Cryptography with One-Way Communication

Sanjam Garg[1]*, Yuval Ishai[2]**, Eyal Kushilevitz[2]***, Rafail Ostrovsky[3]†, and Amit Sahai[3]‡

[1] UC Berkeley
[2] Technion
[3] UCLA

Abstract. There is a large body of work on using noisy communication channels for realizing different cryptographic tasks. In particular, it is known that secure message transmission can be achieved unconditionally using only *one-way* communication from the sender to the receiver. In contrast, known solutions for more general secure computation tasks inherently require interaction, even when the entire input originates from the sender.

We initiate a general study of cryptographic protocols over noisy channels in a setting where only one party speaks. In this setting, we show that the landscape of what a channel is useful for is much richer. Concretely, we obtain the following results.

– **Relationships between channels.** The binary erasure channel (BEC) and the binary symmetric channel (BSC), which are known to be securely reducible to each other in the interactive setting, turn out to be qualitatively different in the setting of one-way communication. In particular, a BEC cannot be implemented from a BSC,

* Supported by NSF CRII Award 1464397.

** Supported by BSF grant 2012378 and by the European Union's Tenth Framework Programme (FP10/2010-2016) under grant agreement no. 259426 ERC-CaC.

*** Supported by ISF grant 1709/14 and BSF grant 2012378.

† Work supported in part by NSF grants 09165174, 1065276, 1118126 and 1136174, US-Israel BSF grant 2008411, OKAWA Foundation Research Award, IBM Faculty Research Award, Xerox Faculty Research Award, B. John Garrick Foundation Award, Teradata Research Award, and Lockheed-Martin Corporation Research Award. This material is based upon work supported by the Defense Advanced Research Projects Agency through the U.S. Office of Naval Research under Contract N00014 -11 -1-0392. The views expressed are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

‡ Research supported in part from a DARPA/ONR PROCEED award, 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 U.S. Office of Naval Research under Contract N00014-11-1-0389. 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.

and while the erasure probability of a BEC can be manipulated in both directions, the crossover probability of a BSC can only be manipulated in one direction.

- **Zero-knowledge proofs and secure computation of deterministic functions.** One-way communication over BEC or BSC is sufficient for securely realizing any deterministic (possibly reactive) functionality which takes its inputs from a sender and delivers its outputs to a receiver. This provides the first truly non-interactive solutions to the problem of zero-knowledge proofs.
- **Secure computation of randomized functions.** One-way communication over BEC or BSC *cannot* be used for realizing general randomized functionalities which take input from a sender and deliver output to a receiver. On the other hand, one-way communication over other natural channels, such as bursty erasure channels, can be used to realize such functionalities. This type of protocols can be used for distributing certified cryptographic keys without revealing the keys to the certification authority.

1 Introduction

The seminal work of Wyner [Wyn75] demonstrated the usefulness of noise for secure communication. Since then, there has been a large body of work on basing various cryptographic primitives, such as key agreement and commitment [BBCM95,BBR88,Mau91,DKS99,WNI03,Wul09,RTWW11], on different types of noisy communication channels.

In 1988, Crépeau and Kilian [CK88] showed that noise in a communication channel can be used to realize essentially everything a cryptographer could wish for. In particular, they showed that any non-trivial *binary-symmetric channel* (BSC) can be used to realize *oblivious transfer* (OT) which is sufficient for realizing two-party secure computation. (More efficient construction were later considered in [KM01,SW02,IKO$^+$11b].) Finally, Crépeau, Morozov and Wolf [CMW04] generalized these results to arbitrary *discrete memory-less* channels. Other results towards characterizing the types of channels on which OT can be based appeared in [Kil88,DKS99,DFMS04,Wul07,Wul09].

Following the work of Crépeau and Kilian [CK88], the entire body of research on secure two-party computation over noisy channels requires parties to interact. In contrast, the present paper considers cryptographic protocols which only use *one-way communication*, namely ones in which only one party speaks. There has been a considerable amount of work on realizing information-theoretic secure message transmission in this setting. These works are motivated not only by the goal of achieving information-theoretic security, but also by the goal of efficiency; see [BTV12] for discussion. Our goal is to extend this study to more general cryptographic tasks, including useful special cases of secure two-party computation in which the input originates from only one party.

1.1 Our Model

We model a channel as an ideal functionality $\mathcal{C}$. This is done in order to capture the security properties of the channel in a clean way and in order to facilitate the use of composition theorems. A channel provides a communication medium between a *sender* and a *receiver*. The sender can invoke the channel $\mathcal{C}$ on an input of its choice. The channel "based on its nature" processes the input and outputs the processed value to the receiver. The correctness and secrecy requirements of a channel and the protocols we build on top of it can be specified in terms of UC security. For example, consider a binary erasure channel (BEC) parameterized by a probability $p \in (0, 1)$. For this channel, the sender inputs a bit $x \in \{0, 1\}$ and the channel outputs (for the receiver) x with a probability p and $\perp$ with a probability $1 - p$. [4] Even for this basic channel, stating the correctness and security properties is non-trivial. Correctness requires that if the sender sends x then the receiver outputs either x or $\perp$ with the right probability distribution. Security is a bit more involved; it requires that no malicious sender can figure out whether the receiver actually received the sent bit or not, and that a malicious receiver does not learn any partial information about the sent bit in the case of an erasure.

In this work, we consider various such channels. Two other channels that would be of great interest to us are the *binary symmetric channel* (BSC) and the *random oblivious transfer* (ROT) channel. A BSC is parameterized by a probability $p \in (\frac{1}{2}, 1)$. For this channel, the sent bit is transmitted correctly with probability p and is flipped with probability $1 - p$. An ROT channel takes as input two strings m_0 and m_1 from the sender and outputs either $(m_0, \perp)$ or $(\perp, m_1)$ to the receiver, with equal probability.

When considering protocols built on top of such channels, we distinguish between the weaker *semi-honest* model, where the sender follows the protocol but tries to learn information about the receiver's output from its random coins, and the *malicious model*, where the sender may send arbitrary information over the channel. When the sender follows the protocol, the receiver's output should be as specified by the functionality. When the sender deviates from the protocol, the security requirement uses the standard real-ideal paradigm, asserting that the sender's strategy can be simulated by a distribution over honest strategies. It is important to note, however, that in this case the standard definition of "security with abort" also allows the sender to make the protocol fail, as long as the receiver can detect this failure. By default, the term "secure" refers to the malicious model, though most of our negative results apply also to the semi-honest model.

1.2 Our Results

We initiate a general study of one-way secure computation (OWSC) protocols over noisy channels in a setting where only one party speaks. Surprisingly, the

[4] In the literature, p sometimes stands for the error probability, while in our paper it is the probability of the "no noise" event.

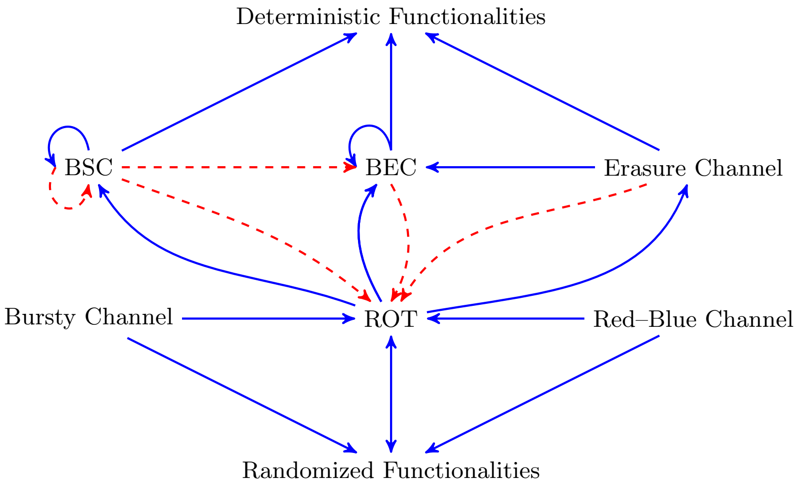

Fig. 1. Relationships among different kinds of channels and their applications. Solid arrows are used to denote a positive reduction, i.e. $A \rightarrow B$ implies that B can be constructed given A. On the other hand, dashed arrows indicate negative results, i.e. $A \dashrightarrow B$ implies that B cannot be constructed given A. Solid self-edge of BEC indicates that the transmission probability of a BEC can be manipulated in both directions. On the other hand, the solid and dashed self-edges of BSC respectively indicate that the probability of correct transmission of a BSC can be diminished (and brought closer to $\frac{1}{2}$) but cannot be amplified.

one-way setting is strikingly different from the interactive setting. In the interactive setting, all finite channels are either trivial, equivalent to secure message transmission, or equivalent to oblivious transfer. On the other hand, in the setting of OWSC, the landscape of what a channel is useful for is much richer. Specifically, we obtain the following results. All the implications have been summarized in Figure 1.

- **Relationships between channels.** Binary erasure channel (BEC) and binary symmetric channel (BSC), which are known to be securely reducible to each other in the interactive setting, turn out to be qualitatively very different in the setting of one-way communication. In particular, we show that a BEC cannot be implemented given a BSC. Also, somewhat surprisingly, we show that while the erasure probability of a BEC can be manipulated in both directions the probability of correct transmission of a BSC can only be manipulated in one direction.
- **Deterministic functions.** We show that both BEC and and BSC are sufficient for securely realizing any deterministic (possibly reactive) functionality that takes input from a sender and delivers its output to a receiver with only one-way communication. This provides the *first* truly non-interactive solution to the problem of zero-knowledge. We extend our results to the

Generalized Erasure Channel (GEC) which is a generalization of BEC (see Section 3 for formal definition).

- **Randomized functions.** We show that neither BEC nor BSC can be used (even assuming computational assumptions) for the task of realizing randomized functionalities which take input from a sender and deliver output to a receiver, in the setting of one-way communication. Nonetheless, one-way communications over natural channels, such as bursty erasure channels, can be used to realize such functionalities. This result is obtained by first constructing a random oblivious-transfer channel (ROT) and building on the techniques from [IPS08,IKO$^+$11a]. This provides the first non-trivial feasibility result for secure-computation in a setting where only one party speaks.

1.3 Applications

One-way secure computation (OWSC) both for deterministic and randomized functionalities enable a number of applications for which there are no known solutions.

Truly non-interactive zero-knowledge. Non-interactive zero-knowledge proof systems (NIZKs) [BFM90,FLS99] are a fundamental tool in cryptography with widespread applications. However, all known constructions rely on a common random string (or a random oracle)[5] and inherently fail to achieve useful features such as non-transferability or deniability [Pas03]. OWSC for deterministic functions provides the *first* truly non-interactive solution to the problem of zero-knowledge. This solution does not rely on a shared string between parties or a random oracle and achieves non-transferability and deniability properties. Furthermore, this solution achieves information theoretic and composable security.

Oblivious certification of cryptographic keys. Public-key cryptography relies on the existence of certification authorities (like Verisign) who sign the public keys of different parties. All known implementations of this certification procedure rely on interaction. Our OWSC for randomized functionalities provides for the *first* candidate to realize this procedure with just one-way communication. More specifically, our protocol allows the certification authority to send a public-key secret-key pair along with a certificate on the public key with just one-way communication. We stress that in this setting the certification authority itself does not learn the secret key of the recipient party, as the randomness used in its generation is derived from the channel. However, if the certificate authority deviates from the protocol, the recipient may detect failure rather than output a pair of keys.

[5] The result of Barak and Pass [BP04] is an exception to this. However they only achieve a weaker notion where security is only guaranteed against uniform provers. We, on the other hand, are interested in the standard notion of zero-knowledge.

Fair puzzle distribution. Consider a Sudoku Puzzle competition where the organizer of the competition would like to generate signed puzzles for all the participants. However the participants do not trust the organizer and would like their challenge Sudoku puzzles to be of the same difficulty. More specifically, we would like to have a mechanism that allows the competition organizer to provide independent puzzles of a pre-specified difficulty level (along with a signature on this puzzle) to each of the participants. The participants should be assured not only that the puzzles were generated independently from the correct distribution, but also that the organizers do not have an edge in solving the puzzles they generated (e.g., by generating random solved puzzles). There are no known solutions for this problem in a setting with just one-way communication. Our OWSC protocol for randomized functions gives the first such solution.

2 Preliminaries

Let λ denote a security parameter. We say that a function is *negligible* in λ if it is asymptotically smaller than the inverse of any fixed polynomial in λ. Otherwise, the function is said to be *non-negligible* in λ. We say that an event happens with *overwhelming* probability if it happens with probability $p(\lambda) = 1 - \nu(\lambda)$, where $\nu(\lambda)$ is a negligible function in λ. We use $[n]$ to denote the set $\{1, \ldots, n\}$.

Monotone Sets. Let $X_1, X_2 \ldots X_n$ be independent Bernoulli variables with $\Pr[X_i = 1] = p_i$. We define $Q_n = \{0,1\}^n$ (the *n-cube*) and identify each element $a \in Q_n$ with the corresponding subset of $[n]$; i.e., $\{i \mid a_i = 1\}$. We define a probability measure Pr on Q_n by:

$$\Pr(a) = \prod_{i \in a} p_i \prod_{i \notin a} (1 - p_i) \ .$$

A set $A \subseteq Q_n$ is said to be a *monotone* if $a \in A$ and $a \subseteq b$ implies that $b \in A$.

Lemma 1 (Harris [Har60], Kleitman [Kle66]). *If A and B are two monotone subsets of Q_n then A and B are* positively correlated*; namely,*

$$\Pr[A \cap B] \geq \Pr[A] \Pr[B].$$

Chernoff bounds. Let $X_1, X_2 \ldots X_n$ be independent Bernoulli variables with $\Pr[X_i = 1] = p_i$. Let $X = \sum_{i=1}^{n} X_i$ and μ be the expectation of X. Then,

$$\Pr(X \geq (1+\delta)\mu) \leq e^{-\frac{\delta^2 \mu}{3}}, \text{ for } 0 < \delta < 1.$$

$$\Pr(X \leq (1-\delta)\mu) \leq e^{-\frac{\delta^2 \mu}{2}}, \text{ for } 0 < \delta < 1.$$

3 Different kinds of channels

In this work, we model a channel as an ideal functionality $\mathcal{C}$. This is done in order to capture the security properties of a channel in a clean way. A channel provides a (one-way) communication medium between a *sender* and a *receiver*. The sender can invoke the channel $\mathcal{C}$ on an input of its choice. The channel "based on its nature", processes the input and outputs the processed value to the receiver. The correctness and secrecy requirements of a channel can be specified by a two-party functionality, which takes an input from the sender, generates some internal randomness, and delivers an output to the receiver. Our formulation of channel functionalities, as well as the security definition of protocols that build on top of them, follow the standard UC framework [Can05]. All of our positive results hold with statistical security, and some of our negative results apply also to the case of computational security. We will consider the following types of channels.

Binary Erasure Channel. The binary erasure channel (BEC) is perhaps the simplest non-trivial channel model considered in the literature. We denote this channel by $\mathcal{C}^p_{BEC}$. For this channel, the sender inputs a bit $x \in \{0,1\}$ and the channel outputs (to the receiver) x with a probability p and $\perp$ with a probability $1-p$.

Binary Symmetric Channel. The binary symmetric channel (BSC) denoted by $\mathcal{C}^p_{BSC}$ (for $p > \frac{1}{2}$) is a channel in which the sender inputs a bit $x \in \{0,1\}$ and the channel outputs (for the receiver) x with a probability p and $1-x$ with a probability $1-p$.

Generalized Erasure Channel. The generalized erasure channel (GEC) is a generalization of the BEC, where k strings are sent by the sender and some subset of them, determined by a probability distribution $\mathcal{D}$, is erased. We denote this channel by $\mathcal{C}^{k,\ell,\mathcal{D}}_{GEC}$. Formally, the functionality takes as input k strings $x_1, \ldots, x_k \in \{0,1\}^\ell$ from the sender. It samples a string $s \in \{0,1\}^k$ (which we call the *randomness of the channel*) according to the distribution $\mathcal{D}$. If $s_i = 1$ then set $y_i = x_i$ and, otherwise, $y_i = \perp$. The functionality outputs $y_1, \ldots, y_k$ to the receiver. We will consider the following special cases of the generalized erasure channel.

- *ℓ-Bit Random Oblivious Transfer.* The ℓ-bit random oblivious transfer channel (ℓ-ROT) denoted by $\mathcal{C}^{\ell}_{ROT}$ corresponds to the channel $\mathcal{C}^{2,\ell,\mathcal{D}_{2,OT}}_{GEC}$, where $\mathcal{D}_{2,OT}$ is the distribution that outputs a uniformly random value in $\{01, 10\}$. We also consider a p-biased ℓ-bit ROT channel denoted by $\mathcal{C}^{\ell,p}_{ROT}$ corresponds to the channel $\mathcal{C}^{2,\ell,\mathcal{D}_{2,p,OT}}_{GEC}$, where $\mathcal{D}_{2,p,OT}$ is the distribution that outputs 10 with probability p and 01 with a probability $1-p$.
- *(k,ℓ,p)-Erasure Channel.* The (k,ℓ,p)-erasure channel corresponds to the channel $\mathcal{C}^{k,\ell,\mathcal{D}_{k,p}}_{GEC}$, where $\mathcal{D}_{k,p}$ is the distribution that outputs a k bit string s such that, for every $i \in [k]$, we have $s_i = 1$ with probability p and $s_i = 0$ with probability $1-p$.

– (k,ℓ)*-Perfect Red-Blue Channel.* The (k,ℓ)-Perfect Red-Blue channel corresponds to the channel $\mathcal{C}_{GEC}^{k,\ell,\mathcal{D}_{k,RB}}$, where $\mathcal{D}_{k,RB}$ is any distribution such that each string in its output space (namely $\{0,1\}^k$) may be labeled either Red or Blue (or none) in a way that $\Pr[\mathsf{Red} \cup \mathsf{Blue}] = 1$, $\Pr[\mathsf{Red}] = \Pr[\mathsf{Blue}]$ and $\forall r \in \mathsf{Red}$ and $\forall s \subseteq r$ we have that $s \notin \mathsf{Blue}$ and, similarly, $\forall b \in \mathsf{Blue}$ and $\forall c \subseteq b$ we have that $c \notin \mathsf{Red}$.[6]
– (k,ℓ,μ,ν,η)*-Statistical Red-Blue Channel.* The (k,ℓ,μ,ν,η)-Statistical Red-Blue channel is a relaxed version of the Perfect Red-Blue Channel, that corresponds to the channel $\mathcal{C}_{GEC}^{k,\ell,\mathcal{D}_{k,\mu,\nu,\eta}}$, where $\mathcal{D}_{k,\mu,\nu,\eta}$ is any distribution whose output space can be labelled Red and Blue such that (i) $\Pr[\mathsf{Red} \cup \mathsf{Blue}] \geq 1-\mu$, (ii) $|\Pr[\mathsf{Red}] - \Pr[\mathsf{Blue}]| \leq \nu$, (iii) $\Pr_{r \in \mathsf{Red}}[\exists s \subseteq r$ such that $s \in \mathsf{Blue}] \leq \eta$, and (iv) $\Pr_{b \in \mathsf{Blue}}[\exists c \subseteq b$ such that $c \in \mathsf{Red}] \leq \eta$.
– (k,ℓ,b)*-Perfect Bursty Channel.* This is an erasure channel where all b erasures appear in a "burst". Formally, the (k,ℓ,b)-Perfect bursty channel corresponds to the channel $\mathcal{C}_{GEC}^{k,\ell,\mathcal{D}_{k,b}}$, where $\mathcal{D}_{k,b}$ is the distribution that outputs a k bit string such that all the bits are set to 1 besides the bits in locations $x+1, x+2, \ldots, x+b$ where x is chosen uniformly from $\{0,\ldots,k-b\}$.
– (k,ℓ,b,σ)*-Noisy Bursty Channel.* This is an erasure channel where erasures still appear in a "burst" but their number b' is normally distributed around b. Formally, the (k,ℓ,b,σ)-noisy bursty channel corresponds to the channel $\mathcal{C}_{GEC}^{k,\ell,\mathcal{D}_{k,b,\sigma}}$ for typical $k \gg b$, where $\mathcal{D}_{k,b,\sigma}$ is the distribution that outputs a k bit string such that all the bits are set to 1 besides the bits in locations $x+1, x+2, \ldots, x+b'$ where b' is sampled from a gaussian and rounded to the closest non-negative integer $\leq k$ with mean b and standard deviation σ and then x is chosen uniformly from $\{0,\ldots,k-b'\}$.

4 Classification of functionalities

Below we define the notion of one-way secure computation (OWSC) over a channel $\mathcal{C}$ (thought of as a non-reactive ideal functionality). We shall refer to such a OWSC scheme as $OWSC/\mathcal{C}$.

An $\mathsf{OWSC}^f/\mathcal{C}$ scheme for a function $f : X \to Y$ is a two-party protocol between Sender and Receiver and it follows the following format:

- Sender gets an input $x \in X$.
- Sender invokes the channel $\mathcal{C}$ (possibly multiple instances of the channel) with inputs of its choice. The channel, based on its nature, processes the input value and outputs it to the Receiver.
- Receiver carries out a local computation and outputs $f(x)$ or an error message.

Similarly, we can consider reactive functionality specified by a *stateful* function $f : \Sigma \times X \to \Sigma \times Y$. The Sender of a $\mathsf{OWSC}^f/\mathcal{C}$ scheme for a stateful function f obtains multiple inputs on the fly. On obtaining an input $x \in X$, Sender can

[6] Here, again, we identify each $a \in \{0,1\}^k$ with a subset of $[k]$ in the natural way.

invoke the channel $\mathcal{C}$ multiple times and in each execution the Receiver should either output y where $(\sigma', y) \leftarrow f(\sigma, x)$ (where $\sigma \in \Sigma$ is the current state and σ' is the state for the next execution) or an error message. The first execution of the protocol sets the state to ϵ.

The correctness and secrecy requirements of an OWSC scheme can be specified in terms of an ideal functionality. An $\mathsf{OWSC}^f/\mathcal{C}$ scheme for f is required to be a secure realization of the following function $\mathcal{F}_f$ in the $\mathcal{C}$-hybrid model.

- $\mathcal{F}_f$ accepts $x \in X$ from the Sender and outputs $f(x)$ to the receiver. If x is a special input `error`, then it outputs `error` to the Receiver.

We shall denote the security parameter by λ and require that the sender and the receiver in any scheme run in time polynomial in λ and the size of the circuit computing the function f. Further, for a scheme to be considered secure, we require that the simulation error be at most $2^{-\Omega(\lambda)}$.

Definition 1 (Completeness for deterministic functionalities). *A channel $\mathcal{C}$ is said to be* OWSC complete for deterministic functionalities*, if for every deterministic function $f : X \to Y$ there exists a $\mathsf{OWSC}^f/\mathcal{C}$ scheme that is a UC-secure realization of the functionality $\mathcal{F}_f$ in the $\mathcal{C}$-hybrid model.*

Definition 2 (Completeness for randomized functionalities). *A channel $\mathcal{C}$ is said to be* OWSC complete for randomized functionalities*, if for every randomized function $f : X \to Y$ there exists a $\mathsf{OWSC}^f/\mathcal{C}$ scheme that is a UC-secure realization of the functionality $\mathcal{F}_f$ in the $\mathcal{C}$-hybrid model.*

5 Reductions among channels

In this section, we study the relationships between different kinds of channels. Specifically:

- **Impossibility results for $\mathcal{C}_{ROT}$.** One of the key channels of interest to us is the random oblivious transfer channel. We start by establishing (in Section 5.1) that this channel cannot be securely realized out of the most basic channels such as $\mathcal{C}_{BEC}$ (in fact, from any $\mathcal{C}_{GEC}^{k,\ell,\mathcal{D}_{k,p}}$, where $\mathcal{D}_{k,p}$ is the distribution that outputs a k bit string s such that, for every $i \in [k]$, we have $s_i = 1$ with probability p and $s_i = 0$ with probability $1-p$) and $\mathcal{C}_{BSC}$. In full-version, we provide extensions of these results to the computational setting (but ruling out only protocols with negligible error rather than small noticeable error).
- **Positive results for $\mathcal{C}_{ROT}$.** We consider a variety of more structured channels, such as the Red-Blue channel and the bursty channel, and give constructions of random oblivious transfer channel from such channels (Section 5.2).
- **Self-transformations for $\mathcal{C}_{BEC}$ and $\mathcal{C}_{BSC}$.** We move back to the basic channels ($\mathcal{C}_{BEC}$ and $\mathcal{C}_{BSC}$) and study additional properties of them. Although both these channels do not imply $\mathcal{C}_{ROT}^1$, they are of a very different nature. We show (in Section 5.3) that erasure probabilities of the $\mathcal{C}_{BEC}$

can be easily manipulated but the flipping probability of $\mathcal{C}_{BSC}$ is harder to manipulate. In particular, we show that, given a $\mathcal{C}_{BEC}$, we can construct another $\mathcal{C}_{BEC}$ with amplified or diminished erasure probabilities. On the other hand, given a $\mathcal{C}_{BSC}$, we can only construct another $\mathcal{C}_{BSC}$ with amplified flipping probability. In fact, diminishing the flipping probability turns out to be is impossible.

We remark that all the impossibility results (in this section) are stated in terms of the simulation based notion but hold even for a weaker game-based security notion. These stronger impossibility results are implied by the proofs and are not spelled out explicitly.

5.1 Impossibility results for $\mathcal{C}_{ROT}$

In this subsection, we rule out the construction of $\mathcal{C}_{ROT}^{1}$ (random oblivious transfer) from the most basic channels such as $\mathcal{C}_{BEC}$ and $\mathcal{C}_{BSC}$. In particular, we show:

- $\mathcal{C}_{ROT}^{\ell'}$ (and, in fact, even biased-ROT) cannot be non-interactively securely realized from $\mathcal{C}_{GEC}^{k,\ell,\mathcal{D}_{k,p}}$.
- $\mathcal{C}_{BEC}^{p'}$ cannot be non-interactively securely realized from $\mathcal{C}_{BSC}^{p}$. It is easy to realize $\mathcal{C}_{BEC}^{\frac{1}{2}}$ from $\mathcal{C}_{ROT}^{\ell'}$. Hence, combining with the above result, we also conclude that $\mathcal{C}_{ROT}^{\ell'}$ cannot be non-interactively securely realized from $\mathcal{C}_{BSC}^{p}$.

The following theorem and its proof can be adapted to rule out even $\mathcal{C}_{ROT}^{\ell',q}$ for any constant q. We state the result and the proof in the simpler setting where $q = \frac{1}{2}$.

Theorem 1. *$\exists\ \varepsilon \in (0,1)$ and $\ell' \in \mathbb{Z}^+$ such that $\forall k, \ell, p$, the channel $\mathcal{C}_{ROT}^{\ell'}$ cannot be ε-securely realized in the $\mathcal{C}_{GEC}^{k,\ell,\mathcal{D}_{k,p}}$ hybrid model even against* semi-honest *adversaries.*

We start by giving some intuition for the case of binary erasure channel. The intuition extends to (k, ℓ, p)-erasure channels in a natural way. In any protocol for non-interactively realizing $\mathcal{C}_{ROT}^{1}$ the sender will need to encode both its inputs m_0, m_1 into its first message. Whether the receiver obtains m_0 or m_1 should depend solely on the random coins of the channel. In other words, erasure of certain bits (or more generally one combination from a list of possible choices) allows the receiver to obtain m_0 while erasure of another combination allows the receiver to learn m_1. The key issue is that a binary erasure channel erases each bit sent by the sender independently with a probability $1 - p$. Consider the scenario in which a receiver can obtain m_0 from the received bits. In this scenario, since each bit sent by the sender is treated independently we have that the receiver also obtains m_1 with a large enough probability, contradicting the security of the protocol. Arguing the last step formally is tricky and we rely on the Harris-Kleitman inequality for our argument. The full proof appears in the full-version.

Theorem 2. *$\forall p \in (\frac{1}{2}, 1)$, $p' \in (0,1)$ and protocol π, $\exists \varepsilon$ such that π does not ε-securely realize $\mathcal{C}^{p'}_{BEC}$ in the $\mathcal{C}^{p}_{BSC}$-hybrid model even against* semi-honest *adversaries.*

We start by giving some intuition. Any protocol for non-interactively securely realizing $\mathcal{C}_{BEC}$ will need the sender to encode its input m into its first message. Whether the receiver obtains m or not should depend solely on the random coins of the channel. In other words when certain bits (or, more generally, one combination from a list of possible choices) is flipped then the receiver loses all information about m while flipping another combination allows the receiver to learn m completely. Consider a sequence of hybrid strings between a pair of strings on which the receiver outputs m and $\perp$ respectively. Among the hybrid strings there must exist two strings that differ in exactly one bit but are such that the receiver's output on the two differs completely. At this point, we argue that a change of just one bit cannot affect the receiver's best guess about the sent bit very dramatically, contradicting the security of the protocol. The key technical challenge of the proof lies in proving that this happens with a noticeable probability. The full proof appears in the full-version.

5.2 Positive constructions for $\mathcal{C}_{ROT}$

We start by presenting a construction of a random oblivious transfer channel in Red-Blue channel hybrid model. Our construction provides a solution for any arbitrary Red-Blue channel and is inefficient. Furthermore, such a channel in its generality is not very natural. Therefore, we study natural examples of Red-Blue channels (and their approximate variants) and attempt at more efficient solutions.

We start by considering the basic setting of an arbitrary Red-Blue Channel and prove that it is sufficient to realize a random oblivious transfer channel.

Theorem 3. *$\mathcal{C}^{\ell}_{ROT}$ can be $\max\{\mu, \nu, \eta\}$-UC-securely realized (even against malicious adversaries) in the $(k, \ell', \mu, \nu, \eta)$-Red-Blue Channel hybrid model where $\ell' = \ell \cdot 2^k$.*

The proof appears in the full-version.Note that for the case of perfect Red-Blue Channel, we have that $\mu = \nu = \eta = 0$, and hence $\mathcal{C}^{\ell}_{ROT}$ can be perfectly-UC-securely realized in the (k, ℓ')-Perfect Red-Blue Channel hybrid model where $\ell' = \ell \cdot 2^k$.

Efficient construction for ROT. We will start by considering the case of perfect bursty channel and show that it can be used to realize ROT. Recall that a (k, ℓ, b)-perfect bursty channel corresponds to the channel $\mathcal{C}^{k,\ell,\mathcal{D}_{k,b}}_{GEC}$, where $\mathcal{D}_{k,b}$ is the distribution that outputs a k bit string such that all the bits are set to 1 besides the "burst" of bits in locations $x+1, x+2, \ldots, x+b$ which are set to 0, where x is chosen uniformly from $\{0, \ldots, k-b\}$. In this setting we claim that:

Theorem 4. *$\mathcal{C}_{ROT}^{\ell}$ can be UC-securely realized (even against malicious adversaries) in the (k, ℓ, b)-perfect bursty channel hybrid model when $b > \frac{k}{2}$ or when b is odd.*

Proof. We start by giving the intuition. The key idea is to use Shamir's secret sharing (with shares of length ℓ) and secret share the first string in the first half and the second string in the second half (with some appropriate threshold). Both when $b > \frac{k}{2}$ or when b is odd we will have an asymmetry in terms of the deletion pattern. If more terms from the first half are erased then the first string is deleted and, on the other hand, if more terms from the second half get erased then the second string is deleted. If k is odd then our construction will only give a biased-ROT but this bias can be corrected using the transformation from Section 7. Similarly, we note that in our construction we do not need the distribution over where the burst happens to be uniform. Our protocol can be very easily modified so that this restriction is not crucial. This would however only give biased ROT protocols and this bias will need to be corrected using the transformation from Section 7.

Next we give the construction for the case when b is odd. We assume, for simplicity, that k is even and $t = \frac{k}{2}$. The construction for the setting when k is odd or when b is not necessarily odd but $k > b/2$ are identical except that the parameters should be adjusted appropriately.

$\Pi = \langle S, R \rangle$ **protocol with sender input** m_0, m_1

1. Let $\theta = t - \lfloor b/2 \rfloor$. Let $\{\alpha_1, \ldots, \alpha_t\}$ be a θ-out-of-t Shamir's secret sharing of m_0. Similarly, let $\{\alpha_{t+1}, \ldots, \alpha_k\}$ be a θ-out-of-t Shamir's secret sharing of m_1.
2. Send $(\alpha_1, \ldots, \alpha_k)$ to the receiver.
3. Let the starting point of the burst in the symbols received by the receiver be i^*. If $i^* > \theta$ compute m_0 using the shares $\alpha_1, \ldots, \alpha_\theta$ and output $(m_0, \perp)$; otherwise, output $(\perp, m_1)$ where m_1 is computed using the shares $\alpha_{k-\theta+1}, \ldots, \alpha_k$.

Fig. 2. $\mathcal{C}_{ROT}^{\ell}$ in the (k, ℓ, b)-perfect bursty channel hybrid model, for odd b

The construction appears in Figure 2. Since b is odd, either in the first half or in the second half at least $\lceil b/2 \rceil$ of the strings are erased and hence that value remains hidden. On the other hand, in the other half the value can always be computed since at most $\lfloor b/2 \rfloor$ strings are deleted. The proof is identical to the case of Red-Blue Channel (proved in the full-version) and is therefore omitted.

Channel with Imprecise Burst. Finally, we consider a bursty erasure channel where the size of burst is not precisely known but comes from roughly a discrete gaussian distribution. Recall that (k, ℓ, b, σ)-noisy bursty channel corresponds to the channel $\mathcal{C}_{GEC}^{k,\ell,\mathcal{D}_{k,b,\sigma}}$, where $\mathcal{D}_{k,b,\sigma}$ is the distribution that outputs a k bit string such that all the bits are set to 1 besides the bits in locations $x+1, x+2, \ldots, x+b'$

where b' is sampled from a gaussian and rounded to the closest non-negative integer $\leq k$ with mean b and standard deviation σ and then x is chosen uniformly from $\{0, \ldots, k - b'\}$.

Theorem 5. *$\mathcal{C}^{\ell}_{ROT}$ can be $\frac{(1-\alpha)b}{k-(1+\alpha)b} + \frac{\sigma^2}{\alpha^2 b^2}$-UC-securely realized in the (k, ℓ, b, σ)-noisy bursty channel hybrid model for any constant $\alpha \in (0, 1)$.*

Proof. We use the same construction as in Figure 2 except the threshold parameter θ of the Shamir secret sharing. We set it up in a way so that it is possible to obtain m_0 if less than $(1-\alpha)b/2$ symbols are erased from the first half. Similarly secret sharing is done for the second half. By Chebyshev's inequality, the probability that the size of the burst, b', lies outside the range $\{(1-\alpha)b, \ldots, (1+\alpha)b\}$ is at most $\frac{\sigma^2}{\alpha^2 b^2}$ (if b' is too big the receiver may not learn any value, while if b' is too small it may learn both values). Assuming this does not happen, then the receiver gets only one of the sent values as long as the burst does not happen "in the middle" (i.e., $(1-\alpha)b/2$ symbols are erased from each half). The probability that the burst happens in the middle is at most $\frac{(1-\alpha)b}{k-(1+\alpha)b}$.

5.3 Self-transformations for $\mathcal{C}_{BEC}$ and $\mathcal{C}_{BSC}$

In this subsection, we show that any erasure channel can be used to construct a binary erasure channel with any desired erasure probability. On the other hand, the case of BSC is very different. The probability of correct transmission in a BSC channel can be reduced but cannot be increased. Formally,

Theorem 6. *$\forall\ \mathcal{C}^{k,\ell,\mathcal{D}}_{GEC}$ such that $\mathcal{D}$ is not a constant distribution, $\exists\ p$ such that $\mathcal{C}^{p}_{BEC}$ can be (perfectly) UC-securely realized (even against malicious adversaries) in the $\mathcal{C}^{k,\ell,\mathcal{D}}_{GEC}$-hybrid model.*

Theorem 7. *$\forall p, p' \in (0, 1)$ and $\epsilon > 1$, $\exists p'' \in [p', \epsilon p']$, such that $\mathcal{C}^{p''}_{BEC}$ can be (perfectly) UC-securely realized (even against malicious adversaries) in the $\mathcal{C}^{p}_{BEC}$-hybrid model.*

Theorem 8. *$\forall p \in (\frac{1}{2}, 1)$ and $t \in \mathbb{Z}^+$, the channel $\mathcal{C}^{p'}_{BSC}$ can be (perfectly) UC-securely realized (even against malicious adversaries) in the $\mathcal{C}^{p}_{BSC}$-hybrid model where $p' = \frac{1}{2} + 2^{t-1}\left(p - \frac{1}{2}\right)^t$.*

Theorem 9. *$\forall\ p, p' \in (\frac{1}{2}, 1), p' > p$ and protocol π, $\exists \varepsilon$ such that π does not ε-securely realize $\mathcal{C}^{p'}_{BSC}$ in the $\mathcal{C}^{p}_{BSC}$-hybrid model even against* semi-honest *adversaries.*

Proofs of the above theorems appear in the full-version.

6 OWSC scheme for Deterministic Functionalities

$\mathsf{OWSC}^f/\mathcal{C}$ is a meaningful notion only for those deterministic functions f such that given a value y identifying if there exists an input x such that $y = f(x)$ is non-trivial (cannot be done in efficiently). This, in particular, rules out all functions with polynomial sized input domains. Furthermore, this notion is useful only in the setting of malicious adversaries because it is trivial to realize this notion in the setting of semi-honest adversaries.

We start by noting that a $\mathsf{OWSC}^f/\mathcal{C}$ scheme, for any deterministic function f, can be realized by using a $\mathsf{OWSC}^{\mathsf{zk}}/\mathcal{C}$ scheme for the zero-knowledge functionality. This can be achieved simply by having the sender send the output to the receiver and along with it prove in zero-knowledge, knowledge of an input x for which $f(x)$ yields the provided output. Here we implicitly assume that besides the channel $\mathcal{C}$ the sender also has access to an error free channel which can be implemented using $\mathcal{C}$ itself (with a negligible error). Formally,

Theorem 10. *For every deterministic function f, there exists a $\mathsf{OWSC}^f/\mathcal{C}$ scheme that is a UC-secure realization (even against malicious adversaries) of the functionality $\mathcal{F}_f$ in the $\mathcal{C}$-hybrid model where $\mathcal{C} \in \{\mathcal{C}_{GEC}^{k,\ell,\mathcal{D}}, \mathcal{C}_{BSC}^{p}\}$.*

As already mentioned, proving the above theorem reduces to the task of realizing a $\mathsf{OWSC}^{\mathsf{zk}}/\mathcal{C}$ scheme. In our construction, we will make use of oblivious ZK-PCPs (see definitions in full-version).

Lemma 2. *There exists a $\mathsf{OWSC}^{\mathsf{zk}}/\mathcal{C}$ scheme that is a UC-secure realization (even against malicious adversaries) of the zero-knowledge functionality in the $\mathcal{C}$-hybrid model where $\mathcal{C} \in \{\mathcal{C}_{GEC}^{k,\ell,\mathcal{D}}, \mathcal{C}_{BSC}^{p}\}$.*

We start by giving some intuition. The key idea is to use an erasure channel or a binary symmetric channel to send over multiple instances of independently chosen ZK-PCPs and observe the statistical gap that can be created only if valid proofs were sent. However, a number of difficulties arise in realizing this intuition, particularly in our construction from BSC. Below, we provide our construction from erasure channels. The more involved construction from binary symmetric channel is deferred to full-version.

Erasure Channels. We start by considering the case of binary erasure channels with error probability $\frac{1}{2}$; i.e., when $\mathcal{C} = \mathcal{C}_{BEC}^{\frac{1}{2}}$. It follows from Theorem 6 and Theorem 7 that any $\mathcal{C}_{GEC}^{k,\ell,\mathcal{D}}$ can be used to realize $\mathcal{C}_{BEC}^{\frac{1}{2}}$.[7] We give the protocol in Figure 3.

[7] Theorem 7 only guarantees a channel $\mathcal{C}_{BEC}^{p'}$ with p' close enough to p. We will use the value $\frac{1}{2}$ for concreteness but any value close enough to $\frac{1}{2}$, say in the range $\frac{1}{2}$ to $\frac{51}{100}$, will suffice as well.

$\mathsf{OWSC}^{\mathsf{zk}}/\mathcal{C}^p_{BEC}$ protocol for language L

Common Input: $x \in \{0,1\}^\lambda$.
Auxiliary Input for prover P: w such that $(x, w) \in R_L$.
Parameters: Let $(P_{\mathsf{oZK}}, V_{\mathsf{oZK}})$ be any (c, ν)-oblivious ZK-PCP system (see full-version)(with $c \leq \frac{n}{4}$ and $\nu \geq \frac{3}{4}$) with knowledge soundness κ. Let $\ell = \frac{\lambda}{\kappa}$.

- P samples proofs $\pi_1, \ldots, \pi_\ell$ from $P_{\mathsf{oZK}}(\lambda, x, w)$ and sends $(\pi_1, \ldots, \pi_\ell)$ to V via the erasure channel $\mathcal{C}^p_{BEC}$.
- V receives $\pi'_1, \ldots, \pi'_\ell$ and for all $i \in [\ell]$ checks if $V_{\mathsf{oZK}}(\pi'_i)$. It outputs accept if all the checks pass and reject otherwise.

Fig. 3. Realizing zero-knowledge from Binary Erasure Channel

Completeness. For every $i \in [k]$, using Chernoff bound, we have that:

$$\Pr\left[\Upsilon(\pi'_i) \leq \frac{n}{4}\right] \leq e^{-\frac{n}{16}},$$

where $\Upsilon(\pi'_i)$ denotes the number of occurrences of $\perp$ in π'_i.

Hence, except with negligible probability for each $i \in [k]$, R receives at least c. Given this the completeness of the protocol follows from the completeness of the oblivious ZK-PCP.

Soundness. We will construct an extractor E', that extracts valid witnesses from any cheating prover P^* that makes the honest verifier accept with non-negligible probability. We will first describe our extractor E' and then argue that it indeed works (with overwhelming probability).

Our extractor E' proceeds as follows. Let $(\pi_1, \pi_2, \ldots, \pi_\ell)$ be the proofs generated by the cheating prover P^*. For every $i \in [\ell]$, E' obtains $y_i = E(x, \pi_i)$. If $\exists i^* \in [\ell]$ such that $y_{i^*} \in R(x)$ then output y_{i^*} (breaking ties arbitrarily). If no such i^* exists then output $\perp$.

Note that since our extractor E' failed to extract witness out of π_i for any $i \in [\ell]$ we have (by soundness of the ZK-PCP) that $\Pr[V_{\mathsf{oZK}}(x, \pi'_i) = 0] \geq \kappa$, for every $i \in [\ell]$, where the probability is taken over the random choices of obtaining π'_i from π_i. Hence, if E' outputs $\perp$ then the verifier must also always reject, except with probability at most $\leq (1-\kappa)^\ell$, which is negligible for $\ell = \frac{\lambda}{\kappa}$.

Zero-Knowledge. We need to construct a simulator $\mathcal{S}'$ for our protocol. This construction follows immediately from the ν-zero-knowledge property of the oblivious ZK-PCP.

The full proof for the case of BSC appears in full-version.

7 $\mathcal{C}^{\ell}_{ROT}$ is OWSC complete for randomized functionalities

In this section, we describe an OWSC scheme for any randomized function in the $\mathcal{C}_{ROT}$-hybrid model that uses only a *single* round of random OTs and no additional interaction. The functionalities considered here provide output to only one party. This result follows directly from [IPS08, Appendix B] and we include the construction and proof in the full-version for completeness (much of the text have been taken verbatim from [IPS08, Appendix B]). More efficient alternatives have been considered by [IKO^{+}11a] however we consider the simplest feasibility result for our setting.

One technical difference in our setting compared to [IPS08] is in the underlying primitive from which the protocols are constructed. While the protocol in [IPS08] uses a regular 1-out-of-N OT protocol, in our case we only have access to a 1-out-of-2 ROT protocol and need to convert it to a 1-out-of-N ROT protocol. (Recall that the choice about which 1-out-of-N strings the receiver obtains is made by the channel in the ROT protocol.) This however can be done easily using standard techniques and a sketch of the construction has been provided in full-version.

Theorem 11. *For every randomized function f, $\exists \ell$ and a $\mathsf{OWSC}^f/\mathcal{C}^{\ell}_{ROT}$ scheme that is a UC-secure realization (even against malicious adversaries) of the functionality $\mathcal{F}_f$ in the $\mathcal{C}^{\ell}_{ROT}$-hybrid model.*

ϵ-secure variant. We can also use the ϵ-UC realization of ROT (based on noisy bursty channel as in Theorem 5) in order to obtain a $\epsilon \cdot r$-UC realization of OWSC^f where r is the number of ROT calls made inside our construction. r for our construction is a fixed polynomial in the security parameter λ, independent of the size of the function being computed.

Construction using biased-ROT. The above theorem is stated just for the case of $\mathcal{C}^{\ell}_{ROT}$-hybrid model. However we note that the same construction continues to work in the $\mathcal{C}^{\ell,p}_{ROT}$-hybrid model, for any constant $p \in (0,1)$, with one small change. When using the $\mathcal{C}^{\ell,p}_{ROT}$ channel, the input provided by the channel for the function evaluation will be biased. This issue can be resolved by using security parameter λ number of independent bits from the channel to obtain each bit for the functionality being evaluated. More specifically, each input bit for the functionality is obtained by taking the exclusive or of λ independent input bits. By the XOR Lemma, we claim that the obtained bits will be close to uniform.

Furthermore, when using the $\mathcal{C}^{\ell,p}_{ROT}$-hybrid model, the construction itself does not depend on the precise value of the constant p. Hence, our construction is robust in the sense that it remains secure even if the adversary gets to specify the value of p (within some bounded range).

References

[Ajt10] Miklós Ajtai. Oblivious RAMs without cryptogrpahic assumptions. In Leonard J. Schulman, editor, *42nd Annual ACM Symposium on Theory* *of Computing*, pages 181–190, Cambridge, Massachusetts, USA, June 5–8, 2010. ACM Press.

[BBCM95] Charles H. Bennett, Gilles Brassard, Claude Crepeau, and Ueli M. Maurer. Generalized privacy amplification. *Information Theory, IEEE Transactions on*, 41(6):1915 –1923, Nov 1995.

[BBR88] Charles H. Bennett, Gilles Brassard, and Jean-Marc Robert. Privacy amplification by public discussion. *SIAM Journal on Computing*, 17(2):210–229, 1988.

[BCR86] Gilles Brassard, Claude Crépeau, and Jean-Marc Robert. Information theoretic reductions among disclosure problems. In *FOCS*, pages 168–173, 1986.

[BFM90] Manuel Blum, Paul Feldman, and Silvio Micali. Proving security against chosen cyphertext attacks. In Shafi Goldwasser, editor, *Advances in Cryptology – CRYPTO'88*, volume 403 of *Lecture Notes in Computer Science*, pages 256–268, Santa Barbara, CA, USA, August 21–25, 1990. Springer, Berlin, Germany.

[BGW88] Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In *Proc. 20th STOC*, pages 1–10. ACM, 1988.

[BP04] Boaz Barak and Rafael Pass. On the possibility of one-message weak zero-knowledge. In Moni Naor, editor, *TCC 2004: 1st Theory of Cryptography Conference*, volume 2951 of *Lecture Notes in Computer Science*, pages 121–132, Cambridge, MA, USA, February 19–21, 2004. Springer, Berlin, Germany.

[BTV12] Mihir Bellare, Stefano Tessaro, and Alexander Vardy. Semantic security for the wiretap channel. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology – CRYPTO 2012*, volume 7417 of *Lecture Notes in Computer Science*, pages 294–311, Santa Barbara, CA, USA, August 19–23, 2012. Springer, Berlin, Germany.

[Can01] Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. Electronic Colloquium on Computational Complexity (ECCC) TR01-016, 2001. Previous version "A unified framework for analyzing security of protocols" availabe at the ECCC archive TR01-016. Extended abstract in FOCS 2001.

[Can05] Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. Cryptology ePrint Archive, Report 2000/067, 2005. Revised version of [Can01].

[CK88] Claude Crépeau and Joe Kilian. Achieving oblivious transfer using weakened security assumptions (extended abstract). In *FOCS*, pages 42–52, 1988.

[CMW04] Claude Crépeau, Kirill Morozov, and Stefan Wolf. Efficient unconditional oblivious transfer from almost any noisy channel. In Carlo Blundo and Stelvio Cimato, editors, *SCN 04: 4th International Conference on Security in Communication Networks*, volume 3352 of *Lecture Notes in Computer Science*, pages 47–59, Amalfi, Italy, September 8–10, 2004. Springer, Berlin, Germany.

[DFMS04] Ivan Damgård, Serge Fehr, Kirill Morozov, and Louis Salvail. Unfair noisy channels and oblivious transfer. In Moni Naor, editor, *TCC 2004: 1st Theory of Cryptography Conference*, volume 2951 of *Lecture Notes in Computer Science*, pages 355–373, Cambridge, MA, USA, February 19–21, 2004. Springer, Berlin, Germany.

[DKS99] Ivan Damgård, Joe Kilian, and Louis Salvail. On the (im)possibility of basing oblivious transfer and bit commitment on weakened security assumptions. In Jacques Stern, editor, *Advances in Cryptology – EUROCRYPT'99*, volume 1592 of *Lecture Notes in Computer Science*, pages 56–73, Prague, Czech Republic, May 2–6, 1999. Springer, Berlin, Germany.

[FLS99] Uriel Feige, Dror Lapidot, and Adi Shamir. Multiple noninteractive zero knowledge proofs under general assumptions. *SIAM J. Comput.*, 29(1):1–28, 1999.

[GMW87] Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play ANY mental game. In ACM, editor, *Proc. 19th STOC*, pages 218–229. ACM, 1987. See [Gol04, Chap. 7] for more details.

[Gol04] Oded Goldreich. *Foundations of Cryptography: Basic Applications*. Cambridge University Press, 2004.

[Har60] Theodore E. Harris. A lower bound for the critical probability in a certain percolation process. *Proc. Cambridge Phil. Soc.*, 56:13–20, 1960.

[IKO$^+$11a] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, Manoj Prabhakaran, and Amit Sahai. Efficient non-interactive secure computation. In Kenneth G. Paterson, editor, *Advances in Cryptology – EUROCRYPT 2011*, volume 6632 of *Lecture Notes in Computer Science*, pages 406–425, Tallinn, Estonia, May 15–19, 2011. Springer, Berlin, Germany.

[IKO$^+$11b] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, Manoj Prabhakaran, Amit Sahai, and Jürg Wullschleger. Constant-rate oblivious transfer from noisy channels. In *CRYPTO*, pages 667–684, 2011.

[IPS08] Yuval Ishai, Manoj Prabhakaran, and Amit Sahai. Founding cryptography on oblivious transfer - efficiently. In *CRYPTO*, pages 572–591, 2008.

[ISW03] Yuval Ishai, Amit Sahai, and David Wagner. Private circuits: Securing hardware against probing attacks. In Dan Boneh, editor, *Advances in Cryptology – CRYPTO 2003*, volume 2729 of *Lecture Notes in Computer Science*, pages 463–481, Santa Barbara, CA, USA, August 17–21, 2003. Springer, Berlin, Germany.

[Kil88] Joe Kilian. Founding cryptography on oblivious transfer. In *STOC*, pages 20–31, 1988.

[Kle66] Daniel J. Kleitman. Families of non-disjoint subsets. *J. Combin. Theory*, 1:153–155, 1966.

[KM01] Valeri Korjik and Kirill Morozov. Generalized oblivious transfer protocols based on noisy channels. In *MMM-ACNS*, pages 219–229, 2001.

[Liu] Henry Liu. M400 msci project - discrete isoperimetric inequalities.

[Mau91] Ueli M. Maurer. Perfect cryptographic security from partially independent channels. In *STOC*, pages 561–571, 1991.

[Mau02] Ueli M. Maurer. Secure multi-party computation made simple. In Stelvio Cimato, Clemente Galdi, and Giuseppe Persiano, editors, *SCN*, volume 2576 of *Lecture Notes in Computer Science*, pages 14–28. Springer, 2002.

[Pas03] Rafael Pass. On deniability in the common reference string and random oracle model. In Dan Boneh, editor, *Advances in Cryptology – CRYPTO 2003*, volume 2729 of *Lecture Notes in Computer Science*, pages 316–337, Santa Barbara, CA, USA, August 17–21, 2003. Springer, Berlin, Germany.

[RTWW11] Samuel Ranellucci, Alain Tapp, Severin Winkler, and Jürg Wullschleger. On the efficiency of bit commitment reductions. In *ASIACRYPT*, pages 520–537, 2011.

[SW02] Douglas Stebila and Stefan Wolf. Efficient oblivious transfer from any non-trivial binary-symmetric channel. In *Information Theory, 2002. Proceedings. 2002 IEEE International Symposium on*, page 293, 2002.

[Wik13] Wikipedia. Binomial distribution, 2013. [Online; accessed 17-Oct-2013].

[WNI03] Andreas Winter, Anderson C. A. Nascimento, and Hideki Imai. Commitment capacity of discrete memoryless channels. In *In: Cryptography and Coding. LNCS*, pages 35–51. Springer-Verlag, 2003.

[Wul07] Jürg Wullschleger. Oblivious-transfer amplification. In Moni Naor, editor, *Advances in Cryptology – EUROCRYPT 2007*, volume 4515 of *Lecture Notes in Computer Science*, pages 555–572, Barcelona, Spain, May 20–24, 2007. Springer, Berlin, Germany.

[Wul09] Jürg Wullschleger. Oblivious transfer from weak noisy channels. In Omer Reingold, editor, *TCC 2009: 6th Theory of Cryptography Conference*, volume 5444 of *Lecture Notes in Computer Science*, pages 332–349. Springer, Berlin, Germany, March 15–17, 2009.

[Wyn75] Aaron D. Wyner. The wire-tap channel. *Bell Syst. Tech. J.*, 54(8):1334–1387, 1975.