

# Public-Key Quantum Authentication and Digital Signature Schemes Based on the QMA-Complete Problem

Le-Ran Liu,<sup>1,2</sup> Min-Quan He,<sup>1,2</sup> Dan-Bo Zhang,<sup>3</sup> and Z. D. Wang<sup>1,2</sup>

<sup>1</sup>*Department of Physics and HK Institute of Quantum Science & Technology,  
The University of Hong Kong, Pokfulam Road, Hong Kong, China*

<sup>2</sup>*Hong Kong Branch for Quantum Science Center of Guangdong-Hong Kong-Macau Greater Bay Area, Shenzhen, China*

<sup>3</sup>*Key Laboratory of Atomic and Subatomic Structure and Quantum Control (Ministry of Education),  
Guangdong Basic Research Center of Excellence for Structure and Fundamental Interactions of Matter,  
and School of Physics, South China Normal University, Guangzhou 510006, China*

We propose a quantum authentication and digital signature protocol whose security is founded on the Quantum Merlin Arthur (QMA)-completeness of the consistency of local density matrices. The protocol functions as a true public-key cryptography system, where the public key is a set of local density matrices generated from the private key, a global quantum state. This construction uniquely eliminates the need for trusted third parties, pre-shared secrets, or authenticated classical channels for public key distribution, making a significant departure from symmetric protocols like quantum key distribution. We provide a rigorous security analysis, proving the scheme's unforgeability against adaptive chosen-message attacks by quantum adversaries. The proof proceeds by a formal reduction, demonstrating that a successful forgery would imply an efficient quantum algorithm for the QMA-complete Consistency of Quantum Marginal Problem (QMP). We further analyze the efficiency of verification using partial quantum state tomography, establishing the protocol's theoretical robustness and outlining a path towards practical implementation.

## INTRODUCTION

The advent of scalable quantum computers threatens the security of conventional public-key cryptosystems [1, 2]. Shor's polynomial-time algorithm for integer factorization and discrete logarithms undermines RSA [3] and elliptic-curve cryptography [4, 5], while Grover's quadratic speed-up lowers the effective strength of symmetric ciphers [6]. Although block ciphers such as AES can be hardened by increasing the key size, the prospective collapse of public-key infrastructure compels the search for alternative paradigms [7].

In response to the quantum threat, two principal directions have emerged. The first is post-quantum cryptography (PQC) [8], which seeks to develop classical cryptographic schemes believed to be secure against both classical and quantum attacks. Notable examples include lattice-based encryption [9], code-based cryptography [10], and multivariate polynomial schemes [11]. While these constructions currently resist known quantum algorithms, their long-term security remains an open question, especially in the face of unforeseen advances in quantum algorithms or cryptanalysis. The second direction is quantum cryptography [12, 13], which leverages the fundamental principles of quantum mechanics to achieve information-theoretic security. Protocols such as quantum key distribution (QKD) offer provable security guarantees based on the laws of physics, rather than computational assumptions, and represent a fundamentally different approach to secure communication in the quantum era [14–17].

QKD is a foundational quantum cryptography method that enables information-theoretically secure key exchange via quantum principles, e.g. the no-cloning theo-

rem [12, 18]. When combined with one-time pads (OTP), it guarantees unconditional security [14, 19]. However, QKD is fundamentally a system for generating symmetric keys that cannot function securely without a pre-authenticated classical channel [16, 20]. QKD also does not provide the public-private key pairs required by modern asymmetric cryptographic systems, which offers features like nonrepudiation and scalable trust models through infrastructures like Public Key Infrastructure (PKI) [21].

Following QKD, another major branch of quantum communication is Quantum Secure Direct Communication (QSDC) [22–24], which aims to transmit secret messages directly over a quantum channel without first establishing a secret key. This approach promises enhanced efficiency and immediacy by condensing key distribution and ciphertext transmission into a single quantum process [24]. Recent advances have demonstrated its potential, with experimental systems achieving communication over 100 km of fiber [25, 26] and the development of small multi-user networks [27]. However, QSDC is not entirely self-sufficient, as it still fundamentally requires an authenticated classical channel for coordination and eavesdropping detection [23].

While QKD and QSDC aim to secure the transmission process, quantum identity authentication (QIA) and quantum digital signature (QDS) protocols are designed to leverage quantum infrastructure to achieve secure communication [28–30]. Identity authentication is the process of ensuring the identity of the communicating parties, guaranteeing they are who they claim to be [31]. Digital signatures, on the other hand, are designed to ensure the authenticity and integrity of the message itself, providing guarantees that it came from a specific sender and was not altered in transit [32, 33]. Both of

these functions are critically important and constitute the foundation of modern cryptography, which is why developing quantum-resistant versions is a major focus of research.

For QIA, early protocols often relied on the principles of QKD as a foundational layer [22, 23]. The logic was to use the tamper-evident nature of quantum communication to establish trust. However, it is well-established that QKD by itself does not solve the authentication problem; it secures a key exchange but cannot verify the identity of the participants at the outset [15, 20]. Later protocols have attempted to build more sophisticated QIA schemes, sometimes embedding authentication directly into other protocols or combining quantum techniques with classical methods like hash functions [34]. Despite these advances, a common thread persists: the need for a trusted third party or, more fundamentally, a pre-existing authenticated classical channel to bootstrap the process [28]. This dependency is required to prevent man-in-the-middle attacks where an adversary could impersonate a legitimate party during the initial communication.

Quantum digital signature is to use quantum methods to sign on messages, either quantum one-way function [29] or relying on non-locality of Bell state, non-cloning theorem, offering a higher level of security than their classical counterparts. However, QDS protocols face significant practical limitations and dependencies. Early schemes explicitly required a trusted third-party, or “arbitrator,” to validate and authenticate the signed message, creating a central point of failure [35, 36]. More recent protocols, including Measurement-Device-Independent (MDI) schemes, have tried to remove this dependency but still explicitly require authenticated classical channels for coordination [33, 37]. Furthermore, the very nature of a “quantum public key” makes it difficult to manage; the no-cloning theorem makes it physically impossible to freely copy and distribute the key, and many protocols require advanced, and still largely experimental, technology like quantum memory to store the fragile quantum states for verification [38, 39]. Recent research aiming to remove the trusted party has had to introduce other strong assumptions, such as the requirement of an un-tamperable quantum channel for key transmission [32, 40].

In this work, we propose a QIA–QDS protocol that eliminates the need for pre-registration, trusted third parties, and pre-authenticated classical channels. Specifically, in our scheme, each user’s private key is represented by a quantum state, while the corresponding set of local reduced density matrices functions as the public key. The digital signature is realized by encoding classical messages into the global quantum state before transmission, thereby ensuring strong guarantees of message integrity and authenticity. Crucially, the security foundation of our protocol lies in the QMA-completeness of the QMP, also known as the Consistency of Local Density Matrices

(CLDM) problem [41]. The QMA-complete problem analogous to classical NP-complete problems—remains computationally intractable even for quantum computers.

## PRELIMINARIES: THE QUANTUM MARGINAL PROBLEM AND COMPLEXITY

The QMP is a fundamental question concerning the relationship between a whole quantum system and its parts [42, 43]. Formally, given a set of  $n$  particles indexed by the set  $I = \{1, \dots, n\}$ , a collection of index subsets  $J_k \subset I$ , and a corresponding set of density matrices  $\rho_{J_k}$ , the QMP asks for the conditions under which a global state  $\rho_I$  exists such that for all  $k$ ,  $\text{Tr}_{I \setminus J_k}(\rho_I) = \rho_{J_k}$ . This problem is also known as the  $N$ -representability problem in quantum chemistry [44].

For cryptographic purposes, we focus on the associated decision problem, known as the CLDM problem [45]. Throughout this paper, we will use QMP to refer to the general conceptual problem and CLDM to denote the precise computational problem that underpins our security proof.

**Definition 1** (CLDM problem [41]). Consider a system of  $n$  qubits. We are given a collection of local density matrices  $\rho_1, \dots, \rho_m$ , where each  $\rho_i$  acts on a subset of qubits  $C_i \subseteq \{1, \dots, n\}$ . Every matrix entry is specified with  $\text{poly}(n)$  bits of precision. We also have  $m \leq \text{poly}(n)$ , and each subset satisfies  $|C_i| \leq k$  for some constant  $k$ .

In addition, a real number  $\beta$  is provided (again with  $\text{poly}(n)$  bits of precision) such that  $\beta \geq 1/\text{poly}(n)$ .

The task is to distinguish between the following two cases:

YES: There exists an  $n$ -qubit state  $\sigma$  such that, for all  $i$ ,

$$\|\text{Tr}_{\{1, \dots, n\} \setminus C_i}(\sigma) - \rho_i\|_1 = 0.$$

NO: For every  $n$ -qubit state  $\sigma$  there is some  $i$  for which

$$\|\text{Tr}_{\{1, \dots, n\} \setminus C_i}(\sigma) - \rho_i\|_1 \geq \beta.$$

The CLDM problem is known to be QMA-complete, indicating that it is as hard as the most difficult problems verifiable by quantum computation. To clarify this classification, we briefly introduce the QMA complexity class. The complexity class QMA is the quantum analogue of the classical complexity class NP. In the QMA framework, an all-powerful but untrustworthy prover (Merlin) sends a quantum state, or “witness,”  $|\psi\rangle$  to a polynomial-time quantum verifier (Arthur). Arthur performs a verification circuit on the witness and outputs ‘accept’ or ‘reject’. A problem is in QMA if it satisfies two conditions:

**Completeness:** For any YES instance of the problem, there exists a witness state  $|\psi\rangle$  that causes Arthur to accept with high probability (e.g.,  $P(\text{accept}) > 2/3$ ).

**Soundness:** For any NO instance of the problem, every possible witness state causes Arthur to be rejected with high probability (i.e.,  $P(\text{accept}) < 1/3$ ).

The gap between the acceptance probabilities for YES and NO instances is crucial and can be amplified by repeating the protocol. A problem is QMA-complete if it is in QMA and any other problem in QMA can be reduced to it in classical polynomial time.

A remarkable result in quantum complexity theory is that the CLDM problem is QMA-complete [41]. The computational structure of QMA is what makes its complete problems suitable for cryptography. QMA problems are fundamentally promise problems. The verifier is guaranteed that the input instance belongs to one of two disjoint sets: YES instances, for which a "good" proof exists, or NO instances, for which no convincing proof can be constructed. For CLDM problem, this promise manifests as a gap: the given marginals are either highly consistent (a YES case) or any potential global state will be highly inconsistent with at least one of them (a NO case). A cryptographic protocol can exploit this gap to distinguish between legitimate and malicious behavior. An honest user's actions, by design, will correspond to a YES instance of the underlying problem. A successful forgery, as will be shown, would require the creation of a valid witness for a NO instance, an act deemed impossible by the soundness property of QMA. Thus, the promise gap inherent to the complexity class provides the necessary separation for cryptographic security.

## THE QMP-BASED CRYPTOGRAPHIC PROTOCOL

Our protocol consists of three phases that together realize a quantum public-key scheme. In the key generation phase, Alice's private key is a polynomial-depth circuit; her public key is the full set of  $k$ -qubit marginals of the circuit's output state, checkable via local consistency. In the authentication phase, Bob challenges Alice with an arbitrary  $M$ -qubit subset; Alice then returns the corresponding fragment, and Bob verifies its marginals against the public key. In the digital signature phase, Alice encodes a message into a unitary generated from some publicly-known, message-dependent transformation. Alice applies the unitary to the challenged fragment, and any verifier can invert the unitary and test the marginals. The scheme requires no pre-registration. Its security is based on the hardness of reconstructing a highly entangled state from sparse local data.

### Key Generation

To initiate the key generation process, Alice first selects a security parameter  $\lambda$  and constructs a classical description of a quantum circuit  $\text{Circuit}_A$  with depth

$\text{poly}(\lambda)$ . Applying  $\text{Circuit}_A$  to the fixed initial state  $|0\rangle^{\otimes N}$  yields her private key, the  $N$ -qubit state  $\rho_A$ . Once the private key state is prepared, Alice computes all  $k$ -qubit marginals by performing state tomography on each overlapping subsystem of size  $k$ . The resulting set of classical density matrices forms her public key, which she publishes. This workflow starts with Alice using her private circuit to prepare the global state  $\rho_A$ . She then publishes all its  $k$ -qubit reduced states. Anyone can download these marginals and check that they fit together consistently. However, without knowing the exact circuit parameters in  $\text{Circuit}_A$ , rebuilding the full  $N$ -qubit state is believed to be computationally infeasible.

**Alice's Private Key ( $sk_A$ ):** Alice's private key is a classical description of an efficient quantum circuit,  $\text{Circuit}_A$ . This circuit, when applied to a standard initial state like  $|0\rangle^{\otimes N}$ , prepares a specific, highly entangled  $N$ -qubit system. The choice of  $\rho_A$  should be such that it is highly-entangled thus its global entangled structure would be destroyed or only partially exist locally. The generation of large, structured entangled states is an active area of experimental research. The classical description of an efficient quantum circuit,  $\text{Circuit}_A$  is to be used to generate Alice's private key.  $\text{Circuit}_A$  is subject to a security parameter  $\lambda$ . The depth of  $\text{Circuit}_A$  is  $\text{poly}(\lambda)$ .

**Alice's Public Key ( $pk_A$ ):** Alice defines a set of  $k$ -local overlapping subsystems,  $\{C_1, C_2, \dots, C_{\binom{N}{k}}\}$ , where  $C_N^k$  is a combinatorial number and  $S$  is a collection of the indices of qubits in the  $N$ -qubit entangled system  $\rho_A$ . Alice then generates the marginal density matrix for each subsystem by state tomography.

Her public key,  $pk_A$ , is the set of classical descriptions of these  $k$ -local density matrices,  $pk_A = \{\rho_{C_1}, \rho_{C_2}, \dots, \rho_{C_{\binom{N}{k}}}\}$ , which she makes publicly available. By its construction, the set of local density matrices representing Alice's public key is perfectly consistent, with the state  $\rho_A$  serving as the unique global-state witness to this consistency. The pseudocode of key generation is shown as Algorithm 1.

---

### Algorithm1 KEYGEN()

---

**Input:** security parameter  $\lambda$

**Output:** ( $sk_A, pk_A$ )

- 1: Choose a circuit  $\text{Circ}_A$  of  $\text{poly}(\lambda)$  size to prepares an  $N$ -qubit state  $\rho_A$ .
  - 2:  $sk_A = \rho_A$
  - 3: Define  $C_N^k$  subsystems  $\{C_1, C_2, \dots, C_{\binom{N}{k}}\}$ .
  - 4: **for**  $k = 1, \dots, \binom{N}{k}$  **do**
  - 5:   Compute local density matrix  $\rho_{C_k} = \text{Tr}_{\{1, \dots, n\} - C_k}(\rho_A)$
  - 6:   Append local density matrix  $\rho_{C_k}$  to public key  $pk_A$
  - 7: **end for**
  - 8: **return** ( $sk_A, pk_A$ )
-

## Authentication

We design a challenge-response protocol to prove Alice's identity with a verifier Bob.

*Challenge:* In this protocol, Bob first send a challenge to Alice by randomly selecting an  $M$ -qubits subsystem from  $\{1, \dots, N\}$  qubits system of Alice, where  $k < M < N$ . He sends the classical description of all the indices of qubits and send this challenge to Alice. The state Bob asked for is denoted as  $s_M$ , which is a string of indices of corresponding qubits.

*Response:* After receiving the challenge string, Alice uses her private key  $\text{Circuit}_A$  to prepare the state  $\rho_A$ . According to the challenge string  $s_M$ . She then sends the state  $\rho_M$  to Bob as a response.

*Verification:* Bob receives multiple copies of the subsystem state  $\rho_M$  and performs quantum state tomography to reconstruct the corresponding  $k$ -qubit local density matrices, which we denote by  $\rho_{C_k} = \text{Tr}_{\{1, \dots, M\} \setminus C_k}(\rho_M)$ . He then checks each reconstructed marginal against the corresponding public-key marginal  $\rho_{C_k}$  by verifying

$$\frac{1}{2} \|\rho_{C_k} - \rho_{C_k}\|_1 \leq \epsilon,$$

for every  $C_k \subset s_M$  and  $|C_k| = k$ , where  $\epsilon$  is a predetermined acceptance threshold. If every inequality holds, Bob accepts that the responder is Alice, as only she can produce the global state  $\rho_A$  from which these statistics arise.

## Digital Signature

*Signing:* To sign a classical message  $m$ , Alice applies a publicly known, message-dependent, and efficiently invertible unitary transformation  $U_m$  to the state asked by Bob,  $\rho_M$ . In many digital signature protocols, there is a preprocessing process: a plain-texted, arbitrary, unstructured  $x$  is first compressed through a publicly specified cryptographic hash function  $h$ , producing the fixed-length message [46]  $m = h(x)$ . The digest  $m$  is then a standardized message that enters the signature protocol. After transformation, the resulting quantum state,  $\sigma_m = U_m \rho_M$ , then constitutes the quantum digital signature for the message  $m$ . Alice prepares multiple identical copies of  $\sigma_m$  and transmits them to the verifier.

In the following paragraph, we first give a proper definition or to say, limitation on the message that is to be sent, and then give a proper definition for a message-dependent transformation  $U_m$ :

**Definition 2** (Classical messages). Let  $\mathcal{L}$  be a finite, publicly agreed-upon alphabet, say language. A message is a finite word

$$m = m_1 m_2 \dots m_{|m|}, \quad m_j \in \mathcal{L} \ (1 \leq j \leq |m|).$$

Typically  $|m| \leq \gamma$ , where  $\gamma$  is the allowed message length. A simple example is: with  $\mathcal{L} = \{0, 1\}$  we recover ordinary binary strings.

**Definition 3** (Message-dependent unitary  $U_m$ ). A publicly known universal gate set is given to construct quantum circuit and give operation on qubits. Such gate set is

$$\mathcal{G} = \{G_1, G_2, \dots, G_L\}.$$

For every  $i \in \{1, \dots, L\}$  and every  $\ell \in \mathcal{L}$  we specify a unitary  $G_i^{(\ell)}$  via the public rule

$$G_i^{(\ell)} = \begin{cases} \mathbb{I}, & \text{if } \ell \text{ encodes "skip",} \\ G_i, & \text{if } \ell \text{ encodes a non-parametric gate,} \\ G_i(\theta_\ell), & \text{if } G_i \text{ is a rotation and } \ell \mapsto \theta_\ell \in [0, 2\pi). \end{cases}$$

*Construction of  $U_m$ .* Read  $m = m_1 \dots m_{|m|}$  from left to right and assign gates cyclically with  $i(j) = (j \bmod L) + 1$ , rightmost-first-ordered,

$$U_m = \prod_{j=1}^{|m|} G_{i(j)}^{(m_j)}. \quad (1)$$

*Properties.*

- (i) Efficient invertibility.  $U_m^{-1}$  is obtained by reversing the product in (1) and taking adjoints, so both  $U_m$  and  $U_m^{-1}$  have depth  $O(|m|)$ .
- (ii) Injectivity. Different messages change at least one factor in (1); hence the map  $\mathcal{U} : \mathcal{L}^* \rightarrow \text{U}(2^n)$ ,  $m \mapsto U_m$  is injective.
- (iii) Public computability. Because the rule  $(i, \ell) \mapsto G_i^{(\ell)}$  is public, both  $\mathcal{U}$  and its inverse  $\mathcal{U}^{-1}$  are efficiently computable.

During the signing phase Alice applies  $U_m$  from Definition 3 to the challenged subsystem  $\rho_M$ , producing the signature state  $\sigma_m = U_m \rho_M$ . The pseudocode of signing a message by private key is shown as Algorithm 2.

---

### Algorithm2 SIGN( $sk_A, s_M, m$ )

---

**Input:** private key  $sk_A$ , challenge  $s_M$ , message  $m$

**Output:** multiple copies of  $\sigma_m$

- 1: Alice uses  $\text{Circ}_A$  to prepare  $\rho_A$ .
  - 2: Alice uses  $s_M$  and  $\rho_A$  to prepare  $\rho_M$ .
  - 3: Alice applies the public, message-dependent unitary  $U_m$  to get  $\sigma_m = U_m \rho_M$ .
  - 4: Alice outputs multiple copies of  $\sigma_m$ .
- 

*Verification:* Any party in possession of Alice's public key  $pk_A$ , the message  $m$ , and the signature copies  $\sigma_m$  can perform verification. The verifier's goal is to confirm that the received state, when untransformed, has marginals consistent with Alice's public key. To do this, the verifier first applies the inverse transformation  $U_m^{-1}$  to each

copy of the signature, yielding the state  $\sigma'_m = U_m^{-1}\sigma_m$ . Verification then proceeds exactly as in the Authentication procedure, with each instance of  $\rho_M$  replaced by  $\sigma'_m$ . The methods for performing this check are detailed in the Section *Security Analysis*. The pseudocode of verifying a signature is shown as Algorithm 3.

---

**Algorithm3** VERIFY( $pk_A, m, \sigma_m$ )

---

**Input:** public key  $pk_A = \{\rho_{C_1}, \rho_{C_2}, \dots, \rho_{C_{\binom{M}{k}}}\}$ , message  $m$ , signature  $\sigma_m$ , acceptance threshold  $\epsilon$

**Output:** ACCEPT or REJECT

```

1: Verifier construct  $U_m^{-1}$  by message  $m$  and defined rule
2: Verifier reduction the signature state to private key fragment:  $\sigma'_m = U_m^{-1}\sigma_m$ .
3: for  $k = 1, \dots, \binom{M}{k}$  do
4:   Verifier compute  $\sigma_{C_k} = \text{Tr}_{\{1, \dots, M\} \setminus C_k}(\sigma'_m)$ 
5:   if  $\frac{1}{2} \|\rho_{C_k} - \rho_{C_k}\|_1 > \epsilon$  then
6:     return REJECT
7:   end if
8: end for
9: return ACCEPT

```

---

### SECURITY ANALYSIS

After rigorously defining the digital signature and authentication protocol, we need to analyze the security of the proposed scheme. The analysis is to be conducted within the standard cryptographic framework of an adaptive chosen-message attack (CMA), which is extended to accommodate a quantum adversary. The adversary, Eve, is hereby modeled as a quantum polynomial-time algorithm. The security goal of this model is to achieve existential unforgeability (EUF) [47], which asserts that an adversary cannot produce a valid signature for any new message.

The security is defined by the Existential Unforgeability under adaptive quantum Chosen Message Attack (EUF-qCMA) game [48], where a challenger runs Algorithm KEYGEN() to generate a key pair  $(sk_A, pk_A)$  and provides the public key  $pk_A$  to the adversary Eve. Eve is then given oracle access to a signing oracle,  $\mathcal{O}_{\text{Sign}}$ . She can adaptively make a polynomial number of queries, sending messages  $m_1, \dots, m_q$  to the oracle. For each query  $m_i$ , the oracle uses  $sk_A$  to compute the signature  $\sigma_{m_i}$  and returns a set of identical copies to Eve. After the query phase, Eve outputs a message-signature pair  $(m_E, \sigma_E)$ , where  $m_E$  is a message she did not query, i.e.  $m_E \notin \{m_1, \dots, m_q\}$ . Eve wins the game if the VERIFY( $pk_A, m_E, \sigma_E$ ) procedure returns ACCEPT with a probability that is non-negligible in the security parameter.

The signature scheme is considered secure if no quantum polynomial-time adversary can win the EUF-qCMA game with more than negligible probability. As the digital signature scheme is constructed on the identity authentication scheme, the proof of security of the authen-

tication model is also given in This model is a quantum generalization of well-established classical security notions.

### Proof of Unforgeability (Reduction to CLDM problem)

The proof of unforgeability of our protocol proceeds by reduction. We demonstrate that if a quantum polynomial-time adversary E could successfully forge a signature, then we could construct another quantum polynomial-time algorithm F that uses E as a subroutine to solve the QMA-complete CLDM problem [44, 45]. Since CLDM problem is believed to be intractable for quantum computers (that is,  $\text{BQP} \neq \text{QMA}$ ), this implies that no such adversary E can exist.

**Theorem:** The QMP-based digital signature scheme is existentially unforgeable under adaptive chosen-message attacks, assuming  $\text{BQP} \neq \text{QMA}$ .

**Proof:** Assume, for the sake of contradiction, that there exists a quantum polynomial-time adversary E that wins the EUF-qCMA game with non-negligible probability  $\delta$ . We construct an algorithm F to solve a given instance of CLDM problem. Such algorithm F receives an instance of the CLDM problem, which consists of a set of  $k$  local density matrices  $\rho'_{C_k}$  and a promise that this set is either a YES instance (highly consistent) or a NO instance (highly inconsistent). F's task is to decide which is the case. Such algorithm F then initiates the EUF-qCMA game with the forger E and sets the public key for the game to be the CLDM instance it was given:  $pk_E \leftarrow \rho'_{C_k}$ . Using the oracle provided in the EUF-qCMA game, when E queries the signing oracle for a message  $m_i$ , B is faced with a challenge: it cannot generate the signature because it does not know the global state  $\rho_E$  corresponding to the public key (and for a NO instance, no such state exists). However, the reduction cleverly avoids this issue. The security proof does not require B to answer the queries correctly. The existence of a successful forger is assumed regardless of how oracle queries are handled.

After its queries, the adversary E outputs its forgery: a pair  $(m_E, \sigma_E)$  for a new message  $m_E$ . By our initial assumption, this forgery must pass the verification check with non-negligible probability. Algorithm F takes the forged quantum state  $\sigma_E$  and applies the publicly known inverse unitary  $U_{m_E}^{-1}$  to obtain the state  $\sigma'_m = U_{m_E}^{-1}\sigma_E$ . According to the VERIFY algorithm, for the signature to be valid, the marginals of  $\sigma'_m$  must be consistent with the public key  $\rho'_{C_k}$ . This means the state  $\sigma'_m$  is a quantum witness that satisfies the consistency conditions of the original CLDM problem instance provided to F. F can now use  $\sigma'_m$  to solve the CLDM problem. It submits the state  $\sigma'_m$  as a witness to a standard QMA verifier for CLDM. If the original CLDM instance was a NO instance, the soundness property of QMA guaran-

tees that no quantum state can serve as a convincing witness. Therefore, if E produces a forgery, the CLDM instance given to F could not have been a NO instance. If the original CLDM instance was a YES instance, a valid witness exists, and the forger E might succeed.

By observing whether the forger succeeds in producing a valid witness, F can distinguish between YES and NO instances of CLDM problem. E successful forgery by E implies the instance is YES. The absence of a successful forgery (over many runs) implies the instance is NO. This allows F to solve CLDM problem with a non-negligible advantage, which contradicts the assumption that CLDM problem is QMA-complete.

Therefore, the initial assumption must be false: no such polynomial-time quantum adversary E can exist. The signature scheme is secure.

### Authentication Security

The security of the authentication protocol follows a similar logic. An imposter, Eve, attempting to respond to Bob's challenges would need to produce quantum states whose measurement statistics on a subsystem  $C_k$  match those of the public marginal  $\rho_{C_k}$ . To do this successfully for arbitrary challenges across all subsystems, Eve would effectively need to possess a global state consistent with the entire set  $\rho_{C_k}$ . The ability to generate such a state on demand is equivalent to solving the CLDM problem.

### Non-Repudiation and Transferability

The protocol provides essential properties for a digital signature scheme.

**Non-Repudiation:** Alice cannot deny having signed a message  $m$  if a valid signature  $\sigma_m$  exists. The verification process is public and relies only on publicly available information  $(pk_A, m)$ . If VERIFY accepts, it is a mathematical proof that the provided state has the correct properties relative to the public key. The link between Alice's identity and her public key is a prerequisite for any public-key system and is typically handled by a public ledger or directory.

**Transferability:** A recipient, Bob, who has received and verified a signature  $(m, \sigma_m)$ , can forward these to a third party, Victor. Victor can independently perform the same VERIFY procedure using Alice's public key to convince himself of the signature's validity. This transferability is a direct consequence of the public nature of the verification algorithm.

### Necessity of the $k < M < N$ restriction

A fundamental design choice in both the authentication and the signature protocol is that Bob's challenge

never asks Alice to reveal her entire  $N$ -qubit private state. Instead, he selects a random subsystem of size  $M$  with  $k < M < N$ . We justify this restriction with the following lemma.

**Lemma 1** (State & Key-extraction attack). Suppose an adversarial verifier is allowed, in a single session, to demand the full  $N$ -qubit state  $\rho_A$  that serves as Alice's private key. Then after that session the verifier can, with overwhelming probability, impersonate Alice in all future executions of the protocol and forge signatures for arbitrary messages.

*Proof.* Once the adversary receives  $\rho_A$ , it can store the state in a quantum memory and reuse it indefinitely; no inverse transformation or measurement is required. In the authentication protocol, responding to any future challenge merely means measuring the appropriate subsystem of that stored state; hence the adversary's success probability is 1.

For the digital signature protocol, recall that Alice signs a message  $m$  by applying the public efficient invertible unitary  $U_m$  to  $\rho_A$ , producing  $\sigma_m = U_m \rho_M$ , where  $\rho_M$  is generated from  $\rho_A$  and new challenger  $s_M$ . Because the adversary now possesses  $\rho_A$ , it can reproduce exactly the same procedure:

$$\sigma_m^{\text{fake}} = U_m \rho_M.$$

Verification applies  $U_m^{-1}$  and checks the marginals of the resulting state against those published in the public key; the forged state passes with certainty. Hence existential unforgeability is utterly broken once the full  $N$ -qubit key leaves Alice's laboratory.  $\square$

Lemma 1 shows that exposing the entire state would collapse security to the trivial level: Bob (or any malicious verifier) could record  $\rho_A$  and become a perfect clone of Alice. By limiting each challenge to an  $M$ -qubit slice, with  $M$  strictly less than  $N$ , we prevent any single verifier from obtaining enough information to reconstruct the global state, guaranteed by the QMA-completeness of the CLDM problem. Moreover, as the locations of the  $M$  qubits are chosen randomly each time, collecting the full state's all possible subsystem of  $M$  qubits would require  $\binom{N}{M}$  protocol runs, during which Alice would notice the abnormal requests and related key leakage. This subsampling strategy is therefore essential to preserve both impersonation resistance and signature unforgeability while still allowing efficient verification.

### Verification Efficiency and Practical Considerations

The practical viability of this protocol hinges on the efficiency of the VERIFY algorithm. The core task is to check the consistency condition  $\|\text{Tr}_{\{1,2,\dots,(N)}\} - C_k \sigma'_m - \rho_{C_k}\| \leq \epsilon$  for each subsystem  $C_k$ . We analyze two prominent quantum procedures for this task — to use partial Quantum State Tomography (pQST) technique.

*Verification via Partial Quantum State Tomography (pQST)* In this approach, the verifier reconstructs a classical description of the marginals of the received state and compares them to the public key.

For each subsystem  $C_k$ , the verifier uses the provided copies of  $\sigma'_m = U_m^{-1} |\sigma_m\rangle$  to perform quantum state tomography on that  $k$ -qubit subsystem. This yields an estimate of the local subsystem  $\rho_{C'_k}$ . The verifier then classically computes a distance metric, such as the trace distance, between the reconstructed local density matrix  $\rho_{C'_k}$  and the public key subsystem  $\rho_{C_k}$ .

*Resource Consumption:* While full tomography of an  $N$ -qubit state is infeasible, scaling exponentially with  $N$ , pQST is only performed on small,  $k$ -qubit subsystems. The number of state copies required to achieve a precision  $\epsilon$  for a  $d$ -dimensional system ( $d = 2^k$ ) scales as  $\mathcal{O}(d^2/\epsilon^2) = \mathcal{O}(4^k/\epsilon^2)$  [49]. For a small and fixed subsystem size  $k$ , this is efficient. The total cost is polynomial in the number of local subsystems.

In the realistic implementation, the quantum states used in our protocol will be subject to decoherence due to environmental interactions and operational imperfections. Such noise will affect both Alice’s preparation of her private state and the transmission of the signature state to the verifier. As a result, even an honest signature will not pass a perfect verification check.

The protocol must therefore incorporate an error threshold. The verifier will accept a signature if the measured inconsistency is below a threshold. This threshold must be carefully calibrated: it must be large enough to tolerate the expected level of natural decoherence but small enough to reliably detect malicious modifications that would constitute a forgery. Ultimately, for the protocol to be truly scalable and secure over long distances or long computational times, it may be implemented using logical qubits protected by a Quantum Error Correction (QEC) code. QEC schemes encode the information of a single logical qubit across many physical qubits, allowing for the detection and correction of errors. The security analysis presented in this paper assumes ideal, error-free qubits and serves as the theoretical foundation upon which a fault-tolerant version of the protocol can be built.

## DISCUSSION

This work has introduced a novel framework for public-key quantum cryptography based on the computational hardness of the quantum marginal problem. The resulting authentication and digital signature protocol is, to our knowledge, the first to leverage the QMA-completeness of a natural physical problem to achieve security.

The protocol’s principal advantage is its self-contained and decentralized nature. It successfully establishes a true public-key system-without any reliance on trusted

third parties, pre-shared secrets between users, or pre-authenticated classical channels for the distribution of public keys. This represents a significant step toward building scalable quantum networks where trust can be established dynamically and securely based on the laws of quantum mechanics and computational complexity. The security is proven to be robust, with existential unforgeability against adaptive chosen-message attacks by quantum adversaries reducible to the intractability of the CLDM problem.

Based on this new formalism of quantum cryptography, we hereby propose several promising avenues for future research based on our protocol. First, the protocol can be optimized by exploring different families of global states  $\rho$  and different configurations of overlapping subsystems  $\{C_k\}$  to find the ideal balance between the strength of the security assumption and the resource costs of key generation and verification. Second, a small-scale proof-of-principle experiment on current noisy intermediate-scale quantum (NISQ) hardware is a direct next step. Such an experiment could involve generating appropriate quantum state as private key, distributing its local subsystems as a public key, and performing the verification steps to demonstrate the protocol’s core mechanics, even in the presence of noise. Finally, the core methodology—using the hardness of a QMA-complete problem as a cryptographic primitive—could be applied to other quantum-computationally hard problems, including estimating the ground-state energy of specific local Hamiltonians or verifying properties of quantum circuits, potentially leading to new cryptographic functionalities with different security and efficiency profiles.

- 
- [1] P. W. Shor, Algorithms for quantum computation: Discrete logarithms and factoring, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (IEEE, 1994) pp. 124–134.
  - [2] M. Mosca, Cybersecurity in an era with quantum computers: Will we be ready?, *IEEE Security & Privacy* **16**, 38 (2018).
  - [3] R. L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM* **21**, 120 (1978).
  - [4] V. S. Miller, Use of elliptic curves in cryptography, in *Advances in Cryptology — CRYPTO '85, Santa Barbara, California, USA, August 18–22, 1985, Proceedings*, Lecture Notes in Computer Science, Vol. 218 (Springer, 1985) pp. 417–426.
  - [5] N. Koblitz, Elliptic curve cryptosystems, *Mathematics of Computation* **48**, 203 (1987).
  - [6] L. K. Grover, A fast quantum mechanical algorithm for database search, in *Proceedings of the 28th Annual ACM Symposium on Theory of Computing* (ACM, 1996) pp. 212–219.
  - [7] D. J. Bernstein and T. Lange, *Post-Quantum Cryptography: Dealing with the Fallout of Physics Success*, Tech. Rep. 2017/314 (IACR Cryptology ePrint Archive, 2017).

- [8] D. J. Bernstein and T. Lange, Post-quantum cryptography: dealing with the fallout of physics success, IACR Cryptology ePrint Archive (2017), preprint, minor revision. Received 2017-04-14.
- [9] D. Micciancio and O. Regev, Lattice-based cryptography, in *Encyclopedia of Cryptography and Security* (Springer, 2011) pp. 713–715.
- [10] R. Overbeck and N. Sendrier, Code-based cryptography, in *Post-quantum cryptography* (Springer, 2009) pp. 95–145.
- [11] K. Sakumoto, T. Shirai, and H. Hiwatari, Public-key identification schemes based on multivariate quadratic polynomials, in *Advances in Cryptology—CRYPTO 2011: 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14–18, 2011. Proceedings 31* (Springer, 2011) pp. 706–723.
- [12] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, *Reviews of Modern Physics* **74**, 145 (2002).
- [13] C. Portmann and R. Renner, Security in quantum cryptography, *Reviews of Modern Physics* **94**, 025008 (2022).
- [14] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, 1984) pp. 175–179.
- [15] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, *Reviews of Modern Physics* **81**, 1301 (2009).
- [16] R. Renner, Security of quantum key distribution, *International Journal of Quantum Information* **6**, 1 (2008).
- [17] P. W. Shor and J. Preskill, Simple proof of security of the bb84 quantum key distribution protocol, *Physical review letters* **85**, 441 (2000).
- [18] W. K. Wootters and W. H. Zurek, A single quantum cannot be cloned, *Nature* **299**, 802 (1982).
- [19] G. S. Vernam, Cipher printing telegraph systems: For secret wire and radio telegraphic communications, *Journal of the A.I.E.E.* **45**, 109 (1926).
- [20] D. Mayers, Unconditional security in quantum cryptography, *Journal of the ACM* **48**, 351 (1998).
- [21] W. Diffie and M. E. Hellman, New directions in cryptography, *IEEE Transactions on Information Theory* **22**, 644 (1976).
- [22] K. Boström and T. Felbinger, Deterministic secure direct communication using entanglement, *Physical Review Letters* **89**, 187902 (2002).
- [23] F.-G. Deng and G.-L. Long, Secure direct communication with a quantum one-time pad, *Physical Review A* **69**, 052319 (2004).
- [24] G.-L. Long, F.-G. Deng, Y. Li, K.-W. Wen, and C.-Y. Wang, Quantum secure direct communication and deterministic secure quantum communication, *Frontiers of Physics in China* **2**, 251 (2007).
- [25] W. Zhang, D.-S. Ding, Y.-B. Sheng, L. Zhou, B.-S. Shi, and G.-C. Guo, Quantum secure direct communication with quantum memory, *Phys. Rev. Lett.* **118**, 220501 (2017).
- [26] H. Zhang, Z. Sun, R. Qi, and et al., Realization of quantum secure direct communication over 100km fiber with time-bin and phase quantum states, *Light: Science & Applications* **11**, 83 (2022).
- [27] Z. Qi, Y. Li, Y. Huang, et al., A 15-user quantum secure direct communication network, *Light: Science & Applications* **10**, 183 (2021).
- [28] H. Barnum, C. Crépeau, D. Gottesman, A. Smith, and A. Tapp, Authentication of quantum messages, in *Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science* (2002) pp. 449–458.
- [29] D. Gottesman and I. L. Chuang, Quantum digital signatures, arXiv preprint arXiv:quant-ph/0105032 (2001).
- [30] P. Wallden, V. Dunjko, A. Kent, and E. Andersson, Quantum digital signatures with quantum key distribution components, *Physical Review A* **91**, 042304 (2015), also available at arXiv:1403.5551v2.
- [31] Z.-j. Zhang and Z.-x. Man, Multiparty quantum secret sharing of classical messages based on entanglement swapping, *Phys. Rev. A* **72**, 022303 (2005).
- [32] V. Dunjko, P. Wallden, and E. Andersson, Quantum digital signatures without quantum memory, *Physical Review Letters* **112**, 040502 (2014).
- [33] G. L. Roberts, M. Lucamarini, Z. L. Yuan, et al., Experimental measurement-device-independent quantum digital signatures, *Nature Communications* **8**, 1098 (2017).
- [34] Y. Du, Y. Liu, C. Yang, X. Zheng, S. Zhu, and X.-s. Ma, Experimental measurement-device-independent quantum cryptographic conferencing, *Phys. Rev. Lett.* **134**, 040802 (2025).
- [35] H.-K. Lo and J. Preskill, Security of quantum key distribution using weak coherent states with nonrandom phases (2006), submitted on 23 Oct 2006 (v1), last revised 2 Jan 2007 (v2), arXiv:quant-ph/0610203 [quant-ph].
- [36] R. Amiri and J. M. Arrazola, Secure quantum signatures using insecure quantum channels, *Physical Review A* **93**, 032325 (2016).
- [37] I. V. Puthoor, R. Amiri, P. Wallden, M. Curty, and E. Andersson, Measurement-device-independent quantum digital signatures, *Phys. Rev. A* **94**, 022328 (2016).
- [38] A. I. Lvovsky, B. C. Sanders, and W. Tittel, Optical quantum memory, *Nature Photonics* **3**, 706 (2009).
- [39] K. Heshami, D. England, and P. C. e. a. Humphreys, Quantum memories: emerging applications and recent advances, *Journal of Modern Optics* **63**, 2005 (2016).
- [40] R. J. Collins, R. J. Donaldson, V. Dunjko, P. Wallden, P. J. Clarke, E. Andersson, J. Jeffers, and G. S. Buller, Realization of quantum digital signatures without the requirement of quantum memory, *Phys. Rev. Lett.* **113**, 040502 (2014).
- [41] Y.-K. Liu, Consistency of local density matrices is qma-complete (2006), last revised Dec 2007, version 3, arXiv:quant-ph/0604166 [quant-ph].
- [42] A. J. Coleman, Structure of fermion density matrices, *Reviews of Modern Physics* **35**, 668 (1963).
- [43] A. A. Klyachko, Quantum marginal problem and  $N$ -representability, in *Proceedings of the International Symposium on Advanced Quantum Theory* (World Scientific, 2006) pp. 3–21.
- [44] Y. Liu, M. Christandl, and F. Verstraete, Quantum computational complexity of the  $N$ -representability problem: QMA-complete, *Physical Review Letters* **98**, 110503 (2007).
- [45] J. Kempe, A. Kitaev, and O. Regev, The complexity of the local hamiltonian problem, *SIAM Journal on Computing* **35**, 1070 (2006).
- [46] B. Preneel, Cryptographic hash functions, *European Transactions on Telecommunications* **5**, 431 (1994).
- [47] S. Goldwasser, S. Micali, and R. L. Rivest, A digital signature scheme secure against adaptive chosen-message attacks, *SIAM Journal on Computing* **17**, 281 (1988).

- [48] D. Boneh and M. Zhandry, Secure signatures and chosen ciphertext security in a quantum computing world, in *Advances in Cryptology-CRYPTO 2013*, Lecture Notes in Computer Science, Vol. 8042 (Springer, 2013) pp. 361–379.
- [49] M. G. A. Paris and J. Reháček, *Quantum State Estimation*, Lecture Notes in Physics, Vol. 649 (Springer, 2004).