Same Point Composable and Nonmalleable Obfuscated Point Functions

Peter Fenteany and Benjamin Fuller

University of Connecticut
Email: {benjamin.fuller,peter.fenteany}@uconn.edu

Abstract. A point obfuscator is an obfuscated program that indicates if a user enters a previously stored password. A digital locker is stronger: outputting a key if a user enters a previously stored password. The real-or-random transform allows one to build a digital locker from a composable point obfuscator (Canetti and Dakdouk, Eurocrypt 2008).
Ideally, both objects would be nonmalleable, detecting adversarial tampering. Appending a non-interactive zero knowledge proof of knowledge adds nonmalleability in the common random string (CRS) model.
Komargodski and Yogev (Eurocrypt, 2018) built a nonmalleable point obfuscator without a CRS. We show a lemma in their proof is false, leaving security of their construction unclear. Bartusek, Ma, and Zhandry (Crypto, 2019) used similar techniques and introduced another nonmalleable point function; their obfuscator is not secure if the same point is obfuscated twice. Thus, there was no composable and nonmalleable point function to instantiate the real-or-random construction.
Our primary contribution is a nonmalleable point obfuscator that can be composed any polynomial number of times with the same point (which must be known ahead of time). Security relies on the assumption used in Bartusek, Ma, and Zhandry. This construction enables a digital locker that is nonmalleable with respect to the input password.
As a secondary contribution, we introduce a key encoding step to detect tampering on the key. This step combines nonmalleable codes and seed-dependent condensers. The seed for the condenser must be public and not tampered, so this can be achieved in the CRS model. The password distribution may depend on the condenser's seed as long as it is efficiently sampleable. This construction is black box in the underlying point obfuscation.
Nonmalleability for the password is ensured for functions that can be represented as low degree polynomials. Key nonmalleability is inherited from the class of functions prevented by the nonmalleable code.
Keywords: Digital lockers; Point obfuscation; Virtual black-box obfuscation; Nonmalleable codes; Seed-dependent condensers; Nonmalleability

1 Introduction

Obfuscation hides the implementation of a program from all users of the program. This work is concerned with *virtual black-box obfuscation*, where an obfuscator creates a program that reveals nothing about the program other than

its input and output behavior [BGI+01,BGI+12]. Barak et al. showed that a virtual black-box obfuscator cannot exist for all polynomial time circuits [BGI+01]. However, this leaves open the possibility of virtual black-box obfuscators for interesting classes of programs [CD08,BC10,CRV10,WZ17,BR17].[1]

We focus on *obfuscated point functions* [Can97] and *digital lockers* [CD08] [BC10]. A *point function obfuscator* is an algorithm $\mathsf{lockP}(\mathsf{val})$ which outputs a circuit $\mathsf{ulockP}_{\mathsf{val}}(\cdot)$. The circuit $\mathsf{ulockP}_{\mathsf{val}}(\cdot)$ stores val and indicates when val is inputted to it. An obfuscated point function needs to hide all partial information about val [Can97].

A digital locker obfuscator inputs a value, val, and key, key. The output is a program $\mathsf{ulock}_{\mathsf{val},\mathsf{key}}(\cdot)$ which outputs key if and only if the input is val. Soundness says $\mathsf{ulock}_{\mathsf{val},\mathsf{key}}$ should reveal nothing about val or key if the adversary cannot guess val. Digital lockers have applications in password [Can97] and biometric authentication [CFP+16,ABC+18].

The *real-or-random* construction composes point functions to build a digital locker [CD08]. It works as so: sample a random point r. For each bit of the key, either r (corresponding to a 0 in key) or val (corresponding to a 1) is obfuscated. An obfuscation of val is prepended as a check value. When running the program, if the check obfuscation opens, the user runs the other programs: failures to open correspond to a key bit 0 and successes correspond to a key bit of 1. The point function must retain security when val is obfuscated multiple times.

Nonmalleability A desirable property of an obfuscated program is nonmalleability. A *nonmalleable* obfuscator detects if an adversary attempts to tamper the obfuscation into a related program [CV09], where being related is defined by some family of functions $\mathcal{F}$. For example, it is desirable to prevent $\mathsf{ulock}_{\mathsf{val},\mathsf{key}}$ from being mauled to $\mathsf{ulock}_{f(\mathsf{val}),f'(\mathsf{key})}$ for $f, f' \in \mathcal{F}$.

In the random oracle model, designing nonmalleable digital lockers and point functions is easy: For a random oracle RO one outputs the program $\mathsf{RO}(\mathsf{val}) \oplus (\mathsf{key}||\mathsf{RO}'(\mathsf{key}))$, where RO and RO' are two independent random oracles of different output length. Similarly, using general non-interactive zero-knowledge proofs of knowledge (NIZKPoKs) in the common random string (CRS) model one can achieve nonmalleability. For $\mathsf{ulock}_{\mathsf{val},\mathsf{key}}(\cdot)$, appending a NIZKPoK of key and val would prevent the adversary from creating a valid obfuscation for any point related to the inputs.[2]

Komargodski and Yogev constructed a nonmalleable point obfuscator without resorting to these tools [KY18a]. Their construction follows. Let g be a fixed group generator. To obfuscate the point val, the obfuscator computes a random r and outputs

$$\mathsf{lockP}(\mathsf{val}) = \left(r, r^{g^{\sum_{i=1}^{4} \mathsf{val}^i}}\right).$$

[1] We do not consider indistinguishability obfuscation in this work [GGH+13,GGH+16,SW14,PST14,GLSW15,AJ15].

[2] The adversary can always substitute an obfuscation on an unrelated point. Thus, it is possible to create obfuscations for functions f where $f(\mathsf{val})$ is easy to guess.

We observe that nonmalleability of Komargodski and Yogev's scheme relies on an incorrect lemma in a way that is not apparently repairable. We discuss this in detail below.

Bartusek, Ma, and Zhandry [BMZ19] using similar mathematical structure showed a nonmalleable point function using random a, b, c:

$$\mathsf{lockP}(\mathsf{val}) = a, g^{a\cdot\mathsf{val}+(\mathsf{val})^2+(\mathsf{val})^3+(\mathsf{val})^4+(\mathsf{val})^5}, b, g^{b\cdot\mathsf{val}+(\mathsf{val})^6}, c, g^{c\cdot\mathsf{val}+(\mathsf{val})^7}.$$

The structure of the group element is similar to Komargodski and Yogev's construction, but with a random scalar in place of "double exponentiation." The terms involving b and c ensure no incorrect point causes the obfuscation to unlock. In both constructions, g is assumed to be fixed; this means the distribution of val may depend on generator g. Bartusek, Ma, and Zhandry [BMZ19] show security based on new Diffie-Hellman variants and show these variants hold in the generic group model, using tools from the auxiliary input generic group model [CDG18].

The natural nonmalleability definition is that, given $\mathsf{ulockP}_{\mathsf{val}}$, an adversary can only output the same obfuscation or obfuscations of independent points. The above constructions use a weaker definition. Given an obfuscation $\mathsf{lockP}_{\mathsf{val}}$, the adversary is required to output a function f and an obfuscation $\mathsf{lockP}_{f(\mathsf{val})}$. That is, the definition requires the adversary to *know* what tampering function they are applying. Both constructions consider f as a polynomial of bounded degree related to the assumed hardness in the DDH assumptions. The definition considers the tampering functions prevented, not what operations are performed by the adversary.

The goal of this work is to construct nonmalleable digital lockers. The real-or-random construction instantiated with nonmalleable point functions would provide nonmalleability over val. Crucially, this construction requires security to hold when the nonmalleable point functions are *composed* though only with the same val. Both previous constructions have issues that prevent incorporation. The proof of nonmalleability for [KY18a] relies on an untrue lemma and the proof does not seem easily repairable, and the construction of [BMZ19] cannot be composed twice or more. We discuss these issues and then introduce our contribution.

[KY18b, Lemma 4.6] is not true Let g be a fixed generator of a group. The version of Komargodski and Yogev published in Eurocrypt 2018 [KY18a] relied on a *fixed generator* power DDH assumption which says for any distribution x with super logarithmic entropy (here the distribution of x can depend on generator g) that

$$g, g^x, g^{x^2}, ..., g^{x^t} \approx_c g, g^{u_1}, g^{u_2}, ..., g^{u_t},$$

for a truly random set of elements $u_1, ..., u_t$. This assumption is used in the proof by assuming that the adversary sees $\sum_{i=1}^{4} u_i$ and arguing they can't predict any linear combinations other than $c\sum_{i=1}^{4} u_i$ for some constant c. However, Bartusek, Ma, and Zhandry [BMZ19] showed that for a fixed generator this

assumption cannot be true: x can be drawn from points where most bits of g^x are fixed. As a result, a revised version [KY18b] proposes a revised assumption called entropic power where

$$g, g^x, g^{x^2}, ..., g^{x^t} \approx_c g, g^{z_1}, g^{z_2}, ..., g^{z_t}.$$

Where z_i are independent and have some super logarithmic min-entropy. This assumption does not appear to suffice. In particular, [KY18b, Lemma 4.6] is incorrect as stated. The lemma states it is hard to predict linear combinations of z_i other than $c\sum_{i=1}^{4} z_i$ for any constant c, even knowing $\sum_{i=1}^{4} z_i$. However, even if each z_i has entropy, the value $\sum_{i=1}^{4} z_i$ may uniquely determine each z_i: let z_i vary in the ith quarter of bits and fix the rest of bits to be 0. The attack of [BMZ19] prevents arguing that z_i has any greater amount of entropy.

This does not seem to be an issue of just the proof technique. The point of the entropic power assumption is to switch to an information-theoretic setting where the adversary cannot predict new powers from a linear combination, but bounding the entropy of each z_i may cause all powers to be predictable. Repairing this scheme seems to require a new Diffie-Hellman assumption or a major change in analysis.

[BMZ19] is not composable One might try to compose the construction of Bartusek et al. [BMZ19]. However, this scheme is not secure even when used twice for the same val. The hardness of finding g^x is the underlying assumption used to show nonmalleability [BMZ19, Assumption 4]. Since the distribution of x may depend on g, one can construct distributions x where g^x is distinguishable from a random group element g^r. If one can find g^x, the scheme can not be secure. If one tries to obfuscate the same point x twice, all the higher order terms can be removed by dividing two instances. That is, given

$$a_1, g_1 = g^{a_1 x + x^2 + x^3 + x^4 + x^5}$$
$$a_2, g_2 = g^{a_2 x + x^2 + x^3 + x^4 + x^5}$$

one can easily compute $g^{(a_1 - a_2)x} = g_1/g_2$, and recover $g^x = (g_1/g_2)^{(a_1 - a_2)^{-1}}$.

1.1 Our Contribution

The primary contribution of this work is the first same-point composable nonmalleable point function. The composable, nonmalleable point function can instantiate the real-or-random construction providing a nonmalleable digital locker that prevents tampering over val only. This construction is in the standard model.

As a secondary contribution, we introduce a key encoding step to detect tampering on key. The key encoding step allows us to achieve a digital locker that is nonmalleable over both val and key. However, our key encoding step requires a public value that all distributions can depend on. This can be achieved in the common random string (CRS) model. In our construction the distribution of val

can depend on the public value. In the CRS model, one can achieve nonmalleability in a non-black box way using non-interactive zero knowledge proofs of knowledge [CV09].

Composable Same Point Nonmalleable Point Function Obfuscation We introduce a new nonmalleable point function that can be safely composed τ times as long as the *same point* is obfuscated each time. The construction builds on the one-time scheme of Bartusek et al. [BMZ19]. We include additional randomized powers to prevent the above attack. The construction needs to know the desired composition parameter τ ahead of time. The value τ would be known in the case when a point function is being used to construct a digital locker. Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}$ be uniform vectors of length τ. The construction is as follows:

$$\mathsf{lockP}(x; \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}) \stackrel{def}{=} \begin{bmatrix} \boldsymbol{a}, & g^{\sum_{i=1}^{\tau} \boldsymbol{a}_i x^i + \sum_{i=\tau+1}^{\tau+5} x^i}, \\ \boldsymbol{b}, & g^{\boldsymbol{b}_1 x + \sum_{i=2}^{\tau} \boldsymbol{b}_i x^{i+\tau+4} + x^{2\tau+5}}, \\ \boldsymbol{c}, & g^{\boldsymbol{c}_1 x + \sum_{i=2}^{\tau} \boldsymbol{c}_i x^{i+2\tau+4} + x^{3\tau+5}}. \end{bmatrix}$$

The intuition for the formation of the first group element is that we need to randomize more powers to prevent the adversary from removing the higher order powers and being able to linear solve for g^x. Since the adversary can create $\tau - 1$ linearly independent pairs, τ randomized powers are necessary. We add a fifth non-randomized power in the $\boldsymbol{a}$ term to deal with the additional flexibility created by τ. The crucial step in the proof is showing that some linear system has no interesting solutions, the extra power is to counteract the degree of freedom introduced by τ (see Theorem 2).

The intuition for the $\boldsymbol{b}$ and $\boldsymbol{c}$ terms is similar. Due to our proof technique, we need to randomize different powers for the $\boldsymbol{a}$ term, the $\boldsymbol{b}$ term, and the $\boldsymbol{c}$ term, resulting in the above construction. All terms have a randomized x^1 coefficient so we can reduce to [BMZ19, Assumption 4].

We can instantiate the real-or-random construction with this construction to yield a nonmalleable digital locker that only provides nonmalleability over the locked val. As mentioned above, one could prove knowledge (using a NIZKPoK) of just key to prevent modification of this value. Such a method would inherently depend on the underlying point function. Our goal is to avoid general NIZKPoKs.

Detecting Key Tampering Our strategy is to use nonmalleable codes [DPW10]. We use nonmalleable codes in a nonstandard way: the adversary sees obfuscations that are correlated to the codeword before choosing how to tamper. This seems okay at first glance, correlated obfuscations shouldn't be distinguishable from random obfuscations. If a tampering adversary performs differently in the presence of correlated obfuscations or random obfuscations, if one can check success probability it be turned into a distinguisher.

However, nonmalleable codes don't yield such a check because nonmalleable codes allow the adversary to tamper to an independent value. When using nonmalleable codes in the reduction, one needs to know if the value is independent. Rather than just encoding key we include the output of a seed-dependent condense [DRV12] applied to val, $\mathtt{cond}(\mathsf{val})$, as part of the encoded value. This allows

us to argue that an adversary that succeeds in mauling the nonmalleable code more frequently when presented with correlated obfuscations breaks soundness of the obfuscation. However, this change necessitates that the seed of the condenser is public and not tampered. This can be achieved in the CRS model.

Our construction does not assume independence of distributions from the random object. The CRS is only necessary for preventing tampering of key, the real-or-random construction prevents tampering of val in the standard model. We discuss alternative tools in Section 4.

Organization In Section 2, we present definitions. In Section 3, we introduce the composable nonmalleable point function. In Section 4, we present the real-or-random digital locker construction and add checks for key tampering.

2 Preliminaries

For random variables X_i over some alphabet $\mathcal{Z}$ we denote by $X = X_1, ..., X_n$ the tuple $(X_1, \ldots, X_n)$. For a set of indices J, X_J is the restriction of X to the indices in J. The *minentropy* of X is $\mathrm{H}_\infty(X) = -\log(\max_x \Pr[X = x])$, and the *average (conditional) minentropy* [DORS08, Section 2.4] of X given Y is $\tilde{\mathrm{H}}_\infty(X|Y) = -\log\left(\mathbb{E}_{y\in Y} \max_x \Pr[X = x|Y = y]\right)$. For a distinguisher D, the *computational distance* between X and Y is $\delta^D(X, Y) = |\mathbb{E}[D(X)] - \mathbb{E}[D(Y)]|$ (we extend it to a class of distinguishers $\mathcal{D}$ by taking the maximum over all distinguishers $D \in \mathcal{D}$). We denote by $\mathcal{D}_s$ the class of randomized circuits which output a single bit and have size at most s. Logarithms are base 2. In general, capitalized letters are used for random variables and the corresponding lowercase letters for their samples. We say that two circuits, C and C', with inputs in $\{0,1\}^\lambda$ are equivalent if $\forall x \in \{0,1\}^\lambda, C(x) = C'(x)$. We denote this as $C \equiv C'$. For a matrix $\mathbf{A}$ let $\mathbf{A}_{i,j}$ denote the entry in the ith row and the jth column. Let $\mathbf{A}_{(\cdot,j)}$ represent the jth column and $\mathbf{A}_{(i,\cdot)}$ represent the ith row.

Definition 1. *An ensemble of distributions $\mathcal{X} = \{X_\lambda\}_{\lambda\in\mathbb{N}}$, where $\mathcal{X}_\lambda$ is over $\{0,1\}^\lambda$, is* well-spread *if*

1. *It is efficiently and uniformly samplable. That is, there exists a PPT algorithm given 1^λ as input whose output is identically distributed as X_λ.*
2. *For all large enough $\lambda \in \mathbb{N}$, it has super-logarithmic minentropy. Namely, $\mathrm{H}_\infty(X_\lambda) = \omega(\log \lambda)$.*

Obfuscation Definitions All obfuscation definitions include a requirement of *polynomial slowdown*, which says the running time should be at most a polynomial factor larger than the original program. Running time of our constructions can be easily verified. For all definitions, we include a tampering function $\mathcal{F}$. The traditional definition can be achieved by taking $\mathcal{F} = \emptyset$. We adapt nonmalleability definitions from Komargodski and Yogev [KY18a]. See Komargodski and Yogev for definitional considerations [KY18a].

Our constructions require that the challenger can recognize a legitimate obfuscation. We call this object a value verifier or $\mathsf{V}_{\mathsf{val}}$. It was called a verifier (without the word value) in [KY18a].

Definition 2 (Value Verifier). *Let $\lambda \in \mathbb{N}$ be a security parameter. Let $\mathcal{O}$ be a program that takes inputs $x \in \{0,1\}^\lambda$ and outputs a program $\mathcal{P}$. A PPT algorithm $\mathsf{V}_{\mathsf{val}}$ is called a* value verifier *if for all $x \in \{0,1\}^\lambda$, it holds that $\Pr[\mathsf{V}_{\mathsf{val}}(\mathcal{P}) = 1 | \mathcal{P} \leftarrow \mathcal{O}(x)] = 1$, (prob. over the randomness of $\mathsf{V}_{\mathsf{val}}$ and $\mathcal{O}$).*

Our constructions consist of tuples of group elements and strings. The obvious value verifier suffices as long as group elements are recognizable. A point function is a function I_{val}: $\{0,1\}^n \mapsto \{0,1\}$ that outputs 1 on input val and 0 elsewhere. An obfuscator preserves functionality while hiding the point val if val is not provided as input to the program. In this work we consider a version that allows for the same point to be obfuscated multiple times while retaining security.

Definition 3 (τ-Same Point Nonmalleable Point Function). *For security parameter $\lambda \in \mathbb{N}$, let $\mathcal{F} : \{0,1\}^\lambda \to \{0,1\}^\lambda$ be a family of functions, let $\mathcal{X}$ be a family of distributions over $\{0,1\}^\lambda$. A $(\mathcal{F}, \mathcal{X})$-*non malleable point function obfuscation lockP *is a PPT algorithm that inputs a point $\mathsf{val} \in \{0,1\}^\lambda$, and outputs a circuit ulockP. Let $\mathsf{V}_{\mathsf{val}}$ be a value verifier for lockP as defined in Definition 2. The following properties must hold:*

1. ***Completeness**: For all $\mathsf{val} \in \{0,1\}^\lambda$, it holds that*

$$\Pr[\mathsf{ulockP}(\cdot) \equiv I_{\mathsf{val}}(\cdot) | \mathsf{ulockP} \leftarrow \mathsf{lockP}(\mathsf{val})] \geq 1 - \mathtt{ngl}(\lambda),$$

   where the probability is over the randomness of lockP.
2. ***Soundness**: For every PPT $\mathcal{A}$ and any polynomial function p, there exists a simulator $\mathcal{S}$ and a polynomial $q(\lambda)$ such that, for all large enough $\lambda \in \mathbb{N}$, all $\mathsf{val} \in \{0,1\}^\lambda$ and for any predicate $\mathcal{P} : \{0,1\}^\lambda \mapsto \{0,1\}$,*

$$\begin{aligned} &|\Pr[\mathcal{A}(\{\mathsf{ulockP}_i\}_{i=1}^\tau) = \mathcal{P}(\mathsf{val}) | \{\mathsf{ulockP}_i\}_{i=1}^\tau \leftarrow \mathsf{lockP}(\mathsf{val})] \\ &- \Pr[\mathcal{S}^{I_{\mathsf{val}}(\cdot)}(1^\lambda) = \mathcal{P}(\mathsf{val})]| \leq \frac{1}{p(\lambda)}, \end{aligned}$$

   where S is allowed $q(\lambda)$ oracle queries to I_{val} and the probabilities are over the internal randomness of $\mathcal{A}$ and lockP, and of $\mathcal{S}$, respectively. Here $I_{\mathsf{val}}(\cdot)$ is an oracle that returns 1 when provided input val and 0 otherwise.
3. ***Nonmalleability** For any $X \in \mathcal{X}$, for any PPT $\mathcal{A}$, there exists $\epsilon = \mathtt{ngl}(\lambda)$, such that:*

$$\Pr_{\mathsf{val} \leftarrow X}\left[\mathsf{V}_{\mathsf{val}}(C) = 1, f \in \mathcal{F}, (I_{f(\mathsf{val})} \equiv C) \,\middle|\, \begin{matrix} \{\mathsf{ulockP}_i\}_{i=1}^\tau \leftarrow \mathsf{lockP}(\mathsf{val}) \\ (C, f) \leftarrow \mathcal{A}(\{\mathsf{ulockP}_i\}_{i=1}^\tau) \end{matrix}\right] \leq \epsilon.$$

In the above ulockP_i are τ outputs of lockP on the same input point val and independent randomness. Note that the simulator is still only provided with a single oracle. In usual composition definitions the simulator has τ oracles. Since we consider the same point being obfuscated multiple times, all of these oracles would have the same functionality and can be reduced to a single oracle.

In addition to the above traditional definition of soundness, in the full version [FF18, Section 2.1] we introduce two auxiliary definitions of privacy for

nonmalleable point functions. These are known as distributional indistinguishability and oracle indistinguishability (both first defined in [Can97]). We show those definitions are equivalent to soundness. We use these two auxiliary definitions in the proof of Theorem 1. We now present our definition of a nonmalleable digital locker. Our notation for digital lockers adds a key verifier which checks if the key should be accepted. This is analogous to the value verifier in the previous subsection:

Definition 4 (Key Verifier). *Let $\lambda \in \mathbb{N}$ be a security parameter and let $n = n(\lambda)$ be a parameter. Let $\mathcal{O}$ be a program that takes inputs $x \in \{0,1\}^\lambda, y \in \{0,1\}^k$ and outputs a program $\mathcal{P}$. A PPT algorithm $\mathsf{V}_{\mathsf{key}}$ (with inputs in $\{0,1\}^{\lambda+n}$ and outputs in $\{0,1\}^k \cup \perp$) for program class $\mathcal{O}$ is called a* key verifier *if it holds that $\Pr[\mathsf{V}_{\mathsf{key}}(x,z) \neq \perp \,|\mathcal{P} \leftarrow \mathcal{O}(x,y), z \leftarrow \mathcal{P}(x)] = 1$, where the probability is over the randomness of $\mathsf{V}_{\mathsf{key}}$ and $\mathcal{O}$).*

Note the three different values x, y, z. The value x is the input value, y is the input key, and z as an encoded version of the key. The output of the locker is z which is then checked. There must be an independent algorithm that checks z otherwise no manipulation detection is possible. A definition for traditional digital lockers is found in Canetti and Dakdouk [CD08]. Our definition considers tampering on both key and val.

Definition 5 (Nonmalleable Digital Locker). *For security parameter $\lambda \in \mathbb{N}$, Let $\mathcal{F} : \{0,1\}^\lambda \to \{0,1\}^\lambda, \mathcal{G} : \{0,1\}^n \to \{0,1\}^n$ be families of functions and $\mathcal{X}$ be a family of distributions over $\{0,1\}^\lambda$. A $(\mathcal{F}, \mathcal{G}, \mathcal{X})$-nonmalleable* digital locker lock *is a PPT algorithm that inputs a point $\mathsf{val} \in \{0,1\}^\lambda$ and string $\mathsf{key} \in \{0,1\}^n$. Let $\mathsf{V}_{\mathsf{val}}$ be a value verifier for lock and let $\mathsf{V}_{\mathsf{key}}$ be a key verifier for lock. The following conditions must be met:*

1. ***Completeness**: For a circuit ulock define the circuit $\mathsf{ulock}'(x) = \mathsf{V}_{\mathsf{key}}(x, \mathsf{ulock}(x))$. For all $\mathsf{val} \in \{0,1\}^\lambda, \mathsf{key} \in \{0,1\}^n$ it holds that*

$$\Pr[\mathsf{ulock}'(\cdot) \equiv I_{\mathsf{val},\mathsf{key}}(\cdot) | \mathsf{ulock} \leftarrow \mathsf{lock}(\mathsf{val}, \mathsf{key})] \geq 1 - \mathtt{ngl}(\lambda),$$

   where the probability is over the randomness of lock.
2. ***Soundness**: For every PPT $\mathcal{A}$ and any polynomial function p, there exists a simulator $\mathcal{S}$ and a polynomial $q(\lambda)$ such that, for all large enough $\lambda \in \mathbb{N}$, all $\mathsf{val} \in \{0,1\}^\lambda$, all $\mathsf{key} \in \{0,1\}^k$, and for any $\mathcal{P} : \{0,1\}^{\lambda+k} \mapsto \{0,1\}$,*

$$\left|\Pr[\mathcal{A}(\mathsf{lock}(\mathsf{val}, \mathsf{key})) = \mathcal{P}(\mathsf{val}, \mathsf{key})] - \Pr[\mathcal{S}^{I_{\mathsf{val},\mathsf{key}}}(1^\lambda) = \mathcal{P}(\mathsf{val}, \mathsf{key})]\right| \leq \frac{1}{p(\lambda)},$$

   where S is allowed $q(\lambda)$ oracle queries to $I_{\mathsf{val},\mathsf{key}}$ and the probabilities are over the internal randomness of $\mathcal{A}$ and lock, and of $\mathcal{S}$, respectively. Here $I_{\mathsf{val},\mathsf{key}}$ is an oracle that returns key when provided input val, otherwise $I_{\mathsf{val},\mathsf{key}}$ returns $\perp$.

3. ***Nonmalleability*** *For any distribution $X \in \mathcal{X}$, for any PPT $\mathcal{A}$, for any $\mathsf{key} \in \{0,1\}^n$, there exists $\epsilon = \mathtt{ngl}(\lambda)$ such that:*

$$\Pr_{\mathsf{val} \leftarrow X}\left[\begin{array}{r|l} \mathsf{V}_{\mathsf{val}}(C) = 1, f \in \mathcal{F}, g \in \mathcal{G}, & \\ y = C(f(\mathsf{val})), & \\ y = g(\mathsf{ulock}_{\mathsf{val},\mathsf{key}}(\mathsf{val})), & \mathsf{ulock}_{\mathsf{val},\mathsf{key}} \leftarrow \mathsf{lock}(\mathsf{val},\mathsf{key}) \\ \mathsf{V}_{\mathsf{key}}(f(\mathsf{val}), y) \neq \perp, & (C,f,g) \leftarrow \mathcal{A}(\mathsf{ulock}_{\mathsf{val},\mathsf{key}}) \\ \exists \alpha \text{ s.t. } I_{f(\mathsf{val}),\alpha} \equiv C & \end{array}\right] \leq \epsilon.$$

where at most one of f and g may be the identity function.

If nonmalleability is not a requirement a traditional digital locker can be obtained by outputting $\mathsf{ulock}'(x) = \mathsf{V}_{\mathsf{key}}(x, \mathsf{ulock}(x))$ instead of $\mathsf{ulock}(x)$.

3 A composable nonmalleable point function

In this section, we introduce a new construction of a nonmalleable point function that can be composed as long as the same point is used each time. Our construction draws on ideas from [BMZ19] and is secure under the same assumptions. Their construction is as follows for randomly sampled a, b, c:

$$\mathsf{lockP}(\mathsf{val}) = a, g^{a\cdot\mathsf{val}+(\mathsf{val})^2+(\mathsf{val})^3+(\mathsf{val})^4+(\mathsf{val})^5}, b, g^{b\cdot\mathsf{val}+(\mathsf{val})^6}, c, g^{c\cdot\mathsf{val}+(\mathsf{val})^7}.$$

The first group element is the key to nonmalleability, the second two group elements are there to provide correctness. Security of their construction and ours relies on two assumptions (they showed security of these assumptions in the generic group model even if the distribution of val depends on the chosen generator of the group).

Assumption 1 *[BMZ19, Assumption 3] Let $\mathcal{G} = \{\mathbb{G}_\lambda\}_{\lambda\in\mathbb{N}}$ be a group ensemble with efficient representation and operations where each $\mathbb{G}_\lambda$ is a group of prime order $p \in (2^\lambda, 2^{\lambda+1})$. We assume that for every $\lambda \in \mathbb{N}$ there is a canonical group (and efficiently computable) and canonical and efficient mapping between the elements of $\{0,1\}^\lambda$ to $\mathbb{G}_\lambda$. Let $\{\mathcal{X}_\lambda\}$ be a family of well-spread distributions over $\{0,1\}^\lambda$. Then for any $\ell = \mathtt{poly}(\lambda)$ for any PPT $\mathcal{A}$:*

$$\left|\Pr[\mathcal{A}(\{k_i, g^{k_i x + x^i}\}_{i\in[2,\ldots,\ell]} = 1] - \Pr[\mathcal{A}(\{k_i, g^{k_i r + r^i}\}_{i\in[2,\ldots,\ell]}\right| = \mathtt{ngl}(\lambda).$$

where $x \leftarrow \mathcal{X}_\lambda, r \leftarrow \mathbb{Z}_{p(\lambda)}, k_i \leftarrow \mathbb{Z}_{p(\lambda)}$.

The second assumption can be proved from Assumption 1, see [BMZ19, Lemma 8], and is useful for arguing nonmalleability:

Assumption 2 *[BMZ19, Assumption 4] Let $\mathcal{G}$ and $\mathcal{X}_\lambda$ be defined as in Assumption 1. Then for any $\ell = \mathtt{poly}(\lambda)$ for any PPT $\mathcal{A}$:*

$$\Pr[g^x \leftarrow \mathcal{A}(\{k_i, g^{k_i x + x^i}\}_{i\in[2,..,\ell]} = \mathtt{ngl}(\lambda).$$

where $x \leftarrow \mathcal{X}_\lambda$ and $k_i \leftarrow \mathbb{Z}_{p(\lambda)}$.

We now introduce our main construction. The intuition behind the construction is to increase the number of randomized powers to deal with the additional constraints on val that the adversary gains by seeing multiple copies; it will be proved secure under Assumptions 1 and 2.

Construction 1 *Let $\lambda \in \mathbb{N}$ be a security parameter. Let $\mathcal{G} = \{\mathbb{G}_\lambda\}_{\lambda\in\mathbb{N}}$ be a group ensemble with efficient representation and operations where each $\mathbb{G}_\lambda$ is a group of prime order $p \in (2^\lambda, 2^{\lambda+1})$. We assume that for every $\lambda \in \mathbb{N}$ there is a canonical and efficient mapping between the elements of $\{0,1\}^\lambda$ to $\mathbb{G}_\lambda$. Let g be a generator of the group $\mathbb{G}_\lambda$. For some parameter $\tau \in \mathbb{Z}^+$, let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c} \xleftarrow{\$} \mathbb{G}_\lambda$ be input randomness and define the algorithm lockP as:*

$$\mathsf{lockP}(\mathsf{val}; \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}) \stackrel{def}{=} \begin{bmatrix} \boldsymbol{a}, & g^{\sum_{i=1}^{\tau} \boldsymbol{a}_i x^i + \sum_{i=\tau+1}^{\tau+5} x^i} \\ \boldsymbol{b}, & g^{\boldsymbol{b}_1 x + \sum_{i=2}^{\tau} \boldsymbol{b}_i x^{i+\tau+4} + x^{2\tau+5}} \\ \boldsymbol{c}, & g^{\boldsymbol{c}_1 x + \sum_{i=2}^{\tau} \boldsymbol{c}_i x^{i+2\tau+4} + x^{3\tau+5}} \end{bmatrix}.$$

Given a program ulockP consisting of three vectors $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}$ and group elements g_1, g_2, g_3 and input val compute:

$$\begin{aligned} g^{\sum_{i=1}^{\tau} \boldsymbol{a}_i \mathsf{val}^i + \sum_{i=\tau+1}^{\tau+5} \mathsf{val}^i} &\stackrel{?}{=} g_1 \\ g^{\boldsymbol{b}_1 \mathsf{val} + \sum_{i=2}^{\tau} \boldsymbol{b}_i \mathsf{val}^{i+\tau+4} + \mathsf{val}^{2\tau+5}} &\stackrel{?}{=} g_2 \\ g^{\boldsymbol{c}_1 \mathsf{val} + \sum_{i=2}^{\tau} \boldsymbol{c}_i \mathsf{val}^{i+2\tau+4} + \mathsf{val}^{3\tau+5}} &\stackrel{?}{=} g_3. \end{aligned}$$

If all of these checks pass, output 1. Otherwise, output 0.

In order to add same point composability, we extend from three scalars to 3τ scalars (while keeping 3 group elements). We note that this scheme is that of [BMZ19] if we let $\tau = 1$.

Lemma 1. *For any $\tau = \mathtt{poly}(\lambda)$ Construction 1 satisfies completeness.*

Proof. This argument is analogous to the functionality preservation argument in [BMZ19]. The only difference is that polynomials are higher degree due to composition. Fix some point $x \in \mathbb{Z}_{p(\lambda)}$. It suffices to argue that over the randomness of $\mathsf{ulockP} \leftarrow \mathsf{lockP}(x)$ that the probability that there exists some y such that $\mathsf{ulockP}(y) = 1$ is $\mathtt{ngl}(\lambda)$.

Recall that the randomness used to construct ulockP is the vectors $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}$. Fix some $x \in \mathbb{Z}_{p(\lambda)}$. Fix some value $\boldsymbol{a}$ and define $\alpha \stackrel{def}{=} \sum_{i=1}^{\tau} x^i + \sum_{i=\tau+1}^{\tau+5} x^i$. For some other value y, since $\mathcal{G}$ is prime order the only way for the first element to match is for $\alpha = \sum_{i=1}^{\tau} y^i + \sum_{i=\tau+1}^{\tau+5} y^i$. Since this is a polynomial of degree $\tau + 5$ there are at most $\tau + 4$ such values y (excluding the original value x). Consider one such value y. Then, consider the polynomial $P(\boldsymbol{b}) \stackrel{def}{=} \boldsymbol{b}_1(x - y) + \sum_{i=2}^{\tau} \boldsymbol{b}_i(x^{i+\tau+4} - y^{i+\tau+4}) + (x^{2\tau+5} - y^{2\tau+5})$. Fix some values of $\boldsymbol{b}_i$ for $i = 2, ..., \tau$. Then this is a linear polynomial in $\boldsymbol{b}_1$ that is zero with probability at most $1/p(\lambda)$. A similar argument holds for the second check value. Thus, a candidate y is a

solution to both equations with probability $1/p(\lambda)^2$. Thus means for a fixed x the probability of one of the y's working is at most $(\tau+5)/p(\lambda)^2$ by union bound. With a second application of union bound, the probability across all x of some y existing is at most $(\tau+5)/p(\lambda) = \mathtt{ngl}(\lambda)$ as desired.

Theorem 1. *Suppose that Assumption 1 holds. Then for any $\tau = \mathtt{poly}(\lambda)$, Construction 1 satisfies virtual black box security (when composed up to τ times).*

Proof. We show that Construction 1 satisfies distributional indistinguishability [FF18, Definition 2.4]. Virtual black box security then follows by [FF18, Theorem 2.1].

Suppose for the aim of arriving at a contradiction that there exists some well-spread distribution $\mathcal{X}_\lambda$ such that there exists a PPT adversary $\mathcal{A}$ and a polynomial $q(\cdot)$ such that

$$|\Pr[\mathcal{A}(\{\mathsf{lockP}(x)\}_{i=1}^{\tau}) = 1] - \Pr[\mathcal{A}(\{\mathsf{lockP}(r)\}_{i=1}^{\tau}) = 1]| > \frac{1}{q(\lambda)},$$

where $x \leftarrow X_\lambda$ and $r \leftarrow \mathbb{Z}_{p(\lambda)}$. We then show how to build an adversary $\mathcal{B}$ that breaks Assumption 1 (with respect to distribution family $\mathcal{X}_\lambda$) receiving $\ell = 3\tau+4$ elements (corresponding to a maximum power of $3\tau+5$). That is, $\mathcal{B}$ will receive $3\tau+4$ pairs of the form

$$\{k_i, g^{k_i z + z^i}\}_{i \in \{2,\ldots,3\tau+5\}},$$

where z is either distributed according to $\mathcal{X}_\lambda$ or uniformly in $\mathbb{Z}_{p(\lambda)}$. Denote by $\{k_i, g^{h_i}\}_{i=2,\ldots,3\tau+5}$ the received values, defining $h_i = k_i z + z^i$. Then, $\mathcal{B}$ samples three matrices $\mathbf{A}, \mathbf{B}, \mathbf{C}$ uniformly in $\mathbb{Z}_{p(\lambda)}^{\tau \times (\tau-1)}$.

Our goal is to produce τ obfuscations (either of x or r). $\mathcal{B}$ compute the matrices $\mathbf{A}', \mathbf{B}', \mathbf{C}' \in \mathbb{Z}_{p(\lambda)}^{\tau \times \tau}$ as follows:

$$\mathbf{A}'_{i,j} = \begin{cases} \sum_{\alpha=1}^{\tau-1} \mathbf{A}_{i,\alpha} k_{\alpha+1} + \sum_{\alpha=\tau}^{\tau+4} k_{\alpha+1} & j = 1 \\ \mathbf{A}_{i,j-1} & \text{otherwise.} \end{cases}$$

$$\mathbf{B}'_{i,j} = \begin{cases} \sum_{\alpha=1}^{\tau-1} \mathbf{B}_{i,\alpha} k_{\alpha+\tau+5} + k_{2\tau+5} & j = 1 \\ \mathbf{B}_{i,\alpha-1} & \text{otherwise.} \end{cases}$$

$$\mathbf{C}'_{i,j} = \begin{cases} \sum_{\alpha=1}^{\tau-1} \mathbf{C}_{i,\alpha} k_{\alpha+2\tau+5} + k_{3\tau+5} & j = 1 \\ \mathbf{C}_{i,j-1} & \text{otherwise.} \end{cases}$$

Then $\mathcal{B}$ computes the ith value to be fed into $\mathcal{A}$ as:

$$\mathsf{lockP}_i = \begin{cases} \mathbf{A}'_{(i,\cdot)}, & g^{\sum_{j=1}^{\tau-1} \mathbf{A}_{i,j} h_{j+1} + \sum_{j=t}^{\tau+5} h_{j+1}}, \\ \mathbf{B}'_{(i,\cdot)}, & g^{\sum_{j=1}^{\tau-1} \mathbf{B}_{i,j} h_{j+\tau+4} + h_{2\tau+5}}, \\ \mathbf{C}'_{(i,\cdot)}, & g^{\sum_{j=1}^{\tau-1} \mathbf{C}_{i,j} h_{j+2\tau+4} + h_{3\tau+5}}. \end{cases}$$

The above group elements can be formed linearly from the received values $\{k_i, g^{h_i}\}_{i\in[2,\ldots,3\tau+5]}$ and $\mathbf{A}, \mathbf{B}, \mathbf{C}$. For the ith obfuscation, the values produced in the exponent are (omitting the exponential notation):

$$\sum_{j=1}^{\tau-1} \mathbf{A}_{i,j} h_{j+1} + \sum_{j=\tau+1}^{\tau+5} h_j = \left(\sum_{j=1}^{\tau-1} \mathbf{A}_{i,j} k_{j+1} + \sum_{j=\tau}^{\tau+4} k_{j+1}\right) z + \sum_{j=1}^{\tau-1} \mathbf{A}_{i,j} z^{j+1} + \sum_{j=\tau+1}^{\tau+5} z^j,$$

$$\sum_{j=1}^{\tau-1} \mathbf{B}_{i,j} h_{j+\tau+5} + h_{2\tau+5} = \left(\sum_{j=1}^{\tau-1} \mathbf{B}_{i,j} k_{i+\tau+5} + k_{2\tau+5}\right) z + \sum_{j=1}^{\tau-1} \mathbf{B}_{i,j} z^{j+\tau+5} + z^{2\tau+5},$$

$$\sum_{j=1}^{t-1} \mathbf{C}_{i,j} h_{j+2\tau+5} + h_{3\tau+5} = \left(\sum_{j=1}^{\tau-1} \mathbf{C}_{i,j} k_{i+2\tau+5} + k_{3\tau+5}\right) z + \sum_{j=1}^{\tau-1} \mathbf{C}_{i,j} z^{j+2\tau+5} + z^{3\tau+5}.$$

From the above equations, it is apparent that the matrices $\mathbf{A}', \mathbf{B}', \mathbf{C}'$ are consistent with the group elements. Furthermore it is clear for $j > 1$ that the coefficients for z^j are appropriately formed. It remains to show that the 3τ coefficients of z are uniformly random. Denote by ζ_i for $i = 1, ..., 3\tau$ coefficients of z respectively. Let $\mathbf{1}^{i,j}$ represent an all 1 matrix of dimension $i \times j$ and define $\mathbf{0}^{i\times j}$ similarly. Define the matrix of coefficients:

$$\mathbf{D} \stackrel{def}{=} \left(\begin{array}{c|c|c|c|c|c} \mathbf{A}_{(\cdot,1)} & \mathbf{A}_{(\cdot,2,\ldots,t-1)} & \mathbf{1}^{\tau\times 5} & \mathbf{0}^{\tau\times\tau-5} & \mathbf{0}^{\tau\times 1} & \mathbf{0}^{\tau\times\tau-1} & \mathbf{0}^{\tau\times 1} \\ \hline \mathbf{B}_{(\cdot,1)} & \mathbf{0}^{\tau\times\tau-1} & \mathbf{0}^{\tau\times 5} & \mathbf{B}_{(\cdot,2,\ldots,t-1)} & \mathbf{1}^{\tau\times 1} & \mathbf{0}^{\tau\times\tau-1} & \mathbf{0}^{\tau\times 1} \\ \hline \mathbf{C}_{(\cdot,1)} & \mathbf{0}^{\tau\times\tau-1} & \mathbf{0}^{\tau\times 5} & \mathbf{0}^{\tau\times\tau-5} & \mathbf{0}^{\tau\times 1} & \mathbf{C}_{(\cdot,2,\ldots,t-1)} & \mathbf{1}^{\tau\times 1} \end{array}\right).$$

The set of values received by the adversary can be described by:

$$\mathbf{D} \begin{bmatrix} k_2 \\ k_2 \\ \ldots \\ k_{3t+5} \end{bmatrix} = \begin{bmatrix} \zeta_1 \\ \zeta_2 \\ \ldots \\ \zeta_{3t} \end{bmatrix}$$

The matrix $\mathbf{D}$ has dimension $3\tau \times 3\tau + 5$. For each coefficient ζ_j to be random it suffices for the matrix $\mathbf{D}$ to have row rank of 3τ. For $\mathbf{D}$ to have rank 3τ it suffices for each $\mathbf{A}||\mathbf{1}, \mathbf{B}|\mathbf{1}, \mathbf{C}||\mathbf{1}$ to have rank of τ. Since each matrix is random this occurs with probability at most $\tau/p = \mathtt{ngl}(\lambda)$. If one these matrices is not full rank, $\mathcal{B}$ aborts and outputs a random value. Conditioning on these matrices being full rank the obfuscation are properly prepared for $\mathcal{A}$. Denote by

$$\mathtt{Disting}_{\mathcal{A}} \stackrel{def}{=} |\Pr[\mathcal{A}(\{\mathsf{lockP}(x)\}_{i=1}^{\tau}) = 1] - \Pr[\mathcal{A}(\{\mathsf{lockP}(r)\}_{i=1}^{\tau}) = 1]|.$$

Then one has that

$$\begin{aligned} \left|\Pr[\mathcal{B}(\{k_i, g^{k_i x + x^i}\}_{i\in[2,\ldots,3\tau+4]} = 1] - \Pr[\mathcal{B}(\{k_i, g^{k_i r + r^i}\}_{i\in[2,\ldots,3\tau+4]}\right| = \\ \Pr[\mathbf{A} \vee \mathbf{B} \vee \mathbf{C} \text{ not full rank}] + \Pr[\mathbf{A} \wedge \mathbf{B} \wedge \mathbf{C} \text{ full rank}] \cdot \mathtt{Disting}_{\mathcal{A}} = \\ \mathtt{ngl}(\lambda) + (1 - \mathtt{ngl}(\lambda)\frac{1}{q(\lambda)} = \frac{1}{q'(\lambda)} \end{aligned}$$

for some polynomial function $q'(\lambda)$. This completes the proof of Theorem 1.

Theorem 2. *Let λ be a security parameter Let $\{\mathcal{X}_\lambda\}$ be a well-spread distribution ensemble and let $m, \tau \in \mathbb{Z}^+$ be parameters that are both $\mathtt{poly}(\lambda)$. Let $\mathcal{F}_{poly}$ be the ensemble of functions f_λ where f_λ is the set of non-constant, non-identity polynomials in $\mathbb{Z}_{p(\lambda)}[x]$ with degree at most m. Suppose that Assumption 1 holds for $\ell = m(3\tau{+}5)$. Then, the above obfuscator is non-malleable for τ-compositions for $\mathcal{F}_{poly}$ and distribution ensemble $\{\mathcal{X}_\lambda\}$.*

Proof. We look to contradict Assumption 2, which follows from Assumption 1. Consider a mauling adversary $\mathcal{A}$ that, given τ obfuscations of a point x, can output a new obfuscation of $f(x)$ for $f \in \mathcal{F}_{poly}$. Consider m to be the degree of f. We build an adversary $\mathcal{B}$ which given the ensemble $\{k_i, g^{k_i x + x^i}\}_{i=2\ldots,m(3\tau+5)}$ and access to $\mathcal{A}$ recovers g^x with noticeable probability.

First, we consider the case when $m > 1$. We set up the reduction as so: upon receiving the ensemble $\{k_i, g^{k_i x + x^i}\}_{i=2\ldots,m(3\tau+5)}$, we create τ obfuscations of x as detailed in Theorem 1. We send these to $\mathcal{A}$, which returns $(f, \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, j_a, j_b, j_c)$ where $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c} \in \mathbb{Z}^\tau_{p(\lambda)}$ and $j_a, j_b, j_c \in \mathbb{G}_\lambda$. Define the vector $\boldsymbol{l}$ as the coefficients of:

$$\boldsymbol{c}_1(f(x)) + \sum_{i=2}^{\tau} \boldsymbol{c}_i (f(x))^{i+2\tau+4} + (f(x))^{3\tau+5} = \sum_{i=0}^{m(3\tau+5)} \boldsymbol{l}_i x^i.$$

In order for the adversary to succeed, this value must equal the exponent of j_c with noticeable probability. $\mathcal{B}$ computes and returns

$$\left(j_c \left(g^{l_0} \cdot \prod_{i=2}^{m(3\tau+5)} h_i^{l_i} \right)^{-1} \right)^{1/(l_1 - \sum_{i=2}^{m(3\tau+5)} k_i l_i)}.$$

Since $\mathcal{B}$ has properly prepared the set of obfuscations to $\mathcal{A}$, $\mathcal{A}$ returns a valid obfuscation of $f(x)$ with probability at least $1/\mathtt{poly}(\lambda)$. In this case then $j_c = g^{l_0 + l_1 x + \ldots + l_{m(3\tau+3)} x^{m(3\tau+5)}}$ with the same probability. In this case, we see that the value in parenthesis is

$$g^{x\left(l_1 - \sum_{i=2}^{m(3\tau+5)} k_i l_i\right)}.$$

Since all l_i, k_i are known, this can be computed unless $l_1 - \sum_{i=2}^{m(3\tau+5)} k_i l_i = 0$. Since $f(x)$ is of degree m, $l_{m(3\tau+5)}$ must be nonzero. $\mathcal{A}$'s view is independent of $k_{m(3\tau+5)}$. So, the probability that the sum is equal to l_1 is $1/(p(\lambda) - 1)$. So, $\mathcal{B}$ returns the correct value with probability $1/\mathtt{poly}(\lambda) - 1/(p(\lambda) - 1) = 1/\mathtt{poly}(\lambda)$ contradicting Assumption 2.

We now consider the case where $m = 1$, or for linear functions f. In this case, we are given the ensemble $\{k_i, g^{k_i x + x^i}\}_{i=2,\ldots,3\tau+5}$. This time, upon receiving

$(f, \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, j_a, j_b, j_c)$ from $\mathcal{A}$, $\mathcal{B}$ instead computes the coefficients $\boldsymbol{l}$ of

$$\sum_{i=1}^{\tau} \boldsymbol{a}_i f(x)^i + \sum_{i=\tau}^{\tau+5} f(x)^i = \sum_{i=0}^{\tau+5} \boldsymbol{l}_i x^i$$

as in the nonlinear case. In this case, $\mathcal{B}$ computes and outputs:

$$\left(j_a \left(g^{l_0} \cdot \prod_{i=2}^{\tau+5} h_i^{l_i} \right)^{-1} \right)^{1/(l_1 - \sum_{i=2}^{\tau+5} k_i l_i)}.$$

Because $\mathcal{A}$ outputs the value $g^{\sum_{i=1}^{\tau} \boldsymbol{a}_i f(x)^\tau + (f(x))^{\tau+1} + \ldots + (f(x))^{\tau+5}}$ with noticeable probability, $\mathcal{B}$'s computation evaluates to g^x unless $l_1 - \sum_{i=2}^{\tau+5} k_i l_i = 0$. Let $\mathbf{R}$ be a random $\mathbb{Z}_{p(\lambda)}^{\tau \times \tau - 1}$ and let $\mathbf{1}^{\tau \times 5}$ be a $\tau \times 5$ matrix of all 1s. To see that this happens with negligible probability, for the first group element of each obfuscation received the coefficient of x^1 are as follows: $\boldsymbol{a}_1 = \left[\mathbf{R} | \mathbf{1}^{\tau \times 5}\right] \cdot \left(k_2 \; k_3 \; \ldots \; k_{\tau+5}\right)^\intercal$.

As shown in the proof of Theorem 1 the values of R are uniformly random conditioned on the other values seen by the adversary. We note that, as all k_i are uniformly chosen, the only information $\mathcal{A}$ learns about $k_{\tau+1}, ..., k_{\tau+5}$ is in the vector $\boldsymbol{a}_1$ Furthermore $\mathbf{R}$ is independent of these values. Thus, we can see that $\mathcal{A}$ receives items of the form

$$\boldsymbol{a}_{1,j} = \sum_{i=2}^{\tau} k_i \mathbf{R}_{i,j} + \sum_{i=\tau+1}^{\tau+5} k_i.$$

Without loss of generality, we assume that an adversary knows the values $k_2, ..., k_\tau$. To change the obfuscated point they will also need to change the higher order powers $x^{\tau+1}, ..., x^{\delta+5}$. The only value they have seen that involves the values $k_{\tau+1}, ..., k_{\tau+5}$ are terms of the form $c + \left(\sum_{i=1}^{5} k_{\tau+i}\right) x$ for some value c. Since the function is linear, we can represent $f(x) = \alpha x + \beta$. So, the adversary must find α, β, γ such that

$$\sum_{i=0}^{4} (\alpha x + \beta)^{i+\tau+1} = \gamma \sum_{i=0}^{4} x^{i+\tau+1}.$$

Define $\delta = \tau + 1$. We can write the desired linear combination as follows:

$$\begin{bmatrix} \alpha^{4+\delta} \\ \alpha^{3+\delta}\left(\binom{\delta+4}{1}\beta + \binom{\delta+3}{0}\right) \\ \alpha^{2+\delta}\left(\binom{\delta+4}{2}\beta^2 + \binom{\delta+3}{1}\beta + \binom{\delta+2}{0}\right) \\ \alpha^{1+\delta}\left(\sum_{i=0}^{3}\left(\binom{\delta+4-i}{3-i}\beta^{3-i}\right)\right) \\ \alpha^{\delta}\left(\sum_{i=0}^{4}\left(\binom{\delta+4-i}{4-i}\beta^{4-i}\right)\right) \end{bmatrix}^\intercal \begin{bmatrix} k_{4+\delta} & 0 & 0 & 0 & 0 \\ 0 & k_{3+\delta} & 0 & 0 & 0 \\ 0 & 0 & k_{2+\delta} & 0 & 0 \\ 0 & 0 & 0 & k_{1+\delta} & 0 \\ 0 & 0 & 0 & 0 & k_\delta \end{bmatrix} = \gamma \begin{bmatrix} k_{4+\delta} \\ k_{3+\delta} \\ k_{2+\delta} \\ k_{1+\delta} \\ k_\delta \end{bmatrix}$$

Substituting, one has that

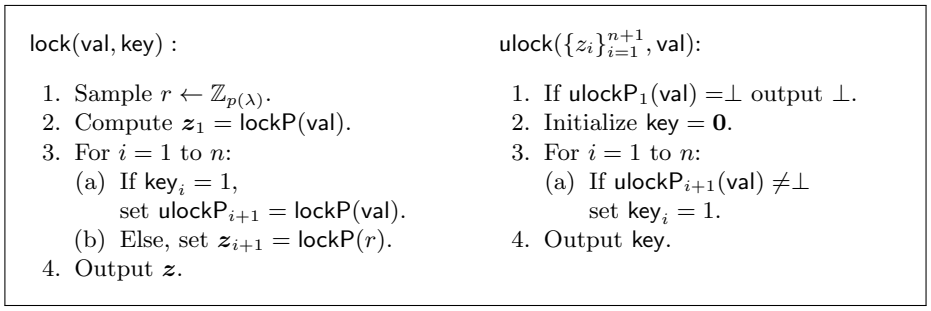

Fig. 1: Nonmalleable digital locker preventing tampering over only val

1. If $\beta = 0$ then this implies $\alpha^{\delta+4} = \alpha^{\delta+3} = \alpha^{\delta+2} = \alpha^{\delta+1} = \alpha^{\delta}$ which only has solutions if $\alpha = 0$ or $\alpha = 1$. These are both considered trivial solutions.
2. Otherwise, $\gamma = \alpha^{\delta+4}$ (using first equation),
3. $(\delta + 4)\beta + 1 = \alpha$ (using second equation),
4. $(\delta + 4)\beta + 2 = 0$ or $\delta = -5$ (using third equation, relying on $\beta \neq 0$).
5. Assume that $\delta \neq -5$, then $\alpha = -1$ (substitution of third constraint into second equation)
6. $\gamma = (-1)^{\delta}$ (substitution of α in first equation). Note that $\gamma = 1$ corresponds to no tampering. Thus, we consider $\gamma = -1$.
7. $\delta \equiv -5$ or $\delta \equiv -6$ (solving fourth equation using prior constraints) and thus $\tau \equiv -6$ or $\tau \equiv -7$.

We note that since $\tau = \mathtt{poly}(\lambda)$ for large enough λ one can be sure that $\tau \not\equiv \{-6, -7\} \mod |\mathbb{G}_\lambda|$. So, the only functions that $\mathcal{A}$ can maul to are the constant and identity functions, neither of which are in $\mathcal{F}_{poly}$. This means that $\mathcal{A}$ returns a solution where $l_1 - \sum_{i=2}^{\tau+5} k_i l_i = 0$. with negligible probability. So, with non-negligible probability, $\mathcal{B}$ can break Assumption 2.

4 Nonmalleable digital lockers

We now use the nonmalleable point function from Construction 1 to construct a nonmalleable digital locker that does not prevent any tampering over the stored key. We use the well known real-or-random construction of digital-lockers [CD08]. The basic real or random construction is in Figure 1. We do not argue security of this basic construction, as long as lockP is $n+1$ same point composable then this construction provides a digital locker that provides nonmalleability over val. The argument is the same as in [CD08] with the worst case for nonmalleability being when all of key is 1 since this provides the adversary with $n + 1$ obfuscations of val.

4.1 Detecting tampering over key

With the ability to instantiate the real or random construction with nonmalleable point functions, we turn to detecting tampering over the encoded key. As mentioned in the introduction, this construction requires a public object that all parties can depend on (as long as the distribution is efficiently sampleable) which can be achieved in the CRS model. However, the construction is black box in the underlying digital locker (unlike a construction from NIZKs).

We combine nonmalleable codes and seed-dependent condensers to check if the adversary tampers over the key value. We use the locked point val as input to a seed-dependent condenser as part of the value encoded in the nonmalleable code. If the adversary tampers to an *independent value*, they are unlikely to match the output of the condenser on the real val. We introduce these tools and then our construction. We first present the notion of nonmalleable codes, introduced by Dziembowski, Pietrzak, and Wichs [DPW10].

Definition 6. *A pair of algorithms* $(\mathsf{Enc}, \mathsf{Dec})$ *is called a* coding scheme *if* $\mathsf{Enc} : \{0,1\}^k \to \{0,1\}^n$ *is randomized and* $\mathsf{Dec} : \{0,1\}^n \to \{0,1\}^k \cup \perp$ *is deterministic and for each* $s \in \{0,1\}^k$ *it holds that* $\Pr[\mathsf{Dec}(\mathsf{Enc}(s)) = s] = 1$.

Definition 7. *A coding scheme* $(\mathsf{Enc}, \mathsf{Dec})$ *is called* $(\epsilon_{nmc}, s_{nmc}, \mathcal{F})$-nonmalleable *if for each* $f \in \mathcal{F}$ *and each* $s \in \{0,1\}^k$*, there exists a distribution* $D_f()$ *over* $\{\{0,1\}^k, \mathtt{same}\}$ *that is efficiently samplable given oracle access to* f *such that the following holds:*

$$\delta^{s_{nmc}}(\{c \leftarrow \mathsf{Enc}(s); \overline{c} \leftarrow f(c), \overline{s} = \mathsf{Dec}(\overline{c}) : \textit{Output } \overline{s}\},$$
$$\{\tilde{s} \leftarrow D_f, \ \textit{Output } s \textit{ if } \tilde{s} = \mathtt{same} \textit{ else } \tilde{s}\}) \leq \epsilon_{nmc}.$$

Seed-dependent condensers were introduced by Dodis, Ristenpart, and Vadhan [DRV12]. Their goal is similar to a traditional randomness extractor, except the output only has to be statistically close to a distribution with minentropy. Importantly, it is possible to construct condensers where the adversary is allowed to output the chosen distribution after seeing the seed.

Definition 8. *Let* $\mathtt{cond} : \{0,1\}^\lambda \times \{0,1\}^d \to \{0,1\}^\alpha$ *be a* (k, k', s, ϵ) seed-dependent condenser *if for all probabilistic adversaries of size at most* s *who take a random seed* $\mathsf{seed} \leftarrow U_d$ *and output a distribution* $X_{\mathsf{seed}} \leftarrow \mathcal{A}(\mathsf{seed})$ *of entropy* $\mathrm{H}_\infty(X|\mathsf{seed}) \geq k$*, then for the joint distribution* (X, U_d) *over* X_{seed} *arising from a random* $\mathsf{seed} \leftarrow U_d$*, there exists a distribution* Y *such that* $\tilde{\mathrm{H}}_\infty(Y|U_d) \geq k'$ *such that* $\Delta((Y, U_d), (\mathtt{cond}(X; U_d), U_d)) \leq \epsilon$.

Dodis, Ristenpart, and Vadhan showed that seed-dependent condensers can be constructed using collision resistant hash functions. Furthermore, this construction works for $\epsilon = 0$. That is, the output has entropy instead of being close to a distribution with entropy. For our construction, we will require $k' = \omega(\log \lambda)$.

We now present the construction. Instead of directly *locking* the value key we instead lock the value $c = \mathsf{Enc}(\mathsf{key} || \mathtt{cond}(\mathsf{val}; \mathsf{seed}))$, where Enc is the encoding

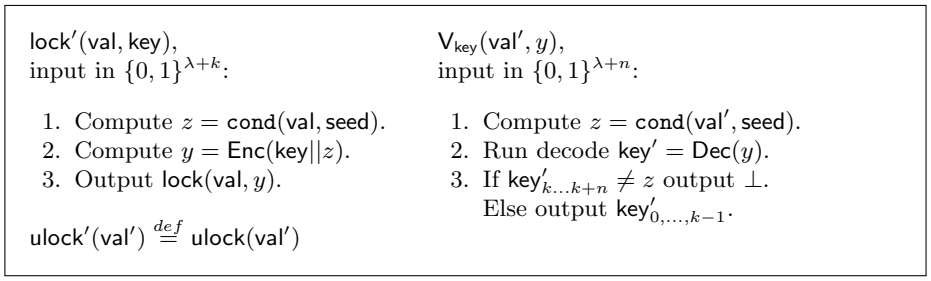

Fig. 2: Nonmalleable digital locker preventing tampering over both val and key. A seed of a seed-dependent condenser must be public and global.

function for a nonmalleable code and cond is a seed dependent condenser. Notionally, the nonmalleable code prevents tampering to *independent* points and the condenser detects if the adversary tampers to an independent point.

Construction 2 *Let* $(\mathsf{lock}', \mathsf{ulock}')$ *be defined as in Figure 1. Let* $(\mathsf{Enc}, \mathsf{Dec})$ *be a coding scheme where* $\mathsf{Enc} : \{0,1\}^{k+\alpha} \to \{0,1\}^n$. *Let* $\mathtt{cond} : \{0,1\}^\lambda \times \{0,1\}^d \to \{0,1\}^\alpha$ *be a seed-dependent condenser. Define the algorithms* $(\mathsf{lock}', \mathsf{ulock}', \mathsf{V}_{\mathsf{key}})$ *as in Figure 2.*

However, security of this construction is not straightforward as we are using nonmalleable codes in a nonstandard way. In a nonmalleable code, the adversary specifies the tampering function before seeing any information about c. In our setting, the adversary sees obfuscations that have c embedded before deciding how to tamper. The crucial part to our argument is that the set of obfuscations is pseudorandom condition on c and $s \stackrel{def}{=} \mathtt{cond}(\mathsf{val}; \mathsf{seed})$. If an adversary is able to tamper substantially better given obfuscations of val from some entropic distribution than with uniformly random val we can check whether they tampered properly and use this to break distributional indistinguishability. The proof of Theorem 3 is deferred to the full version [FF18, Section 4.2].

Theorem 3. *Let* $\lambda \in \mathbb{N}$ *be a security parameter and let* $\{0,1\}^\lambda$ *be the domain. Let* $(\mathsf{lockP}, \mathsf{ulockP})$ *be a* $(n+1)$*-same point composable and* $\mathcal{F}_{single}$*-nonmalleable.*

1. *Suppose for any* $s = \mathtt{poly}(\lambda)$ *there exists* $\mu, \beta = \omega(\log \lambda)$ *such* $\mathtt{cond} : \{0,1\}^\lambda \times \{0,1\}^d \to \{0,1\}^\alpha$ *is a* $(\mu, \beta, s, 0)$*-seed-dependent condenser.*
2. *Let* $\mathsf{seed} \leftarrow \{0,1\}^d$ *be a public parameter.*
3. $X \stackrel{def}{=} X(\mathsf{seed})$ *be an* s*-samplable distribution so* $\tilde{\mathrm{H}}_\infty(X|\mathsf{seed}, \mathtt{cond}(\mathsf{seed}, X)) \geq \beta$.[3]

[3] In the previous sections, we consider X that have worst case min-entropy. However, if $\tilde{\mathrm{H}}_\infty(X|\mathsf{seed}, \mathtt{cond}(\mathsf{seed}, X)) \geq \beta$ for some $\beta = \omega(\log \lambda)$ then there exists some $\beta' = \omega(\log \lambda)$ such that with $\Pr_{\mathsf{seed}}[\mathrm{H}_\infty(X|\mathsf{seed}, \mathtt{cond}(\mathsf{seed}, X)) \geq \beta'] \geq 1 - \mathtt{ngl}(\lambda)$. Thus, this change does not effect the set of distributions assumed to be secure in Assumption 1.

4. *Let a description of* $\mathbb{G}_\lambda$*, a generator* g *for* $\mathbb{G}_\lambda$ *and* $\mathsf{seed} \leftarrow \{0,1\}^d$ *be system parameters.*
5. *Let* $\mathcal{F}_{nmc}$ *be a function class. Suppose for any* $s_{nmc} = \mathtt{poly}(\lambda)$ *there exists* $\epsilon_{nmc} = \mathtt{ngl}(\lambda)$ *such that* $(\mathsf{Enc}, \mathsf{Dec})$ *is an* $(\epsilon_{nmc}, s_{nmc}, \mathcal{F}_{nmc})$ *nonmalleable code.*

Then $(\mathsf{lock}', \mathsf{ulock}')$ *in Construction 2 and Figure 2 is point nonmalleable for* $\mathcal{F}_{single}$ *and key nonmallable for* $\mathcal{F}_{nmc}$*. In particular,* $(\mathsf{lock}', \mathsf{ulock}')$ *is a* $(\mathcal{F}_{single}, \mathcal{F}_{nmc}, \mathcal{X})$*-nonmalleable digital locker.*

We recommend using a nonmalleable code that detects at least permutations and $1 \to 0$ bit tampers, such as [AGM+15a,AGM+15b], as these transforms are otherwise computable in polynomial time.

Constructions using nonmalleable extractors [DW09,CRS14] or one-way hashes [BCFW09,BFS11,CQZ+16] may be possible. However, they are not immediate, we use the primitive of nonmalleable hashes to illustrate. A nonmalleable hash function is a family of functions $h \in \mathcal{H}$ such that an adversary given $h(x)$ (sampled $h \leftarrow \mathcal{H}$ and x from some distribution) cannot find $h(f(x))$ for f in some function class $\mathcal{F}$. Several of these works claim to be "standard model" but all require h is random and not tampered by the adversary. One could append a nonmalleable hash, obfuscating $\mathsf{key}' = \mathsf{key}||h(\mathsf{key}||\mathsf{val})$. However, this approach assumes that the function instance h is assumed to be independently sampled from key and val. In our approach, the public randomness required is for $\mathtt{seed}$ of the condenser, and the distribution of val (and key) can depend on this value. Furthermore, non malleable hashes are analyzed with the adversary only knowing the output value $h(x)$. It is not clear that security would hold in the presence of multiple correlated obfuscations. Similar issues arise with nonmalleable extractors [DW09,CRS14].

Acknowledgements This work was funded in part by a grant from Comcast Inc, by NSF Grant CNS 1849904, and ONR Grant N00014-19-1-2327. This research is based upon work supported in part by the Office of the Director of National Intelligence (ODNI), Intelligence Advanced Research Projects Activity (IARPA), via Contract No. 2019-19020700008. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of ODNI, IARPA, or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for governmental purposes notwithstanding any copyright annotation therein.

The authors thank Luke Demarest, Pratyay Mukherjee, Alex Russell, and Mayank Varia for their helpful feedback. Special thanks to James Bartusek, Fermi Ma, and Mark Zhandry for discussing their work and its compositional properties.

References

ABC+18. Quentin Alamélou, Paul-Edmond Berthier, Chloé Cachet, Stéphane Cauchie, Benjamin Fuller, Philippe Gaborit, and Sailesh Simhadri. Pseudoentropic isometries: A new framework for fuzzy extractor reusability. In *AsiaCCS*, 2018.

AGM+15a. Shashank Agrawal, Divya Gupta, Hemanta K Maji, Omkant Pandey, and Manoj Prabhakaran. Explicit non-malleable codes against bit-wise tampering and permutations. In *Advances in Cryptology – CRYPTO*, pages 538–557. Springer, 2015.

AGM+15b. Shashank Agrawal, Divya Gupta, Hemanta K Maji, Omkant Pandey, and Manoj Prabhakaran. A rate-optimizing compiler for non-malleable codes against bit-wise tampering and permutations. In *Theory of Cryptography Conference*, pages 375–397. Springer, 2015.

AJ15. Prabhanjan Ananth and Abhishek Jain. Indistinguishability obfuscation from compact functional encryption. In *Advances in Cryptology – CRYPTO*, pages 308–326. Springer, 2015.

BC10. Nir Bitansky and Ran Canetti. On strong simulation and composable point obfuscation. In *Advances in Cryptology–CRYPTO 2010*, pages 520–537. Springer, 2010.

BCFW09. Alexandra Boldyreva, David Cash, Marc Fischlin, and Bogdan Warinschi. Foundations of non-malleable hash and one-way functions. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 524–541. Springer, 2009.

BFS11. Paul Baecher, Marc Fischlin, and Dominique Schröder. Expedient non-malleability notions for hash functions. In *Cryptographers Track at the RSA Conference*, pages 268–283. Springer, 2011.

BGI+01. Boaz Barak, Oded Goldreich, Rusell Impagliazzo, Steven Rudich, Amit Sahai, Salil Vadhan, and Ke Yang. On the (im) possibility of obfuscating programs. In *Advances in Cryptology–CRYPTO*, pages 1–18. Springer, 2001.

BGI+12. Boaz Barak, Oded Goldreich, Russell Impagliazzo, Steven Rudich, Amit Sahai, Salil Vadhan, and Ke Yang. On the (im) possibility of obfuscating programs. *Journal of the ACM (JACM)*, 59(2):6, 2012.

BMZ19. James Bartusek, Fermi Ma, and Mark Zhandry. The distinction between fixed and random generators in group-based assumptions. In *Advances in Cryptology – CRYPTO*, 2019.

BR17. Zvika Brakerski and Guy N Rothblum. Obfuscating conjunctions. *Journal of Cryptology*, 30(1):289–320, 2017.

Can97. Ran Canetti. Towards realizing random oracles: Hash functions that hide all partial information. In *Advances in Cryptology-CRYPTO'97*, pages 455–469. Springer, 1997.

CD08. Ran Canetti and Ronny Ramzi Dakdouk. Obfuscating point functions with multibit output. In *Advances in Cryptology–EUROCRYPT 2008*, pages 489–508. Springer, 2008.

CDG18. Sandro Coretti, Yevgeniy Dodis, and Siyao Guo. Non-uniform bounds in the random-permutation, ideal-cipher, and generic-group models. In *Annual International Cryptology Conference*, pages 693–721. Springer, 2018.

CFP+16. Ran Canetti, Benjamin Fuller, Omer Paneth, Leonid Reyzin, and Adam Smith. Reusable fuzzy extractors for low-entropy distributions. In *Advances in Cryptology–Eurocrypt 2016*, pages 117–146. Springer, 2016.

CQZ+16. Yu Chen, Baodong Qin, Jiang Zhang, Yi Deng, and Sherman SM Chow. Non-malleable functions and their applications. In *IACR International Workshop on Public Key Cryptography*, pages 386–416. Springer, 2016.

CRS14. Gil Cohen, Ran Raz, and Gil Segev. Nonmalleable extractors with short seeds and applications to privacy amplification. *SIAM Journal on Computing*, 43(2):450–476, 2014.

CRV10. Ran Canetti, Guy N Rothblum, and Mayank Varia. Obfuscation of hyperplane membership. In *Theory of Cryptography Conference*, pages 72–89. Springer, 2010.

CV09. Ran Canetti and Mayank Varia. Non-malleable obfuscation. In Omer Reingold, editor, *Theory of Cryptography*, pages 73–90, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg.

DORS08. Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin, and Adam Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *SIAM Journal on Computing*, 38(1):97–139, 2008.

DPW10. Stefan Dziembowski, Krzysztof Pietrzak, and Daniel Wichs. Non-malleable codes. In *ICS*, volume 2010, page 1st. Citeseer, 2010.

DRV12. Yevgeniy Dodis, Thomas Ristenpart, and Salil Vadhan. Randomness condensers for efficiently samplable, seed-dependent sources. In *Theory of Cryptography Conference*, pages 618–635. Springer, 2012.

DW09. Yevgeniy Dodis and Daniel Wichs. Non-malleable extractors and symmetric key cryptography from weak secrets. In *Proceedings of the forty-first annual ACM symposium on Theory of computing*, pages 601–610. ACM, 2009.

FF18. Peter Fenteany and Benjamin Fuller. Same point composable and non-malleable obfuscated point functions. Cryptology ePrint Archive, Report 2018/957, 2018. `https://eprint.iacr.org/2018/957`.

GGH+13. Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Amit Sahai, and Brent Waters. Candidate indistinguishability obfuscation and functional encryption for all circuits. In *2013 IEEE 54th Annual Symposium on Foundations of Computer Science*, pages 40–49. IEEE, 2013.

GGH+16. Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Amit Sahai, and Brent Waters. Candidate indistinguishability obfuscation and functional encryption for all circuits. *SIAM Journal on Computing*, 45(3):882–929, 2016.

GLSW15. Craig Gentry, Allison Bishop Lewko, Amit Sahai, and Brent Waters. Indistinguishability obfuscation from the multilinear subgroup elimination assumption. In *2015 IEEE 56th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 151–170. IEEE, 2015.

KY18a. Ilan Komargodski and Eylon Yogev. Another step towards realizing random oracles: Non-malleable point obfuscation. In *Advances in Cryptology – EUROCRYPT*, pages 259–279. Springer, 2018.

KY18b. Ilan Komargodski and Eylon Yogev. Another step towards realizing random oracles: Non-malleable point obfuscation. Cryptology ePrint Archive, Report 2018/149, 2018. Version 20190226:074205, `https://eprint.iacr.org/2018/149`.

PST14. Rafael Pass, Karn Seth, and Sidharth Telang. Indistinguishability obfuscation from semantically-secure multilinear encodings. In *Advances in Cryptology – CRYPTO*, pages 500–517. Springer, 2014.

SW14. Amit Sahai and Brent Waters. How to use indistinguishability obfuscation: deniable encryption, and more. In *Proceedings of the forty-sixth annual ACM symposium on Theory of computing*, pages 475–484. ACM, 2014.

WZ17. Daniel Wichs and Giorgos Zirdelis. Obfuscating compute-and-compare programs under LWE. In *2017 IEEE 58th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 600–611. IEEE, 2017.