Maximal Correlation Secrecy

Cheuk Ting Li and Abbas El Gamal
Department of Electrical Engineering
Stanford University
Stanford, California, USA
Email: ctli@stanford.edu, abbas@ee.stanford.edu

***Abstract*—This paper shows that the maximal correlation between the message and the ciphertext provides good secrecy guarantees for ciphers with short keys. We show that a small maximal correlation ρ can be achieved via a randomly generated cipher with key length $\approx 2\log(1/\rho)$, independent of the message length, and by a stream cipher with key length $\approx 2\log(1/\rho)+\log n$ for a message of length n. We provide a converse result showing that these ciphers are close to optimal. We then show that any cipher with a small maximal correlation achieves a variant of semantic security with computationally unbounded adversary, similar to entropic security proposed by Russell and Wang. Finally, we show that a small maximal correlation implies secrecy with respect to several mutual information based criteria but is not necessarily implied by them.**

***Index Terms*—Information-theoretic secrecy, Hirschfeld-Gebelein-Rényi maximal correlation, stream cipher, expander graph.**

I. Introduction

Consider the symmetric-key cryptosystem setting in which Alice encrypts a message (plaintext) M using a shared secret key K into a ciphertext C and sends it to Bob who recovers the message using the ciphertext and the key. The system is said to provide perfect secrecy if the eavesdropper Eve cannot gain *any* information about the message from the ciphertext C alone, that is, if M and C are independent. Shannon [1] showed that achieving perfect secrecy requires the key to be as long as the message, which is impractical in most applications.

To analyze cryptosystems that employ shorter keys, less stringent secrecy criteria have been developed. One popular criterion in computer science is semantic security [2], which restricts the eavesdropper to use only probabilistic polynomial-time algorithms. Although satisfied by short keys, semantic security relies on unproven computational hardness assumptions. A secrecy criterion which is also satisfied by short keys but does not rely on computational hardness is the mutual information between the message M and the ciphertext, $I(M;C)$. As pointed out by Maurer [3], mutual information is too loose a criterion if it is not required to approach zero because it does not guarantee hiding any bit of the message, or more generally any function of the message. To encrypt an n-bit message M with an s-bit key, the optimal mutual information is $I(M;C)=n-s$. To achieve the optimum, we can just encrypt the most significant s bits of M perfectly and send the rest of the bits in the clear. Hence unless $s \geq n$, mutual information cannot guarantee that any bit of M is not leaked.

There are ciphers that can hide bits (and functions) of M better than the aforementioned strategy. Suppose we wish to encrypt a 2-bit message $M \sim \mathrm{Unif}(\{0,1,2,3\})$ using a 1-bit key $K \sim \mathrm{Bern}(1/2)$. Let $C_1 = M+2K \mod 4$ be the cipher which encrypts only the most significant bit of the message. On the other hand, if we use the cipher $C_2 = M+K \mod 4$, which also achieves $I(M;C)=1$, Eve would not be able to correctly guess either bit of the message with probability greater than $3/4$ — a better secrecy guarantee than using C_1. This shows that the inability to protect bits (and functions) of M is a limitation only of mutual information, and not information-theoretic secrecy in general.

Other information-theoretic measures of secrecy for cryptosystems with keys shorter than the message have been proposed by Massey and Ingemarsson [4] (which imposes delay and memory constraints on the eavesdropper), Maurer and Massey [5] (which imposes a restriction that the eavesdropper can only observe a small number of ciphertext bits), Maurer [6] (which requires a publicly accessible random source), Cachin and Maurer [7] (which imposes memory constraints at the eavesdropper), and Calmon *et al.* [8] (which protect bits of the message, but not functions of it).

A natural question to ask then is whether there is a measure of secrecy for cryptosystems that employ short keys which, by distinguishing between the ciphers illustrated in the aforementioned example, can provide secrecy guarantees for any bit (or function) of the message without constraints on the eavesdropper's computational capabilities or the availability of public randomness.

In this paper we answer this question in the affirmative. We show that the Hirschfeld-Gebelein-Rényi maximal correlation [9]–[11] between the message and the ciphertext, defined as

$$\rho_{\mathrm{m}}(M;C) = \max_{\substack{f(m),g(c):\,\mathsf{E}(f(M))=\mathsf{E}(g(C))=0,\\ \mathsf{E}(f^2(M))=\mathsf{E}(g^2(C))=1}} \mathsf{E}\big(f(M)g(C)\big), \tag{1}$$

satisfies all the properties of the desired measure of secrecy. We say that a cipher achieves *ρ-maximal correlation secrecy* if $\rho_{\mathrm{m}}(M;C) \leq \rho$. While the extreme case of $\rho=0$ is equivalent to perfect secrecy, $\rho<1$ provides better secrecy guarantees than mutual information. Considering the above example in which the ciphers C_1 and C_2 achieve the same

The work of C. T. Li was partially supported by a Hong Kong Alumni Stanford Graduate Fellowship.

mutual information, it can be shown that $\rho_{\mathrm{m}}(M;C_2) = \sqrt{2}/2 < \rho_{\mathrm{m}}(M;C_1) = 1$, signifying that C_2 indeed provides better secrecy than C_1.

A consequence of a small ρ is that Eve cannot guess any function of M substantially better than if she does not know C. Suppose Eve wishes to find an estimate $\tilde{f}(C)$ of the function $f(M)$. If M is uniformly distributed and f is a Boolean function, e.g., one of the bits of the message, then the relationship between maximal correlation and the probability of the correct estimation of the function, $\mathsf{P}\{f(M) = \tilde{f}(C)\}$, follows from the work of Witsenhausen [12]. Calmon *et al.* [13] showed that the advantage of Eve (the difference between $\mathsf{P}\{f(M) = \tilde{f}(C)\}$ and the correct probability if Eve does not know C) for general f is upper-bounded by ρ. In this paper, we generalize this result to scenarios in which the distribution of M is not fixed and Eve has access to some side information about the message. More importantly, we show that maximal correlation ρ can be achieved using a key length $\approx 2\log(1/\rho)$ independent of the message length. Combining these two results, we can guarantee a very small advantage for Eve using a short key. For example, for a 1GB message and a 512-bits key, an advantage can be bounded by $\approx 10^{-70}$.

A similar notion of security is entropic security introduced by Russell and Wang [14], which directly relates key length to the advantage in guessing Boolean functions. This paper shows that maximal correlation is a natural way to relate key length and advantage, and can give stronger and more general guarantees.

The rest of this paper is organized as follows. In Section III, we show that a ρ-maximal correlation secure cipher achieves a variant of semantic security with computationally unbounded adversary. In Section IV, we show the surprising result that ρ-maximal correlation secrecy can be achieved by short keys of length independent of the message length. In Section V, we discuss the relationship between ρ-maximal correlation and strong secrecy, weak secrecy, and leakage rate, which use mutual information. Many of the proofs are omitted and can be found in [15].

II. Notation and Definitions

Define the spectral norm of the matrix $A \in \mathbb{R}^{m\times n}$ as

$$\|A\| = \max_{v\in\mathbb{R}^n:\,\|v\|=1} \|Av\|\,.$$

The $\log$ function is base 2 and the entropy is in bits. We use the notation $[1:n] = \{1,2,\ldots,n\}$ and $\mathrm{Unif}(\mathcal{A})$ for the uniform probability mass function (pmf) over a finite set $\mathcal{A}$.

We consider a cryptosystem that consists of

- a message $M \in \mathcal{M}$, where $\mathcal{M} = [1:2^n]$, i.e., M is an n-bit message, unless specified otherwise,
- a random secret key $K \sim \mathrm{Unif}(\mathcal{K})$, where $\mathcal{K} = [1:2^s]$ unless specified otherwise,
- an encryption function $E(k,m)$ that maps every pair $(k,m) \in \mathcal{K}\times\mathcal{M}$ into a ciphertext $c \in \mathcal{C}$, where $\mathcal{C} = [1:2^n]$ unless specified otherwise, and
- a decryption function $D(k,c)$ that maps every pair $(k,c) \in \mathcal{K}\times\mathcal{C}$ into a message $m \in \mathcal{M}$ such that $D(k,E(k,m)) = m$ for any m,k.

The pair of encryption and decryption functions (E,D) is referred to as the cipher. Unless specified otherwise, we assume throughout that Eve knows the ciphertext C but not the message M or the key K. A cipher is said to be ρ-maximal correlation secure if $\rho_{\mathrm{m}}(M,E(K,M)) \le \rho$ assuming that $M \sim \mathrm{Unif}(\mathcal{M})$, where ρ_{m} is as defined in (1). Note that we assume $M \sim \mathrm{Unif}(\mathcal{M})$ only in the computation of ρ_{m}.

III. Constrained-distribution Security

As discussed in the introduction, it was shown in [13] that when M is uniformly distributed, ρ-maximal correlation secrecy guarantees that the advantage of Eve is upper-bounded by ρ. In this section, we generalize this result to nonuniform M and to the case in which Eve has access to some side information, showing that every ρ-maximal correlation secure cipher also satisfies a variant of semantic security.

Recall that a cipher is said to be semantically secure [16] if for any pmf $p(m)$ on M, any function $f(m)$, and any partial information function $h(m)$ of the message, if M is generated according to $p(m)$, the eavesdropper who observes the ciphertext C and $h(M)$ (and also knows the choices of n, p, f and h) cannot correctly guess $f(M)$ using a probabilistic, polynomial-time algorithm with probability non-negligibly higher than the best probabilistic, polynomial-time algorithm for guessing $f(M)$ using only $h(M)$ (and also the choices of n, p, f and h). In other words, the eavesdropper cannot improve the probability of guessing $f(M)$ correctly by observing C. Note that the definition in [16] allows $p(m)$ to be a pmf on messages with different lengths. For simplicity, we only consider $p(m)$ to be a pmf on messages with the same length n.

Constrained-distribution security is a variant of semantic security in which we remove the limitation on computational power but restrict the choice of the pmf $p(m)$ to have a small χ^2-divergence [17] from the uniform pmf, that is,

$$\chi^2\left(p \,\|\, \mathrm{Unif}[1:2^n]\right) = 2^n \sum_m \left(p(m)\right)^2 - 1 \le \delta$$

for some $\delta \ge 0$, or equivalently, the Rényi entropy $H_2(M) \ge n - \log(\delta+1)$ (note that entropic security uses min-entropy $H_\infty(M)$ instead). The case of partial information $h(m)$ at the eavesdropper will be addressed later. We say that a cipher is (δ,ϵ)-constrained-distribution secure if for any pmf $p(m)$ with $\chi^2\left(p \,\|\, \mathrm{Unif}[1:2^n]\right) \le \delta$, every function $f(m)$ of the message, and every eavesdropper's guess $\tilde{f}(c)$ of $f(m)$, when the message M is generated according to $p(m)$, the advantage of the eavesdropper is upper bounded by

$$\mathsf{P}\{f(M) = \tilde{f}(C)\} - \max_i \mathsf{P}\{f(M) = i\} \le \epsilon.$$

Note that the first term is the probability that the eavesdropper can guess $f(M)$ correctly with knowledge of C, and the second term is the probability that the eavesdropper can guess it correctly without C by setting $\tilde{f}(C) = i$.

We now show that maximal correlation secrecy implies constrained-distribution security.

Theorem 1. *A ρ-maximal correlation secure cipher is (δ, ϵ)-constrained-distribution secure for any $\delta \geq 0$ and*

$$\epsilon = \rho\sqrt{\delta + 1}.$$

Moreover, if the choice of $f(m)$ is restricted to Boolean functions $f(m) \in \{0, 1\}$, then the advantage is bounded by

$$\epsilon = \frac{1}{2}\rho\sqrt{\delta + 1}.$$

The proof of this theorem is given in [15].

Next we present a generalization of constrained-distribution security in which the partial information $h(m)$ is also available to Eve. We restrict the choices of $p(m)$ and $h(m)$ to satisfy the condition

$$\mathsf{E}\left(\sqrt{\chi^2\left(p_{M|h(M)}(\cdot \mid h(M)) \,\|\, \mathrm{Unif}[1:2^n]\right) + 1}\right) \leq \gamma,$$

where $\gamma \geq 1$ is a constant and

$$p_{M|h(M)}(m \mid a) = \frac{p(m)\mathbf{1}_{\{h(m)=a\}}(m)}{\sum_{m'} p(m')\mathbf{1}_{\{h(m')=a\}}(m')},$$

is the conditional pmf of M given $h(M)$, which is a random pmf of M that depends on the value of $h(M)$. The eavesdropper's guess $\tilde{f}(c, h(m))$ can depend on $h(M)$, and the advantage is defined as

$$\mathsf{P}\{f(M) = \tilde{f}(C, h(M))\} - \mathsf{E}\left(\max_i \mathsf{P}\{f(M) = i \mid h(M)\}\right),$$

where the second term is the probability of guessing $f(M)$ correctly using the maximum a posteriori estimation of $f(M)$ given $h(M)$. As a consequence of Theorem 1, for a ρ-maximal correlation secure cipher, the advantage is upper bounded by $\epsilon = \gamma\rho$.

The value of ρ directly corresponds to the eavesdropper advantage and the correct probability of the eavesdropper's guess. For example, if the message M is uniformly distributed, i.e., $\delta = 0$, then the eavesdropper cannot correctly guess any Boolean function such that $\mathsf{P}\{f(M) = 1\} = 1/2$ with probability larger than $(1 + \rho)/2$. As another example, if M is uniformly distributed and l bits of M are provided to the eavesdropper via the partial information $h(m)$, the advantage of the eavesdropper is upper bounded by $2^{l/2}\rho$.

IV. Maximal Correlation Secrecy Key Length

We first establish the following lower bound on the key length of a ρ-maximal correlation secure cipher. Note that this bound applies to any ciphertext length (not necessarily equal to message length) and to probabilistic encryption functions.

Theorem 2. *If a cipher is ρ-maximal correlation secure, then its key length is lower bounded as*

$$s \geq \log\left(\frac{1}{\rho^2 + 2^{-n}}\right).$$

Proof: We assume that the encryption function is randomized, i.e., the ciphertext is $C = E(K, M, W)$, where $W \sim p(w)$ is the local randomness at the sender. Assume error-free decoding, i.e., that $D(k, E(k, m, w)) = m$ for every (k, m, w). We use the following relation between the maximal correlation of jointly distributed (X, Y) and χ^2-divergence:

$$\rho_{\mathrm{m}}^2(X;Y) \geq \frac{\chi^2\left(p(x,y) \,\|\, p(x)p(y)\right)}{\min\left\{|\mathcal{X}|, |\mathcal{Y}|\right\} - 1}.$$

Applying this relation, we have

$$\begin{aligned}
\left(1 - 2^{-n}\right)\rho^2 &\geq \left(1 - 2^{-n}\right)\rho_{\mathrm{m}}^2(M;C) \\
&\geq \left(1 - 2^{-n}\right)\left(2^n - 1\right)^{-1}\chi^2\left(p(m,c) \,\|\, p(m)p(c)\right) \\
&= 2^{-n}\left(\sum_{m,c}\frac{\left(p(m,c)\right)^2}{p(m)p(c)} - 1\right) \\
&= \sum_c \frac{\sum_m \left(p(m,c)\right)^2}{p(c)} - 2^{-n} \\
&\geq \sum_c \frac{\left|\{m:\, p(m,c) > 0\}\right|^{-1}\left(\sum_m p(m,c)\right)^2}{p(c)} - 2^{-n} \\
&= \mathsf{E}\left(\left|\{m:\, p(m,C) > 0\}\right|^{-1}\right) - 2^{-n} \\
&\geq \mathsf{E}\left(\left|\{D(k,C):\, k \in [1:2^s]\}\right|^{-1}\right) - 2^{-n} \\
&\geq 2^{-s} - 2^{-n}.
\end{aligned}$$

The proof is completed by rearranging the terms. ∎

Note that when $\rho > 0$, the lower bound in the above theorem can be rewritten as

$$s \geq 2\log\frac{1}{\rho} - \log\left(1 + \frac{1}{2^n\rho^2}\right),$$

which approaches $2\log(1/\rho)$ as $n \to \infty$.

We now show a construction of a cipher with key length close to the lower bound using expander graphs. The use of expander graphs in constructing ciphers is also studied in [18]. For an integer $d > 0$, let $\sigma_1, \ldots, \sigma_d$ be permutations of $[1 : 2^n]$, which satisfy $|\{i : \sigma_i = \sigma\}| = |\{i : \sigma_i = \sigma^{-1}\}|$ for any σ. These permutations induce a d-regular graph with vertex set $[1 : 2^n]$, edges $(i, \sigma_k(i))$ for $i \in [1 : 2^n]$ and $k \in [1 : d]$, and an adjacency matrix

$$A = \sum_{k=1}^{d} A_k,$$

where A_k is the permutation matrix corresponding to σ_k. If the magnitude of the second largest eigenvalue (in absolute value) of A,

$$|\lambda_2(A)| = \left\|A - \frac{d}{2^n}\mathbf{1}_{2^n \times 2^n}\right\|$$

is small, the graph is referred to as an *expander graph*. An expander graph can be constructed explicitly, for example, using a non-bipartite Ramanujan graph [19], which has a second eigenvalue

$$|\lambda_2(A)| \leq 2\sqrt{d - 1}.$$

Given an expander graph, we can define a corresponding *expander graph cipher* with $\mathcal{M} = \mathcal{C} = [1 : 2^n]$, $\mathcal{K} = [1 : d]$, $E(k, m) = \sigma_k(m)$, and $D(k, c) = \sigma_k^{-1}(c)$. We now find the maximal correlation for such an expander graph cipher.

Theorem 3. *The cipher defined by an expander graph with adjacency matrix A has maximal correlation*

$$\rho_{\mathrm{m}}(M; C) = \frac{1}{d}|\lambda_2(A)|.$$

As a result, the cipher corresponding to a non-bipartite Ramanujan graph is ρ-maximal correlation secure if

$$\log d \geq 2 \log \frac{1}{\rho} + 2.$$

where $s = \log d$ is the key length if it is an integer.

The proof of this theorem is a direct application of the characterization of maximal correlation in [12], and is given in [15]. The relationship between maximal correlation and the second eigenvalue of a graph is also studied in [20]. A limitation of the above construction is that there may not be constructions of Ramanujan graphs for a desired n and s. Using the result in [21] on the second eigenvalue of random regular graphs, we can show the existence of maximal correlation secure ciphers with key lengths close to the lower bound for any large enough n and s.

Theorem 4. *There exists a ρ-maximal correlation secure cipher with $n \geq 2$ and $s \geq 2$ if*

$$s \geq \left(2 \log \frac{1}{\rho}\right)\left(1 + \frac{\alpha}{\log n}\right) + \alpha,$$

where $\alpha > 0$ is a constant.

The following corollary provides a bound on s which is independent of n.

Corollary 1. *There exists a ρ-maximal correlation secure cipher with $n \geq 2$ and $s \geq 2$ if*

$$s \geq \left(2 \log \frac{1}{\rho}\right)\left(1 + \frac{3\alpha/2}{\log(\log(1/\rho) + 1)}\right),$$

where $\alpha > 0$ is a constant.

This corollary shows that for any ρ, a key length which depends only on ρ is sufficient to achieve ρ-maximal correlation secrecy for any message length. This is in a strong contrast to perfect secrecy, which requires the key length to be at least the message length. The proofs of Theorem 4 and Corollary 1 are given in [15].

Maximal correlation secrecy can also be achieved by a an additive stream cipher with a sightly longer key length. Consider a *binary additive stream cipher* $\mathcal{M} = \mathcal{C} = \{0, 1\}^n$, $\mathcal{K} = \{0, 1\}^s$, $E(k, m) = m \oplus g(k)$, $D(k, c) = c \oplus g(k)$, where $g(k) = (g_1(k), g_2(k), \ldots, g_n(k)) \in \{0, 1\}^n$ is the *keystream generator* and $\oplus$ is component-wise $\mathrm{mod}\, 2$ addition. The following theorem shows that most binary additive stream ciphers with slightly longer key than the lower bound in Theorem 2 are ρ-maximal correlation secure.

Theorem 5. *Let $G_i(k)$, $i \in [1 : n]$, $k \in [1 : 2^s]$ be i.i.d.* $\mathrm{Bern}(1/2)$ *random keystream components. Let $\rho > 0$, $\epsilon > 0$, then*

$$\mathsf{P}\{\rho_{\mathrm{m}}(M;\, M \oplus G(K)) \leq \rho\} > 1 - \epsilon,$$

where the randomness of $\rho_{\mathrm{m}}(M; M \oplus G(K))$ is induced by the random keystream generator, if the key length

$$s \geq 2 \log \frac{1}{\rho} + \log n + \log\left(1 + \frac{1}{n} \log \frac{1}{\epsilon}\right) + 2.$$

The proof of this theorem is given in [15]. Substituting $\epsilon = 1$ in the theorem shows that there exists a ρ-maximal correlation secure binary additive stream cipher with key length

$$s \geq 2 \log \frac{1}{\rho} + \log n + 2.$$

Hence for a constant $\rho > 0$, a key size of around $\log n$ is sufficient. Figure 1 plots the lower bound on the key length in Theorem 2, the key length achievable by the expander graph cipher using the Ramanujan graphs in Theorem 3, and the key length achievable by the random stream cipher in Theorem 5 versus ρ for $n = 10000$.

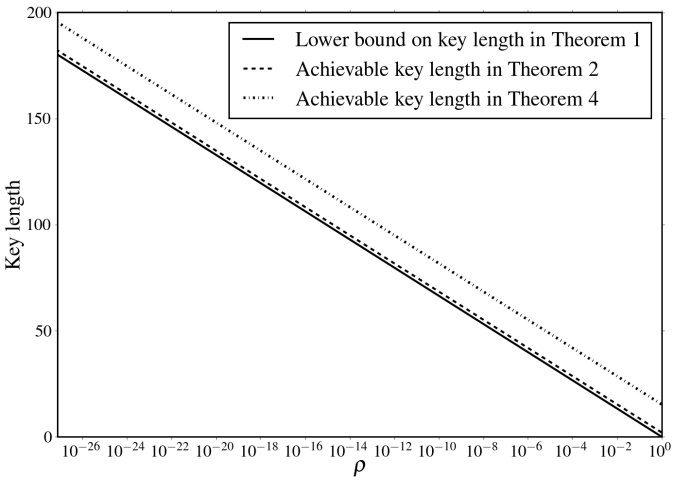

Figure 1. Comparison of the lower bound and the achievable key lengths for $n = 10000$.

To illustrate our results, suppose we wish to protect a message of length $n = 8 \times 10^9$ (i.e., 1GB) with a key of length $s = 512$. By Theorem 5, we can achieve ρ-maximal correlation secrecy for $\rho = 1.54 \times 10^{-72}$ using a binary additive stream cipher. As a result, if M is uniformly distributed, then the advantage of the eavesdropper is upper bounded by 1.54×10^{-72}. If $l = 100$ bits of M are provided to the eavesdropper, then the advantage is bounded by 1.74×10^{-57}. This shows that a cipher with key length much shorter than the message length can provide good security guarantees.

V. Relationship to Mutual Information

We compare maximal correlation secrecy to strong secrecy [3], weak secrecy [22], and leakage rate [23]. We first show that small ρ-maximal correlation secrecy implies small mutual information.

Proposition 1. *Let X and Y be two discrete random variables, then*

$$I(X;Y) \leq \log\left((\min\{|\mathcal{X}|, |\mathcal{Y}|\} - 1) \cdot \rho_{\mathrm{m}}^2(X;Y) + 1\right). \quad (2)$$

The proof of this proposition is in [15]. In the following we assume that $M \sim \mathrm{Unif}([1:2^n])$, which reduces (2) to

$$I(M;C) \leq \log\left((2^n - 1)\rho_{\mathrm{m}}^2(M;C) + 1\right). \quad (3)$$

We now use the above proposition to compare ρ-maximal correlation secrecy to secrecy criteria that use mutual information. *Strong secrecy*. This criterion requires that $\lim_{n\to\infty} I(M;C) = 0$. From (3) this is implied by ρ-maximal correlation secrecy for

$$\rho = o(2^{-n/2}).$$

Weak secrecy. This criterion requires that $\lim_{n\to\infty} I(M;C)/n = 0$. From (3), this is implied by ρ-maximal correlation secrecy for

$$\rho = 2^{-n/2+o(n)}.$$

Leakage rate. Note that both weak and strong secrecy require the key rate $\lim_n s/n = 1$. By requiring that $\lim_n I(M;C)/n \leq R_L$ for some leakage rate R_L, a key rate of $1 - R_L$ can be achieved. From (3), this is implied by ρ-maximal correlation secrecy for

$$\rho = 2^{-(1-R_L)n/2+o(n)}.$$

Note that Theorem 5 implies that such ρ can be achieved also by a key rate of $1 - R_L$. Hence maximal correlation secrecy provides a better security guarantee than leakage rate with no penalty on the key rate.

The above results show that ρ-maximal correlation secrecy implies secrecy with respect to criteria that use mutual information. We now show that a small $I(M;C)$ does not necessarily imply ρ-maximal correlation secrecy. Consider the following cipher: Let $\mathcal{M} = \mathcal{C} = \mathcal{K} = [0 : 2^n - 1]$, and the encryption and decryption functions be

$$E(k,m) = \begin{cases} m + k \mod 2^n - 1 & \text{if } m < 2^n - 1 \\ 2^n - 1 & \text{if } m = 2^n - 1, \end{cases}$$

and $D(k,c) = E(-k,c)$. Direct computation yields $I(M;C) = 2^{-n}(n + 2 - 2^{-(n-1)})$, which approaches zero as n tends to infinity, and thus the cipher satisfies strong secrecy. However, since one can readily determine if $M = 2^n - 1$ or not by observing C, $\rho_{\mathrm{m}}(M;C) = 1$. Hence ρ-maximal correlation secrecy is a strictly stronger secrecy criterion than criteria that use mutual information.

VI. Conclusions

We have shown that maximal correlation is a good measure of secrecy for cryptosystems that employ keys that are shorter than the message. Maximal correlation arises naturally as a bound on the advantage of the eavesdropper in guessing functions of the message. Together with the achievability results in Theorem 4 and 5, it is clear that maximal correlation is an ideal measure for connecting security against eavesdropping to the required key length. It would be interesting to explore applications of maximal correlation secrecy in practical cryptosystems.

References

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

[2] S. Goldwasser and S. Micali, "Probabilistic encryption," *Journal of computer and system sciences*, vol. 28, no. 2, pp. 270–299, 1984.

[3] U. M. Maurer, "The strong secret key rate of discrete random triples," in *Communications and Cryptography*. Springer, 1994, pp. 271–285.

[4] J. L. Massey and I. Ingemarsson, "The Rip van Winkle cipher–a simple and provably computationally secure cipher with a finite key," in *IEEE International Symposium on Information Theory (Abstracts)*, 1985, p. 146.

[5] U. M. Maurer and J. L. Massey, "Local randomness in pseudorandom sequences," *Journal of Cryptology*, vol. 4, no. 2, pp. 135–149, 1991.

[6] U. M. Maurer, "Conditionally-perfect secrecy and a provably-secure randomized cipher," *Journal of Cryptology*, vol. 5, no. 1, pp. 53–66, 1992.

[7] C. Cachin and U. Maurer, "Unconditional security against memory-bounded adversaries," in *Advances in Cryptology-CRYPTO'97*. Springer, 1997, pp. 292–306.

[8] F. P. Calmon, M. Médard, L. M. Zeger, J. Barros, M. M. Christiansen, and K. R. Duffy, "Lists that are smaller than their parts: A coding approach to tunable secrecy," in *Communication, Control, and Computing (Allerton), 2012 50th Annual Allerton Conference on*. IEEE, 2012, pp. 1387–1394.

[9] H. O. Hirschfeld, "A connection between correlation and contingency," in *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 31, no. 04. Cambridge Univ Press, 1935, pp. 520–524.

[10] H. Gebelein, "Das statistische problem der korrelation als variations-und eigenwertproblem und sein zusammenhang mit der ausgleichsrechnung," *ZAMM-Journal of Applied Mathematics and Mechanics/Zeitschrift für Angewandte Mathematik und Mechanik*, vol. 21, no. 6, pp. 364–379, 1941.

[11] A. Rényi, "On measures of dependence," *Acta mathematica hungarica*, vol. 10, no. 3, pp. 441–451, 1959.

[12] H. S. Witsenhausen, "On sequences of pairs of dependent random variables," *SIAM J. Appl. Math.*, vol. 28, no. 1, pp. 100–113, 1975.

[13] F. P. Calmon, M. Varia, M. Médard, M. M. Christiansen, K. R. Duffy, and S. Tessaro, "Bounds on inference," in *Proc. 51st Ann. Allerton Conf. Commun., Contr., and Comput.*, Oct. 2013, pp. 567–574.

[14] A. Russell and H. Wang, "How to fool an unbounded adversary with a short key," in *Advances in Cryptology-EUROCRYPT 2002*. Springer, 2002, pp. 133–148.

[15] C. T. Li and A. El Gamal, "Maximal correlation secrecy," *arXiv preprint*, 2014. [Online]. Available: http://arxiv.org/abs/1412.5374

[16] O. Goldreich, *Foundations of Cryptography: Volume 2, Basic Applications*. Cambridge University Press, 2009, vol. 2.

[17] K. Pearson, "On the criterion that a given system of deviations from the probable in the case of a correlated system of variables is such that it can be reasonably supposed to have arisen from random sampling," *Philosophical Magazine Series 5*, vol. 50, no. 302, pp. 157–175, 1900.

[18] Y. Dodis and A. Smith, "Entropic security and the encryption of high entropy messages," in *Theory of Cryptography*. Springer, 2005, pp. 556–577.

[19] A. Lubotzky, R. Phillips, and P. Sarnak, "Ramanujan graphs," *Combinatorica*, vol. 8, no. 3, pp. 261–277, 1988.

[20] M. Bolla and G. Molnar-Saska, "Optimization problems for weighted graphs and related correlation estimates," *Discrete Mathematics*, vol. 282, no. 1-3, pp. 23 – 33, 2004.

[21] J. Friedman, "On the second eigenvalue and random walks in randomd-regular graphs," *Combinatorica*, vol. 11, no. 4, pp. 331–362, 1991.

[22] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

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