One-One Constrained Pseudorandom Functions

Naty Peter[*] Rotem Tsabary[†] Hoeteck Wee[‡]

Abstract

We define and study a new cryptographic primitive, named *One-One Constrained Pseudorandom Functions*. In this model there are two parties, Alice and Bob, that hold a common random string K, where Alice in addition holds a predicate $f : [N] \to \{0,1\}$ and Bob in addition holds an input $x \in [N]$. We then let Alice generate a key K_f based on f and K, and let Bob evaluate a value K_x based on x and K. We consider a third party that sees the values (x, f, K_f) and the goal is to allow her to reconstruct K_x whenever $f(x) = 1$, while keeping K_x pseudorandom whenever $f(x) = 0$. This primitive can be viewed as a relaxation of constrained PRFs, such that there is only a single key query and a single evaluation query.

We focus on the information-theoretic setting, where the one-one cPRF has perfect correctness and perfect security. Our main results are as follows.

1. *A Lower Bound.* We show that in the information-theoretic setting, any one-one cPRF for punctured predicates is of exponential complexity (and thus the lower bound meets the upper bound that is given by a trivial construction). This stands in contrast with the well known GGM-based punctured PRF from OWF, which is in particular a one-one cPRF. This also implies a similar lower bound for all NC1.
2. *New Constructions.* On the positive side, we present efficient information-theoretic constructions of one-one cPRFs for a few other predicate families, such as equality predicates, inner-product predicates, and subset predicates. We also show a generic AND composition lemma that preserves complexity.
3. *An Amplification to standard cPRF.* We show that all of our one-one cPRF constructions can be amplified to a standard (single-key) cPRF via any key-homomorphic PRF that supports linear computations. More generally, we suggest a new framework that we call *the double-key model* which allows to construct constrained PRFs via key-homomorphic PRFs.
4. *Relation to CDS.* We show that one-one constrained PRFs imply conditional disclosure of secrets (CDS) protocols.

We believe that this simple model can be used to better understand constrained PRFs and related cryptographic primitives, and that further applications of one-one constrained PRFs and our double-key model will be found in the future, in addition to those we show in this paper.

[*] Ben-Gurion University of the Negev, naty@post.bgu.ac.il. Supported by ISF grant 152/17, by a grant from the Cyber Security Research Center at Ben-Gurion University of the Negev, and by the Frankel center for computer science.

[†] Weizmann Institute of Science, rotem.tsabary@weizmann.ac.il. Supported by the Israel Science Foundation (Grant No. 468/14), Binational Science Foundation (Grants No. 2016726, 2014276), by the European Union Horizon 2020 Research and Innovation Program via ERC Project REACT (Grant 756482) and via Project PROMETHEUS (Grant 780701), and by the Azrieli Fellows Program.

[‡] CNRS, ENS, PSL, wee@di.ens.fr. Supported in part by ERC Project aSCEND (H2020 639554).

1 Introduction

In this paper we define and study a new cryptographic primitive, named *One-One Constrained Pseudorandom Functions*. In this model there are two parties, Alice and Bob, that hold a common random string K. In addition, Alice holds a predicate $f : [N] \to \{0, 1\}$ and Bob holds an input $x \in [N]$. We then let Alice generate a key K_f based on f and K, and let Bob evaluate a value K_x based on x and K. We consider a third party that sees the values (x, f, K_f) and the goal is to allow her to reconstruct K_x whenever $f(x) = 1$, while keeping K_x pseudorandom whenever $f(x) = 0$.

This primitive can be viewed as a relaxation of constrained PRFs, such that there is only a single key query and a single evaluation query. In a constrained PRF (first defined in [BW13, KPTZ13, BGI14]), there is a master secret key msk with which it is possible to evaluate the PRF on all inputs x, and in addition there are constrained keys sk_f respective to predicates f, where sk_f is derived from msk, such that sk_f allows to evaluate the PRF only on inputs x where $f(x) = 1$, but on all points where $f(x) = 0$ the PRF value remains pseudorandom even given sk_f. Through this point of view, K is the master secret key of the PRF, K_x is the evaluation of the PRF on an input x and K_f is a constrained key for the predicate f.

We believe that the simplified model of one-one cPRF can be used to better understand constrained PRFs and related cryptographic primitives, and that further applications of one-one constrained PRFs will be found in the future, in addition to those we show in this paper.

Our Contributions. Our main focus is on the information-theoretic setting, where we require perfect correctness and perfect security. Our main results are as follows.

1. *A Lower Bound.* We show that in the information-theoretic setting, any one-one cPRF for punctured predicates is of exponential complexity (and thus the lower bound meets the upper bound that is given by a trivial construction). This stands in contrast with the well known GGM-based punctured PRF from OWF, which is in particular a one-one cPRF. This also implies a similar lower bound for all NC1.

2. *New Constructions.* On the positive side, we present efficient information-theoretic constructions of one-one cPRFs for a few other predicate families, such as equality predicates, inner-product predicates, and subset predicates. We also show a generic AND composition lemma that preserves complexity.

3. *An Amplification to cPRF.* We define a special *double-key* model and show that any one-one cPRF in this model, when combined with a key-homomorphic PRF, can support multiple evaluation queries. We then show that all of our constructions can be initialized in the double-key model, which implies that all of our constructions can be amplified to a standard (single-key) cPRF via any key-homomorphic PRF that supports linear computations. More generally, this approach reduces the task of constructing constrained PRFs to the possibly simpler task of constructing one-one constrained PRFs in the double-key model, and we believe that this framework will have more applications in the future.

4. *Relation to CDS.* We show that one-one constrained PRFs imply conditional disclosure of secrets (CDS) protocols, a cryptographic primitive that is used to construct secure protocols such as attribute based encryption, symmetrically-private information retrieval protocols, and secret-sharing schemes.

5. *Computational Constructions.* To complete the picture, we also go over existing computational cPRFs in the literature, which are in particular computational one-one cPRFs.

2 Technical Overview

2.1 A Lower Bound

We begin with describing our lower bound theorem and its proof. Consider the family of punctured predicates f_y over some field $\mathbb{F}$, such that for all $x, y \in \mathbb{F}$ it hold that $f_y(x) = 1$ if and only if $x \neq y$. We show that any perfect one-one cPRF for this predicate family must have keys K_{f_y} of size $\Omega(|\mathbb{F}|)$. To show that, we first argue that for every $x \in \mathbb{F}$ it must be that K_x has at least one bit of entropy, even given all of the values $\{K_{x'}\}_{x' \neq x}$. This is due to the correctness and security properties respective to the predicate f_x, which means that K_{f_x} allows to reconstruct all $\{K_{x'}\}_{x' \neq x}$ while keeping K_x random. Secondly, due to the fact that K_{f_y} allows to compute $\{K_x\}_{x \neq y}$ (by correctness), and since each such K_x has at least one independent bit of entropy (by the previous claim), it must be the case that K_{f_y} has at least $|\mathbb{F}| - 1 = \Omega(|\mathbb{F}|)$ bits of entropy.

2.2 New Constructions

A Generic Construction. We now describe a simple one-one constrained PRF for general functions over some field $\mathbb{F}$ with complexity $O(\mathbb{F})$. In this construction, we choose a random bit $k_y \overset{\$}{\leftarrow} \{0, 1\}$ for every possible input y, and let the common random string be a concatenation of all of those values $K = \{k_y\}_{y \in \mathbb{F}}$. Alice, which holds a predicate f, returns the values K_y for all the inputs y such that $f(y) = 1$, and Bob, which holds an input x, simply returns $K_x = k_x$. Security and correctness follow immediately (in fact, this construction is also secure with multiple key queries and evaluation queries). The size of the common random string is therefore at most $|\mathbb{F}|$, and for a specific function f, the size of K_f is $|f^{-1}(1)|$.

Equality Testing. Our efficient construction for equality testing over a field $\mathbb{F}$ is as follows. The common random string K consists of two random field elements k_0, k_1. The functions that Alice and Bob compute over their inputs x and f_y respectively, where $f_y(x) = 1$ if and only if $x = y$, are identical: $K_x = k_1 x + k_0$ and $K_{f_y} = k_1 y + k_0$. This is essentially a degree-1 random polynomial computed over two elements, therefore K_x and K_{f_y} look independently random as long as $x \neq y$. This construction can be generalized to any constant number of evaluation / key queries by using a random polynomial of higher degree.

Subset Predicates. Subset predicates are defined with respect to a universe $[N] = \{1, \ldots, N\}$, where the input space is all subsets $X \subseteq [N]$ and the predicates f_Y are characterized by subsets $Y \subseteq [N]$ such that $f_Y(X) = 1$ if and only if $X \subseteq Y$. Our efficient construction for subset predicates is as follows. For every $i \in [N]$ there is a random bit k_i in the common string K. We then define $K_X = \oplus_{i \in X} k_i$ and $K_{f_Y} = \{k_i\}_{i \in Y}$. It is easy to see correctness. In addition, whenever $X \nsubseteq Y$, there exists an $k_i \notin K_{f_Y}$ that completely randomizes K_X.

Inner-Product Predicates. Inner-product predicates for vectors of length ℓ over a field $\mathbb{F}$ are defined such that for every $\mathbf{x}, \mathbf{y} \in \mathbb{F}^\ell$ it holds that $f_{\mathbf{y}}(\mathbf{x}) = 1$ if and only if $\langle \mathbf{y}, \mathbf{x} \rangle = 0$. We now describe our efficient construction. The common random string K consists of a random vector $\mathbf{v}$ and a random field element w. We then define $K_{f_{\mathbf{y}}} = w\mathbf{y} + \mathbf{v}$ and $K_{\mathbf{x}} = \langle \mathbf{v}, \mathbf{x} \rangle$. Correctness holds since whenever $\langle \mathbf{y}, \mathbf{x} \rangle = 0$ it holds that $\langle K_{f_{\mathbf{y}}}, \mathbf{x} \rangle = K_{\mathbf{x}}$. Security holds since $\mathbf{v}$ has one degree of freedom given $K_{f_{\mathbf{y}}}, \mathbf{y}$ and therefore it completely randomizes $K_{\mathbf{x}}$.

2.3 Amplification via Key-Homomorphic PRF

We consider one-one cPRFs that satisfy an additional property and show that such one-one cPRFs can be boosted to standard (single-key) cPRFs via key-homomorphic PRFs. We then show that all of our information-theoretic one-one cPRFs satisfy this property, thus receiving new cPRF constructions.

In more detail, we require an alternative algorithm for Alice, that on input K, f produces a *double-key* $(K_f, \hat{K}_f)$. Such double-key should have the property that $\hat{K}_f$ looks uniformly random even given K_f, but on the other hand, given both of the key parts $(K_f, \hat{K}_f)$ it should be possible to reconstruct K_x for all x (regardless of $f(x)$).

Recall that in a key-homomorphic PRF, given an evaluation $\mathsf{PRF}_k(x)$ of the PRF over some input x and a key k, it is possible to publicly evaluate a function g over the key which results in the value $\mathsf{PRF}_{g(k)}(x)$. Our construction uses a key-homomorphic PRF to homomorphically evaluate the function that takes a double-key $(K_f, \hat{K}_f)$ and outputs K_x. Security relies on the fact that $\hat{K}_f$ looks uniform even given K_f, which implies that multiple evaluations of the form $\mathsf{PRF}_{\hat{K}_f}(x)$ look uniform by the security of the PRF. In the construction we define the cPRF evaluation as $r_x := \mathsf{PRF}_{K_x}(x)$. In the security proof we use the homomorphic evaluation procedure to convert $\mathsf{PRF}_{\hat{K}_f}(x)$ into $r_x = \mathsf{PRF}_{K_x}(x)$.

Lastly, we show that all of our information-theoretic constructions can be instantiated in the double-key model, where the required homomorphic computation is linear. In more detail, in the equality testing construction we let $K_y = k_0 + yk_1$ and $\hat{K}_y = yk_1$, in the subset predicates construction we define $K_Y = \{k_i\}_{i \in Y}$ and $\hat{K}_Y = \{k_i\}_{i \in [N]/Y}$ and in the inner-product construction we define $K_{\mathbf{y}} = w\mathbf{y} + \mathbf{v}$ and $\hat{K}_{\mathbf{y}} = w$.

2.4 One-One Constrained PRFs and CDS Protocols

We study the connection between one-one constrained PRFs and CDS protocols. CDS protocols is a cryptographic primitive, introduced by Gertner et al. [GIKM00]. In a CDS protocol, each of two parties, Alice and Bob, holds a private input and sends one message to a referee, which knows the inputs of the parties, and should learn a secret held by the parties if and only if the inputs of the parties satisfy some condition (e.g., if the inputs are equal).

CDS protocols can be easily generalized into multi-party CDS protocols, and they are used to construct attribute based encryption [GKW15, Wee14, Att14], symmetrically-private information retrieval protocols [GIKM00], priced oblivious transfer [AIR01], and secret-sharing schemes [LV18, BP18, ABF+19, BP19, ABNP20].

We present a transformation from one-one constrained PRFs to CDS protocols. In particular, we show that a one-one constrained PRF implies a CDS protocol for the index predicate. By the reduction of [GKW15] from CDS protocols for general predicates to CDS protocols for the index predicate, we obtain a transformation from one-one constrained PRFs to CDS protocols for general predicates. This transformation preserve complexity, i.e., the message size of the resulting CDS protocol is the complexity of the one-one constrained PRF.

Private Simultaneous Messages Protocols. Another similar primitive is private simultaneous messages (PSM) protocols, presented by Feige et al. [FKN94], which is a private case of MPC protocols. In a PSM protocol, each of the parties, Alice and Bob, holds a private input for a two-input function, and each of them sends only one message to a referee, which is based on its input and a common random string, such that the referee should be able to compute the function on the inputs of Alice and Bob using the messages it gets, without learn any additional information about the inputs of the parties. As CDS protocols, PSM protocols can be generalized into multi-party PSM protocols, and they imply some other cryptographic protocols, such as constant round MPC protocols [IK97], generalized oblivious transfer protocols [IK97], and zero-information Arthur-Merlin protocols [AR16].

The best known PSM protocol for general functions $f : [N] \times [N] \to \{0,1\}$ has message size $O(\sqrt{N})$ [BIKK14], so by our lower bound of $\Omega(N)$ on the complexity of one-one constrained PRFs, we cannot get a transformation that preserve complexity from PSM protocols to one-one constrained PRFs. There is a transformation that preserve message size from PSM protocols to CDS protocols [GIKM00, BIKK14]; the other direction (an existence of transformation from CDS protocols to PSM protocols) is an open problem, and although there is no evidence that shows an equivalence or separation between CDS and PSM protocols, the best known CDS protocols [LVW17] have better message size than the best known PSM protocols [BIKK14]. Studying the connections between one-one constrained PRFs and CDS protocols or PSM protocols may help understanding the connection between CDS protocols and PSM protocols and the bounds on the message size of CDS and PSM protocols.

3 Preliminaries

Notations. For any $n \in \mathbb{N}$ we use $[n]$ to denote the set $\{1, \ldots, n\}$. For any set S we use $s \overset{\$}{\leftarrow} S$ to denote a uniformly random sample s from S. For any distribution X we use $x \leftarrow X$ to denote a value x that is sampled according to the distribution X. For any $n \in \mathbb{N}$ we use $\mathcal{U}_n$ to denote the uniform distribution over the strings of length n, and for any set S we use $\mathcal{U}_S$ to denote the uniform distribution over the elements in S.

3.1 Entropy and Indistinguishability

Definition 3.1 (Shannon Entropy)**.** *For a random variable X and $x \in \sup(X)$, the sample entropy of x with respect to X is $H_X(x) = \log(1/Pr[X = x])$. The Shannon entropy of X is then defined as*

$$H(X) = E_{x \leftarrow X}[H_X(x)] \ .$$

For random variables X, Y, the Shannon entropy of X conditioned on Y is

$$H(X|Y) = H(X,Y) - H(Y) \ .$$

Definition 3.2 (Statistical Distance)**.** *The statistical distance between two random variables* X_1, X_2 *over a finite domain* $\mathcal{X}$ *is*

$$\Delta(X_1, X_2) = \frac{1}{2} \sum_{x \in \mathcal{X}} |Pr[X_1 = x] - Pr[X_2 = x]| \ .$$

We say that X_1, X_2 *are* δ*-close if* $\Delta(X_1, X_2) \leq \delta$*.*

X_1, X_2 *are* 0*-close if and only if* $Pr[X_1 = x] = Pr[X_2 = x]$ *for all* $x \in \mathcal{X}$*, and in that case we say that they are identically distributed.*

A function $\varepsilon(\cdot)$ is *negligible* if for every positive polynomial $p(\cdot)$ and all sufficiently large n's, it holds that $\varepsilon(n) < 1/p(n)$. We define three notions of indistinguishability as follows.

Definition 3.3 (Indistinguishability)**.** *Let* $X = \{X_n\}_{n \in \mathbb{N}}, Y = \{Y_n\}_{n \in \mathbb{N}}$ *be two distribution ensembles.*

1. X *and* Y *are* perfectly *indistinguishable if for every* $n \in \mathbb{N}$*, the random variables* X_n *and* Y_n *are identically distributed.*

2. X *and* Y *are* statistically *indistinguishable if there exists a negligible function* $\varepsilon(\cdot)$ *such that for every* $n \in \mathbb{N}$*,* X_n *and* Y_n *are* $\varepsilon(n)$*-close.*

3. X *and* Y *are* computationally *indistinguishable if for every non-uniform* PPT *distinguisher* D*, there exists a negligible function* $\varepsilon(\cdot)$ *such that for every* $n \in \mathbb{N}$*,*

$$|[Pr[D(X_n) = 1] - [Pr[D(Y_n) = 1]| < \varepsilon(n) \ .$$

3.2 Notions of Pseudorandom Functions

Definition 3.4 (Constrained PRFs)**.** *A* constrained *pseudorandom function (cPRF) for a predicate family* $\mathcal{F}$ *and an input space* $\mathcal{X}$ *is defined by the algorithms* $(\mathsf{KeyGen}, \mathsf{Eval}, \mathsf{Constrain}, \mathsf{ConstrainEval})$ *where:*

- $\mathsf{KeyGen}(1^\lambda)$ *is a* PPT *algorithm that takes as input a security parameter* λ *and outputs a master key* msk*.*

- $\mathsf{Eval}(\mathsf{msk}, x)$ *is a deterministic algorithm that takes as input the master secret key* msk *and an input* $x \in \mathcal{X}$*, and outputs a string* $r_x \in \{0,1\}^*$*.*

- $\mathsf{Constrain}(\mathsf{msk}, f)$ *is a* PPT *algorithm that takes as input the master secret key* msk *and a predicate* $f \in \mathcal{F}$*, and outputs a constrained key* sk_f*.*

- $\mathsf{ConstrainEval}(\mathsf{sk}_f, x)$ *is a deterministic algorithm that takes as input a constrained key* sk_f *and an input* $x \in \mathcal{X}$*, and outputs a string* $r'_x \in \{0,1\}^*$*.*

Correctness of Constrained Keys. *The scheme is* correct *if for all* $x \in \mathcal{X}$ *and* $f \in \mathcal{F}$ *for which* $f(x) = 1$*, and for all* $\mathsf{msk} \leftarrow \mathsf{KeyGen}(1^\lambda)$*,* $\mathsf{sk}_f \leftarrow \mathsf{Constrain}(\mathsf{msk}, f)$*, it holds that*

$$\mathsf{Eval}(\mathsf{msk}, x) = \mathsf{ConstrainEval}(\mathsf{sk}_f, x) \ .$$

(Single-Key) Pseudorandomness. *The security requirement is captured via a game between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$ as follows.*

- *$\mathcal{C}$ computes* $\mathsf{msk} \leftarrow \mathsf{KeyGen}(1^\lambda)$.
- *In an order of her choice, $\mathcal{A}$ makes an arbitrary number of* evaluation queries*, a single* challenge query *and a single* key query*:*
  - Evaluation Query: *$\mathcal{A}$ selects $x \in \mathcal{X}$ and sends it to $\mathcal{C}$. In return, $\mathcal{C}$ computes $r_x \leftarrow$ $\mathsf{Eval}(\mathsf{msk}, x)$ and sends it to $\mathcal{A}$.*
  - Challenge Query: *$\mathcal{A}$ selects $x^* \in \mathcal{X}$ and sends it to $\mathcal{C}$. In return, $\mathcal{C}$ computes $r_{x^*} \leftarrow$ $\mathsf{Eval}(\mathsf{msk}, x^*)$ and samples a bit $b \xleftarrow{\$} \{0,1\}$. If $b = 0$, it sends r_{x^*} to $\mathcal{A}$, otherwise it sends to $\mathcal{A}$ a random value $u \leftarrow \mathcal{U}_{|r_{x^*}|}$.*
  - Key Query: *$\mathcal{A}$ selects $f^* \in \mathcal{F}$ and sends it to $\mathcal{C}$. In return, $\mathcal{C}$ computes $\mathsf{sk}_{f^*} \leftarrow$ $\mathsf{Constrain}(\mathsf{msk}, f^*)$ and sends sk_{f^*} to $\mathcal{A}$.*
- *$\mathcal{C}$ sends to $\mathcal{A}$ a bit b'.*

The advantage *of $\mathcal{A}$ in the game is $Pr[b = b'] - \frac{1}{2}$ where the probability is over the coins of $\mathcal{C}$ and $\mathcal{A}$. The adversary $\mathcal{A}$ is* admissible *if $f^*(x^*) = 0$ and x^* does not appear in any of the evaluation queries. The scheme is computationally secure if for any* PPT *admissible adversary $\mathcal{A}$, her advantage in the game is* $\mathrm{negl}(\lambda)$.

We define key-selective *pseudorandomness identically to the definition above, except that $\mathcal{A}$ is forced to make the key query first.*

Definition 3.5 (Key-Homomorphic PRFs)**.** *A* key-homomorphic *pseudorandom function (khPRF) for an input space $\mathcal{X}$, a key space $\mathcal{K}$, and a function family $\mathcal{G} = \{\mathcal{G}_n : \mathcal{K}^n \to \mathcal{K}\}_{n \in \mathbb{N}}$, is defined by the algorithms* $(\mathsf{KeyGen}, \mathsf{Eval}, \mathsf{HomKeyEval})$ *where:*

- $\mathsf{KeyGen}(1^\lambda)$ *is a* PPT *algorithm that takes as input a security parameter λ and outputs a key* $\mathsf{sk} \in \mathcal{K}$ *and possibly public parameters* pp.
- $\mathsf{Eval}(\mathsf{sk}, x)$ *is a deterministic algorithm that takes as input a key* $\mathsf{sk} \in \mathcal{K}$ *and an input $x \in \mathcal{X}$, and outputs $r_x \in \{0,1\}^*$.*
- $\mathsf{HomKeyEval}(g, r_x)$ *is a* PPT *algorithm that takes as input a function $g \in \mathcal{G}$ and a value $r_x \in \{0,1\}^*$, and outputs a value $\hat{r}_x \in \{0,1\}^*$.*

Correctness of Homomorphic Key Evaluation. *The scheme is* correct *if for all $x \in \mathcal{X}$, all $g \in \mathcal{G}$ where $g : \mathcal{K}^n \to \mathcal{K}$, and all $\{\mathsf{sk}_i\}_{i \in [n]} \in \mathcal{K}$, it holds that*

$$\mathsf{HomKeyEval}\left(g, \mathsf{Eval}(\mathsf{sk}_1, x), \ldots, \mathsf{Eval}(\mathsf{sk}_n, x)\right) = \mathsf{Eval}\left(g(\mathsf{sk}_1, \ldots, \mathsf{sk}_n), x\right) \ .$$

Pseudorandomness. *The security requirement is captured via a game between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$ as follows.*

- *$\mathcal{C}$ computes* $\mathsf{sk} \leftarrow \mathsf{KeyGen}(1^\lambda)$.
- *In an order of her choice, $\mathcal{A}$ makes an arbitrary number of* evaluation queries *and a single* challenge query*:*

- Evaluation Query: *$\mathcal{A}$ selects $x \in \mathcal{X}$ and sends it to $\mathcal{C}$. In return, $\mathcal{C}$ computes $r_x \leftarrow$ $\mathsf{Eval}(\mathsf{sk}, x)$ and sends it to $\mathcal{A}$.*
- Challenge Query: *$\mathcal{A}$ selects $x^* \in \mathcal{X}$ and sends it to $\mathcal{C}$. In return, $\mathcal{C}$ computes $r_{x^*} \leftarrow$ $\mathsf{Eval}(\mathsf{sk}, x^*)$ and samples a bit $b \xleftarrow{\$} \{0,1\}$. If $b = 0$, it sends r_{x^*} to $\mathcal{A}$, otherwise it sends to $\mathcal{A}$ a random value $u \leftarrow \mathcal{U}_{|r_{x^*}|}$.*

- *$\mathcal{C}$ sends to $\mathcal{A}$ a bit b'.*

The advantage *of $\mathcal{A}$ in the game is $Pr[b = b'] - \frac{1}{2}$ where the probability is over the coins of $\mathcal{C}$ and $\mathcal{A}$. The adversary $\mathcal{A}$ is* admissible *if x^* does not appear in any of the evaluation queries. The scheme is computationally secure if for any* PPT *admissible adversary $\mathcal{A}$, her advantage in the game is* $\mathrm{negl}(\lambda)$.

4 Definition of One-One Constrained PRFs

Definition 4.1 (One-One Constrained PRFs)**.** *A* One-One Constrained Pseudorandom Function *for a predicate family $\mathcal{F}$ and an input space $\mathcal{X}$ is a tuple of algorithms* $(\mathsf{Setup}, \mathsf{A}, \mathsf{B}, \mathsf{Recon})$ *with the following syntax.*

- *$\mathsf{Setup}(1^\lambda) \to K$ is a PPT algorithm that (possibly) takes a security parameter λ and outputs a common random string K.*

- *$\mathsf{A}(K, f) \to K_f$ is a PPT algorithm that takes a common random string K and a predicate $f \in \mathcal{F}$. It outputs a key K_f.*

- *$\mathsf{B}(K, x) \to K_x$ is a deterministic algorithm that takes a common random string K and an input $x \in \mathcal{X}$. It outputs a value K_x.*

- *$\mathsf{Recon}(x, f, K_f) \to K'_x$ is a deterministic algorithm that takes an input $x \in \mathcal{X}$, a predicate $f \in \mathcal{F}$, and a key K_f. It outputs a value K'_x.*

Complexity. *We say that the scheme is of complexity $p(\cdot, \cdot, \cdot)$ if for every $(\lambda, \mathcal{X}, \mathcal{F})$, for every $x \in \mathcal{X}$ and $f \in \mathcal{F}$, for every K, K_f, K_x where $K \leftarrow setup(1^\lambda)$, $K_f \leftarrow \mathsf{A}(K, f)$, and $K_x \leftarrow \mathsf{B}(K, x)$, the size of (K, K_f, K_x) is $O(p(\lambda, |\mathcal{X}|, |\mathcal{F}|))$.*

Correctness. *A one-one constrained PRF is* correct *if for all $f \in \mathcal{F}$ and $x \in \mathcal{X}$ for which $f(x) = 1$, for all $K \leftarrow \mathsf{Setup}(1^\lambda)$, and for all coins of A, it holds that*

$$\mathsf{Recon}(x, f, \mathsf{A}(K, f)) = \mathsf{B}(K, x) \ .$$

Security. *The security requirement is captured via a game between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$ as follows.*

- *$\mathcal{C}$ computes $K \leftarrow \mathsf{Setup}(1^\lambda)$.*

- *In an order of her choice, $\mathcal{A}$ makes two queries:*

- Challenge Query: $\mathcal{A}$ *selects* $x^* \in \mathcal{X}$ *and sends it to* $\mathcal{C}$*. In return,* $\mathcal{C}$ *computes* $K_{x^*} \leftarrow \mathsf{B}(K, x^*)$ *and samples a bit* $b \overset{\$}{\leftarrow} \{0,1\}$*. If* $b = 0$*, it sends* K_{x^*} *to* $\mathcal{A}$*, otherwise it sends to* $\mathcal{A}$ *a random value* $u \leftarrow \mathcal{U}_{|K_{x^*}|}$*.*
- Key Query: $\mathcal{A}$ *selects* $f^* \in \mathcal{F}$ *and sends it to* $\mathcal{C}$*. In return,* $\mathcal{C}$ *computes* $K_{f^*} \leftarrow \mathsf{A}(K, f^*)$ *and sends* K_{f^*} *to* $\mathcal{A}$*.*

- $\mathcal{A}$ *sends to* $\mathcal{C}$ *a bit* b'*.*

The advantage *of* $\mathcal{A}$ *in the game is* $Pr[b = b'] - \frac{1}{2}$ *where the probability is over the coins of* $\mathcal{C}$ *and* $\mathcal{A}$*. The scheme is* perfectly (/statistically /computationally) secure *if for any unbounded (/unbounded /*PPT*) adversary* $\mathcal{A}$ *that selects* x^*, f^* *for which* $f^*(x^*) = 0$*, her advantage in the game is 0 (/*$\mathrm{negl}(\lambda)$ */*$\mathrm{negl}(\lambda)$*).*

We define key-selective *(resp.* input-selective*) security identically to the definition above, except that* $\mathcal{A}$ *is forced to make the key query (resp. challenge query) first.*

Indistinguishability Based Perfect Security. *In the* prefect *setting, we can omit the security parameter and selective security implies full security, therefore the following definition is equivalent to the one above:*

A one-one constrained PRF is perfectly secure *if for all* $f^* \in \mathcal{F}$ *and* $x^* \in \mathcal{X}$ *for which* $f^*(x^*) = 0$*, the following distributions are identical:*

$$(f^*, x^*, K_{f^*}, K_{x^*}) \equiv (f^*, x^*, K_{f^*}, u)$$

where $K \leftarrow \mathsf{Setup}(),\ K_{f^*} \leftarrow \mathsf{A}(K, f^*),\ K_{x^*} \leftarrow \mathsf{B}(K, x^*),\ u \leftarrow \mathcal{U}_{|K_{x^*}|}$*.*

Note. This is essentially a constrained PRF secure against one constrained key and one evaluation query. Related primitives: constrained PRFs, conditional disclosure of secrets (CDS), function secret-sharing.

5 A Lower Bound

We now show that for inequality predicates, the upper bound that we show in Theorem 6.1 is tight, i.e., it is not possible to do better than the trivial construction. This means we cannot hope to achieve efficient information-theoretic constructions for NC1.

Theorem 5.1. *Let* $\mathcal{F} = \{f_{\neq y}\}_{y \in \mathbb{F}}$ *be the family of punctured predicates over some field* $\mathbb{F}$*, i.e., for any fixed* $y \in \mathbb{F}$*,* $f_{\neq y} : \mathbb{F} \to \{0,1\}$ *where* $f_{\neq y}(x) = 1$ *if and only if* $x \neq y$*. Then, for any field* $\mathbb{F}$*, any one-one constrained PRF for* $\mathcal{F}$ *with perfect correctness and perfect security is of complexity* $\Omega(|\mathbb{F}|)$*.*

We now prove Theorem 5.1. Denote $N = |\mathbb{F}|$ and consider all of the field elements $x_1, \ldots, x_N$ according to some fixed order. Consider the random variable $K \leftarrow \mathsf{Setup}()$ and for all $i \in [N]$ consider the random variables K_i and $K_{\neq i}$ defined as:

$$K_i \leftarrow \mathsf{B}(K, x_i), \qquad K_{\neq i} \leftarrow \mathsf{A}(K, f_{\neq x_i}) \ .$$

Claim 5.1.1. *For all* $i \in [N]$*, it holds that* $H(K_i \mid K_1, \ldots, K_{i-1}) \geq 1$*.*

Proof. Fix an $i \in [N]$. By the perfect security it holds that $(K_{\neq i}, K_i) \equiv (K_{\neq i}, u)$ where $u \leftarrow \mathcal{U}_{|K_x|}$. Since $H(u \mid K_{\neq i}) \geq 1$, it follows that

$$H(K_i \mid K_{\neq i}) \geq 1 \ . \tag{1}$$

By the perfect correctness, $K_{\neq i}$ uniquely determines all of the values $\{K_j\}_{j \neq i}$. That is,

$$H(\{K_j\}_{j \neq i} \mid K_{\neq i}) = 0 \ ,$$

i.e., (by Theorem 3.1)

$$H(\{K_j\}_{j \neq i}, K_{\neq i}) = H(K_{\neq i}) \ ,$$

and therefore

$$H(K_{\neq i}) \geq H(\{K_j\}_{j \neq i}) \ .$$

Since $\{K_1, \ldots, K_{i-1}\} \subseteq \{K_j\}_{j \neq i}$, it follows that

$$H(K_{\neq i}) \geq H(K_1, \ldots, K_{i-1}) \ . \tag{2}$$

Lastly, equations (1) and (2) imply that

$$H(K_i \mid K_1, \ldots, K_{i-1}) \geq H(K_i \mid K_{\neq i}) \geq 1 \ .$$

□

Claim 5.1.2. *For any subset $I \subseteq [N]$, it holds that $H(\{K_i\}_{i \in I}) \geq |I|$.*

Proof. Fix a subset $I \subseteq [N]$ and denote $I = \{i_1, \ldots, i_{|I|}\}$ such that $i_1 < i_2 < \cdots < i_{|I|}$. By Claim 5.1.1, for all $j = 1, \ldots, |I|$ it holds that

$$H(K_{i_j} \mid K_{i_1}, \ldots, K_{i_{j-1}}) \geq H(K_{i_j} \mid K_1, \ldots, K_{i_j - 1}) \geq 1 \ ,$$

i.e., (by Theorem 3.1)

$$H(K_{i_j}, K_{i_1}, \ldots, K_{i_{j-1}}) - H(K_{i_1}, \ldots, K_{i_{j-1}}) \geq 1 \ ,$$

i.e.,

$$H(K_{i_j}, K_{i_1}, \ldots, K_{i_{j-1}}) \geq 1 + H(K_{i_1}, \ldots, K_{i_{j-1}}) \ .$$

Since this is true for all $j = 1, \ldots, |I|$, it follows that

$$\begin{aligned} H(\{K_i\}_{i \in I}) &= H(K_{i_{|I|}}, K_{i_1}, \ldots, K_{i_{|I|-1}}) \\ &\geq 1 + H(K_{i_1}, \ldots, K_{i_{|I|-1}}) \\ &\geq 1 + 1 + H(K_{i_1}, \ldots, K_{i_{|I|-2}}) \\ &\cdots \\ &\geq |I| \ . \end{aligned}$$

□

Consider now an arbitrary $i \in [N]$. From Claim 5.1.2 it holds that $H(\{K_j\}_{j \neq i}) \geq N - 1$. Since $H(K_{\neq i}) \geq H(\{K_j\}_{j \neq i})$ (see the proof of Claim 5.1.1), it follows that $H(K_{\neq i}) \geq N - 1$. Hence, for any $i \in [N]$ the size of $K_{\neq i}$ is at least $N - 1$, which completes the proof. □

6 Information-Theoretic Constructions

In this section we consider one-one constrained PRFs with perfect correctness and security. We begin in Section 6.1 with a generic construction for all predicates over a field $\mathbb{F}$, which is of complexity $O(|\mathbb{F}|)$. We then present more efficient constructions for specific predicate families; We begin in Section 6.2 with a complexity-preserving composition lemma for the AND operator. That is, we show that given a one-one cPRF for predicates families $\mathcal{F}^1$ and $\mathcal{F}^2$, there is a one-one cPRF for the predicate family $\mathcal{F}^1 \wedge \mathcal{F}^2$ of proportional complexity. In Section 6.3 we show a construction for the equality predicate over a field $\mathbb{F}$ with complexity $O(\log|\mathbb{F}|)$, which extends to a ℓ-vector-equality construction of complexity $O(\ell \cdot \log|\mathbb{F}|)$ via the generic AND composition. In Section 6.4 we show a construction for the subset relation with complexity $O(N)$, where N is the maximal size of sets, which extends to t-CNFs with complexity $O(\binom{\ell}{t} \cdot |\mathbb{F}|^t \cdot \log|\mathbb{F}|)$ as pointed out by [DKNY18, Tsa19]. In Section 6.5 we construct a one-one cPRF for inner-product predicates for vectors in $\mathbb{F}^\ell$ with complexity $O(\ell \cdot \log|\mathbb{F}|)$, which can be extended to polynomials via embedding of polynomial zero testing as inner-product.

6.1 Generic Predicates

Theorem 6.1. *Let $\mathcal{F}$ be the family of all predicates over some field $\mathbb{F}$, i.e., any $f \in \mathcal{F}$ is of the form $f : \mathbb{F} \to \{0,1\}$. Then, there is a one-one constrained PRF for $\mathcal{F}$ with perfect correctness, perfect security, and complexity $O(|\mathbb{F}|)$.*

Proof. The construction is as follows.

- $\mathsf{Setup}()$: For any $y \in \mathbb{F}$ sample $k_y \xleftarrow{\$} \{0,1\}$. Output $K = \{k_y\}_{y\in\mathbb{F}}$.
- $\mathsf{A}(K, f)$: Parse $K = \{k_y\}_{y\in\mathbb{F}}$ and output $K_f = \{k_y : f(y) = 1\}_{y\in\mathbb{F}}$.
- $\mathsf{B}(K, x)$: Parse $K = \{k_y\}_{y\in\mathbb{F}}$ and output $K_x = k_x$.
- $\mathsf{Recon}(x, f, K_f)$: Parse $K_f = \{k_y : f(y) = 1\}_{y\in\mathbb{F}}$. If $f(x) = 1$ then output k_x, otherwise output $\perp$.

Correctness. If $f(x) = 1$ then $k_x \in K_f$.

Security. Consider $K \leftarrow \mathsf{Setup}()$, $K_f \leftarrow \mathsf{A}(K, f)$, $K_x \leftarrow \mathsf{B}(K, x)$, $u \xleftarrow{\$} \{0,1\}$. If $f(x) = 0$ then $k_x \notin K_f$. Since k_x is a uniformly sampled bit and $H(k_x|K_f) = H(k_x)$, it holds that

$$(f, x, K_f, K_x) \equiv (f, x, K_f, u) .$$

□

6.2 AND Composition

Lemma 6.2. *Let $(\mathsf{Setup}^1, \mathsf{A}^1, \mathsf{B}^1, \mathsf{Recon}^1)$ and $(\mathsf{Setup}^2, \mathsf{A}^2, \mathsf{B}^2, \mathsf{Recon}^2)$ be perfect one-one constrained PRFs for some predicate families $\mathcal{F}^1 = \{f^1 : \mathbb{F} \to \{0,1\}\}$ and $\mathcal{F}^2 = \{f^2 : \mathbb{F} \to \{0,1\}\}$ respectively for some field $\mathbb{F}$, with complexity bounded by some functions P^1 and P^2 respectively. Then, there is a perfect one-one constrained PRF for the predicate family $\mathcal{F}^1 \wedge \mathcal{F}^2 = \{f^1 \wedge f^2 : \mathbb{F} \to \{0,1\}\}_{f^1\in\mathcal{F}^1, f^2\in\mathcal{F}^2}$ with complexity bounded by $P^1 + P^2$.*

Proof. For simplicity we assume that for all x it holds that $\left|K_x^1\right| = \left|K_x^2\right|$. This can always be enforced because it is possible to ignore some of the bits of K_x without compromising correctness and security. The construction is as follows.

- $\mathsf{Setup}()$: Compute $K^1 \leftarrow \mathsf{Setup}^1()$ and $K^2 \leftarrow \mathsf{Setup}^2()$, output $K = (K^1, K^2)$.
- $\mathsf{A}(K, f)$: Parse $K = (K^1, K^2)$ and $f = f^1 \wedge f^2$. Compute $K^1_{f^1} \leftarrow \mathsf{A}^1(K^1, f^1)$ and $K^2_{f^2} \leftarrow \mathsf{A}^2(K^2, f^2)$. Output $K_f = (K^1_{f^1}, K^2_{f^2})$.
- $\mathsf{B}(K, x)$: Parse $K = (K^1, K^2)$. Compute $K^1_x \leftarrow \mathsf{B}^1(K^1, x)$ and $K^2_x \leftarrow \mathsf{B}^2(K^2, x)$. Output $K_x = K^1_x + K^2_x$.
- $\mathsf{Recon}(x, f, K_f)$: Parse $K_f = (K^1_{f^1}, K^2_{f^2})$. Compute $R^1_x \leftarrow \mathsf{Recon}^1(x, f^1, K^1_{f^1})$ and $R^2_x \leftarrow \mathsf{Recon}^2(x, f^2, K^2_{f^2})$, output $R_x = R^1_x + R^2_x$.

Correctness. If $f(x) = 1$ then $f^1(x) = 1 \wedge f^2(x) = 1$, therefore by the correctness of the underlying constructions $R^1_x = K^1_x$ and $R^2_x = K^2_x$, thus $R_x = K_x$.

Security. Consider $K \leftarrow \mathsf{Setup}()$, $K_f \leftarrow \mathsf{A}(K, f)$, $K_x \leftarrow \mathsf{B}(K, x)$, $u \leftarrow \mathcal{U}_{|K_x|}$ where $K = (K^1, K^2)$, $f = f^1 \wedge f^2$, $K_f = (K^1_{f^1}, K^2_{f^2})$ and $K_x = K^1_x + K^2_x$. If $f(x) = 0$ then there exists $i \in \{1, 2\}$ for which $f^i(x) = 0$. By the security of the underlying constructions it holds that

$$(f^i, x, K^i_{f^i}, K^i_x) \equiv (f^i, x, K^i_{f^i}, u^i) \ .$$

where $K^i \leftarrow \mathsf{Setup}^i()$, $K^i_{f^i} \leftarrow \mathsf{A}^i(K^i, f^i)$, $K^i_x \leftarrow \mathsf{B}^i(K^i, x)$, $u^i \leftarrow \mathcal{U}_{|K^i_x|}$. Since the two instances of the underlying constructions are independent (i.e., $H(K^1|K^2) = H(K^1)$ and $H(K^2|K^1) = H(K^2)$), and in particular K^i_x is independent of $(K^{3-i}_{f^{3-i}}, K^{3-i}_x)$, it follows that

$$\begin{aligned}
(f, x, K_f, K_x) &= (f, x, (K^1_{f^1}, K^2_{f^2}), K^1_x + K^2_x) \\
&\equiv (f, x, (K^1_{f^1}, K^2_{f^2}), K^{3-i}_x + u^i) \\
&\equiv (f, x, (K^1_{f^1}, K^2_{f^2}), u) \\
&= (f, x, K_f, u) \ .
\end{aligned}$$

□

6.3 Equality Testing

Theorem 6.3. *Let $\mathcal{F} = \{f_y\}_{y \in \mathbb{F}}$ be the family of point predicates over some field $\mathbb{F}$, i.e., for any fixed $y \in \mathbb{F}$, $f_y : \mathbb{F} \to \{0, 1\}$ where $f_y(x) = 1$ if and only if $x = y$. Then, there is a one-one constrained PRF for $\mathcal{F}$ with perfect correctness, perfect security, and complexity $O(\log |\mathbb{F}|)$.*

Proof. The construction is as follows.

- $\mathsf{Setup}()$: Sample $k_0, k_1 \xleftarrow{\$} \mathbb{F}$ and output $K = (k_0, k_1)$.
- $\mathsf{A}(K, f_y)$: Parse $K = (k_0, k_1)$ and output $K_{f_y} = k_0 + yk_1$.
- $\mathsf{B}(K, x)$: Parse $K = (k_0, k_1)$ and output $K_x = k_0 + xk_1$.
- $\mathsf{Recon}(x, f_y, K_{f_y})$: If $x = y$ then output K_{f_y}, otherwise output $\perp$.

Correctness. If $f_y(x) = 1$, i.e., $x = y$, then $K_{f_y} = K_x$.

Security. Consider $K \leftarrow \mathsf{Setup}(),\ K_{f_y} \leftarrow \mathsf{A}(K, f_y),\ K_x \leftarrow \mathsf{B}(K, x),\ u \overset{\$}{\leftarrow} \mathbb{F}$. If $f_y(x) = 0$, i.e., $x \neq y$, then $(K_{f_y}, K_x) = (k_0 + yk_1,\ k_0 + xk_1)$ are two distinct points on a random linear function defined by (k_0, k_1). Since for every possible value of the uniformly sampled $u \in \mathbb{F}$ there is a unique $(k'_0, k'_1) \in \mathbb{F}^2$ such that $k'_0 + yk'_1 = k_0 + yk_1 = K_{f_y}$ and $k'_0 + xk'_1 = u$, it holds that (f_y, x, K_{f_y}, K_x) and (f_y, x, K_{f_y}, u) are identically distributed. □

Extensions. The construction above can be extended to other notions as follows.

- The predicates family of equality testing of *vectors* over some field $\mathbb{F}$, i.e., the family $\mathcal{F} = \{f_{\mathbf{y}}\}_{\mathbf{y} \in \mathbb{F}^\ell}$ where for any fixed $\mathbf{y} \in \mathbb{F}^\ell$, $f_{\mathbf{y}} : \mathbb{F}^\ell \to \{0,1\}$ such that $f_{\mathbf{y}}(\mathbf{x}) = 1$ if and only if $\mathbf{x} = \mathbf{y}$. The construction is derived via the AND composition lemma (see Theorem 6.2) and is of complexity $O(\ell \cdot \log |\mathbb{F}|)$.

- A 1-key t-queries variant, i.e., a construction where for any $f_y \in \mathcal{F}$ and any $\mathcal{X} \subseteq \mathbb{F}/y$ of size $|\mathcal{X}| < t$, it holds that

$$(f_y, x, K_{f_y}, \{K_x\}_{x \in \mathcal{X}}) \equiv (f_y, x, K_{f_y}, \{u_x\}_{x \in \mathcal{X}})$$

  where $K \leftarrow \mathsf{Setup}(),\ K_{f_y} \leftarrow \mathsf{A}(K, f_y),\ K_x \leftarrow \mathsf{B}(K, x),\ u_x \leftarrow \mathcal{U}_{|K_x|}$. In the construction, sample a random polynomial p of degree t as the common random string K and compute $K_x = p(x),\ K_{f_y} = p(y)$. The complexity is $O(t \cdot \log |\mathbb{F}|)$.

6.4 Subset Predicates

Theorem 6.4. *Let $\mathcal{F} = \{f_Y\}_{Y \subseteq [N]}$ be the family of subset predicate over the set $[N]$, i.e., for any fixed subset $Y \subseteq [N]$, $f_Y : 2^{[N]} \to \{0,1\}$ and $f_Y(X) = 1$ if and only if $X \subseteq Y$. Then, there is a one-one constrained PRF for $\mathcal{F}$ with perfect correctness, perfect security, and complexity $O(N)$.*

Proof. The construction is as follows.

- $\mathsf{Setup}()$: For any $i \in [N]$ sample $k_i \overset{\$}{\leftarrow} \{0,1\}$. Output $K = \{k_i\}_{i \in [N]}$.
- $\mathsf{A}(K, f_Y)$: Parse $K = \{k_i\}_{i \in [N]}$ and output $K_{f_Y} = \{k_i\}_{i \in Y}$.
- $\mathsf{B}(K, X)$: Parse $K = \{k_i\}_{i \in [N]}$ and output $K_X = \bigoplus_{i \in X} k_i$.
- $\mathsf{Recon}(X, f_Y, K_{f_Y})$: Parse $K_{f_Y} = \{k_i\}_{i \in Y}$. If $X \subseteq Y$ then compute and output $K'_X = \bigoplus_{i \in X} k_i$, otherwise output $\perp$.

Correctness. If $f_Y(X) = 1$, i.e., $X \subseteq Y$, then $K'_X = K_X$.

Security. If $f_Y(X) = 0$, i.e., $X \nsubseteq Y$, then there exists an index $i^* \in X$ such that $i^* \notin Y$, therefore

$$(f_Y, X, \{k_i\}_{i \in Y}, k_{i^*}) \equiv (f, x, \{k_i\}_{i \in Y}, u)$$

and thus

$$(f_Y, X, \{k_i\}_{i \in Y}, \bigoplus_{i \in X} k_i) \equiv (f_Y, X, \{k_i\}_{i \in Y}, u)$$

and thus

$$(f_Y, X, K_{f_Y}, K_X) \equiv (f_Y, X, K_{f_Y}, u)$$

where $\{k_i\}_{i \in [N]} = K \leftarrow \mathsf{Setup}(),\ K_{f_Y} \leftarrow \mathsf{A}(K, f_Y),\ K_X \leftarrow \mathsf{B}(K, X),\ u \xleftarrow{\$} \{0,1\}$. □

Extensions. Using techniques similar to [DKNY18,Tsa19], the construction above implies a one-one constrained PRF for the class of t-CNF predicates with inputs of length ℓ over some field $\mathbb{F}$, where the construction is of complexity $O(\binom{\ell}{t} \cdot |\mathbb{F}|^t \cdot \log |\mathbb{F}|)$.

6.5 Inner-Product Predicates

Theorem 6.5. *Let $\mathcal{F} = \{f_{\mathbf{y}}\}_{\mathbf{y} \in \mathbb{F}^\ell}$ be the family of inner-product predicates of length-ℓ vectors over some field $\mathbb{F}$, i.e., for any fixed $\mathbf{y} \in \mathbb{F}^\ell$, $f_{\mathbf{y}} : \mathbb{F}^\ell \to \{0,1\}$ where $f_{\mathbf{y}}(\mathbf{x}) = 1$ if and only if $\langle \mathbf{y}, \mathbf{x} \rangle = 0$. Then, there is a one-one constrained PRF for $\mathcal{F}$ with perfect correctness, perfect security, and complexity $O(\ell \cdot \log |\mathbb{F}|)$.*

Proof. The construction is as follows.

- $\mathsf{Setup}()$: Sample $\mathbf{v} \xleftarrow{\$} \mathbb{F}^\ell$ and $w \xleftarrow{\$} \mathbb{F}$. Output $K = (\mathbf{v}, w)$.
- $\mathsf{A}(K, f_{\mathbf{y}})$: Parse $K = (\mathbf{v}, w)$ and output $K_{f_{\mathbf{y}}} = w\mathbf{y} + \mathbf{v}$.
- $\mathsf{B}(K, \mathbf{x})$: Parse $K = (\mathbf{v}, w)$ and output $K_{\mathbf{x}} = \langle \mathbf{v}, \mathbf{x} \rangle$.
- $\mathsf{Recon}(\mathbf{x}, f_{\mathbf{y}}, K_{f_{\mathbf{y}}})$: Output $\langle K_{f_{\mathbf{y}}}, \mathbf{x} \rangle$.

Correctness. If $f_{\mathbf{y}}(\mathbf{x}) = 1$, i.e., $\langle \mathbf{y}, \mathbf{x} \rangle = 0$, then

$$\langle K_{f_{\mathbf{y}}}, \mathbf{x} \rangle = \langle w\mathbf{y} + \mathbf{v}, \mathbf{x} \rangle = \underbrace{w\langle \mathbf{y}, \mathbf{x} \rangle}_{0} + \underbrace{\langle \mathbf{v}, \mathbf{x} \rangle}_{K_x}.$$

Security. If $f_{\mathbf{y}}(\mathbf{x}) = 0$, i.e., $\langle \mathbf{y}, \mathbf{x} \rangle \neq 0$, then

$$(f_{\mathbf{y}}, \mathbf{x}, K_{f_{\mathbf{y}}}, K_{\mathbf{x}}) = (f_{\mathbf{y}}, \mathbf{x}, w\mathbf{y} + \mathbf{v}, \langle \mathbf{v}, \mathbf{x} \rangle) \equiv (f_{\mathbf{y}}, \mathbf{x}, w\mathbf{y} + \mathbf{v}, u) = (f_{\mathbf{y}}, \mathbf{x}, K_{f_{\mathbf{y}}}, u)$$

where $K \leftarrow \mathsf{Setup}(),\ K_{f_{\mathbf{y}}} \leftarrow \mathsf{A}(K, f_{\mathbf{y}}),\ K_{\mathbf{x}} \leftarrow \mathsf{B}(K, \mathbf{x}),\ u \xleftarrow{\$} \mathbb{F}$.

To see that, fix some values $(\mathbf{y}, \mathbf{x}, u)$. Sample a random $\mathbf{v}$ under the constraint that $\langle \mathbf{v}, \mathbf{x} \rangle = u$, then sample w and output $(f_{\mathbf{y}}, \mathbf{x}, w\mathbf{y} + \mathbf{v}, u)$. □

7 Removing the One-One Restriction via Key-Homomorphic PRF

In this section we consider one-one cPRFs that satisfy an additional property and show that such one-one cPRFs can be boosted to standard cPRFs via key-homomorphic PRFs. We then show that all of our information-theoretic one-one cPRFs satisfy this property, thus receiving new cPRF constructions.

In more detail, we require an alternative algorithm for Alice, $\mathsf{dkA}(K, f)$, that produces a *double-key* $(K_f, \hat{K}_f)$. Such double-key should have the property that $\hat{K}_f$ looks uniformly random even given K_f, but on the other hand, given both of the key parts $(K_f, \hat{K}_f)$ it should be possible to compute K_x for all x (regardless of $f(x)$). We now formally define this additional property.

Definition 7.1. *A one-one constrained pseudorandom function for a predicate family $\mathcal{F}$ and an input space $\mathcal{X}$ is in the* double-key *model, if in addition to the algorithms* $(\mathsf{Setup}, \mathsf{B}, \mathsf{Recon})$ *as in Theorem 4.1, there exists algorithms* dkA *and* $\mathsf{dkRecon}$ *with the following syntax.*

- $\mathsf{dkA}(K, f) \to (K_f, \hat{K}_f)$ *is a PPT algorithm that takes a common random string K and a predicate $f \in \mathcal{F}$. It outputs a pair of keys $(K_f, \hat{K}_f)$.*
- $\mathsf{dkRecon}(x, f, K_f, \hat{K}_f) \to K'_x$ *is a deterministic algorithm that takes an input x, a predicate $f \in \mathcal{F}$, and a pair of keys $(K_f, \hat{K}_f)$. It outputs a value K'_x.*

(Standard) Correctness. *A one-one constrained PRF is* correct *if it satisfies standard correctness (as in Theorem 4.1) with respect to the keys K_f. That is, for all $f \in \mathcal{F}$ and $x \in \mathcal{X}$ for which $f(x) = 1$, for all $K \leftarrow \mathsf{Setup}(1^\lambda)$, and for all $(K_f, \hat{K}_f) \leftarrow \mathsf{dkA}(K, f)$, it holds that* $\mathsf{Recon}(x, f, K_f) = \mathsf{B}(K, x)$.

Correctness of Double-Keys. *A one-one constrained PRF has* correct double-key *if for all $f \in \mathcal{F}$ and $x \in \mathcal{X}$ for which $f(x) = 0$, for all $K \leftarrow \mathsf{Setup}(1^\lambda)$, and for all $(K_f, \hat{K}_f) \leftarrow \mathsf{dkA}(K, f)$, it holds that* $\mathsf{dkRecon}(x, f, K_f, \hat{K}_f) = \mathsf{B}(K, x)$.

Security of Double-Keys. *The scheme has perfect (/statistical /computational) double-key security if for any $f \in \mathcal{F}$ and any unbounded (/unbounded /PPT) distinguisher, the following distributions are identical (/statistically close /computationally indistinguishable).*

$$(f, K_f, \hat{K}_f) \equiv (f, K_f, u)$$

where $K \leftarrow \mathsf{Setup}(1^\lambda),\ (K_f, \hat{K}_f) \leftarrow \mathsf{dkA}(K, f),\ u \leftarrow \mathcal{U}_{|\hat{K}_f|}$.

Given the new definition in hand, we now state the main theorem.

Theorem 7.2. *Let* $(\mathsf{KeyGen}, \mathsf{Eval}, \mathsf{HomKeyEval})$ *be a key-homomorphic PRF for an input space $\mathcal{X}_\alpha$, a key space $\mathcal{K}$, and a function family $\mathcal{G} = \{\mathcal{G}_n : \mathcal{K}^n \to \mathcal{K}\}_{n \in \mathbb{N}}$, and let* $(\mathsf{Setup}, \mathsf{dkA}, \mathsf{B}, \mathsf{Recon}, \mathsf{dkRecon})$ *be a one-one cPRF in the double-key model (as in Theorem 7.1) for an input space $\mathcal{X}_\beta$ and a predicate family $\mathcal{F}$, such that:*

- *The key space $\mathcal{K}$ is some field $\mathbb{F}$ and the algorithm* $\mathsf{KeyGen}(1^\lambda)$ *outputs a random value* $\mathsf{sk} \xleftarrow{\$} \mathbb{F}$.
- *For all $x \in \mathcal{X}_\beta$ and all $K \leftarrow \mathsf{Setup}(1^\lambda)$ it holds that $K_x \in \mathbb{F}$ where $K_x \leftarrow \mathsf{B}(K, x)$ and $\mathbb{F}$ is the same field as above.*
- *For all $f \in \mathcal{F}$ there exists $n \in \mathbb{N}$ such that for all $K \leftarrow \mathsf{Setup}(1^\lambda)$ it holds that $\hat{K}_f \in \mathbb{F}^n$, where $(K_f, \hat{K}_f) \leftarrow \mathsf{dkA}(K, f)$ and $\mathbb{F}$ is the same field as above.*
- *For all $x \in \mathcal{X}_\beta$ and $f \in \mathcal{F}$ such that $f(x) = 0$, and all $(K_f, \hat{K}_f) \leftarrow \mathsf{dkA}(K, f)$ where $K \leftarrow \mathsf{Setup}(1^\lambda)$, let $\mathsf{dkRecon}_{x,f,K_f} : \mathbb{F}^n \to \mathbb{F}$ denote the algorithm* $\mathsf{dkRecon}$ *with the hard-coded inputs (x, f, K_f), i.e., $\mathsf{dkRecon}_{x,f,K_f}(\cdot) = \mathsf{dkRecon}(x, f, K_f, \cdot)$. Then:*
  - $\mathsf{dkRecon}_{x,f,K_f}(\cdot)$ *can be homomorphically evaluated over keys of the key-homomorphic scheme, i.e., $\mathsf{dkRecon}_{x,f,K_f}(\cdot) \in \mathcal{G}$.*
  - $\mathsf{dkRecon}_{x,f,K_f}(\cdot)$ *preserves uniformity, i.e., the distributions $\mathsf{dkRecon}_{x,f,K_f}(\mathcal{U}_{\mathbb{F}^n})$ and $\mathcal{U}_{\mathbb{F}}$ are identical.*

Then, there exists a key-selective secure single-key constrained PRF for the predicate family $\mathcal{F}$ and the input space $\mathcal{X} = \mathcal{X}_\alpha \cap \mathcal{X}_\beta$.

7.1 The Reduction

We proceed to the proof of Theorem 7.2. Assuming a key-homomorphic PRF and a one-one constrained PRF as described in the theorem, the constrained PRF is defined as follows.

Construction 7.3. *Define:*

- $\mathsf{CPRF.KeyGen}(1^\lambda)$*: Compute $K \leftarrow \mathsf{Setup}(1^\lambda)$ and output $\mathsf{msk} = K$.*
- $\mathsf{CPRF.Eval}(\mathsf{msk}, x)$*: Parse $\mathsf{msk} = K$. Compute $K_x := \mathsf{B}(K, x)$ and output $r_x := \mathsf{Eval}_{K_x}(x)$.*
- $\mathsf{CPRF.Constrain}(\mathsf{msk}, f)$*: Parse $\mathsf{msk} = K$. Compute $(K_f, \hat{K}_f) \leftarrow \mathsf{dkA}(K, f)$ and output $\mathsf{sk}_f = (f, K_f)$.*
- $\mathsf{CPRF.ConstrainEval}(\mathsf{sk}_f, x)$*: Parse $\mathsf{sk}_f = (f, K_f)$. Compute $K'_x := \mathsf{Recon}(x, f, K_f)$ and output $r'_x := \mathsf{Eval}_{K'_x}(x)$.*

Correctness of Constrained Keys. Fix $x \in \mathcal{X}$ and $f \in \mathcal{F}$ for which $f(x) = 1$, and $\mathsf{msk} \leftarrow \mathsf{CPRF.KeyGen}(1^\lambda)$, $\mathsf{sk}_f \leftarrow \mathsf{CPRF.Constrain}(\mathsf{msk}, f)$. Then $\mathsf{msk} = K$ and $\mathsf{sk}_f = (f, K_f)$ where $K \leftarrow \mathsf{Setup}(1^\lambda)$ and $(K_f, \hat{K}_f) \leftarrow \mathsf{dkA}(K, f)$. Consider $\mathsf{CPRF.ConstrainEval}(\mathsf{sk}_f, x)$ and in particular $K'_x = \mathsf{Recon}(x, f, K_f)$, then by the standard correctness of the one-one cPRF, since $f(x) = 1$ it holds that $K'_x = K_x$ and therefore $\mathsf{Eval}_{K'_x}(x) = \mathsf{Eval}_{K_x}(x)$.

Pseudorandomness. We now prove that Theorem 7.3 is a single-key key-selective secure constrained PRF as in Theorem 3.4. The proof goes via a sequence of hybrids.

Hybrid H_0. This is the real security game as in Theorem 3.4. Note that this is the selective-key game, i.e., the key query for f happens before any other queries. Explicitly, $\mathcal{C}$ computes $K \leftarrow \mathsf{Setup}(1^\lambda)$ and then immediately answers the key query:

- *Key Query:* Upon receiving $f \in \mathcal{F}$, $\mathcal{C}$ computes $(K_f, \hat{K}_f) \leftarrow \mathsf{dkA}(K, f)$ and sends K_f to $\mathcal{A}$.

In the rest of the game $\mathcal{C}$ answers queries made by $\mathcal{A}$ as follows.

- *Evaluation Query:* Upon receiving $x \in \mathcal{X}$, $\mathcal{C}$ computes $K_x := \mathsf{B}(K, x)$ and $r_x := \mathsf{Eval}_{K_x}(x)$.

  It sends r_x to $\mathcal{A}$.

- *Challenge Query:* Upon receiving $x^* \in \mathcal{X}$, $\mathcal{C}$ computes $K_{x^*} := \mathsf{B}(K, x^*)$ and $r_{x^*} := \mathsf{Eval}_{K_{x^*}}(x^*)$.

  It samples a bit $b \xleftarrow{\$} \{0,1\}$. If $b = 0$, it sends r_{x^*} to $\mathcal{A}$, otherwise it sends to $\mathcal{A}$ a random value $u \leftarrow \mathcal{U}_{|r_{x^*}|}$.

Hybrid H_1. In this hybrid we change the way that $\mathcal{C}$ evaluates K_x when it answers evaluation queries and the challenge query. Instead of using the common random string K, it will use the double-key $(K_f, \hat{K}_f)$. That is, upon receiving $x \in \mathcal{X}$, instead of computing $K_x := \mathsf{B}(K, x)$ it computes

$$K_x := \begin{cases} \mathsf{Recon}(x, f, K_f) & f(x) = 1 \\ \mathsf{dkRecon}(x, f, K_f, \hat{K}_f) & f(x) = 0 \end{cases}$$

and then proceeds as in the previous hybrid. Due to the prefect standard correctness and correctness of double-keys, the distributions that $\mathcal{C}$ outputs in Hybrids H_0 and H_1 are identical.

Hybrid H_2. Note that $\mathcal{C}$ does not use K anymore except of when it first generates $(K_f, \hat{K}_f)$. In this hybrid we change $\hat{K}_f$ to uniform. That is, after computing $(K_f, \hat{K}_f) \leftarrow \mathsf{dkA}(K, f)$, $\mathcal{C}$ samples a random value $u \leftarrow \mathcal{U}_{|\hat{K}_f|}$ and overrides the value of $\hat{K}_f$ such that $\hat{K}_f := u$. By the perfect (/statistical /computational) security of double-keys, the distributions that $\mathcal{C}$ outputs in hybrids H_1 and H_2 are identical (/statistically close /computationally indistinguishable).

Hybrid H_3. In this hybrid we change the way that $\mathcal{C}$ evaluates r_x when it answers evaluation queries and the challenge query, whenever $f(x) = 0$. Recall that in the previous hybrid it computes $r_x := \mathsf{Eval}_{K_x}(x)$ where $K_x := \mathsf{dkRecon}(x, f, K_f, \hat{K}_f)$, and recall that by assumption, $\mathsf{dkRecon}_{x,f,K_f}(\cdot) = \mathsf{dkRecon}(x, f, K_f, \cdot)$ can be homomorphically evaluated over the PRF key-space using $\mathsf{HomKeyEval}$. Moreover, by our assumption it holds that $\hat{K}_f \in \mathbb{F}^n$ for some $n \in \mathbb{N}$. Therefore,

$$\begin{aligned} r_x &= \mathsf{Eval}_{K_x}(x) \\ &= \mathsf{Eval}_{\mathsf{dkRecon}(x,f,K_f,\hat{K}_f)}(x) \\ &= \mathsf{Eval}_{\mathsf{dkRecon}_{x,f,K_f}(\hat{K}_f)}(x) \\ &= \mathsf{HomKeyEval}\left(\mathsf{dkRecon}_{x,f,K_f},\ \mathsf{Eval}_{\hat{K}_f^1}(x), \ldots, \mathsf{Eval}_{\hat{K}_f^n}(x)\right) \end{aligned}$$

where $\hat{K}_f = (\hat{K}_f^1, \ldots, \hat{K}_f^n)$. In this hybrid, $\mathcal{C}$ first computes $s_x^i := \mathsf{Eval}_{\hat{K}_f^i}(x)$ for all $i \in [n]$, and then

$$r_x := \mathsf{HomKeyEval}\left(\mathsf{dkRecon}_{x,f,K_f},\ s_x^1, \ldots, s_x^n\right).$$

By the perfect correctness of homomorphic key evaluation, the distributions that $\mathcal{C}$ outputs in hybrids H_2 and H_3 are identical.

Hybrid H_4. In this hybrid we change the way that $\mathcal{C}$ evaluates $s_x^1, \ldots, s_x^n$ whenever $f(x) = 0$. Note that in Hybrid H_3 the value $\hat{K}_f$, which is uniformly random in $\mathbb{F}^n$, is only used when computing $s_x^i := \mathsf{Eval}_{\hat{K}_f^i}(x)$ for all $i \in [n]$. Thus, we can replace the values $s_x^1, \ldots, s_x^n$ with uniformly random strings. That is, whenever a query is made for an x such that $f(x) = 0$, $\mathcal{C}$ samples $s_x^1, \ldots, s_x^n \xleftarrow{\$} \{0,1\}^*$ of appropriate size and then proceeds as in the previous hybrid. By the pseudorandomness of the key-homomorphic PRF respective to the keys $\hat{K}_f^1, \ldots, \hat{K}_f^n$, the distributions that $\mathcal{C}$ outputs in hybrids H_3 and H_4 are computationally indistinguishable.

Hybrid H_5. We change again the way that $\mathcal{C}$ evaluates r_x whenever $f(x) = 0$. In this hybrid the values r_x are replaced with uniformly sampled strings. Indistinguishability will follow immediately from the next lemma, since $s_x^1, \ldots, s_x^n$ are random values and $\mathsf{dkRecon}_{x,f,K_f}(\cdot)$ preserves uniformity. □

Lemma 7.4. *Let* $(\mathsf{KeyGen}, \mathsf{Eval}, \mathsf{HomKeyEval})$ *be a secure key-homomorphic PRF for a key space* $\mathcal{K}$ *and a function family* $\mathcal{G} = \{\mathcal{G}_n : \mathcal{K}^n \to \mathcal{K}\}_{n \in \mathbb{N}}$*, where valid keys are samples from* $\mathcal{U}_{\mathcal{K}}$ *and the output space is* $\mathcal{O}$*. Let* $g \in \mathcal{G}_n$ *be a function such that* $g(\mathcal{U}_{\mathcal{K}^n})$ *and* $\mathcal{U}_{\mathcal{K}}$ *are computationally indistinguishable. Then, the distribution* $\mathsf{HomKeyEval}(g, \mathcal{U}_{\mathcal{O}^n})$ *is computationally indistinguishable from* $\mathcal{U}_{\mathcal{O}}$*.*

Proof. Via hybrids:

1. The distribution $\mathsf{HomKeyEval}(g, \mathcal{U}_{\mathcal{O}^n})$.
2. The distribution $\mathsf{HomKeyEval}\left(g, \mathsf{Eval}_{\mathcal{U}_{\mathcal{K}}}(0), \ldots, \mathsf{Eval}_{\mathcal{U}_{\mathcal{K}}}(0)\right)$ (Ind. by the pseudorandomness). Note that the distribution $\mathsf{Eval}_{\mathcal{U}_{\mathcal{K}}}(0)$ is concatenated n times and that the PRF input 0 was chosen arbitrarily.
3. The distribution $\mathsf{Eval}_{g(\mathcal{U}_{\mathcal{K}^n})}(0)$ (Ind. by the correctness of homomorphic key evaluation).
4. The distribution $\mathsf{Eval}_{\mathcal{U}_{\mathcal{K}}}(0)$ (Ind. by the assumption about g).
5. The distribution $\mathcal{U}_{\mathcal{O}}$ (Ind. by the pseudorandomness).

□

7.2 Constructions of One-One cPRFs in the Double-Key Model

We now show that all of our information-theoretic constructions (see Section 6) have a *double-key* variant (see Theorem 7.1) of the same complexity. Moreover, in all of those double-key constructions, the corresponding function $\mathsf{dkRecon}_{x,f,K_f}$ (see Theorem 7.2 for definition) is linear and preserves uniformity. Due to the similarity to the constructions in Section 6, we provide here an overview.

Generic Predicates. For an input space $\mathbb{F}$ and any predicate family $\mathcal{F}$, the common random string $K = \{k_y\}_{y \in \mathbb{F}}$ consists of random bits $k_y \xleftarrow{\$} \{0,1\}$ for every element in the field. The value K_x is then simply k_x. The double-key for a predicate f splits K into a set of authorized inputs $K_f = \{k_y : f(y) = 1\}_{y \in \mathbb{F}}$ and a set of unauthorized inputs $\hat{K}_f = \{k_y : f(y) = 0\}_{y \in \mathbb{F}}$. Clearly, $\hat{K}_f$ is uniformly distributed even given K_f, and recovering a value k_x from $\hat{K}_f$ is a linear function.

AND Composition. Consider two perfect one-one cPRFs in the double-key model for some predicate families $\mathcal{F}^1 = \{f^1\}$ and $\mathcal{F}^2 = \{f^2\}$. In the construction for the predicate family $\mathcal{F}^1 \wedge \mathcal{F}^2 = \{f^1 \wedge f^2\}_{f^1 \in \mathcal{F}^1, f^2 \in \mathcal{F}^2}$, there is one instance of each of the underlying constructions. The common random string $K = (K^1, K^2)$ and double-keys $K_f = (K^1_{f^1}, K^2_{f^2})$ and $\hat{K}_f = (\hat{K}^1_{f^1}, \hat{K}^2_{f^2})$ where $f = f^1 \wedge f^2$ are a concatenation of the corresponding values in the underlying schemes. The values $K_x = K^1_x + K^2_x$ are the *sum* of the corresponding values in the underlying schemes. Since the two instances are secure and generated independently, uniformity of $\hat{K}_f$ given K_f follows immediately. Moreover, the algorithm $\mathsf{dkRecon}(x, f, K_f, \hat{K}_f)$ that computes and outputs $\mathsf{dkRecon}^1(x, f^1, K^1_{f^1}, \hat{K}^1_{f^1}) + \mathsf{dkRecon}^2(x, f^2, K^2_{f^2}, \hat{K}^2_{f^2})$ is clearly correct, linear in $\hat{K}_f$, and preserves uniformity if the underlying schemes are correct, linear in $\hat{K}^1_{f^1}$ and $\hat{K}^2_{f^2}$, and preserve uniformity.

Equality Testing. Consider equality testing over some field $\mathbb{F}$. The common random string $K = (k_0, k_1)$ consists of two random elements in the field $k_0, k_1 \xleftarrow{\$} \mathbb{F}$, and we define $K_x = k_0 + xk_1$. The double-key for some value y is defined as $K_{f_y} = k_0 + yk_1$ and $\hat{K}_{f_y} = yk_1$. Note that by the uniformity of k_0 and k_1, for all $y \neq 0$ the key part $\hat{K}_{f_y}$ is distributed uniformly in $\mathbb{F}$ even given K_{f_y}. To reconstruct K_x for some $x \neq y$, compute

$$\mathsf{dkRecon}(x, y, K_{f_y}, \hat{K}_{f_y}) = \frac{x - y}{y} \hat{K}_{f_y} + K_{f_y} = (x - y)k_1 + k_0 + yk_1 = k_0 + xk_1 = K_x \ ,$$

which is correct and linear in $\hat{K}_{f_y}$.

Subset Predicates. Recall that we consider all subsets $X \subseteq [N]$ as the input space and all subsets $Y \subseteq [N]$ as the predicate family, such that $f_Y(X) = 1$ if and only if $X \subseteq Y$. The common random string $K = \{k_i\}_{i \in [N]}$ consists of random bits $k_i \xleftarrow{\$} \{0, 1\}$ for every element in the set $[N]$. The value K_X is then set to $K_X = \bigoplus_{i \in X} k_i$. The double-key for a predicate f_Y splits K into a set of authorized elements $K_{f_Y} = \{k_i\}_{i \in Y}$ and a set of unauthorized elements $\hat{K}_{f_Y} = \{k_i\}_{i \in [N]/Y}$. Clearly, $\hat{K}_{f_Y}$ is uniformly distributed even given K_{f_Y}, and recovering a value k_i from $(K_{f_Y}, \hat{K}_{f_Y})$ is a linear function that preserves uniformity.

Inner-Product Predicates. Consider inner-product testing of vectors of length ℓ over some field $\mathbb{F}$. The common random string $K = (\mathbf{v}, w)$ consists of a random vector $\mathbf{v} \xleftarrow{\$} \mathbb{F}^\ell$ and a random field element $w \xleftarrow{\$} \mathbb{F}$. We define $K_{\mathbf{x}} = \langle \mathbf{v}, \mathbf{x} \rangle$. The double-key for a vector predicate $\mathbf{y}$ is defined as $K_{f_{\mathbf{y}}} = w\mathbf{y} + \mathbf{v}$ and $\hat{K}_{f_{\mathbf{y}}} = w$. Note that by the uniformity of $\mathbf{v}$ and w, the key part $\hat{K}_{f_{\mathbf{y}}}$ is distributed uniformly in $\mathbb{F}$ even given $K_{f_{\mathbf{y}}}$. To reconstruct $K_{\mathbf{x}}$ for some $\mathbf{x}$, compute

$$\mathsf{dkRecon}(\mathbf{x}, f_{\mathbf{y}}, K_{f_{\mathbf{y}}}, \hat{K}_{f_{\mathbf{y}}}) = \langle K_{f_{\mathbf{y}}}, \mathbf{x} \rangle - \hat{K}_{f_{\mathbf{y}}} \langle \mathbf{y}, \mathbf{x} \rangle = \langle w\mathbf{y} + \mathbf{v}, \mathbf{x} \rangle - w \langle \mathbf{y}, \mathbf{x} \rangle = \langle \mathbf{v}, \mathbf{x} \rangle = K_{\mathbf{x}} \ ,$$

which is correct, linear in $\hat{K}_{f_{\mathbf{y}}}$, and preserves uniformity.

8 One-One Constrained PRF and CDS Protocols

In this section we study the connection between one-one constrained PRFs and conditional disclosure of secrets (CDS) protocols, a cryptographic primitive used to construct many secure protocols (see discussion in the introduction). In CDS protocols, Alice and Bob hold a secret and a common random string, and each of them holds a private input for some two-input predicate. Then, each of the parties sends one message to a referee, which is based on its private input, the secret, and the common random string. The referee, knowing the inputs of the parties, should learn the secret if and only if the inputs of the parties satisfy the predicate. We next provide a formal definition of CDS protocols, originally presented in [GIKM00].

Definition 8.1 (Conditional Disclosure of Secrets Protocols). *Let $f : X \times Y \to \{0,1\}$ be a predicate. A* conditional disclosure of secrets (CDS) protocol *$\mathcal{P}$ for f with domain of secrets S, domain of common random strings R, and finite message domains M_A, M_B consists of two deterministic message computation functions $\mathsf{Encode}_A, \mathsf{Encode}_B$, where $\mathsf{Encode}_A : X \times S \times R \to M_A$ and $\mathsf{Encode}_B : Y \times S \times R \to M_B$, and a deterministic reconstruction function $\mathsf{Decrypt} : X \times Y \times M_A \times M_B \to S$. We say that $\mathcal{P}$ is a CDS protocol for f if it satisfies the following requirements.*

Correctness. *For every inputs $x \in X$ and $y \in Y$ for which $f(x,y) = 1$, every secret $s \in S$, and every common random string $r \in R$,*

$$\mathsf{Decrypt}(x, y, \mathsf{Encode}_A(x,s,r), \mathsf{Encode}_B(y,s,r)) = s \ .$$

Security. *For every inputs $x \in X$ and $y \in Y$ for which $f(x,y) = 0$ and every secret $s \in S$,*

$$(x, y, \mathsf{Encode}_A(x,s,r), \mathsf{Encode}_B(y,s,r), s) \quad \equiv \quad (x, y, \mathsf{Encode}_A(x,s,r), \mathsf{Encode}_B(y,s,r), u)$$

where $r \overset{\$}{\leftarrow} R$ and $u \overset{\$}{\leftarrow} S$.

Message Size. *The* message size *of a CDS protocol $\mathcal{P}$ is defined as the sizes of the messages sent by the parties, i.e.,* $\log|M_A| + \log|M_B|$.

We consider the index predicate, which gets as inputs an N-bit string (or a database) D and an index $i \in [N]$, and returns the ith bit in D, denoted by D_i.

Definition 8.2 (The Index Function). *The index predicate is the predicate $f_{\text{index}} : \{0,1\}^N \times [N] \to \{0,1\}$, where $f_{\text{index}}(D,i) = D_i$.*

We next show a transformation that preservers complexity from one-one constrained PRFs to CDS protocols for the index predicate.

Theorem 8.3. *Let $f_{\text{index}} : \{0,1\}^N \times [N] \to \{0,1\}$ be the index predicate, and assume that for every predicate $f : [N] \to \{0,1\}$ there is a one-one constrained PRF for f with complexity $c(N)$. Then, there is a CDS protocol for f_{index} with message size $c(N)$.*

Proof. We consider a one-one constrained PRF scheme, when Alice holds a predicate $f : [N] \to \{0,1\}$, Bob holds an input $x \in [N]$, and both hold a common random string $K \leftarrow \mathsf{Setup}(1^\lambda)$, where $K_f \leftarrow \mathsf{A}(K,f)$ and $K_x \leftarrow \mathsf{B}(K,x)$. By the correctness requirement of the one-one constrained

PRF, if $f(x) = 1$ then there exist a deterministic function Recon such that $\mathsf{Recon}(x, f, K_f) = K_x$, and by security requirement, if $f(x) = 0$ then $(f, x, K_f, K_x) \equiv (f, x, K_f, u)$, where $u \leftarrow \mathcal{U}_{|K_x|}$.

We show a construction of a CDS protocol for the index predicate f_{index}, which is based on the above one-one constrained PRF. The construction is as follows.

- Inputs: Alice holds $D \in \{0,1\}^N$ and Bob holds $i \in [N]$. We represent D as the predicate $f_D : [N] \to \{0,1\}$, where $f_D(j) = f_{\text{index}}(D, j) = D_j$.
- The secret: A string s of size at most $|\mathsf{B}(K, i)|$.
- The common random string: An element $K \leftarrow \mathsf{Setup}(1^\lambda)$.
- $\mathsf{Encode}_A(D, K)$: Alice computes and sends the message $\mathsf{Encode}_A(D, K) = \mathsf{A}(K, f_D) = K_{f_D}$.
- $\mathsf{Encode}_B(i, K)$: Bob computes and sends the message $\mathsf{Encode}_B(i, K) = \mathsf{B}(K, i) \oplus s' = K_i \oplus s'$, where $s' = 0^t \circ s$ such that $|s'| = |\mathsf{B}(K, i)|$.
- $\mathsf{Decrypt}(D, i, \mathsf{Encode}_A(D, K), \mathsf{Encode}_B(i, K))$: If $f_{\text{index}}(D, i) = 1$, the referee computes
$$\mathsf{Recon}(i, f_D, \mathsf{Encode}_A(D, K)) \oplus \mathsf{Encode}_B(i, K).$$

Correctness. If $f_{\text{index}}(D, i) = 1$, i.e., $f_D(i) = 1$, then the referee computes

$$\mathsf{Recon}(i, f_D, \mathsf{Encode}_A(D, K)) \oplus \mathsf{Encode}_B(i, K) = \mathsf{Recon}(i, f_D, K_{f_D}) \oplus K_i \oplus s' = K_i \oplus K_i \oplus s' = s'$$

where the second equality follows from the correctness of the one-one constrained PRF. Hence, the referee learns s' and so the secret s.

Security. If $f_{\text{index}}(D, i) = 0$, i.e., $f_D(i) = 0$, then by the security of the one-one constrained PRF,

$$(f_D, i, \mathsf{A}(K, f_D), \mathsf{B}(K, i)) \equiv (f_D, i, \mathsf{A}(K, f_D,), u)$$

where $K \leftarrow \mathsf{Setup}(1^\lambda)$ and $u \leftarrow \mathcal{U}_{|\mathsf{B}(K,i)|}$. Then, since $s' = \mathsf{Encode}_B(i, K) \oplus \mathsf{B}(K, i)$ we get that

$$(D, i, \mathsf{Encode}_A(D, K), \mathsf{Encode}_B(i, K), s') \equiv (D, i, \mathsf{Encode}_A(D, K), \mathsf{Encode}_B(i, K), u)$$

where $K \leftarrow \mathsf{Setup}(1^\lambda)$ and $u \leftarrow \mathcal{U}_{|s'|}$.

Message size. The message size of this CDS protocol is equal to the complexity of the one-one constrained PRF, which is $c(N)$. □

Using the above result and the reduction that appears in [GKW15], from CDS protocols for general predicates to CDS protocols for the index predicate, we get a transformation from one-one constrained PRF to CDS protocols for general predicates.

Corollary 8.4. *Let $g : [N] \times [N] \to \{0,1\}$ be a predicate, and assume that for every predicate $f : [N] \to \{0,1\}$ there is a one-one constrained PRF for f with complexity $c(N)$. Then, there is a CDS protocol for g with message size $c(N)$.*

Note the best known CDS protocol for general predicates $g : [N] \times [N] \to \{0,1\}$ has message size $2^{O(\sqrt{\log N \log\log N})}$ [LVW17]. Thus, by the above lower bound of $\Omega(N)$ on the complexity of one-one constrained PRFs of Theorem 5.1, we cannot get a similar transformation that preserve complexity in the other direction (i.e., a transformation from CDS protocols to one-one constrained PRFs).

9 Computational Constructions

Every single-key constrained PRF is in particular a one-one constrained PRF under the same security notion (which is either adaptive, key selective or challenge selective, see Theorem 4.1). For completeness, we now go over some of the known computational constructions in the literature of single-key constrained PRFs.

9.1 Constructions from OWFs

Punctured Predicates. As was shown in [BW13, KPTZ13, BGI14], the OWF-based PRF of [GGM84] is in fact puncturable. Using our previous terminology, it supports punctured predicates over the input space $\{0,1\}^n$ as defined in Theorem 5.1. The complexity of the construction is $O(\lambda \cdot n)$ where λ is the security parameter. Furthermore, [FKPR14] showed that the aforementioned construction satisfies *adaptive* security with a security loss exponential in the number of queries. Since we focus on the single-query scenario, we can use their proof strategy to claim adaptive security on the implied one-one cPRF.

Theorem 9.1. *Let $\mathcal{F} = \{f_y\}_{y \in \{0,1\}^n}$ be the family of punctured predicates over the set of n-bit strings, i.e., for any fixed $y \in \{0,1\}^n$, $f_{\neq y} : \{0,1\}^n \to \{0,1\}$ where $f_{\neq y}(x) = 1$ if and only if $x \neq y$. Then, for every security parameter λ, there is a one-one constrained PRF for $\mathcal{F}$ with perfect correctness, computational adaptive security, and complexity $O(\lambda \cdot n)$.*

One-Dimensional Interval Predicates. [KPTZ13] showed how to further generalized the [GGM84] approach in order to support (one-dimensional) interval predicates without compromising the complexity. Such predicates allow to compute the PRF on all inputs x that are within some range $[a,b]$, i.e., all x such that $a \leq x \leq b$, where the key size is $O(\lambda \cdot \log |b-a|)$. Due to the similarity to the construction for punctured predicates, the adaptive security proof strategy of [FKPR14] can also be applied here.

Theorem 9.2. *Let $\mathcal{F} = \{f_{[a,b]}\}_{a,b \in \{0,1\}^n}$ be the family of one-dimensional interval predicates over the set of n-bit strings, i.e., for any fixed $a,b \in \{0,1\}^n$, $f_{[a,b]} : \{0,1\}^n \to \{0,1\}$ where $f_{[a,b]}(x) = 1$ if and only if $a \leq x \leq b$. Then, for every security parameter λ, there is a one-one constrained PRF for $\mathcal{F}$ with perfect correctness, computational adaptive security, and complexity $O(\lambda \cdot n)$.*

Multi-Dimensional Interval Predicates. We now consider multi-dimensional interval predicates (that were previously studied in [BW07,SBC+07,GMW15]). Such predicates are characterized by d intervals $\{[a_i,b_i]\}_{i \in [d]}$, and the input space is $(\{0,1\}^n)^d$. An input $X = (x_1, \ldots, x_d) \in (\{0,1\}^n)^d$ is authorized by the multi-dimensional predicate $f_{[a_i,b_i]_{i \in [d]}}$ if and only if $a_i \leq x_i \leq b_i$ for all $i \in [d]$. Each interval $[a_i,b_i]$ can be verified by checking the n bits of the input corresponding to x_i. In particular, in order to verify that the ith dimension of X (i.e., x_i) is within the ith range $[a_i,b_i]$, we have to check whether the ith block of n bits of X is within the range $[a_i,b_i]$. To do so, we will use the AND composition lemma (that is, Theorem 6.2) sequentially $d-1$ times on d independent instances of one-one cPRFs for one-dimensional interval predicates over inputs of length n (as in Theorem 9.2), where each instance i handles the ith block of X.

Theorem 9.3. *Let $\mathcal{F} = \{f_{[a_i,b_i]_{i\in[d]}}\}_{a_i,b_i\in\{0,1\}^n, i\in[d]}$ be the family of d-dimensional interval predicates over the set of n-bit strings, i.e., for any fixed $a_i, b_i \in \{0,1\}^n$ for all $i \in [d]$, $f_{[a_i,b_i]_{i\in[d]}} : (\{0,1\}^n)^d \to \{0,1\}$ where $f_{[a_i,b_i]_{i\in[d]}}(x_1,\ldots,x_d) = 1$ if and only if $a_i \le x_i \le b_i$ for all $i \in [d]$. Then, for every security parameter λ, there is a one-one constrained PRF for $\mathcal{F}_n$ with perfect correctness, computational adaptive security, and complexity $O(d \cdot \lambda \cdot n)$.*

9.2 Additional Constructions

Lattice Assumptions. [BV15] construct a selectively-secure single-key cPRF for all circuits from LWE. [CC17] construct an adaptively-secure single-key cPRF for NC1 from LWE.

Group Assumptions. [AMN+18] construct a selectively-secure single-key bit-fixing cPRF from DDH.

References

[ABF+19] Benny Applebaum, Amos Beimel, Oriol Farràs, Oded Nir, and Naty Peter. Secret-sharing schemes for general and uniform access structures. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part III*, volume 11478 of *Lecture Notes in Computer Science*, pages 441–471. Springer, 2019.

[ABNP20] Benny Applebaum, Amos Beimel, Oded Nir, and Naty Peter. Better secret-sharing via robust conditional disclosure of secrets. *Electronic Colloquium on Computational Complexity (ECCC)*, 27:8, 2020. To be published in *STOC 2020*.

[AIR01] William Aiello, Yuval Ishai, and Omer Reingold. Priced oblivious transfer: How to sell digital goods. In Birgit Pfitzmann, editor, *Advances in Cryptology - EUROCRYPT 2001, International Conference on the Theory and Application of Cryptographic Techniques, Innsbruck, Austria, May 6-10, 2001, Proceeding*, volume 2045 of *Lecture Notes in Computer Science*, pages 119–135. Springer, 2001.

[AMN+18] Nuttapong Attrapadung, Takahiro Matsuda, Ryo Nishimaki, Shota Yamada, and Takashi Yamakawa. Constrained PRFs for NC^1 in traditional groups. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part II*, volume 10992 of *Lecture Notes in Computer Science*, pages 543–574. Springer, 2018.

[AR16] Benny Applebaum and Pavel Raykov. From private simultaneous messages to zero-information arthur-merlin protocols and back. In Eyal Kushilevitz and Tal Malkin, editors, *Theory of Cryptography - 13th International Conference, TCC 2016-A, Tel Aviv, Israel, January 10-13, 2016, Proceedings, Part II*, volume 9563 of *Lecture Notes in Computer Science*, pages 65–82. Springer, 2016.

[Att14] Nuttapong Attrapadung. Dual system encryption via doubly selective security: Framework, fully secure functional encryption for regular languages, and more. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings*, volume 8441 of *Lecture Notes in Computer Science*, pages 557–577. Springer, 2014.

[BGI14] Elette Boyle, Shafi Goldwasser, and Ioana Ivan. Functional signatures and pseudorandom functions. In Hugo Krawczyk, editor, *Public-Key Cryptography - PKC 2014 - 17th International Conference on Practice and Theory in Public-Key Cryptography, Buenos Aires, Argentina, March 26-28, 2014. Proceedings*, volume 8383 of *Lecture Notes in Computer Science*, pages 501–519. Springer, 2014.

[BIKK14] Amos Beimel, Yuval Ishai, Ranjit Kumaresan, and Eyal Kushilevitz. On the cryptographic complexity of the worst functions. In Yehuda Lindell, editor, *Theory of Cryptography - 11th Theory of Cryptography Conference, TCC 2014, San Diego, CA, USA, February 24-26, 2014. Proceedings*, volume 8349 of *Lecture Notes in Computer Science*, pages 317–342. Springer, 2014.

[BP18] Amos Beimel and Naty Peter. Optimal linear multiparty conditional disclosure of secrets protocols. In Thomas Peyrin and Steven D. Galbraith, editors, *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part III*, volume 11274 of *Lecture Notes in Computer Science*, pages 332–362. Springer, 2018.

[BP19] Amos Beimel and Naty Peter. Secret-sharing from robust conditional disclosure of secrets. *IACR Cryptology ePrint Archive*, 2019:522, 2019.

[BV15] Nir Bitansky and Vinod Vaikuntanathan. Indistinguishability obfuscation from functional encryption. In Venkatesan Guruswami, editor, *IEEE 56th Annual Symposium on Foundations of Computer Science, FOCS 2015, Berkeley, CA, USA, 17-20 October, 2015*, pages 171–190. IEEE Computer Society, 2015.

[BW07] Dan Boneh and Brent Waters. Conjunctive, subset, and range queries on encrypted data. In Salil P. Vadhan, editor, *Theory of Cryptography, 4th Theory of Cryptography Conference, TCC 2007, Amsterdam, The Netherlands, February 21-24, 2007, Proceedings*, volume 4392 of *Lecture Notes in Computer Science*, pages 535–554. Springer, 2007.

[BW13] Dan Boneh and Brent Waters. Constrained pseudorandom functions and their applications. In Kazue Sako and Palash Sarkar, editors, *Advances in Cryptology - ASIACRYPT 2013 - 19th International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, India, December 1-5, 2013, Proceedings, Part II*, volume 8270 of *Lecture Notes in Computer Science*, pages 280–300. Springer, 2013.

[CC17] Ran Canetti and Yilei Chen. Constraint-hiding constrained PRFs for NC^1 from LWE. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *Advances in Cryptology -*

EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part I, volume 10210 of *Lecture Notes in Computer Science*, pages 446–476, 2017.

[DKNY18] Alex Davidson, Shuichi Katsumata, Ryo Nishimaki, and Shota Yamada. Constrained PRFs for bit-fixing from OWFs with constant collusion resistance. *IACR Cryptology ePrint Archive*, 2018:982, 2018.

[FKN94] Uriel Feige, Joe Kilian, and Moni Naor. A minimal model for secure computation (extended abstract). In Frank Thomson Leighton and Michael T. Goodrich, editors, *Proceedings of the Twenty-Sixth Annual ACM Symposium on Theory of Computing, 23-25 May 1994, Montréal, Québec, Canada*, pages 554–563. ACM, 1994.

[FKPR14] Georg Fuchsbauer, Momchil Konstantinov, Krzysztof Pietrzak, and Vanishree Rao. Adaptive security of constrained PRFs. In Palash Sarkar and Tetsu Iwata, editors, *Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014, Proceedings, Part II*, volume 8874 of *Lecture Notes in Computer Science*, pages 82–101. Springer, 2014.

[GGM84] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions (extended abstract). In *25th Annual Symposium on Foundations of Computer Science, West Palm Beach, Florida, USA, 24-26 October 1984*, pages 464–479. IEEE Computer Society, 1984.

[GIKM00] Yael Gertner, Yuval Ishai, Eyal Kushilevitz, and Tal Malkin. Protecting data privacy in private information retrieval schemes. *J. Comput. Syst. Sci.*, 60(3):592–629, 2000.

[GKW15] Romain Gay, Iordanis Kerenidis, and Hoeteck Wee. Communication complexity of conditional disclosure of secrets and attribute-based encryption. In Rosario Gennaro and Matthew Robshaw, editors, *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part II*, volume 9216 of *Lecture Notes in Computer Science*, pages 485–502. Springer, 2015.

[GMW15] Romain Gay, Pierrick Méaux, and Hoeteck Wee. Predicate encryption for multi-dimensional range queries from lattices. In Jonathan Katz, editor, *Public-Key Cryptography - PKC 2015 - 18th IACR International Conference on Practice and Theory in Public-Key Cryptography, Gaithersburg, MD, USA, March 30 - April 1, 2015, Proceedings*, volume 9020 of *Lecture Notes in Computer Science*, pages 752–776. Springer, 2015.

[IK97] Yuval Ishai and Eyal Kushilevitz. Private simultaneous messages protocols with applications. In *Fifth Israel Symposium on Theory of Computing and Systems, ISTCS 1997, Ramat-Gan, Israel, June 17-19, 1997, Proceedings*, pages 174–184. IEEE Computer Society, 1997.

[KPTZ13] Aggelos Kiayias, Stavros Papadopoulos, Nikos Triandopoulos, and Thomas Zacharias. Delegatable pseudorandom functions and applications. In Ahmad-Reza Sadeghi, Virgil D. Gligor, and Moti Yung, editors, *2013 ACM SIGSAC Conference on Computer* *and Communications Security, CCS'13, Berlin, Germany, November 4-8, 2013*, pages 669–684. ACM, 2013.

[LV18] Tianren Liu and Vinod Vaikuntanathan. Breaking the circuit-size barrier in secret sharing. In Ilias Diakonikolas, David Kempe, and Monika Henzinger, editors, *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2018, Los Angeles, CA, USA, June 25-29, 2018*, pages 699–708. ACM, 2018.

[LVW17] Tianren Liu, Vinod Vaikuntanathan, and Hoeteck Wee. Conditional disclosure of secrets via non-linear reconstruction. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part I*, volume 10401 of *Lecture Notes in Computer Science*, pages 758–790. Springer, 2017.

[SBC$^+$07] Elaine Shi, John Bethencourt, Hubert T.-H. Chan, Dawn Xiaodong Song, and Adrian Perrig. Multi-dimensional range query over encrypted data. In *2007 IEEE Symposium on Security and Privacy (S&P 2007), 20-23 May 2007, Oakland, California, USA*, pages 350–364. IEEE Computer Society, 2007.

[Tsa19] Rotem Tsabary. Fully secure attribute-based encryption for t-CNF from LWE. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part I*, volume 11692 of *Lecture Notes in Computer Science*, pages 62–85. Springer, 2019.

[Wee14] Hoeteck Wee. Dual system encryption via predicate encodings. In Yehuda Lindell, editor, *Theory of Cryptography - 11th Theory of Cryptography Conference, TCC 2014, San Diego, CA, USA, February 24-26, 2014. Proceedings*, volume 8349 of *Lecture Notes in Computer Science*, pages 616–637. Springer, 2014.