Secure Computation from Elastic Noisy Channels

Dakshita Khurana[1,*], Hemanta K. Maji[2,†], and Amit Sahai[1,*]

[1] Dept of Computer Science, UCLA and Center for Encrypted Functionalities, USA.
{dakshita,sahai}@cs.ucla.edu
[2] Dept of Computer Science, Purdue University, USA.
hmaji@purdue.edu

Abstract. Noisy channels enable unconditionally secure multi-party computation even against parties with unbounded computational power. But inaccurate noise estimation and adversarially determined channel characteristics render known protocols insecure. Such channels are known as unreliable noisy channels. A large body of work in the last three decades has attempted to construct secure multi-party computation from unreliable noisy channels, but this previous work has not been able to deal with most parameter settings.

In this work, we study a form of unreliable noisy channels where the unreliability is one-sided, that we name *elastic* noisy channels: thus, in one form of elastic noisy channel, an adversarial receiver can increase the reception reliability unbeknown to the sender, but the sender cannot change the channel characteristic.

Our work shows feasibility results for a large set of parameters for the elastic binary symmetric channel, significantly improving upon the best results obtainable using prior techniques. In a key departure from existing approaches, we use a more elemental correlated private randomness as an intermediate cryptographic primitive that exhibits only a rudimentary essence of oblivious transfer. Toward this direction, we introduce new information-theoretic techniques that are potentially applicable to other cryptographic settings involving unreliable noisy channels.

Keywords: Noisy Channel, Unfair Noisy Channel, Elastic Noisy Channel, Oblivious Transfer, Information-theoretic Security, Secure Computation.

---

* Research supported in part from a DARPA/ARL SAFEWARE award, NSF Frontier Award 1413955, NSF grants 1228984, 1136174, 1118096, and 1065276, a Xerox Faculty Research Award, a Google Faculty Research Award, an equipment grant from Intel, and an Okawa Foundation Research Grant. This material is based upon work supported by the Defense Advanced Research Projects Agency through the ARL under Contract W911NF-15-C-0205. The views expressed are those of the author and do not reflect the official policy or position of the Department of Defense, the National Science Foundation, or the U.S. Government.

† Work done while at UCLA.

1 Introduction

Secure multi-party computation [57,27] helps mutually distrusting parties to securely compute a function of their private data. General secure computation is impossible in the information-theoretic plain model for most cryptographically interesting functionalities even when parties are semi-honest [36,31,42,3,43,41]. This necessitates restrictions on the power of the adversaries, for example, honest majority [6,12,50,21], computational hardness assumptions [27,33] or physical cryptographic resources, like, noisy channels [17,37,4,38,19], correlated private randomness [38,54,19,44], trusted resources [10,34] or tamper-proof hardware [35,11,46,23,28].

Using cryptographic resources like noisy channels, it is possible to securely compute arbitrary functionalities with unconditional security guarantees against malicious computationally unbounded adversaries as well [17,37,4,38,19]. Aside from unconditional security, this line of work also offers advantages in efficiency [45,5,48]. Additionally, all invocations of the noisy channel can be performed in an offline phase that is independent of the target functionality to be securely computed [54]. But, the security analysis of these protocols crucially hinges on accurate knowledge of the channel characteristic. Inaccurately estimated or, even worse, adversarially determined channel characteristic can violate the security guarantees of known secure computation protocols that rely on noisy channels. We broadly call such channels unreliable noisy channels.

Over the last three decades, a lot of effort has been focussed towards performing information-theoretic secure multi-party computation using unreliable noisy channels, but with limited success. Weak forms of oblivious transfer[3] (OT) [17,22,7,8,55] and noisy channels [16,22,19,20,55,47,56] have been leveraged to perform secure computation with strong security guarantees, but only for limited settings of parameters. For example, the notion of an *unfair* noisy channel allows both the adversarial sender and the receiver to increase their knowledge of the other party's outputs or inputs to the channel. This model captures extremely general physical systems. Unfortunately, strong impossibility results exist for unfair channels [22], thus, significantly limiting the potential set of feasible parameters (Ref. Fig. 1).

Faced with these daunting impossibility results, in this work we ask whether security is possible in meaningful relaxations of the unfair noisy channel model. In particular, we study an unreliable noisy channel model, namely *elastic noisy channels*, where only one party, either the receiver or sender, but not both, can increase their knowledge of the other party's inputs and outputs to the channel. We show that an elastic noisy channel with sender advantage is equivalent to an elastic noisy channel with receiver advantage (see Section 5), and thus in the sequel, we focus on the case where the receiver can increase its knowledge

[3] Oblivious Transfer [49,25,53] is a two-party functionality which takes $(x_0, x_1) \in \{0,1\}^2$ as input from the sender and $c \in \{0,1\}$ from the receiver and provides x_c as output to the receiver. Information-theoretic secure general multi-party computation can be constructed in the OT-hybrid [10,34].

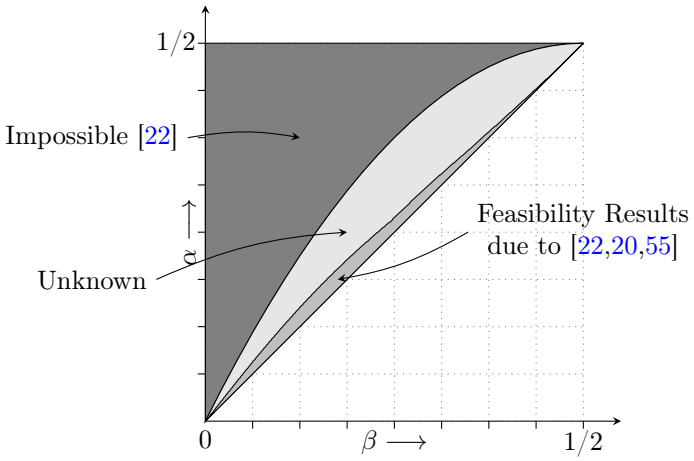

Fig. 1: Unfair binary symmetric channel parameters for binary symmetric channels. Honest channel flips the input symbol with probability α, where $0 < \alpha < 1/2$. Both the sender and the receiver can make the channel more reliable with flip probability β, where $0 < \beta \leqslant \alpha$.

of the sender's inputs to the channel. Such a study is motivated, for example, by transmission and reception of information over physical wireless channels between physically separated parties. This is because in physical wireless systems, thermal noise is always present at the receiver's end and cannot be observed by a physically distant sender. Thus, the sender, even if malicious, cannot anticipate the entire error introduced at the receiver antenna. However, an adversarial receiver, on the other hand, can install a large super-cooled antenna to make its reception more reliable than the reception available to an honest receiver that uses an inexpensive antenna.

While this scenario is *one* example, our study is primarily motivated from a theoretical standpoint, in the face of severe impossibility results for the full unfair channel setting, where very little progress has been made despite decades of research. Interestingly, our elastic channel model avoids the impossibility results of [22] and, hence, holds the promise to yield secure multi-party computation protocols based on a wide range of parameters. Nevertheless, previous work achieve only quite weak results in the elastic noisy channel setting.

Our main result pertains to realization of information-theoretic secure multi-party computation using (α, β)-BSC, a binary symmetric channel where, informally,[4] an honest receiver obtains the sender's input bit flipped with probability α, while the adversarial receiver obtains an the sender's input bit flipped only with probability β, where $0 < \beta \leqslant \alpha < 1/2$. Fig. 2 shows the set of feasible

[4] The actual definition of (α, β)-BSC uses a *degradation channel* model. The channel output is a degradation of the leakage. But for intuitive purposes the description presented here suffices. Section 2 provides a more detailed and accurate description.

parameters that can be achieved using the best previous techniques of [22,55]. The figure also illustrates the much larger set of possible (α, β) pairs for which it is possible to achieve secure multi-party computation on (α, β)-BSC using the techniques we develop in this paper. As a concrete example, if the best antenna in the market incurs only 5% error, then prior techniques need to assume that the honest receiver uses a receiver with at most 14% error. Our protocols, on the other hand, work even when the honest reception error is as high as 30%.

New Ideas. The crux of this significant gain in feasibility parameters is a new perspective on how to securely realize OT from unreliable noisy channels. Over the last several decades, a common underlying theme of previous constructions is a reduction from unreliable noisy channels to weak OT using two-repetition of the underlying channel and the rejection sampling technique of [17] and, subsequently, amplifying the weak OT to a full-fledged OT [17,22,55]. The first reduction in this approach, we find, leads to a significant loss in parameters. We, instead, reduce from unreliable noisy channels to a correlated private randomness that provides extremely weak guarantees and ensures only a rudimentary essence of OT. In this respect, as a departure from prior techniques, our target correlated private randomness is closer to the notion of universal OT as proposed by Cachin [8]. Then, we morph this elemental correlated private randomness into a weak variant of OT using the weak converse of Shannon's Channel Coding Theorem [52,26] as utilized by [40] and fuzzy extractors [24]. Next, this weak variant of OT is amplified to (full-fledged) OT using techniques similar to those proposed in [55]. Section 1.2 provides a summary of our technical contributions and intuition of the protocol designs.

Looking ahead, we believe that the techniques introduced in this paper are of independent interest and are likely to find use in other areas of cryptography where noisy channels are analyzed.

1.1 Our Contributions

Our main contribution is to design protocols that securely realize oblivious transfer and therefore secure multi-party computation, from *elastic* binary symmetric channels. Before summarizing our results, we explain the notion of elastic channels.

Elastic Channels. We will model *elastic* variants of noisy channels as consisting of a pair of noisy channels where the channel for the honest receiver is a degradation of the channel for the adversarial receiver. In general, we view an (α, β)-BSC as a pair of channels, such the honest receiver has reception over a BSC with flip probability α, and an adversarial receiver has reception over a BSC with flip probability $\beta \leqslant \alpha$.

General Secure Computation We prove that general secure computation is possible for a large range of parameters of elastic binary symmetric channels.

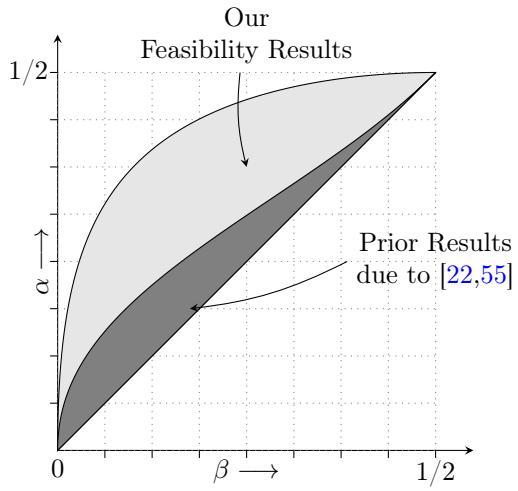

Fig. 2: Space of parameters (β, α), where $0 < \beta \leqslant \alpha < 1/2$, for which we construct secure computation protocol from (α, β)-BSC. The smaller dark region is the space for which such protocols can be obtained using prior techniques from [22,55] combined.

In particular, we obtain oblivious transfer (OT) using elastic noisy channels, and then the OT functionality can be used to obtain general secure computation [57,27,36,10]. Our main theorem is as follows:

Theorem 1 (Elastic BSC Completeness). *There exists a universal constant $c \in (0,1)$, such that for all $0 < \beta \leqslant \alpha < 1/2$, if $\alpha < \left(1 + (4\beta(1-\beta))^{-1/2}\right)^{-1}$ then there exists a protocol $\Pi_{\alpha,\beta}$ such that, $\Pi_{\alpha,\beta}$ securely realizes the OT functionality $\mathcal{F}_{\mathsf{OT}}$ when given access to $((\alpha,\beta)\text{-}\mathsf{BSC})^{\otimes\kappa}$ channels with at most $2^{-\kappa^c}$ simulation error, where κ is the security parameter, with information-theoretic unconditional security against malicious adversaries.*

Refer to Fig. 2 for a summary of the parameter space in Theorem 1 and a comparison of our results with results from previous work[5]. Henceforth, we will use $\ell(\beta) := \left(1 + (4\beta(1-\beta))^{-1/2}\right)^{-1}$.

In addition to elastic noisy channels, both parties also communicate over reliable communication channels in our protocols. These reliable channels can be constructed from the (elastic) noisy channels themselves via standard techniques in error correcting codes (e.g. using polar codes [1,2,29]).

[5] When comparing to previous work, note that no previous work considered the setting of elastic channels. Instead, to provide some context, we plot parameters that would be obtained by combining techniques from [22,55] and adapting these to the setting of elastic channels. We do not attempt to combine also the results from [20], because of definitional differences.

Furthermore, we can strengthen our completeness theorems using techniques from [34,32,40] to achieve *constant rate*: that is, our protocols can produce $\Theta(\kappa)$ OTs with only $O(\kappa)$ total communication and only $O(\kappa)$ calls to the underlying elastic binary symmetric channels.

Corollary 1 (Constant Rate Elastic BSC Completeness) *For all* $0 < \beta \leqslant \alpha < 1/2$, *if* $\alpha < \left(1 + (4\beta(1-\beta))^{-1/2}\right)^{-1}$ *then, there exists a protocol* $\Pi_{\alpha,\beta}$ *and constants* $c_{\alpha,\beta}, d_{\alpha,\beta}$ *such that,* $\Pi_{\alpha,\beta}$ *securely realizes* $\mathcal{F}_{\mathsf{OT}}^{\otimes m}$ *when given access to* $((\alpha,\beta)\text{-}\mathsf{BSC})^{\otimes\kappa}$ *channels with at most* $2^{-\kappa^{c_{\alpha,\beta}}}$ *simulation error and* $m = d_{\alpha,\beta}\kappa$.

1.2 Technical Overview

While our protocols have many ingredients and require a careful analysis, in this section we try to explain the core ideas in our scheme.

A New Take on Previous Approaches. We begin by re-interpreting previous approaches to realize oblivious transfer from noisy channels. Our new understanding of these methods helps abstract out their essence and better illustrate the bottlenecks in our setting. Then, we develop key ideas to achieve oblivious transfer even from channels with adversarial receiver-controlled characteristic, for a large range of parameters of such channels.

To obtain OT from a perfect BSC, a natural starting point is to have the sender pick appropriate codewords (typically simple repetition codes) and send them over the BSC to the receiver. The receiver must then partition the received outputs into two sets establishing two "virtual" channels with the following property: There exists a threshold R, such that one of the virtual channels has capacity $C^* > R$, while the other channel has capacity $\tilde{C} < R$. Moreover, the sender will be unable to tell which virtual channel is which.

In the protocol, the sender pushes information across the virtual channels at rate equal to R. The receiver recovers the information that is transmitted over the virtual channel with capacity $C^* > R$. But, he incurs errors decoding the information transmitted over the virtual channel with capacity $\tilde{C} < R$ because the weak converse of Shannon's Channel Coding Theorem [52,26] kicks in. This decoding error can be amplified using fuzzy extractors [24], to completely erase the other message and guarantee statistical hiding.

But, we would like to design protocols that remain secure even given an (α,β)-BSC. In the following, we will use α-BSC to denote the channel used by the honest receiver; and β-BSC to denote the channel used by the adversarial receiver. Intuitively, the correctness of our protocol needs to be ensured even for an honest receiver who uses a channel prescribed as the "minimum system requirement" of the protocol description (the α-BSC). We also require that the same protocol be secure even against an adversarial receiver who can reduce the noise level significantly (using the β-BSC). Again, we will think of the problem as forcing the receiver to establish two virtual channels of noticeably different capacities. We require the capacity C^* of the better virtual channel established

by the receiver using α-BSC, to be higher than the capacity $\tilde{C}$ of the worse virtual channel established by any adversarial receiver using the β-BSC. The sender will code at a suitable rate intermediate to C^* and $\tilde{C}$. Then, more information will be received over the C^* capacity channel in the honest scenario, than the information received over one of the two virtual channels (of capacity at most $\tilde{C}$) created by the adversarial receiver. This will give oblivious transfer.

Challenges in Our Setting. Let us re-examine our quantitative goal: Suppose the error of the best (adversarial) receiver in the market is 2%, but honest receivers have 20% error. The adversarial receiver can obtain much more information than the honest receiver, without the sender's knowledge. Yet, we want to establish two virtual channels such that the capacity of the better virtual channel established using the α-BSC, is higher than the capacity of the worse virtual channel established by any adversarial receiver using the β-BSC. Such an adversarial receiver is allowed to behave arbitrarily, in particular, it could distribute its total capacity equally between the two channels. Ensuring a capacity gap between the better honest and the worse adversarial capacities in this situation, seems to be a tall order. Indeed, previously the results of Wullschleger [55] could achieve this gap only if the honest adversarial receiver had an error at most 9%.

Towards a Solution. Our first step is to try and relax this goal. Instead of directly shooting for 2-choose-1 oblivious transfer, we try to obtain a weaker form of oblivious transfer, namely $(n, 1, n-1)$ OT, where a sender has n messages, an honest receiver gets to choose 1 message, but a dishonest receiver gets $n-1$ messages of his choice. The sender gets no output. Using the 'virtual channel' intuition presented above, we want the receiver to set up n virtual channels (for some constant n), with a threshold R such that at least one of the n virtual channels set up by the honest receiver has capacity $C^* > R$, while at least one of the n virtual channels set up by the adversarial receiver has capacity less $\tilde{C} < R$. At this point, we have divided our objective into the following two sub-problems:

1. Reduce $(n, 1, n-1)$ OT to (α, β)-BSC
2. Reduce 2-choose-1 OT to $(n, 1, n-1)$ OT

The second result has been considered in the works of [18,51] and can also be demonstrated using techniques presented in [22,55,20] for the setting of weak erasure channels. While this reduction is not the focus of our work, for completeness we provide a protocol securely realizing OT from $(n, 1, n-1)$ OT in the full version, achieving security against malicious adversaries.

Now our main goal is to demonstrate the first reduction. Our next question is, what could be some reasonable ways to take an (α, β)-BSC and build several virtual channels outs of it with varying reliabilities?

A new kind of Channel Decomposition. A logical starting point is to have the sender send λ repetitions of his bit over fresh instantiations of the (α, β)-BSC, and list all possible outputs obtained by the receiver. Each possible output could be used by the receiver to define a "virtual channel". On sending λ repetitions

of a bit b, if the receiver obtains λ identical bits, then his confidence about the original bit b is extremely high. This is the most reliable channel, and will be set to be the choice channel (with capacity C^*) by the honest receiver.

Since errors are independently added at each invocation of the (α, β)-BSC, all receiver outputs with the same number of zeroes, irrespective of the positions of these zeroes, convey the same amount of information to the receiver. Thus, such outputs can be classified into the same equivalence class/virtual channel. Furthermore, for $\eta \in [0, \lfloor \lambda/2 \rfloor + 1]$, let $\mathbb{S}_\eta$ denote all output strings with either η zeroes, or η ones. That is, $\mathbb{S}_\eta$ includes all pairs of output strings of the form $\{0^\eta 1^{\lambda-\eta}, 0^{\lambda-\eta}1^\eta\}$ and their permutations. This results in the creation of $\lfloor \frac{\lambda}{2} \rfloor + 1$ binary symmetric channels[6] of noticeably different capacities, such that the 'best' virtual channel of an honest receiver consists of outputs solely from $\mathbb{S}_0$. It is easy to see that the sender, who gets no output from the BSC, cannot distinguish between various virtual channels created by the receiver.

For security against an adversarial receiver, it suffices to ensure that the capacity of the virtual channel created using values in $\mathbb{S}_0$ corresponding to the α-BSC, is higher than the average capacity (over all possible channels) over all the outputs assembled by an adversarial receiver when he uses the β-BSC. We note that the receiver is *never* allowed to discard any of the outputs he received; he must necessarily divide and distribute them all into his virtual channels.

On analyzing this approach, we find that in fact as we increase λ, the situation improves for many parameters α, β. While both average adversarial and best honest capacities increase as λ increases, in fact the best honest capacity increases faster. Eventually, then, the best honest capacity becomes better than the average adversarial capacity and we obtain the following results (Ref. Fig. 4 for an example illustration of this phenomenon.). For any constants $0 < \beta \leqslant \alpha < \left(1 + \left(4\beta(1-\beta)\right)^{-1}\right)^{-1}$, there exists an efficiently computable constant $\lambda \in \mathbb{N}$ for which the above property holds. Fig. 3 plots the space of these parameters for various values of λ and the limiting curve $\ell(\beta)$.

Although this completes our high-level overview, making these ideas work requires a careful use of the weak converse of Shannon's Channel Coding Theorem, Fuzzy Extractors and other protocol tools, as well as a careful setting of parameters. Refer Section 3 for more details about our construction.

Commitments. Enroute proving Theorem 1, we show that it is possible to obtain string commitments from any (α, β)-BSC, where $0 < \beta \leqslant \alpha < 1$ [7]. Using techniques from [34,32,40], we can also obtain string commitments at a constant rate. We stress that we can obtain commitments from any (α, β) elastic BSC for all parameters $0 < \beta \leqslant \alpha < 1$, unlike our completeness result. Our result is formally stated in the following theorem:

[6] We observe that each set $\mathbb{S}_\eta$ can then be analyzed as a new BSC.

[7] This is in contrast to the setting of unfair noisy channels, which become trivial for a wide range of parameters.

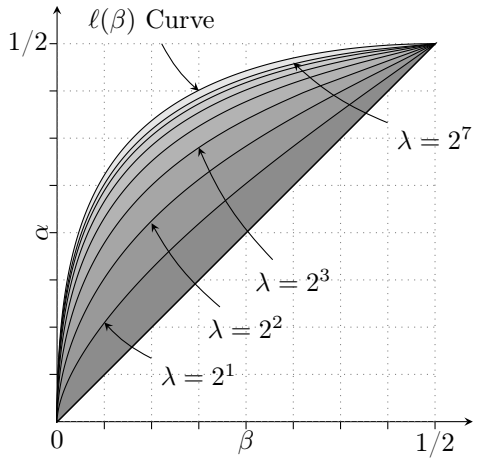

Fig. 3: For $\lambda \in \{2^1, \ldots, 2^7\}$, the space of points (β, α) for which the capacity of the virtual channel created using values in $\mathbb{S}_0$ corresponding to the α-BSC is higher than the average capacity (over all possible channels) over all the outputs assembled by an adversarial receiver when he uses the β-BSC. Finally the limiting $\ell(\beta)$ curve is plotted.

Theorem 2. *There exists a universal constant $c \in (0,1)$, such that for all $0 < \beta \leqslant \alpha < 1/2$, there exists a protocol $\Pi_{\alpha,\beta}$, constant $d \in (0,1)$ such that, $\Pi_{\alpha,\beta}$ securely realizes the string commitment functionality for strings of length $d\kappa$, $\mathcal{F}_{\mathsf{com}}(d\kappa)$, when given access to $((\alpha,\beta)\text{-BSC})^{\otimes\kappa}$ channels, with at most $2^{-\kappa^c}$ simulation error, where κ is the security parameter, with information-theoretic unconditional security against malicious adversaries.*

On adversarial senders. Finally, we note that noisy channels where only the sender can make the transmission more reliable (that is, sender-elastic binary symmetric channels) reduces to the case of elastic noisy channels with an adversarial receiver (receiver-elastic channels), using a tight reduction presented in Section 5. Our one-to-one transformation is optimal and tight.

1.3 Prior Work

There is a lot of literature on constructing secure computation based on noisy channels [17,16,38,39,19,32,40]. An elastic noisy channel, whose characteristic can be altered by adversarial parties, cannot be modeled as a functionality considered by the completeness theorems of [38,44,40]. However, the following channels in the literature, are related to the notion of elastic channels.

– Unfair Noisy Channels. Unfair noisy channels were formally defined by Damgärd et al. [22]: in an unfair noisy channel, *both* the sender and the receiver can

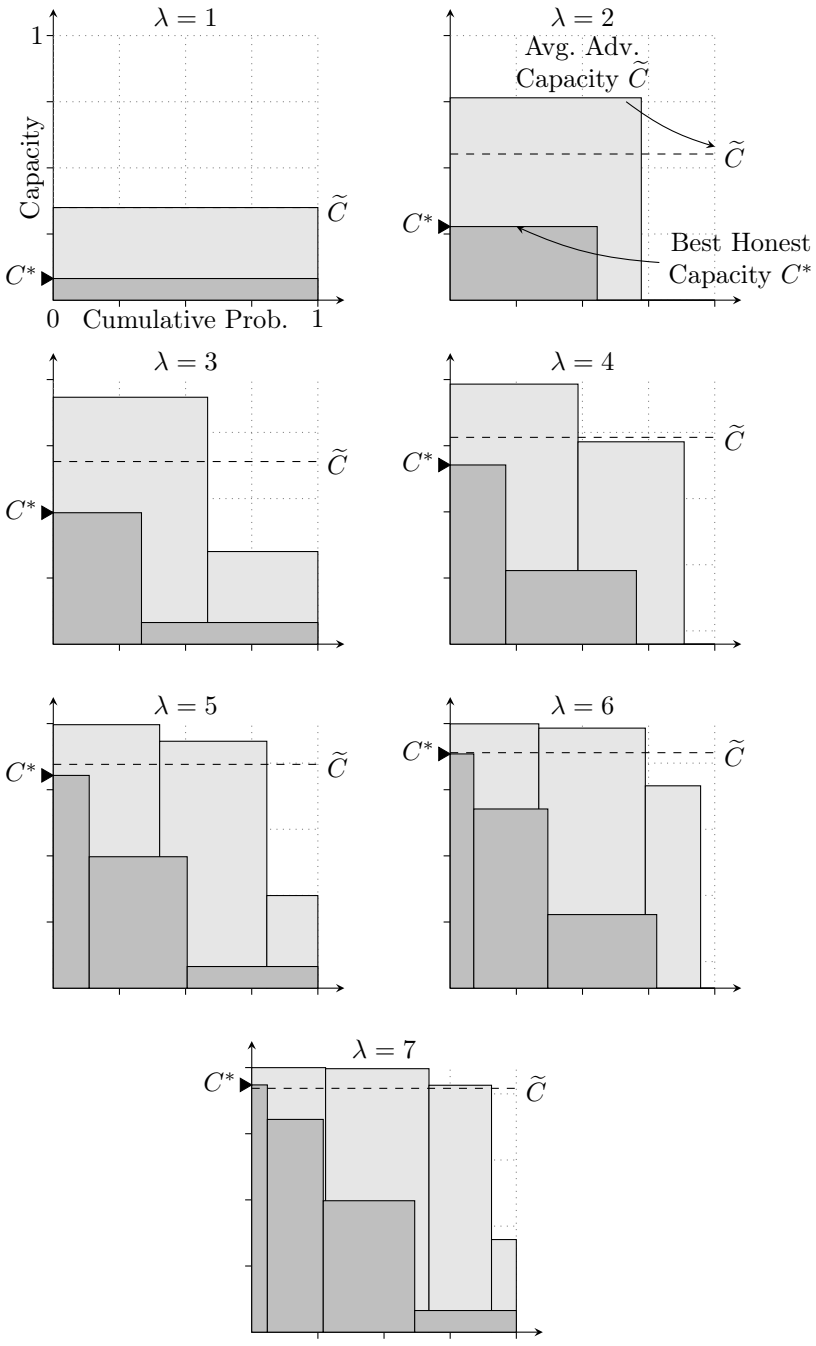

Fig. 4: Obtaining best honest capacity C^* higher than average adversarial capacity $\widetilde{C}$ for (α, β)-BSC, where $(\alpha, \beta) = (1/3, 1/6)$. Each graph represents the capacity profile of sub-channels in the decomposition of $(V, \widehat{V})$, where $\lambda \in \{1, \ldots, 7\}$. The lighter bars denote the adversarial receiver case and the darker bars represent the honest receiver case. When $\lambda = 7$, $C^* > \widetilde{C}$.

change the channel characteristic. Furthermore, the work of [22] showed strong impossibility results in this model. Several works considered performing secure computation from such unfair noisy channels [17,16,22,19,20,55,56]. The feasibility parameters achieved by these works are a small fraction of the parameters not covered by the impossibility result of [22].

– Weak OT with one-sided leakage. The closest notion to elastic channels, is that of weak OT[8] by Wüllschleger [55]. This is an oblivious transfer which allows *either sender or receiver leakage*, but not both. It also allows incorrect output with some probability. It was shown in [55] that OT reduces to weak OT with one-sided leakage for a subset of leakage and error parameters.
It is possible to reduce such a weak OT to elastic noisy channels via the techniques in [22,20,56]. To our knowledge, these give the best known completeness results using techniques implicit in prior work, in the setting of elastic BSC. These parameters are denoted as 'Best Prior Work' in Fig. 2.

Comparison of Techniques. Prior works on unfair noisy channels rely on the technique of [17] which invokes the channel twice to transmit a 2-repetition of the input bit. This implements an *erroneous* version of unfair oblivious transfer. Subsequently, this erroneous unfair OT is amplified to full-fledged OT. Surprisingly, we find that the first reduction in this approach is significantly lossy in parameters, especially when applied to the setting of elastic channels.

Thus, in a departure from previous techniques, we set our first target to obtaining a set of $n \geqslant 2$ channels – where the honest receiver can obtain information on at least one channel, while even an adversarial receiver cannot obtain information on more than $n-1$ channels. To realize such channels, we do not restrict ourselves to 2-repetitions only. A comparison of our parameter space against previous work is illustrated in Fig. 2.

2 Preliminaries

In this section, we introduce some basic definitions and notation, and recall some preliminaries for use in the paper.

Throughout the paper, κ will denote the security parameter. We represent the set $\{1,\ldots,n\}$ by $[n]$. The set of all size-k subsets of a set S is represented by $\binom{S}{k}$. A vector of length n is represented by $(x_1,\ldots,x_n) = x_{[n]}$. For $S = \{i_1,\ldots,i_{|S|}\} \subseteq [n]$, we represent $x_S = (x_{i_1},\ldots,x_{i_{|S|}})$. We use $\mathrm{Ber}(p)$ to represent a sample from a Bernoulli distribution with parameter p.

2.1 Elastic Functionalities

We model elastic variants of noisy channels as a pair of noisy channels where the channel for the honest receiver is a degradation of the channel for the adversarial receiver. The input (say, bit b) is first transmitted over a more reliable

[8] Not to be confused with our notion of (n,k,ℓ)- OT which is complete for all constants $n, (1 < k, \ell < n)$.

(adversarial) channel to obtain leakage z. Then, z is transmitted over a second channel (z is further degraded) to obtain honest receiver output $\tilde{b}$, such that $\tilde{b}$ is effectively, the result of transmitting b over a less reliable channel. The honest receiver obtains output $\tilde{b}$ and the adversarial receiver obtains output leakage z as well as $\tilde{b}$. Note that in our modeling, the leakage z is strictly more informative than honest receiver output $\tilde{b}$. This is exactly why we chose to model elastic channels as degradation channels, as it allows more intuitive analysis. We formalize this notion, as follows, for specific instances of elastic noisy channels.

Definition 1 (Elastic Binary Symmetric Channel.). *Let $Ber(p)$ be a sample of Bernoulli distribution with parameter p. For any $0 < \beta \leqslant \alpha < 1/2$, an (α, β)-BSC channel is defined as follows.*

1. *Emulate β-BSC on input b: Obtain input b from the sender and sample $e_\ell \sim Ber(\beta)$, the compute $z = b \oplus e_\ell$.*
2. *Emulate γ-BSC on input leakage z: Sample $e' \sim Ber(\gamma)$ and compute $\tilde{b} = z \oplus e'$, where $\beta(1-\gamma) + (1-\beta)\gamma = \alpha$. Intuitively, γ is chosen such that $Ber(\alpha) \equiv Ber(\gamma) \oplus Ber(\beta)$.*
3. *Receiver output: Output $\tilde{b}$ to the receiver and, if the receiver is adversarial, then additionally output z to the receiver.*

Let B, Z and $\tilde{B}$ be the random variables corresponding to b, z and $\tilde{b}$, respectively. We have $\tilde{B} = B \oplus Ber(\alpha)$ and $Z = B \oplus Ber(\beta)$, such that $B \to Z \to \tilde{B}$.

Definition 2 ((n, k, ℓ)-OT). *For $0 < k \leqslant \ell < n$, (n, k, ℓ)-OT is defined as:*

1. *Sender inputs bits $x_{[n]}$ and receiver inputs set $T \in \binom{[n]}{k}$.*
2. *Output $\{x_{i:i\in T}\}$ to the receiver.*
3. *If the receiver is corrupted by the adversary, then obtain $S \in \binom{[n]}{\ell}$ such that $T \subseteq S$ from the adversary, and output $\{x_{i:i\in S}\}$ to the adversary.*

2-choose-1 bit OT is equivalent to $(2, 1, 1)$-OT.

2.2 Basic Information Theory

Entropy. The entropy of a distribution X is defined as: $\mathbb{E}_{x\sim X}\left[-\lg \mathsf{P}_{x'\sim X}[x' = x]\right]$. Given a joint distribution (X, Y), the mutual information is: $I(X;Y) = H(X) + H(Y) - H(X,Y)$.

Channel Capacity. The capacity of a channel W is defined to be $I(W) = \max_X I(X; W(X))$, where X is any probability distribution over the input space. If W is output symmetric, then $I(W) = I(U; W(U))$, where U is the uniform distribution over the input space.

For $0 \leqslant \varepsilon \leqslant 1$, the capacity of ε-BEC is $I(\varepsilon\text{-}\mathsf{BEC}) = 1 - \varepsilon$; and the capacity of ε-BSC is $I(\varepsilon\text{-}\mathsf{BSC}) = 1 - h(\varepsilon)$, where $h(x) := -x\lg(x) - (1-x)\lg(1-x)$ is the binary entropy.

$(\mathbf{A}, \mathbf{B}) \to (\mathbf{A}, \mathbf{C})$. For a joint distribution (A, B) and (A, C), if there exists f such that the distributions $(A, f(B))$ and (A, C) are identical, then we say $(A, B) \to (A, C)$. We say that $(A, B) \equiv (A, C)$, if $(A, B) \to (A, C)$ and $(A, C) \to (A, B)$.

$(\mathbf{J}, \mathbf{W_J})$. A channel (J, W_J) is defined as follows:
On input x, sample $j \sim J(x)$ and sample $z \sim W_j(x)$. Output (j, z). We say that a channel $W \equiv (J, W_J)$, if the distributions $(X, W(X)) \equiv (X, J(X), W_{J(X)}(X))$, for all input distributions X.

A binary-input memoryless channel with transition probabilities $(W|0)$ and $(W|1)$ for input symbols 0 and 1, respectively, is called output-symmetric if the probabilities of these two distributions are permutations of each other.

If $I(X; J(X)) = 0$ and all W_j channels are output symmetric, then the capacity of the channel W is $I(W) = \mathbb{E}_{j \sim J}[I(W_j)]$, where J is a fixed distribution over indices (say $J(0)$).[9]

Polar Codes. There are explicit rate achieving Polar Codes with efficient encoding and decoding parameters for ε-BEC and ε-BSC, for $0 \leqslant \varepsilon \leqslant 1$ [1,2,29].

Definition 3. *(Discrete Memoryless Channel) A discrete channel is defined to be a system $W : \mathcal{X} \to \mathcal{Y}$ between a sender and a receiver with sender (input) alphabet $\mathcal{X}$, receiver (output) alphabet $\mathcal{Y}$ and a probability transition matrix $W(y|x)$ specifying the probability that of obtaining output $y \in \mathcal{Y}$ conditioned on input $x \in \mathcal{X}$. The channel is said to be memoryless if the output distribution depends only on the input distribution and is conditionally independent of previous channel inputs and outputs.*

Imported Theorem 1 (Efficient Polar Codes [29]). *There is an absolute constant $\mu < \infty$ such that the following holds. Let W be a binary-input memoryless output-symmetric channel with capacity $I(W)$. Then there exists $a_W < \infty$ such that for all $\varepsilon > 0$ and all powers of two $N \geqslant a_W/\varepsilon^\mu$, there exists a deterministic $\mathsf{poly}(N)$ time construction of a binary linear code of block length N and rate at least $I(W) - \varepsilon$ and a deterministic $N \cdot \mathsf{poly}(\log N)$ decoding algorithm for the code with block error probability at most $2^{-N^{0.49}}$ for communication over W.*

Leftover Hash Lemma. The *min-entropy* of a discrete random variable X is defined to be $H_\infty(X) = -\log \max_{x \in \mathsf{Supp}(X)} \mathsf{P}[X = x]$. For a joint distribution (A, B), the *average min-entropy* of A w.r.t. B is defined as $\tilde{H}_\infty(A|B) = -\log\left(\mathbb{E}_{b \sim B}\left[2^{-H_\infty(A|B=b)}\right]\right)$.

Imported Lemma 1 (Generalized Leftover Hash Lemma(LHL) [24]). *Let $\{H_x : \{0,1\}^n \to \{0,1\}^\ell\}_{x \in X}$ be a family of universal hash functions. Then, for any joint distribution (W, I): $\mathsf{SD}\left((H_X(W), X, I), (\mathcal{U}_\ell, X, I)\right) \leqslant \frac{1}{2}\sqrt{2^{-\tilde{H}_\infty(W|I)} 2^\ell}$.*

[9] Because W is also output symmetric.

Weak Converse of Shannon's Channel Coding Theorem. Let $W^{\otimes N}$ denote N independent instances of channel W, which takes as input alphabets from set $\{0,1\}$. Let the capacity of the channel W be C, for a constant $C > 0$. Let $\mathcal{C} \in \{0,1\}^N$ be a rate $R \in \{0,1\}$ code. Then, if the sender transmits a random codeword $\mathbf{c} \xleftarrow{\$} \mathcal{C}$ over $W^{\otimes N}$, the probability of error of the receiver in predicting is $P_e \geqslant 1 - \frac{1}{NR} - \frac{C}{R}$.

2.3 Chernoff-Hoeffding Bound for Hypergeometric Distribution

Imported Theorem 2 (Multiplicative Chernoff Bound for Binomial Random Variables [13,30]). *Let $X_1, X_2, \ldots X_n$ be independent random variables taking values in $[0,1]$. Let $X = \sum_{i\in[n]} X_i$, and let $\mu = \mathbb{E}[X]$ denote the expected value of the X. Then, for any $\delta > 0$, the following hold.*

- $\Pr[X > (1+\delta)\mu] < \exp\left(-n\mathsf{D}_{\mathsf{KL}}\left(\mu(1+\delta)\|\mu\right)\right)$.
- $\Pr[X > (1-\delta)\mu] < \exp\left(-n\mathsf{D}_{\mathsf{KL}}\left(\mu(1-\delta)\|\mu\right)\right)$.

Imported Theorem 3 (Multiplicative Chernoff Bound for Hypergeometric Random Variables [30,14]). *If X is a random variable with hypergeometric distribution, then it satisfies the Chernoff bounds given in Imported Theorem 2.*

2.4 Constant Rate OT Generation

Imported Theorem 4 ([32]). *Let π be a protocol which UC-securely realizes $\mathcal{F}_{\mathsf{OT}}$ in the f-hybrid with simulation error $1 - o(1)$. Then there exists a protocol ρ which UC-securely realizes $\mathcal{F}_{\mathsf{OT}}^{\otimes m}$ in the $f^{\otimes n}$-hybrid with simulation error $1 - \mathsf{negl}(\kappa)$, such that $n = \mathsf{poly}(\kappa)$ and $m = \Theta(n)$.*

3 Binary Symmetric Channels

3.1 Channel Decomposition

In an (α,β)-BSC, the capacity of each channel invocation in the adversarial receiver case is higher than the capacity when the receiver is honest. Despite this bottleneck, our aim is to (non-interactively) synthesize n new noisy channels such that the highest capacity of these channels when interacting with an honest receiver surpasses the capacity of at least one channel obtained by any adversarial receiver. Intuitively, this is achieved by decomposing the original elastic noisy channel into sub-channels such that the sub-channels are "receiver identifiable." Details are provided in the following paragraphs.

It is not evident how to directly decompose an elastic BSC into receiver identifiable sub-channels with the above property. So, we construct a different channel from BSC channels and, in turn, we decompose that channel.

Consider the channel C_ε (parameterized by $\lambda \in \mathbb{N}$) defined below. Given input bit b from the sender, pass b^λ through $(\varepsilon\text{-}\mathsf{BSC})^{\otimes\lambda}$, i.e. λ independent copies of

ε-BSC, and provide the output string to the receiver. The receiver receives an output string $\tilde{b}_{[\lambda]} \in \{0,1\}^\lambda$.

Let $\mathsf{id}(s)$ represent the number of minority bits in $s \in \{0,1\}^\lambda$.[10] So, we have $\mathsf{id}\colon \{0,1\}^\lambda \to \{0,\ldots,\lfloor \lambda/2 \rfloor\}$. Define $S_i \subseteq \{0,1\}^n$, as the set of all strings $s \in \{0,1\}^\lambda$ such that $\mathsf{id}(s) = i$. Given an output string $\tilde{b}_{[\lambda]}$ of the channel $\widetilde{C}$, we interpret it output from the $\mathsf{id}(\tilde{b}_{[\lambda]})$-th sub-channel.

Now, note that the sub-channel which takes as input $\{0^\lambda, 1^\lambda\}$ and outputs a string in S_i is (isomorphic to) an ε_i-BSC channel, for $i \in \{0,\ldots,\lfloor \lambda/2 \rfloor\}$, where:

$$\varepsilon_i := \frac{\varepsilon^{\lambda-i} \cdot (1-\varepsilon)^i}{\varepsilon^{\lambda-i} \cdot (1-\varepsilon)^i + (1-\varepsilon)^{\lambda-i} \cdot \varepsilon^i} = \frac{\varepsilon^{\lambda-2i}}{\varepsilon^{\lambda-2i} + (1-\varepsilon)^{\lambda-2i}}$$

Note that ε_i is an increasing function of i. The probability that the i-th sub-channel is stochastically obtained by C_ε is:

$$p_i(\varepsilon) := \binom{\lambda}{i} \left(\varepsilon^{\lambda-i}(1-\varepsilon)^i + \varepsilon^i(1-\varepsilon)^{\lambda-i}\right)$$

Now, intuitively, we have decomposed C_ε, a channel synthesized from ε-BSC, into a convex linear combination of receiver identifiable sub-channels. More concretely, we have shown that: $C_\varepsilon \equiv \sum_{i=0}^{\lfloor \lambda/2 \rfloor} p_i(\varepsilon) \cdot (\varepsilon_i\text{-BSC})$.

Now, for any $0 < \beta \leqslant \alpha < 1/2$, we consider the (α,β)-BSC channel. Analogous to the channel C_ε, we consider the channel $C_{\alpha,\beta}$. This is identical to the channel C_ε and $\varepsilon = \alpha$ when the receiver is honest, and $\varepsilon = \beta$ when the receiver is adversarial. The maximum capacity of sub-channels in the honest receiver case is: $C^* = 1 - h(\alpha_0)$, where $h(x) = -x\lg(x) - (1-x)\lg(1-x)$ is the binary entropy function. The average capacity of sub-channels in the adversarial receiver case is:

$$\widetilde{C} = 1 - \sum_{i=0}^{\lfloor \lambda/2 \rfloor + 1} p_i(\beta) \cdot h(\beta_i)$$

If we have $C^* > \widetilde{C}$, then we know that best capacity from α-BSC exceeds the average malicious capacity from β-BSC. We set $n = 1/p_0(\alpha)$ and create n-instantiations of the channel C_ε. Then one of the sub-channels in the honest receiver case has capacity C^*, while the average capacity of sub-channels in the adversarial receiver case is $\widetilde{C}$. So, out of the n sub-channels, there is one sub-channel in the honest receiver case which has capacity higher than some sub-channel in the adversarial receiver case.

The next question is: for what (α,β) does there exist a λ such that $C^* > \widetilde{C}$? In the following lemma, we show that, if $\alpha < \ell(\beta) := \left(1 + (4\beta(1-\beta))^{-1/2}\right)^{-1}$, then such a λ exists.

For $\alpha = 1/3$ and $\beta = 1/6$, Fig. 4 explains the receiver identifiable decomposition of $C_{\alpha,\beta}$ for increasing values of λ until $C^* > \widetilde{C}$.

[10] If s has equal number of 0s and 1s, then we define $\mathsf{id}(s) := |s|/2$.

Lemma 1. *For constants* $0 < \alpha < \ell(\beta) := \left(1 + (4\beta(1-\beta))^{-1/2}\right)^{-1}$*, given an* (α, β)-BSC*, there exists a constant* $\lambda \in \mathbb{N}$ *such that it is possible for the receiver to sender-obliviously construct channels where the maximum capacity* C^* *of one sub-channel in the honest receiver case, over* α-BSC*, is greater than the average capacity* $\widetilde{C}$ *of all sub-channels in the adversarial receiver case, over* β-BSC*.*

Consider an elastic binary symmetric channel (α, β)-BSC. For a given a value of $\lambda \in \mathbb{N}$, define $\pi\colon \{0,1\} \to \{0,1\}^\lambda$ as $\pi(b) = b^\lambda$ (i.e. λ repetitions of the bit b). Corresponding to this, we obtain channels $(V, \widehat{V})$ corresponding to the honest and adversarial receiver respectively. We have $C^* = 1 - h(\alpha_0^{(\lambda)})$ and $\widetilde{C} = 1 - \sum_{i \in [\lfloor \lfloor \lambda/2 \rfloor + 1 \rfloor} p_i^{(\lambda)}(\beta) h(\beta_i^{(\lambda)})$. Define two functions: $h^*(x^{(\lambda)}) := h(x_0^{(\lambda)})$ and $\tilde{h}(x^{(\lambda)}) := \sum_{i \in [\lfloor \lfloor \lambda/2 \rfloor + 1 \rfloor} p_i^{(\lambda)}(x) h(x_i^{(\lambda)})$. Note that $C^* = 1 - h^*(\alpha^{(\lambda)})$ and $\widetilde{C} = 1 - \tilde{h}(\beta^{(\lambda)})$. Consider the following manipulation:

$$\begin{aligned}\tilde{h}(x^{(\lambda)}) &= \sum_{i \in S} p_i^{(\lambda)}(x) h(x_i^{(\lambda)}) > 2 \sum_{i \in S} p_i^{(\lambda)}(x) \cdot x_i^{(\lambda)} \\ &= 2 \sum_{i \in S} \binom{\lambda}{i} x^i (1-x)^i \cdot x^{\lambda - 2i} = \sum_{i \in S} \binom{\lambda}{i} x^{\lambda - i} (1-x)^i\end{aligned}$$

This is a binomial distribution with mean $(1-x)\lambda$. By using anti-concentration bound from [15]):

$$\begin{aligned}\tilde{h}(x^{(\lambda)}) &> \frac{1}{\lambda^2} \exp\left(-\lambda \mathsf{D}_{\mathsf{KL}}\left(1/2 \| x\right)\right) \\ &= h\left(h^{-1}\left(\frac{1}{\lambda^2 \exp\left(\lambda \mathsf{D}_{\mathsf{KL}}\left(1/2 \| x\right)\right)}\right)\right)\end{aligned}$$

Next, we use the inequality $h^{-1}(x) \geqslant x/\left(2\log(6/x)\right)$ from [9]. Set $t(x) = x/\left(2\log(6/x)\right)$. This gives $\tilde{h}(x^{(\lambda)}) > h\left(t\left(\frac{1}{\lambda^2 \exp(\lambda \mathsf{D}_{\mathsf{KL}}(1/2\|x))}\right)\right)$. For any $x \in (0, 1/2)$, consider $\lambda \to \infty$. We analyze the behavior of $t\left(\frac{1}{\lambda^2 \exp(\lambda \mathsf{D}_{\mathsf{KL}}(1/2\|x))}\right)$.

Define a such that: $\frac{1}{\lambda^3 \exp(\lambda \mathsf{D}_{\mathsf{KL}}(1/2\|x)) \mathsf{polylog}(\lambda)} \leqslant t\left(\frac{1}{\lambda^2 \exp(\lambda \mathsf{D}_{\mathsf{KL}}(1/2\|x))}\right) =: \frac{1}{1+\left(\frac{1}{a}-1\right)^\lambda} = h^*(a^{(\lambda)})$ Observe that under these conditions $a \to a^* := \frac{1}{1+\exp(\mathsf{D}_{\mathsf{KL}}(1/2\|x))} = \frac{1}{1+\frac{1}{\sqrt{4x(1-x)}}}$. Now for any fixed x and $y < a^*$ (as defined above), for all sufficiently large $\lambda \in \mathbb{N}$ we have $\tilde{h}(x^{(\lambda)}) > h^*(y^{(\lambda)})$.

This shows that for $0 < \beta \leqslant \alpha < \left(1 + (4\beta(1-\beta))^{-1/2}\right)^{-1}$, there exists a constant $\lambda_{\alpha,\beta}$ such that for $\lambda \geqslant \lambda_{\alpha,\beta}$ we have $\tilde{h}(\beta^{(\lambda)}) > h^*(\alpha^{(\lambda)})$, i.e. $C^* > \widetilde{C}$. Furthermore, this bound is tight.

3.2 Semi-honest completeness of (α, β)-BSC for $0 < \beta \leqslant \alpha < \ell(\beta)$

Consider the channel V_ϵ (parameterized by $\lambda \in \mathbb{N}$) which on input a bit b, passes b^λ through $(\epsilon\text{-BSC})^{\otimes \lambda}$. Then, for the channels $(V, \widehat{V})$ constructed by sending a λ-

repetition code via an (α,β)-BSC, let $C^* := \max_{j\in\mathsf{Supp}(J)} I(V_j)$ and $\widetilde{C} := I(\widehat{V})$. We use Lemma 1 to compute $\lambda_{\alpha,\beta}$ corresponding to α,β where $0<\beta\leqslant\alpha<\ell(\beta)$, such that $C^* > \widetilde{C}$, and use the capacity-inverting encoding $\pi_{\alpha,\beta}(b) = b^{\lambda_{\alpha,\beta}}$. For ease of notation, we will use λ to represent $\lambda_{\alpha,\beta}$.

Let n be an integer, such that $n = \frac{1}{\alpha^\lambda+(1-\alpha)^\lambda-\epsilon}$, where $\epsilon \in (0, {}^{\alpha^\lambda+(1-\alpha)^\lambda}\!/_2)$. Let $\delta = \frac{c^*_h}{\tilde{c}_m} - 1$. Pick a polar code of rational rate r where $\tilde{c}_m(1+\delta/3) < r < \tilde{c}_m(1+2\delta/3)$, and block-length κ/n. Let $\mathsf{enc},\mathsf{dec}$ denote the encoding and decoding algorithms of this polar code. Then, Fig. 5 gives a protocol to UC-securely realize n-choose-1 OT using an (α,β)-BSC, in the semi-honest setting.

Inputs: $\mathcal{S}$ has inputs $(x_1,x_2,\dots x_n)\in\{0,1\}^n$, $\mathcal{R}$ has input choice $c\in[n]$.
Hybrid: (α,β)-BSC for $0<\beta\leqslant\alpha<\ell(\beta)$.
The protocol is parameterized by κ, a multiple of n.

1. Correlation Generation:
   For all $i\in[\kappa^2]$, $\mathcal{S}$ picks bit $b_i\in\{0,1\}$ and sends $b_{i,[\lambda]} = b_i^\lambda$ over the $\left((\alpha,\beta)\text{-BSC}^{\otimes\lambda}\right)$ to $\mathcal{R}$. Let $\mathcal{R}$ obtain output $\tilde{b}_{i,[\lambda]}$.
2. Receiver Message:
   Let $I = \left\{i : i\in[\kappa^2] \text{ and } \tilde{b}_{i,[\lambda]}\in\{0^\lambda,1^\lambda\}\right\}$. Set $\tilde{b}_i = \tilde{b}_{i,1}$ for all $i\in I$.
   If $|I| < \kappa^2/n$, abort. Else, let $S_c \xleftarrow{\$} \binom{I}{\kappa^2/n}$ and for all $\ell\in[n]\setminus\{c\}$, set $S_\ell \xleftarrow{\$} [\kappa^2]\setminus(S_c\cup(S_1\cup S_2\cup\cdots S_{\ell-1}))$. For all $\ell\in[n]$, let $S_\ell = \{\mathsf{ind}_{\frac{(\ell-1)\kappa^2}{n}+1}, \mathsf{ind}_{\frac{(\ell-1)\kappa^2}{n}+2}, \dots \mathsf{ind}_{\frac{\ell\kappa^2}{n}}\}$. Send $(S_1,S_2,\dots S_n)$ to $\mathcal{S}$.
3. Sender Message:
   For $j\in[\kappa]$, $\ell\in[n]$, pick $m_{j,\ell,[r\kappa/n]} \xleftarrow{\$} \{0,1\}^{r\kappa/n}$, compute $m'_{j,\ell,[\kappa/n]} = \mathsf{enc}(m_{j,\ell,[r\kappa/n]})$. For all $j\in[\kappa]$, $\ell\in[n]$, $i\in[\kappa/n]$, compute and send $y_{j,\ell,i} = m'_{j,\ell,i} \oplus \tilde{b}_{\mathsf{ind}_{\frac{(\ell-1)\kappa^2}{n}+\frac{(j-1)\kappa}{n}+i}}$.
   For all $\ell\in[n]$, pick $h_\ell \xleftarrow{\$} \mathcal{H}$, a hash function from $\{0,1\}^{\kappa^2/n}\to\{0,1\}$. Compute $r_\ell = h_\ell(m_{1,\ell,[\kappa/n]}, m_{2,\ell,[\kappa/n]},\dots m_{\kappa,\ell,[\kappa/n]}) \oplus x_\ell$.
   For $\ell\in[n]$, send h_ℓ, r_ℓ to $\mathcal{R}$.
4. Receiver Output:
   For all $j\in[\kappa]$ and $i\in[\kappa/n]$, compute $m'_{j,c,i} = y_{j,c,i} \oplus \tilde{b}_{\mathsf{ind}_{\frac{(c-1)\kappa^2}{n}+\frac{(j-1)\kappa}{n}+i}}$. Compute $m_{j,c,[r\kappa/n]} = \mathsf{dec}(m'_{j,c,[\kappa/n]})$. Output $x_c = h_c(m_{1,c,[\kappa/n]}, m_{2,c,[\kappa/n]},\dots m_{\kappa,c,[\kappa/n]}) \oplus r_c$.

Fig. 5: n-choose-1 bit OT from (α,β)-BSC for $0<\beta\leqslant\alpha<\ell(\beta)$.

Correctness. It is easy to see that the protocol correctly implements 2-choose-1 oblivious transfer.

Lemma 2. *For all* $0 < \beta \leqslant \alpha < \ell(\beta)$*, for all* $(x_1, x_2, \ldots x_n) \in \{0,1\}^n$ *and* $c \in [n]$*, the output of* $\mathcal{R}$ *equals* x_c *with probability at least* $(1 - 2^{-\kappa^{0.4}})$.

Proof. When the sender and the receiver are both honest, the expected fraction of receiver outputs in $\{0^\lambda, 1^\lambda\}$ is $\alpha^\lambda + (1-\alpha)^\lambda - \epsilon$. Then, the probability that the receiver obtains less than $1/n = \alpha^\lambda + (1-\alpha)^\lambda - \epsilon$ outputs in $\{0^\lambda, 1^\lambda\}$ is at most $2^{-\frac{\epsilon^2 \kappa}{\alpha^\lambda + (1-\alpha)^\lambda}}$, by the Chernoff bound. Moreover, by Imported Theorem 1, the decoding error when a code of block length κ/n is sent over κ channels at a rate constant lower than capacity, is at most $\kappa \cdot 2^{-\frac{\kappa^{0.49}}{n}}$.

It is easy to see that, conditioned on the receiver obtaining at least $1/n = \alpha^\lambda + (1-\alpha)^\lambda - \epsilon$ outputs in $\{0^\lambda, 1^\lambda\}$ and no decoding error, the protocol is always correct. Thus, the output of $\mathcal{R}$ equals x_c with probability at least $(1 - 2^{-\kappa^{0.4}})$.

Receiver security The semi-honest simulation strategy $\mathsf{Sim}_{\mathcal{S}}$ is given in Fig. 6.

The simulator $\mathsf{Sim}_{\mathcal{S}}$ does the following.

1. Obtain inputs $(x_1, x_2, \ldots x_n)$ from $\mathcal{S}$.
2. Follow honest strategy: pick $b_{[\kappa^2]} \xleftarrow{\$} \{0,1\}^{\kappa^2}$. Pass $b^\lambda_{[\kappa^2]}$ through an honest emulation of $((\alpha,\beta)\text{-}\mathsf{BSC})^{\otimes \lambda\kappa^2}$ to generate $z_{[\kappa^2],[\lambda]}, \tilde{b}_{[\kappa^2],[\lambda]}$.
3. Generate $I = \left\{i : i \in [\kappa^2], \tilde{b}_{i,[\lambda]} \in \{0^\lambda, 1^\lambda\}\right\}$. Set $\tilde{b}_i = \tilde{b}_{i,1}$ for all $i \in I$. If $|I| < \kappa^2/n$, then $\mathsf{abort}_{\mathsf{Sim}}$. Else send a random partition, $S_1, S_2, \ldots S_n$ of $[\kappa^2]$ to $\mathcal{S}$.
4. For $j \in [\kappa]$ and $\ell \in [n]$, pick $m_{j,\ell,[r\kappa/n]} \xleftarrow{\$} \{0,1\}^{r\kappa/n}$, compute $m'_{j,\ell,[\kappa/n]} = \mathsf{enc}(m_{j,\ell,[r\kappa/n]})$. For all $j \in \kappa$, $\ell \in [n]$ and $i \in [\kappa/n]$, compute and send $y_{j,\ell,i} = m'_{j,\ell,i} \oplus \tilde{b}_{\mathsf{ind}\,\frac{(\ell-1)\kappa^2}{n} + \frac{(j-1)\kappa}{n} + i}$.

   For all $\ell \in [n]$, pick $h \xleftarrow{\$} \mathcal{H}$, a family of universal hash functions. Compute $r_\ell = \left(h_\ell(m_{1,\ell,[\kappa/n]}, m_{2,\ell,[\kappa/n]}, \ldots m_{\kappa,\ell,[\kappa/n]})\right) \oplus x_\ell$.

Fig. 6: Sender simulation strategy for n-choose-1 bit OT.

Lemma 3. *The simulation error for the semi-honest sender is at most* $1 - 2^{-\frac{\epsilon^2 \kappa}{\alpha^\lambda + (1-\alpha)^\lambda}}$.

Proof. The view of the sender is, $V_{\mathcal{S}} := \{(x_1, x_2, \ldots x_n), b_{[\kappa^2]}, S_1, S_2, \ldots S_n\}$.

First, the probability of abort in the real view is at most $2^{-\frac{\epsilon^2\kappa}{\alpha^\lambda+(1-\alpha)^\lambda}}$. Note that the simulator never aborts. But, conditioned on the receiver not aborting, we argue that the simulated sender view is identical to the real view.

For all $i \in [\kappa^2]$, the probability that $\tilde{b}_{i,[\lambda]} \in \{0^\lambda, 1^\lambda\}$, is an i.i.d. random variable, over the randomness of the (α,β)-BSC as well as the receiver. For some fixed size s such that $\kappa^2/n \leqslant s \leqslant \kappa^2$, in the view of the sender, $I : |I| = s$ is a random subset of $[\kappa]$ of size s, and S_c is a random partition of I of size $\kappa/2$. The other sets are a random partition of $[\kappa^2] \setminus S_c$, and thus all the sets are a random equal partition of $[\kappa^2]$. Thus, in this case the simulation is perfect.

Thus, the simulation error is exactly equal to the probability of abort, which is at most $2^{-\frac{\epsilon^2\kappa}{\alpha^\lambda+(1-\alpha)^\lambda}}$.

Sender security The semi-honest simulation strategy $\mathsf{Sim}_{\mathcal{R}}$ is given in Fig. 7.

The simulator $\mathsf{Sim}_{\mathcal{R}}$ does the following.

1. Obtain input choice bit c and output θ from $\mathcal{R}$.
2. Pick $b_{[\kappa^2]} \xleftarrow{\$} \{0,1\}^{\kappa^2}$.
   Pass $b^\lambda_{[\kappa^2]}$ through an honest emulation of $((\alpha,\beta)\text{-BSC})^{\otimes\lambda\cdot\kappa^2}$ and generate $z_{[\kappa^2],[\lambda]}, \tilde{b}_{[\kappa^2],[\lambda]}$.
3. Generate $I = \left\{i : i \in [\kappa^2], \tilde{b}_i \in \{0^\lambda, 1^\lambda\}\right\}$. Set $\tilde{b}_i = \tilde{b}_{i,1}$ for all $i \in I$. Repeat until $|I| \geqslant \kappa^2/n$. Set $S_c \xleftarrow{\$} \binom{I}{\kappa^2/n}$. For all $\ell \in [n] \setminus \{c\}$, set $S_\ell \xleftarrow{\$} \binom{[\kappa^2] \setminus (S_c \cup S_1 \cup S_2 \cup \ldots S_{\ell-1})}{\kappa^2/n}$. For all $\ell \in [n]$, let $S_\ell = \{\mathsf{ind}_{\frac{(\ell-1)\kappa^2}{n}+1}, \mathsf{ind}_{\frac{(\ell-1)\kappa^2}{n}+2}, \ldots \mathsf{ind}_{\frac{\ell\kappa^2}{n}}\}$.
4. Set $x_c = \theta$, and set $x_\ell \xleftarrow{\$} \{0,1\}$ for all $\ell \in [n] \setminus \{c\}$.
   For $j \in [\kappa]$ and $\ell \in [n]$, pick $m_{j,\ell,[r\kappa/n]} \xleftarrow{\$} \{0,1\}^{r\kappa/n}$, compute $m'_{j,\ell,[\kappa/n]} = \mathsf{enc}(m_{j,\ell,[r\kappa/n]})$. For all $j \in \kappa$, $\ell \in [n]$ and $i \in [\kappa/n]$, compute $y_{j,\ell,i} = m'_{j,\ell,i} \oplus \tilde{b}_{\mathsf{ind}_{\frac{(\ell-1)\kappa^2}{n}+\frac{(j-1)\kappa}{n}+i}}$.
   For all $\ell \in [n]$, pick $h \xleftarrow{\$} \mathcal{H}$, a family of universal hash functions.
   Compute $r_\ell = \left(h_\ell(m_{1,\ell,[\kappa/n]}, m_{2,\ell,[\kappa/n]}, \ldots m_{\kappa,\ell,[\kappa/n]})\right) \oplus x_\ell$.

Fig. 7: Receiver simulation strategy for n-choose-1 bit OT.

Lemma 4. *The simulation error for the semi-honest receiver is at most* $2^{-\kappa\delta/4}$.

Proof. The view of the receiver $V_{\mathcal{R}} := \{c, \theta, \tilde{b}_{[\kappa^2],[\lambda]}, z_{[\kappa^2],[\lambda]}, r_0, r_1\}$. The values $\tilde{b}_{[\kappa^2],[\lambda]}, z_{[\kappa^2],[\lambda]}$ are generated using honest sender strategy. There is no abort from the sender side in the (α,β)-BEC hybrid or the simulated view.

Consider channel S_c, composed of κ sub-channels of block-length (κ/n), each of capacity $\tilde{c}_h$. Recall that $B \to Z \to \tilde{B}$, where $B, Z, \tilde{B}$ are random variables denoting the sender input, leakage and receiver output respectively. Thus, the capacity of any sub-channel of S_c, can only increase when the receiver obtains additional leakage. For a semi-honest receiver, the capacity of each sub-channel of S_c is at least $\tilde{c}_h = c_m^*(1+\delta)$ even when the receiver is adversarial and can change channel characteristic. The channels S_ℓ for $\ell \in [n] \setminus \{c\}$ are constructed by sampling sets of κ sub-channels at random, without replacement from the remaining set. Since, the overall average capacity of the adversarial receiver (semi-honest, but changes channel characteristic) is at most c_m^*, the average capacity of any sub-channel in this remaining set is at most $c_m^*(n-1-\delta)/(n-1)$. Then, there are at least a constant fraction $(n-1-\delta)/(n-1)$ sub-channels in this remaining set, each with capacity at most $c_m^* < r$.

Now, consider the event that there exists a channel S_ℓ for $\ell \in [n] \setminus \{c\}$, such that for more than $(\kappa - \sqrt{\kappa})$ sub-channels in S_ℓ, the sub-channel capacity is greater than c_m^*. This event occurs with probability at most $2^{-\kappa/3}$. We argue that conditioned on this event not happening, the simulated view is $(n-1)2^{-\kappa/3}$-close to the receiver view in the (α, β)-BSC hybrid.

For a channel with capacity c and a code of rate $r > c$, a weak converse of Shannon's channel coding theorem proves the decoding error is at least $1 - \frac{c}{r}$, therefore the min-entropy is at least $h_2(1 - \frac{c}{r})$. Then, an application of the Left-over Hash Lemma gives us that for a randomly chosen universal hash function h, if $\sqrt{\kappa}$ sub-channels have constant min-entropy $> \delta/2$, the hash value is at least $2^{-\kappa\delta/3}$ close to uniform. Thus for all channels S_ℓ where $\ell \in [n] \setminus \{c\}$, the output r_ℓ is $2^{-\kappa\delta/3}$ close to uniform. Moreover, r_c is computed using honest sender strategy, so the random variable r_c is identical in the (α, β)-BSC hybrid and simulated views. Thus, the total simulation error is $(n-1)2^{-\kappa\delta/3} + 2^{-\kappa/3} = n2^{-\kappa\delta/3} < 2^{-\kappa\delta/4}$.

3.3 Special-Malicious Completeness of (α, β)-BSC for $0 < \beta \leqslant \alpha < \ell(\beta)$

In fact, it is not difficult to prove that the protocol in Fig. 5 yields $(n, 1, n-1)$ OT in a special-malicious setting. In this setting, the receiver is allowed to behave maliciously, whereas the sender must (semi-)honestly send a repetition code in the first step of the protocol, and after this step the sender is allowed to behave maliciously. Please refer to the full version for a formal proof.

4 Full Malicious Completeness of Binary Symmetric Channels

4.1 $\mathcal{F}_{\mathsf{com}}$ from (α, β)-BSC for $0 < \beta \leqslant \alpha < 1/2$

The protocol is presented in Fig. 8, in terms of a polar code $\mathcal{C}$ over the binary alphabet, with block-length κ, rate $1 - o(1)$ and minimum distance $\omega(\kappa^{4/5})$.

Inputs: $\mathcal{S}$ has input bit $b \in \{0,1\}$ and $\mathcal{R}$ has no input.
Hybrid: (α,β)-BSC for $0 < \beta \leqslant \alpha < 1$.
The protocol is parameterized by κ.

1. Commit Phase:
   (a) For all $i \in [\kappa]$, $\mathcal{S}$ picks codeword $\mathbf{c}_i = (c_{i,1}, c_{i,2}, \dots c_{i,\kappa}) \xleftarrow{\$} \mathcal{C}$, and sends $\mathbf{c}_{i,[2]} = (c_{i,1}, c_{i,2}, \dots c_{i,\kappa}, c_{i,1}, c_{i,2}, \dots c_{i,\kappa})$ over the (α,β)-BSC to $\mathcal{R}$. Let $\mathcal{R}$ obtain $\tilde{\mathbf{c}}_{i,[2]}$.
   (b) $\mathcal{S}$ picks $h \xleftarrow{\$} \mathcal{H}$, a universal hash function family mapping $\{0,1\}^{\kappa^2} \to \{0,1\}$, and sends $h, y = b \oplus h(\mathbf{c}_1, \mathbf{c}_2, \dots \mathbf{c}_\kappa)$ to $\mathcal{R}$.
2. Reveal Phase:
   (a) For all $i \in [\kappa]$, $\mathcal{S}$ sends $b, \mathbf{c}_i = (c_{i,1}, c_{i,2}, \dots c_{i,\kappa})$ to $\mathcal{R}$.
   (b) $\mathcal{R}$ accepts if all the following conditions hold:
   - For all $i \in [\kappa]$, $\mathbf{c}_i$ is a valid codeword.
   - For all $i \in [\kappa]$, set $I_{i,1} = \{j : (\tilde{c}_{i,j}, \tilde{c}_{i,\kappa+j}) = (1-c_{i,j}), (1-c_{i,j})\}$. Then $|I_{i,1}| \leqslant (1-\alpha)^2(\kappa + \kappa^{2/3})$.
   - For all $i \in [\kappa]$, set $I_{i,2} = \{j : \tilde{c}_{i,j} \neq \tilde{c}_{i,\kappa+j}\}$. Then $|I_{i,2}| \leqslant 2\alpha(1-\alpha)(\kappa + \kappa^{2/3})$.
   - $b = y \oplus h(\mathbf{c}_1, \mathbf{c}_2, \dots \mathbf{c}_\kappa)$.

Fig. 8: UC-secure $\mathcal{F}_{\mathsf{com}}$ from (α,β)-BSC for $0 < \beta \leqslant \alpha < 1$.

Intuitively, the sender sends picks a codeword from the appropriate code and sends a 2-repetition of the codeword over the BSC, to the receiver. The commitment is statistically hiding because the capacity of the receiver is less than the rate of the code, and therefore there is constant prediction error for each codeword $\mathbf{c}_i$ for $i \in [\kappa]$. The commitment is statistically binding because the sender cannot flip too many bits, or send too many 'bad' indices to the receiver. If he does, he will be caught with overwhelming probability. If he sends a few bad/flipped bits, the minimum distance of the code will still hash them down to the same value.

Correctness For honest sender strategy, using a Chernoff bound, it is possible to show that the size of I_1 and I_2 is bounded by $(1-\alpha)^2(\kappa + \kappa^{2/3})$ and $2\alpha(1-\alpha)(\kappa+\kappa^{2/3})$ with probability at least $1 - 2.2^{-\kappa/3}$. Thus, when $\mathcal{S}$ and $\mathcal{R}$ are both honest, then $\mathcal{R}$ accepts $\mathsf{Reveal}(\mathsf{Commit}(b))$ for any $b \in \{0,1\}$ with probability at least $1 - 2^{-\kappa/4}$.

Receiver Security (Statistical Binding/Extractability) It suffices to consider a dummy sender $\mathcal{S}$ and malicious environment $\mathcal{Z}_{\mathcal{S}}$, such that the dummy sender forwards all messages from $\mathcal{Z}_{\mathcal{S}}$ to the honest receiver/simulator, and vice-versa.

Without loss of generality, the semi-honest simulation strategy $\mathsf{Sim}_{\mathcal{S}}$ can be viewed to interact directly with $\mathcal{Z}_{\mathcal{S}}$. $\mathsf{Sim}_{\mathcal{S}}$ is described in Fig. 9.

The simulator $\mathsf{Sim}_{\mathcal{S}}$ does the following.

1. Commit Phase:
   (a) For all $i \in [\kappa]$, obtain $h, y, \mathbf{c}_{i,[2]}$ from $\mathcal{Z}_{\mathcal{S}}$.
   (b) For all $i \in [\kappa]$, compute the nearest codeword $\tilde{\mathbf{c}}_i$ to $\mathbf{c}_i = \{c_{i,1}, c_{i,2} \dots c_{i,\kappa}\}$.
   (c) Extract bit $b' = y \oplus h(\tilde{\mathbf{c}}_i, \tilde{\mathbf{c}}_2, \dots \tilde{\mathbf{c}}_\kappa)$ and send it to the ideal $\mathcal{F}_{\mathsf{com}}$ functionality.
2. Reveal Phase:
   (a) For all $i \in [\kappa]$, obtain $\mathbf{c}'_i$ from $\mathcal{Z}_{\mathcal{S}}$.
   (b) Allow the ideal functionality to output the extracted bit b' if all the following conditions hold (and otherwise reject):
      – For all $i \in [\kappa]$, $\mathbf{c}'_i$ is a valid codeword.
      – For all $i \in [\kappa]$, set $I_{i,1} = \{j : c'_{i,j} \neq c_{i,j}\}$. Then $|I_{i,1}| \leqslant 2\kappa^{2/3}$.
      – For all $i \in [\kappa]$, set $I_{i,2} = \{j : c_{i,j} \neq c_{i,\kappa+j}\}$. Then $|I_{i,2}| \leqslant 2\kappa^{2/3}$.

Fig. 9: Sender simulation strategy for $\mathcal{F}_{\mathsf{com}}$.

Lemma 5. *The simulation error for the malicious sender is at most* $2^{-\kappa^{0.5}}$.

Proof. First, note that both the real and ideal views reject with probability 1 when $\mathbf{c}'_i$ is not a valid codeword, for any $i \in [\kappa]$. Next, if $|I_{i,1}| > 2\kappa^{2/3}$ or $|I_{i,2}| > 2\kappa^{2/3}$, then the real view rejects with probability at least $(1 - 2^{-\kappa^{2/3}})$, whereas the ideal view always rejects.

Conditioned on the receiver not rejecting, it remains to argue that the bit b' extracted by the simulator (and later output to the receiver) is distributed identically in the hybrid and ideal worlds. Conditioned on not rejecting, for each $i \in [\kappa]$, the distance between $\mathbf{c}'_i$ and $\mathbf{c}_i$ is at most $|I_{i,1}| + |I_{i,2}| = 4\kappa^{2/3}$. Then, because the code has minimum distance $\omega(\kappa^{4/5})$, the nearest codeword $\tilde{\mathbf{c}}_i$ to $\mathbf{c}_i$ is actually $\mathbf{c'}_i$ itself. Therefore, the bit $b' = y \oplus h(\tilde{\mathbf{c}}_i, \tilde{\mathbf{c}}_2, \dots \tilde{\mathbf{c}}_\kappa) = y \oplus h(\mathbf{c}'_1, \mathbf{c}'_2, \dots \mathbf{c}'_\kappa)$ is distributed identically in the hybrid and ideal worlds in this case.

Thus the simulation error is at most $2.2^{-\kappa^{2/3}} < 2^{-\kappa^{0.5}}$.

Sender Security (Statistical Hiding/Equivocability) It suffices to consider a dummy receiver $\mathcal{R}$ and malicious environment $\mathcal{Z}_{\mathcal{R}}$, such that the dummy receiver forwards all messages from $\mathcal{Z}_{\mathcal{R}}$ to the honest receiver/simulator, and vice-versa.

Without loss of generality, the semi-honest simulation strategy $\mathsf{Sim}_{\mathcal{R}}$ can be viewed to interact directly with $\mathcal{Z}_{\mathcal{R}}$. $\mathsf{Sim}_{\mathcal{R}}$ is described in Fig. 10.

The simulator $\mathsf{Sim}_{\mathcal{R}}$ does the following.

1. Commit Phase:
   (a) Wait for the honest sender to send bit b' to the ideal $\mathcal{F}_{\mathsf{com}}$ functionality.
   (b) For all $i \in [\kappa]$, pick codeword $\mathbf{c}_i = (c_{i,1}, c_{i,2}, \ldots c_{i,\kappa}) \xleftarrow{\$} \mathcal{C}$, and send $\mathbf{c}_{i,[2]} = (c_{i,1}, c_{i,2}, \ldots c_{i,\kappa}, c_{i,1}, c_{i,2}, \ldots c_{i,\kappa})$ over the (α, β)-BSC to $\mathcal{R}$. Obtain output $\tilde{\mathbf{c}}_{i,[2]}$ and leakage $\tilde{\mathbf{z}}_{i,[2]}$ for $\mathcal{R}$.
   (c) Pick $h \xleftarrow{\$} \mathcal{H}$, a universal hash function family mapping $\{0,1\}^{\kappa^2} \to \{0,1\}$, and send $y = h(\mathbf{c}_1, \mathbf{c}_2, \ldots \mathbf{c}_\kappa)$ to $\mathcal{R}$.
2. Reveal Phase:
   (a) Allow the ideal functionality to output the extracted bit b'.
   (b) If $b' = 0$, then output $\mathbf{c}_i, \mathbf{c}_2, \ldots \mathbf{c}_n$ to $\mathcal{R}$.
   (c) Else for all $i \in [\kappa]$,
      – Set codeword $\mathbf{c}'_i = \mathbf{c}_i$.
      – Set $I_i = \{j : \tilde{z}_{i,j} \neq \tilde{z}_{i,\kappa+j}\}$ (these are the erased indices).
      – Flip $c'_{i,j}$ at random indices $\mathsf{ind} \in I_i$, ensuring that $\mathbf{c}'_i$ remains a valid codeword.
   (d) Check if $h(\mathbf{c}'_1, \mathbf{c}'_2, \ldots \mathbf{c}'_\kappa) \neq h(\mathbf{c}_1, \mathbf{c}_2, \ldots \mathbf{c}_\kappa)$. If not, repeat step (c).

Fig. 10: Receiver simulation strategy for $\mathcal{F}_{\mathsf{com}}$.

Lemma 6. *The simulation error for the malicious receiver is at most* $2.2^{-\kappa}$.

Proof. For all $i \in [\kappa]$ and honestly generated $\mathbf{c}_i$, the channel $\tilde{\mathbf{c}}_{i,[2]}$ has a constant fraction $2\beta(1-\beta)$ bits of the form 01 or 10, which count as erasures. Thus, the capacity of each such channel is at most $1 - 2\beta(1-\beta)$. Since the rate of the code sent over channel $\tilde{\mathbf{c}}_{i,[2]}$ is $1 - o(1)$, the entropy in the received string is at least $1 - \frac{1-2\beta(1-\beta)}{1-o(1)} \approx 2\beta(1-\beta)$. Therefore, via the leftover hash lemma, $h(\mathbf{c}_1, \mathbf{c}_2, \ldots \mathbf{c}_\kappa)$ is at least $1 - 2^{-\kappa}$ close to uniform, and therefore, y is at least $1 - 2^{-\kappa}$ close to uniform.

Moreover, with probability at least $1 - 2^{-\kappa}$, it is possible to efficiently find a different set of codewords $\mathbf{c}'_i$ which hash to a different bit, for the same output $\tilde{\mathbf{c}}_i$ and $\tilde{\mathbf{z}}_i$ of the receiver.

4.2 Malicious completeness of (α, β)-BSC for $0 < \beta \leqslant \alpha < \ell(\beta)$

To make the protocol in Section 3.3 secure against a general malicious sender instead of only a special-malicious one, we must ensure correctness of the repetition code sent in Step 1 by the sender. To ensure this, we make use of the commitment protocol $\mathcal{F}_{\mathsf{com}}$.

The functionality $\mathcal{F}_{\mathsf{com}}$ can be constructed from any (α, β)-BSC as demonstrated in Section 4.1. The sender and receiver use $\mathcal{F}_{\mathsf{com}}$ to toss random coins, and then implement a cut-and-choose based protocol to implement Step 1 of the special-malicious protocol. The protocol is presented in Fig. 11 in the $\mathcal{F}_{\mathsf{com}}$

Inputs: $\mathcal{S}$ has inputs $(x_0, x_1) \in \{0,1\}^2$ and $\mathcal{R}$ has input choice bit $c \in \{0,1\}$.
Hybrid: (α, β)-BSC for $0 < \beta \leqslant \alpha < \ell(\beta)$.

1. Correlation Generation:
   (a) Sender Message: For all $i \in [\kappa^6]$, $\mathcal{S}$ picks bit $b_i \in \{0,1\}$ and sends $b_{i,[\lambda]} = b_i^\lambda$ over the (α, β)-BSC to $\mathcal{R}$. Let $\mathcal{R}$ obtain output $\tilde{b}_{i,[\lambda]}$. $\mathcal{S}$ sends $d_i = \mathsf{com}(b_i)$ to $\mathcal{R}$.
   (b) Coin tossing in the well: Parties $\mathcal{S}$ and $\mathcal{R}$ use $\mathcal{F}_{\mathsf{com}}$ to generate random coins in the following manner. $\mathcal{S}$ picks random $r_S \xleftarrow{\$} \{0,1\}^{\kappa^6}$ and sends $\mathsf{com}(r_S)$ to $\mathcal{R}$. Then, $\mathcal{R}$ picks random $r_R \xleftarrow{\$} \{0,1\}^{\kappa^6}$ and sends r_R to $\mathcal{S}$. Then, $\mathcal{S}$ decommits to r_S, and if accepted, both parties obtain shared randomness $r = r_S \oplus r_R$.
   (c) Cut and Choose: Parties use randomness r to pick $S \xleftarrow{\$} \binom{[\kappa^6]}{\kappa^6/2}$ and $T \xleftarrow{\$} \binom{[\kappa^6] \setminus S}{\kappa^2}$. $\mathcal{S}$ reveals b_i for all $i \in S$. Let $\mathcal{I} = \{i : \tilde{b}_i \neq \alpha^\lambda\}$. $\mathcal{R}$ aborts if $|\mathcal{I}| > (1 - \alpha^\lambda)(\kappa^6/2 + \kappa^{3.1})$.
   Else, $\mathcal{S}$ and $\mathcal{R}$ use this set T, to continue the rest of the protocol according to Fig. 5.

Fig. 11: 2-choose-1 bit OT from (α, β)-BSC for $0 < \beta \leqslant \alpha < \ell(\beta)$.

and (α, β)-BSC hybrids. The protocol (including commitments) always uses the (α, β)-BSC from the sender to the receiver. Since OT can be reversed, this demonstrates fixed-role completeness of (α, β)-BSC for $0 < \beta \leqslant \alpha < \ell(\beta)$. Step 1 of the protocol in Section 3.3 is modified as follows.

Analysis. The sender and receiver use $\mathcal{F}_{\mathsf{com}}$ to toss common random coins.

In step 1, the sender sends λ-repetitions of κ^6 bits over the (α, β)-BSC. Additionally, he sends a commitment to each of these bits. Then, the parties pick a random subset, consisting of half of the values sent in step 1, and the sender is required to reveal these values.

Next, out of the remaining $\kappa^6/2$ commitments, both parties pick a random subset of size κ^5. Then, with probability at least $(1-1/\kappa)$, this subset is such that at most $\kappa^{3.1}$ of the values committed to do not match the repetition code (that is, the statistical check would have passed passed). If the sender and receiver pick a random set of κ^2 random values out of this set of κ^5 values, then with probability at least $(1 - 1/\kappa^{1.2})$, all of them are correct repetition codes.

Therefore, we obtain a statistical OT which fails with probability at most $2/\kappa^{1.2}$, we call such a functionality that fails with vanishing probability, $\mathcal{F}_{\widetilde{\mathsf{OT}}}^{(\delta)}$, which is formally described in Fig. 12. This functionality $\mathcal{F}_{\widetilde{\mathsf{OT}}}^{(\delta)}$, can then be compiled using [34,32] to obtain constant-rate OT, following [40]. We provide the details of this compiler in the full version.

This completes the proof of Theorem 1.

Functionality $\mathcal{F}_{\widetilde{\mathsf{OT}}}^{(\delta)}$. Parameterized by a function $\delta(\kappa)$.

- Set $b = 1$ with probability $b = \delta(\kappa)$, otherwise set $b = 0$.
- Provide the parties access to a 2-choose-1 bit OT functionality. If $b = 1$, let the adversary control the functionality.

Fig. 12: $\mathcal{F}_{\widetilde{\mathsf{OT}}}^{(\delta)}$ Functionality

5 Conclusion

It is an interesting open problem to explore whether our completeness results extend to parameters $\alpha > \ell(\beta)$, or if there are impossibility results for this setting.

Unfair channels [22] give a theoretical model, general enough to capture many realistic noisy channels. However, in light of strong impossibility results for the completeness of unfair channels, we weaken the adversarial model resulting in what we call *elastic* noisy channels.

We show that this model circumvents the impossibility results in the unfair channel setting, and show a wide range of parameters for which elastic channels can be used to securely realize OT. We believe our techniques are of independent interest and can be leveraged, along with other ideas, to close the gap between the known feasible and infeasible parameters in the unfair channel setting.

5.1 Sender-Elastic Channels Reduction to (Receiver-) Elastic Channels

We can reduce sender-elastic BSC to a (receiver-) elastic BSC in the following manner. Suppose Alice is the sender and sends a bit b through the sender-elastic BSC. She receives a leakage $b \oplus E_1$, where $E_1 = \mathrm{Ber}(\beta)$. Bob, the receiver, obtains $C = b \oplus E_1 \oplus E_2$, where $E_2 = \mathrm{Ber}(\gamma)$ such that $\mathrm{Ber}(\alpha) \equiv \mathrm{Ber}(\beta) + \mathrm{Ber}(\gamma)$.

We reverse this channel using the following technique. Bob defines $T := C \oplus R$, where R is a uniform random bit, and sends T to Alice. Alice now defines $S := b \oplus T$. Now, interpret R as the bit sent and S as the received bit. It is clear that this is a (α, γ)-BSC channel. And, it can also be formally argued that this one-to-one transformation is tight.

References

1. Arikan, E.: Channel polarization: A method for constructing capacity-achieving codes. In: Kschischang, F.R., Yang, E. (eds.) 2008 IEEE International Symposium

on Information Theory, ISIT 2008, Toronto, ON, Canada, July 6-11, 2008. pp. 1173–1177. IEEE (2008), http://dx.doi.org/10.1109/ISIT.2008.4595172 5, 13
2. Arikan, E.: Channel polarization: a method for constructing capacity-achieving codes for symmetric binary-input memoryless channels. IEEE Transactions on Information Theory 55(7), 3051–3073 (2009), http://dx.doi.org/10.1109/TIT.2009.2021379 5, 13
3. 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) 2
4. Beimel, A., Malkin, T., Micali, S.: The all-or-nothing nature of two-party secure computation. In: Wiener, M.J. (ed.) Advances in Cryptology – CRYPTO'99. Lecture Notes in Computer Science, vol. 1666, pp. 80–97. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 15–19, 1999) 2
5. 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: 15th Conference on Computer and Communications Security. pp. 257–266. ACM Press, Alexandria, Virginia, USA (Oct 27–31, 2008) 2
6. Ben-Or, M., Goldwasser, S., Wigderson, A.: Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract). In: 20th Annual ACM Symposium on Theory of Computing. pp. 1–10. ACM Press, Chicago, Illinois, USA (May 2–4, 1988) 2
7. Brassard, G., Crépeau, C., Wolf, S.: Oblivious transfers and privacy amplification. J. Cryptology 16(4), 219–237 (2003), http://dx.doi.org/10.1007/s00145-002-0146-4 2
8. Cachin, C.: On the foundations of oblivious transfer. In: Nyberg, K. (ed.) Advances in Cryptology – EUROCRYPT'98. Lecture Notes in Computer Science, vol. 1403, pp. 361–374. Springer, Heidelberg, Germany, Espoo, Finland (May 31 – Jun 4, 1998) 2, 4
9. Calabro, C.: The exponential complexity of satisfiability problems. Ph.D. thesis (2009), http://www.escholarship.org/uc/item/0pk5w64k 16
10. Canetti, R., Lindell, Y., Ostrovsky, R., Sahai, A.: Universally composable two-party and multi-party secure computation. In: 34th Annual ACM Symposium on Theory of Computing. pp. 494–503. ACM Press, Montréal, Québec, Canada (May 19–21, 2002) 2, 5
11. Chandran, N., Goyal, V., Sahai, A.: New constructions for UC secure computation using tamper-proof hardware. In: Smart, N.P. (ed.) Advances in Cryptology – EUROCRYPT 2008. Lecture Notes in Computer Science, vol. 4965, pp. 545–562. Springer, Heidelberg, Germany, Istanbul, Turkey (Apr 13–17, 2008) 2
12. Chaum, D., Crépeau, C., Damgård, I.: Multiparty unconditionally secure protocols (extended abstract). In: 20th Annual ACM Symposium on Theory of Computing. pp. 11–19. ACM Press, Chicago, Illinois, USA (May 2–4, 1988) 2
13. Chernoff, H.: A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations. Ann. Math. Stat. 23, 493–507 (1952) 14
14. Chvátal, V.: The tail of the hypergeometric distribution. Discrete Mathematics 25(3), 285 – 287 (1979), http://www.sciencedirect.com/science/article/pii/0012365X79900840 14
15. Cover, T.M., Thomas, J.A.: Elements of information theory (2. ed.). Wiley (2006) 16
16. Crépeau, C.: Efficient cryptographic protocols based on noisy channels. In: Fumy, W. (ed.) Advances in Cryptology – EUROCRYPT'97. Lecture Notes in Computer

Science, vol. 1233, pp. 306–317. Springer, Heidelberg, Germany, Konstanz, Germany (May 11–15, 1997) 2, 9, 11
17. Crépeau, C., Kilian, J.: Achieving oblivious transfer using weakened security assumptions (extended abstract). In: 29th Annual Symposium on Foundations of Computer Science. pp. 42–52. IEEE Computer Society Press, White Plains, New York (Oct 24–26, 1988) 2, 4, 9, 11
18. Crépeau, C., Kilian, J., Savvides, G.: Interactive hashing: An information theoretic tool (invited talk). In: Safavi-Naini, R. (ed.) ICITS 08: 3rd International Conference on Information Theoretic Security. Lecture Notes in Computer Science, vol. 5155, pp. 14–28. Springer, Heidelberg, Germany, Calgary, Canada (Aug 10–13, 2008) 7
19. Crépeau, C., Morozov, K., Wolf, S.: Efficient unconditional oblivious transfer from almost any noisy channel. In: Blundo, C., Cimato, S. (eds.) SCN 04: 4th International Conference on Security in Communication Networks. Lecture Notes in Computer Science, vol. 3352, pp. 47–59. Springer, Heidelberg, Germany, Amalfi, Italy (Sep 8–10, 2005) 2, 9, 11
20. Damgård, I., Fehr, S., Morozov, K., Salvail, L.: Unfair noisy channels and oblivious transfer. In: Naor, M. (ed.) TCC 2004: 1st Theory of Cryptography Conference. Lecture Notes in Computer Science, vol. 2951, pp. 355–373. Springer, Heidelberg, Germany, Cambridge, MA, USA (Feb 19–21, 2004) 2, 3, 5, 7, 11
21. Damgård, I., Ishai, Y.: Scalable secure multiparty computation. In: Dwork, C. (ed.) Advances in Cryptology – CRYPTO 2006. Lecture Notes in Computer Science, vol. 4117, pp. 501–520. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 20–24, 2006) 2
22. Damgård, I., Kilian, J., Salvail, L.: On the (im)possibility of basing oblivious transfer and bit commitment on weakened security assumptions. In: Stern, J. (ed.) Advances in Cryptology – EUROCRYPT'99. Lecture Notes in Computer Science, vol. 1592, pp. 56–73. Springer, Heidelberg, Germany, Prague, Czech Republic (May 2–6, 1999) 2, 3, 4, 5, 7, 9, 11, 25
23. Damgård, I., Nielsen, J.B., Wichs, D.: Isolated proofs of knowledge and isolated zero knowledge. In: Smart, N.P. (ed.) Advances in Cryptology – EUROCRYPT 2008. Lecture Notes in Computer Science, vol. 4965, pp. 509–526. Springer, Heidelberg, Germany, Istanbul, Turkey (Apr 13–17, 2008) 2
24. Dodis, Y., Ostrovsky, R., Reyzin, L., Smith, A.: Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. SIAM J. Comput. 38(1), 97–139 (2008), http://dx.doi.org/10.1137/060651380 4, 6, 13
25. Even, S., Goldreich, O., Lempel, A.: A randomized protocol for signing contracts. In: Chaum, D., Rivest, R.L., Sherman, A.T. (eds.) Advances in Cryptology – CRYPTO'82. pp. 205–210. Plenum Press, New York, USA, Santa Barbara, CA, USA (1982) 2
26. Gallager, R.: Information Theory and Reliable Communication. John Wiley & Sons (1968) 4, 6
27. 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 Annual ACM Symposium on Theory of Computing. pp. 218–229. ACM Press, New York City,, New York, USA (May 25–27, 1987) 2, 5
28. Goyal, V., Ishai, Y., Sahai, A., Venkatesan, R., Wadia, A.: Founding cryptography on tamper-proof hardware tokens. In: Micciancio, D. (ed.) TCC 2010: 7th Theory of Cryptography Conference. Lecture Notes in Computer Science, vol. 5978, pp. 308–326. Springer, Heidelberg, Germany, Zurich, Switzerland (Feb 9–11, 2010) 2

29. Guruswami, V., Xia, P.: Polar codes: Speed of polarization and polynomial gap to capacity. In: 54th Annual Symposium on Foundations of Computer Science. pp. 310–319. IEEE Computer Society Press, Berkeley, CA, USA (Oct 26–29, 2013) 5, 13
30. Hoeffding, W.: Probability inequalities for sums of bounded random variables. Journal of the American Statistical Association 58(301), pp. 13–30 (1963), http://www.jstor.org/stable/2282952 14
31. Impagliazzo, R., Luby, M.: One-way functions are essential for complexity based cryptography (extended abstract). In: 30th Annual Symposium on Foundations of Computer Science. pp. 230–235. IEEE Computer Society Press, Research Triangle Park, North Carolina (Oct 30 – Nov 1, 1989) 2
32. Ishai, Y., Kushilevitz, E., Ostrovsky, R., Prabhakaran, M., Sahai, A., Wullschleger, J.: Constant-rate oblivious transfer from noisy channels. In: Rogaway, P. (ed.) Advances in Cryptology – CRYPTO 2011. Lecture Notes in Computer Science, vol. 6841, pp. 667–684. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 14–18, 2011) 6, 8, 9, 14, 24
33. Ishai, Y., Kushilevitz, E., Ostrovsky, R., Sahai, A.: Extracting correlations. In: 50th Annual Symposium on Foundations of Computer Science. pp. 261–270. IEEE Computer Society Press, Atlanta, Georgia, USA (Oct 25–27, 2009) 2
34. Ishai, Y., Prabhakaran, M., Sahai, A.: Founding cryptography on oblivious transfer - efficiently. In: Wagner, D. (ed.) Advances in Cryptology – CRYPTO 2008. Lecture Notes in Computer Science, vol. 5157, pp. 572–591. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 17–21, 2008) 2, 6, 8, 24
35. Katz, J.: Universally composable multi-party computation using tamper-proof hardware. In: Naor, M. (ed.) Advances in Cryptology – EUROCRYPT 2007. Lecture Notes in Computer Science, vol. 4515, pp. 115–128. Springer, Heidelberg, Germany, Barcelona, Spain (May 20–24, 2007) 2
36. Kilian, J.: Founding cryptography on oblivious transfer. In: 20th Annual ACM Symposium on Theory of Computing. pp. 20–31. ACM Press, Chicago, Illinois, USA (May 2–4, 1988) 2, 5
37. Kilian, J.: A general completeness theorem for two-party games. In: 23rd Annual ACM Symposium on Theory of Computing. pp. 553–560. ACM Press, New Orleans, Louisiana, USA (May 6–8, 1991) 2
38. Kilian, J.: More general completeness theorems for secure two-party computation. In: 32nd Annual ACM Symposium on Theory of Computing. pp. 316–324. ACM Press, Portland, Oregon, USA (May 21–23, 2000) 2, 9
39. Korjik, V., Morozov, K.: Generalized oblivious transfer protocols based on noisy channels. In: Gorodetski, V.I., Skormin, V.A., Popyack, L.J. (eds.) Information Assurance in Computer Networks: Methods, Models, and Architectures for Network Security, International Workshop MMM-ACNS 2001, St. Petersburg, Russia, May 21-23, 2001, Proceedings. Lecture Notes in Computer Science, vol. 2052, pp. 219–229. Springer (2001), http://dx.doi.org/10.1007/3-540-45116-1_22 9
40. Kraschewski, D., Maji, H.K., Prabhakaran, M., Sahai, A.: A full characterization of completeness for two-party randomized function evaluation. In: Nguyen, P.Q., Oswald, E. (eds.) Advances in Cryptology – EUROCRYPT 2014. Lecture Notes in Computer Science, vol. 8441, pp. 659–676. Springer, Heidelberg, Germany, Copenhagen, Denmark (May 11–15, 2014) 4, 6, 8, 9, 24
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: 6th Theory of Cryptography Conference. Lecture

Notes in Computer Science, vol. 5444, pp. 238–255. Springer, Heidelberg, Germany (Mar 15–17, 2009) 2
42. Kushilevitz, E.: Privacy and communication complexity. In: 30th Annual Symposium on Foundations of Computer Science. pp. 416–421. IEEE Computer Society Press, Research Triangle Park, North Carolina (Oct 30 – Nov 1, 1989) 2
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: 6th Theory of Cryptography Conference. Lecture Notes in Computer Science, vol. 5444, pp. 256–273. Springer, Heidelberg, Germany (Mar 15–17, 2009) 2
44. Maji, H.K., Prabhakaran, M., Rosulek, M.: A unified characterization of completeness and triviality for secure function evaluation. In: Galbraith, S.D., Nandi, M. (eds.) Progress in Cryptology - INDOCRYPT 2012: 13th International Conference in Cryptology in India. Lecture Notes in Computer Science, vol. 7668, pp. 40–59. Springer, Heidelberg, Germany, Kolkata, India (Dec 9–12, 2012) 2, 9
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, August 9-13, 2004, San Diego, CA, USA. pp. 287–302. USENIX (2004), http://www.usenix.org/publications/library/proceedings/sec04/tech/malkhi.html 2
46. Moran, T., Segev, G.: David and goliath commitments: UC computation for asymmetric parties using tamper-proof hardware. In: Smart, N.P. (ed.) Advances in Cryptology - EUROCRYPT 2008, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13-17, 2008. Proceedings. Lecture Notes in Computer Science, vol. 4965, pp. 527–544. Springer (2008), http://dx.doi.org/10.1007/978-3-540-78967-3_30 2
47. Nascimento, A.C.A., Winter, A.J.: On the oblivious-transfer capacity of noisy resources. IEEE Transactions on Information Theory 54(6), 2572–2581 (2008), http://dx.doi.org/10.1109/TIT.2008.921856 2
48. 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.) Advances in Cryptology – CRYPTO 2012. Lecture Notes in Computer Science, vol. 7417, pp. 681–700. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 19–23, 2012) 2
49. Rabin, M.: How to exchange secrets by oblivious transfer. Tech. Rep. TR-81, Harvard Aiken Computation Laboratory (1981) 2
50. Rabin, T., Ben-Or, M.: Verifiable secret sharing and multiparty protocols with honest majority (extended abstract). In: 21st Annual ACM Symposium on Theory of Computing. pp. 73–85. ACM Press, Seattle, Washington, USA (May 15–17, 1989) 2
51. Savvides, G.: Interactive Hashing and Reductions Between Oblivious Transfer Variants. Ph.D. thesis, Montreal, Que., Canada, Canada (2007), aAINR32237 7
52. Shannon, C.E.: Communication theory of secrecy systems. Bell Systems Technical Journal 28(4), 656–715 (1949) 4, 6
53. Wiesner, S.: Conjugate coding. SIGACT News 15, 78–88 (January 1983), http://doi.acm.org/10.1145/1008908.1008920 2
54. Wolf, S., Wullschleger, J.: Oblivious transfer is symmetric. In: Vaudenay, S. (ed.) Advances in Cryptology – EUROCRYPT 2006. Lecture Notes in Computer Science, vol. 4004, pp. 222–232. Springer, Heidelberg, Germany, St. Petersburg, Russia (May 28 – Jun 1, 2006) 2

55. Wullschleger, J.: Oblivious-transfer amplification. In: Naor, M. (ed.) Advances in Cryptology – EUROCRYPT 2007. Lecture Notes in Computer Science, vol. 4515, pp. 555–572. Springer, Heidelberg, Germany, Barcelona, Spain (May 20–24, 2007) 2, 3, 4, 5, 7, 11
56. Wullschleger, J.: Oblivious transfer from weak noisy channels. In: Reingold, O. (ed.) TCC 2009: 6th Theory of Cryptography Conference. Lecture Notes in Computer Science, vol. 5444, pp. 332–349. Springer, Heidelberg, Germany (Mar 15–17, 2009) 2, 11
57. Yao, A.C.C.: Theory and applications of trapdoor functions (extended abstract). In: 23rd Annual Symposium on Foundations of Computer Science. pp. 80–91. IEEE Computer Society Press, Chicago, Illinois (Nov 3–5, 1982) 2, 5