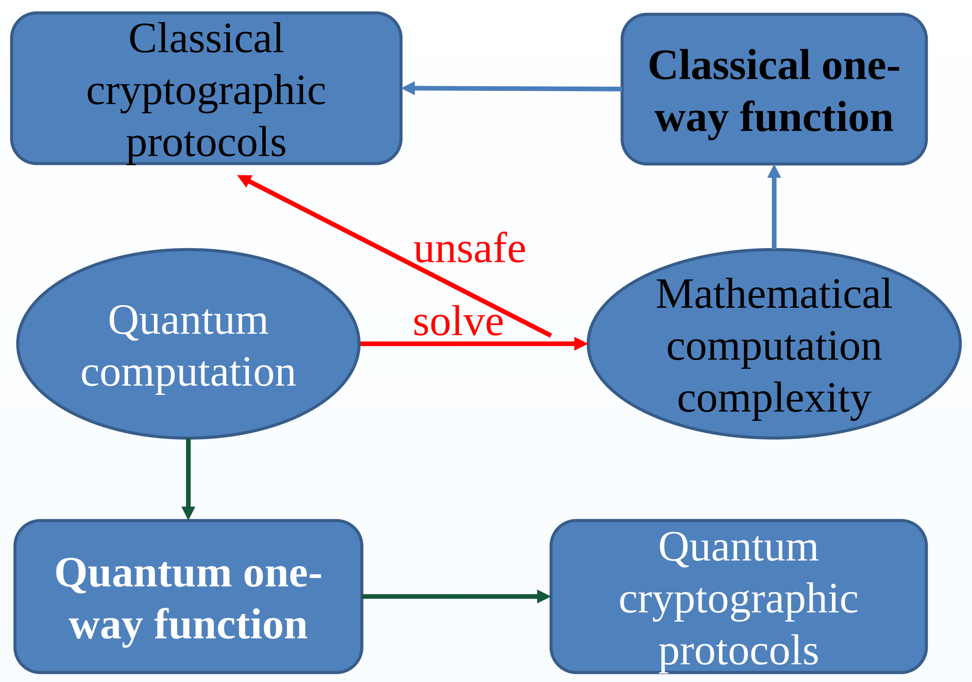
Full Quantum One-way Function for Quantum Cryptography

Tao Shang[1], Yao Tang[1], Ranyiliu Chen[2], and Jianwei Liu[1]
1. School of Cyber Science and Technology, Beihang University, Beijing, CHINA,100191
2. School of Electronic & Information Engineering, Beihang University, Beijing, CHINA,100191
Email: shangtao@buaa.edu.cn

BACKGROUND

One-way function(OWF) quantum vs classical



Quantum one-way function can be applied to quantum cryptographic protocols to ensure the security under quantum adversary.

Quantum one-way function

function: input → output

'Classical-Classical' OWF: $x \to f(x)$	'Classical-Quantum' OWF: $x \to U_x\|0\rangle$
'Quantum-Classical' OWF: $\|x\rangle \to F\|x\rangle$	'Quantum-Quantum' OWF: ?

Accord to input and output form, there is no quantum-quantum' OWF. It is feasible to conceive a one-way function of 'quantum-quantum' mode.

Quantum identify authentication scheme

- The identity authentication enables a prover to gain access to a verifier's resource by submitting credentials to the verifier.
- A challenge-response mode identity authentication can resist active attacks, like verifier-impersonation attack.

MOTIVATION

To further study quantum one-way function, we focus on the design of a full quantum one-way function which is 'quantum-quantum' and consider its application in quantum cryptography.

FULL QUANTUM ONE-WAY FUNCTION

1. Definition

- full quantum one-way function

The full quantum one-way function maps a n−qubit GCH state to a 1−qubit superposition state, i.e.,

$$F: |\psi^n\rangle_{GCH} \to H^2$$

- Algorithm

Step 1. use F_{qc} to extract classical information from $|\psi\rangle$, i.e., $c = F_{qc}|\psi\rangle, c \in \{0,1\}^n$;

where $F_{qc} = |\phi^{(n)}\rangle_{GCH} \to \{0,1\}^n$.

Step 2. rotate the single qubit $|0\rangle$ with angle θ_c according to the obtained classical information c, then calculate Fcq to get the quantum output $F|\psi\rangle$.

$$F|\psi\rangle = F_{cq}(c) = \cos\frac{\theta_c}{2}|0\rangle + \sin\frac{\theta_c}{2}|1\rangle, \quad \theta_c = \frac{c}{2^n}\bullet 2\pi$$

where $F_{cq}(c) = \hat{R}_y(\theta_c)|0\rangle = \cos\frac{\theta_c}{2}|0\rangle + \sin\frac{\theta_c}{2}|1\rangle$.

2. One-wayness

- easy to compute

This property can be analyzed by the time complexity of the full quantum one-way function F. The time complexity of full quantum one-way function F can be measured by the number of used quantum gates in full quantum one-way function F .

For step 1, the number of CNOT gates used by function Fqc is $Y_{qc} \le (n^3 + n^2)/2$.

For step2, it need $O(\log^C(\frac{1}{\varepsilon}))$ universal quantum gates to do single-bit rotation.

The time complexity of the full quantum one-way function F, is $O(F)_{n,\varepsilon} = O(n^3 + \log^C(\frac{1}{\varepsilon}))$.

- hard to invert

By the counter-evidence method, we prove that Given an arbitrary output result $F|\psi\rangle$ of the full quantum one-way function F, for any quantum polynomial time adversary A, the probability of A inverting F is negligible, i.e.

$$\Pr\left[A(F|\psi\rangle) = |\psi\rangle\right] \le \mathrm{negl}(n)$$

- conclusion

The full quantum one-way function F, whose input and output are both quantum states, is "easy to compute" but "hard to invert" in quantum polynomial time.

FULL QUANTUM IDETITY AUTHENTICATION NSCHEME

1. Scheme

Participants: prover and verifier.

Step 1. the prover chooses a GCH state as its private key $|sk\rangle$. It takes $|sk\rangle$ as the input of the full quantum one-way function F and then creates a set of verification key $|vk\rangle = F|sk\rangle$. The prover places the verification key on a trusted platform.

Step 2. the verifier has a message $|m\rangle$, where $|m\rangle = \cos\frac{\theta_m}{2}|0\rangle + \sin\frac{\theta_m}{2}|1\rangle$, $m \in \{0,1\}^n$ and $\theta_m = \frac{m}{2^n}\bullet 2\pi$.
The verifier sends $|m\rangle$ to the prover.

Step 3. the prover uses the private key $|sk\rangle$ to calculate Fcq to get c. Then it performs a rotation operation on the received message $|m\rangle$ as follows

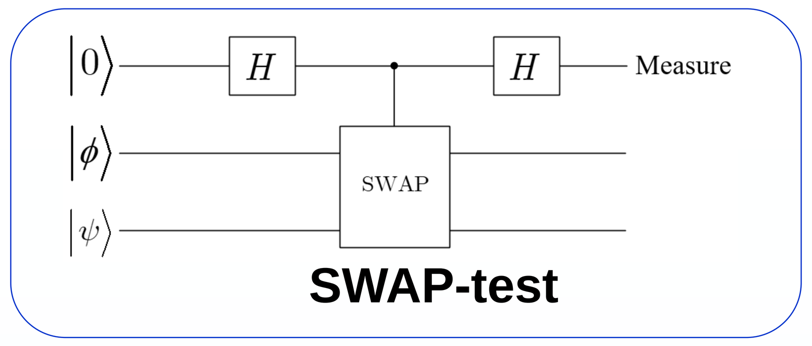
$\hat{R}_y(\theta_c)|m\rangle$, where $\theta_c = \frac{c}{2^n}\bullet 2\pi$.

The result of the rotation is

$$\hat{R}_y(\theta_c|m\rangle) = \cos\frac{\theta_c + \theta_m}{2}|0\rangle + \sin\frac{\theta_c + \theta_m}{2}|1\rangle$$

The result is recorded as $|P\rangle$. Then prover sends $|P\rangle$ to the verifier.

Step 4. the verifier receives $|P\rangle$. It applies a $-\theta_m$ rotation and denotes the result as $|P_s\rangle$. The verifier uses the SWAP-test to compare $|P_s\rangle$ with the prover's verification key $|vk\rangle$. If $|vk\rangle = |P_s\rangle$, it completes the verification of the prover.



SWAP-test

2. Security analysis

- Attack game

Key generation: the challenger runs G to generate secret key $|sk\rangle$ and verification key $|vk\rangle = F|sk\rangle$, where F is the full quantum one-way function. The challenger sends sufficient copies of $|vk\rangle$ to the adversary A.

Verifier impersonation: A in this phase impersonates the verifier to interact with the challenger. A queries the challenger with single qubit $|a_i\rangle$, and gets responses $\hat{R}_y\ c/2^n \bullet 2\pi\ |a_i\rangle$, where $c = F_{qc}|sk\rangle$.

Prover impersonation: the challenger in this phase randomly $|m\rangle = \hat{R}_y\ m/2^n \bullet 2\pi\ |0\rangle$ and sends it to A. With A's response $|P_m\rangle$, the challenger runs $\hat{R}_y(-\theta_m)|P_m\rangle$ and compares the result and $|vk\rangle$ using SWAP-test. The challenger repeats this phase p times and outputs 'accept' only if all SWAP-test results are $|0\rangle$.

- **Advantage:** $\Pr$ *the challengr output 'accept'* $\le 1/2^p$

Thus, the full quantum identity authentication scheme is secure against verifier-impersonation attack.

3. Effect of noisy channels

- In a quantum channel, the noise will make quantum identity authentication scheme insecure.
- Improvement method
  Method 1: quantum error correction code.
  Method 2: change the challenge-response mode and threshold for error.

CONCLUSION

In this paper, we proposed full one-way function and then applied it to the quantum identity authentication scheme. The attack game showed that this quantum identity authentication scheme is secure against verifier-impersonation attack.