Conference Paper

On the binary symmetric wiretap channel

Author(s):
Chen, Yanling; Vinck, Adrianus Johannes

Publication Date:
2010

Permanent Link:
https://doi.org/10.3929/ethz-a-005997132

Rights / License:
In Copyright - Non-Commercial Use Permitted
On the Binary Symmetric Wiretap Channel

Yanling Chen  
Q2S, Centre of Excellence  
Norwegian University of Science and Technology  
7491, Trondheim, Norway  
Email: yanling.chen@q2s.ntnu.no

A. J. Han Vinck  
Institute for Experimental Mathematics  
University of Duisburg-Essen  
45326, Essen, Germany  
Email: vinck@iem.uni-due.de

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. Furthermore, we 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.

I. 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 [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. [3] for the case with a noiseless main channel and a binary erasure wiretap channel. In this paper, we consider the specific case when both the main channel and the wiretap channel are BSCs. Our main contribution is twofold. We start with a random coding scheme similar to the one proposed in [4]. We give a strict 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 insure a secure transmission with limited information leakage.

II. MODEL DESCRIPTION

We consider the communication model as shown in Fig. 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 \(\text{BSC}(p)\).

The wiretap channel is a \(\text{BSC}(p_w)\), where \(0 \leq p < p_w \leq 1/2\). Note that a \(\text{BSC}(p_w)\) is equivalent to the concatenation of a \(\text{BSC}(p)\) and a \(\text{BSC}(p^*)\), where \(p^* = (p_w - p)/(1 - 2p)\). Thus the channel model shown in Fig. 1 is equivalent to Wyner’s model with a \(\text{BSC}(p)\) main channel and a \(\text{BSC}(p^*)\) wiretap channel. Its secrecy capacity due to [1] is \(C_s = h(p_w) - h(p)\).

To transmit a \(K\)-bit secret message \(S^K\), an \(N\)-bit codeword \(X^N\) is sent to the channel. The corresponding output at the legitimate receiver is \(Y^N\), at the wiretapper is \(Z^N\). Thus the error occurred over the main channel is \(E^N_w = Y^N - X^N\). Therefore the wiretap channel is \(E^N_w = Z^N - X^N\). Assume that \(S^K\) is uniformly distributed. The transmission rate to the legitimate receiver is

\[
R = K/N. \tag{1}
\]

The equivocation of the wiretapper is defined to be

\[
d = \frac{H(S^K \mid Z^N)}{H(S^K)} = \frac{H(S^K \mid Z^N)}{K}. \tag{2}
\]

At the legitimate receiver, on receipt of \(Y^N\), the decoder makes an estimate \(\hat{S}^K\) of the message \(S^K\). The error probability \(P_e\) of decoding 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, \(x\) is the sequence \(x^N\) and \(s = s^K\), etc. A similar convention applies to random variables, which are denoted by upper-case letters.

III. SECURITY 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 \(\varepsilon, \zeta, \delta > 0\),

\[
R \geq h(p_w) - h(p) - \varepsilon, \quad d \geq 1 - \zeta, \quad P_e \leq \delta. \tag{4}
\]
A. 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 $K \leq K_1$ and let $K_2 = K_1 - K$. We construct
\[ H_2 = \begin{bmatrix} H_1 \\ H \end{bmatrix}. \] (5)

Then $H_2$ is a binary matrix with $N - K_2$ rows and $N$ columns. For arbitrary small $\varepsilon > 0$, we take
\[ K_1 = \lfloor N[1 - h(p) - 2\varepsilon] \rfloor; \]
\[ K_2 = \lfloor N[1 - h(p_w) - 2\varepsilon] \rfloor. \]

Here $\lfloor x \rfloor$ stands for the maximal integer $\leq x$. For given $\varepsilon > 0$, let $N_0 > 1/\varepsilon$. It is easy to verify that for $N > N_0$, we have
\[ R = K/N \geq h(p_w) - h(p) - \varepsilon. \] (6)

In what follows, we will assume that $H_1$, $H$ and $H_2$ are of full rank. The reason is due to Lemma 6 in [2]. In order to send a secret message, a sequence $x$ is chosen at random from the solution set of the following equation
\[ xH_2^T = \begin{bmatrix} xH_1^T & xH_1^T \end{bmatrix} = \begin{bmatrix} 0 & s \end{bmatrix}, \] (7)
where $H_1^T$, $H^T$ and $H_1^T$ are the transposes of the matrices $H_2$, $H_1$ and $H$, respectively.

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

B. 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 $T^N_e(\epsilon)$, the set of error sequences $e$ that satisfy
\[ 2^{-N[h(p)+\epsilon]} \leq \Pr(e\in T^N_e(\epsilon)) \leq 2^{-N[h(p)-\epsilon]}. \] (8)

If exactly one sequence $e$ satisfies $eH_1^T = yH_1^T$, the typical set decoder reports it as the hypothesized error sequence. Otherwise, the typical decoder reports an error.

The error probability of the typical set decoder at the legitimate receiver, can be written as follows,
\[ P_e = P_T + P_{H_1}, \]
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 $\epsilon, \delta > 0$, there exists $N_1$, such that $\Pr(e \in T^N_e(\epsilon)) \geq 1 - \delta/2$ for $N \geq N_1$. Therefore, when $N \geq N_1$, $P_T = 1 - \Pr(e \in T^N_e(\epsilon)) \leq \delta/2$.

Now we consider $P_{H_1}$. Suppose that the true error sequence is $e \in T^N_e(\epsilon)$. If any of the typical error sequence $e' \neq e$, satisfies $(e' - e)H_1^T = 0$, then we have an error. Let
\[ T_e(e) = \{e' : e' \in T^N_e(\epsilon), e' \neq e\}. \] (10)

We have
\[ P_{H_1} \leq \sum_{e \in T^N_e(\epsilon)} \Pr(e = e) \sum_{e' \in T_e(e)} 1[(e' - e)H_1^T = 0], \]
where $1[\cdot]$ is the truth function, whose value is 1 if the statement in the bracket is true and 0 otherwise.

Consider the average of $P_{H_1}$ over all possible $H_1$. Denote averaging over all possible $H_1$ by $\langle \cdot \rangle_{H_1}$. We have
\[ \bar{P}_{H_1} \leq \sum_{e \in T^N_e(\epsilon)} \Pr(e = e) \sum_{e' \in T_e(e)} 1[(e' - e)H_1^T = 0]\langle H_1 \rangle. \]

Since for any non-zero binary sequence $v$, the probability that $vH_1^T = 0$, averaging over all possible $H_1$, is $2^{-(N-K_1)}$, so
\[ \bar{P}_{H_1} < (T_N^N(\epsilon))2^{-(N-K_1)} \leq 2^{-N(1-h(p)-\epsilon)-K_1/N}. \]

Note that $K_1/N < 1-h(p)-\epsilon$. For given $\epsilon, \delta > 0$, there exists an $N_2$, when $N \geq N_2$, $\bar{P}_{H_1} \leq \delta/8$. By Markov inequality,
\[ \Pr(P_{H_1} > \delta/2) < \frac{\bar{P}_{H_1}}{\delta/2} \leq \frac{\delta/8}{\delta/2} = \frac{1}{4}. \]

Thus we have $\Pr(P_{H_1} \leq \delta/2) = 1 - \Pr(P_{H_1} \geq \delta/2) > 3/4$.

So far we have shown that there are more than $3/4$ random choices from all possible $H_1$ such that, for given $\epsilon, \delta > 0$, when $N \geq \max\{N_1, N_2\}$, $P_e = P_T + P_{H_1} \leq \delta/2 + \delta/2 = \delta$. This concludes the proof of reliability.

C. Security proof

In this subsection, we will prove that $d \to 1$ as $N \to \infty$. Consider the wiretapper’s equivocation in three steps:

1) show that $H(S|Z) \geq N[h(p_w) - h(p)] - H(X|S, Z)$
2) show that $H(X|S, Z) \leq h(P_{ew}) + P_{ew}K_2$. Here $P_{ew}$ means a wiretapper’s probability to decode $x$ in the case that $s$ is known to the wiretapper.
3) show that for arbitrary $0 < \lambda < 1/2$, $P_{ew} \leq \lambda$.

Combining the above steps, we obtain that $d \to 1$ as $N \to \infty$.

First we prove step 1 by considering
\[ H(S|Z) = H(S, Z) - H(Z) \]
\[ = H(S, X, Z) - H(X|S, Z) - H(Z) \]
\[ = H(X|Z) + H(S|X, Z) - H(X|S, Z) \]
\[ \geq H(X|Z) - H(X|Y) - H(X|S, Z) \]
\[ = I(X; Y) - I(X; Z) - H(X|S, Z) \]
\[ = N[I(X; Y) - I(X; Z)] - H(X|S, Z) \]
\[ = N[h(p_{ew}) - h(p)] - H(X|S, Z), \]
where (a) follows from the fact that $H(S|X, Z) = 0$.

Now we prove step 2. Suppose that $S$ takes value $s$. For given $H_2, s$, we consider the solution set of equation (7) as a codebook, $X$ in the codebook as the input codeword, wiretapper’s observation $Z$ as the corresponding output of passing $X$ through the wiretap channel. From $Z$, the decoder estimates $X$ as $\hat{X} = g(Z)$. Define the probability of error
\[ P_{ew} = \Pr(\hat{X} \neq X). \] (11)
From Fano’s inequality, we have \(H(X|s, Z) \leq h(P_{ew}) + P_{ew}K_2\). Therefore, \(H(X|s, Z) \leq h(P_{ew}) + P_{ew}K_2\). Thus we complete the proof of step 2.

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

\[2^{-N[h(p_{ew})+\epsilon]} \leq \Pr(e_w = e_w) \leq 2^{-N[h(p_{ew})-\epsilon]}.
\]

If exactly one sequence \(e_w\) satisfies \(e_wH_2^T = zH_2^T\), the decoder reports it as the hypothesized error sequence. Otherwise, a decoding error is reported.

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

\[P_{ew} = P_{t_1} + P_{t_2},\]

where \(P_{t_1}\) is the probability that the true error sequence is itself not typical, and \(P_{t_2}\) is the probability that the true error sequence is typical and at least one other typical sequence clashes with it.

We first analyze \(P_{t_1}\). For given \(\lambda, \epsilon > 0\), there exists \(N_3\), such that \(\Pr(e_w \in T_{Ew}^N(\epsilon)) \geq 1 - \lambda/2\) for \(N \geq N_3\). Therefore, when \(N \geq N_3\), \(P_{t_1} = 1 - \Pr(e_w \in T_{Ew}^N(\epsilon)) \leq \lambda/2\).

Now we consider \(P_{t_2}\). Suppose that the true error sequence is \(e_w \in T_{Ew}^N(\epsilon)\). If any of the typical error sequence \(e_w' \neq e_w\), satisfies \(e_w'H_2^T = 0\), then we have an error. Let

\[T_{ew}(\epsilon) = \{e_w' : e_w' \in T_{Ew}^N(\epsilon), e_w' \neq e_w\}.
\]

We have

\[P_{t_2} \leq \sum_{e_w \in T_{Ew}^N(\epsilon)} \Pr(e_w = e_w) \sum_{e_w' \in T_{ew}(\epsilon)} 1[e_w' - e_w]H_2^T = 0].
\]

Consider the average of \(P_{t_1}, P_{t_2}\). We have

\[\tilde{P}_{t_1} \leq \sum_{e_w \in T_{Ew}^N(\epsilon)} \Pr(e_w = e_w) \sum_{e_w' \in T_{ew}(\epsilon)} 1[e_w' - e_w]H_2^T = 0].
\]

Note that for fixed \(e_w, e_w'\),

\[1[e_w' - e_w]H_2^T = 0|H_2| = 1, e_w'H_2^T = 0|H_2| = 1, e_w'H_2^T = 0|H_2| = 2^{-N-K_1}. 2^{-K} = 2^{-N-K_2}.
\]

Therefore,

\[\tilde{P}_{t_2} < |T_{Ew}^N(\epsilon)|2^{-(N-K_1+K)} \leq 2^{-N(1-h(p_{ew})-\epsilon-K_2/N)}.
\]

Note that \(K_2/N < 1 - h(p_{ew}) - \epsilon\). For given \(\lambda, \epsilon > 0\), there exists \(N_4\), when \(N \geq N_4\), \(\tilde{P}_{t_2} \leq \lambda/8\). By Markov inequality,

\[\Pr(P_{t_2} > \lambda/2) < \frac{\tilde{P}_{t_2}}{\lambda/2} \leq \frac{\lambda}{\lambda/2} = \frac{\lambda}{\lambda/2} = \frac{4}{4}.
\]

Thus we have \(\Pr(P_{t_2} < \lambda/2) = 1 - \Pr(P_{t_2} > \lambda/2) > 3/4\).

So far we have shown that there are more than \(3/4\) random choices from all possible \(H_1\) and more than \(3/4\) random choices from all possible \(H_1\) and \(H_2\) such that, for given \(\epsilon > 0\) and \(\lambda > 0\), when \(N \geq \max\{N_3, N_4\}\), \(P_{ew} = P_{t_1} + P_{t_2} \leq \lambda/2 + \lambda/2 = \lambda\). This completes the proof of step 3.

As a conclusion of above discussion, for given \(\epsilon, \delta, \zeta, \epsilon > 0\), 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 \(H_2\) such that \(P_{ew} \leq \delta\) and \(P_{ew} \leq \lambda\). In addition to (6), it is shown that there are \(H_1\) and \(H_2\) that lead to a random linear code satisfying (4).

**IV. ANALYSIS OF INFORMATION LEAKAGE**

In this section, we adopt the code structure of the random coding scheme but use normal linear codes in our construction for ease of implementation. We address the security of the coset coding scheme by analyzing its total information loss.

**A. Coset coding scheme**

Consider the communication model in Fig. 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 (equation (7)). The codebook in the encoding scheme is shown in Table I. At the legitimate receiver, the decoder uses syndrome decoding. It is easy to see that the coset code by \(C_1\) and \(C_2\) has error correcting capability beyond \(C_1\).

**B. Security analysis**

The total information obtained by the wiretapper through his observation is \(I(S; Z)\). We define it as the information loss (IL) of the scheme. First we have the following lemma.

**Lemma 4.1:** \(H(Z|S) = H(Z|S = 0)\).

**Proof:** For given \(s(i), 1 \leq i \leq 2^k\), we have

\[p_{Z|S}(x|s(i)) = \sum_{x \in S(x(i))} p_{X|S}(x|s(i))p_{Z|X,S}(z, x, s(i))
\]

\[(a) \leq \frac{1}{2^{k_2}} \sum_{x \in S(x(i))} p_{w}^{w(v)}(1 - p_{w})^{n - w(v)},
\]

\[= \frac{1}{2^{k_2}} \sum_{v \in Z \oplus X(i)} p_{w}^{w(v)}(1 - p_{w})^{n - w(v)},
\]

where \(w(v)\) is the Hamming weight of sequence \(v\) and (a) follows that \(p_{X|S}(x|s(i)) = 1/2^{k_2}\), \(p(z|x, s(i)) = p(z|x)\), and the fact that the wiretap channel is a BSC\(p_{ew}\).

From (14), we see that \(p_{Z|S}(z|s(i))\) is determined by the weight distribution of the coset \(z + x(i) + C_2, z \in \{0, 1\}^n\) is a permutation...
We divide $\text{IL}$ into two parts: $\text{IL} = \text{detection}$ for $\text{IL}$ and the second moment $\text{IL} = |H(Z) - H(Z|S) = 0|$. Thus we have $H(Z|S) = H(Z|S = 0)$. Let $C$ be a set of binary sequences of length $n$. We define

$$P_C(r) = \frac{1}{|C|} \sum_{x \in C} p^{\text{w}(x)}(1 - r)^{n - \text{w}(x)}, \quad (15)$$

where $0 \leq r \leq 1/2$ and $|C|$ is the cardinality of $C$. Note that the set of $x$ corresponding to $s = 0$ is $C_2$. We easily derive

$$p_{Z|S}(z|s = 0) = P_{x+C_2}(p_u); \quad (16)$$

$$p_{Z}(z) = P_{x+C_1}(p_u). \quad (17)$$

Then we have the following theorem.

**Theorem 4.2:** (An upper bound on IL)

$$\text{IL} \leq \log[2^n P_{C_2}(p_u)]. \quad (18)$$

**Proof:** The proof outline is as follows. By Lemma 4.1,

$$\text{IL} = I(S; Z) = H(Z) - H(Z|S = 0). \quad (19)$$

We divide IL into two parts: IL = IL1 + IL2, where

$$\text{IL}_1 = \sum_s P_{x+C_2}(p_u) \log \frac{P_{x+C_2}(p_u)}{P_{x+C_1}(p_u)}; \quad (20)$$

$$\text{IL}_2 = \sum_s P_{x+C_1}(p_u) \log \frac{P_{x+C_1}(p_u)}{P_{x+C_1}(p_u)}. \quad (21)$$

We can easily bound $\text{IL}_1$ by applying Theorem 1.19 in [5].

$$\text{IL}_1 \leq \sum_{x \in C_2} P_{x+C_2}(p_u) \log \frac{1 - (1 - 2p_u)(1 - 2p_u) + (1 - 2p_u)(1 - 2p_u) + (2 - 2p_u)}{1 + (1 - 2p_u)(1 - 2p_u)} \leq 0. \quad (22)$$

For $\text{IL}_2$, we apply the log-sum inequality and obtain

$$\text{IL}_2 \leq \log[2^n P_{C_2}(p_u)]. \quad (23)$$

Combining (22) and (23), we complete our proof. \hspace{1cm} \blacksquare

**Lemma 4.6:** (First and second moment of $2^n P_{C_2}(p_u)$)

$$E_{H_Z}[2^n P_{C_2}(p_u)] = \gamma^n + \gamma(1 - (1 - p_u)); \quad (24)$$

$$E_{H_Z}(2^n P_{C_2}(p_u))^2 = \gamma^n + 29\gamma^n + \gamma + \gamma_2. \quad (25)$$

Let $p = 2^{n-k_2}$, then $2^{n-k_2}C_2$ is the dual code of $C_2$ and $\gamma$ is due to the MacWilliam's identity and Theorem 2.1 in [5].

A binary $(n, k)$ linear code $C$ is called good for error detection if $P_{w}(C, r) \leq 2^{-n}(2^k - 1)$, for all $r, 0 \leq r \leq 1/2$. Let $R_2 = k_2/n$ and $\gamma = 2^{(1-R_2)}(1 - p_u)$. Applying Theorem 2.43 and Theorem 2.51 in [5], we have

**Lemma 4.3:** $1 \leq 2^n P_{C_2}(p_u) \leq [2(1 - p_u)^n - 2^k].$

**Corollary 4.4:** $\text{IL} \leq \gamma(1 - (1 - p_u))/2^k.$

**Lemma 4.5:** If $C_2$ is good for error detection, then

$$1 \leq 2^n P_{C_2}(p_u) < 1 + \gamma^n. \quad (24)$$

In the following, we consider $2^n P_{C_2}(p_u)$ as a random variable and investigate its first moment $E_{H_Z}[2^n P_{C_2}(p_u)]$ and the second moment $E_{H_Z}(2^n P_{C_2}(p_u))^2$ over all possible binary matrices $H_2$ of full rank. We will show that under certain constraint, our bound is asymptotically tight.