# More Efficient Public-Key Cryptography with Leakage and Tamper Resilience 

<br>${ }^{1}$ School of Cyber Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China<br>\{dalen17, dwgu\}@sjtu.edu.cn<br>${ }^{2}$ State Key Laboratory of Cryptology, P.O. Box 5159, Beijing 100878, China<br>${ }^{3}$ Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China<br>slliu@sjtu.edu.cn


#### Abstract

In this paper, we study the design of efficient signature and public-key encryption (PKE) schemes in the presence of both leakage and tampering attacks. Firstly, we formalize the strong leakage and tamperresilient (sLTR) security model for signature, which provides strong existential unforgeability, and deals with bounded leakage and restricted tampering attacks, as a counterpart to the sLTR security introduced by Sun et al. (ACNS 2019) for PKE. Then, we present direct constructions of signature and chosen-ciphertext attack (CCA) secure PKE schemes in the sLTR model, based on the matrix decisional Diffie-Hellman (MDDH) assumptions (which covers the standard symmetric external DH (SXDH) and $k$-Linear assumptions) over asymmetric pairing groups. Our schemes avoid the use of heavy building blocks such as the true-simulation extractable non-interactive zero-knowledge proofs (tSE-NIZK) proposed by Dodis et al. (ASIACRYPT 2010), which are usually needed in constructing schemes with leakage and tamper-resilience. Especially, our SXDHbased signature and PKE schemes are more efficient than the existing schemes in the leakage and tamper-resilient setting: our signature scheme has only 4 group elements in the signature, which is about $5 \times \sim 8 \times$ shorter, and our PKE scheme has only 6 group elements in the ciphertext, which is about $1.3 \times \sim 3.3 \times$ shorter. Finally, we note that our signature scheme is the first one achieving strong existential unforgeability in the leakage and tamper-resilient setting, where strong existential unforgeability has important applications in building more complex primitives such as signcryption and authenticated key exchange.


Keywords: digital signature, public-key encryption, leakage attacks, tampering attacks

## 1 Introduction

Traditionally, when analyzing and proving security of cryptographic schemes, it is always assumed that the only way for an adversary to get information
about the secret keys is through black-box access to the cryptographic devices. In reality, however, an adversary may go far beyond black-box access, and obtain secret key information by directly accessing/tampering with the memory or the internal computation of the devices. To deal with these threats, leakage and tamper-resilient cryptography emerges with the aim of designing provably secure cryptographic schemes in such scenarios.

Leakage-resilient security. The motivation for leakage-resilient cryptography is the increasing popularity of various side-channel attacks [23, 29, 28], including timing measurements, power analysis, electromagnetic measurements and microwave attacks, through which an adversary can recover partial information about the secret keys. Such a capability is usually formulated by a leakage oracle, which allows the adversary to specify arbitrary leakage functions $L$ and obtain the results $L(s k)$ of applying $L$ to the secret key $s k$. Leakage-resilient security requires that the cryptographic schemes remain secure even for the adversary who has access to the leakage oracle. In this work, we focus on the bounded leakageresilient security $[1,32]$, where the total amount $|L(s k)|$ of leakage information is less than the whole secret key $|s k|$ and in particular bounded.

Tamper-resilient security. The attacks that leakage-resilient cryptography considers are in fact passive attacks, while the adversary may also launch active attacks such as fault injection and memory tampering attacks [6, 19], through which the adversary can force the cryptographic devices to operate under a different but related secret key, and observe the input-output behaviour of the device under the modified secret key. The theoretical treatment of such attacks was initiated by Bellare and Kohno [3], where the capability of adversaries is modeled by a class of tampering functions $\mathcal{T}$ on the secret key space. Tamperresilient security stipulates that the cryptographic schemes remain secure even for the adversary who has access to the schemes executed under the related keys $T(s k)$, with $T \in \mathcal{T}$ chosen by the adversary.

As observed by Gennaro et al. [21], it is impossible to achieve tamper-resilient security against any polynomial number of arbitrary tampering queries, without making further assumptions, such as key-updating or self-destruct mechanism ${ }^{1}$.

Leakage and Tamper-resilient public-key cryptography. In light of the fact that physical attacks in the real world include both passive and active attacks, Kalai et al. [26] initiate the study of designing public-key cryptographic schemes that are resilient to both leakage and tampering attacks.

Up to now, there are several models for leakage and tamper-resilient security. The first model is proposed by Kalai et al. [26] and considers continual tampering and leakage (i.e., the CTL model). This model provides a very strong security guarantee, but at the price of inevitably relying on key-updating or self-destruct mechanism. Kalai et al. [26] construct a signature scheme in the CTL model using a true-simulation extractable non-interactive zero-knowledge (tSE-NIZK)

[^0]proof system [12] as a building block. As shown in [12], tSE-NIZK can be built generically from a chosen-ciphertext attack (CCA) secure public-key encryption (PKE) and a regular NIZK. However, even using the efficient Groth-Sahai NIZK [22], it would lead to a tSE-NIZK with proof consisting of at least 20 group elements, and so does the signature of the resulting signature scheme. Kalai et al. [26] also present a PKE scheme with chosen-plaintext attack (CPA) secure in the CTL model, meaning that the adversary is not allowed to observe the effect of tampering on the decryption oracle. Fujisaki et al. [18] further investigate how to construct CCA-secure PKE in the CTL model, and present a scheme based on the one-time lossy filter technique [33]. The ciphertext of their PKE scheme consists of about 8 group elements.

The second model is introduced by Damgård et al. [10] and considers both bounded leakage and bounded tampering (i.e., the BLT model). Here bounded tampering means that the adversary is only allowed to make a limited number of tampering queries, and consequently, it does not need key-updating or selfdestruct mechanisms. To achieve BLT security, they propose a novel approach which reduces tampering to leakage. The benefit of this approach is that it could achieve tampering-resilience against arbitrary function class $\mathcal{T}$. However, the approach suffers from two disadvantages, one being that the amount of leakage tolerated by the leakage-resilience is largely decreasing, and the other being that for PKE it does not allow "post-challenge" tampering queries ${ }^{2}$. Under this approach, Damgård et al. [10] propose a signature scheme from $\Sigma$-protocol via the Fiat-Shamir heuristic [17] in the random oracle model and a CCA-secure PKE scheme from tSE-NIZK [12]. Faonio et al. [15] also follow the approach, and prove that the leakage-resilient signature scheme in [12] and the leakageresilient CCA-secure PKE scheme in [33] are secure in the BLT model. However, the signature scheme also uses tSE-NIZK, and its signature consists of more than 34 group elements. Their PKE scheme avoids the use of NIZK, but the ciphertext is over composite order groups and has a length of more than 5000 bits at the 128 -bit security level, which corresponds to about 19 group elements in typical prime order groups (where each group element is about 256 bits).

The third model is formalized by Sun et al. [36] and is called the leakage and tampering-resilient (LTR) model. This model also considers bounded leakage, but for tampering, it allows an unbounded number of tampering queries, while the tampering functions are restricted in a predefined function class $\mathcal{T}$, the same as the tampering-resilient security introduced by Bellare and Kohno [3]. Similar to the BLT model, the LTR model does not need key-updating or self-destruct mechanisms, and not only that, it also allows "post-challenge" tampering queries for PKE. Subsequently, Sun et al. [35] strengthen the LTR model to the strong $L T R$ (sLTR) model, by imposing only minimal restrictions on the adversary's decryption queries. These two works $[36,35]$ focus on PKE, and construct CCAsecure PKE schemes from tSE-NIZK and new variants of hash proof systems [9] in the LTR model and the sLTR model, respectively. Their schemes achieve

[^1]tamper-resilience against affine function class. However, due to the inefficiency of tSE-NIZK, the ciphertext of their schemes would consist of at least 20 group elements. Accordingly, Sun et al. [35] leave the construction of CCA-secure PKE in the sLTR model without using $t S E-N I Z K$ as an interesting future work.

The fourth model is due to Chakraborty and Rangan [7] and extends the BLT model in the presence of split-state mechanism ${ }^{3}$. This model is called the post-challenge $B L T$ ( $p c B L T$ ) model, since it serves as an alternative way to make "post-challenge" tampering (and also leakage) queries for PKE possible. Chakraborty and Rangan [7] also focus on PKE and construct a CCA-secure PKE scheme from tSE-NIZK in the pcBLT model. Similarly, the ciphertext of their scheme would consist of at least 20 group elements.

There are also other models such as the line of research which protects cryptosystems against leakage and tampering attacks by leveraging (leakage-resilient) non-malleable codes $[13,30,16,25]$. However, these works usually rely on hardware requirements such as key-updating, self-destruct or split-state mechanisms, and the proposed schemes are more like feasibility results and less efficient.

Our Contributions. In this work, we study the design of efficient signature and PKE schemes in the sLTR model, without using tSE-NIZK (or other heavy building blocks). Our contributions are three-fold.

- We formalize the strong LTR (sLTR) model for signature schemes, as a counterpart to the sLTR model for PKE introduced in [35]. Here "strong" means the strong existential unforgeability of signatures, which even guarantees that the adversary cannot forge a new signature for an already signed message. Moreover, for the adversary to win, we impose only minimal restrictions on the forgery produced by the adversary, thus our security provides a very strong guarantee (see Remark 1 for more discussions).
- We give direct constructions of signature and CCA-secure PKE schemes in the sLTR model. Both of the schemes are designed in the standard model, over asymmetric pairing groups and without using tSE-NIZK, thus accomplishing the interesting future work left by Sun et al. [35].

Both of our schemes are proven secure based on the standard matrix decisional Diffie-Hellman (MDDH) assumptions [14], which cover the standard symmetric external DH (SXDH) ${ }^{4}$ and $k$-Linear assumptions. Our signature scheme achieves leakage-resilience with leakage rate ${ }^{5} \frac{1}{4}-o(1)$ and our PKE scheme with leakage rate $\frac{1}{3}-o(1)$. Both of our schemes achieve tamperresilience against affine function class, the same as the existing schemes $[36,35]$ in the (s)LTR model.

[^2]Our SXDH-based schemes are more efficient than the existing schemes in the leakage and tamper-resilient setting (i.e., no matter in the CTL, BLT, LTR, sLTR, or pcBLT model) [26, 18, 10, 15, 36, 35, 7]. More precisely, our signature scheme has only 4 group elements in the signature, which is about $5 \times \sim 8 \times$ shorter, and our PKE scheme has only 6 group elements in the ciphertext, which is about $1.3 \times \sim 3.3 \times$ shorter. We refer to Remark 2 and Remark 4 for a detailed efficiency analysis of our schemes.

- To our best knowledge, our signature scheme is the first one achieving strong existential unforgeability in the leakage and tamper-resilient setting. We note that strong existential unforgeability has important applications in building more complex primitives such as signcryption [2] and authenticated key exchange (AKE) [11], where it can help signcryption to achieve ciphertext integrity [4] and AKE to achieve strong notion of "matching conversations" security [5]. We also stress that the Generalized Boneh-Shen-Waters (GBSW) transform [34], which converts a (non-strongly) secure signature scheme to a strongly secure one with the help of chameleon hash, does not work in the presence of leakage and tampering. The reason is, the resulting signature scheme contains the trapdoor of chameleon hash in its secret key, thus the leakage and tampering of secret key means the leakage and tampering of trapdoor, which is not supported by the security of chameleon hash.


## 2 Preliminaries

Notations. Let $\lambda \in \mathbb{N}$ denote the security parameter throughout the paper, and all algorithms, distributions, functions and adversaries take $1^{\lambda}$ as an implicit input. If $x$ is defined by $y$ or the value of $y$ is assigned to $x$, we write $x:=y$. For a set $\mathcal{X}$, denote by $x \leftarrow \mathcal{X}$ the procedure of sampling $x$ from $\mathcal{X}$ uniformly at random. If $\mathcal{D}$ is distribution, $x \leftarrow \mathcal{D}$ means that $x$ is sampled according to $\mathcal{D}$. All our algorithms are probabilistic unless stated otherwise. We use $y \leftarrow \mathcal{A}(x)$ to define the random variable $y$ obtained by executing algorithm $\mathcal{A}$ on input $x$. If $\mathcal{A}$ is deterministic we write $y \leftarrow \mathcal{A}(x)$. "PPT" abbreviates probabilistic polynomial-time. Denote by negl some negligible function. By $\operatorname{Pr}_{i}[\cdot]$ we denote the probability of a particular event occurring in game $\mathrm{G}_{i}$.

For two random variables $X$ and $Y$, the min-entropy of $X$ is defined as $\mathbf{H}_{\infty}(X):=-\log \left(\max _{x} \operatorname{Pr}[X=x]\right)$, and the statistical distance between $X$ and $Y$ is defined as $\Delta(X, Y):=\frac{1}{2} \cdot \sum_{x}|\operatorname{Pr}[X=x]-\operatorname{Pr}[Y=x]|$.
Lemma 1 (Leftover Hash Lemma [24]). Let $\mathcal{H}=\{H: \mathcal{X} \rightarrow \mathcal{Y}\}$ be a family of universal hash functions, i.e., for any $x_{1} \neq x_{2} \in \mathcal{X}, \operatorname{Pr}\left[H\left(x_{1}\right)=H\left(x_{2}\right)\right] \leq$ $1 /|\mathcal{Y}|$, where $H \leftarrow \mathcal{H}$. Then for any random variable $X$ on $\mathcal{X}$, it holds that $\Delta((H, H(X)),(H, U)) \leq \sqrt{|\mathcal{Y}| \cdot 2^{-\mathbf{H}_{\infty}(X)}}$, where $H \leftarrow \mathcal{H}$ and $U \leftarrow \mathcal{Y}$.

### 2.1 Digital Signatures

Definition 1 (SIG). A digital signature (SIG) scheme SIG = (Setup, Gen, Sign, Vrfy) with message space $\mathcal{M}$ consists of four PPT algorithms:
$-\mathrm{pp} \leftarrow{ }_{\odot}$ Setup: The setup algorithm outputs a public parameter pp , which serves as an implicit input of other algorithms.
$-(v k, s k) \leftarrow{ }^{\circ} \mathrm{Gen}(\mathrm{pp}):$ Taking pp as input, the key generation algorithm outputs a pair of verification key and signing key $(v k, s k)$.
$-\sigma \leftarrow \operatorname{Sign}(s k, m):$ Taking as input a signing key sk and a message $m \in \mathcal{M}$, the signing algorithm outputs a signature $\sigma$.
$-0 / 1 \leftarrow \operatorname{Vrfy}(v k, m, \sigma):$ Taking as input a verification key $v k$, a message $m \in$ $\mathcal{M}$ and a signature $\sigma$, the deterministic verification algorithm outputs a bit indicating whether $\sigma$ is a valid signature for $m$ w.r.t. vk.

Correctness requires that for all $\mathrm{pp} \leftarrow \leftarrow_{\text {s }}$ Setup, $(v k, s k) \leftarrow{ }_{\$} \operatorname{Gen}(\mathrm{pp})$ and $m \in \mathcal{M}$, it holds that $\operatorname{Pr}[\sigma \leftarrow \mathrm{Sign}(s k, m): \operatorname{Vrfy}(v k, m, \sigma)=1] \geq 1-\operatorname{negl}(\lambda)$.

### 2.2 Public-Key Encryption

Definition 2 (PKE). A public-key encryption (PKE) scheme PKE = (Setup, Gen, Enc, Dec) with message space $\mathcal{M}$ consists of four PPT algorithms:
$-\mathrm{pp} \leftarrow_{\$}$ Setup: The setup algorithm outputs a public parameter pp , which serves as an implicit input of other algorithms.
$-(p k, s k) \leftarrow \mathrm{Gen}^{\mathrm{G}}(\mathrm{pp}):$ Taking pp as input, the key generation algorithm outputs a pair of public key and secret key ( $p k, s k$ ).
$-c t \leftarrow_{s} \operatorname{Enc}(p k, m):$ Taking as input a public key $p k$ and a message $m \in \mathcal{M}$, the encryption algorithm outputs a ciphertext ct.
$-m / \perp \leftarrow \operatorname{Dec}(s k, c t):$ Taking as input a secret key sk and a ciphertext ct, the deterministic decryption algorithm outputs either a message $m \in \mathcal{M}$ or a special symbol $\perp$ indicating the failure of decryption.

Correctness requires that for all $\mathrm{pp} \leftarrow \leftarrow_{\mathrm{s}} \operatorname{Setup},(p k, s k) \leftarrow \leftarrow_{\mathrm{Gen}}(\mathrm{pp})$ and $m \in \mathcal{M}$, it holds that $\operatorname{Pr}[c t \leftarrow \& \operatorname{Enc}(p k, m): \operatorname{Dec}(s k, c t)=m] \geq 1-\operatorname{negl}(\lambda)$.

### 2.3 Collision-Resistant Hash Functions

Definition 3 (Collision-resistant hash functions). A family of hash functions $\mathcal{H}$ is collision-resistant, if for any PPT adversary $\mathcal{A}$, it holds that
$\operatorname{Adv}_{\mathcal{H}, \mathcal{A}}^{\mathrm{cr}}(\lambda):=\operatorname{Pr}\left[H \leftarrow \& \mathcal{H},\left(x_{1}, x_{2}\right) \leftarrow \mathcal{A}(H): x_{1} \neq x_{2} \wedge H\left(x_{1}\right)=H\left(x_{2}\right)\right] \leq \operatorname{neg}(\lambda)$.

### 2.4 Pairing Groups and MDDH Assumptions

Let PGGen be a PPT algorithm outputting a description of pairing group gpar = $\left(\mathbb{G}_{1}, \mathbb{G}_{2}, \mathbb{G}_{T}, p, e, P_{1}, P_{2}, P_{T}\right)$, where $\mathbb{G}_{1}, \mathbb{G}_{2}$ and $\mathbb{G}_{T}$ are additive cyclic groups of prime order $p>2^{2 \lambda}, e: \mathbb{G}_{1} \times \mathbb{G}_{2} \longrightarrow \mathbb{G}_{T}$ is a non-degenerated bilinear pairing, and $P_{1}, P_{2}, P_{T}$ are generators of $\mathbb{G}_{1}, \mathbb{G}_{2}, \mathbb{G}_{T}$, respectively, with $P_{T}:=e\left(P_{1}, P_{2}\right)$. We assume that the operations in $\mathbb{G}_{1}, \mathbb{G}_{2}, \mathbb{G}_{T}$ and the pairing $e$ are efficiently computable. We consider Type-III asymmetric pairing group, where $\mathbb{G}_{1} \neq \mathbb{G}_{2}$
and there is no efficient homomorphism between them. We require gpar to be an implicit input of other algorithms.

We use implicit representation of group elements as in [14]. For $s \in\{1,2, T\}$ and $a \in \mathbb{Z}_{p}$, denote by $[a]_{s}=a P_{s} \in \mathbb{G}_{s}$ as the implicit representation of $a$ in $\mathbb{G}_{s}$. Similarly, for a matrix $\mathbf{A}=\left(a_{i, j}\right) \in \mathbb{Z}_{p}^{n \times m}$ we define $[\mathbf{A}]_{s}$ as the implicit representation of $\mathbf{A}$ in $\mathbb{G}_{s}$. $\operatorname{Span}(\mathbf{A}):=\left\{\mathbf{A r} \mid \mathbf{r} \in \mathbb{Z}_{p}^{m}\right\} \subseteq \mathbb{Z}_{p}^{n}$ denotes the linear span of $\mathbf{A}$, and similarly $\operatorname{Span}\left([\mathbf{A}]_{s}\right):=\left\{[\mathbf{A r}]_{s} \mid \mathbf{r} \in \mathbb{Z}_{p}^{m}\right\} \subseteq \mathbb{G}_{s}^{n}$. Note that given $\mathbf{A},[\mathbf{B}]_{s},[\mathbf{C}]_{s}$ and $\mathbf{D}$ with matching dimensions, one can efficiently compute $[\mathbf{A B}]_{s},[\mathbf{B}+\mathbf{C}]_{s},[\mathbf{C D}]_{s}$, and given $[\mathbf{A}]_{1}$ and $[\mathbf{B}]_{2}$, we let $e\left([\mathbf{A}]_{1},[\mathbf{B}]_{2}\right):=[\mathbf{A B}]_{T}$.

Let $\ell, k \in \mathbb{N}$ be integers with $\ell>k$. A probabilistic distribution $\mathcal{D}_{\ell, k}$ is called a matrix distribution, if it outputs matrices in $\mathbb{Z}_{p}^{\ell \times k}$ of full rank $k$ in polynomial time. Without loss of generality, we assume that the first $k$ rows of $\mathbf{A} \leftarrow{ }_{\$} \mathcal{D}_{\ell, k}$ form an invertible matrix. Let $\mathcal{D}_{k}:=\mathcal{D}_{k+1, k}$. Denote by $\mathcal{U}_{\ell, k}$ the uniform distribution over all matrices in $\mathbb{Z}_{p}^{\ell \times k}$. Let $\mathcal{U}_{k}:=\mathcal{U}_{k+1, k}$.
Definition 4 ( $\mathcal{D}_{\ell, k}$-MDDH Assumption). Let $s \in\{1,2\}$. The $\mathcal{D}_{\ell, k}-M D D H$ assumption holds over group $\mathbb{G}_{s}$, if for any PPT adversary $\mathcal{A}$, it holds that $\operatorname{Adv}_{\mathcal{D}_{\ell, k}, \mathbb{G}_{s}, \mathcal{A}}^{\mathrm{mddh}}(\lambda):=\left|\operatorname{Pr}\left[\mathcal{A}\left([\mathbf{A}]_{s},[\mathbf{A w}]_{s}\right)=1\right]-\operatorname{Pr}\left[\mathcal{A}\left([\mathbf{A}]_{s},[\mathbf{u}]_{s}\right)=1\right]\right| \leq \operatorname{negl}(\lambda)$, where the probability is over $\mathbf{A} \leftarrow{ }_{\delta} \mathcal{D}_{\ell, k}, \mathbf{w} \leftarrow s \mathbb{Z}_{p}^{k}$ and $\mathbf{u} \leftarrow s \mathbb{Z}_{p}^{\ell}$.

MDDH assumption covers many well-studied assumptions, such as the DDH and the $k$-Linear ( $k$-LIN) assumptions, by specifying the matrix distribution as $\mathcal{L I N}_{1}$ and $\mathcal{L I}^{\prime} \mathcal{N}_{k}$ respectively [14], where $\mathcal{L I} \mathcal{N}_{k}: \quad \mathbf{A}=\left(\begin{array}{llll}a_{1} & & \\ & \ddots & \\ & & & \\ 1 & \cdots & 1\end{array}\right) \in \mathbb{Z}_{p}^{(k+1) \times k}$. MDDH also covers the standard symmetric external DH (SXDH) assumption, which simply requires the DDH assumption to hold both in $\mathbb{G}_{1}$ and $\mathbb{G}_{2}$.

Several relations among MDDH assumptions parameterized by different matrix distributions were established in [14, 20].

Lemma 2 ( $\mathcal{D}_{\ell, k}$ - MDDH $\Rightarrow \mathcal{U}_{k}$-MDDH [14] $\Rightarrow \mathcal{U}_{\ell^{\prime}, k}$-MDDH [20]). For any PPT adversary $\mathcal{A}$, there exists a PPT B s.t. $\operatorname{Adv}_{\mathcal{U}_{k}, \mathbb{G}_{s}, \mathcal{A}}^{\text {mddh }}(\lambda) \leq \operatorname{Adv}_{\mathcal{D}_{\ell, k}, \mathbb{G}_{s}, \mathcal{B}}^{m d d h}(\lambda)$.

For any PPT $\mathcal{A}$, there exists a PPT $\mathcal{B}$ s.t. $\operatorname{Adv}_{\mathcal{U}_{\ell^{\prime}, k}, \mathbb{G}_{s}, \mathcal{A}}^{\operatorname{mddh}}(\lambda) \leq \operatorname{Adv}_{\mathcal{U}_{k}, \mathbb{G}_{s}, \mathcal{B}}^{m \operatorname{ddt}}(\lambda)$.
Consequently, for any $\ell>k, \mathcal{U}_{\ell, k}-\mathrm{MDDH}$ assumption is tightly implied by the $k$-LIN assumption (i.e., $\mathcal{L I} \mathcal{N}_{k}$-MDDH).

We also define the $\mathcal{D}_{\ell, k}$-Kernel Matrix $\mathrm{DH}\left(\mathcal{D}_{\ell, k}\right.$-KerMDH) assumption according to [31] which is a natural search variant of the $\mathcal{D}_{\ell, k}$ - MDDH assumption.

Definition 5 ( $\mathcal{D}_{\ell, k}$-KerMDH Assumption). Let $s \in\{1,2\}$. The $\mathcal{D}_{\ell, k}-K e r M D H$ assumption holds over group $\mathbb{G}_{s}$, if for any PPT adversary $\mathcal{A}$, it holds that $\operatorname{Adv}_{\mathcal{D}_{\ell, k}, \mathbb{G}_{s}, \mathcal{A}}^{\mathrm{kmd}}(\lambda):=\operatorname{Pr}\left[[\mathbf{x}]_{3-s} \in \mathbb{G}_{3-s}^{\ell} \leftarrow s \mathcal{A}\left([\mathbf{A}]_{s}\right): \mathbf{x}^{\top} \mathbf{A}=\mathbf{0} \wedge \mathbf{x} \neq \mathbf{0}\right] \leq$ $\operatorname{negl}(\lambda)$, where the probability is over $\mathbf{A} \leftarrow \mathcal{D}_{\ell, k}$.

The following lemma shows that the $\mathcal{D}_{\ell, k}$-KerMDH assumption is implied by the $\mathcal{D}_{\ell, k}$ - MDDH assumption, since one can use a non-zero $[\mathbf{x}]_{3-s}$ satisfying $\mathbf{x}^{\top} \mathbf{A}=\mathbf{0}$ to test membership in Span $\left([\mathbf{A}]_{S}\right)$.

Lemma 3 ( $\mathcal{D}_{\ell, k}$ - MDDH $\Rightarrow \mathcal{D}_{\ell, k}$-KerMDH [31]). For any PPT adversary $\mathcal{A}$, there exists a PPT $\mathcal{B}$ s.t. $\operatorname{Adv}_{\mathcal{D}_{\ell, k}, \mathbb{G}_{s}, \mathcal{A}}^{\mathrm{kmdh}^{\prime}}(\lambda) \leq \operatorname{Adv}_{\mathcal{D}_{\ell, k}, \mathbb{G}_{s}, \mathcal{B}}^{\text {mddh }}(\lambda)+1 /(p-1)$.

## 3 More Efficient SIG with Leakage and Tamper-Resilience

In this section, we present a direct and efficient construction of signature scheme with leakage and tamper-resilience, over asymmetric pairing groups based on the MDDH assumptions.

Concretely, in Subsect. 3.1, we formalize the leakage and tamper-resilient security for signature schemes, i.e., the strong LTR-CMA (sLTR-CMA) security, and then in Subsect. 3.2 and Subsect. 3.3, we present our signature scheme and its security proof, respectively.

### 3.1 Definition of sLTR-CMA Security

The standard security notion for signatures is existential unforgeability under chosen-message attacks (EUF-CMA). Here we extend it to ( $\kappa, \mathcal{T}$ )-sLTR-CMA, parameterized by an integer $\kappa$ and a function set $\mathcal{T}$ : it additionally considers leakages attacks, where the total amount of leakage is bounded by $\kappa$ bits, and tampering attacks, where the tampering functions are chosen from $\mathcal{T}$. Moreover, it provides strong existential unforgeability which further guarantees that the adversary cannot even forge a new signature for a message that it has ever queried. Below we present the formal definition of $(\kappa, \mathcal{T})$-sLTR-CMA security.

Definition 6 (sLTR-CMA Security for SIG). Let $\kappa=\kappa(\lambda) \in \mathbb{N}$, and $\mathcal{T}$ be a set of functions from $\mathcal{S K}$ to $\mathcal{S K}$ where $\mathcal{S K}$ is the secret key space. A signature scheme $\mathrm{SIG}=($ Setup, Gen, Sign, Vrfy$)$ is $(\kappa, \mathcal{T})$-sLTR-CMA secure, if for any PPT adversary $\mathcal{A}$, it holds that $\operatorname{Adv}_{\operatorname{SIG}, \mathcal{A}, \kappa, \mathcal{T}}^{\mathrm{Str}-\mathrm{cma}}(\lambda):=\operatorname{Pr}\left[\operatorname{Exp}_{\mathrm{SIG}, \mathcal{A}, \kappa, \mathcal{T}}^{\mathrm{str}-\mathrm{cma}} \Rightarrow 1\right] \leq \operatorname{negl}(\lambda)$, where the experiment $\operatorname{Exp}_{\mathrm{SIG}, \mathcal{A}, \kappa, \mathcal{T}}^{\operatorname{slt}-\mathrm{T}}$ is defined in Fig. 1.

| Exp ${ }_{\text {SIG }, \mathcal{A}, \kappa, \mathcal{T}}^{\text {str-cma }}$ : | $\mathcal{O}_{\text {SIGN }}(T, m):$ |
| :---: | :---: |
| $\mathrm{pp} \leftarrow$ Setup, $(v k, s k) \leftarrow$ Gen $(\mathrm{pp})$ | If $T \notin \mathcal{T}$ : Return $\perp$ |
| $\mathcal{Q}_{\text {id }}:=\emptyset \quad / /$ Record the signing queries | $\sigma \leftarrow ¢ \operatorname{Sign}(T(s k), m)$ |
| // under the identity function | If $T=\mathrm{id}: \mathcal{Q}_{\text {id }}:=\mathcal{Q}_{\text {id }} \cup\{(m, \sigma)\}$ |
| $\ell:=0 \quad / /$ Record the leakage length | Return $\sigma$ |
| $\left(m^{*}, \sigma^{*}\right) \leftarrow ¢ \mathcal{A}^{\mathcal{O}_{\text {Sign }}(\cdot, \cdot), \mathcal{O}_{\text {Leak }}(\cdot)}(\mathrm{pp}, v k)$ | $\underline{\mathcal{O}_{\text {Leak }}(L): / / a t ~ m o s t ~} \kappa$ leakage bits |
| If $\left(\left(m^{*}, \sigma^{*}\right) \notin \mathcal{Q}_{\text {id }}\right) \wedge\left(\operatorname{Vrfy}\left(v k, m^{*}, \sigma^{*}\right)=1\right):$ | If $\ell+\|L(s k)\|>\kappa$ : Return $\perp$ |
| Return 1; | $\ell:=\ell+\|L(s k)\|$ |
| Else: Return 0 | Return $L(s k)$ |

Fig. 1. The $(\kappa, \mathcal{T})$-sLTR-CMA security experiment $\operatorname{Expsich}_{\text {SIG }, \mathcal{A}, \kappa, \mathcal{T}}^{\text {stra }}$ for SIG, where id denotes the identity function and $|L(s k)|$ denotes the bit-length of $L(s k)$.

Remark 1 (On the formalization of sLTR-CMA security). In the experiment $\operatorname{Exp} \underset{\mathrm{SIG}, \mathcal{A}, \kappa, \mathcal{T}}{\text { sItr-cma }}$ defined in Fig. 1, oracle $\mathcal{O}_{\text {SIGN }}$ captures the ability of the adversary to implement tampering attacks and obtain signatures under tampered signing keys $T(s k)$ with $T \in \mathcal{T}$, and oracle $\mathcal{O}_{\text {Leak }}$ captures the ability of the adversary to implement leakage attacks and obtain bounded leakage information $L(s k)$ about the signing key.

For the adversary to win, the condition $\left(m^{*}, \sigma^{*}\right) \notin \mathcal{Q}_{\text {id }}$ is the minimal restriction on the adversary's forgery, since otherwise the adversary can query $\mathcal{O}_{\text {SIGN }}\left(\right.$ id,$\left.m^{*}\right)$ for an arbitrary message $m^{*}$ to obtain a signature $\sigma^{*}$ and simply output ( $m^{*}, \sigma^{*}$ ) as the forgery, and as a result, the adversary would trivially win and it is impossible to achieve the above security.

If we replace the condition $\left(m^{*}, \sigma^{*}\right) \notin \mathcal{Q}_{\text {id }}$ with a stronger one, namely requir$\operatorname{ing} m^{*}$ to be different from all messages that the adversary has queried $\mathcal{O}_{\text {SIGN }}$, we call it (non-strong) LTR-CMA security with standard existential unforgeability. Furthermore, if $\mathcal{T}$ contains only the identity function id, we obtain the leakageresilience security, while if $\kappa=0$, we obtain the tamper-resilience security. If both $\mathcal{T}=\{i d\}$ and $\kappa=0$, we recover the standard EUF-CMA security.

### 3.2 Construction of SIG from MDDH

Now we present our direct construction of sLTR-CMA secure SIG scheme over asymmetric pairing groups based on the MDDH assumptions. Let $\mathcal{D}_{k}$ be a matrix distribution with $k \in \mathbb{N}$, and let $\mathcal{H}$ be a family of collision resistant hash functions from $\{0,1\}^{*}$ to $\mathbb{Z}_{p}$. Our SIG scheme SIG $=$ (Setup, Gen, Sign, Vrfy) is shown in Fig. 2, where the message space is $\mathcal{M}=\{0,1\}^{*}$ and the secret key space is $\mathcal{S K}=\mathbb{Z}_{p}^{(k+1) \times(k+1)}$. Correctness of SIG follows by inspection: for any honestly generated signature $\sigma=\left([\mathbf{c}]_{1},[\mathbf{d}]_{1}\right)$, we have $[\mathbf{c}]_{1}=[\mathbf{U}]_{1} \mathbf{w}$ with $\mathbf{w} \leftarrow \& \mathbb{Z}_{p}^{k}$ and $[\mathbf{d}]_{1}=\mathbf{K}[\mathbf{c}]_{1}+\left[\left(\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right) \mathbf{U}\right]_{1} \mathbf{w}=\left[\left(\mathbf{K}+\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right) \mathbf{c}\right]_{1}$, which directly implies $e\left(\left[\mathbf{c}^{\top}\right]_{1},\left[\left(\mathbf{K}^{\top}+\mathbf{K}_{0}^{\top}+\tau \mathbf{K}_{1}^{\top}\right) \mathbf{A}\right]_{2}\right)=e\left(\left[\mathbf{c}^{\top}\left(\mathbf{K}^{\top}+\mathbf{K}_{0}^{\top}+\tau \mathbf{K}_{1}^{\top}\right)\right]_{1},[\mathbf{A}]_{2}\right)=e\left(\left[\mathbf{d}^{\top}\right]_{1},[\mathbf{A}]_{2}\right)$.

Moreover, since $\mathbf{U}$ output by $\mathcal{D}_{k}$ is of full rank, $[\mathbf{c}]_{1}=[\mathbf{U}]_{1} \mathbf{w} \neq[\mathbf{0}]_{1}$ holds as long as $\mathbf{w} \neq \mathbf{0}$ holds, which happens with overwhelming probability $1-1 / p^{k}$.

Next, we show its ( $\kappa, \mathcal{T}_{\text {aff }}$ )-sLTR-CMA security under $\kappa \leq \log p-\Omega(\lambda)$ bits of leakage information and under the set of affine functions

$$
\begin{equation*}
\mathcal{T}_{\text {aff }}=\left\{T_{(a, \mathbf{B})}: \mathbf{K} \in \mathcal{S K} \mapsto a \mathbf{K}+\mathbf{B} \in \mathcal{S K} \mid a \in \mathbb{Z}_{p}, \mathbf{B} \in \mathcal{S K}\right\} . \tag{1}
\end{equation*}
$$

Theorem 1 ( $\left(\kappa, \mathcal{T}_{\text {aff }}\right)$-sLTR-CMA Security of SIG). Let $\kappa \leq \log p-\Omega(\lambda)$ and let $\mathcal{T}_{\text {aff }}$ be the set of affine functions defined in (1). Assume that the $\mathcal{D}_{k}-M D D H$ assumption holds over both $\mathbb{G}_{1}$ and $\mathbb{G}_{2}$, and $\mathcal{H}$ is collision-resistant. Then the SIG scheme in Fig. 2 is ( $\kappa, \mathcal{T}_{\text {aff }}$ )-sLTR-CMA secure.

Concretely, for any PPT adversary $\mathcal{A}$ who makes at most $Q$ times of $\mathcal{O}_{\text {SIGN }}$ queries, there exist PPT adversaries $\mathcal{B}_{1}, \cdots, \mathcal{B}_{5}$, such that

$$
\begin{aligned}
\operatorname{Adv}_{\text {SIG }, \mathcal{A}, \kappa, \mathcal{T}_{\text {aff }}^{\text {str-cma }}}(\lambda) \leq & \operatorname{Adv}_{\mathcal{D}_{k}, \mathbb{G}_{2}, \mathcal{B}_{1}}^{\mathrm{mddh}}(\lambda)+\operatorname{Adv}_{\mathcal{H}, \mathcal{B}_{2}}^{\text {cr }}(\lambda)+\operatorname{Adv}_{\mathcal{D}_{k}, \mathbb{G}_{2}, \mathcal{B}_{3}}^{\text {mddh }}(\lambda) \\
& +Q \cdot\left(\operatorname{Adv}_{\mathcal{D}_{k}, \mathbb{G}_{1}, \mathcal{B}_{4}}^{\text {mddh}}(\lambda)+\operatorname{Adv}_{\mathcal{D}_{k}, \mathbb{G}_{1}, \mathcal{B}_{5}}^{\text {mddh }}(\lambda)\right)+2^{-\Omega(\lambda)} .
\end{aligned}
$$



Fig. 2. Construction of SIG $=$ (Setup, Gen, Sign, Vrfy) based on MDDH, where the framed boxes and the gray boxes are used to help explain the intuitions behind the construction in Remark 3.

The proof of Theorem 1 is postponed to Subsect. 3.3. Before presenting the formal proof, we give a detailed efficiency analysis and explain the main intuitions of our SIG construction in the following two remarks, respectively.

Remark 2 (Efficiency of our SIG). Let $x \cdot \mathbb{G}$ denote $x$ elements in a group $\mathbb{G}$. Our SIG scheme in Fig. 2 is parameterized by the MDDH parameter $k \in \mathbb{N}$, and has public parameter $\mathrm{pp}:\left(3 k^{2}+3 k\right) \cdot \mathbb{G}_{1}+\left(3 k^{2}+3 k\right) \cdot \mathbb{G}_{2}$, verification key $v k:\left(k^{2}+k\right) \cdot \mathbb{G}_{2}$, signing key $s k:\left(k^{2}+2 k+1\right) \cdot \mathbb{Z}_{p}$ and signature $\sigma:(2 k+2) \cdot \mathbb{G}_{1}$. The verification involves $\left(2 k^{2}+2 k\right)$ pairing operations.

For $k=1$, we get an efficient SIG scheme with pp : $6 \cdot \mathbb{G}_{1}+6 \cdot \mathbb{G}_{2}$, verification key $v k: 2 \cdot \mathbb{G}_{2}$, signing key $s k: 4 \cdot \mathbb{Z}_{p}$ and signature $\sigma: 4 \cdot \mathbb{G}_{1}$, and the verification involves only 4 pairing operations. The resulting SIG scheme is ( $\kappa, \mathcal{T}_{\text {aff }}$ )-sLTR-CMA secure based on the standard SXDH assumption, and supports $\kappa=\log p-\Omega(\lambda)$ bits key leakage. The leakage rate (i.e., $\kappa /$ bit-length of $s k)$ is $\frac{\log p-\Omega(\lambda)}{4 \log p}=\frac{1}{4}-o(1)$ asymptotically as $p$ grows.

Remark 3 (Intuitions of our SIG). On a high level, our SIG in Fig. 2 can be parsed as two components: the terms in framed boxes (which are related to $\mathbf{K}$ ) and the terms in gray boxes (which are related to $\mathbf{K}_{0}$ and $\mathbf{K}_{1}$ ).

Our first idea is to let $s k=\mathbf{K}$ involve only term of the first component. With such a design, to achieve sLTR-CMA security, we only need to analyze the first component in the leakage and tampering-resilient setting, while for the second component we can analyze it without being disturbed by the leakage and tampering attacks on it.

Our second idea is to integrate the two components carefully during the generation (and verification) of signatures, such that the terms $\left[\left(\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right) \mathbf{U}\right]_{1} \mathbf{w}$ in the second component can trigger randomness of certain forms to hide (partial information of) the terms $\mathbf{K}[\mathbf{c}]_{1}$ in the first component, so that the signatures generated under tampered signing keys do not leak much information about $s k=\mathbf{K}$ beyond $v k$ to the adversary in the sLTR-CMA security experiment. Consequently, the signing oracle is of no use to the adversary, and the sLTR-CMA security of our SIG essentially reduces to the security against no-message attacks (i.e., where the adversary obtains no signatures) in the key leakage setting, which is much easier to achieve and is mainly guaranteed by the first component.

Below we explain the intuitions behind these two components in more detail.
Intuitions behind The First Component. Intuitively, the terms in framed boxes can be viewed as a publicly verifiable function on $\mathbb{G}_{1}^{k+1}$ :

- the function is defined by $s k=\mathbf{K}$, and it maps $[\mathbf{c}]_{1} \in \mathbb{G}_{1}^{k+1}$ to $\mathbf{K}[\mathbf{c}]_{1}$;
- given $v k=\left[\mathbf{K}^{\top} \mathbf{A}\right]_{2}$, one can verify the correctness of function value

$$
\begin{equation*}
[\mathbf{d}]_{1}=\mathbf{K}[\mathbf{c}]_{1} \tag{2}
\end{equation*}
$$

publicly via pairing equations:

$$
\begin{equation*}
e\left(\left[\mathbf{c}^{\top}\right]_{1},\left[\mathbf{K}^{\top} \mathbf{A}\right]_{2}\right)=e\left(\left[\mathbf{d}^{\top}\right]_{1},[\mathbf{A}]_{2}\right) . \tag{3}
\end{equation*}
$$

Observe that (2) and (3) are equivalent under the $\mathcal{D}_{k}$ - KerMDH assumption on $[\mathbf{A}]_{2}$ (which is further implied by the $\mathcal{D}_{k}-\mathrm{MDDH}$ assumption according to Lemma 3), since otherwise $\left[\mathbf{c}^{\top} \mathbf{K}^{\top}-\mathbf{d}^{\top}\right]_{1}$ constitutes a non-zero vector in the kernel of $[\mathbf{A}]_{2}$, which is hard to find under the $\mathcal{D}_{k}$-KerMDH assumption.

This publicly verifiable function enjoys a useful property:

- in the presence of only $v k=\left[\mathbf{K}^{\top} \mathbf{A}\right]_{2}$, the function value $\mathbf{K}[\mathbf{c}]_{1}$ of any $[\mathbf{c}]_{1} \neq[\mathbf{0}]_{1}$ retains enough entropy from $\mathbf{K}$, so that it is information-theoretically hard to produce $\left([\mathbf{c}]_{1},[\mathbf{d}]_{1}\right)$ satisfying (2) (and thus computationally hard to satisfy (3) under MDDH assumption).

To see why this property holds more concretely, we can let $\mathbf{a}^{\perp} \in \mathbb{Z}_{p}^{k+1}$ be a nonzero vector in the kernel of $\mathbf{A} \in \mathbb{Z}_{p}^{(k+1) \times k}$ such that $\left(\mathbf{a}^{\perp}\right)^{\top} \mathbf{A}=\mathbf{0}$, and sample $s k=\mathbf{K} \leftarrow_{s} \mathbb{Z}_{p}^{(k+1) \times(k+1)}$ equivalently via
where $\widetilde{\mathbf{K}} \leftarrow \& \mathbb{Z}_{p}^{(k+1) \times(k+1)}$ and $\mathbf{k} \leftarrow{ }_{\mathrm{s}} \mathbb{Z}_{p}^{k+1}$. On the one hand, note that $\mathbf{k}$ is completely hidden in $v k$ since $v k=\left[\mathbf{K}^{\top} \mathbf{A}\right]_{2}=\left[\left(\widetilde{\mathbf{K}}^{\top}+\stackrel{\ulcorner }{\mathbf{k}}\left(\mathbf{a}^{\perp}\right)^{\top}\right) \mathbf{A}\right]_{2}=\left[\tilde{\mathbf{K}}^{\top} \mathbf{A}\right]_{2}$. On
the other hand, for any $[\mathbf{c}]_{1} \neq[\mathbf{0}]_{1}$, its function value is

$$
\mathbf{K}[\mathbf{c}]_{1}=\left(\widetilde{\mathbf{K}}+\mathbf{a}^{\perp} \mathbf{k}^{\top}\right)[\mathbf{c}]_{1}=\widetilde{\mathbf{K}}[\mathbf{c}]_{1}+\left[\begin{array}{c}
{\left[\mathbf{a}^{\perp}\left(\mathbf{k}^{\top} \mathbf{c}\right)\right.}
\end{array}\right]_{1}
$$

 has $\log p$ bits of entropy conditioned on $v k$, as shown by the term ${ }^{\ulcorner } \mathbf{a}^{\perp}\left(\mathbf{k}^{\top} \mathbf{c}\right)$, and consequently it is hard to produce $\left([\mathbf{c}]_{1},[\mathbf{d}]_{1}\right)$ satisfying (2) and $(\overline{3})$.

Insufficiency of The First Component and Arising of The Second. The first component and the aforementioned useful property serve as the basis for the security of our SIG. In particular, if the adversary $\mathcal{A}$ does not obtain any signatures in the security experiment, then it is hard for $\mathcal{A}$ to forge a signature satisfying (3), since the function value $\mathbf{K}[\mathbf{c}]_{1}$ has enough entropy (i.e., $\log p$ bits entropy) conditioned on $v k$. Moreover, the argument holds even if the adversary obtains bounded leakage information about $s k=\mathbf{K}$, as long as the amount of leakage $\kappa$ satisfies $\log p-\kappa \geq \Omega(\lambda)$ so that there are still $\log p-\kappa \geq \Omega(\lambda)$ bits entropy left in $\mathbf{K}[\mathbf{c}]_{1}$. This shows the security against no-message attacks in the leakage setting of our SIG.

However, in the sLTR-CMA security experiment, $\mathcal{A}$ can obtain signatures as many as it wants, under tampered signing keys $T_{(a, \mathbf{B})}(s k)=a \mathbf{K}+\mathbf{B}$. So $\mathcal{A}$ will obtain multiple $(a \mathbf{K}+\mathbf{B})[\mathbf{c}]_{1}$ contained in the signatures $\sigma=\left([\mathbf{c}]_{1},[\mathbf{d}]_{1}\right)$, which would leak additional information about $s k=\mathbf{K}$ beyond $v k$.

To rescue the above arguments, we resort to the terms in gray boxes . Roughly speaking, we use $\left[\left(\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right) \mathbf{U}\right]_{1} \mathbf{w}$ to hide (partial information of) $(a \mathbf{K}+\mathbf{B})[\mathbf{c}]_{1}$ in the generation of $[\mathbf{d}]_{1}$ :

$$
\begin{equation*}
[\mathbf{d}]_{1}=(a \mathbf{K}+\mathbf{B})[\mathbf{c}]_{1}+\left[\left(\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right) \mathbf{U}\right]_{1} \mathbf{w}, \tag{4}
\end{equation*}
$$

so that $\mathcal{A}$ will not learn much information about $s k=\mathbf{K}$ beyond $v k$ from the obtained signatures, and then we can use the above arguments to show the security of our SIG.

More Explanations about The Second Component. It remains to give the intuitions of the terms in gray boxes in more detail, and in particular, explain how $\left[\left(\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right) \mathbf{U}\right]_{1} \mathbf{w}$ hide $(a \mathbf{K}+\mathbf{B})[\mathbf{c}]_{1}$ in the generation of $[\mathbf{d}]_{1}$ in (4).

From a high-level perspective, the terms in gray boxes can be viewed as the one-time simulation-sound (OTSS) NIZK scheme proposed by Kiltz and Wee [27, Section 3.3], and they essentially prove that $[\mathbf{c}]_{1}=[\mathbf{U}]_{1} \mathbf{w}$ belongs to the linear subspace $\operatorname{Span}\left([\mathbf{U}]_{1}\right)$ : in the signing algorithm Sign of our SIG, the term $\left[\left(\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right) \mathbf{U}\right]_{1} \mathbf{w}$ corresponds to the generation of OTSS-NIZK proof; in the
verification algorithm Vrfy, the term $e\left(\left[\mathbf{c}^{\top}\right]_{1},\left[\left(\mathbf{K}_{0}^{\top}+\tau \mathbf{K}_{1}^{\top}\right) \mathbf{A}\right]_{2}\right)$ corresponds to the verification of OTSS-NIZK proof.

- On the one hand, the generation and verification of OTSS-NIZK proofs do not involve any secret key, so they do not introduce additional elements to $s k$. This is very helpful in the key leakage and tampering-resilient setting, since the leakage and tampering of $s k$ do not affect the terms in gray boxes, and we can use properties of this component without the need of considering any leakage and tampering.
- However, the OTSS property is insufficient for our purpose, since in the security experiment of SIG, the adversary can obtain multiple NIZK proofs $\left[\left(\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right) \mathbf{U}\right]_{1} \mathbf{w}$ contained in the multiple signatures $\sigma=\left([\mathbf{c}]_{1},[\mathbf{d}]_{1}\right)$, rather than a single NIZK proof allowed in the OTSS property.

Instead, we resort to another property about the second component $\left[\left(\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right) \mathbf{U}\right]_{1} \mathbf{w}$, namely it can trigger randomness of certain forms in a computationally indistinguishable way, as observed in [27]. To be more concrete, we can prove that the multiple pairs of

$$
\left([\mathbf{c}]_{1}=[\mathbf{U}]_{1} \mathbf{w}, \quad\left[\left(\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right) \mathbf{U}\right]_{1} \mathbf{w}\right)
$$

contained in the signatures that $\mathcal{A}$ obtains are computationally indistinguishable from

$$
\begin{equation*}
([\mathbf{c}]_{1}=[\mathbf{U}]_{1} \mathbf{w}, \quad\left[\left(\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right) \mathbf{U}\right]_{1} \mathbf{w}+[_{[\underbrace{}_{-}}^{\left[\gamma \mathbf{a}^{\perp}\right]_{1}^{\prime}}{ }_{1}^{\prime}), \tag{5}
\end{equation*}
$$

where $\gamma \leftarrow \mathbb{\mathbb { Z }} \mathbb{Z}_{p}$ are randomnesses independently chosen for each pair, and $\mathbf{a}^{\perp} \in$ $\mathbb{Z}_{p}^{k+1}$ is a non-zero vector in the kernel of $\mathbf{A} \in \mathbb{Z}_{p}^{(k+1) \times k}$ such that $\left(\mathbf{a}^{\perp}\right)^{\top} \mathbf{A}=\mathbf{0}$, even conditioned on a single pair

$$
\left(\left[\mathbf{c}^{*}\right]_{1}, \quad\left[\left(\mathbf{K}_{0}+\tau^{*} \mathbf{K}_{1}\right) \mathbf{c}^{*}\right]_{1}\right)
$$

contained in $\mathcal{A}$ 's forgery $\left(m^{*}, \sigma^{*}=\left(\left[\mathbf{c}^{*}\right]_{1},\left[\mathbf{d}^{*}\right]_{1}\right)\right)$ in the case of $\tau^{*} \neq \tau$. Jumping ahead, this corresponds to the game sequence $\left\{\mathrm{G}_{4 . \eta .0}-\mathrm{G}_{4 . \eta .4}\right\}_{0 \leq \eta \leq Q-1}$ and $\mathrm{G}_{4 . Q .0}$ in our security proof in Subsect. 3.3. This property is different from OTSS and is enjoyed by this specific NIZK scheme (in other words, other OTSS-NIZK schemes may not enjoy this property).

However, this property holds only in the case of $\tau^{*} \neq \tau$, i.e., when the following bad event never occurs.

- TagColl: the tag $\tau^{*}=H\left(v k, m^{*},\left[\mathbf{c}^{*}\right]_{1}\right)$ involved in $\mathcal{A}$ 's forgery ( $m^{*}, \sigma^{*}=$ $\left.\left(\left[\mathbf{c}^{*}\right]_{1},\left[\mathbf{d}^{*}\right]_{1}\right)\right)$ is identical to the $\operatorname{tag} \tau=H\left(v k^{\prime}=\left[(a \mathbf{K}+\mathbf{B})^{\top} \mathbf{A}\right]_{2}, m,[\mathbf{c}]_{1}\right)$ involved in some signatures that $\mathcal{A}$ obtains under tampered signing keys.

So to apply this property, we need to first show that the event TagColl can hardly occur. This might be the most technical part of our security proof in Subsect. 3.3 and corresponds to Claim 2 therein. Roughly speaking, we divide TagColl into three sub-cases and analyze them individually to show that they all rarely occur,
by utilizing the concrete algebraic structures of our construction, based on the collision resistance of $H$ and on the MDDH assumption.

Consequently, we can apply the above property, and show that the terms $\left[\gamma \mathbf{a}^{\perp}\right]_{1}$ triggered by $\left[\left(\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right) \mathbf{U}\right]_{1} \mathbf{w}$ in (5) can be used to hide the partial information of $\left.(a \mathbf{K}+\mathbf{B})[\mathbf{c}]_{1}\right]$ in the generation of $[\mathbf{d}]_{1}$ in (4). To see this more concretely, again, we sample $s k=\mathbf{K}$ equivalently via

$$
\mathbf{K}:=\widetilde{\mathbf{K}}+{ }_{\substack{\left.-\mathbf{L}^{-} \mathbf{a}^{-} \mathbf{k}^{-}{ }^{\top}\right\urcorner \\ \hline \\ \hline}}
$$

where $\widetilde{\mathbf{K}} \leftarrow \mathrm{s} \mathbb{Z}_{p}^{(k+1) \times(k+1)}$ and $\mathbf{k} \leftarrow s \mathbb{Z}_{p}^{k+1}$, and then we have

$$
\begin{aligned}
{[\mathbf{d}]_{1} } & \left.=(a \mathbf{K}+\mathbf{B})[\mathbf{c}]_{1}+\left[\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right) \mathbf{U}\right]_{1} \mathbf{w} \\
& \approx\left((a \mathbf{K}+\mathbf{B})[\mathbf{c}]_{1}+\left[\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right) \mathbf{U}\right]_{1} \mathbf{w}+\left[\mathbf{c}^{\perp}\right]_{1} \\
& \left.=\left(a\left(\widetilde{\mathbf{K}}+\mathbf{a}^{\perp} \mathbf{k}^{\top}\right)+\mathbf{B}\right)[\mathbf{c}]_{1}+\left[\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right) \mathbf{U}\right]_{1} \mathbf{w}+\left[\mathbf{a}^{\perp}\right]_{1} \\
& \left.=(a \widetilde{\mathbf{K}}+\mathbf{B})[\mathbf{c}]_{1}+\left[\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right) \mathbf{U}\right]_{1} \mathbf{w}+\left[a \mathbf{a}^{\perp}\left(\mathbf{k}^{\top} \mathbf{c}\right)+{ }_{\llcorner } \mathbf{a}^{\perp}\right]_{1} .
\end{aligned}
$$

Note that the term $\gamma \mathbf{a}^{\perp}$ perfectly hides $a \mathbf{a}^{\perp}\left(\mathbf{k}^{\top} \mathbf{c}\right)=\left(a \mathbf{k}^{\top} \mathbf{c}\right) \mathbf{a}^{\perp}$ by the randomness of $\gamma \leftarrow \varangle \mathbb{Z}_{p}$, thus the information of $\mathbf{k}$ is perfectly hidden in the multiple signatures generated under tampered signing keys.

Putting Two Components Together. Overall, the two components enjoy specific properties and we carefully integrate the two components in our SIG construction to achieve sLTR-CMA security: the terms $\left[\left(\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right) \mathbf{U}\right]_{1} \mathbf{w}$ in the second component can trigger randomness in the form of ${ }_{[ }\left[\gamma \mathbf{a}^{\perp}\right]_{1}$, , which can then be used to hide the terms $(a \mathbf{K}+\mathbf{B})[\mathbf{c}]_{1}$ in the first component, so that the signatures generated under tampered signing keys do not leak much information about $s k=\mathbf{K}$ beyond $v k$ to the adversary, and finally the sLTR-CMA security of our SIG follows from the useful property of the first component in the key leakage setting.

### 3.3 Proof of Theorem 1

Now we present the formal proof of Theorem 1. Let $\mathcal{A}$ be any PPT adversary against the ( $\left.\kappa, \mathcal{T}_{\text {aff }}\right)$-sLTR-CMA security of SIG, where $\mathcal{A}$ makes $Q$ times of $\mathcal{O}_{\text {SIGN }}$ queries. We prove the theorem via a sequence of games $\mathrm{G}_{0}-\mathrm{G}_{3},\left\{\mathrm{G}_{4 . \eta .0}-\mathrm{G}_{4 . \eta .4}\right\}_{0 \leq \eta \leq Q-1}$ and $G_{4 . Q .0}$, where $G_{0}$ is the ( $\kappa, \mathcal{T}_{\text {aff }}$ )-sLTR-CMA experiment (cf. Fig. 1), and in $\mathrm{G}_{4 . Q .0}, \mathcal{A}$ has a negligible advantage. A brief description of differences between adjacent games is summarized in Table 1.

Game $\mathrm{G}_{0}$ : This is the ( $\kappa, \mathcal{T}_{\text {aff }}$ )-sLTR-CMA experiment (cf. Fig. 1).

Table 1. Brief Description of Games $\mathrm{G}_{0}-\mathrm{G}_{3},\left\{\mathrm{G}_{4 . \eta .0}-\mathrm{G}_{4 . \eta .4}\right\}_{0 \leq \eta \leq Q-1}$ and $\mathrm{G}_{4 . Q .0}$ for the ( $\kappa, \mathcal{T}_{\text {aff }}$ )-sLTR-CMA security proof of SIG, where the differences between adjacent games are highlighted in gray boxes. Here column " $\mathcal{O}_{\text {SIGN }}\left(T_{(a, \mathbf{B})} \in \mathcal{T}_{\text {aff }}, m\right)$ " suggests how a signature $\sigma=\left([\mathbf{c}]_{1},[\mathbf{d}]_{1}\right)$ is generated: sub-column " $[\mathbf{c}]_{1} \leftarrow_{8}$ " refers to the space from which $[\mathbf{c}]_{1}$ is chosen; sub-column " $[\mathbf{d}]_{1}=$ " shows the computation of $[\mathbf{d}]_{1}$, where $s k^{\prime}=\mathbf{K}^{\prime}=T_{(a, \mathbf{B})}(s k)=a \mathbf{K}+\mathbf{B}$ denotes the tampered signing key. Column " $\mathcal{O}_{\text {Leak" }}$ shows the output returned by $\mathcal{O}_{\text {Leak. }}$ Column "Win's additional check for forgery ( $m^{*}, \sigma^{*}=\left(\left[\mathbf{c}^{*}\right]_{1},\left[\mathbf{d}^{*}\right]_{1}\right)$ )" describes the additional check that $\mathcal{A}$ 's forgery wins, besides the routine check $\left(m^{*}, \sigma^{*}\right) \notin \mathcal{Q}_{\text {id }} \wedge e\left(\left[\mathbf{c}^{* \top}\right]_{1},\left[\left(\mathbf{K}^{\top}+\mathbf{K}_{0}^{\top}+\tau^{*} \mathbf{K}_{1}^{\top}\right) \mathbf{A}\right]_{2}\right)=e\left(\left[\mathbf{d}^{* \top}\right]_{1},[\mathbf{A}]_{2}\right) \wedge\left[\mathbf{c}^{*}\right]_{1} \neq[\mathbf{0}]_{1}$, where $\mathcal{Q}_{\text {tag }}$ denotes the set of $\tau$ generated in $\mathcal{O}_{\text {SIGN }}$ queries.


Let pp $=\left(\right.$ gpar, $\left.[\mathbf{U}]_{1},\left[\mathbf{K}_{0} \mathbf{U}\right]_{1},\left[\mathbf{K}_{1} \mathbf{U}\right]_{1},[\mathbf{A}]_{2},\left[\mathbf{K}_{0}^{\top} \mathbf{A}\right]_{2},\left[\mathbf{K}_{1}^{\top} \mathbf{A}\right]_{2}, H\right)$ and $(v k=$ $\left.\left[\mathbf{K}^{\top} \mathbf{A}\right]_{2}, s k=\mathbf{K}\right)$. In this game, when answering an $\mathcal{O}_{\text {SIGN }}$ query $\left(T_{(a, \mathbf{B})} \in\right.$ $\left.\mathcal{T}_{\text {aff }}, m\right)$, the challenger computes the tampered key $s k^{\prime}=\mathbf{K}^{\prime}:=T_{(a, \mathbf{B})}(s k)=$ $a \mathbf{K}+\mathbf{B}$ and $v k^{\prime}:=\left[\mathbf{K}^{\prime \top} \mathbf{A}\right]_{2}$, samples $\mathbf{w} \leftarrow_{s} \mathbb{Z}_{p}^{k}$, and computes $[\mathbf{c}]_{1}:=[\mathbf{U}]_{1} \mathbf{w}$, $\tau:=H\left(v k^{\prime}, m,[\mathbf{c}]_{1}\right)$ and $[\mathbf{d}]_{1}:=\mathbf{K}^{\prime}[\mathbf{c}]_{1}+\left[\left(\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right) \mathbf{U}\right]_{1} \mathbf{w}$ using the tampered key $s k^{\prime}=\mathbf{K}^{\prime}$. Then, the challenger returns $\sigma:=\left([\mathbf{c}]_{1},[\mathbf{d}]_{1}\right)$ to $\mathcal{A}$, and further puts $(m, \sigma)$ to set $\mathcal{Q}_{\text {id }}$ if $T_{(a, \mathbf{B})}$ is the identity function id. For an $\mathcal{O}_{\text {Leak }}$ query $L$, the challenger returns $L(s k)$ to $\mathcal{A}$ if the total leakage length is bounded by $\kappa$.

At the end of the game, $\mathcal{A}$ outputs a forgery $\left(m^{*}, \sigma^{*}=\left(\left[\mathbf{c}^{*}\right]_{1},\left[\mathbf{d}^{*}\right]_{1}\right)\right)$. Let Win denote the event that
$\left(m^{*}, \sigma^{*}\right) \notin \mathcal{Q}_{\text {id }} \wedge e\left(\left[\mathbf{c}^{* \top}\right]_{1},\left[\left(\mathbf{K}^{\top}+\mathbf{K}_{0}^{\top}+\tau^{*} \mathbf{K}_{1}^{\top}\right) \mathbf{A}\right]_{2}\right)=e\left(\left[\mathbf{d}^{* \top}\right]_{1},[\mathbf{A}]_{2}\right) \wedge\left[\mathbf{c}^{*}\right]_{1} \neq[\mathbf{0}]_{1}$,
where $\tau^{*}:=H\left(v k, m^{*},\left[\mathbf{c}^{*}\right]_{1}\right)$. By definition, $\operatorname{Adv}_{\text {SIG }, \mathcal{A}, \kappa, \mathcal{T}_{\text {aff }}^{\text {sitr }}}^{\text {sicma }}(\lambda)=\operatorname{Pr}_{0}[\mathrm{Win}]$.
Game $\mathrm{G}_{1}$ : It is the same as $\mathrm{G}_{0}$, except that, when answering $\mathcal{O}_{\text {SIGN }}$ queries, the challenger computes $[\mathbf{d}]_{1}:=\left(\mathbf{K}^{\prime}+\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right)[\mathbf{c}]_{1}$ directly from $[\mathbf{c}]_{1}, \tau$ and $\left(\mathbf{K}^{\prime}, \mathbf{K}_{0}, \mathbf{K}_{1}\right)$, without using the vector $\mathbf{w}$ for $[\mathbf{c}]_{1}=[\mathbf{U}]_{1} \mathbf{w}$.

Since $[\mathbf{c}]_{1}=[\mathbf{U}]_{1} \mathbf{w}$, this change is conceptual and $\operatorname{Pr}_{0}[\mathrm{Win}]=\operatorname{Pr}_{1}[\mathrm{Win}]$.
Game $G_{2}$ : It is the same as $G_{1}$, except that, the event Win is now defined as

$$
\left(m^{*}, \sigma^{*}\right) \notin \mathcal{Q}_{\mathrm{id}} \wedge\left[\mathbf{d}^{*}\right]_{1}=\left[\left(\mathbf{K}+\mathbf{K}_{0}+\tau^{*} \mathbf{K}_{1}\right) \mathbf{c}^{*}\right]_{1} \wedge\left[\mathbf{c}^{*}\right]_{1} \neq[\mathbf{0}]_{1}
$$

Claim 1. $\left|\operatorname{Pr}_{1}[\mathrm{Win}]-\operatorname{Pr}_{2}[\mathrm{Win}]\right| \leq \operatorname{Adv}_{\mathcal{D}_{k}, \mathbb{G}_{2}, \mathcal{B}_{1}}^{\text {mddh }}(\lambda)+1 /(p-1)$ for a PPT adversary $\mathcal{B}_{1}$ against the $\mathcal{D}_{k}-M D D H$ assumption on $[\mathbf{A}]_{2}$.

Proof. By VrfyBad denote the event that $\mathcal{A}$ 's forgery $\left(m^{*}, \sigma^{*}=\left(\left[\mathbf{c}^{*}\right]_{1},\left[\mathbf{d}^{*}\right]_{1}\right)\right)$ satisfying $e\left(\left[\mathbf{c}^{* \top}\right]_{1},\left[\left(\mathbf{K}^{\top}+\mathbf{K}_{0}^{\top}+\tau^{*} \mathbf{K}_{1}^{\top}\right) \mathbf{A}\right]_{2}\right)=e\left(\left[\mathbf{d}^{* \top}\right]_{1},[\mathbf{A}]_{2}\right)$ but $\left[\mathbf{d}^{*}\right]_{1} \neq$ $\left[\left(\mathbf{K}+\mathbf{K}_{0}+\tau^{*} \mathbf{K}_{1}\right) \mathbf{c}^{*}\right]_{1}$. Clearly, $\mathbf{G}_{2}$ is identical to $\mathbf{G}_{1}$ unless VrfyBad occurs, thus $\left|\operatorname{Pr}_{1}[\mathrm{Win}]-\operatorname{Pr}_{2}[\mathrm{Win}]\right| \leq \operatorname{Pr}_{2}[\operatorname{VrfyBad}]$. To bound $\operatorname{Pr}_{2}[\mathrm{VrfyBad}]$, observe that VrfyBad implies that

$$
e(\underbrace{\left[\mathbf{d}^{* \top}\right]_{1}-\left[\mathbf{c}^{* \top}\left(\mathbf{K}^{\top}+\mathbf{K}_{0}^{\top}+\tau^{*} \mathbf{K}_{1}^{\top}\right)\right]_{1}}_{\neq[\mathbf{0}]_{1}},[\mathbf{A}]_{2})=[\mathbf{0}]_{T},
$$

i.e., $\left[\mathbf{d}^{* \top}\right]_{1}-\left[\mathbf{c}^{* \top}\left(\mathbf{K}^{\top}+\mathbf{K}_{0}^{\top}+\tau^{*} \mathbf{K}_{1}^{\top}\right)\right]_{1}$ is a non-zero vector in the kernel of $[\mathbf{A}]_{2}$. Thus VrfyBad rarely occurs under the $\mathcal{D}_{k}$-KerMDH assumption on $[\mathbf{A}]_{2}$, which is further implied by the $\mathcal{D}_{k}-\mathrm{MDDH}$ assumption on $[\mathbf{A}]_{2}$ according to Lemma 3. Consequently, $\operatorname{Pr}_{2}[\operatorname{VrfyBad}] \leq \operatorname{Adv}_{\mathcal{D}_{k}, \mathbb{G}_{2}, \mathcal{B}_{1}}^{\mathrm{mdd}}(\lambda)+1 /(p-1)$ and Claim 1 follows.

Game $\mathrm{G}_{3}$ : It is the same as $\mathrm{G}_{2}$, except that, when answering $\mathcal{O}_{\text {SIGN }}$ queries, the challenger also puts $\tau$ to a set $\mathcal{Q}_{\operatorname{tag}}$, and for the forgery $\left(m^{*}, \sigma^{*}=\left(\left[\mathbf{c}^{*}\right]_{1},\left[\mathbf{d}^{*}\right]_{1}\right)\right)$ output by $\mathcal{A}$, the event Win is now defined as

$$
\left(m^{*}, \sigma^{*}\right) \notin \mathcal{Q}_{\mathrm{id}} \wedge\left[\mathbf{d}^{*}\right]_{1}=\left[\left(\mathbf{K}+\mathbf{K}_{0}+\tau^{*} \mathbf{K}_{1}\right) \mathbf{c}^{*}\right]_{1} \wedge\left[\mathbf{c}^{*}\right]_{1} \neq[\mathbf{0}]_{1} \wedge \tau^{*} \notin \mathcal{Q}_{\mathrm{tag}}
$$

Claim 2. $\left|\operatorname{Pr}_{2}[\mathrm{Win}]-\operatorname{Pr}_{3}[\mathrm{Win}]\right| \leq \operatorname{Adv}_{\mathcal{H}, \mathcal{B}_{2}}^{\mathrm{cr}}(\lambda)+\operatorname{Adv}_{\mathcal{D}_{k}, \mathbb{G}_{2}, \mathcal{B}_{3}}^{\mathrm{mddh}}(\lambda)+1 /(p-1)+$ $2^{-\Omega(\lambda)}$ for PPT adversaries $\mathcal{B}_{2}$ against the collision-resistance of $\mathcal{H}$ and $\mathcal{B}_{3}$ against the $\mathcal{D}_{k}-M D D H$ assumption on $[\mathbf{A}]_{2}$.

Proof. By TagColl denote the event that $\mathcal{A}$ 's forgery $\left(m^{*}, \sigma^{*}=\left(\left[\mathbf{c}^{*}\right]_{1},\left[\mathbf{d}^{*}\right]_{1}\right)\right)$ satisfying

$$
\left(m^{*}, \sigma^{*}\right) \notin \mathcal{Q}_{\text {id }} \wedge\left[\mathbf{d}^{*}\right]_{1}=\left[\left(\mathbf{K}+\mathbf{K}_{0}+\tau^{*} \mathbf{K}_{1}\right) \mathbf{c}^{*}\right]_{1} \wedge\left[\mathbf{c}^{*}\right]_{1} \neq[\mathbf{0}]_{1} \wedge \tau^{*} \in \mathcal{Q}_{\mathrm{tag}} .
$$

Clearly, $G_{2}$ and $G_{3}$ are the same until TagColl occurs, thus $\mid \operatorname{Pr}_{2}[$ Win $]-\operatorname{Pr}_{3}[$ Win $] \mid \leq$ $\mathrm{Pr}_{3}$ [TagColll].

To bound $\mathrm{Pr}_{3}[\mathrm{TagColll}]$, we divide TagColl into the following three cases:

- Case 1: There exists an $\mathcal{O}_{\text {SIGN }}$ query $\left(T_{(a, \mathbf{B})} \in \mathcal{T}_{\text {aff }}, m\right)$, such that

$$
\begin{array}{ll} 
& \tau^{*}=H\left(v k, m^{*},\left[\mathbf{c}^{*}\right]_{1}\right)=H\left(v k^{\prime}, m,[\mathbf{c}]_{1}\right)=\tau \in \mathcal{Q}_{\mathrm{tag}} \\
\text { but } \quad & \left(v k, m^{*},\left[\mathbf{c}^{*}\right]_{1}\right) \neq\left(v k^{\prime}, m,[\mathbf{c}]_{1}\right)
\end{array}
$$

where $v k^{\prime}$ is the tampered verification key involved in this $\mathcal{O}_{\text {SIGN }}$ query.
Clearly, Case 1 suggests a collision of $H$, thus $\operatorname{Pr}_{3}\left[\right.$ Case 1] $\leq \operatorname{Adv}_{\mathcal{H}, \mathcal{B}_{2}}^{\mathrm{cr}}(\lambda)$.

- Case 2: There exists an $\mathcal{O}_{\text {SIGN }}$ query $\left(T_{(a, \mathbf{B})} \in \mathcal{T}_{\text {aff }}, m\right)$, such that

$$
\begin{array}{ll} 
& \tau^{*}=H\left(v k, m^{*},\left[\mathbf{c}^{*}\right]_{1}\right)=H\left(v k^{\prime}, m,[\mathbf{c}]_{1}\right)=\tau \in \mathcal{Q}_{\mathrm{tag}} \\
\text { but } \quad\left(v k, m^{*},\left[\mathbf{c}^{*}\right]_{1}\right)=\left(v k^{\prime}, m,[\mathbf{c}]_{1}\right) \wedge T_{(a, \mathbf{B})}=\mathrm{id}
\end{array}
$$

where id denotes the identity function.
Since $T_{(a, \mathbf{B})}=\mathrm{id}$, the tampered signing key $s k^{\prime}=\mathbf{K}^{\prime}$ is in fact the original key $s k=\mathbf{K}$, and the tuple $\left(m, \sigma=\left([\mathbf{c}]_{1},[\mathbf{d}]_{1}\right)\right)$ involved in this $\mathcal{O}_{\text {SIGN }}$ query is added to $\mathcal{Q}_{\text {id }}$.

Now we show that this case can never occur. On the one hand, TagColl requires $\left(m^{*}, \sigma^{*}=\left(\left[\mathbf{c}^{*}\right]_{1},\left[\mathbf{d}^{*}\right]_{1}\right)\right) \notin \mathcal{Q}_{\text {id }}$ and this case requires $\left(m^{*},\left[\mathbf{c}^{*}\right]_{1}\right)=$ ( $m,[\mathbf{c}]_{1}$ ), so it follows that $\left[\mathbf{d}^{*}\right]_{1} \neq[\mathbf{d}]_{1}$. On the other hand, TagColl requires $\left[\mathbf{d}^{*}\right]_{1}=\left[\left(\mathbf{K}+\mathbf{K}_{0}+\tau^{*} \mathbf{K}_{1}\right) \mathbf{c}^{*}\right]_{1}$ and this case requires $\tau^{*}=\tau$, so we have $\left[\mathbf{d}^{*}\right]_{1}=\left[\left(\mathbf{K}+\mathbf{K}_{0}+\tau^{*} \mathbf{K}_{1}\right) \mathbf{c}^{*}\right]_{1}=\left[\left(\mathbf{K}^{\prime}+\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right) \mathbf{c}\right]_{1}=[\mathbf{d}]_{1}$, which leads to a contradiction. Therefore, this case can never occur, i.e., $\operatorname{Pr}_{3}[$ Case 2] $=0$.

- Case 3: There exists an $\mathcal{O}_{\text {SIGN }}$ query $\left(T_{(a, \mathbf{B})} \in \mathcal{T}_{\text {aff }}, m\right)$, such that

$$
\begin{array}{ll} 
& \tau^{*}=H\left(v k, m^{*},\left[\mathbf{c}^{*}\right]_{1}\right)=H\left(v k^{\prime}, m,[\mathbf{c}]_{1}\right)=\tau \in \mathcal{Q}_{\mathrm{tag}} \\
\text { but } \quad\left(v k, m^{*},\left[\mathbf{c}^{*}\right]_{1}\right)=\left(v k^{\prime}, m,[\mathbf{c}]_{1}\right) \wedge T_{(a, \mathbf{B})} \neq \mathrm{id}
\end{array}
$$

Note that $v k^{\prime}=v k$ means that $\left[\mathbf{K}^{\prime \top} \mathbf{A}\right]_{2}=\left[\mathbf{K}^{\top} \mathbf{A}\right]_{2}$, where $s k^{\prime}=\mathbf{K}^{\prime}=$ $T_{(a, \mathbf{B})}(s k)=a \mathbf{K}+\mathbf{B}$ is the tampered signing key. By rearranging terms, it follows that $\left[\left((a-1) \mathbf{K}^{\top}+\mathbf{B}^{\top}\right) \mathbf{A}\right]_{2}=[\mathbf{0}]_{2}$. This shows that $(a-1) \mathbf{K}^{\top}+\mathbf{B}^{\top}$ is a matrix in the kernel of $[\mathbf{A}]_{2}$. We claim that $(a-1) \mathbf{K}^{\top}+\mathbf{B}^{\top}$ is a nonzero matrix with overwhelming probability $1-2^{-\Omega(\lambda)}$, which will be shown later. Thus by the $\mathcal{D}_{k}$-KerMDH assumption on $[\mathbf{A}]_{2}$ (which is further implied
by the $\mathcal{D}_{k}$-MDDH assumption on $[\mathbf{A}]_{2}$ according to Lemma 3), this case can rarely occurs, and we have $\operatorname{Pr}_{3}[$ Case $\mathbf{3}] \leq \operatorname{Adv}_{\mathcal{D}_{k}, \mathbb{G}_{2}, \mathcal{B}_{3}}^{\mathrm{mddh}}(\lambda)+1 /(p-1)+2^{-\Omega(\lambda)}$.

It remains to show the claim that the matrix $(a-1) \mathbf{K}^{\top}+\mathbf{B}^{\top}$ is non-zero with overwhelming probability $1-2^{-\Omega(\lambda)}$. By the fact that $T_{(a, \mathbf{B})} \neq \mathrm{id}$, there are two sub-cases. The first sub-case is $a=1$ and $\mathbf{B} \neq \mathbf{0}$. In this sub-case, we have $(a-1) \mathbf{K}^{\top}+\mathbf{B}^{\top}=\mathbf{B}^{\top}$, which is clearly non-zero. The second subcase is $a \neq 1$. In this sub-case, we will show that $s k=\mathbf{K}$ contains enough entropy from $\mathcal{A}$ 's view, so that the matrix $(a-1) \mathbf{K}^{\top}+\mathbf{B}^{\top}$ is non-zero with overwhelming probability. To see this, let $\mathbf{u}^{\perp} \in \mathbb{Z}_{p}^{k+1}$ (resp., $\mathbf{a}^{\perp} \in \mathbb{Z}_{p}^{k+1}$ ) be an arbitrary non-zero vector in the kernel of $\mathbf{U}$ (resp., A) such that $\left(\mathbf{u}^{\perp}\right)^{\top} \mathbf{U}=\mathbf{0}$ (resp., $\left.\left(\mathbf{a}^{\perp}\right)^{\top} \mathbf{A}=\mathbf{0}\right)$. For the convenience of our analysis, we sample $s k=\mathbf{K} \leftarrow s \mathbb{Z}_{p}^{(k+1) \times(k+1)}$ equivalently via

$$
\mathbf{K}:=\widetilde{\mathbf{K}}+\mu \mathbf{a}^{\perp}\left(\mathbf{u}^{\perp}\right)^{\top}
$$

where $\widetilde{\mathbf{K}} \leftarrow \& \mathbb{Z}_{p}^{(k+1) \times(k+1)}$ and $\mu \leftarrow \& \mathbb{Z}_{p}$. Below we analyze the information about $\mu$ that $\mathcal{A}$ may obtain in $\mathrm{G}_{3}$.

- Firstly, the verification key $v k$ is

$$
\left[\mathbf{K}^{\top} \mathbf{A}\right]_{2}=\left[\left(\tilde{\mathbf{K}}^{\top}+\mu \mathbf{u}^{\perp}\left(\mathbf{a}^{\perp}\right)^{\top}\right) \mathbf{A}\right]_{2}=\left[\tilde{\mathbf{K}}^{\top} \mathbf{A}\right]_{2}
$$

thus $\mu$ is completely hidden.

- In $\mathcal{O}_{\text {Sign }}$ queries, the tampered verification key $v k^{\prime}$ is

$$
\begin{aligned}
{\left[\mathbf{K}^{\prime \top} \mathbf{A}\right]_{2} } & =\left[\left(a \mathbf{K}^{\top}+\mathbf{B}^{\top}\right) \mathbf{A}\right]_{2}=\left[\left(a\left(\tilde{\mathbf{K}}^{\top}+\mu \mathbf{u}^{\perp}\left(\mathbf{a}^{\perp}\right)^{\top}\right)+\mathbf{B}^{\top}\right) \mathbf{A}\right]_{2} \\
& =\left[\left(a \widetilde{\mathbf{K}}^{\top}+\mathbf{B}^{\top}\right) \mathbf{A}\right]_{2},
\end{aligned}
$$

thus $\mu$ is completely hidden. Moreover, since $[\mathbf{c}]_{1}=[\mathbf{U}]_{1} \mathbf{w}$ with $\mathbf{w} \leftarrow \& \mathbb{Z}_{p}^{k}$, we have

$$
\begin{aligned}
{[\mathbf{d}]_{1} } & =\left(\mathbf{K}^{\prime}+\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right)[\mathbf{c}]_{1}=\left(a \mathbf{K}+\mathbf{B}+\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right)[\mathbf{U}]_{1} \mathbf{w} \\
& =\left(a\left(\widetilde{\mathbf{K}}+\mu \mathbf{a}^{\perp}\left(\mathbf{u}^{\perp}\right)^{\top}\right)+\mathbf{B}+\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right)[\mathbf{U}]_{1} \mathbf{w} \\
& =\left(a \widetilde{\mathbf{K}}+\mathbf{B}+\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right)[\mathbf{U}]_{1} \mathbf{w},
\end{aligned}
$$

thus $\mu$ is also completely hidden.

- From $\mathcal{O}_{\text {Leak }}$ queries, $\mathcal{A}$ obtains at most $\kappa$ bits information $L(s k)=$ $L(\mathbf{K})=L\left(\widetilde{\mathbf{K}}+\mu \mathbf{a}^{\perp}\left(\mathbf{u}^{\perp}\right)^{\top}\right)$ about $s k$, and also about $\mu$.
Overall, the information about $\mu$ that $\mathcal{A}$ learns in $\mathrm{G}_{3}$ is at most $\kappa$ bits. Thus, there are still $\log p-\kappa \geq \Omega(\lambda)$ bits of entropy left in $\mu$, and also in $s k=\mathbf{K}=\widetilde{\mathbf{K}}+\mu \mathbf{a}^{\perp}\left(\mathbf{u}^{\perp}\right)^{\top}$. Consequently, the probability that the matrix $(a-1) \mathbf{K}^{\top}+\mathbf{B}^{\top}$ is non-zero is $\operatorname{Pr}\left[(a-1) \mathbf{K}^{\top}+\mathbf{B}^{\top} \neq \mathbf{0}\right]=1-\operatorname{Pr}\left[(a-1) \mathbf{K}^{\top}+\right.$ $\left.\mathbf{B}^{\top}=\mathbf{0}\right]=1-\operatorname{Pr}\left[\mathbf{K}=(1-a)^{-1} \mathbf{B}\right] \geq 1-2^{-\Omega(\lambda)}$ and the claim follows.
Putting the above three cases together, we have $\operatorname{Pr}_{3}[\operatorname{TagColll}] \leq \operatorname{Adv}_{\mathcal{H}, \mathcal{B}_{2}}^{c r}(\lambda)+$ $\operatorname{Adv}_{\mathcal{D}_{k}, \mathbb{G}_{2}, \mathcal{B}_{3}}^{\mathrm{mddh}}(\lambda)+1 /(p-1)+2^{-\Omega(\lambda)}$, and Claim 2 follows.

Next, we consider a sequence of games $\left\{\mathrm{G}_{4 . \eta .0}-\mathrm{G}_{4 . \eta .4}\right\}_{0 \leq \eta \leq Q-1}$ and $\mathrm{G}_{4 . Q .0}$.
Game $\mathrm{G}_{4 . \eta .0}, 0 \leq \eta \leq Q$ : It is the same as $\mathrm{G}_{3}$, except that, at the beginning of the game, the challenger picks a non-zero vector $\mathbf{a}^{\perp} \in \mathbb{Z}_{p}^{k+1}$ in the kernel of $\mathbf{A}$ such that $\left(\mathbf{a}^{\perp}\right)^{\top} \mathbf{A}=\mathbf{0}$. Moreover, when answering the first $\eta \mathcal{O}_{\text {SIGN }}$ queries, the challenger computes $[\mathbf{d}]_{1}:=\left(\mathbf{K}^{\prime}+\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right)[\mathbf{c}]_{1}+\left[\gamma \mathbf{a}^{\perp}\right]_{1}$ with $\gamma \leftarrow \& \mathbb{Z}_{p}$ chosen uniformly and independently for each query. As for the remaining $Q-\eta \mathcal{O}_{\text {SIGN }}$ queries, the challenger still computes $[\mathbf{d}]_{1}:=\left(\mathbf{K}^{\prime}+\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right)[\mathbf{c}]_{1}$.

It is clearly that $G_{4.0 .0}$ is identical to $G_{3}$, thus $\operatorname{Pr}_{3}[\mathrm{Win}]=\operatorname{Pr}_{4.0 .0}[\mathrm{Win}]$.
Game $\mathrm{G}_{4 . \eta .1}, 0 \leq \eta \leq Q-1$ : It is the same as $\mathrm{G}_{4 . \eta .0}$, except that, when answering the $(\eta+1)$-th $\mathcal{O}_{\text {SIGN }}$ query, the challenger samples $[\mathbf{c}]_{1} \leftarrow_{\infty} \mathbb{G}_{1}^{k+1}$ uniformly at random, instead of computing $[\mathbf{c}]_{1}:=[\mathbf{U}]_{1} \mathbf{w}$ with $\mathbf{w} \leftarrow \leftarrow_{\mathbb{Z}}^{k}$.

It is clearly that $G_{4 . \eta .0}$ and $G_{4 . \eta .1}$ are computationally indistinguishable to $\mathcal{A}$, under the $\mathcal{D}_{k}-\mathrm{MDDH}$ assumption on $[\mathbf{U}]_{1}$. Therefore, we have $\mid \operatorname{Pr}_{4 . \eta .0}[\mathrm{Win}]-$ $\operatorname{Pr}_{4 . \eta .1}[\mathrm{Win}] \mid \leq \operatorname{Adv}_{\mathcal{D}_{k}, \mathbb{G}_{1}, \mathcal{B}_{4}}^{\mathrm{mddh}}(\lambda)$ for a PPT adversary $\mathcal{B}_{4}$.

Game $\mathrm{G}_{4 . \eta \cdot 2}, 0 \leq \eta \leq Q-1$ : It is the same as $\mathrm{G}_{4 . \eta .1}$, except that, the event Win is now defined as
$\left(m^{*}, \sigma^{*}\right) \notin \mathcal{Q}_{\text {id }} \wedge\left[\mathbf{d}^{*}\right]_{1}=\left[\left(\mathbf{K}+\mathbf{K}_{0}+\tau^{*} \mathbf{K}_{1}\right) \mathbf{c}^{*}\right]_{1} \wedge\left[\mathbf{c}^{*}\right]_{1} \neq[\mathbf{0}]_{1} \wedge \tau^{*} \notin \mathcal{Q}_{\operatorname{tag}} \wedge\left[\mathbf{c}^{*}\right]_{1} \in \operatorname{Span}\left([\mathbf{U}]_{1}\right)$.
Claim 3. $\left|\operatorname{Pr}_{4 . \eta .1}[\mathrm{Win}]-\operatorname{Pr}_{4 . \eta .2}[\mathrm{Win}]\right| \leq 1 / p$.
Proof. By CBad denote the event that $\mathcal{A}$ 's forgery $\left(m^{*}, \sigma^{*}=\left(\left[\mathbf{c}^{*}\right]_{1},\left[\mathbf{d}^{*}\right]_{1}\right)\right)$ satisfying
$\left(m^{*}, \sigma^{*}\right) \notin \mathcal{Q}_{\text {id }} \wedge\left[\mathbf{d}^{*}\right]_{1}=\left[\left(\mathbf{K}+\mathbf{K}_{0}+\tau^{*} \mathbf{K}_{1}\right) \mathbf{c}^{*}\right]_{1} \wedge\left[\mathbf{c}^{*}\right]_{1} \neq[\mathbf{0}]_{1} \wedge \tau^{*} \notin \mathcal{Q}_{\mathrm{tag}} \wedge\left[\mathbf{c}^{*}\right]_{1} \notin \operatorname{Span}\left([\mathbf{U}]_{1}\right)$.
Clearly, $\mathrm{G}_{4 . \eta .1}$ and $\mathrm{G}_{4 . \eta .2}$ are the same until CBad occurs, thus $\mid \operatorname{Pr}_{4 . \eta .1}[\mathrm{Win}]$ $\operatorname{Pr}_{4 . \eta .2}[\mathrm{Win}] \mid \leq \mathrm{Pr}_{4 . \eta .2}[\mathrm{CBad}]$.

Next, we analyze $\operatorname{Pr}_{4 . \eta .2}[\mathrm{CBad}]$. Let $\mathbf{u}^{\perp} \in \mathbb{Z}_{p}^{k+1}$ be a non-zero vector in the kernel of $\mathbf{U}$ such that $\left(\mathbf{u}^{\perp}\right)^{\top} \mathbf{U}=\mathbf{0}$ but $\left(\mathbf{u}^{\perp}\right)^{\top} \mathbf{c}^{*} \neq 0$. For the convenience of our analysis, we sample $\mathbf{K}_{0}, \mathbf{K}_{1} \leftarrow s \mathbb{Z}_{p}^{(k+1) \times(k+1)}$ equivalently via

$$
\mathbf{K}_{0}:=\widetilde{\mathbf{K}_{0}}+\mu_{0} \mathbf{a}^{\perp}\left(\mathbf{u}^{\perp}\right)^{\top}, \quad \mathbf{K}_{1}:=\widetilde{\mathbf{K}_{1}}+\mu_{1} \mathbf{a}^{\perp}\left(\mathbf{u}^{\perp}\right)^{\top}
$$

where $\widetilde{\mathbf{K}_{0}}, \widetilde{\mathbf{K}_{1}} \leftarrow_{s} \mathbb{Z}_{p}^{(k+1) \times(k+1)}$ and $\mu_{0}, \mu_{1} \leftarrow s \mathbb{Z}_{p}$. Below we analyze the information about $\mu_{0}$ and $\mu_{1}$ that $\mathcal{A}$ may obtain in $\mathrm{G}_{4 . \eta .2}$.

- Firstly, the public parameter pp contains $\left[\mathbf{K}_{0} \mathbf{U}\right]_{1},\left[\mathbf{K}_{1} \mathbf{U}\right]_{1},\left[\mathbf{K}_{0}^{\top} \mathbf{A}\right]_{2},\left[\mathbf{K}_{1}^{\top} \mathbf{A}\right]_{2}$. Due to the facts that $\left(\mathbf{u}^{\perp}\right)^{\top} \mathbf{U}=\mathbf{0}$ and $\left(\mathbf{a}^{\perp}\right)^{\top} \mathbf{A}=\mathbf{0}$, it is easy to see that

$$
\left[\mathbf{K}_{0} \mathbf{U}\right]_{1}=\left[\widetilde{\mathbf{K}_{0}} \mathbf{U}\right]_{1},\left[\mathbf{K}_{1} \mathbf{U}\right]_{1}=\left[\widetilde{\mathbf{K}_{1}} \mathbf{U}\right]_{1},\left[\mathbf{K}_{0}^{\top} \mathbf{A}\right]_{2}=\left[\widetilde{\mathbf{K}}_{0}^{\top} \mathbf{A}\right]_{2},\left[\mathbf{K}_{1}^{\top} \mathbf{A}\right]_{2}=\left[\widetilde{\mathbf{K}}_{1}^{\top} \mathbf{A}\right]_{2}
$$

Thus $\mu_{0}$ and $\mu_{1}$ are completely hidden. Moreover, the verification key $v k$ does not involve $\mathbf{K}_{0}$ and $\mathbf{K}_{1}$, so $\mu_{0}$ and $\mu_{1}$ are also completely hidden.

- In $\mathcal{O}_{\text {SIGN }}$ queries, the tampered verification key $v k^{\prime}$ does not involve $\mathbf{K}_{0}$ and $\mathbf{K}_{1}$, thus also does not involve $\mu_{0}$ and $\mu_{1}$. Next we analyze the information about $\mu_{0}$ and $\mu_{1}$ contained in $[\mathbf{d}]_{1}$.
* For the first $\eta \mathcal{O}_{\text {Sign }}$ queries, we have

$$
\begin{aligned}
{[\mathbf{d}]_{1} } & =\left(\mathbf{K}^{\prime}+\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right)[\mathbf{c}]_{1}+\left[\gamma \mathbf{a}^{\perp}\right]_{1} \\
& =\left(\mathbf{K}^{\prime}+\widetilde{\mathbf{K}_{0}}+\tau \widetilde{\mathbf{K}_{1}}+\left(\mu_{0}+\tau \mu_{1}\right) \mathbf{a}^{\perp}\left(\mathbf{u}^{\perp}\right)^{\top}\right)[\mathbf{c}]_{1}+\left[\gamma \mathbf{a}^{\perp}\right]_{1}
\end{aligned}
$$

Due to fact that $[\mathbf{c}]_{1}=[\mathbf{U}]_{1} \mathbf{w}$ with $\mathbf{w} \leftarrow{ }_{\delta} \mathbb{Z}_{p}^{k}$, we have

$$
[\mathbf{d}]_{1}=\left(\mathbf{K}^{\prime}+\widetilde{\mathbf{K}_{0}}+\tau \widetilde{\mathbf{K}_{1}}\right)[\mathbf{c}]_{1}+\left[\gamma \mathbf{a}^{\perp}\right]_{1} .
$$

Therefore, $\mu_{0}$ and $\mu_{1}$ are completely hidden.

* For the $(\eta+1)$-th $\mathcal{O}_{\text {SIGN }}$ query, we have

$$
\begin{aligned}
{[\mathbf{d}]_{1} } & =\left(\mathbf{K}^{\prime}+\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right)[\mathbf{c}]_{1} \\
& =\left(\mathbf{K}^{\prime}+\widetilde{\mathbf{K}_{0}}+\tau \widetilde{\mathbf{K}_{1}}+\left(\mu_{0}+\tau \mu_{1}\right) \mathbf{a}^{\perp}\left(\mathbf{u}^{\perp}\right)^{\top}\right)[\mathbf{c}]_{1},
\end{aligned}
$$

so the information of $\mu_{0}$ and $\mu_{1}$ contained in $[\mathbf{d}]_{1}$ is limited in $\left(\mu_{0}+\tau \mu_{1}\right)$.

* For the remaining $(Q-\eta-1) \mathcal{O}_{\text {SIGN }}$ queries, we also have $[\mathbf{d}]_{1}=\left(\mathbf{K}^{\prime}+\right.$ $\left.\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right)[\mathbf{c}]_{1}=\left(\mathbf{K}^{\prime}+\widetilde{\mathbf{K}_{0}}+\tau \widetilde{\mathbf{K}_{1}}+\left(\mu_{0}+\tau \mu_{1}\right) \mathbf{a}^{\perp}\left(\mathbf{u}^{\perp}\right)^{\top}\right)[\mathbf{c}]_{1}$. Due to fact that $[\mathbf{c}]_{1}=[\mathbf{U}]_{1} \mathbf{w}$ with $\mathbf{w} \leftarrow_{\S} \mathbb{Z}_{p}^{k}$, we have $[\mathbf{d}]_{1}=\left(\mathbf{K}^{\prime}+\widetilde{\mathbf{K}_{0}}+\tau \widetilde{\mathbf{K}_{1}}\right)[\mathbf{c}]_{1}$. Therefore, $\mu_{0}$ and $\mu_{1}$ are completely hidden.
- From $\mathcal{O}_{\text {Leak }}$ queries, $\mathcal{A}$ obtains leakage information about $s k=\mathbf{K}$. It does not involve $\mathbf{K}_{0}$ and $\mathbf{K}_{1}$, thus also does not involve $\mu_{0}$ and $\mu_{1}$.

Overall, the information that $\mathcal{A}$ might learn about $\mu_{0}$ and $\mu_{1}$ is limited in $\left(\mu_{0}+\right.$ $\left.\tau \mu_{1}\right)$.

For CBad to occur, $\mathcal{A}$ 's forgery $\left(m^{*}, \sigma^{*}=\left(\left[\mathbf{c}^{*}\right]_{1},\left[\mathbf{d}^{*}\right]_{1}\right)\right)$ should satisfy $\left(m^{*}, \sigma^{*}\right) \notin$ $\mathcal{Q}_{\mathrm{id}},\left[\mathbf{c}^{*}\right]_{1} \neq[\mathbf{0}]_{1}, \tau^{*} \notin \mathcal{Q}_{\mathrm{tag}},\left[\mathbf{c}^{*}\right]_{1} \notin \operatorname{Span}\left([\mathbf{U}]_{1}\right)$, and
$\left[\mathbf{d}^{*}\right]_{1}=\left[\left(\mathbf{K}+\mathbf{K}_{0}+\tau^{*} \mathbf{K}_{1}\right) \mathbf{c}^{*}\right]_{1}=\left[\left(\mathbf{K}+\widetilde{\mathbf{K}_{0}}+\tau^{*} \widetilde{\mathbf{K}_{1}}\right) \mathbf{c}^{*}+\left(\mu_{0}+\tau^{*} \mu_{1}\right) \mathbf{a}^{\perp}\left(\mathbf{u}^{\perp}\right)^{\top} \mathbf{c}^{*}\right]_{1}$.
Below we argue that $\mathcal{A}$ can hardly compute such $\left[\mathbf{d}^{*}\right]_{1}$. Since $\tau^{*} \notin \mathcal{Q}_{\mathrm{tag}}$, the term $\left(\mu_{0}+\tau^{*} \mu_{1}\right)$ is pairwise independent from the information $\left(\mu_{0}+\tau \mu_{1}\right)$ that $\mathcal{A}$ might learn, thus $\left(\mu_{0}+\tau^{*} \mu_{1}\right)$ is uniformly distributed over $\mathbb{Z}_{p}$ from $\mathcal{A}$ 's view. Moreover, $\mathbf{u}^{\perp} \in \mathbb{Z}_{p}^{k+1}$ is chosen to satisfy $\left(\mathbf{u}^{\perp}\right)^{\top} \mathbf{c}^{*} \neq 0$ since $\left[\mathbf{c}^{*}\right]_{1} \notin \operatorname{Span}\left([\mathbf{U}]_{1}\right)$. Therefore, $\left(\mu_{0}+\tau^{*} \mu_{1}\right) \mathbf{a}^{\perp}\left(\mathbf{u}^{\perp}\right)^{\top} \mathbf{c}^{*}$ is uniformly distributed over $\operatorname{Span}\left(\mathbf{a}^{\perp}\right)=\left\{\gamma^{*} \mathbf{a}^{\perp} \mid \gamma^{*} \in\right.$ $\left.\mathbb{Z}_{p}\right\}$ from $\mathcal{A}$ 's view, and consequently, $\mathcal{A}$ can compute such $\left[\mathbf{d}^{*}\right]_{1}$ with probability at most $1 / p$. This shows that $\operatorname{Pr}_{4 . \eta .2}[\mathrm{CBad}] \leq 1 / p$ and Claim 3 follows.

Game $\mathrm{G}_{4 . \eta .3}, 0 \leq \eta \leq Q-1$ : It is the same as $\mathrm{G}_{4 . \eta .2}$, except that, when answering the $(\eta+1)$-th $\mathcal{O}_{\text {SIGN }}$ query, the challenger computes $[\mathbf{d}]_{1}:=\left(\mathbf{K}^{\prime}+\mathbf{K}_{0}+\right.$ $\left.\tau \mathbf{K}_{1}\right)[\mathbf{c}]_{1}+\left[\gamma \mathbf{a}^{\perp}\right]_{1}$ with $\gamma \leftarrow_{s} \mathbb{Z}_{p}$, instead of $[\mathbf{d}]_{1}:=\left(\mathbf{K}^{\prime}+\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right)[\mathbf{c}]_{1}$.
Claim 4. $\left|\operatorname{Pr}_{4 . \eta .2}[\mathrm{Win}]-\operatorname{Pr}_{4 . \eta .3}[\mathrm{Win}]\right| \leq 1 / p$.

Proof. We will show that $\mathrm{G}_{4 . \eta .2}$ and $\mathrm{G}_{4 . \eta .3}$ are identically distributed, except with probability $1 / p$. To see this, let $\mathbf{u}^{\perp} \in \mathbb{Z}_{p}^{k+1}$ be a non-zero vector in the kernel of $\mathbf{U}$ such that $\left(\mathbf{u}^{\perp}\right)^{\top} \mathbf{U}=\mathbf{0}$. Similar to the proof of Claim 3, we sample $\mathbf{K}_{0}, \mathbf{K}_{1} \leftarrow{ }_{ه} \mathbb{Z}_{p}^{(k+1) \times(k+1)}$ equivalently via $\mathbf{K}_{0}:=\widetilde{\mathbf{K}_{0}}+\mu_{0} \mathbf{a}^{\perp}\left(\mathbf{u}^{\perp}\right)^{\top}$ and $\mathbf{K}_{1}:=$ $\widetilde{\mathbf{K}_{1}}+\mu_{1} \mathbf{a}^{\perp}\left(\mathbf{u}^{\perp}\right)^{\top}$, where $\widetilde{\mathbf{K}_{0}}, \widetilde{\mathbf{K}_{1}} \leftarrow \& \mathbb{Z}_{p}^{(k+1) \times(k+1)}$ and $\mu_{0}, \mu_{1} \leftarrow s \mathbb{Z}_{p}$. Recall that in the proof of Claim 3, we observe that $\mu_{0}$ and $\mu_{1}$ are completely hidden in the public parameter pp , the verification key $v k$, all $\mathcal{O}_{\text {SIGN }}$ queries except the $(\eta+1)$ th $\mathcal{O}_{\text {SigN }}$ query, and $\mathcal{O}_{\text {Leak }}$ queries. Moreover, due to the game change in $\mathrm{G}_{4 . \eta .2}$, the event Win checks $\left[\mathbf{d}^{*}\right]_{1}=\left[\left(\mathbf{K}+\mathbf{K}_{0}+\tau^{*} \mathbf{K}_{1}\right) \mathbf{c}^{*}\right]_{1}$ only if $\left[\mathbf{c}^{*}\right]_{1} \in \operatorname{Span}\left([\mathbf{U}]_{1}\right)$, and when $\left[\mathbf{c}^{*}\right]_{1} \in \operatorname{Span}\left([\mathbf{U}]_{1}\right)$, the check becomes

$$
\begin{aligned}
{\left[\mathbf{d}^{*}\right]_{1} } & =\left[\left(\mathbf{K}+\mathbf{K}_{0}+\tau^{*} \mathbf{K}_{1}\right) \mathbf{c}^{*}\right]_{1}=\left[\left(\mathbf{K}+\widetilde{\mathbf{K}_{0}}+\tau^{*} \widetilde{\mathbf{K}_{1}}\right) \mathbf{c}^{*}+\left(\mu_{0}+\tau^{*} \mu_{1}\right) \mathbf{a}^{\perp}\left(\mathbf{u}^{\perp}\right)^{\top} \mathbf{c}^{*}\right]_{1} \\
& =\left[\left(\mathbf{K}+\widetilde{\mathbf{K}_{0}}+\tau^{*} \widetilde{\mathbf{K}_{1}}\right) \mathbf{c}^{*}\right]_{1},
\end{aligned}
$$

where $\mu_{0}$ and $\mu_{1}$ are also completely hidden. Therefore, the only place that involves $\mu_{0}$ and $\mu_{1}$ lies in the computation of $[\mathbf{d}]_{1}$ in the $(\eta+1)$-th $\mathcal{O}_{\text {SIGN }}$ query, where in $\mathrm{G}_{4 . \eta .2}$, we have

$$
\begin{equation*}
[\mathbf{d}]_{1}=\left(\mathbf{K}^{\prime}+\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right)[\mathbf{c}]_{1}=\left(\mathbf{K}^{\prime}+\widetilde{\mathbf{K}_{0}}+\tau \widetilde{\mathbf{K}_{1}}\right)[\mathbf{c}]_{1}+\left[\left(\mu_{0}+\tau \mu_{1}\right) \mathbf{a}^{\perp}\left(\mathbf{u}^{\perp}\right)^{\top} \mathbf{c}\right]_{1} \tag{6}
\end{equation*}
$$

while in $\mathrm{G}_{4 . \eta .3}$, we have

$$
\begin{align*}
{[\mathbf{d}]_{1} } & =\left(\mathbf{K}^{\prime}+\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right)[\mathbf{c}]_{1}+\left[\gamma \mathbf{a}^{\perp}\right]_{1} \\
& =\left(\mathbf{K}^{\prime}+\widetilde{\mathbf{K}_{0}}+\tau \widetilde{\mathbf{K}_{1}}\right)[\mathbf{c}]_{1}+\left[\left(\mu_{0}+\tau \mu_{1}\right) \mathbf{a}^{\perp}\left(\mathbf{u}^{\perp}\right)^{\top} \mathbf{c}+\gamma \mathbf{a}^{\perp}\right]_{1}, \tag{7}
\end{align*}
$$

with $\gamma \leftarrow s \mathbb{Z}_{p}$. Note that due to the game change in $\mathrm{G}_{4 . \eta .1}$, in the $(\eta+1)$-th $\mathcal{O}_{\text {SIGN }}$ query, $[\mathbf{c}]_{1}$ is chosen uniformly from $\mathbb{G}_{1}^{k+1}$, thus except with probability $1 / p$, we have $\left(\mathbf{u}^{\perp}\right)^{\top} \mathbf{c} \neq 0$, and in this case, both the term $\left(\mu_{0}+\tau \mu_{1}\right) \mathbf{a}^{\perp}\left(\mathbf{u}^{\perp}\right)^{\top} \mathbf{c}$ in (6) and the term $\left(\mu_{0}+\tau \mu_{1}\right) \mathbf{a}^{\perp}\left(\mathbf{u}^{\perp}\right)^{\top} \mathbf{c}+\gamma \mathbf{a}^{\perp}$ in (7) are uniformly distributed over $\operatorname{Span}\left(\mathbf{a}^{\perp}\right)=\left\{\gamma^{*} \mathbf{a}^{\perp} \mid \gamma^{*} \in \mathbb{Z}_{p}\right\}$, due to the randomness of $\mu_{0}$ and $\mu_{1}$. Consequently, $\mathbf{G}_{4 . \eta .2}$ (which computes $[\mathbf{d}]_{1}$ in the $(\eta+1)$-th $\mathcal{O}_{\text {SIGN }}$ query according to (6)) and $\mathrm{G}_{4 . \eta .3}$ (which computes $[\mathbf{d}]_{1}$ in the $(\eta+1)$-th $\mathcal{O}_{\text {SIGN }}$ query according to (7)) are identically distributed, except with probability $1 / p$. This shows that $\left|\operatorname{Pr}_{4 . \eta .2}[\mathrm{Win}]-\operatorname{Pr}_{4 . \eta .3}[\mathrm{Win}]\right| \leq 1 / p$, and Claim 4 follows.

Game $\mathrm{G}_{4 . \eta .4}, 0 \leq \eta \leq Q-1$ : It is the same as $\mathrm{G}_{4 . \eta \cdot 3}$, except that, the event Win is changed back to

$$
\left(m^{*}, \sigma^{*}\right) \notin \mathcal{Q}_{\text {id }} \wedge\left[\mathbf{d}^{*}\right]_{1}=\left[\left(\mathbf{K}+\mathbf{K}_{0}+\tau^{*} \mathbf{K}_{1}\right) \mathbf{c}^{*}\right]_{1} \wedge\left[\mathbf{c}^{*}\right]_{1} \neq[\mathbf{0}]_{1} \wedge \tau^{*} \notin \mathcal{Q}_{\operatorname{tag}} \wedge\left[\mathbf{c}^{*}\right]_{1} \in \operatorname{Span}\left([\mathbf{U}]_{1}\right) .
$$

The transition from $\mathrm{G}_{4 . \eta .3}$ to $\mathrm{G}_{4 . \eta .4}$ is reverse to the transition from $\mathrm{G}_{4 . \eta .1}$ to $\mathrm{G}_{4 . \eta .2}$. Similar to Claim 3, we have the following claim.

Claim 5. $\left|\operatorname{Pr}_{4 . \eta .3}[\mathrm{Win}]-\operatorname{Pr}_{4 . \eta \cdot 4}[\mathrm{Win}]\right| \leq 1 / p$.
Now we analyze the difference between $\mathrm{G}_{4 . \eta \cdot 4}$ and $\mathrm{G}_{4 . \eta+1.0}$. The only difference is the distribution of $[\mathbf{c}]_{1}$ in the $(\eta+1)$-th $\mathcal{O}_{\text {SIGN }}$ query, where in $G_{4 . \eta .4}$,
$[\mathbf{c}]_{1} \leftarrow \leftarrow_{\mathbb{S}} \mathbb{G}_{1}^{k+1}$ is chosen uniformly at random, while in $G_{4 . \eta+1.0},[\mathbf{c}]_{1}:=[\mathbf{U}]_{1} \mathbf{w}$ with $\mathbf{w} \leftarrow_{s} \mathbb{Z}_{p}^{k}$. It is clearly that $\mathrm{G}_{4 . \eta .4}$ and $\mathrm{G}_{4 . \eta+1.0}$ are computationally indistinguishable to $\mathcal{A}$, under the $\mathcal{D}_{k}$-MDDH assumption on $[\mathbf{U}]_{1}$. Therefore, we have $\left|\operatorname{Pr}_{4 . \eta .4}[\mathrm{Win}]-\operatorname{Pr}_{4 . \eta+1.0}[\mathrm{Win}]\right| \leq \operatorname{Adv}_{\mathcal{D}_{k}, \mathbb{G}_{1}, \mathcal{B}_{5}}^{\mathrm{mddh}}(\lambda)$ for a PPT adversary $\mathcal{B}_{5}$.

Finally, we arrive at $G_{4 . Q .0}$, which is restated as follows.
Game $\mathrm{G}_{4 . Q .0}$ : It is the same as $\mathrm{G}_{3}$, except that, at the beginning of the game, the challenger picks a non-zero vector $\mathbf{a}^{\perp} \in \mathbb{Z}_{p}^{k+1}$ in the kernel of $\mathbf{A}$ such that $\left(\mathbf{a}^{\perp}\right)^{\top} \mathbf{A}=\mathbf{0}$. Moreover, when answering all $\mathcal{O}_{\text {SIGN }}$ queries, the challenger computes $[\mathbf{d}]_{1}:=\left(\mathbf{K}^{\prime}+\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right)[\mathbf{c}]_{1}+\left[\gamma \mathbf{a}^{\perp}\right]_{1}$ with $\gamma \leftarrow_{8} \mathbb{Z}_{p}$ chosen uniformly and independently for each query.

We have the following claim regarding $\operatorname{Pr}_{4 . Q .0}[\mathrm{Win}]$.
Claim 6. $\operatorname{Pr}_{4 . Q .0}[\mathrm{Win}] \leq 2^{-\Omega(\lambda)}$.
Proof. For the convenience of our analysis, we sample $s k=\mathbf{K} \leftarrow s \mathbb{Z}_{p}^{(k+1) \times(k+1)}$ equivalently via

$$
\mathbf{K}:=\widetilde{\mathbf{K}}+\mathbf{a}^{\perp} \mathbf{k}^{\top}
$$

where $\widetilde{\mathbf{K}} \leftarrow \& \mathbb{Z}_{p}^{(k+1) \times(k+1)}$ and $\mathbf{k} \leftarrow s \mathbb{Z}_{p}^{k+1}$. Below we analyze the information about $\mathbf{k}$ that $\mathcal{A}$ may obtain in $\mathrm{G}_{4 . Q .0}$.

- Firstly, the verification key $v k$ is

$$
\left[\mathbf{K}^{\top} \mathbf{A}\right]_{2}=\left[\left(\tilde{\mathbf{K}}^{\top}+\mathbf{k}\left(\mathbf{a}^{\perp}\right)^{\top}\right) \mathbf{A}\right]_{2}=\left[\tilde{\mathbf{K}}^{\top} \mathbf{A}\right]_{2}
$$

thus $\mathbf{k}$ is completely hidden.

- In $\mathcal{O}_{\text {SIGN }}$ queries, the tampered verification key $v k^{\prime}$ is

$$
\begin{aligned}
{\left[\mathbf{K}^{\prime \top} \mathbf{A}\right]_{2} } & =\left[\left(a \mathbf{K}^{\top}+\mathbf{B}^{\top}\right) \mathbf{A}\right]_{2}=\left[\left(a\left(\widetilde{\mathbf{K}}^{\top}+\mathbf{k}\left(\mathbf{a}^{\perp}\right)^{\top}\right)+\mathbf{B}^{\top}\right) \mathbf{A}\right]_{2} \\
& =\left[\left(a \widetilde{\mathbf{K}}^{\top}+\mathbf{B}^{\top}\right) \mathbf{A}\right]_{2},
\end{aligned}
$$

thus $\mathbf{k}$ is completely hidden. Moreover, due to the game change in $\mathrm{G}_{4 . Q .0}$, we have

$$
\begin{aligned}
{[\mathbf{d}]_{1} } & =\left(\mathbf{K}^{\prime}+\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right)[\mathbf{c}]_{1}+\left[\gamma \mathbf{a}^{\perp}\right]_{1} \\
& =\left(a \mathbf{K}+\mathbf{B}+\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right)[\mathbf{c}]_{1}+\left[\gamma \mathbf{a}^{\perp}\right]_{1} \\
& =\left(a\left(\widetilde{\mathbf{K}}+\mathbf{a}^{\perp} \mathbf{k}^{\top}\right)+\mathbf{B}+\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right)[\mathbf{c}]_{1}+\left[\gamma \mathbf{a}^{\perp}\right]_{1} \\
& =\left(a \widetilde{\mathbf{K}}+\mathbf{B}+\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right)[\mathbf{c}]_{1}+\left[a \mathbf{a}^{\perp} \mathbf{k}^{\top} \mathbf{c}+\gamma \mathbf{a}^{\perp}\right]_{1} .
\end{aligned}
$$

Since $\gamma \leftarrow \varangle \mathbb{Z}_{p}$, the term $\gamma \mathbf{a}^{\perp}$ perfectly hides $a \mathbf{a}^{\perp} \mathbf{k}^{\top} \mathbf{c}=\left(a \mathbf{k}^{\top} \mathbf{c}\right) \mathbf{a}^{\perp}$. Consequently, $\mathbf{k}$ is also completely hidden.

- From $\mathcal{O}_{\text {Leak }}$ queries, $\mathcal{A}$ obtains at most $\kappa$ bits information $L(s k)=L(\mathbf{K})=$ $L\left(\widetilde{\mathbf{K}}+\mathbf{a}^{\perp} \mathbf{k}^{\top}\right)$ about $s k$, and also about $\mathbf{k}$.

Overall, the information about $\mathbf{k}$ that $\mathcal{A}$ learns in $\mathrm{G}_{4 . Q .0}$ is at most $\kappa$ bits.
For Win to occur, $\mathcal{A}$ 's forgery $\left(m^{*}, \sigma^{*}=\left(\left[\mathbf{c}^{*}\right]_{1},\left[\mathbf{d}^{*}\right]_{1}\right)\right)$ should satisfy $\left(m^{*}, \sigma^{*}\right) \notin$ $\mathcal{Q}_{\mathrm{id}},\left[\mathbf{c}^{*}\right]_{1} \neq[\mathbf{0}]_{1}, \tau^{*} \notin \mathcal{Q}_{\mathrm{tag}}$, and

$$
\left[\mathbf{d}^{*}\right]_{1}=\left[\left(\mathbf{K}+\mathbf{K}_{0}+\tau^{*} \mathbf{K}_{1}\right) \mathbf{c}^{*}\right]_{1}=\left[\left(\widetilde{\mathbf{K}}+\mathbf{K}_{0}+\tau^{*} \mathbf{K}_{1}\right) \mathbf{c}^{*}+\mathbf{a}^{\perp} \mathbf{k}^{\top} \mathbf{c}^{*}\right]_{1} .
$$

Below we argue that such $\left[\mathbf{d}^{*}\right]_{1}$ has high entropy so that $\mathcal{A}$ can hardly compute it. We first analyze the entropy of $\left[\mathbf{d}^{*}\right]_{1}$ in the case $\kappa=0$, i.e., there is no leakage at all. In this case, $\mathbf{k}$ is uniformly distributed over $\mathbb{Z}_{p}^{k+1}$ from $\mathcal{A}$ 's view, and by $\left[\mathbf{c}^{*}\right]_{1} \neq[\mathbf{0}]_{1}$, it follows that $\mathbf{k}^{\top} \mathbf{c}^{*}$ is uniformly distributed over $\mathbb{Z}_{p}$ from $\mathcal{A}$ 's view. Therefore, $\mathbf{a}^{\perp} \mathbf{k}^{\top} \mathbf{c}^{*}$ is uniformly distributed over $\operatorname{Span}\left(\mathbf{a}^{\perp}\right)=\left\{\gamma^{*} \mathbf{a}^{\perp} \mid \gamma^{*} \in \mathbb{Z}_{p}\right\}$ from $\mathcal{A}$ 's view, and consequently, such $\left[\mathbf{d}^{*}\right]_{1}$ has $\log p$ bits of entropy from $\mathcal{A}$ 's view. Next, we analyze the entropy of $\left[\mathbf{d}^{*}\right]_{1}$ for any $\kappa \leq \log p-\Omega(\lambda)$. Even in the presence of $\kappa$ bits leakage information, $\left[\mathbf{d}^{*}\right]_{1}$ still has entropy at least $\log p-\kappa \geq \Omega(\lambda)$ bits from $\mathcal{A}$ 's view. Consequently, $\mathcal{A}$ can compute such $\left[\mathbf{d}^{*}\right]_{1}$ with probability at most $2^{-\Omega(\lambda)}$. This shows that $\operatorname{Pr}_{4 . Q .0}[\mathrm{Win}] \leq 2^{-\Omega(\lambda)}$ and Claim 6 follows.

Taking all things together, Theorem 1 follows.

## 4 More Efficient PKE with Leakage and Tamper-Resilience

In this section, we present a direct and efficient construction of public-key encryption (PKE) scheme with leakage and tamper-resilience, over asymmetric pairing groups based on the MDDH assumptions.

Concretely, in Subsect. 4.1, we formalize the leakage and tamper-resilient security for PKE, i.e., the strong LTR-CCA (sLTR-CCA) security, according to [35], and then in Subsect. 4.2 and Subsect. 4.3, we present our PKE scheme and its security proof, respectively.

### 4.1 Definition of sLTR-CCA Security

Below we recall the sLTR-CCA security for PKE defined in [35].
Definition 7 (sLTR-CCA Security for PKE). Let $\kappa=\kappa(\lambda) \in \mathbb{N}$, and $\mathcal{T}$ be a set of functions from $\mathcal{S K}$ to $\mathcal{S K}$ where $\mathcal{S K}$ is the secret key space. A PKE scheme $\mathrm{PKE}=($ Setup, Gen, Enc, Dec) is $(\kappa, \mathcal{T})$-sLTR-CCA secure, if for any PPT adversary $\mathcal{A}$, it holds that $\operatorname{Adv} \operatorname{PKE,\mathcal {A},\kappa ,\mathcal {T}}, \boldsymbol{\text { sltr-ca }}(\lambda):=\left|\operatorname{Pr}[\operatorname{Exp} \underset{\operatorname{PKE}, \mathcal{A}, \kappa, \mathcal{T}}{\text { sltrca }} \Rightarrow 1]-\frac{1}{2}\right| \leq$ $\operatorname{negl}(\lambda)$, where the experiment $\operatorname{Exp}_{\mathrm{PKE}, \mathcal{A}, \kappa, \mathcal{T}}^{\text {sitr-ca }}$ is defined in Fig. 3.

In the experiment $\operatorname{Exp} \underset{\mathrm{PKE}, \mathcal{A}, \kappa, \mathcal{T}}{\mathrm{str}-\mathrm{T}}$ defined in Fig. 3, it imposes only minimal restrictions on the $\mathcal{O}_{\text {Dec }}$ queries that $\mathcal{A}$ can make, i.e., $(T, c t) \neq\left(\mathrm{id}, c t^{*}\right)$. This is formulated in [35], as a strengthening of the (non-strong) LTR-CCA security defined in [36] where $(T, c t)$ is subject to $c t \neq c t^{*}$.

|  | $\mathcal{O}_{\text {Dec }}(T, c t):$ |
| :---: | :---: |
| pp $\leftarrow$ Setup, $(p k, s k) \leftarrow \$ \operatorname{Gen}(\mathrm{pp})$ | If $T \notin \mathcal{T}$ : Return $\perp$ |
| $\ell:=0 \quad / /$ Record the leakage length | If $(T, c t)=\left(i d, c t^{*}\right):$ Return $\perp$ |
| $\left(m_{0}, m_{1}, s t\right) \leftarrow s \mathcal{A}^{\mathcal{O}_{\text {Dec }}(\cdot, \cdot), \mathcal{O}_{\text {Leak }}(\cdot)}(\mathrm{pp}, p k)$ | Return $\operatorname{Dec}(T(s k), c t)$ |
| If $\left\|m_{0}\right\| \neq\left\|m_{1}\right\|:$ Return $\perp$ |  |
| $\beta \leftarrow \&\{0,1\} \quad / /$ Challenge bit | $\underline{\mathcal{O}_{\text {Leak }}(L): ~ / / a t ~ m o s t ~} \kappa$ leakage |
| $c t^{*} \leftarrow \mathrm{Enc}\left(p k, m_{\beta}\right)$ | If $\ell+\|L(s k)\|>\kappa$ : Return $\perp$ |
| $\beta^{\prime} \leftarrow \Phi \mathcal{A}^{\mathcal{O}_{\text {Dec }}(\cdot, \cdot)}\left(s t, c t^{*}\right)$ | $\ell:=\ell+\|L(s k)\|$ |
| If $\beta^{\prime}=\beta$ : Return 1; Else: Return 0 | Return $L(s k)$ |

Fig. 3. The $(\kappa, \mathcal{T})$-sLTR-CCA security experiment $\operatorname{Exp} \mathrm{PKE}, \mathcal{A}, \kappa, \mathcal{T}_{\text {sltr-ca }}$ for PKE , where id denotes the identity function and $|L(s k)|$ denotes the bit-length of $L(s k)$.

### 4.2 Construction of PKE from MDDH

Now we present our direct construction of sLTR-CCA secure PKE scheme over asymmetric pairing groups based on the MDDH assumptions. Let $\mathcal{D}_{k}$ be a matrix distribution with $k \in \mathbb{N}$, let $\mathcal{U}_{k+2, k}$ be the uniform distribution, and let $\mathcal{H}$ be a family of collision resistant hash functions from $\{0,1\}^{*}$ to $\mathbb{Z}_{p}$. Our PKE scheme PKE $=$ (Setup, Gen, Enc, Dec) is shown in Fig. 4, where the message space is $\mathcal{M}=\mathbb{G}_{1}$ and the secret key space is $\mathcal{S K}=\mathbb{Z}_{p}^{k+2}$. Correctness of PKE follows by inspection: for any honestly generated ciphertext $c t=\left([\mathbf{c}]_{1},[d]_{1},[\mathbf{e}]_{1}\right)$, we have $[\mathbf{c}]_{1}=[\mathbf{U}]_{1} \mathbf{w},[d]_{1}=\left[\mathbf{k}^{\top} \mathbf{U}\right]_{1} \mathbf{w}+m=\mathbf{k}^{\top}[\mathbf{c}]_{1}+m$ and $[\mathbf{e}]_{1}=\left[\left(\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right) \mathbf{U}\right]_{1} \mathbf{w}=$ $\left[\left(\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right) \mathbf{c}\right]_{1}$, which implies

$$
e\left(\left[\mathbf{c}^{\top}\right]_{1},\left[\left(\mathbf{K}_{0}^{\top}+\tau \mathbf{K}_{1}^{\top}\right) \mathbf{A}\right]_{2}\right)=e\left(\left[\mathbf{c}^{\top}\left(\mathbf{K}_{0}^{\top}+\tau \mathbf{K}_{1}^{\top}\right)\right]_{1},[\mathbf{A}]_{2}\right)=e\left(\left[\mathbf{e}^{\top}\right]_{1},[\mathbf{A}]_{2}\right) .
$$

Next, we show its $\left(\kappa, \mathcal{T}_{\text {aff }}\right)$-sLTR-CCA security under $\kappa \leq \log p-\Omega(\lambda)$ bits of leakage information and under the set of affine functions

$$
\begin{equation*}
\mathcal{T}_{\text {aff }}=\left\{T_{(a, \mathbf{b})}: \mathbf{k} \in \mathcal{S K} \mapsto a \mathbf{k}+\mathbf{b} \in \mathcal{S K} \mid a \in \mathbb{Z}_{p}, \mathbf{b} \in \mathcal{S K}\right\} \tag{8}
\end{equation*}
$$

Theorem 2 ( $\left(\kappa, \mathcal{T}_{\text {aff }}\right)$-sLTR-CCA Security of PKE). Let $\kappa \leq \log p-\Omega(\lambda)$ and let $\mathcal{T}_{\text {aff }}$ be the set of affine functions defined in (8). Assume that the $\mathcal{D}_{k}-M D D H$ assumption holds over both $\mathbb{G}_{1}$ and $\mathbb{G}_{2}$, and $\mathcal{H}$ is collision-resistant. Then the PKE scheme in Fig. 4 is $\left(\kappa, \mathcal{T}_{\text {aff }}\right)$-sLTR-CCA secure.

Concretely, for any PPT adversary $\mathcal{A}$, there exist PPT adversaries $\mathcal{B}_{1}, \cdots, \mathcal{B}_{4}$, such that

$$
\begin{aligned}
\operatorname{Adv}_{\mathrm{PKE}, \mathcal{A}, \kappa, \mathcal{T}}^{\text {slt-caa }}(\lambda) \leq & \operatorname{Adv}_{\mathcal{D}_{k}, \mathbb{G}_{2}, \mathcal{B}_{1}}^{\mathrm{mdd}}(\lambda)+\operatorname{Adv}_{\mathcal{H}, \mathcal{B}_{2}}^{\mathrm{cr}}(\lambda)+\operatorname{Adv}_{\mathcal{U}_{k+2, k}, \mathbb{G}_{1}, \mathcal{B}_{3}}^{\text {mddh }}(\lambda) \\
& +\operatorname{Adv}_{\mathcal{U}_{k+2, k}, \mathbb{G}_{1}, \mathcal{B}_{4}}^{\text {mddh }}(\lambda)+2^{-\Omega(\lambda)} .
\end{aligned}
$$

The proof of Theorem 2 is postponed to Subsect. 4.3. Before presenting the formal proof, we give a detailed efficiency analysis and explain the main intuitions of our PKE construction in the following two remarks, respectively.

| pp $\leftarrow$ S Setup: | $\frac{c t \leftarrow \mathrm{~s} \operatorname{Enc}\left(p k, m \in \mathbb{G}_{1}\right):}{\mathbf{w} \leftarrow \mathbb{Z}_{p}^{k}, \quad[\mathbf{c}]_{1}:=[\mathbf{U}]_{1} \mathbf{w}} \in \mathbb{G}_{1}^{k+2} .$ |
| :---: | :---: |
| $\begin{aligned} & \text { gpar }=\left(\mathbb{G}_{1}, \mathbb{G}_{2}, \mathbb{G}_{T}, p, e, P_{1}, P_{2}, P_{T}\right) \leftarrow \mathrm{s} \text { PGGen. } \\ & \mathbf{U} \leftarrow \mathrm{s} \mathcal{U}_{k+2, k}, \text { where } \mathbf{U} \in \mathbb{Z}_{p}^{(+2+2) \times k} . \end{aligned}$ | $[d]_{1}:=\left[\mathbf{k}^{\top} \mathbf{U}\right]_{1} \mathbf{w}+m \in \mathbb{G}_{1} .$ |
| $\mathbf{A} \leftarrow \mathcal{D}_{k}$, where $\mathbf{A} \in \mathbb{Z}_{p}^{(k+1) \times k}$. | $\tau:=H\left(p k,[\mathbf{c}]_{1},[d]_{1}\right) \in \mathbb{Z}_{p}$. |
| $\mathbf{K}_{0}, \mathbf{K}_{1} \leftarrow \mathrm{~s} \mathbb{Z}_{p}^{(k+1) \times(k+2)}$. | $[\mathbf{e}]_{1}:=\left[\left(\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right) \mathbf{U}\right]_{1} \mathbf{w} \in \mathbb{G}_{1}^{k+1}$. |
| $H \leftarrow \mathcal{H}$. <br> Return pp : $=\left(\right.$ gpar, $[\mathbf{U}]_{1},\left[\mathbf{K}_{0} \mathbf{U}\right]_{1},\left[\mathbf{K}_{1} \mathbf{U}\right]_{1}$, | $\text { Return } c t:=\left([\mathbf{c}]_{1},[d]_{1},[\mathbf{e}]_{1}\right) \in \mathbb{G}_{1}^{k+2} \times \mathbb{G}_{1} \times \mathbb{G}_{1}^{k+1}$ |
| $\left.[\mathbf{A}]_{2},\left[\mathbf{K}_{0}^{\top} \mathbf{A}\right]_{2},\left[\mathbf{K}_{1}^{\top} \mathbf{A}\right]_{2}, H\right)$. | $\frac{m / \perp \leftarrow \operatorname{Dec}(s k, c t):}{\text { Parse } c t=\left([\mathbf{c}]_{1},[d]_{1},[\mathbf{e}]_{1}\right) .}$ |
| $\underline{(p k, s k) \leftarrow s \mathrm{Gen}(\mathrm{pp})}$ : | $p k:=\left[\mathbf{k}^{\top} \mathbf{U}\right]_{1} .$ |
| $s k:=\mathbf{k} \leftarrow s \mathbb{Z}_{p}^{k+2} .$ | $\tau:=H\left(p k,[\mathbf{c}]_{1},[d]_{1}\right) \in \mathbb{Z}_{p}$. |
| $p k:=\left[\mathbf{k}^{\top} \mathbf{U}\right]_{1} \in \mathbb{G}_{1}^{1 \times k} .$ | If $e\left(\left[\mathbf{c}^{\top}\right]_{1},\left[\left(\mathbf{K}_{0}^{\top}+\tau \mathbf{K}_{1}^{\top}\right) \mathbf{A}\right]_{2}\right)=e\left(\left[\mathbf{e}^{\top}\right]_{1},[\mathbf{A}]_{2}\right)$ : |
| Return ( $p k, s k$ ) . | Return $m:=[d]_{1}-\mathbf{k}^{\top}[\mathbf{c}]_{1} \in \mathbb{G}_{1}$. <br> Else: Return $\perp$. |

Fig. 4. Construction of PKE $=$ (Setup, Gen, Enc, Dec) based on MDDH, where the framed boxes and the gray boxes are used to help explain the intuitions behind the construction in Remark 5.

Remark 4 (Efficiency of our PKE). Let $x \cdot \mathbb{G}$ denote $x$ elements in a group $\mathbb{G}$. Our PKE scheme in Fig. 4 is parameterized by the MDDH parameter $k \in \mathbb{N}$, and has public parameter $\mathrm{pp}:\left(3 k^{2}+4 k\right) \cdot \mathbb{G}_{1}+\left(3 k^{2}+5 k\right) \cdot \mathbb{G}_{2}$, public key $p k: k \cdot \mathbb{G}_{1}$, secret key $s k:(k+2) \cdot \mathbb{Z}_{p}$ and ciphertext $c t:(2 k+4) \cdot \mathbb{G}_{1}$. The decryption involves ( $2 k^{2}+3 k$ ) pairing operations.

For $k=1$, we get an efficient PKE scheme with pp:7• $\mathbb{G}_{1}+8 \cdot \mathbb{G}_{2}$, public key $p k: 1 \cdot \mathbb{G}_{2}$, secret key $s k: 3 \cdot \mathbb{Z}_{p}$ and ciphertext ct: $6 \cdot \mathbb{G}_{1}$, and the decryption involves only 5 pairing operations. The resulting PKE scheme is $\left(\kappa, \mathcal{T}_{\text {aff }}\right)$-sLTR-CCA secure based on the standard SXDH assumption, and supports $\kappa=\log p-\Omega(\lambda)$ bits key leakage. The leakage rate is $\frac{\log p-\Omega(\lambda)}{3 \log p}=\frac{1}{3}-o(1)$ asymptotically as $p$ grows.

Remark 5 (Intuitions of our PKE). Similar to our SIG scheme proposed in Subsect. 3.2, our PKE in Fig. 4 can also be parsed as two components: the terms in framed boxes (which are related to $\mathbf{k}$ ) and the terms in gray boxes
(which are related to $\mathbf{K}_{0}$ and $\mathbf{K}_{1}$ ).
Our first idea is to let $s k=\mathbf{k}$ involve only term of the first component, similar to our SIG scheme, so that we only need to analyze the first component in the leakage and tampering-resilient setting.

Our second idea is to use the first component to mask the message during the generation of ciphertext, while use the second component to prove the wellformedness of ciphertext. More concretely, the first component can be viewed as the CPA-secure variant of the Cramer-Shoup PKE scheme [8] (which corresponds to the $[\mathbf{c}]_{1},[d]_{1}$ in our $c t$ ), and the second component can be viewed as the onetime simulation-sound (OTSS) NIZK scheme proposed by Kiltz and Wee [27]
(which corresponds to the $[\mathbf{e}]_{1}$ in our ct and essentially proves that $[\mathbf{c}]_{1}$ belongs to the linear subspace $\left.\operatorname{Span}\left([\mathbf{U}]_{1}\right)\right)$. The efficiency of our PKE scheme benefits from the efficiency of their schemes. For example, the Kiltz-Wee OTSS-NIZK has a very short proof, which is much shorter than the tSE-NIZK [12] usually required when constructing schemes in the leakage and tamper-resilient setting. However, the sLTR-CCA security of our PKE scheme does not simply follow from the CPA-security of the Cramer-Shoup PKE variant and the OTSS of the Kiltz-Wee NIZK. In fact, our sLTR-CCA security proof also relies on the concrete algebraic structures of the schemes and involves many subtleties similar to the sLTR-CMA security proof of our SIG scheme in Subsect. 3.2, as explained later.

Below we explain the intuitions behind these two components in more detail.
Intuitions behind The First Component. Intuitively, the terms in framed boxes can be viewed as the CPA-secure variant of the Cramer-Shoup PKE scheme [8]:

- the secret key is $s k=\mathbf{k}$ and the public key is $p k=\left[\mathbf{k}^{\top} \mathbf{U}\right]_{1}$;
- the ciphertext of message $m \in \mathbb{G}_{1}$ is simply

$$
\begin{equation*}
\left([\mathbf{c}]_{1}=[\mathbf{U}]_{1} \mathbf{w},[d]_{1}=\left[\mathbf{k}^{\top} \mathbf{U}\right]_{1} \mathbf{w}+m\right), \quad \text { with } \mathbf{w} \leftarrow \mathrm{s} \mathbb{Z}_{p}^{k} \tag{9}
\end{equation*}
$$

and the decryption simply computes $m=[d]_{1}-\mathbf{k}^{\top}[\mathbf{c}]_{1}$.
It is worthwhile to briefly recall why this component is CPA secure. Its CPA security proof consists of two main steps.

- Firstly, we change the generation of the challenge ciphertext as follows

$$
\begin{equation*}
\left(\left[\mathbf{c}^{*}\right]_{1} \leftarrow \mathbb{\mathbb { G } _ { 1 } ^ { k + 2 }},\left[d^{*}\right]_{1}=\left[\mathbf{k}^{\top} \mathbf{c}^{*}\right]_{1}+m\right) \tag{10}
\end{equation*}
$$

Observe that (10) is computationally indistinguishable from (9) under the $\mathcal{U}_{k+2, k}$-MDDH assumption on $[\mathbf{U}]_{1}$ (which is further implied by the $\mathcal{D}_{k^{-}}$ MDDH assumption according to Lemma 2).

- Since $\left[\mathbf{c}^{*}\right]_{1} \leftarrow \leftarrow_{1}^{k+2}$ is uniformly chosen, the mapping $\mathbf{k} \mapsto\left[\mathbf{k}^{\top} \mathbf{c}^{*}\right]_{1}$ indexed by $\left[\mathbf{c}^{*}\right]_{1}$ is a universal hash function.

Note that in the presence of only $p k=\left[\mathbf{k}^{\top} \mathbf{U}\right]_{1}$, where $\mathbf{U} \in \mathbb{Z}_{p}^{(k+2) \times k}$, $s k=\mathbf{k}$ retains $2 \log p$ bits of entropy, so it can be extracted by the universal hash function to yield a (statistically close to) uniform element $\left[\mathbf{k}^{\top} \mathbf{c}^{*}\right]_{1} \in$ $\mathbb{G}_{1}$ in (10) (according to the leftover hash lemma, i.e., Lemma 1). Consequently, the term $\left[\mathbf{k}^{\top} \mathbf{c}^{*}\right]_{1}$ in (10) hides the message $m$.

Insufficiency of The First Component and Arising of The Second.
The first component and its CPA security proof serve as the basis for the security of our PKE. Moreover, the first component is in fact resilient to bounded key
leakage, as noted by Naor and Segev in [32]. This is because the above argument for CPA security holds even if the adversary obtains bounded leakage information about $s k=\mathbf{k}$, as long as the amount of leakage $\kappa$ satisfies $\log p-\kappa \geq \Omega(\lambda)$ so that there are still $2 \log p-\kappa \geq \log p+\Omega(\lambda)$ bits entropy left in $\mathbf{k}$ to extract a uniform group element $\left[\mathbf{k}^{\top} \mathbf{c}^{*}\right]_{1} \in \mathbb{G}_{1}$. This shows the CPA security in the leakage setting of our PKE.

However, in the sLTR-CCA security experiment, $\mathcal{A}$ has also access to a decryption oracle, through which $\mathcal{A}$ can obtain the decryption results of multiple ciphertexts, under tampered secret keys $T_{(a, \mathbf{b})}(s k)=a \mathbf{k}+\mathbf{b}$. So the decryption oracle would leak additional information about $s k=\mathbf{k}$ beyond $p k$.

To rescue the above arguments, we resort to the terms in gray boxes . Roughly speaking, we use $\left[\left(\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right) \mathbf{U}\right]_{1} \mathbf{w}$ as a OTSS-NIZK, as shown in [27], to prove the well-formedness of ciphertexts. This guarantees that the decryption result of a ciphertext $c t=\left([\mathbf{c}]_{1},[d]_{1},[\mathbf{e}]_{1}\right)$ is not $\perp$, i.e., $[\mathbf{e}]_{1}$ satisfies $e\left(\left[\mathbf{c}^{\top}\right]_{1},\left[\left(\mathbf{K}_{0}^{\top}+\tau \mathbf{K}_{1}^{\top}\right) \mathbf{A}\right]_{2}\right)=$ $e\left(\left[\mathbf{e}^{\top}\right]_{1},[\mathbf{A}]_{2}\right)$, only when one of the following two cases occur:

- Case 1: $[\mathbf{c}]_{1} \in \operatorname{Span}\left([\mathbf{U}]_{1}\right)$, or
- Case 2: the tag $\tau=H\left(p k^{\prime}=\left[(a \mathbf{k}+\mathbf{b})^{\top} \mathbf{U}\right]_{1},[\mathbf{c}]_{1},[d]_{1}\right)$ is identical to the $\operatorname{tag} \tau^{*}=H\left(p k=\left[\mathbf{k}^{\top} \mathbf{U}\right]_{1},\left[\mathbf{c}^{*}\right]_{1},\left[d^{*}\right]_{1}\right)$ involved in the challenge ciphertext $c t^{*}=\left(\left[\mathbf{c}^{*}\right]_{1},\left[d^{*}\right]_{1},\left[\mathbf{e}^{*}\right]_{1}\right)$.
If Case 1 occurs, i.e., $[\mathbf{c}]_{1}=[\mathbf{U}]_{1} \mathbf{w}$ for some $\mathbf{w} \in \mathbb{Z}_{p}^{k}$, then the decryption result under tampered secret key $T_{(a, \mathbf{b})}(s k)=a \mathbf{k}+\mathbf{b}$ would be $m=[d]_{1}-$ $\left(a \mathbf{k}^{\top}+\mathbf{b}^{\top}\right)[\mathbf{c}]_{1}=[d]_{1}-\left(a\left[\mathbf{k}^{\top} \mathbf{U}\right]_{1} \mathbf{w}+\mathbf{b}^{\top}[\mathbf{c}]_{1}\right)$, which leaks no information about $s k=\mathbf{k}$ beyond $p k=\left[\mathbf{k}^{\top} \mathbf{U}\right]_{1}$ to $\mathcal{A}$.

However, for all decryption queries made by $\mathcal{A}$, the OTSS property can only ensure either Case 1 or Case 2 occur. So, it is important for us to prove that Case 2 can hardly occur and it is always Case 1 that occurs, then we can use the above argument to show that the decryption oracle does not leak any information about $s k$ beyond $p k$ to $\mathcal{A}$.

To show that Case 2 hardly occurs, we can use similar techniques as the analysis of TagColl in the security proof of our SIG, i.e., dividing Case 2 into three sub-cases and analyzing them individually to show that they all rarely occur, by utilizing the concrete algebraic structures of our construction, based on the collision resistance of $H$ and on the MDDH assumption.

Putting Two Components Together. Overall, we carefully design our PKE construction so that the two components interplay with each other properly and help us to achieve sLTR-CCA security: the terms $\left[\left(\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right) \mathbf{U}\right]_{1} \mathbf{w}$ in the second component ensure that the decryption oracle under tampered secret keys do not leak any information about $s k=\mathbf{k}$ beyond $p k$ to the adversary, so that the decryption oracle is of no use to the adversary, and then the sLTR-CCA security of our PKE follows from the CPA security of the first component in the key leakage setting.

### 4.3 Proof of Theorem 2

Now we present the formal proof of Theorem 2. Let $\mathcal{A}$ be any PPT adversary against the $\left(\kappa, \mathcal{T}_{\text {aff }}\right)$-sLTR-CCA security of PKE, where $\mathcal{A}$ makes $Q$ times of $\mathcal{O}_{\text {Dec }}$ queries. We prove the theorem via a sequence of games $G_{0}-G_{6}$, where $G_{0}$ is the $\left(\kappa, \mathcal{T}_{\text {aff }}\right)$-sLTR-CCA experiment, and in $\mathrm{G}_{6}, \mathcal{A}$ has no advantage. A brief description of differences between adjacent games is summarized in Table 2.

Table 2. Brief Description of Games $\mathrm{G}_{0}-\mathrm{G}_{6}$ for the ( $\kappa, \mathcal{T}_{\text {aff }}$ )-sLTR-CCA security proof of PKE, where the differences between adjacent games are highlighted in gray boxes. Here column "Challenge ciphertext $c t^{*}$ " suggests how the challenge ciphertext $c t^{*}=\left(\left[\mathbf{c}^{*}\right]_{1},\left[d^{*}\right]_{1},\left[\mathbf{e}^{*}\right]_{1}\right)$ is generated: sub-column " $\left[\mathbf{c}^{*}\right]_{1} \leftarrow \Phi$ " refers to the space from which $\left[\mathbf{c}^{*}\right]_{1}$ is chosen; sub-columns " $\left[d^{*}\right]_{1}=$ " and " $\left[\mathbf{e}^{*}\right]_{1}=$ " show the computation of $\left[d^{*}\right]_{1}$ and $\left[\mathbf{e}^{*}\right]_{1}$ respectively, where $\tau^{*}:=H\left(p k,\left[\mathbf{c}^{*}\right]_{1},\left[d^{*}\right]_{1}\right)$. Column " $\mathcal{O}_{\text {Dec }}$ 's additional check" describes the additional check made by $\mathcal{O}_{\text {Dec }}$ upon a decryption query $\left(T_{(a, \mathbf{b})} \in \mathcal{T}_{\text {aff }}, c t=\left([\mathbf{c}]_{1},[d]_{1},[\mathbf{e}]_{1}\right)\right)$, besides the routine check $\left(T_{(a, \mathbf{b})}, c t\right) \neq\left(\mathrm{id}, c t^{*}\right) \wedge e\left(\left[\mathbf{c}^{\top}\right]_{1},\left[\left(\mathbf{K}_{0}^{\top}+\tau \mathbf{K}_{1}^{\top}\right) \mathbf{A}\right]_{2}\right)=e\left(\left[\mathbf{e}^{\top}\right]_{1},[\mathbf{A}]_{2}\right) ; \mathcal{O}_{\text {Dec }}$ outputs $\perp$ if the check fails. Column " $\mathcal{O}_{\text {Leak }}$ " shows the output returned by $\mathcal{O}_{\text {Leak }}$. Recall that $\mathcal{A}$ is not allowed to query $\mathcal{O}_{\text {Leak }}$ after receiving the challenge ciphertext.

|  | Challenge ciphertext $c t^{*}$ |  |  | $\begin{aligned} \mathcal{O}_{\mathrm{DEC}}\left(T_{(a, \mathbf{b})}\right. & \left.\in \mathcal{T}_{\text {aff }}, c t=\left([\mathbf{c}]_{1},[d]_{1},[\mathbf{e}]_{1}\right)\right) \text { 's } \\ & \text { additional check } \end{aligned}$ | $\mathcal{O}_{\text {Leak }}(L)$ | Justification/Assumption |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: |
|  | $\left[\mathrm{c}^{*}\right]_{1} \leftarrow \mathrm{~s}$ | $\left[d^{*}\right]_{1}=$ | $\left[\mathrm{e}^{*}\right]_{1}=$ |  |  |  |
| $\mathrm{G}_{0}$ | Span ([U] ${ }_{1}$ ) | $\left[\mathbf{k}^{\top} \mathbf{U}\right]_{1} \mathbf{w}^{*}+m_{\beta}$ | $\left[\left(\mathbf{K}_{0}+\tau^{*} \mathbf{K}_{1}\right) \mathbf{U}\right]_{1} \mathbf{w}^{*}$ |  | $L(s k)$ | $\left(\kappa, \mathcal{T}_{\text {aff }}\right)$-sLTR-CCA experiment |
| $\mathrm{G}_{1}$ | Span ([U] ${ }_{1}$ ) | $\mathbf{k}^{\top}\left[\mathbf{c}^{*}\right]_{1}+m_{\beta}$ | $\left(\mathbf{K}_{0}+\tau^{*} \mathbf{K}_{1}\right)\left[\mathbf{c}^{*}\right]_{1}$ |  | $L(s k)$ | $\mathrm{G}_{0}=\mathrm{G}_{1}$ |
| $\mathrm{G}_{2}$ | Span ([U] ${ }_{1}$ ) | $\mathbf{k}^{\top}\left[\mathbf{c}^{*}\right]_{1}+m_{\beta}$ | $\left(\mathbf{K}_{0}+\tau^{*} \mathbf{K}_{1}\right)\left[\mathbf{c}^{*}\right]_{1}$ | $[\mathbf{e}]_{1}=\left[\left(\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right) \mathbf{c}\right]_{1}$ | $L(s k)$ | $\mathcal{D}_{k}$-KerMDH on $[\mathbf{A}]_{2}$ |
| $\mathrm{G}_{3}$ | Span ([U] ${ }_{1}$ ) | $\mathbf{k}^{\top}\left[\mathbf{c}^{*}\right]_{1}+m_{\beta}$ | $\left(\mathbf{K}_{0}+\tau^{*} \mathbf{K}_{1}\right)\left[\mathbf{c}^{*}\right]_{1}$ | $[\mathbf{e}]_{1}=\left[\left(\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right) \mathbf{c}\right]_{1}, \tau \neq \tau^{*}$ | $L(s k)$ | $\begin{aligned} & \text { Collision-resistance of } \mathcal{H} \\ & \& \mathcal{U}_{k+2, k} \text {-KerMDH on }[\mathbf{U}]_{1} \end{aligned}$ |
| $\mathrm{G}_{4}$ | $\mathbb{G}_{1}^{k+2}$ | $\mathbf{k}^{\top}\left[\mathbf{c}^{*}\right]_{1}+m_{\beta}$ | $\left(\mathbf{K}_{0}+\tau^{*} \mathbf{K}_{1}\right)\left[\mathbf{c}^{*}\right]_{1}$ | $[\mathbf{e}]_{1}=\left[\left(\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right) \mathbf{c}\right]_{1}, \tau \neq \tau^{*}$ | $L(s k)$ | $\mathcal{U}_{k+2, k}-\mathrm{MDDH}$ on $[\mathbf{U}]_{1}$ |
| $\mathrm{G}_{5}$ | $\mathbb{G}_{1}^{k+2}$ | $\mathbf{k}^{\top}\left[\mathbf{c}^{*}\right]_{1}+m_{\beta}$ | $\left(\mathbf{K}_{0}+\tau^{*} \mathbf{K}_{1}\right)\left[\mathbf{c}^{*}\right]_{1}$ | $[\mathbf{e}]_{1}=\left[\left(\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right) \mathbf{c}\right]_{1}, \tau \neq \tau^{*},[\mathbf{c}]_{1} \in \operatorname{Span}\left([\mathbf{U}]_{1}\right)$ | $L(s k)$ | Statistical arguments using the leftover entropy in $\mathbf{K}_{0}, \mathbf{K}_{1}$ |
| $\mathrm{G}_{6}$ | $\mathbb{G}_{1}^{k+2}$ | random | $\left(\mathbf{K}_{0}+\tau^{*} \mathbf{K}_{1}\right)\left[\mathbf{c}^{*}\right]_{1}$ | $[\mathbf{e}]_{1}=\left[\left(\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right) \mathbf{c}\right]_{1}, \tau \neq \tau^{*},[\mathbf{c}]_{1} \in \operatorname{Span}\left([\mathbf{U}]_{1}\right)$ | $L(s k)$ | Statistical arguments using the leftover entropy in $\mathbf{K}$ |
|  |  |  |  |  |  | $\operatorname{Pr}[\mathrm{Win}]=\frac{1}{2}$ in $\mathrm{G}_{6}$ |

Game $\mathrm{G}_{0}$ : This is the ( $\kappa, \mathcal{T}_{\text {aff }}$ )-sLTR-CCA experiment (cf. Fig. 3). Let Win denote the event that $\beta^{\prime}=\beta$. By definition, $\operatorname{Adv}_{\operatorname{PKE}, \mathcal{A}, \kappa, \mathcal{T}}^{\text {sitr ca }}(\lambda)=\left|\operatorname{Pr}_{0}[\mathrm{Win}]-\frac{1}{2}\right|$.

Let $\mathrm{pp}=\left(\right.$ gpar, $\left.[\mathbf{U}]_{1},\left[\mathbf{K}_{0} \mathbf{U}\right]_{1},\left[\mathbf{K}_{1} \mathbf{U}\right]_{1},[\mathbf{A}]_{2},\left[\mathbf{K}_{0}^{\top} \mathbf{A}\right]_{2},\left[\mathbf{K}_{1}^{\top} \mathbf{A}\right]_{2}, H\right)$ and $(p k=$ $\left[\mathbf{k}^{\top} \mathbf{U}\right]_{1}, s k=\mathbf{k}$ ). In this game, the challenge ciphertext $c t^{*}$ that encrypts $m_{\beta}$ is generated as follows. The challenger samples $\mathbf{w}^{*} \leftarrow_{\&} \mathbb{Z}_{p}^{k}$, computes $\left[\mathbf{c}^{*}\right]_{1}:=$ $[\mathbf{U}]_{1} \mathbf{w}^{*},\left[d^{*}\right]_{1}:=\left[\mathbf{k}^{\top} \mathbf{U}\right]_{1} \mathbf{w}^{*}+m_{\beta}, \tau^{*}:=H\left(p k,\left[\mathbf{c}^{*}\right]_{1},\left[d^{*}\right]_{1}\right) \in \mathbb{Z}_{p},\left[\mathbf{e}^{*}\right]_{1}:=\left[\left(\mathbf{K}_{0}+\right.\right.$ $\left.\left.\tau^{*} \mathbf{K}_{1}\right) \mathbf{U}\right]_{1} \mathbf{w}^{*}$, and returns the challenge ciphertext $c t^{*}:=\left(\left[\mathbf{c}^{*}\right]_{1},\left[d^{*}\right]_{1},\left[\mathbf{e}^{*}\right]_{1}\right)$ to $\mathcal{A}$. Upon an $\mathcal{O}_{\text {Dec }}$ query $\left(T_{(a, \mathbf{b})} \in \mathcal{T}_{\text {aff }}\right.$, $\left.c t=\left([\mathbf{c}]_{1},[d]_{1},[\mathbf{e}]_{1}\right)\right)$, the challenger computes the tampered key $s k^{\prime}=\mathbf{k}^{\prime}:=T_{(a, \mathbf{b})}(s k)=a \mathbf{k}+\mathbf{b}$ and $p k^{\prime}:=\left[\mathbf{k}^{\prime \top} \mathbf{U}\right]_{1}$, computes $\tau:=H\left(p k^{\prime},[\mathbf{c}]_{1},[d]_{1}\right)$, and checks whether $\left(T_{(a, \mathbf{b})}, c t\right) \neq\left(\mathrm{id}, c t^{*}\right) \wedge$ $e\left(\left[\mathbf{c}^{\top}\right]_{1},\left[\left(\mathbf{K}_{0}^{\top}+\tau \mathbf{K}_{1}^{\top}\right) \mathbf{A}\right]_{2}\right)=e\left(\left[\mathbf{e}^{\top}\right]_{1},[\mathbf{A}]_{2}\right)$ holds. If the check passes, the challenger computes $m:=[d]_{1}-\mathbf{k}^{\prime \top}[\mathbf{c}]_{1}$ using the tampered key $s k^{\prime}=\mathbf{k}^{\prime}$ and returns
$m$ to $\mathcal{A}$; otherwise, the challenger returns $\perp$. For an $\mathcal{O}_{\text {Leak }}$ query $L$, the challenger returns $L(s k)$ to $\mathcal{A}$ if the total leakage length is bounded by $\kappa$. Recall that $\mathcal{A}$ can query $\mathcal{O}_{\text {Dec }}$ throughout the game, but is only allowed to query $\mathcal{O}_{\text {Leak }}$ before receiving the challenge ciphertext.

Game $\mathrm{G}_{1}$ : It is the same as $\mathrm{G}_{0}$, except that, when generating the challenge ciphertext $c t^{*}$, the challenger computes $\left[d^{*}\right]_{1}:=\mathbf{k}^{\top}\left[\mathbf{c}^{*}\right]_{1}+m_{\beta}$ and $\left[\mathbf{e}^{*}\right]_{1}:=$ $\left(\mathbf{K}_{0}+\tau^{*} \mathbf{K}_{1}\right)\left[\mathbf{c}^{*}\right]_{1}$ directly from $\left[\mathbf{c}^{*}\right]_{1}, m_{\beta}, \tau^{*}$ and $\left(\mathbf{k}, \mathbf{K}_{0}, \mathbf{K}_{1}\right)$, without using the vector $\mathbf{w}^{*}$ for $\left[\mathbf{c}^{*}\right]_{1}=[\mathbf{U}]_{1} \mathbf{w}^{*}$.

Since $\left[\mathbf{c}^{*}\right]_{1}=[\mathbf{U}]_{1} \mathbf{w}^{*}$, the changes are conceptual and $\operatorname{Pr}_{0}[\mathrm{Win}]=\operatorname{Pr}_{1}[\mathrm{Win}]$.
Game $\mathrm{G}_{2}$ : It is the same as $\mathrm{G}_{1}$, except that, when answering $\mathcal{O}_{\mathrm{DEC}}\left(T_{(a, \mathbf{b})} \in\right.$ $\left.\overline{\mathcal{T}}_{\text {aff }}, c t=\left([\mathbf{c}]_{1},[d]_{1},[\mathbf{e}]_{1}\right)\right)$, the challenger returns $\perp$ to $\mathcal{A}$ directly if the following check fails:

$$
\left(T_{(a, \mathbf{b})}, c t\right) \neq\left(\mathrm{id}, c t^{*}\right) \wedge[\mathbf{e}]_{1}=\left[\left(\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right) \mathbf{c}\right]_{1}
$$

Claim 7. $\left|\operatorname{Pr}_{1}[\mathrm{Win}]-\operatorname{Pr}_{2}[\mathrm{Win}]\right| \leq \operatorname{Adv}_{\mathcal{D}_{k}, \mathbb{G}_{2}, \mathcal{B}_{1}}^{\text {mddh }}(\lambda)+1 /(p-1)$ for a PPT adversary $\mathcal{B}_{1}$ against the $\mathcal{D}_{k}-M D D H$ assumption on $[\mathbf{A}]_{2}$.

Proof sketch. The proof is similar to the proof of Claim 1. Clearly, $\mathrm{G}_{2}$ is identical to $G_{1}$ unless that $\mathcal{A}$ ever makes a $\mathcal{O}_{\text {Dec }}$ query such that

$$
e\left(\left[\mathbf{c}^{\top}\right]_{1},\left[\left(\mathbf{K}_{0}^{\top}+\tau \mathbf{K}_{1}^{\top}\right) \mathbf{A}\right]_{2}\right)=e\left(\left[\mathbf{e}^{\top}\right]_{1},[\mathbf{A}]_{2}\right) \wedge[\mathbf{e}]_{1} \neq\left[\left(\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right) \mathbf{c}\right]_{1} .
$$

We denote such an event by DecBad. Similar to the proof of Claim 1, DecBad rarely happens under the $\mathcal{D}_{k}$-KerMDH assumption on $[\mathbf{A}]_{2}$ (which is further implied by the $\mathcal{D}_{k}-\mathrm{MDDH}$ assumption on $[\mathbf{A}]_{2}$ according to Lemma 3). Consequently, Claim 7 follows.

Game $\mathrm{G}_{3}$ : It is the same as $\mathrm{G}_{2}$, except that, when answering $\mathcal{O}_{\mathrm{DeC}}\left(T_{(a, \mathbf{b})} \in\right.$ $\left.\overline{\mathcal{T}_{\text {aff }}, c t=}\left([\mathbf{c}]_{1},[d]_{1},[\mathbf{e}]_{1}\right)\right)$, the challenger now returns $\perp$ to $\mathcal{A}$ directly if the following check fails:

$$
\left(T_{(a, \mathbf{b})}, c t\right) \neq\left(\mathrm{id}, c t^{*}\right) \wedge[\mathbf{e}]_{1}=\left[\left(\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right) \mathbf{c}\right]_{1} \wedge \tau \neq \tau^{*}
$$

where $\tau:=H\left(p k^{\prime},[\mathbf{c}]_{1},[d]_{1}\right)$ and $\tau^{*}:=H\left(p k,\left[\mathbf{c}^{*}\right]_{1},\left[d^{*}\right]_{1}\right)$ are the tags involved in this $\mathcal{O}_{\text {Dec }}$ query and in the challenge ciphertext $c t^{*}$, respectively.

Claim 8. $\left|\operatorname{Pr}_{2}[\mathrm{Win}]-\operatorname{Pr}_{3}[\mathrm{Win}]\right| \leq \operatorname{Adv}_{\mathcal{H}, \mathcal{B}_{2}}^{\mathrm{cr}}(\lambda)+\operatorname{Adv}_{\mathcal{U}_{k+2, k}, \mathbb{G}_{1}, \mathcal{B}_{3}}^{\operatorname{mddh}}(\lambda)+1 /(p-1)+$ $2^{-\Omega(\lambda)}$ for PPT adversaries $\mathcal{B}_{2}$ against the collision-resistance of $\mathcal{H}$ and $\mathcal{B}_{3}$ against the $\mathcal{U}_{k+2, k}-M D D H$ assumption on $[\mathbf{U}]_{1}$.

Proof sketch. The proof is similar to the proof of Claim 2. Clearly, $\mathrm{G}_{3}$ is identical to $G_{2}$ unless that $\mathcal{A}$ ever makes a $\mathcal{O}_{\text {Dec }}$ query such that

$$
\left(T_{(a, \mathbf{b})}, c t\right) \neq\left(\mathrm{id}, c t^{*}\right) \wedge[\mathbf{e}]_{1}=\left[\left(\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right) \mathbf{c}\right]_{1} \wedge \tau=\tau^{*}
$$

We denote such an event by TagColl. Similar to the proof of Claim 2, we can divide the event TagColl into three cases, analyze them individually and finally obtain Claim 8.

Game $G_{4}$ : It is the same as $G_{3}$, except that, when generating the challenge ciphertext $c t^{*}$, the challenger samples $\left[\mathbf{c}^{*}\right]_{1} \leftarrow s \mathbb{G}_{1}^{k+2}$ uniformly at random, instead of computing $\left[\mathbf{c}^{*}\right]_{1}:=[\mathbf{U}]_{1} \mathbf{w}^{*}$ with $\mathbf{w}^{*} \leftarrow{ }_{\delta} \mathbb{Z}_{p}^{k}$.

By the $\mathcal{U}_{k+2, k}$-MDDH assumption on $[\mathbf{U}]_{1}, \mathrm{G}_{3}$ and $\mathrm{G}_{4}$ are computationally indistinguishable, and we have $\left|\operatorname{Pr}_{3}[\mathrm{Win}]-\operatorname{Pr}_{4}[\mathrm{Win}]\right| \leq \operatorname{Adv}_{\mathcal{U}_{k+2, k}, \mathbb{G}_{1}, \mathcal{B}_{4}}^{\mathrm{mdda}}(\lambda)$ for a PPT adversary $\mathcal{B}_{4}$.

Game $\mathrm{G}_{5}$ : It is the same as $\mathrm{G}_{4}$, except that, when answering $\mathcal{O}_{\mathrm{DeC}}\left(T_{(a, \mathbf{b})} \in\right.$ $\left.\overline{\mathcal{T}_{\text {aff }}, c t=}\left([\mathbf{c}]_{1},[d]_{1},[\mathbf{e}]_{1}\right)\right)$, the challenger now returns $\perp$ to $\mathcal{A}$ directly if the following check fails:
$\left(T_{(a, \mathbf{b})}, c t\right) \neq\left(\mathrm{id}, c t^{*}\right) \wedge[\mathbf{e}]_{1}=\left[\left(\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right) \mathbf{c}\right]_{1} \wedge \tau \neq \tau^{*} \wedge[\mathbf{c}]_{1} \in \operatorname{Span}\left([\mathbf{U}]_{1}\right)$.
Claim 9. $\left|\operatorname{Pr}_{4}[\mathrm{Win}]-\operatorname{Pr}_{5}[\mathrm{Win}]\right| \leq Q / p$.
Proof sketch. The proof is similar to the proof of Claim 3. Clearly, $\mathrm{G}_{5}$ is identical to $G_{4}$ unless that $\mathcal{A}$ ever makes a $\mathcal{O}_{\text {Dec }}$ query such that

$$
\left(T_{(a, \mathbf{b})}, c t\right) \neq\left(\mathrm{id}, c t^{*}\right) \wedge[\mathbf{e}]_{1}=\left[\left(\mathbf{K}_{0}+\tau \mathbf{K}_{1}\right) \mathbf{c}\right]_{1} \wedge \tau \neq \tau^{*} \wedge[\mathbf{c}]_{1} \notin \operatorname{Span}\left([\mathbf{U}]_{1}\right) .
$$

We denote such an event by CBad. Similar to the proof of Claim 3, we can analyze the information about $\mathbf{K}_{0}$ and $\mathbf{K}_{1}$ that $\mathcal{A}$ may obtain in $\mathrm{G}_{5}$, and use the leftover entropy in $\mathbf{K}_{0}$ and $\mathbf{K}_{1}$ to show that CBad occurs in a particular $\mathcal{O}_{\text {Dec }}$ query with probability at most $1 / p$. Consequently, by a union bound over $Q$ times of $\mathcal{O}_{\text {Dec }}$ queries, Claim 9 follows.

Game $\mathrm{G}_{6}$ : It is the same as $\mathrm{G}_{5}$, except that, when generating the challenge $\overline{\text { ciphertext } c t^{*}}$, the challenger samples $\left[d^{*}\right]_{1} \leftarrow \& \mathbb{G}_{1}$ uniformly at random, instead of computing $\left[d^{*}\right]_{1}:=\mathbf{k}^{\top}\left[\mathbf{c}^{*}\right]_{1}+m_{\beta}$.

Claim 10. $\left|\operatorname{Pr}_{5}[\mathrm{Win}]-\operatorname{Pr}_{6}[\mathrm{Win}]\right| \leq 2^{-\Omega(\lambda)}$.
Proof. We will show that the $\left[d^{*}\right]_{1}:=\mathbf{k}^{\top}\left[\mathbf{c}^{*}\right]_{1}+m_{\beta}$ in $G_{5}$ is statistically close to the $\left[d^{*}\right]_{1} \leftarrow \mathbb{G}_{1}$ in $G_{6}$, with statistical distance at most $2^{-\Omega(\lambda)}$.

For the convenience of our analysis, we sample $s k=\mathbf{k} \leftarrow s \mathbb{Z}_{p}^{k+2}$ equivalently via

$$
\mathbf{k}:=\widetilde{\mathbf{k}}+\mathbf{U}^{\perp} \cdot \mathbf{r}
$$

where $\widetilde{\mathbf{k}} \leftarrow \& \mathbb{Z}_{p}^{k+2}$ and $\mathbf{r} \leftarrow \& \mathbb{Z}_{p}^{2}$ are uniformly sampled, and $\mathbf{U}^{\perp} \in \mathbb{Z}_{p}^{(k+2) \times 2}$ is a non-zero vector in the kernel of $\mathbf{U} \in \mathbb{Z}_{p}^{(k+2) \times k}$ such that $\left(\mathbf{U}^{\perp}\right)^{\top} \cdot \mathbf{U}=\mathbf{0}$. Below we analyze the information about $\mathbf{r}$ that $\mathcal{A}$ may obtain in $G_{5}$ (except for the challenge ciphertext $c t^{*}$ ).

- Firstly, the public key $p k$ is

$$
\left[\mathbf{k}^{\top} \mathbf{U}\right]_{1}=\left[\left(\widetilde{\mathbf{k}}^{\top}+\mathbf{r}^{\top} \cdot\left(\mathbf{U}^{\perp}\right)^{\top}\right) \mathbf{U}\right]_{1}=\left[\widetilde{\mathbf{k}}^{\top} \mathbf{U}\right]_{1}
$$

thus $\mathbf{r}$ is completely hidden.

- In $\mathcal{O}_{\text {Dec }}$ queries, the tampered public key $p k^{\prime}$ is

$$
\left[\mathbf{k}^{\prime \top} \mathbf{U}\right]_{1}=\left[\left(a \mathbf{k}^{\top}+\mathbf{b}^{\top}\right) \mathbf{U}\right]_{1}=\left[\left(a\left(\widetilde{\mathbf{k}}^{\top}+\mathbf{r}^{\top} \cdot\left(\mathbf{U}^{\perp}\right)^{\top}\right)+\mathbf{b}^{\top}\right) \mathbf{U}\right]_{1}=\left[\left(a \widetilde{\mathbf{k}}^{\top}+\mathbf{b}^{\top}\right) \mathbf{U}\right]_{1},
$$

thus $\mathbf{r}$ is completely hidden. Moreover, due to the game change in $G_{5}$, the challenger will not output $m:=[d]_{1}-\mathbf{k}^{\top \top}[\mathbf{c}]_{1}$ unless $[\mathbf{c}]_{1} \in \operatorname{Span}\left([\mathbf{U}]_{1}\right)$, and for $[\mathbf{c}]_{1} \in \operatorname{Span}\left([\mathbf{U}]_{1}\right)$, we have

$$
\begin{aligned}
m & =[d]_{1}-\mathbf{k}^{\prime \top}[\mathbf{c}]_{1}=[d]_{1}-\left(a \mathbf{k}^{\top}+\mathbf{b}^{\top}\right)[\mathbf{c}]_{1} \\
& =[d]_{1}-\left(a\left(\widetilde{\mathbf{k}}^{\top}+\mathbf{r}^{\top} \cdot\left(\mathbf{U}^{\perp}\right)^{\top}\right)+\mathbf{b}^{\top}\right)[\mathbf{c}]_{1} \\
& =[d]_{1}-\left(a \widetilde{\mathbf{k}}^{\top}+\mathbf{b}^{\top}\right)[\mathbf{c}]_{1},
\end{aligned}
$$

thus $\mathbf{r}$ is also completely hidden.

- From $\mathcal{O}_{\text {Leak }}$ queries, $\mathcal{A}$ obtains at most $\kappa$ bits information $L(s k)=L(\mathbf{k})=$ $L\left(\widetilde{\mathbf{k}}+\mathbf{U}^{\perp} \cdot \mathbf{r}\right)$ about $s k$, and also about $\mathbf{r}$.

Overall, the information about $\mathbf{r}$ that $\mathcal{A}$ learns in $G_{5}$ (except for the challenge ciphertext $\left.c t^{*}\right)$ is at most $\kappa$ bits. Thus, there are still $2 \log p-\kappa=\log p+(\log p-$ $\kappa) \geq \log p+\Omega(\lambda)$ bits of entropy left in $\mathbf{r}$, and also in $s k=\mathbf{k}=\widetilde{\mathbf{k}}+\mathbf{U}^{\perp} \cdot \mathbf{r}$.

On the other hand, for the challenge ciphertext $c t^{*}$, note that $\left[\mathbf{c}^{*}\right]_{1}$ is uniformly chosen from $\mathbb{G}_{1}^{k+2}$ due to the game change in $\mathrm{G}_{4}$, thus the mapping $\mathbf{k} \mapsto \mathbf{k}^{\top}\left[\mathbf{c}^{*}\right]_{1}$ indexed by $\left[\mathbf{c}^{*}\right]_{1}$ is a universal hash function. By the leftover hash lemma (i.e., Lemma 1 ), $\mathbf{k}^{\top}\left[\mathbf{c}^{*}\right]_{1}$ is statistically close to the uniform distribution over $\mathbb{G}_{1}$, with statistical distance at most $\sqrt{p \cdot 2^{-(\log p+\Omega(\lambda))}}=\sqrt{2^{-\Omega(\lambda)}}$, which is also $2^{-\Omega(\lambda)}$. Consequently, the $\left[d^{*}\right]_{1}:=\mathbf{k}^{\top}\left[\mathbf{c}^{*}\right]_{1}+m_{\beta}$ in $\mathrm{G}_{5}$ is also statistically close to the uniform distribution, with statistical distance at most $2^{-\Omega(\lambda)}$. Therefore, $\mathrm{G}_{5}$ and $\mathrm{G}_{6}$ are statistically indistinguishable to $\mathcal{A}$, and Claim 10 follows.

Finally in $\mathrm{G}_{6},\left[d^{*}\right]_{1}$ is uniformly chosen regardless of the value of $\beta$, thus the challenge bit $\beta$ is completely hidden to $\mathcal{A}$. Then $\operatorname{Pr}_{6}[\mathrm{Win}]=\frac{1}{2}$.

Taking all things together, and noting that by Lemma 2 , the $\mathcal{U}_{k+2, k}-\mathrm{MDDH}$ assumption is implied by the $\mathcal{D}_{k}-\mathrm{MDDH}$ assumption, Theorem 2 follows.

Acknowledgments. We would like to thank the reviewers for their valuable comments. Shuai Han and Shengli Liu were partially supported by National Natural Science Foundation of China (Grant Nos. 62372292, 61925207), the National Key R\&D Program of China under Grant 2022YFB2701500, Guangdong Major Project of Basic and Applied Basic Research (2019B030302008), and Young Elite Scientists Sponsorship Program by China Association for Science and Technology (YESS20200185). Dawu Gu was partially supported by the National Key R\&D Program of China under Grant 2020YFA0712302.

## References

[1] Akavia, A., Goldwasser, S., Vaikuntanathan, V.: Simultaneous hardcore bits and cryptography against memory attacks. In: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, pp. 474-495. Springer, Heidelberg (Mar 2009). https://doi.org/10.1007/978-3-642-00457-5_28
[2] An, J.H., Dodis, Y., Rabin, T.: On the security of joint signature and encryption. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 83-107. Springer, Heidelberg (Apr / May 2002). https://doi.org/10.1007/3-540-46035-7_6
[3] Bellare, M., Kohno, T.: A theoretical treatment of related-key attacks: RKA-PRPs, RKA-PRFs, and applications. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 491-506. Springer, Heidelberg (May 2003). https://doi.org/10.1007/3-540-39200-9_31
[4] Bellare, M., Namprempre, C.: Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. In: Okamoto, T. (ed.) ASIACRYPT 2000. LNCS, vol. 1976, pp. 531-545. Springer, Heidelberg (Dec 2000). https://doi.org/10.1007/3-540-44448-3_41
[5] Bellare, M., Rogaway, P.: Entity authentication and key distribution. In: Stinson, D.R. (ed.) CRYPTO'93. LNCS, vol. 773, pp. 232-249. Springer, Heidelberg (Aug 1994). https://doi.org/10.1007/3-540-48329-2_21
[6] Biham, E., Shamir, A.: Differential fault analysis of secret key cryptosystems. In: Kaliski Jr., B.S. (ed.) CRYPTO'97. LNCS, vol. 1294, pp. 513-525. Springer, Heidelberg (Aug 1997). https://doi.org/10.1007/BFb0052259
[7] Chakraborty, S., Rangan, C.P.: Public key encryption resilient to post-challenge leakage and tampering attacks. In: Matsui, M. (ed.) CT-RSA 2019. LNCS, vol. 11405, pp. 23-43. Springer, Heidelberg (Mar 2019). https://doi.org/10.1007/978-3-030-12612-4_2
[8] Cramer, R., Shoup, V.: A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In: Krawczyk, H. (ed.) CRYPTO'98. LNCS, vol. 1462, pp. 13-25. Springer, Heidelberg (Aug 1998). https://doi.org/10.1007/BFb0055717
[9] Cramer, R., Shoup, V.: Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 45-64. Springer, Heidelberg (Apr / May 2002). https://doi.org/10.1007/3-540-46035-7_4
[10] Damgård, I., Faust, S., Mukherjee, P., Venturi, D.: Bounded tamper resilience: How to go beyond the algebraic barrier. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013, Part II. LNCS, vol. 8270, pp. 140-160. Springer, Heidelberg (Dec 2013). https://doi.org/10.1007/978-3-642-42045-0_8
[11] Diemert, D., Gellert, K., Jager, T., Lyu, L.: More efficient digital signatures with tight multi-user security. In: Garay, J. (ed.) PKC 2021, Part II. LNCS, vol. 12711, pp. 1-31. Springer, Heidelberg (May 2021). https://doi.org/10.1007/978-3-030-75248-4_1
[12] Dodis, Y., Haralambiev, K., López-Alt, A., Wichs, D.: Efficient publickey cryptography in the presence of key leakage. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 613-631. Springer, Heidelberg (Dec 2010). https://doi.org/10.1007/978-3-642-17373-8_35
[13] Dziembowski, S., Pietrzak, K., Wichs, D.: Non-malleable codes. In: Yao, A.C.C. (ed.) ICS 2010. pp. 434-452. Tsinghua University Press (Jan 2010)
[14] Escala, A., Herold, G., Kiltz, E., Ràfols, C., Villar, J.: An algebraic framework for Diffie-Hellman assumptions. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013, Part II. LNCS, vol. 8043, pp. 129-147. Springer, Heidelberg (Aug 2013). https://doi.org/10.1007/978-3-642-40084-1_8
[15] Faonio, A., Venturi, D.: Efficient public-key cryptography with bounded leakage and tamper resilience. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016, Part I. LNCS, vol. 10031, pp. 877-907. Springer, Heidelberg (Dec 2016). https://doi.org/10.1007/978-3-662-53887-6_32
[16] Faust, S., Mukherjee, P., Nielsen, J.B., Venturi, D.: Continuous non-malleable codes. In: Lindell, Y. (ed.) TCC 2014. LNCS, vol. 8349, pp. 465-488. Springer, Heidelberg (Feb 2014). https://doi.org/10.1007/978-3-642-54242-8_20
[17] Fiat, A., Shamir, A.: How to prove yourself: Practical solutions to identification and signature problems. In: Odlyzko, A.M. (ed.) CRYPTO'86. LNCS, vol. 263, pp. 186-194. Springer, Heidelberg (Aug 1987). https://doi.org/10.1007/3-540-477217_12
[18] Fujisaki, E., Xagawa, K.: Public-key cryptosystems resilient to continuous tampering and leakage of arbitrary functions. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016, Part I. LNCS, vol. 10031, pp. 908-938. Springer, Heidelberg (Dec 2016). https://doi.org/10.1007/978-3-662-53887-6_33
[19] Gandolfi, K., Mourtel, C., Olivier, F.: Electromagnetic analysis: Concrete results. In: Koç, Çetin Kaya., Naccache, D., Paar, C. (eds.) CHES 2001. LNCS, vol. 2162, pp. 251-261. Springer, Heidelberg (May 2001). https://doi.org/10.1007/3-540-44709-1_21
[20] Gay, R., Hofheinz, D., Kiltz, E., Wee, H.: Tightly CCA-secure encryption without pairings. In: Fischlin, M., Coron, J.S. (eds.) EUROCRYPT 2016, Part I. LNCS, vol. 9665, pp. 1-27. Springer, Heidelberg (May 2016). https://doi.org/10.1007/978-3-662-49890-3_1
[21] Gennaro, R., Lysyanskaya, A., Malkin, T., Micali, S., Rabin, T.: Algorithmic tamper-proof (ATP) security: Theoretical foundations for security against hardware tampering. In: Naor, M. (ed.) TCC 2004. LNCS, vol. 2951, pp. 258-277. Springer, Heidelberg (Feb 2004). https://doi.org/10.1007/978-3-540-24638-1_15
[22] Groth, J., Sahai, A.: Efficient non-interactive proof systems for bilinear groups. In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 415-432. Springer, Heidelberg (Apr 2008). https://doi.org/10.1007/978-3-540-78967-3_24
[23] Halderman, J.A., Schoen, S.D., Heninger, N., Clarkson, W., Paul, W., Calandrino, J.A., Feldman, A.J., Appelbaum, J., Felten, E.W.: Lest we remember: Cold boot attacks on encryption keys. In: van Oorschot, P.C. (ed.) USENIX Security 2008. pp. 45-60. USENIX Association (Jul / Aug 2008)
[24] Håstad, J., Impagliazzo, R., Levin, L.A., Luby, M.: A pseudorandom generator from any one-way function. SIAM Journal on Computing 28(4), 1364-1396 (1999). https://doi.org/10.1137/S0097539793244708
[25] Jafargholi, Z., Wichs, D.: Tamper detection and continuous non-malleable codes. In: Dodis, Y., Nielsen, J.B. (eds.) TCC 2015, Part I. LNCS, vol. 9014, pp. 451-480. Springer, Heidelberg (Mar 2015). https://doi.org/10.1007/978-3-662-46494-6_19
[26] Kalai, Y.T., Kanukurthi, B., Sahai, A.: Cryptography with tamperable and leaky memory. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 373-390. Springer, Heidelberg (Aug 2011). https://doi.org/10.1007/978-3-642-22792-9_21
[27] Kiltz, E., Wee, H.: Quasi-adaptive NIZK for linear subspaces revisited. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015, Part II. LNCS, vol. 9057, pp. 101-128. Springer, Heidelberg (Apr 2015). https://doi.org/10.1007/978-3-662-46803-6_4
[28] Kocher, P.C.: Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In: Koblitz, N. (ed.) CRYPTO'96. LNCS, vol. 1109, pp. 104113. Springer, Heidelberg (Aug 1996). https://doi.org/10.1007/3-540-68697-5_9
[29] Kocher, P.C., Jaffe, J., Jun, B.: Differential power analysis. In: Wiener, M.J. (ed.) CRYPTO'99. LNCS, vol. 1666, pp. 388-397. Springer, Heidelberg (Aug 1999). https://doi.org/10.1007/3-540-48405-1_25
[30] Liu, F.H., Lysyanskaya, A.: Tamper and leakage resilience in the split-state model. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 517532. Springer, Heidelberg (Aug 2012). https://doi.org/10.1007/978-3-642-320095_30
[31] Morillo, P., Ràfols, C., Villar, J.L.: The kernel matrix Diffie-Hellman assumption. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016, Part I. LNCS, vol. 10031, pp. 729-758. Springer, Heidelberg (Dec 2016). https://doi.org/10.1007/978-3-662-53887-6_27
[32] Naor, M., Segev, G.: Public-key cryptosystems resilient to key leakage. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 18-35. Springer, Heidelberg (Aug 2009). https://doi.org/10.1007/978-3-642-03356-8_2
[33] Qin, B., Liu, S.: Leakage-resilient chosen-ciphertext secure public-key encryption from hash proof system and one-time lossy filter. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013, Part II. LNCS, vol. 8270, pp. 381-400. Springer, Heidelberg (Dec 2013). https://doi.org/10.1007/978-3-642-42045-0_20
[34] Steinfeld, R., Pieprzyk, J., Wang, H.: How to strengthen any weakly unforgeable signature into a strongly unforgeable signature. In: Abe, M. (ed.) CTRSA 2007. LNCS, vol. 4377, pp. 357-371. Springer, Heidelberg (Feb 2007). https://doi.org/10.1007/11967668_23
[35] Sun, S., Gu, D., Au, M.H., Han, S., Yu, Y., Liu, J.K.: Strong leakage and tamper-resilient PKE from refined hash proof system. In: Deng, R.H., GauthierUmaña, V., Ochoa, M., Yung, M. (eds.) ACNS 2019. pp. 486-506 (2019). https://doi.org/10.1007/978-3-030-21568-2_24
[36] Sun, S., Gu, D., Parampalli, U., Yu, Y., Qin, B.: Public key encryption resilient to leakage and tampering attacks. Journal of Computer and System Sciences 89, 142-156 (2017). https://doi.org/10.1016/j.jcss.2017.03.004


[^0]:    ${ }^{1}$ Key-updating mechanism enables the secret key to be periodically updated. Selfdestruct mechanism enables the cryptographic device to blow up and erase all internal states, including $s k$, once a tampering attempt is detected.

[^1]:    ${ }^{2}$ Namely, the adversary is not allowed to make any tampering queries after it receives the challenge ciphertext.

[^2]:    ${ }^{3}$ Split-state mechanism ensures that the secret key is split into two (or more) disjoint parts and the adversary can obtain leakages from each of the secret key parts independently and tamper each of the parts independently.
    ${ }^{4} \mathrm{SXDH}$ is a standard assumption that simply requires the DDH assumption to hold in both source groups $\mathbb{G}_{1}$ and $\mathbb{G}_{2}$ of the asymmetric pairing groups.
    ${ }^{5}$ Leakage rate is defined as the ratio of the leakage amount that can be tolerated to the secret key size.

