SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks 2011; **4**:966–978
Published online 8 September 2010 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.230

RESEARCH ARTICLE

Secrecy coding for the binary symmetric wiretap channel

Yanling Chen[1]* and A. J. Han Vinck[2]

[1] Fraunhofer IESE, 67663 Kaiserslautern, Germany
[2] Institute for Experimental Mathematics, University of Duisburg-Essem, 45326 Essen, Germany

ABSTRACT

In this paper, we investigate the binary symmetric wiretap channel. We show that the *secrecy capacity* can be achieved by using *random linear codes*. The random coding scheme gives insight into the structure of secrecy capacity achieving code but unfortunately involves a rather impractical decoder. We further explore the *coset-coding scheme* constructed by linear codes. As a result, we give an upper bound on the total *information loss*, which sheds light on the design of the applicable coset codes for the secure transmission with limited information leakage. Copyright © 2010 John Wiley & Sons, Ltd.

KEYWORDS

binary symmetric channel; wiretap channel; secrecy capacity; equivocation; random linear codes; information loss

***Correspondence**

Yanling Chen, Fraunhofer IESE, 67663, Kaiserslautern, Germany.
E-mail: julia@iem.uni-due.de

1. INTRODUCTION

The concept of the wiretap channel was first introduced by Wyner [1]. His model is a form of degraded broadcast channel. Assume that the wiretapper knows the encoding scheme used at the transmitter and the decoding scheme used at the legitimate receiver. The objective is to maximize the rate of reliable communication from the source to the legitimate receiver, subject to the constraint that the wiretapper learns as little as possible about the source output. In fact, there is a maximum rate, above which secret communication between the transmitter and the legitimate receiver is impossible. Wyner [1] has determined this *secrecy capacity* when both main channel and the wiretap channel are discrete memoryless.

In this paper, we focus on the problem of developing a forward coding scheme for provably secure, reliable communication over a wiretap channel. Basic idea has been introduced by Wyner in Reference [1] for the special case when the main channel is noiseless and the wiretap channel is a binary symmetric channel (BSC). Another example is given by Thangaraj *et al*. [2] for the case where the main channel is noiseless and the wiretap channel is a binary erasure channel (BEC). In this paper, we consider the specific case when both the main channel and the wiretap channel are BSCs. The model is shown in Figure 1. Our main contribution is twofold. We start with a random coding scheme similar to the one proposed in Reference [3]. We give a detailed mathematical proof to show that the secrecy capacity can be achieved by using random linear codes. Furthermore, we address the coset code constructed by linear codes and analyze its information leakage. We derive an upper bound on the total information loss and show that under certain constraint one can construct a coset code to ensure a secure transmission with limited information leakage.

2. MODEL DESCRIPTION

We consider the communication model as described in Figure 1. Suppose that all alphabets of the source, the channel input, and the channel output are equal to $\{0, 1\}$. The main channel is a BSC with crossover probability p and we denote it by BSC(p). The wiretap channel is a BSC(p_w), where $0 \leq p < p_w \leq 1/2$. Note that a BSC(p_w) is equivalent to the concatenation of a BSC(p) and a BSC(p^*), where $p^* = (p_w - p)/(1 - 2p)$. Thus the channel model shown in Figure 1 is equivalent to Wyner's model with a BSC(p) main channel and a BSC(p^*) wiretap channel. Its secrecy capacity due to Reference [1] is $C_s = h(p_w) - h(p)$. Here $h(\cdot)$ is the binary entropy function.

To transmit a K-bit secret message S^K, an N-bit codeword X^N is sent to the channel. The corresponding output

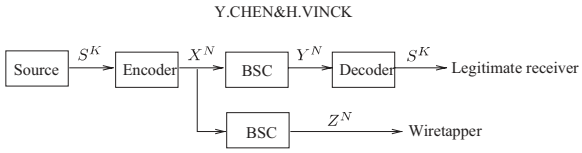

Figure 1. Binary symmetric wiretap channel.

at the legitimate receiver is Y^N, at the wiretapper is Z^N. Because of the channel noises, Y^N and Z^N may be different from X^N. Thus the error occurred over the main channel is $E^N = Y^N - X^N$, over the wiretap channel is $E_w^N = Z^N - X^N$. Every component of E^N and E_w^N, denoted as E_i and E_{wj}, respectively, where $1 \le i, j \le N$, has the following distribution:

$$\Pr(E_i = 1) = p, \quad \Pr(E_i = 0) = 1 - p;$$
$$\Pr(E_{wj} = 1) = p_w, \ \Pr(E_{wj} = 0) = 1 - p_w$$

Assume that S^K is uniformly distributed. The *transmission rate* to the legitimate receiver is

$$R = \frac{K}{N} \tag{1}$$

The *equivocation* of the wiretapper is defined to be

$$d = \frac{H(S^K|Z^N)}{H(S^K)} = \frac{H(S^K|Z^N)}{K} \tag{2}$$

At the legitimate receiver, on receipt of Y^N, the decoder makes an estimate $\hat{S}^K$ of the message S^K. Then, corresponding to a given encoder and decoder, the *error probability* P_e is defined to be

$$P_e = \Pr\{\hat{S}^K \neq S^K\} \tag{3}$$

We refer to the above as an encoder–decoder (K, N, d, P_e).

In this paper, when the dimension of a sequence is clear from the context, we will denote the sequences in boldface letters for simplicity. For example, $\mathbf{x}$ is the sequence x^N and $\mathbf{s}$ is s^K, etc. A similar convention applies to random variables, which are denoted by upper-case letters.

3. SECRECY CAPACITY ACHIEVING CODES

In this section, we perform a random linear code to establish the achievability of the secrecy capacity. For this aim, we need to construct an encoder-decoder (K, N, d, P_e) such that for arbitrary $\varepsilon, \zeta, \delta > 0$,

$$R \ge h(p_w) - h(p) - \varepsilon, \tag{4a}$$
$$d \ge 1 - \zeta, \tag{4b}$$
$$P_e \le \delta \tag{4c}$$

3.1. Parameter settings

First, we set up the parameters for the encoder-decoder (K, N, d, P_e). Randomly choose a binary matrix H_1 with $N - K_1$ rows and N columns. Independently and randomly choose another binary matrix H with K rows and N columns. Assume that $K \le K_1$ and let $K_2 = K_1 - K$. We construct

$$\mathrm{H}_2 = \begin{bmatrix} \mathrm{H}_1 \\ \mathrm{H} \end{bmatrix} \tag{5}$$

Then H_2 is a binary matrix with $N - K_2$ rows and N columns. Later in our proof we will increase N and keep K_1, K proportional to N. In order to ensure that K_1 and K are integers, for arbitrary small $\epsilon > 0$, we take

$$K_1 = \lfloor N[1 - h(p) - 2\epsilon] \rfloor;$$
$$K_2 = \lfloor N[1 - h(p_w) - 2\epsilon] \rfloor$$

Here $\lfloor x \rfloor$ stands for the maximal integer $\le x$. Straightforwardly, we have

$$\begin{aligned} \frac{K}{N} &= \frac{\lfloor N[1 - h(p) - 2\epsilon] \rfloor - \lfloor N[1 - h(p_w) - 2\epsilon] \rfloor}{N} \\ &\ge \frac{N[1 - h(p) - 2\epsilon] - 1 - N[1 - h(p_w) - 2\epsilon]}{N} \\ &= h(p_w) - h(p) - \frac{1}{N} \end{aligned}$$

For given $\varepsilon > 0$, there exists an integer $N_0 > 1/\varepsilon$, such that when $N \ge N_0$, we have

$$R = \frac{K}{N} \ge h(p_w) - h(p) - \varepsilon \tag{6}$$

In what follows, we will assume that H_1, H, and H_2 are of full rank. The reason is that by Lemma 3.1, the rows of the H_1 and H are linear independent with probability approaching 1 as N goes to infinity. Based on this assumption, it is easy to prove that H_2, as defined in the Equation (5), has full rank with probability approaching 1, as N goes to infinity.

Lemma 3.1. *(Lemma 6 in Reference [4]) For a fixed* $R = \frac{K}{N}$, *a randomly chosen binary matrix* H *with K rows and N columns has rank K with probability approaching 1 as N goes to infinity.*

Now let us specify the encoder. In order to send a secret message $\mathbf{s}$, a sequence $\mathbf{x}$ is chosen at random from the solution set of the following equation

$$\mathbf{x}\mathrm{H}_2{}^{\mathrm{T}} = \left[\mathbf{x}\mathrm{H}_1{}^{\mathrm{T}} \ \mathbf{x}\mathrm{H}^{\mathrm{T}}\right] = \left[\mathbf{0} \ \mathbf{s}\right] \tag{7}$$

where $\mathrm{H}_2{}^{\mathrm{T}}$, $\mathrm{H}_1{}^{\mathrm{T}}$ and H^{T} are the transposes of the matrices H_2, H_1 and H, respectively.

Due to the assumption that the matrix H_2 is of rank $N - K_2$, the number of solutions of Equation (7) is 2^{K_2}. Furthermore, for different secret messages $\mathbf{s}$, the solution

sets are disjoint. Note that the number of solutions of the equation $\mathbf{x}\mathrm{H}_1{}^{\mathrm{T}} = \mathbf{0}$ is 2^{K_1}. So corresponding to different secret messages $\mathbf{s}$, the solutions of the equation $\mathbf{x}\mathrm{H}_1{}^{\mathrm{T}} = \mathbf{0}$ is equally divided into $2^{K_1}/2^{K_2} = 2^K$ subsets. Suppose that H_1 is a parity check matrix of linear code C_1 and H_2 is a parity check matrix of C_2. Then C_1 is equally divided into 2^K subsets corresponding to different values of $\mathbf{s}$, and C_2 is the subset of C_1 w.r.t. $\mathbf{s} = \mathbf{0}$.

In the following, we will show that the secrecy capacity can be achieved by a random linear code in two parts, the reliability: $P_e \to 0$ as $N \to \infty$; and the security: $d \to 1$ as $N \to \infty$.

3.2. Reliability proof

In this subsection, we will prove that $P_e \to 0$ as $N \to \infty$.

The legitimate receiver uses typical set decoder. The decoder examines the typical set $T_E^N(\epsilon)$, the set of error sequences $\mathbf{e}$ that satisfy

$$2^{-N[h(p)+\epsilon]} \leq \Pr(\mathbf{E} = \mathbf{e}) \leq 2^{-N[h(p)-\epsilon]}$$

Check to see if any of those typical error sequences, $\mathbf{e}$ satisfies

$$\mathbf{e}\mathrm{H}_1{}^{\mathrm{T}} = \mathbf{y}\mathrm{H}_1{}^{\mathrm{T}}$$

If exactly one typical sequence $\hat{\mathbf{e}}$ does so, the typical set decoder reports $\hat{\mathbf{e}}$ as the hypothesized error sequence. The secret message $\mathbf{s}$ is decoded as $\hat{\mathbf{s}} = (\mathbf{y} - \hat{\mathbf{e}})\mathrm{H}^{\mathrm{T}}$. However, if no typical sequence in the set $T_E^N(\epsilon)$ matches the observed syndrome $\mathbf{y}\mathrm{H}_1{}^{\mathrm{T}}$, or more than one does, then the typical decoder reports an error.

The error probability of the typical set decoder at the legitimate receiver, can be written as follows:

$$P_e = P_T + P_{\mathrm{H}_1} \tag{8}$$

where P_T is the probability that the true error sequence is itself not typical, and P_{H_1} is the probability that the true error sequence is typical and at least one other typical sequence clashes with it.

We first analyze P_T. For given $\epsilon > 0$ and $\delta > 0$, there exists an integer N_1, such that when $N \geq N_1$, $\Pr\{\mathbf{e} \in T_E^N(\epsilon)\} \geq 1 - \delta/2$. Therefore, when $N \geq N_1$, $P_T = 1 - \Pr\{\mathbf{e} \in T_E^N(\epsilon)\} \leq \delta/2$.

Now we consider P_{H_1}. Suppose that the true error sequence is $\mathbf{e}$. It belongs to the set $T_E^N(\epsilon)$. If any of the typical error sequence $\mathbf{e}'$, different from $\mathbf{e}$, satisfies $(\mathbf{e}' - \mathbf{e})\mathrm{H}_1{}^{\mathrm{T}} = \mathbf{0}$, then we have an error. Let

$$T_{\mathbf{e}}(\epsilon) = \{\mathbf{e}' : \mathbf{e}' \in T_E^N(\epsilon), \mathbf{e}' \neq \mathbf{e}\} \tag{9}$$

We have P_{H_1} is equal to or less than

$$\sum_{\mathbf{e} \in T_E^N(\epsilon)} \Pr(\mathbf{E} = \mathbf{e}) \sum_{\mathbf{e}' \in T_{\mathbf{e}}(\epsilon)} \mathbf{1}[(\mathbf{e}' - \mathbf{e})\mathrm{H}_1{}^{\mathrm{T}} = \mathbf{0}]$$

where $\mathbf{1}[\cdot]$ is the truth function, whose value is 1 if the statement in the bracket is true and 0 otherwise.

We will find the average of P_{H_1}, $\bar{P}_{\mathrm{H}_1}$, by averaging over all possible H_1. By showing that $\bar{P}_{\mathrm{H}_1}$ vanishes as N approaches infinity, we will thus show that there exists an H_1 such that P_{H_1} is with vanishing error probability. Denote averaging over all possible binary matrices H_1 by $\langle\cdot\rangle_{\mathrm{H}_1}$. Then we have

$$\begin{aligned}
\bar{P}_{\mathrm{H}_1} &= \langle P_{\mathrm{H}_1} \rangle_{\mathrm{H}_1} \\
&\leq \langle \sum_{\mathbf{e} \in T_E^N(\epsilon)} \Pr(\mathbf{E} = \mathbf{e}) \sum_{\mathbf{e}' \in T_{\mathbf{e}}(\epsilon)} \mathbf{1}[(\mathbf{e}' - \mathbf{e})\mathrm{H}_1{}^{\mathrm{T}} = \mathbf{0}] \rangle_{\mathrm{H}_1} \\
&= \sum_{\mathbf{e} \in T_E^N(\epsilon)} \Pr(E^N = \mathbf{e}) \sum_{\mathbf{e}' \in T_{\mathbf{e}}(\epsilon)} \langle \mathbf{1}[(\mathbf{e}' - \mathbf{e})\mathrm{H}_1{}^{\mathrm{T}} = \mathbf{0}] \rangle_{\mathrm{H}_1}
\end{aligned}$$

Since for any non-zero binary sequence $\mathbf{v}$, the probability that $\mathbf{v}\mathrm{H}_1{}^{\mathrm{T}} = \mathbf{0}$, averaging over all possible H_1, is $2^{-(N-K_1)}$, so

$$\begin{aligned}
\bar{P}_{\mathrm{H}_1} &\leq (\sum_{\mathbf{e} \in T_E^N(\epsilon)} \Pr(\mathbf{E} = \mathbf{e}))|T_{\mathbf{e}}(\epsilon)|2^{-(N-K_1)} \\
&< |T_E^N(\epsilon)|2^{-(N-K_1)} \\
&\leq 2^{N[h(p)+\epsilon]}2^{-(N-K_1)} \\
&= 2^{-N(1-h(p)-\epsilon-K_1/N)}
\end{aligned}$$

Note that $K_1/N \leq 1 - h(p) - 2\epsilon < 1 - h(p) - \epsilon$. Therefore, for given $\epsilon > 0$ and $\delta > 0$, there exists an N_2, when $N \geq N_2$, $\bar{P}_{\mathrm{H}_1} \leq \delta/8$. By Markov inequality,

$$\Pr(P_{\mathrm{H}_1} > \frac{\delta}{2}) < \frac{\bar{P}_{\mathrm{H}_1}}{\delta/2} \leq \frac{\delta/8}{\delta/2} = \frac{1}{4}$$

Thus we have

$$\Pr(P_{\mathrm{H}_1} \leq \frac{\delta}{2}) = 1 - \Pr(P_{\mathrm{H}_1} \geq \frac{\delta}{2}) > \frac{3}{4}$$

That is, from all possible H_1, more than 3/4 random choices yield $P_{\mathrm{H}_1} \leq \delta/2$.

So far we have shown that there are more than 3/4 random choices from all possible H_1 such that, for given $\epsilon > 0$ and $\delta > 0$, when $N \geq \max\{N_1, N_2\}$,

$$P_e = P_T + P_{\mathrm{H}_1} \leq \delta/2 + \delta/2 = \delta$$

This concludes the proof of reliability.

3.3. Security proof

In this subsection, we will prove that $d \to 1$ as $N \to \infty$.

We consider the uncertainty of the secret to the wiretapper in three steps:

(1) show that

$$H(\mathbf{S}|\mathbf{Z}) \geq N[h(p_w) - h(p)] - H(\mathbf{X}|\mathbf{S}, \mathbf{Z})$$

(2) show that

$$H(\mathbf{X}|\mathbf{S}, \mathbf{Z}) \leq h(P_{ew}) + P_{ew}K_2$$

Here P_{ew} means a wiretapper's error probability to decode $\mathbf{x}$ in the case where $\mathbf{s}$ is known to the wiretapper.

(3) show that for arbitrary $0 < \lambda < 1/2$, $P_{ew} \leq \lambda$.

Combining the above steps, we have

$$\begin{aligned} d &= \frac{H(\mathbf{S}|\mathbf{Z})}{H(\mathbf{S})} \\ &\geq \frac{N[h(p_w) - h(p)] - h(P_{ew}) - P_{ew}K_2}{K} \\ &\geq \frac{N[h(p_w) - h(p)] - h(\lambda) - \lambda K_2}{K} \\ &\overset{(a)}{\geq} \frac{[h(p_w) - h(p)] - \varepsilon - \lambda K_2/N}{K/N} \\ &\overset{(b)}{\geq} 1 - \frac{\varepsilon + \lambda K_2/N}{h(p_w) - h(p) - \varepsilon} \\ &\overset{(c)}{\geq} 1 - \frac{\varepsilon + \lambda(1 - h(p_w))}{h(p_w) - h(p) - \varepsilon} \\ &\overset{(d)}{\geq} 1 - \zeta \end{aligned}$$

where

(a) follows from the fact that $h(\lambda) \leq 1$ and when $N \geq N_0$, $\varepsilon \geq 1/N$.

(b) follows from the fact that $h(p_w) - h(p) - \varepsilon \leq K/N \leq h(p_w) - h(p)$.

(c) follows from the fact that $K_2/N < 1 - h(p_w)$.

(d) follows from the fact that there exists $0 < \lambda < 1/2$ such that for given arbitrary small ε and ζ, $\zeta \geq \frac{\varepsilon + \lambda(1-h(p_w))}{h(p_w) - h(p) - \varepsilon}$.

We now proceed to step 1 by considering

$$\begin{aligned} H(\mathbf{S}|\mathbf{Z}) &= H(\mathbf{S}, \mathbf{Z}) - H(\mathbf{Z}) \\ &= H(\mathbf{S}, \mathbf{X}, \mathbf{Z}) - H(\mathbf{X}|\mathbf{S}, \mathbf{Z}) - H(\mathbf{Z}) \\ &= H(\mathbf{S}, \mathbf{X}|\mathbf{Z}) - H(\mathbf{X}|\mathbf{S}, \mathbf{Z}) \\ &= H(\mathbf{X}|\mathbf{Z}) + H(\mathbf{S}|\mathbf{X}, \mathbf{Z}) - H(\mathbf{X}|\mathbf{S}, \mathbf{Z}) \\ &\overset{(a)}{=} H(\mathbf{X}|\mathbf{Z}) - H(\mathbf{X}|\mathbf{S}, \mathbf{Z}) \\ &\overset{(b)}{\geq} H(\mathbf{X}|\mathbf{Z}) - H(\mathbf{X}|\mathbf{Y}) - H(\mathbf{X}|\mathbf{S}, \mathbf{Z}) \\ &= I(\mathbf{X}; \mathbf{Y}) - I(\mathbf{X}; \mathbf{Z}) - H(\mathbf{X}|\mathbf{S}, \mathbf{Z}) \\ &\overset{(c)}{=} N[I(X; Y) - I(X; Z)] - H(\mathbf{X}|\mathbf{S}, \mathbf{Z}) \\ &= N[h(p_w) - h(p)] - H(\mathbf{X}|\mathbf{S}, \mathbf{Z}) \end{aligned}$$

where

(a) follows from the fact that $H(\mathbf{S}|\mathbf{X}, \mathbf{Z}) = 0$ since $\mathbf{S} = \mathbf{X}\mathrm{H}^{\mathrm{T}}$.

(b) follows from the fact that $H(\mathbf{X}|\mathbf{Y}) \geq 0$.

(c) follows from the fact that $I(\mathbf{X}; \mathbf{Y}) = I(X^N; Y^N) = NI(X; Y)$ and $I(\mathbf{X}; \mathbf{Z}) = I(X^N; Z^N) = NI(X; Z)$.

Thus the proof of step 1 is completed.

To prove step 2, we need to bound the entropy of the codeword $\mathbf{X}$ conditioned on the message $\mathbf{S}$ and wiretapper's observation $\mathbf{Z}$. Suppose that $\mathbf{S}$ takes value $\mathbf{s}$. For given H_2, $\mathbf{s}$, we consider the solution set of Equation (7) as a codebook, $\mathbf{X}$ in the codebook as the input codeword, $\mathbf{Z}$ as the corresponding output of passing $\mathbf{X}$ through the wiretap channel. From $\mathbf{Z}$, the decoder estimates $\mathbf{X}$ as $\hat{\mathbf{X}} = g(\mathbf{Z})$. Define the probability of error

$$P_{ew} = \Pr(\hat{\mathbf{X}} \neq \mathbf{X}) \tag{10}$$

From Fano's inequality, we have

$$H(\mathbf{X}|\mathbf{s}, \mathbf{Z}) \overset{(a)}{\leq} h(P_{ew}) + P_{ew}K_2$$

where (a) follows from the fact that, there are 2^{K_2} codewords in the codebook. Furthermore, we have

$$\begin{aligned} H(\mathbf{X}|\mathbf{S}, \mathbf{Z}) &= \sum_{\mathbf{s}} \Pr(\mathbf{S} = \mathbf{s}) H(\mathbf{X}|\mathbf{s}, \mathbf{Z}) \\ &\leq \{h(P_{ew}) + P_{ew}K_2\} \sum_{\mathbf{s}} \Pr(\mathbf{S} = \mathbf{s}) \\ &= h(P_{ew}) + P_{ew}K_2 \end{aligned}$$

Thus we complete the proof of step 2.

Now we proceed to step 3. Note that the estimate $g(\mathbf{Z})$ of the decoder can be arbitrary. Here we use the typical set decoder. With the knowledge of $\mathbf{s}$ and $\mathbf{z}$, the decoder tries to find the codeword $\mathbf{x}$ sent to the channel. The decoder examines the typical set $T_{E_w}^N(\epsilon)$, the set of error sequences $\mathbf{e}_w$ that satisfy

$$2^{-N[h(p_w)+\epsilon]} \leq \Pr(\mathbf{E}_w = \mathbf{e}_w) \leq 2^{-N[h(p_w)-\epsilon]}$$

Check to see if any of those typical error sequences, $\mathbf{e}_w$ satisfies

$$\mathbf{e}_w \mathrm{H}_2{}^{\mathrm{T}} = \mathbf{z}\mathrm{H}_2{}^{\mathrm{T}}$$

If exactly one typical sequence $\hat{\mathbf{e}}_w$ does, the typical set decoder reports $\hat{\mathbf{e}}_w$ as the hypothesized error sequence. The codeword $\mathbf{x}$ is decoded as $\hat{\mathbf{x}} = \mathbf{z} - \hat{\mathbf{e}}_w$. However, if no typical sequence in the set $T_{E_w}^N(\epsilon)$ matches the observed syndrome $\mathbf{z}\mathrm{H}_2{}^{\mathrm{T}}$, or more than one does, then the typical decoder reports an error.

The error probability of the typical set decoder at the wiretapper, can be written as follows:

$$P_{ew} = P_{T_w} + P_{\mathrm{H}_2} \tag{11}$$

where P_{T_w} is the probability that the true error sequence is itself not typical, and P_{H_2} is the probability that the true error sequence is typical and at least one other typical sequence clashes with it.

We first analyze P_{T_w}. For given $\epsilon > 0$ and $\lambda > 0$, there exists an integer N_3, such that when $N \geq N_3$, $\Pr\{\mathbf{e}_w \in T_{E_w}^N(\epsilon)\} \geq 1 - \lambda/2$. Therefore, when $N \geq N_3$, $P_{T_w} = 1 - \Pr\{\mathbf{e}_w \in T_{E_w}^N(\epsilon)\} \leq \lambda/2$.

Now we consider P_{H_2}. Suppose that the true error sequence is $\mathbf{e}_w$. It belongs to the set $T_{E_w}^N(\epsilon)$. If any of the typical error sequence $\mathbf{e}'_w$, different from $\mathbf{e}_w$, satisfies $(\mathbf{e}'_w - \mathbf{e}_w)\mathrm{H}_2{}^{\mathrm{T}} = \mathbf{0}$, then we have an error. Let

$$T_{\mathbf{e}_w}(\epsilon) = \{\mathbf{e}'_w : \mathbf{e}'_w \in T_{E_w}^N(\epsilon), \mathbf{e}'_w \neq \mathbf{e}_w\} \tag{12}$$

We have P_{H_2} is equal to or less than

$$\sum_{\mathbf{e}_w \in T_{E_w}^N(\epsilon)} \Pr(\mathbf{E}_w = \mathbf{e}_w) \sum_{\mathbf{e}'_w \in T_{\mathbf{e}_w}(\epsilon)} \mathbf{1}[(\mathbf{e}'_w - \mathbf{e}_w)\mathrm{H}_2{}^{\mathrm{T}} = \mathbf{0}]$$

Now we will find the average of P_{H_2}, $\bar{P}_{\mathrm{H}_2}$, by averaging over all possible H_2. Note that H_2 can be randomly generated in the way that H_1 and H are randomly generated independently. And due to the structure of H_2 as described in the Equation (5),

$$\begin{aligned}&\mathbf{1}[(\mathbf{e}'_w - \mathbf{e}_w)\mathrm{H}_2{}^{\mathrm{T}} = \mathbf{0}]\\ &= \mathbf{1}[(\mathbf{e}'_w - \mathbf{e}_w)\mathrm{H}_1{}^{\mathrm{T}} = \mathbf{0}] \cdot \mathbf{1}[(\mathbf{e}'_w - \mathbf{e}_w)\mathrm{H}^{\mathrm{T}} = \mathbf{0}]\end{aligned}$$

Therefore, we have

$$\begin{aligned}\bar{P}_{\mathrm{H}_2} &= \langle P_{\mathrm{H}_2}\rangle_{\mathrm{H}_2}\\ &\leq \sum_{\mathbf{e}_w \in T_{E_w}^N(\epsilon)} \Pr(\mathbf{E}_w = \mathbf{e}_w) \sum_{\mathbf{e}'_w \in T_{\mathbf{e}_w}(\epsilon)} \langle \mathbf{1}[(\mathbf{e}'_w - \mathbf{e}_w)\mathrm{H}_2{}^{\mathrm{T}} = \mathbf{0}]\rangle_{\mathrm{H}_2}\\ &= \sum_{\mathbf{e}_w \in T_{E_w}^N(\epsilon)} \Pr(\mathbf{E}_w = \mathbf{e}_w)\\ &\quad \sum_{\mathbf{e}'_w \in T_{\mathbf{e}_w}(\epsilon)} \langle\langle \mathbf{1}[(\mathbf{e}'_w - \mathbf{e}_w)\mathrm{H}_1{}^{\mathrm{T}} = \mathbf{0}] \cdot \mathbf{1}[(\mathbf{e}'_w - \mathbf{e}_w)\mathrm{H}^{\mathrm{T}} = \mathbf{0}]\rangle_{\mathrm{H}_1}\rangle_{\mathrm{H}}\\ &= \sum_{\mathbf{e}_w \in T_{E_w}^N(\epsilon)} \Pr(\mathbf{E}_w = \mathbf{e}_w)\\ &\quad \sum_{\mathbf{e}'_w \in T_{\mathbf{e}_w}(\epsilon)} \langle \mathbf{1}[(\mathbf{e}'_w - \mathbf{e}_w)\mathrm{H}_1{}^{\mathrm{T}} = \mathbf{0}]\rangle_{\mathrm{H}_1} \cdot \langle \mathbf{1}[(\mathbf{e}'_w - \mathbf{e}_w)\mathrm{H}^{\mathrm{T}} = \mathbf{0}]\rangle_{\mathrm{H}}\end{aligned}$$

Since for any non-zero binary sequence $\mathbf{v}$, the probability that $\mathbf{v}\mathrm{H}_1{}^{\mathrm{T}} = \mathbf{0}$, averaging over all possible H_1, is $2^{-(N-K_1)}$ and the probability that $\mathbf{v}\mathrm{H}^{\mathrm{T}} = \mathbf{0}$ averaging over all possible H, is 2^{-K}, so

$$\begin{aligned}\bar{P}_{\mathrm{H}_2} &\leq \Big(\sum_{\mathbf{e}_w \in T_{E_w}^N(\epsilon)} \Pr(\mathbf{E}_w = \mathbf{e}_w)\Big)|T_{\mathbf{e}_w}(\epsilon)|2^{-(N-K_1)} \cdot 2^{-K}\\ &< |T_{E_w}^N(\epsilon)|2^{-(N-K_1+K)} \leq 2^{N[h(p_w)+\epsilon]}2^{-(N-K_2)}\\ &= 2^{-N(1-h(p_w)-\epsilon-K_2/N)}\end{aligned}$$

Note that $K_2/N \leq 1 - h(p_w) - 2\epsilon < 1 - h(p_w) - \epsilon$. Therefore, for given $\epsilon > 0$ and $\lambda > 0$, there exists an N_4, when $N \geq N_4$, $\bar{P}_{\mathrm{H}_2} \leq \lambda/8$. By Markov inequality,

$$\Pr(P_{\mathrm{H}_2} > \frac{\lambda}{2}) < \frac{\bar{P}_{\mathrm{H}_2}}{\lambda/2} \leq \frac{\lambda/8}{\lambda/2} = \frac{1}{4}$$

Thus we have

$$\Pr(P_{\mathrm{H}_2} \leq \frac{\lambda}{2}) = 1 - \Pr(P_{\mathrm{H}_2} \geq \frac{\lambda}{2}) > \frac{3}{4}$$

That is, from all possible H_2, more than $3/4$ random choices yield $P_{\mathrm{H}_2} \leq \lambda/2$. Due to the structure of H_2, this implies that, there are more than $3/4$ random choices from all possible H_1, independently more than $3/4$ random choices from all possible H such that H_2 satisfies $P_{\mathrm{H}_2} \leq \lambda/2$.

So far we have shown that there are more than $3/4$ random choices from all possible H_1 and independently more than $3/4$ random choices from all possible H such that, for given $\epsilon > 0$ and $\lambda > 0$, when $N \geq \max\{N_3, N_4\}$,

$$P_{ew} = P_{T_w} + P_{\mathrm{H}_2} \leq \lambda/2 + \lambda/2 = \lambda$$

This completes the proof of step 3.

As a conclusion of above discussion, for given $\varepsilon, \delta, \zeta, \epsilon > 0$, when $N \geq \max\{N_0, N_1, N_2, N_3, N_4\}$, there are more than $1/2 = 3/4 + 3/4 - 1$ random choices of all possible H_1 and more than $3/4$ random choices from all possible H such that $P_e \leq \delta$ and $P_{ew} \leq \lambda$. In addition to the Equation (6), we have shown that there exist H_1 and H that lead to a random linear code such that

$$\frac{K}{N} \geq h(p_w) - h(p) - \varepsilon, \quad d \geq 1 - \zeta, \quad P_e \leq \delta$$

4. ANALYSIS OF INFORMATION LEAKAGE

We have proved that the secrecy capacity of the binary symmetric wiretap channel can be achieved by using random linear codes. However, the typical set decoder used in the proof is rather impractical. Thus, the method is existent but not effective in practice. Until now it is still an unsolved problem to write down an explicit and practical encoder and decoder to achieve a reliable and secure communication over a wiretap channel at rates close to the secrecy capacity.

The motivation of this section is the need of constructive and applicable codes for the wiretap channel. Adopting the code structure of the random coding scheme, we restrict our attention to the coset-coding scheme by using binary linear

Table I. The codebook in the encoding scheme.

Space of input x	Secret s	Set of codewords w.r.t. secret s
C_1	s(1)	$x(1) + C_2$
	s(2)	$x(2) + C_2$
	⋮	⋮
	$s(2^k)$	$x(2^k) + C_2$

codes in the construction. We will address the security of the coset-coding scheme through analyzing its total information leakage.

4.1. Coset-coding scheme

Consider the communication model shown in Figure 1. Note that in this section, H_1 and H_2 (thus H) are certainly of full rank. In particular, H_1, H_2 are parity check matrices of an (n, k_1) linear code C_1 and an (n, k_2) linear code C_2, respectively. Here $C_2 \subset C_1$ and $k = k_1 - k_2$. We use the same encoding strategy as the one used for the random linear codes, as described by the Equation (7). The codebook used in the encoding scheme is shown in Table I.

According to Table I, to transmit a k-bit secret message $\mathbf{s}$, an n-bit codeword $\mathbf{x}$, randomly chosen from coset $\mathbf{x} + C_2$, is sent to the channel. We can say that the n-bit codeword consists of k bits information for secret recovery, $n - k_1$ bits redundancy for reliable transmission, and k_2 bits randomness for security enhancement. So the rate of the transmission is

$$R = \frac{k}{n} \tag{13}$$

At the legitimate receiver, the decoder uses syndrome decoding, where the true error sequence $\mathbf{e}$ has the same syndrome as $\mathbf{y}$, i.e.,

$$\mathbf{e}{H_1}^{\mathrm{T}} = \mathbf{y}{H_1}^{\mathrm{T}}$$

Note that there are 2^{k_1} error patterns that result in the same syndrome and the decoder chooses the one with the minimum Hamming weight to be the error sequence $\hat{\mathbf{e}}$. Then, the secret $\mathbf{s}$ is decoded as

$$\hat{\mathbf{s}} = (\mathbf{y} - \hat{\mathbf{e}})\mathrm{H}^{\mathrm{T}}$$

Since C_1 is a (n, k_1) linear code, there are 2^{n-k_1} disjoint cosets of C_1 and they together span the whole space $\{0, 1\}^N$. Denote the 2^{n-k_1} coset leaders (the sequences of the minimum Hamming weight from every cosets) as $\mathbf{e}(i)$, where $1 \le i \le 2^{n-k_1}$. If the true error sequence $\mathbf{e}$ is one of 2^{n-k_1} coset leaders, $\mathbf{x} = \mathbf{y} - \mathbf{e}$ will be correctly decoded. So does $\mathbf{s} = \mathbf{x}\mathrm{H}^{\mathrm{T}}$. Furthermore, if the true error sequence $\mathbf{e}$ belongs to any coset $\mathbf{e}(i) + C_2$, where $1 \le i \le 2^{n-k_1}$, $\mathbf{s}$ will also be decoded correctly. Therefore, the error probability of decoding is

$$\begin{aligned}\Pr\{\hat{\mathbf{s}} \neq \mathbf{s}\} &= 1 - \Pr\{\hat{\mathbf{s}} = \mathbf{s}\} \\ &= 1 - \sum_{i=1}^{2^{n-k_1}} \sum_{\mathbf{e} \in \mathbf{e}(i)+C_2} p^{w(\mathbf{e})}(1-p)^{N-w(\mathbf{e})}\end{aligned} \tag{14}$$

where $w(\mathbf{e})$ is the Hamming weight of sequence $\mathbf{e}$. Clearly, the coset code constructed by C_1 and C_2 has better error correcting capability than linear code C_1.

4.2. Preliminaries

Let C be a set of binary sequences of length n. Recall that the *weight distribution function* of C, as defined in Reference [5], is

$$A_C^{\mathrm{w}}(z) = \sum_{i=0}^{n} A_i^{\mathrm{w}} z^i \tag{15}$$

where

$$A_i^{\mathrm{w}} = A_i^{\mathrm{w}}(C) = \sharp\{\mathbf{x} \in C | w(\mathbf{x}) = i\} \tag{16}$$

The sequence $A_0^{\mathrm{w}}, A_1^{\mathrm{w}}, \cdots, A_n^{\mathrm{w}}$ is known as the *weight distribution* of C. In particular, if C is a linear code, the sequence $A_0^{\mathrm{w}}, A_1^{\mathrm{w}}, \cdots, A_n^{\mathrm{w}}$ and the function $A_C^{\mathrm{w}}(z)$ are also its *distance distribution* and *distance distribution function* respectively.

We define

$$P_C(r) = \frac{1}{|C|} \sum_{\mathbf{v} \in C} r^{w(\mathbf{v})}(1-r)^{n-w(\mathbf{v})} \tag{17}$$

where $0 \le r \le 1/2$ and $|C|$ is the cardinality of C. Denote $\mathbf{z} + C$ as the coset of C associated with the sequence $\mathbf{z}$, where $\mathbf{z} \in \{0, 1\}^n$. It is easy to verify that $\{P_{\mathbf{z}+C}(r), \mathbf{z} \in \{0, 1\}^n\}$ is a probability mass function, due to the fact that $P_{\mathbf{z}+C}(r) \ge 0$ for any $\mathbf{z} \in \{0, 1\}^n$, and

$$\sum_{\mathbf{z}} P_{\mathbf{z}+C}(r) = 1 \tag{18}$$

Further, by definition, $P_C(r)$ has a close relation with the weight distribution of C and can be represented as

$$P_C(r) = \frac{1}{|C|}(1-r)^n A_C^{\mathrm{w}}\left(\frac{r}{1-r}\right) \tag{19}$$

Therefore, based on the known results on the weight distribution function of C, we derive the following lemma.

Lemma 4.1. *Let C be an (n, k) binary linear code and $\mathbf{z} + C$ be a proper coset of C, where $\mathbf{z} \notin C$. For any $r \in$*

$[0, 1/2]$,

$$P_{z+C}(r) \geq (\frac{r}{1-r})^{n-k} P_C(r), \tag{20}$$

$$P_{z+C}(r) \leq \frac{1-(1-2r)^{k+1}}{1+(1-2r)^{k+1}} P_C(r) \tag{21}$$

Proof. Please refer to Appendix 5 for the proof. □

If C is a binary linear code, whose codewords are equally likely to be chosen for transmission over a BSC(r), then we adopt the notation $P_{ue}(C, r)$, as defined in Reference [5], for the *probability of undetected error*. We further recall that a binary (n, k) linear code C is called *good for error detection* if C satisfies the condition

$$P_{ue}(C, r) \leq 2^{-n}(2^k - 1)$$

for all $r \in [0, 1/2]$; and it is called *satisfactory for error detection* if C satisfies the condition

$$P_{ue}(C, r) \leq 2^{-(n-k)}$$

for all $r \in [0, 1/2]$.

Lemma 4.2. *(Theorem 2.1 in Reference [5]) Let C be a binary (n, k) linear code and $r \in [0, 1/2]$. Then*

$$P_{ue}(C, r) = (1-r)^n \{A_C^w(\frac{r}{1-r}) - 1\}$$

Lemma 4.3. *(Theorems 2.43 and 2.51 in Reference [5]) Let C be a binary (n, k) code and $r \in [0, 1/2]$. Then*

$$P_{ue}(C, r) \geq 2^{-(n-k)} - (1-r)^n, \tag{22}$$

$$P_{ue}(C, r) \leq (1-r)^{n-k} - (1-r)^n \tag{23}$$

4.3. Security analysis

Now we proceed to the security analysis of the the coset-coding scheme. Note that the total information obtained by the wiretapper through his observation is $I(\mathbf{S}; \mathbf{Z})$. We define it as the *information loss* (IL) of the scheme. Clearly for arbitrary $\zeta > 0$, IL $\leq \zeta$ is a stronger security condition than the one given in Equation (4b): $d \geq 1 - \zeta$. Note that we can simply apply Theorem 2 in Reference [6] and thus strengthen the proof given in Section 3. As a result, the same secrecy capacity holds under the stronger condition: IL $\leq \zeta$ for arbitrary $\zeta > 0$.

In order to provide more security guarantee, in this section we are concerned with IL instead of the normalized equivocation of the wiretapper d as defined in Equation (2). First we have the following observation.

Lemma 4.4. $H(\mathbf{Z}|\mathbf{S}) = H(\mathbf{Z}|\mathbf{S} = \mathbf{0})$.

Proof. For given $\mathbf{s}(i)$, $1 \leq i \leq 2^k$, we have

$$\begin{aligned}
&p_{\mathsf{Z}|\mathsf{S}}(\mathbf{z}|\mathbf{s}(i)) \\
&= \sum_{\mathbf{x} \in \mathbf{x}(i)+C_2} p_{\mathsf{X}|\mathsf{S}}(\mathbf{x}|\mathbf{s}(i)) p_{\mathsf{Z}|\mathsf{X},\mathsf{S}}(\mathbf{z}|\mathbf{x}, \mathbf{s}(i)) \\
&\overset{(a)}{=} \frac{1}{2^{k_2}} \sum_{\mathbf{x} \in \mathbf{x}(i)+C_2} p_{\mathsf{Z}|\mathsf{X}}(\mathbf{z}|\mathbf{x}) \\
&\overset{(b)}{=} \frac{1}{2^{k_2}} \sum_{\mathbf{x} \in \mathbf{x}(i)+C_2} p_w^{w(\mathbf{x}+\mathbf{z})}(1-p_w)^{n-w(\mathbf{x}+\mathbf{z})} \\
&= \frac{1}{2^{k_2}} \sum_{\mathbf{v} \in \mathbf{z}+\mathbf{x}(i)+C_2} p_w^{w(\mathbf{v})}(1-p_w)^{n-w(\mathbf{v})},
\end{aligned} \tag{24}$$

where (a) follows the fact that that $p_{\mathsf{X}|\mathsf{S}}(\mathbf{x}|\mathbf{s}(i)) = 1/2^{k_2}$ and $p(\mathbf{z}|\mathbf{x}, \mathbf{s}(i)) = p(\mathbf{z}|\mathbf{x})$; (b) follows the fact that the wiretap channel is a BSC(p_w).

From Equation (24), we see that $p_{\mathsf{Z}|\mathsf{S}}(\mathbf{z}|\mathbf{s}(i))$ is determined by the weight distribution of the coset $\mathbf{z} + \mathbf{x}(i) + C_2$. Note that for given $\mathbf{s}(i)$, $\{\mathbf{z} + \mathbf{x}(i) + C_2, \mathbf{z} \in \{0, 1\}^n\}$ is a permutation of $\{\mathbf{z} + C_2, \mathbf{z} \in \{0, 1\}^n\}$. As a straightforward consequence, $\{p_{\mathsf{Z}|\mathsf{S}}(\mathbf{z}|\mathbf{s}(i)), \mathbf{z} \in \{0, 1\}^n\}$ is a permutation of $\{p_{\mathsf{Z}|\mathsf{S}}(\mathbf{z}|\mathbf{s} = \mathbf{0}), \mathbf{z} \in \{0, 1\}^n\}$. Thus we have $H(\mathbf{Z}|\mathbf{S}) = H(\mathbf{Z}|\mathbf{S} = \mathbf{0})$. □

Recall the definition given in Equation(17). We have the following lemma for $p_{\mathsf{Z}|\mathsf{S}}(\mathbf{z}|\mathbf{s} = \mathbf{0})$ and $p_{\mathsf{Z}}(\mathbf{z})$.

Lemma 4.5. *For any $\mathbf{z} \in \{0, 1\}^n$, we have*

$$p_{\mathsf{Z}|\mathsf{S}}(\mathbf{z}|\mathbf{s} = \mathbf{0}) = P_{\mathsf{z}+C_2}(p_w); \tag{25}$$

$$p_{\mathsf{Z}}(\mathbf{z}) = P_{\mathsf{z}+C_1}(p_w) \tag{26}$$

Proof. According to Equation (7), given $\mathbf{s} = \mathbf{0}$, the codeword $\mathbf{x}$ sent to the channel is chosen randomly from C_2. Therefore, we have

$$\begin{aligned}
p_{\mathsf{Z}|\mathsf{S}}(\mathbf{z}|\mathbf{s} = \mathbf{0}) &= \frac{1}{2^{k_2}} \sum_{\mathbf{v} \in \mathbf{z}+C_2} p_w^{w(\mathbf{v})}(1-p_w)^{n-w(\mathbf{v})} \\
&= P_{\mathsf{z}+C_2}(p_w)
\end{aligned}$$

Furthermore, we consider the probability $p_{\mathsf{Z}}(\mathbf{z})$.

$$\begin{aligned}
&p_{\mathsf{Z}}(\mathbf{z}) \\
&= \sum_{i=1}^{2^k} p_{\mathsf{S}}(\mathbf{s}(i)) \sum_{\mathbf{x} \in \mathbf{x}(i)+C_2} p_{\mathsf{X}|\mathsf{S}}(\mathbf{x}|\mathbf{s}(i)) p_{\mathsf{Z}|\mathsf{X},\mathsf{S}}(\mathbf{z}|\mathbf{x}, \mathbf{s}(i)) \\
&\overset{(a)}{=} \sum_{i=1}^{2^k} \frac{1}{2^k} \sum_{\mathbf{x} \in \mathbf{x}(i)+C_2} \frac{1}{2^{k_2}} p_{\mathsf{Z}|\mathsf{X}}(\mathbf{z}|\mathbf{x}) \\
&\overset{(b)}{=} \frac{1}{2^{k_1}} \sum_{\mathbf{x} \in C_1} p_w^{w(\mathbf{x}+\mathbf{z})}(1-p_w)^{n-w(\mathbf{x}+\mathbf{z})}
\end{aligned}$$

$$= \frac{1}{2^{k_1}} \sum_{\mathbf{v} \in \mathbf{z}+C_1} p_w^{w(\mathbf{v})}(1-p_w)^{n-w(\mathbf{v})}$$
$$= P_{\mathbf{z}+C_1}(p_w)$$

where (a) follows the fact that $p_{\mathbf{S}}(\mathbf{s}(i)) = 1/2^k$, $p_{\mathbf{X}|\mathbf{S}}(\mathbf{x}|\mathbf{s}) = 1/2^{k_2}$ and $p_{\mathbf{Z}|\mathbf{X},\mathbf{S}}(\mathbf{z}|\mathbf{x}, \mathbf{s}(i)) = p_{\mathbf{Z}|\mathbf{X}}(\mathbf{z}|\mathbf{x})$; (b) follows the fact that $k_1 = k + k_2$ and the wiretap channel is a BSC(p_w). □

Now we give an upper bound on IL in the following theorem.

Theorem 4.6. *(An upper bound on IL)*

$$IL \leq \log[2^n P_{C_2}(p_w)] = \log A^{\mathrm{w}}_{C_2^\perp}(1-2p_w) \tag{27}$$

Proof. By definition, $\mathrm{IL} = I(\mathbf{S};\mathbf{Z})$. Therefore, we have

$$\begin{aligned}
\mathrm{IL} &= I(\mathbf{S};\mathbf{Z}) \\
&= H(\mathbf{Z}) - H(\mathbf{Z}|\mathbf{S}) \\
&\overset{(a)}{=} H(\mathbf{Z}) - H(\mathbf{Z}|\mathbf{S}=\mathbf{0}) \\
&= \sum_{\mathbf{z}} p_{\mathbf{Z}|\mathbf{S}}(\mathbf{z}|\mathbf{s}=\mathbf{0}) \log p_{\mathbf{Z}|\mathbf{S}}(\mathbf{z}|\mathbf{s}=\mathbf{0}) \\
&\quad - \sum_{\mathbf{z}} p_{\mathbf{Z}}(\mathbf{z}) \log p_{\mathbf{Z}}(\mathbf{z}) \\
&\overset{(b)}{=} \sum_{\mathbf{z}} P_{\mathbf{z}+C_2}(p_w) \log P_{\mathbf{z}+C_2}(p_w) \\
&\quad - \sum_{\mathbf{z}} P_{\mathbf{z}+C_1}(p_w) \log P_{\mathbf{z}+C_1}(p_w) \\
&= \sum_{\mathbf{z}} P_{\mathbf{z}+C_2}(p_w) \log \frac{P_{\mathbf{z}+C_2}(p_w)}{P_{C_2}(p_w)} \\
&\quad + \sum_{\mathbf{z}} P_{\mathbf{z}+C_1}(p_w) \log \frac{P_{C_2}(p_w)}{P_{\mathbf{z}+C_1}(p_w)}
\end{aligned}$$

where (a) is due to Lemma 4.4 and (b) is due to Lemma 4.5. Further we let

$$\mathrm{IL}_1 = \sum_{\mathbf{z}} P_{\mathbf{z}+C_2}(p_w) \log \frac{P_{\mathbf{z}+C_2}(p_w)}{P_{C_2}(p_w)}; \tag{28}$$

$$\mathrm{IL}_2 = \sum_{\mathbf{z}} P_{\mathbf{z}+C_1}(p_w) \log \frac{P_{C_2}(p_w)}{P_{\mathbf{z}+C_1}(p_w)} \tag{29}$$

Then we obtain $\mathrm{IL} = \mathrm{IL}_1 + \mathrm{IL}_2$.
For IL_1, we apply Lemma 4.1 and obtain

$$\begin{aligned}
\mathrm{IL}_1 &\leq [\sum_{\mathbf{z} \notin C_2} P_{\mathbf{z}+C_2}(p_w)] \log \frac{1-(1-2p_w)^{k_2+1}}{1+(1-2p_w)^{k_2+1}} \\
&\leq 0
\end{aligned} \tag{30}$$

For IL_2, we apply the log-sum inequality as given in Lemma A.1 and obtain

$$\mathrm{IL}_2 \leq \log[2^n P_{C_2}(p_w)] \tag{31}$$

Combining Equations (30) and (31), we thus prove that $\mathrm{IL} \leq \log[2^n P_{C_2}(p_w)]$.

In the following, we show that $2^n P_{C_2}(p_w) = A^{\mathrm{w}}_{C_2^\perp}(1-2p_w)$ by considering

$$\begin{aligned}
2^n P_{C_2}(p_w) &\overset{(c)}{=} 2^{n-k_2}(1-p_w)^n A^{\mathrm{w}}_{C_2}(\frac{p_w}{1-p_w}) \\
&\overset{(d)}{=} A^{\mathrm{w}}_{C_2^\perp}(1-2p_w)
\end{aligned} \tag{32}$$

where (c) is by Equation (19) and (d) is due to the MacWilliam's identity as given in Lemma A.2. Here $C_2^\perp$ is the dual code of the linear code C_2. □

Lemma 4.7. $1 \leq A^{\mathrm{w}}_{C_2^\perp}(1-2p_w) \leq [2(1-p_w)]^{n-k_2}$

Proof. By Lemma 4.2, we have

$$A^{\mathrm{w}}_{C_2^\perp}(1-2p_w) = 1 + [2(1-p_w)]^n P_{\mathrm{ue}}(C_2^\perp, \frac{1-2p_w}{2-2p_w})$$

It is clear that $A^{\mathrm{w}}_{C_2^\perp}(1-2p_w) \geq 1$. Further we have

$$\begin{aligned}
A^{\mathrm{w}}_{C_2^\perp}(1-2p_w) &\overset{(a)}{=} 2^{n-k_2}(1-p_w)^n A^{\mathrm{w}}_{C_2}(\frac{p_w}{1-p_w}) \\
&\overset{(b)}{=} 2^{n-k_2}[(1-p_w)^n + P_{\mathrm{ue}}(C_2, p_w)]
\end{aligned}$$

where (a) is by Equation (32) and (b) is by Lemma 4.2. In addition, by Lemma 4.3,

$$P_{\mathrm{ue}}(C_2, p_w) \leq (1-p_w)^{n-k_2} - (1-p_w)^n$$

We apply it to the above equation and thus have

$$\begin{aligned}
A^{\mathrm{w}}_{C_2^\perp}(1-2p_w) &\leq 2^{n-k_2} \cdot (1-p_w)^{n-k_2} \\
&= [2(1-p_w)]^{n-k_2}
\end{aligned}$$

□

Following directly from Theorem 4.6 and Lemma 4.7, we have the following corollary.

Corollary 4.8. $IL \leq (n-k_2)[1+\log(1-p_w)]$

Let $R_2 = k_2/n$ and $\gamma = 2^{(1-R_2)}(1-p_w)$. Consider the special case where $C_2^\perp$ is satisfactory for error detection. We have

Lemma 4.9. *If $C_2^\perp$ is satisfactory for error detection, then*

$$1 \leq A^{\mathrm{w}}_{C_2^\perp}(1-2p_w) \leq 1+\gamma^n \tag{33}$$

Proof. Recall that by Lemma 4.2,

$$A^{\mathrm{w}}_{C_2^\perp}(1-2p_w) = 1 + [2(1-p_w)]^n P_{\mathrm{ue}}(C_2^\perp, \frac{1-2p_w}{2-2p_w}).$$

If $C_2^\perp$ is satisfactory for error detection, then by definition

$$P_{\mathrm{ue}}(C_2^\perp, \frac{1-2p_w}{2-2p_w}) \le 2^{-k_2}$$

Therefore, we have

$$\begin{aligned} A^{\mathrm{w}}_{C_2^\perp}(1-2p_w) &\le 1 + 2^{n-k_2}(1-p_w)^n \\ &= 1 + [2^{(1-R_2)}(1-p_w)]^n = 1+\gamma^n \end{aligned}$$

□

As a direct consequence of Lemma 4.9, we have the following corollary.

Corollary 4.10. *If $C_2^\perp$ is satisfactory for error detection, then*

$$IL \le \gamma^n \tag{34}$$

In the following, we consider $2^n P_{C_2}(p_w)$ (thus $A^{\mathrm{w}}_{C_2^\perp}(1-2p_w)$) as a random variable and investigate its first moment $\mathrm{E}_{\mathrm{H}_2}[2^n P_{C_2}(p_w)]$ and the second moment $\mathrm{E}_{\mathrm{H}_2}[(2^n P_{C_2}(p_w))^2]$ over all possible binary matrices H_2 of full rank. We show that under certain constraint, our bound given in Theorem 4.6 is asymptotically tight.

Lemma 4.11. *(First and second moments of $2^n P_{C_2}(p_w)$)*

$$\mathrm{E}_{\mathrm{H}_2}[2^n P_{C_2}(p_w)] = \gamma^n + \theta_1[1-(1-p_w)^n]; \tag{35}$$

$$\begin{aligned} &\mathrm{E}_{\mathrm{H}_2}[(2^n P_{C_2}(p_w))^2] \\ &\quad = \theta_1\theta_2 + \gamma^{2n} + 2\theta_1\gamma^n + \theta_{t_1} + \theta_{t_2} \end{aligned} \tag{36}$$

where $R_2 = k_2/n$, $\gamma = 2^{(1-R_2)}(1-p_w)$ as having been defined, and

$$\begin{aligned} \theta_1 &= (2^n - 2^{n-k_2})/(2^n-1); \\ \theta_2 &= (2^n - 2^{n-k_2+1})/(2^n-2); \\ \theta_{t_1} &= \theta_1\gamma^n\{[(p_w^2+(1-p_w)^2)/(1-p_w)]^n \\ &\quad -3(1-p_w)^n\}; \\ \theta_{t_2} &= -\theta_1\theta_2\{[p_w^2+(1-p_w)^2]^n + 2(1-p_w)^n \\ &\quad -2(1-p_w)^{2n}\} \end{aligned}$$

Proof. Please refer to Appendix D for the detailed proof. □

Lemma 4.12. *If $R_2 > 1+\log(1-p_w)$, then $\gamma < 1$ and*

$$\lim_{n\to\infty} \mathrm{E}_{\mathrm{H}_2}[2^n P_{C_2}(p_w)] = 1 \tag{37}$$

Proof. If $R_2 > 1+\log(1-p_w)$, then $\gamma = 2^{(1-R_2)}(1-p_w) < 1$. As $n\to\infty$, clearly $\gamma^n \to 0$. Besides, as $0 < p_w \le 1/2$, we have $1/2 \le 1-p_w < 1$ and thus $(1-p_w)^n \to 0$ as $n\to\infty$. In addition that $\theta_1 \to 1$ as $n\to\infty$, as a result we obtain

$$\begin{aligned} &\lim_{n\to\infty} \mathrm{E}_{\mathrm{H}_2}[2^n P_{C_2}(p_w)] \\ &= \lim_{n\to\infty}\{\gamma^n + \theta_1[1-(1-p_w)^n]\} = 1 \end{aligned}$$

□

Theorem 4.13. *If $R_2 > 1+\log(1-p_w)$, for any $\epsilon > 0$,*

$$\Pr\{2^n P_{C_2}(p_w) \le 2^\epsilon\} \to 1, \quad \text{as } n\to\infty \tag{38}$$

Proof. By Lemma 4.12, if $R_2 > 1+\log(1-p_w)$, then $\lim_{n\to\infty} \mathrm{E}_{\mathrm{H}_2}[2^n P_{C_2}(p_w)] = 1$. This implies that for any $\epsilon > 0$, there is an N', when $n > N'$, we have

$$\mathrm{E}_{\mathrm{H}_2}[2^n P_{C_2}(p_w)] < 1 + \epsilon/2 \tag{39}$$

Furthermore, we have $\Pr\{2^n P_{C_2}(p_w) \le 2^\epsilon\} = 1 - \Pr\{2^n P_{C_2}(p_w) > 2^\epsilon\}$. Let

$$\mathrm{DEV}[2^n P_{C_2}(p_w)] = 2^n P_{C_2}(p_w) - \mathrm{E}_{\mathrm{H}_2}[2^n P_{C_2}(p_w)].$$

Then when $n > N'$,

$$\begin{aligned} &\Pr\{2^n P_{C_2}(p_w) > 2^\epsilon\} \\ &= \Pr\{\mathrm{DEV}[2^n P_{C_2}(p_w)] > 2^\epsilon - \mathrm{E}_{\mathrm{H}_2}[2^n P_{C_2}(p_w)]\} \\ &\overset{(a)}{\le} \Pr\{\mathrm{DEV}[2^n P_{C_2}(p_w)] > 2^\epsilon - 1 - \epsilon/2\} \\ &\le \Pr\{(\mathrm{DEV}[2^n P_{C_2}(p_w)])^2 > (2^\epsilon - 1 - \epsilon/2)^2\} \end{aligned}$$

where (a) follows from the fact that $\mathrm{E}_{\mathrm{H}_2}[2^n P_{C_2}(p_w)] < 1 + \epsilon/2$ as $n > N'$.

We denote $\mathrm{VAR}[2^n P_{C_2}(p_w)]$ for the variance of $2^n P_{C_2}(p_w)$. Then

$$\begin{aligned} &\mathrm{VAR}[2^n P_{C_2}(p_w)] = \mathrm{E}_{\mathrm{H}_2}[(\mathrm{DEV}[2^n P_{C_2}(p_w)])^2] \\ &= \mathrm{E}_{\mathrm{H}_2}[(2^n P_{C_2}(p_w) - \mathrm{E}_{\mathrm{H}_2}[2^n P_{C_2}(p_w)])^2] \\ &= \mathrm{E}_{\mathrm{H}_2}[(2^n P_{C_2}(p_w))^2] - (\mathrm{E}_{\mathrm{H}_2}[2^n P_{C_2}(p_w)])^2 \\ &\overset{(b)}{=} \theta_1\theta_2 + \theta_{t_1} + \theta_{t_2} + 2\theta_1(1-p_w)^n \\ &\quad -\theta_1^2[1-(1-p_w)^n]^2, \end{aligned}$$

where (b) is by Lemma 4.11. Note that as $n\to\infty$, it is easy to verify that $\theta_1 \to 1, \theta_2 \to 1$ and $\theta_{t_2} \to 0$. If $R_2 >$

$1 + \log(1 - p_w)$, then $\theta_{t_1} \to 0$ and thus the variance of $2^n P_{C_2}(p_w)$ approaches to 0 as $n \to \infty$, i.e.,

$$\mathrm{VAR}[2^n P_{C_2}(p_w)] \to 0, \quad n \to \infty$$

Based on this argument and Chebyshev's inequality, we have

$$\begin{aligned}
&\Pr\{2^n P_{C_2}(p_w) > 2^\epsilon\} \\
&\le \Pr\{(\mathrm{DEV}[2^n P_{C_2}(p_w)])^2 > (2^\epsilon - 1 - \epsilon/2)^2\} \\
&\le \frac{\mathrm{VAR}[2^n P_{C_2}(p_w)]}{(2^\epsilon - 1 - \epsilon/2)^2} \to 0, \quad n \to \infty
\end{aligned}$$

Thus we have

$$\begin{aligned}
&\Pr\{2^n P_{C_2}(p_w) \le 2^\epsilon\} \\
&= 1 - \Pr\{2^n P_{C_2}(p_w) > 2^\epsilon\} \to 1, \quad n \to \infty
\end{aligned}$$

□

As a conclusion of above discussion, C_2 plays a crucial role in ensuring the secure transmission. For coset codes of short length, the one which minimizes $2^n P_{C_2}(p_w)$ might be a good candidate of C_2 by Theorem 4.6. Lighted by Lemma 4.9, codes, whose dual codes are satisfactory or good for error detection, can be good choices for C_2 especially when $R_2 > 1 + \log(1 - p_w)$. If we allow n to grow, by Theorem 4.13 one can bound the information leakage arbitrarily small, once we add enough randomness into the coding scheme via C_2. In fact, $1 + \log(1 - p_w)$ is the maximum information loss per transmission bit limited by the wiretap channel itself by Corollary 4.8. We further note that when $R_2 > 1 + \log(1 - p_w)$, then $R_2 \ge 1 - h(p_w)$. That is, more than enough randomness has been added into the scheme via C_2 so as to ensure the secrecy. As a direct consequence, there is a sacrifice on the efficiency. The maximum secret rate in this case is $-\log(1 - p_w) - h(p)$ instead of $h(p_w) - h(p)$.

5. CONCLUSION

In this paper, we investigate the binary symmetric wiretap channel. We give a detailed proof that its secrecy capacity can be achieved by using random linear codes. The coset-coding method used in our proof is not strictly new. It is implicitly contained in the proof given by Wyner [1] for the special case when the main channel is noiseless and the wiretap channel is a BSC. Note that for that case, the transmitter does not need to think of the reliability of the transmission to the legitimate receiver since the main channel is noiseless. However, in our case, we need to design a secrecy capacity achieving coding scheme which guarantees both the reliability and the security of the transmission at the same time.

Random linear code has a simple code structure and performs well but unfortunately involves a rather impractical decoder. Therefore, we explore the coset-coding scheme and give an upper bound on its total information loss. The bound implies the significance of C_2 in limiting the information leakage and gives hints on how to choose a satisfactory C_2. In particular, due to its close relation with the concept of undetected error probability, numerous results on codes for error detection can be applied to the design of applicable coset codes. Further we show that the bound is asymptotically tight under the constraint $R_2 \ge 1 + \log(1 - p_w)$. Last but not least, we point out that the scheme has a sacrifice on efficiency and is not very suitable for the case when $p < p_w \le 1 - 2^{-h(p)}$.

APPENDIX A: LOG-SUM INEQUALITY AND MACWILLIAM'S IDENTITY

Lemma A.1. *(The Log-Sum Inequality) For arbitrary nonnegative numbers $p_1, \cdots, p_t$ and $q_1, \cdots, q_t$,*

$$\sum_{i=1}^{t} p_i \log \frac{p_i}{q_i} \ge (\sum_{i=1}^{t} p_i) \log \frac{\sum_{i=1}^{t} p_i}{\sum_{i=1}^{t} q_i} \tag{A.1}$$

with equality if and only if $p_i = cq_i$, $1 \le i \le t$. Here $p \log \frac{p}{q}$ is defined to be 0 if $p = 0$ and $+\infty$ if $p > q = 0$.

Lemma A.2. *(Theorem 1.14 in Reference [5]) Let C be a binary (n, k) linear code. Then*

$$A^{\mathrm{w}}_{C^\perp}(z) = \frac{1}{2^k}(1 + z)^n A^{\mathrm{w}}_C(\frac{1 - z}{1 + z}) \tag{A.2}$$

APPENDIX B: PROOF OF LEMMA 4.1

We first recall the following result, regarding the weight distribution function of a proper coset of a linear code.

Theorem B.1. *(Theorem 1.18 & Theorem 1.19 in Reference [5]) Let C be an (n, k) binary code and S a proper coset of C. Then*

$$z^{n-k} A^{\mathrm{w}}_C(z) \le A^{\mathrm{w}}_S(z) \le \frac{1 - y^{k+1}}{1 + y^{k+1}} A^{\mathrm{w}}_C(z) \tag{B.1}$$

for all $z \in [0, 1]$, where $y = (1 - z)/(1 + z)$.

The proof of Lemma 4.1 is given as follows.

Proof. Recall the relation of $P_C(r)$ and the weight distribution of C as illustrated in Equation (19). We have

$$\begin{aligned}
P_C(r) &= \frac{1}{|C|}(1 - r)^n A^{\mathrm{w}}_C(\frac{r}{1 - r}); \\
P_{\mathbf{z}+C}(r) &= \frac{1}{|\mathbf{z} + C|}(1 - r)^n A^{\mathrm{w}}_{\mathbf{z}+C}(\frac{r}{1 - r}) \\
&\overset{(a)}{=} \frac{1}{|C|}(1 - r)^n A^{\mathrm{w}}_{\mathbf{z}+C}(\frac{r}{1 - r}),
\end{aligned}$$

where (a) follows directly from the fact that C and its coset $\mathbf{z}+C$ have the same cardinality. Therefore, we have

$$\frac{P_{\mathbf{z}+C}(r)}{P_C(r)} = \frac{A^{\mathrm{w}}_{\mathbf{z}+C}(\frac{r}{1-r})}{A^{\mathrm{w}}_{C}(\frac{r}{1-r})}$$

and

$$(\frac{r}{1-r})^{n-k} \overset{(b)}{\leq} \frac{P_{\mathbf{z}+C}(r)}{P_C(r)} \overset{(b)}{\leq} \frac{1-(1-2r)^{k+1}}{1+(1-2r)^{k+1}}$$

where (b) follows directly from Theorem B.1. □

APPENDIX C: CONVERGENCE OF THE WEIGHT DISTRIBUTION

Let C_2 be an (n, k_2) binary linear code, and H_2 be its parity check matrix. We denote its weight distribution to be $\{A^{\mathrm{w}}_i, 0 \leq i \leq n\}$. Consider the expectation of A^{w}_i over all possible (n, k_2) binary linear codes, which is the same over all possible H_2 of full rank. We denote M for the number of all possible H_2 of full rank; M_1 for the number of H_2 of full rank which satisfies $\mathbf{x}\mathrm{H}_2^{\mathrm{T}} = \mathbf{0}$, where $\mathbf{x} \neq \mathbf{0}$; M_2 for the number of H_2 of full rank which satisfies $\mathbf{x}\mathrm{H}_2^{\mathrm{T}} = \mathbf{y}\mathrm{H}_2^{\mathrm{T}} = \mathbf{0}$, where $\mathbf{x} \neq \mathbf{y}$ and $\mathbf{x}, \mathbf{y} \neq \mathbf{0}$. Simply by counting, we have

$$\begin{aligned} M &= (2^n-1)\cdot(2^n-2)\cdots(2^n-2^{n-k_2-1}); \\ M_1 &= (2^{n-1}-1)\cdot(2^{n-1}-2)\cdots(2^{n-1}-2^{n-k_2-1}); \\ M_2 &= (2^{n-2}-1)\cdot(2^{n-2}-2)\cdots(2^{n-2}-2^{n-k_2-1}) \end{aligned}$$

It is easy to verify that $M_1/M = \theta_1 2^{-(n-k_2)}$ and $M_2/M = \theta_1\theta_2 2^{-2(n-k_2)}$, where θ_1, θ_2 are as defined in Lemma 4.11.

Lemma C.1.

$$\mathrm{E}_{\mathrm{H}_2}[A^{\mathrm{w}}_i] = \begin{cases} 1 & i = 0 \\ \theta_1 \binom{n}{i} 2^{-(n-k_2)} & i \neq 0 \end{cases} \tag{C.1}$$

Proof. It is clear that $A^{\mathrm{w}}_0 = 1$ holds for all possible C_2, which gives $\mathrm{E}_{\mathrm{H}_2}[A^{\mathrm{w}}_0] = 1$.

In the following, we assume that $i \neq 0$. Note that from the definition of A^{w}_i, it is equal to the number of the binary sequences in C_2, which are of length n and have Hamming weight i. That is, for given C_2 and H_2, $A^{\mathrm{w}}_i = \sum_{\mathbf{x}} \mathbf{1}[w(\mathbf{x}) = i, \mathbf{x}\mathrm{H}_2^{\mathrm{T}} = \mathbf{0}]$.

$$\begin{aligned} \mathrm{E}_{\mathrm{H}_2}[A^{\mathrm{w}}_i] &= \frac{1}{M}\sum_{\mathrm{H}_2}\sum_{\mathbf{x}} \mathbf{1}[w(\mathbf{x}) = i, \mathbf{x}\mathrm{H}_2^{\mathrm{T}} = \mathbf{0}] \\ &= \frac{1}{M}\sum_{\mathbf{x}} \mathbf{1}[w(\mathbf{x}) = i] \sum_{\mathrm{H}_2} \mathbf{1}[\mathbf{x}\mathrm{H}_2^{\mathrm{T}} = \mathbf{0}] \\ &= \frac{1}{M}\cdot M_1 \cdot \sum_{\mathbf{x}} \mathbf{1}[w(\mathbf{x}) = i] \\ &= \theta_1 \binom{n}{i} 2^{-(n-k_2)} \end{aligned}$$

□

Lemma C.2. *Let θ_1, θ_2 be as defined in Lemma 4.11. Then*

□*if $i = 0$, $j = 0$,*

$$\mathrm{E}_{\mathrm{H}_2}[A^{\mathrm{w}}_i \cdot A^{\mathrm{w}}_j] = 1$$

□*if $i = 0$, $j \neq 0$,*

$$\mathrm{E}_{\mathrm{H}_2}[A^{\mathrm{w}}_i \cdot A^{\mathrm{w}}_j] = \theta_1 \binom{n}{j} 2^{-(n-k_2)}$$

□*if $i \neq 0$, $j = 0$,*

$$\mathrm{E}_{\mathrm{H}_2}[A^{\mathrm{w}}_i \cdot A^{\mathrm{w}}_j] = \theta_1 \binom{n}{i} 2^{-(n-k_2)}$$

□*if $i \neq 0$, $j \neq 0$, $i = j$,*

$$\begin{aligned} \mathrm{E}_{\mathrm{H}_2}[A^{\mathrm{w}}_i \cdot A^{\mathrm{w}}_j] &= \theta_1 \binom{n}{i} 2^{-(n-k_2)} \\ &\quad + \theta_1\theta_2 \binom{n}{i} [\binom{n}{i} - 1] 2^{-2(n-k_2)} \end{aligned}$$

□*if $i \neq 0$, $j \neq 0$, $i \neq j$,*

$$\mathrm{E}_{\mathrm{H}_2}[A^{\mathrm{w}}_i \cdot A^{\mathrm{w}}_j] = \theta_1\theta_2 \binom{n}{i}\binom{n}{j} 2^{-2(n-k_2)}$$

Proof. If $i = 0$, $j = 0$, then $A^{\mathrm{w}}_i = A^{\mathrm{w}}_j = 1$ for every possible C_2. Thus we have $\mathrm{E}_{\mathrm{H}_2}[A^{\mathrm{w}}_0 \cdot A^{\mathrm{w}}_0] = 1$.

If $i = 0$, $j \neq 0$, then $A^{\mathrm{w}}_i = 1$ for every possible C_2. Thus we have

$$\mathrm{E}_{\mathrm{H}_2}[A^{\mathrm{w}}_0 \cdot A^{\mathrm{w}}_j] = \mathrm{E}_{\mathrm{H}_2}[A^{\mathrm{w}}_j] \overset{(a)}{=} \theta_1 \binom{n}{j} 2^{-(n-k_2)}$$

where (a) is by Lemma C.1. A similar proof can be applied to the case $i \neq 0$, $j = 0$.

If $i \neq 0$, $j \neq 0$ and $i = j$, then we have

$$\begin{aligned} &\mathrm{E}_{\mathrm{H}_2}[A^{\mathrm{w}}_i \cdot A^{\mathrm{w}}_j] \\ &= \frac{1}{M}\sum_{\mathrm{H}_2}\sum_{\mathbf{x}} \mathbf{1}[w(\mathbf{x}) = i, \mathbf{x}\mathrm{H}_2^{\mathrm{T}} = \mathbf{0}] \\ &\quad \cdot \sum_{\mathbf{y}} \mathbf{1}[w(\mathbf{y}) = j, \mathbf{y}\mathrm{H}_2^{\mathrm{T}} = \mathbf{0}] \\ &= \frac{1}{M}\sum_{\mathrm{H}_2}\sum_{\mathbf{x}=\mathbf{y}} \mathbf{1}[w(\mathbf{x}) = i, \mathbf{x}\mathrm{H}_2^{\mathrm{T}} = \mathbf{0}] \\ &\quad + \frac{1}{M}\sum_{\mathrm{H}_2}\sum_{\mathbf{x}\neq\mathbf{y}} \mathbf{1}[w(\mathbf{x}) = w(\mathbf{y}) = i, \mathbf{x}\mathrm{H}_2^{\mathrm{T}} = \mathbf{y}\mathrm{H}_2^{\mathrm{T}} = \mathbf{0}] \\ &= \mathrm{E}_{\mathrm{H}_2}[A^{\mathrm{w}}_i] \end{aligned}$$

$$+\frac{1}{M}\sum_{\mathrm{x}\neq\mathrm{y}}\mathbf{1}[w(\mathbf{x})=w(\mathbf{y})=i]\cdot\sum_{\mathrm{H}_2}\mathbf{1}[\mathbf{x}\mathrm{H}_2^{\mathrm{T}}=\mathbf{y}\mathrm{H}_2^{\mathrm{T}}=\mathbf{0}]$$

$$=\mathrm{E}_{\mathrm{H}_2}[A_i^{\mathrm{w}}]+\frac{1}{M}\cdot M_2\cdot\sum_{\mathrm{x}\neq\mathrm{y}}\mathbf{1}[w(\mathbf{x})=w(\mathbf{y})=i]$$

$$=\mathrm{E}_{\mathrm{H}_2}[A_i^{\mathrm{w}}]+\theta_1\theta_2\binom{n}{i}[\binom{n}{i}-1]2^{-2(n-k_2)}$$

$$=\theta_1\binom{n}{i}2^{-(n-k_2)}+\theta_1\theta_2\binom{n}{i}[\binom{n}{i}-1]2^{-2(n-k_2)}$$

If $i\neq 0$, $j\neq 0$ and $i\neq j$, then we have

$$\mathrm{E}_{\mathrm{H}_2}[A_i^{\mathrm{w}}\cdot A_j^{\mathrm{w}}]$$

$$=\frac{1}{M}\sum_{\mathrm{H}_2}\sum_{\mathrm{x}}\mathbf{1}[w(\mathbf{x})=i,\mathbf{x}\mathrm{H}_2^{\mathrm{T}}=\mathbf{0}]$$

$$\cdot\sum_{\mathrm{y}}\mathbf{1}[w(\mathbf{y})=j,\mathbf{y}\mathrm{H}_2^{\mathrm{T}}=\mathbf{0}]$$

$$=\frac{1}{M}\sum_{\mathrm{x}}\mathbf{1}[w(\mathbf{x})=i]\cdot\sum_{\mathrm{y}}\mathbf{1}[w(\mathbf{y})=j]$$

$$\cdot\sum_{\mathrm{H}_2}\mathbf{1}[\mathbf{x}\mathrm{H}_2^{\mathrm{T}}=\mathbf{y}\mathrm{H}_2^{\mathrm{T}}=\mathbf{0}]$$

$$=\frac{1}{M}\cdot M_2\sum_{\mathrm{x}}\mathbf{1}[w(\mathbf{x})=i]\cdot\sum_{\mathrm{y}}\mathbf{1}[w(\mathbf{y})=j]$$

$$=\theta_1\theta_2\binom{n}{i}\binom{n}{j}2^{-2(n-k_2)}$$

□

APPENDIX D: PROOF OF LEMMA 4.11

By Lemma C.1, we easily prove the Equation (35), which is the first part of Lemma 4.11.

$$\mathrm{E}_{\mathrm{H}_2}[2^nP_{C_2}(p_w)]$$

$$=\mathrm{E}_{\mathrm{H}_2}[2^{n-k_2}\sum_{i=0}^{n}A_i^{\mathrm{w}}p_w^i(1-p_w)^{n-i}]$$

$$=2^{n-k_2}\sum_{i=0}^{n}\mathrm{E}_{\mathrm{H}_2}[A_i^{\mathrm{w}}]p_w^i(1-p_w)^{n-i}$$

$$=2^{n-k_2}(1-p_w)^n+\sum_{i=1}^{n}\theta_1\binom{n}{i}p_w^i(1-p_w)^{n-i}$$

$$=2^{n-k_2}(1-p_w)^n+\theta_1[1-(1-p_w)^n]$$

$$=\gamma^n+\theta_1[1-(1-p_w)^n]$$

Now we prove the Equation (36), which is the second part of Lemma 4.11, as follows:

$$\mathrm{E}_{\mathrm{H}_2}[(2^nP_{C_2}(p_w))^2]$$

$$=\mathrm{E}_{\mathrm{H}_2}[(2^{n-k_2}\sum_{i=0}^{n}A_i^{\mathrm{w}}p_w^i(1-p_w)^{n-i})^2]$$

$$=2^{2(n-k_2)}\cdot$$

$$\mathrm{E}_{\mathrm{H}_2}[\sum_{i=0}^{n}A_i^{\mathrm{w}}p_w^i(1-p_w)^{n-i}\cdot\sum_{j=0}^{n}A_j^{\mathrm{w}}p_w^j(1-p_w)^{n-j}]$$

$$=2^{2(n-k_2)}\sum_{i=0}^{n}\sum_{j=0}^{n}\mathrm{E}_{\mathrm{H}_2}[A_i^{\mathrm{w}}\cdot A_j^{\mathrm{w}}]p_w^{i+j}(1-p_w)^{2n-i-j}$$

Applying Lemma C.2, we calculate $\mathrm{E}_{\mathrm{H}_2}[(2^nP_{C_2}(p_w))^2]$ as a sum of the following five cases.

For $i=0$, $j=0$, we have

$$2^{2(n-k_2)}\sum_{i=0}^{n}\sum_{j=0}^{n}\mathrm{E}_{\mathrm{H}_2}[A_i^{\mathrm{w}}\cdot A_j^{\mathrm{w}}]p_w^{i+j}(1-p_w)^{2n-i-j}$$

$$=2^{2(n-k_2)}(1-p_w)^{2n}$$

$$=\gamma^{2n}$$

For $i=0$, $j\neq 0$, we have

$$2^{2(n-k_2)}\sum_{i=0}^{n}\sum_{j\neq 0}^{n}\mathrm{E}_{\mathrm{H}_2}[A_i^{\mathrm{w}}\cdot A_j^{\mathrm{w}}]p_w^{i+j}(1-p_w)^{2n-i-j}$$

$$=2^{2(n-k_2)}\sum_{j\neq 0}\theta_1\binom{n}{j}2^{-(n-k_2)}p_w^j(1-p_w)^{2n-j}$$

$$=\theta_1 2^{n-k_2}(1-p_w)^n\sum_{j\neq 0}\binom{n}{j}p_w^j(1-p_w)^{n-j}$$

$$=\theta_1\gamma^n[1-(1-p_w)^n]$$

$$=\theta_1\gamma^n-\theta_1\gamma^n(1-p_w)^n$$

For $i\neq 0$, $j=0$, similar to the case $i=0$, $j\neq 0$, we have

$$2^{2(n-k_2)}\sum_{i\neq 0}^{n}\sum_{j=0}^{n}\mathrm{E}_{\mathrm{H}_2}[A_i^{\mathrm{w}}\cdot A_j^{\mathrm{w}}]p_w^{i+j}(1-p_w)^{2n-i-j}$$

$$=\theta_1\gamma^n-\theta_1\gamma^n(1-p_w)^n$$

For $i\neq 0$, $j\neq 0$ and $i=j$, we have

$$2^{2(n-k_2)}\sum_{i\neq 0}^{n}\sum_{j=i}^{n}\mathrm{E}_{\mathrm{H}_2}[A_i^{\mathrm{w}}\cdot A_j^{\mathrm{w}}]p_w^{i+j}(1-p_w)^{2n-i-j}$$

$$=2^{2(n-k_2)}\sum_{i\neq 0}\mathrm{E}_{\mathrm{H}_2}[A_i^{\mathrm{w}}\cdot A_i^{\mathrm{w}}]p_w^{2i}(1-p_w)^{2n-2i}$$

$$
\begin{aligned}
&= 2^{2(n-k_2)}\sum_{i\neq 0}\{\theta_1\binom{n}{i}2^{-(n-k_2)}+\theta_1\theta_2\binom{n}{i}^2 2^{-2(n-k_2)}\\
&\quad -\theta_1\theta_2\binom{n}{i}2^{-2(n-k_2)}\}p_w^{2i}(1-p_w)^{2n-2i}\\
&= \theta_1 2^{n-k_2}\sum_{i\neq 0}\binom{n}{i}p_w^{2i}(1-p_w)^{2n-2i}\\
&\quad +\theta_1\theta_2\sum_{i\neq 0}\binom{n}{i}^2 p_w^{2i}(1-p_w)^{2n-2i}\\
&\quad -\theta_1\theta_2\sum_{i\neq 0}\binom{n}{i}p_w^{2i}(1-p_w)^{2n-2i}\\
&= \theta_1 2^{n-k_2}[(p_w^2+(1-p_w)^2)^n-(1-p_w)^{2n}]\\
&\quad +\theta_1\theta_2\sum_{i\neq 0}\binom{n}{i}^2 p_w^{2i}(1-p_w)^{2n-2i}\\
&\quad -\theta_1\theta_2[(p_w^2+(1-p_w)^2)^n-(1-p_w)^{2n}]\\
&= \theta_1\gamma^n[(p_w^2+(1-p_w)^2)/(1-p_w)]^n-\theta_1\gamma^n(1-p_w)^n\\
&\quad -\theta_1\theta_2(p_w^2+(1-p_w)^2)^n+\theta_1\theta_2(1-p_w)^{2n}\\
&\quad +\theta_1\theta_2\sum_{i\neq 0}\binom{n}{i}^2 p_w^{2i}(1-p_w)^{2n-2i}
\end{aligned}
$$

For $i\neq 0$, $j\neq 0$ and $i\neq j$, we have

$$
\begin{aligned}
&2^{2(n-k_2)}\sum_{i\neq 0}\sum_{j\neq 0,i}\mathrm{E}_{\mathrm{H}_2}[A_i^{\mathrm{w}}\cdot A_j^{\mathrm{w}}]p_w^{i+j}(1-p_w)^{2n-i-j}\\
&= \theta_1\theta_2\sum_{i\neq 0}\sum_{j\neq 0,i}\binom{n}{i}\binom{n}{j}p_w^{i+j}(1-p_w)^{2n-i-j}\\
&= \theta_1\theta_2\{1-\sum_{i\neq 0}\sum_{j=i}\binom{n}{i}\binom{n}{j}p_w^{i+j}(1-p_w)^{2n-i-j}\\
&\quad -\sum_{i=0}\sum_{j\neq 0}\binom{n}{j}p_w^{j}(1-p_w)^{2n-j}\\
&\quad -\sum_{i\neq 0}\sum_{j=0}\binom{n}{i}p_w^{i}(1-p_w)^{2n-i}-(1-p_w)^{2n}\}\\
&= \theta_1\theta_2\{1-\sum_{i\neq 0}\binom{n}{i}^2 p_w^{2i}(1-p_w)^{2n-2i}\\
&\quad -2\sum_{j\neq 0}\binom{n}{j}p_w^{j}(1-p_w)^{2n-j}-(1-p_w)^{2n}\}\\
&= \theta_1\theta_2\{1-\sum_{i\neq 0}\binom{n}{i}^2 p_w^{2i}(1-p_w)^{2n-2i}\\
&\quad -2(1-p_w)^n[1-(1-p_w)^n]-(1-p_w)^{2n}\}\\
&= \theta_1\theta_2-\theta_1\theta_2\sum_{i\neq 0}\binom{n}{i}^2 p_w^{2i}(1-p_w)^{2n-2i}\\
&\quad -2\theta_1\theta_2(1-p_w)^n+\theta_1\theta_2(1-p_w)^{2n}
\end{aligned}
$$

We sum up the above cases and obtain

$$
\begin{aligned}
&\mathrm{E}_{\mathrm{H}_2}[(2^n P_{C_2}(p_w))^2]\\
&= \gamma^{2n}+2\theta_1\gamma^n-2\theta_1\gamma^n(1-p_w)^n\\
&\quad +\theta_1\gamma^n[(p_w^2+(1-p_w)^2)/(1-p_w)]^n\\
&\quad -\theta_1\gamma^n(1-p_w)^n-\theta_1\theta_2(p_w^2+(1-p_w)^2)^n\\
&\quad +\theta_1\theta_2(1-p_w)^{2n}+\theta_1\theta_2\sum_{i\neq 0}\binom{n}{i}^2 p_w^{2i}(1-p_w)^{2n-2i}\\
&\quad +\theta_1\theta_2-\theta_1\theta_2\sum_{i\neq 0}\binom{n}{i}^2 p_w^{2i}(1-p_w)^{2n-2i}\\
&\quad -2\theta_1\theta_2(1-p_w)^n+\theta_1\theta_2(1-p_w)^{2n}\\
&= \theta_1\theta_2+\gamma^{2n}+2\theta_1\gamma^n\\
&\quad +\theta_1\gamma^n[(p_w^2+(1-p_w)^2)/(1-p_w)]^n\\
&\quad -3\theta_1\gamma^n(1-p_w)^n-\theta_1\theta_2(p_w^2+(1-p_w)^2)^n\\
&\quad -2\theta_1\theta_2(1-p_w)^n+2\theta_1\theta_2(1-p_w)^{2n}\\
&= \theta_1\theta_2+\gamma^{2n}+2\theta_1\gamma^n+\theta_{t_1}+\theta_{t_2}
\end{aligned}
$$

□

REFERENCES

1. Wyner AD. The wire-tap channel. *Bell System Technical Journal* 1975; **54**: 1355–1387.
2. Thangaraj A, Dihidar S, Calderbank AR, McLaughlin SW, Merolla J-M. Applications of LDPC codes to the wiretap channel. *IEEE Transactions on Information Theory* 2007; **53**(8): 2933–2945.
3. Cohen G, Zemor G. The wire-tap channel applied to biometrics. *Proceedings of International Symposium on Information Theory and its Applications*, 2004.
4. Ozarow LH, Wyner AD. Wire-tap channel II. *Proceedings of Eurocrypt 84, Workshop on Advances in Cryptology: Theory and Application of Cryptographic Techniques*, 1985; 33–51.
5. Kløve T. *Codes for Error Detection.* World Scientific Publishing Co. Pte. Ltd, Singapore 2007.
6. Maurer U, Wolf S. *Proceedings of the 19th International Conference on Theory and Application of Cryptographic Techniques, Lecture Note in Computer Science*, Vol. 1807, 2000; 351–368.