Computational Robust (Fuzzy) Extractors for CRS-dependent Sources with Minimal Min-entropy*

Hanwen Feng and Qiang Tang

The University of Sydney, {hanwen.feng, qiang.tang}@sydney.edu.au

Abstract. Robust (fuzzy) extractors are very useful for, e.g., authenticated exchange from shared weak secret and remote biometric authentication against active adversaries. They enable two parties to extract the same uniform randomness with the "helper" string. More importantly, they have an authentication mechanism built in that tampering of the "helper" string will be detected. Unfortunately, as shown by Dodis and Wichs, in the information-theoretic setting, a robust extractor for an (n, k)-source requires k > n/2, which is in sharp contrast with randomness extractors which only require $k = \omega(\log n)$. Existing work either relies on random oracles or introduces CRS and works only for CRS-independent sources (even in the computational setting).

In this work, we give a systematic study of robust (fuzzy) extractors for general CRS dependent sources. We show in the information-theoretic setting, the same entropy lower bound holds even in the CRS model; we then show we can have robust extractors in the computational setting for general CRS-dependent source that is only with minimal entropy. At the heart of our construction lies a new primitive called κ -MAC that is unforgeable with a weak key and hides all partial information about the key (both against auxiliary input), by which we can compile any conventional randomness extractor into a robust one. We further augment κ -MAC to defend against "key manipulation" attacks, which yields a robust fuzzy extractor for CRS-dependent sources.

Keywords: Robust extractor Fuzzy extractor Authenticated key exchange MAC CRS

1 Introduction

Randomness extractors are well-studied tools that enable one to extract uniform randomness (usually with the help of a short random seed) from a weak random source that is with sufficient entropy. Robust (fuzzy) extractors, that are randomness extractors that can be against an active attacker, are very useful in the settings of authenticated key exchange (AKE) from weak secrets and remote biometric authentication. Sometimes, a one-message AKE protocol from weak secrets is directly known as a robust extractor (for close secrets, a robust fuzzy extractor) [6,10,12,13,25,28]. It consists of a generation algorithm Gen producing a nearly-uniform string R from a source W along with a public helper string P (message sent in the public), and a reproduction algorithm Rep recovering R from P using W. Besides the normal requirement as a randomness extractor that the extracted R should be uniform, the robustness ensures that any manipulation on P by active attackers will be detected. Furthermore, for composition with other applications that will use the extracted randomness, stronger robustness (called post-application robustness) is usually

^{*} A preliminary version of this paper appeared in *Theory of Cryptography Conference*- TCC 2021, pp. 689-717. This full version includes proofs for all theorems and lemmas. Among them, the proofs for Lemma 7 and Theorem 4 are redone, giving more accurate bounds on adversary advantages. It also corrects a flaw that the original fuzzy unforgeability definition of κ -MAC is unnecessarily strong and cannot be achieved by our construction. Furthermore, all results are revised to be applicable to sources with *average-case* conditional min-entropy which is more general than the *worst-case* notion used in the preliminary version.

required, by allowing adversaries to have R directly, which ensures security even after adversaries learn information about R from applications using R.

The one-message feature of robust extractors is indeed useful for many natural applications. The most notable example could be secure authentication [6], where Alice could register (R, P) at a server without leaking the secret W (which could be a scan of biometric), authenticate the server by retrieving P, and later start a secure communication with the server using R as the key recovered from P. This application is principally an AKE between Alice and herself at different time points, but the AKE has to be one message. Another interesting application is authenticated group key exchange (AGKE) from weak secrets. With a robust extractor, a user could broadcast the helper information P, and all other users having the same (or close) weak secret can recover the randomness R as the key. The communication cost remains one message. In contrast, it may be onerous to generalize interactive AKEs into the group setting.

Robust extractors turn out to be expensive. It is known those information-theoretic robust extractors require the (min-)entropy k of the source $W \in \{0,1\}^n$ to be larger than n/2 [13, 15], which is in contrast with both regular randomness extractors and interactive AKE protocols [15] that only require a minimal entropy $\omega(\log n)$ from the source.

Naturally, leveraging a random oracle as a "super" randomness extractor could be possible to circumvent this entropy lower bound. Indeed, one can directly hash a source (with a minimal entropy like $\omega(\log n)$) for this purpose. Moreover, one can also transform a fuzzy extractor [5, 14] into a robust fuzzy extractor [6]. However, it is always desirable to see whether we can remove this heuristic assumption [9], particularly in the setting of randomness extraction.

The other approach uses a common reference string (CRS), which could be generated by a trusted third party once and for all. It enables us to transform a strong extractor into a robust extractor, by just using the CRS as the seed. Clearly, this approach won't require more entropy from the source than the underlying extractor. It also can be extended to the fuzzy setting [10,25,26,28]. However, as the seed has to be independent of the source, this approach so far only works for CRS-independent sources.

In many cases, sources could be dependent on the CRS. For example, for sources generated from devices such as PUFs, adversaries might manufacture the devices after seeing the CRS and insert some CRS-dependent backdoor into the device to gain advantages. More seriously, for all sources, given a CRS-dependent leakage (which is possible as the leakage function is adversarially chosen after seeing the CRS), the distribution of the remained secret will be dependent on the CRS as well. We are interested in the following natural open question:

Can we have a robust (fuzzy) extractor that works for general CRS-dependent sources with minimal min-entropy ($\omega(\log n)$) without relying on an RO? ¹

1.1 Our Results

We systematically investigate this question, in both information-theoretic and computational settings, for both non-fuzzy and fuzzy cases. All related results are summarized in Table 1.

¹ For the non-fuzzy case, Dodis *et al.* [12] presented a partial solution in the computational setting. But their construction only works for a very special source: the sample consists of (w, c) where c is a ciphertext that probabilistically encrypts 0s under w; and they require the source to have any linear fraction of min-entropy. In comparison, we are aiming for general sources that only have the minimal super logarithmic entropy. For the fuzzy case, there is no feasibility result at all.

Fuzzy?	Schemes	Model	CRS-	IT/Computa-	Low	General
ruzzy:	Schemes	Moder	${\bf Dependent?}$	tional?	Entropy Rate?	Sources?
	Naive-RO	RO	-	Computational		
	[13]	Plain	-	IT	×	\checkmark
Non	Naive-CRS	CRS	×	IT	$\sqrt{}$	×
	[12]	CRS	\checkmark	Computational	×	×
	Ours(Sect.4)	CRS	\checkmark	Computational	\checkmark	$\sqrt{}$
	[6]	RO	-	Computational		
Fuzzy	[13, 21]	Plain	-	IT	×	\checkmark
	[10]	CRS	×	IT	$\sqrt{}$	×
	[25, 26, 28]	CRS	×	Computational	\checkmark	×
	Ours (Sect.5)	CRS	\checkmark	Computational	$\sqrt{}$	\checkmark

Table 1. Comparison between known robust (fuzzy) extractors. "Low Entropy-Rate?" asks whether the scheme works for (n,k)-sources with $k=\omega(\log n)$; "General Sources?" asks whether the scheme works for sources without other requirements beyond that on (n,k) (so CRS-independent ones are all not general). "Naive-RO" denotes the trivial construction that extracts randomness H(w) using a random oracle H; "Naive-CRS" denotes a strong extractor using the CRS as the seed.

Lower-bound in the information-theoretic setting. We first give a negative answer to the question in the information-theoretic setting, by proving that the lower-bound for plain-model constructions [15] also holds for CRS-dependent constructions. Namely, if there is a CRS-model information-theoretically-secure (IT-secure) pre-application robust extractor working for every source $W \in \{0,1\}^n$ that has min-entropy greater than k even conditioned on the CRS (we refer such a source an (n,k)-source), it must be that k > n/2. This new lower bound justifies the necessity of the CRS-independent requirement in existing CRS-model IT-secure robust (fuzzy) extractors [10].

A generic construction of computational CRS-model robust extractors. We then consider circumventing our new lower bound in the computational setting. We present a generic construction of CRS-model post-application robust extractors for CRS-dependent sources and thus firmly confirm its existence. This construction is built upon a conventional randomness extractor and a novel message authentication code (MAC) termed by key-private auxiliary-input MAC (κ -MAC for short) for which we give efficient constructions from well-studied assumptions. Our construction works for any efficiently samplable sources that have sufficient min-entropy (conditional on CRS) just to admit a conventional randomness extractor.

An extended construction for robust fuzzy extractors. We further extend our solution and construct a computational CRS-model robust fuzzy extractor by using a conventional randomness extractor, a secure sketch, and a stronger κ -MAC that can work in the fuzzy setting. Here, a q-secure sketch is a tool allowing one to convert a weak secret W' to a q-close one W with the help of a small amount of information about W, which is the core of many fuzzy extractors and has IT-secure instantiations.

For achieving error tolerance t, (namely, two close secrets W and W' whose distance is within t), our construction requires the source to support a 2t-secure sketch 2 . We note this requirement indeed matches the requirement made by many existing CRS-model robust fuzzy extractors [25,26], while our construction is the first one working for CRS-dependent sources.

1.2 Our Techniques

We give a technical overview as follows.

² Note that secure sketches achieving t error tolerance are also subject to some entropy-rate lower-bounds [18], but for almost all error-rate t/n (except a small range) the bound is notably smaller than 1/2.

Proving lower-bounds for CRS-model IT-secure robust extractor. Our main technique for the generalized lower bound is to show that a CRS-model IT-secure robust extractor implies a plain-model IT-secure "authentication scheme", which was the main tool for showing the lower-bound on entropy rate [15].

Note that a CRS-model robust extractor for all (n, k)-sources trivially implies a CRS-model "authentication scheme" {Auth, Vrfy}: Auth runs the generation algorithm Gen and outputs the helper string P as an "authentication tag" ς ; Vrfy runs Rep on input P and outputs 1 unless Rep fails. For any (n, k)-source W and any unbounded adversary A, the scheme is correct and unforgeable w.r.t. a randomly sampled crs according to the CRS distribution CRS. To show a CRS-model "authentication schemes" gives a plain model one: we prove that there exists at least one concrete CRS string crs* such that it will enable "correct" authentication and "unforgeability" for all CRS-dependent sources. We proceed in two steps:

For unforgeability, assume that the advantage of any adversary forging a tag in the CRS-model scheme is bounded by δ . First, we show that, for each source W, any adversary \mathcal{A} , and any constant $c_0, c_1 \in (0, 1)$, there will be a good set $S_{W,\mathcal{A}}$ with weight at least c_0 (namely, $\Pr[\mathsf{CRS} \in S_{W,\mathcal{A}}] \geq c_0$) such that for every $\mathsf{crs} \in S_{W,\mathcal{A}}$, the advantage of \mathcal{A} forging a valid tag for W is bounded by δ/c_0 .

Note that the above discussions give a "locally good" set for each W, but we need a "globally good" set of CRSs for all sources and all adversaries. For any \mathcal{A} , we show that, $\widehat{S}_{\mathcal{A}}$, the intersection of $\{S_{W,\mathcal{A}}\}$ for all sources W, is with weight at least c_0 ; and every $\operatorname{crs} \in \widehat{S}_{\mathcal{A}}$, \mathcal{A} 's advantage is bounded by δ/c_0 . We proceed with proof by contradiction: if not, its complement $\widehat{S}_{\mathcal{A}}^C$ will have the weight of at least $(1-c_0)$. By definition, for every $\operatorname{crs}^{(i)} \in \widehat{S}_{\mathcal{A}}^C$, there is one source W (whose conditional distribution is $W_{\operatorname{crs}}^{(i)}$) s.t. \mathcal{A} has advantage greater than δ/c_0 . We can define a "new" (n,k)-source $W^* = \{W|_{\operatorname{crs}}\}$ where $W|_{\operatorname{crs}^{(i)}} = W_{\operatorname{crs}}^{(i)}$ if $\operatorname{crs}^i \in \widehat{S}_{\mathcal{A}}^C$ and uniform otherwise. For such W^* and \mathcal{A} , there is no good $S_{W^*,\mathcal{A}}$ with weight greater than c_0 , which contradicts our previous argument. Finally, we can prove $\bigcap_{\mathcal{A}} \widehat{S}_{\mathcal{A}}$ is globally good, as otherwise, we can "construct" an adversary \mathcal{A}^* contradicting the existence of $\widehat{S}_{\mathcal{A}^*}$.

By similar arguments, we can show there is a globally good CRS set \widetilde{S} for correctness as well. Then by properly choosing c_0 and c_1 , the sum weight of \widehat{S} and \widetilde{S} can be greater than 1, thus there exists a \mathtt{crs}^* which is globally good for both correctness and unforgeability. Hardcoded with this string \mathtt{crs}^* , the CRS-model authentication scheme gives a plain-model authentication scheme.

Adding post-application robustness to randomness extractor for "free". We then turn to computational setting. In a conventional strong extractor Ext (which converts a weak secret w into a uniform r with the help of a uniform seed s) we may view the seed as the "helper string". To make it robust, a natural approach is to let the "helper string" additionally include a MAC tag for the seed such that adversaries cannot malleate it without being detected. One might want to use r as the key, but the verifier will not have r until receiving s, which leads to circularity. We consider taking w as the MAC key directly.

We can see that a normal MAC will be insufficient. On the one hand, the secret w is non-uniform; Especially when we consider post-application robustness, the randomness r and the seed s together give non-trivial information about w and will be leaked to adversaries. On the other hand, the authentication tag itself may contain information about w, which in turn affects the quality of randomness extraction.

We therefore introduce a new MAC called κ -MAC. Besides unforgeability, it satisfies key privacy, that is, adversaries cannot learn anything new about the key from an authentication tag. Thus,

the authentication tag will not affect the randomness extraction (in the computational setting). Moreover, both unforgeability and key privacy should hold even when adversaries have arbitrary admissible auxiliary information about the secret, making this primitive co-exist with (r, s). We define κ -MAC in the CRS-model, and allow the distribution of secrets to be arbitrarily dependent on the CRS, as long as it is efficiently samplable and has sufficient min-entropy (conditioned on the CRS). We remark that a *one-time* κ -MAC suffices for constructing robust extractors.

 κ -MAC from sLRH relation. It is natural to view κ -MAC as a special leakage-resilient (more precisely, auxiliary-input secure) MAC, then upgrade it to add key privacy. A known approach to auxiliary-input MAC is using the auxiliary-input signature in the symmetric setting, by taking both verification key vk and signing key sk as the MAC key k. But in κ -MAC, k is just a non-uniform string sampled from the source, which may not have a structure like (vk, sk); we have to deal with it carefully.

We revisit Katz-Vaikuntanathan signature [22] that is shown to be auxiliary-input secure [16]. On rough terms, they used a true-simulation-extractable NIZK (tSE-NIZK) [11] to prove the knowledge of a witness k^* w.r.t. a statement y (contained in the verification key), such that (k^*, y) satisfy a leakage-resilient hard (LRH) relation. In an LRH relation, for honest generated (y, k), and given y and leakage about k, it is infeasible to find a witness of y. If there is a successful forgery, we can extract k^* for y (by tSE-NIZK), which contradicts the LRH relation.

For our κ -MAC, we take the signing key sk as the authentication key k, but vk cannot be posted on a trusted bulletin board as in signatures, or be in k as the source might not be structured. We address this challenge as follows. First, there is a part of vk (denoted by pp) can be generated without k, and we put them in the CRS. For the other part (denoted by yk), while adversaries can manipulate it, we strengthen the LRH relation to ensure this manipulation will not give advantages. Specifically, we define the strengthened LRH relation (sLRH relation): given honestly generated (pp, yk) along with leakage about k, adversaries cannot "frame" k, that is, find a (yk', k') such that both (pp, yk', k') and (pp, yk', k) satisfy the sLRH relation. Using tSE-NIZK to prove knowledge of k w.r.t. (pp, yk) and attaching yk (and the proof) to the authentication tag could give an auxiliary-input MAC from weak secrets.

For key privacy, we need yk to hide partial information about k, i.e., one can simulate the yk distribution without k. Accordingly, we formulate the privacy of generators for a sLRH relation. With a sLRH relation and its private generator, we have a κ -MAC construction in this way.

Constructing sLRH relation from DPKE+NIZK. The privacy of generator indeed prevents adversaries from finding k from (pp, yk) and the leakage. If it further has a kind of "collision-resistance", namely, it is infeasible to find a distinct k' along with yk' such that both (pp, yk', k) and (pp, yk', k') belong to R_{LR} , R_{LR} with a private generator will be a sLRH relation.

We use an auxiliary-input-secure deterministic encryption scheme to instantiate an NP relation R_{de} with a private generator. Specifically, $(pk, c, m) \in R_{de}$ iff $c = \mathsf{DEnc}(pk, m)$. From the security of DPKE, (pk, c) could hide partial information about m. For handling all hard-to-invert auxiliary information, the DPKE scheme from exponentially hard DDH assumption [30] will be the only choice.

Note that under a valid pk, (pk, c) uniquely determines the message m and thus adversaries cannot find a second message. However, we cannot ensure the validity of pk by putting it into the CRS. The problem is that DPKE only works for message distributions independent of pk, but we need to work for CRS-dependent sources. To get around this obstacle, we use a NIZK to prove the

validity of pk. Though NIZK needs a CRS as well, it is secure even when statements and witnesses are dependent on the CRS.

Augmenting κ -MAC to defend against "key manipulations" attacks. Finally, we extend our solutions to the fuzzy case. The starting point is using κ -MAC to authenticate the helper string of a fuzzy extractor. We take the standard secure-sketch-based fuzzy extractor as a building block, in which one can recover the secret w using his secret w' first.

The κ -MAC we just defined will be insufficient for the fuzzy case. Adversaries may manipulate the helper string, such that one recovers another secret w'' (which is t-close to w') that a forged tag can be verified under w''. We therefore need κ -MAC to satisfy fuzzy unforgeability, that is, given an authentication tag from w, adversaries cannot forge an authentication tag being accepted by $\mathtt{shift}(w)$, where \mathtt{shift} is an efficient function specified by the adversary, modeling the manipulation over w by adversarially altering the helper string. Note that the distance between w'' and w is bounded by 2t, so the output of $\mathtt{shift}(w)$ must be 2t-close to w.

To construct a fuzzy unforgeable κ -MAC, we first introduce a fuzzy version of sLRH relation. More specifically, for a 2t-fuzzy sLRH relation, it is infeasible to find (yk',k') to "frame" the $\mathtt{shift}(k)$ for any efficient \mathtt{shift} whose output is 2t-close to k. It is easy to verify the according κ -MAC satisfies 2t-fuzzy unforgeability.

Interestingly, we do not need other tools to construct a fuzzy sLRH relation. Our construction of sLRH relation is fuzzy already. Particularly, if a sLRH relation is "collision resistant", the adversary can "frame" some k'' only when she finds k''. It remains to argue that, given (pp, yk) from a private generator on input k and the leakage of k, can adversaries find a secret k'' that is 2t-close to k?

This question seems straightforward at first glance but turns out to need some care. Note that the privacy of the generator cannot ensure that (pp, yk) hides all partial information about k, as (pp, yk) itself must be non-trivial about k. The safest way to check whether a value can be recovered from (pp, yk) is to see whether this value is useful for distinguishing yk and yk. For small t (say, logarithmic in the security parameter), one knowing $k'' \in B_{2t}(k)$ can guess the original k with a non-negligible probability, and then she can use k to distinguish. The situation gets complicated when t is large and $B_{2t}(k)$ has exponential many points. In this case, one cannot naively guess k according to k''. We overcome this challenge by observing the task of recovering k from k'' can be done with the help of 2t-secure sketch. More specifically, assume an adversary can recover k'' from (pp, yk). Then, the distinguisher specifies the leakage as a 2t-secure sketch, invokes the adversary to have this $k'' \in B_{2t}(k)$, and converts k'' to k with the help of the secure sketch. Usually, auxiliary inputs are considered a "bad" object to be against, but our proof leverages the auxiliary input to get around barriers of security proof.

1.3 Open Problems and Subsequent Work

Our work raises two natural problems. The first is to construct computational robust extractors in the plain model that work for random sources with a less-than-half entropy rate. In this work, we authenticate the seed of a strong extractor using a κ -MAC which is then constructed in the CRS model, resulting in a CRS-model robust extractor. Nonetheless, as κ -MAC captures the standard properties of the random oracle in Boyen *et al.*'s construction [6], a "trivial" solution can be directly assuming that a standard hash function like SHA3 is a κ -MAC. Therefore, an interesting solution for this problem should be based on standard assumptions, particularly the *complexity assumptions* formalized by Goldwasser and Kalai [20].

Significant progress towards the problem was recently made by Apon *et al.* [2], who introduced a new notion of non-malleable point function obfuscation with associated data that can be viewed as a weaker version of κ -MAC, presented its plain-model construction, and then used it to construct a plain-model robust fuzzy extractor. However, their construction has to rely on an entropic assumption (thus not a complexity assumption [20]) over fixed-generator groups, which is justified in the generic group model [3]. As there exist cryptographic schemes secure in the generic group model but insecure in practice, this problem is still interesting for further study.

Another interesting problem is to achieve reusability and robustness simultaneously for CRS-dependent sources (or in the plain model), particularly in the fuzzy case. Reusability allows the extraction of multiple independent keys from one weak secret, which is important for biometrics that is practically reused and cannot be changed. In the literature, plain-model constructions for reusable fuzzy extractors are known [8] and can also be easily adapted from CRS-model constructions like [25] and [26]. A natural idea is applying our κ -MAC to a plain-model secure-sketch-based reusable extractor. However, the main impediment here is that our κ -MAC scheme only achieves one-time security, while a full-fledged κ -MAC for general auxiliary inputs is required.

2 Preliminaries

Notations. All adversaries considered in this paper are non-uniform, and we model an adversary A by a family of circuits $\{A_{\lambda}\}_{n\in\mathbb{N}}$. For a set \mathbb{X} , $x \leftarrow \mathbb{X}$ denotes sampling x from the uniform distribution over \mathbb{X} . For a distribution X, $x \leftarrow X$ denotes sampling x from X. Let (X,Y) be a joint distribution, $X|_y$ denotes the conditional distribution of X conditioned on Y = y. If A is a probabilistic algorithm, $A(x_1, x_2, \dots; r)$ is the result of running A on the input x_1, x_2, \dots and the random coins r. We use $y \leftarrow A(x_1, x_2, \dots)$ to denote the experiment that choosing r at random and getting $y = A(x_1, x_2, \dots; r)$.

2.1 Entropy and Strong Extractor

Min-entropy. The min-entropy of a distribution W is defined by

$$\mathbf{H}_{\infty}(W) = -\log(\max_{w \in \mathsf{Supp}(W)} \Pr[W = w]).$$

Let n, k be functions of the security parameter. We call an ensemble of distributions $\mathcal{W} = \{W_{\lambda}\}_{{\lambda} \in \mathbb{N}}$ an (n, k)-source, if for every ${\lambda} \in \mathbb{N}$, W_{λ} is an $(n({\lambda}), k({\lambda}))$ -distribution. Namely, W_{λ} is defined over $\{0, 1\}^{n({\lambda})}$, and $\mathbf{H}_{\infty}(W) \geq k({\lambda})$.

Conditional min-entropy. For a joint distribution (W, Z), we mainly use the average-case min-entropy [13] of W conditioned on Z, defined as

$$\widetilde{\mathsf{H}}_{\infty}(W|Z) = -\log(\mathbb{E}_{z \leftarrow Z}[2^{-\mathbf{H}_{\infty}(W|z)}]) = -\log(\mathbb{E}_{z \leftarrow Z}[\max_{w \in \mathsf{Supp}(W)} \Pr[W = w]]).$$

In our negative result (Sect. 3), we also use the *worst-case* entropy [23] of W conditioned on Z, which, denoted by $\mathbf{H}_{\infty}(W|Z)$, is the minimal of $\mathbf{H}(W|z)$ over all $z \in \mathsf{Supp}(Z)$. It is trivial to see $\mathbf{H}_{\infty}(W|Z) \geq \hat{k}$ implies $\widetilde{\mathbf{H}}_{\infty}(W|Z) \geq \hat{k}$ for any joint distribution (W, Z).

We can extend the notions to ensembles. Namely, we call $(W = \{W_{\lambda}\}_{{\lambda} \in \mathbb{N}} | \mathcal{Z} = \{Z_{\lambda}\}_{{\lambda} \in \mathbb{N}})$ an average-case (resp. worst-case) (n,k)-source, if for each λ , W_{λ} is defined over $\{0,1\}^{n(\lambda)}$, and

 $\widetilde{\mathbf{H}}_{\infty}(W_{\lambda}|Z_{\lambda}) \geq k(\lambda)$ (resp. $\mathbf{H}_{\infty}(W_{\lambda}|Z_{\lambda}) \geq k(\lambda)$). For notational convenience, we may call \mathcal{W} an average-case (resp. worst-case) (n,k)-source w.r.t. \mathcal{Z} , meaning $(\mathcal{W}|\mathcal{Z})$ forms an average-case (resp. worst-case) (n,k)-source. Note that a wost-case (n,k)-source is also an average-case (n,k)-source.

Average-case strong extractor. Strong extractors can convert a non-uniform randomness into a nearly uniform randomness with the help of a public randomness called a seed. For generality, we give the computational definition of average-case strong extractors in the following.

Let n,k,ℓ be integer functions of the security parameter. An (n,k,ℓ) -strong randomness extractor Ext is a deterministic algorithm, which on inputs $w \in \{0,1\}^{n(\lambda)}$ along with a public seed i_{ext} (with length $si(\lambda)$) outputs another randomenss $r \in \{0,1\}^{\ell(\lambda)}$. Ext satisfies ϵ -privacy, if for any polynomial-time $\mathcal A$ and any average-case (n,k)-source $(\mathcal W|\mathcal Z)$, $\mathcal A$'s advantage $\mathsf{Adv}^{\text{ext}}_{\mathcal W,\mathcal Z,\mathcal A}(\lambda)$ is not greater than $\epsilon(\lambda)$, with the advantage defined as

$$\left| \Pr \begin{bmatrix} (w,z) \leftarrow (W_{\lambda}, Z_{\lambda}), i_{\mathsf{ext}} \leftarrow \$ \left\{ 0, 1 \right\}^{si(\lambda)} \\ r \leftarrow \mathsf{Ext}(i_{\mathsf{ext}}, w) : 1 \leftarrow \mathcal{A}(i_{\mathsf{ext}}, r, z) \end{bmatrix} - \Pr \begin{bmatrix} (w,z) \leftarrow (W_{\lambda}, Z_{\lambda}), i_{\mathsf{ext}} \leftarrow \$ \left\{ 0, 1 \right\}^{si(\lambda)} \\ r \leftarrow \$ \left\{ 0, 1 \right\}^{(\ell(\lambda))} : 1 \leftarrow \mathcal{A}(i_{\mathsf{ext}}, r, z) \end{bmatrix} \right|.$$

We say an (n, k, ℓ) extractor Ext is ϵ_{inv} -hard to invert, if for any polynomial adversary \mathcal{A} and any (n, k)-source $(\mathcal{W}|\mathcal{Z})$, it holds that,

$$\Pr[(w,z) \leftarrow (W_{\lambda}, Z_{\lambda}), i_{\mathsf{ext}} \leftarrow \$ \{0,1\}^{si(\lambda)}, r \leftarrow \mathsf{Ext}(i_{\mathsf{ext}}, w), w' \leftarrow \mathcal{A}(i_{\mathsf{ext}}, r, z) : w = w'] \leq \epsilon_{\mathsf{inv}}(\lambda).$$

Note that Ext sastifying ϵ -privacy for small ϵ is naturally hard-to-invert w.r.t. some small ϵ_{inv} . We do not view "hard-to-invert" as an extra property for Ext but may use it for convenience.

2.2 CRS-Model Robust Extractor

We present both information-theoretical and computational definitions of robust extractors in the CRS model.

CRS-dependent sources. Being different from all previous CRS-model works of fuzzy extractors [10, 25–28] that require sources to be independent of the CRS, we consider all sources that could potentially depend on the CRS while having sufficient conditional min-entropy. Formally, a source $W = \{W_{\lambda}\}_{{\lambda} \in \mathbb{N}}$ and the CRS CRS = $\{\mathsf{CRS}_{\lambda}\}_{{\lambda} \in \mathbb{N}}$ are ensembles of distributions, and we allow W and CRS to be correlated as long as W has enough average-case min-entropy conditioned on CRS, namely, $\widetilde{\mathbf{H}}(W_{\lambda}|\mathsf{CRS}_{\lambda}) \geq k(\lambda)$ for some k. While CRS is usually described by a specific sampler algorithm, we may explicitly describe the sampling process of (W,CRS) as

$$\operatorname{crs} \leftarrow \operatorname{CRS}_{\lambda}, w \leftarrow W_{\lambda}|_{\operatorname{crs}}.$$

In the computational setting, we further require each $W_{\lambda|crs}$ to be efficiently samplable by a uniform polynomial-bounded circuit.

Definition 1 (Efficiently-samplable source w.r.t. CRS). For a distributions ensembles CRS = $\{CRS_{\lambda}\}_{{\lambda}\in\mathbb{N}}$ and $\mathcal{W}=\{W_{\lambda}\}_{{\lambda}\in\mathbb{N}}$, we call W_{λ} an efficiently-samplable distribution w.r.t. CRS_{λ} , if there is a circuit G_{λ} whose running time is polynomial in λ , such that for every $crs \in Supp(CRS_{\lambda})$, it holds that

$$G_{\lambda}(crs) = W_{\lambda}|_{crs}$$
.

If for every $\lambda \in \mathbb{N}$, W_{λ} is an efficiently-samplable distribution w.r.t. CRS_{λ} , we call \mathcal{W} an efficiently-samplable source w.r.t. CRS .

Remark 1. We consider efficiently samplable sources in the computational setting, as the dependence between a source being extracted and the CRS distribution is usually caused by an efficient adversary. A typical scenario could be that a non-uniform PPT adversary $\mathcal{A} = \{A_{\lambda}\}_{{\lambda} \in \mathbb{N}}$ "creates" a source after seeing the CRS. Therefore, we ask a uniform polynomial-bounded circuit G_{λ} (which can be considered as A_{λ}) for every $\operatorname{crs} \in \operatorname{Supp}(\operatorname{CRS}_{\lambda})$, rather than different polynomial-bounded circuits for different crs . Similar settings appeared in the recent works on two source extractors [1, 19].

Robust extractor. A robust extractor rExt in the CRS-model is defined by a triplet of efficient algorithms {CRS, Gen, Rep}. CRS is a sampler algorithm that specifies the CRS distribution. Gen takes as inputs a CRS and a weak secret w and outputs a randomness R along with a helper string P. Then, Rep can recover R from P using w. rExt requires privacy and robustness. The former says R is pseudorandom conditioned on P, and the latter captures the infeasibility of forging a different P that will not lead to the failure of Rep. Particularly, when A is given both R and P, the robustness is called post-application robustness; when only P is given, it is called pre-application robustness. Formally, we define a robust extractor below.

Definition 2 (Robust extractor). For integer functions n, k, ℓ of the security parameter, an (n, k, ℓ) -robust extractor rExt is defined by the following PPT algorithms.

- $crs \leftarrow CRS(1^{\lambda})$. On input the security parameter λ , it outputs a CRS crs, whose distribution is denoted by CRS_{λ} .
- $-(R,P) \leftarrow \mathsf{Gen}(\mathit{crs},w)$. On inputs crs and a string $w \in \{0,1\}^{n(\lambda)}$, it outputs a randomness $R \in \{0,1\}^{\ell(\lambda)}$ along with a helper string P.
- $-R \leftarrow \mathsf{Rep}(\mathit{crs}, w, P)$. It recovers the randomness R from P by using w.

Correctness: For a function $\rho : \mathbb{N} \to [0,1]$, we say rExt satisfies ρ -correctness, if for any average-case (n,k)-source \mathcal{W} w.r.t. CRS, for every λ , it holds that

$$\Pr[crs \leftarrow \mathsf{CRS}_{\lambda}; w \leftarrow W_{\lambda}|_{crs}; (R, P) \leftarrow \mathsf{Gen}(crs, w) : \mathsf{Rep}(crs, w, P) = R] \ge \rho(\lambda).$$

Privacy: For $\epsilon : \mathbb{N} \to (0,1)$, rExt satisfies the ϵ -IT-privacy, if for any unbounded adversary \mathcal{A} and for any average-case (n,k)-source \mathcal{W} w.r.t. CRS, it holds that

$$\mathsf{Adv}^{\mathrm{priv}}_{\mathcal{A},\mathcal{W}}(\lambda) := |\Pr[\mathsf{Exp}^{\mathsf{priv},0}_{\mathcal{A},\mathcal{W}}(\lambda) = 1] - \Pr[\mathsf{Exp}^{\mathsf{priv},1}_{\mathcal{A},\mathcal{W}}(\lambda) = 1]| \le \epsilon(\lambda). \tag{1}$$

Robustness: For $\delta : \mathbb{N} \to (0,1)$, rExt satisfies δ -IT-post-application-robustness (or pre-application robustness, without boxed items in the experiment $\mathsf{Exp}^{\mathsf{rob}}_{\mathcal{A},\mathcal{W}}$), if for any unbounded adversary \mathcal{A} , and any (n,k)-source \mathcal{W} , it holds that

$$\mathsf{Adv}^{\mathrm{rob}}_{\mathcal{A},\mathcal{W}}(\lambda) = \Pr[\mathsf{Exp}^{\mathsf{rob}}_{\mathcal{A},\mathcal{W}}(\lambda) = 1] \le \delta(\lambda). \tag{2}$$

Computational definitions can be defined by only considering polynomial-time adversaries and efficiently-samplable sources. We directly call these computational versions ϵ -privacy and δ -post-application-robustness (by removing "IT").

$Exp^{priv,b}_{\mathcal{A},\mathcal{W}}(\lambda)$	$Exp^{rob}_{\mathcal{A},\mathcal{W}}(\lambda)$
$\operatorname{crs} \leftarrow \operatorname{CRS}_{\lambda}; w \leftarrow W_{\lambda} _{\operatorname{crs}};$	$\mathtt{crs} \leftarrow CRS_{\lambda}; w \leftarrow W_{\lambda} _{\mathtt{crs}}$
$(R,P) \leftarrow Gen(crs,w);$	$(R,P) \leftarrow Gen(crs,w); P^* \leftarrow \mathcal{A}(crs,P \ ,R \)$
$R_0 \leftarrow \$ \{0,1\}^{\ell(\lambda)}; R_1 = R; b' \leftarrow \mathcal{A}(\mathtt{crs}, P, R_b)$	if $P^* \neq P \land Rep(crs, P^*, w) \neq \perp$) then return 1
$\mathbf{return}\ b'$	return 0

2.3 CRS-Model Robust Fuzzy Extractor

Fuzzy extractors allow the generation algorithm and the reproduction algorithm to use different but close secrets w, \widetilde{w} .

Metric spaces. We first introduce metric spaces that allow us to define "close" secrets formally. A metric space $\mathcal{M} = \{\mathcal{M}_{\lambda}\}_{{\lambda} \in \mathbb{N}}$ is a collection of sets with a distance function $\operatorname{dist} : \mathcal{M}_{\lambda} \times \mathcal{M}_{\lambda} \to [0, \infty)$. Throughout this paper, we consider $\mathcal{M}_{\lambda} = \{0, 1\}^{n(\lambda)}$ equipped with a distance function (e.g., Hamming distance).

For an integer \widehat{t} , we say w is \widehat{t} -close to \widetilde{w} , if $\mathsf{dist}(w,\widetilde{w}) \leq \widehat{t}$. For $(\mathcal{W},\mathcal{Z})$ and $(\widetilde{\mathcal{W}},\mathcal{Z})$ where \mathcal{W} and $\widetilde{\mathcal{W}}$ are defined over \mathcal{M} , we say $(\mathcal{W},\widetilde{\mathcal{W}})$ a t-pair for an integer function t w.r.t. \mathcal{Z} , if for every $\lambda \in \mathbb{N}$ and $z \in \mathsf{Supp}(Z_{\lambda})$, it holds that

$$\Pr[(w, \widetilde{w}) \leftarrow (W_{\lambda}|_z, \widetilde{w}_{\lambda}|_z) : \mathsf{dist}(w, \widetilde{w}) \leq t(\lambda)] = 1.$$

Secure sketch. Secure sketches allow to convert a secret w into a different but close secret w' with the help of certain information from w', which is an essential building block for fuzzy extractors. We introduce average-case secure sketches [13] below. Formally, for a metric space \mathcal{M} , an (\mathcal{M}, k, k', t) -secure sketch scheme is a pair of PPT algorithms SS and Rec that satisfies correctness and security. For every $\lambda \in \mathbb{N}$,

- SS on input $w \in \mathcal{M}_{\lambda}$, outputs a sketch ss;
- Rec takes as inputs a sketch ss and $\widetilde{w} \in \mathcal{M}_{\lambda}$, and ouputs w'.

Correctness. $\forall \widetilde{w} \in \mathcal{M}_{\lambda}$, if $\operatorname{dist}(w, \widetilde{w}) \leq t(\lambda)$, then $\operatorname{Rec}(\widetilde{w}, SS(w)) = w$.

Security. For every λ , any (n,k)-source $(\mathcal{W},\mathcal{Z})$ (where $\mathcal{M}_{\lambda} = \{0,1\}^{n(\lambda)}$), it holds that

$$\widetilde{\mathbf{H}}_{\infty}(W|\mathsf{SS}(W),Z) \geq k'(\lambda).$$

Robust fuzzy extractor. Now we extend the robust extractor definition into the fuzzy case.

Definition 3 (Robust fuzzy extractor). For a metric space \mathcal{M} and integer functions n, k, ℓ of the security parameter, an $(\mathcal{M}, k, \ell, t)$ -robust fuzzy extractor rfExt is defined by the following PPT algorithms.

- $crs \leftarrow CRS(1^{\lambda})$. On input the security parameter λ , it outputs a CRS crs, whose distribution is denoted by CRS_{λ} .
- $-(R,P) \leftarrow \mathsf{Gen}(\mathit{crs},w)$. On inputs crs and a string $w \in \{0,1\}^{n(\lambda)}$, it outputs a randomness $R \in \{0,1\}^{\ell(\lambda)}$ along with a helper string P.
- $-R \leftarrow \mathsf{Rep}(\mathit{crs}, \widetilde{w}, P)$. It recovers the randomness R from P using \widetilde{w} .

Correctness: For a function $\rho : \mathbb{N} \to [0,1]$, we say rfExt satisfies ρ -correctness, if for any t-pair of average-case (n,k)-sources $(\mathcal{W},\widetilde{\mathcal{W}})$ w.r.t. CRS, for every λ , it holds that

$$\Pr[\mathit{crs} \leftarrow \mathsf{CRS}_{\lambda}; (w, \widetilde{w}) \leftarrow (W_{\lambda}|_{\mathit{crs}}, \widetilde{W}_{\lambda}|_{\mathit{crs}}); (R, P) \leftarrow \mathsf{Gen}(\mathit{crs}, w) : \mathsf{Rep}(\mathit{crs}, \widetilde{w}, P) = R] \geq \rho(\lambda).$$

Privacy: For $\epsilon : \mathbb{N} \to (0,1)$, rfExt satisfies the ϵ -IT-privacy, if for any unbounded adversary \mathcal{A} and any average-case (n,k)-source \mathcal{W} w.r.t. CRS, it holds that

$$\mathsf{Adv}^{\mathrm{fpriv}}_{\mathcal{A},\mathcal{W}}(\lambda) := |\Pr[\mathsf{Exp}^{\mathsf{fpriv},0}_{\mathcal{A},\mathcal{W}}(\lambda) = 1] - \Pr[\mathsf{Exp}^{\mathsf{fpriv},1}_{\mathcal{A},\mathcal{W}}(\lambda) = 1]| \le \epsilon(\lambda). \tag{3}$$

Robustness: For $\delta : \mathbb{N} \to (0,1)$, rfExt satisfies the δ -IT-post-application-robustness (or preapplication robustness, without boxed items in the experiment $\mathsf{Exp}^{\mathsf{frob}}_{\mathcal{A},\mathcal{W},\widetilde{\mathcal{W}}}$), if for any unbounded adversary \mathcal{A} , and any t-pair of average-case (n,k)-sources $(\mathcal{W},\widetilde{\mathcal{W}})$ w.r.t. CRS, it holds that

$$\mathsf{Adv}^{\mathrm{frob}}_{\mathcal{A},\mathcal{W}}(\lambda) = \Pr[\mathsf{Exp}^{\mathsf{frob}}_{\mathcal{A},\mathcal{W}}(\lambda) = 1] \le \delta(\lambda). \tag{4}$$

Accordingly, computational robust fuzzy extractors can be defined by focusing on polynomial-time adversaries and efficiently-samplable sources.

2.4 Other Cryptographic Notions

Hard-to-invert Function. A function ensemble $\mathcal{F} = \{f_{\lambda}\}$ is ϵ_{hv} -hard-to-invert w.r.t. a distribution ensemble $\mathcal{W} = \{W_{\lambda}\}$, if for any polynomial-time adversary \mathcal{A} , it holds that

$$\Pr[w \leftarrow W_{\lambda} : \mathcal{A}(f_{\lambda}(w)) = w] \le \epsilon_{\mathsf{hv}}(\lambda).$$

It can be naturally extended to conditional distributions: \mathcal{F} is ϵ_{hv} -hard-to-invert w.r.t. $(\mathcal{W}|\mathcal{Z})$, if for any polynomial-time adversary \mathcal{A} ,

$$\Pr[(w, z) \leftarrow (W_{\lambda}, Z_{\lambda}) : \mathcal{A}(f_{\lambda}(w), z) = w] < \epsilon_{\mathsf{hv}}(\lambda).$$

Equivalently, we can consider $g_{\lambda}(w,z) = (f_{\lambda}(w),z)$ as a hard-to-invert function w.r.t. the distribution $(\mathcal{W},\mathcal{Z})$.

NIZK. Non-interactive zero-knowledge argument systems (NIZKs) enable a prover, having an NP statement x and its witness w, to convince a verifier of the truthness of x, by sending a single message and without disclosing any information about w. For our purpose, it is more convenient to use the notion of same-string NIZKs from [11,24], and we only ask for the single-theorem version.

A NIZK Π for an NP relation R can be described by the following three algorithms.

- $-S_{zk}(1^{\lambda})$. The setup algorithm generates a CRS crs and a trapdoor key tk.
- $P_{zk}(crs, x, \psi)$. The prover algorithm takes as inputs a CRS crs, a statement x and a witness ψ , and outputs a proof π .
- $V_{zk}(crs, x, \pi)$. The verifier algorithm checks the validity of π .

Perfect completeness: if for any $\lambda \in \mathbb{N}$ and for any $(x, \psi) \in R$,

$$\Pr[(\mathtt{crs},\mathtt{tk}) \leftarrow \mathsf{S}_{\mathsf{zk}}(1^{\lambda}); \pi \leftarrow \mathsf{P}_{\mathsf{zk}}(\mathtt{crs},x,\psi) : \mathsf{V}_{\mathsf{zk}}(\mathtt{crs},x,\pi) = 1] = 1.$$

Adaptive soundness: Π satisfies $\epsilon_{\sf snd}$ -soundness, if for any polynomial-time adversary \mathcal{A} , its advantage $\mathsf{Adv}^{\sf snd}_{\mathcal{A}}(\lambda)$ (defined below) is not greater than $\epsilon_{\sf snd}(\lambda)$.

$$\mathsf{Adv}^{\mathrm{snd}}_{\mathcal{A}}(\lambda) = \Pr[(\mathtt{crs},\mathtt{tk}) \leftarrow \mathsf{S}_{\mathtt{zk}}(1^{\lambda}); (x,\pi) \leftarrow \mathcal{A}(\mathtt{crs}) : \mathsf{V}_{\mathtt{zk}}(\sigma,x,\pi) = 1 \land (\forall \psi,(x,\psi) \notin R)].$$

Single-theorem ZK: Π satisfies one-time ϵ_{zk} -ZK, if there exists a simulator SP_{zk} , such that for any polynomial-time $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$, it holds that

$$\mathsf{Adv}^{\mathsf{zk}}_{\mathcal{A}}(\lambda) = \left| \Pr \begin{bmatrix} (\mathsf{crs}, \mathsf{tk}) \leftarrow \mathsf{S}_{\mathsf{zk}}(1^{\lambda}), \\ (x, \psi, st) \leftarrow \mathcal{A}_1(\mathsf{crs}), \\ \pi \leftarrow \mathsf{P}_{\mathsf{zk}}(\mathsf{crs}, x, \psi) : \\ 1 \leftarrow \mathcal{A}_2(st, \pi_b) \end{bmatrix} - \Pr \begin{bmatrix} (\mathsf{crs}, \mathsf{tk}) \leftarrow \mathsf{S}_{\mathsf{zk}}(1^{\lambda}), \\ (x, \psi, st) \leftarrow \mathcal{A}_1(\mathsf{crs}), \\ \pi \leftarrow \mathsf{SP}_{\mathsf{zk}}(\mathsf{crs}, \mathsf{tk}, x) : \\ 1 \leftarrow \mathcal{A}_2(st, \pi_b) \end{bmatrix} \right| \leq \epsilon_{\mathsf{zk}}(\lambda),$$

where A_1 is only allowed to output $(x, \psi) \in R$.

One-time true-simulation extractability (tSE): tSE is a strengthened soundness notion [11], which says that any efficient adversary \mathcal{A} cannot produce a valid proof π^* for x^* without knowing x^* 's witness, even \mathcal{A} can see a simulated proof for a valid statement x.

For a tSE-NIZK, its setup algorithm Setup outputs an additional extraction key ek, apart from outputting crs and tk. We say Π satisfies one-time ϵ_{tse} -tSE, if there exists a simulation-knowledge extractor KExt_{zk}, such that for any polynomial-time adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$, its advantage Adv^{tse}₄(λ) (defined below) is not greater than $\epsilon_{tse2}(\lambda)$,

$$\Pr\left[(\mathtt{crs},\mathtt{tk},\mathtt{ek}) \leftarrow \mathsf{S}_{\mathsf{zk}}(1^{\lambda}), (x,\psi,st) \leftarrow \mathcal{A}_{1}(\mathtt{crs}), \pi \leftarrow \mathsf{SP}_{\mathsf{zk}}(\mathtt{crs},\mathtt{tk},x), \\ (x^{*},\pi^{*}) \leftarrow \mathcal{A}_{2}(st,\pi), \psi^{*} \leftarrow \mathsf{KExt}_{\mathsf{zk}}(\mathtt{crs},\mathtt{tk},x^{*},\pi^{*}) : (x^{*},\psi^{*}) \notin R \right],$$

where (x, ψ) outputted by A_1 must be in R.

Deterministic public-key encryption (DPKE). A DPKE scheme Σ is defined by a triple of PPT algorithms: the generation algorithm K_{de} , the encryption algorithm E_{de} , and the decryption algorithm D_{de} , where E_{de} and D_{de} are deterministic. Below we introduce the PRIV-IND-security with respect to hard-to-invert auxiliary inputs by following [7].

 Σ is $(n, \epsilon_{\mathsf{hv}}, \epsilon_{\mathsf{ind}})$ -PRIV-IND-secure, if for any message source \mathcal{W} defined over $\{\{0, 1\}^{n(\lambda)}\}_{\lambda \in \mathbb{N}}$ and any function ensemble $\mathcal{F} = \{f_{\lambda}\}_{\lambda \in \mathbb{N}}$ such that \mathcal{F} is ϵ_{hv} -hard-to-invert w.r.t. \mathcal{W} , for any polynomial-time adversary \mathcal{A} , its advantage $\mathsf{Adv}^{\mathsf{ind}}_{\mathcal{A},\mathcal{W},\mathcal{F}}(\lambda)$ defined below is not greater than $\epsilon_{\mathsf{ind}}(\lambda)$.

$$\left| \Pr \begin{bmatrix} (pk, sk) \leftarrow \mathsf{K}_{\mathsf{de}}(1^{\lambda}), m \leftarrow W_{\lambda}, \\ c \leftarrow \mathsf{E}_{\mathsf{de}}(pk, m) : \\ 1 \leftarrow \mathcal{A}(c, pk, f_{\lambda}(m)) \end{bmatrix} - \Pr \begin{bmatrix} (pk, sk) \leftarrow \mathsf{K}_{\mathsf{de}}(1^{\lambda}), m \leftarrow W_{\lambda} \\ m' \leftarrow \$ \{0, 1\}^{n(\lambda)}, c \leftarrow \mathsf{E}_{\mathsf{de}}(pk, m') : \\ 1 \leftarrow \mathcal{A}(c, pk, f_{\lambda}(m)) \end{bmatrix} \right|.$$

We assume w.l.o.g. that Σ has a key relation R_{pk} such that for every $(pk, sk) \in R_{pk}$, it follows that $\mathsf{D}_{\mathsf{de}}(sk, \mathsf{E}_{\mathsf{de}}(pk, m)) = m$ for any message m.

3 A New Lower Bound for IT-secure Robust Extractors

As briefly explained in the introduction, a plain-model IT-secure robust extractor for all (n, k)sources exists only when k > n/2 [15]. This lower bound can be trivially circumvented by assuming
a CRS but working only for the special sources *independent* of the CRS. We are interested in the
case of general sources which may be CRS-dependent. In this section, we give a negative result that
IT-secure robust extractors for all (n, k)-sources also require that k > n/2 in the CRS setting. The
fuzzy case trivially inherits this generalized lower bound.

Previous tool for the plain model lower bound. Dodis and Wichs's [15] lower-bound comes from a plain-model IT-secure authentication scheme (for an- $(\widehat{n}, \widehat{k})$ -distribution W), which is trivially implied by an IT-secure robust extractor. Such an authentication scheme could be described by a pair of randomized functions {Auth, Vrfy}, formed by Auth : $\{0,1\}^{\widehat{n}} \to \{0,1\}^{\widehat{s}}$, and Vrfy : $\{0,1\}^{\widehat{n}} \times \{0,1\}^{\widehat{s}} \to \{0,1\}$, where \widehat{n},\widehat{s} are integers. It satisfies (1) $\widehat{\rho}$ -correctness: $\Pr[w \leftarrow W : Vrfy(w, Auth(w)) = 1] \ge \widehat{\rho}$; and (2) $\widehat{\delta}$ -unforgeability: for any adversary \mathcal{A} , $\Pr[w \leftarrow W, \varsigma \leftarrow Auth(w), \varsigma^* \leftarrow \mathcal{A}(\varsigma) : Vrfy(w, \varsigma^*) = 1] \le \widehat{\delta}$.

Lemma 1 ([15]). If there exists an authentication scheme for all $(\widehat{n}, \widehat{k})$ -distributions with $\widehat{\rho}$ -correctness and $\widehat{\delta}$ -unforgeability, and $\widehat{\delta} < \widehat{\rho}^2/4$, it follows that $\widehat{k} > \widehat{n}/2$.

Generalizing the lower-bound. We present a new lower bound for the CRS-model in the following theorem, and our main technical lemma is to show that a CRS-model authentication scheme could imply that in the plain model (Lemma 2).

Theorem 1. Let $n, k, \ell : \mathbb{N} \to \mathbb{N}$ and $\rho, \delta : \mathbb{N} \to \{0, 1\}$ be functions of the security parameter. If there exists an (n, k, ℓ) IT-secure robust extractor with ρ -correctness and δ -pre-application-robustness, then for any $\lambda \in \mathbb{N}$ s.t. $\delta(\lambda) \leq \rho(\lambda)^2/4$, it follows that $k(\lambda) > n(\lambda)/2$.

Proof. For ease of analysis, our proof uses the *worst-case* conditional min-entropy without loss of generality. As, by definition, a robust extractor for average-case sources is one for worst-case sources with the same parameters, any lower bound for the latter naturally applies to the former.

We first define a CRS-model authentication scheme, which consists {CAuth, CVrfy} (randomized) along with a CRS distribution $\widehat{\mathsf{CRS}}$, satisfying the following, for any worst-case $(\widehat{n}, \widehat{k})$ -source W:

- $\widehat{\rho}\text{-correctness: } \Pr[\mathtt{crs} \leftarrow \widehat{\mathsf{CRS}}, w \leftarrow W|_{\mathtt{crs}} : \mathsf{Vrfy}(\mathtt{crs}, w, \mathsf{Auth}(\mathtt{crs}, w)) = 1] \geq \widehat{\rho}.$
- $-\hat{\delta}$ -unforgeability: for any adversary A.

$$\Pr\left[\frac{\mathsf{crs} \leftarrow \widehat{\mathsf{CRS}}, w \leftarrow W|_{\mathsf{crs}}, \varsigma \leftarrow \mathsf{Auth}(\mathsf{crs}, w),}{\varsigma^* \leftarrow \mathcal{A}(\mathsf{crs}, \varsigma) : \mathsf{Vrfy}(\mathsf{crs}, w, \varsigma^*) = 1.} \right] \leq \widehat{\delta}.$$

If there is a CRS-model IT-secure (n, k, ℓ) -robust extractor {CRS, Gen, Rep} with ρ -correctness and δ -robustness, then, for each $\lambda \in \mathbb{N}$, we can construct {CAuth, CVrfy} along with a CRS distribution $\widehat{\mathsf{CRS}} = \mathsf{CRS}_{\lambda}$ that satisfies $\widehat{\rho} = \rho(\lambda)$ -correctness and $\widehat{\delta} = \delta(\lambda)$ -unforgeability w.r.t all worst-case $(n(\lambda), k(\lambda))$ -distributions. More detailly,

- CAuth(crs, w): Invoke $(R, P) \leftarrow \mathsf{Gen}(\mathsf{crs}, w)$, and return $\sigma = P$;
- $\mathsf{CVrfy}(\mathsf{crs}, w, \sigma) : \mathsf{If} \; \mathsf{Rep}(\mathsf{crs}, w, \sigma) = \bot, \; \mathsf{return} \; 0; \; \mathsf{otherwise}, \; \mathsf{return} \; 1.$

Next, we give our main technical lemma for the CRS-model authentication scheme, whose detailed proof is deferred later.

Lemma 2. If there exists a CRS-model IT-secure authentication scheme {CAuth, CVrfy} (along with a CRS distribution $\widehat{\mathsf{CRS}}$) for all worst-case $(\widehat{n}, \widehat{k})$ -distributions (w.r.t. $\widehat{\mathsf{CRS}}$) with $\widehat{\rho}$ -correctness and $\widehat{\delta}$ -unforgeability, then for any $\widehat{c}_0, \widehat{c}_1 \in (0,1)$ satisfying $(1-\widehat{c}_1)\widehat{\rho}+\widehat{c}_0 > 1$, there exists a plain-model IT-secure authentication scheme {Auth, Vrfy} for all $(\widehat{n}, \widehat{k})$ -distributions with $\widehat{c}_1\widehat{\rho}$ -correctness and $\widehat{\delta}/\widehat{c}_0$ -unforgeability.

By Lemma 1, if $\hat{\delta}/\hat{c}_0 < (\hat{c}_1\hat{\rho})^2/4$, {Auth, Vrfy} established in Lemma 2 exists only when $\hat{k} > \hat{n}/2$. Putting requirements together, {CAuth, CVrfy} with $\hat{\rho}$ -correctness and $\hat{\delta}$ -unforgeability could imply such {Auth, Vrfy}, if there exists $\hat{c}_0, \hat{c}_1 \in \{0, 1\}$, such that

$$\hat{\delta} < \frac{\widehat{c}_0 \widehat{c}_1^2 \widehat{\rho}^2}{4}, \quad \text{and} \quad (1 - \widehat{c}_1)\widehat{\rho} + \widehat{c}_0 > 1.$$
 (5)

It remains to show when such $(\widehat{c}_0, \widehat{c}_1)$ exist. Note for any $\widehat{\rho} \in (0, 1)$, there always exists $(\widehat{c}_0, \widehat{c}_1) \in (0, 1)^2$ satisfying $(1 - \widehat{c}_1)\widehat{\rho} + \widehat{c}_0 > 1$ (denote the solution space by $S_{\widehat{\rho}}$). Then, we can have $(\widehat{c}_0, \widehat{c}_1)$ satisfying Eq.5 for $(\widehat{\rho}, \widehat{\delta})$, unless $\frac{4\widehat{\delta}}{\widehat{\rho}^2} \ge \widehat{c}_0\widehat{c}_1^2$ for any $(\widehat{c}_0, \widehat{c}_1) \in S_{\widehat{\rho}}$.

By standard analysis, we have the following result. For any $\widehat{\rho}, \widehat{v} \in (0,1)$, there always exists $(\widehat{c}_0, \widehat{c}_1) \in S_{\widehat{\rho}}$ such that $\widehat{c}_0\widehat{c}_1^2 > \widehat{v}$. It follows that whenever $\widehat{\delta} < \widehat{\rho}^2/4$, such $(\widehat{c}_0, \widehat{c}_1)$ exist. Recall that for any λ s.t. $\delta(\lambda) < \rho(\lambda)^2/4$, the robust extractor could give such {CAuth, CVrfy} for all $(n(\lambda), k(\lambda))$ -distributions. It follows $k(\lambda) < n(\lambda)/2$ in this case.

Deferred proof for Lemma 2. The overall goal is to show there exists a "good" CRS crs* in the support of $\widehat{\mathsf{CRS}}$, such that with crs* hardcoded, $\{\mathsf{CAuth}(\mathsf{crs}^*,\cdot),\mathsf{CVrfy}(\mathsf{crs}^*,\cdot)\}$ is the plain-model authentication scheme. For both *correctness* and *unforgeability*, we will prove that there exists a sufficiently large "good" set of CRSs (S and $\widetilde{\mathsf{S}}$) for each of them. Then by properly tuning parameters, we can see $\mathsf{S} \cap \widetilde{\mathsf{S}} \neq \emptyset$; thus, we can find a string crs*.

In the claim below, we show the existence of S (for *correctness*). We proceed in two steps. (i) For each source W, since we have ρ -correctness for a randomly sampled $crs \leftarrow \widehat{\mathsf{CRS}}$, there must exist a large enough "good" set S_W that every element of it will enable "correctness" (with a smaller correctness parameter). (ii) To show $\bigcap_W \mathsf{S}_W$ is still with sufficient size, we can use proof by contradiction in the sense that if it does not hold, we can define a special source W^* , its "good" set S_{W^*} will be smaller than established in the previous step.

Claim. For any constant $\widehat{c}_1 \in (0,1)$, there exists a set $S \in \text{Supp}(\widehat{CRS})$ satisfying (i) $\Pr[\widehat{CRS} \in S] \ge (1-\widehat{c}_1)\widehat{\rho}$, and (ii) for any $\operatorname{crs} \in S$ and $(\widehat{n}, \widehat{k})$ -distribution W, it holds that

$$\Pr\left[w \leftarrow W|_{\mathtt{crs}}, \varsigma \leftarrow \mathsf{CAuth}(\mathtt{crs}, w) : \mathsf{CVrfy}(\mathtt{crs}, w, \varsigma) = 1\right] \geq \widehat{c}_1 \widehat{\rho}.$$

Proof. For convenience, we define the "verified correctly" event w.r.t. W and crs:

$$\mathtt{VC}_{W,\mathtt{crs}} := [w \leftarrow W|_{\mathtt{crs}}, \varsigma \leftarrow \mathsf{CAuth}(\mathtt{crs}, w) : \mathsf{CVrfy}(\mathtt{crs}, w, \varsigma) = 1].$$

Then define a "good" set S for an $(\widehat{n}, \widehat{k})$ -distribution W. Namely,

$$S_W := \{ crs \in \mathsf{Supp}(\mathsf{CRS}) : \Pr[\mathtt{VC}_{W,\mathsf{crs}}] \ge \widehat{c}_1 \widehat{\rho} \}. \tag{6}$$

We now show

$$\Pr[\widehat{\mathsf{CRS}} \in \mathsf{S}_W] \ge (1 - \widehat{c}_1)\widehat{\rho} \tag{7}$$

for any (\hat{n}, \hat{k}) -distribution W. If not, for some W, we have the following,

$$\begin{split} &\Pr[\texttt{crs} \leftarrow \widehat{\mathsf{CRS}} : \mathtt{VC}_{W,\texttt{crs}}] \\ &\leq \Pr[\mathtt{VC}_{W,\texttt{crs}} | \texttt{crs} \notin \mathtt{S}_W] \Pr[\widehat{\mathsf{CRS}} \notin \mathtt{S}_W] + \Pr[\widehat{\mathsf{CRS}} \in \mathtt{S}_W] \\ &\leq \widehat{c}_1 \widehat{\rho} + (1 - \widehat{c}_1) \widehat{\rho} = \widehat{\rho}, \end{split}$$

which contradicts the assumption that $\{CAuth, CVrfy\}$ along with \widehat{CRS} satisfies the $\widehat{\rho}$ -correctness. Note that S_W is a "locally good" set for W, and we need a "globally good" set S for all $(\widehat{n}, \widehat{k})$ -distributions. By definition, S will be the intersection of all worst-case S_W w.r.t. \widehat{CRS} , namely,

$$\mathtt{S} = igcap_{orall (\widehat{n},\widehat{k}) ext{-distribution }W} \mathtt{S}_W.$$

Our goal is to show $\Pr[\widehat{\mathsf{CRS}} \in \mathsf{S}] \geq (1 - \widehat{c}_1)\widehat{\rho}$. We proceed with it by contradiction. Specifically, if not, the complement of S (denoted by S^C) will satisfy $\Pr[\widehat{\mathsf{CRS}} \in \mathsf{S}^C] > 1 - (1 - \widehat{c}_1)\widehat{\rho}$. By definition, for every $\mathsf{crs}_i \in \mathsf{S}^C$, there exists a $(\widehat{n}, \widehat{k})$ -distribution W_i , such that

$$\Pr[\mathtt{VC}_{W_i,\mathtt{crs}_i}] < \widehat{c}_1 \widehat{\rho}.$$

Next, we can define a distribution W^* for which the set S_{W^*} does not satisfy Eq.7. Specifically, $W^* = \{W^*|_{\mathtt{crs}_i}\}_{\mathtt{crs}_i \in \mathsf{Supp}(\widehat{\mathsf{CRS}})}$, where

$$W^*|_{\operatorname{crs}_i} = \begin{cases} W_i|_{\operatorname{crs}_i}, & \text{if } \operatorname{crs}_i \in S^C, \\ U_{\widehat{n}}, & \text{if } \operatorname{crs}_i \in S. \end{cases}$$
 (8)

Here $U_{\widehat{n}}$ denotes the uniform distribution over $\{0,1\}^{\widehat{n}}$. As every W_i is a worst-case (\hat{n},\hat{k}) -distribution, the min-entropy of each $W_i|_{\mathtt{crs}_i}$ is larger than \hat{k} ; Thus W^* is also a worst-case (\widehat{n},\hat{k}) -distribution. However, from the definition of W^* , it follows that $\mathtt{S}_{W^*} \cap \mathtt{S}^C = \emptyset$, and thus $\Pr[\mathtt{CRS} \in \mathtt{S}_{W^*}] < (1-\widehat{c}_1)\widehat{\rho}$, which contradicts the result Eq.7.

For *unforgeability*, it follows a similar idea but with some more work. In the following claim, we show a set of CRSs, with sufficient weight, under a CRS in which an adversary's advantage of forging an authentication tag is small.

Claim. For any constant $\widehat{c}_0 \in (0,1)$, there exists a set $\widetilde{S} \in \mathsf{Supp}(\widehat{\mathsf{CRS}})$ such that $\Pr[\widehat{\mathsf{CRS}} \in \widetilde{\mathsf{S}}] \ge \widehat{c}_0$, and for any worst-case $\mathsf{crs} \in \widetilde{\mathsf{S}}$, any $(\widehat{n},\widehat{k})$ -distribution W, and any adversary \mathcal{A} , it holds that

$$\Pr\left[w \leftarrow W|_{\mathtt{crs}}, \varsigma \leftarrow \mathsf{CAuth}(\mathtt{crs}, w), \varsigma^* \leftarrow \mathcal{A}(\mathtt{crs}, \varsigma) : \mathsf{CVrfy}(\mathtt{crs}, w, \varsigma^*) = 1\right] < \widehat{\delta}/\widehat{c}_0.$$

Proof. For convenience, we define the "successfully forge" event w.r.t. W, A and crs:

$$SF_{W,A,crs} := [w \leftarrow W|_{crs}, \varsigma \leftarrow CAuth(crs, w), \varsigma^* \leftarrow A(crs, \varsigma) : CVrfy(crs, w, \varsigma^*) = 1].$$

Similarly, we define a "good" set $\widetilde{S}_{W,\mathcal{A}}$ for W and A. Namely,

$$\widetilde{S}_{W,A} := \{ \operatorname{crs} \in \operatorname{Supp}(\widehat{\mathsf{CRS}}) : \Pr[\operatorname{SF}_{W,A,\operatorname{crs}}] < \widehat{\delta}/\widehat{c}_0 \}.$$
 (9)

For any worst-case (\hat{n}, \hat{k}) -distribution W and any unbounded adversary A, it holds that

$$\widehat{\delta} > \Pr[\operatorname{crs} \leftarrow \widehat{\mathsf{CRS}} : \operatorname{SF}_{W,\mathcal{A},\operatorname{crs}}]$$

$$\geq \Pr[\operatorname{SF}_{W,\mathcal{A},\operatorname{crs}}|\operatorname{crs} \notin \widetilde{\operatorname{S}}_{W,\mathcal{A}}] \Pr[\widehat{\mathsf{CRS}} \notin \widetilde{\operatorname{S}}_{W,\mathcal{A}}]$$

$$\geq (\widehat{\delta}/\widehat{c}_0) \Pr[\widehat{\mathsf{CRS}} \notin \widetilde{\operatorname{S}}_{W,\mathcal{A}}], \tag{10}$$

which implies that $\Pr[\widehat{\mathsf{CRS}} \notin \widetilde{\mathsf{S}}_{W,\mathcal{A}}] \leq \widehat{c}_0$. Thus,

$$\Pr[\widehat{\mathsf{CRS}} \in \widetilde{\mathsf{S}}_{W,\mathcal{A}}] > \widehat{c}_0. \tag{11}$$

Then, we use $\widetilde{\mathtt{S}}_{W,\mathcal{A}}$ to "find" a "globally good" set. To this end, we define

$$\widetilde{\mathtt{S}}_{\mathcal{A}} := \bigcap_{egin{array}{c} orall (\widehat{n},\widehat{k}) ext{-distribution } W \end{array}} \widetilde{\mathtt{S}}_{W,\mathcal{A}}$$

and prove that $\Pr[\widehat{\mathsf{CRS}} \in \widetilde{\mathsf{S}}_{\mathcal{A}}] > \widehat{c}_0$.

This is similar to the proof for the above claim. Specifically, for every $\mathtt{crs}_i \in \widetilde{\mathtt{S}}^C_{\mathcal{A}}$, there will be at least one $(\widehat{n}, \widehat{k})$ -source W_i such that

$$\Pr[SF_{W_i,\mathcal{A},crs_i}] > \widehat{\delta}/\widehat{c}_0.$$

Then, we can define a distribution W^* ,

$$W^*|_{\mathtt{crs}_i} = \begin{cases} W_i|_{\mathtt{crs}_i}, \text{ if } \mathtt{crs}_i \in \mathtt{S}_{\mathcal{A}}^C, \\ U_{\hat{n}}, \text{ if } \mathtt{crs}_i \in \mathtt{S}_{\mathcal{A}}. \end{cases}$$

By definition, it follows that $\widetilde{\mathbf{S}}_{W^*,\mathcal{A}} \cap \widetilde{\mathbf{S}}_{\mathcal{A}}^{C} = \emptyset$. If $\Pr[\widehat{\mathsf{CRS}} \in \widetilde{\mathbf{S}}_{\mathcal{A}}^{C}] > 1 - \widehat{c}_0$, if holds that $\Pr[\widehat{\mathsf{CRS}} \in \widetilde{\mathbf{S}}_{W,\mathcal{A}}^{C}] < \widehat{c}_0$, which contradicts our result specified in Eq.11. Therefore, we have

$$\Pr[\widehat{\mathsf{CRS}} \in \widetilde{\mathsf{S}}_{\mathcal{A}}] > \widehat{c}_0 \tag{12}$$

Next, define

$$\widetilde{\mathtt{S}} = \bigcap_{\mathcal{A}} \widetilde{\mathtt{S}}_{\mathcal{A}}$$

and prove that $\Pr[\widehat{\mathsf{CRS}} \in \in \widetilde{\mathsf{S}}] > \widehat{c}_0$. Similar to above arguments, for any $\mathsf{crs}_i \in \widetilde{\mathsf{S}}^C$, there must exist an adversary \mathcal{A}_i such that $\exists W_i$ and

$$\Pr[\mathtt{SF}_{W_i,\mathcal{A}_i,\mathtt{crs}_i}] > \widehat{\delta}/\widehat{c}_0.$$

Then, we can define a "new" adversary A^* which

$$\begin{cases} \text{invokes } \mathcal{A}_i, \text{ if on input } \operatorname{\mathtt{crs}}_i \in \widetilde{\mathtt{S}}; \\ \text{outputs 0, otherwise.} \end{cases}$$
 (13)

By definition, it must hold that $\widetilde{S}_{\mathcal{A}^*} \cap \widetilde{S}^C = \emptyset$. In this case, if $\Pr[\widehat{\mathsf{CRS}} \in \widetilde{\mathsf{S}}^C] > 1 - \widehat{c}_0$, it follows that $\Pr[\widehat{\mathsf{CRS}} \in \widetilde{\mathsf{S}}_{\mathcal{A}^*}] < \widehat{c}_0$, which contradicts our results specified in Eq.12. Thus, we have $\Pr[\widehat{\mathsf{CRS}} \in \widetilde{\mathsf{S}}] > \widehat{c}_0$.

Finally, by the parameter condition in Eq.5 that $(1-\widehat{c}_1)\widehat{\rho}+\widehat{c}_0>1$, it follows that $S\cap\widetilde{S}\neq\emptyset$. We pick one $\mathtt{crs}^*\in S\cap\widetilde{S}$, and define an ensemble of randomized function pairs $\{\mathsf{Auth}=\mathsf{CAuth}(\mathtt{crs}^*,\cdot),\mathsf{Vrfy}=\mathsf{CVrfy}(\mathtt{crs}^*,\cdot)\}$. It is easy to verify this $\{\mathsf{Auth},\mathsf{Vrfy}\}$ satisfies $\widehat{c}_1\widehat{\rho}$ -correctness and $\widehat{\delta}/\widehat{c}_0$ for all $(\widehat{n},\widehat{k})$ -distributions.

4 Computational Robust Extractors

In this section, we provide a generic framework in the CRS model that compiles any computational extractor into a robust one. Compared with previous works, our construction is the first that can work for any CRS dependent source with minimal entropy $(\omega(\log n))$ instead of n/2 as in the IT setting).

Intuitions. As briefly discussed in the Introduction, a fairly intuitive idea is to add a MAC tag on the helper string: with a MAC $\{Tag, Verify\}$ (for simplicity here we omit the public parameters) and a strong extractor Ext, the generation procedure produces a helper string formed by (s, Tag(w, s)) along with a randomness r, where s is the seed for Ext and r is the extracted randomness by Ext. The reproduce procedure first checks the validity of Tag(w, s), and reproduces r = Ext(s, w) if the tag is valid.

However, it is not hard to see the insufficiency of a normal MAC here. First, the secret w is non-uniform, and some information about w will be further leaked by (s,r) (for the strong post-application robustness), while a MAC usually requires a uniform key. Moreover, the tag Tag(w,s) may also leak partial information about w (e.g., some bits of it), and thus affect the quality of r. The above issues inspire us to consider a special MAC that can address the aforementioned concerns simultaneously. At a high level, 1) it should be secure w.r.t. auxiliary information about the weak secret w, as both the seed i_{ext} and the extracted string r generated from w are leaked to adversaries; and 2) the tag of this MAC should also hide all partial information about w, such that given the tag the extracted string r remains pseudorandom. We call such a MAC κ -MAC (Key-Private Auxiliary-input Message Authentication). For constructing a robust extractor, we only need to ask the one-time security of κ -MAC.

In the following, we formally define κ -MAC and present and analyze our framework of robust extractors from κ -MAC. Then, we show how to construct (one-time) κ -MAC from well-studied assumptions.

4.1 κ -MAC Definition

We define the syntax of κ -MAC in the CRS model.

<u>Syntax.</u> A κ-MAC scheme Σ consists of a triple of algorithms {Init, Tag, Verify}, with associated key space $\mathcal{K} = \{\mathcal{K}_{\lambda}\}_{{\lambda} \in \mathbb{N}}$, message space $\mathcal{M}es = \{\mathcal{M}es_{\lambda}\}_{{\lambda} \in \mathbb{N}}$, and tag space $\mathcal{T} = \{\mathcal{T}_{\lambda}\}_{{\lambda} \in \mathbb{N}}$.

- Init(1 $^{\lambda}$). On input a security parameter 1 $^{\lambda}$, it outputs a crs whose distribution is denoted by CRS $_{\lambda}$ and a trapdoor key τ .
- Tag(crs, k, m). The authentication algorithm takes as inputs a CRS crs, a key $k \in \mathcal{K}_{\lambda}$, and a message $m \in \mathcal{M}es_{\lambda}$. It outputs a tag $\varsigma \in \mathcal{T}_{\lambda}$.
- Verify(crs, k, m, ς). The verification algorithm takes as inputs a CRS crs, a key k, a message m, and an authentication tag ς . It outputs either 1 accepting (m, ς) or 0 rejecting (m, ς) .

The correctness states that for every $\operatorname{crs} \leftarrow \operatorname{Init}(1^{\lambda})$, every secret $k \in \mathcal{K}_{\lambda}$, and every message $m \in \mathcal{M}es_{\lambda}$, we have $\Pr[\operatorname{Verify}(\operatorname{crs}, k, m, \operatorname{Tag}(\operatorname{crs}, k, m))] = 1$. A secure κ -MAC scheme should satisfy unforgeability which is similar to regular MAC, and key privacy which requires the tag to be

³ The RO-based MAC (where $\mathsf{Tag}(w,m) = H(w,m)$ for a random oracle H) employed in Boyen *et al.*'s robust (fuzzy) extractor [6] captures all above intuitions, and thus it can be considered as a κ -MAC in the random oracle model.

simulatable without using the key. Note that the trapdoor key outputted by Init is for defining the key-privacy property alone. The main difference (with the conventional definitions) in the security notions is that they are all under auxiliary input. We first discuss the admissible auxiliary input and then present the formal definitions.

Admissible auxiliary inputs. Note that the auxiliary information cannot be arbitrary. (1) it must be hard-to-invert leakage, as defined by Dodis et al. [12] which we recall in Sect. 2.4. (2) to avoid triviality, the auxiliary information should not contain a valid authentication tag. Note that the authentication algorithm is indeed "hard-to-invert", and thus we have to put other restrictions on the leakage function to exclude the trivial case. Similar issues arise in auxiliary-input secure digital signatures [16] requiring the admissible function f to be exponentially hard-to-invert. For our purpose, however, this treatment will impose unnecessary restrictions on the sources being extracted or the underlying extractor. Instead, we observe and leverage the following asymmetry: the authentication algorithm is only required to be hard-to-invert for a randomly chosen CRS for which the adversary does not hold a-priori knowledge; while the auxiliary-input function, particularly, the Gen of the underlying extractor, can be uninvertible regardless of what knowledge $\mathcal A$ may have about CRS. In light of the above, we present the following definition.

Definition 4 (Admissible auxiliary inputs). A function ensemble \mathcal{F} is an ϵ_{hv} -AI w.r.t. \mathcal{W} and the CRS ensemble CRS, if for any function ensemble \mathcal{G} , \mathcal{F} is ϵ_{hv} -hard-to-invert w.r.t. the conditional distribution ensemble (\mathcal{W} |CRS, \mathcal{G} (CRS)).

We may call \mathcal{F} an ϵ_{hv} -AI without specifying \mathcal{W} and CRS if they are obvious in the context.

 $\overline{One\text{-}time\ unforgeability}$. The unforgeability captures the infeasibility of forging an authentication tag being accepted by a secret key k drawn from a high-entropy source. Particularly, it considers a non-uniformly distributed key and allows adversaries to obtain auxiliary information about it.

Definition 5 (One-time unforgeability). Let $\Sigma = \{\text{Init}, \text{Tag}, \text{Verify}\}\ be\ a\ \kappa\text{-}MAC\ scheme\ with\ the\ key\ space}\ \{0,1\}^{n(\lambda)}$. We say Σ satisfies $(n, \epsilon_{\mathsf{unf}}, \epsilon_{\mathsf{hv}})$ one-time unforgeability, if for any polynomial time adversary A, any efficiently-samplable source \mathcal{W} (defined over $\{\{0,1\}^{n(\lambda)}\}_{\lambda \in \mathbb{N}}$) and any ϵ_{hv} - $AI\ \mathcal{F}$, it holds that

$$\mathsf{Adv}^{\mathrm{unf}}_{\mathcal{A},\mathcal{W},\mathcal{F}}(\lambda) = \Pr[\mathsf{Exp}^{\mathsf{unf}}_{\mathcal{A},\mathcal{W},\mathcal{F}}(\lambda) = 1] \leq \epsilon_{\mathsf{unf}}(\lambda).$$

The experiment $\mathsf{Exp}^{\mathsf{unf}}_{A,\mathcal{W},\mathcal{F}}$ is defined below.

```
\begin{split} & \frac{\mathsf{Exp}^{\mathsf{unf}}_{\mathcal{A},\mathcal{W},\mathcal{F}}(\lambda)}{(\mathsf{crs},\tau) \leftarrow \mathsf{Init}(1^{\lambda}); k \leftarrow W_{\lambda}|_{\mathsf{crs}}} \\ & (m,st) \leftarrow \mathcal{A}(\mathsf{crs},f_{\lambda}(\mathsf{crs},k)); \varsigma \leftarrow \mathsf{Tag}(\mathsf{crs},k,m) \\ & (m^*,\varsigma^*) \leftarrow \mathcal{A}(\varsigma,st) \\ & \mathbf{if} \ (m^*,\varsigma^*) \neq (m,\varsigma) \land \mathsf{Verify}(\mathsf{crs},k,m^*,\varsigma^*) = 1 \ \mathbf{then} \quad \mathbf{return} \ 1 \\ & \mathbf{return} \ 0 \end{split}
```

<u>One-time key privacy</u>. This property seeks to capture that an adversary cannot learn anything new about the secret from an authentication tag.

We follow the simulation paradigm that was developed for defining non-interactive zero knowledge [4]. Namely, with the help of the "trapdoor" information about the CRS, these tags can be simulated without the secret, and adversaries cannot distinguish simulated tags from real ones.

Definition 6 (One-time key privacy). Let $\Sigma = \{\text{Init}, \text{Tag}, \text{Verify}\}\$ be a κ -MAC scheme with the key space $\{0,1\}^{n(\lambda)}$. We say Σ satisfies $(n, \epsilon_{\mathsf{kpriv}}, \epsilon_{\mathsf{hv}})$ one-time key privacy, if there is a PPT algorithm SimTag, and for any polynomial-time adversary \mathcal{A} , any efficiently-samplable source \mathcal{W} (defined over $\{\{0,1\}^{n(\lambda)}\}_{\lambda \in \mathbb{N}}$) and any ϵ_{hv} -AI \mathcal{F} , it holds that

$$\mathsf{Adv}^{\mathrm{kpriv}}_{\mathcal{A},\mathcal{W},\mathcal{F}}(\lambda) = |\Pr[\mathsf{Exp}^{\mathsf{kpriv},0}_{\mathcal{A},\mathcal{W},\mathcal{F}}(\lambda) = 1] - \Pr[\mathsf{Exp}^{\mathsf{kpriv},1}_{\mathcal{A},\mathcal{W},\mathcal{F}}(\lambda) = 1]| \leq \epsilon_{\mathsf{unf}}(\lambda).$$

The experiments $\mathsf{Exp}_{\mathcal{A},\mathcal{W},\mathcal{F}}^{\mathsf{kpriv},0}$ and $\mathsf{Exp}_{\mathcal{A},\mathcal{W},\mathcal{F}}^{\mathsf{kpriv},1}$ are defined below.

$\boxed{Exp^{kpriv,0}_{\mathcal{A},\mathcal{W},\mathcal{F}}(\lambda)}$	$Exp^{kpriv,1}_{\mathcal{A},\Sigma,\mathcal{W},\mathcal{F}}(\lambda)$
$(\operatorname{crs}, \tau) \leftarrow \operatorname{Init}(1^{\lambda}); k \leftarrow W_{\lambda} _{\operatorname{crs}}$	$(\mathtt{crs}, \tau) \leftarrow Init(1^{\lambda}); k \leftarrow W_{\lambda} _{\mathtt{crs}}$
$(m,st) \leftarrow \mathcal{A}(\mathtt{crs},f_{\lambda}(\mathtt{crs},k))$	$(m,st) \leftarrow \mathcal{A}(\mathtt{crs},f_{\lambda}(\mathtt{crs},k))$
$\varsigma \leftarrow SimTag(\mathtt{crs},\tau,m); b' \leftarrow \mathcal{A}(\varsigma,st)$	$\varsigma \leftarrow Tag(crs, k, m); b' \leftarrow \mathcal{A}(\varsigma, st)$
$\mathbf{return}\ b'$	$\mathbf{return}\ b'$

4.2 Computational Robust Extractor from κ -MAC

We then show how to compile a strong extractor into a robust extractor (for general CRS-dependent sources) using one-time κ -MAC. Let Ext be a (n, k, ℓ) strong extractor (working on (n, k)-sources, and output ℓ bits) with the seed length $s\ell$, and let $\Sigma = \{\text{Init}, \text{Tag}, \text{Verify}\}$ be a κ -MAC scheme with the key space $\mathcal{K} = \{\{0, 1\}^{n(\lambda)}\}_{\lambda \in \mathbb{N}}$ and the message space $\mathcal{M}es$ that contains $\{\{0, 1\}^{\ell(\lambda) + s\ell(\lambda)}\}_{\lambda \in \mathbb{N}}$. Then, we illustrate our robust extractor construction $\mathcal{E} = \{\text{CRS}, \text{Gen}, \text{Rep}\}$ in Fig.1.

$CRS(1^{\lambda})$	Gen(crs,w)	$Rep(\mathtt{crs}, w, P)$
$\boxed{(\mathtt{crs},\tau) \leftarrow Init(1^{\lambda})}$	$s \leftarrow \$ \{0,1\}^{s\ell(\lambda)}, r \leftarrow Ext(s,w)$	
return crs	$\varsigma \leftarrow Tag(crs, w, s)$	$\mathbf{return}\ R = Ext(s,w)$
	return $R = r, P = (s, \varsigma)$	$\mathbf{return} \ \perp$

Fig. 1. Robust extractor rExt from randomness extractor + one time κ -MAC

Analysis. The correctness and security of our construction are fairly straightforward. We only require the source to have minimal min-entropy to enable a strong extractor. Formally, we have the following theorem.

Theorem 2. Let Ext be an average-case (n, k, ℓ) -strong extractor with ϵ_{ext} -privacy and being ϵ_{inv} -hard-to-invert, Σ be a κ -MAC with $(n, \epsilon_{\mathsf{kpriv}}, \epsilon_{\mathsf{hv}})$ one-time key privacy and $(n, \epsilon_{\mathsf{unf}}, \epsilon_{\mathsf{hv}})$ one-time robustness. If $\epsilon_{\mathsf{hv}} \geq \epsilon_{\mathsf{inv}}$, then for any $\epsilon_{\mathsf{priv}}, \delta_{\mathsf{rob}}$, satisfying $\epsilon_{\mathsf{priv}} \geq \epsilon_{\mathsf{ext}} + 2\epsilon_{\mathsf{kpriv}}$, and $\delta_{\mathsf{rob}} > \epsilon_{\mathsf{unf}}$, the construction in Fig.1 is an (n, k, ℓ) -robust extractor with ϵ_{priv} -privacy and δ_{rob} -post-application-robustness.

We prove the privacy and robustness in Lemma 3 and Lemma 4, respectively.

Lemma 3. rExt (in Fig. 1) satisfies ϵ_{priv} -privacy, for any $\epsilon_{priv} > \epsilon_{ext} + 2\epsilon_{kpriv}$.

Proof. We prove this lemma by contradiction. Assume we have a polynomial-time adversary \mathcal{B} and an efficiently-samplable (n, k)-source \mathcal{W} such that $\mathsf{Adv}^{\mathsf{priv}}_{\mathcal{B}, \mathcal{W}}(\lambda) > \epsilon_{\mathsf{ext}} + 2\epsilon_{\mathsf{kpriv}}$. Then, we leverage \mathcal{B} to construct a polynomial-time adversary $\mathcal{A}_{\mathsf{ext}}$ for Ext, and two polynomial-time adversaries $\mathcal{A}_{\mathsf{mac},0}$ and $\mathcal{A}_{\mathsf{mac},1}$ for κ -MAC Σ , such that, for the source \mathcal{W} , it follows that either

$$\mathsf{Adv}^{\mathrm{ext}}_{\mathcal{A}_{\mathsf{ext}},\mathcal{W}}(\lambda) > \epsilon_{\mathsf{ext}}, \ \mathsf{Adv}^{\mathrm{kpriv}}_{\mathcal{A}_{\mathsf{mac},0},\mathcal{W},\mathcal{F}}(\lambda) > \epsilon_{\mathsf{kpriv}}, \ \mathrm{or} \ \mathsf{Adv}^{\mathrm{kpriv}}_{\mathcal{A}_{\mathsf{mac},1},\mathcal{W},\mathcal{F}}(\lambda) > \epsilon_{\mathsf{kpriv}}. \tag{14}$$

Here, \mathcal{F} is a funtion ensemble implementing Ext. As $\epsilon_{hv} \geq \epsilon_{inv}$, such \mathcal{F} is an admissible auxiliary inputs. (CRS, $\mathcal{T} = \{T_{\lambda}\}$) denotes the random variable ensemble outputted by Init of κ -MAC; As \mathcal{T} can be computed (even inefficiently) using CRS and coins independent of \mathcal{W} , for every λ , we have

$$\widetilde{\mathbf{H}}_{\infty}(W_{\lambda}|\mathsf{CRS}_{\lambda},T_{\lambda}) = \widetilde{\mathbf{H}}_{\infty}(W_{\lambda}|\mathsf{CRS}_{\lambda}) \geq k(\lambda).$$

Therefore, Eq.14 contradcits our assumptions on the underlying tools, and thus $\mathsf{Adv}^{\mathsf{priv}}_{\mathcal{B},\mathcal{W}}(\lambda) \leq \epsilon_{\mathsf{ext}} + 2\epsilon_{\mathsf{kpriv}}$ for all admissible \mathcal{B} and \mathcal{W} .

Now, to proceed with the proof, we turn to construct the adversaries $\mathcal{A}_{\mathsf{ext}}$, $\mathcal{A}_{\mathsf{mac},0}$ and $\mathcal{A}_{\mathsf{mac},1}$, using \mathcal{B} against rExt. The adversaries' codes are presented below. In $\mathcal{A}_{\mathsf{ext}}$, SimTag is the simulator of κ -MAC. In $\mathcal{A}_{\mathsf{mac},b}$, r is the extracted randomness from w with the seed i_{ext} . \mathcal{O}_{β} returns a real tag when $\beta = 1$ or returns a simulated tag when $\beta = 0$.

Recall the privacy definition of a robust extractor (cf. Def.2). The adanvantage of \mathcal{B} against rExt's privay w.r.t. \mathcal{W} is defined by $\mathsf{Adv}^{\mathsf{priv}}_{\mathcal{B},\mathcal{W}}(\lambda) = |\Pr[\mathsf{Exp}^{\mathsf{priv},0}_{\mathcal{B},\mathcal{W}}(\lambda) = 1] - \Pr[\mathsf{Exp}^{\mathsf{priv},1}_{\mathcal{B},\mathcal{W}}(\lambda) = 1]|$. Recall the definition of the strong extractor in Sect.2, and assume that

$$p_0 = \Pr \begin{bmatrix} (\mathtt{crs}, \tau) \leftarrow (\mathsf{CRS}_{\lambda}, T_{\lambda}), w \leftarrow W_{\lambda}|_{\mathtt{crs}}, i_{\mathtt{ext}} \leftarrow \$ \{0, 1\}^{si(\lambda)} \\ r \leftarrow \$ \{0, 1\}^{\ell(\lambda)} : 1 \leftarrow \mathcal{A}_{\mathtt{ext}}(i_{\mathtt{ext}}, r, \mathtt{crs}, \tau) \end{bmatrix},$$

$$p_1 = \Pr \begin{bmatrix} (\mathtt{crs}, \tau) \leftarrow (\mathsf{CRS}_\lambda, T_\lambda), w \leftarrow W_\lambda|_{\mathtt{crs}}, i_{\mathtt{ext}} \leftarrow \$ \left\{0, 1\right\}^{si(\lambda)} \\ r \leftarrow \mathsf{Ext}(i_{\mathtt{ext}}, w) : 1 \leftarrow \mathcal{A}_{\mathtt{ext}}(i_{\mathtt{ext}}, r, \mathtt{crs}, \tau) \end{bmatrix}.$$

Then, the advanatage of $\mathcal{A}_{\mathsf{ext}}$ against Ext is $\mathsf{Adv}^{\mathsf{ext}}_{\mathcal{A}_{\mathsf{ext}},\mathcal{W},(\mathsf{CRS},\mathcal{T})}(\lambda) = |p_0 - p_1|$. For $b \in \{0,1\}$, we denote $\Pr[\mathsf{Exp}^{\mathsf{priv},b}_{\mathcal{B},\mathcal{W}}(\lambda) = 1] - p_b = \Delta_b$. By standard arguments, we have

$$\mathsf{Adv}^{\mathrm{priv}}_{\mathcal{B},\mathcal{W}}(\lambda) = \mathsf{Adv}^{\mathrm{ext}}_{\mathcal{A}_{\mathrm{ext}},\mathcal{W}}(\lambda) + |\Delta_0| + |\Delta_1| \tag{15}$$

It is easy to verify that, at the point of \mathcal{B} 's view, the experiment $\mathsf{Exp}^{\mathsf{priv},b}_{\mathcal{B},\mathcal{W}}$ is identical to $\mathsf{Exp}^{\mathsf{kpriv},1}_{\mathcal{A}_{\mathsf{mac},b},\mathcal{W},\mathcal{F}}$ (cf. Def.6), and thus $\Pr[\mathsf{Exp}^{\mathsf{priv},b}_{\mathcal{B},\mathcal{W}}(\lambda)=1]=\Pr[\mathsf{Exp}^{\mathsf{kpriv},1}_{\mathcal{A}_{\mathsf{mac},b},\mathcal{W},\mathcal{F}}(\lambda)=1]$. Similarly, we have $p_b=\Pr[\mathsf{Exp}^{\mathsf{kpriv},0}_{\mathcal{A}_{\mathsf{mac},b},\mathcal{W},\mathcal{F}}=1]$.

Notice that $\mathsf{Adv}^{\mathrm{kpriv}}_{\mathcal{A}_{\mathsf{mac},b},\mathcal{W},\mathcal{F}}(\lambda) = |\Pr[\mathsf{Exp}^{\mathsf{kpriv},0}_{\mathcal{A}_{\mathsf{mac},b},\mathcal{W},\mathcal{F}}(\lambda) = 1] - \Pr[\mathsf{Exp}^{\mathsf{kpriv},1}_{\mathcal{A}_{\mathsf{mac},b},\mathcal{W},\mathcal{F}}(\lambda) = 1]|$, we have $\mathsf{Adv}^{\mathrm{kpriv}}_{\mathcal{A}_{\mathsf{mac},b},\mathcal{W},\mathcal{F}}(\lambda) = \Delta_b$. Therefore, we have

$$\mathsf{Adv}^{\mathrm{priv}}_{\mathcal{B},\mathcal{W}}(\lambda) = \mathsf{Adv}^{\mathrm{ext}}_{\mathcal{A}_{\mathsf{ext}},\mathcal{W},(\mathsf{CRS},\mathcal{T})}(\lambda) + \mathsf{Adv}^{\mathrm{kpriv}}_{\mathcal{A}_{\mathsf{mac}},0,\mathcal{W},\mathcal{F}}(\lambda) + \mathsf{Adv}^{\mathrm{kpriv}}_{\mathcal{A}_{\mathsf{mac}},1,\mathcal{W},\mathcal{F}}(\lambda).$$

If $\mathsf{Adv}^{\mathrm{priv}}_{\mathcal{B},\mathcal{W}}(\lambda) > \epsilon_{\mathsf{ext}} + 2\epsilon_{\mathsf{kpriv}}$, Eq.14 immediately follows.

Lemma 4. rExt (in Fig.1) satisfies δ_{rob} -post-application-robustness, for any $\delta_{\text{rob}} \geq \epsilon_{\text{unf}}$.

Proof. We prove this lemma by contradiction. Assume there is $\delta_0 > \epsilon_{\sf unf}$, and we have a polynomial-time adversary \mathcal{B} who has an advantage greater than δ_0 w.r.t. some efficiently-samplable (n,k)-source \mathcal{W} . Then, we leverage \mathcal{B} to construct a polynomial adversary $\mathcal{A}_{\sf mac}$ against the unforgeability of κ -MAC Σ w.r.t. \mathcal{W} , with advantage $\mathsf{Adv}^{\sf unf}_{\mathcal{A}_{mac},\mathcal{W},\mathcal{F}}(\lambda) > \delta_0 > \epsilon_{\sf unf}$. Here \mathcal{F} is the function ensemble implementing Ext.

 $\mathcal{A}_{\mathsf{mac}}$ can be easilly constructed. Given crs of Σ and (i_{ext}, r) which are the seed and the extracted randomness respectively from w (treated as auxiliary input), $\mathcal{A}_{\mathsf{mac}}$ asks an authentication tag ς on i_{ext} , and invokes \mathcal{B} by giving $(\mathsf{crs}, (i_{\mathsf{ext}}, \varsigma), r)$. When \mathcal{B} breaks the robustness, i.e., it outputs $P^* = (i_{\mathsf{ext}}^*, \varsigma^*) \neq (i_{\mathsf{ext}}, \varsigma)$ such that $\mathsf{Verify}(\mathsf{crs}, w, i_{\mathsf{ext}}^*, \varsigma^*) = 1$, $\mathcal{A}_{\mathsf{am}}$ can output $(i_{\mathsf{ext}}^*, \varsigma^*)$ as a forgery. It is easy to see that $\mathcal{A}_{\mathsf{am}}$ is polynomial time.

4.3 Constructing one-time κ -MAC.

Now we discuss how to construct a κ -MAC. It is natural to view κ -MAC as a special leakage-resilient MAC, then upgrade it to add "key privacy". Given state of the art, the only known approach to MACs tolerating hard-to-invert leakage is using auxiliary-input secure signatures [16,29]. However, it turns out to be more involved when considering weak keys and key privacy. We have to revisit the design framework of auxiliary-input secure signatures, adapt it to the symmetric setting, and address the subsequent challenges for realizing the new framework. To illustrate the challenges and ideas towards κ -MAC we first briefly recall Katz-Vaikuntanathan's leakage-resilient signature scheme [22] which was later shown by Faust et al. [16] to be secure against hard-to-invert leakage (with minor modifications). For clarification, we follow Dodis et al.'s [11] insightful abstraction, which bases KV signature upon the following building blocks.

- A leakage-resilient hard relation R_{LR} with its sampling algorithm Gen_{LR} . R is an NP relation, and Gen_{LR} is a PPT algorithm which always outputs $(y, k) \in R_{LR}$. We say R_{LR} is leakage-reslient, if for any efficient adversary A and any admissible leakage function f, it holds that

$$\Pr[(y,k) \leftarrow \mathsf{Gen}_{\mathsf{LR}}(1^{\lambda}), k^* \leftarrow \mathcal{A}(y,f(y,k)) : (y,k^*) \in R_{\mathsf{LR}}] \leq \mathsf{negl}(\lambda).$$

– A true-simulation-extractable NIZK (tSE-NIZK) ([11], and definition recalled in the preliminary) Π for the relation $\bar{R}_{LR} := \{(y, k, m) : (y, k) \in R_{LR}\}.$

Informally, Katz-Vaikuntanathan signature proceeds as follows: To sign a message m, the signer with sk proves the knowledge of k for a statement $(y,k,m) \in \bar{R}_{LR}$ and returns the proof π as the signature σ , where $(y,k) \in R_{LR}$ is part of the verification key. Given that Π is a tSE-NIZK, a successful forgery will violate that R_{LR} is a leakage-resilient hard relation. Specifically, the zero-knowledgness guarantees the signature will not leak new information about k, and the

true-simulation-extractability ensures that an adversary who successfully generated a forgery must have k^* s.t. $(y, k^*) \in R_{LR}$. It follows that this adversary could produce k^* only given the verification key y and the leakage f(y, k), which contradicts our assumption that R_{LR} is leakage-resilient hard.

Towards κ -MAC. While we can trivially use a signature scheme as a MAC by taking both vk and sk as the authentication key, this approach will require the key to be structural. However, κ -MAC needs to work for weak keys. The central question is how to safely generate and share (vk, sk) between the sender and the receiver (verifier), while they initially only have a weak key in common that relates to the CRS.

It is safe to treat the CRS of tSE-NIZK (contained in the verification key vk) as a part of CRS in our κ -MAC construction. We then deal with $(y,k) \in R_{LR}$. A natural approach is to take the shared weak key as k and efficiently generate y according to k. However, while signatures can assume a bulletin board for posting verification keys, in κ -MAC, y has to be sent to the verifier via an unauthenticated channel (namely, being a part of the authentication tag). Consequently, adversaries might alter y to y', as the verifier will not notice this change if $(y', k) \in R_{LR}$. To prevent those attacks, we take the following steps.

- Observe that there might be a part of y (denoted by pp) that could be generated without k and reused across statements. We let pp be a part of CRS, so adversaries cannot modify it.
- We strengthen the definition of leakage-resilient hard relation against adversaries who alter the other part of y (denoted by yk). Namely, given (pp, yk) and leakage about k, adversaries cannot generate (yk', k') such that $((pp, yk'), k') \in R_{LR}$ and $((pp, yk'), k) \in R_{LR}$. We call such a relation a strengthened leakage-resilient hard relation (sLRH relation).

Next, for $key\ privacy$, yk (as a statement) should be indistinguishable with another yk (simulated without k). Note that this requirement cannot be bypassed, even when yk is uniquely determined by (pp,k) and is not contained in the authentication tag explicitly, since a NIZK proof is not supposed to hide the statement being proved. We therefore require the generator of κ -MAC to be a private generator.

We formalize all notions and intuitions in the following definition.

Definition 7. Let R_{LR} be an NP relation defined over $\{Y_{\lambda} \times \{0,1\}^{n(\lambda)}\}_{{\lambda} \in \mathbb{N}}$,

- Generator. A pair of PPT algorithms (PGen, SGen) is a generator of R_{LR} , if for every $\lambda \in \mathbb{N}$ and $k \in \{0,1\}^{n(\lambda)}$, it follows that

$$\Pr[\mathbf{\textit{pp}} \leftarrow \mathsf{PGen}(1^{\lambda}), yk \leftarrow \mathsf{SGen}(\mathbf{\textit{pp}}, k) : ((\mathbf{\textit{pp}}, yk), k) \in R_{\mathsf{LR}}] = 1.$$

- sLRH relation. R_{LR} along with (PGen, SGen) is an $(n, \epsilon_{lr}, \epsilon_{hv})$ -sLRH relation, if for any efficiently-samplable source W (over $\{\{0,1\}^{n(\lambda)}\}_{\lambda\in\mathbb{N}}$ and dependent of PGen) and any ϵ_{hv} - $AI\mathcal{F}$ w.r.t. W and PGen, for any P.P.T adversary \mathcal{A} , it holds that $Adv_{\mathcal{A},\mathcal{W},\mathcal{F}}^{slrh}(\lambda) = Pr[Exp_{\mathcal{A},\mathcal{W},\mathcal{F}}^{lr}(\lambda) = 1] \leq \epsilon_{lr}(\lambda)$. $Exp_{\mathcal{A},\mathcal{W},\mathcal{F}}^{lr}$ is defined below.

- **Private generator.** (PGen, SGen) satisfies $(n, \epsilon_{\mathsf{pr}}, \epsilon_{\mathsf{hv}})$ -privacy, if for $(\mathcal{A}, \mathcal{W}, \mathcal{F})$ above, $\mathsf{Adv}^{\mathsf{pr}}_{\mathcal{A}, \mathcal{W}, \mathcal{F}}(\lambda) = |\Pr[\mathsf{Exp}^{\mathsf{pr}, 0}_{\mathcal{A}, \mathcal{W}, \mathcal{F}}(\lambda) = 1] - \Pr[\mathsf{Exp}^{\mathsf{pr}, 1}_{\mathcal{A}, \mathcal{W}, \mathcal{F}}(\lambda) = 1]| \leq \epsilon_{\mathsf{pr}}(\lambda)$. The experiments are defined below.

$\boxed{Exp^{pr,0}_{\mathcal{A},\mathcal{W},\mathcal{F}}(\lambda)}$	$Exp^{pr,1}_{\mathcal{A},\mathcal{W},\mathcal{F}}(\lambda)$
$pp \leftarrow PGen(1^{\lambda})$	$pp \leftarrow PGen(1^{\lambda})$
$k \leftarrow W_{\lambda pp}, k' \leftarrow \$ \{0,1\}^{n(\lambda)}$	$k \leftarrow W_{\lambda} _{pp}$
$yk \leftarrow SGen(pp, k')$	$yk \leftarrow SGen(\textit{pp},k)$
$b' \leftarrow \mathcal{A}(pp, yk, f_{\lambda}(pp, k))$	$b' \leftarrow \mathcal{A}(pp, yk, f_{\lambda}(pp, k))$
$ \mathbf{return} \ b' $	$\mathbf{return}\ b'$

Remark 2. The auxiliary-input function f does not take as input yk, because yk is generated by the authentication algorithm, and the auxiliary input is supposed to be leaked before authenticating. The source W and the leakage are dependent on pp since it is a part of the CRS. Other parts of CRS are not considered explicitly since the generator SGen does not use them.

The final κ -MAC construction. Using an sLRH relation R_{LR} along with its private generator (PGen, SGen) and a one-time tSE-NIZK $\Pi = \{S_{zk}, P_{zk}, V_{zk}\}$ for the relation $\bar{R}_{LR} := \{(pp, yk, k, m) : ((pp, yk), k) \in R_{LR}\}$, we construct an one-time κ -MAC scheme in Fig.2.

$Init(1^\lambda)$	Tag(crs,k,m)	$Verify(crs, k, m, \varsigma)$
$\boxed{(\mathtt{crs}_{\mathtt{zk}},\mathtt{tk},\mathtt{ek}) \leftarrow S_{\mathtt{zk}}(1^{\lambda})}$	$yk \leftarrow SGen(pp,k)$	return 1 iff
$\mathtt{pp} \leftarrow PGen(1^{\lambda})$	$\pi \leftarrow P_{zk}(\mathtt{crs}_{zk},$	$(\mathtt{pp},yk,k)\in R_{LR}$
return	$(\mathtt{pp},yk,m),k)$	$V_{zk}(\mathtt{crs}_{zk}, (\mathtt{pp},$
$\mathtt{crs} = (\mathtt{crs}_{zk}, \mathtt{pp}), au = \mathtt{tk}$	return $\varsigma = (yk, \pi)$	$yk, m), \pi) = 1$

Fig. 2. One-time κ -MAC from tSE-NIZK + sLRH relation

Analysis. Correctness is easy to see. Regarding security: from the privacy of the generator SGen and the zero-knowledgeness of Π , efficient adversaries cannot learn new information about k from the tag (y, π) , and the key privacy follows. The tSE-NIZK ensures an adversary who successfully forges an authentication tag can also output a pair $(y', k') \in R_{LR}$ s.t. $(y', k) \in R_{LR}$, which contradicts the sLRH relation, and thus the unforgeability follows.

Theorem 3. Let (PGen, SGen) be an $(n, \epsilon_{pr}, \epsilon_{hv})$ -private generator for an NP relation R_{LR} , and R_{LR} along with (PGen, SGen) be an $(n, \epsilon_{lr}, \epsilon_{hv})$ -sLRH relation. Let $\Pi = \{S_{zk}, P_{zk}, V_{zk}\}$ be a NIZK for the relation \bar{R}_{LR} satisfying ϵ_{zk} -ZK and ϵ_{tse} -tSE. Then, the construction in Fig.2 satisfies $(n, \epsilon_{kpriv}, \epsilon_{hv})$ one-time key privacy and $(n, \epsilon_{unf}, \epsilon_{hv})$ one-time unforgeability, for any $\epsilon_{kpriv} \geq \epsilon_{pr} + \epsilon_{zk}$, and any $\epsilon_{unf} \geq \epsilon_{zk} + \epsilon_{tse} + \epsilon_{lr}$.

We prove the one-time key-privacy and the one-time unforgeability in Lemma 5 and Lemma 6, respectively.

⁴ The one-time κ -MAC is enough for our purpose; we may generalize our construction to get a full-fledged κ -MAC using multi-message secure DPKE [7], which will require concrete entropy bound on the source though.

Lemma 5. The κ -MAC Σ satisfies $(n, \epsilon_{\mathsf{kpriv}}, \epsilon_{\mathsf{hv}})$ one-time key privacy, for any $\epsilon_{\mathsf{kpriv}} > \epsilon_{\mathsf{pr}} + \epsilon_{\mathsf{zk}}$.

Proof. We first present the simulator SimTag below.

- SimTag(crs, τ , m). Sample $k' \leftarrow \$ \{0, 1\}^{n(\lambda)}$, invoke $yk \leftarrow \mathsf{SGen}(\mathsf{pp}, k')$, run $\pi \leftarrow \mathsf{SP}_{\mathsf{zk}}(\mathsf{crs}_{\mathsf{zk}}, \mathsf{tk}_{\mathsf{zk}}, (\mathsf{pp}, yk))$, and return $\varsigma = (\pi, yk)$.

Suppose, for contradiction, that there exists a polynomial-time adversary \mathcal{B} , an efficiently-samplable source \mathcal{W} and an ϵ_{hv} -AI \mathcal{F} , such that $\mathsf{Adv}^{\mathsf{kpriv}}_{\mathcal{B},\mathcal{W},\mathcal{F}}(\lambda) > \epsilon_{\mathsf{pr}} + \epsilon_{\mathsf{zk}}$. We show there exist either

- a polynomial-time adversary \mathcal{A}_{pr} , an efficiently-samplable source \mathcal{W}' and an ϵ_{hv} -AI \mathcal{F}' w.r.t. \mathcal{W}' and PGen, against the privacy of (PGen, SGen) with the advantage $\mathsf{Adv}^{pr}_{\mathcal{A}_{pr},\mathcal{W}',\mathcal{F}'}(\lambda) > \epsilon_{pr}$; Or,
- a polynomial-time adversary $\mathcal{A}_{\mathsf{zk}}$ against ZK with the advantage $\mathsf{Adv}^{\mathsf{zk}}_{\mathcal{A}_{\mathsf{zk}}}(\lambda) > \epsilon_{\mathsf{zk}}$.

To facilitate the analysis, we define the following hybrid experiment.

$$\begin{split} & \frac{\mathsf{Exp}_{\mathcal{B},\mathcal{W},\mathcal{F}}^{\mathsf{kpriv},1/2}(\lambda)}{(\mathsf{crs},\tau) \leftarrow \mathsf{Init}(1^{\lambda}); k \leftarrow W_{\lambda}|_{\mathsf{crs}}} \\ & (m,st) \leftarrow \mathcal{B}(\mathsf{crs},f_{\lambda}(\mathsf{crs},k)) \\ & yk \leftarrow \mathsf{SGen}(\mathsf{pp},k), \pi_{\mathsf{zk}} \leftarrow \mathsf{SP}_{\mathsf{zk}}(\mathsf{crs}_{\mathsf{zk}},\mathsf{tk}_{\mathsf{zk}},(\mathsf{pp},yk,m)) \\ & b' \leftarrow \mathcal{B}((yk,\pi_{\mathsf{zk}}),st) \\ & \mathbf{return} \ b' \end{split}$$

It is worth noting that, for any $(\mathcal{B}, \mathcal{W}, \mathcal{F})$,

$$\begin{aligned} \mathsf{Adv}^{\mathrm{kpriv}}_{\mathcal{B},\mathcal{W},\mathcal{F}}(\lambda) &\leq |\Pr[\mathsf{Exp}^{\mathsf{kpriv},0}_{\mathcal{B},\mathcal{W},\mathcal{F}}(\lambda) = 1] - \Pr[\mathsf{Exp}^{\mathsf{kpriv},1/2}_{\mathcal{B},\mathcal{W},\mathcal{F}}(\lambda) = 1]| + \\ &|\Pr[\mathsf{Exp}^{\mathsf{kpriv},1/2}_{\mathcal{B},\mathcal{W},\mathcal{F}}(\lambda) = 1] - \Pr[\mathsf{Exp}^{\mathsf{kpriv},1}_{\mathcal{B},\mathcal{W},\mathcal{F}}(\lambda) = 1]|. \end{aligned} \tag{16}$$

We construct $(\mathcal{A}_{pr}, \mathcal{W}', \mathcal{F}')$ below ⁵.

At the point of \mathcal{B} 's view, when $k' \leftarrow \$\{0,1\}^{n(\lambda)}$ and $yk \leftarrow \mathsf{SGen}(\mathsf{pp},k')$, the environment provided by $\mathcal{A}_{\mathsf{pr}}$ (together with \mathcal{W}' and \mathcal{F}') is identical to that of $\mathsf{Exp}_{\mathcal{B},\mathcal{W},\mathcal{F}}^{\mathsf{krpiv},0}$; when $k \leftarrow W'_{\lambda}|_{\mathsf{pp}}$ and $yk \leftarrow \mathsf{SGen}(\mathsf{pp},k)$, the environment provided by $\mathcal{A}_{\mathsf{pr}}$ (together with \mathcal{W}' and \mathcal{F}') is identical to that of $\mathsf{Exp}_{\mathcal{B},\mathcal{W},\mathcal{F}}^{\mathsf{krpiv},1/2}$. Thus,

$$\mathsf{Adv}^{\mathrm{pr}}_{\mathcal{A}_{\mathsf{pr}}, \mathcal{W}', \mathcal{F}'}(\lambda) = |\Pr[\mathsf{Exp}^{\mathsf{kpriv}, 0}_{\mathcal{B}, \mathcal{W}, \mathcal{F}}(\lambda) = 1] - \Pr[\mathsf{Exp}^{\mathsf{kpriv}, 1/2}_{\mathcal{B}, \mathcal{W}, \mathcal{F}}(\lambda) = 1]|. \tag{17}$$

⁵ As every W_{λ} can be sampled using a polynomial-size circuit G on input $(\mathtt{crs}_{\mathsf{zk}}, \mathtt{pp})$, $W_{\lambda}|_{\mathtt{crs}_{\mathsf{zk}}}$ can be sampled using G hard-coding $\mathtt{crs}_{\mathsf{zk}}$, namely, $G(\mathtt{crs}_{\mathsf{zk}}, \cdot)$

Next, we describle the adversary $\mathcal{A}_{\mathsf{zk}}$ against ZK below, where \mathcal{O}_{β} returns the real proof if $\beta = 1$ or the simulated proof if $\beta = 0$;

$$\begin{split} & \underset{\mathsf{pp} \leftarrow \mathsf{PGen}(1^{\lambda}), \, k \leftarrow W_{\lambda}|_{\mathsf{crs}_{\mathsf{zk}}, \mathsf{pp}}, \, (m, st) \leftarrow \mathcal{B}((\mathsf{crs}_{\mathsf{zk}}, \mathsf{pp}), f_{\lambda}(\mathsf{crs}, \mathsf{pp}, k))}{yk \leftarrow \mathsf{SGen}(\mathsf{pp}, k), \, \pi_{\mathsf{zk}} \leftarrow \mathcal{O}_{\beta}(\mathsf{pp}, yk, k), b' \leftarrow \mathcal{B}((yk, \pi_{\mathsf{zk}}), st)} \\ & \mathsf{return} \ b' \end{split}$$

At the point of \mathcal{B} 's view, when $\beta=1$, the environment provided by \mathcal{A}_{zk} is identical to that of $\mathsf{Exp}^{\mathsf{kpriv},1}_{\mathcal{B},\mathcal{W},\mathcal{F}}$; when $\beta=0$, the environment provided by \mathcal{A}_{zk} is identical to that of $\mathsf{Exp}^{\mathsf{kpriv},1/2}_{\mathcal{B},\mathcal{W},\mathcal{F}}$. Therefore,

$$\mathsf{Adv}^{\mathsf{zk}}_{\mathcal{A}_{\mathsf{zk}}}(\lambda) = |\Pr[\mathsf{Exp}^{\mathsf{kpriv},1/2}_{\mathcal{B},\mathcal{W},\mathcal{F}}(\lambda) = 1] - \Pr[\mathsf{Exp}^{\mathsf{kpriv},1}_{\mathcal{B},\mathcal{W},\mathcal{F}}(\lambda) = 1]|. \tag{18}$$

Combining Eq.16, 17, 18, we have

$$\mathsf{Adv}^{\mathrm{kpriv}}_{\mathcal{B},\mathcal{W},\mathcal{F}}(\lambda) \leq \mathsf{Adv}^{\mathrm{pr}}_{\mathcal{A}_{\mathrm{pr}},\mathcal{W}',\mathcal{F}'}(\lambda) + \mathsf{Adv}^{\mathrm{zk}}_{\mathcal{A}_{\mathrm{zk}}}(\lambda).$$

$$\text{If } \epsilon_{\mathsf{pr}} + \epsilon_{\mathsf{zk}} < \mathsf{Adv}^{\mathrm{kpriv}}_{\mathcal{A},\mathcal{W},\mathsf{F}}(\lambda), \text{ it follows either } \mathsf{Adv}^{\mathrm{pr}}_{\mathcal{A}_{\mathsf{pr}},\mathcal{W}',\mathcal{F}'}(\lambda) > \epsilon_{\mathsf{pr}} \text{ or } \mathsf{Adv}^{\mathrm{zk}}_{\mathcal{A}_{\mathsf{zk}}}(\lambda) > \epsilon_{\mathsf{zk}}. \\ \square$$

Lemma 6. The κ -MAC satisfies $(n, \epsilon_{\mathsf{unf}}, \epsilon_{\mathsf{hv}})$ one-time unforgeability, for any $\epsilon_{\mathsf{unf}} > \epsilon_{\mathsf{zk}} + \epsilon_{\mathsf{tse}} + \epsilon_{\mathsf{lr}}$.

Proof. We establish the following hybrid experiments.

 $\mathsf{Exp}^{\mathsf{unf},1}_{\mathcal{A},\mathcal{W},\mathcal{F}}$. It is almost identical to $\mathsf{Exp}^{\mathsf{unf}}_{\mathcal{A},\mathcal{W},\mathcal{F}}$ (in Def.5), except that Tag is replaced with Tag.

- Tag. Compared with Tag, it generates π_{zk} by using the simulator prover algorithm SP_{zk} instead of the real prover P_{zk} .

For any $(\mathcal{A}, \mathcal{W}, \mathcal{F})$, we denote

$$\epsilon_0 = |\Pr[\mathsf{Exp}^{\mathsf{unf}}_{\mathcal{A},\mathcal{W},\mathcal{F}}(\lambda) = 1] - \Pr[\mathsf{Exp}^{\mathsf{unf},1}_{\mathcal{A},\mathcal{W},\mathcal{F}}(\lambda) = 1]|$$

It is easy to see there exists a polynomial-time adversary \mathcal{A}_{zk} breaking the ZK property of Π_{zk} with advantage ϵ_0 . Thus, $\epsilon_0 \leq \epsilon_{zk}$.

 $\mathsf{Exp}^{\mathsf{unf},2}_{\mathcal{A},\mathcal{W},\mathcal{F}}$. It is almost identical to $\mathsf{Exp}^{\mathsf{unf},1}_{\mathcal{A},\mathcal{W},\mathcal{F}}$, except the Verify is replaced with $\widehat{\mathsf{Verify}}$.

- Verify. Compared with Verify, it adds an additional checking step. For an authentication tag (yk, π_{zk}) for m under crs , it runs the knowledge extractor KExt to obtain k^* from π_{zk} . If $(\mathsf{pp}, yk, k^*) \notin R_{\mathsf{LR}}$, it returns \bot .

For any $(\mathcal{A}, \mathcal{W}, \mathcal{F})$, we denote

$$\epsilon_1 = |\Pr[\mathsf{Exp}^{\mathsf{unf},1}_{\mathcal{A},\mathcal{W},\mathcal{F}}(\lambda) = 1] - \Pr[\mathsf{Exp}^{\mathsf{unf},2}_{\mathcal{A},\mathcal{W},\mathcal{F}}(\lambda) = 1]|$$

At the point of \mathcal{A} 's view, $\mathsf{Exp}^{\mathsf{unf},1}_{\mathcal{A},\mathcal{W},\mathcal{F}}$ and $\mathsf{Exp}^{\mathsf{unf},2}_{\mathcal{A},\mathcal{W},\mathcal{F}}$ will be identical, unless that \mathcal{A} makes $\widehat{\mathsf{Verify}}$ abort, breaking the one-time tSE of Π_{zk} . Thus, $\epsilon_1 \leq \epsilon_{\mathsf{tse}}$.

Finally, denoting $\Pr[\mathsf{Exp}^{\mathsf{unf},2}_{\mathcal{A},\mathcal{W},\mathcal{F}}(\lambda)=1]$ by ϵ_2 , we show $\epsilon_2 \leq \epsilon_{\mathsf{lr}}$ for any admissible $(\mathcal{A},\mathcal{W},\mathcal{F})$. Indeed, for any admissible $(\mathcal{A},\mathcal{W},\mathcal{F})$, there exist an admissible tuple of $(\mathcal{A}_{\mathsf{lr}},\mathcal{W}',\mathcal{F}')$ such that $\mathsf{Adv}^{\mathsf{slrh}}_{\mathcal{A}_{\mathsf{lr}},\mathcal{W}',\mathcal{F}'}(\lambda)=\epsilon_2$. We describe $(\mathcal{A}_{\mathsf{lr}},\mathcal{W}',\mathcal{F}')$ below.

Global Setup:	Algorithm $\mathcal{A}_{lr}(pp,yk,f'_{\lambda}(pp,k))$
$(\mathtt{crs}_{\mathtt{zk}},\mathtt{tk},\mathtt{zk}) \leftarrow S_{\mathtt{zk}}(1^{\lambda})$	$(m,st) \leftarrow \mathcal{B}(\mathtt{crs}_{\mathtt{zk}},\mathtt{pp})$
	$\pi_{zk} \leftarrow SP_{zk}(\mathtt{crs}_{zk}, \mathtt{tk}, (\mathtt{pp}, yk, m))$
$\mathcal{F}' = \{f'_{\lambda}\} \text{ and } \mathcal{W}' = \{W'_{\lambda}\}$	$(m^*,(yk^*,\pi_{zk}^*)) \leftarrow \mathcal{B}((yk,\pi_{zk}),st)$
$f'_{\lambda}(\mathtt{pp},k) = f_{\lambda}(\mathtt{crs}_{zk},\mathtt{pp},k)$	$k^* \leftarrow KExt_{zk}(crs_{zk}, ek, (pp, yk^*, m^*), \pi_{zk}^*)$
$W_\lambda' = W_\lambda _{\mathtt{crs}_{\mathtt{zk}}}$	$\mathbf{return}\ (yk^*,k^*)$

Combining all above results, for any polynomial-time \mathcal{B} , any efficiently-samplable \mathcal{W} and \mathcal{F} satisfying \mathcal{F} is ϵ_{hv} w.r.t. \mathcal{W} , it holds that

$$\mathsf{Adv}^{\mathrm{unf}}_{\mathcal{B},\mathcal{W},\mathcal{F}}(\lambda) \leq \epsilon_{\mathsf{zk}} + \epsilon_{\mathsf{tse}} + \epsilon_{\mathsf{lr}}.$$

As shown by Dodis *et al.* [11], a tSE-NIZK could be constructed using CPA-secure PKE and standard NIZK, or CCA-secure PKE and simulation-sound NIZK. Both approaches can be based on standard assumptions. However, while a leakage-resilient hard relation can be instantiated with a second-preimage-resistant hash function H, the statement y = H(k) will leak some information about k. For key privacy, we need new constructions for strengthened LRH relations.

sLRH relation from deterministic public-key encryption. Note that the privacy of the generator is not an orthogonal property of sLRH relation; it prevents adversaries from finding the exact k from (pp, yk) and the leakage. If it is further ensured that adversaries cannot find a distinct k' along with yk' such that both (pp, yk', k) and (pp, yk', k') belong to R_{LR} , R_{LR} with a private generator will be a sLRH relation. We therefore abstract a useful property of R_{LR} called "collision resistance" below.

Definition 8. R_{LR} is $(n, \epsilon_{\mathsf{cr}})$ -collision-resistant w.r.t. PGen, if for any polynomial-time \mathcal{A} , it holds that $\mathsf{Adv}^{\mathsf{cr}}_{\mathcal{A}}(\lambda) \leq \epsilon_{\mathsf{cr}}(\lambda)$, where $\mathsf{Adv}^{\mathsf{cr}}_{\mathcal{A}}(\lambda)$ is defined as

$$\Pr[\mathbf{\textit{pp}} \leftarrow \mathsf{PGen}(1^{\lambda}), (yk, k, k') \leftarrow \mathcal{A}(\mathbf{\textit{pp}}) : k \neq k' \land (\mathbf{\textit{pp}}, yk, k) \in R_{\mathsf{LR}} \land (\mathbf{\textit{pp}}, yk, k') \in R_{\mathsf{LR}}].$$

A collision-resistant relation with a private generator will be a sLRH relation.

Lemma 7. Let (PGen, SGen) be an $(n, \epsilon_{pr}, \epsilon_{hv})$ -private generator for R_{LR} . If R_{LR} satisfies (n, ϵ_{cr}) -collision-resistance w.r.t. PGen, R_{LR} with (PGen, SGen) is an $(n, \epsilon_{lr}, \frac{1}{2}\epsilon_{hv})$ -sLRH relation, for any $\epsilon_{lr} \geq 2\epsilon_{pr} + \epsilon_{cr} + \frac{1}{2}\epsilon_{hv}$.

Proof. Suppose, for contradiction, that there exists a polynomial-time adversary \mathcal{B} , an efficiently-samplable source \mathcal{W} and a $\frac{1}{2}\epsilon_{\mathsf{hv}}$ -AI \mathcal{F} , such that $\mathsf{Adv}^{\mathsf{lr}}_{\mathcal{B},\mathcal{W},\mathcal{F}}(\lambda) > 2\epsilon_{\mathsf{pr}} + \epsilon_{\mathsf{cr}} + \frac{1}{2}\epsilon_{\mathsf{hv}}$. We show there exist either

- a polynomial-time adversary \mathcal{A}_{pr} and a ϵ_{hv} -AI \mathcal{F}' against the privacy of (PGen, SGen) with the advantage $\mathsf{Adv}^{pr}_{\mathcal{A}_{pr},\mathcal{W},\mathcal{F}'}(\lambda) > \epsilon_{pr};$ Or,
- a polynomial-time adversary \mathcal{A}_{cr} against the collision-resistance of R_{LR} with the advantage $\mathsf{Adv}^{cr}_{\mathcal{A}_{cr}}(\lambda) > \epsilon_{cr}$.

To proceed with this proof, we now describe $(\mathcal{A}_{pr}, \mathcal{F}')$ and \mathcal{A}_{cr} . $\mathcal{F}' = \{f'_{\lambda}\}$ is defined as

$$f'_{\lambda}(pp, k) = (r, \langle r, k \rangle, f_{\lambda}(pp, k)),$$

where $r \leftarrow \$ \{0,1\}^{n(\lambda)}$. As any adversary having $f_{\lambda}(pp,k)$ can simulate $f'_{\lambda}(pp,k)$ with at least probability of $\frac{1}{2}$, it follows \mathcal{F}' is at least ϵ_{hv} -hard-to-invert w.r.t. \mathcal{W} . The codes of $\mathcal{A}_{\mathsf{pr}}$ and $\mathcal{A}_{\mathsf{cr}}$ are presented below.

Algorithm $\mathcal{A}_{pr}(pp, yk, f'_{\lambda}(pp, k))$	Algorithm $\mathcal{A}_{cr}(\mathtt{pp})$
Parse $f'_{\lambda}(pp, k) = (r, \beta, f_{\lambda}(pp, k))$	$k \leftarrow W_{\lambda} _{pp}, yk \leftarrow SGen(pp, k)$
$(yk',k') \leftarrow \mathcal{B}(pp,yk,f_{\lambda}(pp,k))$	$(yk', k') \leftarrow \mathcal{B}(\mathtt{pp}, yk, f_{\lambda}(\mathtt{pp}, k))$
if $\langle r, k' \rangle = \beta$ then return 1	$\mathbf{return} \ \ (yk',k,k')$
return 0	

First, we analyze the advantage of \mathcal{A}_{pr} . For notational convenience, we define the following events. (1) $\text{Ev}_{k=k'}$: \mathcal{B} outputs k'=k; (2) $\text{Ev}_{k\neq k'}$: \mathcal{B} outputs k' s.t. $k'\neq k$; (3) $\text{Ev}_{k\neq k'}^0$: $\text{Ev}_{k\neq k'}^0\cap\langle r,k'\rangle\neq\beta$; (4) $\text{Ev}_{k\neq k'}^1$: $\text{Ev}_{k\neq k'}\cap\langle r,k'\rangle=\beta$; (5) $\text{Ev}_{\mathcal{A}_{pr}}^1$: \mathcal{A}_{pr} returns 1.

By the description of \mathcal{A}_{pr} , observe that in $\operatorname{Ev}_{k=k'}$ and $\operatorname{Ev}_{k\neq k'}^1$, \mathcal{A}_{pr} always outputs 1, and that in $\operatorname{Ev}_{k'\neq k}^0$, \mathcal{A}_{pr} always outputs 0. Moreover, as r is independent of the view of \mathcal{B} ,

$$\Pr[\mathtt{Ev}_{k\neq k'}^0] = \Pr[\mathtt{Ev}_{k\neq k'}^1] = \frac{1}{2}\Pr[\mathtt{Ev}_{k\neq k'}].$$

Therefore, regardless the distribution of \mathcal{A}_{pr} 's input, the following equation holds.

$$\Pr[\mathsf{Ev}_{\mathcal{A}_{\mathsf{pr}}}^{1}] = \Pr[\mathsf{Ev}_{\mathcal{A}_{\mathsf{pr}}}^{1} | \mathsf{Ev}_{k=k'}] \Pr[\mathsf{Ev}_{k=k'}] + \Pr[\mathsf{Ev}_{\mathcal{A}_{\mathsf{pr}}}^{1} | \mathsf{Ev}_{k\neq k'}] \Pr[\mathsf{Ev}_{k\neq k'}] \\
= \Pr[\mathsf{Ev}_{k=k'}] + \Pr[\mathsf{Ev}_{\mathcal{A}_{\mathsf{pr}}}^{1} | \mathsf{Ev}_{k\neq k'}] \Pr[\mathsf{Ev}_{k\neq k'}^{1}] \\
= \Pr[\mathsf{Ev}_{k=k'}] + \frac{1}{2} \Pr[\mathsf{Ev}_{k\neq k'}] = \frac{1}{2} + \frac{\Pr[\mathsf{Ev}_{k=k'}]}{2}.$$
(19)

Recall Definition 7, in $\mathsf{Exp}_{\mathcal{A}_{\mathsf{pr}},\mathcal{W},\mathcal{F}'}^{\mathsf{pr},0}$ and $\mathsf{Exp}_{\mathcal{A}_{\mathsf{pr}},\mathcal{W},\mathcal{F}'}^{\mathsf{pr},1}$, the input of $\mathcal{A}_{\mathsf{pr}}$ are two different distributions which we here denote by \mathcal{D}_0 and \mathcal{D}_1 , respectively. Now, we can reformulate the advantage of $\mathcal{A}_{\mathsf{pr}}$ as

$$\mathsf{Adv}^{\mathrm{pr}}_{\mathcal{A}_{\mathsf{pr}},\mathcal{W},\mathcal{F}'}(\lambda) = |\Pr[\mathsf{Ev}^{1,\mathcal{D}_0}_{\mathcal{A}_{\mathsf{pr}}}] - \Pr[\mathsf{Ev}^{1,\mathcal{D}_1}_{\mathcal{A}_{\mathsf{pr}}}]| = \frac{1}{2} |\Pr[\mathsf{Ev}^{\mathcal{D}_0}_{k=k'}] - \Pr[\mathsf{Ev}^{\mathcal{D}_1}_{k=k'}]|, \tag{20}$$

where $\text{Ev}^{\mathcal{D}_b}$ denotes the event Ev conditioned on that \mathcal{A}_{pr} 's input distribution is \mathcal{D}_b , for $b \in \{0, 1\}$. When \mathcal{A}_{pr} 's input distribution is \mathcal{D}_1 , at the point of \mathcal{B} 's view, the environment provided by \mathcal{A}_{pr} is identical to that of $\text{Exp}_{\mathcal{B},\mathcal{W},\mathcal{F}}^{\text{lr}}$. In this case, $\text{Ev}_{k=k'}^{\mathcal{D}_1}$ implies \mathcal{B} breaks the sLRH relation. Thus,

$$\Pr[\mathtt{Ev}_{k=k'}^{\mathcal{D}_1}] = \Pr[\mathtt{Exp}_{\mathcal{B},\mathcal{W},\mathcal{F}}^{\mathsf{lr}}(\lambda) = 1 \cap \mathtt{Ev}_{k=k'}^{\mathcal{D}_1}] = \Pr[\mathtt{Ev}_{k=k'}^{\mathcal{D}_1} | \mathtt{Exp}_{\mathcal{B},\mathcal{W},\mathcal{F}}^{\mathsf{lr}}(\lambda) = 1] \mathsf{Adv}_{\mathcal{B},\mathcal{W},\mathcal{F}}^{\mathsf{lr}}(\lambda). \tag{21}$$

When \mathcal{A}_{pr} 's input distribution is \mathcal{D}_0 , as yk provided to \mathcal{B} is independent of k, $\mathsf{Ev}_{k=k'}^{\mathcal{D}_0}$ means that \mathcal{B} find the exact pre-image k from pp and $f_{\lambda}(\mathsf{pp},k)$. It follows that

$$\Pr[\mathsf{Ev}_{k=k'}^{\mathcal{D}_0}] \le \frac{\epsilon_{\mathsf{hv}}(\lambda)}{2}.\tag{22}$$

Combining Eq.20, 21 and 22, we have

$$\mathsf{Adv}^{\mathrm{pr}}_{\mathcal{A}_{\mathsf{pr}},\mathcal{W},\mathcal{F}'}(\lambda) \ge \frac{\Pr[\mathsf{Ev}^{\mathcal{D}_1}_{k=k'} | \mathsf{Exp}^{\mathsf{lr}}_{\mathcal{B},\mathcal{W},\mathcal{F}}(\lambda) = 1] \mathsf{Adv}^{\mathsf{lr}}_{\mathcal{B},\mathcal{W},\mathcal{F}}(\lambda)}{2} - \frac{\epsilon_{\mathsf{hv}}(\lambda)}{4}. \tag{23}$$

Next, we analyze the advantage of \mathcal{A}_{cr} . At the point of \mathcal{B} 's view, the environment provided by \mathcal{A}_{cr} is identical to that of $\mathsf{Exp}^{\mathsf{lr}}_{\mathcal{B},\mathcal{W},\mathcal{F}}$. Moreover, as analyzed before, the environment provided by $\mathcal{A}_{\mathsf{pr}}$ with input from \mathcal{D}_1 is also identical to that of $\mathsf{Exp}^{\mathsf{lr}}_{\mathcal{B},\mathcal{W},\mathcal{F}}$; thus, we can use the notation $\mathsf{Ev}^{\mathcal{D}_1}_{\mathcal{K}\neq k'}$ to denote the event that, in the environment provided by $\mathcal{A}_{\mathsf{cr}}$, \mathcal{B} outputs $k'\neq k$. Notice that $\mathcal{A}_{\mathsf{cr}}$ wins iff \mathcal{B} wins and $k'\neq k$, we have

$$\mathsf{Adv}^{\mathrm{cr}}_{\mathcal{A}_{\mathsf{cr}}}(\lambda) = \Pr[\mathsf{Exp}^{\mathsf{lr}}_{\mathcal{B},\mathcal{W},\mathcal{F}}(\lambda) = 1 \cap \mathsf{Ev}^{\mathcal{D}_1}_{k \neq k'}] = \Pr[\mathsf{Ev}^{\mathcal{D}_1}_{k \neq k'} | \mathsf{Exp}^{\mathsf{lr}}_{\mathcal{B},\mathcal{W},\mathcal{F}}(\lambda) = 1] \mathsf{Adv}^{\mathsf{lr}}_{\mathcal{B},\mathcal{W},\mathcal{F}}(\lambda). \tag{24}$$

Combining Eq.23 and 24, it follows that

$$\mathsf{Adv}^{\mathrm{cr}}_{\mathcal{A}_{\mathsf{cr}}}(\lambda) + 2\mathsf{Adv}^{\mathrm{pr}}_{\mathcal{A}_{\mathsf{pr}},\mathcal{W},\mathcal{F}'}(\lambda) \ge \mathsf{Adv}^{\mathrm{lr}}_{\mathcal{B},\mathcal{W},\mathcal{F}}(\lambda) - \frac{\epsilon_{\mathsf{hv}}(\lambda)}{2} > \epsilon_{\mathsf{cr}} + 2\epsilon_{\mathsf{pr}}. \tag{25}$$

Thus, it follows either $\mathsf{Adv}^{\mathrm{cr}}_{\mathcal{A}_{\mathsf{cr}}}(\lambda) > \epsilon_{\mathsf{cr}}$ or $\mathsf{Adv}^{\mathrm{pr}}_{\mathcal{A}_{\mathsf{pr}},\mathcal{W},\mathcal{F}'}(\lambda) > \epsilon_{\mathsf{pr}}$. We obtain the contradiction and complete the proof.

We now construct a collision-resistant relation with a private generator. An auxiliary-input secure deterministic public-key encryption (DPKE) scheme is a natural tool for realizing an NP relation with a private generator. Since no randomness is used, it is easy to check whether a ciphertext c_{de} encrypts a message m_{de} under a public key pk_{de} . We can define an NP relation

$$R_{de} = \{ (pk_{de}, c_{de}, m_{de}) : c_{de} = E_{de}(pk_{de}, m_{de}) \}$$
(26)

From the auxiliary-input security of DPKE, the key generation algorithm and the encryption algorithm will give a private generator for R_{de} .

The relation R_{de} is almost collision-resistant. Under a valid public key pk_{de} (namely, there is a secret key sk_{de} to decrypt all ciphertexts under pk_{de}), the (perfect) correctness of DPKE ensures that for any ciphertext c_{de} there is at most one message m_{de} such that $c_{de} = E_{de}(pk_{de}, m_{de})$. While it seems straightforward to ensure the validity of pk_{de} by putting it into the CRS, however, it violates security. The problem inherits from that DPKE only applies to message distributions independent of public key, but our goal is to have a construction for CRS-dependent sources.

We enforce the validity of public key as follows: note that all valid pairs of (pk_{de}, sk_{de}) define an NP relation R_{pk} , and pk_{de} can be guaranteed valid (with overwhelming probability) using a NIZK proof demonstrating the knowledge of sk_{de} s.t. $(pk_{de}, sk_{de}) \in R_{pk}$ (the key relation). Now, pk_{de} (with its validity proof) can be outputted by SGen, and PGen is only used to establish a CRS of NIZK. Though CRS is still in need, adaptively secure NIZK does allow CRS-dependent sources. The relation R_{de} needs to be extended for verifying the proof. Formally, let $\Sigma_{de} = \{K_{de}, E_{de}, D_{de}\}$ be an auxiliary-input secure DPKE scheme with message space $\{\{0,1\}^{n(\lambda)}\}_{\lambda \in \mathbb{N}}$ and the key relation R_{pk} , and $\Pi_{pk} = \{S_{pk}, P_{pk}, V_{pk}\}$ be a NIZK for R_{pk} . We define an NP relation R_{LR}^{de} and construct its generator (PGen_{de}, SGen_{de}) below.

Summarizing the above, we have the following result.

$PGen_{de}(1^\lambda)$	$SGen_{de}(pp, k = m_{de})$	Relation R_{LR}^{de}
$\boxed{(\mathtt{crs}_{pk},\mathtt{tk}_{pk}) \leftarrow S_{pk}(1^{\lambda})}$	$(pk_{de}, sk_{de}) \leftarrow K_{de}(1^{\lambda})$	$(pp, yk, k) \in R_{LR}^{de}$ iff
$egin{aligned} \mathbf{return} \ \mathtt{pp} = \mathtt{crs}_{\mathtt{pk}} \end{aligned}$	$\pi_{de} \leftarrow P_{pk}(crs_{pk}, pk_{de}, sk_{de})$	$c_{de} = E_{de}(pk_{de}, m_{de})$
	$c_{de} \leftarrow E_{de}(pk_{de}, m_{de})$	$\wedge V_{pk}(\mathtt{crs}_{pk}, pk_{de}, \pi_{pk}) = 1$
	$\mathbf{return}\ yk = (c_{de}, pk_{de}, \pi_{de})$	

Fig. 3. sLRH relation from DPKE + NIZK

Lemma 8. Let Σ_{de} be $(n, \epsilon_{\mathsf{hv}}, \epsilon_{\mathsf{ind}})$ -PRIV-IND secure DPKE with message space $\{\{0,1\}^{n(\lambda)}\}_{\lambda \in \mathbb{N}}$, R_{pk} be its key relation. Let Π_{pk} be a NIZK for R_{pk} with ϵ_{zk} -ZK and ϵ_{snd} -adpative-soundness. (PGen_{de}, SGen_{de}) (in Fig.3) is a $(n, \epsilon_{\mathsf{pr}}, \epsilon_{\mathsf{hv}})$ -private generator of $R_{\mathsf{LR}}^{\mathsf{de}}$ for any $\epsilon_{\mathsf{pr}} \geq \epsilon_{\mathsf{ind}} + 2\epsilon_{\mathsf{zk}}$, and $R_{\mathsf{LR}}^{\mathsf{de}}$ is $(n, \epsilon_{\mathsf{cr}})$ -collision resistant w.r.t. PGen_{de}, for any $\epsilon_{\mathsf{cr}} \geq \epsilon_{\mathsf{snd}}$.

Proof. Let us analyze the collision resistance. If $\mathcal{A}_{\mathsf{cr}}$ breaks the collision-resistance w.r.t. PGen, then under an honestly generated $\mathsf{pp} = \mathsf{crs}_{\mathsf{pk}}$, it produces $(\pi_{pk}, pk_{\mathsf{de}}, c_{\mathsf{de}}, k')$ such that π_{pk} is a valid proof showing pk_{de} is a valid public key, i.e., there exists sk_{de} s.t. $(pk_{\mathsf{de}}, sk_{\mathsf{de}}) \in R_{pk}$, and $c = \mathsf{E}_{\mathsf{de}}(pk_{\mathsf{de}}, k) = \mathsf{E}_{\mathsf{de}}(pk_{\mathsf{de}}, k')$ for different $k \neq k'$. However, if pk_{de} is valid, $(c_{\mathsf{de}}, pk_{\mathsf{de}})$ determines k. Therefore, if finding $k' \neq k$, π_{pk} must be valid proof for a false statement. It follows that $\mathsf{Adv}^{\mathsf{cr}}_{\mathcal{A}_{\mathsf{cr}}}(\lambda) \leq \epsilon_{\mathsf{snd}}$ for any polynomial-time $\mathcal{A}_{\mathsf{cr}}$.

We now analyze the key privacy. Recall Definition 7,

$$\mathsf{Adv}^{\mathrm{pr}}_{\mathcal{A},\mathcal{W},\mathcal{F}}(\lambda) = |\Pr[\mathsf{Exp}^{\mathsf{pr},0}_{\mathcal{A},\mathcal{W},\mathcal{F}}(\lambda) = 1] - \Pr[\mathsf{Exp}^{\mathsf{pr},1}_{\mathcal{A},\mathcal{W},\mathcal{F}}(\lambda) = 1]|.$$

Besides $\mathsf{Exp}_{\mathcal{A},\mathcal{W},\mathcal{F}}^{\mathsf{pr},0}$ and $\mathsf{Exp}_{\mathcal{A},\mathcal{W},\mathcal{F}}^{\mathsf{pr},1}$, we define the following hybrid experiments to facilitate our proof.

 $\frac{\mathsf{Exp}_{\mathcal{A},\mathcal{W},\mathcal{F}}^{\mathsf{pr},\frac{1}{3}}}{\pi_{\mathsf{de}} \leftarrow \mathsf{SP}_{\mathsf{pk}}(\mathsf{crs}_{\mathsf{pk}},\mathsf{tk}_{\mathsf{pk}},pk_{\mathsf{de}})}.$ It is almost identical to $\mathsf{Exp}_{\mathcal{A},\mathcal{W},\mathcal{F}}^{\mathsf{pr},0}$, except that π_{de} in yk is a simulated proof, *i.e.*,

 $\underline{\mathsf{Exp}_{\mathcal{A},\mathcal{W},\mathcal{F}}^{\mathsf{pr},\frac{2}{3}}}$. It is almost identical to $\mathsf{Exp}_{\mathcal{A},\mathcal{W},\mathcal{F}}^{\mathsf{pr},\frac{1}{3}}$, except that c_{de} encypts of a uniformly chosen randomness k'.

It is easy to see for any polynomial-time A,

$$|\Pr[\mathsf{Exp}^{\mathsf{pr},0}_{\mathcal{A},\mathcal{W},\mathcal{F}}(\lambda) = 1] - \Pr[\mathsf{Exp}^{\mathsf{pr},\frac{1}{3}}_{\mathcal{A},\mathcal{W},\mathcal{F}}(\lambda) = 1]| \leq \epsilon_{\mathsf{zk}},$$

$$|\Pr[\mathsf{Exp}^{\mathsf{pr},\frac{1}{3}}_{\mathcal{A},\mathcal{W},\mathcal{F}}(\lambda) = 1] - \Pr[\mathsf{Exp}^{\mathsf{pr},\frac{2}{3}}_{\mathcal{A},\mathcal{W},\mathcal{F}}(\lambda) = 1]| \leq \epsilon_{\mathsf{ind}},$$

and

$$|\Pr[\mathsf{Exp}^{\mathsf{pr},\frac{2}{3}}_{\mathcal{A},\mathcal{W},\mathcal{F}}(\lambda) = 1] - \Pr[\mathsf{Exp}^{\mathsf{pr},1}_{\mathcal{A},\mathcal{W},\mathcal{F}}(\lambda) = 1]| \leq \epsilon_{\mathsf{zk}}.$$

It follows that for any polynomial-time \mathcal{A} , any efficiently-sampable \mathcal{W} and any ϵ_{hv} -Al \mathcal{F} , $\mathsf{Adv}^{\mathsf{pr}}_{\mathcal{A},\mathcal{W},\mathcal{F}}(\lambda) \leq \epsilon_{ind} + 2\epsilon_{\mathsf{zk}}$.

Under the exponentially-hard DDH assumption [30], it is known to exist a DPKE which is perfectly correct and secure against any ϵ -hard-to-invert leakage (as long as ϵ is a negligible function). Following Theorem 3 and Lemma 8, we have a κ -MAC against any ϵ -hard-to-invert leakage and thus can compile any secure randomness extractor.

5 Extension to Robust Fuzzy Extractors

In this section, we construct robust fuzzy extractors.

Intuition. Similar to the non-fuzzy case, we use a κ -MAC scheme to authenticate the helper string of the underlying fuzzy extractor. However, correctness and security will not directly inherit from the non-fuzzy case. Correctness can be fixed easily. We can use secure sketches to construct the underlying fuzzy extractor; thus one can recover the original secret w from the helper string using a close secret w'.

We now discuss the obstacles to security. While the helper string has to contain a secure sketch, the adversary may manipulate the secure sketch such that the recovered secret w'' is not identical to the original secret w, and she may forge an authentication tag being accepted by w'' to break the robustness. We can simply reject all w'' that are not t-close to w' (in this case w'' must be incorrect), and an allowed w'' will be 2t-close to w. The challenge is to ensure that adversaries cannot forge an authentication tag being accepted by this 2t-close secret. In the following, we introduce fuzzy unforgeability of κ -MAC, and show that the construction given in the last section already satisfies this property. Then, we construct a robust fuzzy extractor for CRS-dependent sources by using fuzzy-unforgeable κ -MAC.

 κ -MAC with fuzzy unforgeability. A κ -MAC scheme $\Sigma = \{\text{Init}, \mathsf{Tag}, \mathsf{Verify}\}$ satisfies q-fuzzy unforgeability, if given an authentication tag ς from k along with an auxiliary input about k, one cannot forge a new authentication tag being accepted by any target secret k' which is q-close to k. We allow the adversary to shift the original secret k any way she likes. I.e., the adversary can specify an arbitrary efficient function shift such that $k' = \mathsf{shift}(k, z)^6$, where z denotes arbitrary auxiliary information stored in the verifier's machine.

Definition 9 (One-time fuzzy-unforgeability). Let $\Sigma = \{\text{Init}, \text{Tag}, \text{Verify}\}\$ be a κ -MAC scheme with the key space $\{0,1\}^{n(\lambda)}$. We say Σ satisfies $(n,q,\epsilon_{\mathsf{unf}})$ one-time fuzzy-unforgeability w.r.t. (\mathbb{W},\mathbb{F}) , if for any polynomial-time adversary A, any $W \in \mathbb{W}$, any $\mathcal{F} \in \mathbb{F}$, and any \mathcal{Z} , it holds that

$$\mathsf{Adv}^{f-\mathrm{unf}}_{\mathcal{A},\mathcal{W},\mathcal{F}}(\lambda) = \Pr[\mathsf{Exp}^{f-\mathsf{unf}}_{\mathcal{A},\mathcal{W},\mathcal{F}}(\lambda) = 1] \leq \epsilon_{\mathsf{unf}}(\lambda).$$

The experiment $\mathsf{Exp}^\mathsf{f-unf}_{\mathcal{A},\mathcal{W},\mathcal{F}}$ is defined below, where shift is an arbitrary efficient function.

$$\begin{split} & \frac{\mathsf{Exp}_{\mathcal{A},\mathcal{W},\mathcal{F}}^{\mathsf{f-unf}}(\lambda)}{(\mathsf{crs},\tau) \leftarrow \mathsf{Init}(1^{\lambda}); (k,z) \leftarrow (W_{\lambda}|_{\mathsf{crs}}, Z_{\lambda}|_{\mathsf{crs}})} \\ & (m,st) \leftarrow \mathcal{A}(\mathsf{crs},f_{\lambda}(\mathsf{crs},k)); \varsigma \leftarrow \mathsf{Tag}(\mathsf{crs},k,m) \\ & (m^*,\varsigma^*,\mathsf{shift}) \leftarrow \mathcal{A}(\varsigma,st) \\ & \text{if } (m^*,\varsigma^*) \neq (m,\varsigma) \wedge k' = \mathsf{shift}(k,z) \in B_q(k) \\ & \wedge \mathsf{Verify}(\mathsf{crs},k',m^*,\varsigma^*) = 1 \text{ then return } 1 \\ & \text{return } 0 \end{split}$$

Construction from fuzzy sLRH relation. Recall our κ -MAC construction in Fig.2. If an adversary who is given yk and leakage about k outputs a forgery being accepted by a secret k^* , then, by

⁶ In the conference version [17], it was required that the forged authentication tag should not be accepted by any q-close secret, rather than a target secret specified by the adversary. That definition is unnecessarily strong and cannot be achieved by our construction.

tSE-NIZK, the adversary is able to output (yk', k') such that both (pp, yk', k') and (pp, yk', k^*) belong to the relation R_{LR} . For one-time standard unforgeability, k and k^* are equal, and such an adversary contradicts the definition of sLRH relation. For one-time q-fuzzy unforgeability, k^* will just be q-close to w, and we therefore strengthen the sLRH relation into its fuzzy version accordingly.

Definition 10 (Fuzzy-sLRH relation). Let R_{LR} be an NP relation with a generator (PGen, SGen). We say R_{LR} is an $(n, q, \epsilon_{\mathsf{lr}})$ -fuzzy-sLRH relation, if for any adversary $A \in \mathcal{C}_{s(\cdot)}$, any $\mathcal{W} \in \mathbb{W}$ and any $\mathcal{F} \in \mathbb{F}$, it holds that $\mathsf{Adv}^{\mathsf{flr}}_{\mathcal{A},\mathcal{W},\mathcal{F}}(\lambda) = \Pr[\mathsf{Exp}^{\mathsf{flr}}_{\mathcal{A},\mathcal{W},\mathcal{F}}(\lambda) = 1] \leq \epsilon_{\mathsf{lr}}(\lambda)$.

The experiment $\mathsf{Exp}^{\mathsf{flr}}_{\mathcal{A},\mathcal{W},\mathcal{F}}$ is defined below, where **shift** is an arbitrary efficient function, and Z_{λ} denotes an arbitrary distribution of auxiliary information.

We show the κ -MAC construction in Fig.2 will be a q-fuzzy unforgeable, if the underlying sLRH relation is a q-fuzzy sLRH relation.

Lemma 9. Let R_{LR} along with (PGen, SGen) be an (n, ϵ_{lr}) -q-fuzzy sLRH relation w.r.t. \mathbb{W} and \mathbb{F} . Let $\Pi = \{S_{zk}, P_{zk}, V_{zk}\}$ be a NIZK for the relation \bar{R}_{LR} satisfying ϵ_{zk} -ZK and ϵ_{tse} -tSE. Then, the construction in Fig.2 satisfies (n, q, ϵ_{unf}) one-time fuzzy-unforgeability w.r.t. \mathbb{W} and \mathbb{F} , for any $\epsilon_{unf} > \epsilon_{zk} + \epsilon_{tse} + \epsilon_{lr}$.

Proof. This proof is very similar to the proof of Lemma 6. We have the following hybrid experiments. $\mathsf{Exp}_{\mathcal{A},\mathcal{W},\mathcal{F}}^{\mathsf{f-unf},1}$. It is almost identical to $\mathsf{Exp}_{\mathcal{A},\mathcal{W},\mathcal{F}}^{\mathsf{f-unf}}$, except that Tag is replaced with Tag that is defined in the proof of Lemma 6.

 $\frac{\mathsf{Exp}_{\mathcal{A},\mathcal{W},\mathcal{F}}^{\mathsf{f-unf},2}}{\mathsf{the proof}}$. It is almost identical to $\mathsf{Exp}_{\mathcal{A},\mathcal{W},\mathcal{F}}^{\mathsf{f-unf},1}$, except that Verify is replaced with $\widehat{\mathsf{Verify}}$ defined in the proof of Lemma 6.

Following the same arguments in Lemma 6, we have that for any (A, W, F),

$$|\Pr[\mathsf{Exp}_{\mathcal{A},\mathcal{W},\mathcal{F}}^{\mathsf{f-unf},2}(\lambda) = 1] - \Pr[\mathsf{Exp}_{\mathcal{A},\mathcal{W},\mathcal{F}}^{\mathsf{f-unf}}(\lambda) = 1]| \le \epsilon_{\mathsf{zk}} + \epsilon_{\mathsf{tse}}.$$

Now we analysis the probability $\epsilon = \Pr[\mathsf{Exp}_{\mathcal{A},\mathcal{W},\mathcal{F}}^{\mathsf{f-unf},2}(\lambda) = 1]$. In this event, the adversary \mathcal{A} produces $(m^*,\varsigma^* = (yk^*,\pi_{\mathsf{zk}}^*),\mathsf{shift})$ such that $(\mathsf{pp},yk^*,k') \in R_{LR}$ for $k' = \mathsf{shift}(k,z)$, and the verifier algorithm Verify could extract k^* from π_{zk}^* such that $(\mathsf{pp},yk,k^*) \in R_{\mathsf{LR}}$. With this $(\mathcal{A},\mathcal{W},\mathcal{F})$, we can construct an adversary $\mathcal{A}_{\mathsf{lr}}$ against the $(n,q,\epsilon_{\mathsf{lr}})$ -fuzzy-sLRH relation, with probability ϵ . Thus, $\epsilon \leq \epsilon_{\mathsf{lr}}$, and it follows that

$$\Pr[\mathsf{Exp}^{\mathsf{f-unf}}_{\mathcal{A},\mathcal{W},\mathcal{F}}(\lambda) = 1] \leq \epsilon_{\mathsf{zk}} + \epsilon_{\mathsf{tse}} + \epsilon_{\mathsf{lr}}$$

for any polynomial-time \mathcal{A} , any $\mathcal{W} \in \mathbb{W}$, and any $\mathcal{F} \in \mathbb{F}$.

Fuzzy sLRH relation from collision-resistant relation with private generator. For a "collision resistant" sLRH relation, the adversary can "frame" some k' only when she finds k'. If given (pp, yk) finding $k' \in B_q^t$ is hard, then the relation will be a q-fuzzy sLRH relation. We argue when we can have the latter property from the privacy of the generator.

Note that the privacy of the generator cannot ensure that (pp, yk) hides all partial information about k, as (pp, yk) itself must be non-trivial about k. Actually, the privacy ensures that adversaries cannot learn anything which is useful for deciding that yk is either generated by using the leaked key k or using an independent key. Then, for small q such that $B_q(k)$ only contains polynomial points, $k' \in B_q(k)$ is surely hard-to-find from (pp, yk). However, for large q such that $B_q(k)$ could contain super-polynomial points, this argument does not apply.

We overcome this challenge by observing the task of recovering k from k' can be done with the help of 2t-secure sketch. More specifically, assume an adversary can recover k' from (pp, yk). Then, the distinguisher specifies the leakage as a 2t-secure sketch, invokes the adversary to have this $k' \in B_{2t}(k)$, and converts k' to k with the help of the secure sketch. Formally, we have the following theorem.

Theorem 4. Let (PGen, SGen) be a $(n, \epsilon_{pr}, \epsilon_{hv})$ -private generator for an NP relation R_{LR} , and let R_{LR} be (n, ϵ_{cr}) -collision-resistant w.r.t. PGen. Then R_{LR} along with (PGen, SGen) will be a (n, q, ϵ_{lr}) -fuzzy sLRH relation, for any $\epsilon_{lr} > 2\epsilon_{pr} + \epsilon_{cr} + \frac{\epsilon_{hv}}{2}$, w.r.t. \mathbb{W} and \mathbb{F} which satisfy the following conditions. (1) There is a q-secure sketch {SS, Rec} for each $\mathbb{W} \in \mathbb{W}$. (2)For every $\mathcal{F} \in \mathbb{F}$, define $\widetilde{\mathcal{F}} = \{\widetilde{f}_{\lambda}\}$ where

$$\widetilde{f}_{\lambda}(pp, w) = (r, \langle r, w \rangle, SS(w), f_{\lambda}(pp, w)), r \leftarrow \{0, 1\}^{n(\lambda)};$$

then, $\widetilde{\mathcal{F}}$ should be an ϵ_{hv} -AI w.r.t. every \mathcal{W} and PGen .

Proof. The proof is similar to the proof of Lemma.7.

Suppose, for contradiction, that there exist a polynomial-time adversary $\mathcal{B}, \mathcal{W} \in \mathbb{W}, \mathcal{F} \in \mathbb{F}$, and some \mathcal{Z} , such that $\mathsf{Adv}^{\mathrm{slr}}_{\mathcal{B},\mathcal{W},\mathcal{F}}(\lambda) > \epsilon_{\mathsf{lr}} > 2\epsilon_{\mathsf{pr}} + \epsilon_{\mathsf{cr}} + \frac{\epsilon_{\mathsf{hv}}}{2}$. We show there exist either

- a polynomial-time adversary \mathcal{A}_{pr} against the privacy of (PGen, SGen) with the advantage $\mathsf{Adv}^{pr}_{\mathcal{A}_{pr},\mathcal{W},\mathcal{F}'}(\lambda) > \epsilon_{pr}$, where \mathcal{F}' is defined according to \mathcal{F} as specified in this Theorem and thus is an ϵ_{hv} -AI w.r.t \mathcal{W} and PGen; Or,
- a polynomial-time adversary \mathcal{A}_{cr} against the collision-resistance of R_{LR} with the advantage $\mathsf{Adv}^{cr}_{\mathcal{A}_{cr}}(\lambda) > \epsilon_{cr}$.

To proceed the proof, we present the codes of \mathcal{A}_{pr} and \mathcal{A}_{cr} below.

First, we analyze the advantage of \mathcal{A}_{pr} . For notational convenience, we define the following events. (1) $\text{Ev}_{\notin B_{2t}(k)}$: \mathcal{B} outputs $k^* \notin B_{2t}(k)$; (2) $\text{Ev}_{\in B_{2t}(k)}$: \mathcal{B} outputs $k^* \in B_{2t}(k)$; (3) $\text{Ev}_{\notin B_{2t}(k)}^0$:

 $\operatorname{Ev}_{\notin B_{2t}(k)} \cap \langle r, k' \rangle \neq \beta$; (4) $\operatorname{Ev}_{\notin B_{2t}(k)}^1$: $\operatorname{Ev}_{\notin B_{2t}(k)} \cap \langle r, k' \rangle = \beta$; (5) $\operatorname{Ev}_{\mathcal{A}_{\mathsf{pr}}}^1$: $\mathcal{A}_{\mathsf{pr}}$ returns 1. (6) $\operatorname{Ev}_{k=k'}$: the recovered k' = k; (7) $\operatorname{Ev}_{k \neq k'}$: the recovered $k' \neq k$.

Without loss of generality, we assume $Rec(ss, k^*)$ always output $k' \in B_{2t}(k^*)$. By the correctness of $\{SS, Rec\}$, it follows that

 $\text{Ev}_{\notin B_{2t}(k)}$ and $\text{Ev}_{k\neq k'}$ are equivalent; $\text{Ev}_{\in B_{2t}(k)}$ and $\text{Ev}_{k=k'}$ are equivalent.

Then, by the description of \mathcal{A}_{pr} , in $\operatorname{Ev}_{\in B_{2t}(k)}$ and $\operatorname{Ev}_{\notin B_{2t}(k)}^1$, \mathcal{A}_{pr} always outputs 1, and that in $\operatorname{Ev}_{\notin B_{2t}(k)}^0$, \mathcal{A}_{pr} always outputs 0. Moreover, as r is independent of the generation of k',

$$\Pr[\mathtt{Ev}^0_{\not\in B_{2t}(k)}] = \Pr[\mathtt{Ev}^1_{\not\in B_{2t}(k)}] = \frac{1}{2}\Pr[\mathtt{Ev}_{\not\in B_{2t}(k)}].$$

Therefore, the following equation holds regardless of the distribution of \mathcal{A}_{pr} 's input.

$$\Pr[\mathsf{Ev}_{\mathcal{A}_{\mathsf{pr}}}^{1}] = \Pr[\mathsf{Ev}_{\mathcal{A}_{\mathsf{pr}}}^{1} | \mathsf{Ev}_{\in B_{2t}(k)}] \Pr[\mathsf{Ev}_{\in B_{2t}(k)}] + \Pr[\mathsf{Ev}_{\mathcal{A}_{\mathsf{pr}}}^{1} | \mathsf{Ev}_{\notin B_{2t}(k)}] \Pr[\mathsf{Ev}_{\notin B_{2t}(k)}] \\
= \Pr[\mathsf{Ev}_{\in B_{2t}(k)}] + \Pr[\mathsf{Ev}_{\mathcal{A}_{\mathsf{pr}}}^{1} | \mathsf{Ev}_{\notin B_{2t}(k)}] \Pr[\mathsf{Ev}_{\notin B_{2t}(k)}^{1}] \\
= \Pr[\mathsf{Ev}_{\in B_{2t}(k)}] + \frac{1}{2} \Pr[\mathsf{Ev}_{\notin B_{2t}(k)}] = \frac{1}{2} + \frac{\Pr[\mathsf{Ev}_{\in B_{2t}(k)}]}{2}.$$
(27)

Recall Definition 7, in $\mathsf{Exp}_{\mathcal{A}_\mathsf{pr},\mathcal{W},\mathcal{F}'}^{\mathsf{pr},0}$ and $\mathsf{Exp}_{\mathcal{A}_\mathsf{pr},\mathcal{W},\mathcal{F}'}^{\mathsf{pr},1}$, the input of \mathcal{A}_pr are two different distributions which we here denote by \mathcal{D}_0 and \mathcal{D}_1 , respectively. Now, we can reformulate the advantage of \mathcal{A}_pr as

$$\mathsf{Adv}^{\mathrm{pr}}_{\mathcal{A}_{\mathsf{pr}},\mathcal{W},\mathcal{F}'}(\lambda) = |\Pr[\mathsf{Ev}^{1,\mathcal{D}_0}_{\mathcal{A}_{\mathsf{pr}}}] - \Pr[\mathsf{Ev}^{1,\mathcal{D}_1}_{\mathcal{A}_{\mathsf{pr}}}]| = \frac{1}{2} |\Pr[\mathsf{Ev}^{\mathcal{D}_1}_{\in B_{2t}(k)}] - \Pr[\mathsf{Ev}^{\mathcal{D}_0}_{\in B_{2t}(k)}]|, \tag{28}$$

where $\text{Ev}^{\mathcal{D}_b}$ denotes the event Ev conditioned on that \mathcal{A}_{pr} 's input distribution is \mathcal{D}_b , for $b \in \{0, 1\}$.

When \mathcal{A}_{pr} 's input distribution is \mathcal{D}_1 , at the point of \mathcal{B} 's view, the environment provided by \mathcal{A}_{pr} is identical to that of $\mathsf{Exp}^{\mathsf{lr}}_{\mathcal{B},\mathcal{W},\mathcal{F}}$. We argue that, in this case, $\mathsf{Ev}^{\mathcal{D}_1}_{\in B_{2t}(k)}$ can imply that \mathcal{B} breaks the sLRH relation without loss of generality. Indeed, if \mathcal{B} outputs $k^* \in B_{2t}(k)$, she can win by setting shift to be a constant function outputting k^* . Therefore,

$$\Pr[\mathsf{Ev}^{\mathcal{D}_1}_{\in B_{2t}(k)}] = \Pr[\mathsf{Exp}^{\mathsf{lr}}_{\mathcal{B},\mathcal{W},\mathcal{F}}(\lambda) = 1 \cap \mathsf{Ev}^{\mathcal{D}_1}_{\in B_{2t}(k)}] = \Pr[\mathsf{Ev}^{\mathcal{D}_1}_{\in B_{2t}(k)} | \mathsf{Exp}^{\mathsf{lr}}_{\mathcal{B},\mathcal{W},\mathcal{F}}(\lambda) = 1] \mathsf{Adv}^{\mathsf{lr}}_{\mathcal{B},\mathcal{W},\mathcal{F}}(\lambda). \tag{29}$$

When \mathcal{A}_{pr} 's input distribution is \mathcal{D}_0 , as yk provided to \mathcal{B} is independent of k, $\operatorname{Ev}_{k=k'}^{\mathcal{D}_0}$ means that we can find the exact pre-image k from pp, $f_{\lambda}(pp, k)$ and ss. It follows that

$$\Pr[\mathsf{Ev}_{\in B_{2t}(k)}^{\mathcal{D}_0}] \le \frac{\epsilon_{\mathsf{hv}}(\lambda)}{2}.\tag{30}$$

Combining Eq.28, 29 and 30, we have

$$\mathsf{Adv}^{\mathrm{pr}}_{\mathcal{A}_{\mathsf{pr}}, \mathcal{W}, \mathcal{F}'}(\lambda) \ge \frac{\Pr[\mathsf{Ev}^{\mathcal{D}_{1}}_{\in B_{2t}(k)} | \mathsf{Exp}^{\mathsf{lr}}_{\mathcal{B}, \mathcal{W}, \mathcal{F}}(\lambda) = 1] \mathsf{Adv}^{\mathsf{lr}}_{\mathcal{B}, \mathcal{W}, \mathcal{F}}(\lambda)}{2} - \frac{\epsilon_{\mathsf{hv}}(\lambda)}{4}. \tag{31}$$

Next, we analyze the advantage of \mathcal{A}_{cr} . At the point of \mathcal{B} 's view, the environment provided by \mathcal{A}_{cr} is identical to that of $\mathsf{Exp}^{\mathsf{lr}}_{\mathcal{B},\mathcal{W},\mathcal{F}}$. Moreover, as analyzed before, the environment provided by $\mathcal{A}_{\mathsf{pr}}$

with input from \mathcal{D}_1 is also identical to that of $\mathsf{Exp}^{\mathsf{lr}}_{\mathcal{B},\mathcal{W},\mathcal{F}}$. Thus, we can use the notation $\mathsf{Ev}^{\mathcal{D}_1}_{\notin B_{2t}(k)}$ to denote the event that, in the environment provided by $\mathcal{A}_{\mathsf{cr}}$, \mathcal{B} outputs $k^* \notin B_{2t}(k)$. Notice that if \mathcal{B} wins, $\mathsf{shift}(k,z) \in B_{2t}(k)$; if $k^* \notin B_{2t}$, k^* and $\mathsf{shift}(k,z)$ form a collision w.r.t. pp and yk^* . Therefore,

$$\mathsf{Adv}^{\mathrm{cr}}_{\mathcal{A}\mathsf{cr}}(\lambda) \geq \Pr[\mathsf{Exp}^{\mathsf{lr}}_{\mathcal{B},\mathcal{W},\mathcal{F}}(\lambda) = 1 \cap \mathsf{Ev}^{\mathcal{D}_1}_{\notin B_{2t}(k)}] = \Pr[\mathsf{Ev}^{\mathcal{D}_1}_{\notin B_{2t}(k)} | \mathsf{Exp}^{\mathsf{lr}}_{\mathcal{B},\mathcal{W},\mathcal{F}}(\lambda) = 1] \mathsf{Adv}^{\mathrm{lr}}_{\mathcal{B},\mathcal{W},\mathcal{F}}(\lambda). \quad (32)$$

Combining Eq.31 and 32, it follows that

$$\mathsf{Adv}^{\mathrm{cr}}_{\mathcal{A}_{\mathsf{cr}}}(\lambda) + 2\mathsf{Adv}^{\mathrm{pr}}_{\mathcal{A}_{\mathsf{pr}},\mathcal{W},\mathcal{F}'}(\lambda) \ge \mathsf{Adv}^{\mathrm{lr}}_{\mathcal{B},\mathcal{W},\mathcal{F}}(\lambda) - \frac{\epsilon_{\mathsf{hv}}(\lambda)}{2} > \epsilon_{\mathsf{cr}} + 2\epsilon_{\mathsf{pr}}. \tag{33}$$

Thus, it follows either $\mathsf{Adv}^{\mathrm{cr}}_{\mathcal{A}_{\mathsf{cr}}}(\lambda) > \epsilon_{\mathsf{cr}}$ or $\mathsf{Adv}^{\mathrm{pr}}_{\mathcal{A}_{\mathsf{pr}},\mathcal{W},\mathcal{F}'}(\lambda) > \epsilon_{\mathsf{pr}}$. We obtain the contradiction and complete the proof.

Constructing robust fuzzy extractors. For a robust fuzzy extractor with t-error tolerance, we use a 2t-fuzzy unforgeable κ -MAC to authenticate the helper string of a fuzzy extractor with t-error tolerance. Note that the helper string, along with the extracted randomness, forms the auxiliary input f(w) of the κ -MAC, our 2t-fuzzy unforgeable κ -MAC construction allows an auxiliary input function f when f together with a 2t-secure sketch forms a hard-to-invert leakage. Therefore, although a t-secure sketch is sufficient for constructing a fuzzy extractor with t-error tolerance, we will use a 2t-secure sketch instead, such that f(w) along with a 2t-secure sketch must be hard-to-invert.

Let $\{SS, Rec\}$ be a 2t-secure sketch, $\Sigma = \{Init, Tag, Verify\}$ be a κ -MAC with 2t-fuzzy unforgeability, and Ext be a strong extractor. We present the detailed construction of robust fuzzy extractor in Fig. 4 and the analysis in Theorem 5.

$CRS(1^{\lambda})$	Gen(crs,w)	$Rep(crs,\widetilde{w},P)$
$\boxed{(\mathtt{crs},\tau) \leftarrow Init(1^{\lambda})}$	$ss \leftarrow SS(w)$	$w' \leftarrow Rec(ss, \widetilde{w})$
return crs	$i \leftarrow \$ \left\{0,1\right\}^s, r \leftarrow Ext(i,w)$	return $R \leftarrow Ext(i, w'), \mathbf{if}$
	$\varsigma \leftarrow Tag(crs, w, (ss, i))$	$dist(w',\widetilde{w}) \leq t$
	$\mathbf{return}\ R = r, P = (ss, i, \varsigma)$	$Verify(crs, w', (ss, i), \varsigma) = 1$
		return \perp

Fig. 4. Robust fuzzy extractor rfExt from randomness extractor + secure sketch+ κ -MAC

Theorem 5. Assume {SS, Rec} is an $(\mathcal{M}, k, k', 2t)$ -secure sketch scheme, Ext is an (n, k', ℓ) -strong extractor with ϵ_{ext} -privacy and being ϵ_{inv} -hard-to-invert, and Σ is a κ -MAC with $(n, 2t, \epsilon_{\mathsf{unf}})$ -fuzzy unforgeability w.r.t. \mathbb{W} and \mathbb{F} and $(n, \epsilon_{\mathsf{kpriv}}, \epsilon_{\mathsf{hv}})$. Then, if \mathbb{W} is all (n, k)-sources, \mathbb{F} contains function ensembles implementing SS, and $\epsilon_{\mathsf{inv}} < \epsilon_{\mathsf{hv}}$, the construction rfExt in Fig.4 is an $(\mathcal{M}, k, \ell, t)$ -robust fuzzy extractor with perfect correctness, ϵ -privacy and δ -robustness, for any $\epsilon > \epsilon_{\mathsf{ext}} + 2\epsilon_{\mathsf{kpriv}}$ and $\delta > \epsilon_{\mathsf{unf}}$.

This proof is similar to the proof of Theorem 2. We prove the privacy and the robustness in Lemma 10 and Lemma 11, respectively.

Lemma 10. rExt (in Fig.4) satisfies ϵ_{priv} -privacy, for any $\epsilon_{priv} > \epsilon_{ext} + 2\epsilon_{kpriv}$.

Proof. We prove this lemma by contradiction. Assume we have a polynomial-time adversary \mathcal{B} and an efficiently-samplable (n,k)-source \mathcal{W} such that $\mathsf{Adv}^{\mathsf{priv}}_{\mathcal{B},\mathcal{W}}(\lambda) > \epsilon_{\mathsf{ext}} + 2\epsilon_{\mathsf{kpriv}}$. Then, we leverage \mathcal{B} to construct a polynomial-time adversary $\mathcal{A}_{\mathsf{ext}}$ for Ext, and two polynomial-time adversaries $\mathcal{A}_{\mathsf{mac},0}$ and $\mathcal{A}_{\mathsf{mac},1}$ for κ -MAC Σ , such that, for the source \mathcal{W} , it follows that either

$$\mathsf{Adv}^{\mathrm{ext}}_{\mathcal{A}_{\mathrm{ext}},\mathcal{W}}(\lambda) > \epsilon_{\mathrm{ext}}, \ \mathsf{Adv}^{\mathrm{kpriv}}_{\mathcal{A}_{\mathrm{mac},0},\mathcal{W},\mathcal{F}}(\lambda) > \epsilon_{\mathrm{kpriv}}, \ \mathrm{or} \ \mathsf{Adv}^{\mathrm{kpriv}}_{\mathcal{A}_{\mathrm{mac},1},\mathcal{W},\mathcal{F}}(\lambda) > \epsilon_{\mathrm{kpriv}}. \tag{34}$$

where $\mathcal{F} = \{f_{\lambda}\}$ implements the secure sketch SS and the extractor Ext, namely,

$$f_{\lambda}(w) = (SS(w), Ext(w, U_s), U_s)$$

where U_s is a uniform random variable over $\{0,1\}^s$. Note that such \mathcal{F} is an admissible auxiliary inputs, as $\epsilon_{\mathsf{hv}} \geq \epsilon_{\mathsf{inv}}$. (CRS, $\mathcal{T} = \{T_{\lambda}\}$) denotes the random variable ensemble outputted by Init of κ -MAC; As \mathcal{T} can be computed (even inefficiently) using CRS and coins independent of \mathcal{W} , for every λ , we have

$$\widetilde{\mathbf{H}}_{\infty}(W_{\lambda}|\mathsf{CRS}_{\lambda}, T_{\lambda}) = \widetilde{\mathbf{H}}_{\infty}(W_{\lambda}|\mathsf{CRS}_{\lambda}) \ge k(\lambda).$$

As $\{SS, Rec\}$ is an $(\mathcal{M}, k, k', 2t)$ -secure sketch, it follows that

$$\widetilde{\mathbf{H}}_{\infty}(W_{\lambda}|\mathsf{CRS}_{\lambda}, T_{\lambda}, \mathsf{SS}(W_{\lambda})) \geq k'(\lambda).$$

Therefore, Eq.34 contradcits our assumptions on the underlying tools, and thus $\mathsf{Adv}^{\mathsf{priv}}_{\mathcal{B},\mathcal{W}}(\lambda) \leq \epsilon_{\mathsf{ext}} + 2\epsilon_{\mathsf{kpriv}}$ for all admissible \mathcal{B} and \mathcal{W} .

Now, to proceed with the proof, we turn to construct the adversaries $\mathcal{A}_{\mathsf{ext}}$, $\mathcal{A}_{\mathsf{mac},0}$ and $\mathcal{A}_{\mathsf{mac},1}$, using \mathcal{B} against rExt. The adversaries' codes are presented below. In $\mathcal{A}_{\mathsf{ext}}$, SimTag is the simulator of κ -MAC. In $\mathcal{A}_{\mathsf{mac},b}$, r is the extracted randomness from w with the seed i_{ext} . \mathcal{O}_{β} returns a real tag when $\beta = 1$ or returns a simulated tag when $\beta = 0$.

Recall the privacy definition of a robust extractor (cf. Def.3). The adanvantage of \mathcal{B} against rExt's privay w.r.t. \mathcal{W} is defined by $\mathsf{Adv}^{\mathsf{priv}}_{\mathcal{B},\mathcal{W}}(\lambda) = |\Pr[\mathsf{Exp}^{\mathsf{priv},0}_{\mathcal{B},\mathcal{W}}(\lambda) = 1] - \Pr[\mathsf{Exp}^{\mathsf{priv},1}_{\mathcal{B},\mathcal{W}}(\lambda) = 1]|$. Recall the definition of the strong extractor in Sect.2, and assume that

$$p_0 = \Pr \left[(\mathtt{crs}, \tau) \leftarrow (\mathtt{CRS}_{\lambda}, T_{\lambda}), w \leftarrow W_{\lambda}|_{\mathtt{crs}}, i_{\mathtt{ext}} \leftarrow \$ \left\{ 0, 1 \right\}^{si(\lambda)} \right],$$

$$\mathtt{ss} \leftarrow \mathsf{SS}(w), r \leftarrow \$ \left\{ 0, 1 \right\}^{\ell(\lambda)} : 1 \leftarrow \mathcal{A}_{\mathtt{ext}}(i_{\mathtt{ext}}, r, \mathtt{crs}, \tau, \mathtt{ss}) \right],$$

$$p_1 = \Pr \begin{bmatrix} (\mathtt{crs}, \tau) \leftarrow (\mathtt{CRS}_{\lambda}, T_{\lambda}), w \leftarrow W_{\lambda}|_{\mathtt{crs}}, i_{\mathtt{ext}} \leftarrow \$ \left\{0, 1\right\}^{si(\lambda)} \\ \mathtt{ss} \leftarrow \mathtt{SS}(w), r \leftarrow \mathtt{Ext}(i_{\mathtt{ext}}, w) : 1 \leftarrow \mathcal{A}_{\mathtt{ext}}(i_{\mathtt{ext}}, r, \mathtt{crs}, \tau, \mathtt{ss}) \end{bmatrix}.$$

Then, the advanatage of $\mathcal{A}_{\mathsf{ext}}$ against Ext is $\mathsf{Adv}^{\mathsf{ext}}_{\mathcal{A}_{\mathsf{ext}},\mathcal{W},(\mathsf{CRS},\mathcal{T})}(\lambda) = |p_0 - p_1|$. For $b \in \{0,1\}$, we denote $\Pr[\mathsf{Exp}^{\mathsf{priv},b}_{\mathcal{B}.\mathcal{W}}(\lambda) = 1] - p_b = \Delta_b$. By standard arguments, we have

$$\mathsf{Adv}^{\mathrm{priv}}_{\mathcal{B},\mathcal{W}}(\lambda) = \mathsf{Adv}^{\mathrm{ext}}_{\mathcal{A}_{\mathrm{ext}},\mathcal{W}}(\lambda) + |\Delta_0| + |\Delta_1|$$
(35)

It is easy to verify that, at the point of \mathcal{B} 's view, the experiment $\mathsf{Exp}^{\mathsf{priv},b}_{\mathcal{B},\mathcal{W}}$ is identical to $\mathsf{Exp}^{\mathsf{kpriv},1}_{\mathcal{A}_{\mathsf{mac},b},\mathcal{W},\mathcal{F}}$ (cf. Def.6), and thus $\Pr[\mathsf{Exp}^{\mathsf{priv},b}_{\mathcal{B},\mathcal{W}}(\lambda) = 1] = \Pr[\mathsf{Exp}^{\mathsf{kpriv},1}_{\mathcal{A}_{\mathsf{mac},b},\mathcal{W},\mathcal{F}}(\lambda) = 1]$. Similarly, we have $p_b = \Pr[\mathsf{Exp}^{\mathsf{kpriv},0}_{\mathcal{A}_{\mathsf{mac},b},\mathcal{W},\mathcal{F}} = 1]$.

have $p_b = \Pr[\mathsf{Exp}_{\mathcal{A}_{\mathsf{mac},b},\mathcal{W},\mathcal{F}}^{\mathsf{kpriv},0} = 1].$ Notice that $\mathsf{Adv}_{\mathcal{A}_{\mathsf{mac},b},\mathcal{W},\mathcal{F}}^{\mathsf{kpriv},0}(\lambda) = |\Pr[\mathsf{Exp}_{\mathcal{A}_{\mathsf{mac},b},\mathcal{W},\mathcal{F}}^{\mathsf{kpriv},0}(\lambda) = 1] - \Pr[\mathsf{Exp}_{\mathcal{A}_{\mathsf{mac},b},\mathcal{W},\mathcal{F}}^{\mathsf{kpriv},1}(\lambda) = 1]|$, we have $\mathsf{Adv}_{\mathcal{A}_{\mathsf{mac},b},\mathcal{W},\mathcal{F}}^{\mathsf{kpriv}}(\lambda) = \Delta_b$. Therefore, we have

$$\mathsf{Adv}^{\mathrm{priv}}_{\mathcal{B},\mathcal{W}}(\lambda) = \mathsf{Adv}^{\mathrm{ext}}_{\mathcal{A}_{\mathsf{ext}},\mathcal{W},(\mathsf{CRS},\mathcal{T})}(\lambda) + \mathsf{Adv}^{\mathrm{kpriv}}_{\mathcal{A}_{\mathsf{mac},0},\mathcal{W},\mathcal{F}}(\lambda) + \mathsf{Adv}^{\mathrm{kpriv}}_{\mathcal{A}_{\mathsf{mac},1},\mathcal{W},\mathcal{F}}(\lambda).$$

If
$$Adv_{\mathcal{B},\mathcal{W}}^{priv}(\lambda) > \epsilon_{ext} + 2\epsilon_{kpriv}$$
, Eq.34 immediately follows.

Lemma 11. rExt (in Fig.4) satisfies δ_{rob} -post-application-robustness, for any $\delta_{\text{rob}} \geq \epsilon_{\text{unf}}$.

Proof. We prove this lemma by contradiction. Assume there is $\delta_0 > \epsilon_{\sf unf}$, and we have a polynomial-time adversary $\mathcal B$ who has an advantage greater than δ_0 w.r.t. some efficiently-samplable (n,k)-source $\mathcal W$. Then, we leverage $\mathcal B$ to construct a polynomial adversary $\mathcal A_{\sf mac}$ against the unforgeability of κ -MAC Σ w.r.t. $\mathcal W$, with advantage $\mathsf{Adv}^{\sf unf}_{\mathcal A_{mac},\mathcal W,\mathcal F}(\lambda) > \delta_0 > \epsilon_{\sf unf}$. Here $\mathcal F$ is the function ensemble implementing Ext and SS.

Recall the fuzzy-unforgeability definition, in which the adversary $\mathcal{A}_{\mathsf{mac}}$ could specify the target secret by issuing an efficient function shift that takes as inputs the original secret w and some auxiliary information z the verifier has. In the proof, we let the auxiliary information be the close secret \widetilde{w} , which is sampled from \widetilde{W} and held by the verifier. The code of $\mathcal{A}_{\mathsf{mac}}$ and the function shift are presented below, where \mathcal{O} on the query m returns $\varsigma \leftarrow \mathsf{Tag}(\mathsf{crs}, w, m)$.

At the point of \mathcal{B} 's view, the environment provided by \mathcal{A}_{mac} is identical to that of $\mathsf{Exp}_{\mathcal{B},\mathcal{W},\widetilde{\mathcal{W}}}$ (cf. Def.3). Thus, with the probability $\mathsf{Adv}^{\mathsf{frob}}_{\mathcal{B},\mathcal{W},\widetilde{\mathcal{W}}}(\lambda)$, it holds that

$$(\mathsf{ss}^*, i^*_\mathsf{ext}, \varsigma^*) \neq (\mathsf{ss}, i_\mathsf{ext}, \varsigma), w' = \mathsf{Rec}(\widetilde{w}, \mathsf{ss}^*) \in B_{2t}(\widetilde{w}), \text{ and } \mathsf{Verify}(\mathsf{crs}, w', (\mathsf{ss}^*, i^*_\mathsf{ext}), \varsigma^*) = 1.$$

In this case, $\mathcal{A}_{\mathsf{mac}}$ breaks the fuzzy unforgeability of Σ . Therefore, $\mathsf{Adv}^{\mathsf{rob}}_{\mathcal{B} \, \mathcal{W} \, \widetilde{\mathcal{W}}}(\lambda) \leq \epsilon_{\mathsf{unf}}$.

6 Conclusions

Robust (fuzzy) extractors imply and thus usually rely on weak-secret-based MAC schemes. Random oracle is a perfect MAC, only requiring super-logarithmic min-entropy of the source. In contrast, an optimal information-theoretical MAC in the plain model still requires sources with a more-than-half entropy rate. A common reference string (CRS) can empower MAC schemes to work with low-entropy sources; However, all known constructions in this model put another stringent requirement that sources must be CRS-independent.

In the information-theoretical setting, we prove the "equivalence" between a CRS-model MAC for CRS-dependent sources and a plain-model MAC, showing that the former will be subject to the same lower bound. It thus becomes necessary to study computational MACs for general low-entropy sources. Along the direction, we formulate a new cryptographic primitive κ -MAC capturing the standard-model properties of the random oracle as a MAC and present constructions for CRS-dependent sources. They naturally lead to the first CRS-dependent computational (fuzzy) robust extractors with a minimal min-entropy requirement, closing the gap left by the state-of-the-art standard-model robust extractors. Our new tool of κ -MAC could have broader applications and deserve an in-depth study for, e.g., achieving full security rather than the one-time security as our work ensures. Also, it is always interesting to ask if we can have κ -MAC or robust extractors in the plain model from well-founded assumptions. We leave them as interesting open problems.

References

- 1. D. Aggarwal, M. Obremski, J. L. Ribeiro, M. Simkin, and L. Siniscalchi. Two-source non-malleable extractors and applications to privacy amplification with tamperable memory. *IACR Cryptology ePrint Archive*, 2020:1371, 2020
- 2. D. Apon, C. Cachet, B. Fuller, P. Hall, and F. Liu. Nonmalleable digital lockers and robust fuzzy extractors in the plain model. *IACR Cryptology ePrint Archive*, page 1108, 2022.
- 3. J. Bartusek, F. Ma, and M. Zhandry. The distinction between fixed and random generators in group-based assumptions. In *Annual International Cryptology Conference CRYPTO 2019*, volume 11693 of *Lecture Notes in Computer Science*, pages 801–830. Springer, 2019.
- 4. M. Blum, P. Feldman, and S. Micali. Non-interactive zero-knowledge and its applications (extended abstract). In *Annual ACM Symposium on Theory of Computing STOC 1988*, pages 103–112. ACM, 1988.
- 5. X. Boyen. Reusable cryptographic fuzzy extractors. In ACM Conference on Computer and Communications Security, pages 82–91. ACM, 2004.
- X. Boyen, Y. Dodis, J. Katz, R. Ostrovsky, and A. D. Smith. Secure remote authentication using biometric data. In Annual International Conference on the Theory and Applications of Cryptographic Techniques - EUROCRYPT 2005, volume 3494 of Lecture Notes in Computer Science, pages 147–163. Springer, 2005.
- Z. Brakerski and G. Segev. Better security for deterministic public-key encryption: The auxiliary-input setting. In Annual International Cryptology Conference - CRYPTO 2011, volume 6841 of Lecture Notes in Computer Science, pages 543–560. Springer, 2011.
- 8. R. Canetti, B. W. Fuller, O. Paneth, L. Reyzin, and A. D. Smith. Reusable fuzzy extractors for low-entropy distributions. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques EUROCRYPT 2016*, volume 9665 of *Lecture Notes in Computer Science*, pages 117–146. Springer, 2016.
- 9. R. Canetti, O. Goldreich, and S. Halevi. The random oracle methodology, revisited (preliminary version). In *Annual ACM Symposium on Theory of Computing STOC 1998*, pages 209–218. ACM, 1998.
- R. Cramer, Y. Dodis, S. Fehr, C. Padró, and D. Wichs. Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors. In *Annual International Conference on the Theory and Applications* of Cryptographic Techniques - EUROCRYPT 2008, volume 4965 of Lecture Notes in Computer Science, pages 471–488. Springer, 2008.
- 11. Y. Dodis, K. Haralambiev, A. López-Alt, and D. Wichs. Efficient public-key cryptography in the presence of key leakage. In *International Conference on the Theory and Application of Cryptology and Information Security ASIACRYPT 2010*, volume 6477 of *Lecture Notes in Computer Science*, pages 613–631. Springer, 2010.

- 12. Y. Dodis, Y. T. Kalai, and S. Lovett. On cryptography with auxiliary input. In *Annual ACM Symposium on Theory of Computing STOC 2009*, pages 621–630. ACM, 2009.
- Y. Dodis, J. Katz, L. Reyzin, and A. D. Smith. Robust fuzzy extractors and authenticated key agreement from close secrets. In *Annual International Cryptology Conference - CRYPTO 2006*, volume 4117 of *Lecture Notes in Computer Science*, pages 232–250. Springer, 2006.
- 14. Y. Dodis, L. Reyzin, and A. D. Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In Annual International Conference on the Theory and Applications of Cryptographic Techniques -EUROCRYPT 2004, volume 3027 of Lecture Notes in Computer Science, pages 523-540. Springer, 2004.
- 15. Y. Dodis and D. Wichs. Non-malleable extractors and symmetric key cryptography from weak secrets. In *Annual ACM Symposium on Theory of Computing STOC 2009*, pages 601–610. ACM, 2009.
- S. Faust, C. Hazay, J. B. Nielsen, P. S. Nordholt, and A. Zottarel. Signature schemes secure against hard-to-invert leakage. In *International Conference on the Theory and Application of Cryptology and Information Security -*ASIACRYPT 2012, volume 7658 of Lecture Notes in Computer Science, pages 98–115. Springer, 2012.
- 17. H. Feng and Q. Tang. Computational robust (fuzzy) extractors for crs-dependent sources with minimal minentropy. In *Theory of Cryptography Conference TCC 2021*, volume 13043 of *Lecture Notes in Computer Science*, pages 689–717. Springer, 2021.
- B. Fuller, L. Reyzin, and A. D. Smith. When are fuzzy extractors possible? In *International Conference on the Theory and Application of Cryptology and Information Security ASIACRYPT 2016*, volume 10031 of *Lecture Notes in Computer Science*, pages 277–306, 2016.
- A. Garg, Y. T. Kalai, and D. Khurana. Low error efficient computational extractors in the CRS model. In Annual International Conference on the Theory and Applications of Cryptographic Techniques - EUROCRYPT 2020, volume 12105 of Lecture Notes in Computer Science, pages 373-402. Springer, 2020.
- S. Goldwasser and Y. T. Kalai. Cryptographic assumptions: A position paper. In Theory of Cryptography Conference - TCC 2016, volume 9562 of Lecture Notes in Computer Science, pages 505–522. Springer, 2016.
- B. Kanukurthi and L. Reyzin. An improved robust fuzzy extractor. In *International Conference on Security and Cryptography for Networks SCN 2008*, volume 5229 of *Lecture Notes in Computer Science*, pages 156–171. Springer, 2008.
- J. Katz and V. Vaikuntanathan. Signature schemes with bounded leakage resilience. In *International Conference* on the Theory and Application of Cryptology and Information Security - ASIACRYPT 2009, volume 5912 of Lecture Notes in Computer Science, pages 703–720. Springer, 2009.
- 23. R. Renner and S. Wolf. Simple and tight bounds for information reconciliation and privacy amplification. In International Conference on the Theory and Application of Cryptology and Information Security - ASIACRYPT 2005, volume 3788 of Lecture Notes in Computer Science, pages 199–216. Springer, 2005.
- A. D. Santis, G. D. Crescenzo, R. Ostrovsky, G. Persiano, and A. Sahai. Robust non-interactive zero knowledge. In Annual International Cryptology Conference - CRYPTO 2001, volume 2139 of Lecture Notes in Computer Science, pages 566–598. Springer, 2001.
- 25. Y. Wen and S. Liu. Robustly reusable fuzzy extractor from standard assumptions. In *International Conference* on the Theory and Application of Cryptology and Information Security ASIACRYPT 2018, volume 11274 of Lecture Notes in Computer Science, pages 459–489. Springer, 2018.
- 26. Y. Wen, S. Liu, and D. Gu. Generic constructions of robustly reusable fuzzy extractor. In *Public Key Cryptography* (2), volume 11443 of *Lecture Notes in Computer Science*, pages 349–378. Springer, 2019.
- 27. Y. Wen, S. Liu, and S. Han. Reusable fuzzy extractor from the decisional diffie-hellman assumption. *Design*, Codes, and Cryptography., 86(11):2495–2512, 2018.
- Y. Wen, S. Liu, Z. Hu, and S. Han. Computational robust fuzzy extractor. The Computer Journal, 61(12):1794– 1805, 2018.
- T. H. Yuen, S. Yiu, and L. C. K. Hui. Fully leakage-resilient signatures with auxiliary inputs. In Australasian Conference on Information Security and Privacy - ACISP 2012, volume 7372 of Lecture Notes in Computer Science, pages 294–307. Springer, 2012.
- 30. M. Zhandry. On elfs, deterministic encryption, and correlated-input security. In *International Conference on the Theory and Application of Cryptographic Techniques EUROCRYPT 2019*, volume 11478 of *Lecture Notes in Computer Science*, pages 3–32. Springer, 2019.