Secure Computation of Linear Functions Over Linear Discrete Multiple-Access Wiretap Channels

Mario Goldenbaum*, Holger Boche†, and H. Vincent Poor*

*Department of Electrical Engineering, Princeton University
†Chair of Theoretical Information Technology, Technical University of Munich

***Abstract*—In this paper, a joint source-channel coding approach is taken to the problem of securely computing a function of distributed sources over a multiple-access wiretap channel that is linear with respect to a finite field. It is shown that if the joint source distribution fulfills certain conditions and the function to be computed matches the linear structure of the channel, secrecy comes for free in the sense that the fundamental limit (i.e., the secrecy computation-capacity) is achieved without the need for stochastic encoding. Furthermore, the legitimate receiver does not need any advantage over the eavesdropper, which is in stark contrast to standard physical-layer security results.**

***Index Terms*—Secure distributed computation, computation coding, multiple-access wiretap channel, physical-layer security**

I. Introduction

Secure distributed computation, also known as secure multiparty computation, has a long-standing history in computer science and dates back to the seminal work of Yao [1]. From an information-theoretic perspective, however, it is still in its infancy and there exist only very few results. In [2], for instance, Tyagi et al. introduce a new multiuser source model and provide necessary and sufficient conditions under which a function of the sources can be securely computed. Within the original model of [1], Lee and Abbe determine in [3] the least amount of randomness needed to securely compute a function of distributed sources, which provides a novel notion of the complexity of a function. In the second part of that paper, the authors consider a probabilistic (i.e., Shannon-type) source model for which security is assumed to be achieved asymptotically in the coding block length. In [4], Data et al. take a distributed source coding approach similar to that in [3]. They assume the information to be drawn from a joint memoryless source and then derive bounds on the amount of randomness and communication needed to asymptotically obtain secure computation results.

Each of the above-referenced works assumes the communication between any given pair of source terminals takes place over a noiseless channel of infinite capacity. Whereas distributed computation over noisy channels and networks has been received a lot of attention in recent years [5]–[10], potential security issues have not yet been sufficiently addressed. In this paper, we therefore take a *joint source-channel coding approach* to the problem of securely computing a function of distributed sources over a multiple-access wiretap channel (MAWC). In particular, we extend our previous work [11] to the class of MAWCs that are linear with respect to some finite field. It is shown that if the joint source distribution fulfills certain conditions and the function to be computed matches the linear structure of the channel, *secrecy comes for free* in the sense that the secrecy computation-capacity is achieved without the need for stochastic encoding. Furthermore, the legitimate receiver does not need any advantage over the eavesdropper, which is in stark contrast to secure separation-based coding schemes.

Separation-based schemes suffer from imposing a secrecy constraint as they only exploit the random structure of the underlying MAWC. The coding scheme considered in this paper goes one step further and also exploits the *algebraic structure* of the channel. Note that a similar approach is taken in [12] and [13] for the problem of securely communicating messages over a Gaussian bidirectional relay channel.

The rest of the paper is organized as follows. Section II introduces the system model and provides the problem statement. In Section III, we define the class of $\mathbb{F}_p$-linear MAWCs and provide the main results of this paper. By means of a simple example, the results are then discussed in Section IV. Finally, Section V concludes the paper and provides a short discussion of the results.

Notation: A length-n sequence X^n of random variables is considered as a column vector whenever multiplied by a matrix. For $\mu \in [0,1]$, $H(\mu) = -\mu \log_2 \mu - (1-\mu)\log_2(1-\mu)$ denotes the binary entropy function with the convention $0 \log_2 0 = 0$. The Bernoulli distribution with parameter $\mu \in [0,1]$ is denoted as $\mathrm{Bern}(\mu)$, which means that $X \sim \mathrm{Bern}(\mu)$ takes on value 1 with probability μ. Finally, δ_{ij} denotes the Kronecker delta, which is 1 for $i = j$ and 0 otherwise.

II. Problem Statement

Let S_1 and S_2 be two sources defined over finite alphabets $\mathcal{S}_1$ and $\mathcal{S}_2$, and assume they are drawn from some joint probability mass function $P_{S_1 S_2}$. In the presence of an eavesdropper, the sources are communicated to a legitimate receiver over a noisy channel. Unlike the usual setup in which the legitimate receiver wishes to reliably reconstruct the sources while keeping the eavesdropper ignorant of them [14]–[17],

This work was supported in part by the German Research Foundation (DFG) under Grant GO 2669/1-1 and by the U. S. National Science Foundation (NSF) under Grants CMMI-1435778 and ECCS-1647198.

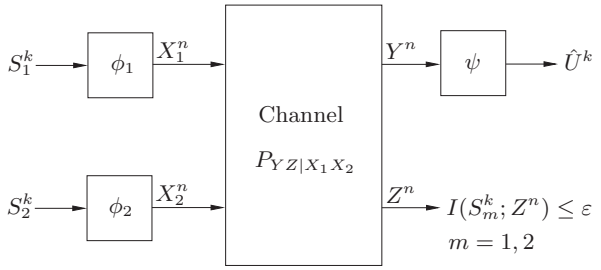

Fig. 1. Secure computation of a function $U = f(S_1, S_2)$ over a MAWC.

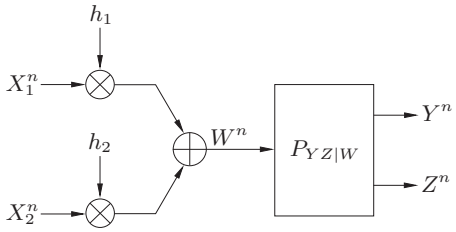

Fig. 2. $\mathbb{F}_p$-linear MAWC.

in this paper the legitimate receiver intends to *reliably and securely* compute a symbol-by-symbol function

$$f : \mathcal{S}_1 \times \mathcal{S}_2 \to \mathcal{U} \ , \ (S_1, S_2) \mapsto U \coloneqq f(S_1, S_2)$$

of the sources, where $\mathcal{U}$ denotes the range of f (finite set). In what follows, we simply refer to f as the *desired function*.

As illustrated in Fig. 1, we model the communication between the source terminals and the receiving parties as a discrete memoryless MAWC, which consists of finite input alphabets $\mathcal{X}_1$ and $\mathcal{X}_2$, two finite output alphabets $\mathcal{Y}$ and $\mathcal{Z}$, and a conditional probability mass function $P_{YZ|X_1X_2}$. As the channel is assumed to be memoryless, we have

$$P_{Y^nZ^n|X_1^nX_2^n}(y^n, z^n|x_1^n, x_2^n) = \prod_{i=1}^{n} P_{YZ|X_1X_2}(y_i, z_i|x_{1i}, x_{2i})$$

for all $(x_1^n, x_2^n, y^n, z^n) \in \mathcal{X}_1^n \times \mathcal{X}_2^n \times \mathcal{Y}^n \times \mathcal{Z}^n$ and $n \in \mathbb{N}$.

For some $k \in \mathbb{N}$, $S_m^k \in \mathcal{S}_m^k$ denotes a length-k sequence of independent and identically distributed copies of source m, $m = 1, 2$. In order to reliably compute the corresponding sequence of function values, U^k, at the legitimate receiver, the source terminals employ a length-n computation code defined as follows [5].

Definition 1. Let f be a fixed desired function. A (k, n) *computation code* for f and any given MAWC consists of:

- Encoders
$$\phi_m : \mathcal{S}_m^k \to \mathcal{X}_m^n \ , \ m = 1, 2 \ ,$$
each of which maps k source symbols to a length-n codeword (i.e., $\phi_m(s_m^k) = x_m^n$);
- A decoder at the legitimate receiver
$$\psi : \mathcal{Y}^n \to \mathcal{U}^k \ ,$$
which maps each channel output sequence to a length-k sequence of function values (i.e., $\psi(y^n) = \hat{u}^k$).

The *average probability or error* of a (k, n) computation code is defined as

$$P_e^{(n)} \coloneqq \mathbb{P}\big[\hat{U}^k \neq U^k\big] \ ,$$

whereas the information about the source sequences *leaked* to the eavesdropper is measured by[1]

$$L^{(n)} \coloneqq I(S_1^k; Z^n) + I(S_2^k; Z^n) \ .$$

[1]Note that $L^{(n)}$ simply combines the individual leakages $I(S_m^k; Z^n)$, $m = 1, 2$, into a single constraint.

Definition 2. For a given desired function and a given MAWC, a rate $R \coloneqq k/n$ is said to be an *achievable secrecy computation-rate* if for every $\varepsilon > 0$ there exists an $n_0 = n_0(\varepsilon)$ and a sequence of (nR, n) computation codes such that for all $n \geq n_0$

$$P_e^{(n)} \leq \varepsilon \quad \text{and} \quad L^{(n)} \leq \varepsilon \ .$$

Definition 3. For a given desired function and a given MAWC, the *secrecy computation-capacity* is defined as

$$C_{\mathsf{sc}} \coloneqq \sup\{R : R \text{ is an achievable secrecy computation-rate}\}.$$

Characterizing the secrecy computation-capacity for arbitrary desired functions and arbitrary MAWCs is a challenging problem. Throughout the rest of the paper, we therefore focus on the particular class of $\mathbb{F}_p$-linear MAWCs.

III. $\mathbb{F}_p$-Linear Multiple-Access Wiretap Channels

Let $\mathbb{F}_p$ denote some finite field of order p and let the source and the channel input and output alphabets be all equal to $\mathbb{F}_p$. Then, we define an $\mathbb{F}_p$-linear MAWC as follows.

Definition 4. A memoryless MAWC is said to be $\mathbb{F}_p$*-linear* if and only if

$$P_{YZ|X_1X_2} = P_{YZ|W} \quad \text{with} \quad W \coloneqq h_1X_1 \oplus_p h_2X_2 \ ,$$

and $h_m \in \mathbb{F}_p \backslash \{0\}$, $m = 1, 2$. Here and hereafter, 0 denotes the zero symbol in $\mathbb{F}_p$ and $\oplus_p$ addition over $\mathbb{F}_p$, respectively.

A. Secrecy Computation-Capacity

Before stating the main result of this paper, we need the notion of a weakly symmetric channel [18, p. 190].

Definition 5. A discrete memoryless channel with transition-probability matrix $P_{Y|W}$ is *weakly symmetric* if the rows of $P_{Y|W}$ are permutations of each other and $\sum_w P_{Y|W}(y|w) = \sum_w P_{Y|W}(y'|w)$, for all $y, y' \in \mathcal{Y}$.

Theorem 1. Let the desired function be

$$f : \mathbb{F}_p^2 \to \mathbb{F}_p \ , \ U = f(S_1, S_2) = a_1S_1 \oplus_p a_2S_2 \ ,$$

for some $a_1, a_2 \in \mathbb{F}_p \backslash \{0\}$, and the joint source distribution, $P_{S_1S_2}$, such that $P_{S_mU} = P_{S_m}P_U$, $m = 1, 2$. Furthermore, let $P_{Y|W}$ (i.e., the channel to the legitimate receiver) be weakly symmetric. Then,

$$C_{\mathsf{sc}} = \frac{\log_2(p) - H\big(P_{Y|W}(\cdot|w)\big)}{H(U)} \ , \tag{1}$$

where $H\big(P_{Y|W}(\cdot|w)\big)$ denotes the entropy of an arbitrary row of transition-probability matrix $P_{Y|W}$.

Proof: The proof is deferred to Appendix A. ∎

Carefully examining (1) reveals that under the assumptions made, the secrecy computation-capacity does not depend on $P_{Z|W}$ (i.e., the eavesdropper's channel). This is possible as the source sequences protect each other like one-time pads.

Corollary 1. If we drop the assumption that $P_{Y|W}$ is weakly symmetric, then

$$R = \frac{I(W;Y)}{H(U)}$$

is an achievable secrecy computation-rate, with W uniformly distributed over $\mathbb{F}_p$.

Remark 1. The leakage analysis in the proof of Theorem 1 implies also $I(S_m^k; Y^n) \equiv 0$, $m = 1, 2$. In other words, the legitimate receiver is prevented from obtaining information about the source sequences as well.

B. Secure Separation-Based Computation

The coding scheme used in the achievability part of the proof of Theorem 1 (see Appendix A-A) is based on linear random codes. In particular, the source terminals employ the same linear joint source-channel code and transmit their codewords concurrently to make use of the algebraic structure of the $\mathbb{F}_p$-linear MAWC. In this section, we analyze what computation rates are achievable when the terminals follow a *secure separation-based approach* [11]. In a secure separation-based scheme, encoders and decoders are divided into two parts. The first part (i.e., the source code) distributively compresses the sources into messages, whereas the second part (i.e., the multiple-access wiretap code) is used to protect the messages against the channel noise and the eavesdropper.

The feasibility of a secure separation-based scheme is determined by the distributed compression-rate region of f along with the secrecy capacity region of the underlying MAWC.

Definition 6. Let f be a fixed desired function and $\mathcal{M}_1$ and $\mathcal{M}_2$ finite message sets. Then, the *distributed compression-rate region* of f, $\mathcal{R}(f)$, is the set of all rate pairs (R_1, R_2), with $R_m \coloneqq \log_2|\mathcal{M}_m|/n$, such that for every $\varepsilon > 0$ there exists a $k_0 = k_0(\varepsilon)$, sequences of source encoders $\phi_m^{(\mathrm{s})} : \mathcal{S}_m^k \to \mathcal{M}_m$, $m = 1, 2$, and a sequence of source decoders $\psi^{(\mathrm{s})} : \mathcal{M}_1 \times \mathcal{M}_2 \to \mathcal{U}^k$ such that $\mathbb{P}[\hat{U}^k \neq U^k] \leq \varepsilon$ for all $k \geq k_0$.

Definition 7. The *secrecy capacity region*, $\mathcal{C}_{\mathsf{s}}$, of a given MAWC is the closure of the convex hull of all rate pairs (R_1, R_2) such that for every $\varepsilon > 0$ there exists an $n_0 = n_0(\varepsilon)$, sequences of channel encoders $\phi_m^{(\mathrm{c})} : \mathcal{M}_m \to \mathcal{X}_m^n$, $m = 1, 2$, and a sequence of channel decoders $\psi^{(\mathrm{c})} : \mathcal{Y}^n \to \mathcal{M}_1 \times \mathcal{M}_2$ such that $\mathbb{P}[(\hat{M}_1, \hat{M}_2) \neq (M_1, M_2)] \leq \varepsilon$ and $I(M_1, M_2; Z^n) \leq \varepsilon$ for all $n \geq n_0$. Here, $M_m \in \mathcal{M}_m$ denotes the message sent by terminal m.

Definition 8. A secrecy computation-rate R is said to be achievable with a separation-based coding scheme if

$$\mathcal{R}(f) \cap \mathcal{C}_{\mathsf{s}}(R) \neq \varnothing \ ,$$

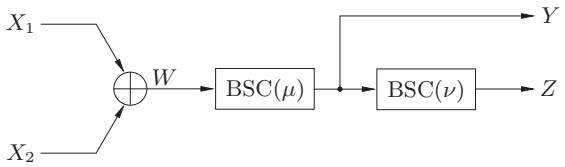

Fig. 3. Physically degraded binary modulo-2 adder MAWC, where BSC(μ) denotes a binary symmetric channel with crossover probability μ.

where $\mathcal{C}_{\mathsf{s}}(R) \coloneqq \big\{\big(\frac{R_1}{R}, \frac{R_2}{R}\big) \,\big|\, (R_1, R_2) \in \mathcal{C}_{\mathsf{s}}\big\}$.

Remark 2. Slepian-Wolf source coding in combination with multiple-access wiretap coding can be seen as a particular instance of a secure separation-based scheme. A secrecy computation-rate, R, is then achievable if $\mathcal{R}_{\mathsf{SW}} \cap \mathcal{C}_{\mathsf{s}}(R) \neq \varnothing$, where $\mathcal{R}_{\mathsf{SW}}$ refers to the Slepian-Wolf rate region [18].

As of the writing of this paper, for arbitrary f and arbitrary MAWCs, $\mathcal{R}(f)$ and $\mathcal{C}_{\mathsf{s}}$ are unknown. Thus, we restrict our attention to $\mathbb{F}_p$-linear MAWCs that are physically degraded.

Definition 9. An $\mathbb{F}_p$-linear MAWC is said to be *physically degraded* if the wiretap channel $P_{YZ|W}$ is physically degraded; that is, if $W \to Y \to Z$ forms a Markov chain in that order.

Theorem 2. Let the sources be statistically independent, $U = S_1 \oplus_p S_2$, and the MAWC $\mathbb{F}_p$-linear and physically degraded. Then, the best secrecy computation-rate achievable with separation is

$$R = \frac{\max_{P_W}\big(I(W;Y) - I(W;Z)\big)}{H(S_1) + H(S_2)} \ .$$

Proof: The proof is deferred to Appendix B. ∎

The result demonstrates that secure separation-based coding schemes generally suffer from imposing a secrecy constraint (i.e., the achievable secrecy computation-rates depend on the eavesdropper's channel).

Corollary 2. In addition to the assumptions of Theorem 2 let $P_{Y|W}$ and $P_{Z|W}$ be weakly symmetric. Then,

$$R = \frac{H\big(P_{Z|W}(\cdot|w)\big) - H\big(P_{Y|W}(\cdot|w)\big)}{H(S_1) + H(S_2)}$$

is the best secrecy computation-rate achievable with separation.

IV. A Simple Example

Consider the physically degraded $\mathbb{F}_2$-linear MAWC illustrated in Fig. 3, which is known as the *binary modulo-2 adder MAWC* [11]. It is characterized by the input-output relations

$$Y = X_1 \oplus_2 X_2 \oplus_2 N_Y \ , \tag{2a}$$

$$Z = Y \oplus_2 N_Z \ , \tag{2b}$$

where $N_Y \sim \mathrm{Bern}(\mu)$ and $N_Z \sim \mathrm{Bern}(\nu)$, $\mu, \nu \in [0, 1]$.

Assume the joint source distribution to be doubly symmetric; that is,

$$P_{S_1S_2}(s_1, s_2) = \frac{1}{2}(1-\theta)\delta_{s_1 s_2} + \frac{1}{2}\theta(1 - \delta_{s_1 s_2}) \ , \tag{3}$$

for $(s_1, s_2) \in \mathbb{F}_2^2$ and some $\theta \in [0,1]$. We have the following corollary to Theorem 1.

Corollary 3. Let the desired function be $f : \mathbb{F}_2^2 \to \mathbb{F}_2$, $U = S_1 \oplus_2 S_2$. Then, the secrecy computation-capacity of the binary modulo-2 adder MAWC given in (2) is

$$C_{\mathsf{sc}} = \frac{1 - H(\mu)}{H(\theta)} \, . \tag{4}$$

Proof: The result follows by the facts that the binary symmetric channel with parameter $\mu \in [0,1]$ is of capacity $\max_{P_W} I(W;Y) = 1 - H(\mu)$ and for the joint source distribution given in (3) we have $H(U) = H(\theta)$. ∎

The following result, which is a corollary to Theorem 2, provides the secrecy computation-rate achievable with the best separation-based coding scheme.

Corollary 4. Let the desired function be $f : \mathbb{F}_2^2 \to \mathbb{F}_2$, $U = S_1 \oplus_2 S_2$. Then, for the binary modulo-2 adder MAWC given in (2),

$$R = \frac{1}{2}\left(\frac{H(\nu') - H(\mu)}{H(\theta)}\right) , \tag{5}$$

with $\nu' \coloneqq (1-\mu)\nu + (1-\nu)\mu$, is the best secrecy computation-rate achievable with separation.

Proof: For $\theta \in (0,1)$ the sources are correlated, which contradicts the assumption of Theorem 2. Nevertheless, if we use the linear source-code of the proof of Theorem 1, we achieve a sum compression-rate of $2H(\theta) \leq H(S_1) + H(S_2)$, which is optimal for $P_{S_1 S_2}$ as given in (3) [11]. ∎

According to Remark 2, using Slepian-Wolf coding also results in a valid secure separation-based strategy: the legitimate receiver first reliably and securely decodes the individual source sequences and then computes $\hat{S}_1^k \oplus_2 \hat{S}_2^k$ to obtain an estimate of U^k. The corresponding achievable secrecy computation-rate is

$$R = \frac{H(\nu') - H(\mu)}{1 + H(\theta)} \, . \tag{6}$$

Fig. 4 compares (4), (5), and (6) for $\mu = \theta = 0.1$ and different values of ν. It can be seen that for the particular example considered in this section, secure separation-based computation achieves at best half the secrecy computation-capacity. What is more remarkable, however, is that for ν either zero or one, the secrecy computation-rates vanish. Thus, joint source-channel coding schemes may not only significantly outperform separation-based schemes but in certain cases they are even necessary to achieve nonzero performance.

V. Conclusion

We have considered the problem of securely computing linear functions over discrete multiple-access wiretap channels. For the class of channels that are linear with respect to some finite field, we have determined the secrecy computation-capacity as the corresponding fundamental limit. In comparison to the computation rates achievable with a secure separation-based strategy, the capacity achieving scheme does not depend on the eavesdropper's channel and hence there is no need for stochastic encoding.

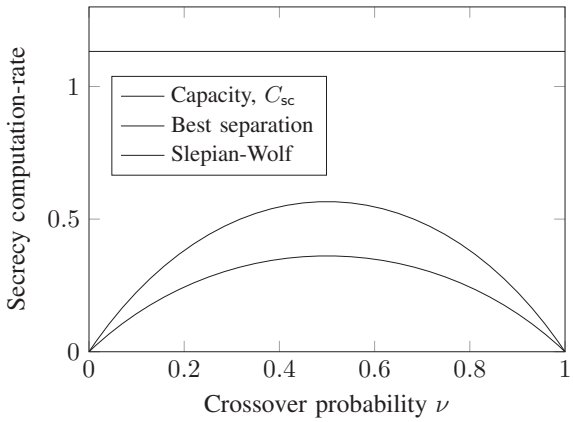

Fig. 4. Comparison of the secrecy computation-capacity (4) with the best achievable separation-based rate (5) and the rate achievable with Slepian-Wolf source coding (6), for $\mu = \theta = 0.1$.

Interesting problems for future work include extensions to the Gaussian case as well as characterizing the set of joint source distributions for which $P_{S_m U} = P_{S_m} P_U$, $m = 1, 2$, which was a crucial assumption. Note that for the binary case this question has a clear answer [11, Th. 2].

Appendix A
Proof of Theorem 1

For the proof of the theorem, we are mainly following the proof of [5, Th. 1] (see also [11]).

A. Achievability

1) Code Construction: For every fixed n, generate two matrices $A_n \in \mathbb{F}_p^{n \times \ell}$ and $B_k \in \mathbb{F}_p^{\ell \times k}$, each entry drawn uniformly and independently at random from $\mathbb{F}_p$, with

$$k H(U) < \ell < n \max_{P_W} I(W;Y) \, . \tag{7}$$

Reveal A_n and B_k to the source terminals, the legitimate receiver, and the eavesdropper.

Given source sequence s_m^k, transmit the codeword

$$x_m^n = \phi(s_m^k) = h_m^{-1} a_m A_n B_k s_m^k \, ,$$

$m = 1, 2$, where all operations are carried out over $\mathbb{F}_p$.

2) Probability of Error Analysis: Notice that

$$\begin{aligned} W^n &= h_1 X_1^n \oplus_p h_2 X_2^n \\ &= A_n B_k (a_1 S_1^k \oplus_p a_2 S_2^k) \\ &= A_n B_k U^k \, . \end{aligned} \tag{8}$$

Effectively, (8) is a single terminal that wishes to reliably and efficiently transmit the source sequences U^k over the discrete memoryless channel $P_{Y|W}$. The random linear code induced by the generator matrix A_n therefore has the objective of protecting $B_k U^k$ against the channel noise, whereas the linear code induced by B_k is used to compress U^k to its entropy.

As long as condition (7) is fulfilled, it follows from [19] and [20] that there exist decoding functions $\psi' : \mathbb{F}_p^n \to \mathbb{F}_p^\ell$ and $\psi'' : \mathbb{F}_p^\ell \to \mathbb{F}_p^k$ such that for arbitrary $\varepsilon > 0$ and k, n large enough, the average probabilities of error (averaged over A_n and B_k) fulfill $\mathbb{P}[\psi'(Y^n) \neq BU^k] < \frac{\varepsilon}{2}$ and $\mathbb{P}[\psi''(BU^k) \neq U^k] < \frac{\varepsilon}{2}$. Thus, by means of the union of events bound we obtain $P_e^{(n)} < \varepsilon$ as long as $R = \frac{k}{n} < \frac{\max_{P_W} I(W;Y)}{H(U)}$.

Now, as $P_{Y|W}$ is weakly symmetric, its capacity is

$$\max_{P_W} I(W;Y) = \log_2(p) - H\big(P_{Y|W}(\cdot|w)\big) \,, \tag{9}$$

which is achieved with P_W the uniform distribution over $\mathbb{F}_p$. It can be easily shown that multiplying U^k with A_n and B_k results in W^n being uniformly distributed over $\mathbb{F}_p^n$.

3) Leakage Analysis: In order to show that $L^{(n)}$ vanishes, we analyze each of its terms individually. Notice that the source and channel output sequences form the Markov chains

$$(S_1^k, S_2^k) \to (X_1^n, X_2^n) \to W^n \to (Y^n, Z^n) \,, \tag{10a}$$

$$S_m^k \to U^k \to A_n B_k U^k \,, \tag{10b}$$

$m = 1, 2$. Therefore, we conclude

$$\begin{aligned} I(S_m^k; Z^n | A_n, B_k) &\overset{\text{(a)}}{\leq} I(S_m^k; W^n | A_n, B_k) \\ &\overset{\text{(b)}}{=} I(S_m^k; A_n B_k U^k | A_n, B_k) \\ &\overset{\text{(c)}}{\leq} I(S_m^k; U^k | A_n, B_k) \\ &= I(S_m^k; U^k) \\ &\overset{\text{(d)}}{=} 0 \,, \end{aligned}$$

where (a) follows with (10a) from the data-processing inequality, (b) from (8), (c) with (10b) from the data-processing inequality, and (d) from the assumption $P_{S_m U} = P_{S_m} P_U$ and the memorylessness of the sources. As this applies to $m = 1, 2$, we have $L^{(n)} \equiv 0$.

B. Converse

Dropping the secrecy constraint and joining the encoders, it follows from the converse of the point-to-point separation theorem [18] that for the average probability of error, $P_e^{(n)}$, to vanish with increasing block length, every coding scheme has to fulfill

$$kH(U) \leq \max_{P_{X_1 X_2}} I(X_1^n, X_2^n; Y^n) = n \max_{P_W} I(W;Y) \,.$$

Comparing the left with the right-hand side results in combination with (9) in a tight upper bound.

Appendix B
Proof of Theorem 2

In [21], Dai and Ma were able to characterize the secrecy capacity region for those MAWCs that are physically degraded (i.e., $(X_1, X_2) \to Y \to Z$ forms a Markov chain). From their characterization it follows that the secrecy capacity region of a physically degraded $\mathbb{F}_p$-linear MAWC is given by

$$\mathcal{C}_\mathsf{s} = \Big\{ (R_1, R_2) \,\Big|\, R_1 + R_2 < \max_{P_W} \big((I(W;Y) - I(W;Z) \big) \Big\} \,. \tag{11}$$

Thus, time sharing together with single-user wiretap coding is optimal. On the other hand, it follows from [5, Lemma 1] that for S_1 and S_2 statistically independent and $U = S_1 \oplus_p S_2$, the sources have to be transmitted in their entirety (i.e., $R_1 + R_2 \geq H(S_1) + H(S_2)$) in order to reliably decode U. Combining this with (11) proves the result.

References

[1] A. C. Yao, "Protocols for secure computations," in *Proc. 23rd Annu. Symp. Found. Comput. Sci. (FOCS)*, Chicago, IL, USA, Nov. 1982, pp. 160–164.

[2] H. Tyagi, P. Narayan, and P. Gupta, "When is a function securely computable?" *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6337–6350, Oct. 2011.

[3] E. J. Lee and E. Abbe, "Two Shannon-type problems on secure multiparty computations," in *Proc. 52nd Annu. Allerton Conf. Commun., Control, Computing*, Monticello, IL, USA, Oct. 2014, pp. 1287–1293.

[4] D. Data, V. M. Prabhakaran, and M. M. Prabhakaran, "Communication and randomness lower bounds for secure computation," *IEEE Trans. Inf. Theory*, vol. 62, no. 7, pp. 3901–3929, Jul. 2016.

[5] B. Nazer and M. Gastpar, "Computation over multiple-access channels," *IEEE Trans. Inf. Theory*, vol. 53, no. 10, pp. 3498–3516, Oct. 2007.

[6] R. Soundararajan and S. Vishwanath, "Communicating linear functions of correlated Gaussian sources over a MAC," *IEEE Trans. Inf. Theory*, vol. 58, no. 3, pp. 1853–1860, Mar. 2012.

[7] A. Khisti, B. Hern, and K. Narayanan, "On modulo-sum computation over an erasure multiple-access channel," *IEEE Trans. Inf. Theory*, vol. 59, no. 7, pp. 4129–4138, Jul. 2013.

[8] M. Goldenbaum and S. Stańczak, "Robust analog function computation via wireless multiple-access channels," *IEEE Trans. Commun.*, vol. 61, no. 9, pp. 3863–3877, Sep. 2013.

[9] M. Goldenbaum, H. Boche, and S. Stańczak, "Nomographic functions: Efficient computation in clustered Gaussian sensor networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 4, pp. 2093–2105, Apr. 2015.

[10] S.-W. Jeon and B. C. Jung, "Opportunistic function computation for wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 6, pp. 4045–4059, Jun. 2016.

[11] M. Goldenbaum, H. Boche, and H. V. Poor, "On secure computation over the binary modulo-2 adder multiple-access wiretap channel," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Cambridge, UK, Sep. 2016, pp. 21–25.

[12] X. He and A. Yener, "Strong secrecy and reliable Byzantine detection in the presence of an untrusted relay," *IEEE Trans. Inf. Theory*, vol. 59, no. 1, pp. 177–192, Jan. 2013.

[13] S. Vatedka, N. Kashyap, and A. Thangaraj, "Secure compute-and-forward in a bidirectional relay," *IEEE Trans. Inf. Theory*, vol. 61, no. 5, pp. 2531–2556, May 2015.

[14] Y. Liang and H. V. Poor, "Multiple-access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.

[15] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5747–5755, Dec. 2008.

[16] E. Ekrem and S. Ulukus, "On the secrecy of multiple access wiretap channel," in *Proc. 46th Annu. Allerton Conf. Commun., Control, Computing*, Monticello, IL, USA, Sep. 2008, pp. 1014–1021.

[17] M. Goldenbaum, R. F. Schaefer, and H. V. Poor, "The multiple-access channel with an external eavesdropper: Trusted vs. untrusted users," in *Proc. 49th Asilomar Conf. Signals, Syst., Comput.*, Pacific Grove, CA, USA, Nov. 2015, pp. 564–568.

[18] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. New York: John Wiley & Sons, 2006.

[19] T. S. Han and K. Kobayashi, "A dichotomy of functions $F(X, Y)$ of correlated sources (X, Y) from the viewpoint of the achievable rate region," *IEEE Trans. Inf. Theory*, vol. 33, no. 1, pp. 69–76, Jan. 1987.

[20] M. Effros *et al.*, "Linear network codes: A unified framework for source, channel, and network coding," in *Proc. DIMACS Workshop Netw. Inform. Theory*, Piscataway, NJ, Mar. 2003, pp. 197–216.

[21] B. Dai and Z. Ma, "Some new results on the multiple-access wiretap channel," *Entropy*, vol. 16, no. 8, pp. 4693–4712, Aug. 2014.