Physical Layer Security for Space Shift Keying Transmission With Precoding

Sina Rezaei Aghdam and Tolga M. Duman

***Abstract*—We investigate the effect of transmitter side channel state information on the achievable secrecy rates of space shift keying. Through derivation of the gradient of the secrecy rate, we formulate an iterative algorithm to maximize the achievable secrecy rates. We also introduce two lower complexity signal design algorithms for different scenarios based on the number of antennas at the eavesdropper. Our results illustrate the effectiveness of the proposed precoding techniques in attaining positive secrecy rates over a wide range of signal to noise ratios.**

***Index Terms*—Space shift keying, physical layer security, precoding, channel state information.**

I. Introduction

SPACE shift keying (SSK) represents a transmission method for low-complexity implementation of multiple-input-multiple-output (MIMO) wireless systems in which antenna indices are employed for data transmission. So as to realize an SSK transmission, a one-to-one mapping is established between blocks of information bits to be transmitted and the spatial position of the transmit antenna in the antenna array. At each time instance, among the multiple antennas at the transmitter, only one of them is activated and a reference signal is transmitted to the receiver. This signal goes through a generic wireless channel which plays the role of a modulation unit. Since the channels corresponding to different transmit-to-receive wireless links are different, it is possible to detect the index of the activated antenna with the aid of the channel state information (CSI) at the receiver [1].

SSK has many unique characteristics which makes it a promising candidate for future wireless systems. Along with the various studies on the performance and the applications of SSK [2], some attention has recently been devoted to its use in the context of physical layer security. Physical layer security is an alternative or a complement to the cryptographic schemes, which is capable of providing secrecy by taking advantage of the inherent randomness of the physical medium, including noise and channel fluctuations due to fading. Various secure transmission strategies have been introduced for point-to-point channels followed by generalizations to multiple-antenna systems in recent literature (e.g., see [3] and the references therein). A semi-analytical study of secrecy capacity of SSK with two transmit antennas has been provided in [4]. Authors in [5] have formulated the secrecy mutual information for spatial modulation (SM) for scenarios where the legitimate receiver and the eavesdropper are equipped with a single antenna. In [6], we have provided a more general study of SSK and SM in the context of physical layer security, where the achievable secrecy rates have been analyzed with an arbitrary number of antennas at the participating nodes. Among other related work, the authors in [7] and [8] have introduced the idea of employing precoding together with SM to attain positive secrecy rates along with a low complexity detection at the desired receiver. In [7], this enhanced secrecy is achieved by obtaining a precoder via solving an optimization problem, while an artificial noise-aided transmission is utilized in [8].

In this letter, we introduce secrecy-enhancing transmit signal design algorithms for SSK with the aid of the CSI. Unlike [7], where the optimization problem is defined according to a trade-off between the improvement of Bob's reception and the degradation of Eve's signal, we propose an iterative algorithm which directly maximizes the achievable secrecy rates. This approach is optimal, however the proposed iterative algorithm possesses a relatively high computational complexities. This is mainly due to the fact that the mutual information expression for SSK lacks a tractable and closed form. Hence, we further introduce two lower complexity transmit signal design algorithms.

We show through examples that, when Eve is equipped with a single antenna, it is possible to maximize her level of confusion. This can be done by simply mapping the SSK symbols to a single constellation point from eavesdropper's point of view. Different from the solution provided in [5] which does not satisfy any power constraints, we propose a transmit signal design scheme for which the transmit power does not change with respect to nonprecoded transmission. For scenarios where the number of antennas at the eavesdropper is larger than one, a low-complexity transmission algorithm is proposed which either maximizes the minimum Euclidean distance over the main channel or minimizes it over the eavesdropper's channel.

The letter is organized as follows. Section II illustrates the system model. The iterative algorithm for maximization of the secrecy rate is formulated and proposed in Section III. In Section IV, we introduce the low complexity transmit signal design schemes. Numerical results are provided in Section V, and the letter is concluded in Section VI.

II. System Model

We consider a MIMO wiretap channel with N_t antennas at the transmitter, Alice. The legitimate receiver, Bob, and the eavesdropper, Eve, are assumed to be equipped with N_{r_b} and N_{r_e} antennas, respectively. The received signals at Bob and Eve can be written as

$$\mathbf{y} = \mathbf{H_b X p} + \mathbf{n_y}, \tag{1}$$

$$\mathbf{z} = \mathbf{H_e X p} + \mathbf{n_z}, \tag{2}$$

respectively, where $\mathbf{X}$ is the $N_t \times N_t$ SSK signal matrix which is of the form $\mathbf{X} = diag(\{0, \ldots, 1, \ldots, 0\})$, with the position of "1" indicating the antenna being activated. $\mathbf{H_b}$ and $\mathbf{H_e}$ are the $N_{r_b} \times N_t$ and $N_{r_e} \times N_t$ channel matrices with independent fading coefficients from the transmitter to the legitimate receiver

Manuscript received August 5, 2015; revised December 15, 2015; accepted December 30, 2015. Date of publication January 7, 2016; date of current version April 7, 2016. This work was supported by the Scientific and Technical Research Council of Turkey (TUBITAK) under Grant #113E223. The associate editor coordinating the review of this paper and approving it for publication was K. K. Wong.

The authors are with the Department of Electrical Engineering, Bilkent University, Ankara TR-06800, Turkey (e-mail: aghdam@ee.bilkent.edu.tr; duman@ee.bilkent.edu.tr).

Digital Object Identifier 10.1109/LWC.2016.2515601

and to the eavesdropper, respectively. $\mathbf{n_y}$ and $\mathbf{n_z}$ are independent and identically distributed (i.i.d.) additive white Gaussian noise. It is assumed that the elements of the channel matrices and the noise follow circularly symmetric complex Gaussian distributions, $\mathcal{CN}(0,1)$ and $\mathcal{CN}(0,\sigma_n^2)$, respectively. $\mathbf{p}$ stands for the $N_t \times 1$ precoding vector. The fading process is ergodic and the channel gains corresponding to both channels remain constant during each coherence interval and vary independently from one interval to the next. Also, the coherence times are assumed to be large enough so that the random coding arguments can be applied as in [9].

Similar to various other studies in the literature, we employ the ergodic secrecy rate to characterize the secrecy behavior, which is given as [9]

$$\bar{R}_s = \mathbb{E}_{\mathbf{H_b},\mathbf{H_e}} \left(I(\mathbf{X};\mathbf{y}|\mathbf{H_b}) - I(\mathbf{X};\mathbf{z}|\mathbf{H_e}) \right)^+, \tag{3}$$

where $(a)^+ = \max(a,0)$ and transmit antennas are assumed to be equally likely to be activated, i.e., $P_X(X) = 1/N_t$. We assume that the instantaneous knowledge of $\mathbf{H}_b$ and $\mathbf{H}_e$ is available at the transmitter, which would be true for active eavesdroppers and also for the cases where the eavesdropper is a participating system user in a wireless system [3].

III. Precoding for Secrecy Rate Maximization

The average mutual information of SSK transmission, assuming $P_X(X) = 1/N_t$, is given by [6]

$$\mathbb{E}_{\mathbf{H}} I(\mathbf{X};\mathbf{y}|\mathbf{H}) = \log N_t - \frac{1}{N_t}\sum_{i=1}^{N_t} \mathbb{E}_{\mathbf{H},\mathbf{n}} \cdot \log \sum_{j=1}^{N_t} \exp\left(-\frac{\|\mathbf{H}\mathbf{E}_{ij}\mathbf{p} + \mathbf{n}\|^2 - \|\mathbf{n}\|^2}{\sigma_n^2} \right), \tag{4}$$

where $\mathbf{E}_{ij} = \mathbf{X}_i - \mathbf{X}_j$ and $\|.\|$ denotes the norm operation.

For a specific channel realization, we obtain the instantaneous mutual information as

$$I(\mathbf{X};\mathbf{y}|\mathbf{H}) = \log N_t - \mathbb{E}_{\mathbf{n}} \log \exp\left(\frac{\|\mathbf{n}\|^2}{\sigma_n^2} \right) - \frac{1}{N_t}\sum_{i=1}^{N_t} \mathbb{E}_{\mathbf{n}} \log \sum_{j=1}^{N_t} \exp\left(-\frac{\|\mathbf{H}\mathbf{E}_{ij}\mathbf{p} + \mathbf{n}\|^2}{\sigma_n^2} \right). \tag{5}$$

Accordingly, for specific realizations of $\mathbf{H}_b$ and $\mathbf{H}_e$, the secrecy rate can be written from (3) as

$$R_s = \frac{1}{N_t}\left(\sum_{i=1}^{N_t} \mathbb{E}_{\mathbf{n}_z} \log \sum_{j=1}^{N_t} \exp\left(-\frac{\|\mathbf{H}_e\mathbf{E}_{ij}\mathbf{p} + \mathbf{n}_z\|^2}{\sigma_{n_z}^2} \right) - \sum_{k=1}^{N_t} \mathbb{E}_{\mathbf{n}_y} \log \sum_{l=1}^{N_t} \exp\left(-\frac{\|\mathbf{H}_b\mathbf{E}_{kl}\mathbf{p} + \mathbf{n}_y\|^2}{\sigma_{n_y}^2} \right) \right)^+. \tag{6}$$

The objective is to solve the following optimization problem

$$\max_{\mathbf{p}} R_s \tag{7}$$

$$\text{subject to } \mathbf{p}^H\mathbf{p} \le N_t. \tag{8}$$

The Lagrangian corresponding to this problem can be constructed as

$$L(\mathbf{p},\theta) = -R_s(\mathbf{p}) + \theta\left(\mathbf{p}^H\mathbf{p} - N_t \right), \tag{9}$$

Algorithm 1. Gradient Descent for Maximizing R_s

Step 1: Initialize $\mathbf{p}_1$ with constraint $\mathbf{p}^H\mathbf{p} \le N_t$. Set step size u and minimum tolerance u_{min}.
Step 2: Set $k = 1$, compute $R_{s1} = R_s(\mathbf{p}_1)$ using (6).
Step 3: Compute $\nabla_{P_1} R_s(\mathbf{p})$.
Step 4: If $u \ge u_{min}$ goto Step 5, otherwise Stop algorithm and return $\mathbf{p}_k$.
Step 5: Calculate $\mathbf{p}'_k = \mathbf{p}_k + u\nabla_{\mathbf{p}_k} R(\mathbf{p})$. Normalize $\mathbf{p}'_k$ so that $\mathbf{p}^H\mathbf{p} \le N_t$ is satisfied.
Step 6: Compute $R' = R(\mathbf{p}'_k)$.
Step 7: If $R' \ge R_k$ update $R_{k+1} = R'$ and $\mathbf{p}_{k+1} = \mathbf{p}'_k$ and goto Step 8, otherwise let $u = 0.5u$ and goto Step 4.
Step 8: $k = k + 1$ goto Step 3.

where θ is the Lagrange multiplier. We solve the optimization problem in (7)–(8) numerically using the gradient descent method as illustrated in Algorithm 1.

The implementation of Algorithm 1 requires calculation of the gradient of R_s, which can be derived as

$$-\nabla_{\mathbf{p}} R_s(\mathbf{p}) + \theta\mathbf{p} = 0, \tag{10}$$

where

$$\nabla_{\mathbf{p}} R_s(\mathbf{p}) = \frac{1}{N_t}\left(\sum_{i=1}^{N_t} \mathbb{E}_{\mathbf{n}_z} \left(\frac{\sum_{j=1, j\ne i}^{N_t} -\nabla_{\mathbf{p}}\Psi_{e,ij}(\mathbf{p}) \exp\left(-\frac{\Psi_{e,ij}(\mathbf{p})}{\sigma_{n_z}^2} \right)}{\sigma_{n_z}^2 \ln 2 \sum_{j=1}^{N_t} \exp\left(-\frac{\Psi_{e,ij}(\mathbf{p})}{\sigma_{n_z}^2} \right)} \right) - \sum_{k=1}^{N_t} \mathbb{E}_{\mathbf{n}_y} \left(\frac{\sum_{l=1, l\ne k}^{N_t} -\nabla_{\mathbf{p}}\Psi_{b,kl}(\mathbf{p}) \exp\left(-\frac{\Psi_{b,kl}(\mathbf{p})}{\sigma_{n_y}^2} \right)}{\sigma_{n_y}^2 \ln 2 \sum_{l=1}^{N_t} \exp\left(-\frac{\Psi_{b,kl}(\mathbf{p})}{\sigma_{n_y}^2} \right)} \right) \right), \tag{11}$$

where

$$\Psi_{b,kl}(\mathbf{p}) = \|\mathbf{H}_b\mathbf{E}_{kl}\mathbf{p} + \mathbf{n}_y\|^2, \tag{12}$$

$$\Psi_{e,ij}(\mathbf{p}) = \|\mathbf{H}_e\mathbf{E}_{ij}\mathbf{p} + \mathbf{n}_z\|^2. \tag{13}$$

Using the definition of the complex gradient vector which is

$$[\nabla_{\mathbf{g}} f]_i = \frac{\partial f}{\partial [\mathbf{g}^*]_i}, \tag{14}$$

where the complex derivative of scalar function f is defined as

$$\frac{\partial f}{\partial g^*} = \frac{\partial Re\{f\}}{\partial g^*} + j\frac{\partial Im\{f\}}{\partial g^*}, \tag{15}$$

we obtain

$$\nabla_{\mathbf{p}}\Psi_{b,kl}(\mathbf{p}) = \mathbf{E}_{kl}^H\mathbf{H}_b^H\mathbf{H}_b\mathbf{E}_{kl}\mathbf{p} + \mathbf{E}_{kl}^H\mathbf{H}_b^H\mathbf{n}_y, \tag{16}$$

$$\nabla_{\mathbf{p}}\Psi_{e,ij}(\mathbf{p}) = \mathbf{E}_{ij}^H\mathbf{H}_e^H\mathbf{H}_e\mathbf{E}_{ij}\mathbf{p} + \mathbf{E}_{ij}^H\mathbf{H}_e^H\mathbf{n}_z. \tag{17}$$

By substituting these expressions in (11), we can numerically evaluate the gradient and implement a gradient descent algorithm. Algorithm 1 illustrates the iterative search for the optimal $\mathbf{p}$ using the gradient descent method which is guaranteed to converge to a local optimum. Hence, by repeating the algorithm with different initializations for $\mathbf{p}$, it is possible to obtain improved solutions.

IV. Low Complexity Precoding Schemes

The previous section developed the optimal precoding in Algorithm 1 which maximizes the secrecy rate. However, due to the need for many evaluations of the mutual information expression, which requires numerical evaluation of the expectation operator, Algorithm 1 is computationally complex. Hence, in this section, we propose precoding schemes which are of significantly lower complexity in the sense that their implementation are based on closed-form solutions. Both algorithms are based on the observation that, in the high SNR region, the term corresponding to the points with the minimum Euclidean distance is dominant in (6). Accordingly, modification of the received constellation vectors which results in an increased minimum Euclidean distance from Bob's point of view and a reduced minimum Euclidean distance at Eve can be an effective transmission scheme.

First, let us consider scenarios where eavesdropper is equipped with a single antenna. For these scenarios it is possible to apply precoding with the aid of the instantaneous knowledge on eavesdropper's channel, which results in zero information leakage to the eavesdropper. Consider $N_t = 2$, where we have $\mathbf{p} = [\rho_1\ \rho_2]^T$. Let $\rho_i = r_i \exp(j\phi_i)$. For this case, it is straightforward to find ρ_1 and ρ_2 such that

$$\rho_1 h_{e_1} = \rho_2 h_{e_2} \tag{18}$$

is satisfied. This increases Eve's confusion to the highest level, as the precoder maps the constellation points to a single point from the eavesdropper's point of view.

In order to solve (18), we substitute $r_1 = \sqrt{2 - r_2^2}$ and by letting $\frac{h_{e_2}}{h_{e_1}} = \lambda \exp(j\varphi)$, we obtain

$$\rho_1 = \sqrt{\frac{2\lambda^2}{1+\lambda^2}} \exp(j\varphi), \quad \rho_2 = \sqrt{\frac{2}{1+\lambda^2}}. \tag{19}$$

While the stated approach addresses the signal design for $N_t = 2$, for $N_t > 2$, the set of precoding coefficients can be found by repeatedly applying (19) as stated in Algorithm 2. We will show in Section V that, this algorithm which is of the complexity $\mathcal{O}(N_t^3)$ is capable of achieving maximum secrecy rate at sufficiently high SNR values.

Algorithm 2. Low-complexity Algorithm with ($N_{r_e} = 1$)

Step 1: Consider the set of all combinations of N_t as $\mathbf{i}$.
Step 2: For each combination, consider $\mathbf{h}_{e(i_1)}$ and $\mathbf{h}_{e(i_2)}$, namely i_1^{th} and i_2^{th} columns of $\mathbf{H}_e$, and obtain ρ_1 and ρ_2 using (19).
Step 3: Consider the precoded channel $\rho_1 \mathbf{h}_{e(i_1)} = \rho_2 \mathbf{h}_{e(i_2)} = \mathbf{h}_{\text{eff}}$.
Step 4: Apply (19) to $\mathbf{h}_{\text{eff}}$ and $\mathbf{h}_{e(i_3)}$.
Step 5: Repeat this procedure until all the points are mapped to a single point.
Step 6: Calculate the minimum Euclidean distance over the main channel for each combination and choose $\{\rho_1, \rho_2, \ldots, \rho_{N_t}\}$ corresponding to the combination which results in the maximum minimum Euclidean distance at Bob.

For the scenarios where $N_{r_e} > 1$, finding a precoding vector which results in zero mutual information over the eavesdropper's channel is not possible. Hence, we introduce a low-complexity alternative for Algorithm 1 by modifying the minimum Euclidean distances over the main channel as well as the eavesdropper's channel. Consider $N_t = 2$, where we have $\mathbf{p} = [\rho_1\ \rho_2]^T$. The term to be optimized can be written as [10]

$$\begin{aligned} d(r_1) &= \|\mathbf{H}\mathbf{E}_{12}\mathbf{p}\|^2 = \|\rho_1\mathbf{h}_1 - \rho_2\mathbf{h}_2\|^2 \\ &= \tau r_1^2 - (2\mu\cos(\psi_1 - \psi_2 + \phi))r_1\sqrt{2 - r_1^2} + 2\|\mathbf{h}_2\|^2, \end{aligned} \tag{20}$$

where $\mathbf{h}_2^H\mathbf{h}_1 = \mu\exp(j\phi)$ and $\|\mathbf{h}_1\|^2 - \|\mathbf{h}_2\|^2 = \tau$. In derivation of (20), we have used $r_2 = \sqrt{2 - r_1^2}$ which is a result of the constraint in (8). So as to derive the conditions under which $d(r_1)$ has a maximum or a minimum, we take the second derivative of (20) with respect to r_1, as

$$d''(r_1) = 2\tau - (4\mu\cos(\psi_1 - \psi_2 + \phi))\frac{\sqrt{2 - r_1^2}(r_1^3 - 3r_1)}{r_1^4 - 4r_1^2 + 4}. \tag{21}$$

By considering $\cos(\psi_1 - \psi_2 + \phi) = \pm 1$, the second term in (21) is dominant in determining the sign of $d''(r_1)$. In order for (20) to have a minimum, it is required that $\psi_1 - \psi_2 + \phi = 0$. On the other hand, so as to maximize (20), we need to consider $\psi_1 - \psi_2 + \phi = \pi$. By taking into the account these conditions, the optimal value of $d(r_1)$ can be obtained by setting the first derivative of (20) equal to zero, as

$$2\tau r_1 - (2\mu\cos(\psi_1 - \psi_2 + \phi))\frac{2 - 2r_1^2}{\sqrt{2 - r_1^2}} = 0. \tag{22}$$

Accordingly, the elements of the optimal $\mathbf{p}$ is attained as

$$\rho_1 = A\exp(j\psi_1), \quad \rho_2 = B\exp(j\psi_2), \tag{23}$$

where $d(r_1)$ is maximized with $A = (1 + \frac{\tau}{(4\mu^2+\tau^2)^{1/2}})^{1/2}$, $B = (1 - \frac{\tau}{(4\mu^2+\tau^2)^{1/2}})^{1/2}$ and $\psi_1 - \psi_2 + \phi = \pi$. Also, minimum of $d(r_1)$ is attained with $A = (1 - \frac{\tau}{(4\mu^2+\tau^2)^{1/2}})^{1/2}$, $B = (1 + \frac{\tau}{(4\mu^2+\tau^2)^{1/2}})^{1/2}$ and $\psi_1 - \psi_2 + \phi = 0$.

With the aid of the calculations above, we propose a low-complexity signal design algorithm as stated in Algorithm 3. More specifically, in Algorithm 3, the intention is to maximize the minimum Euclidean distance over the main channel (strategy 1) or to minimize it from Eve's point of view (strategy 2). At each time instance, after finding the precoding coefficients corresponding to these two strategies, transmitter selects the strategy which gives rise to a higher secrecy rate.

Algorithm 3. Low-complexity minimum Euclidean distance modification algorithm ($N_t = 2$, $N_{r_e} > 1$)

Step 1: Apply (23) to obtain $\mathbf{p}_1 = [\rho_1^{(b)}\rho_2^{(b)}]$ which maximizes (20).
Step 2: Apply (23) to obtain $\mathbf{p}_2 = [\rho_1^{(e)}\rho_2^{(e)}]$ which minimizes (20).
Step 3: Using (6), calculate the secrecy rates corresponding to $\mathbf{p}_1$ and $\mathbf{p}_2$ and select the precoder which gives rise to the higher R_s.

For the scenarios with $N_{r_e} > 1$ and $N_t > 2$, obtaining a closed-form precoder which maximizes or minimizes the minimum Euclidean distance is not straight forward. In these

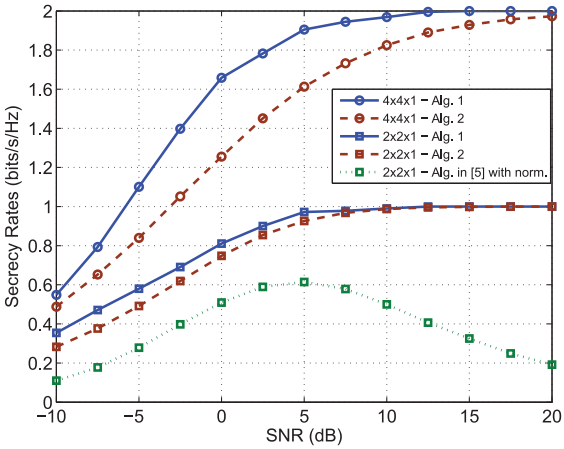

Fig. 1. Average secrecy rate for precoded SSK with $N_{r_e} = 1$.

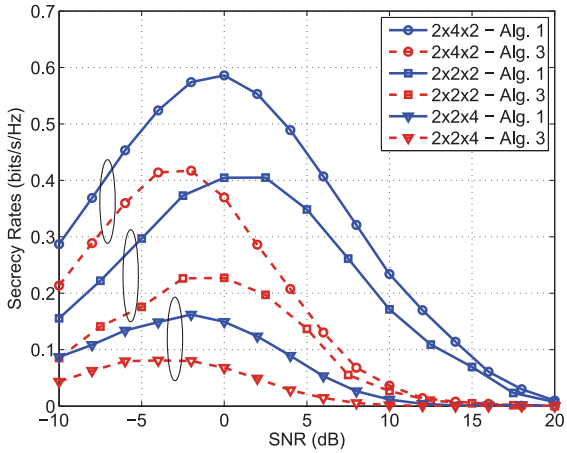

Fig. 2. Average secrecy rate for precoded SSK with $N_{r_e} > 1$.

scenarios, the maximization and the minimization in steps 1 and 2 of the Algorithm 3 can be done using the optimization proposed in [11, Eq. (8)]. Besides serving as low complexity transmit signal design schemes, the solutions attained from Algorithms 2 and 3 are appropriate candidates for initialization of Algorithm 1.

V. Numerical Results

In this section, we quantify the achievable secrecy rates for SSK using the proposed precoding techniques. Throughout the simulations, equal noise power is assumed at Bob and Eve. We consider independent identically distributed (i.i.d.) Rayleigh channel coefficients for the main channel and the eavesdropper's channel, and evaluate the achievable secrecy rates by averaging (3) over many channel realizations.

Figure 1 denotes the achievable secrecy rates with the aid of the proposed algorithms when the eavesdropper is equipped with a single antenna. An increased secrecy rate is achieved with a higher number of transmit antennas as the rate is increased over the main channel while the transmission rate over the eavesdropper's channel is restricted as a result of the precoding in Algorithms 1 and 2. Figure 1 also compares the performance of the algorithms proposed with that of the scheme in [5]. Clearly, the newly proposed algorithms considerably outperform the precoding scheme in [5], when an additional normalization is carried out on the precoding coefficients obtained to satisfy (8).

Figure 2 illustrates that, in scenarios where the eavesdropper has more than one antenna, the proposed precoding schemes are not capable of providing positive secrecy rates for high SNRs. This is because, neither of the precoding schemes in Algorithms 1 and 3 have the capability to realize a transmission with no leakage over the eavesdropper's channel. Accordingly, when SNR is sufficiently high, the mutual information over the eavesdropper's channel will also approach the saturation value of $\log N_t$ which results in zero secrecy rate.

The numerical results provided in Fig. 1 and Fig. 2 reveal the gap between Algorithm 1 and its low complexity alternatives, Algorithms 2 and 3. Finally, we compare the CPU times associated with the implementation of each of the proposed algorithms for a given realization of $\mathbf{H}_b$ and $\mathbf{H}_e$. We assume that Algorithm 1 is repeated with 10 initializations and expectations are estimated using 1000 samples. Table I clearly shows that the computational complexities associated with Algorithms 2 and 3 are notably less than that of Algorithm 1.

TABLE I
CPU Times (Intel Core-i7-4770, 3.4 GHz)

$N_t \times N_{r_b} \times N_{r_e}$	Alg. 1	Alg. 2	Alg. 3
$2 \times 1 \times 1$	2.4476 (s)	0.1299 (s)	–
$2 \times 2 \times 2$	3.0647 (s)	–	0.1386 (s)

VI. Conclusions

We have examined the secrecy rate enhancements that can be attained by applying CSI aided transmit signal design algorithms in SSK transmission. We have formulated and solved an optimal iterative algorithm along with two low complexity precoding algorithms. The results demonstrate that the proposed precoding schemes are capable of providing positive secrecy over a relatively wide range of SNR values.

References

[1] J. Jeganathan, A. Ghrayeb, L. Szczecinski, and A. Ceron, "Space shift keying modulation for MIMO channels," *IEEE Trans. Wireless Commun.*, vol. 8, no. 7, pp. 3692–3703, Jul. 2009.

[2] M. Di Renzo, H. Haas, A. Ghrayeb, S. Suguira, and L. Hanzo, "Spatial modulation for generalized MIMO: Challenges, opportunities and implementation," *Proc. IEEE*, vol. 102, no. 1, pp. 56–103, Jan. 2014.

[3] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, Jan. 2014.

[4] M. Di Renzo, H. Haas, N. Serafimovski, and S. Sinanovic, "Secrecy capacity of space keying with two antennas," *IEEE Veh. Technol. Conf.*, 2012, pp. 1–5.

[5] X. Guan, Y. Cai, and W. Yang, "On the secrecy mutual information of spatial modulation with finite alphabet," in *Proc. IEEE Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Oct. 2012, pp. 1–4.

[6] S. Rezaei Aghdam, T. M. Duman, and M. Di Renzo, "On secrecy rate analysis of spatial modulation and space shift keying," *IEEE Int. Black Sea Conf. Commun. Netw. (BlackSeaCom)*, May 2015, pp. 63–67.

[7] F. Wu, R. Zhang, L.-L. Yang, and W. Wang, "Transmitter precoding aided spatial modulation for secrecy communications," *IEEE Trans. Veh. Technol.*, vol. PP, no. 99, pp. 1–6, Jan. 2015.

[8] F. Wu, L.-L. Yang, W. Wang, and R. Zhang, "Secret precoding-aided spatial modulation," *IEEE Commun. Lett.*, vol. 19, no. 9, pp. 1544–1547, Sep. 2015.

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

[10] M. Maleki, H. Bahrami, S. Beygi, M. Kafashan, and N. H. Tran, "Space modulation with CSI: Constellation design and performance evaluation," *IEEE Trans. Veh. Technol.*, vol. 62, no. 4, pp. 1623–1634, May 2013.

[11] M.-C. Lee, W.-H. Chung, and T.-S. Lee, "Generalized precoder design formulation and iterative algorithm for spatial modulation in MIMO systems with CSIT," *IEEE Trans. Commun.*, vol. 63, no. 4, pp. 1230–1244, Apr. 2015.