Chapter 2
Unconditional Security Wireless Communication

Wyner [2], Csiszar and Korner [3] developed the concept of the wiretap channel for wired links. In a wiretap channel, the eavesdropper is assumed to receive messages transmitted by the sender over a channel that is noisier than the legitimate receiver's channel. Under this condition, it is possible to establish perfectly secure source–destination link without relying on secret keys. Unfortunately, it may often be impossible to guarantee that the adversary's channel is noisier than the one of the legitimate partner. In a general communication model, it is possible that the received signal of the intended receiver is worse than the received signal of the eavesdropper. Wyner proved that the transmitter could send information to the legitimate receiver in virtually unconditional secrecy without sharing a secret key with the legitimate receiver if the eavesdropper's channel is a degraded version of the main channel.

In the 1970s and 1980s, the impact of these works was limited, partly because practical wiretap codes were not available, but mostly because a strictly positive secrecy capacity in the classical wiretap channel setup requires the legitimate sender and receiver to have some advantage over the wiretapper in terms of channel quality. In Wyner's model, building unconditional security communication generally takes the following two steps. Firstly, a practical wiretap channel is built by initiating advantages for the legitimate communication peers in terms of channel quality against the eavesdroppers; while the second step is to achieve the unconditional secure communication by security codes. In this chapter, we first present a different approach to build the wiretap channel is presented, and then intorduce the Wyner coset codes.

In this chapter, firstly we utilize the feedback and low density parity check (LDPC) codes to build the wiretap channel I [2] in which the eavesdropper sees a binary symmetric channel (BSC) with error probability p and the main channel is error free. In our model, we consider the situation that an external eavesdropper can receive the signals through the main channel and the feedback channel. Firstly, we developed the Maurer's idea [7] and used a powerful interactive communication to build an unconditionally-secure communication model in which the eavesdropper's channel is noisier than the legitimate partner. Then we utilize the

H. Wen, *Physical Layer Approaches for Securing Wireless Communication Systems*, SpringerBriefs in Computer Science,
DOI: 10.1007/978-1-4614-6510-2_2, © The Author(s) 2013

threshold property of LDPC codes [19] to correct the error of the main channel and remain the error of eavesdropper's channel. In the second step, we developed the security codes on top of the interactive communication model in [16], aiming to achieve an error-free legitimate channel while keeping the eavesdropper from any useful information (i.e., with an error probability of 0.5). By integrating a multi-round two-way communication model with a security code, an unconditional security model is built such that the wiretapper is subject to an error probability close to 0.5 while the main channel is almost error-free.

2.1 Perfect Security Model

Consider a communication system consisting of a source, a destination and an eavesdropper as shown in Fig. 2.1. The source produces a message $\boldsymbol{S} = [s_1 \quad s_2 \cdots s_m]$, and encodes this message as a vector $\boldsymbol{X} = [x_1 \quad x_2 \quad \cdots \quad x_n]$. This vector is transmitted through a communication main channel and received as $\boldsymbol{Y} = [y_1 \quad y_2 \cdots y_n]$ by the destination. The eavesdropper has access to t ($t < n$) symbols of $\boldsymbol{X}$ through a communication wiretap channel and we denote the received vector of an eavesdropper as $\boldsymbol{Z} = [z_1 \quad z_2 \quad \cdots \quad z_n]$. The destination and eavesdropper can decode information as $\hat{\boldsymbol{S}} = [\hat{s}_1 \quad \hat{s}_2 \quad \cdots \quad \hat{s}_m]$ and $\tilde{\boldsymbol{S}} = [\tilde{s}_1 \quad \tilde{s}_2 \quad \cdots \quad \tilde{s}_m]$ from $\boldsymbol{Y}$ and $\boldsymbol{Z}$, respectively. If the error rate of the destination and eavesdropper are:

$$P_e^m = \frac{1}{m}\sum_{i=1}^{m} \Pr(\hat{s}_i \neq s_i) \tag{2.1}$$

$$P_e^w = \frac{1}{m}\sum_{i=1}^{m} \Pr(\tilde{s}_i \neq s_i), \tag{2.2}$$

The two conditions for security communication are:

$$P_e^m \to 0 \tag{2.3}$$

$$P_e^w \to 0.5 \tag{2.4}$$

Condition (2.3) is called reliability condition which implies that X must be determinate by S. Condition (2.4) is called security condition such that an

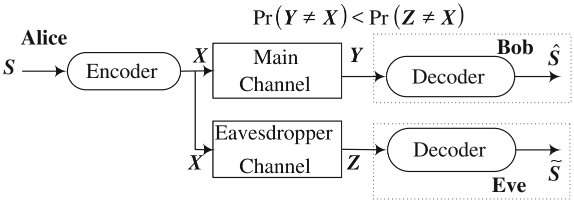

Fig. 2.1 Wyner's perfect security model

eavesdropper can not get any useful information from t intercepted symbols. An alternately expression can be as following: the equivocation of the system is

$$\Delta = H(S^m|Z^n) \tag{2.5}$$

which means that the eavesdropper's remaining uncertainty about the source vector is at least Δ. When $\Delta = K$, the eavesdropper obtains on information about the source, and the system obtained perfect secrecy, which means that the transmitter could send information to the legitimate receiver in virtually unconditional secrecy without sharing a secret key with the legitimate receiver. Such model is called perfect security model.

2.2 Powerful Multi-round Feedback for Build Wiretap Channel Model

2.2.1 Two Way Communication for Build-in Wiretap Channel

Wyner proved that the transmitter could send information to the legitimate receiver in virtually perfect secrecy without sharing a secret key with the legitimate receiver if the eavesdropper's channel is a degraded version of the main channel. The assumption that the adversary only receives a degraded version of the legitimate receiver's information is unrealistic in general. But this assumption is impractical. Sometimes the adversary can have a better channel than that of legitimate user. In [7], two way communications are developed to realize the practical adversary degraded channel building.

We introduce the two way communications approach as following. Let $E = \{e_0, e_1, \cdots, e_{n-1}\}$ and $EA = \{ea_0, ea_1, \cdots, ea_{n-1}\}$ denote the error vectors of the Alice's and the eavesdropper's channel, respectively. The received signals of Alice and the eavesdropper are

$$\begin{aligned} T &= \{t_0, t_1, \cdots, t_{n-1}\}, t_i = q_i \oplus e_i \\ TE &= \{te_0, te_1, \cdots, te_{n-1}\}, te_i = q_i \oplus ea_i \end{aligned} \tag{2.6}$$

where $P_r(e_i = 1) = \alpha$ and $P_r(ea_i = 1) = \beta$. Then Alice use the received signal $\boldsymbol{T}$ to calculate

$$U = \{u_0, u_1, \cdots, u_{n-1}\}, u_i = t_i \oplus m_i \tag{2.7}$$

and encode U such that

$$W = \phi(U) \tag{2.8}$$

where ϕ is the encoder function. Alice sends W over the channel. Alice and the eavesdropper receive the noise version of W as W' and decodeW'as

$$\tilde{U} = \psi(W') \tag{2.9}$$

where ψ is the decoder function. We assume the decoding error probability $P_r\left(\tilde{U} \neq U\right) \to 0$. Bob and the eavesdropper received the $\boldsymbol{U}$ with almost error free. Bob knows the random sequence $\boldsymbol{Q}$, so he can add wise $\boldsymbol{Q}$ to $\boldsymbol{U}$ as

$$Y = U \oplus Q = M \oplus E \tag{2.10}$$

where $Y = \{y_0, y_1, \cdots, y_{n-1}\}$. The eavesdropper only knows $\boldsymbol{TE}$ that is the noise version of $\boldsymbol{Q}$ and he only can add wise Eq. (2.6) to $\boldsymbol{U}$ as:

$$Z = U \oplus TE = M \oplus E \oplus EA \tag{2.11}$$

where $z = \{z_0, z_1, \cdots, z_{n-1}\}$. Comparing Eq. (2.10) with Eq. (2.11), EA becomes the extra noise. Therefore, after two way communication in Fig. 2.2, the direction of the main channel is inverted when the eavesdropper initially has a better channel.

Lemma 2.1 *After two way communication, the error probability of main channel is* α *and the error probability of eaveasdropper's channel is* $\alpha + \beta - 2\alpha\beta$.

Proof Since

$$Pr(y_i \neq m_i) = Pr(e_i = 1),$$

and

$$Pr(z_i \neq m_i) = Pr(e_i = 1) \cdot Pr(ea_i = 0) + Pr(e_i = 0) \cdot Pr(ea_i = 1)$$

Thus $r(z_i \neq m_i) = \alpha + \beta - 2\alpha\beta$.

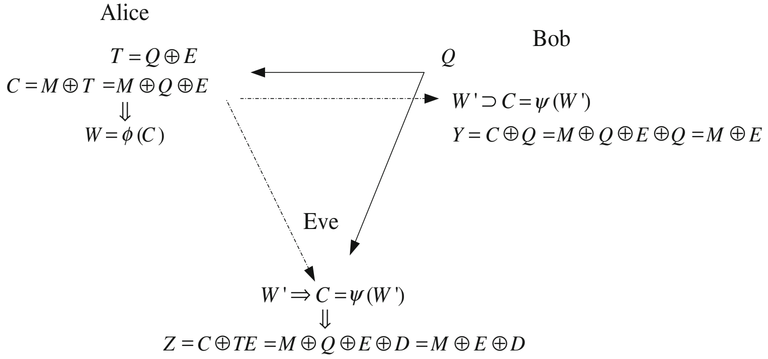

Fig. 2.2 Two way communication

Because $\alpha \leq 0.5$ and $\beta \leq 0.5$, so we have $\alpha \leq \alpha + \beta - 2\alpha\beta$, where the equality holds for $\alpha = 0.5$ or $\beta = 0.5$.

2.2.2 Multi-round Feedback for Build Wiretap Channel Model

In [7], the secrecy capacity ***Cs*** is defined as the maximum rate at which a transmitter can reliably send information to an intended receiver such that the rate at which the attacker obtains this information is arbitrarily small. If the channel from the transmitter to the intended receiver and the channel from the transmitter to the eavesdropper have different bit error probabilities (BER) δ and ε, respectively, the secret capacity ***Cs*** is [7].

$$C_s = \begin{cases} h(\delta) - h(\varepsilon), & if\ \delta > \varepsilon \\ 0, & \text{otherwise} \end{cases} \tag{2.12}$$

where h denotes the binary entropy function defined by

$$h(p) = -p \log_2 p - (1-p) \log_2(1-p)$$

After two way communication, the main channel has advantage over the eavesdropper's channel. One of his attacking methods to the wiretap channel is eliminating the secrecy capacity which means trying to let $\delta \leq \varepsilon$. When β is very small, from Eq. (2.12) we know that the secrecy capacity ***Cs*** is very small. The secret lever of system is weak. By several rounds of two way communication or several parallel channel feedbacks, the advantage of the main channel can be increased. Our scheme to build wiretap channel I is presented as following. To transmit k-bit messages $\boldsymbol{M}$, we first select a (n, k) linear binary code $\boldsymbol{C}$ such that

$$C = \chi(M) \tag{2.13}$$

where χ is the encoder function which maps the k bits message $\boldsymbol{M}$ into a n bits codeword $\boldsymbol{C}$. By randomly choosing $\boldsymbol{C}_0, \boldsymbol{C}_1, \boldsymbol{C}_2, \cdots, \boldsymbol{C}_{t-2}$, where $\boldsymbol{C}_i = \left(c_i^0, c_i^1, c_i^2, \cdots, c_i^{n-1}\right)$, $0 \leq i \leq t-2$, we can calculate the vector

$$\boldsymbol{C}_{t-1} = \boldsymbol{C}_0 \oplus \boldsymbol{C}_1 \oplus \boldsymbol{C}_2 \oplus \cdots \oplus \boldsymbol{C}_{t-2} \oplus \boldsymbol{C} \tag{2.14}$$

Firstly, Bob sends t random sequence $\boldsymbol{Q}_i = \left(q_i^0, q_i^1, \cdots, q_i^{n-1}\right), \quad i = 0, 1, 2, \cdots t-1$ to Alice by the t independent parallel channels or a channel in different time slots. Let $\boldsymbol{E}_i = \left(e_i^0, e_i^1, \cdots, e_i^{n-1}\right)$ and $\boldsymbol{EA}_i = \left(ea_i^0, ea_i^1, \cdots, ea_i^{n-1}\right)$ denote the error vectors of the Alice's and the eavesdropper's channel corresponding to the transmitting the random sequence $\boldsymbol{Q}_i$ respectively. The received signals of Alice and the eavesdropper are $\boldsymbol{T}_i$ and $\boldsymbol{E}_i$. Then Alice uses the received signal calculate $\boldsymbol{U}_i = \boldsymbol{C}_i \oplus \boldsymbol{T}_i$ according to Eq. (2.7) and encode to get $\boldsymbol{W}_i$ according to Eq. (2.8). Alice sends $\boldsymbol{W}_i$ over the channel. Alice and the eavesdropper receive the noise version of $\boldsymbol{W}_i$ as $\boldsymbol{W}_i'$ and decode $\boldsymbol{W}_i^{'}$ according to Eq. (2.9). From Eqs. (2.10) and (2.11), Bob and the eavesdropper can get $\boldsymbol{Y}_i = \boldsymbol{C}_i \oplus \boldsymbol{E}_i$ and $\boldsymbol{Z}_i = \boldsymbol{C}_i \oplus \boldsymbol{E}_i \oplus \boldsymbol{EA}_i$. Here we consider the discrete memoryless channel (DMC). We assume that the t words $\boldsymbol{C}_0, \boldsymbol{C}_1, \boldsymbol{C}_2, \cdots, \boldsymbol{C}_{t-1}$ and t random sequence are transmitted from the t independent parallel channels or a channel in t different time slots, respectively. In each time slot the transmitting signals are independent. Our scheme is shown in Fig. 2.3.

We sum the $Y_i, \mathrm{i} = 0,\ 1,\ 2, \cdots,\ \mathrm{t} - 1$ and $Z_i, \mathrm{i} = 0,\ 1,\ 2, \cdots,\ \mathrm{t} - 1$ respectively as

$$\boldsymbol{Y} = \sum_{i=0}^{t-1} \boldsymbol{Y}_i = \sum_{i=0}^{t-1} \boldsymbol{C}_i \oplus \sum_{i=0}^{t-1} \boldsymbol{E}_i \tag{2.15a}$$

$$\boldsymbol{Z} = \sum_{i=0}^{t-1} \boldsymbol{Z}_i = \sum_{i=0}^{t-1} \boldsymbol{C}_i \oplus \sum_{i=0}^{t-1} \boldsymbol{E}_i \oplus \sum_{i=0}^{t-1} \boldsymbol{EA}_i \tag{2.15b}$$

According to Eq. (2.14), Eqs. (2.15a) and (2.15b) become:

$$\begin{aligned} \boldsymbol{Y} &= \boldsymbol{C} \oplus \sum_{i=0}^{t-1} \boldsymbol{E}_i \\ \boldsymbol{Z} &= \boldsymbol{C} \oplus \sum_{i=0}^{t-1} \boldsymbol{E}_i \oplus \sum_{i=0}^{t-1} \boldsymbol{EA}_i \end{aligned} \tag{2.16}$$

The term$\sum_{i=0}^{t-1} \boldsymbol{EA}_i$ in Eq. (2.16) becomes the extra error. Therefore, what we want to do is to extract the correct information $\boldsymbol{M}$ from $\boldsymbol{Y}$ and keep the extra error

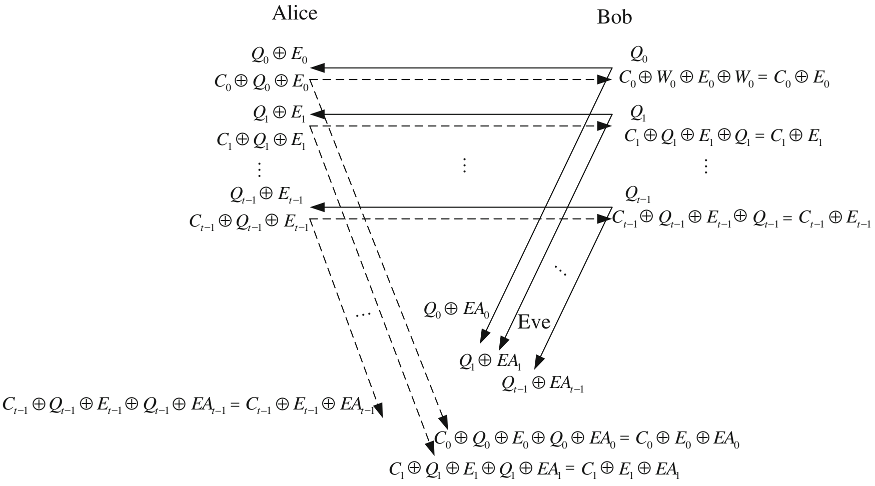
Alice
Bob
$Q_0 \oplus E_0$
$C_0 \oplus Q_0 \oplus E_0$
$Q_1 \oplus E_1$
$C_1 \oplus Q_1 \oplus E_1$
$\vdots$
$Q_{t-1} \oplus E_{t-1}$
$C_{t-1} \oplus Q_{t-1} \oplus E_{t-1}$
Q_0
$C_0 \oplus W_0 \oplus E_0 \oplus W_0 = C_0 \oplus E_0$
Q_1
$C_1 \oplus Q_1 \oplus E_1 \oplus Q_1 = C_1 \oplus E_1$
$\vdots$
Q_{t-1}
$C_{t-1} \oplus Q_{t-1} \oplus E_{t-1} \oplus Q_{t-1} = C_{t-1} \oplus E_{t-1}$
$Q_0 \oplus EA_0$
Eve
$Q_1 \oplus EA_1$
$Q_{t-1} \oplus EA_{t-1}$
$C_{t-1} \oplus Q_{t-1} \oplus E_{t-1} \oplus Q_{t-1} \oplus EA_{t-1} = C_{t-1} \oplus E_{t-1} \oplus EA_{t-1}$
$C_0 \oplus Q_0 \oplus E_0 \oplus Q_0 \oplus EA_0 = C_0 \oplus E_0 \oplus EA_0$
$C_1 \oplus Q_1 \oplus E_1 \oplus Q_1 \oplus EA_1 = C_1 \oplus E_1 \oplus EA_1$

Fig. 2.3 Multi-round feedback communication

remaining in $\boldsymbol{Z}$ by decoding. Then we can get the wiretap channel model I [2] in which the main channel is almost error free and the eavesdropper's channel is noisy.

Lemma 2.2 *Let the error probability of* $\boldsymbol{E}_i$ *denote* $\Pr(e_j^i = 1) = \alpha_i$ *and the error probability of* $\boldsymbol{EA}_i$ *denote* $\Pr(ea_j^i = 1) = \beta_i$, *the error probability of* $\boldsymbol{Y}$ *in Eq.* (2.15a) *and* $\boldsymbol{Z}$ *in Eq.* (2.15b) *are*:

$$\begin{aligned} p(Y) = \sum_{i=0}^{t-1} \alpha_i - 2 \sum_{\substack{i_1, i_2 = 0 \\ i_1 > i_2}}^{t-1} \alpha_{i1}\alpha_{i2} + 4 \sum_{\substack{i_1, i_2, i_3 = 0 \\ i_1 > i_2 > i_3}}^{t-1} \alpha_{i1}\alpha_{i2}\alpha_{i_3} + \cdots + (-1)^t 2^t \\ \sum_{\substack{i_1, i_2, i_3 = 0 \\ i_1 > i_2 > i_3}}^{t-1} \alpha_{i1}\alpha_{i2}\alpha_{i_3} \cdots \alpha_{i_t} \qquad (2.17) \\ P(Z) = P(Y) + P(ZEA) - 2P(Y)P(ZEA) \end{aligned}$$

where

$$\begin{aligned} p(ZEA) = \sum_{i=0}^{t-1} \beta_i - 2 \sum_{\substack{i_1, i_2 = 0 \\ i_1 > i_2}}^{t-1} \beta_{i1}\beta_{i2} \\ + 4 \sum_{\substack{i_1, i_2, i_3 = 0 \\ i_1 > i_2 > i_3}}^{t-1} \beta_{i1}\beta_{i2}\beta_{i_3} + \cdots + (-1)^t 2^t \sum_{\substack{i_1, i_2, i_3 = 0 \\ i_1 > i_2 > i_3}}^{t-1} \beta_{i1}\beta_{i2}\beta_{i_3} \cdots \beta_{i_t} \end{aligned}$$

The proof is derived from lemma 2.1 directly.

By interactive communication we can get an unconditionally-secure communication model in which the legitimate partner can realize the secret information transmitting without pre-shared secret key even if the eavesdropper have better channel at the beginning. The secret strength of the wiretap channel partly depends on the secret capacity. In our scheme, the choosing a larger number of interactive communication round (parameter t) can lead to larger the secret capacity. The feedback sequences are chosen randomly and error vectors caused by the channel noise are random. The feedback signals from the destination plays the role of a private key. Therefore, if one data frame is broken, the other data frames still keep secret.

2.3 Performance with LDPC Codes

Turbo codes [16] and LDPC codes [17, 18] have already proved their excellent performance for error correction therefore both are good candidates for our scheme. This book focuses on LDPC codes although we believe that turbo-codes or any other strong channel codes would yield similar results. But the long codeword length is necessary, which can let the exhaust attacking complexity of the attacker become high.

2.3.1 The Threshold Property of LDPC Codes

LDPC code has been shown to provide excellent decoding performance that can approach the Shannon limit in some case. The LDPC code exhibits a threshold phenomenon with certain decoding method, which determines the asymptotic (in the codeword length) behavior of the ensemble of code: roughly speaking, for a code chosen randomly from the ensemble, with high probability decoding will be successful if transmission takes place below this threshold, and the error probability will stay above a fixed constant if transmission takes place above this threshold. This property can let us correct the error of the main channel and remain the error of eavesdropper's channel at the some time. Because we consider the BSC channel, we use Bit-Flip (BF) iterative decoding method, which was devised by Gallagher in the early 1960s [17].

Firstly, we discuss the upper bound of threshold that can be decoded correctly. We consider the regular LDPC codes, define a (n, d_l, d_r) parity-check matrix as a matrix of n columns that has d_l ones in each column, d_r ones in each row, and zeros elsewhere. Let p_0 denote the crossover probability of the binary-symmetric channel. It was shown in [19] that the expected number of errors in the ith iteration is given by the recursion:

$$a_i = p_0 - p_0 f^+(a_{i-1}) + (1-p_0) f^-(a_{i-1}) \tag{2.18}$$

where $f^+(x) = \lambda\left(\frac{1+\rho(1-2x)}{2}\right), f^-(x) = \lambda\left(\frac{1-\rho(1-2x)}{2}\right)$ and the degree distribution pair $(\lambda(\mathrm{x}), \rho(\mathrm{x}))$ are function of the form: $\lambda(x) = \sum_{j=2}^{\infty} \lambda_j x^{j-1}, \rho(x) = \sum_{j=2}^{\infty} \rho_j x^{j-1}$, where λ_j and ρ_j denote the fraction of ones in the parity-check matrix of the LDPC code which are in columns (rows) of weight j.

Definition 2.1 The threshold p_{up}^* is the supremum of all p_0 in $\left[1, \frac{1}{2}\right]$ such that as defined in (2.18) converges to zero as i tend to infinity.

Lemma 2.3 *Let τ denotes the smallest positive real root of the polynomial and* $p(x) = xf^+(x) + (x-1)$

$f^-(x)$ *and* $\lambda_2 \rho(1) < 1$ *hold. Then*

$$P_{up}^* \leq \min\left\{\frac{1-\lambda_2\rho'(1)}{\lambda'(1)\rho'(1) - \lambda_2\rho'(1)}\right\} \tag{2.19}$$

where $\lambda'(\mathrm{x})$ *and* $\rho'(x)$ denote *derivatives of* $\lambda(\mathrm{x})$ *and* $\rho(x)$, *respectively* [19].

Table 2.1 The thresholds of some regular LDPC code ensembles

d_l	d_r	Rate	p_{up}^*	$p_{0.2}^*$	d_l	d_r	Rate	p_{up}^*	$p_{0.2}^*$
3	6	0.5	0.04	0.145	4	5	0.2	0.123	0.255
4	8	0.5	0.048	0.145	5	6	0.167	0.142	0.279
3	5	0.4	0.061	0.178	7	8	0.125	0.175	0.0306
4	6	0.333	0.067	0.205	9	10	0.1	0.197	0.0325
3	4	0.25	0.107	0.228					

Then we consider the threshold that can not be decoded correctly. We use the Shannon limit in the BSC as the threshold that the channel error can not be corrected by decoding.

Definition 2.2 The threshold p_{ep}^* is the infimum of all p_0 in $\left[1,\frac{1}{2}\right]$ such that the average error probability of the codeword is greater than a constant number $ep \leq 0.5$ as the number of iterative decoding tends to infinity.

Therefore, we hope $P(Y) < p_{up}^*$ and $P(Z) > p_{ep}^*$ after several rounds of interactive communication, which means the main channel will be almost error free and the eavesdropper still remains ep error probability that can not be corrected at least in the same time after LDPC code decoding.

Table 2.1 includes the thresholds of some regular LDPC code ensembles. We let $ep = 0.2$ in Table 2.1. The results of Table 2.1 are also shown in the Fig. 2.4.

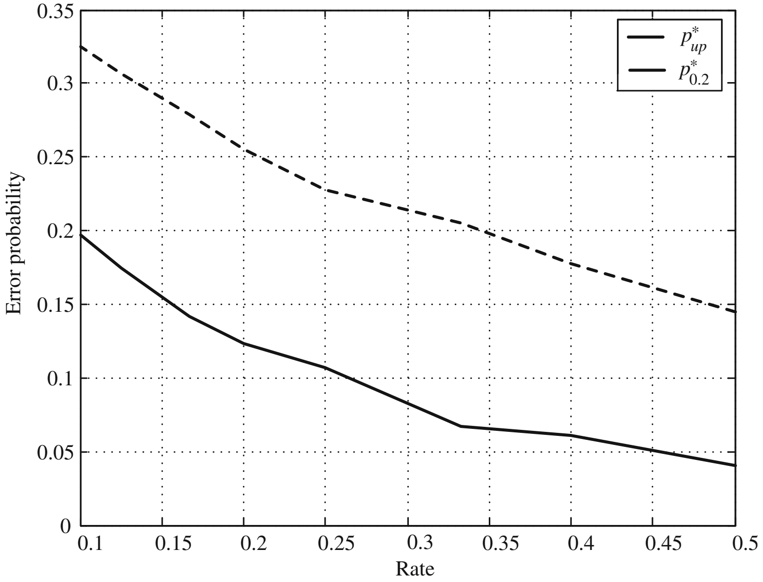

Fig. 2.4 The thresholds of some regular LDPC code ensemble

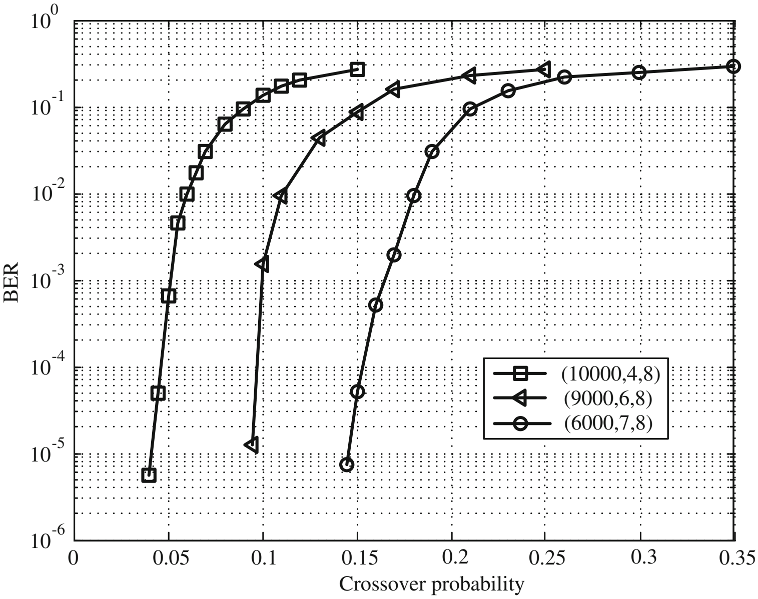

Fig. 2.5 The BER performances of LDPC codes

2.3.2 *Some Performance Results*

We use the random LDPC codes (10000, 4, 8), (9000, 6, 8) and (6000, 7, 8) as the encoder function in Eq. (2.13). The BF decoding bit error probability (BER) of these codes is shown in Fig. 2.5. The maximum iterative number of decoding is 200. We set $t = 1$ (two way communication) and $t = 2$, respectively. The BER after interaction and the BER after LDPC codes decoding are given in Table 2.2 and 2.3, where P_{ir} and P_{Eve} denote the BER of the intended receiver and the eavesdropper after decoding. From the results we can know that the positive secret capacity can be achieved by interaction communication when the eavesdropper has better channel. Because the encoder function φ in Eq. (2.8) and the decoder function ψ in Eq. (2.9) don't have essential effect to our results, we can assume that there are the powerful error correcting codes which can let $P_r(\widehat{U}_i \neq U_i) \rightarrow 0$.

2.4 Security Code

2.4.1 *Coset Security Code*

Obviously, the scheme described in the previous section goes only half-way to providing an unconditional security communication. After multiple rounds of

Table 2.2 The performance properties with $t = 1$

Crossover probability	$\alpha = 0.04$	$\alpha = 0.08$	$\alpha = 0.08$	$\alpha = 0.15$	$\alpha = 0.15$
	$\beta = 0.04$	$\beta = 0.04$	$\beta = 0.08$	$\beta = 0.075$	$\beta = 0.15$
LDPC code	(1000, 4, 8)	(9000, 6, 8)	(9000, 6, 8)	(6000, 7, 8)	(6000, 7, 8)
BER after interaction	$P(Y) = 0.04$	$P(Y) = 0.08$	$P(Y) = 0.08$	$P(Y) = 0.015$	$P(Y) = 0.15$
	$P(Z) = 0.0768$	$P(Z) = 0.1136$	$P(Z) = 0.1472$	$P(Z) = 0.2138$	$P(Z) = 0.255$
BER after decoding	$P_{ir} < 10^{-5}$	$P_{ir} < 0.25 \times 10^{-5}$	$P_{ir} = 1.25 \times 10^{-5}$	$P_{ir} = 5.2 \times 10^{-5}$	$P_{ir} = 5.2 \times 10^{-5}$
	$P_{Eve} = 0.05$	$P_{Eve} = 0.011$	$P_{Eve} = 0.075$	$P_{Eve} = 0.095$	$P_{Eve} = 0.2$
Csin (7)	0.2862	0.0871	0.3841	0.4521	0.7211

Table 2.3 The performance properties with $t = 2$

Crossover probability	$\alpha_1 = \beta_2 = 0.02$	$\alpha_1 = \beta_2 = 0.04$	$\alpha_1 = \beta_2 = 0.04$	$\alpha_1 = \beta_2 = 0.08$	$\alpha_1 = \beta_2 = 0.08$
	$\alpha_1 = \beta_2 = 0.02$	$\alpha_1 = \beta_2 = 0.02$	$\alpha_1 = \beta_2 = 0.04$	$\alpha_1 = \beta_2 = 0.04$	$\alpha_1 = \beta_2 = 0.08$
LDPC code	(1000, 4, 8)	(9000, 6, 8)	(9000, 6, 8)	(6000, 7, 8)	(6000, 7, 8)
BER after interaction	$P(Y) = 0.0392$	$P(Y) = 0.0768$	$P(Y) = 0.0768$	$P(Y) = 0.01472$	$P(Y) = 0.1472$
	$P(Z) = 0.0753$	$P(Z) = 0.11$	$P(Z) = 0.1418$	$P(Z) = 0.201$	$P(Z) = 0.251$
BER after decoding	$P_{ir} < 10^{-5}$	$P_{ir} < 1.25 \times 10^{-5}$	$P_{ir} = 1.25 \times 10^{-5}$	$P_{ir} = 1.5 \times 10^{-5}$	$P_{ir} = 1.5 \times 10^{-5}$
	$P_{Eve} = 0.048$	$P_{Eve} = 0.0093$	$P_{Eve} = 0.071$	$P_{Eve} = 0.055$	$P_{Eve} = 0.205$
C_s in (2.12)	0.2777	0.0759	0.3694	0.3070	0.7316

two-way communication, the two legitimate parties Alice and Bob are connected by a noiseless binary channel, and the wiretapper Eve receives the bits sent over the channel with some error probability $\varepsilon > 0$. Our object is to let error probability $\varepsilon = 0.5$. Formally, let $M = \{m_1, m_2, \cdots, m_k\}$ and $\hat{M} = \{\hat{m}_1, \hat{m}_2, \cdots, \hat{m}_k\}$ and $\hat{M}_E = \{\hat{m}_{E_1}, \hat{m}_{E_2}, \cdots, \hat{m}_{E_k}\}$ be vectors denoting Alice's message, Bob's decoded message and Eve's decoded message, respectively. Unconditional security is said to be achieved if the following relation holds:

$$\begin{aligned} &\Pr(m_i \neq \widehat{m}_i) = 0 \\ &\Pr(m_i \neq \widehat{m}_{Ei}) = 0 \end{aligned} \tag{2.20}$$

To achieve this goal, we need to develop the security codes (SC) that can further degrade the wiretapper's information while without damnifying the legitimate users'. To the best of our knowledge, code construction and their relation to security, although explored in a few studies, are still subject to further research due to their deficiency for practical capacity approaching security code. Here we present some existing results and use it to complete the unconditional security communication scheme in the next section.

Following the special case considered by Wyner [2], we consider the coding method as following. To transmit k bits message $M^j = \left\{m_1^j, m_2^j, \cdots m_k^j\right\}, j = 1, 2, \cdots, 2^k$, a $(n, n-k)$ linear binary code $\boldsymbol{C}_{\mathrm{e}}$ with coset $\boldsymbol{V} = \left\{\boldsymbol{V}^1, \boldsymbol{V}^2, \cdots, \boldsymbol{V}^{2^k}\right\}$ is chosen. Let each message $\boldsymbol{M}^j$ correspond to a coset $\boldsymbol{V}^j = \left\{\boldsymbol{V}_1^j, \boldsymbol{V}_2^j, \cdots, \boldsymbol{V}_{2^{n-k}}^j\right\}$ where n-tuple $\boldsymbol{V}_i^j = w^j \oplus \boldsymbol{Ce}^i, i = 2^{n-k}, j = 2^k, w^j$ and $\boldsymbol{Ce}^i \in \{0, 1\}$, $\boldsymbol{Ce}^i$ is codeword of $(n, n-k)$ linear binary code. We construct the encoder such that the encoder output $V_i^j \in \{0, 1\}^n$ is a randomly chosen member of the coset when the sending message is $\boldsymbol{M}^{j\cdot}$ Therefore, message $\boldsymbol{M}^j$ and $\boldsymbol{w}^j$ corresponding the syndrome and error vector of the code $\boldsymbol{C}_{\mathrm{e}}$, respectively. Clearly, the decoder of the legitimate receiver can perfectly recover $\boldsymbol{M}^j$ from output V_i^j perfectly if the legitimate communication partners hold an error free channel. Now we turn to eavesdroppers who observe the noisy version $Ze^j \in \{0, 1\}^n$, which is the output of the BSC corresponding to the input V_i^j, We can state the security criterion to guarantee security of Alice's message $\boldsymbol{M}^j$ in the following lemma.

Lemma 2.4 *The average bit error rate* (BER) *of the recovering message* $\boldsymbol{M}^j$ *from* $\boldsymbol{Ze}^j$ *equals to* 0.5, *i.e.*, $\Pr(m_i \neq \widehat{m}_{Ei}) = 0.5$, *when the received noisy version* $\boldsymbol{Ze}^j$ *has the equal probability to fall into one of cosets* $\boldsymbol{V}$, *i.e.*,, $\Pr\left(\boldsymbol{Ze}^j \neq \boldsymbol{V}^j\right) = 2^{-k}$, *for* $j = 1, 2, \cdots, 2^k$.

Proof We have $\Pr(Ze^j \in V^j) = 2^{-k}$, which means that there is probability 2^{-k} to take arbitrary k bits vector from entire space $\{0,1\}^k$. Let $A_{t,j}$ denote the number of k dimension vectors which have a distance t with vector $\boldsymbol{M}^j$ and

$\Pr\left(m_i^j \neq \hat{m}_{Ei}^j | \boldsymbol{Ze}^j\right) = 2^{-k}$ denote the average BER of the recovered message $\boldsymbol{M}^j$, we have:

$$\begin{aligned}\Pr\left(m_i \neq \widehat{m}_{Ei} | \boldsymbol{Ze}^j\right) &= \left(\Pr\left(\boldsymbol{Ze}^j \in \boldsymbol{V}^j\right) \sum_{t=0}^{k} \left(A_{t,j}.t\right)\right) \Big/ k \\ &= \left(2^{-k} \sum_{t=0}^{k} \binom{k}{t} \cdot t\right) \Big/ k \\ &= \frac{1}{2}\end{aligned}$$

Now the best result of the security codes over wire-tap channel I is the linear code (n, $n-k$) which can provide the maximum security rate $R < -\log_2 (1-p)$ if this code is an optimum error detection code whose undetected error probability meets the upper bound 2^{-k}, where p is the error probability of Eve's channel [7]. However, a few small classes of linear codes have been proved to have an undetected error probability satisfying the upper bound 2^{-k}. The known optimum error detection codes included Hamming codes, double error-correcting BCH codes and Golay codes [28].

2.4.2 Unconditional Security Communication Model

In this section, we present our unconditional secure communication system by combining our building wiretap channel process and security codes together, which

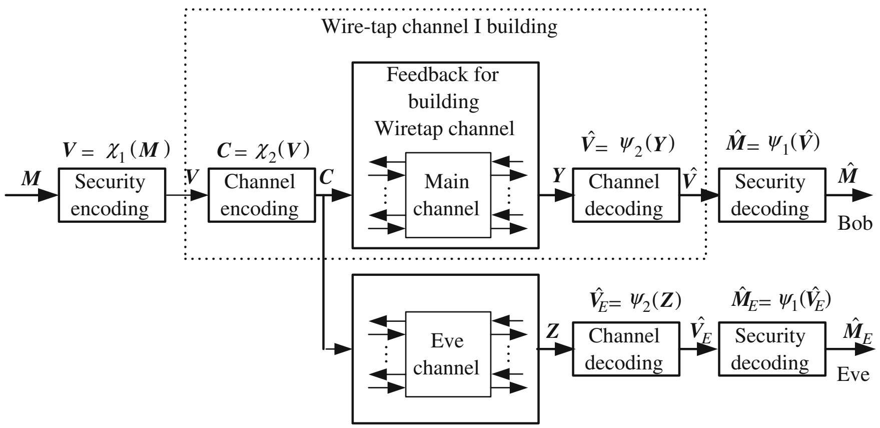
Wire-tap channel I building
Feedback for building Wiretap channel
$V = \chi_1(\boldsymbol{M})$
$\boldsymbol{C} = \chi_2(\boldsymbol{V})$
$\hat{\boldsymbol{V}} = \psi_2(\boldsymbol{Y})$
$\hat{\boldsymbol{M}} = \psi_1(\hat{\boldsymbol{V}})$
$\boldsymbol{M}$
Security encoding
$\boldsymbol{V}$
Channel encoding
$\boldsymbol{C}$
Main channel
$\boldsymbol{Y}$
Channel decoding
$\hat{\boldsymbol{V}}$
Security decoding
$\hat{\boldsymbol{M}}$
Bob
$\hat{\boldsymbol{V}}_E = \psi_2(\boldsymbol{Z})$
$\hat{\boldsymbol{M}}_E = \psi_1(\hat{\boldsymbol{V}}_E)$
Eve channel
$\boldsymbol{Z}$
Channel decoding
$\hat{\boldsymbol{V}}_E$
Security decoding
$\hat{\boldsymbol{M}}_E$
Eve

Fig. 2.6 Unconditional secure communication system model

is shown in Fig. 2.6. Alice wants to send k bits message $M^j = \left\{m_1^j, m_2^j, \cdots m_k^j\right\}$, $j = 1, 2, \cdots, 2^k$ to Bob. Firstly, Alice encodes the message such that

$$\boldsymbol{V} = \chi_1(M), \boldsymbol{V} \in \{0, 1\}^{n_1} \tag{2.21}$$

where χ_1 is the security encoder function. Alice continues to encode $\boldsymbol{V}$ such that

$$\boldsymbol{C} = \chi_2(M), \boldsymbol{C} \in \{0, 1\}^{n_2} \tag{2.22}$$

where χ_2 is the channel encoder function. Then Alice and Bob perform feedback process from Eq. (2.7) to Eq. (2.14). After several rounds of two-way communication between Alice and Bob (how many rounds need to be performed depends on the channel noisy level), Bob received the sequence $\boldsymbol{Y}$ which is the noisy version of sequence $\boldsymbol{C}$. At the same time, the Eve can also observe the noisy sequence $\boldsymbol{Z}$. Bob and Eve perform channel decoding as:

$$\begin{aligned} \hat{\boldsymbol{V}} &= \psi_2(\boldsymbol{Y}) \\ \hat{\boldsymbol{V}}_E &= \psi_2(\boldsymbol{Z}) \end{aligned} \tag{2.23}$$

where ψ_2 is the channel decoding function, which is an invertible function of channel encoding function χ_2. We have $Pr(\boldsymbol{Y} \neq \boldsymbol{C}) = p_1$, and $Pr(\boldsymbol{Z} \neq \boldsymbol{C}) = p_2$ where $p_2 > p_1$. By channel decoding, Bob can recover the sequence $\boldsymbol{C}$ as $\hat{\boldsymbol{V}}$ perfectly and Eve can only get a noisy version of sequence $\boldsymbol{C}$ as $\hat{\boldsymbol{V}}_E$, such that $Pr\left(\hat{\boldsymbol{V}} \neq \boldsymbol{C}\right) \to 0$ and $Pr\left(\hat{\boldsymbol{V}}_E \neq \boldsymbol{C}\right) \to \varepsilon > 0$. So the wiretap channel I have been built.

Then security decoding is performed as following:

$$\begin{aligned} \hat{\boldsymbol{M}} &= \psi_1\left(\hat{\boldsymbol{V}}\right) \\ \hat{\boldsymbol{M}}_E &= \psi_1\left(\hat{\boldsymbol{V}}_E\right) \end{aligned} \tag{2.24}$$

where ψ_1 is the security decoding function, which is an invertible function of security encoding function χ_1. By security decoding, Bob gets the message estimation $\hat{\boldsymbol{M}}$ from $\hat{\boldsymbol{V}}$ with error probability $Pr\left(\hat{\boldsymbol{M}} \neq \boldsymbol{M}\right) \to 0$ and Eve gets the message estimation $\hat{\boldsymbol{M}}_E$ from $\boldsymbol{V}_E$ with error probability $Pr\left(\hat{\boldsymbol{M}}_E \neq \boldsymbol{M}\right) \to 0.5$ at the same time. Therefore, the security of Alice's message $\boldsymbol{M}$ is guaranteed.

2.4.3 Some Performance Results

We use parallel concatenated LDPC (PC-LDPC) codes in our performance. PC-LDPC code [25] is a kind of rate compatible codes which can easily adjust code rate to adapt to varying channel quality. The parity-check matrix $\boldsymbol{H}$ of the PC-LDPC codes has following form:

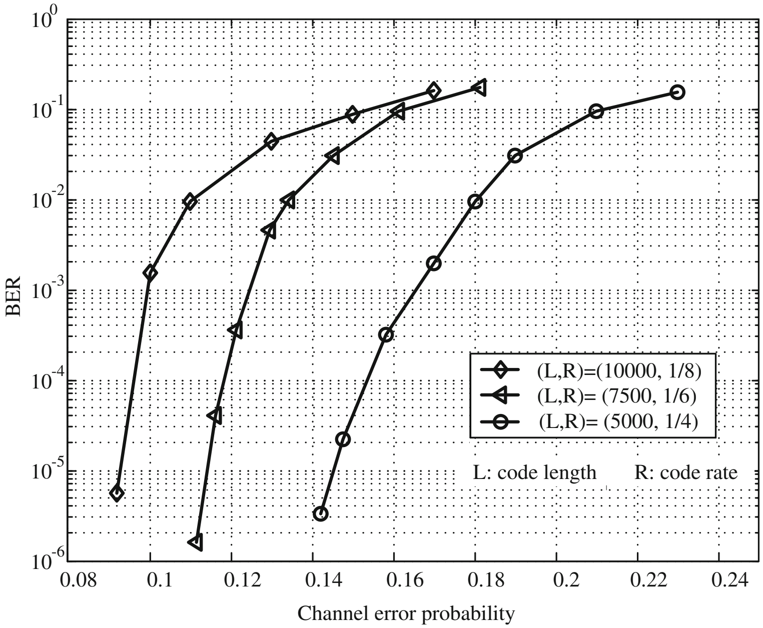

Fig. 2.7 The BER performances of LDPC codes

$$\boldsymbol{H} = \begin{bmatrix} \boldsymbol{H}_1^d & \boldsymbol{H}_1^p & O & \cdots & O \\ \boldsymbol{H}_2^d & O & \boldsymbol{H}_2^p & \cdots & O \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{H}_s^d & O & O & \cdots & \boldsymbol{H}_s^p \end{bmatrix} \tag{2.25}$$

We employ seven random LDPC codes with rate $1/2$ as component codes. The overall code (mother code) length and rate are 10000 and $1/8$, respectively. The source block has 1250 bits. The component matrixes $\boldsymbol{H}_i^d$ and $\boldsymbol{H}_i^p$ in (2.25) are 1250 columns and 1250 rows with 3 weights for every column and row. By puncture the component matrixes $\boldsymbol{H}_i^p$ from the mother code matrix $\boldsymbol{H}$, we can get the LDPC codes with length from 2500 to 10000 and the rate from $1/2$ to $1/8$.. The belief propagation iterative decoding algorithm is used and maximum number of iterations is 200. The performance of these codes is shown in Fig. 2.7. We launch the scenarios with two rounds (i.e., $t = 2$) of two-way communication. The bits error rate (BER) after LDPC codes decoding process are given in Table 1.4, where P_{ir} and P_{Eve} denote the BER of the intended receiver and the eavesdropper after decoding.

We take double error-correcting BCH codes as our security codes. Let the error probability of $\boldsymbol{E}_i$ be denoted as $Pr\left(e_i^j = 1\right) = \alpha_i$ and the error probability of $\boldsymbol{E}e_i$ be denoted as $Pr\left(e_{ei}^j = 1\right) = \beta_i$. Two rounds (i.e., $t = 2$) of two-way communication are performed. The security code parameters are shown in Table 2.4. We present

Table 2.4 The performance properties with $t = 2$

Crossover probability	$\alpha_1 = \alpha_2 = 0.04$	$\alpha_1 = \alpha_2 = 0.04$	$\alpha_1 = \alpha_2 = 0.06$	$\alpha_1 = \alpha_2 = 0.06$	$\alpha_1 = \alpha_2 = 0.08$	$\alpha_1 = \alpha_2 = 0.08$
	$\beta_1 = \beta_2 = 0.02$	$\beta_1 = \beta_2 = 0.04$	$\beta_1 = \beta_2 = 0.04$	$\beta_1 = \beta_2 = 0.06$	$\beta_1 = \beta_2 = 0.04$	$\beta_1 = \beta_2 = 0.08$
LDPC code	(5000, 1/4)	(5000,1/4)	(5000, 1/6)	(7500, 1/6)	(10000, 1/8)	(10000, 1/8)
BER after interaction	$P(Y) = 0.0768$	$P(Y) = 0.0768$	$P(Y) = 0.1128$	$P(Y) = 0.1128$	$P(Y) = 0.1472$	$P(Y) = 0.1472$
	$P(Z) = 0.11$	$P(Z) = 0.1418$	$P(Z) = 0.1723$	$P(Z) = 0.2002$	$P(Z) = 0.201$	$P(Z) = 0.251$
BER after CC decoding	$P_{ir} < 1.5 < 10^{-5}$	$P_{ir} < 1.5 \times 10^{-5}$	$P_{ir} < 1.16 \times 10^{-5}$	$P_{ir} < 1.16 \times 10^{-5}$	$P_{ir} = 1.9 \times 10^{-5}$	$P_{ir} < 1.9 \times 10^{-5}$
	$P_{Eve} = 0.0102$	$P_{Eve} = 0.073$	$P_{Eve} = 0.0125$	$P_{Eve} = 0.0172$	$P_{Eve} = 0.056$	$P_{Eve} = 0.195$
Cs	0.0819	0.3768	0.5434	0.6621	0.3110	0.7115
BCH code	(511, 493, 5)	(63, 51, 5)	(63, 51, 5)	(31, 21, 5)	(127, 113, 5)	(31, 31, 5)
BER after SC decoding	$P_B < 7.25 \times 10^{-3}$	$P_B < 5.35 \times 10^{-4}$	$P_B < 3.5 \times 10^{-4}$	$P_B < 6.2 \times 10^{-3}$	$P_B < 9.1 \times 10^{-4}$	$P_B < 5.2 \times 10^{-4}$
	$P_E = 0.4997$	$P_E = 0.4999$	$P_E = 0.4996$	$P_E = 0.4999$	$P_E = 0.4993$	$P_E = 0.4995$
Rater of SC	0.0352	0.1905	0.1905	0.3226	0.1102	0.3226

the BER results after security decoding in Table 1.4, where P_B and P_E denote the BER of Bob and Eve after decoding, respectively. **SC** and **CC** is the logogram of security code and channel code. When the BER of Eve after **SC** decoding is less than 0.49, Eve is kept from receiving the information. From Table 1.4, we can conclude that the errors of Eve's received messages are higher than 0.49 and the errors of Bob's received messages are less than 10^{-3} even if the Eve has a same or better channel at the beginning.

Table 2.4 also shows the upper bound on the secret capacity C_s calculated according to lemma 2.1 in [4]. Although lower than the optimal secret capacity, the proposed security code is considered of practical use in realizing the unconditional security system. If we define the communication rate of a system as useful secret information bits via total transmission bits, our communication rate is higher than those of existing unconditional security schemes. In [15], it takes about 30 s to generate a 128 bits length secret key, which means that the total communication rate is about 7.2×10^{-7}. If our method is used to generate this length key, fourteen rounds (i.e., $t = 14$) of two-way communication need to be performed. $1/8$ code rate LDPC and 0.11 security code rate are used. If we estimate the overhead of communication as 25 %, the total communication rate is 2.45×10^{-5}. The other advantage of our scheme is that the multiple rounds two-way communication can be performed in parallel.

2.5 Summary

In this chapter, we have shown that the perfect security communication can be achieved by two steps. The first step is building wire tap channel by combining the feedback and LDPC codes. The second step is to extend the advantage of legitimate partners by the security codes. Instead of raising any unpractical assumption on the wiretapper's channels, the proposed approach in this chapter is applicable in any scenario with known noisy channels from the sender to the intended receiver and to the wiretapper, respectively. Thus, the proposed approach yields practical usage in many circumstances, such as on achieving confidentiality in a symmetric cryptographic system for key exchange, distribution, and message confidentiality.