# Some New Characters on the Wire-Tap Channel of Type II

Yuan Luo, Chaichana Mitrpant, A. J. Han Vinck, *Senior Member, IEEE*, and Kefei Chen

***Abstract*—The noiseless wire-tap channel of type II with coset coding scheme was provided by Ozarow and Wyner. In this correspondence, the user is split into multiple parties who are coordinated in coding their data symbols by using the same encoder. The adversary can tap not only partial transmitted symbols but also partial data symbols. We are interested in the equivocation of the data symbols to this adversary who has more power than that of Ozarow and Wyner.**

**The generalized Hamming weight of Wei and the dimension/length profile (DLP) of Forney are extended to two-code formats: relative generalized Hamming weight and relative dimension/length profile (RDLP). Upper and lower bounds of the new concepts are investigated. They are useful to design a perfect secrecy coding scheme for the coordinated multiparty model. Under a general secrecy standard, the coordinated model can provide a higher transmission rate than an uncoordinated (time-sharing) model.**

***Index Terms*—Dimension/length profile (DLP), generalized Hamming weight, relative dimension/length profile (RDLP), relative generalized Hamming weight, wire-tap channel of type II.**

## I. Introduction

The wire-tap channel invented by Wyner [16] was extensively studied by many authors in binary and nonbinary cases. In an application of linear codes to cryptology, Ozarow and Wyner provided a noiseless wire-tap channel of type II with coset coding scheme in [12]. This scheme is to use $q^r$ cosets of an $[n, n-r]$ linear code over GF$(q)$, where each coset corresponds to $r$ data symbols. The user is composed of a sender and a receiver. The sender has $r$ data symbols to convey to the receiver by encoding them into an $n$-tuple randomly in a corresponding coset. The redundancies are used to confuse an adversary who has full knowledge about the code and cosets, and has the ability to tap $\mu$ symbols of his choice from the $n$-tuple. By checking the cosets, the receiver can retrieve the $r$ data symbols from the $n$-tuple. The adversary tries to retrieve the $r$ data symbols by guessing the coset. For the given $[n, n-r]$ code, he gets a corresponding minimum uncertainty by choosing the positions of the $\mu$ tapped symbols.

This minimum uncertainty, i.e., equivocation, was described by the generalized Hamming weight presented by Wei [15], which played an important role in coding theory. For example, it was used in connection with trellis complexity by Forney [6], in the analysis of reliability-based decoding, and so on. Helleseth, Kløve, and Mykkeltveit also contributed a lot to the original idea [7].

In this correspondence, the user of the noiseless wire-tap channel of type II with coset coding scheme is split into multiple parties (for example, $m$ senders and $m$ corresponding receivers). They are **coordinated** in coding their data symbols by using the same encoder. A serious case is that the data symbols of nonlegitimate parties are leaked to the adversary, i.e., the adversary can tap not only $\mu$ transmitted symbols but also partial data symbols. We are interested in the equivocation of legitimate parties' data symbols to this adversary who has more power than that of [12].

In Section II, a coordinated two-party wire-tap channel of type II is introduced over GF$(2)$. We assume that the second party is nonlegitimate, i.e., his data symbols are leaked to the adversary. The equivocation of the first party's data symbols to this more powerful adversary is calculated in Theorem 1. These results can be generalized for multiple parties over GF$(q)$ easily.

In Section III, the dimension/length profile (DLP), the inverse dimension/length profile (IDLP). and the length/dimension profile (LDP) [6] are extended to two-code formats: relative dimension/length profile (RDLP), inverse relative dimension/length profile (IRDLP), and relative length/dimension profile (RLDP). These two-code formats are determined from each other, see Theorems 2 and 3; and used to analyze the equivocation in the coordinated multiparty model, see Corollary 1 and the remark of Theorem 3. In addition, the LDP is a sequence of the generalized Hamming weight, and the RLDP can be called a sequence of relative generalized Hamming weight.

For a given pair of codes, the adversary can minimize the uncertainty by selecting the positions of his tapped symbols. In Section IV, we consider some suitable pairs of codes in such a way that the equivocation is as large as possible. We provide an upper bound on the equivocation in Theorem 4, and present some pairs of codes achieving the bound. This bound has two other equivalent forms, one of which is a generalization of the Singleton bound. Some equivalent conditions for achieving the bounds are also investigated.

The bounds are useful to design a perfect secrecy coding scheme for the coordinated multiparty wire-tap channel of type II, see Proposition 4 and Theorem 5 of Section V. Since perfect secrecy cannot be obtained in many cases, $\alpha$(or less)-perfect secrecy is also considered. Under a general secrecy standard, it is possible for the coordinated multiparty model to provide a higher transmission rate than an uncoordinated (time-sharing) multiparty model.

Final conclusions are presented in Section VI.

## II. Coordinated Two-Party Wiretap Channel of Type II

In this section, we are interested in a coordinated two-party wire-tap channel of type II with coset coding scheme over GF$(2)$.

In the general noiseless wire-tap channel of type II with coset coding scheme over GF$(2)$ [12], let $S$ be the data bits of a sender, which is a random vector of length $r$ with uniform distribution over GF$(2)^r$. Let $A$ be an $r \times n$ matrix with rank $r$ over GF$(2)$. For a given $S = \boldsymbol{s}$, the coset coding scheme is to encode $S$ into $X = \boldsymbol{x}$ uniformly from the solutions of $A \cdot \boldsymbol{x}^T = \boldsymbol{s}^T$

$$p(X = \boldsymbol{x} \mid S = \boldsymbol{s}) = \begin{cases} \frac{1}{2^{n-r}}, & \text{if } A \cdot \boldsymbol{x}^T = \boldsymbol{s}^T \\ 0, & \text{otherwise} \end{cases} \tag{1}$$

where $X$ is transmitted as a random vector of length $n$ to a receiver. It is easy to verify that $X$ is uniformly distributed on GF$(2)^n$. The receiver can retrieve the $r$ data bits by calculating $A \cdot X^T$. Denote

$$X = (X_1, \ldots, X_n) \quad \text{and} \quad \boldsymbol{x} = (x_1, \ldots, x_n).$$

The redundant $n-r$ bits are used to confuse an adversary, who has full knowledge of the matrix $A$ and has ability to tap $\mu$ transmitted bits

$$Z^{\mu} = \{X_t : t \in \tau\} \tag{2}$$

Manuscript received December 22, 2003; revised October 28, 2004. This work was supported in part by the German Science Foundation-DFG and the National Natural Science Foundation of China under Grants 60402022, 90104005, 60173032, and 60303026.

Y. Luo and K. Chen are with the Computer Science and Engineering Department, Shanghai Jiao Tong University, Shanghai 200030, China (e-mail: yuanluo@sjtu.edu.cn, kfchen@sjtu.edu.cn).

C. Mitrpant is with the NECTEC, Klong Luang, Phathumthani 12120, Thailand (e-mail: cmi@nectec.or.th).

A. J. H. Vinck is with the Institute for Experimental Mathematics, Duisburg-Essen University, 45326 Essen, Germany (e-mail: vinck@exp-math.uni-essen.de).

Communicated by K. A. S. Abdel-Ghaffar, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2004.842763

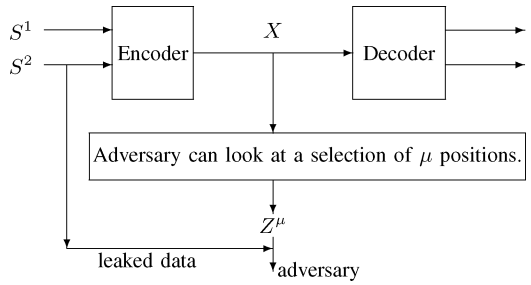


Fig. 1. A coordinated two-party wire-tap channel of type II when $S^2$ are leaked.

where $\tau \subseteq \{1, \ldots, n\}$ and $|\tau| = \mu$. For the given matrix $A$, the adversary tries to retrieve the $r$ data bits by guessing the $n - \mu$ remaining bits of $X$, and gets a corresponding minimum uncertainty by selecting the positions of the $\mu$ tapped bits. The minimum uncertainty

$$\Delta_\mu := \min_{\tau:|\tau|=\mu} H(S \mid Z^\mu) \tag{3}$$

is called equivocation and described by the generalized Hamming weight [15]. A goal for the sender is to maximize the equivocation by searching for a suitable matrix $A$. Another interesting parameter is the minimal number of further tapped bits for the adversary to get one additional data bit, which was considered in [2]–[4]. For some other variations of the channel in cryptosystems, see [9], [11].

In this section, we consider a serious case: some data bits are leaked to the adversary, i.e., the adversary can tap not only $\mu$ transmitted bits but also partial data bits. It is easy to see that this adversary has more power than that of [12]. The user (a sender and a corresponding receiver) is split into two parties (two senders and two corresponding receivers), see Fig. 1. They are coordinated in coding their data bits by using the same encoder of the matrix $A$. Let $S = (S^1, S^2)$, where $S^1$ is the data bits of the first sender with $r_1$ components and $S^2$ is of the second sender with $r_2 = r - r_1$ components. Assume that the second party is nonlegitimate, i.e., $S^2$ is leaked to the adversary. We are interested in the equivocation of the first party's data bits to this more powerful adversary

$$\Delta_{1|2;\mu} := \min_{\tau:|\tau|=\mu} H(S^1 \mid Z^\mu, S^2). \tag{4}$$

The following results are for two parties over binary field, but can be generalized to multiple parties over GF$(q)$ easily. For the $q$-ary case, the entropy is the $q$-ary entropy, see [13, p. 15].

Theorem 1 provides an algebraic expression of the equivocation (4), where the matrix $A$ is expressed as

$$A := \begin{pmatrix} A^1 \\ A^2 \end{pmatrix}_{r \times n}$$
$$A^1 := (A_1^1, \ldots, A_n^1)_{r_1 \times n}, \quad A^2 := (A_1^2, \ldots, A_n^2)_{r_2 \times n}$$

and $A_t^\eta$ $(1 \le \eta \le 2, 1 \le t \le n)$ is a column vector with $r_\eta$ components.

*Theorem 1:* In the model of Fig. 1 for a coordinated two-party wire-tap channel of type II over binary field, we have

$$\Delta_{1|2;\mu} = \min_{\varphi:|\varphi|=n-\mu} \left[ \operatorname{rank} \begin{pmatrix} A_{l_1}^1, \ldots, A_{l_{n-\mu}}^1 \\ A_{l_1}^2, \ldots, A_{l_{n-\mu}}^2 \end{pmatrix} - \operatorname{rank} \left( A_{l_1}^2, \ldots, A_{l_{n-\mu}}^2 \right) \right] \tag{5}$$

where $\varphi = \{l_1, \ldots, l_{n-\mu}\} \subseteq \{1, \ldots, n\}$.

*Proof:* From the definition (4) and the chain rule of entropy, it is easy to verify that

$$\begin{aligned} \Delta_{1|2;\mu} &= \min_{\tau:|\tau|=\mu} H(S^1 \mid Z^\mu, S^2), \\ &= \min_{\tau:|\tau|=\mu} [H(S^1, S^2 \mid Z^\mu) - H(S^2 \mid Z^\mu)] \end{aligned} \tag{6}$$

where $\tau$ is a subset of $\{1, \ldots, n\}$ with size $\mu$ and $Z^\mu = \{X_t : t \in \tau\}$. Let $\{l_1, \ldots, l_{n-\mu}\} = \{1, \ldots, n\} \backslash \tau$. We will show that

$$H(S^1, S^2 | Z^\mu) = \operatorname{rank} \begin{pmatrix} A_{l_1}^1, \ldots, A_{l_{n-\mu}}^1 \\ A_{l_1}^2, \ldots, A_{l_{n-\mu}}^2 \end{pmatrix} \tag{7}$$

and

$$H(S^2 | Z^\mu) = \operatorname{rank} \left( A_{l_1}^2, \ldots, A_{l_{n-\mu}}^2 \right). \tag{8}$$

This theorem can be obtained by using (6)–(8). Without loss of generality, assume that $\tau = \{1, \ldots, \mu\}$. Then

$$\{l_1, \ldots, l_{n-\mu}\} = \{1, \ldots, n\} \backslash \tau = \{\mu + 1, \ldots, n\}.$$

The proof of (7) is the same as the following algebraic proof of (8).

Denote $\Lambda = \operatorname{rank}(A_{\mu+1}^2, \ldots, A_n^2)$. For fixed $(x_1, \ldots, x_\mu)$ and given $S^2 = \boldsymbol{s}^2$, let $\Gamma$ be the set of solutions for $(x_{\mu+1}, \ldots, x_n)$ in (9) or (10)

$$A^2 \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = (\boldsymbol{s}^2)^T \tag{9}$$

i.e.,

$$(A_{\mu+1}^2, \ldots, A_n^2) \begin{pmatrix} x_{\mu+1} \\ \vdots \\ x_n \end{pmatrix} = (\boldsymbol{s}^2)^T - (A_1^2, \ldots, A_\mu^2) \begin{pmatrix} x_1 \\ \vdots \\ x_\mu \end{pmatrix}. \tag{10}$$

Then $|\Gamma| = 0$ or $2^{n-\mu-\Lambda}$. Note that $\Gamma$ can be empty.

It follows from the coding method that $X_1, \ldots, X_n, S^1$, and $S^2$ are all uniformly distributed. Furthermore, $X_1, \ldots, X_n$ are independent, and $S^1$ and $S^2$ are also independent. Then

$$\begin{aligned} &p(X_1 = x_1, \ldots, X_n = x_n \mid S^2 = \boldsymbol{s}^2) \\ &\quad = p(X_1 = x_1, \ldots, X_n = x_n, S^1 = \boldsymbol{s}^1 \mid S^2 = \boldsymbol{s}^2) \\ &\quad = 2^{-r_1} p(X_1 = x_1, \ldots, X_n = x_n \mid S^1 = \boldsymbol{s}^1, S^2 = \boldsymbol{s}^2) \end{aligned}$$

where

$$(\boldsymbol{s}^1)^T = A^1 \cdot (x_1, \ldots, x_n)^T.$$

If (9) is satisfied, i.e., if $A^2 \cdot \boldsymbol{x}^T = (\boldsymbol{s}^2)^T$, we have $A \cdot \boldsymbol{x}^T = (\boldsymbol{s}^1, \boldsymbol{s}^2)^T$ and then

$$\begin{aligned} &p(X_1 = x_1, \ldots, X_n = x_n \mid S^2 = \boldsymbol{s}^2) \\ &\quad = 2^{-r_1} \cdot 2^{-(n-r)} = 2^{-(n-r_2)}. \end{aligned} \tag{11}$$

Otherwise,

$$p(X_1 = x_1, \ldots, X_n = x_n \mid S^2 = \boldsymbol{s}^2) = 0.$$

Since $\tau = \{1, \ldots, \mu\}$, by using (11)

$$\begin{aligned} &p(S^2 = \boldsymbol{s}^2 \mid Z^\mu = (x_1, \ldots, x_\mu)) \\ &\quad = p(S^2 = \boldsymbol{s}^2 \mid X_1 = x_1, \ldots, X_\mu = x_\mu) \\ &\quad = \frac{p(X_1 = x_1, \ldots, X_\mu = x_\mu \mid S^2 = \boldsymbol{s}^2) p(S^2 = \boldsymbol{s}^2)}{p(X_1 = x_1, \ldots, X_\mu = x_\mu)} \\ &\quad = p(X_1 = x_1, \ldots, X_\mu = x_\mu \mid S^2 = \boldsymbol{s}^2) 2^{\mu - r_2} \end{aligned}$$

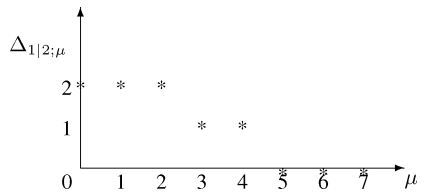


Fig. 2. The equivocation $\Delta_{1|2;\mu}$ in Example 1.

$$
\begin{aligned}
&= 2^{\mu-r_2} \sum_{(x_{\mu+1},\ldots,x_n)} p(X_1 = x_1, \ldots, X_n = x_n \mid S^2 = \boldsymbol{s}^2) \\
&= 2^{\mu-r_2} \sum_{(x_{\mu+1},\ldots,x_n)\in\Gamma} 2^{-(n-r_2)} \\
&= 2^{\mu-n} \mid \Gamma \mid \\
&= 0 \text{ or } 2^{-\Lambda}.
\end{aligned}
$$

Note that $\sum_{\boldsymbol{s}^2} p(S^2 = \boldsymbol{s}^2 \mid Z^\mu = (x_1, \ldots, x_\mu)) = 1$. Therefore,

$$\left| \{\boldsymbol{s}^2 : p(S^2 = \boldsymbol{s}^2 \mid Z^\mu = (x_1, \ldots, x_\mu)) = 1/2^\Lambda\} \right| = 2^\Lambda.$$

Thus, $H(S^2 \mid Z^\mu = (x_1, \ldots, x_\mu)) = \Lambda$ and $H(S^2 \mid Z^\mu) = \Lambda$, and (8) is obtained. □

Theorem 1 shows that the equivocation to a more powerful adversary can be investigated by analyzing the difference between the ranks of a matrix and a submatrix. For the case $r_2 = 0$, the Wyner–Ozarow's result is retrieved.

*Example 1:* In the model of Fig. 1, for $r = 4$ and $n = 7$, let $A$ be a generator matrix of the binary $[7, 4, 3]$ Hamming code

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Assume that $S^1$ is a random vector with $r_1 = 2$ components of the legitimate party, and $S^2$ is a random vector with $r_2 = 2$ components of the nonlegitimate party. Then

$$A^2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

The equivocation $\Delta_{1|2;\mu}$ of $S^1$ to the more powerful adversary is obtained in Fig. 2 via Theorem 1.

It follows that the perfect secrecy $\Delta_{1|2;\mu} = 2$ is achieved if and only if $\mu \leq 2$. Furthermore, the equivocation drops at $\mu = 3$ because at this point the first row of $A$ can be punctured, and drops again at $\mu = 5$ because at this point the first two rows of $A$ can be punctured.

Further investigations of the properties of equivocation and secrecy will be given later.

## III. Relative Dimension/Length Profile (RDLP)

For linear block codes, the DLP, the IDLP, and the LDP, were introduced in [6]. In this section, these concepts are extended to two-code formats by adding a modifier "relative": RDLP, IRDLP, and RLDP. These two-code formats behave similarly to Forney's concepts. They are useful for the study of the equivocation to the more powerful adversary introduced in Section II, see Corollary 1 and the remark of Theorem 3.

Let $J$ be a subset of $I = \{1, \ldots, n\}$. For an $[n, k]$ linear code $C$, its subcode $C_J$ is defined as $\{(c_1, \ldots, c_n) \in C : c_t = 0 \text{ for } t \notin J\}$. Its projection $P_J(C)$ is defined as $\{P_J(\boldsymbol{c}) : \boldsymbol{c} = (c_1, \ldots, c_n) \in C\}$, where $P_J(\boldsymbol{c})$ is a vector of length $n$, and the $t$th component of $P_J(\boldsymbol{c})$ is given by $c_t$ if $t \in J$ and given by 0 if $t \notin J$. A relation between $C_J$ and $P_J(C)$ is presented in Lemma 1.

*Lemma 1 (First Duality Lemma [6]):* For an $[n, k]$ linear code $C$ and a set $J \subseteq I = \{1, \ldots, n\}$

$$\dim[P_J(C)] + \dim(C_{I-J}) = k.$$

For example, let $C$ be a binary $[7, 4, 3]$ Hamming code with the generator matrix $A$ of Example 1. Assume that $J = \{3, 4\}$. Then $I - J = \{1, 2, 5, 6, 7\}$. The code $C_{I-J}$ has generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

The code $P_J(C)$ has generator matrix

$$\begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

It is easy to see that $\dim[P_J(C)] = 2$ and $\dim(C_{I-J}) = 2$.

Let $C^1$ be an $[n, a_1]$ linear code and $C^2$ be an $[n, a_2]$ subcode of $C^1$. The RDLP of $C^1$ and $C^2$ is defined as a sequence

$$K(C^1, C^2) = \{K_i(C^1, C^2) : 0 \leq i \leq n\}$$

where

$$K_i(C^1, C^2) := \max\{\dim(C^1_J) - \dim(C^2_J) :\mid J \mid = i\}. \tag{12}$$

The IRDLP of $C^1$ and $C^2$ is defined as

$$\widetilde{K}(C^1, C^2) = \{\widetilde{K}_i(C^1, C^2) : 0 \leq i \leq n\}$$

where

$$\widetilde{K}_i(C^1, C^2) := \min\{\dim[P_J(C^1)] - \dim[P_J(C^2)] :\mid J \mid = i\}. \tag{13}$$

Let $\Phi$ denote the empty set. Then the DLP and the IDLP of $C^1$ can be retrieved from $K(C^1, \Phi)$ and $\widetilde{K}(C^1, \Phi)$, respectively. By using these two-code formats, Theorem 1 can be described as follows.

*Corollary 1:* In the model of Fig. 1, let $C^1$ be a code with the generator matrix $A$ and $C^2$ be a subcode with the generator matrix $A^2$. For $0 \leq \mu \leq n$

$$\Delta_{1|2;\mu} = \widetilde{K}_{n-\mu}(C^1, C^2).$$

The RDLP and the IRDLP behave similarly to the DLP and the IDLP. Theorem 2 shows that the RDLP and the IRDLP can be determined from each other.

*Theorem 2:* For an $[n, a_1]$ linear code $C^1$ and an $[n, a_2]$ subcode $C^2$, their RDLP and IRDLP are related by

$$K_i(C^1, C^2) = (a_1 - a_2) - \widetilde{K}_{n-i}(C^1, C^2) \quad \text{for} \quad 0 \leq i \leq n.$$

*Proof:* By using Lemma 1, for $0 \leq i \leq n$

$$
\begin{aligned}
&\widetilde{K}_i(C^1, C^2) \\
&\quad = \min\{\dim[P_J(C^1)] - \dim[P_J(C^2)] : |J| = i\} \\
&\quad = \min\{(a_1 - a_2) - \dim(C^1_{I-J}) + \dim(C^2_{I-J}) : |J| = i\} \\
&\quad = \min\{(a_1 - a_2) - \dim(C^1_J) + \dim(C^2_J) : |J| = n - i\} \\
&\quad = (a_1 - a_2) - K_{n-i}(C^1, C^2).
\end{aligned}
$$

□

Then, it is easy to see from Corollary 1 and Theorem 2 that $K(C^1, C^2)$ is a measure of the certainty of the first party's data symbols to the more powerful adversary. Let $i$ denote the number of tapped symbols. The certainty $K_i(C^1, C^2)$ is nondecreasing with $i$ from

$$K_0(C^1, C^2) = \widetilde{K}_0(C^1, C^2) = 0$$

to

$$K_n(C^1, C^2) = \widetilde{K}_n(C^1, C^2) = a_1 - a_2$$

see Proposition 1. The increment at each step is at most 1.

*Proposition 1:* Let $C^1$ be an $[n, a_1]$ linear code, and $C^2$ be an $[n, a_2]$ subcode. For $0 \le i \le n-1$

$$0 \le K_{i+1}(C^1, C^2) - K_i(C^1, C^2) \le 1 \tag{14}$$

$$0 \le \widetilde{K}_{i+1}(C^1, C^2) - \widetilde{K}_i(C^1, C^2) \le 1. \tag{15}$$

In addition, it is easy to see that

$$K_0(C^1, C^2) = \widetilde{K}_0(C^1, C^2) = 0$$

and

$$K_n(C^1, C^2) = \widetilde{K}_n(C^1, C^2) = a_1 - a_2.$$

*Proof:* From Theorem 2, it is easy to see that (14) and (15) are equivalent. Here, we only give a proof of (15). For any fixed subset $J \subset I = \{1, \ldots, n\}$ and an index $t \notin J$, let

$$f = \dim[P_J(C^1)] - \dim[P_J(C^2)]$$

and

$$g = \dim[P_{J \bigcup \{t\}}(C^1)] - \dim[P_{J \bigcup \{t\}}(C^2)].$$

We have to consider the following two cases.

1) $\dim[P_{J \bigcup \{t\}}(C^2)] = \dim[P_J(C^2)]$. We have
$$f + 1 \ge g \ge f. \tag{16}$$

2) $\dim[P_{J \bigcup \{t\}}(C^2)] = \dim[P_J(C^2)] + 1$. By considering a code as a matrix (each row is a codeword), we know that the $t$th column of $P_{J \bigcup \{t\}}(C^2)$ is linearly independent of all the columns of $P_J(C^2)$. Then the $t$th column of $P_{J \bigcup \{t\}}(C^1)$ is also linearly independent of all the columns of $P_J(C^1)$. Therefore,
$$\dim[P_{J \bigcup \{t\}}(C^1)] = \dim[P_J(C^1)] + 1$$
and
$$g = f. \tag{17}$$

From (16) and (17), it follows that $f + 1 \ge g \ge f$. Therefore, it is easy to verify that

$$\widetilde{K}_i(C^1, C^2) + 1 \ge \widetilde{K}_{i+1}(C^1, C^2) \ge \widetilde{K}_i(C^1, C^2)$$

and (15) is obtained. □

For the Wyner–Ozarow scheme, it was shown in [15] that the adversary can obtain at least $r$ symbols of information if and only if he can tap at least $d_r$ transmitted symbols, where $d_r$ is the $r$th generalized Hamming weight of a linear code. For the more powerful adversary, some corresponding results are as follows.

Let $C^1$ be an $[n, a_1]$ linear code and $C^2$ be an $[n, a_2]$ subcode of $C^1$. The RLDP of $C^1$ and $C^2$ is defined as a sequence

$$M(C^1, C^2) = \{M_j(C^1, C^2) : 0 \le j \le a_1 - a_2\}$$

where

$$M_j(C^1, C^2) := \min\{|J| : \dim(C^1_J) - \dim(C^2_J) \ge j\}. \tag{18}$$

If $C^2$ is the empty set $\Phi$, the $j$th generalized Hamming weight of code $C^1$ is retrieved. The RLDP can be called a sequence of **relative generalized Hamming weight**. A relation between the RLDP and the RDLP is shown in Theorem 3. Theorems 2 and 3 imply that the RDLP, the IRDLP, and the RLDP can be determined from each other.

*Theorem 3:* For an $[n, a_1]$ linear code $C^1$ and an $[n, a_2]$ subcode $C^2$

$$\min\{i : K_i(C^1, C^2) \ge j\} = M_j(C^1, C^2)$$

and

$$\max\{j : M_j(C^1, C^2) \le i\} = K_i(C^1, C^2)$$

where $0 \le j \le a_1 - a_2$ and $0 \le i \le n$.

*Proof:*

$$\begin{aligned}&\min\{i : K_i(C^1, C^2) \ge j\}\\ &\quad = \min\{i : \exists |J| = i \text{ such that } \dim(C^1_J) - \dim(C^2_J) \ge j\}\\ &\quad = \min\{|J| : \dim(C^1_J) - \dim(C^2_J) \ge j\} = M_j(C^1, C^2),\end{aligned}$$

and

$$\begin{aligned}&\max\{j : M_j(C^1, C^2) \le i\}\\ &\quad = \max\{j : \exists |J| \le i \text{ such that } \dim(C^1_J) - \dim(C^2_J) \ge j\}\\ &\quad = \max\{\dim(C^1_J) - \dim(C^2_J) : |J| \le i\} = K_i(C^1, C^2).\end{aligned}$$ □

*Remark:* For $0 \le \mu \le n$ and $0 \le j \le a_1 - a_2$, $K_\mu(C^1, C^2) \ge j$ if and only if $M_j(C^1, C^2) \le \mu$. Therefore, in the model of Fig. 1, the adversary can obtain at least $j$ information bits of $S^1$ if and only if he can tap at least $M_j(C^1, C^2)$ transmitted bits from $X$, where $C^1$ is a linear code with the generator matrix $A$ and $C^2$ is a subcode with the generator matrix $A^2$.

From Proposition 1, we know that $K_i(C^1, C^2)$ is nondecreasing with $i$ from $K_0(C^1, C^2) = 0$ to $K_n(C^1, C^2) = a_1 - a_2$. The increment at each step is at most 1. In addition

$$\{i : K_i(C^1, C^2) = j\} \cap \{i : K_i(C^1, C^2) \ge j + 1\} = \Phi.$$

Then, it follows from Theorem 3 that

$$\begin{aligned}M_j(C^1, C^2) &= \min\{i : K_i(C^1, C^2) \ge j\}\\ &= \min\{i : K_i(C^1, C^2) = j\}\end{aligned}$$

where $0 \le j \le a_1 - a_2$. So $M_j(C^1, C^2)$ is strictly increasing with $j$ and thus,

$$M_j(C^1, C^2) = \min\{|J| : \dim(C^1_J) - \dim(C^2_J) = j\}.$$

Therefore, Proposition 2 follows.

*Proposition 2:* For an $[n, a_1]$ linear code $C^1$ and an $[n, a_2]$ subcode $C^2$, $M_j(C^1, C^2)$ is strictly increasing with $j$. Moreover, $M_0(C^1, C^2) = 0$ and

$$\begin{aligned}M_j(C^1, C^2) &= \min\{i : K_i(C^1, C^2) = j\}\\ &= \min\{|J| : \dim(C^1_J) - \dim(C^2_J) = j\}\end{aligned}$$

where $0 \le j \le a_1 - a_2$.

*Example 2:* Let $C^1$ be the binary $[7, 4, 3]$ Hamming code with the generator matrix $A$ of Example 1. Let $C^2$ be the subcode with the generator matrix $A^2$. Then

$$\begin{aligned}K(C^1, C^2) &= \{0,\ 0,\ 0,\ 1,\ 1,\ 2,\ 2,\ 2\}\\ \widetilde{K}(C^1, C^2) &= \{0,\ 0,\ 0,\ 1,\ 1,\ 2,\ 2,\ 2\}\\ M(C^1, C^2) &= \{0,\ 3,\ 5\}.\end{aligned}$$

The properties of Theorem 2, Proposition 1, Theorem 3, and Proposition 2 are all satisfied. We know from the remark of Theorem 3 that the adversary can get at least 1 information bit of $S^1$ if and only if he can tap at least $M_1(C^1, C^2) = 3$ transmitted bits; and get at least

2 information bits if and only if he can tap at least $M_2(C^1, C^2) = 5$ transmitted bits.

## IV. A Generalization of the Singleton Bound

For a given pair of codes $C^1$ and $C^2$, it follows from Corollary 1 that the adversary with parameter $\mu$ can obtain a minimum uncertainty, i.e., the equivocation, by selecting the positions of the $\mu$ tapped symbols. We try to search some suitable pairs of codes in such a way that the equivocation is as large as possible. In this section, we provide an upper bound $UP(\widetilde{K})$ on the equivocation, and present some pairs of codes achieving the bound. This bound has two other equivalent forms $LO(K)$ and $UP(M)$, where $UP(M)$ is a generalization of the Singleton bound. Some equivalent conditions for achieving the bounds are also investigated.

For any two integer sequences $\{\pi_0, \ldots, \pi_n\}$ and $\{\delta_0, \ldots, \delta_n\}$, we say that $\{\pi_0, \ldots, \pi_n\}$ is upper-bounded by $\{\delta_0, \ldots, \delta_n\}$ if $\pi_i \leq \delta_i$ for $0 \leq i \leq n$. We say that $\{\pi_0, \ldots, \pi_n\}$ is lower-bounded by $\{\delta_0, \ldots, \delta_n\}$ if $\pi_i \geq \delta_i$ for $0 \leq i \leq n$. The following Lemma 2 is useful to establish the main results of this section. It presents an upper bound and a lower bound for a special kind of nondecreasing sequences.

*Lemma 2:* Let $\{\pi_i : 0 \leq i \leq n\}$ be an integer sequence of length $n+1$. If $\pi_i$ is nondecreasing with $i$ from $\pi_0 = 0$ to $\pi_n = k$ where $k \leq n$, and the increment of each step is at most 1, then

$$\{\pi_i : 0 \leq i \leq n\} \leq \{\epsilon_i : 0 \leq i \leq n\} := \{0, 1, 2, \ldots, k, \ldots, k\} \quad (19)$$

where $\min\{i : \epsilon_i = k\} = k$, and

$$\{\pi_i : 0 \leq i \leq n\} \geq \{\gamma_i : 0 \leq i \leq n\} := \{0, \ldots, 0, 1, 2, \ldots, k\} \quad (20)$$

where $\max\{i : \gamma_i = 0\} = n - k$. Furthermore, for $k = n$, if (19) and (20) are both satisfied, we have

$$\{\pi_i : 0 \leq i \leq n\} = \{0, 1, 2, \ldots, n\}.$$

*Proof:* Formula (19) follows from $\pi_0 = 0$ and $\pi_{i+1} \leq \pi_i + 1$. Formula (20) follows from $\pi_n = k$ and $\pi_{i-1} \geq \pi_i - 1$. □

The bounds $UP(\widetilde{K})$, $LO(K)$, and $UP(M)$ are provided in Theorem 4. In Proposition 3, we show that if one of these bounds is achieved, so are the other two. Then, some equivalent conditions and examples achieving these bounds are provided.

*Theorem 4:* For an $[n, a_1]$ linear code $C^1$ and an $[n, a_2]$ subcode $C^2$, their inverse RDLP $\widetilde{K}(C^1, C^2)$ is upper-bounded by $UP(\widetilde{K})$

$$\{UP(\widetilde{K})_i : 0 \leq i \leq n\} := \{0, \ldots, 0, 1, 2, \ldots, a_1 - a_2, \ldots, a_1 - a_2\} \quad (21)$$

where $\max\{i : UP(\widetilde{K})_i = 0\} = a_2$. Furthermore, their RDLP $K(C^1, C^2)$ is lower-bounded by $LO(K)$

$$\{LO(K)_i : 0 \leq i \leq n\} := \{0, \ldots, 0, 1, 2, \ldots, a_1 - a_2, \ldots, a_1 - a_2\} \quad (22)$$

where $\max\{i : LO(K)_i = 0\} = n - a_1$. Their RLDP $M(C^1, C^2)$ is upper-bounded by $UP(M)$ (a generalized Singleton bound)

$$\{UP(M)_j : 0 \leq j \leq a_1 - a_2\} := \{0, n - a_1 + 1, n - a_1 + 2, \ldots, n - a_2\}. \quad (23)$$

*Proof:* First, we show that $\widetilde{K}_{a_2}(C^1, C^2) = 0$. Since $\dim(C^2) = a_2$, there is a set $J \subseteq \{1, \ldots, n\}$ such that $|J| = a_2$ and $\dim[P_J(C^2)] = a_2$. Therefore,

$$\dim[P_J(C^1)] - \dim[P_J(C^2)] = 0$$

since

$$\dim[P_J(C^2)] \leq \dim[P_J(C^1)] \leq |J|.$$

So $\widetilde{K}_{a_2}(C^1, C^2) = 0$.

Second, it follows from $\widetilde{K}_{a_2}(C^1, C^2) = 0$ and Proposition 1 that $\widetilde{K}_i(C^1, C^2)$ is nondecreasing with $i$ from $\widetilde{K}_{a_2}(C^1, C^2) = 0$ to $\widetilde{K}_n(C^1, C^2) = a_1 - a_2$, and the increment of each step is at most 1. Then, by using Lemma 2, $\widetilde{K}(C^1, C^2) \leq UP(\widetilde{K})$.

Third, it is easy to see from the upper bound $UP(\widetilde{K})$ and Theorem 2 that $K(C^1, C^2) \geq LO(K)$.

Finally, the upper bound $UP(M)$ is obtained below. From the second part of this theorem, we have $K_{n-a_2}(C^1, C^2) \geq a_1 - a_2$. Then by using the relation of $M(C^1, C^2)$ and $K(C^1, C^2)$ in Theorem 3, it follows that

$$M_{a_1 - a_2}(C^1, C^2) = \min\{i : K_i(C^1, C^2) \geq a_1 - a_2\} \leq n - a_2.$$

Moreover, Proposition 2 shows that $M_j(C^1, C^2)$ is strictly increasing with $j$. Therefore, $M(C^1, C^2)$ is upper-bounded by $UP(M)$ since $M_{a_1 - a_2}(C^1, C^2) \leq n - a_2$ and $M_0(C^1, C^2) = 0$. □

It follows from the upper bound $UP(M)$ that for $1 \leq j \leq a_1 - a_2$

$$M_j(C^1, C^2) \leq n - a_1 + j. \quad (24)$$

The Singleton bound is retrieved from $UP(M)$ when $C^2 = \Phi$. A relation among the bounds $UP(\widetilde{K})$, $LO(K)$, and $UP(M)$ is presented in Proposition 3.

*Proposition 3:* For an $[n, a_1]$ linear code $C^1$ and an $[n, a_2]$ subcode $C^2$, if one of the bounds $UP(\widetilde{K})$, $LO(K)$, or $UP(M)$ is achieved, then so are the other two. Furthermore, $UP(\widetilde{K})$ is achieved if and only if $\widetilde{K}_{a_1}(C^1, C^2) = a_1 - a_2$, $LO(K)$ is achieved if and only if $K_{n-a_1}(C^1, C^2) = 0$, and $UP(M)$ is achieved if and only if $M_1(C^1, C^2) = n - a_1 + 1$.

*Proof:* The first part of this proposition is obvious since $\widetilde{K}(C^1, C^2)$, $K(C^1, C^2)$, and $M(C^1, C^2)$ can be determined from each other via Theorems 2 and 3. A proof of the second part is given as follows.

Assume that $\widetilde{K}_{a_1}(C^1, C^2) = a_1 - a_2$. We know from Theorem 4 that $\widetilde{K}_{a_2}(C^1, C^2)$ is always 0. Then, it follows from Proposition 1 that $\widetilde{K}_i(C^1, C^2)$ is nondecreasing with $i$ from $\widetilde{K}_{a_2}(C^1, C^2) = 0$ to $\widetilde{K}_{a_1}(C^1, C^2) = a_1 - a_2$. The increment at each step is at most 1. By using Lemma 2, we have

$$\{\widetilde{K}_i(C^1, C^2) : a_2 \leq i \leq a_1\} = \{0, 1, \ldots, a_1 - a_2\}.$$

Therefore, $\widetilde{K}(C^1, C^2)$ achieves the upper bound $UP(\widetilde{K})$. This implies that $UP(\widetilde{K})$ is achieved if and only if $\widetilde{K}_{a_1}(C^1, C^2) = a_1 - a_2$.

By using the same arguments, $LO(K)$ is achieved if and only if $K_{n-a_1}(C^1, C^2) = 0$.

Assume that $M_1(C^1, C^2) = n - a_1 + 1$. We know from Theorem 4 that $M_{a_1 - a_2}(C^1, C^2) \leq n - a_2$. Then, it follows from Proposition 2 that $M_j(C^1, C^2)$ is strictly increasing with $j$ from $M_1(C^1, C^2) = n - a_1 + 1$ to $M_{a_1 - a_2}(C^1, C^2) = n - a_2$, and $M_0(C^1, C^2) = 0$. Therefore, $M(C^1, C^2)$ achieves the upper bound $UP(M)$. This implies that $UP(M)$ is achieved if and only if $M_1(C^1, C^2) = n - a_1 + 1$. □

The Singleton bound can be retrieved from $UP(M)$ when $C^2 = \Phi$, i.e., $C^1$ is a maximum distance separable (MDS) code if and only if one of the following conditions is true:

- $M_1(C^1, \Phi) = n - a_1 + 1$;
- $K_{n-a_1}(C^1, \Phi) = 0$, i.e.,

$$\max\{\dim(C^1_J) : |J| = n - a_1\} = 0$$

where $J \subseteq \{1, \ldots, n\}$.

Therefore, for any MDS code $C^1$ and any subcode $\Pi \subseteq C^1$, we have

$$\max\{\dim(C^1_J) - \dim(\Pi_J) : |J| = n - a_1\} = 0$$

where $J \subseteq \{1, \ldots, n\}$, i.e., we have $K_{n-a_1}(C^1, \Pi) = 0$. For the pair of codes $C^1$ and $\Pi$, the bounds $UP(\widetilde{K})$, $LO(K)$, and $UP(M)$ are all achieved.

*Corollary 2:* For any MDS code $C^1$ and any subcode $\Pi \subseteq C^1$, the bounds $UP(\widetilde{K})$, $LO(K)$, and $UP(M)$ are all achieved.

Note that $C^1$ need not be MDS for achieving the bounds. For example, let $C^1$ be a binary non-MDS code with a generator matrix $A$ and $C^2$ be a subcode with a generator matrix $A^2$, where

$$A = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix} \quad \text{and} \quad A^2 = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}. \quad (25)$$

It is easy to verify that the bounds $UP(\widetilde{K})$, $LO(K)$, and $UP(M)$ are also achieved since $K_2(C^1, C^2) = 0$. More research about the bounds are provided in [10].

## V. Secrecy System

### A. Perfect Secrecy

The strongest possible notion of security of a cryptosystem is the perfect secrecy defined in [14]. Almost-perfect secrecy is considered when the perfect secrecy is hard to be achieved. Perfect secrecy and almost-perfect secrecy are also investigated in some other cryptosystems, for examples, see the wire-tap channel [16], the broadcast channel [5], and the generalized privacy amplification [1].

In the model of Fig. 1 of the coordinated two-party wire-tap channel of type II, denote

$$a_1 = r \quad \text{and} \quad a_2 = r_2.$$

"Perfect secrecy with respect to $\Delta_{1|2;\mu}$" is denoted by

$$\min_{\tau:|\tau|=\mu} H(S^1 \mid Z^\mu, S^2) = H(S^1). \quad (26)$$

It is easy to see from Corollary 1 that (26) is equivalent to

$$\widetilde{K}_{n-\mu}(C^1, C^2) = a_1 - a_2 \quad (27)$$

where $a_1$ is the dimension of $C^1$ and $a_2$ is the dimension of the subcode $C^2$. But it follows from Theorem 4 that (27) is not possible for $n - \mu < a_1$. In this section, we consider a suboptimal case "$\alpha$-perfect secrecy with respect to $\Delta_{1|2;\mu}$"

$$\widetilde{K}_{n-\mu}(C^1, C^2) \geq \lceil \alpha(a_1 - a_2) \rceil \quad (28)$$

where $\alpha$ is a little less than 1. Some equivalent expressions of $\alpha$-perfect secrecy are presented in Proposition 4.

*Proposition 4:* In the model of Fig. 1 for the coordinated two-party wire-tap channel of type II, let $C^1$ be a linear code with the generator matrix $A$ and $C^2$ be a subcode with the generator matrix $A^2$. Denote $a_1 = r$ and $a_2 = r_2$. Then the channel has $\alpha$-perfect secrecy with respect to $\Delta_{1|2;\mu}$ if and only if

$$K_\mu(C^1, C^2) \leq \beta \quad (29)$$

where $\beta = \lfloor (1 - \alpha)(a_1 - a_2) \rfloor$, which is also equivalent to

$$M_{\beta+1}(C^1, C^2) \geq \mu + 1. \quad (30)$$

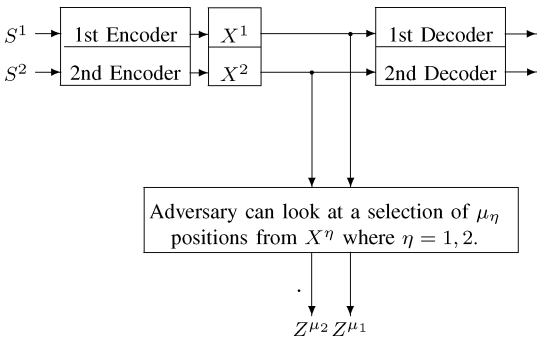


Fig. 3. A time-sharing two-party wire-tap channel of type II.

*Proof:* This proposition can be derived from (28) by using Theorem 2 and Theorem 3. □

Unfortunately, high transmission rate and high secrecy cannot be obtained at the same time. A relation between the transmission rate and the parameter $\alpha$ is given in Theorem 5 for the coordinated two-party wire-tap channel of type II. If the channel has $\alpha$-perfect secrecy with respect to $\Delta_{1|2;\mu}$, it follows from (23) and (30) that

$$n - a_1 + \beta + 1 \geq M_{\beta+1}(C^1, C^2) \geq \mu + 1. \quad (31)$$

Therefore,

$$n \geq \mu + a_1 - \beta = \mu + \lceil \alpha(a_1 - a_2) + a_2 \rceil. \quad (32)$$

In other words, if $n < \mu + \lceil \alpha(a_1 - a_2) + a_2 \rceil$, there is no channel with $\alpha$-perfect secrecy for the legitimate party $S^1$ against the more powerful adversary with parameter $\mu$. This implies Theorem 5.

*Theorem 5:* In the model of Fig. 1 for a coordinated two-party wire-tap channel of type II, if the channel has $\alpha$-perfect secrecy with respect to $\Delta_{1|2;\mu}$, the transmission rate $r/n$ is upper-bounded by

$$\frac{r}{\mu + \lceil \alpha(r - r_2) + r_2 \rceil}. \quad (33)$$

Moreover, the upper bound is achieved if and only if the equalities of (31) hold.

For Example, in the model of Fig. 1, if the matrices $A$ and $A^2$ are of Example 1, then for $\mu = 4$, $r = 4$, $r_2 = 2$, and $\alpha = 0.5$, the transmission rate $4/7$ reaches the upper bound (33) since $M_2(C^1, C^2) = 5$. Another example is for perfect secrecy, i.e., $\alpha = 1$. We can take $A$ and $A^2$ from (25). Then for parameters $\mu = 2$, $r = 3$, $r_2 = 2$, and $\alpha = 1$, the upper bound $3/5$ is achieved.

### B. A Comparison With Time-Sharing Model

A time-sharing multiparty wire-tap channel of type II is a true multiuser model with independent parallel channels, see Fig. 3. Since the encoders are independent, we do not consider the nonlegitimate party case. In this subsection, by a comparison with the time-sharing model under a general secrecy standard, we show that it is possible for the model of Fig. 1 to provide a higher transmission rate when $S^2$ is not leaked to the adversary.

In the model of Fig. 1, suppose that $S^2$ is not leaked to the adversary. Let $\Delta_{1|;\mu}$ denote $\min_{\tau:|\tau|=\mu} H(S^1 \mid Z^\mu)$ and $\Delta_{2|;\mu}$ denote $\min_{\tau:|\tau|=\mu} H(S^2 \mid Z^\mu)$. By using the same arguments of Theorem 1 and Corollary 1, we have

$$\Delta_{1|;\mu} = \widetilde{K}_{n-\mu}(C^3, \Phi) \quad \text{and} \quad \Delta_{2|;\mu} = \widetilde{K}_{n-\mu}(C^2, \Phi)$$

where $C^3$ is an $[n, r_1]$ linear code with the generator matrix $A^1$ and $C^2$ is an $[n, r_2]$ linear code with the generator matrix $A^2$. As mentioned in Section V-A, perfect secrecy of each party, i.e.,

$$\widetilde{K}_{n-\mu}(C^3, \Phi) = r_1 \quad \text{and} \quad \widetilde{K}_{n-\mu}(C^2, \Phi) = r_2 \tag{34}$$

cannot be achieved for $n - \mu < r_1$ and $n - \mu < r_2$, respectively. A weaker secrecy standard is $\alpha$-perfect secrecy of each party, i.e.,

$$\widetilde{K}_{n-\mu}(C^3, \Phi) \geq \lceil \alpha r_1 \rceil \quad \text{and} \quad \widetilde{K}_{n-\mu}(C^2, \Phi) \geq \lceil \alpha r_2 \rceil \tag{35}$$

where $\alpha$ is a little less than 1. By using the same arguments as those of (32), we have $n \geq \mu + \lceil \alpha r_1 \rceil$ and $n \geq \mu + \lceil \alpha r_2 \rceil$. Then Corollary 3 follows.

*Corollary 3:* In the model of Fig. 1, suppose $S^2$ is not leaked to the adversary. If the channel has $\alpha$-perfect secrecy of each party, the transmission rate $r/n$ is upper-bounded by

$$\frac{r}{\mu + \max\{\lceil \alpha r_1 \rceil, \lceil \alpha r_2 \rceil\}}. \tag{36}$$

A time-sharing two-party wire-tap channel of type II described in Fig. 3 is a system of two single wire-tap channels of type II arranged in parallel. For a comparison with Fig. 1, denote the message length of input $S^\eta$ by $r_\eta$, and denote the corresponding codeword length of $X^\eta$ by $n_\eta$, where $\eta = 1, 2$. An adversary can look at a selection of $\mu_\eta$ positions from $X^\eta$. Let $r = r_1 + r_2$, $n = n_1 + n_2$, and $\mu = \mu_1 + \mu_2$. If the channel has $\alpha$-perfect secrecy of each party, i.e., if each party has $\alpha$-perfect secrecy with respect to the corresponding $\Delta_{\eta|;\mu_\eta}$, then it is easy to see from (32) that $n_\eta \geq \mu_\eta + \lceil \alpha r_\eta \rceil$. Therefore, the transmission rate $r/n$ is upper-bounded by

$$\frac{r}{\mu + \sum_{1 \leq \eta \leq 2} \lceil \alpha r_\eta \rceil} \tag{37}$$

since

$$n = \sum_\eta n_\eta \geq \sum_\eta (\mu_\eta + \lceil \alpha r_\eta \rceil) = \mu + \sum_\eta \lceil \alpha r_\eta \rceil.$$

Observe that the upper bound (37) is much smaller than the upper bound (36). An explanation is that, in (36), the data of one party can be used by another party to confuse the adversary, which is not possible in (37). In other words, more redundancies are needed in (37) for each party to confuse the adversary. Therefore, if the channel is requested to have $\alpha$-perfect secrecy of each party, it is possible for the model of Fig. 1 (when $S^2$ is not leaked to the adversary) to provide a higher transmission rate than the time-sharing model of Fig. 3.

*Example 3:* In the model of Fig. 1 for a coordinated two-party wire-tap channel of type II, assume that $S^2$ is not leaked to the adversary. Let the matrix $A$ be over GF$(8)$

$$A = \begin{pmatrix} \omega^6 & \omega^5 & \omega^5 & \omega^2 & 1 & 0 & 0 \\ 0 & \omega^6 & \omega^5 & \omega^5 & \omega^2 & 1 & 0 \\ 0 & 0 & \omega^6 & \omega^5 & \omega^5 & \omega^2 & 1 \\ 0 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 \\ \omega & \omega & \omega & \omega & \omega & \omega & \omega \end{pmatrix}_{5 \times 7}$$

where GF$(8) = F_2[x]_{x^3+x+1}$ and $\omega$ is the primitive element $x$. Let $r_1 = 3$ and $r_2 = 2$. Then the corresponding matrix $A^1$ generates a $[7, 3]$ Reed–Solomon code $C^R$, see [8, p. 145]; and the corresponding matrix $A^2$ generates a $[7, 2]$ linear code $C^L$. It is easy to verify that the channel has perfect secrecy of each party when $\mu = 4$ since $\Delta_{1|;4} = \widetilde{K}_3(C^R, \Phi) = 3$ and $\Delta_{2|;4} = \widetilde{K}_3(C^L, \Phi) = 2$. Its transmission rate $r/n = (r_1 + r_2)/n = 5/7$ reaches the upper bound (36). But we know from (37) that, for $r_1 = 3$, $r_2 = 2$, and $\mu = 4$, if a time-sharing two-party wire-tap channel of type II has perfect secrecy of each party, the transmission rate is at most $5/9$.

## VI. Conclusion

In this correspondence, by studying the coset coding method in a coordinated two-party wire-tap channel of type II, we provide some new concepts: RDLP, relative generalized Hamming weight, and so on, to describe the relation between a linear block code and a subcode. The original concepts; DLP and generalized Hamming weight, were introduced in [6] and [15], respectively. Our new concepts are used to investigate the equivocation to a more powerful adversary who can tap not only partial transmitted symbols but also partial data symbols.

Upper and lower bounds of the new concepts are considered. Some equivalent conditions for achieving these bounds are provided. These bounds are useful to design a perfect secrecy coding scheme for the coordinated model. Unfortunately, perfect secrecy cannot be achieved in many cases. Then, $\alpha$-perfect secrecy is also considered, where $\alpha$ is a little less than 1.

For a comparison with a time-sharing model of Fig. 3, we suppose in Fig. 1 that $S^2$ is not leaked to the adversary. Under a general secrecy standard, the model of Fig. 1 can provide a higher transmission rate than the time-sharing model. An explanation is that, in (36), the data of one party can be used by another party to confuse the adversary, which is not possible in (37).

## Acknowledgment

The authors would like to thank the anonymous reviewers and Associate Editor Khaled Abdel-Ghaffar for their comments and suggestions that helped to improve this correspondence.

## References

[1] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995.

[2] W. Chen and T. Kløve, "On the second greedy weight for linear codes of dimension 3," *Discr. Math.*, vol. 241, pp. 171–187, Oct. 2001.

[3] G. D. Cohen, S. B. Encheva, and G. Zémor, "Antichain codes," in *Proc. IEEE Int. Symp. Information Theory*, Cambridge, MA, Aug. 1998, p. 232.

[4] ——, "Antichain codes," *Des., Codes Cryptogr.*, vol. 18, pp. 71–80, Dec. 1999.

[5] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[6] G. D. Forney, "Dimension/length profiles and trellis complexity of linear block codes," *IEEE Trans. Inf. Theory*, vol. 40, no. 6, pp. 1741–1752, Nov. 1994.

[7] T. Helleseth, T. Kløve, and J. Mykkeltveit, "The weight distribution of irreducible cyclic codes with block lengths $n_1((q^l - 1)/N)$," *Discr. Math.*, vol. 18, pp. 179–211, 1977.

[8] D. G. Hoffman, D. A. Leonard, C. C. Lindner, K. T. Phelps, C. A. Rodger, and J. R. Wall, *Coding Theory*. New York: Marcel Dekker, 1991.

[9] V. Korjik and D. Kushnir, "Key sharing based on the wire-tap channel type II concept with noisy main channel," in *Lecture Notes Computer Science*. Berlin, Germany: Springer-Verlag, 1996, vol. 1163, pp. 210–217.

[10] Y. Luo, F. Fu, C. Mitrpant, and A. J. H. Vinck, "Relative MDS pairs," unpublished manuscript.

[11] M. J. Mihaljević, "On message protection in cryptosystems modeled as the generalized wire-tap channel II," in *Lecture Notes in Computer Science*. Berlin, Germany: Springer-Verlag, 1994, vol. 829, pp. 13–24.

[12] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," *AT&T Bell Labs. Tech. J.*, vol. 63, no. 10, pp. 2135–2157, Dec. 1984.

[13] S. Roman, *Coding and Information Theory*. New York: Springer-Verlag, 1992.

[14] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[15] V. K. Wei, "Generalized Hamming weights for linear codes," *IEEE Trans. Inf. Theory*, vol. 37, no. 5, pp. 1412–1418, Sep. 1991.
[16] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

# On the Scaling Laws of Dense Wireless Sensor Networks: The Data Gathering Channel

Hesham El Gamal, *Senior Member, IEEE*

***Abstract*—We consider dense wireless sensor networks deployed to observe arbitrary random fields. The requirement is to reconstruct an estimate of the random field at a certain *collector node*. This creates a *many-to-one* data gathering wireless channel. In this note, we first characterize the transport capacity of many-to-one dense wireless networks subject to a constraint on the total average power. In particular, we show that the transport capacity scales as $\Theta(\log(N))$ when the number of sensors $N$ grows to infinity and the total average power remains fixed. We then use this result along with some information-theoretic tools to derive sufficient and necessary conditions that characterize the set of *observable* random fields by dense sensor networks. In particular, for random fields that can be modeled as discrete random sequences, we derive a certain form of source/channel coding separation theorem. We further show that one can achieve any desired *nonzero* mean-square estimation error for continuous, Gaussian, and *spatially bandlimited* fields through a scheme composed of single-dimensional quantization, distributed Slepian–Wolf source coding, and the proposed antenna sharing strategy. Based on our results, we revisit earlier conclusions about the feasibility of data gathering applications using dense sensor networks.**

***Index Terms*—Distributed source–channel coding, relay channel, sensor networks, the many-to-one channel, the separation principle.**

## I. Introduction

In a seminal paper, Gupta and Kumar have shown that the capacity of large scale *ad hoc* wireless networks scales as $\Theta(\sqrt{N})$ as the number of nodes $N$ per unit area grows to infinity [1]. This result means that the capacity per node only scales as $\Theta(\sqrt{\frac{1}{N}})$, and hence, goes to zero as $N \to \infty$. While this result advises against deploying dense *ad hoc* networks, the situation may be different in the context of wireless sensor networks. The enabling observation in this context is that the traffic generated at the different sensors is not *independent* as in the case of *ad hoc* networks studied by Gupta and Kumar [2], [3]. In fact, the correlation between the traffic generated at adjacent sensor nodes increases as the density of the sensor nodes per unit area grows. Therefore, as $N \to \infty$, the high correlation between the different observations will result in a traffic per sensor node that goes to zero [2], [3].

There is, however, another important difference between the sensing application and the model used by Gupta and Kumar which was recently observed in [4]. The scenario investigated in [1] assumes *peer-to-peer* communication where the information generated at an *arbitrary* node is transported to another *arbitrary* node. The sensing application, however, implies a fundamental difference in the topology of the network from this peer-to-peer scenario. In this note, we focus on the case where all the sensing information must be collected at *a single* node. We will refer to this scenario as the *many-to-one* channel and to the information sink as the collector node. This architectural difference in the network topology has implications on the maximum traffic carrying capacity of the network. For example, in [4], the authors used the modeling assumptions of [1] to derive the following upper bound on the capacity of this many-to-one channel: Based on the assumption that every node can transmit or receive a maximum of $W$ bits per second [1], it is straightforward to see that the capacity of the many-to-one channel is upper-bounded by $W$. The first contribution of this note is to show that this result is, in fact, *over-restrictive*.

In particular, we show that the transport capacity scales as $\Theta(\log(N))$ when the number of sensors $N$ grows to infinity and the total average power remains fixed. An important part of our approach is a novel transmission scheme that exploits the high density of sensor nodes to facilitate *antenna sharing* at minimal cost in resources. We show that this scheme achieves the same scaling law as the optimal approach while employing single user receivers (i.e., receivers that attempt to detect only one information stream at any point in time treating all other information streams as noise). One of the interesting insights allowed by our proof is that, contrary to the *peer-to-peer* scenario, spatial reuse of the bandwidth does not factor prominently in this many-to-one case. In a nutshell, one san say that the single sink node in the many-to-one channel acts like a *bottleneck*, as predicted by [4]. The cost entailed by this bottleneck is, however, not as dramatic as argued in [4] (instead of lowering the traffic from $\Theta(\sqrt{N})$ to $\Theta(1)$, we show that the traffic is only reduced to $\Theta(\log(N))$). It is worth noting that the transport capacity result can be obtained from the transmission protocol proposed by Gastpar and Vetterli for large relay networks[1] [5]. In the sequel, we will elaborate more on the link between our work and [5].

We then use this result to characterize the set of *observable*[2] random processes by this class of dense sensor networks. For random fields that can be modeled as discrete random sequences, we derive necessary and sufficient conditions for observability. We further establish a certain form of source/channel coding separation in this scenario. The significance of this separation theorem is that it allows for constructing low-complexity coding and decoding algorithms. Next, we investigate the more realistic, and challenging, scenario of continuous random processes. In this case, we show that all Gaussian and spatially bandlimited processes can be estimated at the collector node, subject to any nonzero constraint on the mean-square error, using a simple strategy composed of single-dimensional quantization, Slepian–Wolf distributed source coding, and the proposed antenna sharing approach. Toward the end of the note, we shed some light on the limitation of the multiple-access formulation used earlier to investigate the capacity of the many-to-one channel [6].

## II. System Model and Assumptions

For simplicity of presentation, unless otherwise stated, we consider the scenario where the $N$ sensor nodes are distributed uniformly over the surface of a sphere with a unit radius. The collector node is assumed to be at the center of the sphere, and hence, all the source nodes are

Manuscript received April 11, 2003; revised September 27, 2004. This work was supported by the National Science Foundation under Grant ITR 0219892. The material in this correspondence was presented in part at the IEEE 2003 Vehicular Technology Conference, Orlando, FL, September 2003.

The author is with the Electrical and Computer Engineering Department, The Ohio State University, Columbus, OH 43210-1272 USA (e-mail: helgamal@ece.osu.edu).

Communicated by L. Tassiulas, Associate Editor for Communications Networks.

Digital Object Identifier 10.1109/TIT.2004.842563

[1]The link between our work and [5] was pointed out by one of the reviewers.

[2]This notion of observability will be rigorously defined in the sequel.