Unbounded Leakage-Resilient Encryption and Signatures

Alper Çakan[*] Vipul Goyal[†]

Abstract

Given the devastating security compromises caused by side-channel attacks on existing classical systems, can we store our private data encoded as a quantum state so that they can be kept private in the face of arbitrary side-channel attacks?

The unclonable nature of quantum information allows us to build various *quantum protection* schemes for cryptographic information such as secret keys. Examples of quantum protection notions include copy-protection, secure leasing, and finally, unbounded leakage-resilience, which was recently introduced by Çakan, Goyal, Liu-Zhang and Ribeiro (TCC'24). Çakan et al show that secrets of various cryptographic schemes (such as cryptographic keys or secret shares) can be protected by storing them as quantum states so that they satisfy LOCC (local operation and classical communication) leakage-resilience: the scheme can tolerate any *unbounded* amount of *adaptive* leakage over *unbounded* rounds. As a special case (dubbed 1-round leakage), this also means that those quantum states cannot be converted to classical strings (without completely losing their functionality).

In this work, we continue the study of unbounded/LOCC leakage-resilience and consider several new primitive. In more details, we build ciphertexts, signatures and non-interactive zero-knowledge proofs with unbounded leakage-resilience. We show the following results.

- Assuming the existence of a classical $X \in \{\text{secret-key encryption}, \text{public-key encryption}\}$ scheme, we construct an X scheme with LOCC leakage-resilient ciphertexts. This guarantees that an adversary who obtains LOCC-leakage on ciphertexts cannot learn anything about their contents, even if they obtain the secret key later on.
- Assuming the existence of a classical signature scheme and indistinguishability obfuscation (iO), we construct a signature scheme with LOCC leakage-resilient signatures. This guarantees that an adversary who obtains LOCC-leakage on various signatures cannot produce any valid signatures at all other than the ones it obtained honestly!
- Assuming the existence of one-way functions and indistinguishability obfuscation (iO), we construct a NIZK proof system with LOCC leakage-resilient proofs. This guarantees that an adversary who obtains LOCC-leakage on a NIZK proof of an hard instance cannot produce a valid proof!

[*] Carnegie Mellon University. acakan@andrew.cmu.edu.

[†] NTT Research & Carnegie Mellon University. vipul@vipulgoyal.org

Contents

1 Introduction

Starting with the seminal work of Wiesner [Wie83] on *quantum money*, a long of line research has shown that quantum information allows us to build cryptographic applications with previously unimaginable security guarantees, in fact, guarantees that are provably impossible to achieve with classical information alone. In particular, based on the *no-cloning* principle, recent work has shown how to achieve various security notions which can be collectively called *quantum protection.* These security notions can be grouped into three categories, copy-protection (also called *unclonable* or *anti-piracy security*) , secure leasing (also called *revocable security*) and finally, unbounded leakage-resilience (also called *LOCC-leakage-resilience*) and intrusion detection, both recently introduced by Çakan, Goyal, Liu-Zhang, Ribeiro [ÇGLZR24]. In the setting of LOCC leakage-resilience, we consider a cryptographic scheme whose secret information is stored as a quantum state, and the goal is to achieve security against adversaries who obtain *any* amount of *adaptive* leakage over *any* number of rounds by specifying measurement circuits[1]. As a special case (dubbed 1-round leakage), this security guarantee also means the cryptographic object that is stored as a quantum state using such a scheme cannot be converted to a classical string without completely losing its functionality. We note LOCC-leakage-resilience is an extremely strong security guarantee which is in stark contrast to the classical setting, where there exists a long line of research on leakage-resilience[2] that all necessarily put arbitrary bounds on the size of the allowed leakage since otherwise the adversary can simply obtain the secret information in full. We also note that LOCC-leakage-resilience model readily captures all known leakage attacks (e.g. [Koc96, QS01, AARR03]) since leakage can be naturally modeled as measurements.

Çakan et al show how to construct LOCC-leakage-resilient scheme for a wide of primitives: such as public-key encryption, signature and PRF schemes whose secret keys satisfy unbounded leakage-resilience. In this work, we continue the study of LOCC-leakage-resilience and consider LOCC-leakage-resilient scheme for several new primitives: namely, ciphertexts, signatures, and proofs. As motivation, consider the following example. Suppose a user is storing their private date on their computer (or on a server), and an adversary obtains leakage on the storage, and later on the secret key of the user is leaked. Another real-life scenario is a company's employees storing important signed internal documents and their authentication/ID cards on their computers. An adversary obtaining leakage on such stored data should not be able to prove to other parties that some particular documents were signed or should not be able to forge an ID card. Note that encryption cannot be used in this scenario since the documents and the ID badge will all need to be usable by anyone in the company. This bring us to the following question.

Is it possible to design encryption/signature/NIZK schemes with ciphertexts/signatures/proofs that can tolerate arbitrary leakage?

In this work, we work answer this question positively by constructing an encrpytion scheme with LOCC-leakage-resilient ciphertexts, a signature scheme with LOCC-leakage-resilient signatures and a NIZK proof system with LOCC-leakage-resilient proofs.

[1] A measurement circuit is a quantum circuit with classical output

[2] See [KR19] for a survey

2 Preliminaries

2.1 Notation

Unless otherwise specified, adversaries are stateful quantum polynomial time (QPT) and our cryptographic assumptions are implicitly post-quantum. We write $\leftarrow$ to denote a random sampling from some distribution or uniform sampling from a set. We will use the quantum registers model. We consider registers as objects *storing* quantum states, which can be correlated or entangled with other registers, and whose states evolve as a result of applying channels to them.

2.2 Digital Signature Schemes

In this section we introduce the basic definitions of signatures schemes.

Definition 1. *A digital signature scheme with message space $\mathcal{M}$ consists of the following algorithms that satisfy the correctness and security guarantees below.*

- $\mathsf{Setup}(1^\lambda)$: *Outputs a signing key sk and a verification key vk.*
- $\mathsf{Sign}(sk, m)$: *Takes the signing key sk, returns a signature for m.*
- $\mathsf{Verify}(vk, m, s)$: *Takes the public verification key vk, a message m and supposed signature s for m, outputs 1 if s is a valid signature for m.*

Correctness *We require the following for all messages $m \in \mathcal{M}$.*

$$\Pr\left[\mathsf{Verify}(vk, m, s) = 1 : \begin{array}{c} sk, vk \leftarrow \mathsf{Setup}(1^\lambda) \\ s \leftarrow \mathsf{Sign}(sk, m) \end{array}\right] = 1.$$

Adaptive existential-unforgability security under chosen message attack (EUF-CMA) *Any QPT adversary $\mathcal{A}$ with* classical *access to the signing oracle has negligible probability of winning (i.e. challenger outputting 1) in the following game.*

1. *Challenger samples the keys $sk, vk \leftarrow \mathsf{Setup}(1)$.*
2. *$\mathcal{A}$ receives vk, interacts with the signing oracle by sending classical messages and receiving the corresponding signatures.*
3. *$\mathcal{A}$ outputs a message m that it has not queried the oracle with and a forged signature s for m.*
4. *The challenger outputs 1 if and only if $\mathsf{Ver}(vk, m, s) = 1$.*

If $\mathcal{A}$ outputs the message m before the challenger samples the keys, we call it selective EUF-CMA *security.*

2.3 Indistinguishability Obfuscation

In this section, we recall indistinguishability obfuscation.

Definition 2. *An indistinguishability obfuscation scheme $i\mathcal{O}$ for a class of circuits $\mathcal{C} = \{\mathcal{C}_\lambda\}_\lambda$ satisfies the following.*

Correctness. *For all* $\lambda, C \in \mathcal{C}_\lambda$ *and inputs* x, $\Pr\left[\tilde{C}(x) = C(x) : \tilde{C} \leftarrow i\mathcal{O}(1^\lambda, C)\right] = 1$.

Security. Let $\mathcal{B}$ be any QPT algorithm that outputs two circuits $C_0, C_1 \in \mathcal{C}$ of the same size, along with auxiliary information, such that $\Pr\left[\forall x\ C_0(x) = C_1(x) : (C_0, C_1, \mathsf{R_{aux}}) \leftarrow \mathcal{B}(1^\lambda)\right] \geq 1 - \mathsf{negl}(\lambda)$. Then, for any QPT adversary $\mathcal{A}$,

$$\Big| \Pr\left[\mathcal{A}(i\mathcal{O}(1^\lambda, C_0), \mathsf{R_{aux}}) = 1 : (C_0, C_1, \mathsf{R_{aux}}) \leftarrow \mathcal{B}(1^\lambda)\right] - \Pr\left[\mathcal{A}(i\mathcal{O}(1^\lambda, C_1), \mathsf{R_{aux}}) = 1 : (C_0, C_1, \mathsf{R_{aux}}) \leftarrow \mathcal{B}(1^\lambda)\right] \Big| \leq \mathsf{negl}(\lambda).$$

2.4 Recevier Non-Committing Encryption

In this section, we recall receiver non-committing public-key encryption, and the secret-key setting is defined similarly.

Definition 3 (Receiver Non-Committing Encryption)**.** *A receiver non-committing public-key encryption scheme is a public-key with the following algorithms.*

- $\mathsf{Setup}(1^\lambda)$*: Outputs a classical secret key* sk*, a classical public key* pk *and a classical auxiliary information* aux*.*
- $\mathsf{Enc}(pk, m)$*: Takes as input the encryption key* pk *and a message* m*, outputs a classical ciphertext.*
- $\mathsf{Dec}(sk, ct)$*: Takes as input the secret key and a ciphertext, outputs a message or* $\perp$*.*
- $\mathsf{Sim}(pk, sk, aux)$*: Takes as input the keys and the auxiliary string, and outputs a simulated ciphertext* ct*.*
- $\mathsf{Open}(pk, sk, aux, ct, m)$*: Takes as input the keys, the auxiliary string, a simulated ciphertext and a message, outputs a simulated secret key.*

We require correctness and semantic security as usual. We also recall receiver non-committing security.

Definition 4 (Receiver Non-Committing Security)**.** *Consider the following game between an adversary and a challenger.*

$\mathsf{Exp}(\lambda, \mathcal{A})$

1. *The challenger samples* $pk, sk, aux \leftarrow \mathsf{NCE.Setup}(1^\lambda)$ *and submits* pk *to the adversary.*
2. *The adversary outputs a message* m*.*
3. *The challenger samples* $ct_0 \leftarrow \mathsf{NCE.Enc}(pk, m)$ *and sets* $sk_0 = sk$*.*
4. *The challenger samples* $ct_1 \leftarrow \mathsf{NCE.Sim}(pk, sk, aux)$ *and* $sk_1 \leftarrow \mathsf{NCE.Open}(pk, sk, aux, ct_1, m)$*.*
5. *The challenger samples a bit* $b \leftarrow \{0, 1\}$ *and submits* (ct_b, sk_b) *to the adversary.*
6. *The adversary outputs a bit* b'*.*

7. *The challenger outputs* 1 *if and only if* $b' = b$.

An encryption scheme NCE *is said to satisfy receiver non-committing security if for all QPT adversaries* $\mathcal{A}$, *we have*

$$\Pr[\mathsf{Exp}(\lambda, \mathcal{A}) = 1] \leq \frac{1}{2} + \mathsf{negl}(\lambda).$$

Theorem 1 ([KNTY19, HMNY21])**.** *Assuming the existence of (post-quantum) public-key encryption, there exists a (post-quantum) receiver non-committing public-key encryption for any polynomial plaintext length.*

Theorem 2 ([KNTY19])**.** *Assuming the existence of (post-quantum) secret-key encryption, there exists a (post-quantum) receiver non-committing secret-key encryption for any polynomial plaintext length.*

2.5 Quantum Information Theory

In this section we recall various results from quantum information theory that will be useful in our constructions and proofs. We refer the reader to [NC10] for basics of quantum information and computation.

Theorem 3 (Quantum Goldreich-Levin [CLLZ21])**.** *Let* x, ρ_x *be a classical-quantum distribution with* $x \in \{0,1\}^n$. *Suppose there exists an algorithm* $\mathcal{A}$ *such that* $\Pr_{\substack{x,\rho_x \\ r \leftarrow \{0,1\}^n}}[\mathcal{A}(\rho_x, r) = \langle x, r\rangle] > \frac{1}{2} + \varepsilon$. *Then, there exists an algorithm* $\mathcal{A}'$ *such that* $\Pr_{x,\rho_x}[\mathcal{A}'(\rho_x) = x] > 4 \cdot \varepsilon^2$.

Theorem 4 (Almost As Good As New Lemma [Aar16], verbatim)**.** *Let* ρ *be a mixed state acting on* $\mathbb{C}^d$. *Let* U *be a unitary and* $(\Pi_0, \Pi_1 = I - \Pi_0)$ *be projectors all acting on* $\mathbb{C}^d \otimes \mathbb{C}^{d'}$. *We interpret* (U, Π_0, Π_1) *as a measurement performed by appending an ancillary system of dimension* d' *in the state* $|0\rangle\langle 0|$, *applying* U, *and then performing the projective measurement* Π_0, Π_1 *on the larger system. Assuming that the outcome corresponding to* Π_0 *has probability* $1 - \varepsilon$, *we have*

$$\left\|\rho - \rho'\right\|_{Tr} \leq \sqrt{\varepsilon},$$

where ρ' *is the state after performing the measurement, undoing the unitary* U, *and tracing out the ancillary system.*

2.5.1 BB84 States

A BB84 state [BB14] is a state of the form $H^{\theta_2}|X_2\rangle \otimes H^{\theta_2}|X_2\rangle \cdots H^{\theta_n}|X_n\rangle = H^{\theta}|X\rangle$ where $\theta, X \in \{0,1\}^n$.

Theorem 5 (Monogamy-of-Entanglement for BB84 States [TFKW13, ÇGLZR24])**.** *Consider the following game between a challenger and a tuple of adversaries* $\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1, \mathcal{A}_2)$.

$\underline{\mathsf{Exp}(\lambda, \mathcal{A})}$

1. *The challenger samples* $X, \theta \leftarrow \{0,1\}^\lambda$.

2. *The challenger submits* $H^\theta|X\rangle$ *to* $\mathcal{A}_0$.

3. $\mathcal{A}_0$ *outputs a bipartite register* $\mathsf{R}_1, \mathsf{R}_2$.

4. *For $i \in \{1,2\}$, $\mathcal{A}_i$ receives R_i and θ, and it outputs X_1', X_2'.*

5. *The challenger checks if $X = X_1' = X_2'$ and outputs 1 if so. Otherwise, it outputs 0.*

Then, for any (unbounded) adversary tuple $\mathcal{A}$, we have $\Pr[\mathsf{Exp}(\lambda, \mathcal{A}) = 1] \leq 2^{-\lambda^{C_{\mathsf{MoE}}}}$ where $C_{\mathsf{MoE}} = -\log\left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right) \approx 0.22$.

2.5.2 Subspace States

A subspace state is $|A\rangle = \sum_{v \in A} |v\rangle$ where A is a subspace of the vector space $\mathbb{F}_2^n$. We will overload the notation and usually write $A, A^\perp$ to also denote the membership checking programs for the subspace A and its orthogonal complement $A^\perp$.

Theorem 6 ([AC12])**.** *For a subspace A, the following applied on a register R implements a projection onto the subspace state $|A\rangle$:*

1. *Check for membership in A coherently on R and then rewind (Theorem 4).*

2. *Apply QFT to R.*

3. *Check for membership in $A^\perp$ coherently R, check if the output is 1, and then rewind (Theorem 4).*

4. *Output 1 if all the verification passed. Otherwise, output 0.*

Theorem 7 (Unclonability of Subspace States [Zha19])**.** *Consider the following game between a challenger and an adversary $\mathcal{A}$.*

$\underline{\mathsf{Exp}(\lambda, \mathcal{A})}$

1. *The challenger samples a subspace $A \leq \mathbb{F}_2^\lambda$ of dimension $\lambda/2$.*

2. *The challenger samples $\mathsf{OP}_0 \leftarrow i\mathcal{O}(A)$ and $\mathsf{OP}_1 \leftarrow i\mathcal{O}(A^\perp)$.*

3. *The challenger submits $|A\rangle, \mathsf{OP}_0, \mathsf{OP}_1$ to $\mathcal{A}$.*

4. *The adversary outputs a bipartite register $\mathsf{R}_1, \mathsf{R}_2$.*

5. *The challenger applies the projection onto $|A\rangle$ to the both registers $\mathsf{R}_1, \mathsf{R}_2$, and it outputs 1 if and only if both projective measurements accept. Otherwise, it outputs 0.*

Then, for any QPT adversary $\mathcal{A}$, we have $\Pr[\mathsf{Exp}(\lambda, \mathcal{A}) = 1] \leq \mathsf{negl}(\lambda)$.

Theorem 8 (Direct Product Hardness [BDS23])**.** *Consider the following game between a challenger and an adversary $\mathcal{A}$.*

$\underline{\mathsf{Exp}(\lambda, \mathcal{A})}$

1. *The challenger samples a subspace $A \leq \mathbb{F}_2^\lambda$ of dimension $\lambda/2$.*

2. *The challenger submits $|A\rangle$ to $\mathcal{A}$.*

3. *The adversary outputs two vectors $v, w \in \mathbb{F}_2^\lambda$.*

4. *The challenger checks if $v \in A \setminus \{0\}$ and $w \in A^\perp \in A \setminus \{0\}$, and outputs 1 if so. Otherwise, it outputs 0.*

Then, for any (unbounded) adversary $\mathcal{A}$, we have $\Pr[\mathsf{Exp}(\lambda, \mathcal{A}) = 1] \leq \mathsf{negl}(\lambda)$.

3 LOCC-Leakage-Resilience Preliminaries

In this section, we recall the notion of LOCC-leakage resilience and a useful result from prior work.

We start with our definition of an LOCC-leakage adversary. This is a slight generalization of the formal definition of [ÇGLZR24].

Definition 5 (LOCC-Leakage Adversary)**.** *An LOCC-leakage adversary is a* stateful *quantum algorithm $\mathcal{A}$ that (adaptively) specifies quantum leakage circuits for multiple rounds to leak on a secret quantum state. More formally, we will consider the following generalized experiment between an LOCC-leakage adversary $\mathcal{A}$ and a (stateful) challenger* Chal.

$\underline{\mathsf{LEAKAGE\_EXP}(1^\lambda)}$

1. ***Setup Phase:*** *The challenger* Chal *and the adversary $\mathcal{A}$ interact. At the end,* Chal *outputs a quantum register* R_0 *and outputs a public parameter pp.*

2. ***Leakage Phase:*** *Adversary $\mathcal{A}$ receives pp. Then, for multiple rounds, the following is executed*

   1. *The adversary $\mathcal{A}$ and the challenger* Chal *interact.*
   2. *$\mathcal{A}$ specifies a quantum leakage circuit E_i that takes as input a quantum register and outputs a classical string and the updated quantum register.*
   3. *The challenger* Chal *executes* $L_i, \mathsf{R}_i \leftarrow E_i(\mathsf{R}_{i-1})$ *and submits the classical string L_i to $\mathcal{A}$.*

3. ***Challenge Phase:*** *The challenger* Chal *and the adversary $\mathcal{A}$ interact. At the end, the challenger outputs a decision bit.*

We will require that the leakage circuits specified by $\mathcal{A}$ are consistent in the sense that the input size of E_i is the same as the size of the quantum register R_{i-1}.

Note that there is no bound on the number of rounds leakage for an LOCC leakage adversary*, however, in the computational setting, this will implicitly be any unbounded polynomial. If an adversary is allowed to leak for only k-rounds, we call it a k-*round LOCC leakage adversary*. We also define an* unbounded classical leakage adversary[3] *to be a pair of quantum algorithms $(E_0, \mathcal{A})$ where $\mathcal{A}$ only obtains the single shot classical leakage L where* $L_1, \mathsf{R}_1 \leftarrow E_0(\mathsf{R}_0, pp)$.

We now recall a computational LOCC-leakage-resilience property for subspace states. While this property was originally shown for coset-subspace states by [ÇGLZR24] through a reduction to the monogamy-of-entanglement games for these states, an inspection of their proof shows that the same reduction also works to prove LOCC-leakage property for subspace states using the direct product hardness for subspace states ([BDS23]). We will utilize this result in our NIZK and signature constructions.

Theorem 9 (Computational LOCC Leakage Property for Subspace States)**.** *Consider the following game between an LOCC-leakage adversary (Definition 5) $\mathcal{A}$ and the challenger.*

[3] In the terminology of [ÇGLZR24], this is also called a *non-adaptive unbounded classical leakage adversary*, since the leakage circuit is not specified by $\mathcal{A}$ after getting the public parameters. However, we note that this is still somewhat adaptive since the leakage circuit E_0 does get the public parameters

$\underline{\mathsf{Subspace\_CompLOCC}(\lambda, \mathcal{A})}$

1. *The challenger samples a subspace A of dimension $\lambda/2$ of $\mathbb{F}_2^\lambda$.*
2. *The challenger samples $\mathsf{OP}^0 \leftarrow i\mathcal{O}(A)$ and $\mathsf{OP}^1 \leftarrow i\mathcal{O}(A^\perp)$.*
3. *The challenger submits $(\mathsf{OP}_i^0, \mathsf{OP}_i^1)_{i \in [sc(\lambda)]}$ to the adversary.*
4. *$\mathcal{A}$ obtains leakage on $|A\rangle$ as in Definition 5.*
5. *$\mathcal{A}$ outputs a register R.*
6. *The challenger runs OP_0 coherently on R, checks if the output is 1, and then rewinds (Theorem 4).*
7. *The challenger applies QFT to R'.*
8. *The challenger runs OP_1 coherently on R, checks if the output is 1.*
9. *Challenger outputs 1 if and only if all the checks pass. Otherwise, it outputs 0.*

Then, assuming the existence of $i\mathcal{O}$ and one-way functions, for any QPT LOCC leakage adversary $\mathcal{A}$ we have that

$$\Pr[\mathsf{Subspace\_CompLOCC}(\lambda, \mathcal{A}) = 1] \leq \mathsf{negl}(\lambda).$$

If we assume the existence of subexponentially-secure $i\mathcal{O}$ and one-way functions, then there exists a universal constant $c_{Subsp\_LOCC} > 0$ such that for any QPT LOCC leakage adversary $\mathcal{A}$ we have that

$$\Pr[\mathsf{Subspace\_CompLOCC}(\lambda, \mathcal{A}) = 1] \leq 2^{-\lambda^{c_{Subsp\_LOCC}}}$$

for all sufficiently large λ.

4 LOCC Leakage-Resilient Encryption

In this section, we introduce the notion of encryption with unbounded leakage-resilient ciphertexts. Then, we give our information-theoretic one-time secure construction, CPA-secure secret-key construction assuming classical SKE and finally public-key construction assuming classical PKE.

Definition 6 (Encryption with quantum ciphertexts)**.** *An encryption scheme with quantum ciphertexts consists of the following efficient algorithms.*

- $\mathsf{Setup}(1^\lambda)$*: Outputs a classical secret key sk and a classical public key pk, which will be $\perp$ if the scheme is secret-key.*
- $\mathsf{Enc}(k, m)$*: Takes as input the encryption key k (pk in the public-key setting and sk in the secret-key setting) and a message m, outputs a quantum register R_{ct}.*
- $\mathsf{Dec}(sk, \mathsf{R}_{\mathsf{ct}})$*: Takes as input the secret key and a ciphertext register ct, outputs a message or $\perp$.*

We require correctness and semantic security as usual.

Definition 7 (Encryption with LOCC Leakage-Resilient Ciphertexts)**.** *Consider the following game between an LOCC-leakage-adversary (Definition 5) and a challenger.*

$\underline{\mathsf{LOCC\_CT}(\lambda, \mathcal{A})}$

1. *The challenger samples $pk, sk \leftarrow \mathsf{Sch.Setup}(1^\lambda)$ and submits pk to the adversary.*
2. *The adversary outputs pairs of messages $(m_1^0, m_i^1)_{i\in[q(\lambda)]}$.*
3. *The challenger samples a bit $b \leftarrow \{0,1\}$ and samples $\mathsf{R}_i \leftarrow \mathsf{Sch.Enc}(sk, m_i^b)$ for $i \in [q(\lambda)]$.*
4. *The adversary $\mathcal{A}$ obtains leakage on $\mathsf{R} = (\mathsf{R}_i)_{i\in[q(\lambda)]}$ as in Definition 5.*
5. *The challenger submits sk to the adversary.*
6. *The adversary outputs a bit b'.*
7. *The challenger outputs 1 if and only if $b' = b$.*

An encryption scheme Sch with quantum ciphertexts (Definition 6) is said to satisfy computational/information-theoretic LOCC-leakage-resilient ciphertext security if for all QPT/unbounded adversaries $\mathcal{A}$, we have

$$\Pr[\mathsf{LOCC\_CT}(\lambda, \mathcal{A}) = 1] \leq \frac{1}{2} + \mathsf{negl}(\lambda).$$

If the above is satisfied only for adversaries with an a-priori bound on the number of challenge ciphertexts $q(\lambda)$, then the scheme is said to satisfy $q(\lambda)$-time LOCC-leakage-resilient ciphertext security.

We emphasize that the adversary obtains even the secret key (after the leakage phase) and still it gains no advantage over random guessing.

4.1 LOCC Leakage-Resilience of BB84 States

We first prove an information-theoretic LOCC leakage-resilience property for BB84 states.

Theorem 10 (LOCC Leakage Property for BB84 States)**.** *Consider the following LOCC-leakage game (Definition 5) between an LOCC leakage adversary $\mathcal{A}$ and the challenger.*

$\underline{\mathsf{BB84\_LOCC}(\lambda, \mathcal{A})}$

1. *The challenger samples $X, \theta \leftarrow \{0,1\}^\lambda$.*
2. *$\mathcal{A}$ obtains leakage on $H^\theta|X\rangle$ as in Definition 5.*
3. *After the leakage is over, the challenger submits θ to $\mathcal{A}$.*
4. *$\mathcal{A}$ outputs X'.*
5. *The challenger outputs 1 if $X' = X$, and otherwise it outputs 0.*

Then, for any LOCC leakage adversary $\mathcal{A}$,

$$\Pr[\mathsf{BB84\_LOCC}(\lambda, \mathcal{A}) = 1] \leq 2^{-\frac{C_{\mathsf{MoE}}}{2}\cdot\lambda + 2^{-\lambda}}$$

for all sufficiently large λ, where $C_{\mathsf{MoE}} = -\log\left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right) \approx 0.22$ is the universal constant from BB84 monogamy-of-entanglement games (Theorem 5).

Note that the above theorem can also be phrased as showing that the min-entropy of X conditioned on the final internal state of the leakage adversary is at least $\frac{C_{\mathsf{MoE}}}{2} + 2^{-\lambda} \approx 0.11 \cdot \lambda + 2^{-\lambda}$ bits.

Proof. We will prove this through a reduction to the monogamy-of-entanglement (MoE) game for BB84 states. Suppose for a contradiction that there exists an LOCC-leakage adversary $\mathcal{A}$ such that $\Pr[\mathsf{BB84\_LOCC}(\lambda, \mathcal{A}) = 1] > 2^{-\frac{C_{\mathsf{MoE}}}{2} \cdot \lambda + 2^{-\lambda}}$ for infinitely many values of λ. Any claims below will be only for such values of λ. We will also assume that $\mathcal{A}$ has a fixed number of leakage rounds $n(\lambda)$, with a fixed size $c(\lambda)$ for each leakage circuit description and fixed size $\ell(\lambda)$ for leakage output; it is easy to see that this is all without loss of generality.

Let $\mathcal{T} = (E_1, L_1, \ldots, E_\ell, L_\ell)$ be the random variable defined as the transcript of the leakage phase of $\mathcal{A}$ playing $\mathsf{BB84\_LOCC}$. That is, E_i denotes the leakage circuit output by $\mathcal{A}$ at round i, and L_i denotes the corresponding measurement result. Define T^*_λ to be the transcript with the lowest probability, that is,

$$T^*_\lambda = \underset{T \in \mathsf{Supp}(\mathcal{T})}{\operatorname{argmin}} \Pr_{\mathcal{T}}[\mathcal{T} = T]$$

and also set k to be the smallest integer such that

$$(2^{-\frac{C_{\mathsf{MoE}}}{2} + 2^{-\lambda}})^2 \cdot \left(1 - \exp\left[-\Pr_{\mathcal{T}}[\mathcal{T} = T^*_\lambda] \cdot k\right]\right) \geq 2^{-C_{\mathsf{MoE}} \cdot \lambda}.$$

Note that since $\mathsf{Supp}(\mathcal{T})$ is of finite size (namely, $2^{n(\lambda) \cdot c(\lambda) \cdot \ell(\lambda)}$), T^*_λ is well-defined, and consequently k is finite. Let ρ_0 denote the non-uniform quantum advice of $\mathcal{A}$. We create a tuple for adversaries $\mathcal{A}' = (\mathcal{A}'_0, \mathcal{A}'_2, \mathcal{A}'_2)$ for the MoE game, where $\mathcal{A}'_0$ has the advice $\rho^{\otimes k}$. Note that if $\mathcal{A}$ does not have non-uniform advice, then we consider ρ to be $\perp$, and in that case our MoE adversary will not have non-uniform advice either. Now we define our MoE adversaries.

$\underline{\mathcal{A}'_0(\mathsf{R}_{\mathsf{BB84}})}$

1. Simulate the leakage phase of $\mathcal{A}$ on $\mathsf{R}_{\mathsf{BB84}}$. Let $T = (E_1, L_1, \ldots, E_\ell, L_\ell)$ be the transcript of the leakage phase. That is, E_i denotes the leakage circuit output by $\mathcal{A}$ at round i, and L_i denotes the corresponding measurement result. Let ρ_T be the internal state of $\mathcal{A}$ after the leakage phase is done.

2. Set $cnt = k^*$. While $cnt > 0$, run the following:

    1. Simulate the leakage phase of $\mathcal{A}$ as follows, starting with $i = 1$. When it outputs a measurement circuit E'_i, check if $E'_i = E_i$. If so, submit L_i to $\mathcal{A}$ and move to next round of leakage simulation by increasing i. Otherwise, decrement cnt by one and move to the next iteration of the outer loop.
    2. When the simulated leakage phase of $\mathcal{A}$ is complete, let ρ' be the internal state of the adversary.

3. If $cnt = 0$, output $(\perp, \perp)$. Otherwise, output $(\mathsf{R}_1 = \rho_T, \mathsf{R}_2 = \rho')$.

$\underline{\mathcal{A}'_i(\mathsf{R}_i, \theta)}$ **for** $i \in \{1, 2\}$

- If the input register $\perp$, output $\perp$. Otherwise, simulate the challenge phase of $\mathcal{A}$ on θ, with the internal state R_i.

Now we will prove that $\mathcal{A}'$ wins $\mathsf{BB84\_MoE}$ with probability greater than $2^{-C_{\mathsf{MoE}}\cdot\lambda}$, which will be a contradiction by Theorem 5. Observe that for any fixed transcript T, conditioned on obtaining that transcript during the run of $\mathcal{A}'$ and conditioned on not terminating with $\perp$, we have that the probability of $\mathcal{A}'$ winning is $\Pr[\mathcal{A} \text{ wins } \mathsf{BB84\_LOCC}|\mathcal{T} = T]^2$. This is since for each transcript T, we have two completely independent runs of the challenge phase of $\mathcal{A}$. Further, we have that the probability of $\mathcal{A}'$ terminating with $\perp$ is $1 - (1 - \Pr_{\mathcal{T}}[\mathcal{T} = T])^k$. Combining these, we get that the probability of $\mathcal{A}'$ winning $\mathsf{BB84\_MoE}$ is

$$\begin{aligned}
&\sum_{T\in\mathsf{Supp}(\mathcal{T})} \Pr_T[\mathcal{T} = T]\cdot(1-(1-\Pr_{\mathcal{T}}[\mathcal{T} = T])^k)\cdot\Pr[\mathcal{A} \text{ wins } \mathsf{BB84\_LOCC}|\mathcal{T} = T]^2\\
\geq &\sum_{T\in\mathsf{Supp}(\mathcal{T})} \Pr_T[\mathcal{T} = T]\cdot\left(1-\exp\left[-\Pr_{\mathcal{T}}[\mathcal{T} = T^*]_\lambda\cdot k\right]\right)\cdot\Pr[\mathcal{A} \text{ wins } \mathsf{BB84\_LOCC}|\mathcal{T} = T]^2\\
\geq &\left(\sum_{T\in\mathsf{Supp}(\mathcal{T})} \Pr_T[\mathcal{T} = T]\cdot\Pr[\mathcal{A} \text{ wins } \mathsf{BB84\_LOCC}|\mathcal{T} = T]^2\right)\cdot\frac{2^{-C_{\mathsf{MoE}}\cdot\lambda}}{(2^{-\frac{C_{\mathsf{MoE}}}{2}}+2^{-\lambda})^2}\\
\geq &\left(\sum_{T\in\mathsf{Supp}(\mathcal{T})} \Pr_T[\mathcal{T} = T]\cdot\Pr[\mathcal{A} \text{ wins } \mathsf{BB84\_LOCC}|\mathcal{T} = T]\right)^2\cdot\frac{2^{-C_{\mathsf{MoE}}\cdot\lambda}}{(2^{-\frac{C_{\mathsf{MoE}}}{2}}+2^{-\lambda})^2}\\
= &(\Pr[\mathcal{A} \text{ wins } \mathsf{BB84\_LOCC}])^2\cdot\frac{2^{-C_{\mathsf{MoE}}\cdot\lambda}}{(2^{-\frac{C_{\mathsf{MoE}}}{2}}+2^{-\lambda})^2} > 2^{-C_{\mathsf{MoE}}\cdot\lambda}
\end{aligned}$$

The third line follows by definition of k, fourth line follows by Jensen's inequality, and the last line follows by our contradiction hypothesis for $\mathcal{A}$. Note that the above contradicts Theorem 5, thus the proof is complete.

□

4.2 One-Time Secure Secret Key Encryption

In this section, we give our information-theoretically 1-time secure encryption scheme with LOCC-leakage-resilient ciphertexts for 1-bit messages. In the later sections, we show how to generically upgrade such schemes to CPA-secure SKE or PKE schemes for plaintexts of any length.

$\mathsf{OTE.Setup}(1^\lambda)$

1. Sample $\theta \leftarrow \{0,1\}^\lambda$.
2. Output $sk = \theta$.

$\mathsf{OTE.Enc}(sk, b)$

1. Parse $\theta = sk$.
2. Sample $X, r \leftarrow \{0,1\}^\lambda$.
3. Output $\mathsf{R}_{\mathsf{ct}} = (H^\theta|X\rangle, r, (\langle X, r\rangle \oplus b))$.

$\underline{\mathsf{OTE.Dec}(sk, \mathsf{R}_{\mathsf{ct}})}$

1. Parse $(\mathsf{R}', r, eb) = \mathsf{R}_{\mathsf{ct}}$ and $\theta = sk$.
2. Apply H^θ to R'.
3. Measure R' in the computational basis and let s be the measurement result.
4. Output $eb \oplus \langle s, r\rangle$.

Perfect correctness follows easily due to the fact that $(H^\theta)(H^\theta) = I$.

Theorem 11. OTE *satisfies* 1*-time information-theoretic semantic security.*

Proof. Suppose for a contradiction that there exists an adversary that can predict b with probability $1/2 + \varepsilon$ for non-negligible ε, given $H^\theta|X\rangle, r, (\langle X, r\rangle \oplus b)$. Then, by a simple argument (e.g. see Theorem 12), there exists an adversary that can predict $\langle X, r\rangle$ with probability $1/2 + \varepsilon$, given $H^\theta|X\rangle$. Then, by quantum Goldreich-Levin theorem (Theorem 3), there exists an adversary that can predict X with probability $4 \cdot \varepsilon^2$, given $H^\theta|X\rangle$. Since ε is non-negligible, so is $4 \cdot \varepsilon^2$, however, this is a contradiction since maximum prediction probability for X given $H^\theta|X\rangle$ is exponentially small in λ by a simple trace distance argument. □

Theorem 12. OTE *satisfies* 1*-time information-theoretic LOCC-leakage-resilient ciphertext security for* 1*-bit messages.*

Proof. We will prove our result through a reduction to the LOCC-leakage-resilience property for BB84 states.

Suppose for a contradiction that there exists an LOCC-leakage adversary $\mathcal{A}$ such that $\Pr[\mathsf{LOCC\_CT}(\lambda, \mathcal{A}) = 1] > \frac{1}{2} + \varepsilon(\lambda)$ for infinitely many values of λ where $\varepsilon = \frac{1}{2} \cdot 2^{-\frac{C_{\mathsf{MoE}}}{4}\cdot\lambda + 2^{-\lambda-1}}$. Let $\mathcal{A}_1$ denote the leakage-phase of the adversary $\mathcal{A}$ and let $\mathcal{A}_2$ denote the challenge phase. We will construct an LOCC-leakage-adversary $\mathcal{A}_{BB84}$ for BB84 leakage game $\mathsf{BB84\_LOCC}$. First, we construct the leakage-phase $\mathcal{A}_{Leak,BB84}$ of the adversary.

$\underline{\mathcal{A}_{Leak,BB84}(\mathsf{R})}$

1. Sample $r \leftarrow \{0,1\}^\lambda$ and $b' \leftarrow \{0,1\}$.
2. Simulate $\mathcal{A}_1$ on R, r, b' to obtain a state ρ.
3. Output ρ, b'.

Now, consider the following adversary $\mathcal{A}'$ that accepts as input θ and the output R, b' of $\mathcal{A}_{Leak,BB84}$: It simulates $\mathcal{A}_2$ on R, θ, and then it outputs $b' \oplus b''$ where b'' is the output of $\mathcal{A}_2$. By a standard argument it is easy to see that $\mathcal{A}'$ predicts $\langle x, r\rangle$ with probability $1/2 + \varepsilon(\lambda)$.

Now we will construct the challenge phase adversary $\mathcal{A}_{Chal,BB84}$. Consider the classical-quantum distribution $X, \rho_X = \mathcal{A}_{Leak,BB84}(H^\theta|X\rangle$ where $X, \theta \leftarrow \{0,1\}^\lambda$. Note that this is simply the distribution of X along with the side-information which is the final internal state of the leakage-phase adversary $\mathcal{A}_{Leak,BB84}$ (which will be the input of $\mathcal{A}_{Chal,BB84}$). By above, we have that given ρ_X, $\mathcal{A}'$ can output $\langle x, r\rangle$ with probability $1/2 + \varepsilon(\lambda)$. Then, by the quantum Goldreich-Levin theorem (Theorem 3), there exists an algorithm $\mathcal{A}_{Chal,BB84}$ that can predict X with probability $4 \cdot \varepsilon^2 > 2^{-\frac{C_{\mathsf{MoE}}}{2}\cdot\lambda + 2^{-\lambda}}$, which is a contradiction by Theorem 10. □

It is easy to see that $\ell(\lambda)$-way parallel repetition of our scheme is secure for $\ell(\lambda)$-bit messages.

4.3 Upgrading to Public-key Encryption

In this section, we show how to construct a public-key encryption with LOCC-leakage-resilient ciphertexts for ℓ-bit messages, based on a one-time secure LOCC-leakage-resilient scheme (OTE) for ℓ-bit messages and a classical receiver non-committing public-key encryption scheme (NCE). We note that the latter can be constructed based on any standard public-key encryption scheme (Definition 3). We further note that the same transformation technique has been previously used by [HMNY21] to upgrade 1-time secure unclonable encryption to PKE with unclonable ciphertexts.

$\underline{\mathsf{PKE.Setup}(1^\lambda)}$

1. Sample $pk, sk \leftarrow \mathsf{NCE.Setup}(1^\lambda)$.
2. Output pk, sk.

$\underline{\mathsf{PKE.Enc}(pk, m)}$

1. Sample $isk \leftarrow \mathsf{OTE.Setup}(1^\lambda)$.
2. Sample $\mathsf{R} \leftarrow \mathsf{OTE.Enc}(isk, m)$.
3. Sample $ict \leftarrow \mathsf{NCE.Enc}(pk, isk)$.
4. Output R, ict.

$\underline{\mathsf{PKE.Dec}(sk, \mathsf{R})}$

1. Parse $(\mathsf{R}', ict) = \mathsf{R}$.
2. Decrypt $isk = \mathsf{NCE.Dec}(sk, ict)$.
3. Decrypt $m \leftarrow \mathsf{OTE.Dec}(isk, \mathsf{R})$.
4. Output m.

Correctness and the semantic security of the scheme follows in a straightforward way.

Theorem 13. PKE *satisfies LOCC leakage-resilient ciphertext security.*

Proof. Suppose there exists an LOCC-leakage adversary $\mathcal{A}$ that wins the leakage-resilience game with non-negligible advantage. Define Hyb_0 to be the original leakage-resilience game $\mathsf{LOCC\_CT}(\lambda, \mathcal{A})$. We define Hyb_1 by modifying Hyb_1 as follows: First, when encrypting the challenge message m_b, instead of sampling the ciphertext as $\mathsf{R} \leftarrow \mathsf{PKE.Enc}(pk, m_b)$, we instead sample it as

1. Sample $isk \leftarrow \mathsf{OTE.Setup}(1^\lambda)$.
2. Sample $\mathsf{R}' \leftarrow \mathsf{OTE.Enc}(isk, m)$.
3. Sample $ict \leftarrow \mathsf{NCE.Sim}(pk, sk)$.
4. $\mathsf{R} = (\mathsf{R}', ict)$.

Further, later during the challenge phase, instead of submitting sk to the adversary, we instead sample $sk' \leftarrow \mathsf{NCE.Open}(sk, ict, isk)$ and submit sk'. By the security of NCE, we get $\mathsf{Hyb}_0 \approx \mathsf{Hyb}_1$. Thus, $\Pr[\mathsf{Hyb}_1 = 1] \geq \frac{1}{2} + \frac{1}{p(\lambda)}$ for a polynomial $p(\cdot)$. Now we construct an adversary $\mathcal{A}'$ for the one-time leakage-resilience game for OTE.

$\underline{\mathcal{A}'(\mathsf{R})}$

1. **Setup Phase:** Simulate $\mathcal{A}$ to obtain the challenge messages m_0, m_1, output m_0, m_1.
2. **Leakage Phase:** Sample $pk, sk \leftarrow \mathsf{NCE.Setup}(1^\lambda)$ and $ict \leftarrow \mathsf{NCE.Sim}(pk, sk)$. Then, simulate $\mathcal{A}$ on R, ict.
3. **Challenge Phase:** On input isk, simulate $\mathcal{A}$ on $\mathsf{NCE.Open}(sk, ict, isk)$, and output its output.

Then, observe that probability of $\mathcal{A}'$ winning the one-time leakage-resilience game for OTE is exactly the same as $\Pr[\mathsf{Hyb}_1 = 1]$. Thus, $\mathcal{A}'$ wins with probability $\frac{1}{2} + \frac{1}{p(\lambda)}$, which is a contradiction to the leakage-resilience security of OTE.

□

Since non-committing public-key encryption can be constructed from any standard public-key encryption scheme (Theorem 1), we obtain the following.

Corollary 1. *Assuming the existence of a public-key encryption scheme, there exists a secret-key encryption scheme with LOCC-leakage-resilient ciphertexts.*

It is easy to see that our transformation works the same in the secret-key setting too. Since non-committing secret-key encryption can be constructed from any standard secret-key encryption (Theorem 2), we obtain the following.

Theorem 14. *Assuming the existence of a secret-key encryption scheme, there exists a secret-key encryption scheme with LOCC-leakage-resilient ciphertexts.*

5 LOCC Leakage-Resilient Signatures and Non-Interactive Zero-Knowledge Proofs

We first formally introduce signature schemes with unbounded leakage-resilience, then we give our construction based on indistinguishability obfuscation and any signature scheme.

Definition 8 (Signature scheme with quantum signatures)**.** *An signature scheme with quantum signatures consists of the following efficient algorithms.*

- $\mathsf{Setup}(1^\lambda)$*: Outputs a classical signing key sk and a classical verification key vk.*
- $\mathsf{Sign}(sk, m)$*: Takes as input the signing key and a message m, outputs a quantum register $\mathsf{R}_{\mathsf{sig}}$.*
- $\mathsf{Verify}(vk, m, \mathsf{R}_{\mathsf{sig}})$*: Takes as input the verification key, a message m and a register $\mathsf{R}_{\mathsf{sig}}$ containing an alleged signature for m, outputs 1 or 0.*

We require correctness and existential unforgeability under chosen message attacks (EUF-CMA) security as usual.

Definition 9 (Signature Scheme with LOCC Leakage-Resilient Signatures)**.** *Consider the following game between an LOCC-leakage adversary (Definition 5) and challenger.*

$\underline{\mathsf{LOCC\_SIG}(\lambda, \mathcal{A})}$

1. ***Setup Phase:*** *The challenger samples $sk, vk \leftarrow \mathsf{Sch.Setup}(1^\lambda)$ and submits vk to the adversary. It also initializes the list $M = []$.*

2. ***Query Phase:*** *For multiple rounds, the adversary outputs a message and the challenger responds by sampling $\mathsf{R}_{\mathsf{sig}} \leftarrow \mathsf{Sch.Sign}(sk, m)$ and submitting $\mathsf{R}_{\mathsf{sig}}$ to the adversary. For each the challenger also adds m to the list M.*

3. *The adversary outputs a list of messages $(m_i)_{i \in [q(\lambda)]}$.*

4. ***Leakage Phase:*** *The challenger samples $\mathsf{R}_i \leftarrow \mathsf{Sch.Sign}(sk, m_i)$ for $i \in [q(\lambda)]$. The adversary $\mathcal{A}$ obtains leakage on $\mathsf{R} = (\mathsf{R}_i)_{i \in [q(\lambda)]}$ as in Definition 5. During each leakage round, the adversary can submit signature queries to the challenger, and the challenger responds by sampling the signature as $\mathsf{R}_{\mathsf{sig}} \leftarrow \mathsf{Sch.Sign}(sk, m)$, submitting $\mathsf{R}_{\mathsf{sig}}$ to the adversary and adding m to the list M.*

5. ***Challenge Phase:*** *The adversary outputs a message m_{chal} and an alleged signature $\mathsf{R}_{\mathsf{forged}}$. The challenger executes $b \leftarrow \mathsf{Sch.Verify}(vk, m_{chal}, \mathsf{R}_{\mathsf{forged}})$ and outputs 1 if and only if $b = 1$ and $m_{chal} \notin M$.*

A signature scheme Sch *with quantums signatures (Definition 6) is said to satisfy LOCC-leakage-resilient signature security if for all QPT adversaries $\mathcal{A}$, we have*

$$\Pr[\mathsf{LOCC\_SIG}(\lambda, \mathcal{A}) = 1] \leq \mathsf{negl}(\lambda).$$

Our definition requires that an adversary, who obtains multiple signatures directly and also LOCC-leakage on multiple signatures, cannot produce a valid signature for a message for which it has not honestly obtained a signature for. That is, it can be thought of as EUF-CMA security with the addition that adversary obtains leakage on various signatures, however, the leakage should not help it at all.

Theorem 15. *Assuming the existence of indistinguishability obfuscation and a signature scheme, there exists a signature scheme with LOCC-leakage-resilient signatures.*

Since signature schemes can be constructed from iO and one-way functions ([SW14]), we obtain the following corollary.

Corollary 2. *Assuming the existence of indistinguishability obfuscation and one-way functions, there exists a signature scheme with LOCC-leakage-resilient signatures.*

5.1 Construction

In this section, we give our construction. We note that our construction is similar to the folklore construction of unclonable signatures from public-key quantum money and a classical signature scheme, where a signature on a message m consists a banknote along with a classical signature on the serial number concatenated with the message m. While this construction can be proven to be unclonable based on any public-key quantum money, we note that this is not the case for LOCC-leakage. In fact, instantiating this signature scheme with a *classically-transferable public-key quantum money* scheme [AGKZ20] yields a scheme that is provably insecure against LOCC-leakage! Thus, we rely specifically on the subspace state quantum money and prove the leakage-resilience of the construction through a new proof. This also shows that unclonable signature security does not imply LOCC-leakage-resilient signature security.

Now we move onto our construction. Let CSS be a classical signature scheme.

$\underline{\mathsf{DS.Setup}(1^\lambda)}$

1. Sample $sk, vk \leftarrow \mathsf{CSS.Setup}(1^\lambda)$.
2. Output sk, vk.

$\underline{\mathsf{DS.Sign}(sk, m)}$

1. Sample a subspace A of $\mathbb{F}_2^\lambda$ of dimension $\lambda/2$.
2. Initialize the register R with $|A\rangle$.
3. Sample $isig \leftarrow \mathsf{CSS.Sign}(sk, m||i\mathcal{O}(A)||i\mathcal{O}(A^\perp))$.
4. Output $\mathsf{R}, isig, i\mathcal{O}(A), i\mathcal{O}(A^\perp)$.

$\underline{\mathsf{DS.Verify}(vk, m, \mathsf{R})}$

1. Parse $(\mathsf{R}', isig, P_0, P_1) = \mathsf{R}$.
2. Verify $\mathsf{CSS.Verify}(vk, m||P_0||P_1, isig)$.
3. Run P_0 coherently on R', check if the output is 1, and then rewind (Theorem 4).
4. Apply QFT to R'.
5. Run P_1 coherently on R', check if the output is 1, and then rewind (Theorem 4).
6. Output 1 if all the verification passed. Otherwise, output 0.

The correctness follows in a straightforward manner. EUF-CMA security is implied by leakage-resilience security since an adversary can simply ignore the leakage information it obtains.

5.2 Proof of Security

We will prove leakage-resilience security through a series of hybrids, each of which is constructed by modifying the previous one. Without loss of generality, we will assume that the adversary obtains leakage on a fixed number $q(\lambda)$ of signatures.

$\underline{\mathsf{Hyb}_0}$**:** The original game $\mathsf{LOCC\_SIG}(\lambda, \mathcal{A})$.

$\underline{\mathsf{Hyb}_1}$**:** Let M_{Leak} be the set of message on which the adversary obtains leakage on. We add an additional condition for winning the game as follows: At the end of the game, the challenger also checks if $m_{chal} \in M_{Leak}$, and if not, the challenger outputs 0 (hence the adversary loses).

$\underline{\mathsf{Hyb}_2}$**:** At the beginning of the game, we sample a random index $i^* \leftarrow [q(\lambda)]$. Let m_{i^*} be the i^*-th element of M_{Leak}. We add another winning requirement: The challenger checks if $m_{chal} = m_{i^*}$, and if not it outputs 0.

Lemma 1. $\mathsf{Hyb}_0 \approx \mathsf{Hyb}_1$.

Proof. In Hyb_0, the challenge message needs to satisfy $m \notin M$, whereas in Hyb_1, it needs to satisfy $m \in M_{Leak} \backslash M$. Therefore, the two hybrids can differ only if the adversary outputs a valid signature for some $m_{chal} \notin M \cup M_{Leak}$. However, observe that the adversary only obtains signatures of the scheme for CSS for messages in $M \cup M_{Leak}$, and its forged signature needs to include a CSS signature for m_{chal} by construction of DSS.Verify. By EUF-CMA security of DSS, this can only happen with negligible probability, thus showing $\mathsf{Hyb}_0 \approx \mathsf{Hyb}_1$. □

Lemma 2. $\Pr[\mathsf{Hyb}_2 = 1] \geq \frac{\Pr[\mathsf{Hyb}_1 = 1]}{q(\lambda)}$.

Proof. Note that in Hyb_1, it is required that $m_{chal} \in M_{Leak}$. Let $i^{**} \in [q(\lambda)]$ denote the position of m_{chal} in M_{Leak}. Then, independent of all the previous events, i^* will satisfy $i^* = i^{**}$ with probability $1/q(\lambda)$, and thus the result follows. □

Now suppose for a contradiction that there exists a QPT adversary $\mathcal{A}$ such that $\Pr[\mathsf{LOCC\_SIG}(\lambda, \mathcal{A}) = 1] > 1/p(\lambda)$ for some polynomial $p(\cdot)$ and infinitely many values of λ. We construct an adversary for the LOCC-leakage-resilience game Subspace_CompLOCC for subspace states (Theorem 9). We first construct the leakage-phase adversary.

$\underline{\mathcal{A}_{Leak}(\mathsf{R})}$

1. Simulate the setup phase and the query phase of the game Hyb_2 by simulating both the challenger and the adversary $\mathcal{A}$.
2. Simulate the adversary $\mathcal{A}$ and the challenger to obtain the first leakage circuit output E_0 of $\mathcal{A}$. Let P_0, P_1 be the obfuscated membership checking programs received from the challenger of Subspace_CompLOCC. Then, output the following circuit E_0' to the challenger of Subspace_CompLOCC.

   $\underline{E_0'(\mathsf{R}_{\mathsf{subsp}})}$

   Hardcoded: $E_0, (m_i)_{i \in [q(\lambda)]}, sk, P_0, P_1$

   1. For $i \in [q(\lambda)] \setminus \{i^*\}$, sample $\mathsf{R}_i \leftarrow \mathsf{DSS.Sign}(sk, m_i)$.
   2. Sample $isig \leftarrow \mathsf{CSS.Sign}(sk, m_{i^*} || P_0 || P_1)$.
   3. Set $\mathsf{R}_{i^*} = (\mathsf{R}_{\mathsf{subsp}}, isig, P_0, P_1)$ and $\mathsf{R} = (\mathsf{R}_i)_{i \in [q(\lambda)]}$.
   4. Simulate E_0 on R to obtain the leakage output L and the leftover state R'.
   5. Output L as the leakage output L and R' as the leftover state.

3. Simulate the rest of the leakage phase by simulating both the challenger and the adversary $\mathcal{A}$, by forwarding the leakage circuit outputs of $\mathcal{A}$ to the challenger of Subspace_CompLOCC and forwarding leakage results to $\mathcal{A}$.
4. Output the final internal state of $\mathcal{A}$ and the internal state of the challenger of LOCC_SIG.

Now we construct the challenge-phase adversary $\mathcal{A}_{Chal}$ for Subspace_CompLOCC.

$\underline{\mathcal{A}_{Leak}(\mathsf{R}_{\mathsf{internal}})}$

1. Simulate the challenge phase of the game $\mathsf{LOCC\_SIG}$ by simulating the adversary $\mathcal{A}$ and the challenger using $\mathsf{R}_{\mathsf{internal}}$.
2. Let m_{chal} and $\mathsf{R}_{\mathsf{forged}}$ be the output $\mathcal{A}$. Parse $(\mathsf{R}'_{\mathsf{forged}}, isig^*, P_1^*, P_2^*)$. Output $\mathsf{R}'_{\mathsf{forged}}$ to the challenger of $\mathsf{Subspace\_CompLOCC}$.

Observe that the probability of $(\mathcal{A}_{Leak}, \mathcal{A}_{Chal})$ winning $\mathsf{Subspace\_CompLOCC}$ is exactly the same as $\Pr[\mathsf{Hyb}_2 = 1]$. We assumed for contradiction that $\Pr[\mathsf{LOCC\_SIG}(\lambda, \mathcal{A}) = 1] > 1/p(\lambda)$, which by above implies $\Pr[\mathsf{Hyb}_2 = 1] \geq \frac{1}{2 \cdot q(\lambda) \cdot p(\lambda)}$, which is thus a contradiction by Theorem 9.

5.3 Non-Interactive Zero-Knowledge Proofs

In this section, we introduce the notion of non-interactive zero-knowledge proofs with LOCC-leakage-resilient proofs. Then, we give our construction, which is similar to the constructions of [JK23] and [GMR23]. However, as in the case of signatures, while their constructions can be based black-box on any public-key quantum money (PKQM) scheme, in our setting there are explicit attacks if the construction is instantiated with a large class of PKQM schemes (namely, classically-transferable PKQM). Thus, our construction explicitly uses subspace quantum money and needs a new proof security.

Since the high level ideas are similar to signature construction, we will focus on the single proof for simplicity, and the general case follows similarly.

We recall hard instance distributions.

Definition 10 (Hard Distributions for NP)**.** *Let L be an NP language with the relation R_L. Let $\mathcal{D}$ be an efficient distribution over R_L. Then, $\mathcal{D}$ is said to be a hard distribution if for any QPT adversary,*

$$\Pr\left[(x, w^*) \in R_L : \begin{array}{c} x, w \leftarrow \mathcal{D} \\ w^* \leftarrow \mathcal{A}(x) \end{array}\right] \leq \mathsf{negl}(\lambda).$$

Now we define LOCC-leakage-resilient proofs.

Definition 11 (NIZK Proof Systems with LOCC Leakage-Resilient Proofs)**.** *Consider the following game between an LOCC-leakage-adversary (Definition 5) and a challenger.*

$\underline{\mathsf{LOCC\_PROOF}(\lambda, \mathcal{A})}$

1. *The challenger samples $crs \leftarrow \mathsf{NIZK.Setup}(1^\lambda)$ and submits crs to the adversary.*
2. *The challenger samples an instance $(x, w) \leftarrow \mathcal{D}$.*
3. *The challenger samples a proof $\mathsf{R} \leftarrow \mathsf{NIZK.Proof}(crs, x, w)$.*
4. *The adversary $\mathcal{A}$ obtains leakage on R as in Definition 5.*
5. *The adversary outputs a proof $\mathsf{R}_{\mathsf{proof}}$.*
6. *The challenger outputs the output $\mathsf{NIZK.Verify}(crs, x, \mathsf{R}_{\mathsf{proof}})$.*

A NIZK scheme Sch with quantum proofs is said to satisfy LOCC-leakage-resilient proof security if for all hard distributions $\mathcal{D}$ and for all QPT adversaries $\mathcal{A}$, we have

$$\Pr[\mathsf{LOCC\_PROOF}(\lambda, \mathcal{A}) = 1] \leq \mathsf{negl}(\lambda).$$

Now we give our construction for an NP language L. Let Com be a perfectly binding commitment scheme, PKE be a public-key encryption scheme and CNIZK be a classical NIZK scheme for following language L'

$$\{(x, ct, P_0||P_1) : \exists w, r_1, r_2 \text{ such that } (ct = \mathsf{PKE.Enc}(pk, w; r_1) \wedge (x, w) \in R_L) \vee (com^* = \mathsf{Com}(P_0||P_1; r_2))\}$$

where pk, com^* will be sampled during setup of NIZK.

$\mathsf{NIZK.Setup}(1^\lambda)$

1. Sample $icrs \leftarrow \mathsf{CNIZK.Setup}(1^\lambda)$.
2. Sample $pk, sk \leftarrow \mathsf{PKE.Setup}(1^\lambda)$.
3. Sample a subspace A^* of $\mathbb{F}_2^\lambda$ of dimension $\lambda/2$.
4. Sample $\mathsf{OP}_0^* \leftarrow i\mathcal{O}(A^*)$.
5. Sample $\mathsf{OP}_1^* \leftarrow i\mathcal{O}((A^*)^\perp)$.
6. Sample $com^* \leftarrow \mathsf{Com}(\mathsf{OP}_0^*||\mathsf{OP}_1^*)$.
7. Output $icrs, com^*, pk$.

$\mathsf{NIZK.Prove}(crs, x, w)$

1. Parse $(icrs, com^*) = crs$.
2. Check if $(x, w) \in R_L$, otherwise output $\perp$ and terminate.
3. Sample $r \leftarrow \{0, 1\}^{r(\lambda)}$.
4. Compute $ct = \mathsf{PKE.Enc}(pk, w; r)$.
5. Sample a subspace A of $\mathbb{F}_2^\lambda$ of dimension $\lambda/2$.
6. Sample $\mathsf{OP}_0 \leftarrow i\mathcal{O}(A)$.
7. Sample $\mathsf{OP}_1 \leftarrow i\mathcal{O}(A^\perp)$.
8. Sample a proof π using $\mathsf{CNIZK.Prove}$ for the statement $(x, ct, \mathsf{OP}_0||\mathsf{OP}_1)$ using the witness $(w, r, \perp)$.
9. Initialize the register R with $|A\rangle$.
10. Output $\mathsf{R}, i\mathcal{O}(A), i\mathcal{O}(A^\perp), \pi, ct$.

$\underline{\mathsf{NIZK.Verify}(crs, x, \mathsf{R})}$

1. Parse $(icrs, com^*) = crs$.
2. Parse $(\mathsf{R}', P_0, P_1, \pi, ct) = \mathsf{R}$.
3. Verify $\mathsf{CNIZK.Verify}(crs, x, ct, P_0||P_1, com^*, \pi)$.
4. Run P_0 coherently on R', check if the output is 1, and then rewind (Theorem 4).
5. Apply QFT to R'.
6. Run P_1 coherently on R', check if the output is 1, and then rewind (Theorem 4).
7. Output 1 if all the verification passed. Otherwise, output 0.

Theorem 16. NIZK *satisfies completeness, computational soundness and zero-knowledge.*

Proof. Completeness and zero-knowledge property follows in a straightforward manner from the same properties of CNIZK. For soundness, observe that by soundness of CNIZK, any statement-proof that passes verification must satisfy either the PKE part in definition of the language L', or the commitment part. By perfect binding of the commitment scheme, there does not exist r, P_0, P_1 such that $com^* = \mathsf{Com}(P_0||P_1; r)$ but $P_0||P_1 \neq \mathsf{OP}_0^*||\mathsf{OP}_1^*$. However, note that given only $\mathsf{OP}_0^*, \mathsf{OP}_1^*$, a QPT adversary cannot output a state that passes the state verification of NIZK.Verify due to unclonability of $|A^*\rangle$ (Theorem 7). Thus, for a proof to be accepted, the statement must satisfy the PKE condition, which necessarily means x is in L, thus completing the proof. □

Theorem 17. NIZK *satisfies LOCC-leakage-resilience.*

Proof. We will prove security through a series of hybrids.

$\underline{\mathsf{Hyb}_0}$: The original game $\mathsf{LOCC\_PROOF}(\lambda, \mathcal{A})$.

$\underline{\mathsf{Hyb}_1}$: Instead of sampling the subspace state $|A\rangle$ and the associated programs $\mathsf{OP}_0, \mathsf{OP}_1$ during proof generation, we move these samplings to the setup phase. Then, instead of sampling com^* as $com^* \leftarrow \mathsf{Com}(\mathsf{OP}_0^*||\mathsf{OP}_1^*)$, we instead sample r' and compute $com^* = \mathsf{Com}(\mathsf{OP}_0||\mathsf{OP}_1; r')$.

$\underline{\mathsf{Hyb}_2}$: During the proof generation, instead of using the witness $(w, r, \perp)$, we instead use $(\perp, \perp, r')$.

$\underline{\mathsf{Hyb}_3}$: Instead sampling r and computing ct as $ct = \mathsf{PKE.Enc}(pk, w; r)$, we instead sample ct as $ct \leftarrow \mathsf{PKE.Enc}(pk, 0^{\ell(\lambda)})$.

Now we argue indistinguishability of the hybrids. We first claim $\mathsf{Hyb}_0 \approx \mathsf{Hyb}_1$. This follows due to the hiding property of the commitment scheme Com.

We claim $\mathsf{Hyb}_1 \approx \mathsf{Hyb}_2$. This follows by the zero-knowledge property of CNIZK.

We claim $\mathsf{Hyb}_2 \approx \mathsf{Hyb}_3$. This follows by the semantic security of PKE since sk is never used in the experiment.

Suppose for a contradiction that $\Pr[\mathsf{LOCC\_PROOF}(\lambda, \mathcal{A}) = 1]$ is non-negligible, then so is $\Pr[\mathsf{Hyb}_3 = 1]$ by the hybrid argument above. Now we claim that decrypting the ciphertext ct' contained in the proof output yields a witness w' such that $(x, w) \in R_L$. First, observe that by perfect binding property of Com, there does not exist r such that $com^* = \mathsf{Com}(P_0||P_1; r)$ and $P_0||P_1 \neq \mathsf{OP}_0||\mathsf{OP}_1$.

Then suppose that the programs P_0, P_1 contained in the proof output by the adversary satisfy $P_0||P_1 \neq \mathsf{OP}_0||\mathsf{OP}_1$. However, then observe that we can create an adversary for LOCC-leakage-resilience game for subspace states (Theorem 9) by simulating our NIZK leakage adversary, since the state verification of NIZK in Hyb_3 exactly corresponds to the verification of the LOCC-leakage-resilience game. Thus, we must have $P_0||P_1 \neq \mathsf{OP}_0||\mathsf{OP}_1$, Now, since the commitment condition cannot be satisfied, by soundness of CNIZK, we must have that there exist r'' such that $ct' = \mathsf{PKE.Enc}(pk, w')$ and $(x, w') \in R_L$. This means that decrypting ct' gives us a valid witness w' for x, whereas the experiment never uses a witness for x. This contradicts the hardness of the distribution $\mathcal{D}$. □

Since classical NIZKs can be constructed from one-way functions and iO ([SW14]), we obtain the following corollary.

Corollary 3. *Assuming the existence of indistinguishability obfuscation and one-way functions, there exists a NIZK proof system with LOCC-leakage-resilient proofs.*

6 Acknowledgments

Alper Çakan was supported by the following grants of Vipul Goyal: NSF award 1916939, DARPA SIEVE program, a gift from Ripple, a DoE NETL award, a JP Morgan Faculty Fellowship, a PNC center for financial services innovation award, and a Cylab seed funding award.

References

[Aar16] Scott Aaronson. The complexity of quantum states and transformations: From quantum money to black holes, 2016.

[AARR03] Dakshi Agrawal, Bruce Archambeault, Josyula R. Rao, and Pankaj Rohatgi. The EM side—channel(s). In Burton S. Kaliski, Çetin K. Koç, and Christof Paar, editors, *Cryptographic Hardware and Embedded Systems - CHES 2002*, pages 29–45, Berlin, Heidelberg, 2003. Springer Berlin Heidelberg.

[AC12] Scott Aaronson and Paul Christiano. Quantum money from hidden subspaces. In *Proceedings of the Forty-Fourth Annual ACM Symposium on Theory of Computing*, STOC '12, page 41–60, New York, NY, USA, 2012. Association for Computing Machinery.

[AGKZ20] Ryan Amos, Marios Georgiou, Aggelos Kiayias, and Mark Zhandry. One-shot signatures and applications to hybrid quantum/classical authentication. In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*, pages 255–268, 2020.

[BB14] Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical computer science*, 560:7–11, 2014.

[BDS23] Shalev Ben-David and Or Sattath. Quantum Tokens for Digital Signatures. *Quantum*, 7:901, January 2023.

[ÇGLZR24] Alper Çakan, Vipul Goyal, Chen-Da Liu-Zhang, and João Ribeiro. Unbounded leakage-resilience and intrusion-detection in a quantum world. In *Theory of Cryptography*. Springer, 2024.

[CLLZ21] Andrea Coladangelo, Jiahui Liu, Qipeng Liu, and Mark Zhandry. Hidden cosets and applications to unclonable cryptography. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology – CRYPTO 2021*, pages 556–584, Cham, 2021. Springer International Publishing.

[GMR23] Vipul Goyal, Giulio Malavolta, and Justin Raizes. Unclonable commitments and proofs. *Cryptology ePrint Archive*, 2023.

[HMNY21] Taiga Hiroka, Tomoyuki Morimae, Ryo Nishimaki, and Takashi Yamakawa. Quantum encryption with certified deletion, revisited: Public key, attribute-based, and classical communication. In *Advances in Cryptology–ASIACRYPT 2021: 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6–10, 2021, Proceedings, Part I 27*, pages 606–636. Springer, 2021.

[JK23] Ruta Jawale and Dakshita Khurana. Unclonable non-interactive zero-knowledge. *Cryptology ePrint Archive*, 2023.

[KNTY19] Fuyuki Kitagawa, Ryo Nishimaki, Keisuke Tanaka, and Takashi Yamakawa. Adaptively secure and succinct functional encryption: improving security and efficiency, simultaneously. In *Advances in Cryptology–CRYPTO 2019: 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18–22, 2019, Proceedings, Part III 39*, pages 521–551. Springer, 2019.

[Koc96] Paul C. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In Neal Koblitz, editor, *Advances in Cryptology — CRYPTO '96*, pages 104–113, 1996.

[KR19] Yael Tauman Kalai and Leonid Reyzin. A survey of leakage-resilient cryptography. In *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*, pages 727–794. ACM, 2019.

[NC10] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition.* Cambridge University Press, 2010.

[QS01] Jean-Jacques Quisquater and David Samyde. ElectroMagnetic Analysis (EMA): Measures and counter-measures for smart cards. In Isabelle Attali and Thomas Jensen, editors, *Smart Card Programming and Security*, pages 200–210, Berlin, Heidelberg, 2001. Springer Berlin Heidelberg.

[SW14] Amit Sahai and Brent Waters. How to use indistinguishability obfuscation: Deniable encryption, and more. In *Proceedings of the Forty-Sixth Annual ACM Symposium on Theory of Computing*, STOC '14, page 475–484, New York, NY, USA, 2014. Association for Computing Machinery.

[TFKW13] Marco Tomamichel, Serge Fehr, Jedrzej Kaniewski, and Stephanie Wehner. A monogamy-of-entanglement game with applications to device-independent quantum cryptography. *New Journal of Physics*, 15(10):103002, oct 2013.

[Wie83] Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, jan 1983.

[Zha19] Mark Zhandry. Quantum lightning never strikes the same state twice. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2019*, pages 408–438, Cham, 2019. Springer International Publishing.