Fine-Grained Cryptography Revisited

Shohei Egashira[1], Yuyu Wang[2]*, and Keisuke Tanaka[1]

[1] Tokyo Institute of Technology, Tokyo, Japan
egashira.s.aa@m.titech.ac.jp, keisuke@is.titech.ac.jp
[2] University of Electronic Science and Technology of China, Chengdu, China
wangyuyu@uestc.edu.cn

Abstract. *Fine-grained cryptographic primitives* are secure against adversaries with bounded resources and can be computed by honest users with less resources than the adversaries. In this paper, we revisit the results by Degwekar, Vaikuntanathan, and Vasudevan in Crypto 2016 on fine-grained cryptography and show the constructions of three key fundamental fine-grained cryptographic primitives: *one-way permutations*, *hash proof systems* (which in turn implies a *public-key encryption scheme against chosen chiphertext attacks*), and *trapdoor one-way functions*. All of our constructions are computable in NC^1 and secure against (*non-uniform*) NC^1 circuits under the widely believed worst-case assumption $\mathsf{NC}^1 \subsetneq \oplus\mathsf{L}/\mathsf{poly}$.

Keywords: Fine-grained cryptography · NC^1 circuit · One-way permutation · Hash proof system · Trapdoor one-way function

1 Introduction

1.1 Background

To prove the security of a cryptographic scheme, we typically reduce the security to some computational hardness assumption with a precise security definition. Due to the fact that most assumptions are unproven, it is desirable to make the underlying assumptions as weak as possible. However, it turns out to be very hard to construct a public-key cryptographic scheme without assuming the existence of one-way functions (OWF). Moreover, for a vast majority of primitives (including public-key encryption (PKE)), we further need to assume the hardness of specific problems such as factoring, discrete-logarithm, learning with errors, etc.. It still remains open whether it is possible to construct even basic cryptographic primitives under no assumptions, or at least mild complexity-theoretic assumptions. For instance, the complexity-theoretic assumption $\mathsf{NP} \not\subseteq \mathsf{BPP}$, which is strictly weaker than the assumption of OWFs, has been proven to be insufficient for constructing even OWFs as shown by Akavia et al. [4].

Due to the difficulty of directly constructing cryptographic primitives against any polynomial probabilistic time adversaries based on mild complexity-theoretic

* Corresponding author, ORCID: 0000-0002-1198-1903.

assumptions such as $\mathsf{NP} \not\subseteq \mathsf{BPP}$, a line of beautiful works focused on fine-grained cryptographic primitives [16], where (1) the resource of an adversary is a-prior bounded, (2) an honest party can run the algorithms with less resource than an adversary, and (3) the underlying assumption is extremely mild.

Merkle [35] initialized the study in this field by constructing a non-interactive key exchange scheme, which can be run in time $O(n)$ and adversaries running in time $o(n^2)$ cannot break the security. The construction only requires random functions (i.e., the random oracle). Subsequent to his work, Biham et al. [10] showed the existence of strong OWFs based on the same assumption.

While Merkle restricted adversaries in the term of running time, Maurer considered a model where adversaries have infinite computing power but only restricted storage [34]. Afterwards, he proposed a key exchange protocol in this model [36]. Following these works, Cachin and Maurer [13] constructed a symmetric-key encryption scheme and a key exchange protocol which can be run with storage $O(s)$ and are unconditionally secure against adversaries with storage $o(s^2)$. Besides, there have been many other works focusing on primitives in this model [9, 42, 18, 8, 19, 20].

In the constant depth circuit model, Ajtai and Wigderson [3] constructed an unconditional secure pseudo-random generator. Then, Boppana and Lagarias [12] exploited the results by Ajitai [2] and Furst et al. [21], which shows that parity cannot be computed in size-bounded circuits, to achieve OWFs. The proposed OWF can be computed in AC^0 (constant-depth polynomial-sized) circuits consisting of AND, OR, and NOT gates of unbounded fan-in, while the inverse cannot. Afterwards, several works treating the same model have been proposed [28, 6, 43, 44].

Recently, Degwekar et al. [16] proposed fine-grained cryptographic primitives against adversaries captured by two (non-uniform) classes of adversaries, which are AC^0 and NC^1 (logarithmic-depth polynomial-sized) circuits consisting of AND, OR, and NOT gates of fan-in 2. They first constructed an unconditionally secure pseudorandom generator with arbitrary polynomial stretch, a weak pseudorandom function, and a secret-key encryption scheme, all of which are computable in AC^0 and secure against adversaries that are AC^0 circuits. Then, under the widely believed separation assumption $\mathsf{NC}^1 \subsetneq \oplus\mathsf{L}/\mathsf{poly}$, they constructed a OWF, a pseudorandom generator, a collision-resistant hash function, and a semantically secure PKE scheme that are computable in NC^1 and secure against NC^1 circuits.

Following the above work, Campanelli and Gennaro [14] constructed a somewhat homomorphic encryption and a verifiable computation against NC^1 circuits. As in [16], the underlying assumption is $\mathsf{NC}^1 \subsetneq \oplus\mathsf{L}/\mathsf{poly}$.

While the above sequence of works have achieved amazing success, it still remains open whether it is possible to construct other fine-grained primitives, such as one-way permutation (OWP), PKE against chosen ciphertext attacks (CCA), and even trapdoor one-way function (TDF).

1.2 Our Results and Techniques

In this paper, we propose several fine-grained cryptographic primitives under the assumption $\mathsf{NC}^1 \subsetneq \oplus\mathsf{L}/\mathsf{poly}$. Specifically, we propose a OWP, a hash proof system (HPS) (which in turn derives a CCA-secure PKE scheme), and a TDF. All of them are computable in NC^1 and secure against adversaries captured by the class of NC^1 circuits. Since a lot of results have been devoted to constructing advanced primitives from these fundamental ones, our results greatly alleviate the efforts to achieve more fine-grained primitives from scratch.

Our constructions rely on the fact shown in the papers by Appelebaum, Ishai, and Kushilevitz [29, 5], that if $\mathsf{NC}^1 \subsetneq \oplus\mathsf{L}/\mathsf{poly}$, there exist a distribution D_0^n over $n \times n$ matrices of rank $(n-1)$ and a distribution D_1^n over $n \times n$ matrices of rank n, which are indistinguishable for NC^1 circuits.

One-way permutation. As one of the most fundamental cryptographic primitives, OWP has been shown to be sufficient for constructing many primitives (e.g. pseudorandom generators [11] and universal one-way hash functions [37]). Compared with primitives built from OWFs which are not bijective (e.g., [40, 26]), ones built from OWPs are usually more efficient [7, 33].

In the previous work, Degwekar et al. [16] showed a construction of fine-grained OWFs in NC^1. Their construction relies on a randomized encoding of a boolean function f, which is a randomized function outputting the distribution related only to $f(x)$. Specifically, let $\hat{f} : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}^{m+1} \in \mathsf{NC}^1$ be the randomized encoding of $f \in \oplus\mathsf{L}/\mathsf{poly}$, where the existence of $\hat{f}$ is shown in [5]. Then, their construction of a OWF is $g(x) = \hat{f}(0^n, x)$.[3] However, the domain and range of g are $\{0,1\}^m$ and $\{0,1\}^{m+1}$ respectively, i.e., the domain and range of g are inconsistent. Thus their construction is not a permutation. Moreover, since they define OWFs using randomized encoding directly, it is difficult to make their construction a permutation, i.e., it is not clear how to further achieve OWPs under the same worst-case assumption.

In this work, we propose a collection of OWPs and extend it to a OWP, both of which are computable in NC^1 and secure against NC^1 circuits under the assumption $\mathsf{NC}^1 \subsetneq \oplus\mathsf{L}/\mathsf{poly}$.

To achieve the goal, we exploit the two distributions D_0^n and D_1^n described above. Essentially, our idea is to construct a "lossy function family" $\{f_{\mathbf{M}}(\mathbf{x}) = \mathbf{M}\mathbf{x}\}_{\mathbf{M}\in D_1^n}$. We let $\mathbf{M} \leftarrow D_1^n$ and $\mathbf{M} \leftarrow D_0^n$ in the injective and lossy model respectively, and the indistinguishability between the two models can be reduced to the indistinguishability between D_1^n and D_0^n. Then we follow the Peikert-Waters [38] approach to prove that $f_{\mathbf{M}}$ in the injective model satisfies one-wayness. Furthermore, since a matrix $\mathbf{M} \leftarrow D_1^n$ is of full rank, it holds that $f_{\mathbf{M}}$ in the injective model is a permutation. Therefore, $\{f_{\mathbf{M}}(\mathbf{x}) = \mathbf{M}\mathbf{x}\}_{\mathbf{M}\in D_1^n}$ is a collection of OWPs. Next, we extend it to a OWP, i.e., we give a construction of OWP based on a collection of OWPs which satisfies the distribution of index

[3] The one-wayness of g is based on the indistinguishability of the output distributions of $\hat{f}$ conditioned on $f(x) = 0$ and $f(x) = 1$, which can be reduced to $\mathsf{NC}^1 \subsetneq \oplus\mathsf{L}/\mathsf{poly}$.

sample algorithm is identical to the uniform distribution over index set as follows. For a collection of OWPs $\{f_i : D_i \to D_i\}_{i \in I}$ where I is an index set, define a function g with the domain $D := \bigcup_{i \in I}(\{i\} \times D_i)$ and $g((i,x) \in D) = (i, f_i(x))$. Since f_i is a permutation and one-way, g is a permutation and one-way as well, i.e., g is a OWP.

Hash proof system and CCA secure PKE scheme. The notion of HPS, which can be treated as designated verifier non-interactive zero-knowledge proof system for a language, was first introduced by Cramer and Shoup [15] for the purpose of constructing a CCA secure PKE scheme. An HPS allows one to generate a valid proof π proving that a statement x is in a language L by using a witness w and a public key pk. Also, one can generate a valid proof for x (not necessarily in L) by using only a secret key sk. For $x \in L$, proofs generated in these two ways should be the same. Typically, L is required to be a hard subset membership one, i.e., statements sampled from inside and outside the language should be indistinguishable. Furthermore, an HPS usually satisfies universality and smoothness. Universality means that for fixed x outside L and pk, the entropy of π is high enough (due to the entropy of sk). Smoothness means that for x outside L, the distribution of π honestly generated with sk is close to the uniform distribution in the proof space. HPSs are very versatile. Besides the application of PKE schemes, they play important roles in constructing various primitives, such as password authenticated key exchange [24, 32], oblivious transfer [31, 1], and zero-knowledge arguments [30].

In previous works, there has been no known way to construct HPSs that is computable in NC^1 and secure against adversaries bounded in NC^1 yet. Note that HPS is a quite different primitive from the ones in [16, 14], and its instantiation cannot be achieved via some simple extension. The main bottleneck is that it is not clear how to construct an HPS, where we can reduce the hardness of the subset membership problem to the indistinguishability between D_0^n and D_1^n. To overcome this problem, we define two sets L and L' that are identical to the supported language in a somewhat sophisticated way. The interesting part is that we can reduce the indistinguishability between L' and X/L to that between D_0^n and D_1^n. Also we did very careful analysis on the entropy of secret keys with respect to fixed public keys the to prove smoothness and universality. More details are given as follows.

In this work, we propose the first HPS that is computable in NC^1 and secure against NC^1 adversaries based on the worst-case assumption $\mathsf{NC}^1 \subsetneq \oplus\mathsf{L/poly}$.

Our idea is to let a proof in the HPS be of the form $\mathbf{sk}^\top \mathbf{M}^\top \mathbf{w}$, where $\mathbf{M} \leftarrow D_0^n$, $\mathbf{x} = \mathbf{M}^\top \mathbf{w}$ is the statement with witness $\mathbf{w}$, $\mathbf{sk}$ is the secret key, and $\mathbf{M}\,\mathbf{sk} = \mathbf{pk}$ is the public key. A proof can be generated as either $\mathbf{pk}^\top \mathbf{w}$ or $\mathbf{sk}^\top \mathbf{x}$. The language that our HPS supports is $\mathrm{Im}(\mathbf{M}^\top)$. To achieve the the hardness of our subset membership problem, we exploit the fact that $\mathrm{Im}(\mathbf{M}^\top)$ is identical to both

$$L = \{\mathbf{x} | \mathbf{w} \in 1 \times \{0,1\}^{n-1}, \mathbf{x} = \mathbf{M}^\top \mathbf{w}\} \text{ and } L' = \{\mathbf{x} | \mathbf{w} \in 0 \times \{0,1\}^{n-1}, \mathbf{x} = \mathbf{M}^\top \mathbf{w}\}.$$

We prove that if we sample $\mathbf{M}$ as $\mathbf{M} \leftarrow D_1^n$ instead of $\mathbf{M} \leftarrow D_0^n$ for L', L' becomes exactly $X \setminus L$ where $X = \{0,1\}^n$. Then we reduce the indistinguishability between the uniform distributions over L' and $X \setminus L$ to that between D_0^n and D_1^n. To prove the universality and smoothness, we show that for one $\mathbf{pk}$, there exist different valid secret keys, which lead to different outputs for any statement not in the language. Hence, the entropy of the proof is high due to the entropy of the secret key for a fixed $\mathbf{pk}$ and statement. We refer the reader to Section 4 for further details.

The proof size of the above scheme is only one single bit, while we can extend it to an HPS with multi-bit proofs by running many HPSs in parallel and show that the extension is still computable in NC^1 and secure against NC^1 circuits.

We now can instantiate the generic constructions [15] of a CCA-secure PKE scheme with our HPSs. The resulting scheme is secure against NC^1 circuits allowed to make constant rounds of adaptive decryption queries, while in each round, it can make arbitrary polynomial number of queries. This restriction is natural and defined in the same way as the adversaries for the NC^1-verifiable computation scheme in [14].

As far as we know, this is the first PKE that is CCA secure against NC^1 circuits under a mild complexity-theoretic assumptions, and there is no known way to make the PKE in [16] and the somewhat homomorphic encryption scheme in [14], which are malleable, CCA secure.

Trapdoor one-way function. TDF is a fundamental primitive introduced by Diffie and Hellman [17]. Unlike PKE schemes, where the decryption algorithm only recovers the plaintext (not including the internal randomness used in the encryption procedure), the inversion algorithm of a TDF recovers the entire preimage. The property of TDF mentioned above is useful in many applications, where proofs of well-formedness are required [22]. However, in the same time, it makes constructing TDFs very challenging.

In the previous works [16, 14], the PKEs use randomness in the encrypting procedures and it is difficult to recover the randomness in the decrypting procedures since the constructions recover the plaintexts by canceling the randomness using the property of the kernel of $\mathbf{M} \leftarrow D_0^n$. Namely, it is not easy to extend their construction to achieve a TDF. In fact, it has been shown that a TDF cannot be built from a PKE scheme in a black-box way [25][4]. On the other hand, it seems that there is a naive approach to construct a TDF f by defining it in the same way as our OWP, i.e., $f(\mathbf{x}) = \mathbf{M}_1\mathbf{x}$ where $\mathbf{M}_1$ is a sampled from D_1^n, and sample the inverse $\mathbf{M}_1^{-1}$ or some other elements that can be used to solve linear equations efficiently as the trapdoor. However, there is no known way to perform such a sampling procedure in NC^1 circuits. Therefore, some more sophisticated approach has to be taken.

In this work, we propose a TDF computable in NC^1 and secure against NC^1 circuits based on $\mathsf{NC}^1 \subsetneq \oplus\mathsf{L/poly}$. The intuition is as follows.

[4] There is no rigorous proof showing that the separation holds for NC^1, while it is an evidence that TDF is not easy to achieve.

We first change the domain to $\{0,1\}^t \times (L \times X \setminus L)^t$ where $\mathbf{M} \leftarrow D_0^n$, $L = \mathrm{Im}(\mathbf{M})$, and $X = \{0,1\}^n$. On input $(x, (\mathbf{c}_1, \mathbf{c}'_1), \cdots, (\mathbf{c}_t, \mathbf{c}'_t)) \in \{0,1\}^t \times (L \times X \setminus L)^t$, our TDF computes $y = f(\mathbf{x})$, and additionally outputs $(\mathbf{c}_i, \mathbf{c}'_i)$ if $x_i = 0$ and $(\mathbf{c}'_i, \mathbf{c}_i)$ otherwise for all i. Here, f is a OWF that is computable in NC^1 and secure against NC^1 and x_i denotes the ith bit of x. Then, if we have a non-zero vector $\mathbf{k}$ in the kernel of $\mathbf{M}$, which is samplable in NC^1 [16], we can determine whether $\mathbf{x} \in \{0,1\}^n$ is in $\mathrm{Im}(\mathbf{M}^\top)$ or $\{0,1\}^n \setminus \mathrm{Im}(\mathbf{M}^\top)$ and recover x_i by checking whether $\mathbf{c}_i$ and $\mathbf{c}'_i$ are swapped. This provides us an efficiently samplable trapdoor. Due to the subset membership problem for $L = \mathrm{Im}(\mathbf{M})$ we described before, the uniform distributions over $\mathrm{Im}(\mathbf{M}^\top)$ and $\{0,1\}^n \setminus \mathrm{Im}(\mathbf{M}^\top)$ are indistinguishable when $\mathbf{M}$ is a matrix sampled from D_0^n. Therefore, the adversary in the one-wayness game can only obtain information on $f(x)$ (which is one-way) and the additional pairs do little help to it.

The above technique of sampling additional pairs is called *bits planting* which was used by Garg et al. [23] to construct a TDF based on the computational Diffie-Hellman problem. Although both our construction and the one in [23] aim at constructing trapdoor TDFs, we use the *bits planting* in a different way. In [23], this technique is exploited to recover the randomness used in the computation procedure of the TDF (see [23] for details), while in our work, we use it to avoid sampling the inverse of $\mathbf{M}$ so that every operation can be performed in NC^1.

1.3 Possibility on the Extension from Our Proposed NC^1 Fine-Grained Primitives

As described above, the fundamental cryptographic primitives we considered play key roles in a great deal of applications. Hence, our results directly imply the existence of more advanced NC^1-fine-grained primitives. As a simple instance, besides CCA secure PKE schemes, our HPS immediately implies the existence of a non-interactive key exchange scheme according to the recent construction by [27]. However, some NC^1 primitives can not be directly derived from existing ones by adopting previous generic conversions in the polynomial-time world since the resulting primitive may not be in NC^1 any more. For example, although it is well known that pseudorandom functions can be constructed from OWF/OWPs, ones in NC^1 are neither implied by our NC^1-OWP nor the OWF in [16]. It remains open how to construct such fine-grained primitives, and we believe that our works will serve a good starting point.

2 Preliminaries

2.1 Notation

For a distribution D, we denote sampling x according to D by $x \leftarrow D$. For a set S, we denote sampling x from S uniformly at random by $x \leftarrow S$. We denote the set $\{1, \cdots, n\}$ by $[n]$ and the ith element of a vector $\boldsymbol{x}$ by x_i. For a vector $\mathbf{x} \in \{0,1\}^*$, $\mathbf{x}$ will be regarded by default as a column vector. For a matrix $\mathbf{M}$, we denote the sets $\{\mathbf{y} \mid \exists \mathbf{x} \;\; s.t. \;\; \mathbf{y} = \mathbf{M}\mathbf{x}\}$ and $\{\mathbf{x} \mid \mathbf{M}\mathbf{x} = 0\}$ by $\mathrm{Im}(\mathbf{M})$ and $\mathrm{Ker}(\mathbf{M})$ respectively. Let X and Y be random variables over a finite set S. The *statistical distance* between X and Y is defined to be

$$\mathrm{Dist}(X, Y) = \frac{1}{2} \sum_{s \in S} |\Pr[X = s] - \Pr[Y = s]|.$$

We say that X and Y are ϵ-close if $\mathrm{Dist}(X, Y) \leq \epsilon$

We note that all arithmetic computations are over $GF(2)$ in this work. Namely, all arithmetic computations are performed with a modulus of 2. By negl we denote an unspecified negligible function.

2.2 Definitions

In this section, we recall the definitions of a function family, NC^1 circuits, $\oplus\mathsf{L/poly}$.

Definition 1 (Function Family) *A function family is a family of (possibly randomized) functions $\mathcal{F} = \{f_\lambda\}_{\lambda \in \mathbb{N}}$, where for each λ, f_λ has a domain D_λ^f and a range R_λ^f.*

Definition 2 (NC^1) *The class of (non-uniform) NC^1 function families is the set of all function families $\mathcal{F} = \{f_\lambda\}$ for which there is a polynomial p and constant c such that for each λ, f_λ can be computed by a (randomized) circuit of size $p(\lambda)$, depth $c\log(\lambda)$ and fan-in 2 using AND, OR, and NOT gates.*

Definition 3 ($\oplus\mathsf{L/poly}$) *$\oplus\mathsf{L/poly}$ is the set of all boolean function families $\mathcal{F} = \{f_\lambda\}$ for which there is a constant c such that for each λ, there is a non-deterministic Turing machine M_λ such that for each input x with length λ, $M_\lambda(x)$ uses at most $c\log(\lambda)$ space, and $f_\lambda(x)$ is equal to the parity of the number of accepting paths of $M_\lambda(x)$.*

We now give the lemma about the number of solutions for the linear equations defined by a matrix. It is straightforwardly follows from the fact that the rank of $\mathcal{A}$ is $n - 1$.

Lemma 1 *For any $n \times n$ matrix $\mathbf{A}$, if the rank of $\mathbf{A}$ is $n - 1$ and all arithmetic computations are over $GF(2)$, then for any $\mathbf{y} \in \mathrm{Im}(\mathbf{A})$, there exist and only exist two different vectors $\mathbf{x}$ and $\mathbf{x}'$ such that $\mathbf{A}\mathbf{x} = \mathbf{A}\mathbf{x}' = \mathbf{y}$.*

2.3 Definitions in Fine-Grained Cryptography

In this section, we define several cryptographic primitives which are secure against restricted complexity classes of adversaries and easy to run for honest parties. In the following definitions, we denote the class of honest parties by $\mathcal{C}_1$ i.e., function families that compose the primitive are in the class $\mathcal{C}_1$ and the class of adversaries by $\mathcal{C}_2$, and the condition $\mathcal{C}_1 \subseteq \mathcal{C}_2$ is implicit in each definition and hence left unmentioned.

Definition 4 (One-way Function [16]) *Let l be a polynomial in λ. Let $\mathcal{F} = \{f_\lambda : \{0,1\}^\lambda \to \{0,1\}^{l(\lambda)}\}$ be function families. $\mathcal{F}$ is a $\mathcal{C}_1$-*one-way function (OWF) *against $\mathcal{C}_2$ if:*

- **Computability:** *For each λ, f_λ is deterministic.*
- **One-wayness:** *For any $\mathcal{G} = \{g_\lambda : \{0,1\}^{l(\lambda)} \to \{0,1\}^\lambda\}$ and any $\lambda \in \mathbb{N}$:*

$$\Pr\left[f_\lambda(g_\lambda(y)) = y \,\middle|\, \begin{array}{c} x \leftarrow \{0,1\}^\lambda \\ y = f_\lambda(x) \end{array}\right] \le \mathsf{negl}(\lambda).$$

Definition 5 (One-way Permutation) *Let $\mathcal{F} = \{f_\lambda : D_\lambda \to D_\lambda\}$ be function families. $\mathcal{F}$ is a $\mathcal{C}_1$-*one-way permutation (OWP) *against $\mathcal{C}_2$ if:*

- **Permutation:** *For each λ, f_λ is a permutation.*
- **One-wayness:** *For any $\mathcal{G} = \{g_\lambda : D_\lambda \to D_\lambda\}$ and any $\lambda \in \mathbb{N}$:*

$$\Pr\left[g_\lambda(y) = x \,\middle|\, \begin{array}{c} x \leftarrow D_\lambda \\ y = f_\lambda(x) \end{array}\right] \le \mathsf{negl}(\lambda).$$

Definition 6 (Collection of OWPs) *Let $\mathcal{KeyGen} = \{\mathsf{KeyGen}_\lambda : \phi \to K_\lambda\}$ and $\mathcal{Eval} = \{\mathsf{Eval}_\lambda : K_\lambda \times \{0,1\}^\lambda \to \{0,1\}^\lambda\}$ be function families. $(\mathcal{KeyGen}, \mathcal{Eval})$ is a collection of $\mathcal{C}_1$-OWPs against $\mathcal{C}_2$ if:*

- **Permutation:** *For each λ and $k \leftarrow \mathsf{KeyGen}_\lambda$, $\mathsf{Eval}_\lambda(k, \cdot) : D_{\lambda,k} \to D_{\lambda,k}$ is a permutation where $D_{\lambda,k} \subseteq \{0,1\}^\lambda$.*
- **One-wayness:** *For any $\mathcal{G} = \{g_\lambda : K_\lambda \times \{0,1\}^\lambda \to \{0,1\}^\lambda\}$ and any $\lambda \in \mathbb{N}$:*

$$\Pr\left[g_\lambda(k, y) = x \,\middle|\, \begin{array}{c} k \leftarrow \mathsf{KeyGen}_\lambda \\ x \leftarrow D_{\lambda,k} \subseteq \{0,1\}^\lambda \\ y = \mathsf{Eval}_\lambda(k, x) \end{array}\right] \le \mathsf{negl}(\lambda).$$

Definition 7 (Hash Proof System) *Let $PP_\lambda = (X_\lambda,\ L_\lambda,\ W_\lambda,\ R_\lambda,\ SK_\lambda,\ PK_\lambda,\ \Pi_\lambda,\ H_\lambda,\ \alpha_\lambda,\ \mathsf{aux}_\lambda)$ where X_λ is a finite non-empty set, L_λ is a subset of X such that $x \in L_\lambda$ iff there exists a witness $w \in W_\lambda$ with $(x, w) \in R_\lambda \subset X_\lambda \times W_\lambda$, SK_λ is a secret key space, PK_λ is a public key space, Π_λ is a proof space, $H_\lambda : SK_\lambda \times X_\lambda \to \Pi_\lambda$ is a hash function, $\alpha_\lambda : SK_\lambda \to PK_\lambda$ is a projective map, and aux_λ is an auxiliary information. Define the following function families.*

- · *$\mathcal{Setup} = \{\mathsf{Setup}_\lambda : \phi \to PP_\lambda\}$ where Setup_λ outputs a public parameter $\mathsf{pp} \in PP_\lambda$.*
- · *$\mathcal{SampYes} = \{\mathsf{SampYes}_\lambda : PP_\lambda \to R_\lambda\}$ where $\mathsf{SampYes}_\lambda$ on input $\mathsf{pp} \in PP_\lambda$ outputs a random element $x \in L_\lambda$ with a witness $w \in W_\lambda$, i.e., a random element $(x, w) \in R_\lambda$.*
- · *$\mathcal{SampNo} = \{\mathsf{SampNo}_\lambda : PP_\lambda \to X_\lambda \setminus L_\lambda\}$ where SampNo_λ on input $\mathsf{pp} \in PP_\lambda$ outputs a random element $x \in X_\lambda \setminus L_\lambda$.*
- · *$\mathcal{KeyGen} = \{\mathsf{KeyGen}_\lambda : PP_\lambda \to PK_\lambda \times SK_\lambda\}$ where KeyGen_λ on input $\mathsf{pp} \in PP_\lambda$ outputs a public key pk and secret key sk such that $pk = \alpha_\lambda(sk)$.*
- · *$\mathcal{Priv} = \{\mathsf{Priv}_\lambda : PP_\lambda \times SK_\lambda \times X_\lambda \to \Pi_\lambda\}$ where Priv_λ on input $\mathsf{pp} \in PP_\lambda$, $sk \in SK_\lambda$, and an instance $x \in X_\lambda$ outputs its proof $\pi = H_\lambda(sk, x)$.*

· $\mathcal{P}ub = \{\mathsf{Pub}_\lambda : PP_\lambda \times PK_\lambda \times R_\lambda \to \Pi_\lambda\}$ *where* Pub_λ *on input* $\mathsf{pp} \in PP_\lambda$, $pk \in PK_\lambda$, *and an instance with a witness* $(x, w) \in R_\lambda$ *outputs its proof* $\pi \in \Pi_\lambda$.

$(\mathcal{S}etup, \mathcal{S}amp\mathcal{Y}es, \mathcal{S}amp\mathcal{N}o, \mathcal{K}ey\mathcal{G}en, \mathcal{P}riv, \mathcal{P}ub)$ *is a* $\mathcal{C}_1$-hash proof system (HPS) against $\mathcal{C}_2$ *if for any* $\lambda \in \mathbb{N}$, *it holds that:*

- **Correctness**: *For any* $(x, w) \in R_\lambda$, *we have*

$$\mathsf{Priv}_\lambda(\mathsf{pp}, sk, x) = H_\lambda(sk, x) = \mathsf{Pub}_\lambda(\mathsf{pp}, pk, x, w)$$

  where $\mathsf{pp} \leftarrow \mathsf{Setup}_\lambda$ *and* $(pk, sk) \leftarrow \mathsf{KeyGen}_\lambda(\mathsf{pp})$.
- **Subset membership problem**:
  - *The distributions of* x *and* x' *are identical where* $\mathsf{pp} \leftarrow \mathsf{Setup}_\lambda$, $(x, w) \leftarrow \mathsf{SampYes}_\lambda(\mathsf{pp})$, *and* $x' \leftarrow L_\lambda$.
  - *The distributions of* x *and* x' *are identical where* $\mathsf{pp} \leftarrow \mathsf{Setup}_\lambda$, $x \leftarrow \mathsf{SampNo}_\lambda(\mathsf{pp})$, *and* $x' \leftarrow X_\lambda \setminus L_\lambda$.
  - *For any* $\mathcal{G} = \{g_\lambda\} \in \mathcal{C}_2$,

$$|\Pr[g_\lambda(\mathsf{pp}, x_0) = 1] - \Pr[g_\lambda(\mathsf{pp}, x_1) = 1]| \leq \mathsf{negl}(\lambda)$$

  where $\mathsf{pp} \leftarrow \mathsf{Setup}_\lambda$, $(x_0, w) \leftarrow \mathsf{SampYes}_\lambda(\mathsf{pp})$ *and* $x_1 \leftarrow \mathsf{SampNo}_\lambda(\mathsf{pp})$.

$(\mathcal{S}etup, \mathcal{S}amp\mathcal{Y}es, \mathcal{S}amp\mathcal{N}o, \mathcal{K}ey\mathcal{G}en, \mathcal{P}riv, \mathcal{P}ub)$ *is* perfectly smooth $\mathcal{C}_1$-HPS against $\mathcal{C}_2$ *if it satisfies the following property.*

- **Perfect smoothness**: *For any* $\mathsf{pp} \leftarrow \mathsf{Setup}_\lambda$, *the following random variables are identical, i.e.,* 0-*close.*

$$(x, pk, \pi),\ (x, pk, \pi')$$

  where $\mathbf{x} \leftarrow \mathsf{SampNo}_\lambda(\mathsf{pp})$, $(pk, sk) \leftarrow \mathsf{KeyGen}_\lambda(\mathsf{pp})$, $\pi = \mathsf{Priv}_\lambda(\mathsf{pp}, sk, x)$, *and* $\pi' \leftarrow \Pi$.

$(\mathcal{S}etup, \mathcal{S}amp\mathcal{Y}es, \mathcal{S}amp\mathcal{N}o, \mathcal{K}ey\mathcal{G}en, \mathcal{P}riv, \mathcal{P}ub)$ *is* ϵ-universal$_1$ $\mathcal{C}_1$-HPS against $\mathcal{C}_2$ *if it satisfies the following property.*

- **ϵ-universality$_1$**: *For any* $\mathsf{pp} \leftarrow \mathsf{Setup}_\lambda$, $pk \in PK_\lambda$, $x \in X_\lambda \backslash L_\lambda$ *and* $\pi \in \Pi_\lambda$, *it holds that*

$$\Pr[\mathsf{Priv}_\lambda(\mathsf{pp}, sk, x) = \pi \mid \alpha_\lambda(sk) = pk] \leq \epsilon.$$

  If ϵ *is a negligible function, then* $(\mathcal{S}etup,\ \mathcal{S}amp\mathcal{Y}es,\ \mathcal{S}amp\mathcal{N}o,\ \mathcal{K}ey\mathcal{G}en,\ \mathcal{P}riv,\ \mathcal{P}ub)$ *is a* strong universal$_1$ $\mathcal{C}_1$-HPS against $\mathcal{C}_2$.

$(\mathcal{S}etup, \mathcal{S}amp\mathcal{Y}es, \mathcal{S}amp\mathcal{N}o, \mathcal{K}ey\mathcal{G}en, \mathcal{P}riv, \mathcal{P}ub)$ *is* ϵ-universal$_2$ $\mathcal{C}_1$-HPS against $\mathcal{C}_2$ *if it satisfies the following property.*

- **ϵ-universality$_2$**: *For any* $\mathsf{pp} \leftarrow \mathsf{Setup}_\lambda$, $pk \in PK_\lambda$, $x, x^* \in X_\lambda$ *and* $\pi, \pi^* \in \Pi_\lambda$ *with* $x \notin L_\lambda \cup \{x^*\}$, *it holds that*

$$\Pr[\mathsf{Priv}_\lambda(\mathsf{pp}, sk, x) = \pi \mid \mathsf{Priv}_\lambda(\mathsf{pp}, sk, x^*) = \pi^* \wedge \alpha_\lambda(sk) = pk] \leq \epsilon.$$

  If ϵ *is a negligible function, then* $(\mathcal{S}etup,\ \mathcal{S}amp\mathcal{Y}es,\ \mathcal{S}amp\mathcal{N}o,\ \mathcal{K}ey\mathcal{G}en,\ \mathcal{P}riv,\ \mathcal{P}ub)$ *is a* strong universal$_2$ $\mathcal{C}_1$-HPS against $\mathcal{C}_2$.

Definition 8 (Trapdoor One-Way Function) *Let* $\mathcal{KeyGen} = \{\mathsf{KeyGen}_\lambda : \phi \to EK_\lambda \times TK_\lambda\}$*,* $\mathcal{Eval} = \{\mathsf{Eval}_\lambda : EK_\lambda \times \mathcal{D}_\lambda \to \mathcal{R}_\lambda\}$ *and* $\mathcal{Inverse} = \{\mathsf{Inverse}_\lambda : TK_\lambda \times \mathcal{D}_\lambda \to \mathcal{R}_\lambda\}$ *be a function families where* $\mathcal{D}_\lambda$ *and* $\mathcal{R}_\lambda$ *are determined by the key pair* (ek, tk) *generated by* KeyGen_λ*.* $(\mathcal{KeyGen}, \mathcal{Eval}, \mathcal{Inverse})$ *is a* $\mathcal{C}_1$-trapdoor one-way function (TDF) against $\mathcal{C}_2$ *if:*

- **Correctness:** *For any* $\lambda \in \mathbb{N}$*, any* $(ek, tk) \leftarrow \mathsf{KeyGen}_\lambda$*, and any* $X \in \mathcal{D}_\lambda$*:*

$$\mathsf{Inverse}_\lambda(tk, \mathsf{Eval}_\lambda(ek, X)) = X.$$

- **One-wayness:** *For any* $\mathcal{G} = \{g_\lambda\} \in \mathcal{C}_2$*, and any* $\lambda \in \mathbb{N}$*:*

$$\Pr\left[\mathsf{Eval}_\lambda(ek, g_\lambda(ek, Y)) = Y \;\middle|\; \begin{array}{c} (ek, tk) \leftarrow \mathsf{KeyGen}_\lambda \\ X \leftarrow \mathcal{D}_\lambda \\ Y = \mathsf{Eval}_\lambda(ek, X) \end{array}\right] \leq \mathsf{negl}(\lambda).$$

2.4 Sampling Procedure

In this section, we recall the sampling procedure in [16], and then show several lemmas on the sampling procedure that will be used later in the security proofs.

Construction 1 (Sampling Procedure) *Let* $\mathbf{M}_0^n$ *and* $\mathbf{M}_1^n$ *be the following* $n \times n$ *matrices:*

$$\mathbf{M}_0^n = \begin{pmatrix} 0 & & \cdots & 0 & 0 \\ 1 & 0 & & & 0 \\ 0 & 1 & \ddots & & \vdots \\ \vdots & \vdots & \ddots & 0 \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}, \ \mathbf{M}_1^n = \begin{pmatrix} 0 & & \cdots & 0 & 1 \\ 1 & 0 & & & 0 \\ 0 & 1 & \ddots & & \vdots \\ \vdots & \vdots & \ddots & 0 \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}.$$

- $\mathsf{LSamp}(n)$*:*
  1. *Output the following* $n \times n$ *upper triangular matrix:*

$$\begin{pmatrix} 1 & r_{1,2} & \cdots & r_{1,n-1} & r_{1,n} \\ 0 & 1 & r_{2,3} & \cdots & r_{2,n} \\ 0 & 0 & \ddots & & \vdots \\ \vdots & \vdots & \ddots & 1 & r_{n-1,n} \\ 0 & \cdots & 0 & 0 & 1 \end{pmatrix}$$

  where $r_{i,j} \leftarrow \{0, 1\}$.

- $\mathsf{RSamp}(n)$*:*
  1. *Output the following* $n \times n$ *matrix:*

$$\begin{pmatrix} 1 & & \cdots & 0 & r_1 \\ 0 & 1 & & & r_2 \\ 0 & 0 & \ddots & & \vdots \\ \vdots & \vdots & \ddots & 1 & r_{n-1} \\ 0 & \cdots & 0 & 0 & 1 \end{pmatrix}$$

  where $r_i \leftarrow \{0, 1\}$.

- $\mathsf{ZeroSamp}$*(n):*
  1. *Sample* $\mathbf{R}_1 \leftarrow \mathsf{LSamp}(n)$ *and* $\mathbf{R}_2 \leftarrow \mathsf{RSamp}(n)$*.*
  2. *Output* $\mathbf{R}_1\mathbf{M}_0^n\mathbf{R}_2$*.*
- $\mathsf{OneSamp}$*(n):*
  1. *Sample* $\mathbf{R}_1 \leftarrow \mathsf{LSamp}(n)$ *and* $\mathbf{R}_2 \leftarrow \mathsf{RSamp}(n)$*.*
  2. *Output* $\mathbf{R}_1\mathbf{M}_1^n\mathbf{R}_2$*.*

Here, the output of $\mathsf{ZeroSamp}(n)$ *is always a matrix of rank* $n-1$ *and the output of* $\mathsf{OneSamp}(n)$ *is always a matrix of full rank.*

Lemma 2 ([29, 5]) *If* $\mathsf{NC}^1 \subsetneq \oplus\mathsf{L/poly}$*, then there is a polynomial* n *such that for any family* $\mathcal{F} = \{f_\lambda\}$ *in* NC^1 *and any* $\lambda \in \mathbb{N}$*, we have*

$$\begin{aligned}&|\Pr[f_\lambda(\mathbf{M}) = 1 \mid \mathbf{M} \leftarrow \mathsf{ZeroSamp}(n(\lambda))] - \\ &\qquad \Pr[f_\lambda(\mathbf{M}') = 1 \mid \mathbf{M}' \leftarrow \mathsf{OneSamp}(n(\lambda))]| \leq \mathsf{negl}(\lambda).\end{aligned}$$

Lemma 3 *For any* $\mathbf{M} \leftarrow \mathsf{ZeroSamp}(n)$*, it holds that* $\mathrm{Ker}(\mathbf{M}) = \{\mathbf{0}, \mathbf{k}\}$ *where* $\mathbf{k}$ *is a vector such that* $\mathbf{k} \in \{0,1\}^{n-1} \times 1$*.*

Proof. $\mathbf{M}$ is a matrix sampled from $\mathsf{ZeroSamp}(n)$, i.e.,

$$\begin{aligned}\mathbf{M} &= \mathbf{R}_1\mathbf{M}_1^n\mathbf{R}_2 \\ &= \mathbf{R}_1 \begin{pmatrix} 0 & & \cdots & 0 & 0 \\ 1 & 0 & & & 0 \\ 0 & 1 & \ddots & & \vdots \\ \vdots & \vdots & \ddots & 0 & \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & & \cdots & 0 & r_1 \\ 0 & 1 & & & r_2 \\ 0 & 0 & \ddots & & \vdots \\ \vdots & \vdots & \ddots & 1 & r_{n-1} \\ 0 & \cdots & 0 & 0 & 1 \end{pmatrix}\end{aligned}$$

where $\mathbf{R}_1 \leftarrow \mathsf{LSamp}(n)$ and $\mathbf{R}_2 \leftarrow \mathsf{RSamp}(n)$. Then, we have $\mathbf{k} = (r_1 r_2 \cdots 1)^\top \in \mathrm{Ker}(\mathbf{M})$ since

$$\begin{aligned}\mathbf{M} &= \mathbf{R}_1\mathbf{M}_1^n\mathbf{R}_2\mathbf{k} \\ &= \mathbf{R}_1 \begin{pmatrix} 0 & & \cdots & 0 & 0 \\ 1 & 0 & & & 0 \\ 0 & 1 & \ddots & & \vdots \\ \vdots & \vdots & \ddots & 0 & \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & & \cdots & 0 & r_1 \\ 0 & 1 & & & r_2 \\ 0 & 0 & \ddots & & \vdots \\ \vdots & \vdots & \ddots & 1 & r_{n-1} \\ 0 & \cdots & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_{n-1} \\ 1 \end{pmatrix} \\ &= \mathbf{R}_1 \begin{pmatrix} 0 & & \cdots & 0 & 0 \\ 1 & 0 & & & 0 \\ 0 & 1 & \ddots & & \vdots \\ \vdots & \vdots & \ddots & 0 & \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} = \mathbf{R}_1\mathbf{0} = \mathbf{0}.\end{aligned}$$

Moreover, according to Lemma 1, there are only two vectors $\boldsymbol{v}$ such that $\mathbf{M}\boldsymbol{v} = \mathbf{0}$. Therefore, we have $\mathrm{Ker}(\mathbf{M}) = \{\mathbf{0}, \mathbf{k}\}$, completing the proof of Lemma 3. □

Lemma 4 *For any* $\mathbf{M} \leftarrow \mathsf{ZeroSamp}(n)$*, it holds that* $\mathrm{Ker}(\mathbf{M}^\top) = \{\mathbf{0}, \mathbf{k}\}$ *where* $\mathbf{k}$ *is a vector such that* $\mathbf{k} \in 1 \times \{0,1\}^{n-1}$.

Proof. $\mathbf{M}$ is a matrix sampled from $\mathsf{ZeroSamp}(n)$ i.e., $\mathbf{M} = \mathbf{R}_1\mathbf{M}_0^n\mathbf{R}_2$, where $\mathbf{R}_1 \leftarrow \mathsf{LSamp}(n)$, $\mathbf{R}_2 \leftarrow \mathsf{RSamp}(n)$. Since $\mathbf{R}_1^\top$ has full rank, the equation $\mathbf{R}_1^\top\mathbf{x} = (1\ 0\ \cdots\ 0)^\top$ has a unique solution $\mathbf{x}^*$. $\mathbf{x}^*$ is in the kernel of $\mathbf{M}^\top$ since $\mathbf{R}_2^\top\mathbf{M}_0^{n\top}\mathbf{R}_1^\top\mathbf{x}^* = \mathbf{R}_2^\top\mathbf{M}_0^{n\top}(1\ 0\ \cdots\ 0)^\top = \mathbf{R}_2^\top\mathbf{0} = \mathbf{0}$. According to the following equation

$$\mathbf{R}_1^\top\mathbf{x}^* = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ r_{2,1} & 1 & 0 & \cdots & 0 \\ r_{3,1} & r_{3,2} & \ddots & & \vdots \\ \vdots & \vdots & \ddots & 1 & 0 \\ r_{n,1} & \cdots & & r_{n,n-1} & 1 \end{pmatrix} \begin{pmatrix} x_1^* \\ x_2^* \\ x_3^* \\ \vdots \\ x_n^* \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

we have $x_1^* = 1$, i.e., $\mathbf{x} \in 1 \times \{0,1\}^{n-1}$.

Moreover, according to Lemma 1 and the fact that the rank of $\mathbf{M}^\top$ is $n-1$, there are only two vectors $\boldsymbol{v}$ such that $\mathbf{M}^\top\boldsymbol{v} = \mathbf{0}$. Therefore, we have $\mathrm{Ker}(\mathbf{M}^\top) = \{\mathbf{0}, \mathbf{x}^*\}$, completing the proof of Lemma 4. □

Lemma 5 *For any* $\mathbf{M} \leftarrow \mathsf{ZeroSamp}(\lambda)$*, it holds that*

$$\mathrm{Im}(\mathbf{M}^\top) = \{\mathbf{x} | \mathbf{w} \in 0 \times \{0,1\}^{\lambda-1}, \mathbf{x} = \mathbf{M}^\top\mathbf{w}\} = \{\mathbf{x} | \mathbf{w} \in 1 \times \{0,1\}^{\lambda-1}, \mathbf{x} = \mathbf{M}^\top\mathbf{w}\}.$$

Proof. Let U be a set such that $U = \{\mathbf{x} | \mathbf{w} \in 0 \times \{0,1\}^{\lambda-1}, \mathbf{x} = \mathbf{M}^\top\mathbf{w}\}$ and V be a set such that $V = \{\mathbf{x} | \mathbf{w} \in 1 \times \{0,1\}^{\lambda-1}, \mathbf{x} = \mathbf{M}^\top\mathbf{w}\}$. Let $\mathbf{k}$ be a non-zero vector such that $\mathbf{k} \in \mathrm{Ker}(\mathbf{M}^\top)$. According to Lemma 4, we have $\mathbf{k} \in 1 \times \{0,1\}^{\lambda-1}$. Therefore, for any $\mathbf{x} \in U$ such that $\mathbf{x} = \mathbf{M}^\top\mathbf{w}$ where $\mathbf{w} \in 0 \times \{0,1\}^{\lambda-1}$, we have $\mathbf{x} = \mathbf{M}^\top\mathbf{w} = \mathbf{M}^\top(\mathbf{w}+\mathbf{k}) \in V$ since $(\mathbf{w}+\mathbf{k}) \in 1 \times \{0,1\}^{\lambda-1}$. Moreover, for any $\mathbf{x} \in V$ such that $\mathbf{x} = \mathbf{M}^\top\mathbf{w}$ where $\mathbf{w} \in 1 \times \{0,1\}^{\lambda-1}$, we have $\mathbf{x} = \mathbf{M}^\top\mathbf{w} = \mathbf{M}^\top(\mathbf{w}+\mathbf{k}) \in U$ since $(\mathbf{w}+\mathbf{k}) \in 0 \times \{0,1\}^{\lambda-1}$. Therefore, we have $U = V$ and it follows that $\mathrm{Im}(\mathbf{M}^\top) = U \cup V = U \cup U = U = \{\mathbf{x} | \mathbf{w} \in 0 \times \{0,1\}^{\lambda-1}, \mathbf{x} = \mathbf{M}^\top\mathbf{w}\}$. In the same way, we have $\mathrm{Im}(\mathbf{M}^\top) = U \cup V = V \cup V = V = \{\mathbf{x} | \mathbf{w} \in 1 \times \{0,1\}^{\lambda-1}, \mathbf{x} = \mathbf{M}^\top\mathbf{w}\}$. As a result, we have

$$\mathrm{Im}(\mathbf{M}^\top) = \{\mathbf{x} | \mathbf{w} \in 0 \times \{0,1\}^{\lambda-1}, \mathbf{x} = \mathbf{M}^\top\mathbf{w}\} = \{\mathbf{x} | \mathbf{w} \in 1 \times \{0,1\}^{\lambda-1}, \mathbf{x} = \mathbf{M}^\top\mathbf{w}\},$$

completing the proof of Lemma 5. □

Lemma 6 *The distributions of* $\mathbf{M} + \mathbf{N}$ *and* $\mathbf{M}'$ *are identical, where* $\mathbf{M} \leftarrow \mathsf{ZeroSamp}(\lambda)$*,* $\mathbf{M}' \leftarrow \mathsf{OneSamp}(\lambda)$*, and* $\mathbf{N}$ *is the following matrix.*

$$\mathbf{N} = \begin{pmatrix} 0 \cdots & 0 & 1 \\ 0 & 0 & \cdots 0 \\ \vdots & & \ddots \vdots \\ 0 \cdots & 0 & 0 \end{pmatrix}.$$

Proof. For $\mathbf{R}_1 \leftarrow \mathsf{LSamp}(\lambda)$ and $\mathbf{R}_2 \leftarrow \mathsf{RSamp}(\lambda)$, we have

$$\begin{aligned}
\mathbf{M}' = \mathbf{R}_1\mathbf{M}_1^{\lambda}\mathbf{R}_2 &= \mathbf{R}_1 \begin{pmatrix} 0 & & \cdots & 0 & 1 \\ 1 & 0 & & \vdots & 0 \\ \vdots & \vdots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix} \mathbf{R}_2 \\
&= \mathbf{R}_1 \begin{pmatrix} 0 & & \cdots & 0 & 0 \\ 1 & 0 & & \vdots & 0 \\ \vdots & \vdots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix} \mathbf{R}_2 + \mathbf{R}_1 \begin{pmatrix} 0 & & \cdots & 0 & 1 \\ 0 & 0 & & \vdots & 0 \\ \vdots & \vdots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 0 & 0 \end{pmatrix} \mathbf{R}_2 \\
&= \mathbf{R}_1 \begin{pmatrix} 0 & & \cdots & 0 & 0 \\ 1 & 0 & & \vdots & 0 \\ \vdots & \vdots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix} \mathbf{R}_2 + \begin{pmatrix} 0 & & \cdots & 0 & 1 \\ 0 & 0 & & \vdots & 0 \\ \vdots & \vdots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 0 & 0 \end{pmatrix} \\
&= \mathbf{R}_1\mathbf{M}_0^{\lambda}\mathbf{R}_2 + \mathbf{N} = \mathbf{M} + \mathbf{N}.
\end{aligned}$$

Hence, the distributions of $\mathbf{M} + \mathbf{N}$ and $\mathbf{M}'$ are identical for $\mathbf{M} \leftarrow \mathsf{ZeroSamp}(\lambda)$ and $\mathbf{M}' \leftarrow \mathsf{OneSamp}(\lambda)$, completing the proof of Lemma 6. □

3 Construction of NC^1-OWP against NC^1

In this section, we first give our construction of a collection of NC^1-OWPs against NC^1 under the assumption $\mathsf{NC}^1 \subsetneq \oplus\mathsf{L/poly}$. Next, we extend it to a NC^1-OWP against NC^1 based on the same assumption.

Construction 2 (Collection of NC^1-OWPs) *Let λ be a security parameter. We define the families $\mathcal{KeyGen} = \{\mathsf{KeyGen}_\lambda\}$ with key spaces $\{K_\lambda = \{\mathbf{M} \mid \mathbf{M} \in \mathsf{OneSamp}(\lambda)\}\}$ and $\mathcal{Eval} = \{\mathsf{Eval}_\lambda\}$ as follows.*

- KeyGen_λ*:*
  1. *Sample* $\mathbf{M} \leftarrow \mathsf{OneSamp}(\lambda)$*.*
  2. *Output* $\mathbf{M}$ *(which defines the domain as $D_{\lambda,\mathbf{M}} := \{0,1\}^\lambda$).*
- $\mathsf{Eval}_\lambda(\mathbf{M}, \mathbf{x})$*:*
  1. *Compute* $\mathbf{y} := \mathbf{M}\mathbf{x}$ *and output* $\mathbf{y}$*.*

Theorem 1 *($\mathcal{KeyGen}, \mathcal{Eval}$) defined as Construction 2 is a collection of* NC^1*-OWPs against* NC^1 *under the assumption* $\mathsf{NC}^1 \subsetneq \oplus\mathsf{L/poly}$*.*

Proof sketch. As described in Introduction, our construction is essentially a "lossy function". More specifically, it is straightforward that our scheme is a permutation, since $\mathbf{M}$ is of full rank when $\mathbf{M} \leftarrow \mathsf{OneSamp}(\lambda)$. Moreover, when we generate $\mathbf{M} \leftarrow \mathsf{ZeroSamp}(\lambda)$ instead of $\mathbf{M} \leftarrow \mathsf{OneSamp}(\lambda)$ in KeyGen_λ, we can prove that an adversary $\mathcal{A}$ breaking the one-wayness of our construction with probability ϵ can also be used to find a second pre-image $\mathbf{x}'$ for $\mathsf{Eval}_\lambda(\mathbf{M}, \mathbf{x})$ such that $\mathbf{x} \neq \mathbf{x}'$ with probability $\frac{1}{2}\epsilon$. This is due to the fact that $\mathbf{M}$ is not of full rank in this case and $\mathcal{A}$ has no information on whether the pre-image is $\mathbf{x}$ or $\mathbf{x}'$. However, it is unlikely that $\mathcal{A}$ can find such a second pre-image, since this construction is indistinguishable with the original one, where $\mathbf{M}$ is generated as $\mathbf{M} \leftarrow \mathsf{OneSamp}(\lambda)$ and there exists no second pre-image for each $\mathbf{M}$. Therefore, we can conclude that this scheme is one-way, which immediately gives us the one-wayness of the original scheme (due to the indistinguishability between $\mathsf{OneSamp}(\lambda)$ and $\mathsf{ZeroSamp}(\lambda)$).

The formal proof is as follows.

Proof. First note that both $\mathcal{KeyGen}$ and $\mathcal{Eval}$ are computable in NC^1, since they only involve operations including multiplications of a constant number of matrices, inner products, and sampling random bits. We now show that $(\mathcal{KeyGen}, \mathcal{Eval})$ satisfies computability and one-wayness.

Permutation. Since for $\mathbf{M} \leftarrow \mathsf{OneSamp}_\lambda$, $\mathbf{M}$ is a full rank matrix, we have that $\mathsf{Eval}_\lambda(\mathbf{M}, \mathbf{x}) = \mathbf{M}\mathbf{x} \in D_{\lambda,\mathbf{M}} = \{0,1\}^\lambda$ is a permutation.

One-wayness. Let $\mathcal{A} = \{a_\lambda\}$ be any adversary in NC^1. We give hybrid games to show that the advantage of $\mathcal{A}$ in breaking the one-wayness of Construction 2 is negligible.

Game 0: This is the original one-wayness game for $\mathcal{A} = \{a_\lambda\}$. $\mathcal{CH}$ runs $\mathbf{M} \leftarrow \mathsf{KeyGen}_\lambda$ and samples $\mathbf{x} \leftarrow \{0,1\}^\lambda$. Then, it runs $\mathbf{y} = \mathsf{Eval}_\lambda(\mathbf{M}, \mathbf{x})$ and sends $\mathbf{y}$ to a_λ. a_λ succeeds if it outputs $\tilde{\mathbf{x}}$ such that $\mathbf{x} = \tilde{\mathbf{x}}$. Otherwise, it fails.

Game 1: This game is the same as **Game 0** except that $\mathcal{CH}$ runs $\mathsf{ZeroSamp}(\lambda)$ instead of $\mathsf{OneSamp}(\lambda)$ in the key generation procedure.

Lemma 7 *If $\mathcal{A} = \{a_\lambda\}$ succeeds with advantage ϵ_0 (resp., ϵ_1) in* **Game 0** *(resp.,* **Game 1***), then $|\epsilon_0 - \epsilon_1| = \mathsf{negl}(\lambda)$.*

Proof. We now construct $\mathcal{B} = \{b_\lambda\} \in \mathsf{NC}^1$ that distinguishes $\mathbf{M} \leftarrow \mathsf{ZeroSamp}(\lambda)$ and $\mathbf{M} \leftarrow \mathsf{OneSamp}(\lambda)$ with advantage $|\epsilon_0 - \epsilon_1|$, which contradicts to Lemma 2.

b_λ takes as input $\mathbf{M}$, which is generated as $\mathbf{M} \leftarrow \mathsf{ZeroSamp}(\lambda)$ or $\mathbf{M} \leftarrow \mathsf{OneSamp}(\lambda)$ from its challenger. Then, it samples $\mathbf{x} \leftarrow \{0,1\}^\lambda$. Next, b_λ runs $\mathbf{y} = \mathsf{Eval}_\lambda(\mathbf{M}, \mathbf{x})$ and sends $\mathbf{y}$ to a_λ. When a_λ outputs $\tilde{\mathbf{x}}$, if $\mathbf{x} = \tilde{\mathbf{x}}$, b_λ outputs 1. Otherwise, it outputs 0.

Since all operations in b_λ are performed in NC^1, we have $\mathcal{B} = \{b_\lambda\} \in \mathsf{NC}^1$.

One can see that when $\mathbf{M} \leftarrow \mathsf{ZeroSamp}(\lambda)$ (resp., $\mathbf{M} \leftarrow \mathsf{OneSamp}(\lambda)$), the view of a_λ is identical to its view in **Game 0** (resp., **Game 1**), i.e., b_λ outputs 1 with probability ϵ_0 (resp., ϵ_1). Therefore, $\mathcal{B} = \{b_\lambda\}$ distinguishes $\mathbf{M} \leftarrow \mathsf{ZeroSamp}(\lambda)$ and $\mathbf{M} \leftarrow \mathsf{OneSamp}(\lambda)$ with advantage $|\epsilon_0 - \epsilon_1|$, which should be negligible according to Lemma 2, completing the proof of Lemma 7. □

Game 2: This game is the same as **Game 1** except that a_λ succeeds if $\mathbf{x} \neq \tilde{\mathbf{x}} \wedge \mathsf{Eval}_\lambda(\mathbf{M}, \mathbf{x}) = \mathsf{Eval}(\mathbf{M}, \tilde{\mathbf{x}})$.

Lemma 8 *If $\mathcal{A} = \{a_\lambda\}$ succeeds with advantage ϵ_1 (resp., ϵ_2) in* **Game 1** *(resp.,* **Game 2***), then $\epsilon_1 = \epsilon_2$.*

Proof. According to Lemma 1 and due to the fact that the rank of $\mathbf{M} \leftarrow \mathsf{ZeroSamp}(\lambda)$ is $\lambda - 1$, for any $\mathbf{y} \in \mathrm{Im}(\mathbf{M})$, there are two vectors $\mathbf{x}, \mathbf{x}'$ such that $\mathbf{M}\mathbf{x} = \mathbf{M}\mathbf{x}' = \mathbf{y} \wedge \mathbf{x} \neq \mathbf{x}'$, and we have

$$\begin{aligned}
\epsilon_1 &= \Pr\left[\tilde{\mathbf{x}} = \mathbf{x}^* \,\middle|\, \begin{array}{c} \mathbf{x}^* \leftarrow \{\mathbf{x}, \mathbf{x}'\} \\ \mathbf{y} = \mathbf{M}\mathbf{x}^* \\ \tilde{\mathbf{x}} \leftarrow a_\lambda(\mathbf{y}) \end{array}\right] \\
&= \frac{1}{2}\Pr\left[\tilde{\mathbf{x}} = \mathbf{x} \,\middle|\, \begin{array}{c} \mathbf{x}^* = \mathbf{x} \\ \mathbf{y} = \mathbf{M}\mathbf{x}^* \\ \tilde{\mathbf{x}} \leftarrow a_\lambda(\mathbf{y}) \end{array}\right] + \frac{1}{2}\Pr\left[\tilde{\mathbf{x}} = \mathbf{x}' \,\middle|\, \begin{array}{c} \mathbf{x}^* = \mathbf{x}' \\ \mathbf{y} = \mathbf{M}\mathbf{x}^* \\ \tilde{\mathbf{x}} \leftarrow a_\lambda(\mathbf{y}) \end{array}\right] \\
&= \frac{1}{2}\Pr\left[\tilde{\mathbf{x}} = \mathbf{x} \,\middle|\, \begin{array}{c} \mathbf{x}^* = \mathbf{x}' \\ \mathbf{y} = \mathbf{M}\mathbf{x}^* \\ \tilde{\mathbf{x}} \leftarrow a_\lambda(\mathbf{y}) \end{array}\right] + \frac{1}{2}\Pr\left[\tilde{\mathbf{x}} = \mathbf{x}' \,\middle|\, \begin{array}{c} \mathbf{x}^* = \mathbf{x} \\ \mathbf{y} = \mathbf{M}\mathbf{x}^* \\ \tilde{\mathbf{x}} \leftarrow a_\lambda(\mathbf{y}) \end{array}\right] \\
&= \Pr\left[\begin{array}{c} \tilde{\mathbf{x}} \neq \mathbf{x}^* \wedge \\ \mathsf{Eval}_\lambda(\mathbf{M}, \tilde{\mathbf{x}}) = \mathsf{Eval}_\lambda(\mathbf{M}, \mathbf{x}^*) \end{array} \,\middle|\, \begin{array}{c} \mathbf{x}^* \leftarrow \{\mathbf{x}, \mathbf{x}'\} \\ \mathbf{y} = \mathbf{M}\mathbf{x}^* \\ \tilde{\mathbf{x}} \leftarrow a_\lambda(\mathbf{y}) \end{array}\right] = \epsilon_2,
\end{aligned}$$

completing the proof of Lemma 8.

Lemma 9 *If $\mathcal{A} = \{a_\lambda\}$ succeeds with advantage ϵ_2 in* **Game 2***, then $\epsilon_2 = \mathsf{negl}(\lambda)$.*

Proof. We now construct $\mathcal{B} = \{b_\lambda\} \in \mathsf{NC}^1$ that distinguishes $\mathbf{M} \leftarrow \mathsf{ZeroSamp}(\lambda)$ and $\mathbf{M} \leftarrow \mathsf{OneSamp}(\lambda)$ with advantage ϵ_2, which contradicts to Lemma 2.

b_λ takes as input $\mathbf{M}$, which is generated as $\mathbf{M} \leftarrow \mathsf{ZeroSamp}(\lambda)$ or $\mathbf{M} \leftarrow \mathsf{OneSamp}(\lambda)$ from its challenger. Then, it samples $\mathbf{x} \leftarrow \{0,1\}^\lambda$. Next, b_λ runs $\mathbf{y} = \mathsf{Eval}_\lambda(\mathbf{M}, \mathbf{x})$ and send $\mathbf{y}$ to a_λ. When a_λ outputs $\tilde{\mathbf{x}}$, if $\mathbf{x} \neq \tilde{\mathbf{x}} \wedge \mathbf{y} = \mathsf{Eval}_\lambda(\mathbf{M}, \mathbf{x})$, b_λ outputs 1. Otherwise, it outputs 0.

Since all operations in b_λ are performed in NC^1, we have $\mathcal{B} = \{b_\lambda\} \in \mathsf{NC}^1$.

One can see that when $\mathbf{M} \leftarrow \mathsf{ZeroSamp}(\lambda)$, the view of a_λ is identical to its view in **Game 2**, i.e., b_λ outputs 1 with probability ϵ_2.

When $\mathbf{M} \leftarrow \mathsf{OneSamp}(\lambda)$, since $\mathsf{Eval}(\mathbf{M}, \tilde{\mathbf{x}})$ is permutation, there is no vector $\tilde{\mathbf{x}}$ such that $\mathbf{x} \neq \tilde{\mathbf{x}} \wedge \mathbf{y} = \mathsf{Eval}_\lambda(\mathbf{k}, \mathbf{x})$, i.e. b_λ outputs 1 with probability 0.

Therefore, $\mathcal{B} = \{b_\lambda\}$ distinguishes $\mathbf{M} \leftarrow \mathsf{ZeroSamp}(\lambda)$ and $\mathbf{M} \leftarrow \mathsf{OneSamp}(\lambda)$ with advantage ϵ_2, which should be negligible according to Lemma 2, completing the proof of Lemma 9. □

Since $|\epsilon_0 - \epsilon_1| = \mathsf{negl}(\lambda)$, $\epsilon_1 = \epsilon_2$, and $\epsilon_2 = \mathsf{negl}(\lambda)$, we have

$$\epsilon_0 \leq |\epsilon_0 - \epsilon_1| + \epsilon_1 = \mathsf{negl}(\lambda) + \epsilon_2 = \mathsf{negl}(\lambda),$$

i.e., Construction 2 satisfies one-wayness. This completes the proof of Theorem 1. □

Extension to NC^1-OWPs against NC^1. We now show a transformation from collections of NC^1-OWPs against NC^1, where the output distributions of the key generation algorithms are uniformly random over key space, to NC^1-OWPs against NC^1. Specifically, given a collection of OWPs $\{f_k : D_k \to D_k\}_{k \in K}$ where K is the key space, we construct a OWP $g : D \to D$ where $D := \bigcup_{k \in K}(\{k\} \times D_k)$ and $g((k, x) \in D) = (k, f_k(x))$. This transformation can be applied in NC^1, and the properties of permutation and one-wayness of g hold due to those properties of f. Note that in [5], it is shown that $\mathsf{OneSamp}(\lambda)$ samples $\mathbf{M} \leftarrow \{\mathbf{M} \in \mathsf{OneSamp}(\lambda)\}$ uniformly. Thus, KeyGen_λ of our construction samples $k \leftarrow K_\lambda = \{\mathbf{M} \mid \mathbf{M} \in \mathsf{OneSamp}(\lambda)\}$ uniformly, and we can apply this transformation to our collection of NC^1-OWPs against NC^1. We refer the reader to the full paper for the details.

Computability in $\mathsf{AC}^0[2]$. Perhaps interestingly, our one-way permutation can be run by an even smaller class of circuits $\mathsf{AC}^0[2]$, which satisfies $\mathsf{AC}^0[2] \subsetneq \mathsf{NC}^1$ [39, 41] and consists of constant-depth circuits with $\mathsf{MOD2}$ gates. The reason is that it only involves multiplications of a constant number of matrices, inner products, and sampling random bits. Due to the same reason, our constructions of single-bit HPS introduced later in Section 4 is also computable in $\mathsf{AC}^0[2]$.

4 Construction of NC^1-HPS against NC^1

In this section, we start by giving a construction of perfectly smooth and $\frac{1}{2}$-universal$_1$ NC^1-HPS against NC^1 such that the proof space is one-bit. Next, we turn this construction into a perfectly smooth and strong universal$_1$ NC^1-HPS against NC^1 such that the proof space is multi-bit. Finally, we construct a strong universal$_2$ NC^1-HPS against NC^1 such that the language L supports $\{0, 1\}^n$.

4.1 Perfectly Smooth and Universal$_1$ for One-Bit

In this section, we give our construction of perfectly smooth and $\frac{1}{2}$-universal$_1$ NC^1-HPS against NC^1 circuits under the assumption $\mathsf{NC}^1 \subsetneq \oplus\mathsf{L/poly}$.

Construction 3 (NC^1-HPS) *Let λ be a security parameter. We define the families $\mathcal{S}etup = \{\mathsf{Setup}_\lambda\}$, $\mathcal{S}amp\mathcal{Y}es = \{\mathsf{SampYes}_\lambda\}$, $\mathcal{S}amp\mathcal{N}o = \{\mathsf{SampNo}_\lambda\}$, $\mathcal{K}ey\mathcal{G}en = \{\mathsf{KeyGen}_\lambda\}$, $\mathcal{P}riv = \{\mathsf{Priv}_\lambda\}$ and $\mathcal{P}ub = \{\mathsf{Pub}_\lambda\}$ as follows.*

- Setup_λ*:*
  1. *Sample* $\mathbf{M} \leftarrow \mathsf{ZeroSamp}(\lambda)$.
  2. *Output* $\mathsf{pp} = (X_\lambda, L_\lambda, W_\lambda, R_\lambda, SK_\lambda, PK_\lambda, \Pi_\lambda, H_\lambda, \alpha_\lambda, \mathsf{aux}_\lambda)$ *where*
     - $X_\lambda := \{0, 1\}^\lambda$.
     - $L_\lambda := \{\mathbf{x} | \mathbf{w} \in 1 \times \{0, 1\}^{\lambda-1}, \mathbf{x} = \mathbf{M}\mathbf{w}\} = \mathrm{Im}(\mathbf{M}^\top)$ *($\because$ Lemma 5).*
     - $W_\lambda := 1 \times \{0, 1\}^{\lambda-1}$.
     - $R_\lambda := \{(\mathbf{x}, \mathbf{w}) |\ \mathbf{w} \in 1 \times \{0, 1\}^{\lambda-1}, \mathbf{x} = \mathbf{M}\mathbf{w}\}$.
     - $SK_\lambda := \{0, 1\}^\lambda$.
     - $PK_\lambda := \mathrm{Im}(\mathbf{M})$.

  - $\Pi_\lambda := \{0,1\}$.
  - $H_\lambda(\mathbf{sk}, \mathbf{x}) := \mathbf{sk}^\top \mathbf{x}$.
  - $\alpha_\lambda(\mathbf{sk}) := \mathbf{M}\,\mathbf{sk}$.
  - $\mathsf{aux}_\lambda := \mathbf{M}$.

- $\mathsf{SampYes}_\lambda(\mathsf{pp})$*:*
  1. *Parse* $\mathsf{pp} = (X_\lambda, L_\lambda, W_\lambda, R_\lambda, SK_\lambda, PK_\lambda, \Pi_\lambda, H_\lambda, \alpha_\lambda, \mathsf{aux}_\lambda)$ *and let* $\mathsf{aux}_\lambda = \mathbf{M}$.
  2. *Sample* $\mathbf{w} \leftarrow 1 \times \{0,1\}^{\lambda-1}$.
  3. *Compute* $\mathbf{x} := \mathbf{M}^\top \mathbf{w}$ *and output* $\mathbf{x}$.
- $\mathsf{SampNo}_\lambda(\mathsf{pp})$*:*
  1. *Parse* $\mathsf{pp} = (X_\lambda, L_\lambda, W_\lambda, R_\lambda, SK_\lambda, PK_\lambda, \Pi_\lambda, H_\lambda, \alpha_\lambda, \mathsf{aux}_\lambda)$ *and let* $\mathsf{aux}_\lambda = \mathbf{M}$.
  2. *Sample* $\mathbf{w} \leftarrow 1 \times \{0,1\}^{\lambda-1}$.
  3. *Compute* $\mathbf{M}'$ *as*
$$\mathbf{M}' = \mathbf{M} + \begin{pmatrix} 0 \cdots & 0 & 1 \\ 0 \;\; 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 \cdots & 0 & 0 \end{pmatrix}.$$
  4. *Compute* $\mathbf{x} := \mathbf{M}'^\top \mathbf{w}$ *and output* $\mathbf{x}$.
- $\mathsf{KeyGen}_\lambda(\mathsf{pp})$*:*
  1. *Parse* $\mathsf{pp} = (X_\lambda, L_\lambda, W_\lambda, R_\lambda, SK_\lambda, PK_\lambda, H_\lambda, \Pi_\lambda, \alpha_\lambda, \mathsf{aux}_\lambda)$.
  2. *Sample* $\mathbf{sk} \leftarrow SK_\lambda$.
  3. *Compute* $\mathbf{pk} := \alpha_\lambda(\mathbf{sk})$ *and output* $(\mathbf{pk}, \mathbf{sk})$.
- $\mathsf{Priv}_\lambda(\mathsf{pp}, \mathbf{sk}, \mathbf{x})$*:*
  1. *Parse* $\mathsf{pp} = (X_\lambda, L_\lambda, W_\lambda, R_\lambda, SK_\lambda, PK_\lambda, \Pi_\lambda, H_\lambda, \alpha_\lambda, \mathsf{aux}_\lambda)$.
  2. *Compute* $\pi := H_\lambda(\mathbf{sk}, \mathbf{x})$ *and output* π.
- $\mathsf{Pub}_\lambda(\mathsf{pp}, \mathbf{pk}, \mathbf{x}, \mathbf{w})$*:*
  1. *Compute* $\pi := \mathbf{pk}^\top \mathbf{w}$ *and output* π.

Theorem 2 *If* $\mathsf{NC}^1 \subsetneq \oplus\mathsf{L/poly}$*, then (*$\mathcal{S}etup$*,* $\mathcal{S}amp\mathcal{Y}es$*,* $\mathcal{S}amp\mathcal{N}o$*,* $\mathcal{K}ey\mathcal{G}en$*,* $\mathcal{P}riv$*,* $\mathcal{P}ub$*) defined as Construction 3 is a perfectly smooth and* $\frac{1}{2}$*-universal*$_1$ NC^1*-HPS against* NC^1 *circuits.*

Proof sketch. It is straightforward that this HPS is correct.

To show the subset membership problem of our construction, we first give two observations: (1) for any $\mathbf{M}$ sampled from $\mathsf{ZeroSamp}(\lambda)$, the distribution of $\mathbf{M} + \mathbf{N}$ is identical to $\mathsf{OneSamp}(\lambda)$, where

$$\mathbf{N} = \begin{pmatrix} 0 \cdots & 0 & 1 \\ 0 \;\; 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 \cdots & 0 & 0 \end{pmatrix},$$

and (2) perhaps interestingly, for any $\mathbf{w} \in 0 \times \{0,1\}^{n-1}$ (respectively, $\mathbf{w} \in 1 \times \{0,1\}^{n-1}$), there is a vector $\mathbf{k}$ in the kernel of $\mathbf{M}$ such that $\mathbf{M}\mathbf{w}^\top =$

$\mathbf{M}(\mathbf{w}+\mathbf{k})^\top$ and $(\mathbf{w}+\mathbf{k}) \in 1 \times \{0,1\}^{n-1}$ (respectively, $(\mathbf{w}+\mathbf{k}) \in 0 \times \{0,1\}^{n-1}$), which implies $\mathrm{Im}(\mathbf{M}^\top) = \{\mathbf{x}|\mathbf{w} \in 0 \times \{0,1\}^{n-1}, \mathbf{x} = \mathbf{M}^\top\mathbf{w}\} = \{\mathbf{x}|\mathbf{w} \in 1 \times \{0,1\}^{n-1}, \mathbf{x} = \mathbf{M}^\top\mathbf{w}\}$. Since for any vector $\mathbf{w} \in 0 \times \{0,1\}^{n-1}$, it holds that $(\mathbf{M}+\mathbf{N})^\top\mathbf{w} = \mathbf{M}^\top\mathbf{w} + \mathbf{N}^\top\mathbf{w} = \mathbf{M}^\top\mathbf{w} + \mathbf{0} = \mathbf{M}^\top\mathbf{w}$, we have $L = \mathrm{Im}(\mathbf{M}^\top) = \{\mathbf{x}|\mathbf{w} \in 0 \times \{0,1\}^{n-1}, \mathbf{x} = (\mathbf{M}+\mathbf{N})^\top\mathbf{w}\}$ due to observation (2). Moreover, since $\mathbf{M}+\mathbf{N}$ is of full rank due to observation (1), we have $X = \{0,1\}^n = \{\mathbf{x}|\mathbf{w} \in \{0,1\}^n, \mathbf{x} = (\mathbf{M}+\mathbf{N})^\top\mathbf{w}\}$. Thus, we can conclude that $X \setminus L = \{\mathbf{x}|\mathbf{w} \in 1 \times \{0,1\}^{n-1}, \mathbf{x} = (\mathbf{M}+\mathbf{N})^\top\mathbf{w}\}$. Then, the subset membership problem follows from the fact that $\mathrm{Im}(\mathbf{M}^\top) = \{\mathbf{x}|\mathbf{w} \in 1 \times \{0,1\}^{n-1}, \mathbf{x} = \mathbf{M}^\top\mathbf{w}\}$ and the indistinguishability between the distributions over $\mathrm{Im}(\mathbf{M}^\top)$ and $X \setminus L$ can be reduced to the indistinguishability between $\mathsf{ZeroSamp}(\lambda)$ and $\mathsf{OneSamp}(\lambda)$.

We now explain the intuition of the proof of universal$_1$. Since the rank of $\mathbf{M}$ is $n-1$, when we fix the public key $\mathbf{pk}$, there are two different secret keys $\mathbf{sk}$ and $\mathbf{sk}'$ such that $\mathbf{pk} = \mathbf{M}\,\mathbf{sk} = \mathbf{M}\,\mathbf{sk}'$. As explained before, for any $\mathbf{x} \in X \setminus L$, there exists $\mathbf{w} \in 1 \times \{0,1\}^{n-1}$ such that $\mathbf{x} = (\mathbf{M}+\mathbf{N})^\top\mathbf{w}$, and $(\mathbf{M}+\mathbf{N})$ is a full rank matrix. Therefore, we have $(\mathbf{M}+\mathbf{N})\mathbf{sk} \neq (\mathbf{M}+\mathbf{N})\mathbf{sk}'$ which implies $\mathbf{N}\,\mathbf{sk} \neq \mathbf{N}\,\mathbf{sk}'$, i.e., either $\mathbf{N}\,\mathbf{sk}$ or $\mathbf{N}\,\mathbf{sk}'$ is zero-vector and the other is $(1\ 0 \cdots 0)^\top$. Therefore, when we let $\mathbf{N}\,\mathbf{sk} = (0 \cdots 0)^\top$ and $\mathbf{N}\,\mathbf{sk}' = (1\ 0 \cdots 0)^\top$, it holds that $H(\mathbf{sk}, \mathbf{x}) = \mathbf{sk}^\top(\mathbf{M}+\mathbf{N})^\top\mathbf{w} = \mathbf{sk}^\top\mathbf{M}^\top\mathbf{w} + (0 \cdots 0)\mathbf{w} = \mathbf{sk}^\top\mathbf{M}^\top\mathbf{w}$ and $H(\mathbf{sk}', \mathbf{x}) = \mathbf{sk}'^\top(\mathbf{M}+\mathbf{N})^\top\mathbf{w} = \mathbf{sk}'^\top\mathbf{M}^\top\mathbf{w} + (1\ 0 \cdots 0)\mathbf{w} = \mathbf{sk}'^\top\mathbf{M}^\top\mathbf{w} + 1$, which implies $H(\mathbf{sk}, \mathbf{x}) \neq H(\mathbf{sk}', \mathbf{x})$. As a result, for fixed $\mathbf{pk}$, one can guess the proof for an instance $\mathbf{x} \in X \setminus L$ with probability at most $\frac{1}{2}$ since there is no information on whether the secret key is $\mathbf{sk}$ or $\mathbf{sk}'$.

The formal proof is as follows.

Proof. First note that all of the algorithms $\mathcal{S}etup$, $\mathcal{S}amp\mathcal{Y}es$, $\mathcal{S}amp\mathcal{N}o$, $\mathcal{K}ey\mathcal{G}en$, $\mathcal{P}riv$, and $\mathcal{P}ub$ are in NC^1, since they only involve operations including multiplications of a constant number of matrices, inner products, and sampling random bits.

Next we prove that Construction 3 satisfies correctness, subset membership problem, perfect smoothness, and $\frac{1}{2}$-universality$_1$.

Correctness. Since $\mathsf{Priv}_\lambda(\mathsf{pp}, \mathbf{sk}, \mathbf{x}) = H_\lambda(\mathbf{sk}, \mathbf{x}) = \mathbf{sk}^\top\mathbf{x} = \mathbf{sk}^\top\mathbf{M}^\top\mathbf{w} = (\mathbf{M}\mathbf{sk})^\top\mathbf{w} = \mathbf{pk}^\top\mathbf{w} = \mathsf{Pub}_\lambda(\mathsf{pp}, \mathbf{pk}, \mathbf{x}, \mathbf{w})$, Construction 3 satisfies correctness.

Subset membership problem. We now propose and prove three propositions corresponding to the three properties in the definition of subset membership problem (see Definition 7) respectively.

Proposition 1 *The distributions of* $\mathbf{x}$ *and* $\mathbf{x}'$ *are identical where* $\mathsf{pp} \leftarrow \mathsf{Setup}_\lambda$, $\mathbf{x} \leftarrow \mathsf{SampYes}_\lambda(\mathsf{pp})$*, and* $\mathbf{x}' \leftarrow L_\lambda$.

Proof. Let $\mathbf{M} \leftarrow \mathsf{ZeroSamp}(\lambda)$ be a matrix generated in the procedure of Setup_λ. Let f be a map $f : 1 \times \{0,1\}^{\lambda-1} \to \mathrm{Im}(\mathbf{M}^\top)$ such that $f(\mathbf{w}) = \mathbf{M}^\top\mathbf{w}$. One can see that for any $\mathsf{pp} \leftarrow \mathsf{Setup}_\lambda$, the distributions of $\mathbf{x}$ and $\mathbf{x}'$ are identical where $\mathbf{x} \leftarrow \mathsf{SampYes}_\lambda(\mathsf{pp})$, $\mathbf{w}' \leftarrow 1 \times \{0,1\}^{\lambda-1}$, and $\mathbf{x}' = f(\mathbf{w}')$. Moreover, if f is bijective, the distributions of $\mathbf{x}'$ and $\mathbf{x}''$ are identical for $\mathbf{w}' \leftarrow 1 \times \{0,1\}^{\lambda-1}$, $\mathbf{x}' = f(\mathbf{w}')$, and $\mathbf{x}'' \leftarrow \mathrm{Im}(\mathbf{M}^\top)$. Therefore, if f is bijective, the distributions of $\mathbf{x}$ and $\mathbf{x}''$ are identical. Namely, to show Proposition 1, we only have to show that f is bijective.

Injectivity. We now show that for any $\mathbf{w}, \mathbf{w}' \leftarrow 1 \times \{0,1\}^{\lambda-1}$ such that $\mathbf{w} \neq \mathbf{w}'$, we have $f(\mathbf{w}) \neq f(\mathbf{w}')$. We prove by contradiction, i.e. we show that if there are $\mathbf{w}, \mathbf{w}' \leftarrow 1 \times \{0,1\}^{\lambda-1}$ such that $\mathbf{w} \neq \mathbf{w}'$ and $f(\mathbf{w}) = f(\mathbf{w}')$, then it contradicts on Lemma 4.

Since $\mathbf{M}^\top \mathbf{w} = \mathbf{M}^\top \mathbf{w}'$, we have $\mathbf{M}^\top(\mathbf{w} - \mathbf{w}') = \mathbf{0}$. Moreover, since $\mathbf{w} \neq \mathbf{w}'$ and $\mathbf{w}, \mathbf{w}' \in 1 \times \{0,1\}^{\lambda-1}$, $\mathbf{w} - \mathbf{w}'$ is the non-zero vector in the kernel of $\mathbf{M}^\top$ and $\mathbf{w} - \mathbf{w}' \in 0 \times \{0,1\}^{\lambda-1}$. However, according to Lemma 4, we have $\mathrm{Ker}(\mathbf{M}^\top) = \{\mathbf{0}, \mathbf{k}\}$ where $\mathbf{k} \in 1 \times \{0,1\}^\lambda$, which gives us the conflict.

Surjectivity. We now show that for any $\mathbf{x} \in \mathrm{Im}(\mathbf{M}^\top)$, there exists a vector $\mathbf{w} \in 1 \times \{0,1\}^{\lambda-1}$ such that $\mathbf{x} = f(\mathbf{w})$, i.e., $\mathbf{x} = \mathbf{M}^\top \mathbf{w}$. According to Lemma 5, we have $\mathrm{Im}(\mathbf{M}^\top) = \{\mathbf{x} | \mathbf{w} \in 1 \times \{0,1\}^\lambda, \mathbf{x} = \mathbf{M}^\top \mathbf{w}\}$. Therefore, it holds that for any $\mathbf{x} \in \mathrm{Im}(\mathbf{M}^\top)$, there exists $\mathbf{w} \in 1 \times \{0,1\}^\lambda$ such that $\mathbf{x} = \mathbf{M}^\top \mathbf{w}$, i.e., $\mathbf{x} = f(\mathbf{w})$, completing the proof of surjectivity.

Putting all the above together, Proposition 1 immediately follows. □

Proposition 2 *The distributions of* $\mathbf{x}$ *and* $\mathbf{x}'$ *are identical for* $\mathsf{pp} \leftarrow \mathsf{Setup}_\lambda$, $\mathbf{x} \leftarrow \mathsf{SampNo}_\lambda(\mathsf{pp})$*, and* $\mathbf{x}' \leftarrow X_\lambda \setminus L_\lambda$.

Proof. Let $\mathbf{M} \leftarrow \mathsf{ZeroSamp}(\lambda)$ and $\mathbf{M}'$ be

$$\mathbf{M}' = \mathbf{M} + \begin{pmatrix} 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & 0 \end{pmatrix}.$$

We first show that for any $\mathbf{w} \in 1 \times \{0,1\}^{\lambda-1}$, we have $\mathbf{M}'^\top \mathbf{w} \in \{0,1\}^\lambda \setminus \mathrm{Im}(\mathbf{M}^\top)$.

($\bigstar$) For any $\mathbf{w} \in 0 \times \{0,1\}^{\lambda-1}$, we have

$$\begin{aligned} \mathbf{M}'\mathbf{w} &= \left(\mathbf{M} + \begin{pmatrix} 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & 0 \end{pmatrix} \right)^\top \mathbf{w} \\ &= \mathbf{M}^\top \mathbf{w} + \begin{pmatrix} 0 & \cdots & & 0 \\ \vdots & 0 & \cdots & 0 \\ 0 & & \ddots & \vdots \\ 1 & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} 0 \\ w_2 \\ \vdots \\ w_\lambda \end{pmatrix} = \mathbf{M}^\top \mathbf{w} + \mathbf{0} = \mathbf{M}^\top \mathbf{w}. \end{aligned}$$

Moreover, according to Lemma 5, we have $\mathrm{Im}(\mathbf{M}^\top) = \{\mathbf{x} | \mathbf{w} \in 0 \times \{0,1\}^{\lambda-1}, \mathbf{x} = \mathbf{M}^\top \mathbf{w}\}$. Hence, we have

$$\begin{aligned}\{\mathbf{x} \mid \mathbf{w} \in 0 \times \{0,1\}^{\lambda-1}, \mathbf{x} = \mathbf{M}'^\top \mathbf{w}\} &= \{\mathbf{x} \mid \mathbf{w} \in 0 \times \{0,1\}^{\lambda-1}, \mathbf{x} = \mathbf{M}^\top \mathbf{w}\} \quad (\bigstar) \\ &= \mathrm{Im}(\mathbf{M}^\top).\end{aligned}$$

As a result, for all $\mathbf{x} \in \mathrm{Im}(\mathbf{M}^\top)$, there exists $\mathbf{w}' \in 0 \times \{0,1\}^{\lambda-1}$ such that $\mathbf{x} = \mathbf{M}'^\top \mathbf{w}'$. Moreover, according to Lemma 6, $\mathbf{M}'$ is a full rank matrix, which means that for any $\mathbf{w} \in 1 \times \{0,1\}^{\lambda-1}$ and any $\mathbf{x} \in \mathrm{Im}(\mathbf{M}^\top)$, we have $\mathbf{M}'^\top \mathbf{w} \neq \mathbf{x}$. Namely, for any $\mathbf{w} \in 1 \times \{0,1\}^{\lambda-1}$, we have $\mathbf{M}'^\top \mathbf{w} \in \{0,1\}^\lambda \setminus \mathrm{Im}(\mathbf{M}^\top)$.

It is straightforward that for any $\mathsf{pp} \leftarrow \mathsf{Setup}_\lambda$, the distributions of $\mathbf{x} \leftarrow \mathsf{SampNo}_\lambda(\mathsf{pp})$ and $\mathbf{x}' = \mathbf{M}'^\top \mathbf{w}'$ are identical where $\mathbf{w}' \leftarrow 1 \times \{0,1\}^{\lambda-1}$. Moreover, since $\mathbf{M}'^\top$ is of full rank, the map $f : 1 \times \{0,1\}^{n-1} \to \{0,1\}^\lambda \setminus \mathrm{Im}(\mathbf{M}^\top)$ such that $f(\mathbf{w}) = \mathbf{M}'^\top \mathbf{w}$ is bijective, i.e., the distributions of $\mathbf{x}' = f(\mathbf{w}')$ and $\mathbf{x}'' \leftarrow \{0,1\}^\lambda \setminus \mathrm{Im}(\mathbf{M}^\top)$ are identical for $\mathbf{w}' \leftarrow 1 \times \{0,1\}^{\lambda-1}$, completing the proof of Proposition 2. □

Proposition 3 *For any* $\mathcal{A} = \{a_\lambda\} \in \mathsf{NC}^1$,

$$|\Pr[a_\lambda(\mathsf{pp}, \mathbf{x}_0) = 1] - \Pr[a_\lambda(\mathsf{pp}, \mathbf{x}_1) = 1]| \leq \mathsf{negl}(\lambda)$$

where $\mathsf{pp} \leftarrow \mathsf{Setup}_\lambda$, $(\mathbf{x}_0, \mathbf{w}) \leftarrow \mathsf{SampYes}_\lambda(\mathsf{pp})$, *and* $\mathbf{x}_1 \leftarrow \mathsf{SampNo}_\lambda(\mathsf{pp})$.

Proof. Let $\mathcal{A} = \{a_\lambda\}$ be any adversary in NC^1. We give hybrid games to show that the advantage of $\mathcal{A}$ in breaking the hardness of subset membership problem is negligible.

Game 0: This is the original $\mathsf{SampYes}$ game for $\mathcal{A}$. $\mathcal{CH}$ runs $\mathsf{pp} \leftarrow \mathsf{Setup}_\lambda$, $(\mathbf{x}, \mathbf{w}) \leftarrow \mathsf{SampYes}_\lambda(\mathsf{pp})$. Then it sends $(\mathsf{pp}, \mathbf{x})$ to a_λ. a_λ succeeds if a_λ outputs 1. Otherwise, it fails.

Game 1: This game is the same as **Game 0** except that $\mathcal{CH}$ runs $\mathbf{M} \leftarrow \mathsf{OneSamp}_\lambda$ in the procedure of Setup_λ.

Lemma 10 *If* $\mathcal{A} = \{a_\lambda\}$ *succeeds with advantage* ϵ_0 *(resp.,* ϵ_1*) in* **Game 0** *(resp.,* **Game 1***), then* $|\epsilon_0 - \epsilon_1| = \mathsf{negl}(\lambda)$.

Proof. We now construct $\mathcal{B} = \{b_\lambda\} \in \mathsf{NC}^1$ that distinguishes $\mathbf{M} \leftarrow \mathsf{ZeroSamp}(\lambda)$ and $\mathbf{M} \leftarrow \mathsf{OneSamp}(\lambda)$ with advantage $|\epsilon_0 - \epsilon_1|$, which contradicts to Lemma 2.

b_λ takes as input $\mathbf{M}$, which is generated as $\mathbf{M} \leftarrow \mathsf{ZeroSamp}_\lambda$ or $\mathbf{M} \leftarrow \mathsf{OneSamp}_\lambda$ from its challenger. Then, it runs $\mathsf{pp} \leftarrow \mathsf{Setup}_\lambda$ using $\mathbf{M}$, samples $\mathbf{w} \leftarrow 1 \times \{0,1\}^{\lambda-1}$, and sets $x := \mathbf{M}^\top \mathbf{w}$. Next, b_λ gives $(\mathsf{pp}, \mathbf{x})$ to a_λ. When a_λ outputs b, then b_λ outputs b.

Since all operations in b_λ are performed in NC^1, we have $\mathcal{B} = \{b_\lambda\} \in \mathsf{NC}^1$.

One can see that when $\mathbf{M} \leftarrow \mathsf{ZeroSamp}(\lambda)$ (resp., $\mathbf{M} \leftarrow \mathsf{OneSamp}(\lambda)$), the view of a_λ is identical to its view in **Game 1** (resp., **Game 2**), i.e., b_λ outputs 1 with probability ϵ_0 (resp., ϵ_1). Therefore, $\mathcal{B} = \{b_\lambda\}$ distinguishes $\mathbf{M} \leftarrow \mathsf{ZeroSamp}(\lambda)$ and $\mathbf{M} \leftarrow \mathsf{OneSamp}(\lambda)$ with advantage $|\epsilon_0 - \epsilon_1|$, which should be negligible according to Lemma 2, completing the proof of Lemma 10. □

Game 2: This is the original SampNo game for $\mathcal{A}$, i.e., it is the same as **Game 1** except that $\mathcal{CH}$ runs $\mathbf{M}' \leftarrow \mathsf{ZeroSamp}(\lambda)$ and set $\mathbf{M} := \mathbf{M}' + \mathbf{N}$ in the procedure of Setup_λ, where

$$\mathbf{N} = \begin{pmatrix} 0 \cdots & 0 & 1 \\ 0 & 0 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 \cdots & 0 & 0 \end{pmatrix}.$$

Lemma 11 *If $\mathcal{A} = \{a_\lambda\}$ succeeds with advantage ϵ_1 (resp., ϵ_2) in* **Game 1** *(resp.,* **Game 2***), then $\epsilon_1 = \epsilon_2$.*

Proof. Lemma 11 follows from the fact that the distributions of $\mathbf{M}_0 + \mathbf{N}$ and $\mathbf{M}_1$ are identical where $\mathbf{M}_0 \leftarrow \mathsf{ZeroSamp}(\lambda)$ and $\mathbf{M}_1 \leftarrow \mathsf{OneSamp}(\lambda)$ (according to Lemma 6). □

Note that, $\epsilon_0 = \Pr[a_\lambda(\mathsf{pp}, \mathbf{x}) = 1]$ and $\epsilon_2 = \Pr[a_\lambda(\mathsf{pp}, \mathbf{x}') = 1]$ where $\mathsf{pp} \leftarrow \mathsf{Setup}_\lambda$, $(\mathbf{x}, \mathbf{w}) \leftarrow \mathsf{SampYes}_\lambda(\mathsf{pp})$, and $\mathbf{x}' \leftarrow \mathsf{SampNo}_\lambda(\mathsf{pp})$. Moreover, since $|\epsilon_0 - \epsilon_1| = \mathsf{negl}(\lambda)$ and $\epsilon_1 = \epsilon_2$, we have

$$|\epsilon_0 - \epsilon_2| \leq |\epsilon_0 - \epsilon_1| + |\epsilon_1 - \epsilon_2| = \mathsf{negl}(\lambda).$$

□

According to Proposition 1, 2, and 3, Construction 3 satisfies the subset membership problem, completing this part of proof.

Perfect smoothness. We now show that for any $\mathsf{pp} \leftarrow \mathsf{Setup}_\lambda$, the random variables $(\mathbf{x}, \mathbf{pk}, \pi)$ and $(\mathbf{x}, \mathbf{pk}, \pi')$ are identical where $\mathbf{x} \leftarrow X_\lambda \setminus L_\lambda$, $(\mathbf{pk}, \mathbf{sk}) \leftarrow \mathsf{KeyGen}_\lambda(\mathsf{pp})$, and $\pi' \leftarrow \Pi_\lambda$.

According to Lemma 1, for any $\mathbf{pk}^* \in PK_\lambda$, there are only two secret keys $\mathbf{sk}$ and $\mathbf{sk}'$ such that $\mathbf{pk}^* = \alpha_\lambda(\mathbf{sk}) = \mathbf{M}\,\mathbf{sk} = \alpha_\lambda(\mathbf{sk}') = \mathbf{M}\,\mathbf{sk}'$. Moreover, according to Lemma 3, we have $\mathbf{sk} = \mathbf{sk}' + \mathbf{k}$ where $\mathbf{k}$ is a vector such that $\mathbf{k} \in \mathrm{Ker}(\mathbf{M})$ and $\mathbf{k} \in \{0,1\}^{\lambda-1} \times 1$, i.e., the last elements in $\mathbf{sk}$ and $\mathbf{sk}'$ are different (one is 1 and other is 0). Therefore, for any $\mathbf{x}^* \in X_\lambda \setminus L_\lambda$ and $\mathbf{pk}^* \in PK_\lambda$, we have

$$\begin{aligned}
\pi = \mathsf{Priv}_\lambda(\mathsf{pp}, \mathbf{sk}, \mathbf{x}^*) &= \mathbf{sk}^\top \mathbf{M}'^\top \mathbf{w}^* \\
&= \mathbf{sk}^\top \left(\mathbf{M} + \begin{pmatrix} 0 \cdots & 0 & 1 \\ 0 & 0 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 \cdots & 0 & 0 \end{pmatrix} \right)^\top \mathbf{w}^* \\
&= \mathbf{sk}^\top \mathbf{M}^\top \mathbf{w}^* + (sk_1 \cdots sk_\lambda) \begin{pmatrix} 0 \cdots & & 0 \\ \vdots & 0 & \cdots & 0 \\ 0 & & \ddots & \vdots \\ 1 & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} 1 \\ w_2^* \\ \vdots \\ w_\lambda^* \end{pmatrix} \\
&= \mathbf{pk^*}^\top \mathbf{w}^* + sk_\lambda,
\end{aligned}$$

and it follows that for any $\mathbf{x}^* \in X_\lambda \setminus L_\lambda$ and $\mathbf{pk}^* \in PK_\lambda$, there are two secret key $\mathbf{sk}, \mathbf{sk}'$ such that $\mathbf{pk}^* = \alpha_\lambda(\mathbf{sk}) = \alpha_\lambda(\mathbf{sk}')$, $\mathsf{Priv}_\lambda(\mathbf{sk}, \mathbf{x}^*) = 0$, and $\mathsf{Priv}_\lambda(\mathsf{pp}, \mathbf{sk}', \mathbf{x}^*) = 1$. Namely, the number of secret keys satisfying $\mathbf{pk}^* = \alpha_\lambda(\mathbf{sk}) \wedge \pi^* = \mathsf{Priv}_\lambda(\mathbf{sk}, \mathbf{x}^*)$ is 1. Therefore, we have

$$\begin{aligned}\Pr[(\mathbf{x}, \mathbf{pk}, \pi) = (\mathbf{x}^*, \mathbf{pk}^*, \pi^*)] &= \Pr\left[\begin{matrix}\mathbf{pk} = \mathbf{pk}^* \wedge \\ \pi = \pi^*\end{matrix}\middle|\, \mathbf{x} = \mathbf{x}^*\right] \Pr[\mathbf{x} = \mathbf{x}^*] \\ &= \Pr\left[\begin{matrix}\mathbf{pk}^* = \alpha_\lambda(\mathbf{sk}) \wedge \\ \pi^* = \mathsf{Priv}_\lambda(\mathsf{pp}, \mathbf{sk}, \mathbf{x}^*)\end{matrix}\right] \Pr\left[\mathbf{x} = \mathbf{x}^*\right] \\ &= \frac{1}{|SK_\lambda|} \Pr\left[\mathbf{x} = \mathbf{x}^*\right]\end{aligned}$$

where $\mathbf{sk} \leftarrow SK_\lambda$ and $\mathbf{x} \leftarrow X_\lambda \times L_\lambda$. Similarly, we have

$$\begin{aligned}\Pr[(\mathbf{x}, \mathbf{pk}, \pi') = (\mathbf{x}^*, \mathbf{pk}^*, \pi^*)] &= \Pr[\pi' = \pi^*] \Pr[\mathbf{pk} = \mathbf{pk}^*] \Pr[\mathbf{x} = \mathbf{x}^*] \\ &= \frac{1}{2} \frac{2}{|SK_\lambda|} \Pr\left[\mathbf{x} = \mathbf{x}^*\right] \\ &= \frac{1}{|SK_\lambda|} \Pr\left[\mathbf{x} = \mathbf{x}^*\right].\end{aligned}$$

Therefore, we have $\Pr[(\mathbf{x}, \mathbf{pk}, \pi) = (\mathbf{x}^*, \mathbf{pk}^*, \pi^*)] = \Pr[(\mathbf{x}, \mathbf{pk}, \pi') = (\mathbf{x}^*, \mathbf{pk}^*, \pi^*)]$ and it follows that Construction 3 satisfies perfect smoothness.

$\frac{1}{2}$-universality$_1$. $\frac{1}{2}$-universality$_1$ follows from the fact that for any $\mathsf{pp} \leftarrow \mathsf{Setup}_\lambda$, $\mathbf{x} \in X_\lambda \setminus L_\lambda$, $\mathbf{pk} \in PK_\lambda$, and $\pi \in \Pi_\lambda$, the number of secret keys such that $\mathbf{pk} = \alpha_\lambda(\mathbf{sk})$ is 2 and the number of secret keys such that $\mathbf{pk} = \alpha_\lambda(\mathbf{sk}) \wedge \pi = \mathsf{Priv}_\lambda(\mathsf{pp}, \mathbf{sk}, \mathbf{x})$ is 1 as described above. Therefore, we have

$$\begin{aligned}\Pr[\mathsf{Priv}_\lambda(\mathsf{pp}, \mathbf{sk}, \mathbf{x}) = \pi \wedge \alpha_\lambda(\mathbf{sk}) = \mathbf{pk}] &= \frac{1}{|SK_\lambda|} = \frac{1}{2} \frac{2}{|SK_\lambda|} \\ &= \frac{1}{2} \Pr[\alpha_\lambda(\mathbf{sk}) = \mathbf{pk}] \\ \Leftrightarrow \Pr[\mathsf{Priv}_\lambda(\mathsf{pp}, \mathbf{sk}, \mathbf{x}) = \pi | \alpha_\lambda(\mathbf{sk}) = \mathbf{pk}] &= \frac{1}{2}.\end{aligned}$$

Therefore, Construction 3 satisfies $\frac{1}{2}$-universality$_1$.

Putting all the above together, Theorem 2 immediately follows. □

Multi-bit NC^1-HPS. Notice that the size of proof space of Construction 3 is only one-bit, which makes it less useful. However, we can extend this construction with multi-bit proofs by running multiple HPS in parallel. We refer the reader to the full paper for the multi-bit version of our HPS and the security proof.

Universal$_2$ NC^1-HPS. By carefully adopting the technique by Cramer and Shoup [15], we achieve a universal$_2$ NC^1-HPS. The resulting scheme can be computed in NC^1 and it is secure against NC^1 circuits under the assumption $\mathsf{NC}^1 \subsetneq \oplus\mathsf{L}/\mathsf{poly}$. We refer the reader to the full paper for the details.

4.2 Application: NC^1-CCA Secure PKE

As one of the most important application of HPSs, Cramer and shoup [15] constructed a CCA secure PKE scheme. Interestingly, by instantiating the underlying HPS with our construction, we immediately achieve an NC^1-CCA secure PKE scheme against NC^1 circuits restricted in the same way as the ones defined for verifiable computation schemes by Campanelli and Gennaro [14], i.e., ones allowed to make constant rounds of adaptive queries to the decryption oracle, while in each round, they can make arbitrary polynomial number of queries. We refer the reader to the full paper for the details on this application.

5 Construction of NC^1-TDF against NC^1

In this section, we give our construction of NC^1-TDF against NC^1 under the assumption $\mathsf{NC}^1 \subsetneq \oplus\mathsf{L/poly}$.

Construction 4 (NC^1-TDF) *Let λ be a security parameter and l be a polynomial in λ. Let $\mathcal{F} = \{f_\lambda : \{0,1\}^\lambda \to \{0,1\}^{l(\lambda)}\}$ be a NC^1-OWF against NC^1. We define the families $\mathcal{KeyGen} = \{\mathsf{KeyGen}_\lambda\}$ with key spaces $EK_\lambda = \{\mathbf{M} \mid \mathbf{M} \leftarrow \mathsf{ZeroSamp}(\lambda)\}$ and $TK_\lambda = \mathrm{Ker}(\mathbf{M})$, $\mathcal{E}val = \{\mathsf{Eval}_\lambda\}$ and $\mathcal{I}nverse = \{\mathsf{Inverse}_\lambda\}$ as follows.*

- KeyGen_λ*:*
  1. *Run $\mathbf{R} \leftarrow \mathsf{LSamp}(\lambda)$, $\mathbf{R}' \leftarrow \mathsf{RSamp}(\lambda)$.*
  2. *Set $\mathbf{k} := (\boldsymbol{r}\ 1)^\top$ where $(\boldsymbol{r}\ 1)^\top$ is the last column of $\mathbf{R}'$.*
  3. *Compute $\mathbf{M} := \mathbf{R}\mathbf{M}_0^\lambda\mathbf{R}'$ where $\mathbf{M}_0^\lambda$ is defined as Construction 1.*
  4. *Set $ek := \mathbf{M}$ and $tk := \mathbf{k}$, and output (ek, tk) (according to the proof of Lemma 3, it holds that $\mathbf{k} \in \mathrm{Ker}(\mathbf{M})$).*

  The domain $\mathcal{D}_{\lambda,ek}$ and range $\mathcal{R}_{\lambda,ek}$ are defined as follows.

$$\mathcal{D}_{\lambda,ek} := \{0,1\}^\lambda \times \left(\mathrm{Im}(\mathbf{M}^\top) \times \{0,1\}^\lambda \setminus \mathrm{Im}(\mathbf{M}^\top)\right)^\lambda.$$
$$\mathcal{R}_{\lambda,ek} := \{0,1\}^{l(\lambda)+2\lambda^2}.$$

- $\mathsf{Eval}_\lambda(ek, X)$*:*
  1. *Parse $X := (x, (\mathbf{c}_{1,0}, \mathbf{c}_{1,1}), (\mathbf{c}_{2,0}, \mathbf{c}_{2,1}), \cdots, (\mathbf{c}_{\lambda,0}, \mathbf{c}_{\lambda,1})) \in \mathcal{D}_{\lambda,ek}$.*
  2. *For $x = x_1x_2\cdots x_\lambda \in \{0,1\}^\lambda$ and all $i \in [\lambda]$, if $x_i = 0$, set $(\mathbf{c}_i, \mathbf{c}'_i) := (\mathbf{c}_{i,0}, \mathbf{c}_{i,1})$, otherwise set $(\mathbf{c}_i, \mathbf{c}'_i) := (\mathbf{c}_{i,1}, \mathbf{c}_{i,0})$.*
  3. *Compute $y := f_\lambda(x)$.*
  4. *Set $Y := (y, (\mathbf{c}_1, \mathbf{c}'_1), (\mathbf{c}_2, \mathbf{c}'_2), \cdots, (\mathbf{c}_\lambda, \mathbf{c}'_\lambda))$ and output Y.*
- $\mathsf{Inverse}_\lambda(tk, Y)$*:*
  1. *Parse $tk := \mathbf{k}$ and $Y := (y, (\mathbf{c}_1, \mathbf{c}'_1), (\mathbf{c}_2, \mathbf{c}'_2), \cdots, (\mathbf{c}_\lambda, \mathbf{c}'_\lambda)) \in \mathcal{R}_{\lambda,ek}$.*
  2. *For all $i \in [\lambda]$, if $\mathbf{k}^\top\mathbf{c}_i = 0 \wedge \mathbf{k}^\top\mathbf{c}'_i = 1$, then set $x_i := 0$ and $(\mathbf{c}_{i,0}, \mathbf{c}_{i,1}) := (\mathbf{c}_i, \mathbf{c}'_i)$.*
  3. *Else if $\mathbf{k}^\top\mathbf{c}_i = 1 \wedge \mathbf{k}^\top\mathbf{c}'_i = 0$, then set $x_i := 1$ and $(\mathbf{c}_{i,0}, \mathbf{c}_{i,1}) := (\mathbf{c}'_i, \mathbf{c}_i)$.*
  4. *Else output $\perp$ and halt.*
  5. *Set $X = (x, (\mathbf{c}_{1,0}, \mathbf{c}_{1,1}), \cdots, (\mathbf{c}_{\lambda,0}, \mathbf{c}_{\lambda,1}))$ and output X.*

Theorem 3 *If $\mathsf{NC}^1 \subsetneq \oplus\mathsf{L/poly}$ and there exists an NC^1-OWF against NC^1 circuits, Construction 4 is an NC^1-TDF against NC^1.*

Proof sketch. Let $\mathbf{k}$ and $\mathbf{M}$ be the trapdoor key and evaluation key generated by KeyGen_λ respectively. For any $\mathbf{c} \in \mathrm{Im}(\mathbf{M}^\top)$, we must have $\mathbf{k}^\top\mathbf{c} = 0$ since $\mathbf{k} \in \mathrm{Ker}(\mathbf{M})$. Also, we prove that for any $\mathbf{c} \in \{0,1\}^\lambda \setminus \mathrm{Im}(\mathbf{M}^\top)$, there must exists $\mathbf{w}$ such that $\mathbf{w} \in 1 \times \{0,1\}^{\lambda-1}$ and $\mathbf{c} = \left(\mathbf{M} + \begin{pmatrix} 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & 0 \end{pmatrix}\right)\mathbf{w}$. Since $\mathbf{k}^\top\mathbf{M}^\top\mathbf{w} = 0$ and $\mathbf{k}^\top \begin{pmatrix} 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & 0 \end{pmatrix}^\top \mathbf{w} = 1$, we must have $\mathbf{k}^\top\mathbf{c} = 1$ in this case. Therefore, $\mathbf{k}$, which is samplable in NC^1, can be used to determine whether $\mathbf{c}$ is in $\mathrm{Im}(\mathbf{M}^\top)$ or $\{0,1\}^\lambda \setminus \mathrm{Im}(\mathbf{M}^\top)$ and recover x_i by checking whether $\mathbf{c}_i$ and $\mathbf{c}'_i$ are swapped in the inversing procedure, i.e., correctness holds.

Moreover, due to the subset membership problem for $L = \mathrm{Im}(\mathbf{M})$, the uniform distributions over $\mathrm{Im}(\mathbf{M}^\top)$ and $\{0,1\}^\lambda \setminus \mathrm{Im}(\mathbf{M}^\top)$ are indistinguishable when $\mathbf{M}$ is a correctly generated evaluation key, i.e., the distributions $(\mathbf{c}_{i,0}, \mathbf{c}_{i,1}) \leftarrow \mathrm{Im}(\mathbf{M}^\top) \times \{0,1\}^\lambda \setminus \mathrm{Im}(\mathbf{M}^\top)$ and $(\mathbf{c}_{i,0}, \mathbf{c}_{i,1}) \leftarrow \mathrm{Im}(\mathbf{M}^\top) \times \mathrm{Im}(\mathbf{M}^\top)$ are indistinguishable. Therefore, the adversary in the one-way game can only obtain information on $f_\lambda(x)$ (which is one-way), and the additional pairs $(\mathbf{c}_{i,0}, \mathbf{c}_{i,1})$ can be simulated by just sampling them from $\mathrm{Im}(\mathbf{M}^\top) \times \mathrm{Im}(\mathbf{M}^\top)$, i.e., they reveal little information on x.

The formal proof is as follows.

Proof. Note that $\mathcal{K}ey\mathcal{G}en$, $\mathcal{E}val$, and $\mathcal{I}nverse$ only involve operations including multiplications of the constant number of matrices, inner products and sampling random bits. Since these operation can be performed in NC^1, we have $\mathcal{K}ey\mathcal{G}en$, $\mathcal{E}val$, and $\mathcal{I}nverse$ can be computed in NC^1.

Next, we prove that Construction 4 satisfies correctness and one-wayness.

Correctness. For any $\mathbf{M} \leftarrow \mathsf{ZeroSamp}(\lambda)$ and any $\boldsymbol{c} \in \mathrm{Im}(\mathbf{M}^\top)$, we have

$$\mathbf{k}^\top\boldsymbol{c} = \mathbf{k}^\top\mathbf{M}^\top\mathbf{w} = (\mathbf{M}\mathbf{k})^\top\mathbf{w} = \mathbf{0}^\top\mathbf{w} = 0$$

where $\mathbf{k} \in \mathrm{Ker}(\mathbf{M})$ and $\mathbf{w}$ is a vector such that $\boldsymbol{c} = \mathbf{M}\mathbf{w}$.

Next we show that when $\boldsymbol{c} \in \{0,1\}^\lambda \setminus \mathrm{Im}(\mathbf{M}^\top)$ then $\mathbf{k}^\top\mathbf{c} = 1$. Before showing this, we first propose the following lemma, which is straightforwardly implied by Proposition 2 in Theorem 2.

Lemma 12 *For any* $\mathbf{M} \leftarrow \mathsf{ZeroSamp}(\lambda)$*, it holds that*

$$\{0,1\}^\lambda \setminus \mathrm{Im}(\mathbf{M}^\top) = \{\mathbf{x} \mid \exists \mathbf{w} \in 1 \times \{0,1\}^{\lambda-1}, \mathbf{x} = \mathbf{M}'^\top\mathbf{w}\}$$

where

$$\mathbf{M}' = \mathbf{M} + \begin{pmatrix} 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & 0 \end{pmatrix}.$$

According to Lemma 12, for any $\mathbf{M} \leftarrow \mathsf{ZeroSamp}(\lambda)$ and any $\boldsymbol{c} \in \{0,1\}^\lambda \setminus \mathrm{Im}(\mathbf{M}^\top)$, we have

$$\begin{aligned}
\mathbf{k}^\top \boldsymbol{c} = \mathbf{k}^\top \mathbf{M}'^\top \mathbf{w} = \mathbf{k}^\top & \left(\mathbf{M} + \begin{pmatrix} 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & 0 \end{pmatrix} \right)^\top \mathbf{w} \\
&= (\mathbf{M}\mathbf{k})^\top \mathbf{w} + \left(\begin{pmatrix} 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & 0 \end{pmatrix} \mathbf{k} \right)^\top \mathbf{w} \\
&= \mathbf{0}^\top \mathbf{w} + (1\ 0\ \cdots\ 0)\mathbf{w} = 0 + 1 = 1
\end{aligned}$$

where $\mathbf{k}$ is a vector in the kernel of $\mathbf{M}$ and $\mathbf{w}$ is a vector such that $\mathbf{w} \in 1 \times \{0,1\}^{\lambda-1} \wedge \boldsymbol{c} = \mathbf{M}'^\top \mathbf{w}$.

As a result, for all $i \in [\lambda]$, $\mathbf{k}$ generated by KeyGen_λ can be used to determine whether $\boldsymbol{c}_i$ (resp., $\boldsymbol{c}'_i$) generated by Eval_λ are in $\mathrm{Im}(\mathbf{M}^\top)$ or $\{0,1\}^\lambda \setminus \mathrm{Im}(\mathbf{M}^\top)$, and hence recover x_i.

One-wayness. Let $\mathcal{A} = \{a_\lambda\}$ be any adversary in NC^1. We give hybrid games to show that the advantage of $\mathcal{A}$ in breaking the one-wayness of Construction 4 is negligible.

Game 0: This is the original one-wayness game for $\mathcal{A} = \{a_\lambda\}$. $\mathcal{CH}$ runs $(ek, tk) \leftarrow \mathsf{KeyGen}_\lambda$, samples $X \leftarrow \mathcal{D}_{\lambda,ek}$, and runs $Y = \mathsf{Eval}_\lambda(ek, X)$. Then it sends (ek, Y) to a_λ. a_λ succeeds if a_λ outputs X^* such that $\mathsf{Eval}_\lambda(ek, X^*) = Y$. Otherwise it fails.

Game 1 $\sim$ Game $\boldsymbol{\lambda}$: For $i \in [\lambda]$, **Game i** is the same as **Game i-1** except that $\mathcal{CH}$ samples $(\mathbf{c}_{i,0}, \mathbf{c}_{i,1}) \leftarrow \mathrm{Im}(\mathbf{M}^\top) \times \mathrm{Im}(\mathbf{M}^\top)$.

Lemma 13 *If $\mathcal{A} = \{a_\lambda\}$ succeeds with advantage ϵ_{i-1} (resp., ϵ_i) in* **Game i-1** *(resp.,* **Game i***), then $|\epsilon_{i-1} - \epsilon_i| = \mathsf{negl}(\lambda)$.*

Proof. According to the proof of the part of subset membership problem in Theorem 2, we have the following lemma.

Lemma 14 *For any $\mathcal{G} = \{g_\lambda\} \in \mathsf{NC}^1$,*

$$|\Pr[g_\lambda(\mathbf{M}, \mathbf{c}_0) = 1] - \Pr[g_\lambda(\mathbf{M}, \mathbf{c}_1) = 1]| \le \mathsf{negl}(\lambda),$$

where $\mathbf{M} \leftarrow \mathsf{ZeroSamp}(\lambda)$, $\mathbf{c}_0 \leftarrow \mathrm{Im}(\mathbf{M}^\top)$, and $\mathbf{c}_1 \leftarrow \{0,1\}^\lambda \setminus \mathrm{Im}(\mathbf{M}^\top)$.

Proof. Let $(\mathcal{S}etup, \mathcal{S}amp\mathcal{Y}es, \mathcal{S}amp\mathcal{N}o, \mathcal{K}ey\mathcal{G}en, \mathcal{P}riv, \mathcal{P}ub)$ be a strong smooth HPS defined as Construction 3. According to Proposition 1, 2, and 3, we have

- the distributions of $\mathbf{x}_0$ and $\mathbf{c}_0$ are identical where $\mathsf{pp} \leftarrow \mathsf{Setup}_\lambda$, $(\mathbf{x}_0, w) \leftarrow \mathsf{SampYes}_\lambda(\mathsf{pp})$, and $\mathbf{c} \leftarrow \mathrm{Im}(\mathbf{M}^\top)$ ($\because$ Proposition 1).
- the distributions of $\mathbf{x}_1$ and $\mathbf{c}_1$ are identical where $\mathsf{pp} \leftarrow \mathsf{Setup}_\lambda$, $(\mathbf{x}_0, w) \leftarrow \mathsf{SampNo}_\lambda(\mathsf{pp})$, and $\mathbf{c} \leftarrow \{0,1\}^\lambda \setminus \mathrm{Im}(\mathbf{M}^\top)$ ($\because$ Proposition 2).
- it holds that for any $\mathcal{G} = \{g_\lambda\} \in \mathcal{C}_2$,

$$|\Pr[g_\lambda(\mathsf{pp}, \mathbf{x}_0) = 1] - \Pr[g_\lambda(\mathsf{pp}, \mathbf{x}_1) = 1]| \leq \mathsf{negl}(\lambda)$$

  where $\mathsf{pp} \leftarrow \mathsf{Setup}_\lambda$, $(\mathbf{x}_0, w) \leftarrow \mathsf{SampYes}_\lambda(\mathsf{pp})$, and $\mathbf{x}_1 \leftarrow \mathsf{SampNo}_\lambda(\mathsf{pp})$ ($\because$ Proposition 3).

Moreover, the distribution of $\mathsf{pp} \leftarrow \mathsf{Setup}_\lambda$ depends only on the distribution of $\mathbf{M} \leftarrow \mathsf{ZeroSamp}(\lambda)$. Therefore, for any $\mathcal{G} = \{g_\lambda\} \in \mathcal{C}_2$, we have

$$|\Pr[g_\lambda(\mathbf{M}, \mathbf{c}_0) = 1] - \Pr[g_\lambda(\mathbf{M}, \mathbf{c}_1) = 1]| \leq \mathsf{negl}(\lambda),$$

where $\mathbf{M} \leftarrow \mathsf{ZeroSamp}(\lambda)$, $\mathbf{c}_0 \leftarrow \mathrm{Im}(\mathbf{M}^\top)$, and $\mathbf{c}_1 \leftarrow \{0,1\}^\lambda \setminus \mathrm{Im}(\mathbf{M}^\top)$, completing the proof of Lemma 14. □

We now construct $\mathcal{B} = \{b_\lambda\} \in \mathsf{NC}^1$ that distinguishes $\mathbf{c} \leftarrow \mathrm{Im}(\mathbf{M}^\top)$ and $\mathbf{c} \leftarrow \{0,1\}^\lambda \setminus \mathrm{Im}(\mathbf{M}^\top)$ with advantage $|\epsilon_{i-1} - \epsilon_i|$, which contradicts to Lemma 14.

b_λ takes as input $(\mathbf{M}, \mathbf{c})$, which is generated as $\mathbf{M} \leftarrow \mathsf{ZeroSamp}(\lambda)$ and $\mathbf{c}$ sampled as $\mathbf{c} \leftarrow \mathrm{Im}(\mathbf{M}^\top)$ or $\mathbf{c} \leftarrow \{0,1\}^\lambda \setminus \mathrm{Im}(\mathbf{M}^\top)$ from its challenger. Then, it sets $ek := \mathbf{M}$ and $\mathbf{c}_{i,1} := \mathbf{c}$. Next, b_λ samples $x \leftarrow \{0,1\}^\lambda$, $(\mathbf{c}_{j,0}, \mathbf{c}_{j,1}) \leftarrow \mathrm{Im}(\mathbf{M}^\top) \times \mathrm{Im}(\mathbf{M}^\top)$ for all $j \in [i-1]$, $\mathbf{c}_{i,0} \leftarrow \mathrm{Im}(\mathbf{M}^\top)$, and $(\mathbf{c}_{j,0}, \mathbf{c}_{j,1}) \leftarrow \mathrm{Im}(\mathbf{M}^\top) \times \{0,1\}^\lambda \setminus \mathrm{Im}(\mathbf{M}^\top)$ for all $j \in \{i+1, \cdots, \lambda\}$. Next, b_λ sets $X := (x, (\mathbf{c}_{1,0}, \mathbf{c}_{1,1}), (\mathbf{c}_{2,0}, \mathbf{c}_{2,1}), \cdots, (\mathbf{c}_{\lambda,0}, \mathbf{c}_{\lambda,1}))$ and computes $Y = \mathsf{Eval}_\lambda(ek, X)$. Finally, b_λ gives (ek, Y) to a_λ. When a_λ output X^*, if $Y = \mathsf{Eval}_\lambda(ek, X^*)$, b_λ outputs 1. Otherwise, it outputs 0.

Since all operations in b_λ are performed in NC^1, we have $\mathcal{B} = \{b_\lambda\} \in \mathsf{NC}^1$.

One can see that when $\mathbf{c} \leftarrow \mathrm{Im}(\mathbf{M}^\top)$ (resp., $\mathbf{c} \leftarrow \{0,1\}^\lambda \setminus \mathrm{Im}(\mathbf{M}^\top)$), the view of a_λ is identical to its view in **Game i-1** (resp., **Game i**), i.e., b_λ outputs 1 with probability ϵ_{i-1} (resp., ϵ_i). Therefore, $\mathcal{B} = \{b_\lambda\}$ distinguishes $\mathbf{c} \leftarrow \mathrm{Im}(\mathbf{M}^\top)$ and $\mathbf{c} \leftarrow \{0,1\}^\lambda \setminus \mathrm{Im}(\mathbf{M}^\top)$ with advantage $|\epsilon_{i-1} - \epsilon_i|$, which should be negligible according to Lemma 14, completing the proof of Lemma 13. □

Lemma 15 *If $\mathcal{A} = \{a_\lambda\}$ succeeds with advantage ϵ_λ in* **Game $\boldsymbol{\lambda}$**, *then $\epsilon_\lambda = \mathsf{negl}(\lambda)$.*

Proof. We now construct $\mathcal{B} = \{b_\lambda\} \in \mathsf{NC}^1$ that breaks the one-wayness of $\mathcal{F} = \{f_\lambda\}$ with advantage ϵ_n.

b_λ takes as input y, which is generated as $x \leftarrow \{0,1\}^\lambda$ and $y = f_\lambda(y)$ from its challenger. Then, b_λ runs $(ek, tk) \leftarrow \mathsf{KeyGen}_\lambda$, parses $ek := \mathbf{M}$, and samples $((\mathbf{c}_{0,0}, \mathbf{c}_{0,1}), \cdots, (\mathbf{c}_{\lambda,0}, \mathbf{c}_{\lambda,1})) \leftarrow \mathrm{Im}(\mathbf{M}^\top)^{2\lambda}$. Next b_λ gives $(y, (\mathbf{c}_{0,0}, \mathbf{c}_{0,1}), \cdots, (\mathbf{c}_{\lambda,0}, \mathbf{c}_{\lambda,1}))$ to a_λ. When a_λ outputs X^*, b_λ parses $X^* := (x^*(\mathbf{c}^*_{0,0}, \mathbf{c}^*_{0,1}), \cdots, (\mathbf{c}^*_{\lambda,0}, \mathbf{c}^*_{\lambda,1}))$ and outputs x^*.

Since all operations in b_λ are performed in NC^1, we have $\mathcal{B} = \{b_\lambda\} \in \mathsf{NC}^1$.

One can see that the view of a_λ is identical to its view in **Game $\boldsymbol{\lambda}$**, i.e., b_λ outputs x^* such that $y = f_\lambda(x^*)$ with probability ϵ_λ. Therefore, $\mathcal{B} = \{b_\lambda\}$ breaks the one-wayness of $\mathcal{F} = \{f_\lambda\}$ with advantage ϵ_λ, which should be negligible, completing the proof of Lemma 15.

Since for $i \in [\lambda]$, $|\epsilon_{i-1} - \epsilon_i| = \mathsf{negl}(\lambda)$, $\epsilon_\lambda = \mathsf{negl}(\lambda)$, we have

$$\epsilon_0 \leq \sum_{i=1}^{\lambda} |\epsilon_{i-1} - \epsilon_i| + \epsilon_\lambda = \mathsf{negl}(\lambda).$$

Therefore, Construction 4 satisfies one-wayness. □

Putting all the above together, Theorem 3 immediately follows. □

6 Conclusion

In this paper, we formalize fine-grained OWPs, HPSs (which in turn derives a CCA-secure PKE), and TDFs, and show how to construct the NC^1 versions of them secure against NC^1 adversaries. Compared with traditional cryptographic primitives, our schemes treat restricted class of adversaries, while they can be run more efficiently and are only based on the mild worst case assumption $\mathsf{NC}^1 \subsetneq \oplus\mathsf{L/poly}$. It remains open how to construct more fine-grained primitives not implied by our results, such as pseudo-random functions and signature schemes, in the same model.

Acknowledgements

A part of this work was supported by NTT Secure Platform Laboratories, JST OPERA JPMJOP1612, JST CREST JPMJCR14D6, JSPS KAKENHI JP16H01705, JP17H01695, and the Sichuan Science and Technology Program under Grant 2017GZDZX0002.

References

1. Michel Abdalla, Fabrice Benhamouda, Olivier Blazy, Céline Chevalier, and David Pointcheval. SPHF-friendly non-interactive commitments. In Kazue Sako and Palash Sarkar, editors, *Advances in Cryptology – ASIACRYPT 2013, Part I*, volume 8269 of *Lecture Notes in Computer Science*, pages 214–234. Springer, Heidelberg, December 2013.
2. M. Ajtai. Σ^1_1-formulae on finite structures. *Annals of Pure and Applied Logic*, 24(1):1 – 48, 1983.
3. Miklós Ajtai and Avi Wigderson. Deterministic simulation of probabilistic constant depth circuits (preliminary version). In *26th Annual Symposium on Foundations of Computer Science*, pages 11–19. IEEE Computer Society Press, October 1985.
4. Adi Akavia, Oded Goldreich, Shafi Goldwasser, and Dana Moshkovitz. Erratum for: on basing one-way functions on NP-hardness. In Leonard J. Schulman, editor, *42nd Annual ACM Symposium on Theory of Computing*, pages 795–796. ACM Press, June 2010.

5. Benny Applebaum, Yuval Ishai, and Eyal Kushilevitz. Cryptography in NC^0. In *45th Annual Symposium on Foundations of Computer Science*, pages 166–175. IEEE Computer Society Press, October 2004.
6. Benny Applebaum, Yuval Ishai, and Eyal Kushilevitz. On pseudorandom generators with linear stretch in nc^0. *Computational Complexity*, 17(1):38–69, 2008.
7. Gilad Asharov and Gil Segev. On constructing one-way permutations from indistinguishability obfuscation. In Eyal Kushilevitz and Tal Malkin, editors, *TCC 2016-A: 13th Theory of Cryptography Conference, Part II*, volume 9563 of *Lecture Notes in Computer Science*, pages 512–541. Springer, Heidelberg, January 2016.
8. Yonatan Aumann, Yan Zong Ding, and Michael O. Rabin. Everlasting security in the bounded storage model. *IEEE Trans. Information Theory*, 48(6):1668–1680, 2002.
9. Yonatan Aumann and Michael O. Rabin. Information theoretically secure communication in the limited storage space model. In Michael J. Wiener, editor, *Advances in Cryptology – CRYPTO'99*, volume 1666 of *Lecture Notes in Computer Science*, pages 65–79. Springer, Heidelberg, August 1999.
10. Eli Biham, Yaron J. Goren, and Yuval Ishai. Basing weak public-key cryptography on strong one-way functions. In Ran Canetti, editor, *TCC 2008: 5th Theory of Cryptography Conference*, volume 4948 of *Lecture Notes in Computer Science*, pages 55–72. Springer, Heidelberg, March 2008.
11. Manuel Blum and Silvio Micali. How to generate cryptographically strong sequences of pseudo-random bits. *SIAM J. Comput.*, 13(4):850–864, November 1984.
12. Ravi B. Boppana and J. C. Lagarias. One- way functions and circuit complexity. In *Structure in Complexity Theory, Proceedings of the Conference hold at the University of California, Berkeley, California, USA, June 2-5, 1986*, pages 51–65, 1986.
13. Christian Cachin and Ueli M. Maurer. Unconditional security against memory-bounded adversaries. In Burton S. Kaliski Jr., editor, *Advances in Cryptology – CRYPTO'97*, volume 1294 of *Lecture Notes in Computer Science*, pages 292–306. Springer, Heidelberg, August 1997.
14. Matteo Campanelli and Rosario Gennaro. Fine-grained secure computation. In Amos Beimel and Stefan Dziembowski, editors, *TCC 2018: 16th Theory of Cryptography Conference, Part II*, volume 11240 of *Lecture Notes in Computer Science*, pages 66–97. Springer, Heidelberg, November 2018.
15. Ronald Cramer and Victor Shoup. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In Lars R. Knudsen, editor, *Advances in Cryptology – EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 45–64. Springer, Heidelberg, April / May 2002.
16. Akshay Degwekar, Vinod Vaikuntanathan, and Prashant Nalini Vasudevan. Fine-grained cryptography. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology – CRYPTO 2016, Part III*, volume 9816 of *Lecture Notes in Computer Science*, pages 533–562. Springer, Heidelberg, August 2016.
17. Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Trans. Information Theory*, 22(6):644–654, 1976.
18. Yan Zong Ding. Oblivious transfer in the bounded storage model. In Joe Kilian, editor, *Advances in Cryptology – CRYPTO 2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 155–170. Springer, Heidelberg, August 2001.
19. Yan Zong Ding, Danny Harnik, Alon Rosen, and Ronen Shaltiel. Constant-round oblivious transfer in the bounded storage model. In Moni Naor, editor, *TCC 2004: 1st Theory of Cryptography Conference*, volume 2951 of *Lecture Notes in Computer Science*, pages 446–472. Springer, Heidelberg, February 2004.

20. Stefan Dziembowski and Ueli M. Maurer. On generating the initial key in the bounded-storage model. In Christian Cachin and Jan Camenisch, editors, *Advances in Cryptology – EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 126–137. Springer, Heidelberg, May 2004.
21. Merrick L. Furst, James B. Saxe, and Michael Sipser. Parity, circuits, and the polynomial-time hierarchy. In *22nd Annual Symposium on Foundations of Computer Science, Nashville, Tennessee, USA, 28-30 October 1981*, pages 260–270, 1981.
22. Sanjam Garg, Romain Gay, and Mohammad Hajiabadi. New techniques for efficient trapdoor functions and applications. *IACR Cryptology ePrint Archive*, 2018:872, 2018.
23. Sanjam Garg and Mohammad Hajiabadi. Trapdoor functions from the computational Diffie-Hellman assumption. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology – CRYPTO 2018, Part II*, volume 10992 of *Lecture Notes in Computer Science*, pages 362–391. Springer, Heidelberg, August 2018.
24. Rosario Gennaro and Yehuda Lindell. A framework for password-based authenticated key exchange. In Eli Biham, editor, *Advances in Cryptology – EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Computer Science*, pages 524–543. Springer, Heidelberg, May 2003. `http://eprint.iacr.org/2003/032.ps.gz`.
25. Yael Gertner, Tal Malkin, and Omer Reingold. On the impossibility of basing trapdoor functions on trapdoor predicates. In *42nd Annual Symposium on Foundations of Computer Science*, pages 126–135. IEEE Computer Society Press, October 2001.
26. Johan Håstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. A pseudorandom generator from any one-way function. *SIAM Journal on Computing*, 28(4):1364–1396, 1999.
27. Julia Hesse, Dennis Hofheinz, and Lisa Kohl. On tightly secure non-interactive key exchange. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology – CRYPTO 2018, Part II*, volume 10992 of *Lecture Notes in Computer Science*, pages 65–94. Springer, Heidelberg, August 2018.
28. Russell Impagliazzo and Moni Naor. Efficient cryptographic schemes provably as secure as subset sum. In *30th Annual Symposium on Foundations of Computer Science*, pages 236–241. IEEE Computer Society Press, October / November 1989.
29. Yuval Ishai and Eyal Kushilevitz. Randomizing polynomials: A new representation with applications to round-efficient secure computation. In *41st Annual Symposium on Foundations of Computer Science*, pages 294–304. IEEE Computer Society Press, November 2000.
30. Charanjit S. Jutla and Arnab Roy. Relatively-sound NIZKs and password-based key-exchange. In Marc Fischlin, Johannes Buchmann, and Mark Manulis, editors, *PKC 2012: 15th International Conference on Theory and Practice of Public Key Cryptography*, volume 7293 of *Lecture Notes in Computer Science*, pages 485–503. Springer, Heidelberg, May 2012.
31. Yael Tauman Kalai. Smooth projective hashing and two-message oblivious transfer. In Ronald Cramer, editor, *Advances in Cryptology – EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 78–95. Springer, Heidelberg, May 2005.
32. Jonathan Katz and Vinod Vaikuntanathan. Round-optimal password-based authenticated key exchange. In Yuval Ishai, editor, *TCC 2011: 8th Theory of Cryptography Conference*, volume 6597 of *Lecture Notes in Computer Science*, pages 293–310. Springer, Heidelberg, March 2011.

33. Takahiro Matsuda. On the impossibility of basing public-coin one-way permutations on trapdoor permutations. In Yehuda Lindell, editor, *TCC 2014: 11th Theory of Cryptography Conference*, volume 8349 of *Lecture Notes in Computer Science*, pages 265–290. Springer, Heidelberg, February 2014.
34. Ueli M. Maurer. Conditionally-perfect secrecy and a provably-secure randomized cipher. *Journal of Cryptology*, 5(1):53–66, January 1992.
35. Ralph C. Merkle. Secure communications over insecure channels. *Communications of the ACM (CACM)*, 21(4):294–299, 1978.
36. Chris J. Mitchell. A storage complexity based analogue of maurer key establishment using public channels. In Colin Boyd, editor, *5th IMA International Conference on Cryptography and Coding*, volume 1025 of *Lecture Notes in Computer Science*, pages 84–93. Springer, Heidelberg, December 1995.
37. Moni Naor and Moti Yung. Universal one-way hash functions and their cryptographic applications. In *21st Annual ACM Symposium on Theory of Computing*, pages 33–43. ACM Press, May 1989.
38. Chris Peikert and Brent Waters. Lossy trapdoor functions and their applications. In Richard E. Ladner and Cynthia Dwork, editors, *40th Annual ACM Symposium on Theory of Computing*, pages 187–196. ACM Press, May 2008.
39. A. A. Razborov. Lower bounds on the size of bounded depth circuits over a complete basis with logical addition. *Mathematical notes of the Academy of Sciences of the USSR*, 41(4):333–338, Apr 1987.
40. John Rompel. One-way functions are necessary and sufficient for secure signatures. In *22nd Annual ACM Symposium on Theory of Computing*, pages 387–394. ACM Press, May 1990.
41. R. Smolensky. Algebraic methods in the theory of lower bounds for boolean circuit complexity. In *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing*, STOC '87, pages 77–82, New York, NY, USA, 1987. ACM.
42. Salil P. Vadhan. On constructing locally computable extractors and cryptosystems in the bounded storage model. In Dan Boneh, editor, *Advances in Cryptology – CRYPTO 2003*, volume 2729 of *Lecture Notes in Computer Science*, pages 61–77. Springer, Heidelberg, August 2003.
43. Emanuele Viola. On constructing parallel pseudorandom generators from one-way functions. Cryptology ePrint Archive, Report 2005/159, 2005. `http://eprint.iacr.org/2005/159`.
44. Emanuele Viola. The complexity of distributions. In *51st Annual Symposium on Foundations of Computer Science*, pages 202–211. IEEE Computer Society Press, October 2010.