This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2017.2749161, IEEE Transactions on Information Forensics and Security

Low-complexity power control and energy harvesting algorithms for wiretap channels employing finite-alphabet input schemes

Weichen Xiang, Martin Johnston, *Member, IEEE*, Stéphane Le Goff,

***Abstract*—We discuss the design rules of an energy-efficient wireless wiretap channel in this paper. On the transmitter side, we investigate the optimal power control policy for secrecy rate maximization over wiretap channels with the bit-interleaved coded modulation (BICM) scheme. On the receiver side, an energy harvesting (EH) algorithm is used to collect wireless signal energy without degrading the secrecy rate performance. These objectives are challenging as the closed-form solution to the mutual information of finite-alphabet input schemes remains unknown. In this paper, we derive a closed-form relationship between the secrecy rate and the signal-to-noise ratio (SNR) by transforming the SNR from the linear domain to the logarithm domain. The optimal power control policy (PCP) can be easily obtained by exhaustive search in a small interval, whereas the traditional search is performed over the entire SNR range. We also propose a sub-optimal PCP algorithm that significantly reduces the search complexity with only a minor performance loss. The optimal power splitting ratio (PSR) is studied to save energy while achieving the target secrecy rate. We show that if the transmission power is too high, the receiver is unable to simultaneously harvest energy from the wireless signals and achieve the target secrecy rate.**

I. Introduction

Secure and energy-saving communication receives a large amount of attention in current research on 5G communications technology because wireless devices are widely used and battery capacity is usually limited. Traditional methods to secure communication focus on cryptography techniques at higher layers, while prolonging battery life relies on evolution of the battery materials. However, there are two promising techniques, namely, physical layer security (PLS) and EH, that secures communications from an information theoretical perspective and enable devices to recharge their battery within the wireless signal coverage.

In a wireless network, a message sent from a transmitter can be intercepted by many terminals within the broadcast coverage. Hence, securing communications between legitimate users to protect against potential eavesdroppers is challenging, especially when the eavesdropper possesses sufficient computational resources. Physical layer security is a popular information-theoretic approach that was first proposed in [1]. Wyner introduced the wiretap channel model [2], in which three users are considered: the transmitter *Alice* sends a confidential message to the legitimate receiver *Bob*, while eavesdropper *Eve* is listening on a wiretap channel. Wyner proved that communication on the main channel (*Alice* to *Bob*) can be perfectly secured provided that the wiretap channel (*Alice* to *Eve*) is a degraded form of the main channel. The maximum information transmission rate from *Alice* to *Bob* with total ignorance from *Eve* is defined as the *secrecy capacity*. The wiretap channel model was further studied in [4], where the wiretap channel was a non-degraded version of the main channel. They showed that a positive secrecy capacity is always achievable provided the main channel is less noisy than the wiretap channel. Around the same time, research on secrecy capacity in [3] extended the channels to the Gaussian channel model and proved that the secrecy capacity is given by the difference in channel capacity between the main channel and the wiretap channel. Considering this as an optimization problem, [5] found that the secrecy capacity is a convex problem with respect to the input distribution; thus, by using a maximization technique, the secrecy capacity is obtained. The secrecy capacity under a fading channel environment was studied in [6] and [23], and it was shown that a positive secrecy capacity is achieved even when the main channel is noisier than the wiretap channel on average, provided perfect global channel state information (CSI) is available at the transmitter. The optimal power allocation policy that maximizes the achievable secrecy rate was also given in a closed-form expression [6], [7]. Moreover, in [8], the impact of correlation between the main and wiretap channels on secrecy capacity was considered, and it was shown that the secrecy capacity is a logarithmic function of the average SNR of the two channels and their correlation. The information rate can be enhanced by using multiple antennas or by using a cooperative communication strategy. The secrecy capacity of multi-antenna communications was studied in [9]–[11], where the relay assisted the wiretap channel model and showed an advantage in secrecy capacity performance compared to all users equipped with a single antenna.

Until now, most analyses on secrecy capacity relied on the assumption that the codeword is infinitely long and that the input symbols follow a Gaussian distribution. However, in practice, the constellation size is finite due to computational power constraints and the decoding complexity. The “channel capacity” often refers to Shannon’s capacity, which is achievable by using Gaussian input. For finite-alphabet input schemes, we replace the *secrecy capacity* with the *secrecy rate* to avoid ambiguity. The secrecy rate of finite-alphabet input schemes was studied in [12], where a power

Weichen Xiang, Martin Johnston and Stéphane Le Goff are with the School of Electrical and Electronic Engineering, Newcastle University, NE1 7RU, UK.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2017.2749161, IEEE Transactions on Information Forensics and Security

allocation policy for coded modulation (CM) was introduced for a multiple-in-multiple-out (MIMO) wiretap channel model by using an adaptive search algorithm. However, for wireless communications, BICM is the *de facto* standard for improved BER performance [15]. It was noted in [13] that the secrecy rate can vary significantly for BICM schemes when different mapping schemes are applied. One feature of finite-alphabet input schemes is that the maximum secrecy rate is achieved at a finite SNR. Therefore, research on very-high SNR regimes is of limited importance because the secrecy rate performance degrades when the SNR surpasses the optimal value.

Mobile devices are normally equipped with limited batteries, and in many cases, replacing the battery is extremely difficult or impossible, such as implanted devices for medical use. Therefore, developing a reliable method to recharge the device is vital. A promising EH approach to gather energy from radio frequency signals was introduced in [29], which proved that power and information can be carried by RF signals simultaneously. Several EH protocols were presented in [31], [32]; among the protocols, time switching and power splitting are the most commonly researched due to the simplicity of the circuit realization. Since the receiver uses part of the signal energy for EH, the information rate performance is degraded compared to conventional transmission. [32] noted that the EH approach also has a negative impact on the secrecy performance of wiretap channels. However, the secrecy rate does not necessarily have to be maximized but only needs to exceed a target rate. Thus, it is possible to jointly optimize the EH and PLS algorithms over one wiretap channel.

In this paper, we study the problems of secrecy rate maximization, transmission power minimization and the regime of the power splitting ratio on a BICM wiretap channel. By exploring the relationship between the channel SNR and the secrecy rate, low-computational-complexity solutions are obtained for the above problems. Specifically, the main contributions of this paper are summarized as follows:

1) A closed-form approximation of the secrecy rate at medium SNR is obtained by applying linear-to-logarithm domain transformation of the SNR.
2) A closed-form, suboptimal, low-complexity reducing PCP is introduced. The secrecy rate performance is optimal if the SNR difference between the channels is small.
3) For a wiretap channel with a constant rate and fixed transmission power transmitter, the range of PSR is studied to scavenge the “wasted” energy while meeting the target secrecy rate.

The remainder of this paper is organized as follows: In section II, the finite-alphabet input communication schemes are introduced. In section III, the secrecy rate maximization problem is addressed, and a novel transformation of the minimum mean square error (MMSE) is introduced to solve this problem. In section IV, the design of the EH receiver is considered, and we investigate the relationship between the power splitting ratio and the secrecy rate. The range of power splitting ratios that enables the wiretap channel to satisfy the predefined target secrecy rate is computed. Finally, in sections V and VI, simulation results and conclusions are provided, respectively.

II. System model

The following assumptions are made in this section: First, the transmitter *Alice* has knowledge of the global channel statement information (CSI), while both receivers have the CSI of their respective channels. Second, we assume the SNR difference between the main and wiretap channels is small. These two assumptions are realistic when *Bob* and *Eve* are users in one communication party, and *Eve* becomes a potential eavesdropper as the message is confidential and only intended to be decoded by *Bob*. In the remainder of this paper, the SNR is denoted by γ for convenience.

A. Minimum mean squared error

Consider the AWGN channel where the channel input-output function is given by

$$Y = \sqrt{\gamma}X + N, \tag{1}$$

where N is zero mean, unit variance Gaussian noise and X and Y are the channel input symbol vector and channel output signal vector, respectively. The probability density function (pdf) of the output is

$$p_{Y|X}(y|x) = \frac{1}{\pi}e^{-|y-\sqrt{\gamma}x|^2}. \tag{2}$$

Let $\hat{X}$ denote the estimate of the channel input X based on the observation of the channel output Y; the error of the estimation is measured using the mean square. The best estimation of X is given by the conditional mean estimator [19], denoted as $\hat{X}$,

$$\hat{X} = E[X|\sqrt{\gamma}X + N]. \tag{3}$$

The mean square error is the expectation of the difference between X and $\hat{X}$, which is given by

$$E[|X - \hat{X}|^2], \tag{4}$$

while the MMSE is the minimum value of (4). Let $M(\gamma)$ denote the MMSE as a function of SNR; then, we have

$$M(\gamma) = \min E[|X - \hat{X}|^2]. \tag{5}$$

Let $I(\gamma)$ denote the mutual information of the channel. The relationship between $I(\gamma)$ and $M(\gamma)$ is given by

$$M(\gamma) = \frac{dI(\gamma)}{d\gamma}. \tag{6}$$

Consider the Gaussian input case where the MMSE is given by

$$M^G(\gamma) = \frac{1}{1+\gamma}\log_2 e. \tag{7}$$

The MMSE of a finite-alphabet input needs to be evaluated by Monte Carlo method. Using (6), the achievable secrecy rate and the optimal PCP are obtained by employing an exhaustive search algorithm.

B. CM and BICM

In a CM scheme, the encoder output sequences are fed into a pseudo-random interleaver π, where the interleaving is performed at the symbol level. The output sequences of the interleaver are modulated to the symbols on constellation χ. The received signal is designated as y, and perfect CSI is assumed at the receiver side. The mutual information (MI) is given by

$$C^{CM} = m - E_{c,h,y}\left\{\log_2 \frac{\sum_{s\in\chi} p(y|s)}{p(y|x)}\right\}, \tag{8}$$

where h denotes the channel coefficient, c denotes the m-bit input to the constellation χ, and s denotes the constellation symbols. It is proved in [25] that the CM scheme also satisfies the relationship in (6).

BICM is an alternative to CM with better BER performance over Rayleigh fading channels. The major difference between BICM and CM is that the BICM channel capacity is affected by the mapping technique, for example, Gray mapping and set-partitioning (SP) mapping. Binary-reflected Gray mapping [14] is optimal in terms of channel capacity at medium-to-high SNR, and many alternative mappings have been proposed to improve the BER performance with iterative decoding [21], [22]. In the BICM scheme, the output sequences of the encoder are bit-wise interleaved before being mapped onto the constellation. At the receiver side, the log-likelihood ratio (LLR) of each bit is determined and fed to the decoder. The MI of the BICM scheme is computed via a Monte Carlo method, as shown below

$$C^{BICM} = m - \sum_{i=1}^{m} E_{\hat{c},h,y}\left\{\log_2 \frac{\sum_{s\in\chi} p\left(y|s\right)}{\sum_{s\in\chi_i^{c_j}} p\left(y|s\right)}\right\}, \tag{9}$$

where $s \in \chi_i^b$ represents the subset of all signals $s \in \chi$ whose labels are equal to $b \in \{0,1\}$ at position i. Since BICM estimates the LLR of the bit sequences at the receiver rather than the transmission symbol x, (6) is not directly applicable to BICM schemes.

The relationship between C^{CM} and C^{BICM} was presented in [27]:

$$C^{BICM} = \sum_{i=1}^{m} \frac{1}{2} \sum_{b=0,1} (C_{\chi}^{CM} - C_{\chi_i^b}^{CM}), \tag{10}$$

where C_{χ}^{CM} and $C_{\chi_i^b}^{CM}$ are the CM capacities of constellations χ and χ_i^b, respectively.

In the next section, a transformed MMSE is introduced to obtain the closed-form approximation of the secrecy rate. This is followed by comparison of a low-complexity PCP algorithm to the adaptive searching method.

III. Secrecy rate on Rayleigh fading channels

Initially, we consider that *Alice* is able to perform coding rate and transmission power adaptive strategies provided the perfect CSI of both channels. We introduce a method to compute the achievable secrecy rate for cases of Gaussian input and finite-alphabet input. Subscripts D and E represent the source-destination channel and the source-eavesdropper channel, respectively. We consider a classic three-terminal wiretap model with the channel outputs given by

$$y_D = \sqrt{P_S} h_D x + n_D, \tag{11}$$

$$y_E = \sqrt{P_S} h_D x + n_E, \tag{12}$$

where P_S is the transmission power and h_D and h_E are the channel coefficients of the main channel and wiretap channel, respectively. By definition, the achievable secrecy rate is given by

$$C_s = I(\gamma_D) - I(\gamma_E). \tag{13}$$

When the input message is infinitely long and Gaussian distributed, the secrecy capacity is given by $\log_2(\frac{1+P_S|h_D|^2}{1+P_S|h_E|^2})$, and the optimal transmission power that maximizes the secrecy capacity is found in [6] and is given by $R_S = \log_2(\frac{|h_D|^2}{|h_E|^2})$ when $P_S \to \infty$. However, when the input scheme employs a finite-sized constellation and follows an arbitrary distribution, the secrecy rate is difficult to determine, and optimizing the transmission power is even more challenging. Hence, we introduce a new method to analyze the secrecy rate and power control policy.

We write the secrecy rate R_S in the integrated form rather than the classic definition of substitution of the mutual information:

$$R_S = \int_{\gamma_E}^{\gamma_D} \frac{dI(\gamma)}{d\gamma} d\gamma, \tag{14}$$

where $\frac{dI(\gamma)}{d\gamma}$ is the gradient of the mutual information. The gradient of the mutual information is equal to the minimum mean squared error (MMSE) of the receiver estimation $\hat{x}$ based on observation y. Thus, the secrecy rate is given by

$$R_S = \int_{\gamma_E}^{\gamma_D} M(\gamma) d\gamma, \tag{15}$$

where $M(\gamma)$ is a decreasing function for a complex Gaussian input and the CM and BICM schemes with Gray mapping on AWGN channels [20]. However, the interval $[\gamma_E, \gamma_D]$ is scaled (increasing) as P_S increases. Thus, maximizing the secrecy rate in (15) is not possible. We present a logarithm domain transform method that greatly reduces the complexity of the R_S optimization.

First, it is important to note that the SNR difference when measured in decibels is independent of P_S and remains constant over one fading realization.

$$\begin{aligned}\Delta\gamma_{dB} &= \gamma_{D,dB} - \gamma_{E,dB}\\ &= 10\log_{10}\frac{|h_D|^2}{|h_E|^2}.\end{aligned} \tag{16}$$

Second, we denote $\mathcal{M}(\gamma_{dB})$ as the MMSE when the SNR is in dB, which has the relationship $M(\gamma) = \mathcal{M}(\gamma_{dB})$. Similarly, the mutual information corresponding to the SNR in dB is denoted as $I_{dB}(\gamma)$, which has the relationship $I_{dB}(\gamma_{dB}) = I(\gamma)$. By applying the derivative chain rule, we obtain

$$\begin{aligned}\mathcal{M}(\gamma_{dB}) &= \frac{dI_{dB}(\gamma_{dB})}{d\gamma_{dB}}\\ &= \frac{dI(\gamma)}{d\gamma}\frac{d\gamma}{d\gamma_{dB}}\\ &= 0.1\gamma\ln(10)M(\gamma).\end{aligned} \tag{17}$$

Therefore, the secrecy rate is given by

$$R_S = \int_{\gamma_{E,dB}}^{\gamma_{D,dB}} \mathcal{M}(\gamma_{dB}) d\gamma_{dB}. \tag{18}$$

Define $\bar{\mathcal{M}}(\gamma_{dB})$ as the mean value of $\mathcal{M}(\gamma_{dB})$ within $[\gamma_{E,dB}, \gamma_{D,dB}]$; the secrecy rate is then simplified to

$$R_S = \mathcal{M}(\bar{\gamma}_{dB})(\gamma_{D,dB} - \gamma_{E,dB}). \tag{19}$$

It is shown in 19 that the secrecy rate is the linear equation of the difference of SNR in dB. The curves of $M(\gamma)$ and $\mathcal{M}(\gamma_{dB})$ for Gaussian input, CM and BICM on AWGN channels are compared in Fig.1 and Fig. 2, respectively.

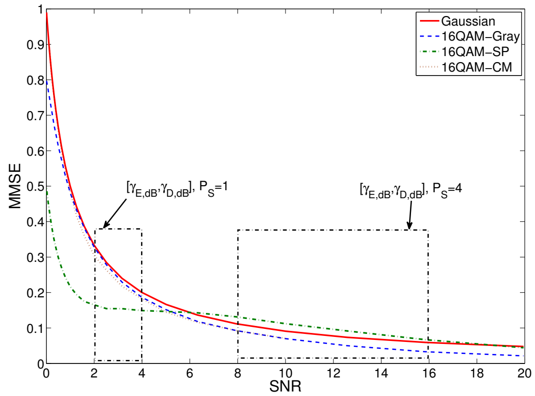

Fig. 1. The MMSE for Gaussian input, CM and various mappings for BICM on the AWGN channel

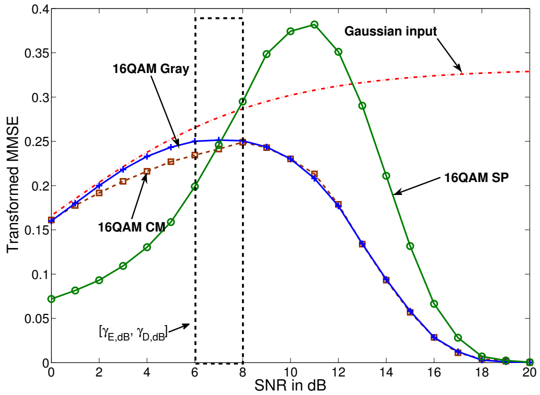

Fig. 2. The transformed MMSE for Gaussian input, CM and various mappings for BICM on the AWGN channel

A. Power control policy

The PCP enables the transmitter to adapt its transmission power according to the CSI to achieve higher secrecy rate performance than fixed power transmission. Assume a wiretap channel in which *Alice* is allowed the maximum transmission power P_T. According to (14), increasing P_S leads to expansion of $[\gamma_E, \gamma_D]$, but $M(\gamma)$ approaches zero as MI achieves $\log_2 M$. By applying (19), the optimal transmission power that maximizes the secrecy rate is equivalent to maximizing $\bar{\mathcal{M}}(\gamma_{dB})$ within the SNR range of interest.

The $\mathcal{M}(\gamma_{dB})$ curves are shown in Fig. 2. The global maximum $\mathcal{M}(\gamma_{dB})$ values for each CM and BICM curve are achieved at finite SNRs, while the maximum $\mathcal{M}(\gamma_{dB})$ value for the Gaussian input is achieved when $\gamma_{dB} \to \infty$. We define γ_{opt} as the SNR when $\mathcal{M}(\gamma_{dB})$ reaches the maximum. Since γ_{opt} is unique for to each modulation format and signal labelling combination, it is reasonable for the communication system to generate a look-up table of γ_{opt} of common communication schemes for quick searching. Gray mapping has lower values of γ_{opt} and $\mathcal{M}(\gamma_{opt})$ than SP mapping for a given same constellation. As the maximum value of $\mathcal{M}(\gamma_{dB})$ is achieved at finite SNR, the optimal PCP shifts $[\gamma_{E,dB}, \gamma_{D,dB}]$ by varying the input power P_S until (18) is maximized. However, exhaustive search is the only possible method to determine the optimal value of P_S. Therefore, we present a low-complexity sub-optimal PCP in Algorithm I.

ALGORITHM I: FAST PCP	
1	Find γ_{opt} from the look-up table,
2	If $\lim_{P_S \to P_T} \frac{\gamma_{D,dB}+\gamma_{E,dB}}{2} \geq \gamma_{opt}$, the optimal transmission power$\hat{P_S}$ is to let $\frac{\gamma_{D,dB}+\gamma_{E,dB}}{2} = \gamma_{opt}$
3	If $\lim_{P_S \to P_T} \frac{\gamma_{D,dB}+\gamma_{E,dB}}{2} \leq \gamma_{opt}$, full power transmission.

Algorithm I shows that $\hat{P_S}$ is given by

$$\hat{P_S} = \begin{cases} \dfrac{10^{\frac{\gamma_{opt}}{10}}}{|h_D||h_E|}, & \text{for } P_T \geq \frac{10^{\frac{\gamma_{opt}}{10}}}{|h_D||h_E|} \\ P_T, & \text{for } P_T \leq \frac{10^{\frac{\gamma_{opt}}{10}}}{|h_D||h_E|}, \end{cases} \tag{20}$$

where $\hat{P_S}$ is the transmission power computed from the proposed PCP, and P_T is the total available transmission power.

B. High transit power budget analysis

In cases where sufficient power is available at the transmitter, an optimal PCP is always applicable. Thus, the achievable secrecy rate is optimized in the high SNR regime. The relationship between γ_{dB} and R_S can be approximated in closed form. The following conclusions can be drawn from the small SNR gap assumption.

Theorem 1: The achievable secrecy rate at high SNR, denoted as R_S^{high}, is a linear function of the SNR_{dB} difference between the main channel and the wiretap channel on AWGN channels.

$$R_S^{high} \leq \mathcal{M}_{dB}(\gamma_{opt})(\gamma_{D,dB} - \gamma_{E,dB}). \tag{21}$$

proof *1:* Since $\mathcal{M}_{dB}(\gamma_{opt}) \geq \mathcal{M}_{dB}(\gamma)$, we have

$$\begin{aligned} R_S &= \int_{\gamma_{E,dB}}^{\gamma_{D,dB}} \mathcal{M}(\gamma_{dB}) d\gamma_{dB} \\ &\leq \int_{\gamma_{E,dB}}^{\gamma_{D,dB}} \mathcal{M}(\gamma_{opt}) d\gamma_{dB} \\ &= \mathcal{M}(\gamma_{opt})(\gamma_{D,dB} - \gamma_{E,dB}) \\ &\triangleq R_S^{high}. \end{aligned} \tag{22}$$

TABLE I
$\mathcal{M}_{dB}(\gamma_{opt})$ AND γ_{opt} VALUES OF WIDELY USED SCHEMES

Input scheme	$\mathcal{M}(\gamma_{opt})$	γ_{opt}
16QAM-CM	0.244	8 dB
16QAM-Gray	0.252	7 dB
16QAM-SP	0.382	10.7 dB
64QAM-CM	0.288	14.7 dB
64QAM-Gray	0.308	13 dB
64QAM-SP	0.398	16 dB

One special case is when $\gamma_{opt} \to \infty$, which implies the Gaussian input is adapted, and the secrecy capacity C_S^G is given by

$$\begin{aligned} C_S^G &= \lim_{P_S \to \infty} \int_{\gamma_{E,dB}}^{\gamma_{D,dB}} 0.1 \log_2(10) \frac{\gamma}{1+\gamma} d\gamma \\ &= 0.33(\gamma_{D,dB} - \gamma_{E,dB}), \end{aligned} \tag{23}$$

where $\mathcal{M}(\gamma \to \infty) = 0.33$, which completes the proof.

The values of $\mathcal{M}_{dB}(\gamma_{opt})$ and γ_{opt} of various modulation and mapping schemes are listed in Table I.

C. Secrecy rate approximation in the medium SNR range

A closed-form solution for the secrecy rate performance of a BICM scheme is desirable in information theory. Fig. 2 shows that for finite-alphabet input wiretap channels, the secrecy rate achieves the same value for two P_S values, which demonstrates that additional power can be consumed with no secrecy rate performance enhancement for a finite-alphabet input wiretap channel. This feature indicates that to achieve a target secrecy rate, the transmission power must be selected from a limited range. However, the search for proper P_S relies on an adaptive search method; it is interesting to obtain a closed-form approximation of $\mathcal{M}(\gamma_{opt})$ that fits the exact curve with considerable accuracy and low complexity in the SNR of interest. Fig. 2 demonstrates that the $\mathcal{M}$ curves of various mappings around γ_{opt} closely match general quadratic functions. We define a function $\hat{\mathcal{M}}(\gamma_{dB}) = \beta_1\gamma_{dB}^2 + \beta_2\gamma + \beta_3$ to approximate the $\mathcal{M}$ curves in the medium SNR range. The coefficients $\beta_1, \beta_2, and \beta_3$ are obtained by substituting $(\gamma_{dB}, \mathcal{M}(\gamma))$ of the curves into the general quadratic function. $\beta_1, \beta_2, and \beta_3$ are rounded to 4 decimal places to balance the accuracy of the approximation and the complexity of the computation. We list some coefficients of the quadratic curve that approximates $\mathcal{M}(\gamma)$ for 16QAM and 8PSK constellations around γ_{opt}.

For 4QAM, Gray mapping, $\beta_1 = -0.0024, \beta_2 = 0.0097$, and $\beta_3 = 0.1497$, the quadratic function is

$$\hat{\mathcal{M}}_{4QAM}(\gamma_{dB}) = -0.0024\gamma_{dB}^2 + 0.0097\gamma_{dB} + 0.1497. \tag{24}$$

For 8PSK, Gray mapping, $\beta_1 = -0.0019, \beta_2 = 0.0168$, and $\beta_3 = 0.158$, the quadratic function is

$$\hat{\mathcal{M}}_{8PSK}(\gamma_{dB}) = -0.0019\gamma_{dB}^2 + 0.0168\gamma_{dB} + 0.1580. \tag{25}$$

For 16QAM, Gray mapping, $\beta_1 = -0.0019, \beta_2 = 0.027$, and $\beta_3 = 0.155$, we obtain the approximation function

$$\hat{\mathcal{M}}_{16QAM}(\gamma_{dB}) = -0.0019\gamma_{dB}^2 + 0.027\gamma_{dB} + 0.155. \tag{26}$$

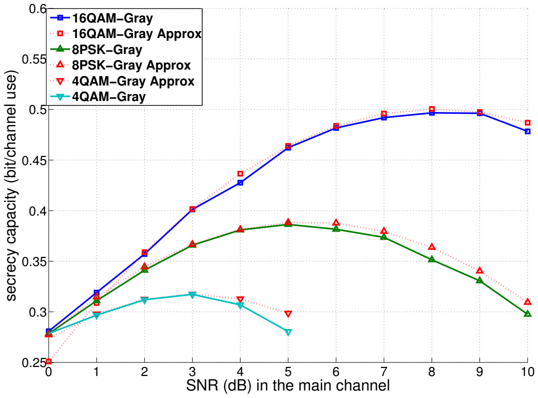

Fig. 3. The actual and approximated secrecy rate for Gray-mapped 16QAM and 8PSK

According to (14), the approximation of the secrecy rate, denoted as $\hat{R}_S$ is given by

$$\begin{aligned} \hat{R}_S \approx \frac{\beta_1}{3}(\gamma_{D,dB}^3 - \gamma_{E,dB}^3) + \frac{\beta_2}{2}(\gamma_{D,dB}^2 - \gamma_{E,dB}^2) \\ + \beta_3(\gamma_{D,dB} - \gamma_{E,dB}). \end{aligned} \tag{27}$$

The approximation matches the secrecy rate in the low-to-medium SNR range, which is of most interest to PCP because the secrecy rate performance degrades at higher SNR.

D. Transmission power minimization

Consider that *Alice* sends a confidential message at a constant information rate rather than performing adaptive rate transmission according to the CSI. The target secrecy rate, denoted as R_T, has to satisfy $R_S > R_T$ for perfect secrecy.

To determine the minimum P_S for R_T, we simplify (27) into a function of P_S

$$\begin{aligned} R_T &\leq \hat{R}_S \\ &= (\gamma_{D,dB} - \gamma_{E,dB})(\frac{\beta_1}{3}(\gamma_{D,dB}^2 + \gamma_{E,dB}^2 + \gamma_{D,dB}\gamma_{E,dB}) \\ &\quad + \frac{\beta_2}{2}(\gamma_{D,dB} + \gamma_{E,dB}) + \beta_3) \\ &= \frac{3\beta_1}{4}\Delta\gamma_{dB}T^2 + \beta_2\Delta\gamma_{dB}T + \frac{\beta_1}{4}\Delta\gamma_{dB}^3 + \beta_3\Delta\gamma_{dB}, \end{aligned} \tag{28}$$

where $T = \gamma_{D,dB} + \gamma_{E,dB}$, which can be expressed by

$$T = 10\log_{10}|h_D|^2 + 10\log_{10}|h_E|^2 + 20\log_{10}P_S. \tag{29}$$

It is shown that T is an incremental function of P_S, and the minimum P_S is obtained when T is minimized. The minimum T is obtained by solving

$$\frac{3\beta_1}{4}\Delta\gamma_{dB}T^2 + \beta_2\Delta\gamma_{dB}T + \frac{\beta_1}{4}\Delta\gamma_{dB}^3 + \beta_3\Delta\gamma_{dB} - R_T = 0. \tag{30}$$

Because $\beta_1 < 0$, the minimum T is given by

$$T = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}, \tag{31}$$

where $a = \frac{3\beta_1}{4}\Delta\gamma_{dB}$, $b = \beta_2\Delta\gamma_{dB}$ and $c = \frac{\beta_1}{4}\Delta\gamma_{dB}^3 + \beta_3\Delta\gamma_{dB} - R_T$. Note that there exist two values of T for

(30): the larger value represents the maximum value of P_S for the wiretap channel to achieve R_T. Thus, the minimum transmission power is given by

$$P_S = \frac{10^{\frac{T}{20}}}{\sqrt{|h_D|^2 |h_E|^2}}. \tag{32}$$

IV. Design of the energy harvesting receiver

The curves compared in Fig. 3 showed that the approximation of the secrecy rate matches the simulation results very well at medium SNRs, while at high SNRs, the approximation is less accurate. For 4QAM, the approximation is very accurate from low SNRs up to γ_{opt}, but as the constellation size increases, the accuracy of the approximation decreases. However, the secrecy rate approximation still matches the simulation of the 16QAM Gray mapping scheme very well from 1 dB to 9 dB. Since the R_T is achieved at two values of SNR, one is smaller than γ_{opt}, while the other is larger than γ_{opt}. From the perspective of energy saving, the smaller SNR, whose secrecy rate performance $R_S \geq R_T$, is optimal. Consider the wiretap channel with target secrecy rate R_T where the transmitter is unable to perform rate and power adaptive transmission. In this case, partial transmission energy is wasted if the channel condition is good and R_S is greater than R_T. However, the "wasted energy" can be scavenged and stored in the battery by applying EH. Among the various EH techniques, we focus on power splitting. Assume a wiretap channel model with a target secrecy rate R_T and with all nodes equipped with EH receivers. The power splitting coefficients of the intended receiver and the eavesdropper receiver are denoted as ρ_D and ρ_E, respectively. If $\rho_D = 0$, the intended receiver harvests no energy from the RF signal and uses all the power for information decoding, while $\rho_D = 1$ indicates that the intended receiver collects all the energy for battery charging.

In a typical EH receiver, there are two types of noise, one introduced by the analogue-to-digital conversion (ADC) process, which we denote by n_a, and the other due to channel noise, which is denoted as n_c. Both n_a and n_c are Gaussian noise with zero mean and variances σ_a^2 and σ_c^2. Normally, the channel noise n_c is ignorable because it is negligible relative to n_a. Thus, we only consider the ADC noise and assume the channel noise $n_c = 0$. For convenience, we assume that $\sigma_a^2 = 1$ at both receiver devices. After power splitting, the received signals for information decoding y^I are given by

$$y_D^I = \sqrt{(1-\rho_D)P_S}h_D x + n_{a,D}, \tag{33}$$
$$y_E^I = \sqrt{(1-\rho_E)P_S}h_E x + n_{a,E}. \tag{34}$$

The receiver can harvest energy from both the RF signal and the channel noise, while the ADC noise remains constant. In terms of the achievable secrecy rate, the worst case is that the eavesdropper uses all the power to decode the confidential message and harvests no energy from the RF signal, i.e., $\rho_E = 0$. We use $\hat{\gamma}_{D,dB}$ and $\hat{\gamma}_{E,dB}$ to define the SNRs at the signal decoding input of the main channel receiver and the wiretap channel receiver, respectively. Thus, $\hat{\gamma}_{D,dB}$ and $\hat{\gamma}_{E,dB}$ satisfy the following relations

$$\begin{aligned}\hat{\gamma}_{D,dB} &= 10\log_{10}|h_D|^2 P_S + 10\log_{10}(1-\rho_D)\\ &= \gamma_{D,dB} + \mu, \qquad (35)\\ \hat{\gamma}_{E,dB} &= \gamma_{E,dB}, \qquad (36)\end{aligned}$$

where $\mu = 10\log_{10}(1-\rho_D)$ denotes the power splitting ratio in decibels. To achieve the target secrecy rate R_T, the EH ratio of the destination receiver has to be chosen properly to satisfy the following conditions

$$R_T < R_S \tag{37}$$

subject to

$$\rho_D > 0, P_S > 0. \tag{38}$$

If ρ_D is too small, excessive energy is wasted, and the battery of the receiver is charged slowly. If ρ_D is too large, then the secrecy rate of the wiretap channel is smaller than the predefined target secrecy rate, and as a result, the confidential message cannot be transmitted to the destination with perfect secrecy. The condition in (37) can be reformulated to

$$\begin{aligned}R_T &\leq \hat{R}_S\\ &= \frac{\beta_1}{3}(\hat{\gamma}_{D,dB}^3 - \gamma_{E,dB}^3) + \frac{\beta_2}{2}(\hat{\gamma}_{D,dB}^2 - \gamma_{E,dB}^2)\\ &\quad + \beta_3(\hat{\gamma}_{D,dB} - \gamma_{E,dB}). \qquad (39)\end{aligned}$$

The maximum $\hat{\gamma}_{D,dB}$ is obtained when $R_T = R_S$. Define $J(\hat{\gamma}_{D,dB})$ as a function of $\hat{\gamma}_{D,dB}$,

$$J(\hat{\gamma}_{D,dB}) = \frac{\beta_1}{3}\hat{\gamma}_{D,dB}^3 + \frac{\beta_2}{2}\hat{\gamma}_{D,dB}^2 + \beta_3\hat{\gamma}_{D,dB} + \omega, \tag{40}$$

where

$$\omega = -(\frac{\beta_1}{3}\gamma_{E,dB}^3 + \frac{\beta_2}{2}\gamma_{E,dB}^2 + \beta_3\gamma_{E,dB}) - R_T. \tag{41}$$

Let $J(\hat{\gamma}_{D,dB}) = 0$. The three roots of $J(\hat{\gamma}_{D,dB})$ can be solved by Cardano's method [33], and the roots are denoted as $\mathcal{R}_1, \mathcal{R}_2$, and $\mathcal{R}_3$. We assume the three roots satisfy

$$\mathcal{R}_1 \leq \mathcal{R}_2 \leq \mathcal{R}_3. \tag{42}$$

Only $\mathcal{R}_2$ is in the range $(\gamma_{E,dB}, \gamma_{D,dB})$ as $\mathcal{R}_1$ and $\mathcal{R}_3$ are generated by the negative values of $\hat{R}_S$. The maximum ρ_D and minimum P_S are given by

$$\rho_D^{max} = 1 - \frac{10^{0.1\mathcal{R}_2}}{P_S|h_D|^2}. \tag{43}$$

$$P_S^{min} = \frac{10^{0.1\mathcal{R}_2}}{|h_D|^2}. \tag{44}$$

V. Numerical results

In this section, simulation results are presented to validate the analysis of the previous sections.

First, we evaluate the secrecy rate of BICM schemes with the proposed fast PCP on AWGN channels. 16QAM and 64QAM are selected as the modulation schemes with Gray and set-partitioning mapping. The total transmission power $P_T = 1$. At high SNRs, the transmitter is able to allocate sufficient power to implement the fast PCP algorithm, the simulation of the secrecy rate performance at high SNR is very

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2017.2749161, IEEE Transactions on Information Forensics and Security

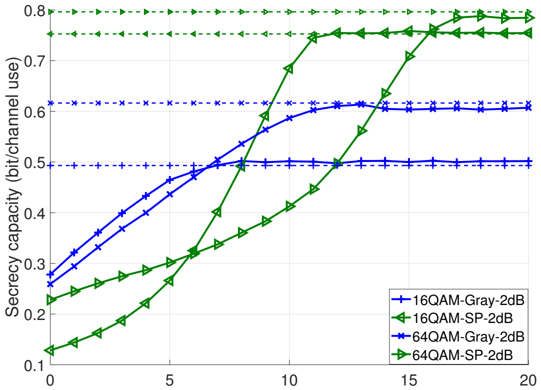

Fig. 4. Secrecy rate on AWGN channels. The SNR gap is 2 dB. The dashed lines are the high SNR approximations of the secrecy rate.

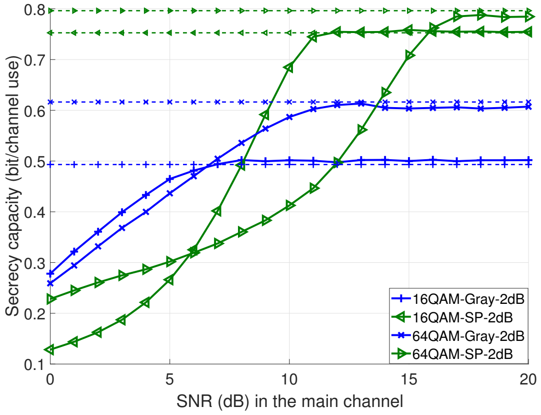

Fig. 5. Secrecy rate on AWGN channels. The SNR gap is 5 dB. The dashed lines are the high SNR approximations of the secrecy rate.

close to the high SNR approximation results. We illustrate the high SNR secrecy performance at SNR gaps of 2 dB and 5 dB and show that the approximation is more accurate when the SNR gap is smaller.

It is shown in Fig. 4 and Fig. 5 that the upper bound on the secrecy rate R_S^{high} derived in (22) is an accurate estimation of C_S when the SNR difference between the main and eavesdropper channels is small at high SNR. However, the accuracy decreases as the SNR gap increases, such as a gap of 5 dB. Additionally, R_S^{high} is less accurate when SP mapping is employed than when Gray mapping is employed for the same constellation at high SNR. This is because the curve for $\mathcal{M}(\gamma_{dB})$ with SP mapping is not as *flat* as that of Gray mapping near γ_{opt}; therefore, the accuracy of R_S^{high} decreases as the difference between $\bar{\mathcal{M}}$ and $\mathcal{M}(\gamma_{opt})$ increases. Furthermore, SP mapping achieves a higher secrecy rate than Gray mapping at high SNR but costs additional transmission power.

Fig. 6 and Fig. 7 show the performance of R_S with and without the proposed fast PCP. The dotted curves indicate that the transmitter always performs full power transmission $P_S = P_T = 1$, while the dashed curves inidcate that the secrecy rate is obtained by using optimal PCP (exhaustive search algorithm). Without PCP, R_S increases as the SNR increases before reaching γ_{opt}. However, after reaching the peak value, R_S decreases as the SNR increases and ultimately approaches zero. By contrast, with the proposed fast PCP, R_S performs the same as fixed power transmission at low SNRs, but R_S does not decrease at high SNRs and remains at the maximum value.

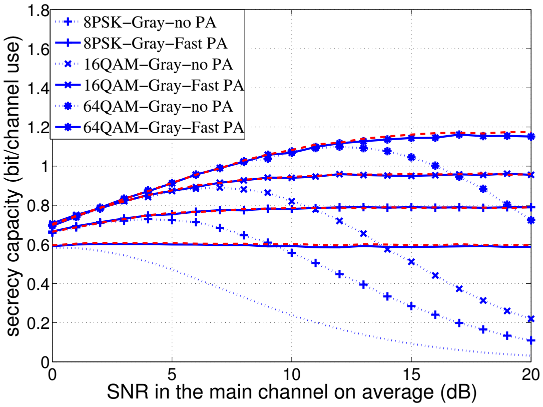

Fig. 6. Secrecy rate performance over Rayleigh fading channels. $\bar{\gamma_D} = \bar{\gamma_E}$.

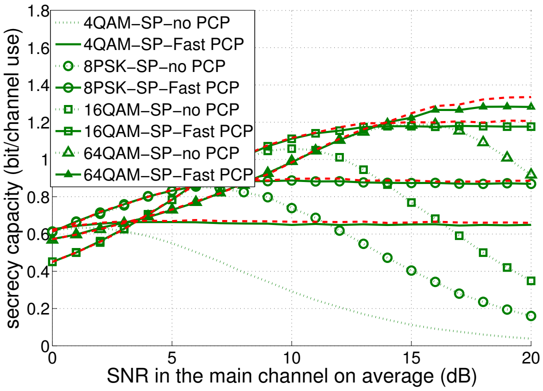

Fig. 7. Secrecy rate performance over Rayleigh fading channels with sub-optimal PCP. $\bar{\gamma_D} = \bar{\gamma_E}$.

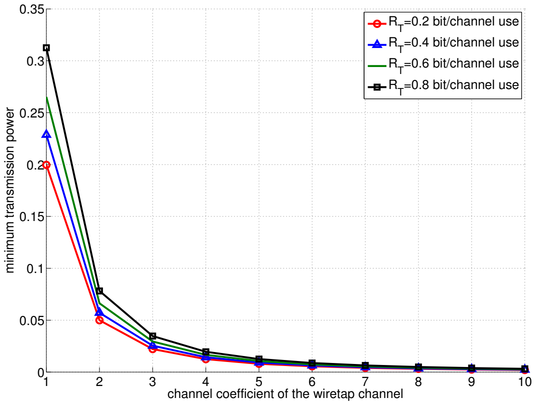

Fig. 8. The minimum P_S for target R_T. $\Delta\gamma = 4$ dB.

In Fig. 8, the SNR gap is 4 dB. The simulation shows that, on one hand, the required P_S for target secrecy rate R_T decreases exponentially as the SNR in both channels increases. On the other hand, the curves demonstrate that to achieve a

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2017.2749161, IEEE Transactions on Information Forensics and Security

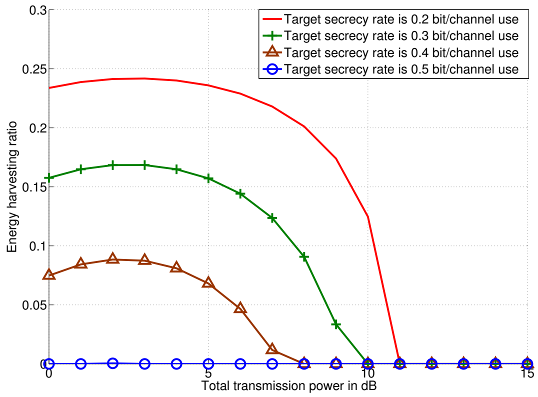

Fig. 9. The maximum EH ratio at the destination receiver: the main channel gain is 6 dB and the wiretap channel gain is 4 dB.

higher target rate, a larger P_S is required.

Fig. 9 demonstrates the maximum EH ratio at the destination receiver, provided the target secrecy rate R_T. As the target secrecy rate increases, the amount of harvested energy decreases. At high P_S, ρ_D decreases to 0 because the information rate in the wiretap channel is increased and the secrecy rate $R_S < R_T$. Thus, no energy can be harvested from the RF signal.

VI. Conclusion

The secrecy rate of the finite-alphabet input of the SISO wiretap channel model is investigated in this paper. Similar to Gaussian input, the minimum transmission power for the target secrecy rate is a decremental function of the wiretap channel coefficient. In contrast to Gaussian input, the maximum secrecy rate is achieved in the medium SNR range, depending on the modulation and signal labeling. The EH ratio of the BICM wiretap channel decreases to 0 when the input power increases to infinity. In future works, we will study the secrecy rate on the MIMO BICM wiretap channel where, because the SNR gap no longer remains constant, designing an optimal power allocation algorithm is a major challenge.

References

[1] C. E. Shannon,"Communication theory of secrecy systems," Bell Syst. Tech. J., vol. 28, pp. 656715, 1949.

[2] A. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355-1387, 1975.

[3] S. Lueng-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451-456, Jul. 1978.

[4] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, pp. 339348, May 1978.

[5] M. V. Dijk, "On a special class of broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 43, no. 2, pp. 712-714, Mar. 1997.

[6] P. K. Gopala, L. Lai and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687-4698, Oct. 2008.

[7] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515-2534, Jun. 2008.

[8] H. Joen, N. Kim, J. Choi, H. Lee and J. Ha, "Bounds on secrecy capacity over correlated Ergodic fading channels at high SNR," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, Apr., 2011.

[9] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 40054019, Sep. 2008.

[10] L. Dong, Z. Han, A. P. Petropulu and H. V. Poor, "Improving Wireless Physical Layer Security via Cooperating Relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, Mar. 2010.

[11] M. Abouelseoud and A. Nosratinia, "Opportunistic Wireless Relay Networks: Diversity-Multiplexing Tradeoff," vol. 57, no. 10, Oct. 2011.

[12] S. Bashar, Z. Ding and C. Xiao, "On secrecy rate analysis of MIMO wiretap channels driven by finite-alphabet input," *IEEE Trans. Commun.*, vol. 60, no. 12, pp. 3816-3825, Jan. 2012.

[13] W. Xiang, S. Le Goff, M. Jonston, K. Cumanan, "Signal mapping for bit-interleaved coded modulation schemes to achieve secure communications," *IEEE Wireless Comm. Lett.*, no. 4, issue 3, pp. 249-252, 2015.

[14] E. Agrell, J. Lassing, E. G. Ström, T. Ottosson, " On the optimality of the binary reflected Gray code." *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3170-3182, Dec. 2004.

[15] E. Zehavi, "8-PSK trellis codes for Rayleigh channel," *IEEE Trans. Commun.*, vol. 40, pp. 873-884, May 1992.

[16] G. Caire, G. Taricco and E. Biglieri, "Bit-interleaved coded modulation," *IEEE Trans. Commun.*, vol. 40, no. 3, pp. 927-946, May 1998.

[17] S. Y. Le Goff, "Signaling constellation for power-efficient bit-interleaved coded modulation schemes," *IEEE Trans. Inf. Theory*, vol. 49, no. 1, pp. 307-313, Jan. 2003.

[18] A. Chindapol and J. A. Ritcey, "Design, analysis and performance evaluation for BICM-ID with square QAM constellation in Rayleigh fading channels," *IEEE J. Sel. Areas Commun.*, vol. 19, pp. 944-957, May 2001.

[19] D. Guo, S. Shamai, S. Verdú, "Mutual information and minimum mean square error in Gaussian channels," *IEEE Trans. Inf. Theory*, no. 4, vol. 51, pp. 1261-1282, Apr. 2005.

[20] D. Guo, Y.Wu, S. S. Shitz and S. Verdú, Estimation in Gaussian Noise: Properties of the Minimum Mean-Square Error , *IEEE Transactions on Information Theory* Vol. 57, no. 4, Apr. 2011 .

[21] F. Schreckenbach, N. Görtz, J. Hagenauer, and G. Bauch, "Optimized symbol mappings for bit-interleaved coded modulation with iterative decoding," *IEEE Commun. Lett.*, vol. 7, no. 12, pp. 593-595, Dec. 2003.

[22] S. Pfletschinger and F. Sanzi, "Error floor removal for bit-interleaved coded modulation with iterative detection," *IEEE Trans. Wireless Commun.*, vol. 5, no. 11, pp. 3174-3181, Nov. 2006.

[23] 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.

[24] S. Verdú, "Spectral efficiency in the wideband regime," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1319-1343, Jun. 2002.

[25] A. Lonzano, A. M. Tulino, S. Verdú, "Optimal Power allocation for parallel Gaussian channels with arbitrary input distributions," *IEEE Inf. Theory*, no. 7, vol. 52, pp. 3033-3051, Jul. 2006

[26] V. Prelov and S. Verdú, "Second-order asymptotics of mutual information," *IEEE Trans. Inf. Theory*, vol. 50, no. 8, pp. 1567-1580, Aug. 2004.

[27] A.Martinez, A. G. i Fàbregas, G. Caire, F. M. J. Willems, "Bit-interleaved coded modulation in the wideband regime," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5447-5455, Dec. 2008.

[28] C. Stierstorfer and R. F. H. Fischer, Mappings for BICM in UWB scenarios, *7th International ITG Conference on Source and Channel Coding (SCC)*, Ulm, Germany, Jan. 2008.

[29] L. R. Varshney, "Transporting information and energy simultaneously," in Proc. *IEEE Int. Symp. Inf. Theory (ISIT)*, Toronto, Canada, Jul. 2008.

[30] L. Liu, R. Zhang and K. C. Chua, "Wireless information transfer with opportunistic energy harvesting," *IEEE Trans. Wireless Commun.*, 2012. Available at http://arxiv.org/abs/1204.2035.

[31] Z. Xiang and M. Tao, "Robust beamforming for wireless information and power transmission," *IEEE Wireless Commun. Lett.*, vol. 1, no. 4, pp. 372-375, 2012.

[32] L. Liu, R. Zhang and K. C. Chua, "Secrecy wireless information and power transfer with MISO beamforming," *IEEE Trans. Signal Process.*, vol. 62, no. 7, pp. 1850-1863, Apr. 2014.

[33] Dence, T., "Cubics, chaos and Newton's method", *Mathematical Gazette*, Mathematical Association , 1997,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2017.2749161, IEEE Transactions on Information Forensics and Security

Weichen Xiang received his BSc degree from Harbin Institute of Technology (Weihai), China, in 2009, his MSc degree in communications and signal processing from Newcastle University, in 2011. He received his Ph.D degree in wireless communication and physical layer security in 2016, from Newcastle University. From 2016-present, he worked as a senior engineer in TouchAir co. ltd. His research interests include information theory, physical layer security and energy harvesting.

Martin Johnston received his BSc (Hons) degree in Physics with Electronics from Birmingham University, UK, in 1999, his MSc degree in Electronic Engineering from Staffordshire University, UK, in 2001 and his PhD degree in 2006 from Newcastle University, UK. From 2006 - 2014 he worked as a Research Associate at the School of Electrical and Electronic Engineering in Newcastle University and he is now employed as a Lecturer. His research interests include the design of advanced error-correcting schemes and low-complexity decoding algorithms, physical-layer network coding and physical-layer security.

Stéphane Le Goff received the BSc, MSc, and PhD degrees, all in electrical engineering, from the Université de Bretagne Occidentale (University of Western Brittany), Brest, France, in 1990, 1991, and 1995, respectively. From 1995 to 1998, he worked as an Adjunct Lecturer at the *Institut Supérieur dElectronique de Bretagne*, a French college of electronic engineering, Brest. During 1999-2003, Dr. Le Goff was an Assistant Professor at the Etisalat College of Engineering, UAE. In 2003, he joined the Department of Physics and Electronics at the University of Waikato, Hamilton, New Zealand, as a Senior Lecturer in Electronics. Since March 2005, he has been a Lecturer in the School of Electrical and Electronic Engineering at Newcastle University, UK. Dr. Le Goff also held visiting positions at the Eastern Mediterranean University, Cyprus, during the academic year 1998-1999 and at the Sultan Qaboos University, Oman, in 2004. His research interests include information theory, channel coding, and wireless communication systems.