Investigation of STEEP Using Phase-Shift-Keying Signaling for Secure Communications

Moontasir Rafique and Yingbo Hua

***Abstract*—Secret-message transmission by echoing encrypted probes (STEEP) using phase-shift-keying (PSK) constellation of asymmetric sizes is investigated, and compared with a prior scheme which is limited to binary signaling. While both schemes can yield positive secrecy rates over a wiretap channel with eavesdropping channel being stronger than user's, PSK-STEEP is more general and results in higher secrecy rates than the prior scheme. The secrecy rate of PSK-STEEP is shown to be increasing with the size of PSK constellation in phase 1 but is maximized by a binary PSK constellation in phase 2.**

***Index Terms*—Secure communication, physical-layer security.**

I. Introduction

Secure communications between two nodes (or users) with limited pre-shared secrecy is an important problem, for which the existing solutions fall under two broad categories. One is known as cryptography, which is largely based on certain functions that are computationally hard (but not impossible) to invert. The other is physical layer security, which is based on information-theoretic security and is unbreakable by computation. This paper is concerned about the latter.

The problems of physical layer security are typically divided into two groups: wire-tap channel (WTC) problems since Wyner's work in 1970s [1], and secret-key generation (SKG) problems since Maurer's work in 1990s [2]. Although the benefits from solving WTC and SKG problems can be both quantified by a common measure such as the number of secret bits mutually established by two nodes against an eavesdropper (Eve), most works on WTC continue to require Eve's channel to be weaker (at least in some time windows) than users' in terms of channel gains and/or number of antennas [3], and most works on SKG continue to require reciprocal and randomly fading channels between users [4]. Very little of the synergy between WTC and SKG has been exploited until recent years [5]-[11].

The two-way scheme in [5]-[6] and the scheme called "secret-message transmission by echoing encrypted probes (STEEP)" in [8]-[11] are related. But the former scheme is limited to binary signaling while the latter is much more general and includes the former as a special case. STEEP is a round-trip scheme with two phases of transmission: a probing phase (phase 1) from node 1 to node 2, and an echoing phase (phase 2) from node 2 to node 1. Inspired by SKG capacity and an encryption lemma [8], STEEP enables an application of WTC coding in phase 2 to achieve a positive secrecy rate, under an asymmetric power allocation, even if Eve's receive channel is constantly stronger than user's. Unlike numerous prior works such as [12], [13], STEEP does not need secure feedback channel, or require legitimate users to know Eve's channel; nor does STEEP require full-duplex or collaborative 3rd party.

In this paper, we dive deeper into a special case of STEEP where asymmetric phase-shift-keying (PSK) signaling is used in phases 1 and 2. One advantage of PSK is its tolerance to nonlinearity of amplifiers and/or channels. We will start with a description of the WTC system of interest and PSK-STEEP, followed by secrecy analysis of PSK-STEEP and a revisit of the prior scheme in [6]. The secrecy performances of the two schemes are compared via simulation results based on selected cases and satellite channel models.

II. Round-Trip WTC System

Let us consider a round-trip WTC system as follows. Let $x_1(k_1)$ be the signal transmitted by node 1 in phase 1, and the corresponding signals received by node 2 and Eve are respectively

$$y_1(k_1) = x_1(k_1) + w_1(k_1), \tag{1}$$

$$y_{E1}(k_1) = x_1(k_1) + w_{E1}(k_1). \tag{2}$$

Let $x_2(k_2)$ be the signal transmitted by node 2 in phase 2, and the corresponding signals received by node 1 and Eve are respectively

$$y_2(k_2) = x_2(k_2) + w_2(k_2), \tag{3}$$

$$y_{E2}(k_2) = x_2(k_2) + w_{E2}(k_2). \tag{4}$$

The sample indices k_1 and k_2 for phases 1 and 2 respectively will be dropped for notational convenience. But our discussion will mostly refer to an arbitrary $k_1 \in \{1, \cdots, K\}$ and the corresponding $k_2 = k_1$. We will also assume a sufficiently large K for the validity of secrecy rate to be discussed.

Here all channels are SISO AWGN channels. Without loss of generality, all channel gains are normalized to be one, but the (zero-mean) noises w_1, w_2, w_{E1} and w_{E2} have the variances σ_1^2, σ_2^2, σ_{E1}^2 and σ_{E2}^2 respectively. We will denote the PDF of the circular complex Gaussian distributed

Department of ECE, Univ. of California at Riverside, Riverside, CA, 92521 USA. Emails: moontasir.rafique@email.ucr.edu, yhua@ece.ucr.edu. This work was supported in part by the U.S. Department of Defense under the Agreement W911NF-20-2-0267.

random variable X with mean m and variance σ^2 by $\mathcal{CN}_x(m,\sigma^2)=\frac{1}{\pi\sigma^2}\exp\left(-\frac{|x-m|^2}{\sigma^2}\right)$.

In all conventional WTC coding schemes [3], there is no dependency between x_1 and x_2. In this case, the achievable secrecy rate in each phase is zero if $\alpha_1\doteq\sigma_1^2/\sigma_{E1}^2\geq 1$ and $\alpha_2\doteq\sigma_2^2/\sigma_{E2}^2\geq 1$.

Unlike all conventional WTC schemes, STEEP is a round-trip scheme where node 2 chooses x_2 as an encrypted function of x_1. The secret used by node 2 to encrypt this function is meant to be received by node 1 after the transmission in phase 2.

III. PSK Based STEEP

In this work, we assume that x_1 is a random symbol of unit power from M_1-PSK constellation $\mathcal{C}_{M_1}$. Furthermore, x_2 is defined to be (a multiplicative encryption of s_2 by $\tilde{x}_1$)

$$x_2=\tilde{x}_1 s_2 \tag{5}$$

where $\tilde{x}_1$ is the MMSE estimate of x_1 from y_1, and s_2 is a random (secret) symbol of unit power from M_2-PSK constellation $\mathcal{C}_{M_2}$. It is known that

$$\tilde{x}_1=\mathbb{E}\{x_1|y_1\}=\frac{\sum_{x_1\in\mathcal{C}_{M_1}}x_1 f(y_1|x_1)}{\sum_{x_1\in\mathcal{C}_{M_1}}f(y_1|x_1)}\doteq G(y_1). \tag{6}$$

Here $f(y_1|x_1)$ denotes the PDF of y_1 given x_1, i.e., $\mathcal{CN}_{y_1}(x_1,\sigma_1^2)$. We will also consider the following choice of x_2:

$$x_2=\tilde{x}_1' s_2 \tag{7}$$

where $\tilde{x}_1'$ is the LMMSE estimate of x_1 from y_1, i.e.,

$$\tilde{x}_1'=y_1/(1+\sigma_1^2)\doteq G'(y_1). \tag{8}$$

IV. Secrecy Rate Analysis of PSK-STEEP

Applying the established WTC theory to the above transmission in phase 2, an achievable secrecy rate from node 2 to node 1 via WTC coding on s_2 is

$$\begin{aligned}C_s&\overset{a}{=}\mathbb{I}(s_2;x_1,y_2)-\mathbb{I}(s_2;\mathbf{y}_E)\overset{b}{=}\mathbb{I}(s_2;y_2|x_1)-\mathbb{I}(s_2;\mathbf{y}_E)\\&=\mathbb{H}(s_2|\mathbf{y}_E)-\mathbb{H}(s_2|x_1,y_2)\end{aligned} \tag{9}$$

where $\mathbf{y}_E=[y_{E1},y_{E2}]^T$. Note that x_1 is unknown to node 2 but known to node 1 (used for $\overset{a}{=}$), and is independent of s_2 (used for $\overset{b}{=}$). Since the transmission of each sample of s_2 from node 2 requires a sample of x_1 previously transmitted from node 1, the above C_s is in (secret) bits per round-trip sample interval. It follows from (9) that

$$\begin{aligned}C_s=&-\mathbb{E}_{\mathbf{y}_E}\{\sum_{s_2\in\mathcal{C}_{M_2}}p(s_2|\mathbf{y}_E)\log p(s_2|\mathbf{y}_E)\}\\&+\mathbb{E}_{x_1,y_2}\{\sum_{s_2\in\mathcal{C}_{M_2}}p(s_2|x_1,y_2)\log p(s_2|x_1,y_2)\}.\end{aligned} \tag{10}$$

Here

$$p(s_2|\mathbf{y}_E)=\frac{f(\mathbf{y}_E|s_2)}{\sum_{s_2\in\mathcal{C}_{M_2}}f(\mathbf{y}_E|s_2)} \tag{11}$$

where $f(\mathbf{y}_E|s_2)=\frac{1}{M_1}\sum_{x_1\in\mathcal{C}_{M_1}}f(y_{E1}|x_1)f(y_{E2}|x_1,s_2)$, $f(y_{E1}|x_1)$ is $\mathcal{CN}_{y_{E1}}(x_1,\sigma_{E1}^2)$, and $f(y_{E2}|x_1,s_2)=\mathbb{E}_{w_1}\{\mathcal{CN}_{y_{E1}}(G(x_1+w_1)s_2,\sigma_{E2}^2)\}$. Furthermore,

$$p(s_2|x_1,y_2)=\frac{f(y_2|x_1,s_2)}{\sum_{s_2\in\mathcal{C}_{M_2}}f(y_2|x_1,s_2)} \tag{12}$$

with $f(y_2|x_1,s_2)=\mathbb{E}_{w_1}\{\mathcal{CN}_{y_2}(G(x_1+w_1)s_2,\sigma_2^2)\}$.

In [6], both M_1 and M_2 are limited to be 2, and $\tilde{x}_1$ in (5) is chosen to be a binary hard decision on x_1. While both hard and soft decisions at Eve are considered in [6], they also assume that node 2 only makes a binary hard decision on s_2.

The above described C_s in (10) for PSK-STEEP with any $M_1\geq 2$ and $M_2\geq 2$ is based on soft-decision at both node 1 and Eve, i.e., for each symbol of s_2, node 1 and Eve yield $p(s_2|x_1,y_2)$ and $p(s_2|\mathbf{y}_E)$ respectively. And the final decoding of the packet containing a stream of s_2 symbols is based on $p(s_2|x_1,y_2)$ at user 1, or on $p(s_2|\mathbf{y}_E)$ at Eve.

To make a comprehensive comparison with [6], we will also examine the situations where node 1 and/or Eve make a hard decision on each symbol of s_2 for $M_2=2$. Note that PSK-STEEP always chooses an estimate of x_1 (rather than a hard decision on x_1) by node 2 in phase 1 for any $M_1\geq 2$, which is in contrast to [6] where only $M_1=2$ is chosen and only hard decision on x_1 is made by node 2 in phase 1.

A. For $M_2=2$

Let $p_{e|E}$ be the error rate of making (optimal) hard decision on s_2 by Eve using $\mathbf{y}_E$, and $p_{e|U}$ be the error rate of making (optimal) hard decision on s_2 by user 1 using x_1 and y_2. Also let

$$\mathtt{h}(p)\doteq -p\log p-(1-p)\log(1-p). \tag{13}$$

If Eve applies hard decision on each s_2, then $\mathbb{H}(s_2|\mathbf{y}_E)$ in (10) should be replaced by $\mathtt{h}(p_{e|E})$. Similarly, if node 1 (or user 1) applies hard decision on each s_2, then $\mathbb{H}(s_2|x_1,y_2)$ in (10) should be replaced by $\mathtt{h}(p_{e|U})$.

It should be clear that $\mathbb{H}(s_2|\mathbf{y}_E)>\mathtt{h}(p_{e|E})$ if and only if $|p(s_2|\mathbf{y}_E)-\frac{1}{2}|<|p_{e|E}-\frac{1}{2}|$. And a similar statement applies to $\mathbb{H}(s_2|x_1,y_2)$ vs $\mathtt{h}(p_{e|U})$.

1) Secrecy rate of PSK-STEEP for $M_2=2$: If the hard decision is made at both node 1 and Eve, then (10) is replaced by

$$C_{s,P,H,H}=\mathtt{h}(p_{e|E})-\mathtt{h}(p_{e|U}). \tag{14}$$

Here $_P$ denotes PSK-STEEP, and $_{H,H}$ denotes hard decisions at node 1 and Eve.

If the hard decision is made at node 1 but soft decision is made at Eve, then (10) is replaced by

$$C_{s,P,H,S}=\mathbb{E}_{\mathbf{y}_E}\left\{\mathtt{h}(\epsilon_E(\mathbf{y}_E))\right\}-\mathtt{h}(p_{e|U}) \tag{15}$$

where $\epsilon_E(\mathbf{y}_E)=p(s_2|\mathbf{y}_E)_{s_2=1}$ which is (11) with $s_2=1$ and $M_2=2$. Note that $\mathcal{C}_2=\{1,-1\}$.

If the soft decision is made at both node 1 and Eve, (10) is replaced by

$$C_{s,P,S,S} = \mathbb{E}_{y_E}\left\{\mathrm{h}(\epsilon_E(y_E))\right\} - \mathbb{E}_{x_1,y_1}\left\{\mathrm{h}(\epsilon_U(x_1,y_1))\right\} \tag{16}$$

where $\epsilon_U(x_1,y_1) = p\left(s_2|x_1,y_2\right)_{s_2=1}$ which is (12) with $M_2 = 2$.

If the soft decision is made at node 1 but hard decision is made at Eve, then (10) is replaced by

$$C_{s,P,S,H} = \mathrm{h}(p_{e|E}) - \mathbb{E}_{x_1,y_2}\left\{\mathrm{h}(\epsilon_U(x_1,y_2))\right\}. \tag{17}$$

2) Maximum likelihood decision at node 1: The (optimal) hard decision $\hat{s}_{2|U}$ on s_2 at node 1 is the maximum likelihood decision, i.e.,

$$\hat{s}_{2|U} = arg \max_{s_2 \in \mathcal{C}_{M_2}} f(y_2|x_1,s_2), \tag{18}$$

where $f(y_2|x_1,s_2) = \mathbb{E}_{w_1}\{\mathcal{CN}_{y_2}(G(x_1+w_1)s_2,\sigma_2^2)\}$.

If the MMSE estimate $G(y_1)$ of x_1 is replaced by the LMMSE estimate $G'(y_1)$ of x_1, then $f(y_2|x_1,s_2) = \mathcal{CN}_{y_2}\left(\frac{1}{1+\sigma_1^2}x_1s_2, \frac{\sigma_1^2}{1+\sigma_1^2}+\sigma_2^2\right)$.

3) Maximum likelihood decision at Eve: The (optimal) hard decision $\hat{s}_{2|E}$ on s_2 by Eve using $\mathbf{y}_E$ is the following maximum likelihood decision:

$$\hat{s}_{2|E} = arg \max_{s_2 \in \mathcal{C}_{M_2}} f(\mathbf{y}_E|s_2) \tag{19}$$

where

$$\begin{aligned} &f(\mathbf{y}_E|s_2) = f(y_{E1},y_{E2}|s_2) \\ &= \mathbb{E}_{x_1,w_1}\{f(y_{E1}|x_1)f(y_{E2}|G(x_1+w_1)s_2)\} \\ &= \frac{1}{M_1}\mathbb{E}_{w_1}\{\sum_{x_1\in\mathcal{C}_{M_1}} f(y_{E1}|x_1)f(y_{E2}|G(x_1+w_1)s_2)\} \end{aligned}$$

with $f(y_{E1}|x_1) = \mathcal{CN}_{y_{E1}}(x_1,\sigma_{E1}^2)$ and $f(y_{E2}|G(x_1+w_1)s_2) = \mathcal{CN}(G(x_1+w_1)s_2,\sigma_{E2}^2)$.

If the MMSE estimate $G(y_1)$ is replaced by the LMMSE estimate $G'(y_1)$, then

$$y_{E2} = \tilde{x}_1's_2 + w_{E2} = \frac{1}{1+\sigma_1^2}x_1s_2 + \frac{1}{1+\sigma_1^2}w_1s_2 + w_{E2}$$

and hence

$$\begin{aligned} f(\mathbf{y}_E|s_2) = &\frac{1}{M_1}\sum_{x_1\in\mathcal{C}_{M_1}} \mathcal{CN}_{y_{E1}}(x_1,\sigma_{E1}^2) \\ &\cdot \mathcal{CN}_{y_{E2}}\left(\frac{1}{1+\sigma_1^2}x_1s_2, \frac{\sigma_1^2}{1+\sigma_1^2}+\sigma_{E2}^2\right). \end{aligned} \tag{20}$$

V. Revisit of the Protocol in [6]

In order to have a precise comparison between our PSK-STEEP and the scheme in [6], let us revisit the latter below.

In phase 1, node 1 sends a sequence of binary symbols $(-1)^{b_1} \in \{1,-1\}$ (or equivalently $b_1 \in \{0,1\}$), and node 2 and Eve receive $y_1 = (-1)^{b_1} + w_1'$ and $y_{E1} = (-1)^{b_1} + w_{E1}'$ respectively. Also node 2 makes a binary decision $\hat{b}_1$ on b_1 based on y_1. The decision error is

$$p_e = Q\left(1/\sigma_1'\right) \tag{21}$$

Here w_1' and w_{E1}' are equivalent to the real parts of w_1 and w_{E1} respectively. Then $\sigma_1'^2 = \frac{1}{2}\sigma_1^2$.

In phase 2, node 2 generates a uniform binary bit $b_2 \in \{0,1\}$, and transmits $\hat{b}_1 \oplus b_2$ (Exclusive OR) via public channel. So, node 1 can make a decision on b_2 by computing $\hat{b}_2 = b_1 \oplus \hat{b}_1 \oplus b_2 = \Delta b_1 \oplus b_2$ with $\Delta b_1 = b_1 \oplus \hat{b}_1$. The error rate of $\hat{b}_2$ is the same as that of $\hat{b}_1$, which is p_e as shown above.

As discussed next, two options of decision on b_2 at Eve are considered in [6].

A. Hard decision on b_2 at Eve

The optimal hard decision $\hat{b}_{2|E}$ on b_2 by Eve is based on her knowledge of $y_{E1} = b_1 + w_{E1}$ and $b \doteq \hat{b}_1 \oplus b_2 = \Delta b_1 \oplus b_1 \oplus b_2$. It follows that

$$\hat{b}_{2|E} = arg \max_{b_2} f(y_{E1},b|b_2) \tag{22}$$

where $f(y_{E1},b|b_2)$ is the joint (probability-density and probability) distribution of y_{E1} and b given b_2. We know

$$\begin{aligned} &f(y_{E1},b|b_2) = \sum_{b_1} f(y_{E1},b,b_1|b_2) = \frac{1}{2}\sum_{b_1} f(y_{E1},b|b_1,b_2) \\ &= \frac{1}{2}\sum_{b_1} p(b|b_1,b_2)f(y_{E1}|b_1). \end{aligned} \tag{23}$$

Here $p(0|b_1,b_2) = p_e$ if $b_1 \neq b_2$, $p(0|b_1,b_2) = 1-p_e$ if $b_1 = b_2$, and $f(y_{E1}|b_1) = \mathcal{N}\left((-1)^{b_1},\sigma_{E1}'^2\right)$. Hence

$$\begin{aligned} &f(y_{E1},b|b_2) = \frac{1}{2}\left[p(b|0,b_2)f(y_{E1}|0) + p(b|1,b_2)f(y_{E1}|1)\right] \\ &= \frac{1}{2}\begin{cases} A, & (b,b_2) = (1,0),(0,1); \\ B, & (b,b_2) = (1,1),(0,0); \end{cases} \end{aligned} \tag{24}$$

where $A = p_e f(y_{E1}|0) + (1-p_e)f(y_{E1}|1)$ and $B = (1-p_e)f(y_{E1}|0) + p_e f(y_{E1}|1)$.

Let $p'_{e|E} = \mathtt{P}\{\hat{b}_{2|E} \neq b_2\}$ where $\mathtt{P}$ denotes the probability of a condition. Then

$$\begin{aligned} p'_{e|E} &= \mathtt{P}\{\hat{b}_{2|E} = 1|b_2 = 0\} \\ &= \mathtt{P}\{\hat{b}_{2|E} = 1|b = 0,b_2 = 0\}\mathtt{P}\{b = 0|b_2 = 0\} \\ &\quad + \mathtt{P}\{\hat{b}_{2|E} = 1|b = 1,b_2 = 0\}\mathtt{P}\{b = 1|b_2 = 0\}. \end{aligned} \tag{25}$$

Since b_1 is uniform, so is $b = \Delta b_1 \oplus b_1 \oplus b_2$ given b_2, i.e., $\mathtt{P}\{b = 0|b_2 = 0\} = \mathtt{P}\{b = 1|b_2 = 0\} = \frac{1}{2}$. Hence,

$$\begin{aligned} p'_{e|E} &= \frac{1}{2}\mathtt{P}\{\hat{b}_{2|E} = 1|b = 0,b_2 = 0\} \\ &\quad + \frac{1}{2}\mathtt{P}\{\hat{b}_{2|E} = 1|b = 1,b_2 = 0\} \\ &= \frac{1}{2}\mathtt{P}\left\{A > B|b = 0,b_2 = 0\right\} + \frac{1}{2}\mathtt{P}\{A < B|b = 1,b_2 = 0\}. \end{aligned} \tag{26}$$

TABLE I: Key features of PSK-STEEP and a prior scheme in [6]

Methods	M_1	M_2	Decision at node 2 in phase 1	Decision at node 1 in phase 2	Decision at Eve	Power from node 2 in phase 2
[6]	2	2	hard	hard	hard or soft	unlimited
PSK-STEEP	≥ 2	≥ 2	soft (MMSE or LMMSE)	hard or soft	hard or soft	limited or unlimited

Assuming $p_e < \frac{1}{2}$, we have

$$p'_{e|E} = \frac{1}{2}\mathtt{P}\{f(y_{E1}|1) > f(y_{E1}|0)|b=0, b_2=0\} + \frac{1}{2}\mathtt{P}\{f(y_{E1}|0) > f(y_{E1}|1)|b=1, b_2=0\}, \quad (27)$$

Here

$$\begin{aligned}&\mathtt{P}\{f(y_{E1}|1) > f(y_{E1}|0)|b=0, b_2=0\}\\ &= (1-p_e)\mathtt{P}\{f(y_{E1}|1) > f(y_{E1}|0)|b=0, b_1=0, b_2=0\}\\ &\quad + p_e\mathtt{P}\{f(y_{E1}|1) > f(y_{E1}|0)|b=0, b_1=1, b_2=0\}\\ &= (1-p_e)p_{e,E1} + p_e(1-p_{e,E1}) \quad (28)\end{aligned}$$

and

$$\begin{aligned}&\mathtt{P}\{f(y_{E1}|0) > f(y_{E1}|1)|b=1, b_2=0\}\\ &= p_e\mathtt{P}\{f(y_{E1}|0) > f(y_{E1}|1)|b=1, b_1=0, b_2=0\}\\ &\quad + (1-p_e)\mathtt{P}\{f(y_{E1}|0) > f(y_{E1}|1)|b=1, b_1=1, b_2=0\}\\ &= p_e(1-p_{e,E1}) + (1-p_e)p_{e,E1}. \quad (29)\end{aligned}$$

where $p_{e,E1}$ is the error rate of the hard decision on b_1 using y_{E1}. Therefore,

$$p'_{e|E} = p_e(1-p_{e,E1}) + (1-p_e)p_{e,E1}. \quad (30)$$

This is the error rate of optimal hard-decision on b_2 by Eve based on y_{E1} and b without explicit hard decision on b_1. But the above result shows that the (optimal) hard decision on b_2 using y_{E1} and b automatically implies the (optimal) hard decision on b_1 using y_{E1}.

The secrecy rate of the above protocol is

$$\begin{aligned}C_{s,p} &= \mathbb{I}(b_1, b; b_2) - \mathbb{I}(y_{E1}, b; b_2)\\ &= [\mathbb{H}(b_2) - \mathbb{H}(b_2|b_1, b)] - [\mathbb{H}(b_2) - \mathbb{H}(b_2|y_{E1}, b)]\\ &= \mathbb{H}(b_2|y_{E1}, b) - \mathbb{H}(b_2|b_1, b) \quad (31)\end{aligned}$$

Here $\mathbb{H}(b_2|b_1, b) = \mathbb{H}(b_2 \oplus b_1 \oplus b|b_1, b) = \mathbb{H}(\Delta b_1|b_1, b) = \mathbb{H}(\Delta b_1) = \mathbb{H}(\hat{b}_1)$.

If we replace "b_2 given y_{E1} and b" by the hard decision $\hat{b}_{2,E}$, then

$$C_{s,p,hard} \doteq \mathbb{H}(\hat{b}_{2|E}) - \mathbb{H}(\hat{b}_1) = \mathtt{h}(p'_{e|E}) - \mathtt{h}(p_e). \quad (32)$$

Here $C_{s,p,hard}$ is based on hard decision at both nodes 1 and 2 as well as hard decision at Eve.

B. Soft Decision on b_2 at Eve

The soft decision on b_2 at Eve is the determination of the probability of b_2 given y_{E1} and b, which is

$$p(b_2|y_{E1}, b) = \frac{\sum_{b_1} f(y_{E1}|b, b_1, b_2)p(b|b_1, b_2)}{\sum_{b_1} f(y_{E1}|b, b_1)} \quad (33)$$

where we have used $p(b_1) = p(b_2) = \frac{1}{2}$ and $p(b|b_1) = \frac{1}{2}$. Also note $f(y_{E1}|b, b_1, b_2) = f(y_{E1}|b, b_1) = f(y_{E1}|b_1) = \mathcal{N}((-1)^{b_1}, \sigma'^2_{E1})$. Hence,

$$\begin{aligned}p(0|y_{E1}, b) &= \frac{f(y_{E1}|0)p(b|0,0) + f(y_{E1}|1)p(b|1,0)}{f(y_{E1}|0) + f(y_{E1}|1)}\\ &= \begin{cases}\frac{(1-p_e)f(y_{E1}|0)+p_e f(y_{E1}|1)}{f(y_{E1}|0)+f(y_{E1}|1)} \doteq \epsilon'_E(y_{E1}), & b=0;\\ \frac{p_e f(y_{E1}|0)+(1-p_e)f(y_{E1}|1)}{f(y_{E1}|0)+f(y_{E1}|1)} \doteq 1-\epsilon'_E(y_{E1}), & b=1.\end{cases}\end{aligned}$$

Note that $p(1|y_{E1}, b) = 1 - p(0|y_{E1}, b)$. It follows that

$$\begin{aligned}\mathbb{H}(b_2|y_{E1}, b) &= \mathbb{E}\{-\sum_{b_2} p(b_2|y_{E1}, b)\log p(b_2|y_{E1}, b)\}\\ &= \mathbb{E}\{-\sum_{b_2} p(b_2|y_{E1}, 0)\log p(b_2|y_{E1}, 0)\}\\ &= \mathbb{E}\{\mathtt{h}(\epsilon'_E(y_{E1}))\}. \quad (34)\end{aligned}$$

Then the secrecy rate of the above protocol subject to soft-decision at Eve is

$$\begin{aligned}C_{s,p,soft} &= \mathbb{H}(b_2|y_{E1}, b) - \mathbb{H}(\hat{b}_1)\\ &= \mathbb{E}_{y_{E1}}\{\mathtt{h}(\epsilon'_E(y_{E1}))\} - \mathtt{h}(p_e)\\ &= \frac{1}{2}\int_{-\infty}^{\infty} \mathtt{h}(\epsilon'_E(y))[f(y|0) + f(y|1)]dy - \mathtt{h}(p_e) \quad (35)\end{aligned}$$

where $\epsilon'_E(y) = \frac{(1-p_e)f(y|0)+p_e f(y|1)}{f(y|0)+f(y|1)}$, $f(y|0) = \frac{1}{\sqrt{2\pi}\sigma'_{E1}}\exp(-\frac{(y-1)^2}{2\sigma'^2_{E1}})$ and $f(y|1) = \frac{1}{\sqrt{2\pi}\sigma'_{E1}}\exp(-\frac{(y+1)^2}{2\sigma'^2_{E1}})$.

Both (32) and (35) are consistent with the results stated in [6].

The key features of PSK-STEEP in comparison to the two-way scheme in [6] are highlighted in Table I.

For both schemes, we can define $\alpha_1 = \frac{\sigma_1^2}{\sigma_{E1}^2} = \frac{\sigma_1'^2}{\sigma_{E1}'^2}$ as Eve's channel advantage in phase 1, $\alpha_2 = \frac{\sigma_2^2}{\sigma_{E2}^2} = \frac{\sigma_2'^2}{\sigma_{E2}'^2}$ as Eve's channel advantage in phase 2, $p_1 = \frac{1}{\sigma_1^2} = \frac{1}{2\sigma_1'^2}$ as the effective transmission power from node 1 in phase 1, and $p_2 = \frac{\mathbb{E}\{|\tilde{x}_1|^2\}}{\sigma_2^2} = \frac{1}{2\sigma_2'^2}$ as the effective transmission power from node 2 in phase 2. If the LMMSE estimate $\tilde{x}'_1$ (instead of the MMSE estimate $\tilde{x}_1$) of x_1 is used for PSK-STEEP, then $p_2 = \frac{\mathbb{E}\{|\tilde{x}'_1|^2\}}{\sigma_2^2} = \frac{1}{2\sigma_2'^2}$. Note that $\mathbb{E}\{|\tilde{x}'_1|^2\} = \frac{1+\sigma_1^2}{(1+\sigma_1^2)^2}$ and

$$\begin{aligned}\mathbb{E}\{|\tilde{x}_1|^2\} &= \mathbb{E}_{y_1}\{|G(y_1)|^2\} = \frac{1}{M_1}\sum_{x_1}\mathbb{E}_{w_1}\{|G(x_1+w_1)|^2\}\\ &= \mathbb{E}_{w_1}\{|G(1+w_1)|^2\}. \quad (36)\end{aligned}$$

VI. Simulation

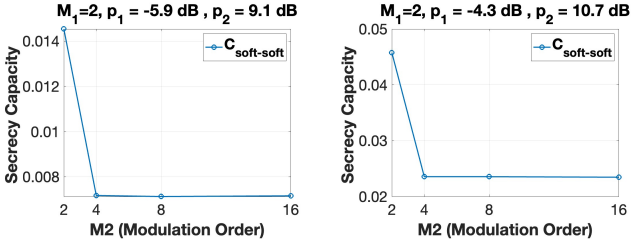
Due to the PSK signaling, the secrecy rate expressions shown earlier do not have closed-form expressions. In this

section, we show Monte Carlo simulation results using up to 10^8 independent runs. To reduce the complexity of simulation, we focus on PSK-STEEP using LMMSE, which is expected to be a lower bound on the secrecy rate of PSK-STEEP using MMSE.

We will also use $C_{s,P,hard,soft}$ for $C_{s,P,H,S}$, for example. As in [6], we let $p^*_{1,\text{hard}} = \max_{p_1} C_{s,p,\text{hard}}$ and $p^*_{1,\text{soft}} = \max_{p_1} C_{s,p,\text{soft}}$.

A. Selected Cases

Figs. 1a and 1b show that the secrecy rate $C_{s,P,S,S}$ of PSK-STEEP is maximized by $M_2 = 2$. Here $M_1 = 2$, $p_1 = p^*_{1,\text{soft}}$, and $p_2(\text{dB}) = p_1(\text{dB}) + 15\text{dB}$. The same finding was observed for $M_1 > 2$ and other choices of parameters.



(a) Secrecy capacity vs M_2 for $\alpha_1 = 4$, $\alpha_2 = 1$

(b) Secrecy capacity vs M_2 for $\alpha_1 = 2$, $\alpha_2 = 1$

Fig. 1: $C_{s,P,S,S}$ versus M_2.

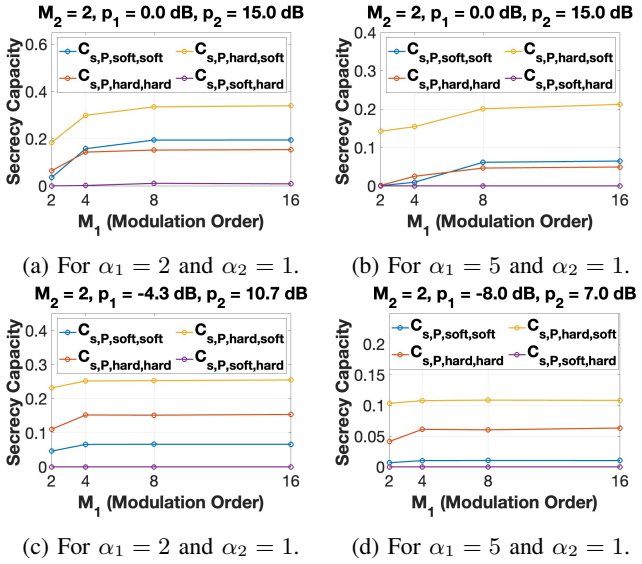
Figs. 2a, 2b, 2c and 2d show that $C_{s,P,S,S}$, $C_{s,P,S,H}$, $C_{s,P,H,S}$ and $C_{s,P,H,H}$ are increasing functions of M_1 although they are saturating quickly after M_1 becomes 4 or 8. Here $p_1(\text{dB}) = 0$ and $p_2(\text{dB}) = 15\text{dB}$ in Figs 2a and 2b. And p_1 is chosen to be $p^*_{1,hard}$ or $p^*_{1,soft}$, and $p_2(\text{dB}) = p_1(\text{dB}) + 15\text{dB}$ in Figs 2c and 2d.

We see that the use of soft decision at user 1 in phase 2 is not to user's advantage. Instead, user 1 should apply the hard decision in phase 2. We also see that the use of soft decision at Eve is not to Eve's advantage either. So, after ruling out soft decision at either user 1 in phase 2 or at Eve, the resulting secrecy rate of PSK-STEEP should be represented by $C_{s,P,H,H}$.

Furthermore, we see that $C_{s,P,H,H}$ is positive for all cases where α_1 equals 2 or 5 (Eve's channel is 2 or 5 times stronger than user's in phase 1). Although α_2 is chosen to be 1 in all four figures, the secrecy rate of PSK-STEEP is not very sensitive to values of $\alpha_2 > 1$ since p_2 is 15dB higher than p_1. If α_2 decreases, the secrecy rate always increases.

Figs. 3a, 3b, 3c and 3d show that PSK-STEEP using $M_1 > M_2 = 2$ outperforms the scheme in [6]. Figs. 3a and 3b use $p_1 = 0\text{dB}$, and Figs. 3c and 3d use $p_1 = p^*_{1,hard}$ or $p_1 = p^*_{1,soft}$ (as functions of α_1). In all cases here and later, p_2 is 50dB higher than p_1 in order to mimic the public channel assumed in [6] for phase 2. With such a large p_2, typical values of α_2 would not have any impact.

When choosing $M_1 = M_2 = 2$ and hard decision at node 1 in phase 2, PSK-STEEP has the same performance as



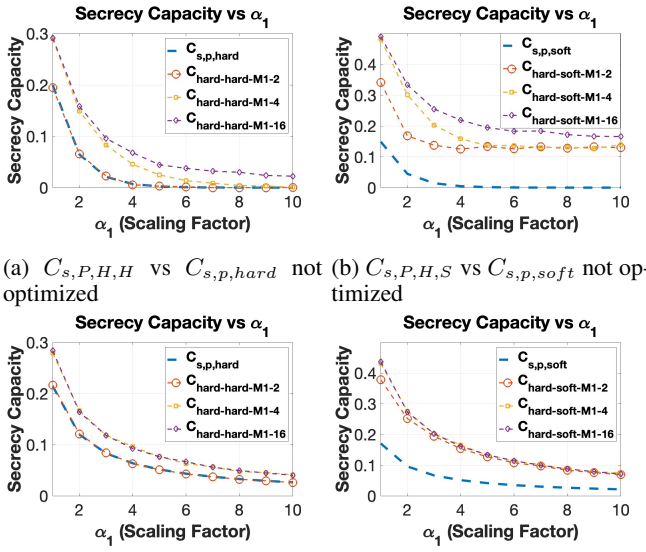
(a) For $\alpha_1 = 2$ and $\alpha_2 = 1$.

(b) For $\alpha_1 = 5$ and $\alpha_2 = 1$.

(c) For $\alpha_1 = 2$ and $\alpha_2 = 1$.

(d) For $\alpha_1 = 5$ and $\alpha_2 = 1$.

Fig. 2: $C_{s,P,S,S}$, $C_{s,P,S,H}$, $C_{s,P,H,S}$ and $C_{s,P,H,H}$ vs M_1.



(a) $C_{s,P,H,H}$ vs $C_{s,p,hard}$ not optimized

(b) $C_{s,P,H,S}$ vs $C_{s,p,soft}$ not optimized

(c) $C_{s,P,H,H}$ vs $C_{s,p,hard}$ optimized

(d) $C_{s,P,H,S}$ vs $C_{s,p,soft}$ optimized

Fig. 3: Comparison between PSK-STEEP and the scheme in [6]

[6] if Eve also applies hard decision. But if Eve applies soft decision, PSK-STEEP outperforms [6] even with $M_1 = M_2 = 2$.

An explanation of the above is not straightforward. But in [6] node 2 makes a hard decision on x_1 in phase 1, which has caused $C_{s,p,soft} < C_{s,p,hard}$, i.e., soft decision at Eve is to Eve's advantage. But in PSK-STEEP, node 2 uses an (soft) estimate of x_1, which has caused $C_{s,P,H,S} > C_{s,P,H,H}$, i.e., soft decision at Eve is not to Eve's advantage. Note that hard or soft decision at Eve directly affects the first entropy terms in (14), (15), (16), (17), (32) and (35).

B. Application to satellite channel model

We will follow the satellite channel model given in [6]. Satellites can be Geostationary (GEO), Low earth orbit (LEO) and Medium earth orbit (MEO). Depending on transmitter, receiver and eavesdropper positions, we have two different cases. Case I: node 1 is ground-station, node 2 is GEO, and Eve is LEO, MEO or GEO. Case II: node 1 is GEO, node 2 is ground station, and Eve is LEO, MEO or GEO.

We consider a RF large scale satellite channel model without considering the impact of small scale fading. We also consider the situation where Eve has the most advantage. According to the models shown in [6], the maximum α_1 can be shown below:

	$\alpha_{1,\max,LEO}$	$\alpha_{1,\max,MEO}$	$\alpha_{1,\max,GEO}$
Case I	240	7.2	1.00002
Case II	1.058	2.25	36000

TABLE II: $\alpha_{1,\max}$ values for different orbits of Eve.

The optimal values of p_1 for the scheme in [6] are as follows. If hard decision is used at Eve, these values of $p_1(\mathtt{dB})$ for LEP, MEO and GEO are $(-24.7, -9.5, -1.7)$ for Case I, and $(-1.9, -4.7, -46.4)$ for Case II. But if soft decision is used at Eve, those values are $(-25, -10, -2.3)$ for Case I, and $(-2.5, -5.3, -46.80)$ for Case II.

Cases	$C_{s,p,hard}$ [6]	$C_{s,P,H,H}$ (M_1= 2)	$C_{s,P,H,H}$ (M_1= 4)	$C_{s,P,H,H}$ (M_1= 16)
LEO,I	0.0011	0.0012	0.0016	0.0017
LEO,II	0.2058	0.2063	0.2666	0.2744
MEO,I	0.0360	0.0358	0.053	0.0055
MEO,II	0.109	0.1101	0.1512	0.1551
GEO,I	0.2144	0.2139	0.2812	0.2813
GEO,II	7.5421e-6	7.63e-6	1.11e-5	1.19e-5

TABLE III: Using hard decision at Eve.

In Tables III and IV, we show the secrecy rates for various cases. We see that PSK-STEEP consistently outperforms the scheme in [6]. Note that the averaged secrecy rate of Cases I and II is also a meaningful metric.

Cases	$C_{s,p,soft}$ [6]	$C_{s,P,H,S}$ (M_1= 2)	$C_{s,P,H,S}$ (M_1= 4)	$C_{s,P,H,S}$ (M_1= 16)
LEO,I	9.16e-4	0.0029	0.0031	0.0038
LEO,II	0.1649	0.3705	0.4195	0.4200
MEO,I	0.0294	0.0935	0.0957	0.0966
MEO,II	0.0870	0.236	0.2557	0.2570
GEO,I	0.1725	0.3745	0.4325	0.4338
GEO,II	6.110e-6	1.536e-5	2.081e-5	2.272e-5

TABLE IV: Using soft decision at Eve

VII. Conclusion

We have investigated STEEP using PSK signaling for secure communication over a wiretap channel where eavesdropper (Eve) has a higher receive SNR than user's. We considered PSK of asymmetric constellation sizes: $M_1 \geq 2$ for phase 1, and $M_2 \geq 2$ for phase 2. It turns out that using $M_2 = 2$ consistently resulted in the highest secrecy rate $C_{s,P}$ of PSK-STEEP. We also found that $C_{s,P}$ is an increasing function of M_1 although C_s saturates quickly when M_1 is larger than 4 or 8. We also compared $C_{s,P}$ with the secrecy rate $C_{s,p}$ of the scheme in [6], the latter of which is restricted to $M_1 = M_2 = 2$. We found that $C_{s,P}$ with $M_1 = M_2 = 2$ is virtually the same as $C_{s,p}$ if (symbol-wise) hard decision is performed at Eve. But if soft decision is performed at Eve, $C_{s,P}$ is increased while $C_{s,p}$ is decreased. This is a surprising advantage of PSK-STEEP over [6]. A key difference between the two schemes under $M_1 = M_2 = 2$ is that the binary probing symbol x_1 transmitted from node 1 to node 2 in phase 1 is estimated (without quantization) by node 2 in PSK-STEEP, but is detected (i.e., a binary quantization) by node 2 in [6]. The results of our investigation indicate that a quantization by node 1 in phase 1 is not to user's advantage if Eve performs soft decision using her observations from both phases 1 and 2. We also applied PSK-STEEP to satellite channel models, which resulted in positive secrecy rates despite the channel advantages of Eve over users. These secrecy rates are larger than those from [6].

References

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

[2] U. Maurer, "Secret key agreement by public discussion from common information," IEEE Transactions on Information Theory, vol. 39, no. 3, pp. 733–742, 1993.

[3] H. V. Poor and R. F. Schaefer, "Wireless physical layer security", PNAS, vol. 114, no. 1, pp.19–26, 2017.

[4] J. Zhang, G. Li, A. Marshall, A. Hu, and L. Hanzo, "A new frontier for IoT security emerging from three decades of key generation relying on wireless channels," IEEE Access, vol. 8, pp. 138406–138446, 2020.

[5] M. A. Vazquez-Castro and M. Hayashi, "One-way and two-way physical layer security protocols for the gaussian satellite channel," IEEE International Conference on Communications (ICC), pp. 1-7, 2019.

[6] M. Hayashi, and A. Vazquez-Castro, "Two-way physical layer security protocol for Gaussian channel," IEEE Transactions on Communications, Vol. 68, No. 5, May 2020.

[7] Y. Hua, "Generalized channel probing and generalized pre-processing for secret key generation," IEEE Transactions on Signal Processing, vol. 71, pp. 1067-1082, March 2023.

[8] Y. Hua, "On secret-message transmission by echoing encrypted probes", IEEE Transactions on Communications, Early Access, July 2025. doi: 10.1109/TCOMM.2025.3588569.

[9] Y. Hua and M. S. Rahman, "Unification of secret key generation and wiretap channel transmission," IEEE ICC, Denver, CO, USA, June 2024.

[10] Y. Hua, M. S. Rahman and A. Swami, "A method for low-latency secure multiple access," IEEE LANMAN, Boston, MA, USA, July 2024.

[11] M. S. Rahman and Y. Hua, "Secure UAV communications by STEEP against full-duplex active eavesdropper," Asilomar Conference on Signals, Sysetms and Computers, Oct 2024.

[12] B. Dai, C. Li, Y. Liang, Z. Ma, and S. Shamai, "Self-secure capacity-achieving feedback schemes of Gaussian multiple-access wiretap channels with degraded message sets," IEEE Trans. Info. Forensic and security, Vol. 17, 2022.

[13] Y. Fan, et al, "Robust deception scheme for secure interference exploitation under PSK modulations," IEEE Transactions on Communications, vol. 69, no. 8, pp. 5425-5440, Aug. 2021.