### Full Quantum One-way Function for Quantum Cryptography

**Tao Shang**, **Yao Tang**, **Ranyiliu Chen**, **Jianwei Liu**
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)**

<table>
<thead>
<tr>
<th>Classical cryptographic protocols</th>
<th>Classical one-way function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quantum computation</td>
<td>Mathematical computation complexity</td>
</tr>
<tr>
<td>Quantum one-way function</td>
<td>Quantum cryptographic protocols</td>
</tr>
</tbody>
</table>

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

---

#### 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.,
     \[
     F: |\psi\rangle \rightarrow |\varphi\rangle
     \]
   - **Algorithm**
     - **Step 1.** use $F_{c}$ to extract classical information from $|\psi\rangle$, i.e., $c = F_{c}(|\psi\rangle), c \in \{0,1\}^{n}$
       - where $F_{c} = F_{c}(|\psi\rangle) \in \{0,1\}$
     - **Step 2.** rotate the single qubit $|0\rangle$ with angle $\theta$ according to the obtained classical information $c$, then calculate $F_{\varphi}$ to get the quantum output $F_{\varphi}$.
       - $F_{\varphi} = F_{\varphi}(c) = \cos \frac{2\theta}{2} |0\rangle + \sin \frac{2\theta}{2} |1\rangle$
       - $\theta = \frac{\pi}{2^{2^{m,n}}}$
       - where $F_{\varphi} = F_{\varphi}(\theta)(|0\rangle) = \cos \frac{\theta}{2} |0\rangle + \sin \frac{\theta}{2} |1\rangle$.

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 $F_{QC}$ is $T_{QC} \leq (n^{2} + n^{2})/2$.
     - For step 2, it need $O(\log^{2} \frac{1}{\varepsilon})$ universal quantum gates to do single-bit rotation.
     - The time complexity of the full quantum one-way function $F$, is $O(T) = O(\log^{2} \frac{1}{\varepsilon})$.

---

#### FULL QUANTUM IDENTIFICATION AUTHENTICATION NSCHEME

1. **Scheme**
   - **Participants:** prover and verifier.
     - **Step 1.** the prover chooses a GCH state as its private key $|\psi\rangle$. It takes $|\psi\rangle$ as the input of the full quantum one-way function $F$ and then creates a set of verification key $|\hat{y}\rangle = F(|\psi\rangle)$. The prover places the verification key on a trusted platform.
     - **Step 2.** the verifier has a message $|m\rangle$, where $|m\rangle = \cos \frac{2\theta}{2} |0\rangle + \sin \frac{2\theta}{2} |1\rangle$ and $\theta = \frac{\pi}{2^{2^{m,n}}}$.
     - The verifier sends $|m\rangle$ to the prover.
     - **Step 3.** the prover uses the private key $|\psi\rangle$ to calculate $F_{QC}$ to get $c$. Then it performs a rotation operation on the received message $|m\rangle$ as follows
       - $k_{c}(|0\rangle) = |c\rangle$.
       - $k_{c}(|m\rangle) = k_{c}(|0\rangle) - \frac{\lambda_{c} + \theta_{c}}{2} |1\rangle$.
     - The result is recorded as $|\hat{y}\rangle$. Then prover sends $|\hat{y}\rangle$ to the verifier.
     - **Step 4.** the verifier receives $|\hat{y}\rangle$. It applies a _$-d_{c}$_ rotation and denotes the result as $|\hat{y}\rangle$. The verifier uses the SWAP test to compare $|\hat{y}\rangle$ with the prover’s verification key $|\hat{y}\rangle$. If $|\hat{y}\rangle = |\hat{y}\rangle$, it completes the verification of the prover.

---

#### 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.