Secrecy Systems for Identification Via Channels with Additive-Like Instantaneous Block Encipherer

R. Ahlswede, N. Cai, and Z. Zhang*

Abstract. In this paper we propose a model of secrecy systems for identification via channels with ALIB encipherers and find the smallest asymptotic key rate of the ALIB encipherers needed for the requirement of security.

1 Introduction

Attention: This is the only paper in the collection which works with the **optimistic capacity**, which is the optimal rate achivable with arbitrary small error probability again and again as the blocklength goes to infinity.

The criticism of this concept made in [B34] has been supplemented by a new aspect:

in cryptology enemies strongest time in wire-taping must be taken into consideration!

The model of identification via channels was introduced by R. Ahlswede and G. Dueck [1] based on the following cases. The receivers of channels only are interested in whether a specified message was sent but not in which message was sent and the senders do not know in which message the receivers are interested. Sometimes the sender requires that the message sent can be identified only by legitimate receivers of the channel but not by any one else (e.g. wiretapper). For example, a company produces N kinds of products which are labelled by $j = 1, 2, \cdots, N$. The company wants to sell a kind of products only to the members of the company's association. For other customers it even does not want them to know what it is going to sell. In this case the company can use a secrecy system for identification via channels with additive-like instantaneous block (ALIB) encipherers, i.e. the sender encrypts the message (identification code) with a private key sending it via the channel and sends the same key only to the members of the company's association through a secure channel. The secrecy system with ALIB encipherers was investigated by R. Ahlswede and G. Dueck [2], but their model needs to be adapted to satisfy the requirement of identification via channels. In this paper we consider the model of secrecy systems for identification via channels with ALIB encipherers and investigate the

* Zhang's research was supported by the ZiF research group "General Theory of Information Transfer and Combinatorics".

R. Ahlswede et al. (Eds.): Information Transfer and Combinatorics, LNCS 4123, pp. 285–292, 2006.

smallest asymptotic key rate of the ALIB encipherers needed for the requirement of security.

In Section 2, we review the necessary background of identification via channels. Our model is described in Section 3. Our result for symmetric channels is proved in Section 4.

2 Background

Let $\mathcal{X}, \mathcal{K}, \mathcal{Y}, \mathcal{Z}$ be finite sets. For simplicity, we assume that $\mathcal{X} = \mathcal{K} = \mathcal{Y} = \mathcal{Z} = GF(q)(q \geq 2)$. Let $W = \{W^n\}_{n=1}^{\infty}$ be a memoryless channel with transmission matrix $(w(z|x); x \in \mathcal{X}, z \in \mathcal{Z})$.

Definition 1. *A randomized $(n, N_n, \mu_n, \lambda_n)$ identification (Id) code for the channel W^n is a system $\{(Q_i, D_i); 1 \leq i \leq N_n\}$, where Q_i is a probability distribution (PD) of the random codeword $X^n(i)$ generated by a randomized encoder $\varphi_n(i)$, i.e. $Q_i(x^n) = \Pr\{X^n(i) = x^n\}$, $x^n \in \mathcal{X}^n$, $D_i \subset \mathcal{Z}^n$ is a decoding set.*

Denote by $Z^n(i)$ the output of W^n when the input is $X^n(i)$ and $Q_i W^n$ the PD of $Z^n(i)$. Set $\mu_n^{(i)} = Q_i W^n(D_i^c) = \Pr\{Z^n(i) \in \mathcal{Z}^n - D_i\}$ and $\lambda_n^{(j,i)} = Q_j W^n(D_i) = \Pr\{Z^n(j) \in D_i\}(j \neq i)$. $\mu_n = \max\limits_{1 \leq i \leq N_n} \mu_n^{(i)}$ and $\lambda_n = \max\limits_{1 \leq j, i \leq N_n, j \neq i} \lambda_n^{(j,i)}$ are called the error probability of the first and second kind for the Id code, respectively, $\frac{1}{n} \log \log N_n = r_n$ is called the rate of the Id code.

Definition 2. *Rate R is (μ, λ)–achievable if there exists a sequence of $(n, N_n, \mu_n, \lambda_n)$ Id codes for the channel W^n $(1 \leq n < \infty)$ satisfying the following conditions.*
1) $\overline{\lim\limits_{n \to \infty}} \mu_n \leq \mu$, 2) $\overline{\lim\limits_{n \to \infty}} \lambda_n \leq \lambda$, 3) $\liminf\limits_{n \to \infty} r_n \geq R$.
The (μ, λ)–Id capacity for the channel W is defined by $D(\mu, \lambda|W) = \sup(R|R$ is $(\mu, \lambda)-$achievable).

Theorem 1. *([1]) Let $W = \{W^n\}_{n=1}^{\infty}$ be an arbitrary channel. If there exists a number ε satisfying $0 \leq \varepsilon \leq \mu$ and $0 \leq \varepsilon \leq \lambda$, then it holds that $D(\mu, \lambda|W) \geq C(\varepsilon|W)$, where $C(\varepsilon|W)$ denotes the ε–channel capacity of the channel W which is defined as follows.*

Definition 3. *Rate R is ε–achievable if there exists a sequence of (n, M_n, ε_n) codes for the channel $W^n (1 \leq n \leq \infty)$ satisfying the following conditions.*
1) $\overline{\lim\limits_{n \to \infty}} \varepsilon_n \leq \varepsilon$, 2) $\liminf\limits_{n \to \infty} \frac{1}{n} \log M_n \geq R$.
The ε-channel capacity for the channel W is defined by

$$C(\varepsilon|W) = \sup(R|R \text{ is } \varepsilon-\text{achievable}).$$

Theorem 1 is proved by using the following lemma.

Lemma 1. *([1]) Let $\mathcal{M}$ be an arbitrary finite set of size $M = \mid \mathcal{M} \mid$. Choose constants τ and κ satisfying $0 < \tau \leq \frac{1}{3}$ and $0 < \kappa < 1$ and $\kappa \log(\frac{1}{\tau} - 1) \geq \log 2 + 1$, where the natural logarithms are used. Define $N = \lfloor e^{\tau M}/Me \rfloor$. Then, there exist N subsets $A_1, A_2, \cdots, A_N$ of $\mathcal{M}$ satisfying $\mid A_i \mid = \lfloor \tau M \rfloor$ $(1 \leq i \leq N)$ and $\mid A_i \cap A_j \mid < \kappa \lfloor \tau M \rfloor (i \neq j)$.*

Using Lemma 1 the ID-code for proving Theorem 1 can be constructed as follows.

Let $\gamma > 0$ be an arbitrarily small constant and set $R = C(\varepsilon|W) - \gamma$. By Definition 3 R is ε–achievable as a rate of the transmission code. Therefore, there exists a sequence of (n, M_n, ε_n) codes for the channel $W^n (1 \leq n < \infty)$ satisfying the following conditions:

1) $\overline{\lim_{n\to\infty}} \varepsilon_n \leq \varepsilon$, 2) $\liminf_{n\to} \frac{1}{n} \log M_n \geq R$, where ε_n denotes the maximum decoding error probability of the code. Denote the (n, M_n, ε_n) code by $\mathcal{C}_n = \{c_1, c_2, \cdots, c_{M_n}\}$
$(c_i \in \mathcal{X}^n)$ and let E_i be the decoding region corresponding to $c_i (1 \leq i \leq M_n)$. Now we apply Lemma 1 by setting $\mathcal{M} = \{1, 2, \cdots, M_n\}$, $M = M_n$, $\tau = \tau_n = \frac{1}{(n+3)}$, $\kappa = \kappa_n = \frac{2}{\log(n+2)}$ and $N = N_n = \lfloor e^{\tau_n M_n} / M_n e \rfloor$. Since all conditions of Lemma 1 are satisfied, there exist N_n subsets $A_1, A_2, \cdots, A_{N_n}$ of $\mathcal{M}$ satisfying $|A_j| = \lfloor \tau_n M_n \rfloor (1 \leq j \leq N_n)$ and $| A_j \cap A_k | < \kappa_n \lfloor \tau_n M_n \rfloor (j \neq k)$. Define the subsets S_j $(1 \leq j \leq N_n)$ of $\mathcal{C}_n$ by $S_j = \bigcup_{i \in A_j} \{c_i\}$ and let Q_j denote the uniform distribution over S_j. Define $D_j = \bigcup_{i \in A_j} E_i$ as the decoding set corresponding to Q_j. It is shown that the constructed Id code $\{(Q_j, D_j); 1 \leq j \leq N_n\}$ can be used to prove Theorem 1.

Theorem 1 gives the direct theorem on the Id coding problem. We need the converse theorem also. Since the converse theorem is essentially related to the channel resolvability problem, we can introduce the channel resolvability instead.

Let $W = \{W^n\}_{n=1}^{\infty}$ be an arbitrary channel with input and output alphabets $\mathcal{X}$ and $\mathcal{Y}$ respectively. Let $Y = \{Y^n\}_{n=1}^{\infty}$ be the output from the channel W corresponding to a given input $X = \{X^n\}_{n=1}^{\infty}$. We transform the uniform random number U_{M_n} of size M_n into another input $\widetilde{X} = \{\widetilde{X}^n\}_{n=1}^{\infty}$. That is, $\widetilde{X}^n = f_n(U_{M_n})$, $f_n : \{1, 2, \cdots, M_n\} \to \mathcal{X}^n$.

Denote by $\widetilde{Y} = \{\widetilde{Y}^n\}_{n=1}^{\infty}$ the output from the channel W with an input $\widetilde{X}$. The problem of how we can choose the size M_n of the uniform random number U_{M_n} and the transform f_n such that the variational distance between $Y = \{Y^n\}_{n=1}^{\infty}$ and $\widetilde{Y} = \{\widetilde{Y}^n\}_{n=1}^{\infty}$ satisfies $\lim_{n\to\infty} d(Y^n, \widetilde{Y}^n) = 0$ is sometimes called the channel resolvability problem. In this problem, the criterion of approximation can be slightly generalized to $\overline{\lim_{n\to\infty}} d(Y^n, \widetilde{Y}^n) \leq \delta$, where δ is an arbitrary constant satisfying $0 \leq \delta < 2$.

Definition 4. *Rate R is δ–achievable for an input $X = \{X^n\}_{n=1}^{\infty}$ if there exists a sequence of transforms $\widetilde{X}^n = f_n(U_{M_n}) (1 \leq n < \infty)$ satisfying*

$$\overline{\lim_{n\to\infty}} d(Y^n, \widetilde{Y}^n) \leq \delta \quad \textit{and} \quad \overline{\lim_{n\to\infty}} \frac{1}{n} \log M_n \leq R,$$

where Y^n and $\widetilde{Y}^n$ denote the channel outputs corresponding to X^n and $\widetilde{X}^n$, respectively. The channel δ–resolvability for an input X is defined by

$$S_X(\delta|W) = \inf(R|R \textit{ is } \delta\textit{–achievable for an input } X).$$

Theorem 2. *([3]) Let W be an arbitrary channel with time structure and X an arbitrary input variable. Then, it holds that $S_X(\delta|W) \leq \overline{I}(X;Y)$ for all $\delta \geq 0$, where Y denotes the channel output variable corresponding to X and $\overline{I}(X;Y)$ represents the sup-mutual information rate defined by*

$$\begin{aligned}\overline{I}(X;Y) &= p - \overline{\lim_{n\to\infty}} \tfrac{1}{n} \log \tfrac{W^n(Y^n|X^n)}{P_{Y^n}(Y^n)} \\ &= \inf\left(\alpha \Big| \lim_{n\to\infty} \Pr_{X^nY^n}\left\{\tfrac{1}{n}\log \tfrac{W^n(Y^n|X^n)}{P_{Y^n}(Y^n)} > \alpha\right\} = 0\right). \qquad (1)\end{aligned}$$

3 Model

In this section we propose a model of the secrecy systems for identification via channels with ALIB encipherers. We keep the notations and assumptions given in Section 2 for reviewing the background of identification via channels.

Let $\{(Q_i, D_i) : 1 \leq i \leq N_n\}$ be the $(n, N_n, \mu_n, \lambda_n)$ Id code constructed as in the proof of Theorem 1 for the channel W. Recall that an (n, R) ALIB encipherer is a subset $C \subset \mathcal{K}^n$ with $\mid C \mid < e^{nR}$. Let $f : \mathcal{X} \times \mathcal{K} \to \mathcal{Y}$ be a function, where $f(x, \cdot)$ is bijective for each $x \in \mathcal{X}$ and $f(\cdot, k)$ is bijective for each $k \in \mathcal{K}$. $f^n : \mathcal{X}^n \times \mathcal{K}^n \to \mathcal{Y}^n$ denotes the n–fold product of f. Given a pair (f, C) we define a secrecy system which works as follows. If the sender wants to send a message $i(1 \leq i \leq N_n)$, he sends the random codeword $X^n(i)$ generated by the randomized encoder $\varphi_n(i)$. Before he transmits $X^n(i)$ he uses a random key generator K^n to generate k^n according to the uniform distribution on C. Then the sender encrypts $X^n(i)$ into the random cryptogram $Y^n(i) = f^n(X^n(i), K^n)$ and sends it to the receiver over the channel W^n. Suppose that $X^n(i)$ and K^n are mutually independent. The used key k^n is sent to the receiver over a secure channel. Denote by $\widetilde{Z}^n(i)$ the output of the channel W^n when the input is the cryptogram $Y^n(i)$. In general, the receiver cannot use the same key k^n to recover the received codeword $Z^n(i)$ from the received cryptogram $\widetilde{Z}^n(i)$ since the channel W^n is noisy. In order to solve this problem, we assume that $f(x, k) = x + k$, where $+$ operates in $GF(q)$. Then we have $Y^n(i) = X^n(i) + K^n$. Further, we need to assume that the channel W^n is memoryless with **symmetric transmission matrix**, more specifically, the output and input of the channel W^n have the following relation: $\widetilde{Z}^n(i) = Y^n(i) + E^n$, where $E^n = (E_1, E_2, \cdots, E_n)$ is a sequence of independent random variables with the same PD on $GF(q)$. Combining the two assumptions, we obtain $\widetilde{Z}^n(i) = X^n(i) + K^n + E^n = Z^n(i) + K^n$ or $Z^n(i) = \widetilde{Z}^n(i) - K^n$. Hence the receiver can get $Z^n(i)$ from $\widetilde{Z}^n(i)$ by using the same key k^n and decides that the message $i(1 \leq i \leq N_n)$ is sent if $Z^n(i) \in D_i$. Since the PD of $Z^n(i)$ is Q_iW^n and $Q_iW^n(D_i^c) \leq \mu_n$, $Q_jW^n(D_i) \leq \lambda_n(j \neq i)$, the receiver can identify the message i with error probabilities of the first kind and second kind not greater than μ_n and λ_n, respectively. Another customer intercepts the channel output $\widetilde{Z}^n(i)$ and attempts to identify a message $j(1 \leq j \leq N_n)$ being sent. Since the customer does not know the actual key k^n being used, he has to use $\widetilde{Z}^n(i)$ and his knowledge of the system for deciding that the message j is

sent. We need a security condition under which the customer can not decide for any fixed message $j(1 \le j \le N_n)$ being sent with small error probability. Such a condition was given by R. Ahlswede and Z. Zhang [4] for investigating the problem of identification via a wiretap channel. This condition is also suitable for our model. The condition is stated as follows.

Security Condition. For any pair of messages $(i,j)(1 \le i \ne j \le N_n)$ and $D \subset \mathcal{Z}^n$, it holds that $\widetilde{Q}_i W^n(D^c) + \widetilde{Q}_j W^n(D) > 1 - \delta_n$ and $\lim_{n\to\infty} \delta_n = 0$, where $\widetilde{Q}_i$ and $\widetilde{Q}_i W^n$ denote the PD of $Y^n(i)$ and $\widetilde{Z}^n(i)$ respectively.

From the identity $\widetilde{Q}_i W^n(D^c) + \widetilde{Q}_i W^n(D) = 1$ for any $i(1 \le i \le N_n)$ and any $D \subset \mathcal{Z}$ and the Security Condition, we obtain $\widetilde{Q}_j W^n(D) > 1 - \widetilde{Q}_i W^n(D^c) - \delta_n = \widetilde{Q}_i W^n(D) - \delta_n$ for any pair $(i,j)(1 \le i \ne j \le N_n)$. Therefore, the Security Condition means that $\widetilde{Q}_i W^n$ and $\widetilde{Q}_j W^n$ are almost the same for any pair (i,j) with $i \ne j$. Hence the customer can not decide on any fixed message $j(1 \le j \le N_n)$ being sent with small error probability.

We are interested in the following problem. What is the largest rate R of the ALIB encipherer C so that the distributions $\widetilde{Q}_i W^n (i = 1, 2, \cdots, N_n)$ satisfy the Security Condition.

4 Main Result

For the model of a secrecy system described in Section 3 we obtain the following main result.

Theorem 3. *1) Assume for the alphabets $\mathcal{X} = \mathcal{K} = \mathcal{Y} = \mathcal{Z} = GF(q)(q \ge 2)$ and that $W = \{W^n\}_{n=1}^{\infty}$ is a memoryless symmetric channel with the transmission matrix $(w(z|x) > 0; x \in \mathcal{X}, z \in \mathcal{Z})$.*

2) Assume that the function $f(x,k) = x + k$, where $+$ operates in the finite field $GF(q)$.

3) Suppose that the random key K^n has uniform distribution on the ALIB encipherer $C \subset \mathcal{K}^n$ and is mutually independent with each random codeword $X^n(i)(1 \le i \le N_n)$.

Then, the secrecy system for identification via the channel W with ALIB encipherers possesses the following properties.

1) The secrecy system can transmit N_n messages $i = 1, 2, \cdots, N_n$ with

$$\liminf_{n\to\infty} \frac{1}{n} \log\log N_n \ge \log q + \sum_{z\in\mathcal{Z}} w(z|x) \log w(z|x) - \gamma,$$

where $\gamma > 0$ is an arbitrarily small number and $x \in \mathcal{X}$ is fixed, the legitimate receiver can identify the message $i(1 \le i \le N_n)$ with arbitrarily small error probability.

2) The smallest asymptotic key rate R of the ALIB encipherer C is $R = -\sum_{z\in\mathcal{Z}} w(z|x) \log w(z|x)$ ($x \in \mathcal{X}$ is fixed) for the distributions $\widetilde{Q}_i W^n (i = 1, 2, \cdots, N_n)$ satisfying the Security Condition. Hence, the other customer can not judge any fixed message $j(1 \le j \le N_n)$ being sent from $\widetilde{Q}_i W^n$ with small error probability.

Proof. 1) By assumption 1), the channel capacity of the channel W is $C(W) = C(0|W) = \log q + \sum_{z\in\mathcal{Z}} w(z|x)\log w(z|x)$. Using Theorem 1 with $\varepsilon = 0$, we obtain that the (μ,λ)–Id capacity of the channel W, $D(\mu,\lambda|W) \geq C(W)$ for $\mu \geq 0$, $\lambda \geq 0$. Hence, there exists a sequence of $(n, N_n, \mu_n, \lambda_n)$ Id codes for the channel $W^n (1 \leq n < \infty)$ satisfying the conditions: 1) $\lim_{n\to\infty} \mu_n = 0$; 2) $\lim_{n\to\infty} \lambda_n = 0$; 3) $\liminf_{n\to\infty} r_n \geq C(W) - \gamma$. Using the Id codes in the secrecy system, the property 1) holds.

2) By assumption 2), the random cryptogram $Y^n(i) = X^n(i) + K^n$, where the random key K^n has uniform distribution on an ALIB encipherer $C \subset \mathcal{K}^n$. R. Ahlswede and G. Dueck [2] have pointed out that $Y^n(i)$ and K^n can be regarded as the output and input of the channel denoted by $V = \{V^n\}_{n=1}^{\infty}$. In the case of identification, the channel V is a general channel rather than a memoryless channel. By assumption 3), the transmission probability of the channel V^n can be defined as $V^n_{y^n|k^n} = \sum_{x^n} Q_i(x^n)\delta(y^n, x^n + k^n)$, where

$$\delta(y^n, x^n + k^n) = \begin{cases} 1, & \text{if } y^n = x^n + k^n, \\ 0, & \text{otherwise.} \end{cases}$$

In order to prove property 2), we want to apply Theorem 2 for the general channel V. First, we consider the input U^n of the channel V^n which has uniform distribution on the ALIB encipherer $C = \mathcal{K}^n$. It is evident that the PD of the output $Y^n(i)$ corresponding to the input U^n is the uniform distribution on $\mathcal{Y}^n$, i.e. $\widetilde{Q}_i(y^n) = \Pr\{Y^n(i) = y^n\} = q^{-n}$ for any $y^n \in \mathcal{Y}$ and any $i (1 \leq i \leq N_n)$. By the assumption 1), it is also evident that the PD of the output $\widetilde{Z}^n(i)$ of the channel W^n corresponding to the input $Y^n(i)$ is the uniform distribution on $\mathcal{Z}^n$, i.e. $\widetilde{Q}_i W^n(z^n) = q^{-n}$ for any $z^n \in \mathcal{Z}^n$ and any $i (1 \leq i \leq N_n)$. Hence $\widetilde{Q}_i W^n (1 = 1, 2, \cdots, N_n)$ satisfy the Security Condition. But the key rate of $C = \mathcal{K}^n$ equals $\log q$, it can be reduced. Then, applying Theorem 2 for the input $U = \{U^n\}_{n=1}^{\infty}$ and $\delta = 0$, we obtain $S_U(0|V) \leq \overline{I}(U, Y(i))$, where $Y(i) = \{Y^n(i)\}_{n=1}^{\infty}$. We use formula (1) to compute $\overline{I}(U, Y(i))$. We have seen that $\Pr\{Y^n(i) = y^n\} = P_{Y^n(i)}(y^n) = q^{-n}$ for any $y^n \in \mathcal{Y}^n$ and $V^n_{y^n|k^n} = \sum_{x^n} Q_i(x^n)\delta(y^n, x^n + k^n) = \sum_{x^n \in S_i} \mid S_i \mid^{-1} \delta(y^n, x^n + k^n)$ for $k^n \in \mathcal{K}^n$, where $\mid S_i \mid = \tau_n M_n$, $\tau_n = \frac{1}{(n+3)}$, $\liminf_{n\to\infty} \frac{1}{n}\log M_n \geq C(W) - \gamma$. Then, the joint distribution of U^n and $Y^n(i)$

$$\Pr\{U^n = k^n,\ Y^n(i) = y^n\} = \begin{cases} q^{-n} \mid S_i \mid^{-1}, \text{ for } y^n \in S_i + k^n = \{x^n + k^n; x^n \in S_i\} \\ 0, \qquad\qquad \text{otherwise.} \end{cases}$$

Hence,

$$\frac{1}{n}\log\frac{V^n(Y^n(i)|U^n)}{P_{Y^n(i)}(Y^n(i))} = \frac{1}{n}\log\frac{|S_i|^{-1}}{q^{-n}} = \log q - \frac{1}{n}\log|S_i|$$

$$= \log q - \frac{1}{n}\log M_n + \frac{1}{n}\log(n+3)$$

with probability one. Therefore, by formula (1):

$$\overline{I}(U;Y(i)) \le \log q - C(W) + \gamma = -\sum_{z\in\mathcal{Z}} w(z|x)\log w(z|x) + \gamma.$$

Since γ is an arbitrarily small number, so $\overline{I}(U,Y(i)) = H(\{w(z|x); z \in \mathcal{Z}\})$, where $H(\cdot)$ is the entropy function. Then, we obtain $S_U(0|V) \le H(\{w(z|x); z \in \mathcal{Z}\})$. By the definition 4, there exists a sequence of transforms $K^n{=}f_n(U_{M_n})(1 \le n < \infty)$ satisfying $\lim\limits_{n\to\infty} d(Y^n(i), \widetilde{Y}^n(i)) = 0$ and $\liminf\limits_{n\to\infty} \frac{1}{n}\log M_n \le H(\{w(z|x); z \in \mathcal{Z}\}) + \gamma$, where $Y^n(i)$ and $\widetilde{Y}^n(i)$ denote the outputs of channel V corresponding to the inputs U^n and K^n respectively.

In other words, there exists a sequence of (n, R) ALIB encipherers C with $R \le H(\{w(z|x); z \in \mathcal{Z}\}) + \gamma$, such that if the random key K^n generates the key k^n according to the uniform distribution on C, then the random cryptogram $\widetilde{Y}^n(i) = X^n(i) + K^n$ satisfies $\lim\limits_{n\to\infty} d(Y^n(i), \widetilde{Y}^n(i)) = 0$.

In the following, in order to avoid confusion, the PDs of $Y^n(i)$ and $\widetilde{Y}^n(i)$ are denoted by $Q_{Y^n(i)}$ and $\widetilde{Q}_i$, respectively, denote $\widetilde{Z}^n(i)$ the output of the channel W^n corresponding to the input $\widetilde{Y}^n(i)$. Now, we prove that the PD of $\widetilde{Z}^n(i)$, $\widetilde{Q}_i W^n (i = 1, 2, \cdots, N_n)$ satisfies the Security Condition. In fact, $Q_{Y^n(i)}W^n$ is the uniform distribution on $\mathcal{Z}^n$ and $Q_{Y^n(i)}W^n(D) + Q_{Y^n(i)}W^n(D^c) = 1$ for any $D \subset \mathcal{Z}^n$. On the other hand,

$$\begin{aligned} d(Q_{Y^n(i)}W^n, \widetilde{Q}_i W^n) &= \sum_{z^n\in\mathcal{Z}^n} \mid Q_{Y^n(i)}W^n(z^n) - \widetilde{Q}_i W^n(z^n) \mid \\ &\le \sum_{z^n\in\mathcal{Z}^n}\sum_{y^n\in\mathcal{Y}^n} \mid Q_{Y^n(i)}(y^n) - \widetilde{Q}_i(y^n) \mid W^n_{z^n|y^n} \\ &= d(Q_{Y^n(i)}, \widetilde{Q}_i). \end{aligned}$$

Consequently, $\lim\limits_{n\to\infty} d(Q_{Y^n(i)}W^n, \widetilde{Q}_i W^n) = 0$. Evidently, for any $i(1 \le i \le N_n)$,

$$\mid Q_{Y^n(i)}W^n(D^c) - \widetilde{Q}_i W^n(D^c) \mid \le d(Q_{Y^n(i)}W^n, \widetilde{Q}_i W^n),$$

then,

$$\widetilde{Q}_i W^n(D^c) \ge Q_{Y^n(i)}W^n(D^c) - d(Q_{Y^n(i)}W^n, \widetilde{Q}_i W^n).$$

Similarly, for any $j(j \ne i)$,

$$Q_j W^n(D) \ge Q_{Y^n(j)}W^n(D) - d(Q_{Y^n(j)}W^n, \widetilde{Q}_j W^n).$$

Combine these two inequalities and set

$$\delta_n = 2[d(Q_{Y^n(i)}W^n, \widetilde{Q}_i W^n) + d(Q_{Y^n(j)}W^n, \widetilde{Q}_j W^n)].$$

We obtain $\widetilde{Q}_i W^n(D^c) + \widetilde{Q}_j W^n(D) > 1 - \delta_n$ and $\lim\limits_{n\to\infty} \delta_n = 0$. Our proof is complete.

References

1. R. Ahlswede and G. Dueck, Identification via channels, IEEE Trans. Inform. Theory, Vol. 35, No. 1, 15–29, 1989.
2. R. Ahlswede and G. Dueck, Bad codes are good ciphers, Prob. Cont. Info. Theory 11, 337–351, 1982.
3. T.S. Han, Information-Spectrum Methods in Information Theory, Springer, Berlin, 2003.
4. R. Ahlswede and Z. Zhang, New directions in the theory of identification via channels, IEEE Trans. Inform. Theory, Vol. 41, No. 1, 14–25, 1995.
5. N. Cai and K.Y. Lam, On identification secret sharing schemes, Information and Computation, 184, 298–310, 2003.