Public Key Encryption Secure Against Quantum Leakage

Alper Çakan[2], Fuyuki Kitagawa[3], Ryo Nishimaki[3], Manasi Shingane[1,*], and Takashi Yamakawa[3]

[1]QuICS, University of Maryland, College Park, MD 20742, USA
[2]Carnegie Mellon University, Pittsburgh, PA
[3]NTT Social Informatics Laboratories, Tokyo, Japan

May 19, 2026

Abstract

Side-channel attacks are a relevant threat to many modern cryptographic schemes and often have fatal consequences such as revealing partial information about secret keys. While leakage-resilient cryptography aims to solve this problem, existing works focus exclusively on showing security against classical leakage. Moreover, recent public key encryption (PKE) schemes utilizing quantum secret keys achieve security against unbounded classical leakage, but offer no guarantees on any amount of quantum leakage. Since security guarantees on classical side information do not necessarily translate to guarantees on quantum side information, showing PKE schemes that are secure in the presence of quantum leakage remains open.

In this work, we address this problem by extending the definition of leakage resilience for PKE in the bounded-leakage model to allow for quantum leakage. We provide the following two constructions:

- **PKE with Quantum Secret Keys** We construct a PKE scheme that tolerates unbounded classical leakage alongside bounded, constant-rate ($\lambda < 0.057$) quantum leakage. Our construction assumes the existence of polynomially secure post-quantum indistinguishability obfuscation (iO) as well as one-way functions (OWFs).
- **PKE with Classical Secret Keys** We construct a classical PKE scheme that is secure against bounded quantum leakage. Our construction offers a tradeoff between the achievable leakage rate and the underlying cryptographic assumptions. Assuming the hardness of the learning with errors problem (LWE) we obtain an optimal leakage rate of $\lambda \leq 1 - o(1)$. Alternatively, assuming only post-quantum PKE, we obtain a leakge rate of $\lambda \leq \frac{1}{poly(n)}$.

1 Introduction

Modern cryptographic schemes are often deployed in environments where secret keys may not remain perfectly hidden. Partial information about a secret key can be exposed through side-channel attacks, compromised randomness, or timing attacks. *Leakage-resilient* cryptography [ISW03, MR04, DP08] studies the extent to which such leakage can be tolerated while preserving the security of the underlying scheme.

In the public key setting, leakage-resilient public key encryption (PKE) has been studied under a variety of leakage models, including bounded leakage model [AGV09, NS09, HLWW16], bounded

*Part of this work was done while visiting NTT Social Informatics Laboratories for an internship.

retrieval model [DLW06, Dzi06, ADW09], auxiliary-input leakage model [DKL09], and continual leakage model [BKKV10, DHLW10]. Among these models, the bounded leakage model is the most relevant to this work. In this model, the number of leakage bits that an adversary can obtain from the secret key is bounded. This bound is necessary for meaningful security: without such a bound, the entire secret key could be leaked, in which case security is trivially impossible.

Interestingly, a recent work of Çakan, Goyal, Liu-Zhang, and Ribeiro [ÇGLZR24] shows that this seemingly unavoidable barrier in the bounded-leakage model can be overcome if one uses quantum secret keys while allowing only classical leakage. In this setting, the trivial attack of leaking the entire secret key is ruled out, since a quantum secret key cannot in general be fully encoded as classical leakage.

They construct a PKE scheme with quantum secret keys that tolerates unbounded classical leakage, building on earlier techniques for PKE with copy-protected secret keys (a.k.a. single-decryptor encryption) [CLLZ21]. A caveat of their construction, however, is that it offers no security guarantee in the presence of *quantum* leakage. This is a natural concern once the secret key itself is quantum: a compromised implementation may expose part of the quantum register holding the secret key, rather than merely producing classical side information about it. For example, quantum leakage could correspond to a certain fraction of the qubits of the secret key becoming public. Ideally, one would like to have guarantees on how much of the quantum secret key can be leaked while still preserving the security of the underlying scheme. Of course, it is impossible to tolerate unbounded quantum leakage: if the entire secret key is leaked, security is impossible. Nevertheless, it may still be possible to achieve security against bounded quantum leakage.

This motivates the following natural question:

Can we construct a PKE scheme with quantum secret keys that tolerates unbounded classical leakage and bounded quantum leakage?

The question is not limited to PKE schemes with quantum secret keys. One can also ask whether classical PKE schemes with classical secret keys can be secure against quantum leakage. Of course, in this classical setting, unbounded classical leakage cannot be tolerated, since such leakage could reveal the entire secret key. Thus, the relevant question is whether classical PKE can tolerate bounded quantum leakage.

To the best of our knowledge, existing works on leakage-resilient PKE consider only classical leakage. This remains true even for post-quantum PKE schemes, which are designed to be secure against quantum attacks. In the post-quantum setting, however, it is natural to consider adversaries that may obtain quantum side information about the secret key. Even when the secret key is classical, leakage is ultimately generated by a physical process. A quantum adversary may keep this process coherent and obtain a quantum system correlated with the secret key, rather than a measured classical outcome. Such a model may capture future settings in which devices interact with quantum communication networks, as well as physical side channels whose leakage may be better modeled as quantum information.

The distinction between classical and quantum leakage is substantive. Gavinsky, Kempe, Kerenidis, Raz, and de Wolf [GKK+07], building on a classical–quantum separation in communication complexity, showed that there exists a classical randomness extractor that is secure against a certain amount of classical side information but fails in the presence of a much smaller amount of quantum side information. This yields a direct example of a one-time symmetric-key encryption (SKE) scheme that tolerates a certain amount of classical leakage, yet can be broken by a much smaller amount of quantum leakage. Thus, security against classical leakage does not by itself provide evidence of security against quantum leakage.

This naturally motivates the following question:

Can we construct classical PKE schemes with classical secret keys that tolerate bounded quantum leakage?

1.1 Our Results

We answer these questions affirmatively. First, we extend the definition of leakage resilience for PKE in the bounded-leakage model to allow quantum leakage. We then construct the following two PKE schemes.

1. **A PKE scheme with quantum secret keys that is secure against unbounded classical leakage and bounded quantum leakage.** Our scheme remains secure against *unbounded* classical leakage L_c and constant-rate bounded quantum leakage L_q. Specifically, security holds as long as the leakage ratio $\lambda = \frac{|L_q|}{|sk|}$ is at most a certain constant $\lambda \approx 0.057$. Our construction relies on polynomially secure indistinguishability obfuscation (iO) and one-way functions (OWFs). In comparison, the prior work of [ÇGLZR24] achieved resilience only against unbounded classical leakage, and did so under subexponentially secure iO, subexponentially secure OWFs, and the polynomial hardness of learning with errors (LWE). Thus, our result simultaneously weakens the assumptions and achieves constant-rate bounded quantum leakage resilience.

2. **A classical PKE scheme that is secure against bounded quantum leakage.** We give two different instantiations of this scheme, yielding a tradeoff between assumptions and leakage ratio. Assuming ciphertext-policy functional encryption (CPFE) with succinct keys, which exists under the polynomial hardness of LWE [KN23], our scheme achieves the optimal leakage ratio $\lambda = 1 - o(1)$. That is, the scheme remains secure even if quantum leakage of length almost as large as the entire secret key is leaked. Alternatively, assuming only post-quantum PKE, we obtain leakage ratio $\lambda = 1/\mathsf{poly}(n)$, where n is the security parameter.

   This tradeoff matches the known tradeoff in the classical-leakage setting: an optimal leakage ratio is achievable under LWE [BLSV18], while an inverse-polynomial leakage ratio is achievable under any PKE [HLWW16].[1] Our contribution is to obtain the analogous tradeoff for quantum leakage in a unified framework based on CPFE. This unification is new even in the classical setting, and may be of independent interest.

1.2 Discussion

To motivate our work, it is natural to ask whether quantum leakage resilience follows from classical leakage resilience.

In the quantum secret key setting, such a separation is trivial to obtain. Start with a PKE scheme with quantum secret keys that tolerates unbounded classical leakage, and append to its secret key a large amount of garbage quantum state. This clearly does not affect resilience to unbounded classical leakage. On the other hand, if the quantum secret key of the original scheme is leaked, then the scheme is clearly insecure. If the secret-key length of the original scheme is $|\mathsf{sk}|$ and the length of the garbage state is ℓ, then the actual key part constitutes only a $\frac{|\mathsf{sk}|}{|\mathsf{sk}|+\ell}$ fraction of the secret key of the compiled scheme. Since ℓ can be chosen to be an arbitrarily large polynomial, this

[1] It is plausible that the schemes of [HLWW16, BLSV18] can also be shown to be secure against bounded quantum leakage, since they ultimately rely on the leftover hash lemma, which is known to hold against quantum side information [TSSR11]. However, making such extensions formal would require reanalyzing those schemes in the quantum leakage setting. We instead obtain the same tradeoff in a unified framework based on CPFE.

shows that unbounded classical leakage resilience does not even imply bounded quantum leakage resilience with inverse-polynomial leakage ratio.

The situation is more subtle in the classical secret key setting. There seems to be no trivial example separating classical and quantum leakage resilience for PKE. As already mentioned, such a separation is known for one-time SKE, based on [GKK+07]. We observe that this separation can be lifted directly to the PKE setting in the non-adaptive leakage model, where the leakage function cannot depend on the public key.

The idea is as follows. Starting from any classical PKE scheme, we augment the public key with an encryption of the PKE secret key under the above one-time SKE scheme. The secret key of the resulting PKE scheme is then the secret key of the one-time SKE scheme. To decrypt, one first recovers the secret key of the base PKE scheme by decrypting the additional public-key component using the one-time SKE secret key, and then runs the decryption algorithm of the base PKE scheme.

In the non-adaptive leakage model, where the leakage function cannot depend on the public key, we can rely on the classical leakage resilience of the one-time SKE scheme to prove classical leakage resilience of the resulting PKE scheme. On the other hand, the insecurity of the one-time SKE scheme against quantum leakage directly lifts to insecurity of the resulting PKE scheme against quantum leakage. This gives a separation in the non-adaptive leakage model.

Unfortunately, this idea does not work in the adaptive leakage model considered in this work. Indeed, the above scheme is trivially insecure even against classical leakage in the adaptive leakage model: once the public key is available, the leakage function can simply recover and output the secret key of the base PKE scheme. Thus, we leave open the problem of separating classical and quantum leakage resilience in the adaptive leakage model.

1.3 Related Works

Classical leakage-resilient PKE Many works have studied leakage-resilient PKE in the classical bounded-leakage model [AGV09, NS09, HLWW16, BLSV18]. In particular, prior works establish a tradeoff between assumptions and achievable leakage ratios in the classical-leakage setting [HLWW16, BLSV18]. Our work gives an analogous tradeoff in the presence of quantum leakage.

Classical leakage-resilient PKE has also been studied in several other models, including the bounded-retrieval model [DLW06, Dzi06, ADW09], the auxiliary-input leakage model [DKL09], and the continual-leakage model [BKKV10, DHLW10]. Extending these models to the quantum-leakage setting is beyond the scope of this paper and is left for future work. We refer to [KR19] for a more extensive survey of the classical leakage-resilience literature.

PKE with quantum secret keys Considering PKE schemes with quantum secret keys as a way to circumvent classical impossibility has recently emerged as an active line of research. The earliest works of this kind constructed single-decryptor encryption [GZ20, CLLZ21, LLQZ22, ÇG24b, KY25], which enables copy-protection of secret keys. These works can be viewed as special cases of the broader notion of quantum copy-protection [Aar09], which has also been studied extensively in recent years [ALL+21, AB24, ÇG26, ABH+26].

As a notion related to copy-protection, another line of work studies secure key leasing for PKE [AKN+23, APV23, AHH24, KMY25], which can be viewed as an instance of the more general concept of secure software leasing [AL21, KNY21, BJL+21].

The relationship between copy-protected secret keys and unbounded classical leakage resilience was first pointed out and studied in [ÇGLZR24]. Subsequent works extended this perspective

to broader primitives, such as signatures, zero-knowledge proofs, and secret sharing [ÇG24a, CKNY25]. However, none of these works consider quantum leakage.

Quantum side information. To the best of our knowledge, this work is the first to study leakage-resilient PKE against quantum leakage. More broadly, however, there is a substantial body of work on information-theoretic security in the presence of quantum side information. This line of work goes back at least to Renner's framework for analyzing privacy amplification in quantum key distribution [Ren05]. Subsequent works studied randomness extraction against quantum side information, including the leftover hash lemma [TSSR11] and Trevisan's extractor [DPVR12], as well as non-malleable extractors [ACLV19, ABJO24, BJK24]. The work of Gavinsky, Kempe, Kerenidis, Raz, and de Wolf [GKK+07] shows that classical and quantum side information can behave very differently, by separating extractors secure against classical side information from those secure against quantum side information.

2 Technical Overview

We now given an overview of both PKE constructions and their respective security proofs.

2.1 Constant-Leakage Secure PKE

Coset States We construct our PKE using *coset states*, previously studied by [CLLZ21, VZ21]. A coset state is defined by a subspace $A \subseteq \mathbb{F}^n$ where $\dim(A) = \frac{n}{2}$ and two vectors $s, t \in \mathbb{F}_2^n$. A coset state is then defined as

$$|A_{s,t}\rangle = \frac{1}{\sqrt{|A|}} \sum_{a \in A} (-1)^{\langle a,t \rangle} |a + s\rangle .$$

Let $A^\perp$ denote the dual space of A. We will also define the *canonical representative* of a coset $A+s$ to be the lexicographically smallest vector contained in $A + s$. We define the function $\mathsf{Can}_A(s)$ to be the function that outputs the canonical representative of $A + s$. We will also define a set $\mathsf{CS}(A)$ as the set of canonical representatives relative to the subspace A. Formally,

$$\mathsf{CS}(A) = \{\mathsf{Can}_A(s) : s \in \mathbb{F}_2^n\}.$$

At times, we will write $iO(A+s)$ and $iO(A^\perp+t)$ to be the obfuscated circuit that checks membership of a vector in $A+s$ and $A^\perp+t$ respectively. That is, $iO(A+s)(v) = 1$ if $v \in A+s$ (and analogously for $iO(A^\perp + t)$).

We will use the fact that coset states satisfy a certain monogamy of entanglement (MoE) property which was proven by [CLLZ21, CV22]. The property is modeled as a game between a challenger and a tuple of adversaries, $(\mathcal{A}_0, \mathcal{A}_1, \mathcal{A}_2)$:

MoE Game

1. The challenger samples a uniformly random subspace $A \subseteq \mathbb{F}_2^n$ of dimension $\frac{n}{2}$ and also samples two elements $s, t \in \mathbb{F}_2^\lambda$ uniformly at random.
2. The challenger sends the coset state $|A_{s,t}\rangle$ to $\mathcal{A}_0$.
3. $\mathcal{A}_0$ outputs two arbitrary registers R_1 and R_2. Then $\mathcal{A}_0$ sends R_1 to $\mathcal{A}_1$ and sends R_2 to $\mathcal{A}_2$ respectively.

4. The challenger sends the description of A to $\mathcal{A}_1$ and $\mathcal{A}_2$.

5. $\mathcal{A}_1$ and $\mathcal{A}_2$ outputs guesses u and v respectively.

$(\mathcal{A}_0, \mathcal{A}_1, \mathcal{A}_2)$ win the game if $u \in A + s$ and $v \in A^\perp + t$. The probability that $(\mathcal{A}_0, \mathcal{A}_1, \mathcal{A}_2)$ win the game is negligible.

Monogamy of Entanglement to LOCC Leakage We use a slightly modified version of the MoE property of coset states, known as the Extended Monogamy of Entanglement property. This is exactly the original MoE game defined above, except that in addition to choosing the subspace A, the challenger also

1. Samples a uniformly random subspace $B \subseteq \mathbb{F}_2^n$ of dimension $3n/4$ such that $A \subset B$ and a uniformly random subspace $C \subseteq A$ of dimension $n/4$.

2. Samples vectors $v \leftarrow B$ and $w \leftarrow C^\perp$.

Then the challenger sends descriptions of $B, C, (s+v)$, and $(t+w)$ along with the coset state $|A_{s,t}\rangle$ to $\mathcal{A}_0$. It was first shown in [CLLZ21] that the MoE property of coset states implies the Extended MoE property. The game formalizing the Extended MoE property was later defined in [ABH+26].

Next, we formalize the connection between the Extended MoE property of cosets states and cryptographic leakage. At a high level, we bound the success probability of an adversary in the Extended MoE game, even when the adversary is additionally given arbitrary classical side information correlated with the coset state. Following, [ÇGLZR24], we denote classical side information correlated with a quantum secret key as leakage generated under local operations and classical communication, or LOCC leakage.

Previously, [ÇGLZR24] proved that the standard MoE property of coset states implies that coset states also satisfy the standard MoE property when the adversary is also given LOCC leakage. We call this the LOCC Leakage property of Coset States. The authors of [ÇGLZR24] formalized the LOCC Leakage property via a leakage game between a challenger and a quantum leakage adversary, $\mathcal{A} = (\mathcal{A}_{Main}, \mathcal{A}_{Leak})$. The challenger sends the coset state to $\mathcal{A}_{Leak}$, who then sends a (potentially unbounded) amount of LOCC leakage to $\mathcal{A}_{Main}$.

Although the standard MoE property of coset states implies the Extended MoE property, it is not a priori clear whether the Extended MoE property suffices to establish the LOCC leakage property. Using similar techniques to [ÇGLZR24], we show the implication indeed holds for the Extended MoE Property of coset states. Specifically, we show that even given the additional side information, $(B, C, s+t, t+w)$ and LOCC leakage, the probability that $(\mathcal{A}_0, \mathcal{A}_1, \mathcal{A}_2)$ win the MoE game is small.

LOCC Leakage to Quantum Leakage Next, we argue coset states also satisfy the MoE property in the presence of quantum leakage. In this model, the quantum leakage adversary $\mathcal{A} = (\mathcal{A}_{Main}, \mathcal{A}_{Leak})$ plays the same Extended MoE game with the challenger, except now $\mathcal{A}_{Leak}$ is allowed to output bounded quantum information as well as unbounded classical information. We denote the quantum state output by $\mathcal{A}_{Leak}$ as quantum leakage. Our proof relies on a previous lemma proven by Boneh and Zhandry [BZ13]. At a high level, their lemma states that performing an intermediate k-outcome partial measurement in the middle of a quantum algorithm can reduce the probability of any fixed output by at most a factor of k.

We use this lemma in order to prove that the Extended MoE property of coset states with quantum leakage is implied by the Extended MoE property of coset states with LOCC leakage. In

the reduction, we simulate quantum leakage by explicitly measuring the leakage state produced by $\mathcal{A}_{Leak}$. By the lemma, this intermediate measurement decreases the success probability of $\mathcal{A}_{Main}$ by at most a multiplicative constant. Since the total quantum leakage is bounded by a sufficiently small constant fraction of the secret key length, this loss is only incurs a constant factor loss in the exponent of the success probability.

Quantum Leakage in the Computational Setting The next step in our proof is to upgrade the established information theoretic guarantees of cosets states to the computational setting. Looking forward, our PKE construction relies on the ability to check if a vector is in the coset $A+s$ or $A^{\perp}+t$. This implies that the membership checking algorithm must be public. [CLLZ21] showed that it is indeed possible to have public coset membership by instead relying on the *computational* MoE property of coset states. Their reduction assumes the existence of post-quantum indistinguishability obfuscation and uses *subspace hiding obfuscation* [Zha21] in order to construct an adversary for the information theoretic MoE property.

In our setting, the main technical challenge is to establish that a similar reduction continues to hold when (1) the adversary is permitted quantum leakage, and (2) we analyze the Extended MoE property of coset states. To address this, we first formalize a version of the Extended MoE property that is secure against computationally bounded quantum leakage adversaries. We then prove a reduction from the information-theoretic Extended MoE property with quantum leakage to its computational counterpart.

PKE Construction and Security under Quantum Leakage Finally, we argue security of our PKE construction under quantum leakage. We first provide a sketch of our PKE construction.

Algorithm 1 Program $P[C, \mathsf{str}](x)$

Hardwired Constant:A description of a circuit C with 1-bit output and a ℓ_{msg}-bit string str.
Input: $x \in \{0,1\}^{\ell_{msg}}$.
if $C(x) = 1$ **then**:
  Output str
else:
  Output $0^{\ell_{msg}}$
end if

Key Generation: The key generation algorithm generates a coset state $|A_{s,t}\rangle$ by sampling a subspace $A \subseteq \mathbb{F}_2^n$ and two vectors, $s, t \in \mathsf{CS}(A) \times \mathsf{CS}(A^{\perp})$. It also generates two algorithms, $C_{mc} = iO(A + s)$ and $C_{mc}^{\perp} = iO(A^{\perp} + t)$. C_{mc} and $C_{mc}^{\perp}$ are obfuscations of the algorithms that check membership in $A + s$ and $A^{\perp} + t$ respectively. The public key is set as $\mathsf{pk} = (C_{mc}, C_{mc}^{\perp})$ and the secret key is $\mathsf{sk} = |A_{s,t}\rangle$.

Encryption: To encrypt a message $m = m_1||m_2$ where $m_1, m_2 \in \{0,1\}^{\ell} \times \{0,1\}^{\ell}$ under the public key $\mathsf{pk} = (C_{mc}, C_{mc}^{\perp})$, the algorithms first generates two obfuscated circuits $\tilde{P} = iO(P[C_{mc}, m_1]$ and $\tilde{P}^{\perp} = iO(P[C_{mc}^{\perp}, m_2])$ where the circuits $P[C_{mc}, m_1]$ and $P[C_{mc}^{\perp}, m_2]$ are circuits that respectively output m_1 and m_2 when the input is accepted by the appropriate coset membership checking algorithm. The full description is in Algorithm 1. The ciphertext is set to be $\mathsf{ct} = (\tilde{P}, \tilde{P}^{\perp})$.

Decryption: To decrypt a message $\mathsf{ct} = (\tilde{P}, \tilde{P}^{\perp})$ using the secret key $\mathsf{sk} = |A_{s,t}\rangle$, we can use the fact that measuring sk in the computational basis yields a a vector in $A + s$ and measuring sk in the Hadamard basis yields a vector in $A^{\perp} + t$. Together with $\tilde{P}$ and $\tilde{P}^{\perp}$, we can obtain the message $m = m_1||m_2$.

Proof sketch for One-Way Security under Quantum Leakage. Next, we describe our security proof for the PKE scheme. Our proof strategy follows similarly to the techniques used by [KY25]. We first prove One-Way Security under Quantum Leakage, in which an efficient challenger encrypts a message $m \in \{0,1\}^{2\ell}$ and sends the ciphertext to the quantum leakage adversary who is then tasked with decryption. If the adversary succeeds with non-negligible probably, the adversary wins the game. We will show that given a quantum leakage adversary for the One-Way Security game, we can construct a quantum leakage adversary for the computational Extended MoE property of coset states with quantum leakage.

Algorithm 2 Program $Q[C, A, \mathsf{str}](x)$

Hardwired Constant:A description of a circuit C with 1-bit output, a description of an $\frac{n}{2}$ dimensional subspace A, and a ℓ_{msg}-bit string str.
Input: $x \in \{0,1\}^n$.
if $C(x) = 1$ **then**:
  Compute $s = \mathsf{Can}_A(x)$, output $\mathsf{str} \oplus s$.
else:
  Output $0^{\ell_{msg}}$
end if

Our proof crucially relies on the argument that the the encryption of the ciphertext can be simulated given only knowledge of the public key and A. First, we slightly modify how the ciphertext is generated using P. We hardcode the vectors s and t into the circuit P and generate the ciphertext as $\tilde{P} \leftarrow iO(P[C_{mc}, m_1 \oplus s])$ and $\tilde{P}^{\perp} \leftarrow iO(P[C^{\perp}_{mc}, m_2 \oplus t])$. Notice that the ciphertexts in this scheme are distributed identically to those in the actual scheme. Next, we describe our simulated ciphertexts. On input the public key $\mathsf{pk} = (C_{mc}, C^{\perp}_{mc})$, A, and the message the challenger will use an alternative circuits $Q[C_{mc}, A, m_1]$ and $Q[C^{\perp}_{mc}, A, m_2]$ to generate the ciphertext (as opposed to the circuit P described above). Circuit Q takes input an n bit string x and outputs $m_1 \oplus s$ (respectively, $m_2 \oplus t$) if $x \in A + s$ (respectively, $x \in A^{\perp} + t$) and 0 otherwise. The full description can be found in Algorithm 2. The challenger then generates $\tilde{P} \leftarrow iO(Q[C_{mc}, A, m_1])$ and $\tilde{P}^{\perp} \leftarrow iO(Q[C_{mc}, A^{\perp}, m_2])$ and sets the ciphertext to be the obfuscations $\mathsf{ct} = (\tilde{P}, \tilde{P}^{\perp})$.

We show that $Q[C_{mc}, A, m_1]$ is functionally equivalent to $P[C_{mc}, m_1 \oplus s]$. This is true because on input x, if $x \in A + s$, then both programs output $m_1 \oplus s$ and if $x \notin A + s$, then both programs output 0^{ℓ}. Analogously, $Q[C^{\perp}_{mc}, A^{\perp}, m_2]$ is functionally equivalent to $P[C^{\perp}_{mc}, m_2 \oplus t]$ since both programs output $m_2 \oplus t$ if $x \in A^{\perp} + t$ and 0^{ℓ} otherwise. Therefore, by the security of post-quantum iO, the obfuscations of P and Q are indistinguishable to a QPT adversary. Then a reduction to the computational Extended MoE property is straightforward: Given One-Way Security leakage adversary that outputs a decryption of $\mathsf{ct} = (\tilde{P}, \tilde{P}^{\perp})$ where $\tilde{P}$ and $\tilde{P}^{\perp}$ are generated according to the circuit Q, we can extract s and t. This is because P encrypts the message $m_1 \oplus s$ and $\tilde{P}^{\perp}$ encrypts the message $m_2 \oplus t$ when generated according to the circuit Q. This directly breaks the computational Extended MOE property of coset states under quantum leakage.

One-Way Security to IND Security The final argument is to upgrade One-Way Security under Quantum Leakage of our PKE scheme to the more standard IND Security under Quantum

Leakage. We do this using the Quanutm Goldreich-Levin Theorem (Theorem 3.4). Our process takes a One-Way Secure PKE, $\mathsf{PKE}_{\mathsf{OW}}$ that encrypts n-bit strings and constructs an IND-Secure PKE, $\mathsf{PKE}_{\mathsf{IND}}$ that encrypts a singly bit. $\mathsf{PKE}_{\mathsf{IND}}$ is constructed as follows:

Key Generation: The key generation algorithm runs $\mathsf{PKE}_{\mathsf{OW}}.\mathsf{KeyGen} \to (\mathsf{pk}, \mathsf{sk})$ and outputs the public key pk and the secret key sk,

Encryption: The encryption algorithm generates a ciphertext encrypting a single bit message m under the public key pk. The algorithm first samples a n-bit string x and generates $\tilde{\mathsf{ct}} \leftarrow \mathsf{PKE}_{\mathsf{OW}}.\mathsf{Enc}(\mathsf{pk}, x)$. Next, the algorithm generates a bit string $r \leftarrow \{0,1\}^n$ uniformly at random and computes $\beta = \langle x, r\rangle \oplus m$. Finally, it outputs the ciphertext, $\mathsf{ct} = (\tilde{\mathsf{ct}}, r, \beta)$.

Decryption: The decryption algorithm first obtains x by running $\mathsf{PKE}_{\mathsf{OW}}.\mathsf{Dec}(\mathsf{sk}, \tilde{\mathsf{ct}})$. Then it computes the message m given x, r, and β.

Proof Sketch for Security of $\mathsf{PKE}_{\mathsf{IND}}$: The security of our scheme follows from a reduction from the One-Way Security of $\mathsf{PKE}_{\mathsf{OW}}$ under quantum leakage. Specifically, we argue that since an IND adversary can distinguish between a ciphertexts encrypting message bits $m_0 = 0$ and $m_1 = 1$, there exists an algorithm that is able to computer $\langle x, r\rangle$ with advantage ϵ where ϵ is a term that scales non-negligibly in the security parameter. Then, we can apply the Quantum Goldreich-Levin Theorem (Theorem 3.4) which argues that given an algorithm that computes $\langle x, r\rangle$ with advantage ϵ, then there exists an algorithm that computes x with probability $\Omega(\epsilon^2)$. Moreover, since the construction of $\mathsf{PKE}_{\mathsf{IND}}$ preserves the secret key of $\mathsf{PKE}_{\mathsf{OW}}$ the leakage guarantees are preserved as well.

2.2 Classical PKE with Security under Quantum Leakage

In this section we provide a technical overview of the construction and security proof of our second PKE scheme. This PKE scheme is purely classical, and we ultimately show IND-Security under bounded quantum leakage. As stated in the introduction, this scheme is able to tolerate up to $(1 - o(1))n$ qubits of leakage, where n is the length of the secret key. The main idea is to begin with a secret key encryption (SKE) scheme that is secure against bounded leakage, and then use a variant of a functional encryption scheme to upgrade the SKE scheme to a PKE scheme.

Leakage Resilience of the One-Time Pad We begin by arguing that the one-time pad scheme satisfies one-way security under bounded quantum leakage. The One-Way security game is again defined with a leakage adversary $\mathcal{A} = (\mathcal{A}_{Main}, \mathcal{A}_{Leak})$. In the security game, the challenger samples a particular key $K \leftarrow \{0,1\}^n$ uniformly at random and then sends K to $\mathcal{A}_{Leak}$. Then, $\mathcal{A}_{leak}$ and $\mathcal{A}_{Main}$ run their leakage protocol in which they exchange up to $(1-o(1))n$ qubits of leakage. Finally, the challenger randomly chooses a message m and sends the ciphertext $\mathsf{ct} = K \oplus m$ to $\mathcal{A}_{Main}$ who is then tasked with guessing the encrypted message.

Our proof relies on the Quantum Leakage Chain Rule (Theorem 7.1), which was proven by Lai and Chung [LC18]. At a high level, the Leakage Chain Rule provides a formal bound on the entropy loss of a private bit string when a finite amount of information is leaked to the adversary. While the classical bound is linear in the number of bits leaked, the Quantum Leakage Chain rule of [LC18] generalize this bound to the interactive quantum setting. It establishes that if an adversary with quantum side information B obtains leakage registers $L_1, \ldots, L_t$ in some interactive quantum

protocol, then the conditional min entropy of a classical secret X degrades proportionally to the total leakage:

$$H_{min}(X|BL_1,\ldots,L_t) \geq H_{min}(X|B) - \sum_i \log|L_i|.$$

Since the leakage obtained by $\mathcal{A}_{Main}$ is bounded by $(1-o(1))n$ and security is with respect to uniform message distributions over n-bit messages, it holds that the overall success probability of the leakage adversary $\mathcal{A}$ is negligible in n.

From SKE to PKE Next we show that by combining the one-time pad and a primitive known as a ciphertext-policy functional encryption scheme (CPFE), we can construct a PKE scheme satisfying one-way security under bounded quantum leakage. We use the CPFE formalism defined in [KN23] and define a CPFE scheme by four algorithms:

- $\mathsf{CPFE.Setup}$: The setup algorithm takes in a security parameter n and outputs a master public key and master secret key, (MPK, MSK).
- $\mathsf{CPFE.Keygen}$: The key generation algorithm takes input the master secret key MSK as well as a string x and outputs a secret key sk_x.
- $\mathsf{CPFE.Enc}$: The encryption algorithm takes input the public key pk and a circuit C and outputs a ciphertext, ct.
- $\mathsf{CPFE.Dec}$: The decryption algorithm takes in sk_x and the ciphertext ct and outputs $C(x)$.

[KN23] showed that by assuming the existence of hash encryption (which is known to be constructed assuming polynomial hardness of the learning with error (LWE) problem [DGHM18]), one can construct a CPFE scheme. Moreover, the authors showed that the constructed CPFE scheme satisfies a certain "succinctness" property, which states that the secret key of is the form (x, sk_x) and the length of the secret key does not scale multiplicatively with length of x, i.e. $|\mathsf{sk}_x| = \mathsf{poly}(n') + |x|$ (where n' is the security parameter of the CPFE scheme). We use the CPFE scheme as well as the One-Time Pad scheme to construct our PKE as follows:

Key Generation: The key generation algorithm first generates a key $K \leftarrow \{0,1\}^n$ uniformly at random. It also runs $\mathsf{CPFE.Setup}$ generate a master public key MPK as well as $\mathsf{CPFE.Keygen}$ on input K and MSK to generate a secret key sk_K. It then ouputs the public key as $\mathsf{pk} = MPK$ and the secret key as $\mathsf{sk} = (K, \mathsf{sk}_K)$.

Encryption: The encryption algorithm generates a ciphertext that encrypts an n-bit message. It runs $\mathsf{CPFE.Enc}$ on the public key $\mathsf{pk} = MPK$ and a circuit C_m, which maps the key K to $K \oplus m$, and outputs the resulting ciphertext.

Decryption: The decryption algorithm first runs $\mathsf{CPFE.Dec}$ using sk_K, which results in a One-Time Pad ciphertext encrypted under the key K. It then uses the key K to decrypt the resulting One-Time Pad ciphertext and outputs the message.

It is not hard to see that the leakage rate of this PKE scheme depends on the leakage rate of the underlying One-Time Pad scheme. Let us define leakage rate of our scheme to be λ_{PKE} and the leakage rate of the OTP scheme as λ_{OTP}. The leakage of the PKE scheme must not exceed the leakage tolerated by the OTP scheme. It then holds that

$$\lambda_{\mathsf{PKE}}(|K| + |\mathsf{sk}_K|) \leq \lambda_{\mathsf{OTP}}|K| \tag{1}$$

or equivalently,

$$\lambda_{\mathsf{PKE}} \leq \lambda_{\mathsf{OTP}} \frac{|K|}{(|K| + |\mathsf{sk}_K|)}. \tag{2}$$

Then, by the succinctness property of the CPFE scheme and taking the first order approximation with a sufficiently large OTP key K, we know that

$$\lambda_{\mathsf{PKE}} \leq \lambda_{\mathsf{OTP}}(1 - \frac{1}{poly(n)}) \approx 1 - \frac{1}{poly(n)} \tag{3}$$

when $\lambda_{\mathsf{OTP}} = 1 - \frac{1}{poly(n)}$. Thus, the PKE we construct tolerates a leakage rate λ_{PKE} that depends on the leakage rate of the underlying OTP scheme and the size of the OTP secret key $|K|$. Note that the existence of hash encryption is not necessary to construct CPFE. In fact, [KN23] also show that if one requires only the minimal assumption of post-quantum PKE, one can still construct CPFE. However, the resulting CPFE does not satisfy the succinctness property, rather $|\mathsf{sk}| = |x| \cdot poly(n)$. The resulting PKE scheme we obtain is instead satisfies a much weaker leakage rate of $\lambda_{\mathsf{PKE}} = 1/poly(n)$. Finally, analgous to the previous construction, we again use the Quantum Goldreich-Levin Theorem (Theorem 3.4) to compile our One-Way Secure PKE that tolerates leakage rate λ_{PKE} into an IND-Secure PKE that tolerates the same leakage rate.

3 Definitions

3.1 Standard Cryptographic Definitions

In this paper we use the following definitions. For an integer k, we let $[k] = \{1, 2, \ldots, k\}$. For a set X, we use the notation $x \leftarrow X$ to mean that an element x is sampled uniformly at random from X. For a distribution D, we use the notation that $x \leftarrow D$ is sampled according to the distribution D. We will use n to define the security parameter. We say that a function $\epsilon : \mathbb{N} \to \mathbb{N}$ is negligible if for all polynomials p, $\epsilon(n) < 1/p(n)$ for all sufficiently large $n \in \mathbb{N}$. We will use PPT to mean a probabilistic polynomial time algorithm. For PPT algorithms, we will use n to define the security parameter.

3.1.1 Classical Cryptographic Primitives

We will also need the following definition of indistinguishability obfuscation (iO).

Definition 3.1 (Indistinguishability Obfuscation [BGI+01])**.** *We say a PPT algorithm iO is a secure indistinguishability obfuscator iO for a class of circuit families $\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ if it satisfies:*

1. ***Correctness:*** *For all security parameters $n \in \mathbb{N}$, circuits $C \in \mathcal{C}_n$, and inputs x,*

$$\Pr[\mathcal{C}(x) = \mathcal{C}'(x) | \mathcal{C}' \leftarrow \mathsf{iO}(\mathcal{C})] = 1. \tag{4}$$

2. ***Security:*** *Let $n \in \mathbb{N}$. For any QPT distinguisher $\mathcal{D}(1^n)$, there exists a negligible function $\epsilon(n)$ such that for any two circuits $C_0, C_1 \in \mathcal{C}_n$ such that for all inputs x, $C_0(x) = C_1(x)$ and $|C_0| = |C_1|$,*

$$|\Pr[\mathcal{D}(\mathsf{iO}(C_0)) = 1] - \Pr[\mathcal{D}(\mathsf{iO}(C_1)) = 1]| \leq \epsilon(n). \tag{5}$$

There are many known candidates for post-quantum iO of polynomial classical circuits ([CLW25, BGMZ18, CHVW19, APM20, DQV+21]).

We will need to use subspace hiding obfuscation, a technique introduced by Zhandry in [Zha21].

Definition 3.2 (Subspace Hiding Obfuscator [Zha21])**.** *A subspace hiding obfuscator (shO) for a field $\mathbb{F}$ and dimensions (d_0, d_1) is a PPT algorithm shO defined as follows:*

- $\mathsf{shO}(S) \to \hat{S}$*: shO takes input a subspace $S \subseteq \mathbb{F}^n$ of dimension $d \in \{d_0, d_1\}$ and outputs a PPT circuit $\hat{S}$.*
- ***Correctness:*** *Let $\lambda \in \mathbb{N}$. For any linear subspace $S \subseteq \mathbb{F}^n$, dimension $d \in \{d_0, d_1\}$,*

$$\Pr[S(x) = \hat{S}(x) \forall x \in \mathbb{F}^n : \hat{S} \leftarrow \mathsf{shO}(S)] \geq 1 - \mathsf{negl}(n)$$

  where $S(x)$ is the circuit that decides membership in S.

- ***Security:*** *Let b be a uniformly random bit and let $n \in \mathbb{N}$. Consider the following game between an adversary, and a challenger:*
  - *The adversary sends the challenger a subspace S_0 with dimension d_0.*
  - *The challenger chooses a random subspace $S_1 \subseteq \mathbb{F}_2^n$ of dimension d_1 such that $S_0 \subseteq S_1$. The challenger runs $\mathsf{shO}(S_b) \to \hat{S}$ and sends $\hat{S}$ to the adversary.*
  - *The adversary outputs a guess b'.*

  For all QPT adversaries, it holds that

$$|\Pr[b' = b] - \frac{1}{2}| \leq \mathsf{negl}(n)$$

3.2 Classical Information

Definition 3.3 (Min Entropy)**.** *Let P be a classical finite probability distribution. Let $p_{max} = \max_i p_i$. Then the min-entropy of P is defined as*

$$H_{\min}(P) = \frac{1}{\log p_{\max}}. \tag{6}$$

3.3 Quantum Information

We will assume the reader has familiarity with basic concepts from quantum information, such as pure and mixed states, quantum registers, measurements, entanglement, and quantum channels. We refer the reader to [NC10] for more information on these topics.

Let $\mathcal{X}$ be a Hilbert space. We will use $D(\mathcal{X})$ to describe the space of density operators on the Hilbert space $\mathcal{X}$. When we say a joint quantum system is on registers AB, we mean that the quantum system is defined on the tensor product of their respective Hilbert spaces, $\mathcal{A} \otimes \mathcal{B}$. Let $\mathbb{I}$ be the identity operator. For $\rho_{AB} \in D(\mathcal{A} \otimes \mathcal{B})$, we define the reduced density operator on system A as $\rho_A = \mathsf{Tr}_B(\rho_{AB})$ where Tr_B is the partial trace on system B. Formally, for some orthonormal basis $\{|i\rangle_B\}$,

$$\mathsf{Tr}_B(\rho_{AB}) = \sum_i \mathbb{I}_A \otimes \langle i|_B \, \rho_{AB} \mathbb{I}_A \otimes |i\rangle_B \tag{7}$$

At times we will also make use of specific types of states known as classical-quantum (cq) states. These are states with a a density operator ρ_{AB} of the form

$$\rho_{AB} = \sum_i p_i \, |i\rangle \langle i|_A \otimes \rho_B^i \tag{8}$$

for some orthonormal basis $\{|i\rangle_A\}$ and where $\rho_B^i \in D(\mathcal{B})$.

Computational Model Throughout this paper we consider the quantum circuit model of computation. A *quantum algorithm* is an infinite family $\mathsf{C} = \{\mathsf{C}_m\}_{m\in\mathbb{N}}$ of quantum circuits over some universal gate set, indexed by the input size m. If there exists a polynomial p such that C is a size-p quantum circuit family, then we say that C is an *efficient* quantum algorithm (or a quantum polynomial-time algorithm, or a QPT).

Next, we provide the Quantum Goldreich Levin theorem, proven by [CLLZ21].

Theorem 3.4 (Quantum Goldreich Levin, with Quantum Auxilliary Input (Lemma B.12, [CLLZ21]))**.**

Let A be a quantum algorithm that takes input a random string r and an auxilliary quantum state $|\psi_x\rangle$ and computes $\langle x, r\rangle$. If A computes $\langle x, r\rangle$ with probability at least $\frac{1}{2} + \epsilon$ (where the probability is taken over the choice of x and r) then there exists a quantum algorithm that takes input $|\psi_x\rangle$ and computes x with probability $4 \cdot \epsilon^2$.

We will also make use of the definition of quantum conditional min-entropy, as defined by [Ren08].

Definition 3.5 (Quantum Conditional Min-Entropy)**.** *Let $\rho_{AB} \in \mathcal{D}(\mathcal{A} \otimes \mathcal{B})$ be a bipartite state. The quantum conditional min-entropy of system A conditioned on system B is defined as:*

$$H_{\min}(A|B)_\rho = \sup_{\sigma_B} \max\left\{\lambda \in \mathbb{R} : 2^{-\lambda} I_A \otimes \sigma_B \geq \rho_{AB}\right\} \tag{9}$$

Note that if ρ_{AB} is a cq-state, then the quantum conditional min-entropy reduces to

$$H_{\min}(A|B) = -\log P_{guess}(A|B) \tag{10}$$

where $P_{guess}(X|B) = \max_{\{M_x\}} \sum_x P_X(x)\mathsf{Tr}(M_x \rho_B^x)$ where the max *is taken over all valid POVMs $\{M_x\}$ on system B.*

4 Monogamy Properties of Coset States

Here we formally define the extended monogamy of entanglement (MoE) property of coset states. As mentioned earlier, this security game was first introduced in [CLLZ21] but first formally defined in [ABH+25]. The reduction from the MoE property of coset states to Theorem 4.2 was shown in Lemma C.16 of [CLLZ21]. Since this reduction incurs no loss, we elect to use the precise upper bound on the adversarial success probability shown by [CV22] for the same game.

Theorem 4.1 (Theorem 2.1 [CV22])**.** *Let $n \geq 1$ be an even integer. Let $(\mathcal{A}_0, \mathcal{A}_1, \mathcal{A}_2)$ be parties playing the Monogamy of Entanglement game described in Section 2.1. Then,*

$$\Pr[(\mathcal{A}_0, \mathcal{A}_1, \mathcal{A}_2) \text{ succeed}] \leq \sqrt{e}\left(\cos\frac{\pi}{8}\right)^n \tag{11}$$

Theorem 4.2 (Extended MoE Property of Coset States (Corollary 4.6 [ABH+25]))**.** *Consider the following experiment $\mathsf{Exp}^{\mathsf{ex\text{-}MoE}}_{\mathcal{A}_{\mathsf{MoE}}}$ between a challenger and an adversary tuple, $\mathcal{A}_{\mathsf{MoE}} = (\mathcal{A}, \mathcal{B}, \mathcal{C})$.*

1. *The challenger samples uniformly at random the following three subspaces: a subspace $A \subseteq \mathbb{F}_2^n$ where the dimension of A is $\frac{n}{2}$, a subspace B such that $A \subseteq B$ where the dimension of B is $\frac{3n}{4}$, and a subspace $C \subseteq A$ such that the dimension of C is $\frac{n}{4}$.*

2. *The challenger chooses the following elements uniformly at random:* $(s,t) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$ *and* $(v,w) \in B \times C^\perp$. *The challenger sends the state* $|A_{s,t}\rangle$, *the descriptions of* B, C, *and vectors* $(s+v, t+w)$ *to* $\mathcal{A}$.

3. $\mathcal{A}$*outputs two arbitrary registers* R_1 *and* R_2. *Then* $\mathcal{A}$ *sends* R_1 *to* $\mathcal{B}$ *and sends* R_2 *to* $\mathcal{C}$ *respectively.*

4. *The challenger sends the description of* A *to* $\mathcal{B}$ *and* $\mathcal{C}$.

5. $\mathcal{B}$ *and* $\mathcal{C}$ *outputs guesses* $(s_\mathcal{B}, t_\mathcal{B})$ *and* $(s_\mathcal{C}, t_\mathcal{C})$ *respectively.*

The challenger outputs 1 if $(s_\mathcal{B}, t_\mathcal{B}) \in (A+s)\times(A^\perp+t)$ *and* $(s_\mathcal{C}, t_\mathcal{C}) \in (A+s)\times(A^\perp+t)$ *respectively and* 0 *otherwise.*

Then for any quantum adversary, $\mathcal{A}_{MoE} = (\mathcal{A}, \mathcal{B}, \mathcal{C})$ *and sufficiently large* n,

$$\Pr[\mathsf{Exp}^{\mathsf{ex\text{-}MoE}}_{\mathcal{A}_{\mathsf{MoE}}} = 1] \leq 2^{-0.114n}.$$

Remark 4.3. *Note that the bound defined in Theorem 4.1 is slightly different than the bound we use. This follows simply from writing the bound in base* 2. *Specifically, we use the fact that*

$$\sqrt{e}\left(\cos\frac{\pi}{8}\right)^n = 2^{\log_2\sqrt{e}} \cdot 2^{\left(n\log_2\cos\frac{\pi}{8}\right)} \tag{12}$$

$$\leq 2^{0.721-0.1142n} \tag{13}$$

$$\leq 2^{-0.114n} \tag{14}$$

for sufficiently large n.

Next, we formally define the extended MoE property of coset states under unbounded LOCC leakage. This is exactly the original security game for the extended MoE property of coset states (Theorem 4.2) except in the presence of unbounded LOCC leakage.

In this theorem, we show that the extended MoE property of coset states under unbounded LOCC leakage is implied by the extended MoE property of coset states. This proof follows similarly that of [ÇGLZR24] in the standard (not extended) MoE setting.

Theorem 4.4 (Extended MoE Property of Coset States under Unbounded LOCC Leakage)**.**

Consider the following experiment $\mathsf{Exp}^{\mathsf{ex\text{-}LOCC}}_{\mathcal{A}_{\mathsf{LOCC}}}$ *between a challenger and an LOCC leakage adversary,* $\mathcal{A}_{\mathsf{LOCC}} = (\mathcal{A}_{Main}, \mathcal{A}_{Leak})$.

1. *The challenger samples uniformly at random the following three subspaces: a subspace* $A \subseteq \mathbb{F}_2^n$ *where the dimension of* A *is* $\frac{n}{2}$, *a subspace* B *such that* $A \subseteq B$ *where the dimension of* B *is* $\frac{3n}{4}$, *and a subspace* $C \subseteq A$ *such that the dimension of* C *is* $\frac{n}{4}$.

2. *The challenger chooses the following elements uniformly at random:* $(s,t) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$ *and* $(v,w) \in B \times C^\perp$. *The challenger sends the state* $|A_{s,t}\rangle$ *to* $\mathcal{A}_{Leak}$.

3. $\mathcal{A}_{Main}$ *and* $\mathcal{A}_{Leak}$ *execute their LOCC protocol that leaks* λn *qubits of the state* $|A_{s,t}\rangle$.

4. *After the protocol is completed, the challenger sends the description of* A, *the description of* B *and* C, *and the elements* $(s+v)$ *and* $(t+w)$ *to* $\mathcal{A}_{Main}$.

5. $\mathcal{A}_{Main}$ *outputs* v_0 *and* v_1.

6. *If* $v_0 \in A+s$ *and if* $v_1 \in A^\perp + t$, *the challenger outputs 1. Otherwise, the challenger outputs* 0.

Then for any quantum leakage adversary, $\mathcal{A}_{\mathsf{LOCC}} = (\mathcal{A}_{Main}, \mathcal{A}_{Leak})$, sufficiently large n,

$$\Pr[\mathsf{Exp}^{\mathsf{ex\text{-}LOCC}}_{\mathcal{A}_{\mathsf{LOCC}}} = 1] \leq 2^{-0.057n}.$$

Proof. Assume towards contradiction that there exists a $g(n)$-round quantum leakage adversary $\mathcal{A}_{\mathsf{LOCC}} = (\mathcal{A}_{main}, \mathcal{A}_{Leak})$ such that $\Pr[\mathsf{Exp}^{\mathsf{ex\text{-}LOCC}}_{\mathcal{A}_{\mathsf{LOCC}}}(n)] > 2^{-0.057n}$. Assume without loss of generality the messages sent by either party are the same length and denote this length $k(n)$. Our goal is to construct an adversary $\mathcal{A}_{\mathsf{MoE}} = (\mathcal{A}, \mathcal{B}, \mathsf{C})$ that succeeds in $\mathsf{Exp}^{\mathsf{ex\text{-}MoE}}_{\mathcal{A}_{\mathsf{MoE}}}$ as defined in Theorem 4.2 with probability strictly greater than $2^{-0.114n}$.

Let $\mathcal{P}$ be the random variable containing the transcript of the LOCC protocol of $\mathcal{A}_{Main}$ and $\mathcal{A}_{Leak}$ in $\mathsf{Exp}^{\mathsf{ex\text{-}LOCC}}_{\mathcal{A}_{\mathsf{LOCC}}}(\lambda)$ and let $\rho_{g(n)}$ be the state of $\mathcal{A}_{Main}$ in the final round of the LOCC protocol conditioned on the transcript $\mathcal{P} = m$ where $m = \{\ell_i\}_{[g(n)]}$ is defined to be the set of messages in the LOCC protocol.

Consider steps 1 and 2 of the game $\Pr[\mathsf{Exp}^{\mathsf{ex\text{-}LOCC}}_{\mathcal{A}_{\mathsf{LOCC}}}(\lambda)]$ in which the challenger generates all subspaces and vectors, $(A, B, C, (s, t), (v, w))$. Define the deterministic function f as $f(r) = A$ where r is the randomness that fixes the samples $(A, B, C, (s, t), (v, w))$. Similarly define a deterministic predicate V as the function that outputs 1 if and only if the vectors output by $\mathcal{A}_{Main}$, (v_0, v_1), are in the correct cosets. Then the winning probability of $\mathcal{A}_{\mathsf{LOCC}}$ is

$$\mathbb{E}_{(r,(\ell,m))\leftarrow(R,\mathcal{P})}\big[\Pr[V(\mathcal{A}_{Main}(\rho_{g(n)}, f(r)), r) = 1]\big] \tag{15}$$

If we are given two copies of $\rho_{g(n)}$ for the same coset state as well as the transcript $\{\ell_i\}_{[g(n)-1]}$ and we ran the last step of $\mathcal{A}_{Main}$ twice independently, we would obtain the probability of $\mathcal{A}$ winning on both copies simultaneously:

$$\mathbb{E}_{(r,(\ell,m))\leftarrow(R,\mathcal{P})}\big[\Pr[V(\mathcal{A}_{Main}(\rho_{g(n)}, f(r)), r) = 1]^2\big].$$

Then, since the probability of winning in one instance is strictly greater than $2^{-0.057n}$, the probability $\mathcal{A}$ wins after running $\mathcal{A}_{Main}$ in two independent and simultaneous instances is strictly greater $2^{-2(0.057)n}$ by Jensen's inequality.

Now we construct an adversary $\mathcal{A}_{\mathsf{MoE}} = (\mathcal{A}, \mathcal{B}, \mathcal{C})$ for $\mathsf{Exp}^{\mathsf{ex\text{-}MoE}}_{\mathcal{A}_{\mathsf{MoE}}}(\lambda)$ such that when $\mathcal{A}$ is given $(|A_{s,t}\rangle, B, C, (s+v), (t+w))$ and $\mathcal{B}$ and $\mathcal{C}$ are additionally given A,it produces two copies of $\rho_{g(n)-1}$ with probability at least $1/2$.

$\mathcal{A}_{\mathsf{MoE}}$ postselects on the transcript, $\mathcal{P}$, and repeatedly runs the LOCC protocol of $\mathcal{A}_{Main}$ and $\mathcal{A}_{Leak}$ until $\mathcal{A}_{Main}$ outputs another copy of $\rho_{g(n)}$. While this may require exponential runs of $\mathcal{A}_{Main}$, since $\mathcal{A}_{\mathsf{MoE}}$ is unbounded, $\mathcal{A}_{\mathsf{MoE}}$ will be successful. Then the reduction proceeds as follows: $\mathcal{A}_{\mathsf{MoE}}$, given two copies $\rho^{\otimes 2}_{g(n)}$ sends one copy to $\mathcal{B}$ and the other copy to $\mathcal{C}$. $\mathcal{B}$ and $\mathcal{C}$ simulate the actions of $\mathcal{A}_{Main}$ and then output guesses $\tilde{s}_1, \tilde{t}_1$ and $\tilde{s}_2, \tilde{t}_2$ respectively. By the argument above, $\tilde{s}_1, \tilde{t}_1$ and $\tilde{s}_2, \tilde{t}_2$ are accepted with probability at least $2^{-2(0.057)n}$. This yields a contradiction to Theorem 4.2. □

5 Quantum Leakage Security

In this section we generalize the previous leakage security games to also allow for bounded quantum leakage. First, we define the extended version of the quantum leakage security game. It follows exactly that of the LOCC version Theorem 4.4, except, in addition to unbounded LOCC leakage, the leakage is also allowed to be a quantum state of bounded length. We now argue that the extended MoE property of coset states under unbounded LOCC leakage implies the same property of coset states under unbounded LOCC leakage *and* bounded quantum leakage.

That is, if there exists a quantum leakage adversary $\mathcal{A}_{\mathsf{Quant}} = (\mathcal{A}_{Main}, \mathcal{A}_{Leak})$ that succeeds in the experiment, $\mathsf{Exp}^{\mathsf{ex\text{-}Quant}}_{\mathcal{A}_{\mathsf{Quant}}}(n, \lambda)$, with probability greater than $2^{-0.057\lambda}$ for a constant λ (where $\lambda < 0.057$), then there also exists an LOCC leakage adversary $\hat{\mathcal{A}}_{\mathsf{LOCC}} = (\hat{\mathcal{A}}_{Main}, \hat{\mathcal{A}}_{Leak})$ that succeeds at $\mathsf{Exp}^{\mathsf{ex\text{-}LOCC}}_{\hat{\mathcal{A}}_{\mathsf{LOCC}}}(\lambda)$ with the same probability. We will utilize a corollary of the following lemma concerning partial measurements proven in the paper of Boneh and Zhandry [BZ13].

Lemma 5.1 (Lemma 2.1, [BZ13])**.** *Let Q be a quantum algorithm and let p_x be the probability that Q outputs x. Let Q' be another quantum algorithm obtained from Q by pausing Q at an arbitrary point of execution. Q' then performs a partial measurement obtaining one of k outcomes and then resumes Q. Let p'_x be the probability that Q' outputs x. It holds that $p'_x \geq p_x/k$.*

Here we provide a simple extension of the above lemma to account for a constant number of partial measurements, instead of a single partial measurement.

Corollary 5.2. *Let $q > 0$. Let Q be a quantum algorithm and let p_x be the probability that Q outputs x. Let Q' be another quantum algorithm obtained from Q that perform q partial measurements at arbitrary stages of execution. If these measurements have $(k_1, k_2, \ldots, k_q)$ possible outcomes, respectively, then the probability that Q' outputs x is denoted by p'_x and bounded by $p'_x \geq p_x/(k_1 * k_2 * \cdots * k_q)$.*

Proof. The corollary follows from a simple inductive argument. The base case is a single measurement, and follows from the above lemma.

- **Inductive Hypothesis:** Let Q_m be the algorithm obtained from Q that performs m many partial measurements where each measurement has $k_1, \ldots, k_m$ many possible outcomes respectively. Let $p_{m,x}$ be the probability that Q_m outputs x. We assume $p_{m,x} \geq p_x/(k_1 * k_2 * \cdots * k_m)$.
- **Inductive Step:** We now argue the claim for $m+1$ measurements. Let Q_{m+1} be exactly Q_m except it performs one additional partial measurement that has k_{m+1} possible outcomes. We can then use Lemma 5.1 to bound the probability Q_{m+1} outputs x,

$$p_{m+1,x} \geq \frac{p_{m,x}}{k_{m+1}}.$$

Given our inductive hypothesis, we obtain

$$p_{m,x} \geq \frac{p_x}{(k_1 \cdot k_2 \cdot, \ldots, \cdot k_{m+1})}$$

which completes the proof.

□

Theorem 5.3 (Extended MoE property of Coset States under Bounded Quantum Leakage λ)**.** *Let $n \in \mathbb{N}$ and let λ be the leakage rate. Consider the following experiment $\mathsf{Exp}^{\mathsf{ex\text{-}Quant}}_{\mathcal{A}_{\mathsf{Quant}}}(n, \lambda)$ between a challenger and an adversary tuple, $\mathcal{A}_{\mathsf{Quant}} = (\mathcal{A}_{Main}, \mathcal{A}_{Leak})$.*

1. *The challenger samples uniformly at random the following three subspaces: a subspace $A \subseteq \mathbb{F}_2^n$ where the dimension of A is $\frac{n}{2}$, a subspace B such that $A \subseteq B$ where the dimension of B is $\frac{3n}{4}$, and a subspace $C \subseteq A$ such that the dimension of C is $\frac{n}{4}$.*
2. *The challenger chooses the following elements uniformly at random: $(s, t) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$ and $(v, w) \in B \times C^{\perp}$. The challenger sends the state $|A_{s,t}\rangle$ to $\mathcal{A}_{Leak}$. We denote this setup stage as $\mathsf{CosetGen}(1^\lambda) \to (A, B, C, (s, t), (v, w))$.*

3. *$\mathcal{A}_{Main}$ and $\mathcal{A}_{Leak}$ execute their protocol which includes sending at most λn qubits (but have no restrictions on the amount of classical communication).*

4. *After the protocol is completed, the challenger sends the description of A, the description of B and C, and the elements $(s+v)$ and $(t+w)$ to $\mathcal{A}_{Main}$.*

5. *$\mathcal{A}_{Main}$ outputs v_0 and v_1.*

6. *If $v_0 \in A+s$ and if $v_1 \in A^{\perp}+t$, the challenger outputs 1. Otherwise, the challenger outputs 0.*

For all $\lambda < 0.057$, any quantum adversary, $\mathcal{A} = (\mathcal{A}_{Main}, \mathcal{A}_{Leak})$, and sufficiently large n,

$$\Pr[\mathsf{Exp}^{\mathsf{ex\text{-}Quant}}_{\mathcal{A}_{\mathsf{Quant}}}(n,\lambda)=1] \leq 2^{-(0.057-\lambda)n}.$$

Proof. Assume for all $\lambda < 0.057$, $\mathcal{A}_{\mathsf{Quant}} = (\mathcal{A}_{Main}, \mathcal{A}_{Leak})$ that succeeds in $\mathsf{Exp}^{\mathsf{ex\text{-}Quant}}_{\mathcal{A}_{\mathsf{Quant}}}(\lambda, q)$ with probability greater than $2^{-(0.057-\lambda)n}$. We construct an LOCC leakage adversary $\hat{\mathcal{A}}_{\mathsf{LOCC}} = (\hat{\mathcal{A}}_{main}, \hat{\mathcal{A}}_{leak})$ that succeeds in $\mathsf{Exp}^{\mathsf{ex\text{-}LOCC}}_{\hat{\mathcal{A}}_{\mathsf{LOCC}}}(\lambda)$ as follows.

1. The challenger samples $(A, B, C, (s,t), (v,w)) \leftarrow \mathsf{CosetGen}(1^{\lambda})$.

2. The challenger sends $|A_{s,t}\rangle$ to $\hat{\mathcal{A}}_{leak}$.

3. $\hat{\mathcal{A}}_{Main}$ and $\hat{\mathcal{A}}_{Leak}$ simulate the protocol of $\mathcal{A}_{\mathsf{Quant}}$ on $|A_{s,t}\rangle$. $\hat{\mathcal{A}}_{Main}$ runs the local operations of $\mathcal{A}_{Main}$ while $\hat{\mathcal{A}}_{Leak}$ runs the local operations of $\mathcal{A}_{Leak}$. Recall that $\mathcal{A}_{\mathsf{Quant}}$ is guaranteed to only leak at most λn qubits. For each instance in which $\mathcal{A}_{\mathsf{Quant}}$ (or $\mathcal{A}_{Leak}$ respectively) sends a state, $\hat{\mathcal{A}}_{Main}$ (and respectively $\hat{\mathcal{A}}_{Leak}$) measures the states according to the measurements guaranteed by Corollary 5.2. $\hat{\mathcal{A}}_{main}$ sends the measurement outcomes instead of sending the quantum state.

4. The challenger sends descriptions of A, B, and C to $\hat{\mathcal{A}}_{Main}$. $\hat{\mathcal{A}}_{Main}$ runs $\mathcal{A}_{Main}$ and outputs values $\tilde{v}_0, \tilde{v}_1$ that $\mathcal{A}_{Main}$ outputs.

Recall by assumption, $\mathcal{A}_{Quant}$ succeeds with probability greater than $2^{-(0.057-\lambda)n}$. Since $\hat{\mathcal{A}}_{LOCC}$ simulates $\mathcal{A}_{Quant}$, the fact that $\lambda < 0.057$, and by the success probability of the measurements guaranteed by Corollary 5.2, it follows that the success probability of $\mathcal{A}_{LOCC}$ is

$$\Pr[\mathsf{Exp}^{\mathsf{ex\text{-}LOCC}}_{\hat{\mathcal{A}}_{\mathsf{LOCC}}}(n)=1] \geq \frac{\Pr[\mathsf{Exp}^{\mathsf{ex\text{-}Quant}}_{\mathcal{A}_{\mathsf{Quant}}}(n,\lambda)=1]}{2^{\lambda n}} \tag{16}$$

$$> \frac{1}{2^{\lambda n}} \cdot \frac{1}{2^{(0.057-\lambda)n}} \tag{17}$$

$$= \frac{1}{2^{0.057n}} \tag{18}$$

which contradicts Theorem 4.4. □

Next we argue the hardness of the computational version of the quantum leakage security, Computation $\mathsf{Coset\text{-}Quantum}$. Using similar methods to [CLLZ21], we show that the hardness of the information theoretic version implies the security of the computational version. We will also need to use subspace hiding obfuscation, as defined in Definition 3.2. Note that we will be using a slight variant of the game described in [CLLZ21] in which the vectors s and t used to ultimately define the coset state $|A_{s,t}\rangle$ are sampled from $\mathsf{CS}(A)$ and $\mathsf{CS}(A^{\perp})$ respectively. However, this version

of the game is equivalent to the original version in which s and t are sampled randomly from the vector space. This is because given the outputs of the MoE game, $u \in A + s$ and $v \in A^\perp + t$, if $s \in \mathsf{CS}(A)$ and $t \in \mathsf{CS}(A^\perp)$ then one can always compute $\mathsf{Can}_A(u) = s$ and $\mathsf{Can}_{A^\perp}(v) = t$ at no loss to the overall success probability of the adversaries.

Theorem 5.4 (Computational MoE Property of Coset States under Bounded Quantum Leakage)**.** *Let $n \in \mathbb{N}$. Let iO be an $i\mathcal{O}$. Consider the following experiment $\mathsf{Exp}^{\mathsf{Comp}}_{\mathcal{A}_{\mathsf{Quant}}}(n, \lambda)$ between a QPT challenger and a QPT leakage adversary, $\mathcal{A}_{\mathsf{Quant}} = (\mathcal{A}_{Main}, \mathcal{A}_{Leak})$.*

1. *The challenger uniformly at random samples a subspace $A \subseteq \mathbb{F}_2^n$ of dimension $\frac{n}{2}$ and two elements $s, t \in \mathsf{CS}(A) \times \mathsf{CS}(A^\perp)$.*
2. *The challenger samples two programs, $V_0 \leftarrow iO(A + s)$ and $V_1 \leftarrow iO(A^\perp + t)$.*
3. *The challenger sends $|A_{s,t}\rangle$ to $\mathcal{A}_{Leak}$.*
4. *$\mathcal{A}_{Main}$ and $\mathcal{A}_{Leak}$ execute their protocol in which they exchange at most $\lambda \cdot n$ bits of quantum leakage (but have no restrictions on the amount classical communication).*
5. *After their protocol is completed, the challenger sends A and (V_0, V_1) to $\mathcal{A}_{Main}$.*
6. *$\mathcal{A}_{Main}$ outputs (u, v)*
7. *The challenger checks if $u \in A + s$ and if $v \in A^\perp + t$. Output 1 if yes, otherwise output 0.*

Assuming the existence of $i\mathcal{O}$ and OWFs, for any sufficiently large n, any QPT leakage adversary $\mathcal{A}_{\mathsf{Quant}} = (\mathcal{A}_{Main}, \mathcal{A}_{Leak})$, and any constant fraction $0 \leq \lambda < 0.057$,

$$\Pr[\mathsf{Exp}^{\mathsf{Comp}}_{\hat{\mathcal{A}}_{\mathsf{Quant}}}(n, \lambda) = 1] \leq \mathsf{negl}(n).$$

Proof. We prove the above theorem via reduction from the information theoretic version of the same experiment, $\mathsf{Exp}^{\mathsf{Quant}}_{\mathcal{A}_{\mathsf{Quant}}}(\lambda, q)$. Our proof follows a similar structure to that of [CLLZ21]. We do this via the following set of hybrids:

- $\mathcal{H}_0$: This is the original experiment, $\mathsf{Exp}^{\mathsf{Comp}}_{\mathcal{A}_{\mathsf{Comp}}}(n, \lambda) = 1$.
- $\mathcal{H}_1$: This is the same as $\mathcal{H}_0$ except instead of computing $V_0 \leftarrow iO(A+s)$ and $V_1 \leftarrow iO(A^\perp+t)$, we compute $\tilde{V}_0 \leftarrow iO(\mathsf{shO}(A)(\cdot - s))$ and $\tilde{V}_1 \leftarrow iO(\mathsf{shO}(A^\perp)(\cdot - t))$ and forward $\tilde{V}_0$ and $\tilde{V}_1$ to the $\mathcal{A}_{Main}$ instead. Here $\mathsf{shO}(A)(\cdot - s)$ is defined as the algorithm that takes input an element $x \in \mathbb{F}^n$, subtracts s and then checks if the resulting element is in A. It follows by the correctness of shO that $\mathsf{shO}(A)(\cdot - s)$ is functionally equivalent to checking membership in the space $A + s$. An analagous argument holds to argue that $\mathsf{shO}(A^\perp)(\cdot - t)$ and checking membership in the space $A^\perp + t$ are functionally equivalent. Therefore, by the security of iO,
$$|\Pr[\mathcal{H}_0 = 1] - \Pr[\mathcal{H}_1 = 1]| \leq \mathsf{negl}(n).$$
- $\mathcal{H}_2$: This is the same as $\mathcal{H}_1$ except we replace $iO(\mathsf{shO}(A)(\cdot - s))$ with $iO(\mathsf{shO}(B)(\cdot - s))$ where $B \subseteq \mathbb{F}_2^q$ where B is a subspace chosen uniformly at random of dimension $\frac{3q}{4}$ and $A \subseteq B$. Additionally, we replace $iO(\mathsf{shO}(A^\perp)(\cdot - t))$ with $iO(\mathsf{shO}(C^\perp)(\cdot - t))$ where C is a subspace chosen uniformly at random of dimension $\frac{n}{4}$ where $C \subseteq A$. By the security of shO
$$|\Pr[\mathcal{H}_1 = 1] - \Pr[\mathcal{H}_2 = 1]| \leq \mathsf{negl}(n)$$

- $\mathcal{H}_3$: This is the same as $\mathcal{H}_2$ except we replace $iO(\mathsf{shO}(B)(\cdot - s))$ with $iO(\mathsf{shO}(B)(\cdot - (s+v)))$ for a uniformly random element $v \in B$. By the correctness of shO, $\mathsf{shO}(B)(\cdot - s)$ and $\mathsf{shO}(B)(\cdot - (s+v)))$ are functionally equivalent with high probability. Therefore, by the security of iO,
$$|\Pr[\mathcal{H}_2 = 1] - \Pr[\mathcal{H}_3 = 1]| \leq \mathsf{negl}(n)$$

- $\mathcal{H}_4$: This is the same as $\mathcal{H}_3$ except we replace $iO(\mathsf{shO}(C^\perp)(\cdot - t))$ with $iO(\mathsf{shO}(C^\perp)(\cdot - (t+w)))$ for a uniformly random element $w \in C^\perp$. By the correctness of shO, $\mathsf{shO}(C^\perp)(\cdot - t)$ and $\mathsf{shO}(B)(\cdot - (t+w)))$ are functionally equivalent with high probability. Therefore, by the security of iO,
$$|\Pr[\mathcal{H}_3 = 1] - \Pr[\mathcal{H}_4 = 1]| \leq \mathsf{negl}(n)$$

- $\mathcal{H}_5$: The same as $\mathcal{H}_4$ except we send the adversary, $\mathcal{A}_{Main}$, $(B, C, s+v, t+w)$ in the clear. Then, since given $(B, C, s+v, t+w)$ we can directly construct $iO(\mathsf{shO}(B)(\cdot - (s+v)))$ and $iO(\mathsf{shO}(C^\perp)(\cdot - (t+w)))$, it holds that
$$\Pr[\mathcal{H}_4 = 1] \leq \Pr[\mathcal{H}_5 = 1].$$

Finally, we argue that
$$Pr[H_5 = 1] \leq \mathsf{negl}(n).$$
Notice that $\mathcal{H}_5$ is exactly the same as $\mathsf{Exp}^{\mathsf{Quant}}_{\mathcal{A}_{\mathsf{Quant}}}(n, \lambda)$. Applying Theorem 5.3, we get that
$$Pr[H_5 = 1] \leq \mathsf{Exp}^{\mathsf{Quant}}_{\mathcal{A}_{\mathsf{Quant}}}(n, \lambda) \leq 2^{-O(n)} = \mathsf{negl}(n)$$
Combing the above, we get that for any QPT leakage adversary $\mathcal{A}_{Comp} = (\mathcal{A}_{Main}, \mathcal{A}_{Leak})$,
$$\Pr[\mathsf{Exp}^{\mathsf{Comp}}_{\mathcal{A}_{\mathsf{Comp}}}(n, \lambda) = 1] \leq \sum_{i=1}^{4} |\Pr[H_i = 1] - \Pr[H_{i+1} = 1]| \leq \mathsf{negl}(n).$$

□

6 Leakage Resillient PKE Construction

6.1 Construction

Here we describe the construction of the PKE scheme, $\mathsf{PKE} = \mathsf{PKE}.(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ for ℓ_{msg} bit messages where $\ell_{msg} = \ell(n)$ is a polynomial. Let iO be an iO. The construction follows that of [KY25] with some modifications.

- $\mathsf{PKE.KeyGen}(1^n)$:
  - Generate uniformly random subspace $A \subseteq \mathbb{F}_2^n$ of dimension $\frac{n}{2}$ and sample two vectors $s, t \in \mathsf{CS}(A) \times \mathsf{CS}(A^\perp)$.
  - Output $|\mathsf{sk}\rangle := |A_{s,t}\rangle$ and $\mathsf{pk} = (C_{mc}, C^\perp_{mc})$ where $C_{mc} = iO(A+s)$ and $C^\perp_{mc} = iO(A^\perp + t)$.
- $\mathsf{PKE.Enc}(\mathsf{pk}, m)$:
  - Parse $\mathsf{pk} = (C_{mc}, C^\perp_{mc})$.
  - parse m as $\mathrm{m} = m_1 || m_2 \in \{0,1\}^{\ell_{msg}} \times \{0,1\}^{\ell_{msg}}$.

– Generate two obfuscated circuits $\tilde{P} \leftarrow iO(P[C_{mc}, m_1])$ and $\tilde{P}^{\perp} \leftarrow iO(P[C^{\perp}_{mc}, m_2])$ as described in Algorithm 3. Output $\mathsf{ct} := (\tilde{P}, \tilde{P}^{\perp})$.

- $\mathsf{PKE.Dec}(|\mathsf{sk}\rangle, \mathsf{ct})$:
  - Parse $\mathsf{ct} = (\tilde{P}, \tilde{P}^{\perp})$.
  - Let D and $D^{\perp}$ be unitaries that work as

$$D|u\rangle|v\rangle \mapsto |u\rangle|v \oplus \tilde{P}(u)\rangle \text{ and } D^{\perp}|u\rangle|v\rangle \mapsto |u\rangle|v \oplus \tilde{P}^{\perp}(u)\rangle$$

    for any $u \in \{0,1\}^{\ell_{msg}}$ and $v \in \{0,1\}^{\ell_{msg}}$.
  - Apply D to $|\mathsf{sk}\rangle \otimes |0^{\ell_{msg}}\rangle$ and measure the second register to obtain the outcome m'_1
  - Apply $D^{\perp}$ to $|\mathsf{sk}\rangle \otimes |0^{\ell_{msg}}\rangle$ and measure the second register to obtain the outcome m'_2
  - Output $m' = m'_1||m'_2$.

Algorithm 3 Program $P[C, \mathsf{str}](x)$

Hardwired Constant:A description of a circuit C with 1-bit output and a ℓ_{msg}-bit string str.
Input: $x \in \{0,1\}^{\ell_{msg}}$.
if $C(x) = 1$ **then**:
  Output str
else:
  Output $0^{\ell_{msg}}$
end if

6.2 Correctness

Fix $m = m_1||m_2$ where $m_1, m_2 \in \{0,1\}^{\ell_{msg}} \times \{0,1\}^{\ell_{msg}}$. Suppose $\mathsf{pk} = (C_{mc} = iO(A + s), C^{\perp}_{mc} = iO(A^{\perp} + t))$, $|\mathsf{sk}\rangle = |A_{s,t}\rangle$, $\mathsf{ct} = (\tilde{P}, \tilde{P}^{\perp})$ where $\tilde{P} = iO(P[C_{mc}, m_1])$, $\tilde{P}^{\perp} = iO(P[C^{\perp}_{mc}, m_2])$ are generated as specified in the construction of PKE. Let m'_1 and m'_2 be the values computed when executing $\mathsf{PKE.Dec}(|\mathsf{sk}\rangle, \mathsf{ct})$.

We now prove that $m'_1 = m_1$ and $m'_2 = m_2$. For any $u \in A$, we have that $\tilde{P}(u + s) = m_1$ from the functionality of iO. Therefore, given that

$$|\mathsf{sk}\rangle = |A_{s,t}\rangle = \sum_{u \in A} (-1)^{\langle u,t\rangle} |u + s\rangle,$$

applying D to $|\mathsf{sk}\rangle \otimes |0^{\ell_{msg}}\rangle$ yields $|\mathsf{sk}\rangle \otimes |m_1\rangle$. Therefore when we measure the second register we obtain m_1 and tracing out the second register gives us $|\mathsf{sk}\rangle$.

Similarly, for any $v \in A^{\perp}$, $\tilde{P}^{\perp}(v + t) = m_2$ from the functionality of iO. Given that

$$H^{\otimes n}|\mathsf{sk}\rangle = H^{\otimes n}|A_{s,t}\rangle = \sum_{v \in A^{\perp}} (-1)^{\langle v,s\rangle} |v + t\rangle,$$

if we apply the unitary $D^{\perp}$ to $H^{\otimes n}|\mathsf{sk}\rangle \otimes |0^{\ell_{msg}}\rangle$ we get the state $H^{\otimes n}|\mathsf{sk}\rangle \otimes |m_2\rangle$. This implies that $m'_2 = m_2$.

6.3 Proof of Leakage Security

We argue that PKE satisfies one-way security under bounded quantum leakage. We define the security model and argue that the construction of PKE satisfies the definition of security as follows:

Definition 6.1 (One-Way Security of PKE under Bounded Quantum Leakage with Leakage Ratio λ)**.** *Consider the following experiment* $\mathsf{Exp}^{\mathsf{PKE}}_{\mathcal{A}_{\mathsf{Quant}}}(n,\lambda)$ *between a QPT challenger and a QPT quantum leakage adversary* $\mathcal{A}_{\mathsf{Quant}} = (\mathcal{A}_{Main}, \mathcal{A}_{Leak})$ *with security parameter* n *and leakage ratio* λ*. Let* $\mathsf{PKE} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *be a public key encryption scheme with a quantum secret key that encrypts* $\ell = poly(n)$ *bits.*

1. *The challenger runs* $\mathsf{PKE.KeyGen}(1^n) \to (\mathsf{pk}, \rho_{\mathsf{sk}})$
2. *Let* ℓ_{sk} *denote the number of qubits of* ρ_{sk}*.* $(\mathcal{A}_{main}, \mathcal{A}_{Leak})$ *execute their interactive protocol in which they exchange at most* $\lambda \cdot \ell_{\mathsf{sk}}$ *qubits and potentially unbounded classical information.*
3. *After the protocol is over, the challenger samples* $m \leftarrow \{0,1\}^\ell$ *and generates* $\mathsf{ct} \leftarrow \mathsf{PKE.Enc}(\mathsf{pk}, m)$*. The challenger submits* ct *to* $\mathcal{A}_{main}$*.*
4. $\mathcal{A}_{main}$ *outputs a guess* $m' \in \{0,1\}^\ell$
5. *The challenger outputs 1 if and only if* $m' = m$*.*

PKE *satisfies One Way Security under Bounded Quantum Leakage with Leakage Ratio* λ *if for any sufficiently large* $n \in \mathbb{N}$*, QPT leakage adversary* $\mathcal{A}_{\mathsf{Quant}} = (\mathcal{A}_{main}, \mathcal{A}_{Leak})$*,*

$$\Pr[\mathsf{Exp}^{\mathsf{PKE}}_{\mathcal{A}_{\mathsf{Quant}}}(n,\lambda) = 1] \leq \mathsf{negl}(n) \tag{19}$$

Theorem 6.2 (One-Way Security of PKE under Bounded Quantum Leakage with Leakage Ratio λ)**.**

Let PKE *be the PKE construction defined in Section 6.1. Then for any sufficiently large* $n \in \mathbb{N}$*, QPT leakage adversary* $\mathcal{A}_{\mathsf{Quant}} = (\mathcal{A}_{main}, \mathcal{A}_{Leak})$*, and constant* $\lambda < 0.057$*,* PKE *satisfies One Way Security under Bounded Quantum Leakage with Leakage Ratio* λ*.*

Proof. Let $\mathcal{A}_{\mathsf{PKE}} = (\mathcal{A}_{main}, \mathcal{A}_{Leak})$ be a QPT adversary that succeeds with non-negligible probability $p(n,\lambda)$. We argue security via the following hybrids

- Hyb_0: This is the original security experiment, $\mathsf{Exp}^{\mathsf{PKE}}_{\mathcal{A}_{\mathsf{Quant}}}(n,\lambda)$.
- Hyb_1: The same as Hyb_0 except we change the generation of ct as follows. The circuit $\tilde{P}$ is generated as $\tilde{P} \leftarrow iO(P[C_{mc}, m_1 \oplus s])$ and $\tilde{P}^\perp$ is generated as $\tilde{P}^\perp \leftarrow iO(P[C_{mc}, m_2 \oplus t])$ where s and t are hard coded into the circuit. We then set $\mathsf{ct} = (\tilde{P}, \tilde{P}^\perp)$. Then the challenger returns 1 if $m' = m_1 \oplus s || m_2 \oplus t$ and otherwise outputs 0. Since m was sampled uniformly at random, $m_1 \oplus s$ and $m_2 \oplus t$ are distributed uniformly at random as well. Therefore

$$\Pr[\mathsf{Hyb}_0 = 1] = \Pr[\mathsf{Hyb}_0 = 1].$$

- Hyb_2: The same as Hyb_1 except we again change the computation of the ciphertext. We will replace the program P with the program Q as defined in Algorithm 4. The change in this hybrid is follows. The circuit $\tilde{P}$ is generated as $\tilde{P} \leftarrow iO(Q[C_{mc}, A, m_1])$ and the circuit $\tilde{P}^\perp \leftarrow iO(Q[C^\perp_{mc}, A^\perp, m_2](x))$. As in the previous hybrid, the challenger returns 1 if the returned value $m' = m_1 \oplus s || m_2 \oplus t$ and otherwise 0. We now argue that the programs

$P[C_{mc}, \mathsf{str}](x)$ and $Q[C_{mc}, A, \mathsf{str}](x)$ are functionally equivalent. For x such that $C(x) = 0$, or when $x \notin A+s$, both circuits output 0^n. Alternatively, when $C(x) = 1$, or when $x \in A+s$, the two programs also provide functionally equivalent outputs. in this case,

$$\begin{aligned} Q[C_{mc}, A, m_1] &= m_1 \oplus \mathsf{Can}_A(x) && (20)\\ &= m_1 \oplus s && (21)\\ &= P[C_{mc}, m_1 \oplus s](x) && (22) \end{aligned}$$

where the second equation holds because s was sampled from $\mathsf{CS}(A)$. In an analogous way, we can also argue that $P[C^{\perp}_{mc}, m_2 \oplus t]$ and $Q[C^{\perp}_{mc}, A^{\perp}, m_2](x)$ are functionally equivalent. On input $x \in A^{\perp} + t$, both programs will output $m_2 \oplus t$, otherwise they will output 0^n.

Since both programs are functionally equivalent, by the security of iO, it holds that

$$|\Pr[\mathsf{Hyb}_2 = 1] - \Pr[\mathsf{Hyb}_3 = 1]| \leq \mathsf{negl}(n)$$

Algorithm 4 Program $Q[C, A, \mathsf{str}](x)$

Hardwired Constant:A description of a circuit C with 1-bit output, a description of an $\frac{n}{2}$ dimensional subspace A, and a ℓ_{msg}-bit string str.
Input: $x \in \{0,1\}^n$.
if $C(x) = 1$ **then**:
  Compute $s = \mathsf{Can}_A(x)$, output $\mathsf{str} \oplus s$.
else:
  Output $0^{\ell_{msg}}$
end if

Next we argue, by a reduction from Theorem 5.4,

$$\Pr[\mathsf{Hyb}_3 = 1] \leq \mathsf{negl}(n).$$

We will construct a QPT dversary $\hat{\mathcal{A}}_{\mathsf{Quant}} = (\hat{\mathcal{A}}_{Main}, \hat{\mathcal{A}}_{Leak})$ for the experiment $\mathsf{Exp}^{\mathsf{Comp}}_{\mathcal{A}_{\mathsf{Quant}}}(n, \lambda)$, as defined in Theorem 5.4.

1. The challenger first generates a random subspace $A \subseteq \mathbb{F}_2^n$ of dimension $\frac{n}{2}$ and two elements $s, t \in \mathbb{F}_2^n$. Then the challenger samples $A, pk = (C_{mc}, C^{\perp}_{mc})$ where $C_{mc} = iO(A + s)$ and $C^{\perp}_{mc} = iO(A^{\perp} + t)$ and constructs $|\mathsf{sk}\rangle = |A_{s,t}\rangle$.
2. The challenger sends $|\mathsf{sk}\rangle$ to $\hat{\mathcal{A}}_{Leak}$
3. $\hat{\mathcal{A}}_{Main}$ and $\hat{\mathcal{A}}_{Leak}$ run the interactive protocol of $\mathcal{A}_{Main}$ and $\mathcal{A}_{Leak}$ respectively in which they exchange $\lambda \cdot \ell_{sk}$ qubits and potentially unbounded classical information.
4. After the protocol is completed, the challenger sends A, C_{mc}, and $C^{\perp}_{mc}$ to $\hat{\mathcal{A}}_{Main}$. Then, $\hat{\mathcal{A}}_{Main}$ samples random messages $m = (m_1||m_2) \leftarrow \mathcal{M}$ and then generates a ciphertext $\mathsf{PKE.Enc}(\mathsf{pk}, m) \rightarrow \mathsf{ct}$ and invokes $\mathcal{A}_{main}$ on ct. Recall that here $\mathsf{ct} = (\tilde{P}, \tilde{P}^{\perp})$ as defined in Hyb_3.
5. $\hat{\mathcal{A}}_{Main}$ decrypts ct and outputs messages $\tilde{m}_1||\tilde{m}_2$. $\mathcal{A}_{Main}$ outputs a guess $(m_1 \oplus \tilde{m}_1, m_2 \oplus \tilde{m}_2) = (s, t)$.

Recall $\mathcal{A}_{\mathsf{Quant}}$ is a successful adversary for the experiment, $\mathsf{Exp}^{\mathsf{PKE}}_{\mathcal{A}_{\mathsf{Quant}}}(n,\lambda)$ with probability $p(n)$. By applying the triangle inequality, we get that

$$|\Pr[\mathsf{Hyb}_0 = 1] - \Pr[\mathsf{Hyb}_3 = 1]| \leq \mathsf{negl}(n).$$

Therefore $\mathcal{A}_{\mathsf{Quant}}$ is also a successful adversary for Hyb_3 and outputs $(m_1 \oplus \tilde{m}_1, m_2 \oplus \tilde{m}_2) = (s,t)$ with probability at least $p(n,\lambda) - \mathsf{negl}(n)$. Then since $\hat{\mathcal{A}}_{\mathsf{Quant}}$ perfectly simulates Hyb_3 for $\mathcal{A}_{\mathsf{Quant}}$,

$$\begin{aligned}\Pr[\mathsf{Exp}^{\mathsf{Comp}}_{\hat{\mathcal{A}}_{\mathsf{Quant}}}(n,\lambda)] = 1] &\geq \Pr[\mathsf{Exp}^{\mathsf{PKE}}_{\mathcal{A}_{\mathsf{Quant}}}(n,\lambda)] = 1] - \mathsf{negl}(n) &(23)\\ &\geq p(n,\lambda) - \mathsf{negl}(n) &(24)\\ &> \mathsf{negl}(n) &(25)\end{aligned}$$

which is a contradiction.

□

6.4 Indistinguishability Security of Leakage Secure PKE

In this section we argue that If a PKE scheme satisfies one-way leakage security (as defined in Definition 6.1), then there exists another public key encryption scheme $\tilde{\mathsf{PKE}}$ that satisfies indistinguishability leakage security, as defined below.

Definition 6.3 (IND Security of PKE under Bounded Quantum Leakage with Leakage Rate λ)**.** *Let $n \in \mathbb{N}$ let λ be the leakage parameter, and let $\mathcal{M} = \{0,1\}$ be the message space. Let $\mathsf{PKE} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$. Consider the following security game, $\mathsf{Exp}^{\mathsf{IND}}_{\mathsf{PKE},\mathcal{A}}(n,\lambda)$ between a challenger and a QPT adversary $\mathcal{A}_{\mathsf{IND}} = (\mathcal{A}_{Leak}, \mathcal{A}_{Main})$.*

1. *The challenger runs $\mathsf{KeyGen}(1^n) \to (\mathsf{pk}, \rho_{\mathsf{sk}})$ and sends $(\mathsf{pk}, \rho_{\mathsf{sk}})$ to $\mathcal{A}_{Leak}$.*
2. *Let ℓ_{sk} be the number of qubits of ρ_{sk}. $\mathcal{A}_{Leak}$ and $\mathcal{A}_{Main}$ run their interactive protocol in which $\mathcal{A}_{Leak}$ sends $\lambda \cdot \ell_{\mathsf{sk}}$ qubits to $\mathcal{A}_{Main}$ and potentially unbounded classical information.*
3. *$\mathcal{A}_{Main}$ selects two messages $m_0, m_1 \leftarrow \mathcal{M} \times \mathcal{M}$. $\mathcal{A}_{Main}$ sends (m_0, m_1) to the challenger.*
4. *The challenger samples a bit b uniformly at random. The challenger then compute $\mathsf{ct} \leftarrow \mathsf{PKE.Enc}(\mathsf{pk}, m_b)$ and sends ct to $\mathcal{A}_{Main}$.*
5. *$\mathcal{A}_{Main}$ outputs a guess b'.*
6. *The challenger outputs 1 if $b' = b$, otherwise it outputs 0.*

We say PKE satisfies IND-CPA Security under One-Time Leakage with Leakage Rate λ if for any QPT leakage adversary $\mathcal{A}_{\mathsf{IND}}$,

$$\Pr[\mathsf{Exp}^{\mathsf{IND}}_{\mathsf{PKE},\mathcal{A}}(n,\lambda) = 1] \leq \frac{1}{2} + \mathsf{negl}(n). \tag{26}$$

Next, we argue that any PKE scheme that satisfies One-Way Security under Bounded Quantum Leakage satisfies indistinguishability (IND) security under Bounded Quantum Leakage. We formalize this security notion below.

Lemma 6.4 (One-way Security to IND Security under Bounded Quantum Leakage)**.** *Let $\tilde{\mathsf{PKE}}$ be a PKE scheme that satisfies One-Way Security under Bounded Quantum Leakage that tolerates a leakage rate of λ. Then there exists a scheme PKE also satisfies IND- Security under Bounded Quantum Leakage for the same leakage rate λ.*

Proof. Let $\tilde{\mathsf{PKE}}$ be a PKE scheme that satisfies One-Way Security under Bounded Quantum Leakage. We will construct a PKE scheme, PKE, that encrypts a single bit and satisfies IND Security under One-Time Leakage.

PKE**:**

- $\mathsf{PKE.KeyGen}(1^n)$:
  1. Run $\tilde{\mathsf{PKE}}.\mathsf{KeyGen}(1^n) \to (\mathsf{pk}, |\mathsf{sk}\rangle)$.
- $\mathsf{PKE.Enc}(\mathsf{pk}, m)$:
  1. Let $\mathcal{M}$ be the message space of $\tilde{\mathsf{PKE}}$. sample $x \leftarrow \mathcal{M}$ and $r \leftarrow \{0,1\}^n$ uniformly at random.
  2. Generate $\tilde{\mathsf{ct}} \leftarrow \tilde{\mathsf{PKE}}.\mathsf{Enc}(\mathsf{pk}, x)$.
  3. Set $\beta = \langle x, r\rangle \oplus m$ and output $\mathsf{ct} = (\tilde{\mathsf{ct}}, r, \beta)$.
- $\mathsf{PKE.Dec}(\rho_{\mathsf{sk}}, \mathsf{ct})$:
  1. Parse $\mathsf{ct} = (\tilde{\mathsf{ct}}, r, \beta)$. Compute $x \leftarrow \tilde{\mathsf{PKE}}.\mathsf{Dec}(\tilde{\mathsf{ct}}, \rho_{\mathsf{sk}})$.
  2. Compute $m = \langle x, r\rangle \oplus \beta$ and output m.

We prove the above PKE scheme, PKE, satisfies Indistinguishability Leakage security. Assume towards contradiction that PKE did not satisfies indistinguishability leakage security. This means there exists an adversary $\mathcal{A} = (\mathcal{A}_{Main}, \mathcal{A}_{Leak})$ that succeeds in $\mathsf{Exp}_{\mathsf{PKE},\mathcal{A}}$ and a non-negligible function $\epsilon(n)$ such that:

$$\Pr[\mathsf{Exp}^{\mathsf{IND}}_{\mathcal{A}}(1^n, \lambda) = 1] \geq \frac{1}{2} + \epsilon(n). \tag{27}$$

Using $\mathcal{A}$, we can construct an adversary $\tilde{\mathcal{A}} = (\tilde{\mathcal{A}}_{Leak}, \tilde{\mathcal{A}}_{Main})$ that breaks one-way leakage security of $\tilde{\mathsf{PKE}}$ as follows. Recall the one way leakage security game, $\mathsf{Exp}^{\mathsf{OW}}_{\tilde{\mathcal{A}}}(1^n, \lambda)$.

1. The challenger first runs $\tilde{\mathsf{PKE}}.\mathsf{KeyGen}(1^n) \to (\mathsf{pk}, |\mathsf{sk}\rangle)$ and sends $|\mathsf{sk}\rangle$ to $\tilde{\mathcal{A}}_{Leak}$ and pk to $\tilde{\mathcal{A}}_{Leak}$ and $\tilde{\mathcal{A}}_{Main}$. $\tilde{\mathcal{A}}_{Main}$ and $\tilde{\mathcal{A}}_{Leak}$ run the leakage protocol of $\mathcal{A}_{Main}$ and $\mathcal{A}_{Leak}$ respectively.
2. The challenger also samples a message $x \leftarrow \mathcal{M}$ and sends the ciphertext $\mathsf{ct}_{\mathsf{OW}} \leftarrow \tilde{\mathsf{PKE}}.\mathsf{Enc}(\mathsf{pk}, x)$ to $\tilde{\mathcal{A}}_{Main}$.
3. Next, we construct the ciphertext. Assume without loss of generality that $\mathcal{A}_{Main}$ submits $(m_0 = 0, m_1 = 1)$. Then, we sample $r \leftarrow \{0,1\}^n$ and $\beta' \leftarrow \{0,1\}$ uniformly at random. Then, we set $\mathsf{ct} = (\mathsf{ct}_{\mathsf{OW}}, r, \beta')$ Note that for challenge messages (m_0, m_1), the true ciphertext is of the form
$$\beta = \langle x, r\rangle \oplus m_b = \langle x, r\rangle \oplus b. \tag{28}$$
Since $\mathsf{ct}_{\mathsf{OW}}$ is generated according to $\tilde{\mathsf{PKE}}$ and r and β' are sampled uniformly at random, the ciphertext ct is distributed identically to that of a PKE ciphertext.
4. Run $\mathcal{A}_{Main}$ on ct and obtain a bit b'.

By assumption,

$$\Pr[b' = b] \geq \frac{1}{2} + \epsilon(n) \tag{29}$$

Moreover, since $b \oplus \beta = \langle x, r \rangle$, whenever $b = b'$ it holds that

$$\Pr[b' \oplus \beta' = \langle x, r \rangle] \geq \frac{1}{2} + \epsilon(n). \tag{30}$$

Then we can apply Theorem 3.4 with the state of $\tilde{\mathcal{A}}_{Main}$ and $b' \oplus \beta'$. This implies that there exists an algorithm A that outputs x' such that

$$\Pr[x' = x] \geq 4\epsilon(n)^2 \tag{31}$$

Using the fact that $H_{\min}(M) \geq \lambda n + \omega(\log n)$, this yields a contradiction. □

Finally, we argue that our PKE scheme constructed in Section 6.1 satisfies IND-Security under Bounded Quantum Leakage.

Theorem 6.5. *Let* PKE *be the PKE construction defined in Section 6.1. Then, there exist a PKE scheme* PKE' *that satisfies IND-Security under Bounded Quantum Leakage up to a leakage rate of* $\lambda < 0.057$.

Proof. Applying Lemma 6.4 to Theorem 6.2, and using the fact that we obtain the theorem. □

7 Classical PKE with Quantum Leakage Security

In this section we construct a classical PKE scheme with security against quantum leakage. At a high level, we will first argue one way leakage security of a secret key encryption (SKE) scheme, and then upgrade the SKE scheme into a public key encryption (PKE) scheme.

In order to prove the lemma Lemma 7.2, we will require the quantum leakage chain rule, as proven by [LC18].

Theorem 7.1 (Quantum Leakage Chain Rule (Theorem 1, [LC18])**.** *Suppose two parties Alice and Bob share a cq-state* $\rho_{XY} \in D(\mathcal{X} \otimes \mathcal{Y} \otimes \mathcal{Z})$ *where Alice holds the register* X *and Bob holds the register* Y*. Let* n_A *and* n_B *be the total number of qubits sent by Alice and Bob respectively in an arbitrary interactive protocol. Let* σ *be the final state held by Alice and Bob after completing the interactive protocol. Then it holds that*

$$H_{\min}(X|Y)_\sigma \geq H_{\min}(X|Y)_\rho - \min(n_A + n_B, 2n_A). \tag{32}$$

First we prove that the one-time pad is a one-way leakage resilient secret key encryption scheme.

Lemma 7.2 (One-way Security of OTP under Bounded Quantum Leakage with Leakage Rate λ)**.** *Let* $n \in \mathbb{N}$ *and let* $p(n)$ *be a sufficiently large polynomial. Consider the following game between a challenger and a quantum leakage adversary,* $\mathcal{A}_{OTP} = (\mathcal{A}_{Main}, \mathcal{A}_{Leak})$, $\mathsf{Exp}^{OTP}_{\mathcal{A}_{OTP}}(n, \lambda)$*:*

1. *The challenger samples a key* $K \leftarrow \{0,1\}^{p(n)}$ *uniformly at random. The challenger sends* K *to* $\mathcal{A}_{Leak}$*.*
2. $\mathcal{A}_{Main}$ *and* $\mathcal{A}_{Leak}$ *run their leakage protocol in which* $\mathcal{A}_{Leak}$ *leaks at most* $\lambda p(n)$ *qubits related to the secret key* K *to* $\mathcal{A}_{Main}$*.*

3. *The challenger samples a message* $m \leftarrow \{0,1\}^{p(n)}$ *uniformly at random and generates a ciphertext,* $\mathsf{ct} = K \oplus m$ *and sends* ct *to* $\mathcal{A}_{Main}$.

4. $\mathcal{A}_{Main}$ *outputs a guess,* m'.

5. *If* $m' = m$ *the challenger outputs 1. Otherwise, the challenger outputs 0.*

For any quantum adversary, $\mathcal{A}_{OTP} = (\mathcal{A}_{Main}, \mathcal{A}_{Leak})$ *and sufficiently large* n,

$$\Pr[\mathsf{Exp}^{OTP}_{\mathcal{A}_{OTP}}(n,\lambda) = 1] \leq \frac{2^{\lambda p(n)}}{2^{p(n)}}. \tag{33}$$

Proof. We will prove the above lemma via an entropy argument. Let $\rho_{XY} \in D(\mathcal{X} \otimes \mathcal{Y})$ be the initial cq-state of $\mathcal{A}_{Leak}$ holds system $X := K$ and $\mathcal{A}_{Main}$ holds system Y. Let σ_{XY} be the state held by $\mathcal{A}_{Leak}$ and $\mathcal{A}_{Main}$ respectively after receiving the quantum leakage denoted by register E and ciphertext, ct in step 3. Let the maximal guessing probability of guessing $X = x$ given quantum side information E be defined by the following function p_{guess} :

$$p_{guess}(X|E) = \max_{\{P_x\}} \sum_x p(x) \mathsf{Tr}(P_x \rho_E^x) \tag{34}$$

where $\{P_x\}$ is the set of POVMs applied to ρ_E^x.

Then since for a fixed ciphertext $CT = \mathsf{ct}$, there exists a unique key $K = m \oplus \mathsf{ct}$. So for any measurement applied to the quantum leakage register E and for any ciphertext ct, the probability of guessing the message and key are equivalent. Formally,

$$p_{guess}(M|E, CT = \mathsf{ct}) = p_{guess}(K|E, CT = \mathsf{ct}). \tag{35}$$

Note that this also implies that

$$\Pr[K = k|CT = \mathsf{ct}] = \Pr[M = k \oplus \mathsf{ct}]. \tag{36}$$

So therefore $H_{\min}(K|E, CT) = H_{\min}(M)$ By averaging over ct, we get that

$$H_{\min}(M|E, CT) = H_{\min}(K|E, CT). \tag{37}$$

Applying the quantum leakage chain rule Theorem 7.1 with $X = K$ held by$\mathcal{A}_{Leak}$ and $Y = (E, CT)$ held by $\mathcal{A}_{Main}$ we get that

$$H_{min}(M|E, CT)_\sigma = H_{\min}(K|E, CT)_\sigma \geq H_{\min}(K|CT) - \lambda \cdot p(n) \tag{38}$$

We can now compute the success probability of adversaries in the experiment $\mathsf{Exp}^{OTP}_{\mathcal{A}_{OTP}}(\lambda)$:

$$\begin{aligned}
\Pr[\mathsf{Exp}^{OTP}_{\mathcal{A}_{OTP}}(\lambda) = 1] &= p_{guess}(M|E, CT) && (39)\\
&= O(2^{-H_{\min}(M|E,CT)_\sigma}) && (40)\\
&\leq O(\frac{2^{\lambda p(n)}}{2^{H_{min}(M)}}) && (41)\\
&= O(\frac{2^{\lambda p(n)}}{2^{p(n)}}). && (42)
\end{aligned}$$

□

Next, we construct a public key encryption (PKE) scheme secure against quantum leakage using a ciphertext policy functional encryption scheme. We show that one-way leakage resilience of the OTP implies one-way leakage security of the PKE scheme. We will use a ciphertext-policy functional encryption scheme (CPFE), which was introduced and defined by [KN23], to construct our PKE scheme. We first provide the definition of a CPFE scheme.

Definition 7.3 (Ciphertext-Policy Functional Encryption Scheme (CPFE), [KN23])**.** *A ciphertext policy functional encryption scheme for the circuit space $\mathcal{C}$ and the input space $\mathcal{X}$ is a tuple of algorithms, (Setup, Keygen, Enc, Dec).*

- $\mathsf{Setup}(1^n) \to MPK, MSK$*:* Setup *takes input a security parameter n and outputs a master public key, MPK and a master secret key, MSK.*
- $\mathsf{Keygen}(MSK, x) \to \mathsf{sk}_x$*:* Keygen *takes input the master secret key, MSK, and an input $x \in \mathcal{X}$ and outputs a secret key,* sk*.*
- $\mathsf{Enc}(MPK, C) \to \mathsf{ct}$*:* Enc *takes input the master public key, MPK and a circuit $C \in \mathcal{C}$ and outputs a ciphertext,* ct*.*
- $\mathsf{Dec}(\mathsf{sk}_x, \mathsf{ct}) \to y$*:* Dec *takes input a secret key sk_x and a ciphertext* ct *and outputs a value y.*

The correctness and security follows as previously defined.

Definition 7.4 (CPFE Correctness [KN23])**.** *We say that a CPFE = (Setup, Keygen, Enc, Dec) scheme satisfies correctness if for all $C \in \mathcal{C}, x \in \mathcal{X}$, $Setup(1^n) \to (MSK, MPK)$, and $\mathsf{Keygen}(MSK, x) \to sk_x$,*

$$\mathsf{Dec}(\mathsf{sk}_x, \mathsf{Enc}(MPK, C)) \to C(x).$$

Definition 7.5 (CPFE 1-bounded Security [KN23])**.** *Let $\mathsf{CPFE} = (\mathsf{Setup}, \mathsf{Keygen}, \mathsf{Enc}, \mathsf{Dec})$ be a CPFE scheme as defined above. We define the following security game, $\mathsf{Exp}^{1-\mathsf{Bounded}}_{\mathsf{CPFE},\mathcal{A}}(1^n, \mathsf{coin})$, between a challenger and a QPT adversary $\mathcal{A}$.*

1. *$\mathcal{A}$ chooses $x \in \mathcal{X}$ and sends x to the challenger.*
2. *The challenger generates $\mathsf{Setup}(1^n) \to (MPK, MSK)$ and $\mathsf{KeyGen}(MSK, x) \to sk_x$ and sends MPK and sk_x to $\mathcal{A}$.*
3. *$\mathcal{A}$ outputs C_0 and C_1 such that $C_0(x) = C_1(x)$. The challenger generates $\mathsf{Enc}(MPK, C_{\mathsf{coin}}) \to \mathsf{ct}$. The challenger sends ct to $\mathcal{A}$.*
4. *$\mathcal{A}$ outputs $\mathsf{coin}' \in \{0, 1\}$.*

The challenger outputs 1 if $\mathsf{coin}' = \mathsf{coin}$ and outputs 0 otherwise. We say that CPFE is 1-bounded secure if for all QPT $\mathcal{A}$,

$$\left| \Pr[\mathsf{Exp}^{1-\mathsf{Bounded}}_{\mathsf{CPFE},\mathcal{A}}(1^n, 0) = 1] - \Pr[\mathsf{Exp}^{1-\mathsf{Bounded}}_{\mathsf{CPFE},\mathcal{A}}(1^n, 1) = 1] \right| \leq \mathsf{negl}(n). \tag{43}$$

Definition 7.6 (Succinct CPFE Scheme)**.** *We say that a CPFE scheme is succinct if $|sk_x| = |x| + \mathsf{poly}(n)$.*

It was shown in [KN23], that a succinct CPFE scheme could be constructed from a has encryption scheme. Moreover, it was shown in [DGHM17] that one can construct a hash encryption scheme assuming the hardness of LWE.

Theorem 7.7 (Existence of CPFE (Theorem B.4, [KN23]))**.** *Assuming the hardness of LWE, there exists a succinct CPFE scheme.*

7.1 Construction

We now give the construction of the leakage resilient PKE scheme, $\mathsf{PKE} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ for a particular leakage rate λ. Our construction will use a one time pad scheme $\mathsf{OTP} = \mathsf{OTP}.(\mathsf{Enc}, \mathsf{Dec})$ and a CPFE scheme $\mathsf{CPFE} = \mathsf{CPFE}.(\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$.

- $\mathsf{PKE}.\mathsf{KeyGen}(1^n, \lambda)$:
  - First choose a sufficiently large polynomial $p(n)$ such that $\lambda p(n) - p(n) = -\omega(\log(n))$ pick a uniformly random key $K \leftarrow \{0,1\}^{p(n)}$.
  - Run $(MPK, MSK) \leftarrow \mathsf{CPFE}.\mathsf{Setup}(1^n)$ and run $sk_K \leftarrow \mathsf{CPFE}.\mathsf{KeyGen}(MSK, K)$.
  - Output $\mathsf{pk} = MPK$ and $\mathsf{sk} = (K, \mathsf{sk}_K)$.
- $\mathsf{PKE}.\mathsf{Enc}(\mathsf{pk}, m)$:
  - Let C_m be the circuit that takes a key K to $\mathsf{OTP}.\mathsf{Enc}(K, m)$ and parse $\mathsf{pk} = MPK$. Run $\mathsf{ct}_{\mathsf{CPFE}} \leftarrow \mathsf{CPFE}.\mathsf{Enc}(MPK, C_m)$.
  - Output $\mathsf{ct} = \mathsf{ct}_{\mathsf{CPFE}}$.
- $\mathsf{PKE}.\mathsf{Dec}(\mathsf{sk}, \mathsf{ct})$:
  - Parse $\mathsf{sk} = (K, \mathsf{sk}_k)$ and $\mathsf{ct} = \mathsf{ct}_{\mathsf{CPFE}}$. Then compute $\mathsf{ct}_{\mathsf{OTP}} \leftarrow \mathsf{CPFE}.\mathsf{Dec}(\mathsf{sk}_K, \mathsf{ct})$ where $\mathsf{ct}_{\mathsf{OTP}} = \mathsf{OTP}.\mathsf{Enc}(K, m)$ and compute $m \leftarrow \mathsf{OTP}.\mathsf{Dec}(K, \mathsf{ct}_{\mathsf{OTP}})$.

Correctness of PKE Correctness follows from the correctness of OTP and CPFE.

We now argue that PKE satisfies one-way leakage security under bounded quantum leakage, as defined below.

Definition 7.8 (One-Way Security of PKE under Bounded Quantum Leakage with Leakage Rate λ)**.** *Let $n \in \mathbb{N}$. Let $\mathsf{PKE} = (\mathsf{Keygen}, \mathsf{Enc}, \mathsf{Dec})$ be a public key encryption scheme. Consider the following security game $\mathsf{Exp}^{\mathsf{OW}}_{\mathcal{A}_{\mathsf{PKE}}}(\lambda)$ parametrized by a leakage rate λ, between a challenger and a QPT adversary, $\mathcal{A}_{\mathsf{PKE}} = (\mathcal{A}_{Leak}, \mathcal{A}_{Main})$.*

1. *The challenger runs $\mathsf{Keygen}(1^n) \to (\mathsf{pk}, \mathsf{sk})$ and sends pk to $\mathcal{A}_{Main}$ and $(\mathsf{pk}, \mathsf{sk})$ to $\mathcal{A}_{Leak}$.*
2. *$\mathcal{A}_{Leak}$ sends at most $\lambda \cdot |\mathsf{sk}|$ total qubits (which includes any classical information) to $\mathcal{A}_{Main}$.*
3. *The challenger randomly samples a message $m \leftarrow \{0,1\}^{p(n)}$ uniformly at random and generates $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, m)$ and sends ct to $\mathcal{A}_{Main}$.*
4. *$\mathcal{A}_{Main}$ outputs a guess $m' \in \{0,1\}^{p(n)}$.*
5. *If $m' = m$ the challenger outputs 1. Otherwise, the challenger outputs 0.*

PKE satisfies One-Way Security under Bounded Quantum Leakage with Leakage Rate λ if for any QPT adversary $\mathcal{A}_{\mathsf{PKE}} = (\mathcal{A}_{Main}, \mathcal{A}_{Leak})$, and any sufficiently large n,

$$\Pr[\mathsf{Exp}^{\mathsf{OW}}_{\mathcal{A}_{\mathsf{PKE}}}(1^n, \lambda) = 1] \leq \mathsf{negl}(n). \tag{44}$$

Theorem 7.9 (One-Way Security of PKE Construction under Bounded Leakage)**.** *Let PKE be the PKE scheme as defined in Section 7.1. Assuming the hardness of LWE, for any QPT adversary $\mathcal{A}_{\mathsf{PKE}} = (\mathcal{A}_{Main}, \mathcal{A}_{Leak})$, $\lambda < 1 - \frac{1}{poly(n)}$ and any sufficiently large n, PKE satisfies One-Way Security under Bounded Leakage with leakage ration λ.*

Proof. Assume towards contradiction that there exists an adversary $\mathcal{A}_{\mathsf{PKE}} = (\mathcal{A}_{Main}, \mathcal{A}_{Leak})$ and a non-negligible function $\epsilon(n, \lambda)$ such that

$$\Pr[\mathsf{Exp}^{\mathsf{OW}}_{\mathcal{A}_{\mathsf{PKE}}}(1^n, \lambda) = 1] \geq \epsilon(n, \lambda). \tag{45}$$

Then, using $\mathcal{A}_{\mathsf{PKE}}$, we construct an adversary $\hat{A}_{\mathsf{OTP}} = (\hat{\mathcal{A}}_{Main}, \hat{\mathcal{A}}_{Leak})$ for the one-way leakage security of the one-time pad scheme. We first consider the following hybrids.

- $\mathcal{H}_0$: This is the original security game, $\mathsf{Exp}^{\mathsf{OW}}_{\mathcal{A}_{\mathsf{PKE}}}(n, \lambda)$.
- $\mathcal{H}_1$: This is the same as $\mathcal{H}_0$ except we modify the encryption process of $\mathsf{PKE.Enc}(\mathsf{pk}, m)$. Instead of using the circuit C_m to generate $\mathsf{ct}_{\mathsf{CPFE}}$, we use the circuit $\tilde{C}[K \oplus m]$, which is the constant circuit that, for a uniformly random K, has $K \oplus m$ hardcoded and outputs $K \oplus m$ on any input.

  To argue indistinguishability of $\mathcal{H}_0$ and $\mathcal{H}_1$ we will rely on the security of the underlying CPFE scheme. That is, on input K, $C_m(K) = K \oplus m$. Similarly, on input K, $\tilde{C}[K \oplus m] = K \oplus m$. Therefore by the security of CPFE,

$$\Pr[\mathcal{H}_0 = 1] - \Pr[\mathcal{H}_1 = 1] \leq \mathsf{negl}(n).$$

We now provide the reduction from the OTP security game. Recall $p(n)$ be a sufficiently large polynomial in n such that $\lambda p(n) - p(n) = -\omega \log n$.

1. The challenger first randomly samples a ket $K \leftarrow \{0,1\}^{p(n)}$. The challenger sends K to $\hat{\mathcal{A}}_{Leak}$.
2. $\hat{\mathcal{A}}_{Leak}$ runs $\mathsf{CPFE.Setup}(1^n) \rightarrow (MPK, MSK)$ and uses K to generate $\mathsf{sk}_K \leftarrow \mathsf{CPFE.KeyGen}(MSK, K)$. $\hat{\mathcal{A}}_{Leak}$ sets $\mathsf{pk} = MPK$ and $\mathsf{sk} = (K, \mathsf{sk}_K)$ and sends pk to $\hat{\mathcal{A}}_{Main}$.
3. $\hat{\mathcal{A}}_{Leak}$ and $\hat{\mathcal{A}}_{Main}$ simulate the leakage protocol for $\mathcal{A}_{\mathsf{PKE}}$:
   (a) $\hat{\mathcal{A}}_{Leak}$ forwards $(\mathsf{pk}, \mathsf{sk})$ to $\mathcal{A}_{Leak}$.
   (b) $\hat{\mathcal{A}}_{Leak}$ and $\hat{\mathcal{A}}_{Main}$ run the leakage protocol of $\mathcal{A}_{Leak}$ and $\mathcal{A}_{Main}$. That is, $\hat{\mathcal{A}}_{Leak}$ runs $\mathcal{A}_{Leak}$ and sends at most $\lambda|\mathsf{sk}|$ qubits to $\mathcal{A}_{Main}$.
4. The challenger randomly samples a message $m \leftarrow \mathcal{M}$ and sends a ciphertext $\mathsf{ct} = K \oplus m$ to $\hat{\mathcal{A}}_{Main}$
5. $\hat{\mathcal{A}}_{Main}$ uses the circuit $\tilde{C}[\mathsf{ct}]$ which is the constant circuit such that on any input, will output ct. $\hat{\mathcal{A}}_{Main}$ then runs $\mathsf{CPFE.Enc}(MPK, \tilde{C}[\mathsf{ct}]) \rightarrow \mathsf{ct}_{\mathsf{CPFE}}$. $\hat{\mathcal{A}}_{Main}$ then runs $\mathcal{A}_{Main}$ on $\mathsf{ct}_{\mathsf{CPFE}}$ and obtains an output m'. $\hat{\mathcal{A}}_{Main}$ outputs m'.

Next we argue the leakage rate tolerated by the PKE scheme. Let λ_{OTP} be the leakage rate tolerated by the underlying OTP scheme. Then,

$$\lambda(|K| + |\mathsf{sk}_K|) \leq \lambda_{OTP}|K| \tag{46}$$

which implies that

$$\lambda \leq \lambda_{\mathsf{OTP}} \frac{|K|}{|K| + |\mathsf{sk}_K|}. \tag{47}$$

By the succinctness property of the CPFE scheme and the fact that $p(n)$ is chosen to be a sufficiently large polynomial, $\frac{|K|}{|K|+|\mathsf{sk}_K|} \leq 1 - \frac{1}{poly(n)}$. Then we can compute the success probability of $\hat{\mathcal{A}}_{\mathsf{OTP}}$ as

$$\Pr[\mathsf{Exp}^{\mathsf{Leakage}}_{\hat{\mathcal{A}}_{\mathsf{OTP}}}(1^n, \lambda) = 1] \geq \Pr[\mathsf{Exp}^{\mathsf{OW}}_{\mathcal{A}_{\mathsf{PKE}}}(1^n, \lambda) = 1] + \mathsf{negl}(n) \tag{48}$$

$$\geq \epsilon(n, \lambda) + \mathsf{negl}(n) > +\mathsf{negl}(n). \tag{49}$$

which contradicts Lemma 7.2 and completes the proof. □

Remark 7.10. *As mentioned earlier, that it is also known that we can construct CPFE with a much weaker assumption, the existence of PKE [GVW12]. However, the resulting CPFE scheme is not succinct and the secret key size grows polynomially with the input length, meaning $|sk_x| = |x| \cdot poly(n)$. Consequently, $|x|/|\mathsf{sk}_x| = 1/poly(n)$ and if we use this CPFE scheme to construct our PKE, we obtain a scheme with a leakage ratio of $1/poly(n)$. Therefore, there is a trade off between the leakage ratio of our PKE scheme and the assumption we require to construct the underlying CPFE scheme.*

Finally, we argue that our PKE scheme constructed in Section 7.1 satisfies IND-Security under Bounded Leakage. We adapt this from our previous definition, Definition 6.3, except now we consider only bounded classical leakage.

Definition 7.11 (IND Security of PKE under Bounded Quantum Leakage with Leakage Rate λ)**.** *Let $n \in \mathbb{N}$ let λ be the leakage rate, and let $\mathcal{M} = \{0,1\}$ be the message space. Let $\mathsf{PKE} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ be a PKE scheme. Consider the following security game, $\mathsf{Exp}^{\mathsf{IND}}_{\mathsf{PKE},\mathcal{A}}(n, \lambda)$ between a challenger and a QPT adversary $\mathcal{A}_{\mathsf{IND}} = (\mathcal{A}_{Leak}, \mathcal{A}_{Main})$.*

1. *The challenger runs $\mathsf{KeyGen}(1^n) \to (\mathsf{pk}, \mathsf{sk})$ and sends $(\mathsf{pk}, |\mathsf{sk}\rangle)$ to $\mathcal{A}_{Leak}$.*
2. *$\mathcal{A}_{Leak}$ and $\mathcal{A}_{Main}$ run their interactive protocol in which $\mathcal{A}_{Leak}$ sends $\lambda \cdot |\mathsf{sk}|$ qubits (which includes any classical leakage) to $\mathcal{A}_{Main}$.*
3. *$\mathcal{A}_{Main}$ selects two messages $m_0, m_1 \leftarrow \mathcal{M} \times \mathcal{M}$. $\mathcal{A}_{Main}$ sends (m_0, m_1) to the challenger.*
4. *The challenger samples a bit b uniformly at random. The challenger then compute $\mathsf{ct} \leftarrow \mathsf{PKE.Enc}(\mathsf{pk}, m_b)$ and sends ct to $\mathcal{A}_{Main}$.*
5. *$\mathcal{A}_{Main}$ outputs a guess b'.*
6. *The challenger outputs 1 if $b' = b$, otherwise it outputs 0.*

We say PKE satisfies IND Security under One-Time Leakage with Leakage Rate λ if for any QPT leakage adversary $\mathcal{A}_{\mathsf{IND}}$,

$$\Pr[\mathsf{Exp}^{\mathsf{IND}}_{\mathsf{PKE},\mathcal{A}}(n, \lambda) = 1] \leq \frac{1}{2} + \mathsf{negl}(n). \tag{50}$$

Lemma 7.12 (One-Way Secuirty to IND Security under Bounded Classical Leakage)**.** *Let $\tilde{\mathsf{PKE}}$ be a PKE scheme that satisfies One-Way Security under Bounded Classical Leakage with leakage rate λ. Then there exists a PKE scheme PKE that satisfies IND-Security under Bounded Classical Leakage with the same leakage rate λ.*

Proof. Our proof follows identically to Lemma 6.4 except we consider bounded classical leakage instead of bounded quantum leakage and unbounded classical leakage. The primary difference in the proof is that we construct the IND-Secure PKE using a One-Way Secure PKE that uses a classical

secret key. That is, $\tilde{\mathsf{PKE}} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ where $\tilde{\mathsf{PKE}}.\mathsf{KeyGen}(1^n) \to (\mathsf{pk}, \mathsf{sk})$. The IND-Secure scheme, PKE, is constructed exactly the same. Then the IND-Security leakage adversary, $\mathcal{A}_{IND} = (\mathcal{A}_{Leak}, \mathcal{A}_{Main})$ run an interactive leakage protocol in which they exchange at most $\lambda|\mathsf{sk}|$ bits of information correlated with sk, instead of bounded quantum leakage. The rest of the proof proceeds identically. □

Theorem 7.13. *Let* PKE *be the PKE construction defined in Section 7.1. Then, assuming the hardness of the LWE problem there exists a PKE scheme* PKE' *that satisfies IND-Security under Bounded Quantum Leakage with leakage rate* $\lambda \leq (1 - 1/poly(n))$ *for any* $poly(n)$.

Alternatively, assuming the existence of post-quantum PKE, there exists a PKE scheme PKE' *that satisfies IND-Security under Bounded Leakge with leakage rate* $\lambda \leq 1/poly(n)$ *for some poly(n)*

Proof. Applying Lemma 7.12 to Theorem 7.9, we obtain the first part of the theorem.

Observing Remark 7.10, we can also obtain our One-Way Secure Leakage Resilient PKE under the minimal assumption of post-quantum secure PKE at those coset of a slightly weaker leakage rate. Then applying Lemma 7.12, we obtain the second part of the theorem. □

Acknowledgment. Generative AI tools were used for language editing.

References

[Aar09] Scott Aaronson. Quantum copy-protection and quantum money. In *Proceedings of the 24th Annual IEEE Conference on Computational Complexity, CCC 2009, Paris, France, 15-18 July 2009*, pages 229–242. IEEE Computer Society, 2009.

[AB24] Prabhanjan Ananth and Amit Behera. A modular approach to unclonable cryptography. In Leonid Reyzin and Douglas Stebila, editors, *CRYPTO 2024, Part VII*, volume 14926 of *LNCS*, pages 3–37. Springer, Cham, August 2024.

[ABH+25] Prabhanjan Ananth, Amit Behera, Zikuan Huang, Fuyuki Kitagawa, and Takashi Yamakawa. Copy-protection from unclonable puncturable obfuscation, revisited. Cryptology ePrint Archive, Paper 2025/1880, 2025.

[ABH+26] Prabhanjan Ananth, Amit Behera, Zikuan Huang, Fuyuki Kitagawa, and Takashi Yamakawa. Copy-protection from unclonable puncturable obfuscation, revisited. In *Eurocrypt 2026 (to appear)*, 2026.

[ABJO24] Divesh Aggarwal, Naresh Goud Boddu, Rahul Jain, and Maciej Obremski. Quantum measurement adversary. *IEEE Trans. Inf. Theory*, 70(1):318–335, 2024.

[ACLV19] Divesh Aggarwal, Kai-Min Chung, Han-Hsuan Lin, and Thomas Vidick. A quantum-proof non-malleable extractor - with application to privacy amplification against active quantum adversaries. In Yuval Ishai and Vincent Rijmen, editors, *EUROCRYPT 2019, Part II*, volume 11477 of *LNCS*, pages 442–469. Springer, Cham, May 2019.

[ADW09] Joël Alwen, Yevgeniy Dodis, and Daniel Wichs. Leakage-resilient public-key cryptography in the bounded-retrieval model. In Shai Halevi, editor, *CRYPTO 2009*, volume 5677 of *LNCS*, pages 36–54. Springer, Berlin, Heidelberg, August 2009.

[AGV09] Adi Akavia, Shafi Goldwasser, and Vinod Vaikuntanathan. Simultaneous hardcore bits and cryptography against memory attacks. In Omer Reingold, editor, *TCC 2009*, volume 5444 of *LNCS*, pages 474–495. Springer, Berlin, Heidelberg, March 2009.

[AHH24] Prabhanjan Ananth, Zihan Hu, and Zikuan Huang. Quantum key-revocable dual-regev encryption, revisited. In Elette Boyle and Mohammad Mahmoody, editors, *TCC 2024, Part III*, volume 15366 of *LNCS*, pages 257–288. Springer, Cham, December 2024.

[AKN+23] Shweta Agrawal, Fuyuki Kitagawa, Ryo Nishimaki, Shota Yamada, and Takashi Yamakawa. Public key encryption with secure key leasing. In Carmit Hazay and Martijn Stam, editors, *EUROCRYPT 2023, Part I*, volume 14004 of *LNCS*, pages 581–610. Springer, Cham, April 2023.

[AL21] Prabhanjan Ananth and Rolando L. La Placa. Secure software leasing. In Anne Canteaut and François-Xavier Standaert, editors, *EUROCRYPT 2021, Part II*, volume 12697 of *LNCS*, pages 501–530. Springer, Cham, October 2021.

[ALL+21] Scott Aaronson, Jiahui Liu, Qipeng Liu, Mark Zhandry, and Ruizhe Zhang. New approaches for quantum copy-protection. In Tal Malkin and Chris Peikert, editors, *CRYPTO 2021, Part I*, volume 12825 of *LNCS*, pages 526–555, Virtual Event, August 2021. Springer, Cham.

[APM20] Shweta Agrawal and Alice Pellet-Mary. Indistinguishability obfuscation without maps: Attacks and fixes for noisy linear fe. In *Advances in Cryptology – EUROCRYPT 2020: 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10–14, 2020, Proceedings, Part I*, page 110–140, Berlin, Heidelberg, 2020. Springer-Verlag.

[APV23] Prabhanjan Ananth, Alexander Poremba, and Vinod Vaikuntanathan. Revocable cryptography from learning with errors. In Guy N. Rothblum and Hoeteck Wee, editors, *TCC 2023, Part IV*, volume 14372 of *LNCS*, pages 93–122. Springer, Cham, November / December 2023.

[BGI+01] Boaz Barak, Oded Goldreich, Rusell Impagliazzo, Steven Rudich, Amit Sahai, Salil Vadhan, and Ke Yang. On the (im) possibility of obfuscating programs. In *Annual international cryptology conference*, pages 1–18. Springer, 2001.

[BGMZ18] James Bartusek, Jiaxin Guan, Fermi Ma, and Mark Zhandry. Return of ggh15: Provable security against zeroizing attacks. In *Theory of Cryptography: 16th International Conference, TCC 2018, Panaji, India, November 11–14, 2018, Proceedings, Part II*, page 544–574, Berlin, Heidelberg, 2018. Springer-Verlag.

[BJK24] Naresh Goud Boddu, Rahul Jain, and Upendra Kapshikar. Quantum secure non-malleable-extractors, 2024.

[BJL+21] Anne Broadbent, Stacey Jeffery, Sébastien Lord, Supartha Podder, and Aarthi Sundaram. Secure software leasing without assumptions. In Kobbi Nissim and Brent Waters, editors, *TCC 2021, Part I*, volume 13042 of *LNCS*, pages 90–120. Springer, Cham, November 2021.

[BKKV10] Zvika Brakerski, Yael Tauman Kalai, Jonathan Katz, and Vinod Vaikuntanathan. Overcoming the hole in the bucket: Public-key cryptography resilient to continual memory leakage. In *51st FOCS*, pages 501–510. IEEE Computer Society Press, October 2010.

[BLSV18] Zvika Brakerski, Alex Lombardi, Gil Segev, and Vinod Vaikuntanathan. Anonymous IBE, leakage resilience and circular security from new assumptions. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part I*, volume 10820 of *LNCS*, pages 535–564. Springer, Cham, April / May 2018.

[BZ13] Dan Boneh and Mark Zhandry. Secure signatures and chosen ciphertext security in a quantum computing world. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 361–379. Springer, Berlin, Heidelberg, August 2013.

[ÇG24a] Alper Çakan and Vipul Goyal. Unbounded leakage-resilient encryption and signatures. Cryptology ePrint Archive, Report 2024/1876, 2024.

[ÇG24b] Alper Çakan and Vipul Goyal. Unclonable cryptography with unbounded collusions and impossibility of hyperefficient shadow tomography. In Elette Boyle and Mohammad Mahmoody, editors, *TCC 2024, Part III*, volume 15366 of *LNCS*, pages 225–256. Springer, Cham, December 2024.

[ÇG26] Alper Çakan and Vipul Goyal. How to copy-protect malleable-puncturable cryptographic functionalities under arbitrary challenge distributions: A unified solution to quantum protection. In *Eurocrypt 2026 (to appear)*, 2026.

[ÇGLZR24] Alper Çakan, Vipul Goyal, Chen-Da Liu-Zhang, and João Ribeiro. Unbounded leakage-resilience and intrusion-detection in a quantum world. In Elette Boyle and Mohammad Mahmoody, editors, *TCC 2024, Part II*, volume 15365 of *LNCS*, pages 159–191. Springer, Cham, December 2024.

[CHVW19] Yilei Chen, Minki Hhan, Vinod Vaikuntanathan, and Hoeteck Wee. Matrix prfs: Constructions, attacks, and applications to obfuscation. In *Theory of Cryptography: 17th International Conference, TCC 2019, Nuremberg, Germany, December 1–5, 2019, Proceedings, Part I*, page 55–80, Berlin, Heidelberg, 2019. Springer-Verlag.

[CKNY25] Jeffrey Champion, Fuyuki Kitagawa, Ryo Nishimaki, and Takashi Yamakawa. Untelegraphable encryption and its applications. In Benny Applebaum and Huijia (Rachel) Lin, editors, *TCC 2025, Part III*, volume 16270 of *LNCS*, pages 3–35. Springer, Cham, December 2025.

[CLLZ21] Andrea Coladangelo, Jiahui Liu, Qipeng Liu, and Mark Zhandry. Hidden cosets and applications to unclonable cryptography. In Tal Malkin and Chris Peikert, editors, *CRYPTO 2021, Part I*, volume 12825 of *LNCS*, pages 556–584, Virtual Event, August 2021. Springer, Cham.

[CLW25] Valerio Cini, Russell WF Lai, and Ivy KY Woo. Lattice-based obfuscation from ntru and equivocal lwe. In *Annual International Cryptology Conference*, pages 39–72. Springer, 2025.

[CV22] Eric Culf and Thomas Vidick. A monogamy-of-entanglement game for subspace coset states. *Quantum*, 6:791, September 2022.

[DGHM17] Nico Döttling, Sanjam Garg, Mohammad Hajiabadi, and Daniel Masny. New constructions of identity-based and key-dependent message secure encryption schemes. Cryptology ePrint Archive, Paper 2017/978, 2017.

[DGHM18] Nico Döttling, Sanjam Garg, Mohammad Hajiabadi, and Daniel Masny. New constructions of identity-based and key-dependent message secure encryption schemes. In Michel Abdalla and Ricardo Dahab, editors, *PKC 2018, Part I*, volume 10769 of *LNCS*, pages 3–31. Springer, Cham, March 2018.

[DHLW10] Yevgeniy Dodis, Kristiyan Haralambiev, Adriana López-Alt, and Daniel Wichs. Cryptography against continuous memory attacks. In *51st FOCS*, pages 511–520. IEEE Computer Society Press, October 2010.

[DKL09] Yevgeniy Dodis, Yael Tauman Kalai, and Shachar Lovett. On cryptography with auxiliary input. In Michael Mitzenmacher, editor, *41st ACM STOC*, pages 621–630. ACM Press, May / June 2009.

[DLW06] Giovanni Di Crescenzo, Richard J. Lipton, and Shabsi Walfish. Perfectly secure password protocols in the bounded retrieval model. In Shai Halevi and Tal Rabin, editors, *TCC 2006*, volume 3876 of *LNCS*, pages 225–244. Springer, Berlin, Heidelberg, March 2006.

[DP08] Stefan Dziembowski and Krzysztof Pietrzak. Leakage-resilient cryptography. In *49th FOCS*, pages 293–302. IEEE Computer Society Press, October 2008.

[DPVR12] Anindya De, Christopher Portmann, Thomas Vidick, and Renato Renner. Trevisan's extractor in the presence of quantum side information. *SIAM J. Comput.*, 41(4):915–940, 2012.

[DQV+21] Lalita Devadas, Willy Quach, Vinod Vaikuntanathan, Hoeteck Wee, and Daniel Wichs. Succinct LWE sampling, random polynomials, and obfuscation. Cryptology ePrint Archive, Paper 2021/1226, 2021.

[Dzi06] Stefan Dziembowski. Intrusion-resilience via the bounded-storage model. In Shai Halevi and Tal Rabin, editors, *TCC 2006*, volume 3876 of *LNCS*, pages 207–224. Springer, Berlin, Heidelberg, March 2006.

[GKK+07] Dmitry Gavinsky, Julia Kempe, Iordanis Kerenidis, Ran Raz, and Ronald de Wolf. Exponential separations for one-way quantum communication complexity, with applications to cryptography. In David S. Johnson and Uriel Feige, editors, *39th ACM STOC*, pages 516–525. ACM Press, June 2007.

[GVW12] Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee. Functional encryption with bounded collusions via multi-party computation. In Reihaneh Safavi-Naini and Ran Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 162–179. Springer, Berlin, Heidelberg, August 2012.

[GZ20] Marios Georgiou and Mark Zhandry. Unclonable decryption keys. Cryptology ePrint Archive, Report 2020/877, 2020.

[HLWW16] Carmit Hazay, Adriana López-Alt, Hoeteck Wee, and Daniel Wichs. Leakage-resilient cryptography from minimal assumptions. *Journal of Cryptology*, 29(3):514–551, July 2016.

[ISW03] Yuval Ishai, Amit Sahai, and David Wagner. Private circuits: Securing hardware against probing attacks. In Dan Boneh, editor, *CRYPTO 2003*, volume 2729 of *LNCS*, pages 463–481. Springer, Berlin, Heidelberg, August 2003.

[KMY25] Fuyuki Kitagawa, Tomoyuki Morimae, and Takashi Yamakawa. A simple framework for secure key leasing. In Serge Fehr and Pierre-Alain Fouque, editors, *EUROCRYPT 2025, Part III*, volume 15603 of *LNCS*, pages 217–247. Springer, Cham, May 2025.

[KN23] Fuyuki Kitagawa and Ryo Nishimaki. One-out-of-many unclonable cryptography: Definitions, constructions, and more. In Guy N. Rothblum and Hoeteck Wee, editors, *TCC 2023, Part IV*, volume 14372 of *LNCS*, pages 246–275. Springer, Cham, November / December 2023.

[KNY21] Fuyuki Kitagawa, Ryo Nishimaki, and Takashi Yamakawa. Secure software leasing from standard assumptions. In Kobbi Nissim and Brent Waters, editors, *TCC 2021, Part I*, volume 13042 of *LNCS*, pages 31–61. Springer, Cham, November 2021.

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

[KY25] Fuyuki Kitagawa and Takashi Yamakawa. Foundations of single-decryptor encryption. In Benny Applebaum and Huijia (Rachel) Lin, editors, *TCC 2025, Part III*, volume 16270 of *LNCS*, pages 166–197. Springer, Cham, December 2025.

[LC18] Ching-Yi Lai and Kai-Min Chung. Interactive leakage chain rule for quantum min-entropy, 2018.

[LLQZ22] Jiahui Liu, Qipeng Liu, Luowen Qian, and Mark Zhandry. Collusion resistant copy-protection for watermarkable functionalities. In Eike Kiltz and Vinod Vaikuntanathan, editors, *TCC 2022, Part I*, volume 13747 of *LNCS*, pages 294–323. Springer, Cham, November 2022.

[MR04] Silvio Micali and Leonid Reyzin. Physically observable cryptography (extended abstract). In Moni Naor, editor, *TCC 2004*, volume 2951 of *LNCS*, pages 278–296. Springer, Berlin, Heidelberg, February 2004.

[NC10] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.

[NS09] Moni Naor and Gil Segev. Public-key cryptosystems resilient to key leakage. In Shai Halevi, editor, *CRYPTO 2009*, volume 5677 of *LNCS*, pages 18–35. Springer, Berlin, Heidelberg, August 2009.

[Ren05] Renato Renner. *Security of Quantum Key Distribution*. PhD thesis, ETH Zurich, 2005. Diss. ETH No. 16242, arXiv:quant-ph/0512258.

[Ren08] Renato Renner. *Security of quantum key distribution*. PhD thesis, ETH Zurich, 2008. arXiv:quant-ph/0512258.

[TSSR11] Marco Tomamichel, Christian Schaffner, Adam D. Smith, and Renato Renner. Leftover hashing against quantum side information. *IEEE Trans. Inf. Theory*, 57(8):5524–5535, 2011.

[VZ21] Thomas Vidick and Tina Zhang. Classical proofs of quantum knowledge. In *Advances in Cryptology – EUROCRYPT 2021: 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17–21, 2021, Proceedings, Part II*, page 630–660, Berlin, Heidelberg, 2021. Springer-Verlag.

[Zha21] Mark Zhandry. Quantum lightning never strikes the same state twice. or: Quantum money from cryptographic assumptions. *Journal of Cryptology*, 34(1):6, January 2021.