# Communication Complexity of the Secret Key Agreement in Algorithmic Information Theory

**Emirhan Gürpınar**
LIRMM, Université de Montpellier, CNRS, France
emirhan.gurpinar@lirmm.fr

**Andrei Romashchenko**
LIRMM, Université de Montpellier, CNRS, France
andrei.romashchenko@lirmm.fr

## Abstract

It is known that the mutual information, in the sense of Kolmogorov complexity, of any pair of strings $x$ and $y$ is equal to the length of the longest shared secret key that two parties can establish via a probabilistic protocol with interaction on a public channel, assuming that the parties hold as their inputs $x$ and $y$ respectively. We determine the worst-case communication complexity of this problem for the setting where the parties can use private sources of random bits.

We show that for some $x$, $y$ the communication complexity of the secret key agreement does not decrease even if the parties have to agree on a secret key the size of which is much smaller than the mutual information between $x$ and $y$. On the other hand, we provide examples of $x$, $y$ such that the communication complexity of the protocol declines gradually with the size of the derived secret key.

The proof of the main result uses spectral properties of appropriate graphs and the expander mixing lemma as well as various information theoretic techniques.

**2012 ACM Subject Classification** Mathematics of computing → Information theory; Theory of computation → Communication complexity; Security and privacy → Information-theoretic techniques; Theory of computation → Expander graphs and randomness extractors

**Keywords and phrases** Kolmogorov complexity, mutual information, communication complexity, expander mixing lemma, finite geometry

**Digital Object Identifier** 10.4230/LIPIcs.MFCS.2020.44

**Related Version** (the full version of the paper): `https://arxiv.org/abs/2004.13411`

**Funding** Supported in part by the ANR project RaCAF ANR-15-CE40-0016-01.
*Andrei Romashchenko*: is grateful to the Max Planck Institute for Mathematics in the Sciences (Leipzig, Germany) for hospitality, and thanks Rostislav Matveev and Jacobus Portegies for useful discussions.

**Acknowledgements** We thank the anonymous reviewers for instructive suggestions and corrections concerning this conference publication as well as the full version of the paper.

## 1 Introduction

In this paper we deal with *Kolmogorov complexity* and *mutual information*, which are the central notions of algorithmic information theory. Kolmogorov complexity $C(x)$ of a string $x$ is the length of the shortest program that prints $x$. Similarly, Kolmogorov complexity $C(x|y)$ of a string $x$ given $y$ is the length of the shortest program that prints $x$ when $y$ is given as the input. Let us consider two strings $x$ and $y$. The mutual information $I(x : y)$ can be defined by a formula: $I(x : y) = C(x) + C(y) - C(x, y)$. Intuitively, this quantity is the information shared by $x$ and $y$. In general, it cannot be "materialized" as one object of complexity $I(x : y)$ that can be easily extracted from both $x$ and $y$. However, this quantity has a sort of *operational interpretation*. The mutual information of $x$ and $y$ is essentially


equal to the size of a longest shared secret key that two parties, one having $x$ and the other one having $y$, and both parties also possessing the complexity profile of the two strings can establish via a probabilistic protocol:

▶ **Theorem 1** (sketchy version; see [16] for a more precise statement).

**(a)** There is a secret key agreement protocol that, for every $n$-bit strings $x$ and $y$, allows Alice and Bob to compute with high probability a shared secret key $z$ of length equal to the mutual information of $x$ and $y$ (up to an $O(\log n)$ additive term).

**(b)** No protocol can produce a longer shared secret key (up to an $O(\log n)$ additive term).

In this paper we study the communication complexity of the protocols that appear in this theorem. The statement of Theorem 1 in the form given above is vague and sketchy. Before we proceed with our results, we must clarify the setting of this theorem: we should explain the rules of the game between Alice, Bob, and the eavesdropper, and specify the notion of "secrecy" of the key in this context.

▶ **Clarification 1** (secrecy). In this theorem we say that the obtained key $z$ is "secret" in the sense that it looks random. Technically, it must be (almost) incompressible, even from the point of view of the eavesdropper who does not know the inputs $x$ and $y$ but intercepts the communication between Alice and Bob. More formally, if $t$ denotes the transcript of the communication, we require that $C(z|t) \geq |z| - O(1)$. We will need to make this requirement even slightly stronger, see below.

▶ **Clarification 2** (randomized protocols). In this communication model we assume that Alice and Bob may use additional randomness. Each of them can toss a fair coin and produce a sequence of random bits with a uniform distribution. The private random bits produced by Alice and Bob are accessible only to Alice and Bob respectively. (Of course, Alice and Bob can send the produced random bits to each other, but then this information becomes visible to the eavesdropper.)

In an alternative setting, Alice and Bob use a common *public* source of randomness (also accessible to the eavesdropper). The model with public randomness is easier to analyze, see [16], and in this paper we focus on the setting with private randomness.

▶ **Clarification 3** (minor auxiliary inputs). We assume also that besides the main inputs $x$ and $y$ Alice and Bob both are given the *complexity profile* of the input, i.e., the values $C(x)$, $C(y)$, and $I(x : y)$. Such a concession is unavoidable for the positive part of the theorem. Indeed, Kolmogorov complexity and mutual information are non-computable; so there is no computable protocol that finds a $z$ of size $I(x : y)$ unless the value of the mutual information is given to Alice and Bob as a promise. This supplementary information is rather small, it can be represented by only $O(\log n)$ bits. The theorem remains valid if we assume that this auxiliary data is known to the eavesdropper. So, formally speaking, the protocol should find a key $z$ such that $C(z|t, \text{complexity profile of } (x, y)) \geq |z| - O(1)$.

Now we can formulate the main question studied in this paper:

▶ **Central Question.** What is the optimal communication complexity of the communication problem from Theorem 1? That is, how many bits should Alice and Bob send to each other to agree on a common secret key?

A protocol proposed in [16] allows to compute for *all* pairs of inputs a shared secret key of length equal to the mutual information of $x$ and $y$ with communication complexity

$$\min\{C(x|y), C(y|x)\} + O(\log n). \tag{1}$$

Alice and Bob may need to send to each other different number of bits for different pairs of input (even with the same mutual information). It was proven in [16] that in the worst case (i.e., for *some* pairs of inputs $(x, y)$) the communication complexity (1) is optimal for communication protocols using only *public randomness*. The natural question whether this bound remains optimal for protocols with *private* sources of random bits remained open (see *Open Question 1* in [16]). The main result of this paper is the positive answer to this question. More specifically, we provide explicit examples of pairs $(x, y)$ such that

$$\begin{cases} I(x:y) &= 0.5n + O(\log n) \\ C(x|y) &= 0.5n + O(\log n) \\ C(y|x) &= 0.5n + O(\log n) \end{cases} \tag{2}$$

and in every communication protocol satisfying Theorem 1 (with private random bits) Alice and Bob must exchange approximately $0.5n$ bits of information. Moreover, the same communication complexity is required even if Alice and Bob want to agree on a much smaller secret key of size, say, $\omega(\log n)$.

▶ **Theorem 2.** Let $\pi$ be a communication protocol such that given inputs $x$ and $y$ satisfying (2) Alice and Bob use $\mathrm{poly}(n)$ private random bits and compute with probability $> 1/2$ a shared secret key $z$ of length $\delta(n) = \omega(\log n)$. Then for every $n$ there exists a pair of $n$-bit strings $(x, y)$ satisfying (2) such that following this communication protocol with inputs $x$ and $y$, Alice and Bob send to each other messages with a total length of at least $0.5n - O(\log n)$ bits. In other words, the worst-case communication complexity of the protocol is at least $0.5n - O(\log n)$.

▶ Remark 1. We assume that the computational protocol $\pi$ used by Alice and Bob is computable, i.e., the parties send messages and compute the final result by following rules that can be computed given the length of the inputs. We may assume that the protocol is public (known to the eavesdropper). The constants hidden in the $O(\cdot)$ notation may depend on the protocol, as well as on the choice of the optimal description method in the definition of Kolmogorov complexity.

An alternative approach might be as follows. We might assume that the protocol $\pi$ is not uniformly computable (but its description is available to Alice, Bob, and to the eavesdropper). Then substantially the same result can be proven for Kolmogorov complexity relativized conditional on $\pi$. That is, we should define Kolmogorov complexity and mutual information in terms of programs that can access $\pi$ as an oracle, and the inputs $x$ and $y$ should satisfy a version of (2) with the relativized Kolmogorov complexity. Our main result can be proven for this setting (literally the same arguments applies). However, to simplify the notation, we focus on the setting with only computable communication protocols (whose size does not depend on $n$).

Theorem 2 can be viewed as a special case of the general question of "extractability" of the mutual information studied in [4]. We prove this theorem for two specific examples of pairs $(x, y)$. In the first example $x$ and $y$ are a *line* and a *point* incident with each other in a discrete affine plane. In the second example $x$ and $y$ are points of the discrete plane with a fixed distance between them. The proof consists in a combination of a spectral and information-theoretical techniques. In fact, our argument applies to all pairs with similar spectral properties. Our main technical tools are the Expander Mixing Lemma (see Lemma 9) and the lemma on non-negativity of the triple mutual information (see Lemma 14). We also use Muchnik's theorem on conditional descriptions with multiple conditions (see Proposition 15).

The communication protocol proposed in [16] and Theorem 2 imply together that we have the following phase transition phenomenon. When the inputs given to Alice and Bob are a line and a point (incident with each other in a discrete affine plane), then the parties can agree on a secret key of size $I(x:y)$ with a communication complexity slightly *above* $\min\{C(x|y), C(y|x)\}$. But when a communication complexity is slightly *below* this threshold, the optimal size of the secret key sinks immediately to $O(\log n)$.

We also show that the "phase transition" property mentioned above is not universally true. There exist pairs $(x, y)$ with the same values of Kolmogorov complexities and the same mutual information as in the example above, but with a sharply different trade-off between the size of a secret key and the communication complexity needed to establish this key. In fact, for some $(x, y)$ the size of the optimal secret key decreases gradually with the communication complexity of the protocol. More specifically, we show that for some $x$ and $y$, Alice and Bob can agree on a secret key of any size $k$ (which can be chosen arbitrarily between 0 and $I(x:y)$) via a protocol with a communication complexity of $\Theta(k)$.

**Historical digression: classical information theory.** The problem of *secret key agreement* was initially proposed in the framework of classical information theory by Ahlswede and Csiszár, [1] and Maurer, [12]. In these original papers the problem was studied for the case when the input data is a pair of random variables $(X, Y)$ obtained by $n$ independent draws from a joint distribution (Alice can access $X$ and Bob can access $Y$). In this setting, the mutual information between $X$ and $Y$ and the secrecy of the key are measured in terms of Shannon entropy. Ahlswede and Csiszár in [1] and Maurer in [12] proved that the longest shared secret key that Alice and Bob can establish via a communication protocol is equal to Shannon's mutual information between $X$ and $Y$. This problem was extensively studied by many subsequent works in various restricted settings, see the survey [19]. The optimal communication complexity of this problem for the general setting remains unknown, though substantial progress has been made (see, e.g., [20, 10]).

There is a deep connection between the frameworks of classical information theory (based in Shannon entropy) and algorithmic information theory (based on Kolmogorov complexity). It can be shown that the statements of Theorem 1 and Theorem 2 imply similar statements in Shannon's theory. We refer the reader to [16] for a more detailed discussion of parallels and differences between Shannon's and Kolmogorov's version of the problem of secret key agreement. Here we only mention two important distinctions between Shannon's and Kolmogorov's framework. The first one regards ergodicity of the input data. Most results on secret key agreement in Shannon's framework are proven with the assumption that the input data are obtained from a sequence of independent identically distributed random variables (or at least enjoy some properties of ergodicity and stationarity). In the setting of Kolmogorov complexity we usually deal with inputs obtained in "one shot" without any assumption of ergodicity of the sources (see, in particular, Example 1 and Example 2 below). Another distinction regards the definition of correctness of the protocol. The usual paradigm in classical information theory is to require that the communication protocol works properly for *most* randomly chosen inputs. In our approach, we prove a stronger property: for *each* valid pair of input data, the protocol works properly with high probability (this approach is more typical for the theory of communication complexity).

**Organization of the paper.** The rest of the paper is organized as follows. In Section 2 we translate information theoretic properties of pairs $(x, y)$ in the language of graph theory and present three explicit examples of pairs $(x, y)$ satisfying (2),

- Example 1 involves finite geometry, $x$ and $y$ are incident points and lines on a finite plane;
- Example 2 uses a discrete version of the Euclidean distance, $x$ and $y$ are points on the discrete plane with a known quasi-Euclidean distance between them;
- Example 3 involves $x$ and $y$ that are binary strings with a fixed Hamming distance between them.

The pairs $(x, y)$ from these examples have pretty much the same complexity profile, but the third example has significantly different spectral properties. In Section 3 we use a spectral technique to analyze combinatorial properties of graphs and prove our main result (Theorem 2) for the pairs $(x, y)$ from Example 1 and Example 2 mentioned above. In Section 4 we show that the statement of Theorem 2 is not true for the pairs $(x, y)$ from our Example 3: for those $x$ and $y$ there is no "phase transition" mentioned above, and the size of the longest achievable secret key depends continuously on the communication complexity of the protocol, see Theorem 3 and Theorem 4.

**Notation.** Throughout this paper, $|\cdot|$ denotes the length of a string, $C(x)$ denotes Kolmogorov complexity of $x$, and $C(x|y)$ denotes conditional complexity of $x$ given $y$. We use the following standard notation: $I(x : y) := C(x) + C(y) - C(x, y)$ stands for the mutual information between $x$ and $y$, and $I(x : y|z) := C(x|z) + C(y|z) - C(x, y|z)$ stands for the conditional mutual information between $x$ and $y$ given $z$. We refer the reader to the classical paper [22] and to the textbooks [18] and [9] for a systematic introduction to Kolmogorov complexity.

We study randomized communication protocols for parties (Alice and Bob) with private sources of randomness. The *transcript* of the communication is the concatenation of messages sent the parties to each other while following the protocol. Communication complexity of a protocol is the maximal length of the transcript. A comprehensive introduction to communication complexity can be found in [8].

## 2 From information theoretic properties to combinatorics of graphs

To study information theoretic properties of a pairs $(x, y)$ we will embed this pair of strings in a large set of pairs that are in some sense similar to each other. We will do it in the language of bipartite graphs. The information theoretic properties of the initial pair $(x, y)$ will be determined by combinatorial properties of these graphs. In their turn, combinatorial properties of these graphs will be proven using the spectral technique. In this section we present three examples of $(x, y)$ corresponding to three different constructions of graphs. In next sections we will study spectral and combinatorial properties of these graphs and, accordingly, information theoretic properties of these pairs $(x, y)$.

We start with a simple lemma that establishes a correspondence between information theoretic and combinatorial language for the properties of pairs $(x, y)$.

▶ **Lemma 2.** *Let $G = (L \cup R, E)$ be a bipartite graph such that $|L| = |R| = 2^{n+O(1)}$ and the degree of each vertex is $D = 2^{0.5n+O(\log n)}$. We assume that this graph has an* explicit construction *in the sense that the complete description of this graph (its adjacency matrix) has Kolmogorov complexity $O(\log n)$. Then most $(x, y) \in E$ (pairs of vertices connected by an edge) have the complexity profile* (2).

(See the proof of the lemma in the full version of the paper.)

▶ Remark 3. In a graph satisfying the conditions of Lemma 2 each vertex has $D = 2^{0.5n}$ neighbors. Therefore, for *all* $(x, y) \in E$ we have $C(x|y) \leq 0.5n + O(\log n)$, $C(y|x) \leq$

$0.5n + O(\log n)$, (given $x$, we can specify $y$ by its index in the list of all neighbors of $x$ and vice-versa.) From Lemma 2 it follows that for *most* $(x, y) \in E$ these inequalities are tight, i.e., $C(x|y) = 0.5n + O(\log n)$ and $C(y|x) = 0.5n + O(\log n)$.

▶ **Example 1** (discrete plane)**.** Let $\mathbb{F}_q$ be a finite field of cardinality $q = 2^n$. Consider the set $L$ of points on plane $\mathbb{F}_q^2$ and the set $R$ of non-vertical lines, which can be represented as affine functions $y = ax - b$ for $(a, b) \in \mathbb{F}_q^2$. Let $G = (L \cup R, E)$ be the bipartite graph where a point $(x_0, y_0)$ is connected to a line $y = ax - b$ if and only if it is on the line i.e. $y_0 = ax_0 - b$. Clearly $|L| = |R| = 2^{2n}$. The degree of each vertex is $2^n$ since there are exactly $q$ points on each line and there are exactly $q$ lines on each point. In the sequel we denote this graph by $G_n^{Pl}$.

This graph (or its adjacency matrix) can be constructed effectively when the field $\mathbb{F}_q$ is given. We assume a standard construction of the field $\mathbb{F}_{2^n}$ to be fixed. Thus, the graph is uniquely defined by the binary representation of $n$. Therefore, we need only $O(\log n)$ bits to describe the graph (as a finite object). Lemma 2 applies to this graph, so for most $(x, y) \in E$ the equalities in (2) are satisfied.

▶ **Example 2** (discrete Euclidean distance)**.** Let $\mathbb{F}_q$ be a finite field of order $q$, where $q$ is an odd prime power. Let us define the distance function between two points in $\mathbb{F}_q^2$ as $\mathrm{dist}((x_1, x_2), (y_1, y_2)) = (x_1 - y_1)^2 + (x_2 - y_2)^2$. For every $r \in \mathbb{F}_q \setminus \{0\}$ we define the *finite Euclidean distance graph* $G = (L \cup R, E)$ as follows: $L = R = \mathbb{F}_q^2$, and $E = \{((x_1, x_2), (y_1, y_2)) \ : \ \mathrm{dist}((x_1, x_2), (y_1, y_2)) = r\}$. Obviously, $|L| = |R| = q^2$. It can be shown that the degree of this graph is $O(q)$, and $|E| = O(q^3)$, see [13].

For every integer $n > 0$ we fix a prime number $q_n$ such that $\lceil 2 \log q_n \rceil = n$. For the defined above graph $G = (L \cup R, E)$ for this $\mathbb{F}_{q_n}$ we have $|L| = |R| = 2^{n+O(1)}$ and $|E| = 2^{1.5n+O(1)}$, and Lemma 2 applies to this graph. We should also fix the value of $r$. Any non-zero element of $\mathbb{F}_{q_n}$ would serve the purpose, it only should be computable from $n$. For simplicity we may assume that $r = 1$. In the sequel we denote this graph by $G_n^{Euc}$.

▶ **Example 3** (Hamming distance)**.** We choose $\theta \in (0, \frac{1}{2})$ such that $h(\theta) = 0.5$ for $h(\theta) := -\theta \log \theta - (1-\theta) \log(1-\theta)$. Let $L = R = \{0, 1\}^n$. We define the bipartite graph $G = (L \cup R, E)$ so that two strings (vertices) from $L$ and $R$ are connected if and only if the Hamming distance between them is $\theta n$. Clearly $|L| = |R| = 2^n$. The degree of each vertex is $D = \binom{n}{\theta n} = 2^{0.5n+O(\log n)}$. Lemma 2 applies to this graph. Therefore, for most $(x, y) \in E$ we have (2). In the sequel we denote this graph by $G_{\theta,n}^{Ham}$.

We are interested in properties of $(x, y)$ that are much subtler than those from Lemma 2. For example, we would like to know whether there exists a $z$ materializing a part of the mutual information between $x$ and $y$ (i.e., such that $C(z|x) \approx 0$, $C(z|y) \approx 0$, and $C(z) \gg 0$). These subtler properties are not determined completely by the "complexity profile" of $(x, y)$. In particular, we will see that some of these properties are different for pairs $(x, y)$ from Example 1 and Example 2 on the one hand and from Example 3 on the other hand. In the next section we will show that some information theoretic properties of $(x, y)$ are connected with the spectral properties of these graphs.

**Randomized communication protocols in the information theoretic framework.** In our main results we discuss communication protocols with two parties, Alice and Bob, who are given inputs $x$ and $y$. We will assume that Alice and Bob are given the ends of some edge $(x, y)$ from $G_n^{Pl}$, from $G_n^{Euc}$, or from $G_{\theta,n}^{Ham}$.

We admit randomized communication protocols with private sources of randomness. Technically this means that besides the inputs $x$ and $y$, Alice and Bob are given strings of random bits, $r_A$ and $r_B$ respectively. We assume that both $r_A$ and $r_B$ are binary strings from $\{0,1\}^m$ for some $m = \mathrm{poly}(n)$.

It is helpful to represent the entire inputs available to Alice and Bob as an edge in a graph. The data available to Alice are $x' := \langle x, r_A\rangle$ and the data available to Bob are $y' := \langle y, r_B\rangle$. We can think of the pair $(x', y')$ as an edge in the graph $\widehat{G_n^{Pl}} := G_n^{Pl} \otimes K_{M,M}$ (if $(x,y)$ is an edge in $G_n^{Pl}$), or $\widehat{G_n^{Euc}} := G_n^{Euc} \otimes K_{M,M}$ (if $(x,y)$ is an edge in $G_n^{Euc}$), or $\widehat{G_{\theta,n}^{Ham}} := G_{\theta,n}^{Ham} \otimes K_{M,M}$ (if, respectively, $(x,y)$ is an edge in $G_{\theta,n}^{Ham}$). Here $K_{M,M}$ is a complete bipartite graph with $M = 2^m$ vertices in each part, and $\otimes$ denotes the usual tensor product of bipartite graphs.

Keeping in mind Example 1, Example 2, and Example 3, we obtain that for *most* edges $(x', y')$ in $\widehat{G_n^{Pl}}$, in $\widehat{G_n^{Euc}}$, and in $\widehat{G_{\theta,n}^{Ham}}$ we have

$$\begin{array}{rcrcl} C(x') & = & n & + & m + O(\log n),\\ C(y') & = & n & + & m + O(\log n),\\ C(x',y') & = & 1.5n & + & 2m + O(\log n). \end{array}$$

# 3 Bounds with the spectral method

## 3.1 Information inequalities from the graph spectrum

In this section we show that spectral properties of a graph can be used to prove information theoretic inequalities for pairs $(x, y)$ corresponding to the edges in this graph. We start with a reminder of the standard considerations involving the spectral gap of a graph.

Let $G = (L \cup R, E)$ be a regular bipartite graph of degree $D$ on $2N$ vertices ($|L| = |R| = N$, each edge $e \in E$ connects one vertex from $L$ with another one from $R$, and each vertex is incident to exactly $D$ edges). The adjacency matrix of such a graph is a $(2N) \times (2N)$ zero-one matrix $H$ of the form $\begin{pmatrix} 0 & J \\ J^\top & 0 \end{pmatrix}$ (the $N \times N$ submatrix $J$ is usually called *bi-adjacency* matrix of the graph; $J_{ab} = 1$ if and only if there is an edge between the $a$-th vertex in $L$ and the $b$-th vertex in $R$). Let $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_{2N}$ be the eigenvalues of $H$. Since $H$ is symmetric, all $\lambda_i$ are real numbers. It is well know that for a bipartite graph the spectrum is symmetric, i.e., $\lambda_i = -\lambda_{2N-i+1}$ for each $i$. As the degree of each vertex in the graph is equal to $D$, we have $\lambda_1 = -\lambda_{2N} = D$. We focus on the second eigenvalue of the graph $\lambda_2$; we are interested in graphs such that $\lambda_2 \ll \lambda_1$ (that is, the *spectral gap* is large).

▶ Remark 4. If the bi-adjacency matrix of the graph is symmetric, then the spectrum of the $(2N) \times (2N)$ matrix $H$ consists of the eigenvalues of the $N \times N$ matrix $J$ and their opposites. This observation makes the computation of the eigenvalues simpler.

It is immediately clear that the bi-adjacency matrices of the bipartite graphs from Example 2 and Example 3 are symmetric. For Example 1 this is also true, since a point with coordinates $(x, y)$ and a line indexed $(a, b)$ are incident if $a \cdot x - y - b = 0$.

In the sequel we will use the fact that for the graphs from Example 1 and Example 2 the value of $\lambda_2$ is much less than $\lambda_1 = D$:

▶ **Lemma 5** (see lemma 5.1 in [15]). *For the bipartite graph $G_n^{Pl}$ from Example 1 (incident points and lines on plane $\mathbb{F}_q^2$) the second eigenvalue is equal to $\sqrt{q} = \sqrt{D}$.*

▶ Remark 6. We prove the main result of this paper (Theorem 2) for the construction of $(x, y)$ from Example 1. The same result can be proven for a similar (and even somewhat more symmetric) construction: we can take lines and points in the *projective* plane over a finite field. The projective plane has spectral properties similar to Lemma 5.

▶ **Lemma 7** (see theorem 3 in [13]). *For the bipartite graph $G_n^{Euc}$ from Example 2 (a discrete version of the Euclidean distance) the second eigenvalue is equal to $O(\sqrt{q}) = O(\sqrt{D})$.*

▶ Remark 8. For the tensor product of two graphs $G_1 \otimes G_2$, the eigenvalues can be obtained as pairwise products of the eigenvalues of $G_1$ and $G_2$. So, for the graph $\widehat{G_n^{Pl}}$ (see p. 7) the eigenvalues are all pairwise products of the graph of incidents lines and points $G_n^{Pl}$ and the complete bipartite graph $K_{M,M}$. For $G_n^{Pl}$ the first eigenvalue $D$ and the second eigenvalue $\sqrt{D}$. The bi-adjacency matrix of $K_{M,M}$ is the $M \times M$ matrix with 1's in each cell. It is not hard to see that its maximal eigenvalue is $M$ and all other eigenvalues are 0. Therefore, the first eigenvalue of $\widehat{G_n^{Pl}}$ is equal to $MD$ and the second one is equal to $M\sqrt{D}$. A similar observation is valid for $G_n^{Euc}$.

It is well known that the graphs with a large gap between the first and the second eigenvalues have nice combinatorial properties (vertex expansion, strong connectivity, mixing). One version of this property is expressed by the expander mixing lemma, which was observed by several researchers (see, e.g., [6, lemma 2.5] or [2, theorem 9.2.1]). We use a variant of the expander mixing lemma for bipartite graphs (see [5]):

▶ **Lemma 9** (Expander Mixing Lemma). *Let $G = (L \cup R, E)$ be a regular bipartite graph, where $|L| = |R| = N$ and each vertex has degree $D$. Then for each $A \subseteq L$ and $B \subseteq R$ we have $\left|E(A,B) - \frac{D \cdot |A| \cdot |B|}{N}\right| \leq \lambda_2 \sqrt{|A| \cdot |B|}$, where $\lambda_2$ is the second largest eigenvalue of the adjacency matrix of $G$ and $E(A,B)$ is the number of edges between $A$ and $B$.*

▶ Remark 10. In what follows we apply Lemma 9 to the graphs with a large gap between $D$ and $\lambda_2$. This technique is pretty common. See, e.g., [21, Theorem 3] where the Expander Mixing Lemma was applied to the graph from Example 1. Due to technical reasons, we will need to apply the Expander Mixing Lemma not only to the graph $G_n^{Pl}$ from Example 1 and $G_n^{Euc}$ from Example 2 but also to the tensor product of these graphs and a complete bipartite graph, see below.

In what follows we use a straightforward corollary of the expander mixing lemma:

▶ **Corollary 11.** *(a) Let $G = (L \cup R, E)$ be a graph satisfying the same conditions as in Lemma 2 with $\lambda_2 = O(\sqrt{D})$. Then for $A \subseteq L$ and $B \subseteq R$ such that $|A| \cdot |B| \geq N^2/D$ we have*

$$|E(A,B)| = O\left(\frac{D \cdot |A| \cdot |B|}{N}\right). \tag{3}$$

*(b) Let $G = (L \cup R, E)$ be the same graph as in (a), and let $K_{M,M}$ be a complete bipartite graph for some integer $M$. Define the tensor product of these graphs $\hat{G} := G \otimes K_{M,M}$ (this is a bipartite graph $(\hat{L} \cup \hat{R}, \hat{E})$ with $|\hat{L}| = |\hat{R}| = N \cdot M$, with degree $D \cdot M$). Then for all subsets $A \subset \hat{L}$ and $B \subset \hat{R}$ such that $|A| \cdot |B| \geq (MN)^2/D$ inequality (3) holds true.*

(See the proof of the corollary in the full version of the paper.)

Now we translate the combinatorial property of *mixing* in the information-theoretic language. We show that a large spectral gap in a graph implies some inequality for Kolmogorov complexity that is valid for each pair of adjacent vertex in this graph. We do it in the next lemma, which is the main technical ingredient of the proof of our main result.

▶ **Lemma 12.** *Let $G = (L \cup R, E)$ be a graph satisfying the same conditions as in Lemma 2, with $|L| = |R| = N$ and degree $D = O(\sqrt{N})$. Assume also that the second largest eigenvalue of this graph is $\lambda_2 = O(\sqrt{D})$. Let $K_{M,M}$ be a complete bipartite graph for some $M = 2^m$. Define the tensor product of these graphs $\hat{G} := G \otimes K_{M,M}$.*

*For each edge $(x, y)$ in $\hat{G}$ and for all $w$, if $C(x|w) + C(y|w) > 1.5n + 2m$ then we have $I(x : y|w) \geq 0.5n + O(\log k)$, where $k = n + m$.*

▶ Remark 13. Note that Lemma 12 applies to the graphs from Example 1 and Example 2 due to Lemma 5 and Lemma 7 respectively.

**Proof.** Denote $a = C(x|w)$ and $b = C(y|w)$. By the assumption of the lemma we have $a + b > 1.5n + 2m$. Let $A$ be the set of all $x' \in L$ such that $C(x'|w) \leq a$ and $B$ be the set of all $y' \in R$ such that $C(y'|w) \leq b$. Note that by definition $A$ contains $x$ and $B$ contains $y$. In what follows we show that for all pairs $(x', y') \in (A \times B) \cap E$ we have $C(x, y) \leq a + b - 0.5n$.

▷ Claim 1. We have $|A| = 2^{a+O(\log k)}$ and $|B| = 2^{b+O(\log k)}$.

Proof of the claim 1: We start with a proof of the upper bounds. Each element of $A$ can be obtained from $w$ with a programs (description) of length at most $a$. Therefore, the number of elements in $A$ is not greater than the number of such descriptions, which is at most $1 + 2 + \ldots + 2^a < 2^{a+1}$. Similarly, the number of elements in $B$ is less than $2^{b+1}$.

Now we proceed with the lower bounds. Given $w$ and an integer number $a$ we can take all programs of size at most $a$, apply them to $w$ and run in parallel. As some programs converge, we will discover one by one all elements in $A$ (though we do not know when the last stopping program terminates, and when the last element of $A$ is revealed). The element $x$ must appear in this enumeration. Therefore, we can identify it given its position in this list, which requires only $\log |A|$ bits. Thus, we have $C(x|w) \leq \log |A| + O(\log k)$ (the logarithmic additive term is needed to specify the binary expansion of $a$). On the other hand, we know that $C(x|w) = a$. It follows that $|A| \geq 2^{a-O(\log k)}$, and we are done. The lower bound $|B| \geq 2^{b-O(\log k)}$ can be proven in a similar way. ◁

▷ Claim 2. The number of edges between $A$ and $B$ is rather small: $|(A \times B) \cap E| \leq O\left(\frac{D \cdot |A| \cdot |B|}{N}\right)$.

Proof of the claim 2: By Claim 1 we have $|A| = 2^{a+O(\log k)}$ and $|B| = 2^{b+O(\log k)}$. Since $a + b > 1.5n$ we obtain $|A| \cdot |B| = 2^{a+b+O(\log k)} > 2^{1.5n+2m} = (NM)^2/D$. Hence, we can apply Corollary 11 (b) and obtain the claim. ◁

▷ Claim 3. For all pairs $(x', y') \in (A \times B) \cap E$ we have $C(x', y'|w) \leq \log |E(A, B)| + O(\log k)$.

Proof of the claim 3: Given a string $w$ and the integer numbers $a$, $b$, we can run in parallel all programs of length at most $a$ and $b$ (applied to $w$) and reveal one by one all elements of $A$ and $B$. If we have in addition the integer number $n$, then we can construct the graph $G$ and enumerate all edges between $A$ and $B$ in the graph $G$. The pair $(a', b')$ must appear in this enumeration. Therefore, we can identify it by its ordinal number in this enumeration. Thus, $C(x', y'|w) \leq \log |E(A, B)| + O(\log k)$, where the logarithmic term involves the binary expansions of $n$, $a$, and $b$.

Now we can finish the proof of the lemma. By claim 3, we have $C(x', y'|w) \leq \log |E(A, B)| + O(\log k)$ for all pairs $x', y' \in (A \times B) \cap E$. By using claim 2, we obtain $C(x', y'|w) \leq \log D +$

$\log|A|+\log|B|-\log N+O(1)$. With claim 1 this rewrites to $C(x',y'|w)\le a+b-0.5n+O(1)$. Now we apply this inequality to the initial $x$ and $y$:

$$\begin{aligned} I(x:y|w) &= C(x'|w)+C(y'|w)-C(x',y'|w)+O(\log n)\\ &\ge a+b-(a+b-0.5n)+O(\log k)-O(\log n)=0.5n+O(\log n). \end{aligned}$$

◁

◀

## 3.2 Information inequalities for a secret key agreement

In this section we prove some information theoretic inequalities that hold true for the objects involved in a communication protocol: the inputs given to Alice and Bob, the transcript of the communication, and the final result computed by Alice and Bob.

In the sequel we use the following lemma from [16] (see also a similar result proven for Shannon entropy in [7]):

▶ **Lemma 14** ([16]). *Let us consider a communication protocol with two parties. Denote by $x$ and $y$ the inputs of the parties, and denote by $t=t(x,y)$ the transcript of the communication between the parties. Then $I(x:y|t)\le I(x:y)+O(\log n)$, where $n$ is the sum of complexities of $x,y,t$.*

▶ **Proposition 15** (Muchnik's theorem on conditional descriptions, [14]). *(a) Let $a$ and $b$ be arbitrary strings of length at most $n$. Then there exists a string $p$ of length $C(a|b)$ such that $C(p|a)=O(\log n)$ and $C(a|p,b)=O(\log n)$.*

*(b) Let $a,b_1,b_2$ be arbitrary strings of length at most $n$. Then there exist strings $q_1$, $q_2$ of length $C(a|b_1)$ and length $C(a|b_2)$ respectively such that $C(q_j|a)=O(\log n)$ and $C(a|b_j,q_j)=O(\log n)$ for $j=1,2$; we may also require that one of the strings $q_1,q_2$ is a prefix of another one. As usual, the constants in $O(\log n)$-notation do not depend on $n$.*

▶ Remark 16. In Proposition 15(a) the string $p$ can be interpreted as an almost shortest description of $a$ conditional on $b$ that satisfies a nice additional property: it can be easily computed given $a$. Similarly, in Proposition 15(b) the strings $q_1$ and $q_2$ can be interpreted as almost shortest descriptions of $a$ given $b_1$ and $b_2$ respectively. The non-trivial part of (b) is the requirement that one of the strings $q_1,q_2$ (the shorter one) is a prefix of the other (the longer) one. In particular, if $C(a|b_1)=C(a|b_2)$, then $q_1=q_2$, and we can use *one and the same* shortest program to transform $b_1$ or $b_2$ into $a$.

We combine Lemma 14 and Proposition 15 to prove the next technical lemma.

▶ **Lemma 17.** *Assume a deterministic communication protocol for two parties on inputs $x$ and $y$ gives transcript $t$ and denote $n=C(x,y,t)$.*
*(a) $C(t|x,y)=O(\log n)$; (b) $C(t|x)=I(t:y|x)+O(\log n)$; (c) $C(t|y)=I(t:x|y)+O(\log n)$;*
*(d) $C(t|x)+C(t|y)=I(t:x|y)+I(t:y|x)+O(\log n)\le C(t)+O(\log n)$;*
*(e) There exist $t_x$ and $t_y$ such that*

- *$C(t_x)=C(t|x)$ and $C(t_y)=C(t|y)$,*
- *$C(t_x|t)=O(\log n)$ and $C(t_y|t)=O(\log n)$,*
- *$C(t|t_x,x)=O(\log n)$ and $C(t|t_y,y)=O(\log n)$,*
- *$C(t_x,t_y)=C(t_x)+C(t_y)+O(\log n)$.*

*Speaking informally, $t_x$ and $t_y$ are "fingerprints" of $t$ that can play the roles of (almost) shortest descriptions of $t$ conditional on $x$ and $y$ respectively. The last condition means that the mutual information between $t_x$ and $t_y$ is negligibly small.*

This lemma is a technical statement, and its claim (e) might look artificial. However, this claim has an intuitive motivation. In natural examples of communication protocols, each message of Alice can be chosen in such a way that it is has virtually no mutual information with Bob's input $y$ (even given all the previous messages of the protocol as a condition). Similarly, each message of Bob can be chosen in such a way that it has virtually no mutual information with Alice's input $x$ (again, given all the previous messages of the protocol as a condition). In such a "natural" protocol, the communication transcript can be subdivided into two components with (virtually) no mutual information between them: the first component $t_A$ consists of all Alice's messages, and the second component $t_B$ consists of all Bob's messages. Then, these components would have properties similar to those of $t_y$ and $t_x$ in the lemma. Thus, a transformation of the transcript $t$ into a pair $\langle t_x, t_y\rangle$ can be interpreted as a reduction of an arbitrary protocol to a "compressed" form.

If a protocol is not "natural" in the sense explained above, we can compress all its messages using Muchnik's method (Lemma 15). But technically, the reduction of an arbitrary protocol to its compressed version is more involved when the number of rounds in the protocol is unbounded. In this case we have to use a less intuitive argument based on Lemma 14, which helps to handle the transcript of a protocol in one piece, without splitting it into separate messages. The complete proof of Lemma 17 is given in the full version of the paper.

## 3.3 Proof of the main result

Now we are ready to combine the spectral technique from Section 3.1 and the information theoretic technique from Section 3.2 and prove our main result.

**Proof of Theorem 2.** Let us take a pair of $(x, y)$ from Example 1 or Example 2. We know that it satisfies (2). Assume that in a communication protocol $\pi$ Alice and Bob (given as inputs $x$ and $y$ respectively) agree on a secret key $z$ of size $\delta(n)$. We will prove a lower bound on the communication in this protocol. To simplify the notation, in what follows we ignore the description of $\pi$ in all complexity terms (assuming that it is a constant, which is negligible compared with $n$).

In this proof we will deal with four objects: the inputs $x' = \langle x, r_A\rangle$ and $y' = \langle y, r_B\rangle$, the transcript $t$, and the output of the protocol (secret key) $z$. Our aim is to prove that $C(t)$ cannot be much less than $0.5n$. This is enough to conclude that the length of the transcript measured in bits (which is exactly the communication complexity of the protocol) also cannot be much less than $0.5n$. Due to some technical reasons that will be clarified below we need to reduce in some sense the sizes of $t$ and $z$.

**Reduction of the key.** First of all, we reduce the size of $z$. This step might seem counter-intuitive: we make the assumption of the theorem *weaker* suggesting that Alice and Bob agree on a rather small secret key. We know from [16] that $C(z)$ can be pretty large (more specifically, it can be of complexity $0.5n + O(\log n)$). However, we prefer to deal with protocols where Alice and Bob agree on a moderately small (but still not *negligibly* small) key. To this end we may need to degrade the given communication protocol and reduce the size of the secret key to the value $\mu \log n$ (the constant $\mu$ to be chosen later). It is simple to make the protocol weaker: if the original protocol provides a common secret key $z$ of bigger size, then in the degraded protocol Alice and Bob can take only the $\delta(n)$ first bits of this key. Thus, without loss of generality, we may assume that the protocol gives a secret key $z$ with complexity $\delta(n) = \mu \log n$.

**Reduction of the transcript.** Now we perform a reduction of $t$. We known from Lemma 14 that the difference $I(x' : y') - I(x' : y'|t)$ is non-negative. We want to reduce $t$ to a $t'$ such that the difference $I(x' : y') - I(x' : y'|t')$ is exactly 0 (here *exactly* means, as usual, an equality that holds up to $O(\log n)$). To this end, we apply Lemma 17 to the triple $(x', y', t)$ and obtain $t_x$ and $t_y$, which play the roles of optimal descriptions of $t$ given the conditions $x'$ and $y'$ respectively. We let $t' := \langle t_x, t_y \rangle$. Though technically this $t'$ is not a transcript of any communication protocol, we will see that in some sense it behaves similarly to the initial transcript.

We know from Lemma 17(d,e) that $C(t') \le C(t) + O(\log n)$. Thus, to prove the theorem, it is enough to show that $C(t') \ge 0.5n - 2\delta(n) - O(\log n)$.

▶ **Lemma 18.** *For $t' = \langle t_x, t_y \rangle$ we have the following equalities:*
*(a) $C(x'|t', z) = n + m - C(t_y) - \delta(n) + O(\log n)$,*
*(b) $C(y'|t', z) = n + m - C(t_x) - \delta(n) + O(\log n)$, and*
*(c) $I(x' : y'|t', z) = I(x' : y') - C(z) + O(\log n) = 0.5n - \delta(n) + O(\log n)$.*

(See the proof of the lemma in the full version of the paper.)

Now we are ready to prove the theorem. Assume that

$$C(t_x) + C(t_y) < 0.5n - 2\delta(n) - \lambda \log n. \tag{4}$$

If the constant $\lambda$ is large enough, then we obtain from Lemma 18(a,b) $C(x'|t', z) + C(y'|t', z) > 1.5n + 2m$. Now we can apply Lemma 12 (the spectral bound applies to Example 1 and Example 2, see Remark 13), which gives

$$I(x' : y'|t', z) \ge 0.5n + O(\log n). \tag{5}$$

Comparing Lemma 18(c) and (5) we conclude that $\delta(n) = O(\log n)$ (the constant hidden in $O(\cdot)$ depends only on the choice of optimal description method in the definition of Kolmogorov complexity). This contradicts the assumption $\delta(n) = \mu \log n$, if $\mu$ is chosen large enough. Therefore, the assumption in (4) is false (without this assumption we cannot apply Lemma 12 and conclude with (5)).

The negation of (4) gives $C(t) \ge C(t_x) + C(t_y) - O(\log n) \ge 0.5n - 2\delta(n) - O(\log n)$, and we are done. ◀

## 4 Pairs with a fixed Hamming distance

Theorem 2 estimates communication complexity of the protocol in the worst case. For some classes of inputs $(x, y)$ there might exist more efficient communication protocol. In this section we study one such special class – the pairs $(x, y)$ from Example 3. The spectral argument from the previous section does not apply to this example. The spectral gap for the graph from Example 3 is too small: for this graph we have $\lambda_2 = \Theta(\lambda_1)$, while in Example 1 and Example 2 we had $\lambda_2 = O(\sqrt{\lambda_1})$ (the eigenvalues of the graph from Example 3 can be computed explicitly, see [3] and the survey [11]).

It is no accident that our *proof* of Theorem 2 fails on Example 3. In fact, the *statement* of the theorem is not true for $(x, y)$ from this example. In what follows we show that given these $x$ and $y$ Alice and Bob can agree on a secret key of any size $m$ (intermediate between $\log n$ and $n/2$) with communication complexity $\Theta(m)$. The positive part of this statement (the existence of a communication protocol with communication complexity $O(m)$) is proven in Theorem 3. The negative part of the statement (the lower bound $\Omega(m)$ for all communication protocols) is proven in Theorem 4.

▶ **Theorem 3.** For every $\delta \in (0,1)$ there exists a two-parties randomized communication protocol $\pi$ such that given inputs $x$ and $y$ from Example 3 (a pair of $n$-bit strings with the Hamming distance $\theta n$ and complexity profile (2)) Alice and Bob with probability $> 0.99$ agree on a secret key $z$ of size $\delta n/2 - o(n)$ with communication complexity $O(\delta n)$. (The constant hidden in the $O(\cdot)$ does not depend on $n$ or $\delta$.)

**Sketch of the proof.** It is enough to apply the communication protocol from Theorem 1 (see [16]) to the prefixes of $x$ and $y$ of length $\delta n$. See the full version of the paper for details. ◀

▶ **Theorem 4.** For every $\delta \in (0,1)$ for every randomized communication protocol $\pi$ such that for inputs $x$ and $y$ from Example 3 Alice and Bob with probability $> 0.99$ agree on a secret key $z$ of size $\geq \delta n$, the communication complexity is at least $\Omega(\delta n)$. (The constant hidden in the $\Omega(\cdot)$ does not depend on $n$ or $\delta$.)

**Sketch of the proof.** The argument is based on the following fact proven in [17]. For some $k = O(1)$ there exist two sequences of $n$-bit binary strings $x_1, \dots, x_k$ and $y_1, \dots, y_k$ such that

- $I(x_i : y_i | x_{i+1}) = O(\log n)$ for $i = 0, \dots, k-1$,
- $I(x_i : y_i | y_{i+1}) = O(\log n)$ for $i = 0, \dots, k-1$,
- $I(x_k : y_k) = O(\log n)$

(here $x_0 = x$ and $y_0 = y$). The lower bound for communication complexity can be proven with standard information inequalities applied to $x = x_0, x_1, \dots, x_k$ and $y = y_0, y_1, \dots, y_k$, see the full version of the paper for details. ◀

## 5 Conclusion

In Theorem 2 we have proven a lower bound for communication complexity of protocols with *private* randomness. The argument can be extended to the setting where Alice and Bob use both *private* and *public* random bits (the private sources of randomness are available only to Alice and Bob respectively; the public source of randomness is available to both parties and to the eavesdropper). Thus, the problem of the *worst case* complexity is resolved for the most general natural model of communication. At the same time, we have no characterization of the optimal communication complexity of the secret key agreement for pairs of inputs $(x, y)$ that do not enjoy the spectral property required in Corollary 11. In particular, there is a large gap between constant hidden in the $O(\delta n)$ notation in Theorem 3 and in the $\Omega(\delta n)$ notation in and Theorem 4, so the question on the optimal trade-off between the secret key size and communication complexity for $(x, y)$ from Example 3 remains open (*cf.* Conjecture 1 in [10] for an analogous problem in Shannon's setting).

Our main result is proven only for communication protocols where Alice and Bob use at most $m \leq \text{poly}(C(x) + C(y))$ random bits. The reason is that the proven bounds involve an error term $O(\log m)$, which comes from the Kolmogorov–Levin theorem. We conjecture that Theorem 2 remains valid without this restriction, although our proof fails if the number of public random bits used in the protocol is super-polynomial.

## References

1 Rudolf Ahlswede and Imre Csiszár. Common randomness in information theory and cryptography. I. Secret sharing. *IEEE Transactions on Information Theory*, 39(4):1121–1132, 1993.

2 Noga Alon and Joel H. Spencer. *The probabilistic method*. John Wiley & Sons, 2004.

3 Andries E. Brouwer, Sebastian M. Cioabă, Ferdinand Ihringer, and Matt McGinnis. The smallest eigenvalues of hamming graphs, johnson graphs and other distance-regular graphs with classical parameters. *Journal of Combinatorial Theory, Series B*, 133:88–121, 2018.

4 Alexei Chernov, Andrej Muchnik, Andrei Romashchenko, Alexander Shen, and Nikolai Vereshchagin. Upper semi-lattice of binary strings with the relation "x is simple conditional to y". *Theoretical Computer Science*, 271(1-2):69–95, 2002.

5 Shai Evra, Konstantin Golubev, and Alexander Lubotzky. Mixing properties and the chromatic number of ramanujan complexes. *International Mathematics Research Notices*, 2015(22):11520–11548, 2015.

6 Shlomo Hoory, Nathan Linial, and Avi Wigderson. Expander graphs and their applications. *Bulletin of the American Mathematical Society*, 43(4):439–561, 2006.

7 Tarik Kaced, Andrei Romashchenko, and Nikolai Vereshchagin. A conditional information inequality and its combinatorial applications. *IEEE Transactions on Information Theory*, 64(5):3610–3615, 2018.

8 Eyal Kushilevitz and Noam Nisan. *Communication Complexity*. Cambridge University Press, 2006.

9 Ming Li and Paul Vitányi. *An introduction to Kolmogorov complexity and its applications*. Springer, 4 edition, 2019.

10 Jingbo Liu, Paul Cuff, and Sergio Verdú. Secret key generation with limited interaction. *IEEE Transactions on Information Theory*, 63(11):7358–7381, 2017.

11 Xiaogang Liu and Sanming Zhou. Eigenvalues of cayley graphs. *arXiv preprint arXiv:1809.09829*, 2018.

12 Ueli M. Maurer. Secret key agreement by public discussion from common information. *IEEE transactions on information theory*, 39(3):733–742, 1993.

13 Archie Medrano, Perla Myers, Harold M. Stark, and Audrey Terras. Finite analogues of euclidean space. *Journal of Computational and Applied Mathematics*, 68(1-2):221–238, 1996.

14 Andrej A. Muchnik. Conditional complexity and codes. *Theoretical Computer Science*, 271(1-2):97–109, 2002.

15 Omer Reingold, Salil Vadhan, and Avi Wigderson. Entropy waves, the zig-zag graph product, and new constant-degree expanders and extractors. In *Proceedings 41st Annual Symposium on Foundations of Computer Science*, pages 3–13. IEEE, 2000.

16 Andrei Romashchenko and Marius Zimand. An operational characterization of mutual information in algorithmic information theory. *Journal of the ACM (JACM)*, 66(5):1–42, 2019.

17 Andrei E. Romashchenko. Pairs of words with nonmaterializable mutual information. *Problems of Information Transmission*, 36(1), 2000.

18 Alexander Shen, Vladimir Uspensky, and Nikolay Vereshchagin. *Kolmogorov complexity and algorithmic randomness*, volume 220. American Mathematical Soc., 2017.

19 Madhu Sudan, Himanshu Tyagi, and Shun Watanabe. Communication for generating correlation: A unifying survey. *IEEE Transactions on Information Theory*, 66(1):5–37, 2019.

20 Himanshu Tyagi. Common information and secret key capacity. *IEEE Transactions on Information Theory*, 59(9):5627–5640, 2013.

21 Le Anh Vinh. The Szemerédi–Trotter type theorem and the sum-product estimate in finite fields. *European Journal of Combinatorics*, 32(8):1177–1181, 2011.

22 Alexander K. Zvonkin and Leonid A. Levin. The complexity of finite objects and the development of the concepts of information and randomness by means of the theory of algorithms. *Russian Mathematical Surveys*, 25(6):83, 1970.