UNIVERSITY OF HONG KONG
HK INSTITUTE OF QUANTUM SCIENCE & TECHNOLOGY

Public-Key Quantum Authentication and Digital Signature Schemes

Based on Quantum Marginal Problem

Liu Leran

Contact Information:
Room 616, Department of Physics
The University of Hong Kong

Phone: +852 60965082
Email: leran@connect.hku.hk

Abstract

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

Quantum identity authentication (QIA) and quantum digital signature (QDS) protocols are designed to leverage quantum infrastructure to achieve secure communication. Identity authentication is the process of ensuring the identity of the communicating parties, guaranteeing they are who they claim to be. 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. 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 [3]. 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 Quantum marginal problem (QMP) is a fundamental question concerning the relationship between a whole quantum system and its parts [4]. Formally, given a set of n particles indexed by the set $I = \{1, \ldots, n\}$, a collection of index subsets $J_k \subset I$, and a corresponding set of density matrices ρ_{J_k}, the QMP asks for the conditions under which a global state ρ_I exists such that for all k, $\mathrm{Tr}_{I\setminus J_k}(\rho_I) = \rho_{J_k}$.

For cryptographic purposes, we focus on the associated decision problem, known as the CLDM problem.

Definition 1 (CLDM problem [3])**.** Consider a system of n qubits. We are given a collection of local density matrices $\rho_1, \ldots, \rho_m$, where each ρ_i acts on a subset of qubits $C_i \subseteq \{1, \ldots, n\}$. Every matrix entry is specified with $\mathrm{poly}(n)$ bits of precision. We also have $m \leq \mathrm{poly}(n)$, and each subset satisfies $|C_i| \leq k$ for some constant k.

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

The task is to distinguish between the following two cases:

YES: There exists an n-qubit state σ such that, for all i,

$$\left\|\mathrm{Tr}_{\{1,\ldots,n\}\setminus C_i}(\sigma) - \rho_i\right\|_1 = 0.$$

NO: For every n-qubit state σ there is some i for which

$$\left\|\mathrm{Tr}_{\{1,\ldots,n\}\setminus C_i}(\sigma) - \rho_i\right\|_1 \geq \beta.$$

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 [1]. 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:

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. A;ice 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 λ and constructs a classical description of a quantum circuit $\mathrm{Circuit}_A$ with depth $\mathrm{poly}(\lambda)$. Applying $\mathrm{Circuit}_A$ to the fixed initial state $|0\rangle^{\otimes N}$ yields her private key, the N-qubit state ρ_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 ρ_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 $\mathrm{Circuit}_A$, 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, $\mathrm{Circuit}_A$. 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 ρ_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, $\mathrm{Circuit}_A$ is to be used to generate Alice's private key. $\mathrm{Circuit}_A$ is subject to a security parameter λ. The depth of $\mathrm{Circuit}_A$ is $\mathrm{poly}(\lambda)$.

Alice's Public Key (pk_A): Alice defines a set of k-local overlapping subsystems, $\{C_1, C_2, \ldots, C_{\binom{N}{k}}\}$, where C_N^k is a combinatorial number and S is a collection of the indices of qubits in the N-qubit entangled system ρ_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, $pk_\mathrm{A} = \{\rho_{C_1}, \rho_{C_2}, \ldots, \rho_{C_{\binom{N}{k}}}\}$, 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 ρ_A serving as the unique global-state witness to this consistency. The pseudocode of key generation is shown as the below algorithm.

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 $\{1, \ldots, N\}$ 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 $\mathrm{Circuit}_A$ to prepare the state ρ_A. According to the challenge string s_M. She then sends the state ρ_M to Bob as a response.

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

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

for every $C_k \subset s_M$ and $|C_k| = k$, where ϵ is a predetermined acceptance threshold. If every inequality holds, Bob accepts that the responder is Alice, as only she can produce the global state ρ_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, ρ_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 $m = h(x)$. 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 σ_m and transmits them to the verifier.

During the signing phase Alice applies U_m to the challenged subsystem ρ_M, producing the signature state $\sigma_m = U_m \rho_M$.

Verification: Any party in possession of Alice's public key pk_A, the message m, and the signature copies σ_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 ρ_M replaced by σ'_m. The methods for performing this check are detailed in the Section *Security Analysis* in the arxiv paper [2].

Conclusions

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.

References

[1] Julia Kempe, Alexei Kitaev, and Oded Regev. The complexity of the local hamiltonian problem. *SIAM Journal on Computing*, 35(5):1070–1097, 2006.

[2] Le-Ran Liu, Min-Quan He, Dan-Bo Zhang, and Z. D. Wang. Public-key quantum authentication and digital signature schemes based on the qma-complete problem, 2025.

[3] Yi-Kai Liu. Consistency of local density matrices is qma-complete, 2006. Last revised Dec 2007, version 3.

[4] Christian Schilling. The quantum marginal problem. *arXiv preprint arXiv:1404.1085*, 2014.