2024 IEEE International Symposium on Information Theory (ISIT) | 979-8-3503-8284-6/24/$31.00 ©2024 IEEE | DOI: 10.1109/ISIT57864.2024.10619079

Unconditional Security using (Random) Anonymous Bulletin Board

Albert Yu[*], Hai H. Nguyen[†], Aniket Kate[*‡], Hemanta K. Maji[*]
[*]Purdue University, {yu646, aniket, hmaji}@purdue.edu
[†]ETH Zurich, nhhai196@gmail.com
[‡]Supra Research

***Abstract*—In a seminal work, Ishai et al. (FOCS–2006) studied the viability of designing unconditionally secure protocols for key agreement and secure multi-party computation (MPC) using an anonymous bulletin board (ABB) as a building block. While their results establish the feasibility of key agreement and honest-majority MPC in the ABB model, the optimality of protocols with respect to their round and communication complexity is not studied. This paper enriches this study of unconditional security in the ABB model in multiple ways.**

- **We present a key agreement protocol with a novel combinatorial insight to offer a 200% throughput over the (FOCS–2006) study; i.e., using the same number of messages, we can (almost) double the bit-length of the agreed key. We also prove the near optimality of our approach.**
- **We offer unconditionally secure protocols for the (random) string oblivious transfer functionalities. We present a 1-round chosen message random string oblivious transfer and show how to extend it to a non-interactive (random) string oblivious transfer protocol and a 2-round chosen message string oblivious transfer.**
- **We prove a 1-round communication lower bound for BEC under certain conditions.**

Central to our technical contributions is the abstraction of a distributional variant of the random ABB functionality. Investigating the concrete efficiency of founding MPC from this primitive leads to fascinating new mathematical challenges in well-established MPC models, which will be of broader interest to the community.

I. Introduction

Securely realizing unconditionally secure cryptographic primitives is a topic of immense value and has a rich history. This work revisits a particularly surprising work by Ishai et al. [22] that analyzes the possibility of performing cryptography with unconditional security using an *anonymous bulletin board* (ABB). Ishai et al. establish unconditional security for prominent cryptographic tasks such as key agreement and honest-majority secure multiparty computation (MPC) based solely on access to an ABB that allows a sender to publish her message without revealing her identity. In particular, they demonstrate that ABB is sufficient to implement unconditionally secure point-to-point channels between two parties without making any other assumption. Ishai et al. then extend it to achieve MPC with unconditional security in the presence of an honest majority, diversifying the primitives that facilitate secure computation. Interestingly, they complement these constructions by showing the impossibility of unconditional secure computation using anonymous broadcast without an honest majority.

Since the publication of the paper by Ishai et al. in 2006, the field of anonymous communication has witnessed tremendous growth: the anonymous communication network Tor [14] serves more than two million unique users daily using an overlay network of several thousand nodes all over the Internet. As the use of blockchains brings users' financial dealings to the (public) Internet, there have been significant efforts towards introducing and improving anonymity over the Internet. Startups such as Nym [13] and xx.network [35], [36] are developing generic anonymous communication networks to break the link between users' identity and their transactions, and several blockchain projects have started incorporating anonymous communications, such as Tor and I2P, in their designs [21]. Academic literature on anonymous communication, as well as protocol implementations, have significantly expanded in the last two decades [1], [6], [11], [15], [26]. It is safe to say that ABBs are prevalent on the Internet today. Motivated by these real-world applications, we aim to understand the efficacy and concrete efficiency of developing cryptography assuming access to such an ABB.

The utility of the ABB towards unconditional security is easy to illustrate using Alpern and Schneider's [5] elegant key agreement protocol between Alice and Bob against an honest-but-curious adversary, which is referenced in Ishai et al. [22]. Alice and Bob independently pick random integers (say r_A and r_B, respectively) and publish those to the anonymous broadcast channel. The agreed single secret bit is 1 if $r_A > r_B$ and 0 if $r_A < r_B$. If $r_A = r_B$, Alice and Bob fail to establish the secret bit and rerun the protocol. Notice that Alice and Bob know their respective input and thus can compute the secret bit; however, eavesdroppers cannot distinguish r_A from r_B and have no information about the agreed bit. Moreover, the failure probability (using the birthday bound) depends on the size of the sample space of the integers.

This "indistinguishability property" can be abstracted as a multi-set. Conceptually, we observe that using ABB converts a vector (or key-value store) of user inputs to a multi-set. This brings us to the question: what if Alice and Bob send multiple (say m) messages each? Can we agree on more than m bits using this $2m$-sized multi-set? We answer this question affirmatively to demonstrate that Alice and Bob can indeed agree on close to $2m$ secret bits, which improves the through-

979-8-3503-8284-6/24/$31.00 ©2024 IEEE

put of the key agreement to 200%, as compared to Alpern and Schneider [5]. This work aims to determine the concrete communication and round complexity of key cryptographic functionalities based on anonymity. This investigation leads to both qualitative and quantitative research questions in this context.

To this end, we establish connections of implementing functionalities using ABB in our context with various well-studied communication-limited MPC models (like *non-interactive correlation distillation* [32], [33], *secure non-interactive simulation/reduction* [2], [24], *one-way secure computation* [18], and *private simultaneous messages* [16]). Our problems translate into analytically tractable instances of these MPC models, which are generally challenging to analyze. These connections lead us to several near-optimal protocol constructions. Our practically-motivated research objectives lead to fascinating research questions in these MPC models, potentially of interest to the broader cryptographic & information theory community.

A. Our Contributions

From the modeling perspective, this work assumes the existence of an anonymous broadcast, which we model as an Anonymous Bulletin Board (ABB) hybrid. There are four parties $\mathcal{A}, \mathcal{B}, \mathcal{C}$, and $\mathcal{D}$. The bulletin board ideal functionality, represented as $\mathsf{ABB}_{m_A,m_B,m_C}$, takes as input three multi-sets: (1) $A := \{a_1, \ldots, a_{m_A}\}$ from party $\mathcal{A}$, (2) $B := \{b_1, \ldots, b_{m_B}\}$ from $\mathcal{B}$, and (3) $C := \{c_1, \ldots, c_{m_C}\}$ from $\mathcal{C}$. Note that party $\mathcal{D}$ does not provide any input. The functionality outputs the multi-set $\Gamma = A \cup B \cup C := \{\gamma_1, \ldots, \gamma_{m_A+m_B+m_C}\}$ to all four parties.

We refer to party $\mathcal{C}$ as the *helper* and party $\mathcal{D}$ as the *eavesdropper*. In the randomized version of bulletin board (rABB), the three multi-sets A, B, C are sampled according to some independent distributions P, Q, R, respectively. We note that the rABB functionality is as powerful as the ABB functionality when messages are not chosen adaptively.

In addition to the bulletin board, parties also have public authenticated channels between them. In the ABB setting, we define each party's *communication complexity* as the number of bits that the party sends to the ABB plus the number of bits it sends to other parties through the public authenticated channels. We define the communication complexity in the rABB setting in a similar manner.

The sequel summarizes our contributions.

Result 1 (Key-agreement Protocol: Informal)**.** *We present a* non-interactive *two-party key-agreement protocol using* $\mathsf{rABB}_{m,m,0}$ *with individual message length* n *that establishes (near-optimal)* $2m$*-bit keys with* $(m \cdot n)$*-bit communication complexity.* [1]

Our construction is secure against a computationally unbounded eavesdropper $\mathcal{D}$. Our construction is straightforward to implement, and the key length (i.e., throughput) is near-optimal. Here, throughput is the ratio of the key length to the number of messages. The length n of the individual messages affects our algorithm's failure probability, the event where parties fail to agree on a key. Small messages would result in close-to-1 failure probability. Surprisingly, when n is larger than a particular threshold, it has essentially no impact on the key length. We also present a duplicate-recovery variant of the protocol in Result 1, which is suitable for other parameter regimes.

Remark 1 (Upper bound on our key length: additional comments)**.** *Our proof of the optimality of our key length considers a wide family of protocols. In these protocols, parties can interact over multiple rounds using the public authenticated channels after the* rABB *invocation. The parties* $\mathcal{A}$*,* $\mathcal{B}$*, and* $\mathcal{C}$ *receive messages from arbitrary independent message distributions* P, Q*, and* R*, respectively (not necessarily the uniform distribution). In our protocol,* rABB *delivers random independent messages to the parties. We prove this result using mutual information, entropy-based arguments, and the recent results of [27], [28].*

In our protocol, parties have access to a *single* ABB *or* rABB that they call once. Many other protocols (such as [8], [12], and some protocols in [22]) either require additional assumptions, such as on the synchrony of the system model or require multiple independent instances of ABB to be implemented. We emphasize that this is qualitatively different from our protocol setting, and a direct comparison of the communication costs of these protocols against ours results in an inaccurate representation of both their protocols and ours. Therefore, we focus our concrete communication cost analysis on comparison with the state-of-the-art protocol in this setting, which is [5].

For typical values of k such as 128, [5] requires roughly $2.9\times$ our communication cost. (See Figure 1 in [38].)

In the context of implementing oblivious transfers, Ishai et al. [22] proved the impossibility of realizing oblivious transfer (OT) using ABB when honest parties are not in the majority. This implies that it is impossible to realize oblivious transfers (as well as their randomized versions) in the ABB-hybrid without the helper party $\mathcal{C}$. We construct oblivious transfer protocols that achieve a few different functionality variants – a step towards diversifying setups for oblivious transfers.

Result 2. *We present a* 1*-round protocol for establishing chosen message random string oblivious transfer (*cmROT^{ℓ}*) from sender* $\mathcal{B}$ *to receiver* $\mathcal{A}$ *with the helper* $\mathcal{C}$*. The protocol is round-optimal.*

The cmROT^{ℓ} functionality takes as input two ℓ-bit messages x_0 and x_1 from the sender and delivers the tuple (b, x_b) to the receiver, where the bit b is chosen uniformly at random.

The round optimality of this construction is a consequence of Result 3 and the fact that one can use (chosen message)

[1] The formal statement for this result can be found as Theorem 1 in Section V-C in the full version of the paper [38].

random string OT to implement an erasure channel.[2] The following results are consequences of Result 2.

Corollary I.1. *There is a non-interactive protocol for establishing random string oblivious transfer (*ROT^ℓ*) from sender* $\mathcal{B}$ *to receiver* $\mathcal{A}$ *with the helper* $\mathcal{C}$.[3]

Corollary I.2. *There is a two-round protocol for establishing (chosen message) string oblivious transfer (*cmOT^ℓ*) from sender* $\mathcal{B}$ *to receiver* $\mathcal{A}$ *with the helper* $\mathcal{C}$.[3]

Corollary I.3. *All protocols in Result 2, Corollary I.1, and Corollary I.2 are easily extended to 1-out-of-*N *OT (where the sender has* N *inputs).*

Corollary I.4. *Binary Erasure Channel (BEC) with erasure probability* $\frac{e}{d} \in (0,1)$ *is realizable using 1-out-of-*d *ROT from Corollary I.3.*

This can be done by having e of the messages be a special "erasure" symbol while the remaining $(d-e)$ messages are identical to the transmitted bit.

Garg et al. [18] showed that any (possibly randomized) sender-receiver function is realizable using one-way communication over ROT channel that is equivalent to cmROT^ℓ without communication. Thus, the following result is a straightforward consequence of Result 2 and [18].

Corollary I.5. *Any (possibly randomized) sender-receiver function is realizable using* rABB *with one round of communication.*

Remark 2 (New research problems in interaction-limited MPC models)**.** *Our use of* $\mathsf{rABB}^{P,Q,R}$ *can be interpreted as sampling from the joint distribution* $(P,Q,R|\Gamma)$ *in a preprocessing step, where* Γ *is the union of the three. Under this interpretation, our research problems translate into research questions in the NICD [32], [33], SNIS [24], SNIR [2], OWSC [18], and PSM [16] models.*

1) *For key agreement, we prove that the uniform distribution achieves the optimal result even against arbitrary independent distributions.*
2) *For random string oblivious transfer, we show that by using specialized distributions* P, Q, R*, we are able to obtain non-interactive random string oblivious transfer.*

Result 3. *We prove a* 1*-round lower bound for implementing a binary erasure channel from* $\mathcal{B}$ *to* $\mathcal{A}$ *utilizing the* rABB *(with a helper) and a public authenticated channel from* $\mathcal{B}$ *(the sender) to* $\mathcal{A}$ *(the receiver) when the messages are sampled from* uniform distributions P, Q, R.

We employ the techniques from secure non-interactive simulation (SNIS/SNIR), recently introduced in [2], [24], [25], to prove the above result.

Note that proving the optimality for *arbitrary independent distributions* P, Q, R remains open. Recall P, Q, R represent the distribution of the messages sent by rABB to the parties $\mathcal{A}, \mathcal{B}$, and $\mathcal{C}$, respectively. Analyzing this distributional variant of rABB motivates new research directions in interaction-limited MPC models, like SNIS and SNIR. This problem is challenging even when P, Q, R are flat distributions over a sparse subset of the message space. Typically, these models (like NICD [32], [33], SNIS [24], SNIR [2], OWSC [18], and PSM [16]) have strong hardness-of-computation results. However, for our application scenarios, there are non-trivial and practically useful constructions as well.

B. Related Works

1) Key-Agreement: Many works focus on key-agreement or developing secure point-to-point links based on anonymous communication. [5] performs key agreements using sets of position-labeled bits sent by the parties. [39] expands [5] to work over semi-honest channels. [8] relies on the fact that parties can set the source of the message to be honest or false and send messages in random orders. [12] similarly proposes a protocol that requires the parties to send messages in random order by implementing random wait times. [34] considers key-agreement when the receivers (instead of the senders) are anonymous. [17] considers key-agreement in a similar setting, where a "deck of cards" is dealt to the parties with the remaining cards dealt to the adversary. Finally, Gilad and Herzberg [19] demonstrate the practical utility of [22] for the IP-level security protocol IPSec.

There has been extensive study of establishing fixed length secret key in the source model in which parties observe i.i.d samples from a joint distribution and the eavesdropper possibly observes some side information from these samples [4], [10], [20], [29]–[31]. The main objective is to study the achievable key rate when the number of samples tends to infinity.

[23] studies the question of bootstrapping anonymous communication. The objective is to communicate a large amount of data using non-anonymous communication and only a small amount of anonymous broadcasts.

2) Communication-limited MPC Models: **Non-interactive Correlation Distillation.** In information theory and theoretical computer science, non-interactive correlation distillation (NICD) is a well-studied analytically-tractable problem [7], [9], [32], [33], [37]. NICD also aims to establish secure key agreements. In NICD, each party holds a noise version of some source bits, a particular form of correlated private randomness. It is common in NICD that the failure probability for the key-agreement instances is high. On the other hand, parties have access to ABB that generates a different form of conditional distribution in the rABB-hybrid model. We are the first to choose this distribution and achieve near-optimal key length.

Secure Non-interactive Simulation/Reduction. Secure non-interactive simulation/reduction (SNIS/SNIR) is a cryptographic primitive introduced recently [2], [24]. In this model, parties have i.i.d samples of a source correlated private randomness; the objective is to non-interactively and securely

[2] The sender can choose to send $x_0 = 11$ and $x_1 = 0m$ for a bit $m \in \{0,1\}$. The receiver receives the bit m with a probability of $1/2$; otherwise, it is erased with a probability of $1/2$. Therefore, the impossibility of implementing an erasure channel extends to this case.

[3] Section VI-D of [38].

transform these samples into i.i.d samples of another target correlated private randomness. This line of work investigates both the feasibility and efficiency of SNIS/SNIR constructions. We shall employ the techniques to prove the impossibility results in their settings to show the round-complexity of realizing BEC or OT using rABB-hybrid.

One-way Secure Computation. One-way secure computation [3], [18] uses one round of communication to securely transform the samples of the source distribution to the samples of the target distribution.

II. Technical Overview

This section provides a technical overview of our results. The formal definition of the anonymous bulletin board (ABB) and its variant are in Section IV of the full paper [38].

A. Key Agreement

We construct a key agreement protocol in which parties $\mathcal{A}$ and $\mathcal{B}$ receive a set of m messages of n bits each (A and B respectively). Additionally, all parties ($\mathcal{A}$, $\mathcal{B}$, $\mathcal{D}$) receive the set of $2m$ messages ($\Gamma = A \cup B$) from the rABB. The parties first discard any duplicate messages in Γ, resulting in $2m'$ total messages where m' messages belong to each set A and B. Since no duplicate messages exist, only parties $\mathcal{A}$ and $\mathcal{B}$ can identify which of the $2m'$ messages belong to each set A and B. By using a canonical ordering of the $2m'$ messages and assigning messages belonging to A as 1 and messages belonging to B as 0, the two parties can agree on a $2m'$ bit string that is known only to them. Then, by using standard techniques in combinatorics, the two parties can index the agreed upon bit string out of the $\binom{2m'}{m'}$ possible bit strings and agree on a key of length $\log\left(\binom{2m'}{m'}\right) \approx 2m' - \log m'$.

Our protocol has two main parameters, m and n. The expected key length increases with m and n. At the same time, the communication cost increases with m and n as well. However, we note that this is a simple optimization problem and that automatic searches for optimal parameters can be done. Furthermore, for common key-length such as 128 or 256 bits, the search only has to be performed once.

We perform this automated search and present our results in Figure 2 in the full version [38]. Concretely, using 702-bits of communication, $\mathcal{A}$ and $\mathcal{B}$ can agree on a 128-bit key in expectation, and using 1550-bits of communication, $\mathcal{A}$ and $\mathcal{B}$ can agree on a 256-bit key in expectation.

Additionally, we present a variant of our protocol called duplicate recovery, which is suitable for small values of n. (See Section V-G in [38].) In duplicate recovery, instead of removing all duplicates, the protocol considers the duplicates as part of the possible distributions. We note that in this case, indexing the possible distributions becomes non-trivial. We present such a problem as a new problem in combinatorics, as well as reformulate it as an Integer Programming (IP) problem. We believe this problem may be of independent interest.

The complete description and analysis of the key agreement protocol can be found in Section V of the full version [38].

Finally, using techniques on mutual information, we prove that under the setting of arbitrary/unlimited message length, our protocol achieves the optimal expected key length given parameter m. We include an overview of the theorems and many of the proofs, while the detailed proofs can be found in Section V-E in the full version [38].

Theorem 1. *Let $m, n \in \mathbb{N}$ and P, Q be independent distributions over $(\{0,1\}^n)^m$. Suppose parties are in the random public anonymous bulletin board hybrid $\mathsf{rABB}^{P,Q}_{m,m}$. Then, the expected key length in any key agreement protocol (allowing interaction) is at most $I(\mathsf{rABB}^{P,Q}_{m,m}) + 1 + \log 3$.*

We shall employ the techniques developed recently in [27], [28] to prove the theorem above. We say that Alice and Bob are in (X, Y)-correlation hybrid if Alice has x and Bob has y, where (x, y) is sampled according to the joint distribution (X, Y). The following result shall be useful for the proof.

Theorem 2. *[27], [28] Let (X, Y) be a joint distribution. Then, the maximal expected key length in the (X, Y)-correlation hybrid (allowing an arbitrary amount of communication) is at most $I(X, Y) + 1 + \log 3$.*

Proof of Theorem 1. The correlation $\mathsf{rABB}^{P,Q}_{m,m}$ is a conditional distribution of the form $(X, Y|Z)$, where Z the random variable denoting the eavesdropper's view (the set $A \cup B \cup C$). Conditioned on fixing the eavesdropper's view ($Z = z$), applying Theorem 2 to the joint distribution $(X, Y|Z = z)$ yields that the key length is at most $I(X, Y|Z = z) + 1 + \log 3$. Thus, the expected key length is at most

$$\mathbb{E}_z[I(X, Y|Z = z) + 1 + \log 3] = I(X, Y|Z) + 1 + \log 3.$$

Next, we bound the mutual information of the rABB.

Lemma 1. *Let $(X, Y|Z)$ be the correlation corresponding to the random public bulletin board $\mathsf{rABB}^{P,Q}_{m,m}$. For each z in the sample space of the random variable Z, let ℓ_z be the length of z after removing all duplicate elements. Then*

$$I(X, Y|Z) = \sum_z p_Z(z) \cdot \log \binom{2\ell_z}{\ell_z} = \mathbb{E}_z\left[\log \binom{2\ell_z}{\ell_z}\right].$$

Proof.

Fact 1. *It holds that $I(X, Y) = H(X) - H(X|Y) = H(Y) - H(Y|X)$. Furthermore,*

$$I(X, Y|Z) =$$
$$H(X|Z) - H(X|Y, Z) = H(Y|Z) - H(Y|X, Z).$$

First, note that $Z = X \cup Y$. Thus, $H(X|Y, Z) = 0$ since X is completely determined conditioned on knowing Y and Z. We have

$$\begin{aligned} I(X, Y|Z) &= \sum_z p_Z(z) \cdot I(X, Y|Z = z) \\ &= \sum_z p_Z(z) \cdot (H(X|Z = z) - H(X|Y, Z = z)) \quad (Fact\ 1) \\ &= \sum_z p_Z(z) \cdot H(X|Z = z) \end{aligned}$$

For each $x = \{a_1, a_2, \ldots, a_m\}$ in the sample space of X, there is no duplicates in x; that is $a_i \neq a_j$ for every $i \neq j$. Conditioned on $Z = z = \{a_1, \ldots, a_m, b_1, \ldots, b_m\}$, which might contain duplicates, the number of x that are consistent with z is $\binom{2\ell_z}{\ell_z}$. Thus, the support's size of the random variable $(X|Z = z)$ is $\binom{2\ell_z}{\ell_z}$. Observe that the random variable $(X|Z = z)$ is uniform over its support. This implies that $H(X|Z = z) = \log \binom{2\ell_z}{\ell_z}$, for every z such that $p_Z(z) > 0$. Therefore, we have

$$H(X, Y|Z) = \sum_z p_Z(z) \cdot \log \binom{2\ell_z}{\ell_z},$$

which completes the proof. □

The expected key length of our protocol is the quantity $E_z \log \binom{2\ell_z}{\ell_z}$ defined above. The following results are consequences of Lemma 1.

Corollary II.1. *The expected key length of our protocol is exactly $I(\mathsf{rABB}^{P,Q}_{m,m})$, where P and Q are the distribution that samples m messages randomly without replacement.*

Corollary II.2. *Let $m, n \in \mathbb{N}$ and let P, Q be arbitrary distributions over $(\{0,1\}^n)^m$. Then, the expected key length of any protocol in the $\mathsf{rABB}^{P,Q}_{m,m}$ is at most $\log \binom{2m}{m}$.*

B. Chosen Message Random String Oblivious Transfer

A single bit of random oblivious transfer can be seen as two BEC instances that are correlated in a way such that whenever one of the messages is erased, the other message is delivered.

We use a set of four elements – one belonging to $\mathcal{A}$, one belonging to $\mathcal{C}$, and two belonging to $\mathcal{B}$– that is divided into two subsets that each contain an element belonging to $\mathcal{B}$. $\mathcal{B}$ can identify both messages that belong to $\mathcal{B}$ in the two subsets and can therefore obtain two bits. On the other hand, $\mathcal{A}$ can only identify the element belonging to $\mathcal{B}$ in the subset that contains $\mathcal{A}$'s element. This creates a setting where $\mathcal{B}$ can identify two messages while $\mathcal{A}$ can only identify one.

When we directly perform the above step multiple times, a natural issue arises in which $\mathcal{B}$ is unable to identify what messages $\mathcal{A}$ can obtain but will instead get a Cartesian product of all the possible bits.

The key observation is that security still holds if we set all elements belonging to $\mathcal{A}$ to be even (or odd), all elements belonging to $\mathcal{C}$ to be odd (or even, respectively), and half the elements belonging to $\mathcal{B}$ to be even and half to be odd. This will allow $\mathcal{B}$ to "link" the bits that form the same message, thus identifying the two possible messages that $\mathcal{A}$ can obtain without learning which message $\mathcal{A}$ obtains.

We can also compress the multiple calls to rABB into a single call using sequence identifiers and parallel identifiers. (See Section IV-D in [38].) Finally, to ensure that $\mathcal{C}$ learns nothing about either message, $\mathcal{B}$ sends two "correction messages" that get XORed with the original message to create the final message to $\mathcal{A}$ through a private authenticated channel (such a private channel can be established in parallel with no additional round using our key-agreement protocol).

The complete description and analysis of the random string oblivious transfer protocol is in Section VI of [38].

Here, we provide the formal theorem and proof sketch of Result 3, which is used to prove the round optimality of our protocol.

Theorem 3. *Let $p \in (0, 1)$ be the erasure probability. Any zero round protocol implementing $\mathsf{BEC}(p)$ in $\mathsf{rABB}^{U_A,U_B,U_C}_{m_A,m_B,m_C}$-hybrid has constant insecurity, where U_A, U_B, U_C are uniform distribution over $(\{0,1\}^n)^{m_A}, (\{0,1\}^n)^{m_B}, (\{0,1\}^n)^{m_C}$ respectively, and n is the message length.*

Proof Sketch. We prove this by contradiction. Suppose that it is possible to get $\mathsf{BEC}(p)$ from the $\mathsf{rABB}^{U_A,U_B,U_C}_{m_A,m_B,m_C}$. It follows from [2], [24] that if it is possible to implement the randomized inputs $\mathsf{BEC}(p)$ from some other distribution (X, Y), then the eigenvalues of $\mathsf{BEC}(p)$ must be a subset of eigenvalues of the distribution (X, Y). Note that the eigenvalues of $\mathsf{BEC}(p)$ are 1 and $\sqrt{1-p}$. The correlation $\mathsf{rABB}_{m_A,m_B,m_C}$ is a family of joint distributions of the form $(X, Y|Z)$. Therefore, it must be the case that $\sqrt{1-p}$ is an eigenvalue of the correlation $(X, Y|Z = z)$, for every z in support of the random variable Z. This implies that $\sqrt{1-p}$ is an eigenvalue of all the conditional distributions $(X, Y|Z = z)$, which is impossible.

We provide elaborated arguments and an alternative round-optimal protocol for achieving BEC in the appendix of the full version of the paper.

III. Acknowledgement

We want to thank the anonymous reviewers for their valuable comments.

Hemanta K. Maji and Albert Yu are supported in part by an NSF CRII Award CNS–1566499, NSF SMALL Awards CNS–1618822, CNS–2055605, and CCF–2327981, the IARPA HECTOR project, MITRE Innovation Program Academic Cybersecurity Research Awards (2019–2020, 2020–2021), a Ross-Lynn Research Scholars Grant (2021–2022), a Purdue Research Foundation (PRF) Award (2017–2018), and The Center for Science of Information, an NSF Science and Technology Center, Cooperative Agreement CCF–0939370.

Hai H. Nguyen is supported by the Zurich Information Security & Privacy Center (ZISC).

References

[1] Ittai Abraham, Benny Pinkas, and Avishay Yanai. Blinder - scalable, robust anonymous committed broadcast. In Jay Ligatti, Xinming Ou, Jonathan Katz, and Giovanni Vigna, editors, *CCS '20: 2020 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event, USA, November 9-13, 2020*, pages 1233–1252. ACM, 2020. doi:10.1145/3372297.3417261.

[2] Pratyush Agarwal, Varun Narayanan, Shreya Pathak, Manoj Prabhakaran, Vinod M. Prabhakaran, and Mohammad Ali Rehan. Secure non-interactive reduction and spectral analysis of correlations. In Orr Dunkelman and Stefan Dziembowski, editors, *EUROCRYPT 2022, Part III*, volume 13277 of *LNCS*, pages 797–827. Springer, Heidelberg, May / June 2022. doi:10.1007/978-3-031-07082-2_28.

[3] Shweta Agrawal, Yuval Ishai, Eyal Kushilevitz, Varun Narayanan, Manoj Prabhakaran, Vinod M. Prabhakaran, and Alon Rosen. Cryptography from one-way communication: On completeness of finite channels. In Shiho Moriai and Huaxiong Wang, editors, *ASIACRYPT 2020, Part III*, volume 12493 of *LNCS*, pages 653–685. Springer, Heidelberg, December 2020. doi:10.1007/978-3-030-64840-4_22.

[4] Rudolf Ahlswede and Imre Csiszár. Common randomness in information theory and cryptography - I: secret sharing. *IEEE Trans. Inf. Theory*, 39(4):1121–1132, 1993. doi:10.1109/18.243431.

[5] Bowen Alpern and Fred B. Schneider. Key exchange using 'keyless cryptography'. *Information Processing Letters*, 16(2):79–81, 1983. URL: https://www.sciencedirect.com/science/article/pii/0020019083900297, doi:https://doi.org/10.1016/0020-0190(83)90029-7.

[6] Megumi Ando, Anna Lysyanskaya, and Eli Upfal. On the complexity of anonymous communication through public networks. In Stefano Tessaro, editor, *2nd Conference on Information-Theoretic Cryptography, ITC 2021, July 23-26, 2021, Virtual Conference*, volume 199 of *LIPIcs*, pages 9:1–9:25. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021. doi:10.4230/LIPIcs.ITC.2021.9.

[7] Andrej Bogdanov and Elchanan Mossel. On extracting common random bits from correlated sources. *IEEE Trans. Inf. Theory*, 57(10):6351–6355, 2011. doi:10.1109/TIT.2011.2134067.

[8] Claude Castelluccia and Pars Mutaf. Shake them up! a movement-based pairing protocol for CPU-constrained devices. In *Third International Conference on Mobile Systems, Applications, and Services (MobiSys2005)*, Seattle, WA, June 2005. USENIX Association. URL: https://www.usenix.org/conference/mobisys2005/shake-them-movement-based-pairing-protocol-cpu-constrained-devices.

[9] Siu On Chan, Elchanan Mossel, and Joe Neeman. On extracting common random bits from correlated sources on large alphabets. *IEEE Trans. Inf. Theory*, 60(3):1630–1637, 2014. doi:10.1109/TIT.2014.2301155.

[10] Imre Csiszár and Prakash Narayan. Secrecy capacities for multiple terminals. *IEEE Trans. Inf. Theory*, 50(12):3047–3061, 2004. doi:10.1109/TIT.2004.838380.

[11] Debajyoti Das, Sebastian Meiser, Esfandiar Mohammadi, and Aniket Kate. Anonymity trilemma: Strong anonymity, low bandwidth overhead, low latency - choose two. In *2018 IEEE Symposium on Security and Privacy, SP 2018, Proceedings, 21-23 May 2018, San Francisco, California, USA*, pages 108–126. IEEE Computer Society, 2018. doi:10.1109/SP.2018.00011.

[12] Roberto Di Pietro and Gabriele Oligeri. Coke crypto-less over-the-air key establishment. *IEEE Transactions on Information Forensics and Security*, 8(1):163–173, 2013. doi:10.1109/TIFS.2012.2226718.

[13] Claudia Diaz, Harry Halpin, and Aggelos Kiayias. The nym network the next generation of privacy infrastructure. Technical report, Nym Technologies SA, 2021 [Online]. URL: https://nymtech.net/nym-whitepaper.pdf.

[14] Roger Dingledine, Nick Mathewson, and Paul F. Syverson. Tor: The second-generation onion router. In Matt Blaze, editor, *USENIX Security 2004*, pages 303–320. USENIX Association, August 2004.

[15] Saba Eskandarian, Henry Corrigan-Gibbs, Matei Zaharia, and Dan Boneh. Express: Lowering the cost of metadata-hiding communication with cryptographic privacy. In Michael Bailey and Rachel Greenstadt, editors, *30th USENIX Security Symposium, USENIX Security 2021, August 11-13, 2021*, pages 1775–1792. USENIX Association, 2021. URL: https://www.usenix.org/conference/usenixsecurity21/presentation/eskandarian.

[16] Uriel Feige, Joe Kilian, and Moni Naor. A minimal model for secure computation (extended abstract). In *26th ACM STOC*, pages 554–563. ACM Press, May 1994. doi:10.1145/195058.195408.

[17] Michael J. Fischer and Rebecca N. Wright. Multiparty secret key exchange using a random deal of cards. In Joan Feigenbaum, editor, *CRYPTO'91*, volume 576 of *LNCS*, pages 141–155. Springer, Heidelberg, August 1992. doi:10.1007/3-540-46766-1_10.

[18] Sanjam Garg, Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Cryptography with one-way communication. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part II*, volume 9216 of *LNCS*, pages 191–208. Springer, Heidelberg, August 2015. doi:10.1007/978-3-662-48000-7_10.

[19] Yossi Gilad and Amir Herzberg. Plug-and-play IP security - anonymity infrastructure instead of PKI. In Jason Crampton, Sushil Jajodia, and Keith Mayes, editors, *Computer Security - ESORICS 2013 - 18th European Symposium on Research in Computer Security, Egham, UK, September 9-13, 2013. Proceedings*, volume 8134 of *Lecture Notes in Computer Science*, pages 255–272. Springer, 2013. doi:10.1007/978-3-642-40203-6_15.

[20] Amin Aminzadeh Gohari and Venkat Anantharam. Information-theoretic key agreement of multiple terminals: part I. *IEEE Trans. Inf. Theory*, 56(8):3973–3996, 2010. doi:10.1109/TIT.2010.2050832.

[21] Ryan Henry, Amir Herzberg, and Aniket Kate. Blockchain access privacy: Challenges and directions. *IEEE Secur. Priv.*, 16(4):38–45, 2018. doi:10.1109/MSP.2018.3111245.

[22] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Cryptography from anonymity. In *47th FOCS*, pages 239–248. IEEE Computer Society Press, October 2006. doi:10.1109/FOCS.2006.25.

[23] Sune K. Jakobsen and Claudio Orlandi. How to bootstrap anonymous communication. In Madhu Sudan, editor, *ITCS 2016*, pages 333–344. ACM, January 2016. doi:10.1145/2840728.2840743.

[24] Hamidreza Amini Khorasgani, Hemanta K. Maji, and Hai H. Nguyen. Secure non-interactive simulation: Feasibility and rate. In Orr Dunkelman and Stefan Dziembowski, editors, *EUROCRYPT 2022, Part III*, volume 13277 of *LNCS*, pages 767–796. Springer, Heidelberg, May / June 2022. doi:10.1007/978-3-031-07082-2_27.

[25] Hamidreza Amini Khorasgani, Hemanta K. Maji, and Hai H. Nguyen. Secure non-interactive simulation from arbitrary joint distributions. In Eike Kiltz and Vinod Vaikuntanathan, editors, *TCC 2022, Part II*, volume 13748 of *LNCS*, pages 378–407. Springer, Heidelberg, November 2022. doi:10.1007/978-3-031-22365-5_14.

[26] Albert Kwon, Henry Corrigan-Gibbs, Srinivas Devadas, and Bryan Ford. Atom: Horizontally scaling strong anonymity. In *Proceedings of the 26th Symposium on Operating Systems Principles, Shanghai, China, October 28-31, 2017*, pages 406–422. ACM, 2017. doi:10.1145/3132747.3132755.

[27] Cheuk Ting Li and Venkat Anantharam. One-shot variable-length secret key agreement approaching mutual information. In *56th Annual Allerton Conference on Communication, Control, and Computing, Allerton 2018, Monticello, IL, USA, October 2-5, 2018*, pages 259–266. IEEE, 2018. doi:10.1109/ALLERTON.2018.8635830.

[28] Cheuk Ting Li and Venkat Anantharam. One-shot variable-length secret key agreement approaching mutual information. *IEEE Trans. Inf. Theory*, 67(8):5509–5525, 2021. doi:10.1109/TIT.2021.3087963.

[29] Ueli M. Maurer. Protocols for secret key agreement by public discussion based on common information. In Ernest F. Brickell, editor, *CRYPTO'92*, volume 740 of *LNCS*, pages 461–470. Springer, Heidelberg, August 1993. doi:10.1007/3-540-48071-4_32.

[30] Ueli M. Maurer and Stefan Wolf. Unconditionally secure key agreement and the intrinsic conditional information. *IEEE Trans. Inf. Theory*, 45(2):499–514, 1999. doi:10.1109/18.748999.

[31] Ueli M. Maurer and Stefan Wolf. Information-theoretic key agreement: From weak to strong secrecy for free. In Bart Preneel, editor, *EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 351–368. Springer, Heidelberg, May 2000. doi:10.1007/3-540-45539-6_24.

[32] Elchanan Mossel and Ryan O'Donnell. Coin flipping from a cosmic source: On error correction of truly random bits. *Random Structures & Algorithms*, 26(4):418–436, 2005. doi:10.1002/rsa.20062.

[33] Elchanan Mossel, Ryan O'Donnell, Oded Regev, Jeffrey E Steif, and Benny Sudakov. Non-interactive correlation distillation, inhomogeneous markov chains, and the reverse bonami-beckner inequality. *Israel Journal of Mathematics*, 154(1):299–336, 2006.

[34] Andreas Pfitzmann and Michael Waidner. Networks without user observability — design options. In Franz Pichler, editor, *Advances in Cryptology — EUROCRYPT' 85*, pages 245–253, Berlin, Heidelberg, 1986. Springer Berlin Heidelberg.

[35] xx Foundation. xx network white paper. Technical report, xx Foundation, 2021 [Online]. URL: https://xx.network/wp-content/uploads/2021/10/xx-whitepaper-v2.0.pdf.

[36] xx Foundation. xx network white paper xx cmix. Technical report, xx Foundation, 2021 [Online]. URL: https://xx.network/wp-content/uploads/2021/10/xx-whitepaper-v2.0.pdf.

[37] Ke Yang. On the (im)possibility of non-interactive correlation distillation. In Martin Farach-Colton, editor, *LATIN 2004*, volume 2976 of *LNCS*, pages 222–231. Springer, Heidelberg, April 2004.

[38] Albert Yu, Hai H. Nguyen, Aniket Kate, and Hemanta K. Maji. Unconditional security using (random) anonymous bulletin board. Cryptology ePrint Archive, Paper 2024/101, 2024. https://eprint.iacr.org/2024/101. URL: https://eprint.iacr.org/2024/101.

[39] Mordechai M. Yung. A secure and useful "keyless cryptosystem". *Information Processing Letters*, 21(1):35–38, 1985. URL: https://www.sciencedirect.com/science/article/pii/0020019085901061, doi:https://doi.org/10.1016/0020-0190(85)90106-1.