Secure Computation Based on Leaky Correlations: High Resilience Setting

Alexander R. Block(✉), Hemanta K. Maji, and Hai H. Nguyen

Department of Computer Science, Purdue University, West Lafayette, IN 47906, USA
{block9,hmaji,nguye245}@cs.purdue.edu

Abstract. Correlated private randomness, or correlation in short, is a fundamental cryptographic resource that helps parties compute securely over their private data. An offline preprocessing step, which is independent of the eventual secure computation, generates correlated secret shares for the parties and the parties use these shares during the final secure computation step. However, these secret shares are vulnerable to leakage attacks.

Inspired by the quintessential problem of privacy amplification, Ishai, Kushilevitz, Ostrovsky, and Sahai (FOCS 2009) introduced the concept of correlation extractors. Correlation extractors are interactive protocols that take leaky correlations as input and produce secure independent copies of oblivious transfer (OT), the building blocks of secure computation protocols. Although their initial feasibility result is resilient to linear leakage and produces a linear number of "fresh" OTs, the constants involved are minuscule. The output of this correlation extractor can be used to perform only small secure computation tasks, because the number of OTs needed to evaluate a functionality securely is roughly proportional to its circuit size. Recently, Gupta, Ishai, Maji, and Sahai (CRYPTO 2015) constructed an extractor that is resilient to 1/4 fractional leakage and has near-linear production rate. They also constructed an extractor from a large correlation that has 1/2 fractional resilience but produces only one OT, which does not suffice to compute even constant size functionalities securely.

In this paper, we show the existence of a correlation that produces n-bit shares for the parties and allows the extraction of $n^{1-o(1)}$ secure OTs, despite $n/2$ bits of leakage. The key technical idea is to embed several multiplications over a field into one multiplication over an extension field. The packing efficiency of this embedding directly translates into the production rate of our correlation extractor. Our work establishes a connection between this problem and a rich vein of research in additive combinatorics on constructing dense sets of integers that are free of arithmetic progressions, a.k.a. 3-free sets. We introduce a new combinatorial problem that suffices for our multiplication embedding, and produces concrete embeddings that beat the efficiency of the embeddings inspired by the reduction to 3-free sets.

A.R. Block, H.K. Maji and H.H. Nguyen—The research effort is supported in part by an NSF CRII Award CNS–1566499, an NSF SMALL Award CNS–1618822, and an REU CNS–1724673.

J. Katz and H. Shacham (Eds.): CRYPTO 2017, Part II, LNCS 10402, pp. 3–32, 2017.
DOI: 10.1007/978-3-319-63715-0_1

Finally, the paper introduces a graph-theoretic measure to upper-bound the leakage resilience of correlations, namely the *simple partition number*. This measure is similar in spirit to graph covering problems like the biclique partition number. If the simple partition number of a correlation is 2^λ, then it is impossible to extract even one OT if parties can perform λ-bits of leakage. We compute tight estimates of the simple partition number of several correlations that are relevant to this paper, and, in particular, show that our extractor and the extractor for the large correlation by Gupta et al. have optimal leakage resilience and (qualitatively) optimal simulation error.

1 Introduction

Secure multi-party computation [22,71] helps mutually distrusting parties to compute securely over their private data. Unfortunately, it is impossible to securely compute most functionalities in the information-theoretic plain model even against parties who honestly follow the protocol but are curious to find additional information about the other parties' private input [2,19,32,38,41–43]. However, we can securely compute any functionality if honest parties are in the majority [5,12,16,56], parties use some trusted setup [10,11,17,23,35,37,49] or correlated private randomness [15,39,44,68], or there are bounds on the computational power of the parties [22,35].

The study of secure computation using correlated private randomness, primarily initiated due to efficiency concerns, has produced several success stories, for example FairPlay [4,45], TinyOT [50] and SPDZ [18] (pronounced Speedz). These secure computation protocols offload most of the computational and cryptographic complexity to an offline preprocessing phase. During this preprocessing phase, a trusted dealer samples two shares (r_A, r_B) from the joint distribution (R_A, R_B), namely the *correlated private randomness*, or *correlation* in short, and provides the secret shares r_A to Alice and r_B to Bob. During the online secure computation phase, parties use their respective secret shares in an interactive protocol to securely compute the intended functionality. Note that the preprocessing phase is independent of the functionality or the inputs fed to the functionality by the parties.

A prominent and extremely well-studied correlation is the *random oblivious transfer correlation*, represented by ROT. It samples three bits x_0, x_1, b independently and uniformly at random, and provides the secret shares (x_0, x_1) to Alice and (b, x_b) to Bob. Note that Alice does not know the choice bit b, and Bob does not know the other bit $x_{\overline{b}}$. Intuitively, ROT is an input-less functionality that implements a randomized version of *oblivious transfer* functionality, where the sender sends (x_0, x_1) as input to the functionality and the receiver picks x_b out of the two input bits. Given m independent samples from this distribution, parties can securely compute any functionality with circuit complexity (roughly) m. For example, we can utilize the randomized self-reducibility of oblivious transfer to reimagine the GMW protocol [22] in this framework naturally.

However, the storage of the secret shares by the parties brings to fore several vulnerabilities. For instance, parties can leak additional information from the secret shares of the other parties. We emphasize that the leakage need not necessarily reveal individual bits of the other party's share. The leakage can be on the entire share and encode crucial global information that can potentially jeopardize the security of the secure computation protocol.

To address these concerns, Ishai, Kushilevitz, Ostrovsky, and Sahai [33] introduced the notion of *correlation extractors*. Correlation extractors distill leaky correlations into independent samples of the ROT correlation that are secure. That is, for each of the new samples Alice does not know Bob's choice bit and Bob does not know Alice's other bit. This problem is a direct analog of the quintessential problems of privacy amplification and randomness extraction problems in the secure computation setting. With the exception that, correlation extractors ensure security against insider attacks, i.e., the parties who perform the leakage are participants in the secure protocol itself. This additional requirement makes the task of correlation extraction significantly more challenging. It is, thus, not surprising that relatively few results are known in the field of correlation extractor construction.

For example, in the setting of privacy amplification, if Alice and Bob start with a secret n-bit random string then, in the presence of t-bits of arbitrary leakage to an eavesdropper, parties can re-establish a fresh m-bit secret key such that the advantage of the eavesdropper in guessing the secret key is roughly $2^{-\Delta} \approx 2^{-(n-t-m)}$. Intuitively, the sum of "entropy deficiency" (t), "entropy of production" (m), and "$-\log$ of the adversarial advantage" (Δ) is roughly n, the initial entropy of the secret. Analogous results also exist in the setting of randomness extraction, where we can extract nearly all of the min-entropy of a source. But similar tight extraction results are not known for correlation extractors. In fact, the task of designing correlations that simultaneously support high leakage resilience and production rate with exponential security has been elusive.

The number of the output ROT samples and their high security are crucial for the secure computation protocol. For example, protocols with exponential security can reduce the ROT production or increase the statistical security parameter only slightly to prohibitively increase the effort needed by adversaries to

	Correlation Description	Number of OTs Produced (m)	Number of Leakage bits (t)	Simulation Error (ε)	Round Complexity
IKOS [33]	$\mathsf{ROT}^{n/2}$	αn	βn	$2^{-\gamma n}$	4
GIMS [26]	$\mathsf{ROT}^{n/2}$	$n/\operatorname{poly}\log n$	$(1/4 - g)n$	$2^{-gn/m}$	2
	$\mathsf{IP}\,(\mathbb{GF}\,[2]^n)$	1	$(1/2 - g)n$	2^{-gn}	2
Our Work	$\mathsf{IP}\left(\mathbb{F}^{n/\log\lvert\mathbb{F}\rvert}\right)$	$n^{1-o(1)}$	$(1/2 - g)n$	2^{-gn}	2

Fig. 1. A qualitative summary of prior relevant works in correlation extractors and a comparison to our correlation extractor construction. All correlations have been normalized so that each party gets an n-bit secret share. The positive constants α, β, and γ are minuscule. And $g < 1/2$ is an arbitrary positive constant.

break them. Furthermore, the number of these ROT samples limit the size of the eventual functionality that can be securely computed, because the number of ROT samples needed to implement a functionality securely is directly proportional to its circuit size. As highlighted in [26], the initial feasibility result of Ishai et al. [33], though asymptotically linear in leakage resilience and production rate, has unsatisfactorily low resilience and production rate for realistic values of n, the size of the original share of the parties. The subsequent work of Gupta et al. [26], improves the resilience to (roughly) $n/4$ but trades-off the security of the protocol for high production rate and, consequently, achieves only negligible (and, not exponentially low) insecurity. They also consider a new correlation, namely the *inner-product correlation* where the secret shares of the parties are random n-bit binary vectors subject to the constraint that they are orthogonal to each other.[1] They construct a correlation extractor for the inner-product correlation with resilience $n/2$ and exponential security. However, it is inherently limited to producing one ROT sample as output, which is not adequate for the end goal of performing interesting secure computations. Our work shows that the inner-product correlation over an *appropriately large field* admits a correlation extractor that is resilient to $n/2$ bits of leakage, has high concrete production rate, and has exponentially high security. Figure 1 summarizes the entire preceding discussion tersely. Finally, similar to Gupta et al. [26], although our construction is stated in the information-theoretic setting, it is also relevant to the setting where computationally secure protocol generate the correlations or use the output OTs.

However, is the upper-bound of $n/2$ resilience inherent to the inner-product correlation? For example, $n/2$ samples of the ROT correlation cannot be resilient to more than $n/4$ bits of leakage. A partition argument can demonstrate this upper bound of the maximum resilience of this correlation [34]. In this partition argument, Alice emulates the generation of $n/4$ (i.e., half of $n/2$) independent samples (x_0, x_1) and (c, x_c) from the ROT correlation and sends the corresponding (c, x_c) to Bob. Moreover, Bob emulates the generation of the remaining $n/4$ samples and sends the corresponding (x_0, x_1) shares to Alice. Finally, we reimagine any correlation extractor that is resilient to $n/4$ bits of leakage and produces even one secure ROT sample as a secure ROT protocol in the plain model where Alice implements $n/4$ ROT samples, and Bob implements the remaining $n/4$ ROT samples; which is impossible. Typically, the partition argument applies to "multiple independent samples of small correlations," but its extension to one huge global correlation is not apparent.

To address this question, we introduce a new graph-theoretic measure for the maximum resilience of a correlation, namely its *simple partition number*. In particular, a correlation with simple partition number $\leqslant 2^\lambda$ cannot be resilient to λ

[1] The actual inner-product correlation is defined slightly differently. Parties get shares $(x_0, x_1, \ldots, x_n)$ and $(y_0, y_1, \ldots, y_n)$ such that $x_0 + y_0 = \sum_{i=1}^{n} x_i y_i$. That is, x_0 and y_0 are additive secret shares of the inner product of $(x_1, \ldots, x_n)$ and $(y_1, \ldots, y_n)$. But for intuition, it suffices to consider the correlation where the secret shares of the parties are orthogonal vectors instead.

Correlation Description	Secret Share Size (s)	Simple Partition Number (sp)	Upper Bound on the Max. Fractional Leakage ($\log \mathsf{sp}/s$)
$\mathsf{ROT}^{n/2}$	n	$2^{n/4}$	1/4
$\mathsf{ROLE}\,(\mathbb{F})^{n/2}$	$n \log \lvert\mathbb{F}\rvert$	$\lvert\mathbb{F}\rvert^{n/4}$	1/4
$\mathsf{IP}\,(\mathbb{F}^n)$	$n \log \lvert\mathbb{F}\rvert$	$\lvert\mathbb{F}\rvert^{n/2}$	1/2

Fig. 2. A summary of the estimates of the simple partition number for the correlations relevant to our work.

bits of leakage (refer to Fig. 2 for a summary of these estimates). Finally, we prove the optimality of the resilience demonstrated by the correlation extractors for the inner-product correlation presented in [26] and our work. Refer to Sect. 5.7 for a discussion on how the relation between simple partition number and maximum resilience is similar to the connection between biclique partition number and Wyner's common information [69]. The existence of correlation extractors for a slightly lesser amount of leakage implies the tightness of our upper bounds on leakage resilience. Finally, we leverage the simple partition number bounds and use an averaging argument to show that the decay in simulation security with entropy gap as achieved by [26] and our correlation extractor are qualitatively optimal.

1.1 Model

This section presents the standard model of Ishai et al. [33] for correlation extractors, which subsequent works also use. We consider 2-party semi-honest secure computation in the preprocessing model. In the preprocessing step, a trusted dealer draws a sample (r_A, r_B) from the joint distribution (R_A, R_B). The joint distribution (R_A, R_B) is referred to as the correlated private randomness, and r_A and r_B, respectively, are the secret shares of Alice and Bob. The dealer provides the secret share r_A to Alice and r_B to Bob. An adversarial party can perform arbitrary t-bits of leakage on the secret share of the other party at the end of the preprocessing step. We represent this leaky correlation hybrid as $(R_A, R_B)^{[t]}$.[2]

In the leaky correlation $(R_A, R_B)^{[t]}$ hybrid, during the secure computation phase, parties perform an interactive protocol to realize their target functionality securely. No leakage occurs during the execution of the secure computation protocol. In this work, we consider the functionality that implements m independent oblivious transfers between the parties, referred to as the OT^m functionality.

Definition 1 (Correlation Extractor). *Let (R_A, R_B) be a correlated private randomness such that the secret share size of each party is n-bits.*

[2] That is, the functionality samples secret shares (r_A, r_B) according to the correlation (R_A, R_B). The adversarial party sends a t-bit leakage function $\mathcal{L}$ to the functionality and receives the leakage $\mathcal{L}(r_A, r_B)$ from the functionality. The functionality sends r_A to Alice and r_B to Bob. Note that the adversary does not need to know its secret share to construct the leakage function because the leakage function gets the secret shares of both parties as input.

An (n, m, t, ε)-correlation extractor for (R_A, R_B) *is a two-party interactive protocol in the* $(R_A, R_B)^{[t]}$ *hybrid that securely implements the* OT^m *functionality against information-theoretic semi-honest adversaries with* ε*-simulation error.*

1.2 Our Contribution

Our work makes a two-fold contribution regarding correlation extractors. First, we construct a highly resilient correlation extractor that produces a large number of secure OTs as output and has exponential security. Finally, we provide a general graph-theoretic measure that upper bounds the maximal resilience of any correlation.

Correlation Extraction Construction. For any field $(\mathbb{F}, +, \cdot)$, the *inner-product correlation over* $\mathbb{F}^{n+1}$, represented by $\mathsf{IP}\left(\mathbb{F}^{n+1}\right)$, is a correlation that samples random $r_A = (x_0, x_1, \ldots, x_n) \in \mathbb{F}^{n+1}$ and $r_B = (y_0, y_1, \ldots, y_n) \in \mathbb{F}^{n+1}$ such that $x_0 + y_0 = \sum_{i=1}^{n} x_i y_i$. That is, x_0 and y_0 are the additive secret shares of the inner product of $x_{[n]} := (x_1, \ldots, x_n)$ and $y_{[n]} := (y_1, \ldots, y_n)$. Gupta et al. [26] consider a special case of the inner-product correlation, where $\mathbb{F} = \mathbb{GF}[2]$. Note that each party receives $(n + 1)$ field elements as its secret share. In particular, if $\mathbb{F} = \mathbb{GF}[2^a]$, then each party gets an $a(n + 1)$-bit secret share.

Theorem 1 (High Resilience High Production Correlation Extractor). *For all constants* $0 < \delta < g < 1/2$*, there exists a correlation* (R_A, R_B)*, where each party gets* n*-bit secret share, such that there exists a two-round* (n, m, t, ε)*-correlation extractor for* (R_A, R_B)*, where* $m = (\delta n)^{1-o(1)}$*,* $t = (1/2 - g)n$*, and* $\varepsilon = 2^{-(g-\delta)n/2}$*.*

We use $(R_A, R_B) = \mathsf{IP}\left(\mathbb{GF}\left[2^{\delta n}\right]^{1/\delta}\right)$ in this theorem. Note that we maintain the dependence on δ explicitly in the theorem statement to enable computation of concrete efficiency. As we shall see later, this theorem achieves high production rate of $(\delta n)^{\log 10/\log 38} \approx (\delta n)^{0.633}$ even for realistic values of n. The simulation error is exponentially low in the difference between the entropy gap gn and the parameter δn. Our construction achieves $(\delta n)^{1-o(1)}$ production asymptotically, which is close to the ideal target of δn production. Qualitatively, the decay in our simulation error is near optimal as demonstrated by Theorem 2 and Corollary 1.

The crux of our construction is the composition of two technical contributions. First, we observe that the correlation extractor for $\mathsf{IP}\left(\mathbb{GF}[2]^n\right)$ constructed by Gupta et al. [26] extends to the $\mathsf{IP}\left(\mathbb{F}^{1/\delta}\right)$ correlation, where $\mathbb{F}$ is a large field. However, in this case, instead of producing a secure OT, it produces a generalization of oblivious transfer, namely *oblivious linear-function evaluation over* $\mathbb{F}$ [68] (represented as $\mathsf{OLE}(\mathbb{F})$). An oblivious linear-function evaluation is a 2-party functionality that takes $(A, B) \in \mathbb{F}^2$ as input from Alice and $X \in \mathbb{F}$ as input from Bob, and provides $Z = AX + B$ as output to Bob. Note that oblivious transfer is equivalent to oblivious linear-function evaluation over $\mathbb{GF}[2]$, because $x_b = (x_1 - x_0)b + x_0$, for $x_0, x_1, b \in \mathbb{GF}[2]$.

Finally, we embed m OT evaluations simultaneously into one $\mathsf{OLE}(\mathbb{F})$ evaluation. Note that, this is *not* an asymptotic reduction. Asymptotically, there are several techniques to construct multiple copies of OT using multiple copies of OLE at a good rate. Our focus is on securely implementing multiple OT evaluations from *only one* $\mathsf{OLE}(\mathbb{F})$ evaluation. Development of more efficient embeddings will directly improve the production rate of our construction. We demonstrate that dense sets of integers that avoid any arithmetic progressions, 3-free sets, provide such embedding of multiplications. We formulate a relaxed version of this combinatorial problem (see Fig. 5) that suffices for our embedding problem and obtain more efficient embeddings than those that are inspired by the 3-free set constructions.

We emphasize that although we state our correlation extractor for the bounded leakage model, i.e. an adversary can perform at most t-bits of leakage, it also extends to the noisy leakage setting. As long as the noise is high enough to maintain $(n-t)$ bits of (average) min-entropy in the secret share of the parties, our extractor construction remains secure.

Bound on the Maximum Resilience. The construction of Theorem 1 and the correlation extractor of Gupta et al. [26], with fractional resilience 1/2, lead naturally to a fascinating question. Can there exist a correlation extractor for $\mathsf{IP}(\mathbb{F}^n)$ that achieves over 1/2 fractional resilience? In fact, more generally, can we meaningfully upper-bound the maximum leakage resilience of an arbitrary correlation?

Note that if parties obtain multiple independent samples from identical correlations, then the partition argument can be leveraged to deduce an upper bound. For example, either Alice or Bob by getting adequate information on half of the other party's secret shares can break the security of the correlation extractor protocol. As discussed earlier, this argument implies that the correlation $\mathsf{ROT}^{n/2}$ is not resilient to $\lceil n/4 \rceil$ bits of leakage, because every ROT hides only one bit of information from each party [34]. However, this approach does not apply to correlation extractors for secret shares drawn from one large correlation, for example, $\mathsf{IP}(\mathbb{F}^n)$. We prove the following main result.

Theorem 2 (Hardness of Correlation Extraction). *Let $(\mathbb{F}, +, \cdot)$ be an arbitrary field. There exists a universal constant $\varepsilon^* > 0$ such that, for $(R_A, R_B) = \mathsf{IP}(\mathbb{F}^k)$, any $(n, 1, (n/k)\lceil (k+1)/2 \rceil, \varepsilon)$-correlation extractor for (R_A, R_B) has $\varepsilon \geqslant \varepsilon^*$, where $n = k \log |\mathbb{F}|$.*

This result proves the optimality of the leakage resilience achieved by our extractor in Theorem 1 and the correlation extractor for $\mathsf{IP}(\mathbb{GF}[2]^n)$ proposed by Gupta et al. [26]. In fact, a more general version of this result (using averaging arguments) shows that any $(n, 1, n/2 - gn, \varepsilon)$-correlation extractor for $\mathsf{IP}(\mathbb{F}^k)$ has $\varepsilon \geqslant \varepsilon^* 2^{-gn}$ (see Corollary 1). This result proves the qualitative optimality of simulation error achieved by these two correlation extractors.

The technical heart of this result is a new graph-theoretic measure for maximum leakage resilience in correlations, namely *simple partition number*

(see Definition 4 in Sect. 2). Theorem 2 is a consequence of precise estimation of this quantity for the $\mathsf{IP}(\mathbb{F}^n)$ correlation. This quantity is similar in spirit to the biclique partition number of a graph [24,25], the minimum number of bicliques needed to partition the edges of a graph. Moreover, the connection of simple partition number to maximum resilience is intuitively analogous to the link between biclique partition number and Wyner's common information [69]. Section 5.7 provides details on this connection.

1.3 Prior Relevant Works

This work lies at the intersection of several fields like correlation extractors, additive combinatorics, graph covering problems, and information theory. In this section, we provide only a summary of the work on combiners and extractors. The prior relevant works related to the remaining topics are covered in appropriate sections later.

Combiners and Extractors. A closely related concept is the notion of OT combiners, which are a restricted variant of OT extractors in which the leakage is limited to local information about individual OT correlations, and there is no global leakage. The study of OT combiners was initiated by Harnik et al. [28]. Since then, there has been work on several variants and extensions of OT combiners [27,35,47,48,55]. Recently, Ishai et al. [34] constructed OT combiners with nearly optimal leakage parameters. However, combiners consider a restricted variant of leakage where the leakage function leaks only individual bits of the secret shares.

To address general leakage, Ishai, Kushilevitz, Ostrovsky, and Sahai [33], proposed the notion of correlation extractors. Their construction has a linear leakage resilience, production rate, and exponential security. However, as indicated by Gupta et al. [26], all the constants involved are minuscule. To address this concern, they [26] construct correlation extractor for $\mathsf{ROT}^{n/2}$ that has optimal leakage resilience with only a negligible (not exponentially-low) simulation error. They also provide a correlation extractor construction from a large correlation that exhibits 1/2 leakage resilience but outputs only one OT. Our work will achieve (roughly) the best of both these constructions, i.e., fractional resilience 1/2, (near) linear production rate, and exponential security.

1.4 Technical Overview

In this section we present a brief overview of our correlation extractor construction and the graph-theoretic measure of the maximum resilience of an arbitrary correlation.

Correlation Extractor Construction. Suppose we are given $0 < \delta < g < 1/2$, and parties are in the $\mathsf{IP}\left(\mathbb{K}^{1/\delta}\right)^{[t]}$-hybrid, where $t = (1/2 - g)n$ and $\mathbb{K} = \mathbb{GF}\left[2^{\delta n}\right]$. For $m = (\delta n)^{1-o(1)}$, we want to implement the $\mathsf{OLE}\left(\mathbb{GF}[2]\right)^m$

$\mathsf{ROLE}(\mathbb{F})$	Given a field $\mathbb{F}$, Alice receives $r_A = (A, B)$ and Bob receives $r_B = (X, Z)$ such that A, B, X are independently and uniformly sampled from $\mathbb{F}$ and $Z = A \cdot X + B$.
$\mathsf{IP}(\mathbb{F}^n)$	Given a field $\mathbb{F}$, Alice receives $r_A = (x_0, x_1, \ldots, x_{n-1})$ and Bob receives $r_B = (y_0, y_1, \ldots, y_{n-1})$ such that $x_0, \ldots, x_{n-1}, y_0, \ldots, y_{n-1}$ are randomly selected from $\mathbb{F}$, where $x_0 + y_0 = \sum_{i=1}^{n-1} x_i \cdot y_i$.

Fig. 3. A quick summary of the definitions of a few correlations that are relevant to this paper.

functionality. Figure 4 presents the outline of our correlation extractor construction. The extraction protocol π is similar to the correlation extractor of Gupta et al. [26]. Except that, in their case the inner-product correlation was over $\mathbb{GF}[2]$ instead of a large field $\mathbb{K}$. The security of the protocol is argued in Sect. 3. Our correlation extractor securely computes a sample from the $\mathsf{ROLE}(\mathbb{K})$ correlation. The protocol ρ is the standard protocol that implements the $\mathsf{OLE}(\mathbb{K})$ functionality in the $\mathsf{ROLE}(\mathbb{K})$-hybrid with perfect security. So, all that remains is to simultaneously embed $\mathsf{OLE}(\mathbb{GF}[2])^m$ into one $\mathsf{OLE}(\mathbb{K})$. This embedding relies on finding solutions to a combinatorial problem that is summarized in Fig. 5. Section 4 outlines the technique of choosing the inputs to the $\mathsf{OLE}(\mathbb{K})$ functionality so that the parties can implement the $\mathsf{OLE}(\mathbb{GF}[2])^m$ functionality with perfect security.

Ensure. Let $\mathbb{F} = \mathbb{GF}[2]$ and $\mathbb{K} = \mathbb{GF}\left[2^{\delta n}\right]$ be an extension field of $\mathbb{F}$. Let $0 < \delta < g < 1/2$.

Private Input. Let $m = (\delta n)^{1-o(1)}$. Alice has private input $(a_0, \ldots, a_{m-1}) \in \mathbb{F}^m$ and $(b_0, \ldots, b_{m-1}) \in \mathbb{F}^m$. Bob has private input $(x_0, \ldots, x_{m-1}) \in \mathbb{F}^m$.

Hybrid. Parties are in the $\mathsf{IP}\left(\mathbb{K}^{1/\delta}\right)^{[t]}$-hybrid, where $t = (1/2 - g)n$.

Protocol.

1. Let $\pi(\mathbb{K}, 1/\delta - 1)$ be a protocol in the $\mathsf{IP}\left(\mathbb{K}^{1/\delta}\right)^{[t]}$-hybrid that securely computes $\mathsf{ROLE}(\mathbb{K})$ with simulation error $2^{-(g-\delta)n/2-1}$. Fig. 7 provides the details of the protocol in Section 3.
2. Let $\rho(\mathbb{K}, A^*, B^*, X^*)$ be a perfectly secure protocol for $\mathsf{OLE}(\mathbb{K})$ in the $\mathsf{ROLE}(\mathbb{K})$-hybrid. The private input of Alice is $(A^*, B^*) \in \mathbb{K}^2$ and the private input of Bob is $X^* \in \mathbb{K}$. Bob obtains the output $Z^* = A^*X^* + B^*$. Fig. 8 provides the details of the protocol in Section 3.
3. The protocol $\sigma(\mathbb{K}, 1/\delta - 1, A^*, B^*, X^*)$ is the parallel composition of $\pi(\mathbb{K}, 1/\delta - 1)$ and $\rho(\mathbb{K}, A^*, B^*, X^*)$ protocol.
4. Parties run the two-round protocol $\sigma(\mathbb{K}, 1/\delta - 1, A^*, B^*, X^*)$ with Alice's private input (A^*, B^*) and Bob's private input X^*. Lemma 3 in Section 4 explains the choice of the inputs A^*, B^*, and X^*.

Output Computation. Lemma 3 in Section 4 presents Bob's algorithm to compute $(z_0, \ldots, z_{m-1})$ from Z^*.

Fig. 4. For $0 < \delta < g < 1/2$, the outline of the (n, m, t, ε)-correlation extractor in the $\mathsf{IP}\left(\mathbb{K}^{1/\delta}\right)^{[t]}$-hybrid, where $m = (\delta n)^{1-o(1)}$, $t = (1/2 - g)n$, $\varepsilon = 2^{-(g-\delta)n/2-1}$.

Our Combinatorial Problem. Find S and T such that
- S and T are ordered sets of non-negative integers of equal size.
- The set $S + T$ represents the set of the sum of every element of S with every element in T.
- Interpret the set $S + T$ as a matrix, where the (i, j)-th entry represents the sum of the i-th entry in S and the j-th entry in T. All entries in $S + T$ are in the range $[0, n)$, and $(S + T)_{i,i}$ is not equal to any other element in $S + T$, for $i \in \{0, \ldots, |S| - 1\}$.
- Size of $|S| = |T|$ is maximum

Fig. 5. Our combinatorial problem for embedding multiple OLE over small fields into one OLE over an extension field.

Hardness of Computation Result. The starting point of this result is the observation that we know the exact characterization of the correlations which *do not* suffice to construct OT asymptotically [2,32,38,41–43], namely *simple correlations*. Constructing one OT given a single sample from a simple correlation is even more restrictive, and, hence, the hardness of computation result carries over.[3] This result holds true even when there is no leakage on (R_A, R_B). In fact, there exists a universal constant $\varepsilon^* > 0$ such that any OT protocol using any simple correlation has simulation error at least ε^*.

Intuitively, the simple partition number of a correlation (R_A, R_B), represented by $\mathsf{sp}(R_A, R_B)$, is the minimum Λ such that (R_A, R_B) can be "decomposed into a union of" Λ simple correlations. Section 5 formalizes this notion of decomposition. Next, we prove in Lemma 4 that for any correlation (R_A, R_B), in the presence of $t = \log \mathsf{sp}(R_A, R_B)$ bits of leakage, any protocol π for OT has simulation error at least ε^*. Using this result, we translate tight upper bounds on the simple partition number of relevant correlations into corresponding meaningful upper bounds on their maximum resilience. Figure 2 summarizes our results. We construct a smoother version of this technical lemma using averaging arguments, see Corollary 1. For example, if the leakage bound $t \geqslant (\log \mathsf{sp}(G)) - gn$, then any $(n, 1, t, \varepsilon)$-correlation extractor for (R_A, R_B) has $\varepsilon \geqslant \varepsilon^* \cdot 2^{-gn}$.

2 Preliminaries

We represent the set $\{1, \ldots, n\}$ by $[n]$. For a vector $(x_1, \ldots, x_n)$ and $S = \{i_1, \ldots, i_{|S|}\} \subseteq [n]$, the set x_S represents $(x_{i_1}, \ldots, x_{i_{|S|}})$. In this work we work with fields $\mathbb{F} = \mathbb{GF}[p^a]$, where p is a prime and a is a positive integer. An extension field $\mathbb{K}$ of $\mathbb{F}$ of degree n is interpreted as the field of all polynomials of degree $< n$ and coefficients in $\mathbb{F}$.

[3] The problem of characterizing correlations whose single sample suffice to construct OT is a fascinating open problem that lies beyond the purview of this study.

2.1 Functionalities and Correlations

We introduce some useful functionalities and correlations.

Oblivious Transfer. Oblivious transfer, represented by OT, is a two-party functionality that takes as input $(x_0, x_1) \in \{0,1\}^2$ from Alice and $b \in \{0,1\}$ from Bob and outputs x_b to Bob.

Oblivious Linear-function Evaluation. For a field $(\mathbb{F}, +, \cdot)$, oblivious linear-function evaluation over $\mathbb{F}$, represented by $\mathsf{OLE}(\mathbb{F})$, is a two-party functionality that takes as input $(a, b) \in \mathbb{F}^2$ from Alice and $x \in \mathbb{F}$ from Bob and outputs $z = ax + b$ to Bob. In particular, OLE refers to the $\mathsf{OLE}(\mathbb{GF}[2])$ functionality. Note that OT is identical (functionally equivalent) to OLE because $x_b = (x_1 - x_0)b + x_0$.

Random Oblivious Transfer Correlation. Random oblivious transfer, represented by ROT, is a correlation that samples x_0, x_1, b uniformly and independently at random. It provides Alice the secret share $r_A = (x_0, x_1)$ and provides Bob the secret share $r_B = (b, x_b)$.

Random Oblivious Linear-function Evaluation. For a field $(\mathbb{F}, +, \cdot)$, random oblivious linear-function evaluation over $\mathbb{F}$, represented by $\mathsf{ROLE}(\mathbb{F})$, is a correlation that samples $a, b, x \in \mathbb{F}$ uniformly and independently at random. It provides Alice the secret share $r_A = (a, b)$ and provides Bob the secret share $r_B = (x, z)$, where $z = ax + b$. In particular, ROLE refers to the $\mathsf{ROLE}(\mathbb{GF}[2])$ correlation. Note that ROT and ROLE are identical (functionally equivalent) correlations.

Inner-product Correlation. For a field $(\mathbb{F}, +, \cdot)$ and $n \in \mathbb{N}$, inner-product correlation over $\mathbb{F}$ of size n, represented by $\mathsf{IP}(\mathbb{F}^n)$, is a correlation that samples random $r_A = (x_0, \ldots, x_{n-1}) \in \mathbb{F}^n$ and $r_B = (y_0, \ldots, y_{n-1}) \in \mathbb{F}^n$ subject to the constraint that $x_0 + y_0 = \sum_{i=1}^{n-1} x_i y_i$. The secret shares of Alice and Bob are, respectively, r_A and r_B.

For $m \in \mathbb{N}$, the functionality $\mathcal{F}^m$ represents the functionality that implements m independent copies of any functionality/correlation $\mathcal{F}$.

2.2 Toeplitz Matrix Distribution

Given a field $\mathbb{F}$, the distribution $\mathbb{T}_{(k,n)}$ represents a uniform distribution over all matrices of the form $[I_{k\times k}|P_{k\times n-k}]$, where $I_{k\times k}$ is the identity matrix and $P_{k\times n-k}$ is a Toeplitz matrix with each entry in $\mathbb{F}$. The distribution $\mathbb{T}_{\perp,(k,n)}$ is the uniform distribution over all matrices of the form $[P_{n-k\times k}|I_{n-k\times n-k}]$, where $I_{n-k\times n-k}$ is the identity matrix and $P_{n-k\times k}$ is a Toeplitz matrix with each entry in $\mathbb{F}$.

2.3 Graph Representation of Correlations

We introduce a graph-theoretic representation of correlations for a more intuitive presentation.

Definition 2 (Graph of a Correlation). *Let* (R_A, R_B) *be the joint distribution for a correlation. The* graph of the correlation (R_A, R_B) *is the weighted bipartite graph* $G = (L, R, E)$ *defined as follows.*

1. *The left partite set* L *is the set of all possible secret shares* r_A *for Alice,*
2. *The right partite set* R *is the set of all possible secret shares* r_B *for Bob, and*
3. *The weight connecting the vertices* r_A *and* r_B *is the probability of sampling the shares* (r_A, r_B) *according to the distribution* (R_A, R_B).

In this paper, the notation (R_A, R_B) also represents the bipartite graph corresponding to it. If the correlation is a uniform distribution over a subset E of all possible edges, then we normalize the entire graph such that the weights on each edge is 1. For example, consider the correlations presented in Fig. 3. Henceforth, for the ease of presentation, we assume that the graph of a correlation is an unweighted bipartite graph. The left-most graph in Fig. 12 is the graph of the ROLE correlation.

A bipartite graph $G = (L, R, E)$ is a *biclique* if there exists $L' \subseteq L$ and $R' \subseteq R$ such that that edge-set $E(G) = L' \times R'$.

Definition 3 (Simple Graph). *A* simple graph *is a bipartite graph such that each of its connected components is a biclique.*

For example, consider the graph in Fig. 6.[4] A *simple correlation* is a correlation whose graph is simple.

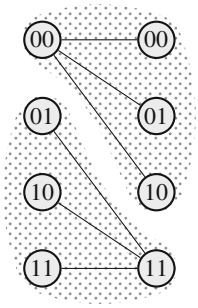

Fig. 6. A representative example of a simple graph.

Definition 4 (Simple Partition Number). *The* simple partition number *of a graph* G*, represented by* $\mathsf{sp}(G)$*, is the minimum number of simple graphs needed to partition its edges.*

Figures 12 and 13 show that the simple partition number for both $\mathsf{ROLE}(\mathbb{GF}[2])$ and $\mathsf{ROLE}(\mathbb{GF}[2])^2$ is 2.

In this work, we use the tensor product of bipartite graphs defined as follows.

[4] This definition naturally generalizes to weighted graphs. Suppose $p(r_A, r_B)$ represents the probability of jointly sampling (r_A, r_B) from the correlation (R_A, R_B). Then a simple graph has $p(r_A, r_B) = p(r_A) \cdot p(r_B)$, for every (r_A, r_B) edge with positive weight.

Definition 5 (Tensor Product Graph). *For bipartite graphs* $G = (L_G, R_G, E_G)$ *and* $H = (L_H, R_H, E_H)$ *the* tensor product of G and H *is the bipartite graph* $J = (L_J, R_J, E_J)$ *defined as follows.*

1. *The left partite set* $L_J := L_G \times L_H$*, the right partite set* $R_J := R_G \times R_H$*, and*
2. *The vertices* $(u, v) \in L_J$ *and* $(u', v') \in R_J$ *are connected if* $(u, u') \in E_G$ *and* $(v, v') \in E_H$*.*

Applying this definition recursively, we define $G^m := \overbrace{G \times \cdots \times G}^{m-\text{times}}$.

3 Extracting One OLE over a Large Field

In this section we will build some of the building blocks needed to construct the correlation extractor claimed in Theorem 1. In particular, we outline the extraction protocol that, given a leaky $\mathsf{IP}\left(\mathbb{K}^{\eta+1}\right)^{[t]}$ correlation, realizes a secure $\mathsf{OLE}\left(\mathbb{K}\right)$ functionality.

1. First, given the $\mathsf{IP}\left(\mathbb{K}^{\eta+1}\right)$ correlation where parties can perform t-bits of arbitrary leakage, we construct a secure sample of an $\mathsf{ROLE}\left(\mathbb{K}\right)$ correlation. This protocol $\pi(\mathbb{K}, \eta)$ is presented in Fig. 7. At the end of the protocol Alice has $(\widetilde{A}_0, \widetilde{B}_0) \in \mathbb{K}^2$ and Bob has $(\widetilde{X}_0, \widetilde{Z}_0) \in \mathbb{K}^2$, such that $\widetilde{A}_0, \widetilde{B}_0, \widetilde{X}_0$ are uniformly random elements in $\mathbb{K}$ and $\widetilde{Z}_0 = \widetilde{A}_0\widetilde{X}_0 + \widetilde{B}_0$. The simulation error of this protocol is $\frac{1}{2}\sqrt{\frac{|\mathbb{K}|2^t}{|\mathbb{K}|^{\eta/2}}}$, refer to Lemma 2.
2. Next, starting with the private shares $(\widetilde{A}_0, \widetilde{B}_0)$ with Alice and $(\widetilde{X}_0, \widetilde{Z}_0)$ with Bob, we implement a protocol $\rho(\mathbb{K}, A^*, B^*, X^*)$. Alice has private inputs (A^*, B^*) that are arbitrary elements in $\mathbb{K}^2$. Bob has private input X^* that is an arbitrary element in $\mathbb{K}$. The protocol $\rho(\mathbb{K}, A^*, B^*, X^*)$, described in Fig. 8 is a perfectly secure protocol where Bob outputs $Z^* = A^*X^* + B^*$.

We emphasize that both $\pi(\mathbb{K}, \eta)$ and $\rho(\mathbb{K}, A^*, B^*, X^*)$ are 2-round protocols and we can compose these two protocols in parallel. The resultant protocol $\sigma(\mathbb{K}, \eta, A^*, B^*, X^*)$ is an extraction protocol that takes as input a leaky $\mathsf{IP}\left(\mathbb{K}^{\eta+1}\right)^{[t]}$ correlation where parties can perform t-bits of arbitrary leakage and implements the $\mathsf{ROLE}\left(\mathbb{K}\right)$ functionality with simulation error $\frac{1}{2}\sqrt{\frac{|\mathbb{K}|2^t}{|\mathbb{K}|^{\eta/2}}}$. This is formalized in the following lemma and the proof is included below.

Lemma 1 (Security of Correlation Extractor). *The protocol* $\sigma(\mathbb{K}, \eta, A^*, B^*, X^*)$ *obtained by the parallel composition of the protocols* $\pi(\mathbb{K}, \eta)$ *(see Fig. 7) and* $\rho(\mathbb{K}, A^*, B^*, X^*)$ *(see Fig. 8) is a secure protocol in the* $\mathsf{IP}\left(\mathbb{K}^{\eta+1}\right)^{[t]}$ *hybrid that implements the* $\mathsf{OLE}\left(\mathbb{K}\right)$ *functionality with simulation error at most* $\frac{1}{2}\sqrt{\frac{|\mathbb{K}|2^t}{|\mathbb{K}|^{\eta/2}}}$.

Section 4 elaborates the exact technique to choose appropriate $\mathbb{K}, \eta, A^*, B^*, X^*$ to imply Theorem 1.

3.1 Extraction of One Secure ROLE $(\mathbb{K})$ Correlation

The protocol is provided in Fig. 7. The security of the protocol is analogous to the proof in [26] that reduces to the unpredictability lemma over fields. We state this lemma in our context.

Lemma 2 (Unpredictability Lemma). *Let* $\mathcal{G} \in \left\{\mathbb{T}_{(k,\eta+1)}, \mathbb{T}_{\perp,(k,\eta+1)}\right\}$. *Consider the following game between an honest challenger and an adversary:*

1. $\mathcal{H}$ *samples* $m_{[\eta]} \sim U_{\mathbb{K}^\eta}$.
2. $\mathcal{A}$ *sends a leakage function* $\mathcal{L}\colon \mathbb{K}^\eta \to \{0,1\}^t$.
3. $\mathcal{H}$ *sends* $\mathcal{L}\left(m_{[\eta]}\right)$ *to* $\mathcal{A}$.
4. $\mathcal{H}$ *samples* $x_{[k]} \sim U_{\mathbb{K}^k}$, $G \sim \mathcal{G}$, *and computes* $y_{\{0\}\cup[n]} = x \cdot G + (0, m_{[\eta]})$. $\mathcal{H}$ *sends* $(y_{[\eta]}, G)$ *to* $\mathcal{A}$. $\mathcal{H}$ *picks* $b \xleftarrow{\$} \{0,1\}$. *If* $b = 0$, *then she sends* $\mathsf{chal} = y_0$ *to* $\mathcal{A}$; *otherwise (if* $b = 1$*) then she sends* $\mathsf{chal} = u \sim U_{\mathbb{K}}$ *to* $\mathcal{A}$.
5. $\mathcal{A}$ *replies with an element* $\tilde{b} \in \{0,1\}$.

The adversary $\mathcal{A}$ *wins the game if* $b = \tilde{b}$. *For any* $\mathcal{A}$, *the advantage of the adversary is* $\leqslant \frac{1}{4}\sqrt{\frac{|\mathbb{K}|2^t}{|\mathbb{K}|^k}}$.

Similar to the security proof provided by Gupta et al. [26], the simulation error of the protocol in Fig. 7 is the bound provided by the unpredictability lemma over fields (Lemma 2). Refer to the full version of the paper [6] for a proof of correctness.

Pseudocode of the extraction protocol $\pi(\mathbb{K}, \eta)$.

Given. Alice has $(X_0, X_1, \ldots, X_\eta)$ and Bob has $(Y_0, Y_1, \ldots, Y_\eta)$ such that $X_0 + Y_0 = \sum_{i=1}^{\eta} X_i Y_i$, where $X_0, \ldots, X_\eta, Y_0, \ldots, Y_\eta \in \mathbb{K}$. For ease of presentation assume that η is odd and set $w = (\eta+1)/2$. An adversarial party can obtain arbitrary t-bit leakage on the share of the other party.

Interactive Protocol.

1. **First Round.** Bob samples a random generator matrix G from the distribution $\mathbb{T}_{w\times(\eta+1)}$ such that its elements are in $\mathbb{K}$. Let $\mathcal{C}$ be the code generated by G, and $\mathcal{C}^\perp$ be its dual code. Let H be the generator matrix for the code $\mathcal{C}^\perp$. If the first column of H is $0^{\eta+1-w}$ (i.e., all zeros), then abort the protocol. Bob picks a random codeword $(\widetilde{X}_0, \widetilde{X}_1, \ldots, \widetilde{X}_\eta) \in \mathcal{C}^\perp$ and calculates $M_{[\eta]} = Y_{[\eta]} - \widetilde{X}_{[\eta]}$. Bob sends $M_{[\eta]}$ and G to Alice.
2. **Second Round.** Alice samples a random codeword $(\widetilde{A}_0, \widetilde{A}_1, \ldots, \widetilde{A}_\eta) \in \mathcal{C}$ and a random field element $\widetilde{B}_0 \in \mathbb{K}$. Alice computes $\alpha_{[\eta]} = X_{[\eta]} + \widetilde{A}_{[\eta]}$ and $\beta = \left\langle X_{[\eta]}, M_{[\eta]} \right\rangle - \widetilde{B}_0 - X_0$. Alice sends $\alpha_{[\eta]}$ and β to Bob.

Output Computation. Alice outputs $(\widetilde{A}_0, \widetilde{B}_0)$ and Bob outputs $(\widetilde{X}_0, \widetilde{Z}_0)$, where $\widetilde{Z}_0 = -\left\langle \alpha_{[\eta]}, \widetilde{X}_{[\eta]} \right\rangle - \beta + Y_0$.

Fig. 7. Protocol to securely extract one random sample of the ROLE $(\mathbb{K})$ functionality from the leaky $\mathsf{IP}\left(\mathbb{K}^{\eta+1}\right)^{[t]}$ correlation.

3.2 Securely Realizing $\mathsf{OLE}(\mathbb{K})$ Using $\mathsf{ROLE}(\mathbb{K})$ Correlation

The protocol presented in Fig. 8 is a perfectly semi-honest secure protocol for $\mathsf{OLE}(\mathbb{K})$ in the $\mathsf{ROLE}(\mathbb{K})$ correlation hybrid. Note that the protocols $\pi(\mathbb{K}, \eta)$ in Fig. 7 and $\rho(\mathbb{K}, A^*, B^*, X^*)$ in Fig. 8 can be composed in parallel. Let $\sigma(\mathbb{K}, \eta, A^*, B^*, X^*)$ be the parallel composition of the protocols $\pi(\mathbb{K}, \eta)$ and $\rho(\mathbb{K}, A^*, B^*, X^*)$. This completes the proof of Lemma 1.

Pseudocode of the OLE protocol $\rho(\mathbb{K}, A^*, B^*, X^*)$

Given. Alice has $(\widetilde{A}_0, \widetilde{B}_0)$ and Bob has $(\widetilde{X}_0, \widetilde{Z}_0)$, where $\widetilde{A}_0, \widetilde{B}_0, \widetilde{X}_0$ are random elements in $\mathbb{K}$ and $\widetilde{Z}_0 = \widetilde{A}_0\widetilde{X}_0 + \widetilde{B}_0$.

Private Inputs. Alice has private input $(A^*, B^*) \in \mathbb{K}^2$ and Bob has $X^* \in \mathbb{K}$.

Interactive Protocol.

1. **First Round.** Bob sends $M' = \widetilde{X}_0 - X^*$ to Alice.
2. **Second Round.** Alice sends $\alpha' = \widetilde{A}_0 + A^*$ and $\beta' = \widetilde{A}_0 M + B^* + \widetilde{B}_0$.

Output Computation. Bob outputs $Z^* = \alpha' X^* + \beta' - \widetilde{Z}_0$.

Fig. 8. Perfectly secure protocol to realize $\mathsf{OLE}(\mathbb{K})$ in the $\mathsf{ROLE}(\mathbb{K})$ correlation hybrid.

4 Embedding Multiple OLEs into an OLE over an Extension Field

One of the primary goals in this section is to prove the following lemma.

Lemma 3 (Embedding Multiple small OLE into a Large OLE). *Let $\mathbb{K}$ be an extension field of $\mathbb{F}$ of degree n. There exists a perfectly secure protocol for $\mathsf{OLE}(\mathbb{F})^m$ in the $\mathsf{OLE}(\mathbb{K})$-hybrid that makes only one call to the $\mathsf{OLE}(\mathbb{K})$ functionality and $m = n^{1-o(1)}$.*

Proof. Section 4.3 provides this lemma and proves Theorem 1.

4.1 Intuition of the Embedding

We illustrate the main underlying ideas of this embedding problem and our proposed solution using the representative field $\mathbb{F} = \mathbb{GF}[2]$ and its extension field $\mathbb{K} = \mathbb{GF}[2^n]$. Suppose we are provided with an oracle that takes as input $A^*, B^* \in \mathbb{K}$ from Alice and $X^* \in \mathbb{K}$ from Bob, and outputs $Z^* := A^* \cdot X^* + B^*$ to Bob. Our aim is to implement the following functionality. Alice has inputs $(a_0, \ldots, a_{m-1}) \in \mathbb{F}^m$ and $(b_0, \ldots, b_{m-1}) \in \mathbb{F}^m$, and Bob has inputs $(x_0, \ldots, x_{m-1}) \in \mathbb{F}^m$. We want Bob to obtain $(z_0, \ldots, z_{m-1}) \in \mathbb{F}^m$, where each $z_i = a_i \cdot x_i + b_i$, for $i \in \{0, \ldots, m-1\}$. Intuitively, we want maximize m and embed $\mathsf{OLE}(\mathbb{F})^m$ into one $\mathsf{OLE}(\mathbb{K})$.

Preliminary Idea. Consider the following simple preliminary embedding. Let $m = \sqrt{n}$. Alice defines $A^* = a_0 + a_1\zeta + \cdots + a_{m-1}\zeta^{m-1}$, where $a_0, \ldots, a_{m-1} \in \mathbb{F}$. And, Alice defines $B^* = \sum_{i=0}^{n-1} r_i\zeta^i$, where each r_i is a random element in $\mathbb{F}$; except when $(m+1)$ divides i, then we set $r_{t(m+1)} = b_t$, for $t \in \{0, \ldots, m-1\}$. Bob defines $X^* = x_0 + x_1\zeta^m + \cdots + x_{m-1}\zeta^{(m-1)m}$, where $x_0, \ldots, x_{m-1} \in \mathbb{F}$.

Now, the parties compute $Z^* = A^*X^* + B^*$ using one oracle call to $\mathsf{OLE}(\mathbb{K})$ and Bob obtains the output Z^*. Note that the intended $z_i = a_i \cdot x_i + b_i$ is the coefficient of $\zeta^{i(m+1)}$ in Z^*, for each $i \in \{0, \ldots, m-1\}$. Coefficients of all other powers of ζ contain no information about $a_0, \ldots, a_{m-1}, b_0, \ldots, b_{m-1}$, because they are masked with random elements in $\mathbb{F}$. So, for $m = \sqrt{n}$, we have embedded $\mathsf{OLE}(\mathbb{F})^m$ into one $\mathsf{OLE}(\mathbb{K})$.

Better Embedding. Observe that $(a_0 + a_1\zeta) \cdot (x_0 + x_1\zeta) = a_0x_0 + (a_0x_1 + a_1x_0)\zeta + a_1x_1\zeta^2$. So, we can embed $\mathsf{OLE}(\mathbb{F})^2$ into one $\mathsf{OLE}(\mathbb{K})$, where $\mathbb{K}$ is an extension field of $\mathbb{F}$ of degree 3, as follows. Alice chooses $A^* = a_0 + a_1\zeta \in \mathbb{GF}[2^2]$ and $B^* = b_0 + r\zeta + b_1\zeta^2$ (where r is a random element from $\mathbb{F}$), and Bob chooses $X^* = x_0 + x_1\zeta$. Note that the coefficients of ζ^0 and ζ^2 in Z^*, respectively, correspond to $a_0x_0 + b_0$ and $a_1x_1 + b_1$. Recursively applying this idea, we can construct an embedding of $\mathsf{OLE}(\mathbb{GF}[2])^{2^k}$ into one $\mathsf{OLE}\left(\mathbb{GF}\left[2^{3^k}\right]\right)$. Asymptotically, this scheme embeds $m = n^{\log 2/\log 3} \approx n^{0.631}$ copies of $\mathsf{OLE}(\mathbb{GF}[2])$ into one $\mathsf{OLE}(\mathbb{GF}[2^n])$.

Generalization to 3-free sets. Consider the previous solution when $n = 3^k$. Let $S = \{s_0 < s_1 < \cdots < s_{m-1}\}$ be the set of indices. The set S corresponding to the previous solution contains all integers less than 3^k whose ternary representation does not contain the digit 2. This is the famous greedy sequence of integers that does not include an arithmetic progression of length 3; namely, 3-free sets. In fact, there is nothing sacrosanct about the S chosen in the previous embedding, and *any* 3-free set suffices.

For example, let $S = \{s_0 < s_1 < \cdots < s_{m-1}\}$ be any 3-free set such that each entry is in the range $[0, n/2)$, $\mathbb{F} = \mathbb{GF}[2]$, and $\mathbb{K} = \mathbb{GF}[2^n]$. Alice prepares $A^* = \sum_{i=0}^{m-1} a_i\zeta^{s_i}$ and $B^* = \sum_{k=0}^{n-1} r_k\zeta^k$, where $r_{2s_i} = b_i$; otherwise it is a random element in $\mathbb{F}$. Bob prepares $X^* = \sum_{i=0}^{m-1} x_i\zeta^{s_i}$. Using one call to $\mathsf{OLE}(\mathbb{K})$ Bob obtains Z^*. The coefficient of ζ^{2s_i} is $a_ix_i + b_i$, because no other $s_j + s_k = 2s_i$. Now, we can embed $m = n^{1-o(1)}$ copies of $\mathsf{OLE}(\mathbb{F})$ into $\mathsf{OLE}(\mathbb{K})$ using the state-of-the-art constructions of 3-free sets [3,20]. However, this approach cannot give us $m = \Theta(n)$ due to sub-linear upper bounds on m [8,9,29,58,60,61].

New Problem. Note that although solutions to the 3-free set problem imply embeddings in our setting, our embedding problem is potentially less restrictive. For example, the solution for $m = \sqrt{n}$ presented above is not obtained by the reduction to 3-free sets. Are we missing something?

Suppose $S = (s_0, \ldots, s_{m-1})$ and $T = (t_0, \ldots, t_{m-1})$ be tuples of indices in the range $[0, n/2)$. Consider the combinatorial problem proposed in Fig. 5.

Given. Two sets S and T of size m that is a solution to the combinatorial problem presented in Fig. 5. Let $\mathbb{K}$ be an extension field of $\mathbb{F}$ of degree n.

Private input. Alice has private input $(a_0, \ldots, a_{m-1}) \in \mathbb{F}^m$ and $(b_0, \ldots, b_{m-1}) \in \mathbb{F}^m$. Bob has private input $(x_0, \ldots, x_{m-1}) \in \mathbb{F}^m$.

Hybrid. Parties are in the $\mathsf{OLE}(\mathbb{K})$-hybrid.

Private Input Construction.

1. Alice creates private input $A^* = \sum_{i=0}^{m-1} a_i \zeta^{s_i} \in \mathbb{K}$.
2. Alice chooses r_i, for $i \in \{0, \ldots, n-1\}$, as follows.

$$r_i = \begin{cases} b_k & \text{, if } i = s_k + t_k \text{ for some } k \in \{0, \ldots, m-1\} \\ U_{\mathbb{F}} & \text{, otherwise.} \end{cases}$$

   Alice creates private input $B^* = \sum_{i=0}^{n-1} r_i \zeta^i \in \mathbb{K}$.
3. Bob creates private input $X^* = \sum_{i=0}^{m-1} x_i \zeta^{t_i} \in \mathbb{K}$.
4. Both parties invoke the $\mathsf{OLE}(\mathbb{K})$ functionality with respective Alice input (A^*, B^*) and Bob input X^*. Bob receives $Z^* = A^* X^* + B^*$.

Output Decoding. Bob outputs $(z_0, \ldots, z_{m-1})$, where z_i is the coefficient of $\zeta^{s_i + t_i}$ and $i \in \{0, \ldots, m-1\}$.

Fig. 9. Embedding $\mathsf{OLE}(\mathbb{F})^m$ into one $\mathsf{OLE}(\mathbb{K})$, where $\mathbb{K}$ is an extension field of $\mathbb{F}$ of degree n.

Given S and T that are solutions to the problem in Fig. 5, Alice and Bob use the strategy explained in Fig. 9. Note that the initial solution for $m = \sqrt{n}$ indeed corresponds to the solution $S = \{0, \ldots, m-1\}$ and $T = \{0, m, \ldots, (m-1)m\}$. Restricted to $S = T$, our combinatorial problem is identical to the 3-free set problem. We numerically solve this problem for small values of n and, indeed, it produces more efficient embeddings than the embedding based on the optimal 3-free set constructions. We emphasize that we compare our solutions against the largest 3-free set computed by *exhaustive search*. We summarize our observations in Fig. 10.

4.2 Relevant Prior Work on 3-Free Sets

Our asymptotic construction for Theorem 1 relies on constructing a dense subset S of $\{0, 1, \cdots, n-1\}$ that does not contain any arithmetic progression, namely 3-free sets. Erdős and Turán introduced this problem in 1936 and presented a greedy construction with $|S| = \Omega\left(n^{\log 2/\log 3}\right) \approx n^{0{,}631}$. Salem and Spencer [59] showed that the surface of high-dimensional convex bodies can be embedded in the integers to construct 3-free sets of size $n^{1-o(1)}$. Later, Behrend [3] noticed that points lying on the surface of a sphere of suitable radius are a particularly good choice, and gave a construction with $|S| = \Omega\left(\frac{n}{2^{2\sqrt{2\log n}} \cdot \log^{1/4} n}\right)$. Recently, after a gap of over sixty years, Elkin [20] improved this further by a factor of $\Theta(\sqrt{\log n})$ by thickening the spheres to produce the largest known 3-free set. The proofs of Behrend [3] and Elkin [20] are constructive in nature and the sets can be constructed in poly(n) time. Although the greedy construction is asymptotically worse than these two constructions, it performs well for realistic values of n. See Fig. 11 for details.

m	$n(m)$	Solution Sets	$n'(m)$	3-free Set
1	1	$S = \{0\}$ $T = \{0\}$	1	$S = \{0\}$
2	3	$S = \{0, 1\}$ $T = \{0, 1\}$	3	$S = \{0, 1\}$
3	7	$S = \{0, 1, 3\}$ $T = \{0, 1, 3\}$	7	$S = \{0, 1, 3\}$
4	9	$S = \{0, 1, 3, 4\}$ $T = \{0, 1, 3, 4\}$	9	$S = \{0, 1, 3, 4\}$
5	14	$S = \{0, 1, 3, 5, 8\}$ $T = \{0, 1, 4, 5, 3\}$	17	$S = \{0, 1, 3, 7, 8\}$
6	19	$S = \{0, 1, 3, 4, 7, 9\}$ $T = \{0, 1, 3, 9, 7, 8\}$	21	$S = \{0, 1, 3, 4, 9, 10\}$
7	24	$S = \{0, 1, 3, 4, 11, 6, 10\}$ $T = \{0, 1, 5, 10, 6, 12, 9\}$	25	$S = \{0, 1, 3, 4, 9, 10, 12\}$
8	27	$S = \{0, 1, 3, 4, 9, 10, 12, 13\}$ $T = \{0, 1, 3, 4, 9, 10, 12, 13\}$	27	$S = \{0, 1, 3, 4, 9, 10, 12, 13\}$
9	34	$S = \{0, 1, 3, 4, 9, 12, 14, 16, 17\}$ $T = \{0, 1, 3, 4, 13, 11, 12, 15, 16\}$	39	$S = \{0, 1, 5, 6, 8, 13, 14, 17, 19\}$
10	38	$S = \{0, 1, 3, 5, 8, 12, 13, 16, 17, 15\}$ $T = \{0, 1, 4, 5, 3, 12, 13, 15, 17, 20\}$	47	$S = \{0, 1, 4, 6, 10, 15, 17, 18, 22, 23\}$

Fig. 10. Let $\mathbb{K}$ be an extension field of $\mathbb{F}$ of degree n. Our goal is to embed m copies of $\mathsf{OLE}(\mathbb{F})$ into one $\mathsf{OLE}(\mathbb{K})$ using minimum n. The number $n(m)$ represents the minimum n obtained by using solutions to our combinatorial problem in Fig. 5. The number $n'(m)$ represents the minimum n obtained by using the optimum solutions to the 3-free set problem.

Roth [58] provided the first nontrivial upper bound of $O\left(\frac{n}{\log\log n}\right)$ on the size of 3-free sets. More than thirty years later, Heath-Brown [29] showed that $|S| = O\left(\frac{n}{\log^c n}\right)$, for some constant $c > 0$, and then Szemeredi [61] produced an explicit value $c = 1/20$. Bourgain [8,9] improved the upper bound by polylog factors. Currently, the best known upper bound is $O\left(\frac{n(\log\log n)^4}{\log n}\right)$ [7,60]. Nathan [46] provides a comprehensive summary for both 3-free set size constructions and upper bounds.

4.3 Generating Explicit Embedding and Proof of Theorem 1

First, we prove Lemma 3. Let $S(n)$ be a 3-free set with elements in the range $[0, n/2)$. Behrend [3] and Elkin [20] provide constructions for $S(n)$ such that $|S(n)| \geqslant n^{1-o(1)}$. Note that $S = T = S(n)$ is a solution to the combinatorial problem proposed in Fig. 5. Now, we use the protocol described in Fig. 9.

It is clear that the protocol is correct. The coefficients of all other ζ^i in Z^* are random elements in $\mathbb{F}$, if $i \neq s_k + t_k$, for all $k \in \{0, \ldots, m-1\}$. It is, therefore, easy to see that this is a perfectly secure protocol for $\mathsf{OLE}(\mathbb{F})^m$ in the $\mathsf{OLE}(\mathbb{K})$-hybrid.

Remark. We provide a short discussion on how to pick the 3-free set S for *concrete* values of n. The greedy construction is the fastest and runs in $O(n \log n)$ time. It picks all numbers that do not have 2 in their ternary representation, and $|S(n)| = n^{\log 2/\log 3} \approx n^{0.631}$. The proofs of Behrend [3] and Elkin [20] are also

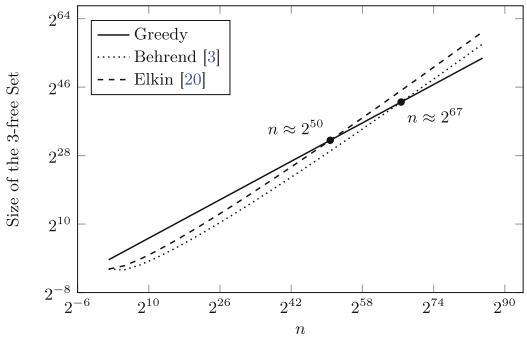

Fig. 11. A logarithmic scaled graph of the size of the 3-free sets produced by the greedy, Behrend [3], and Elkin [20] constructions.

constructive in nature and the set can be constructed in poly(n) time. However, their performance for realistic values of n are worse than the greedy algorithm.

Further, for concrete values of n, one of the solutions to our combinatorial problem generates better embeddings than the greedy solution. Note that, Fig. 10 presents a solution that enables the embedding of 10 independent $\mathsf{OLE}(\mathbb{F})$ evaluations into one $\mathsf{OLE}(\mathbb{K})$ evaluation, where $\mathbb{K}$ is an extension field of $\mathbb{F}$ of degree 38. Recursively applying this embedding, we embed $m = n^{\log 10/\log 38} \approx n^{0.633} \gg n^{0.631} \approx n^{\log 2/\log 3}$ independent $\mathsf{OLE}(\mathbb{GF}[2])$ evaluations into one $\mathsf{OLE}(\mathbb{GF}[2^n])$ evaluation.

Proof of Theorem 1. Suppose we given n, $0 < \delta < g < 1/2$, and $t = (1/2 - g)n$. Let $\mathbb{K} = \mathbb{GF}\left[2^{\delta n}\right]$ and $\mathbb{F} = \mathbb{GF}[2]$. We construct $A^*, B^*, X^* \in \mathbb{K}$ using Lemma 3 and $m \geqslant (\delta n)^{1-o(1)}$. Perform the protocol $\sigma(\mathbb{K}, 1/\delta - 1, A^*, B^*, X^*)$ in the $\mathsf{IP}\left(\mathbb{K}^{1/\delta}\right)^{[t]}$-hybrid.[5] The simulation error is

$$\varepsilon \leqslant \frac{1}{2}\sqrt{\frac{2^{\delta n}2^t}{2^{\delta n(1/\delta-1)/2}}} = 2^{-(g-\delta)n/2-1}$$

This is an (n, m, t, ε)-correlation extractor for the correlation $\mathsf{IP}\left(\mathbb{K}^{1/\delta}\right)$.

5 Simple Partition Number

This section defines the simple partition number of a graph, provides estimates of this quantity for correlations relevant to our work, and proves Theorem 2.

5.1 Intuition of the Hardness of Computation Result

We know that if parties have multiple independent samples of secret shares sampled according to a simple correlation, then the parties cannot securely compute

[5] Recall that in the protocol $\pi(\mathbb{K}, \eta)$, all parties have share size $(\eta + 1)\log|\mathbb{K}|$.

OT [2,32,38,41–43]. Constructing one OT given a single sample from such a correlation is even more restrictive, and, hence, the hardness of computation result carries over. This result holds true even when there is no leakage on (R_A, R_B). More precisely, we import the following result that we restate in our context.

Imported Theorem 1 [43]. *Let (R_A, R_B) be a simple correlation with n-bit secret shares for each party. There exists a universal constant $\varepsilon^* > 0$, such that any $(n, 1, 0, \varepsilon)$-correlation extractor for (R_A, R_B) has $\varepsilon \geqslant \varepsilon^*$.*

Suppose (R_A, R_B) is a correlation that has simple partition number $\mathsf{sp}(G) = 2^\lambda$ and $G = G^{(1)} + \cdots + G^{(2^\lambda)}$, where each $G^{(i)}$ is a simple graph. Then we consider the leakage function $\mathcal{L}(r_A, r_B) = \ell$, where $\ell \in \{1, \ldots, 2^\lambda\}$ is the unique index such that $(r_A, r_B) \in E(G^{(\ell)})$. Note that $\mathcal{L}$ is a λ-bit leakage function and conditioned on the leakage being ℓ, for any $\ell \in \{1, \ldots, 2^\lambda\}$, the correlation $(R_A, R_B|\ell)$ is a simple correlation. So, one of the parties can break the security of any purported OT protocol where parties get secret shares sampled from the $(R_A, R_B|\ell)$ correlation. Overall, with probability half, one of the parties can break the security of any purported OT protocol where parties get secret shares sampled from the (R_A, R_B) by performing the leakage $\mathcal{L}$ described above. This technique upper-bounds the leakage resilience of (R_A, R_B) and we summarize it as follows.

Lemma 4 (Connection between Maximum Leakage Resilience and Simple Partition Number). *Let (R_A, R_B) is a correlated private randomness that provides n-bit private shares to Alice and Bob. Let G be the bipartite graph corresponding to the correlation (R_A, R_B). There exists a universal constant $\varepsilon^* > 0$ such that any $(n, 1, t, \varepsilon)$-correlation extractor for (R_A, R_B) with $t \geqslant \lceil \lg \mathsf{sp}(G) \rceil$ has $\varepsilon \geqslant \varepsilon^*$.*

We construct a smoother version of this technical lemma using averaging arguments. For example, if the leakage bound t is roughly $(\log \mathsf{sp}(G)) - gn$, then we consider a subset of simple graphs of size $\mathsf{sp}(G) \cdot 2^{-gn}$ from the set $\left\{G^{(1)}, \ldots, G^{(\mathsf{sp}(G))}\right\}$ that covers at least 2^{-gn} fraction of the edges of G. Applying the previous lemma, we can conclude that $(n, 1, t, \varepsilon)$-correlation extractor for (R_A, R_B) with $t \geqslant \lceil \log \mathsf{sp}(G) - gn \rceil$ has $\varepsilon \geqslant \varepsilon^* \cdot 2^{-gn}$.

Corollary 1 ((Smooth Version of the) Connection between Maximum Leakage Resilience and Simple Partition Number). *Let (R_A, R_B) is a correlated private randomness that provides n-bit private shares to Alice and Bob. Let G be the bipartite graph corresponding to the correlation (R_A, R_B). There exists a universal constant $\varepsilon^* > 0$ such that any $(n, 1, t, \varepsilon)$-correlation extractor for (R_A, R_B) with $t \geqslant \lceil \lg \mathsf{sp}(G) - gn \rceil$ has $\varepsilon \geqslant \varepsilon^* \cdot 2^{-gn}$.*

5.2 Relevant Prior Work on Graph Covering Problems

The graph-theoretic measure proposed in our work to measure the maximum resilience of correlations in best presented in the framework of graph covering

problems. Several problems in graph theory, for example, clique partition number, biparticity, arboricity, edge-chromatic number, vertex cover number and biclique partition number, can be expressed as covering a graph with subgraphs from a family of graphs. Of these representative examples, the concept of *biclique partition number* is most relevant to our paper. For a graph G, its biclique partition number, represented by $\mathsf{bp}(G)$, is the minimum number of bicliques that suffice to partition it.

Refer to [40] for a comprehensive survey on graph covering problems. Motivated by network addressing problem and graph storage problem, Graham and Pollak [24,25] introduced the biclique partition problem (see also [1,63,64,70]). The celebrated Graham-Pollak Theorem states that $\mathsf{bp}(K_n) = (n-1)$ [25,52,62,65,66], but all proofs are algebraic, and no purely combinatorial proof is known. In general, $\mathsf{bp}(G) \geqslant \max\{n_+(G), n_-(G)\}$ [25,30,52,62], where $n_+(\cdot)$ and $n_-(\cdot)$, respectively, represents the number of positive and negative eigenvalues of the adjacency matrix of the graph. Determining the $\mathsf{bp}(G)$ of a general graph is a hard problem [40], but it admits a trivial upper bound $\mathsf{bp}(G) \leqslant$ the size of the smallest vertex cover of G. Variants of this quantity have been considered recently by [14].

This quantity is closely related to the recently disproved [13,31] Alon-Saks-Seymour Conjecture [36] that $\mathsf{bp}(G) + 1$ colors suffice to color a graph. This conjecture can be interpreted as a generalization of the Graham-Pollak Theorem and has close relations to computational complexity [31,51,57]. In the context of this paper, intuitively, the biclique partition number is a combinatorial version of the *Wyner's Common Information* [69] that corresponds to the minimum description complexity of the information that kills the mutual information of correlations. We interpret a correlation as a weighted bipartite graph with the left-partite set being all possible values of r_A, and the right partite set being all possible values of r_B. The weight on an edge joining r_A and r_B represents the probability of jointly sampling (r_A, r_B). This graph-theoretic interpretation of correlations helps establish connections between combinatorial and information-theoretic concepts.

5.3 Relation to Leakage Resilience: Proof of Lemma 4

In this section we prove Lemma 4, i.e. the maximum leakage resilience of a correlation (R_A, R_B) is at most $\lg \mathsf{sp}(R_A, R_B)$.

Let G be the bipartite graph corresponding to the correlation (R_A, R_B). Let π be a $(n, 1, t, \varepsilon)$-correlation extractor for G, where $t = \lceil \log \mathsf{sp}(G) \rceil$. Let $G = G^{(1)} + \cdots + G^{(\mathsf{sp}(G))}$ be the simple partition of G. Define the leakage function $\mathcal{L}\colon E(G) \to \{1, \ldots, \mathsf{sp}(G)\}$ as follows. For $e \in E(G)$, we have $\mathcal{L}(e) = \ell$, where ℓ is the unique index in $\{1, \ldots, \mathsf{sp}(G)\}$ such that $e \in E(G^{(\ell)})$.

Consider an interactive protocol that runs π between Alice and Bob with secret samples drawn from the correlation G, and *both parties* receive the leakage $\mathcal{L}(r_A, r_B)$.

Note that this is identical to the interactive protocol, where the correlation G^+ that samples $\ell \in \{1, \ldots, \mathsf{sp}(G)\}$ with probability proportional to $\left|E(G^{(\ell)})\right|$, samples $(u, v) \equiv e \xleftarrow{\$} E(G^{(\ell)})$, and provides (u, ℓ) to Alice and (v, ℓ) to Bob.

The functionality G^+ itself is simple, because each $G^{(\ell)}$ is simple. So, we can use Imported Theorem 1. Therefore, one of the parties' view cannot be simulated with less than $\varepsilon^* > 0$ simulation error when the parties follow the protocol π. Suppose, that party is Alice, without loss of generality. That is, the view of the party Alice* (to represent the semi-honest adversarial strategy) in the interactive protocol between Alice* and B incurs at least ε^* simulation error.

Now consider the case where only Alice* receives the leakage from the correlation and not Bob. The view of Alice* remains identical to the previous hybrid. Therefore, this protocol also incurs a simulation error at least ε^*

This implies that for any $(n, 1, t, \varepsilon)$-correlation extractor for (R_A, R_B), if $t \geqslant \log \mathsf{sp}(R_A, R_B)$, then $\varepsilon \geqslant \varepsilon^*$.

Intuitively, Lemma 4 can be summarized as follows. A small simple partition number of the correlated private randomness (R_A, R_B) implies a low maximum leakage-resilience of (R_A, R_B).

Proof of Corollary 1. Suppose $2^t = \mathsf{sp}(G)/2^{gn}$ and π is an $(n, 1, t, \varepsilon)$-correlation extractor for (R_A, R_B). Now, we choose the $\mathsf{sp}(G)/(2^{gn} - 1)$ simple graphs among $\{G^{(1)}, \ldots, G^{(\mathsf{sp}(G))}\}$ that cover a subset $E' \subset E(G)$ such that $|E'|/|E(G)| \geqslant (2^{gn} - 1)^{-1}$. The leakage function $\mathcal{L}(r_A, r_B)$ outputs the index of the simple graph from which the edge $e = (r_A, r_B)$ comes, if $e \in E'$; otherwise, it returns $\perp$. Using the same proof as Lemma 4 we can conclude that the simulation error is $\varepsilon \geqslant \varepsilon^* (2^{gn} - 1)^{-1} \approx \varepsilon^* 2^{-gn}$.

5.4 Estimates of Simple Partition Number and Proof of Theorem 2

In this section we present the lemma that provides the estimates of the simple partition number of relevant correlations.

Lemma 5 (Simple Partition Number Estimates). *The following holds true for arbitrary field* $\mathbb{F}$.

1. $\mathsf{sp}(\mathsf{IP}(\mathbb{F}^n)) \leqslant |\mathbb{F}|^{\lceil (n+1)/2 \rceil}$, *and*
2. *For even* n, $\mathsf{sp}\left(\mathsf{ROLE}(\mathbb{F})^{n/2}\right) \leqslant |\mathbb{F}|^{\lceil n/4 \rceil}$.

Refer to the full version [6] for a proof of the first part. The proof outline of the second part is provided in Sect. 5.5. The simple decomposition we construct for the correlations mentioned above have an additional property. Given an edge $(r_A, r_B) \sim (R_A, R_B)$, we can efficiently compute the index of the simple graph in the decomposition that contains it. Thus, the leakage that demonstrates the upper bound of the maximal resilience in Lemma 4 is computationally efficient.

The proof of Theorem 2 is a direct application of Lemmas 4 and 5.

5.5 Subsuming the Partition Argument

In this section, using a particular example, we want to illustrate that the simple partition number is sophisticated enough to subsume partition argument based impossibility results. To begin, let us consider an example. Let (R_A, R_B) be the random oblivious linear-function evaluation over $\mathbb{GF}[2]$. So, the correlation samples $a, b, x \in \mathbb{GF}[2]$ independently and uniformly at random. The secret share of Alice is $r_A = (a, b)$ and the secret share of Bob is $r_B = (x, z)$, where $z = ax+b$. The secrecy of $\mathsf{ROLE}(\mathbb{GF}[2])$ ensures that Alice has no advantage in guessing x and Bob has no advantage in guessing a. The graph of the correlation is provided in Fig. 12. The figure presents the simple decomposition corresponding to the leakage $\ell = x - a$.

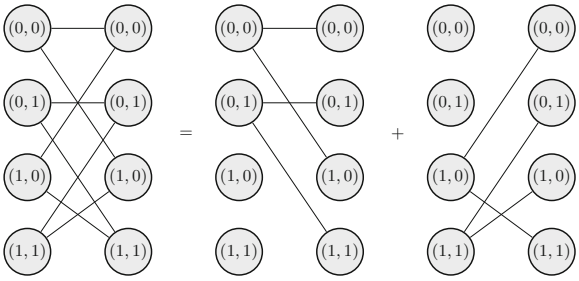

Fig. 12. The graph of the correlated private randomness $\mathsf{ROLE}(\mathbb{GF}[2])$ and its decomposition into two simple graphs.

Now, let us consider $\mathsf{ROLE}(\mathbb{GF}[2])^2$, i.e. two independent samples from the $\mathsf{ROLE}(\mathbb{GF}[2])$ correlation. Alice gets secret share (a_1, b_1, a_2, b_2) and Bob gets secret share (x_1, z_1, x_2, z_2), where $z_1 = a_1x_1 + b_1$ and $z_2 = a_2x_2 + b_2$. Suppose in the partition argument Alice implements the first correlation and Bob implements the second correlation. This implies that Alice knows x_1 and Bob knows a_2. We want to achieve this effect using only one-bit leakage that is provided to both the parties.

Given the decomposition in Fig. 12, note that we can define a two-bit leakage to achieve this. For example the first leakage bit represents $\ell_1 = x_1 - a_1$, and the second leakage bit represents $\ell_2 = x_2 - a_2$. We show in Fig. 13 that even a one-bit leakage suffices. In particular, we use $\mathcal{L}(r_A, r_B) = x_1 - a_2$. In the full version [6], we show that $\mathsf{sp}\left(\mathsf{ROLE}(\mathbb{F})^2\right) \leqslant |\mathbb{F}|$.

Using this observation and the fact that $\mathsf{sp}(G \times H) \leqslant \mathsf{sp}(G) \cdot \mathsf{sp}(H)$ (see full version [6] for the proof), Lemma 5 shows that $\mathsf{sp}(\mathsf{ROLE}(\mathbb{F})^n) \leqslant |\mathbb{F}|^{\lceil n/2 \rceil}$. This demonstrates that the simple partition number subsumes the partition argument.

5.6 Relevant Prior Work on Common Information and Assisted Common Information

We briefly introduce a few relevant information-theoretic measures for maximum resilience and maximum production rate. For a joint distribution, the mutual information $I(R_A; R_B)$ measures the distance (KL-divergence) between the joint probability distribution $p(r_A, r_B)$ and the distribution $p(r_A) \cdot p(r_B)$. The mutual information between (R_A, R_B) represents the number of bits of the secret key that the two parties can agree. The Gács-Körner [21] common information, represented by $K(R_A; R_B)$, represents the largest entropy of the common random variable that each party can generate based on their respective secret share. Intuitively, this corresponds to the number of connected components in a bipartite graph representing the correlation. The Wyner common information [69], represented by $J(R_A; R_B)$, is the minimum information that, when leaked to the eavesdropper, ensures that the parties cannot establish a secret key. This quantity roughly corresponds to the biclique partition number of a bipartite graph for the correlation, where the correlation is a uniform distribution over the edges of the bipartite graph. Prabhakaran and Prabhakaran [53,54], generalizing [67], introduced the concept of *assisted common information* that, among its various applications, helps characterize an upper bound on the number of OTs that a correlation can produce.

Relation to Mutual Information. In the setting of key-agreement, the mutual information $I(R_A; R_B)$ of a correlation (R_A, R_B) measures the length of the secret key that the two parties can agree on. We emphasize that this is a measure of production, and not a measure of resilience. For example, $I(\mathsf{IP}(\mathbb{GF}[2]^n)) = 1$. Since, secure OT implies one-bit key-agreement, mutual information is also an upper bound on the OT production that a correlation can support. However, production capacity and resilience to leakage are extremely disparate quantities. For example, in the secure computation setting, the correlation $\mathsf{IP}(\mathbb{GF}[2]^n)$ is resilient to $n/2$ bits of leakage but can only produce one OT. Additionally, mutual information significantly overestimates the maximum OT production capacity. For example, n-bit shared private key cannot produce one OT even without any leakage. However, it has n-bits of mutual information.

We emphasize that the simple partition number is only a measure for the maximum leakage resilience of correlations in the setting of secure computation. Our measure *does not* provide any estimates on the OT production. The most relevant measure for OT production is the notion of assisted common information proposed by Prabhakaran and Prabhakaran [53,54].

5.7 Analogy of Biclique Partition Number and Wyner's Common Information

A correlation that is a biclique has no mutual-information and, hence, is useless for parties to agree on a secret key even asymptotically. In particular, one sample from a correlation that is a biclique is also useless for key-agreement.

Suppose (R_A, R_B) is an arbitrary correlation and has biclique partition complexity $\mathsf{bp}(R_A, R_B)$. Similar to Lemma 4, in the presence of $t = \log \mathsf{bp}(R_A, R_B)$ bits of leakage there is not even a one-bit secure key-agreement protocols using (R_A, R_B). The random variable J for the leakage function $\mathcal{L}(R_A, R_B)$ outputs the index of the biclique that contains the edge $e = (r_A, r_B)$.

Wyner's common information [69] is defined to be the minimum entropy random variable J that suffices to ensure $I(R_A; R_B|J) = 0$. If the bicliques that partition G have roughly equal number of edges then these two concepts are identical. Analogously, $\mathsf{sp}(R_A, R_B)$ can be interpreted as the analog for Wyner's common information in the secure computation setting.

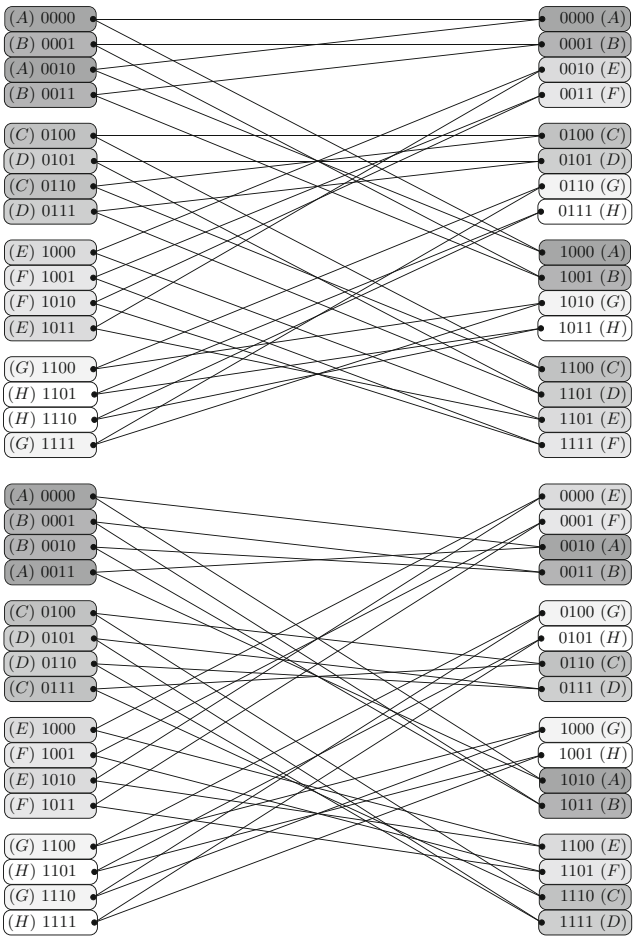

Fig. 13. A simple decomposition of $\mathsf{ROLE}(\mathbb{GF}[2])^2$, into two simple graphs. Each collection of nodes with identical shade of gray and letter represents a connected component.

However, we cannot use biclique partition number or Wyner's Common Information to meaningfully measure the resilience of a correlation against leakage in the secure computation setting. The biclique partition number $\mathsf{bp}(R_A, R_B)$ can be significantly higher than the simple partition number $\mathsf{sp}(R_A, R_B)$, which is an upper bound on the maximum resilience. For example, the biclique partition number $\mathsf{bp}(\mathsf{IP}(\mathbb{F}^n)) \approx |\mathbb{F}|^{n-1}$ while its simple partition number $\mathsf{sp}(\mathsf{IP}(\mathbb{F}^n)) \approx |\mathbb{F}|^{n/2}$ is exponentially small. This example demonstrates the non-trivial utility of the new measure introduced by us in the secure computation setting.

References

1. Babai, L., Frankl, P.: Linear Algebra Methods in Combinatorics: With Applications to Geometry and Computer Science. Department of Computer Science, University of Chicago (1992). 23
2. Beaver, D.: Perfect privacy for two-party protocols. In: Feigenbaum, J., Merritt, M. (eds.) Proceedings of DIMACS Workshop on Distributed Computing and Cryptography, vol. 2, pp. 65–77. American Mathematical Society (1989). 4, 12, 22
3. Behrend, F.A.: On sets of integers which contain no three terms in arithmetical progression. Proc. Natl. Acad. Sci. **32**(12), 331–332 (1946). 18, 19, 20, 21
4. Ben-David, A., Nisan, N., Pinkas, B.: FairplayMP: a system for secure multi-party computation. In: Ning, P., Syverson, P.F., Jha, S. (eds.) ACM CCS 08, pp. 257–266. ACM Press, October 2008. 4
5. Ben-Or, M., Goldwasser, S., Wigderson, A.: Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract). In: 20th ACM STOC, pp. 1–10. ACM Press, May 1988. 4
6. Block, A.R., Maji, H.K., Nguyen, H.H.: Secure computation based on leaky correlations: high resilience setting. https://www.cs.purdue.edu/homes/hmaji/papers/C:BloMajNgu17.pdf. (Full Version). 16, 24, 25
7. Bloom, T.F.: A quantitative improvement for Roth's theorem on arithmetic progressions. J. Lond. Math. Soc. **93**(3), 643–663 (2016). 20
8. Bourgain, J.: On triples in arithmetic progression. Geom. Funct. Anal. **9**(5), 968–984 (1999). 18, 20
9. Bourgain, J.: Roth's theorem on progressions revisited. J. d'Analyse Math. **104**(1), 155–192 (2008). 18, 20
10. Canetti, R., Lindell, Y., Ostrovsky, R., Sahai, A.: Universally composable two-party and multi-party secure computation. In: 34th ACM STOC, pp. 494–503. ACM Press, May 2002. 4
11. Chandran, N., Goyal, V., Sahai, A.: New constructions for UC secure computation using tamper-proof hardware. In: Smart, N. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 545–562. Springer, Heidelberg (2008). doi:10.1007/978-3-540-78967-3_31. 4
12. Chaum, D., Crépeau, C., Damgård, I.: Multiparty unconditionally secure protocols (extended abstract). In: 20th ACM STOC, pp. 11–19. ACM Press, May 1988. 4
13. Cioaba, S.M., Tait, M.: More counterexamples to the Alon-Saks-Seymour and rank-coloring conjectures. Electron. J. Comb. **18**(P26), 1 (2011). 23
14. Cioabă, S.M., Tait, M.: Variations on a theme of Graham and Pollak. Discret. Math. **313**(5), 665–676 (2013). 23

15. Crépeau, C., Morozov, K., Wolf, S.: Efficient unconditional oblivious transfer from almost any noisy channel. In: Blundo, C., Cimato, S. (eds.) SCN 2004. LNCS, vol. 3352, pp. 47–59. Springer, Heidelberg (2005). doi:10.1007/978-3-540-30598-9_4. 4
16. Damgård, I., Ishai, Y.: Scalable secure multiparty computation. In: Dwork, C. (ed.) CRYPTO 2006. LNCS, vol. 4117, pp. 501–520. Springer, Heidelberg (2006). doi:10.1007/11818175_30. 4
17. Damgård, I., Nielsen, J.B., Wichs, D.: Isolated proofs of knowledge and isolated zero knowledge. In: Smart, N. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 509–526. Springer, Heidelberg (2008). doi:10.1007/978-3-540-78967-3_29. 4
18. Damgård, I., Pastro, V., Smart, N., Zakarias, S.: Multiparty computation from somewhat homomorphic encryption. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 643–662. Springer, Heidelberg (2012). doi:10.1007/978-3-642-32009-5_38. 4
19. Dolev, D.: The Byzantine generals strike again. J. Algorithms **3**(1), 14–30 (1982). 4
20. Elkin, M.: An improved construction of progression-free sets. In: Proceedings of the Twenty-first Annual ACM-SIAM Symposium on Discrete Algorithms, pp. 886–905. Society for Industrial and Applied Mathematics (2010). 18, 19, 20, 21
21. Gács, P., Körner, J.: Common information is far less than mutual information. Probl. Control Inf. Theory **2**(2), 149–162 (1973). 26
22. Goldreich, O., Micali, S., Wigderson, A.: How to play any mental game or a completeness theorem for protocols with honest majority. In: Aho, A. (ed.) 19th ACM STOC, pp. 218–229. ACM Press, May 1987. 4
23. Goyal, V., Ishai, Y., Sahai, A., Venkatesan, R., Wadia, A.: Founding cryptography on tamper-proof hardware tokens. In: Micciancio, D. (ed.) TCC 2010. LNCS, vol. 5978, pp. 308–326. Springer, Heidelberg (2010). doi:10.1007/978-3-642-11799-2_19. 4
24. Graham, R.L., Pollak, H.O.: On the addressing problem for loop switching. Bell Syst. Tech. J. **50**(8), 2495–2519 (1971). 10, 23
25. Graham, R.L., Pollak, H.O.: On embedding graphs in squashed cubes. In: Alavi, Y., Lick, D.R., White, A.T. (eds.) Graph Theory and Applications. LNM, vol. 303, pp. 99–110. Springer, Heidelberg (1972). doi:10.1007/BFb0067362. 10, 23
26. Gupta, D., Ishai, Y., Maji, H.K., Sahai, A.: Secure computation from leaky correlated randomness. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015. LNCS, vol. 9216, pp. 701–720. Springer, Heidelberg (2015). doi:10.1007/978-3-662-48000-7_34. 6, 7, 8, 9, 10, 11, 16
27. Harnik, D., Ishai, Y., Kushilevitz, E., Nielsen, J.B.: OT-combiners via secure computation. In: Canetti, R. (ed.) TCC 2008. LNCS, vol. 4948, pp. 393–411. Springer, Heidelberg (2008). doi:10.1007/978-3-540-78524-8_22. 10
28. Harnik, D., Kilian, J., Naor, M., Reingold, O., Rosen, A.: On robust combiners for oblivious transfer and other primitives. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 96–113. Springer, Heidelberg (2005). doi:10.1007/11426639_6. 10
29. Heath-Brown, D.R.: Integer sets containing no arithmetic progressions. J. Lond. Math. Soc. (2) **35**(3), 385–394 (1987). 18, 20
30. Hoffman, A.J.: Eigenvalues and partitionings of the edges of a graph. Linear Algebra Appl. **5**(2), 137–146 (1972). 23
31. Huang, H., Sudakov, B.: A counterexample to the alon-saks-seymour conjecture and related problems. Combinatorica **32**(2), 205–219 (2012). 23

32. Impagliazzo, R., Luby, M.: One-way functions are essential for complexity based cryptography (extended abstract). In: 30th FOCS, pp. 230–235. IEEE Computer Society Press, October/November 1989. 4, 12, 22
33. Ishai, Y., Kushilevitz, E., Ostrovsky, R., Sahai, A.: Extracting correlations. In: 50th FOCS, pp. 261–270. IEEE Computer Society Press, October 2009. 5, 6, 7, 10
34. Ishai, Y., Maji, H.K., Sahai, A., Wullschleger, J.: Single-use OT combiners with near-optimal resilience. In: 2014 IEEE International Symposium on Information Theory, Honolulu, HI, USA, 29 June–4 July 2014, pp. 1544–1548. IEEE (2014). 6, 9, 10
35. Ishai, Y., Prabhakaran, M., Sahai, A.: Founding cryptography on oblivious transfer – efficiently. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 572–591. Springer, Heidelberg (2008). doi:10.1007/978-3-540-85174-5_32. 4, 10
36. Kahn, J.: Recent results on some not-so-recent hypergraph matching and covering problems. DIMACS, Center for Discrete Mathematics and Theoretical Computer Science (1991). 23
37. Katz, J.: Universally composable multi-party computation using tamper-proof hardware. In: Naor, M. (ed.) EUROCRYPT 2007. LNCS, vol. 4515, pp. 115–128. Springer, Heidelberg (2007). doi:10.1007/978-3-540-72540-4_7. 4
38. Kilian, J.: Founding cryptography on oblivious transfer. In: 20th ACM STOC, pp. 20–31. ACM Press, May 1988. 4, 12, 22
39. Kilian, J.: More general completeness theorems for secure two-party computation. In: 32nd ACM STOC, pp. 316–324. ACM Press, May 2000. 4
40. Kratzke, T., Reznick, B., West, D.: Eigensharp graphs: decomposition into complete bipartite subgraphs. Trans. Am. Math. Soc. **308**(2), 637–653 (1988). 23
41. Künzler, R., Müller-Quade, J., Raub, D.: Secure computability of functions in the IT setting with dishonest majority and applications to long-term security. In: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, pp. 238–255. Springer, Heidelberg (2009). doi:10.1007/978-3-642-00457-5_15. 4, 12, 22
42. Kushilevitz, E.: Privacy and communication complexity. In: 30th FOCS, pp. 416–421. IEEE Computer Society Press, October/November 1989. 4, 12, 22
43. Maji, H.K., Prabhakaran, M., Rosulek, M.: Complexity of multi-party computation problems: the case of 2-party symmetric secure function evaluation. In: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, pp. 256–273. Springer, Heidelberg (2009). doi:10.1007/978-3-642-00457-5_16. 4, 12, 22
44. Maji, H.K., Prabhakaran, M., Rosulek, M.: A unified characterization of completeness and triviality for secure function evaluation. In: Galbraith, S., Nandi, M. (eds.) INDOCRYPT 2012. LNCS, vol. 7668, pp. 40–59. Springer, Heidelberg (2012). doi:10.1007/978-3-642-34931-7_4. 4
45. Malkhi, D., Nisan, N., Pinkas, B., Sella, Y.: Fairplay - secure two-party computation system. In: Blaze, M. (ed.) Proceedings of the 13th USENIX Security Symposium, San Diego, CA, USA, 9–13 August 2004, pp. 287–302. USENIX (2004). 4
46. McNew, N.: Avoiding geometric progressions in the integers, 02 May 2017. https://math.dartmouth.edu/graduate-students/works/2013-14/McNew-GradPosterSession.pdf. 20
47. Meier, R., Przydatek, B.: On robust combiners for private information retrieval and other primitives. In: Dwork, C. (ed.) CRYPTO 2006. LNCS, vol. 4117, pp. 555–569. Springer, Heidelberg (2006). doi:10.1007/11818175_33. 10
48. Meier, R., Przydatek, B., Wullschleger, J.: Robuster combiners for oblivious transfer. In: Vadhan, S.P. (ed.) TCC 2007. LNCS, vol. 4392, pp. 404–418. Springer, Heidelberg (2007). doi:10.1007/978-3-540-70936-7_22. 10

49. Moran, T., Segev, G.: David and Goliath commitments: UC computation for asymmetric parties using tamper-proof hardware. In: Smart, N. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 527–544. Springer, Heidelberg (2008). doi:10.1007/978-3-540-78967-3_30. 4
50. Nielsen, J.B., Nordholt, P.S., Orlandi, C., Burra, S.S.: A new approach to practical active-secure two-party computation. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 681–700. Springer, Heidelberg (2012). doi:10.1007/978-3-642-32009-5_40. 4
51. Nisan, N., Wigderson, A.: On rank vs. communication complexity. Combinatorica **15**(4), 557–565 (1995). 23
52. Peck, G.W.: A new proof of a theorem of Graham and Pollak. Discret. Math. **49**(3), 327–328 (1984). 23
53. Prabhakaran, V.M., Prabhakaran, M.: Assisted common information. In: 2010 IEEE International Symposium on Information Theory, ISIT Proceedings, Austin, Texas, USA, 13–18 June 2010, pp. 2602–2606. IEEE (2010). 26
54. Prabhakaran, V.M., Prabhakaran, M.: Assisted common information: further results. In: Kuleshov, A., Blinovsky, V., Ephremides, A. (eds.) 2011 IEEE International Symposium on Information Theory Proceedings, ISIT 2011, St. Petersburg, Russia, 31 July–5 August 2011, pp. 2861–2865. IEEE (2011). 26
55. Przydatek, B., Wullschleger, J.: Error-tolerant combiners for oblivious primitives. In: Aceto, L., Damgård, I., Goldberg, L.A., Halldórsson, M.M., Ingólfsdóttir, A., Walukiewicz, I. (eds.) ICALP 2008. LNCS, vol. 5126, pp. 461–472. Springer, Heidelberg (2008). doi:10.1007/978-3-540-70583-3_38. 10
56. Rabin, T., Ben-Or, M.: Verifiable secret sharing and multiparty protocols with honest majority (extended abstract). In: 21st ACM STOC, pp. 73–85. ACM Press, May 1989. 4
57. Razborov, A.A.: The gap between the chromatic number of a graph and the rank of its adjacency matrix is superlinear. Discret. Math. **108**(1), 393–396 (1992). 23
58. Roth, K.F.: On certain sets of integers. J. Lond. Math. Soc. **1**(1), 104–109 (1953). 18, 20
59. Salem, R., Spencer, D.C.: On sets of integers which contain no three terms in arithmetical progression. Proc. Natl. Acad. Sci. **28**(12), 561–563 (1942). 19
60. Sanders, T.: On Roth's theorem on progressions. Ann. Math. **174**, 619–636 (2011). 18, 20
61. Szemerédi, E.: Integer sets containing no arithmetic progressions. Acta Math. Hung. **56**(1–2), 155–158 (1990). 18, 20
62. Tverberg, H.: On the decomposition of kn into complete bipartite graphs. J. Graph Theory **6**(4), 493–494 (1982). 23
63. van Lint, J.H., Wilson, R.M.: A Course in Combinatorics. Cambridge University Press, Cambridge (2001). 23
64. Van Lint, J.H.: {0, 1,*} distance problems in combinatorics (1985). 23
65. Vishwanathan, S.: A polynomial space proof of the Graham-Pollak theorem. J. Comb. Theory Ser. A **115**(4), 674–676 (2008). 23
66. Vishwanathan, S.: A counting proof of the Graham-Pollak theorem. Discret. Math. **313**(6), 765–766 (2013). 23
67. Wolf, S., Wullschleger, J.: New monotones and lower bounds in unconditional two-party computation. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 467–477. Springer, Heidelberg (2005). doi:10.1007/11535218_28. 26
68. Wolf, S., Wullschleger, J.: Oblivious transfer is symmetric. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 222–232. Springer, Heidelberg (2006). doi:10.1007/11761679_14. 4, 8

69. Wyner, A.D.: The common information of two dependent random variables. IEEE Trans. Inf. Theory **21**(2), 163–179 (1975). 7, 10, 23, 26, 27
70. Yan, W., Yeh, Y.-N.: A simple proof of Graham and Pollak's theorem. J. Comb. Theory Ser. A **113**(5), 892–893 (2006). 23
71. Yao, A.C.-C.: Protocols for secure computations (extended abstract). In: 23rd FOCS, pp. 160–164. IEEE Computer Society Press, November 1982. 4