

On Secure Computation Over the Binary Modulo-2 Adder Multiple-Access Wiretap Channel

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, the problem of securely computing a function over the binary modulo-2 adder multiple-access wiretap channel is considered. The problem involves a legitimate receiver that wishes to reliably and efficiently compute a function of distributed binary sources while an eavesdropper has to be kept ignorant of them. In order to characterize the corresponding fundamental limit, the notion of *secrecy computation-capacity* is introduced. Although determining the secrecy computation-capacity is challenging for arbitrary functions, it surprisingly turns out that if the function perfectly matches the algebraic structure of the channel and the joint source distribution fulfills certain conditions, the secrecy computation-capacity equals the computation capacity, which is the supremum of all achievable computation rates without secrecy constraints. Unlike the case of securely transmitting messages, no additional randomness is needed at the encoders nor does the legitimate receiver need any advantage over the eavesdropper. The results therefore show that the problem of securely computing a function over a multiple-access wiretap channel may significantly differ from the one of securely communicating messages.

Index Terms

Secure distributed computation, computation coding, multiple-access wiretap channel, physical-layer security

I. INTRODUCTION

In their seminal work [1], Nazer and Gastpar lay the information-theoretic foundation of distributed computation over unreliable channels. The big difference between this approach and the standard theory dealing with reliable message transfer is that, in [1], the intended receiver decodes function values immediately from the channel output. In other words, the receiver does not care about individual messages and penalizes itself only when the function is incorrectly decoded.

In this regard, Nazer and Gastpar show that in many cases, the performance gain over separation-based computation strategies is proportional to the number of source terminals. In a separation-based strategy, the receiver first reliably decodes all individual messages and subsequently computes the sought function value. It is remarkable that the gains over separation-based strategies stem from a match between the desired function and the algebraic structure of the channel. Since the publication of [1], the results and ideas have been extended in many different ways [2]–[6].

Due to the trend towards large-scale decentralized networks consisting of many mutually distrusting terminals, *security and integrity* of computation results are of high priority in order to guarantee trustworthy operation. In this work, we therefore make a first attempt to extend the concept of computation coding [1] by taking information theoretic security aspects into account. In particular, we consider the problem of computing a function over the binary modulo-2 adder multiple-access wiretap channel (MAWC). The problem involves a legitimate receiver that wishes to reliably compute a function of distributed binary sources in the presence of an eavesdropper. To characterize the corresponding fundamental limit, we introduce

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 under Grant CMMI-1435778.

the notion of *secrecy computation-capacity*. Although determining the secrecy computation-capacity for arbitrary functions is challenging, it turns out that if the function perfectly matches the algebraic structure of the modulo-2 adder MAWC and the joint source distribution fulfills certain conditions, the secrecy computation-capacity *equals* the computation capacity. Thus, the algebraic structure of the channel not only helps to efficiently compute the desired function but also to protect the transmitted source sequences against eavesdropping. It is noteworthy that, to achieve this, the source terminals *do not need* any additional source of randomness nor does the legitimate receiver need any advantage over the eavesdropper. This is in contrast to standard physical-layer security results.

A. Related Work

Considering secure distributed computation, also known as secure multi-party computation, from an information theoretic (i.e., Shannon) perspective is still in its infancy. To the best of the authors' knowledge there exist only some very recent results. For instance, Tyagi et al. introduce a new Shannon theoretic multiuser source model in [7] and [8] and characterize when a function is securely computable. In this context, they provide necessary and sufficient conditions for the existence of protocols that achieve this.

Within the standard secure multi-party computation model of [9], Lee and Abbe determine in [10] the least amount of randomness needed for securely computing a given function. This provides a novel notion of the complexity of a function for its secure computation. In the second part of that paper, the considerations are extended to a probabilistic source model for which the decoding error probability is required to vanish asymptotically in the block length.

In [11], Data et al. take a distributed source coding approach to the problem of securely computing the modulo-2 sum of two distributed binary sources. Similarly to [10], they assume the data to be drawn from some joint memoryless source and derive bounds on the amount of randomness and communication needed to asymptotically achieve secrecy. In [12], the results are extended to arbitrary functions.

All these works are through the lens of source coding, which means that the communication between terminals is assumed to take place over noiseless channels. In this paper, we therefore choose a *joint source-channel coding* perspective.

B. Paper Organization

This paper is organized as follows. Section II introduces the binary modulo-2 adder MAWC and provides the problem statement. In order to obtain some insight, in Section III we focus first on the noiseless case. The noisy case is then considered in Section IV, which also contains a comparison with separation-based schemes. Section V concludes the paper.

C. Notational Remarks

If multiplied by a matrix, a random length- n sequence $X^n := (X_1, \dots, X_n)$ is considered as a column vector. For $p \in [0, 1]$, $H(p) = -p \log_2 p - (1-p) \log_2 (1-p)$ denotes the binary entropy function with the convention $0 \log_2 0 = 0$. The Bernoulli distribution with parameter $p \in [0, 1]$ is denoted as $\text{Bern}(p)$, which means that $X \sim \text{Bern}(p)$ takes on value 1 with probability p . Addition modulo-2 is denoted as \oplus and δ_{ij} represents the Kronecker delta, which is 1 for $i = j$ and 0 otherwise.

II. SYSTEM MODEL AND PROBLEM STATEMENT

Let S_1, \dots, S_M be M binary memoryless sources drawn from a joint probability mass function $P_{S_1 \dots S_M}$. 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 each individual source while keeping the eavesdropper ignorant of them [13]–[15], in this paper the legitimate receiver is interested in reliably and securely computing a Boolean function

$$f : \{0, 1\}^M \rightarrow \{0, 1\}, \quad U = f(S_1, \dots, S_M)$$

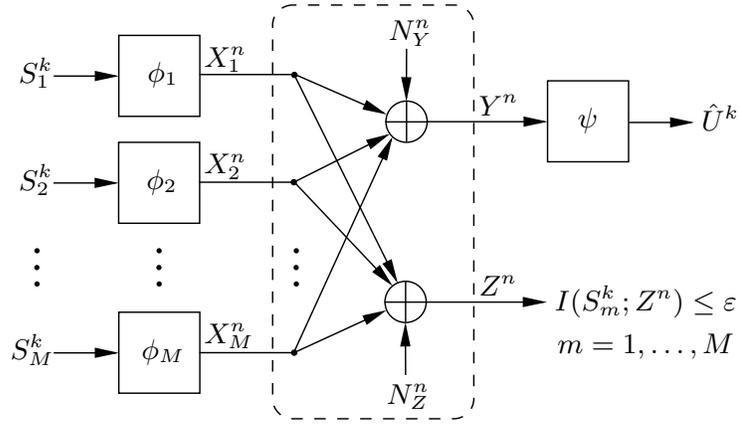


Fig. 1. Secure computation over the binary modulo-2 adder multiple-access wiretap channel: a legitimate receiver wishes to reliably compute a function $U = f(S_1, \dots, S_M)$ of the sources while an eavesdropper has to be kept ignorant of them.

of the sources, to which we refer as the *desired function*.

In particular, as illustrated in Fig. 1, we consider the toy scenario in which the channel between the sources and the destinations can be modeled as a memoryless *binary modulo-2 adder multiple-access wiretap channel*, which is characterized by the input-output relations

$$Y = X_1 \oplus \dots \oplus X_M \oplus N_Y, \quad (1a)$$

$$Z = X_1 \oplus \dots \oplus X_M \oplus N_Z. \quad (1b)$$

Here and hereafter, $X_m \in \{0, 1\}$ is the channel input of source terminal m , Y is the channel output seen by the legitimate receiver and Z the output observed by the eavesdropper, respectively. The noise variables $N_Y \sim \text{Bern}(p)$ and $N_Z \sim \text{Bern}(q)$, for some $p, q \in [0, 1/2]$, are assumed to be independent of the channel inputs.

Remark 1. Note that each of the two multiple-access channels (MACs) in (1) is a modulo-2 adder followed by a binary symmetric channel (BSC).

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

Definition 1. Given a fixed desired function, a (k, n) *computation code* for the binary modulo-2 adder MAWC consists of the following:

- Encoding functions

$$\phi_m : \{0, 1\}^k \rightarrow \{0, 1\}^n, \quad m = 1, \dots, M,$$

each of which maps k source symbols to a length- n codeword (i.e., $\phi_m(s_m^k) = x_m^n$);

- A decoding function at the legitimate receiver

$$\psi : \{0, 1\}^n \rightarrow \{0, 1\}^k,$$

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 of error* of a (k, n) computation code is defined as

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

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

$$I(S_m^k; Z^n), \quad m = 1, \dots, M,$$

which we combine to the single constraint

$$L^{(n)} := I(S_1^k; Z^n) + \cdots + I(S_M^k; Z^n). \quad (2)$$

Definition 2. For some given desired function, a rate $R := k/n$ is said to be an *achievable secrecy computation-rate* if there exists a sequence of (nR, n) computation codes such that

$$\lim_{n \rightarrow \infty} P_e^{(n)} = 0 \quad \text{and} \quad \lim_{n \rightarrow \infty} L^{(n)} = 0.$$

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

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

Since the problem is challenging for arbitrary f , in this paper we focus on securely computing the modulo-2 sum of the source symbols: $f(s_1, \dots, s_M) = s_1 \oplus \cdots \oplus s_M$.

III. THE NOISELESS CASE

First, in order to fix ideas and obtain insight, in this section we consider the noiseless case (i.e., $p = q = 0$), which results in the channel outputs

$$Y = Z = X_1 \oplus X_2 \oplus \cdots \oplus X_M.$$

For a certain class of joint source distributions, we have the following result.

Theorem 1. Let the desired function be the modulo-2 sum and the joint source distribution such that $P_{S_m U} = P_{S_m} P_U$ for all $m = 1, \dots, M$. Then, the secrecy computation-capacity is $C_{\text{sc}} = 1$ function values per channel use.

Proof: (Achievability). Transmitting the source samples *uncoded* results in the channel output sequences

$$Z^k = Y^k = S_1^k \oplus \cdots \oplus S_M^k = U^k$$

and thus in $P_e^{(n)} \equiv 0$. On the other hand, we have

$$I(S_m^k; Z^k) = kI(S_m; Z) = kI(S_m; U).$$

But if $P_{S_m U} = P_{S_m} P_U$, then S_m and U are statistically independent and therefore $I(S_m; U) = 0$. As this applies to all $m = 1, \dots, M$, it follows for the leakage $L^{(n)} \equiv 0$. That is, we are able to reliably compute one function value per channel use while the eavesdropper is not able to obtain any information about the source sequences.

(Converse). If we allow the encoders to fully cooperate, then the sum rate of the MAC in (1a) cannot exceed $\max_{P_{X_1 \dots X_M}} I(X_1, \dots, X_M; Y)$, where $P_{X_1 \dots X_M}$ denotes the joint distribution of the channel inputs. With or without secrecy constraint, we have

$$\begin{aligned} I(U; \hat{U}) &\stackrel{(a)}{\leq} I(X_1, \dots, X_M; Y) \\ &= H(Y) - H(Y|X_1, \dots, X_M) \\ &= H(U) - H(U|S_1, \dots, S_M) \\ &\stackrel{(b)}{=} H(U) \\ &\leq 1, \end{aligned}$$

which is a tight upper bound in our case. Note that (a) follows from the data processing inequality and (b) from the fact that U is a function of S_1, \dots, S_M . ■

Due to the modulo-2 additivity of the channel along with the fact that the desired function perfectly matches this algebraic structure, the source sequences behave like *one-time pads* protecting each other. Thus, the algebraic structure of the channel not only helps to efficiently compute the desired function at the legitimate receiver but also to protect the source sequences against eavesdropping. A remarkable fact is that the source terminals *do not need* any additional source of randomness nor does the legitimate receiver need any advantage over the eavesdropper. This is in stark contrast to standard physical layer security problems in which a legitimate receiver typically wishes to securely decode messages. For instance, when the objective is to securely communicate messages over a MAWC, without local randomness the achievable secrecy rate region would be an empty set [13]–[15].

Remark 2. Note that the coding strategy used in the proof of Theorem 1 achieves *perfect secrecy*. Furthermore, the converse part of the proof implies that for the considered scenario, the secrecy computation-capacity equals the computation capacity C_c . The latter is defined as the supremum over all achievable computation rates (i.e., without secrecy constraints) [1].

It is obvious that independent Bern(1/2) sources fulfill the condition of Theorem 1 (i.e., $P_{S_m U} = P_{S_m} P_U$ for all $m = 1, \dots, M$). Characterizing the set of all joint source distributions that fulfill this condition, however, is a nontrivial problem and beyond the scope of this paper. For the special case $M = 2$, we have the following result.

Theorem 2. Let $U := S_1 \oplus S_2$. Then, $P_{S_m U} = P_{S_m} P_U$, $m = 1, 2$, if and only if $P_{S_1 S_2}$ is doubly symmetric. That is, if and only if $P_{S_1 S_2}$ is of the form

$$P_{S_1 S_2}(s_1, s_2) = \frac{1}{2}(1 - \theta)\delta_{s_1 s_2} + \frac{1}{2}\theta(1 - \delta_{s_1 s_2}), \quad (3)$$

for $\theta \in [0, 1]$.

Proof: The proof is deferred to the Appendix. ■

IV. THE NOISY CASE

Now, we extend our considerations to the noisy case in which parameters p and q can be chosen arbitrarily (see (1)).

A. Computation Capacity vs. Secrecy Computation-Capacity

Before presenting the main result of this paper, we recap a result that provides the computation capacity of the binary modulo-2 adder MAC given in (1a).

Theorem 3 (Nazer-Gastpar [1]). Let f be the modulo-2 sum. Then, the computation capacity of the binary modulo-2 adder MAC (1a) is given by

$$C_c = \frac{C}{H(U)} = \frac{1 - H(p)}{H(U)},$$

where C denotes the capacity of a BSC with crossover probability p .

For the achievability part of the proof, Nazer and Gastpar employ random linear code ensembles for source compression and channel coding. By following their approach, we are able to extend Theorem 1 to the following.

Theorem 4. Let f be the modulo-2 sum and the joint source distribution such that $P_{S_m U} = P_{S_m} P_U$ for all $m = 1, \dots, M$. Then, the secrecy computation-capacity of the binary modulo-2 adder MAWC is

$$C_{sc} = C_c = \frac{1 - H(p)}{H(U)}.$$

Proof: (Achievability). Let $C = 1 - H(p)$ denote the capacity of a BSC with crossover probability $p \in [0, 1/2]$.

- *Code construction:* Generate two matrices $A \in \{0, 1\}^{n \times \ell}$ and $B \in \{0, 1\}^{\ell \times k}$, each entry drawn uniformly and independently at random, with

$$kH(U) < \ell < nC. \quad (4)$$

Reveal A and B to the source terminals, the legitimate receiver, and the eavesdropper.

- *Encoding:* Given s_m^k at source terminal m , transmit

$$x_m^n = \phi_m(s_m^k) = ABs_m^k, \quad (5)$$

where all operations are carried out modulo-2.

With this encoding rule, the legitimate receiver observes the sequence of channel output symbols

$$\begin{aligned} Y^n &= X_1^n \oplus \dots \oplus X_M^n \oplus N_Y^n \\ &= ABS_1^k \oplus \dots \oplus ABS_M^k \oplus N_Y^n \\ &= AB \underbrace{(S_1^k \oplus \dots \oplus S_M^k)}_{=U^k} \oplus N_Y^n. \end{aligned} \quad (6)$$

Effectively, (6) is a BSC with crossover probability p . The random linear code induced by generator matrix A therefore has the objective of protecting BU^k against the noise N_Y^n , whereas the linear code induced by B is used to compress U^k to its entropy. As long as condition (4) is fulfilled, there exist decoding functions $\psi' : \{0, 1\}^n \rightarrow \{0, 1\}^\ell$ and $\psi'' : \{0, 1\}^\ell \rightarrow \{0, 1\}^k$ such that for arbitrary $\varepsilon > 0$ and n large enough, the average probabilities of error (averaged over A and B) fulfill $\mathbb{P}(\psi'(Y^n) \neq BU^k) < \frac{\varepsilon}{2}$ and $\mathbb{P}(\psi''(BU^k) \neq U^k) < \frac{\varepsilon}{2}$. This was shown in [1] based on results from [16] and [17]. Thus, defining the decoding function of Definition 1 as

$$\psi(y^n) := (\psi'' \circ \psi')(y^n),$$

by means of the union of events bound we have $P_e^{(n)} < \varepsilon$ as long as $R = \frac{k}{n} < \frac{C}{H(U)}$ and n sufficiently large.

Now, we analyze the leakage. As in the proof of Theorem 1, we consider each term of $L^{(n)}$ separately. Towards this end,

$$\begin{aligned} I(S_m^k; Z^n | A, B) &= I(S_m^k; ABU^k \oplus N_Z^n | A, B) \\ &\leq I(S_m^k; ABU^k \oplus N_Z^n, U^k | A, B) \\ &= I(S_m^k; U^k | A, B) + I(S_m^k; ABU^k \oplus N_Z^n | A, B, U^k) \\ &= I(S_m^k; U^k) + I(S_m^k; N_Z^n | U^k) \\ &= 0, \end{aligned}$$

where the last equality follows from the assumption $P_{S_m U} = P_{S_m} P_U$, the memorylessness of the sources, and the independence of S_m and N_Z . As this applies to all $m = 1, \dots, M$, we have $L^{(n)} \equiv 0$.

(Converse). For the average probability of error, $P_e^{(n)}$, to vanish with increasing block length, with or without a secrecy constraint every computation code has to fulfill

$$kH(U) \leq I(U^k; \hat{U}^k) \quad (7)$$

$$\begin{aligned} &\stackrel{(a)}{\leq} I(X_1^n, \dots, X_M^n; Y^n) \\ &\leq \max_{P_{X_1, \dots, X_M}} I(X_1^n, \dots, X_M^n; Y^n) \\ &= n(1 - H(p)), \end{aligned} \quad (8)$$

where (a) is due to the data processing inequality. Combining the left hand side of (7) with (8) results in the upper bound $R = \frac{k}{n} \leq \frac{1-H(p)}{H(U)}$, which is tight in our case. ■

Remark 3. It has to be emphasized that the secrecy computation-capacity of Theorem 4 is independent of the MAC between the source terminals and the eavesdropper (i.e., independent of q). Note also that *perfect secrecy* is achieved.

Surprisingly, the sequence of linear random codes that achieves the computation capacity also achieves the secrecy computation-capacity. No additional source of randomness is needed at the encoders as in the noisy case the source sequences act as one-time pads as well.

B. Comparison with Separation-Based Computation

Consider the case $M = 2$ and let (S_1, S_2) be a doubly symmetric source with joint probability mass function given by (3). By means of this explicit example, in this subsection we compare Theorem 4 with the secrecy computation-rate that is achievable with a separation-based coding scheme. A separation-based scheme first distributively compresses the source sequences into messages and then uses a capacity achieving MAC code in order to reliably reconstruct the messages at the legitimate receiver. Once \hat{S}_1^k and \hat{S}_2^k are known to the legitimate receiver it computes $\hat{U}^k = \hat{S}_1^k \oplus \hat{S}_2^k$, resulting in an estimate of the sequence of function values.

For this scenario, in [1] it is shown that the best possible computation rate (i.e., without secrecy constraint) achievable with separation is

$$R = \frac{1}{2} \left(\frac{1 - H(p)}{H(\theta)} \right). \quad (9)$$

The rate can be achieved with Körner-Marton compression for U [18] in combination with time-sharing.¹ Compared with Theorem 3, this rate is only half the computation capacity. Because of time-sharing, however, when adding secrecy constraints the other source sequences may not act as one-time pads any longer so that local randomness has to be used at the encoders in order to confuse the eavesdropper.

Theorem 5. Let $M = 2$, f be the modulo-2 sum, and the joint source distribution as given in (3). Furthermore, let $p \in [0, 1/2)$ and $q = q'(1 - 2p) + p$ for some $q' \in (0, 1/2]$. Then, for the binary modulo-2 adder MAWC, the best secrecy computation-rate achievable with separation is

$$R = \frac{1}{2} \left(\frac{H(q) - H(p)}{H(\theta)} \right). \quad (10)$$

Proof: (Achievability). As in the achievability part of the proof of Theorem 4, the source terminals use the same linear random code for compressing U to its entropy $H(U) = H(\theta)$. In [18], Körner and Marton show that this is optimal for the joint source distribution given in (3). Now, using time-sharing, the legitimate receiver alternately observes the channel outputs

$$Y' = X_1 \oplus N_Y \quad \text{and} \quad Y'' = X_2 \oplus N_Y \quad (11)$$

while the eavesdropper sees

$$Z' = X_1 \oplus N_Z \quad \text{and} \quad Z'' = X_2 \oplus N_Z. \quad (12)$$

Thus, for each channel use we effectively have a binary symmetric wiretap channel of secrecy capacity

$$\begin{aligned} C(p) - C(q) &= 1 - H(p) - (1 - H(q)) \\ &= H(q) - H(p), \end{aligned}$$

¹Note that for the two MACs given in (1), time-sharing is optimal.

where $C(q)$ denotes the capacity of the BSCs in (11) and $C(p)$ the capacity of the BSCs in (12), respectively.² Thus, using standard wiretap coding allows $P_e^{(n)}$ and $L^{(n)}$ to be driven to zero as long as the sum rate fulfills

$$k2H(\theta) < n(H(q) - H(p)) ,$$

which provides the rate in (10).

(*Converse*). It can easily be checked that for $p \in [0, 1/2)$ and $q' \in (0, 1/2]$, the condition $q = q'(1 - 2p) + p$ implies an eavesdropper channel that is physically degraded with respect to the legitimate receiver's channel. In this case, the secrecy capacity region of the two-user binary modulo-2 adder MAWC is given by all rate pairs

$$\{(R_1, R_2) \in \mathbb{R}_+^2 \mid R_1 + R_2 < H(q) - H(p)\} ,$$

which follows from [19, Th. 1]. Thus, time-sharing in combination with single-user wiretap coding is optimal. ■

After comparing (10) with (9), we conclude that separation-based computation schemes generally suffer from imposing a secrecy constraint. In order to keep the source sequences secret from the eavesdropper, wiretap coding is needed and therefore local randomness at the encoders. This generally further reduces the achievable computation rate.

V. CONCLUSION

We have considered the problem of securely computing a function of distributed sources over the binary modulo-2 adder MAWC. Instead of individual source samples, the legitimate receiver is interested in reliably decoding from the channel output a function of the sources. To characterize the corresponding fundamental limit, we have introduced the notion of secrecy computation-capacity and determined it for a function that perfectly matches the structure of the channel. Unlike standard results in physical-layer security, no additional randomness is needed in order to confuse the eavesdropper.

Future work includes extensions to more general functions and MAWCs as well as to the case in which the joint source distribution does not fulfill the condition $P_{S_m U} = P_{S_m} P_U$, $m = 1, \dots, M$. On the other hand, the leakage in (2) might be replaced by another secrecy criterion such as $L^{(n)} = I(U^k; Z^n)$. This criterion is less restrictive as it prohibits the eavesdropper only from knowing anything about the function to be computed at the legitimate receiver.

APPENDIX PROOF OF THEOREM 2

Let $U := S_1 \oplus S_2$. We have to show that $P_{S_m U} = P_{S_m} P_U$, for $m = 1, 2$, if and only if the joint source distribution, $P_{S_1 S_2}$, is doubly symmetric. That is, if and only if both of the equalities

$$P_{S_1 S_2}(0, 0) = P_{S_1 S_2}(1, 1) , \tag{13a}$$

$$P_{S_1 S_2}(0, 1) = P_{S_1 S_2}(1, 0) \tag{13b}$$

hold. As the “ \Leftarrow ” part is trivial, we treat the “ \Rightarrow ” part only.

Note that for $P_{S_m U} = P_{S_m} P_U$ to be true, the following set of equations has to be fulfilled:

$$P_{U|S_m}(0|0) = P_{U|S_m}(0|1) , \tag{14a}$$

$$P_{U|S_m}(1|0) = P_{U|S_m}(1|1) , \tag{14b}$$

²For $p \in [0, 1/2)$ and $q' \in (0, 1/2]$, $q = q'(1 - 2p) + p > p$ and therefore $H(q) > H(p)$.

for $m = 1, 2$. As $u = 0$ if and only if $(s_1, s_2) = (0, 0)$ or $(s_1, s_2) = (1, 1)$ and $u = 1$ if and only if $(s_1, s_2) = (0, 1)$ or $(s_1, s_2) = (1, 0)$, the conditions in (14) can equivalently be expressed as

$$\frac{P_{S_1 S_2}(0, 0)}{P_{S_1}(0)} = \frac{P_{S_1 S_2}(1, 1)}{1 - P_{S_1}(0)}, \quad (15a)$$

$$\frac{P_{S_1 S_2}(0, 1)}{P_{S_1}(0)} = \frac{P_{S_1 S_2}(1, 0)}{1 - P_{S_1}(0)}, \quad (15b)$$

$$\frac{P_{S_1 S_2}(0, 0)}{P_{S_2}(0)} = \frac{P_{S_1 S_2}(1, 1)}{1 - P_{S_2}(0)}, \quad (15c)$$

$$\frac{P_{S_1 S_2}(0, 1)}{1 - P_{S_2}(0)} = \frac{P_{S_1 S_2}(1, 0)}{P_{S_2}(0)}. \quad (15d)$$

Solving this system of equations subject to the constraints

$$\begin{aligned} P_{S_1}(s_1) &= P_{S_1 S_2}(s_1, 0) + P_{S_1 S_2}(s_1, 1), \\ P_{S_2}(s_2) &= P_{S_1 S_2}(0, s_2) + P_{S_1 S_2}(1, s_2) \end{aligned}$$

results in

$$P_{S_1}(0) = P_{S_2}(1) = P_{S_2}(0) = P_{S_2}(1) = 1/2$$

and thus in Bern(1/2) marginals. Inserting this into (15) provides (13), which concludes the proof.

REFERENCES

- [1] B. Nazer and M. Gastpar, "Computation over multiple-access channels," *IEEE Trans. Inf. Theory*, vol. 53, no. 10, pp. 3498–3516, Oct. 2007.
- [2] 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.
- [3] 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.
- [4] N. Karamchandani, U. Niesen, and S. Diggavi, "Computation over mismatched channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 4, pp. 666–677, Apr. 2013.
- [5] 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.
- [6] C.-Y. Wang, S.-W. Jeon, and M. Gastpar, "Interactive computation of type-threshold functions in collocated Gaussian networks," *IEEE Trans. Inf. Theory*, vol. 61, no. 9, pp. 4765–4775, Sep. 2015.
- [7] 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.
- [8] H. Tyagi, "Distributed function computation with confidentiality," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 4, pp. 691–701, Apr. 2013.
- [9] A. C. Yao, "Protocols for secure computations," in *Proc. 23rd Annu. Symp. Found. Comput. Sci. (SFCS)*, Chicago, IL, USA, Nov. 1982, pp. 160–164.
- [10] E. J. Lee and E. Abbe, "Two Shannon-type problems on secure multi-party computations," in *Proc. 52nd Annu. Allerton Conf. Commun., Control, Computing*, Monticello, IL, USA, Oct. 2014, pp. 1287–1293.
- [11] D. Data, B. K. Dey, M. Mishra, and V. M. Prabhakaran, "How to securely compute the modulo-two sum of binary sources," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Hobart, Australia, Nov. 2014, pp. 496–500.
- [12] D. Data and V. M. Prabhakaran, "On coding for secure computing," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Hong Kong, Jun. 2015, pp. 2737–2741.
- [13] 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.
- [14] 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.
- [15] 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.
- [16] P. Elias, "Coding for noisy channels," *IRE Conv. Rec.*, vol. 4, pp. 37–46, 1955.
- [17] A. D. Wyner, "Recent results in the Shannon theory," *IEEE Trans. Inf. Theory*, vol. 20, no. 1, pp. 2–10, Jan. 1974.
- [18] J. Körner and K. Marton, "How to encode the modulo-two sum of binary sources," *IEEE Trans. Inf. Theory*, vol. 25, no. 2, pp. 219–221, Mar. 1979.
- [19] B. Dai and Z. Ma, "Some new results on the multiple-access wiretap channel," *Entropy*, vol. 16, no. 8, pp. 4693–4712, Aug. 2014.