environment. In most cellular channels it is further enhanced by the high number of scatterers. If both terminals possess some means of observing their mutual channel, the resulting observations are highly statistically dependent. On the other hand, the observations of a third terminal almost certainly remain independent with the channel-specific observations of the first two terminals if the third terminal is located more

than half a wavelength away from these two terminals. The reference [14] proposes a practical system to construct a secret key from a single path Rayleigh or Rician fading channel.

The problem of generating a secret key from an ultra-wideband (UWB) channel has been studied previously in [11]. In this paper we consider channels of much narrower bandwidth, such as those commonly observed in cellular communications. We observe that there are two key differences between such channels and UWB channels:

- In cellular channels discrete multipath components can overlap in a manner where they are no longer resolvable (uniquely separable) at the receiver. This is typically not an issue for UWB.
- On the other hand, for cellular channels multipath components can be reasonably assumed to fade according to Rayleigh or Rician fading processes, allowing for a direct application of the results in [14]. Such an assumption is not reasonable for UWB channels and in fact more complex fading distributions are usually considered [11].

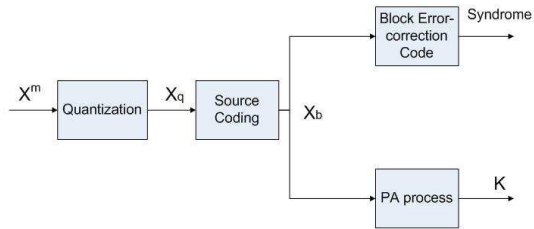
In this paper, we summarize an approach to extend the techniques in [14] to non-UWB multipath fading channels. We then use these techniques to quantify the secrecy capacities of some of the ITU channels that are used for performance testing of modern cellular communication systems [1].

II. PRELIMINARIES

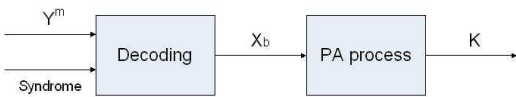
A. Secret Key Construction From Jointly Gaussian Random Variables

Suppose two terminals, Alice and Bob, respectively observe m independent and identically distributed (i.i.d.) repetitions of the dependent random variables X and Y , denoted by $X^m = (X_1, \dots, X_m)$ and $Y^m = (Y_1, \dots, Y_m)$. Based on their observations, Alice and Bob wish to generate a common secret key K by communicating with each other over an error-free public channel. The resulting secret key K should be nearly statistically independent of the public transmissions, and should satisfy a certain uniformity condition (see [2], [6] for detailed description). The entropy rate of the resulting secret key, viz., $H(K)/m$, is called a secret key rate. It is known [2], [6] that the secret key rate is upper bounded by the mutual information between X and Y , viz., $I(X; Y)$.

An efficient system is proposed in [14] to construct a secret key for the above problem with the random variables X and Y being jointly Gaussian random variables. This system is drawn in Fig. 1. In the system, Alice first equiprobably quantizes



Block diagram of secrecy processing for Alice



Block diagram of secrecy processing for Bob

Fig. 1. Secret key construction system

her Gaussian random variables X^m . The quantization result X_q is converted to a bit string X_b using Gray coding. The syndrome of the bit string X_b , in terms of a given LDPC code, is then transmitted through an error-free public channel to Bob. Based on the syndrome and his Gaussian random variables Y^m , Bob then tries to decode X_b by applying a modified belief-propagation algorithm, in which the log-likelihood ratio is softly encoded. Finally, both terminals hash out the publicly revealed information (i.e., the syndrome) from the common bit string X_b , leaving purely secret bits K . The process of hashing, also called privacy amplification (PA), has been extensively discussed in [3]. It is reported in [14] that at a target key bit error rate of 10^{-4} , the secret key resulting from this system has a rate within 1.2 bits of the upper bound $I(X; Y)$.

B. Multipath Fading Channel Model

A wireless channel is well modeled by a collection of discrete pulses with different amplitude and delay. Moreover, except in the ultra-wideband scenario, each pulse is usually well modeled as being subject to Rayleigh or Rician fading. In other words, a wireless channel can be expressed as

$$a(t) = \sum_{i=1}^L \alpha_i \delta(t - \tau_i), \quad (1)$$

where $\delta(\bullet)$ is the unit impulse function, $L \in [1, \infty)$ is the number of paths of the wireless channel, and α_i, τ_i represent amplitude and delay of the i^{th} path. In the Rayleigh fading case, the amplitudes $\alpha_1, \dots, \alpha_L$ are independent zero-mean complex Gaussian random variables. In the Rician fading case, the amplitudes $\alpha_1, \dots, \alpha_L$ are independent non-zero-mean complex Gaussian random variables. Effectively, the two cases are processed identically, once the mean is subtracted from the

Rician process. Therefore, it is sufficient to consider Rayleigh fading only and we concentrate on this in the rest of the paper.

The channel impulse response (CIR) of a wireless channel is given by

$$h(t) = p(t) * a(t) = \sum_{i=1}^L \alpha_i p(t - \tau_i), \quad (2)$$

where $p(t)$ is the “pulse shape” resulting from the pre-determined band-limited transmit and receive filters. Equation (2) implies that the CIR is the superimposition of multiple delayed and scaled copies of the pulse shape $p(t)$.

A wireless terminal can learn the condition of a wireless channel by observing its impulse response. Typically, the observation $h[n]$ is a sampled noisy version of the CIR $h(t)$, i.e.,

$$h[n] = h(nT_S - \eta) + Z[nT_S], \quad (3)$$

where T_S is the sample interval, η is the sampling time offset, and $Z[nT_S]$ is the independent additive white Gaussian noise sequence.

C. Upper Bound on Secret Key Rates

Consider two wireless terminals, Alice and Bob, which communicate with each other on the same frequency in a wireless environment. These two terminals are able to apply training sequences in their transmissions to enable the receivers to observe the CIR of their reciprocal wireless channel. The CIR observations of Alice and Bob, denoted by $h_A[n]$ and $h_B[n]$ respectively, are given by (3) with individual sample interval, sampling time offset, and additive white Gaussian noise. Nevertheless, the CIR observations $h_A[n]$ and $h_B[n]$ are statistically similar because they originate from the same CIR $h(t)$ ¹.

If Alice and Bob wish to generate a common secret key K , based on their m i.i.d. repeated observations $h_A[n]$ and $h_B[n]$ followed by public transmissions between them, then according to [2], [6], the entropy rate of the resulting secret key $H(K)/m$ is upper bounded by the mutual information $I(h_A[n]; h_B[n])$.

In the interest of presenting the mutual information $I(h_A[n]; h_B[n])$ as a function of a single variable, we assume hereafter that the power of the additive white Gaussian noise in (3) is N . Let the mutual wireless channel between Alice and Bob be an L -path fading channel with average path powers (p_1, \dots, p_L) . Then it follows from the union bound that

$$I(h_A[n]; h_B[n]) \leq \sum_{i=1}^L \log \left(1 + \frac{p_i}{2 + \frac{N}{p_i}} \right). \quad (4)$$

When the first path in this L -path fading channel is set as the reference path, the relative average path power of this channel

¹The CIR observations of Alice and Bob should be made as close as possible to the same time in order to achieve the highest similarity for a time varying channel.

can be written as $(\bar{p}_1, \dots, \bar{p}_L)$, with $\bar{p}_i = \frac{p_i}{p_1}$. Thus, the upper bound in (4) becomes

$$\sum_{i=1}^L \log \left(1 + \frac{\text{SNR} \cdot \bar{p}_i}{2 + \frac{1}{\text{SNR} \cdot \bar{p}_i}} \right), \quad (5)$$

where $\text{SNR} (= \frac{p_1}{N})$ is defined for the reference path. The convention of letting the first path have a nominal 0 dB power is consistent with channel definitions used in [1], and we shall follow it here. For the reader's convenience, we list some ITU channels in Table I.

TABLE I

PROPAGATION CONDITIONS FOR MULTIPATH FADING ENVIRONMENTS

Channel model	Number of paths	Relative path delay (ns)	Relative average path power (dB)
ITU PA3	4	0, 110, 190, 410	0, -3.0, -6.0, -9.0
ITU PB3	6	0, 200, 800, 1200, 2300, 3700	0, -0.9, -4.9, -8.0, -7.9, -23.9
ITU VA30	6	0, 310, 710, 1090, 1730, 2510	0, -1.0, -9.0, -10.0, -15.0, -20.0

Note that the upper bound given by (5) is not tight in general due to inter-path interference. However, we expect this upper bound to be tight for most of the ITU multipath fading channels, since most of the paths of these channels turn out to be separable paths. Hence, we shall still use this upper bound in the rest of this paper. More generally, it may be possible to estimate the mutual information between $h_A[n]$ and $h_B[n]$ using the channel covariance matrix or non-parametric estimation techniques, such as, e.g., [9], [10].

III. PROBLEM SETUP

The secret key construction system in Fig. 1 is directly applicable to the single path Rayleigh fading channel. Suppose Alice and Bob observe the CIR of their mutual channel, which is a single path Rayleigh fading channel. Each terminal can select a single sample from a series of samples in $h[n]^2$. The selected samples at both terminals are jointly Gaussian random variables. Since the samples are based on independent observations, these samples could be set as the inputs to the secret key construction system.

However, such a simple approach is highly suboptimal in the multipath case. To approach the true secrecy generation capabilities in the multipath case, it is necessary for both Alice and Bob to remove the dependence among their CIR samples, while still keeping the cross-dependence between their selected samples. This is not a trivial problem. Note, for example, that standard compression techniques fail. Although these do produce independent samples (at least asymptotically) the small differences present prior to compression will cause the result to be quite different at the two terminals, making agreement on a common key very difficult.

²Typically, the selected sample should have the largest amplitude in order to achieve the maximal SNR.

Hence, it is desirable for both Alice and Bob to post-process their CIR observations such that the process outputs *independent* pairs of jointly Gaussian random variables that remain *highly correlated*. To implement this operation we introduce the *CIR post-process block*. With the availability of this block, Alice and Bob are able to generate a common secret key from their mutual multipath fading channel by applying the techniques in [14] to each path.

IV. CIR POST-PROCESS BLOCK

Our approach to design the CIR post-process block is to look for the discrete constituent multipath components that produce the observed CIR. This is done independently by Alice and Bob. The discrete path amplitudes derived at these two terminals should satisfy the following properties:

- i). Consistency: Alice and Bob should arrive at the same paths.
- ii). Independence: the resulting random variables should be independent (or closely so).

Note however, that we do not require correctness: i.e., as long as Alice and Bob identify the same candidate paths leading to independent path amplitudes, we do not require that these paths be the actual ones that created the observed CIR. This suggests that every orthogonal decomposition of the observed CIR, whenever it is consistent, provides a solution to the CIR post-process block.

We propose an orthogonal greedy decomposition algorithm (OGA), which is based on the solutions to the sparse representation problem [5], [8]. The basic principle of this algorithm is that given an observed CIR, it selects a single discrete pulse that provides the best possible fit according to some criterion. The contribution of this pulse is then computed and subtracted from the observed CIR. This process is repeated until some stopping threshold is reached.

A. Orthogonal Greedy Algorithm

The orthogonal greedy algorithm is given below:

Let $H(f)$ and $P(f)$ be the Fourier transforms of the sampled CIR $h[n]$ (can be either $h_A[n]$ or $h_B[n]$) and sampled pulse shape $p[n] = p(nT_S)$, respectively. Let THR be a pre-determined threshold. Set $H_1(f) = H(f)$ and $i = 1$.

Step 1: Find $m > 0$, $\phi \in [0, 2\pi)$ and $\tau \in R$, which minimize

$$\| H_i(f) - m e^{j\phi} P(f) e^{-j2\pi f\tau} \|_2, \quad (6)$$

where $\| \mathbf{a} \|_2$ denotes the l^2 -norm of a vector \mathbf{a} . Denote the corresponding values by m_i , ϕ_i and τ_i . Let $\alpha_i = m_i e^{j\phi_i}$

Step 2: Set $H_{i+1}(f) = H_i(f) - \alpha_i P(f) e^{-2\pi f\tau_i}$.

Step 3: If $m_i < \text{THR}$, then output

$$(\alpha_1, \tau_1), \dots, (\alpha_{i-1}, \tau_{i-1})$$

and stop. Otherwise, let $i = i + 1$ and return to **Step 1**. \square

It can be derived from **Step 1** that

$$(\phi_i, \tau_i) = \underset{\phi, \tau}{\operatorname{argmax}} \operatorname{Re} \left\{ e^{j\phi} \sum_{n=-\infty}^{\infty} h_i[n] p_\tau^*[n] \right\}, \quad (7)$$

and

$$m_i = \frac{\operatorname{Re} \left\{ e^{j\phi} \sum_{n=-\infty}^{\infty} h_i[n] p_{\tau}^*[n] \right\}}{\|P(f)\|_2^2}, \quad (8)$$

where $\operatorname{Re}\{\bullet\}$ denotes the real part of a complex number, $p_{\tau}[n] = p(nT_S - \tau)$, and $h_i[n]$ is the inverse Fourier transform of $H_i(f)$. Equations (7) and (8) suggest that we first correlate $h_i[n]$ against all delayed-and-sampled versions of $p(t)$. The optimum τ_i is the delay for which the absolute value of the correlation is maximum; the optimum ϕ_i is minus the angle of the correlation at τ_i ; and the optimum m_i is the absolute value of the correlation at τ_i , divided by the square of the l^2 -norm of $P(f)$.

B. Implementation and Performance of OGA

In practice, it is impossible to correlate against all the values of τ . Note that $p_{\tau_1}[n]$ and $p_{\tau_2}[n]$ are delayed versions of each other if $(\tau_1 - \tau_2)$ is an integer multiple of T_S . If we discretize the time line such that the time grid spacing is $\frac{1}{G}$, for some integer G , we need to implement a finite bank of filters, each representing $p_{\tau}[n]$ for a different fractional delay $\tau \in [0, T_S)$. The resulting algorithm is observed to have the following properties:

- (Consistency) Subject to a small error probability this algorithm is consistent, i.e., the paths detected by Alice and Bob are identical. Ensuring full consistency motivates a double-pass approach, which shall be briefly summarized below.
- (Independence) The fitness criterion in (6) guarantees the residual signal is uncorrelated with the selected signal. Recall that a sampled CIR is a jointly Gaussian random vector since it is composed of Gaussian noise and Gaussian pulse amplitude. Because the OGA conducts linear operations, the amplitude outputs of this algorithm (i.e., α) are also Gaussian random variables. Thus, the resulting Gaussian random variables are independent – i.e., for Rayleigh fading, the OGA guarantees *independence* of the output data.

Finally we note that small consistency errors between terminals can have a significant impact on the resulting secrecy rate as they can cause a failure to reach an agreement on a complete block of bits. These can be mitigated through a double pass OGA approach, which operates as follows: (due to space restrictions we have to omit the details)

- Perform OGA on each CIR observation to identify its path delays.
- Since path delays change significantly less frequently than path amplitudes, averaging the delays across many CIR observations will provide a reliable indication of the actual path delays.
- For each observed CIR, use the derived paths from the averaged path delays to complete the OGA process.

Note that the first two steps in the above operations serve as a path searcher, which may be implemented in alternate ways such as utilization of the tap information gained from a rake receiver or equalizer.

V. SIMULATION RESULTS

In this section, we examine the simulated secret key rate resulting from passing the observed CIR of ITU standard, reference multipath channels through the CIR post-process block and the subsequent secret key construction systems.

The same LDPC code as in [14] is also used in the secret key construction systems in the simulations, i.e., the irregular LDPC code with rate $\frac{1}{2}$, block size 4800 bits, and degree distribution pair as

$$\begin{aligned} \lambda(x) &= 0.234029x + 0.212425x^2 + 0.146898x^5 \\ &\quad + 0.102849x^6 + 0.303808x^{19} \\ \rho(x) &= 0.71875x^7 + 0.28125x^8. \end{aligned}$$

Thirty iterations of the belief-propagation algorithm are allowed. A target secret key bit error rate of 10^{-4} is achieved in all the simulations.

Figures 2 – 4 respectively show the secret key rates achieved for ITU PA3, PB3 and VA30 channels. For comparison, we also plot the upper bound (5) in these figures. It can be seen from the figures that there are several kinks on the achieved secret key rate curves. This is because when the SNR passes a certain value, the given LDPC code is able to correct all the errors between Alice and Bob’s CIR post-processed samples from a certain path. At this point, the resulting secret key bits from the additional detected path begin contributing, resulting in a steep secret key rate increase.

Since most of the actual paths for ITU PB3 and VA30 channels can be detected by the path searcher, the achieved secret key rates for these two channels have almost the same slopes as the upper bounds. For these two channels, the gaps between the achieved secret key rates and the corresponding upper bounds are mainly migrated from the gap reported in [14].

A large gap between the achieved secret key rate and the upper bound for ITU PA3 channel is observed in Fig. 2. An obvious reason is that only 1 or 2 paths out of 4 actual paths are detected by the path searcher. The achieved secret key rate is based on the detected paths, while the upper bound (5) is derived from all 4 actual paths. To justify the above arguments, we also plot a new “upper bound” based on the first two paths of the ITU PA3 channel in Fig. 4. It is seen that the achieved secret key rate has almost the same slope as this new “upper bound.”

Note that the achieved secret key rates illustrated in these figures are in terms of bits per channel observation. Since our secret key generation system focuses on extracting secrecy bits from independent channel observations, the terminals need to wait for at least the coherence time of the channel before sampling a new channel observation. With the carrier frequency of 2150 MHz, the coherence times for ITU PA3, PB3 and VA30 channels are around 71, 71 and 7.1 ms, respectively. Hence, the achieved secret key rates can be expressed in terms of bits per second. For examples, it follows from Figures 2 – 4 that the respective achieved secret key rates for ITU PA3, PB3 and VA30 channels at a SNR of 30 dB are about 11.2, 30 and

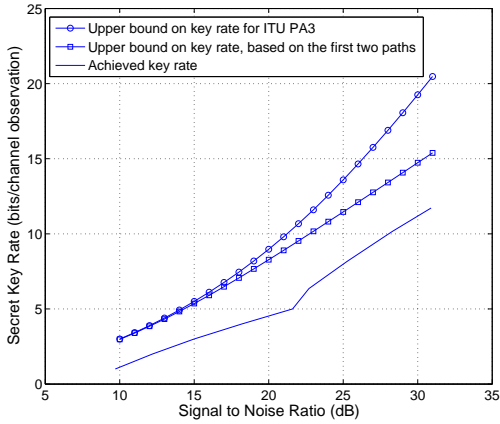


Fig. 2. Secret key rate for ITU PA3 channel

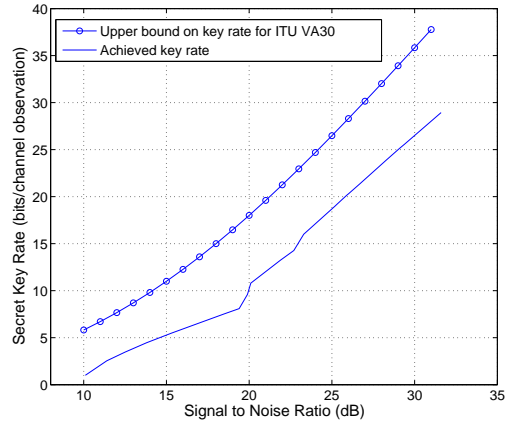


Fig. 4. Secret key rate for ITU VA30 channel

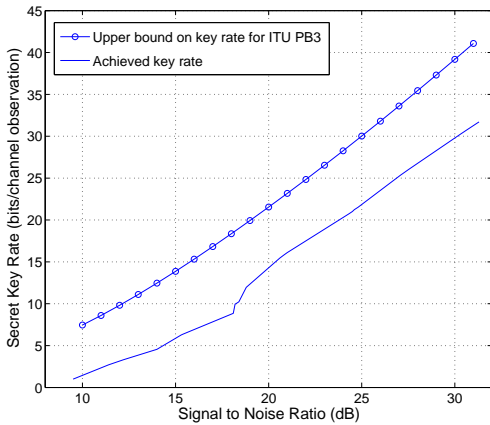


Fig. 3. Secret key rate for ITU PB3 channel

26.5 bits/channel observation. This corresponds to the secret key rates of 158, 423 and 3732 bits/second.

VI. DISCUSSION AND FUTURE WORK

In this paper we presented an OGA-based scheme for channel decomposition which is then combined with techniques in [14] for secrecy generation from multipath fading channels in the non-UWB scenarios. While we observe that our technique generally achieves the same slope as the secrecy upper bound, a significant gap to the upper bound still exists. The main reason for the gap is that we apply the techniques developed in [14] in our secret key generation system. The 1-bit gap observed by [14] translates to a 1-bit gap per path in our simulation results. Hence, a good approach to increasing the achieved secret key rates for multipath fading channels is to close the gap for a single path Rayleigh fading channel.

The analysis presented in this paper is based on the computer simulated CIR samples. Practical CIR measurements are needed to establish true secrecy-generation capabilities of wireless channels.

REFERENCES

- [1] 3GPP TS 25.101, *User Equipment (UE) radio transmission and reception (FDD) (Release 6)*, 2005. (available at <http://www.3gpp.org>).
- [2] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography, Part I: Secret sharing," *IEEE Trans. Inform. Theory*, vol. 39, pp. 1121–1132, July 1993.
- [3] C. H. Bennett, G. Brassard, C. Crepeau and U. Maurer, "Generalized privacy amplification," *IEEE Trans. Inform. Theory*, vol. 41, pp. 1915–1923, Nov. 1995.
- [4] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Trans. Inform. Theory*, vol. 50, pp. 3047–3061, Dec. 2004.
- [5] R. Gribonval and M. Nielsen, "Sparse representations in unions of bases," *IEEE Trans. Inform. Theory*, vol. 49, pp. 3320–3325, Dec. 2003.
- [6] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inform. Theory*, vol. 39, pp. 733–742, May 1993.
- [7] U. Maurer and S. Wolf, "Secret key agreement over a non-authenticated channel — parts I–III," *IEEE Trans. Inform. Theory*, vol. 49, pp. 822–851, Apr. 2003.
- [8] J. A. Tropp, "Greed is good: Algorithmic results for sparse approximation," *IEEE Trans. Inform. Theory*, vol. 50, pp. 2231–2242, Oct. 2004.
- [9] Q. Wang, S. R. Kulkarni and S. Verdú, "Divergence estimation for continuous distributions based on data-dependent partitions," *IEEE Trans. Inform. Theory*, vol. 51, pp. 3064–3074, Sept. 2005.
- [10] Q. Wang, S. R. Kulkarni and S. Verdú, "A nearest-neighbor approach to estimating divergence between continuous random vectors," *Processings Int. Symp. on Inform. Theory*, pp. 242–246, 2006.
- [11] R. Wilson, D. Tse and R. Scholtz, "Channel identification: Secret sharing using reciprocity in UWB channels," submitted to *IEEE Trans. Inform. Forensics. and Security*. (available at <http://www.eecs.berkeley.edu/~dtse>).
- [12] C. Ye and P. Narayan, "The private key capacity region for three terminals," *Proceedings Int. Symp. on Inform. Theory*, p. 44, 2004.
- [13] C. Ye and P. Narayan, "Secret key and private key constructions for simple multiterminal source models," *Proceedings Int. Symp. on Inform. Theory*, pp. 2133–2137, 2005.
- [14] C. Ye, A. Reznik and Y. Shah, "Extracting secrecy from jointly Gaussian random variables," *Processings Int. Symp. on Inform. Theory*, pp. 2593–2597, 2006.