ISIT'2013 1569719145

The Kraft inequality for EPS systems

Chinthani Uduwerelle, Terence Chan and Siu-Wai Ho
Institute for Telecommunications Research
University of South Australia
Email: uduhk001@mymail.unisa.edu.au, {terence.chan, siuwai.ho}@unisa.edu.au

***Abstract*—It is a well known result that the Kraft inequality is a necessary and sufficient condition for the existence of a uniquely decodable code. This paper provides an inequality which is a counterpart of the Kraft inequality in Error free Perfect Secrecy (EPS) system. Our inequality is a necessary and sufficient condition for the existence of an EPS system. It also illustrates some necessary and sufficient conditions for an EPS system to achieve the minimal expected key consumption.**

I. Introduction

Consider the following scenario where Alice wants to send a secret message to Bob over a public network. To achieve this, Alice and Bob share a secret key R and encrypt the transmitted message U with the key. The encrypted message X will then be transmitted over a public network.

A crypto-system $P_{RX|U}$ is an **Error free Perfect Secrecy (EPS) System** as shown in Fig. 1 if it satisfies the following conditions:

1) (Perfect Secrecy) X is independent of U so that
$$\sum_r P_{XR|U}(x,r|u) = \sum_r P_{XR|U}(x,r|u') \quad (1)$$
for all $u, u' \in \mathcal{U}$ and all $x \in \mathcal{X}$. Here, $\mathcal{U}$ and $\mathcal{X}$ are the supports of U and X, respectively.
2) (Key independence) R is independent of U so that
$$\sum_x P_{XR|U}(x,r|u) = \sum_x P_{XR|U}(x,r|u') \quad (2)$$
for all $u, u' \in \mathcal{U}$ and all $r \in \mathcal{R}$. Here $\mathcal{R}$ is the support of R.
3) (Error-free) if $P_{RX|U}(r,x|u) > 0$, then for all $u' \neq u$, $P_{RX|U}(r,x|u') = 0$.

For a given distribution $P_U(u)$, the joint probability distribution of (U,X,R) (with respect to a given EPS system) is thus well-defined. It can be directly verified that

$$I(U;R) = 0, \quad (3)$$
$$H(U|R,X) = 0, \quad (4)$$
$$I(U;X) = 0 \quad (5)$$

are satisfied in an EPS system for any given P_U [3].

In [1], [2], it was shown that for any perfectly secure crypto-system $P_{RX|U}$, i.e, a crypto-system that satisfies (5) together with the error free property (4), the size of the pre-shared common randomness (or simply called the secret key) R should satisfy,

$$H(R) \geq H(U). \quad (6)$$

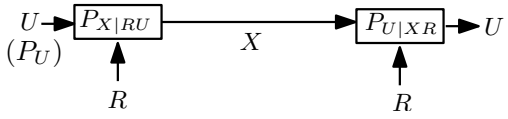

Fig. 1. An EPS system for source U with distribution P_U

In other words, the entropy of the message U cannot be greater than the entropy of the key.

In [3], it was pointed out that the bound given in (6) can be further tightened, with the additional constraint $I(U;R) = 0$, i.e., the message U is independent of the key R. The tighter lower bound shows that the entropy of the secret key is at least the logarithm of the message support size, i.e.,

$$H(R) \geq \log |\mathcal{U}|. \quad (7)$$

In this paper, all logarithms will be in base 2.

For an EPS system, the transmission cost, which measures the number of channel uses required to transmit X from the source to the legitimate receiver, is also lower bounded by

$$H(X) \geq \log |\mathcal{U}|, \quad (8)$$

similar to the bound given in (7) due to the symmetric roles of R and X in (3)–(5). The equalities in the bounds given in (7), (8) can be simultaneously achieved using the One-Time Pad (OTP) scheme [3].

EPS system model (U,R,X) is a $(2,2)$-threshold secret sharing scheme, where U is the secret and R, X are the shares. Here eavesdropper has access to only one channel (X). The secret can be reconstructed together with R, X. By considering the size of shares in a secret sharing environment, results similar to (7), (8) were obtained in [4], [5].

Apart form the above results, [3] showed that if an EPS system will be used multiple times, then $H(R)$ is not necessarily equal to the "amount of key consumed". Instead, a better measure is $I(R;UX)$. It was further proved in [3] that

$$I(R;UX) \geq H(U), \quad (9)$$

a result analogous to (6) obtained in [1], [2].

If we rewrite

$$I(R;UX) = I(R;X|U) + I(U;R) \quad (10)$$
$$= I(R;X|U) \quad (11)$$
$$= \sum_u P_U(u) I(R;X|U=u), \quad (12)$$

where (11) follows from (3). Then the expected key consumption is clearly a linear function of $P_U(u)$. Furthermore, $I(R;X|U=u)$ is well defined from the crypto-system $P_{RX|U}(r,x|u)$, even if the distribution $P_U(u)$ is unknown.

Roughly speaking, $I(R;X|U=u)$ can be interpreted as the amount of key that will be used if the input is u. Therefore, the expected amount of key consumed is

$$\sum_u P_U(u) I(R;X|U=u).$$

To illustrate this idea, we consider the following example.

Example 1. *Consider a source distribution $P_U(0) = 5/8, P_U(1) = 2/8$ and $P_U(2) = 1/8$.*

- *Coding scheme 1 (One-Time Pad): In OTP we select a key R, which is uniformly distributed over the support of U and hence $H(R) = \log 3$. Then $X = U + R$ (mod 3). We can verify that $I(R;X|U=u) = H(R) = \log 3$.*
- *Coding scheme 2 (Prefix codes with padding after the encryption): Construct the Huffman code for this source U. A possible assignment of codewords is*

U	Codeword $C(U)$
0	0
1	10
2	11

Let $R = (B_1, B_2)$ be two uniform bits and R is generated independent of U. We generate another random bit B_3 which is independent of other random variables. If $U = 0$, $X = (0 \oplus B_1, B_3)$. If $U = 1$, $X = (1 \oplus B_1, 0 \oplus B_2)$. If $U = 2$, $X = (1 \oplus B_1, 1 \oplus B_2)$. Let $l_0 = 1$, $l_1 = 2$ and $l_2 = 2$. We can verify that

$$\begin{aligned} I(R;X|U=u) &= H(R) - H(R|X,U=u) && (13)\\ &= 2 - (2 - l_u) && (14)\\ &= l_u. && (15)\end{aligned}$$

Hence $I(R;X|U=0) = 1$ bit, $I(R;X|U=1) = 2$ bits and $I(R;X|U=2) = 2$ bits. This is exactly the same as how many bits in R have been used.

Above encryption schemes in example 1, involve source coding, encryption and padding. In coding scheme 1 (OTP), it uses a block length source code whereas in the coding scheme 2, a variable length source code is used. In this example, coding scheme 2 outperforms the coding scheme 1. It can be shown that the partition code (a joint source coding and encryption scheme) proposed in [3] will outperform both coding schemes. This paper aims to determine if there are any rules that the key consumption profile $I(R;X|U=u)$ should satisfy. Our results will be shown in the next section.

II. Kraft's inequality for EPS systems

Consider a D-ary uniquely-decodable code C for a source U. Let $(\ell_u,\ u \in \mathcal{U})$ be the set of codeword lengths. Then the tuple satisfies the following Kraft's inequality [6]

$$\sum_{u\in\mathcal{U}} D^{-l_u} \le 1. \tag{16}$$

On the other hand, if a set of codeword lengths $(\ell_u,\ u \in \mathcal{U})$ satisfies Kraft's inequality, there exists a D-ary prefix code (and hence also uniquely-decodable) whose codeword lengths are exactly $(\ell_u,\ u \in \mathcal{U})$. While the original Kraft's inequality holds for any uniquely-decodable code, we will show in this paper that there is an analogous result for EPS systems.

For a given EPS system $P_{RX|U}(r,x|u)$, let

$$f(u) \triangleq I(R;X|U=u),$$

so that

$$f(u) = \sum_{r,x} P_{RX|U}(r,x|u) \log \frac{P_{RX|U}(r,x|u)}{P_{R|U}(r|u) P_{X|U}(x|u)}.$$

Due to (11), the expected key consumption can be re-expressed in terms of $f(u)$ and equals

$$\sum_u P_U(u) f(u).$$

We call $(f(u), u \in \mathcal{U})$ (or simply $f(u)$) the *key consumption profile* of the EPS scheme.

To minimise the expected key consumption, it is sufficient to determine which key consumption profile $(f(u), u \in \mathcal{U})$ can be realised by an EPS scheme. In this paper, we will show that the key consumption profile $(f(u), u \in \mathcal{U})$ of an EPS scheme must satisfy Kraft's inequality.

Theorem 1. ***[Kraft's inequality for EPS systems]*** *If $(f(u), u \in \mathcal{U})$ is a key consumption profile of an EPS system, then*

$$\sum_u 2^{-f(u)} \le 1, \tag{17}$$

where the logarithms in $f(u)$ are in base 2.

Not only the theorem itself looks similar to (16) with $D = 2$, the proof technique also resembles the one used to prove Kraft's inequality in [6]. Before we outline our proof, we introduce several intermediate results.

Consider a sequence $\mathbf{u} \triangleq (u_1, \ldots, u_n)$ of n source symbols. The sequence $\mathbf{u}$ induces the empirical distribution

$$Q_{\mathbf{u}}(u) \triangleq \frac{|\{i = 1, \ldots, n :\ u_i = u\}|}{n}.$$

We call $Q_{\mathbf{u}}$ the type induced by the sequence $\mathbf{u}$. Obviously, it is possible that two different sequences $\mathbf{u}'$ and $\mathbf{u}''$ may induce the same type. The following two lemmas are fundamental results regarding types. Their proofs can be found in [6].

Lemma 1. *Let Q be a type and*

$$T_n(Q) \triangleq \{\mathbf{u} = (u_1, \ldots, u_n) :\ Q = Q_{\mathbf{u}}\}.$$

Then

$$|T_n(Q)| \le 2^{nH(Q)}, \tag{18}$$

where $H(Q)$ is used to denote the entropy of a random variable whose distribution is Q.

Lemma 2. *Let $\mathcal{S}_n$ be the set of all possible types induced by a length n sequence $\mathbf{u}$. Then*

$$|\mathcal{S}_n| \quad \leq \quad (n+1)^{|\mathcal{U}|}. \tag{19}$$

More results on types can be found in [7].

Theorem 2. *Consider any conditional probability distribution $P_{RX|U}(r,x|u)$. For any probability distribution $q(u)$ of U, it induces a joint distribution of (U,R,X) which is defined as $q(u)P_{RX|U}(r,x|u)$. Let*

$$C \quad = \quad \max_q H(q(u)P_{RX|U}(r,x|u)). \tag{20}$$

In other words, C is the maximal entropy of (U,R,X) subject to the constraint that the conditional probability distribution of R,X given U is $P_{RX|U}(r,x|u)$. Then

$$\sum_u \frac{2^{H(RX|U=u)}}{2^C} \leq 1. \tag{21}$$

Proof: First notice that

$$\left(\sum_{u\in\mathcal{U}} \frac{2^{H(RX|U=u)}}{2^C}\right)^n \tag{22}$$

$$= \quad \left(\sum_{u_1\in\mathcal{U}} \frac{2^{H(RX|U=u_1)}}{2^C}\right)\cdots\left(\sum_{u_n\in\mathcal{U}} \frac{2^{H(RX|U=u_n)}}{2^C}\right) \tag{23}$$

$$= \quad \frac{1}{2^{nC}} \sum_{u_1\in\mathcal{U}} \cdots \sum_{u_n\in\mathcal{U}} 2^{H(RX|U=u_1)}\cdots 2^{H(RX|U=u_n)} \tag{24}$$

$$= \quad \frac{1}{2^{nC}} \sum_{u_1,\ldots,u_n\in\mathcal{U}^n} 2^{H(RX|U=u_1)}\cdots 2^{H(RX|U=u_n)} \tag{25}$$

$$= \quad \frac{1}{2^{nC}} \sum_{\mathbf{u}\in\mathcal{U}^n} \prod_{i=1}^n 2^{H(RX|U=u_i)}, \tag{26}$$

where $\mathbf{u} = (u_1,\ldots,u_n)$.

Consider a sequence $\mathbf{u}$ with the type $Q_{\mathbf{u}}$. For each $\mathbf{u}$, it is clear that

$$\prod_{i=1}^n 2^{H(RX|U=u_i)} = 2^{\sum_{u\in\mathcal{U}} nQ_{\mathbf{u}}(u)H(RX|U=u)}.$$

Hence,

$$\left(\sum_{u\in\mathcal{U}} \frac{2^{H(RX|U=u)}}{2^C}\right)^n \tag{27}$$

$$= \quad \frac{1}{2^{nC}} \sum_{\mathbf{u}\in\mathcal{U}^n} 2^{\sum_{u\in\mathcal{U}} nQ_{\mathbf{u}}(u)H(RX|U=u)} \tag{28}$$

$$= \quad \sum_{Q\in\mathcal{S}_n} |T(Q)| \frac{2^{\sum_{u\in\mathcal{U}} nQ_{\mathbf{u}(u)}H(RX|U=u)}}{2^{nC}} \tag{29}$$

$$\leq \quad \sum_{Q\in\mathcal{S}_n} 2^{nH(Q)} \frac{2^{\sum_{u\in\mathcal{U}} nQ_{\mathbf{u}(u)}H(RX|U=u)}}{2^{nC}} \tag{30}$$

$$= \quad \sum_{Q\in\mathcal{S}_n} \frac{2^{nH(RXU)}}{2^{nC}}, \tag{31}$$

where in (31) the joint distribution of (U,R,X) is $Q(u)P_{RX|U}(r,x|u)$.

By definition, $C \geq H(RXU)$ and hence,

$$\left(\sum_{u\in\mathcal{U}} \frac{2^{H(RX|U=u)}}{2^C}\right)^n \quad \leq \quad |\mathcal{S}_n| \tag{32}$$

$$\leq \quad (n+1)^{|\mathcal{U}|}, \tag{33}$$

where (33) follows from Lemma 2. In other words,

$$\log\left(\sum_{u\in\mathcal{U}} \frac{2^{H(RX|U=u)}}{2^C}\right) \leq \frac{|\mathcal{U}|\log(n+1)}{n}. \tag{34}$$

Since this inequality is true for all n, it is true in the limit as $n\to\infty$. Since

$$\lim_{n\to\infty} \frac{|\mathcal{U}|\log(n+1)}{n} = 0,$$

$$\log\left(\sum_{u\in\mathcal{U}} \frac{2^{H(RX|U=u)}}{2^C}\right) \leq 0 \tag{35}$$

and consequently,

$$\sum_u \frac{2^{H(RX|U=u)}}{2^C} \leq 1. \tag{36}$$

■

In the following, we will use the above intermediate results to prove Theorem 1.

Proof of Theorem 1:

Let (R,X,U) be a set of random variables. For any given probability distribution $q(u)$ the joint distribution is given by

$$P_{RXU}(r,x,u) = q(u)P_{RX|U}(r,x|u). \tag{37}$$

Since $P_{RX|U}(r,x|u)$ is an EPS system, its error-free property implies that $H(U|RX) = 0$. Hence,

$$H(RXU) = H(RX) \leq H(R) + H(X). \tag{38}$$

Consequently,

$$C = \max_q H(RXU) \leq H(R) + H(X). \tag{39}$$

Therefore,

$$\frac{2^{H(RX|U=u)}}{2^C} \quad \geq \quad \frac{2^{H(RX|U=u)}}{2^{H(R)+H(X)}} \tag{40}$$

$$= \quad 2^{-I(R;X|U=u)}, \tag{41}$$

where the last equality follows from $H(R) = H(R|U=u)$ and $H(X) = H(X|U=u)$ due to (3) and (5). Consequently, Theorem 1 follows from Theorem 2.

■

The proof for Theorem 2 resembles the proof for Kraft's inequality in [6]. In the following, we will prove a stronger version of Theorem 2 in the sense that the equality in (21) indeed always holds. While Theorem 3 is stronger than Theorem 2, we deliberatively keep Theorem 2 to highlight the similarities between Kraft's inequality for source coding and our Kraft's inequality for EPS systems.

Theorem 3. *The equality in* (21) *always holds and the maximum in* (20) *is attained by*

$$q(u) = \frac{2^{H(RX|U=u)}}{\sum_u 2^{H(RX|U=u)}}. \quad (42)$$

Proof: To prove the theorem, first we need to identify the distribution $q(u)$ which achieve the maximum in (20). The optimisation problem in (20) is a simple convex optimisation problem. Using the Karush-Kuhn Tucker (KKT) conditions [8], it is straightforward to verify that the optimal distribution $q(u)$ satisfies (42). In this case, C can be explicitly calculated as

$$2^C = \sum_u 2^{H(RX|U=u)} \quad (43)$$

and the theorem is proved. ∎

Before we end this section, the implication of the equality in (17) is shown. In (9), we have seen the lower bound on the expected key consumption. Under the constraints for EPS systems (i.e., (3)–(5)), the minimal expected key consumption, i.e., $I(R;UX) = H(U)$, is achieved if and only if $I(R;X) = 0$. The connection between (21) and $I(R;X) = 0$ is revealed in the following theorem.

Theorem 4. *For an EPS system $P_{RX|U}(r,x|u)$, the equality in Kraft's inequality for EPS systems holds if and only if there exists a source distribution P_U with the form*

$$P_U(u) = 2^{-I(R;X|U=u)} \quad \forall u \quad (44)$$

such that $I(R;X) = 0$.

Proof: From the proof of Theorem 1, it can be seen directly that the equality in (17) holds if and only if the equality holds in (39), i.e.,

$$C = \max_q H(q(u)P_{RX|U}(r,x|u)) \quad (45)$$

$$= H(R,X) = H(R) + H(X). \quad (46)$$

Therefore, there exists a distribution $P_U = q$ which induces independence between R and X. From Theorem 3, the distribution P_U satisfies (42). Together with (43) and (46),

$$P_U(u) = 2^{H(RX|U=u)-C} = 2^{-I(R;X|U=u)}, \quad (47)$$

where the last equality follows from (3) and (5). Therefore, the theorem is proved. ∎

III. Existence

For a set of integers $(\ell_u,\ u \in \mathcal{U})$ satisfying the Kraft inequality, there always exists a uniquely decodable code with codeword lengths $(\ell_u,\ u \in \mathcal{U})$ [6]. So it is natural to ask whether the inequality in (17) can offer the same insight. To be specific, we consider a set of positive real numbers $\tilde{V} = \{v_1, v_2, \ldots, v_M\}$. If $\tilde{V}$ satisfies

$$\sum_u 2^{-v_u} \le 1, \quad (48)$$

is there an EPS system such that the expected key consumption for message u is equal to v_u for all u? The answer is yes and it will be illustrated through the following code which is derived from the partition code in [3]. For the sake of completeness, we define it here.

Definition 1 (Amended Partition Code $\mathcal{C}(\Psi,\theta)$)**.** *Assume that U is a random variable defined on $\{1,\ldots,M\}$. Let $\Psi = (\psi_1,\psi_2,\ldots,\psi_M)$. Here, we assume that $\theta \ge \sum_{i=1}^M \psi_i$ where ψ_i and θ are positive integers. Let A' be a random variable such that*

$$\Pr(A' = j \mid U = i) = \begin{cases} \frac{1}{\psi_i} & \text{if } 1 \le j \le \psi_i, \\ 0 & \text{otherwise.} \end{cases}$$

Let $A = \sum_{i=1}^{U-1} \psi_i + A' - 1$, R be uniformly distributed on the set $\{0,1,\ldots,\theta-1\}$ and $X = (A+R) \mod \theta$. The so defined cipher system (R,U,X) is called the amended partition code *$\mathcal{C}(\Psi,\theta)$. When $\theta = \sum_{i=1}^M \psi_i$, it reduces to the partition code proposed in [3].*

It is easy to verify that Definition 1 defines an EPS system. Furthermore, the system has the following property.

Lemma 3. *For the amended partition code $\mathcal{C}(\Psi,\theta)$,*

$$I(R;X|U=u) = \log\frac{\theta}{\psi_u}. \quad (49)$$

Proof: Since

$$I(R;X|U=u) = H(X) - H(X|R,U=u) \quad (50)$$

$$= H(X) - H(A|R,U=u) \quad (51)$$

$$= \log\theta - \log\psi_u, \quad (52)$$

the lemma is proved. ∎

Theorem 5 (Existence)**.** *For any given set of positive real values $\tilde{V} = \{v_1, v_2, \ldots, v_M\}$ satisfying* (48)*, there exists an amended partition code $\mathcal{C}(\Psi,\theta)$ such that for any $\varepsilon > 0$ and any $u \in \mathcal{U}$,*

$$|I(R;X|U=u) - v_u| < \varepsilon. \quad (53)$$

Proof: For $1 \le u \le M$, let $\psi_u = \lfloor \theta \cdot 2^{-v_u} \rfloor$. Note that $\theta \ge \sum_{u=1}^M \psi_u$ and we can apply the amended partition code in Definition 1 to construct an EPS system. Together with Lemma 3,

$$|I(R;X|U=u) - v_u| = \left| \log\frac{\theta}{\lfloor \theta \cdot 2^{-v_u} \rfloor} - v_u \right|, \quad (54)$$

which goes to 0 as $\theta \to \infty$. Therefore, the theorem is proved. ∎

Remarks: i) If 2^{-v_u} is a rational number, $I(R;X|U=u) = v_u$ for $1 \le u \le M$ can be achieved with a finite θ. ii) If the equality in Kraft's inequality holds, one of the implications has been shown in Theorem 4. Another implication can be shown from a corollary of Theorem 5 as follows.

Corollary 6. *Consider a key consumption profile $f(u)$ for $1 \leq u \leq M$ of an EPS system. If*

$$\sum_u 2^{-f(u)} < 1, \tag{55}$$

then the given EPS system can be improved by reducing the expected key consumption.

Proof: Suppose $\sum_u 2^{-f(u)} = 1 - \gamma$ for $\gamma > 0$. Consider $\tilde{V} = (v_u)$ with $v_1 = -\log(2^{-f(1)} + \gamma)$ and $v_u = f(u)$ for $2 \leq u \leq M$. Then $\sum_u 2^{-v_u} = 1$. Theorem 5 shows that there exists an amended partition code whose expected key consumption for message u is arbitrarily close to v_u. Therefore, the given EPS system can be improved. ∎

We can see from (55) that $\sum_u 2^{-f(u)} = 1$ is a necessary condition for an EPS system to achieve the minimal key consumption. Note that the condition is independent of the source distribution P_U and hence it cannot be sufficient. However, it can help us to find a sufficient condition as shown in the following Theorem 8. It gives us better ideas about how to design an EPS system achieving the minimal key consumption. In order to prove Theorem 8, we need the following information inequality which is interesting in its own. More background about information inequalities can be found in [9]. In contrast to Theorem 4, the following theorem does not require the assumptions in (3)–(5).

Theorem 7. ***[Information inequality]*** *If*

$$\sum_u 2^{-I(R;X|U=u)} = 1, \tag{56}$$

then

$$I(R;X|U) \geq H(U), \tag{57}$$

with equality holds if and only if

$$I(R;X|U=u) = \log \frac{1}{P_U(u)} \quad \forall u. \tag{58}$$

Proof: Let $q(u) = 2^{-I(R;X|U=u)}$ which is nonnegative. Therefore, we can define a probability distribution $Q_U = \{q(u)\}$. Consider

$$I(R;X|U) - H(U) = \sum_u P_U(u) \log \frac{P_U(u)}{Q_U(u)} \geq 0, \tag{59}$$

where the inequality follows form the relative entropy and the equality holds if and only if $P_U(u) = q(u) = 2^{-I(R;X|U=u)}$ for all u [9]. Therefore, the theorem is proved. ∎

Together with Corollary 6, it is easy to verify the following theorem.

Theorem 8. ***[Minimal expected key consumption]*** *For a given P_U, an EPS system with key consumption profile $f(u)$ achieves the minimal expected key consumption if and only if*

$$f(u) = \log \frac{1}{P_U(u)} \quad \forall u. \tag{60}$$

In [3], we only know that the minimal expected key consumption is achieved if and only if

$$I(R;X|U) = I(R;UX) = H(U). \tag{61}$$

Comparing with (61), (60) is a stronger condition which applies to $I(R;X|U=u)$ for all u. Therefore, Theorem 8 can give us new insights about the design of an efficient EPS system. Note that when we minimise the expected key consumption in an EPS system, we also want to minimise the transmission cost measured by $H(X)$. Although partition code can achieve the minimum expected key consumption [3], $H(X)$ can be very large. If an upper bound on $H(X)$ is imposed, how to design an EPS system to achieve the minimal expected key consumption is still an open problem. We believe that Theorem 8 is potentially useful for this problem.

IV. Conclusion

For an EPS system, a new term namely key consumption profile has been introduced which measures the amount of key required for each source symbol. We have derived an inequality which serves as the counterpart of Kraft's inequality in EPS systems. The key consumption profiles of all EPS systems must satisfy the inequality. If a key consumption profile satisfies the inequality, there exists an EPS system with such profile. If the inequality is strict for certain EPS system, the system can be further improved by reducing the key consumption. Sufficient and necessary conditions for an EPS system to achieve the minimum key consumption have been shown.

Acknowledgement

This work was supported by the Australian Research Council (DP1094571).

References

[1] C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, Oct. 1949.

[2] J. L. Massey, "An introduction to contemporary cryptology," *Proc. IEEE*, vol. 76, pp. 533–549, May 1988.

[3] S.-W. Ho, T. Chan and C. Uduwerelle, "Error-free perfect-secrecy systems," in *IEEE International Symposium on Information Theory Proceedings (ISIT)*, pp. 1613–1617, IEEE, 2011.

[4] C. Blundo, A. De Santis, and U. Vaccaro, "On secret sharing schemes," *Information Processing Letters*, vol. 65, pp. 169–175, 1999.

[5] C. Blundo, A. De Santis and A. Giorgio Gaggia, "Probability of shares in secret sharing schemes," *Information Processing Letters*, vol. 72, pp. 25–32, 1998.

[6] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, Wiley-Interscience, 2 Ed., 2006.

[7] I. Csiszár, "The method of types," *IEEE Transactions on Information Theory*, vol. 44, pp. 2505–2523,1998.

[8] S. Boyd and L. Vandenberghe, *Convex optimization*, Cambridge university press, 2004.

[9] R. W. Yeung, *Information Theory and Network Coding*, Springer, 2008.