Jamming to Foil an Eavesdropper

Navin Kashyap
Dept of ECE
Indian Institute of Science Bangalore
nkashyap@ece.iisc.ernet.in

Yogesh Sankarasubramaniam
HP Labs India
Bangalore, India
yogesh@hp.com

Andrew Thangaraj
Dept of EE
Indian Institute of Technology Madras
andrew@ee.iitm.ac.in

***Abstract*—We consider key-less secure communication against a passive adversary, by allowing the legitimate receiver to selectively jam transmitted bits. The channel between the transmitter and legitimate receiver is assumed to be half-duplex (i.e., one cannot jam and receive simultaneously), while the only degradation seen by the eavesdropper is due to jamming done by the legitimate receiver. However, jamming must be done without knowledge of the transmitted sequence, and the transmitted sequence must be recovered *exactly* by the receiver from the unjammed bits alone. We study the resulting coding problem in this setup, both under complete equivocation (CE) and partial equivocation (PE) of the eavesdropper. For (CE), we give explicit code-constructions that achieve the maximum transmission rate, while for (PE) we compute upper and lower bounds on the maximum possible transmission rate.**

I. Introduction

Suppose A wants to transmit a codeword $\mathbf{x}$, chosen randomly from a (public) codebook $\mathcal{C}$, to B across a noiseless channel with E acting as an eavesdropper. Then, A and B are said to communicate in *perfect secrecy*, if E cannot obtain any information about which $\mathbf{x} \in \mathcal{C}$ was transmitted, but B can reconstruct $\mathbf{x}$ without error. Shannon [1] showed that if E has complete access to the transmitted codeword, then it is necessary for A and B to use at least one shared secret-key-bit per message-bit to achieve perfect secrecy. However, the use of shared secrets that are statistically independent of and commensurate with every message, is considered impractical.

In this paper, we are interested in key-less security, i.e., A and B need not share secret keys apriori. The transmission from A to B is now secured by having B take on the role of an active jammer, in addition to being a passive receiver. Specifically, B is allowed to selectively jam the transmitted codeword, so that E gets the least possible information. We propose a systematic study of the resulting coding problem, both for complete equivocation (CE) and partial equivocation (PE) of the eavesdropper. For (CE), we give explicit code-constructions that achieve the maximum transmission rate, while for (PE) we compute upper and lower bounds on the maximum possible transmission rate. Before formalizing our set-up, we briefly review related literature and point out connections to this work.

There have been several efforts to modify the original setup considered by Shannon. It is well-known that A and B need not share any secrets to communicate under slightly relaxed security requirements. For example, public-key cryptosystems (e.g. RSA) retain Shannon's assumption that E has complete access to the transmitted codeword (ciphertext), but relax the requirement of statistical independence between messages and transmitted codewords. This means that short keys are now permissible, and the goal is to design a cryptosystem that is computationally secure, i.e., it cannot be broken within a bounded computation model. Another example is that of physical-layer security under appropriate channel/source models (see for e.g. [2], [3], [4], [5] and the upcoming book [6]), where it is assumed that E only receives a degraded version of $\mathbf{x}$, and that B can tolerate vanishing decoding errors[1]. The resulting security, termed information-theoretic security (also called weak/strong security), is weaker than Shannon's perfect secrecy requirement[2], but stronger than computational security because E is now allowed unbounded computational power.

There are also several other modifications and generalizations of the above two models, which offer varying degrees of security without the use of any shared secret keys. However, our immediate interest is in key-less security by allowing B to actively foil E. Interestingly, there is a history of such non-secret encryption [7], which dates back to even before Shannon. The ingenious idea was to allow the receiver also to participate in the encryption process by first adding noise to the telephone line, and then subtracting the same to recover the transmitted signal. This idea was rediscovered recently in the context of secure communication in sensor networks [8], where the receiving node could selectively jam signals from the transmitting node under a half-duplex model. However, we feel that the resulting coding problem requires a systematic study, which we aim to provide in this paper. It is also worth noting that active jamming under the half-duplex model has been well-studied in the context of information-theoretic security [9], [10]. In contrast, security definitions in this paper are combinatorial, requiring error-free decoding at B.

II. The Set-up

Suppose A wants to transmit an n-bit codeword $\mathbf{x} = (x_1, \ldots, x_n) \in \{0,1\}^n$ to B across a noiseless channel, with E acting as an eavesdropper. To foil the eavesdropper, B is able to selectively degrade ("jam") some bits of the transmission, so that E sees a degraded version of the transmitted sequence. We stress here that the only degradation in the channel that E

[1] This is weaker than error-free decoding in Shannon's model.

[2] Information-theoretic security offers *asymptotic* statistical independence between messages and E's observations, as opposed to statistical independence between messages and transmitted codewords required in Shannon's model.

sees is due to the jamming done by B. The jamming is done according to some "jamming sequence" chosen randomly from some collection, $\mathcal{J}$, of jamming sequences. Here, a jamming sequence (henceforth, j-sequence) is just a list of coordinates of $\mathbf{x}$ that are to be jammed. The effect of jamming a particular coordinate is to flip the bit in that coordinate.[3]

It is assumed that (a) B performs the jamming without knowledge of the transmitted codeword $\mathbf{x}$; and (b) B cannot jam and receive simultaneously, meaning that B only receives the unjammed bits. This is termed the "half-duplex model".

E receives a binary sequence $\mathbf{y}$ that differs from the transmitted sequence $\mathbf{x}$ in some of the jammed positions. The assumption, of course, is that the eavesdropper E does not know which positions are jammed (i.e., she is unable to distinguish a jammed bit from a clean one). On the other hand, B knows that the (unjammed) bits he receives are clean, and can use them to reconstruct the transmitted codeword $\mathbf{x}$.

The goal is to design a codebook $\mathcal{C}$ and a collection of j-sequences $\mathcal{J}$ that allows B to uniquely reconstruct the transmitted codeword $\mathbf{x}$ from the unjammed bits in the sequence $\mathbf{y}$, but E gets the least possible information about $\mathbf{x}$ from $\mathbf{y}$. It is assumed that the codebook $\mathcal{C}$ and the j-sequence collection $\mathcal{J}$ are known to all parties — A, B and E. So, B acts as an adversary for E, and the goal of the code design problem is to help the adversary, as opposed to the usual setting in which the adversary is to be defeated. We present a couple of examples to make things more concrete.

Example 2.1: Let $\mathcal{C}$ be the repeat-twice code for even n: $\mathcal{C} = \{(c_1, c_1, c_2, c_2, \ldots, c_{n/2}, c_{n/2}) : c_i \in \{0,1\}\}$. In other words, $\mathcal{C}$ is the (Cartesian) product of $n/2$ copies of the repetition code $\{00, 11\}$. Each j-sequence in $\mathcal{J}$ jams exactly one of the coordinates $\{1,2\}$, exactly one of $\{3,4\}$, ..., exactly one of $\{n-1, n\}$, so that the number of j-sequences in $\mathcal{J}$ is $2^{n/2}$. Then, B can always reconstruct the transmitted codeword $\mathbf{x}$, but E gets no information whatsoever about $\mathbf{x}$.

Example 2.2: Let $\mathcal{C}$ be the even-weight code of length n: $\mathcal{C} = \{(c_1, \ldots, c_n) \in \{0,1\}^n : c_1 \oplus \cdots \oplus c_n = 0\}$, where $\oplus$ denotes modulo-2 addition. A j-sequence jams exactly one position i in $\{1, 2, \ldots, n\}$, so that there are n j-sequences in $\mathcal{J}$. Again, B is able to uniquely reconstruct the transmitted codeword, but E can only narrow it down to n possibilities.

We now introduce some terminology and notation to be used in the rest of the paper. We identify a j-sequence $J \subseteq [n]$ with its "incidence vector" $(j_1, \ldots, j_n) \in \{0,1\}^n$, where $j_i = 1$ iff $i \in J$. Thus, if $\mathbf{x} = (x_1, \ldots, x_n)$ is a transmitted codeword, and $\mathbf{j} = (j_1, \ldots, j_n)$ a j-sequence applied to it, then B receives the word $\hat{\mathbf{x}} = (\hat{x}_1, \ldots, \hat{x}_n)$, where

$$\hat{x}_i = \begin{cases} x_i & \text{if } j_i = 0 \\ \varepsilon & \text{if } j_i = 1 \end{cases} \tag{1}$$

ε denoting an erasure symbol. Correspondingly, E receives the word $\mathbf{x} \oplus \mathbf{j} = (x_1 \oplus j_1, \ldots, x_n \oplus j_n)$. Henceforth, we shall denote by $\mathcal{Y}$ the set of all words received by E:

$$\mathcal{Y} = \{\mathbf{x} \oplus \mathbf{j} : \mathbf{x} \in \mathcal{C}, \mathbf{j} \in \mathcal{J}\}.$$

Translating the codebook $\mathcal{C}$ if necessary, we will assume, without loss of generality, that the all-zero word $\mathbf{0}$ is in $\mathcal{C}$. Consequently, $\mathcal{J} \subseteq \mathcal{Y}$.

The *support* of a binary sequence $\mathbf{z} = (z_1, \ldots, z_n)$ is defined to be $\text{supp}(\mathbf{z}) = \{i : z_i = 1\}$. For a collection of binary sequences $\mathcal{Z} \subseteq \{0,1\}^n$, we define $\text{supp}(\mathcal{Z}) = \{\text{supp}(\mathbf{z}) : \mathbf{z} \in \mathcal{Z}\}$.

For $J \subseteq [n]$, we set $\mathcal{C}|_J = \{\mathbf{x}|_J : \mathbf{x} \in \mathcal{C}\}$, where $\mathbf{x}|_J = (x_j : j \in J)$ is the sequence $\mathbf{x}$ restricted to the coordinates in J. We then write $\mathcal{C} \setminus J$ to denote $\mathcal{C}|_{J^c}$, which is the codebook obtained by puncturing $\mathcal{C}$ at the coordinates in J. If A is a matrix with n columns, then for $J \subseteq [n]$, we set $A|_J$ to be the submatrix of A obtained by deleting the columns not indexed by J. Thus, if G is a generator matrix for a linear code $\mathcal{C}$, then $G|_J$ is a generator matrix for $\mathcal{C}|_J$.

A subset $J \subset [n]$ is defined to be a *correctable erasure pattern* for a length-n code $\mathcal{C}$ if the canonical projection from $\mathcal{C}$ to $\mathcal{C} \setminus J$ defined by $\mathbf{x} \mapsto \mathbf{x}|_{J^c}$ is a bijection.

III. Complete Equivocation

We consider here the situation of Example 2.1, where the codebook $\mathcal{C}$ and collection of j-sequences $\mathcal{J}$ have been chosen so that B can always uniquely reconstruct the transmitted codeword $\mathbf{x}$, but E gets no information about $\mathbf{x}$ beyond the fact that $\mathbf{x}$ is in $\mathcal{C}$. Formally, the pair $(\mathcal{C}, \mathcal{J})$, with $|\mathcal{C}| \geq 2$, has the *complete equivocation property*

(CE) given any $\mathbf{y} \in \mathcal{Y}$, for each $\mathbf{x} \in \mathcal{C}$, there exists a $\mathbf{j} \in \mathcal{J}$ such that $\mathbf{x} \oplus \mathbf{j} = \mathbf{y}$,

and the *exact recovery property*

(ER) each $J \in \text{supp}(\mathcal{J})$ is a correctable erasure pattern.

We require $|\mathcal{C}| \geq 2$, as the case of $\mathcal{C}$ consisting of a single codeword is trivial and of no use. The (CE) property ensures that the eavesdropper, E — who receives $\mathbf{y}$ but does not have knowledge of the j-sequence used by B — is unable to eliminate any codeword in $\mathcal{C}$ as potentially being the transmitted sequence $\mathbf{x}$. The (ER) property allows B — who receives $\hat{\mathbf{x}}$ as given by (1) and knows the set, J, of jammed coordinates — to recover the transmitted word $\mathbf{x}$ from the unerased positions in $\hat{\mathbf{x}}$. In this section, we attempt to determine when it is possible for both properties (CE) and (ER) to hold.

Recall that $\mathbf{0} \in \mathcal{C}$, so that $\mathcal{J} \subseteq \mathcal{Y}$. In fact, if (CE) holds, then $\mathcal{J} = \mathcal{Y}$: for any $\mathbf{y} \in \mathcal{Y}$, there exists, by (CE), a $j \in \mathcal{J}$ such that $\mathbf{0} \oplus \mathbf{j} = \mathbf{y}$. A straightforward consequence of this is that $\mathbf{x} \oplus \mathcal{J} = \mathcal{J}$ for all $\mathbf{x} \in \mathcal{C}$.

Note that if we define $\overline{\mathcal{C}}$ to be the binary linear code generated by the codewords in $\mathcal{C}$ (i.e., the vector space over the binary field spanned by the vectors in $\mathcal{C}$), then it is easy to verify that we also have $\mathbf{x} \oplus \mathcal{J} = \mathcal{J}$ for all $\mathbf{x} \in \overline{\mathcal{C}}$. This is possible iff $\mathcal{J}$ is a union of cosets of $\overline{\mathcal{C}}$. In summary, (CE) holds only if $\mathcal{J}$ is a union of cosets of $\overline{\mathcal{C}}$. The converse is also readily verified to be true. We thus have the following proposition.

[3]It is also possible to assume that the bit in a jammed coordinate only gets flipped with some probability $p \in [0,1]$. We consider only $p = 1$ here.

Proposition 1: A codebook $\mathcal{C}$ and a collection of j-sequences $\mathcal{J}$ have the property (CE) iff $\mathcal{J}$ is a union of cosets of the binary linear code $\overline{\mathcal{C}}$ generated by the codewords in $\mathcal{C}$.

With this proposition in hand, it remains to determine when it is possible for a coset $\mathcal{J}$ of $\overline{\mathcal{C}}$ to have the exact recovery property (ER). This seems difficult to answer in general, but good progress can be made if we additionally require that $\mathcal{C}$ be a linear code. Note that if $\mathcal{C}$ is a linear code, then $\overline{\mathcal{C}} = \mathcal{C}$, and so we have the following corollary to Proposition 1.

Corollary 2: A binary linear code $\mathcal{C}$ and a set of j-sequences $\mathcal{J}$ have the property (CE) iff $\mathcal{J}$ is a union of cosets of $\mathcal{C}$.

So, when does a binary linear code $\mathcal{C}$ (of dimension at least 1, so that $|\mathcal{C}| \geq 2$) have a coset $\mathcal{J}$ for which (ER) holds? To study this question, we will use the following simple lemma which characterizes correctable erasure patterns in terms of a parity-check matrix for $\mathcal{C}$. This result can be recovered from Lemma 1 in [11], for example.

Lemma 3: Let H be a parity-check matrix for a linear code $\mathcal{C}$. $J \subseteq [n]$ is a correctable erasure pattern for $\mathcal{C}$ iff the columns of $H|_J$ are linearly independent.

Hence, for a linear code $\mathcal{C}$, (ER) is equivalent to

(ER′): for each $J \in \text{supp}(\mathcal{J})$, the columns of $H|_J$ are linearly independent.

In fact, (ER) can be strengthened further as follows.

Lemma 4: If $\mathcal{J}$ is a coset of $\mathcal{C}$, (ER) is equivalent to

(ER*): for each $J \in \text{supp}(\mathcal{J})$, both J and J^c are correctable erasure patterns for $\mathcal{C}$.

Proof: Let $\mathcal{J}$ be a coset of $\mathcal{C}$. The lemma is proved once we show that if (ER′) holds, then it is also true that for each $J \in \text{supp}(\mathcal{J})$, the columns of $H|_{J^c}$ are linearly independent.

We prove the contrapositive. Let $\mathbf{j} \in \mathcal{J}$, with $J = \text{supp}(\mathbf{j})$, be such that the columns of H_{J^c} are linearly dependent. Then, there is a non-zero codeword $\mathbf{c} \in \mathcal{C}$ such that $\text{supp}(\mathbf{c}) \subseteq J^c$. Set $\widehat{J} = \text{supp}(\mathbf{c} \oplus \mathbf{j})$, and note that $\text{supp}(\mathbf{c}) \subseteq \text{supp}(\mathbf{c} \oplus \mathbf{j})$. Hence, the columns of $H|_{\widehat{J}}$ are linearly dependent. Moreover, since $\mathcal{J}$ is a coset of $\mathcal{C}$, we have $\mathbf{c} \oplus \mathbf{j} \in \mathcal{J}$, and consequently, $\widehat{J} \in \text{supp}(\mathcal{J})$. Thus, (ER′) does not hold. ∎

Theorem 5: Let $\mathcal{C}$ be a binary linear code of length n. If for some set of j-sequences $\mathcal{J}$, the pair $(\mathcal{C}, \mathcal{J})$ satisfies both (CE) and (ER), $\dim(\mathcal{C}) \leq \lfloor n/2 \rfloor$.

Proof: By Corollary 2, $\mathcal{J}$ must be a union of cosets of $\mathcal{C}$. In fact, we may take $\mathcal{J}$ to be a single coset — any one of the cosets in the union will do. For any $J \in \text{supp}(\mathcal{J})$, $\text{rank}(H) \geq \max\{\text{rank}(H|_J), \text{rank}(H|_{J^c})\} = \max\{|J|, n-|J|\} \geq n/2$, with the equality in the middle being a consequence of (ER*). Hence, $\dim(\mathcal{C}) \leq n/2$. ∎

The above theorem shows that the maximum rate of a length-n binary linear code $\mathcal{C}$ such that $(\mathcal{C}, \mathcal{J})$ satisfies (CE) and (ER), is $\lfloor n/2 \rfloor / n$. One might ask if higher rates are possible upon relaxing the linearity requirement. The following theorem, proved in the appendix, answers in the negative. In fact, it turns out that any binary code achieving the maximum rate under (CE) and (ER) must be linear.

Theorem 6: Let $\mathcal{C}$ be a binary code of length n. If for some set of j-sequences $\mathcal{J}$, the pair $(\mathcal{C}, \mathcal{J})$ satisfies both (CE) and (ER), $|\mathcal{C}| \leq 2^{\lfloor n/2 \rfloor}$. Thus, the code rate is at most $\frac{\lfloor n/2 \rfloor}{n}$.

The above result was claimed in [8, Theorem 3.2], but the proof given by them appears to be incomplete in our reading. The bound of Theorem 5 is achieved with equality by certain linear codes. When n is even, the code of Example 2.1 has dimension $n/2$. For odd $n \geq 3$, we may take $\mathcal{C}$ to be the product of $\{000, 111\}$ and $(n-3)/2$ copies of $\{00, 11\}$.

At this point, we do not have a complete answer for which binary linear codes $\mathcal{C}$ have a coset $\mathcal{J}$ for which (ER) holds. It is easy to check that any repetition code $\{0^r, 1^r\}$, with $r \geq 2$, has this property. Consequently, products of such repetition codes also have this property. We conjecture that, up to equivalence, coordinate extensions of such codes (i.e., codes obtained by appending extra coordinates) are the only codes with the desired property.

IV. Partial Equivocation

Theorem 5 shows that if we require complete equivocation and exact recovery, then the maximum rate achievable by a linear code is $1/2$. We here attempt to examine the rate versus equivocation-rate tradeoff when we relax (CE) to (α-E) as below, for $\alpha \in [0, 1]$:

(α-E) For each $y \in \mathcal{Y}$, we have $|\{\mathbf{x} \in \mathcal{C} : \exists \mathbf{j} \in \mathcal{J} \text{ such that } \mathbf{x} \oplus \mathbf{j} = \mathbf{y}\}| \geq |\mathcal{C}|^\alpha$.

Clearly, for $\alpha = 1$, the above is simply (CE).

Define a code $\mathcal{C}$ to be *equivocation-α achieving* if there exists a collection of j-sequences $\mathcal{J}$ such that $(\mathcal{C}, \mathcal{J})$ satisfies (α-E) and (ER). We wish to determine the maximum rate achievable, or to be precise, the supremum of the rates achievable by equivocation-α achieving codes. We shall, in this paper, consider linear codes only, as the additional structure helps with the analysis. As before, (ER) is equivalent to (ER′).

Also as before, $\mathcal{Y}$ must be a union of cosets of $\mathcal{C}$, since $\mathcal{Y} = \bigcup_{\mathbf{j} \in \mathcal{J}} (\mathbf{j} \oplus \mathcal{C})$. Define, for $\mathbf{y} \in \mathcal{Y}$,

$$\deg(\mathbf{y}) = |\{\mathbf{x} \in \mathcal{C} : \exists \mathbf{j} \in J \text{ such that } \mathbf{x} \oplus \mathbf{j} = \mathbf{y}\}|,$$

so that (α-E) requires that $\deg(\mathbf{y}) \geq |\mathcal{C}|^\alpha$ for all $\mathbf{y} \in \mathcal{Y}$. We note here that $\deg(\mathbf{y})$ equals the number of $\mathbf{j} \in \mathcal{J}$ that belong to the same coset of $\mathcal{C}$ as $\mathbf{y}$.

As the requirement that $\deg(\mathbf{y}) \geq |\mathcal{C}|^\alpha$ applies in particular to each $\mathbf{y}$ from any individual coset $\mathbf{j} \oplus \mathcal{C}$, $\mathbf{j} \in \mathcal{J}$, it suffices to analyze the scenario when $\mathcal{Y}$ is a single coset of $\mathcal{C}$. In this case, $\deg(\mathbf{y}) = |\mathcal{J}|$ for all $\mathbf{y} \in \mathcal{Y}$. Thus, an equivocation-$\alpha$ achieving linear code $\mathcal{C}$ is one that has a coset containing at least $|\mathcal{C}|^\alpha$ sequences whose supports are correctable erasure patterns. Our aim is to determine the supremum of the rates achieved by such codes. Let $R(\alpha)$ denote this supremum. $R(\alpha)$ is a non-increasing function of α, with $R(0) = 1$ and $R(1) = 1/2$. Thus, we have $R(\alpha) \geq 1/2$ for all $\alpha \in [0, 1]$. Let $h(x) = -x \log_2(x) - (1-x) \log_2(1-x)$, $x \in [0, 1]$.

Proposition 7: For $\alpha \in [0, 1]$, let $\rho(\alpha)$ denote the unique positive real solution to $h(x) = \alpha x$. Then, $R(\alpha) \leq \rho(\alpha)$.

Proof: Let $\mathcal{C}$ be a linear code of length n and rate $R \geq 1/2$ that has a coset containing a subset $\mathcal{J}$ of size at least $|\mathcal{C}|^\alpha$ for which (ER′) holds. By (ER′), each $\mathbf{j} \in \mathcal{J}$ can have weight at most $n(1-R)$. So, $|\mathcal{J}| \leq \sum_{j=0}^{n(1-R)} \binom{n}{j} \leq 2^{nh(1-R)} =$

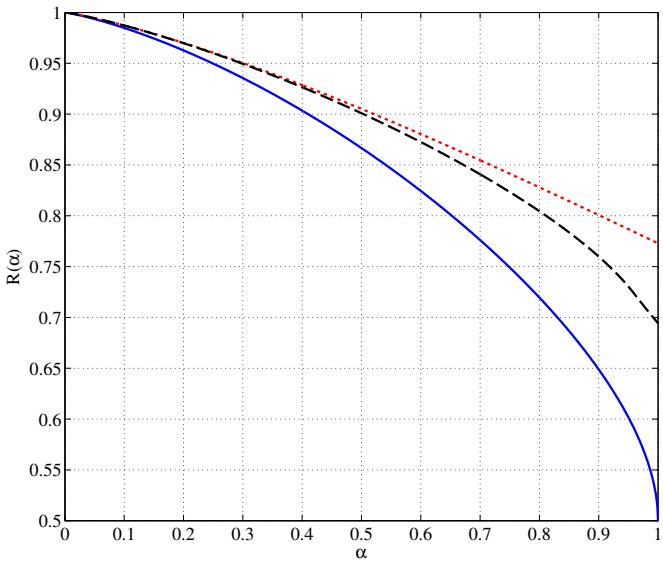

Fig. 1. Bounds on $R(\alpha)$: upper bounds $\rho(\alpha)$ of Prop. 7 (dotted line) and $\hat{\rho}(\alpha)$ of Prop. 8 (dashed line), and lower bound $\lambda(\alpha)$ of Prop. 9 (solid line).

$2^{nh(R)}$. Hence, $2^{nh(R)} \geq |\mathcal{C}|^{\alpha} = 2^{n\alpha R}$, from which we obtain $h(R) \geq \alpha R$, and the proposition follows. ∎

We remark that the proof above does not use the fact that $\mathcal{J}$ lies within a coset of $\mathcal{C}$. So, it should be possible to improve the bound. One possible idea for this is to use the fact that for distinct $\mathbf{j}, \mathbf{j}' \in \mathcal{J}$, $\mathrm{supp}(\mathbf{j}) \not\subseteq \mathrm{supp}(\mathbf{j}')$; otherwise, we would have a codeword, $\mathbf{j} \oplus \mathbf{j}'$, supported within $\mathrm{supp}(\mathbf{j}')$, contradicting (ER′). This allows us to use the LYM inequality (see e.g., [13, p. 3]) to get: $\sum_{w=1}^{\lfloor n(1-R) \rfloor} \frac{b_w}{\binom{n}{w}} \leq 1$, where b_w is the number of words of weight w in $\mathcal{J}$. From this, we obtain, for instance (cf. Sperner's theorem), $|\mathcal{J}| \leq \binom{n}{\lfloor n(1-R) \rfloor}$, which does not improve upon Proposition 7.

However, the bound can be improved by using the condition that for any $\mathbf{j}, \mathbf{j}', \mathbf{j}'' \in \mathcal{J}$, $\mathrm{supp}(\mathbf{j}' \oplus \mathbf{j}'') \not\subseteq \mathrm{supp}(\mathbf{j})$, which is again a consequence of (ER′). To state the improved bound, we define a function $g : [2/3, 1] \to [0, 1]$ as follows: let ϕ be the golden ratio $\frac{1+\sqrt{5}}{2}$; then,

$$g(x) = \begin{cases} \log_2 \phi & \text{if } \frac{2}{3} \leq x \leq \frac{\phi}{\sqrt{5}}, \\ x\, h\left(\frac{1-x}{x}\right) & \text{if } \frac{\phi}{\sqrt{5}} \leq x \leq 1. \end{cases} \tag{2}$$

Some straightforward calculus shows that $g(x)$ is continuous and non-increasing. Also, we have for any $x \in [1/2, 1]$,

$$x\, h(\tfrac{1-x}{x}) = (1-x)\, h(0) + x\, h(\tfrac{1-x}{x}) \leq h(1-x) = h(x),$$

with the inequality above resulting from the concavity of the binary entropy function. It follows that $g(x) \leq h(x)$ for all $x \in [2/3, 1]$. Consequently, the following bound is an improvement over the bound of Proposition 7.

Proposition 8: For $\alpha \in [0, 1]$, let $\hat{\rho}(\alpha)$ denote the unique positive real solution to $g(x) = \alpha x$. Then, $R(\alpha) \leq \hat{\rho}(\alpha)$.

Proof: Fix an $\alpha \in [0, 1]$, and let $\mathcal{C}$ be a linear code of length n and rate $R \geq 2/3$ with a coset containing a subset $\mathcal{J}$ of size at least $2^{n\alpha R}$ for which (ER′) holds. By (ER′), $\mathbf{j} \in \mathcal{J}$ has weight $\leq n(1-R)$, and the maximum weight $t = \max_{\mathbf{j} \in \mathcal{J}} |\mathrm{supp}(\mathbf{j})|$ is such that $t/n = \tau \in [0, 1-R]$.

For a weight-t $\mathbf{j} \in \mathcal{J}$ with $J = \mathrm{supp}(\mathbf{j})$, we claim that the canonical projection from $\mathcal{J}$ to $\mathcal{J} \setminus J$ defined by $\mathbf{j} \mapsto \mathbf{j}|_{J^c}$ is a bijection. Suppose that there exist $\mathbf{j}', \mathbf{j}'' \in \mathcal{J}$ such that $\mathbf{j}'|_{J^c} = \mathbf{j}''|_{J^c}$. Then, $\mathrm{supp}(\mathbf{j}' \oplus \mathbf{j}'') \subseteq J$, which contradicts (ER′). So, $|\mathcal{J}|$ is bounded by the number of binary sequences of weight at most t supported within J^c, i.e.,

$$|\mathcal{J}| \leq \sum_{w=0}^{t} \binom{n-t}{w}. \tag{3}$$

Since $R \geq 2/3$, we have $t/n \leq 1/3$, or $t \leq (n-t)/2$. So, the largest term in the summation in (3) is $\binom{n-t}{t}$. Thus, asymptotically in n, the summation behaves as $2^{n\tau\, h((1-\tau)/\tau)}$. Therefore, combining the bound in (3) with $|\mathcal{J}| \geq 2^{n\alpha R}$, we obtain $\alpha R \leq \tau\, h((1-\tau)/\tau)$. Maximizing the right-hand side of this last inequality over $\tau \in [0, 1-R]$, we get $\alpha R \leq g(R)$, where g is as in (2). Now, $g(R)$ is a continuous, non-increasing function of R, and αR is a continuous, increasing function of R. So, $\hat{\rho}(\alpha)$ defined in the statement of the proposition is precisely the largest R for which $\alpha R \leq g(R)$ holds. ∎

The following proposition gives a lower bound on $R(\alpha)$.

Proposition 9: For $\alpha \in (0, 1)$, let $\lambda(\alpha)$ be the unique solution in the interval $(1/2, 1)$ to the equation $1 - h(x) = (1-\alpha)x$. Then, $R(\alpha) \geq \lambda(\alpha)$.

Proof: For the purpose of this proof, an (R, α) code is a binary linear code of rate at least R that satisfies (α-E).

The idea of the proof is to show the existence of a code $\mathcal{C}$ of length n and rate $R > 1/2$, having $2^{nh(R)}$ correctable erasure patterns. Then, some coset of $\mathcal{C}$ must contain at least $2^{nh(R)}/2^{n(1-R)} = 2^{nR[1-\frac{1-h(R)}{R}]}$ correctable erasure patterns, and $\mathcal{C}$ is a $(R, 1 - \frac{1-h(R)}{R})$ code. So, for $\alpha \in (0, 1)$ and $R > \lambda(\alpha)$, there exists an $(\lambda(\alpha), \alpha)$ code.

We will show something slightly weaker in the formal proof: for any $R > 1/2$ and $\epsilon > 0$, there exists an $(R - \epsilon, 1 - \frac{1-h(R)}{R})$ code. In particular, for $R = \lambda(\alpha)$, there exists an $(\lambda(\alpha) - \epsilon, \alpha)$ code for any $\epsilon > 0$, and the proposition follows.

Consider a random binary $m \times n$ matrix H, with $m \leq n$, in which each entry is 0 or 1 with equal probability, independent of other entries. Any fixed $m \times m$ submatrix of H has rank m with probability at least $1/4$ for all sufficiently large m (see e.g. [14]). Therefore, for $n \geq m$ sufficiently large, the expected number of $m \times m$ non-singular submatrices of a random binary $m \times n$ matrix is at least $(1/4)\binom{n}{m}$. So, for large enough m, n, there exists an $m \times n$ binary matrix with at least $(1/4)\binom{n}{m}$ square submatrices of rank m.

Let $R \in (1/2, 1)$ and $\epsilon > 0$ be such that $R - \epsilon > 1/2$ (else $(R-\epsilon, 1)$ codes exist). For $m = \lfloor n(1-R+\epsilon) \rfloor$ and sufficiently large n, let H be a binary $m \times n$ matrix with at least $(1/4)\binom{n}{m}$ square submatrices of rank m. The code $\mathcal{C} = \ker(H)$ has rate at least $R - \epsilon$. By Lemma 3, there are at least $(1/4)\binom{n}{m}$ correctable erasure patterns for $\mathcal{C}$, so some coset of $\mathcal{C}$ contains at least

$$\frac{(1/4)\binom{n}{m}}{2^m} \geq \frac{1}{4(n+1)} 2^{n[h(m/n) - m/n]} = |\mathcal{C}|^{\alpha'},$$

correctable erasure patterns, where $\alpha' = 1 - \frac{1-h(R-\epsilon)}{R-\epsilon} - \delta_n$, and $\delta_n \to 0$ as $n \to \infty$. The function $1 - \frac{1-h(x)}{x}$ is decreasing in the interval $(1/2, 1)$. So, for sufficiently large n, we have $\alpha' \geq 1 - \frac{1-h(R)}{R}$, and $\mathcal{C}$ is an $(R-\epsilon, 1-\frac{1-h(R)}{R})$ code. ∎

The bounds from Propositions 7–9 are plotted in Figure 1.

ACKNOWLEDGMENT

We would like to thank Matthieu Bloch for helpful discussions, and Amitabh Saxena for pointing out reference [7]. N. Kashyap wishes to thank Anish Arora for initial discussions leading to this work.

REFERENCES

[1] C.E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal,* vol. 28, pp. 656–715, Oct. 1949.

[2] A.D. Wyner, "The wire-tap channel," *Bell System Technical Journal,* vol. 54, no. 8, pp. 1355–1367, Oct. 1975.

[3] I. Csiszár and J. Körner, "Broadcast Channels with Confidential Messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339-348, May 1978.

[4] U. Maurer, "Secret key agreement by public discussion from common information,", *IEEE Trans. Inf. Theory,* vol. 39, no. 3, pp. 733–742, May 1993.

[5] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. I. secret sharing," *IEEE Trans. Inf. Theory,* vol. 39, no. 4, pp. 1121–1132, July 1993.

[6] M. Bloch and J. Barros, *Physical Layer Security: From Information Theory to Security Engineering*, Cambridge University Press, 2011.

[7] J. H. Ellis, "The history of Non-Secret Encryption," available online http://cryptocellar.web.cern.ch/cryptocellar/cesg/ellis.pdf

[8] A. Arora and L. Sang, "Dialog Codes for Perfect Wireless Communications," in *Proc. 8th ACM/IEEE Int. Conf. Information Processing in Sensor Networks (IPSN'09)*, April 15–18, 2009, San Francisco, USA.

[9] L. Lai, H. El Gamal and H.V. Poor, "The wiretap channel with feedback: Encryption over the channel," *IEEE Trans. Inf. Theory,* vol. 54, no. 11, pp. 5059-5067, Nov. 2008.

[10] M. Bloch, "Channel scrambling for secrecy," in *Proc. IEEE Int. Symp. Inform. Theory (ISIT'09)*, June 28–Jul 3, 2009, pp.2452-2456, Seoul, South Korea.

[11] I. Dumer and P.G. Farrell, "Erasure correction performance of linear block codes," in *Lecture Notes in Computer Science vol. 781*, G. Cohen, S. Litsyn, A. Lobstein, and G. Zemor (Eds.), pp. 316–326, Springer-Verlag, 1993.

[12] James Oxley, *Matroid Theory*, Oxford University Press, 1992.

[13] I. Anderson, *Combinatorics of Finite Sets*, Dover Publications, 2002.

[14] E. R. Berlekamp, "The technology of error-correcting codes," *Proc. IEEE*, vol. 68, pp. 564–593, 1980.

APPENDIX

Let us first prove the following:

Lemma 10: If $\mathcal{J}$ contains a j-sequence of length t, and $(\mathcal{C}, \mathcal{J})$ satisfies both (CE) and (ER), $|\mathcal{C}| \leq 2^{\min\{t, n-t\}}$.

Proof: We start by considering $t \geq n/2$. (ER) requires that B should be able to reconstruct $\mathbf{x}$ in spite of the t erasures. Thus, no two codewords in $\mathcal{C}$ can be identical in the unjammed positions. This straightaway yields $|\mathcal{C}| \leq 2^{n-t}$.

Next, consider $t < n/2$. Without loss of generality, we assume that $\mathbf{j} = 1^t \parallel 0^{n-t}$. Let $\mathbf{x}_k$ and $\mathbf{x}_l$ be any two codewords in $\mathcal{C}$. Then, (ER) stipulates that

$$\begin{aligned} \mathbf{x}_k &= \mathbf{x}_{\varepsilon,k} \parallel \tilde{\mathbf{x}}_k, \\ \mathbf{x}_l &= \mathbf{x}_{\varepsilon,l} \parallel \tilde{\mathbf{x}}_l, \end{aligned} \tag{4}$$

where $\tilde{\mathbf{x}}_k$,$\tilde{\mathbf{x}}_l \in \{0,1\}^{n-t}$ with $\tilde{\mathbf{x}}_k \neq \tilde{\mathbf{x}}_l$, and $\mathbf{x}_{\varepsilon,k}$,$\mathbf{x}_{\varepsilon,l} \in \{0,1\}^t$. Now, there exists a $\mathbf{y}_k \in \mathcal{Y}$ such that $\mathbf{y}_k = \overline{\mathbf{x}}_{\varepsilon,k} \parallel \tilde{\mathbf{x}}_k$. Under (CE), we require that there exist a j-sequence in $\mathcal{J}$ with incidence vector $\mathbf{j}_{kl}$ such that $\mathbf{j}_{kl} = \mathbf{y}_k \oplus \mathbf{x}_l$. Using (4), we can write

$$\mathbf{j}_{kl} = (\overline{\mathbf{x}}_{\varepsilon,k} \oplus \mathbf{x}_{\varepsilon,l}) \parallel (\tilde{\mathbf{x}}_k \oplus \tilde{\mathbf{x}}_l)\,. \tag{5}$$

Essentially, (5) shows that there exists a j-sequence in $\mathcal{J}$ which lists positions where $\tilde{\mathbf{x}}_k$ and $\tilde{\mathbf{x}}_l$ are different. Applying this j-sequence to $\mathbf{x}_k$ (or $\mathbf{x}_l$) would thus erase the corresponding bits, i.e., B would not see any of the bit positions where $\tilde{\mathbf{x}}_k$ and $\tilde{\mathbf{x}}_l$ are different. However, (ER) requires that B should still be able to correct this erasure pattern. This is possible only if $\mathbf{x}_{\varepsilon,k} \neq \mathbf{x}_{\varepsilon,l}$ in (4).

Repeating the above argument, we conclude that $\mathbf{x}_{\varepsilon,k} \neq \mathbf{x}_{\varepsilon,l}$ for any pair $\mathbf{x}_k$,$\mathbf{x}_l \in \mathcal{C}$. Thus, $|\mathcal{C}| \leq 2^t$. ∎

Theorem 6 now follows from Lemma 10 by setting $t = \lfloor n/2 \rfloor$ for all j-sequences. The following result shows that only linear codes can achieve the bound of Theorem 6.

Theorem 11: For any pair $(\mathcal{C}, \mathcal{J})$ satisfying (CE) and (ER), if $|\mathcal{C}| = 2^{\lfloor n/2 \rfloor}$, then $\mathcal{C}$ must be linear.

Proof: We assume for simplicity that n is even, though the arguments carry over for odd n as well. Since $\mathcal{C}$ is maximum-rate, we find from Lemma 10 that all j-sequences in $\mathcal{J}$ are of length $n/2$. Let us assume, without loss of generality, that the incidence vector of a j-sequence is $\mathbf{j} = 1^{n/2} \parallel 0^{n/2}$. Then, using the same arguments as in Lemma 10, we find that any two codewords $\mathbf{x}_k$ and $\mathbf{x}_l$ in $\mathcal{C}$ must be of the form[4]

$$\begin{aligned} \mathbf{x}_k &= \mathbf{x}_{\varepsilon,k} \parallel \tilde{\mathbf{x}}_k \\ \mathbf{x}_l &= \mathbf{x}_{\varepsilon,l} \parallel \tilde{\mathbf{x}}_l, \end{aligned} \tag{6}$$

where $\mathbf{x}_{\varepsilon,k}$, $\mathbf{x}_{\varepsilon,l}$, $\tilde{\mathbf{x}}_k$, $\tilde{\mathbf{x}}_l \in \{0,1\}^{n/2}$ with $\tilde{\mathbf{x}}_k \neq \tilde{\mathbf{x}}_l$ and $\mathbf{x}_{\varepsilon,k} \neq \mathbf{x}_{\varepsilon,l}$. To show that $\mathcal{C}$ is linear, it is enough to show that for any pair $\mathbf{x}_k, \mathbf{x}_l \in \mathcal{C}$, $\mathbf{x}_k \oplus \mathbf{x}_l$ is also in $\mathcal{C}$.

Suppose that $\mathbf{x}_k \oplus \mathbf{x}_l \notin \mathcal{C}$. Then, there exist two other codewords, say $\mathbf{x}_1$ and $\mathbf{x}_2$, in $\mathcal{C}$ such that

$$\begin{aligned} \mathbf{x}_1 &= \mathbf{x}_{\varepsilon,k} \oplus \mathbf{x}_{\varepsilon,l} \parallel \tilde{\mathbf{x}}_1 \\ \mathbf{x}_2 &= \mathbf{x}_{\varepsilon,2} \parallel \tilde{\mathbf{x}}_k \oplus \tilde{\mathbf{x}}_l, \end{aligned} \tag{7}$$

where $\tilde{\mathbf{x}}_1, \mathbf{x}_{\varepsilon,2} \in \{0,1\}^{n/2}$ with $\tilde{\mathbf{x}}_1 \neq \tilde{\mathbf{x}}_k \oplus \tilde{\mathbf{x}}_l$ and $\mathbf{x}_{\varepsilon,2} \neq \mathbf{x}_{\varepsilon,k} \oplus \mathbf{x}_{\varepsilon,l}$. This is a consequence of the fact that for maximum codebook size (i.e. for $|\mathcal{C}| = 2^{n/2}$), $\mathbf{x}_{\varepsilon,k}$ (and similarly $\tilde{\mathbf{x}}_k$) takes all the $2^{n/2}$ possibilities (cf. equation (6)). Now, proceeding as in Lemma 10, equation (5), we find that under (CE), there exists a j-sequence in $\mathcal{J}$ with incidence vector $\mathbf{j}_{kl} = (\overline{\mathbf{x}}_{\varepsilon,k} \oplus \mathbf{x}_{\varepsilon,l}) \parallel (\tilde{\mathbf{x}}_k \oplus \tilde{\mathbf{x}}_l)$. Again, invoking (CE), we find that $\mathbf{j}_{kl} \oplus \mathbf{x}_1$ must correspond to a j-sequence in $\mathcal{J}$. Using equation (7), we can write

$$\begin{aligned} \mathbf{j}_{kl} \oplus \mathbf{x}_1 &= (\overline{\mathbf{x}}_{\varepsilon,k} \oplus \mathbf{x}_{\varepsilon,l} \parallel \tilde{\mathbf{x}}_k \oplus \tilde{\mathbf{x}}_l) \oplus (\mathbf{x}_{\varepsilon,k} \oplus \mathbf{x}_{\varepsilon,l} \parallel \tilde{\mathbf{x}}_1) \\ &= 1^{n/2} \parallel \tilde{\mathbf{x}}_1 \oplus \tilde{\mathbf{x}}_k \oplus \tilde{\mathbf{x}}_l. \end{aligned} \tag{8}$$

It follows that $\mathbf{j}_{kl} \oplus \mathbf{x}_1$ has weight greater than $n/2$, since $\tilde{\mathbf{x}}_1 \oplus \tilde{\mathbf{x}}_k \oplus \tilde{\mathbf{x}}_l$ has positive weight (since $\tilde{\mathbf{x}}_1 \neq \tilde{\mathbf{x}}_k \oplus \tilde{\mathbf{x}}_l$). This contradicts the fact all j-sequences for a maximum-rate code $\mathcal{C}$ must have length $n/2$. Thus, we conclude that $\mathbf{x}_k \oplus \mathbf{x}_l \in \mathcal{C}$, and hence $\mathcal{C}$ must be linear. ∎

[4]This also follows upon noting that $0^{n/2} \parallel 1^{n/2}$ must also be a j-sequence if $\mathcal{C}$ is maximum-rate.