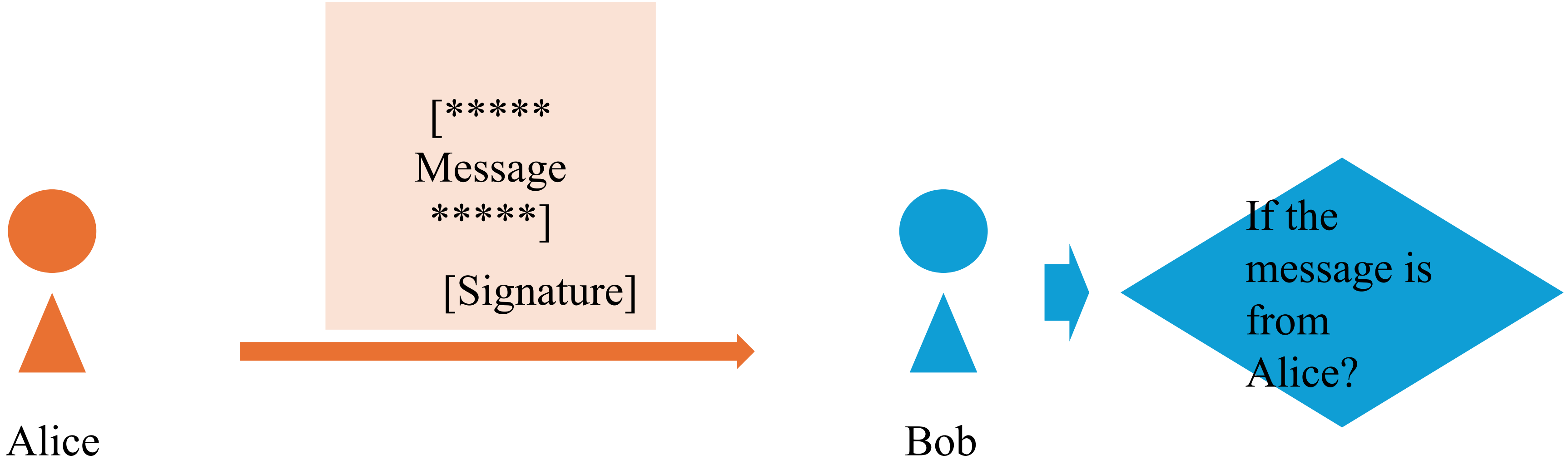
Quantum digital signature based on single-qubit without a trusted third-party

Authors: W. Wang, M. Hayashi

Background

- Digital signatures are fundamental for authenticity.
- Many quantum signature schemes still rely on a *trusted third-party* — this breaks decentralization.



[***** Message *****]

[Signature]

Alice

Bob

If the message is from Alice?

Figure 1. The task of digital signature.

- **Definition for quantum digital signature**

- Key generation phase

Alice performs $SKGen(1^{\lambda})$ to generate a private key sk, where λ is the security parameter, subsequently performs $PKGen(sk)$ to generate a quantum public key ρ_{pk}, then she sends ρ_{pk} to Bob.

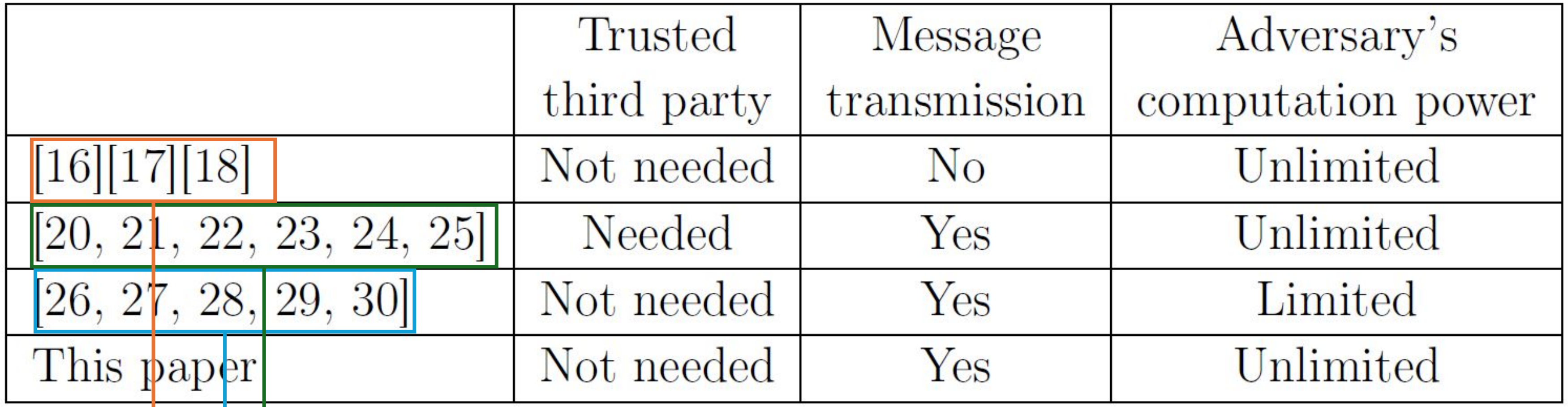
- Signing phase

Alice performs $Sign(sk, m)$ to generate a classical signature sgn, where m is the message, then sends (m, sgn) to Bob.

- Verification phase

Bob performs $Ver(pk, m, sgn)$ to generate 0(reject the signature) or 1(accept the signature).

- Comparison with existing studies:



	Trusted third party	Message transmission	Adversary's computation power
[16][17][18]	Not needed	No	Unlimited
[20, 21, 22, 23, 24, 25]	Needed	Yes	Unlimited
[26, 27, 28, 29, 30]	Not needed	Yes	Limited
This paper	Not needed	Yes	Unlimited

- Authentications based on quantum physically unclonable functions.
- Quantum digital signatures with a trusted third-party.
- General quantum digital signature frameworks.

- Forging attack

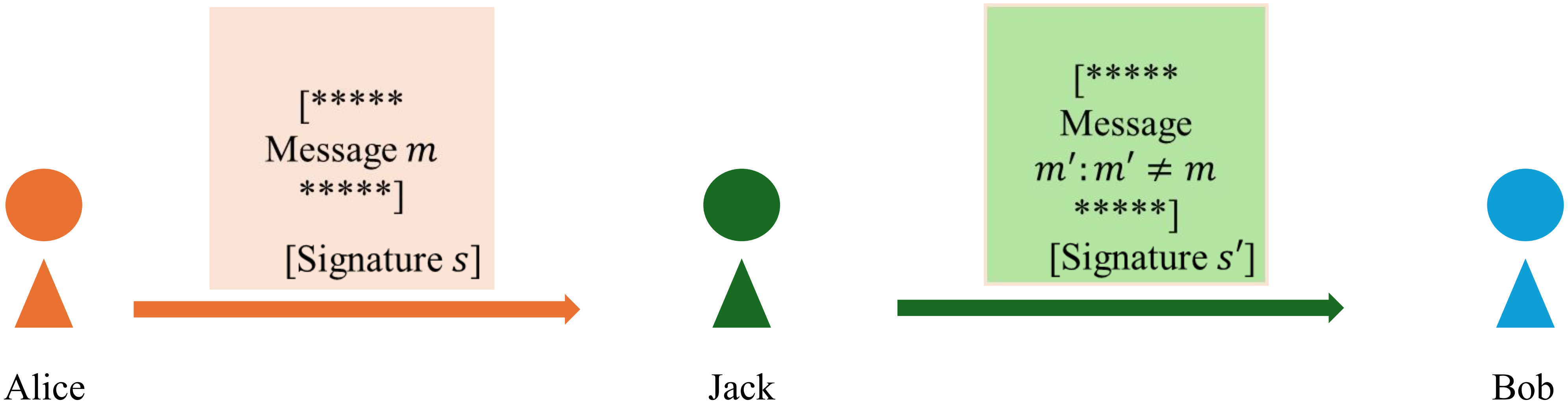


Figure 2. The schematic of the forging attack.

Requirements

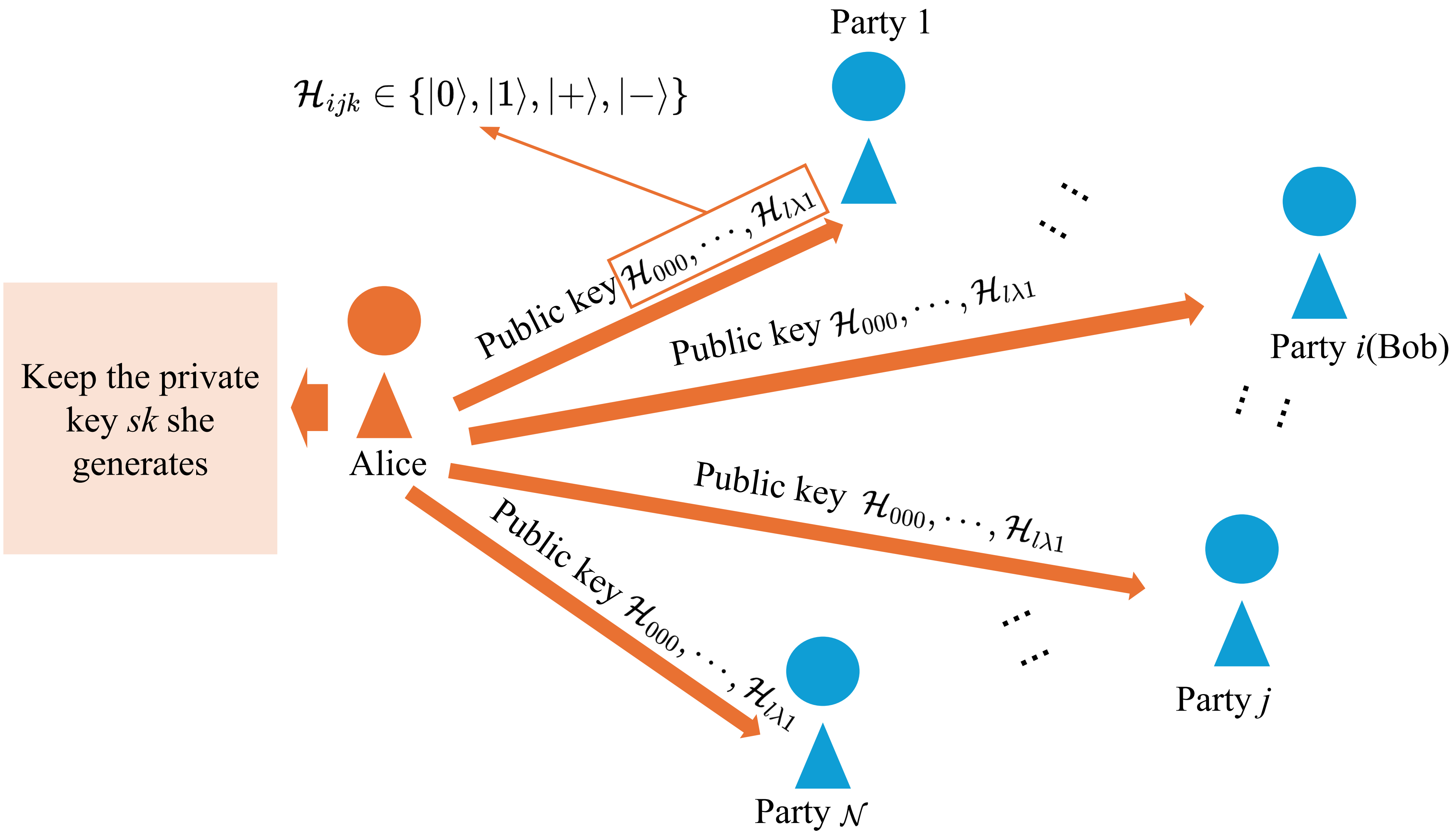
- A specific quantum digital signature protocol satisfying the following requirements is proposed:

1. A trusted third-party is not needed in the protocol.
2. **Theoretic (k, ϵ)-unforgeability**: A party in the protocol holds k-copies of the public key succeeds forging attacks with at most the probability of ϵ.
3. **Undeniability**: The signer cannot make the verifier to reject the signature.
4. **Expandability**: The cost of the protocol does not increase so fast as the length of the message increases.

Our protocol

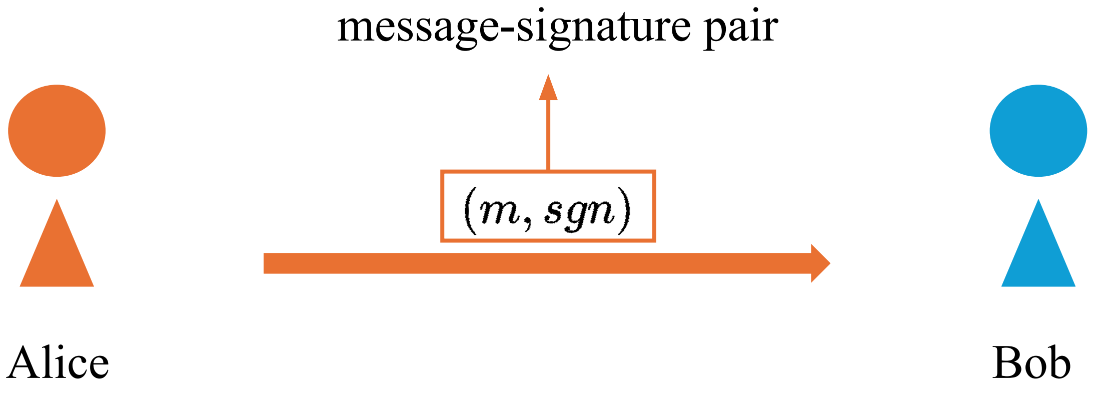
- We assume that the message needed to be authenticated is a l-bit message $m = m_1 \cdots m_l$. Our protocol uses the following algorithms:

1. $SKGen(1^\lambda) \rightarrow sk = \{B_{ijk}, V_{ijk}\}_{ijk}$, where
$$i \in \{1, \cdots, l\}, j \in \{1, \cdots, \lambda\}, k \in \{0, 1\}, B_{ijk} \in \{X, Z\}, V_{ijk} \in \{1, -1\}.$$
2. $PKGen(sk) \rightarrow pk = \{\mathcal{H}_{ijk}\}_{ijk}$, where $\mathcal{H}_{ijk} \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}.$
3. $Sign(sk, m) \rightarrow sgn = \{B_{ijm_i}, V_{ijm_i}\}_{ij}$.
4. $Ver(pk, m, sgn) \rightarrow 1/0$.



$\mathcal{H}_{ijk} \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$
Party 1
Party i(Bob)
Party j
Party $\mathcal{N}$
Alice
Keep the private key *sk* she generates
Public key $\mathcal{H}_{000}, \cdots, \mathcal{H}_{l\lambda 1}$
Public key $\mathcal{H}_{000}, \cdots, \mathcal{H}_{l\lambda 1}$
Public key $\mathcal{H}_{000}, \cdots, \mathcal{H}_{l\lambda 1}$
Public key $\mathcal{H}_{000}, \cdots, \mathcal{H}_{l\lambda 1}$

Figure 3: Key generation phase.


message-signature pair

(m, sgn)

Alice

Bob

Figure 4: Signing phase.

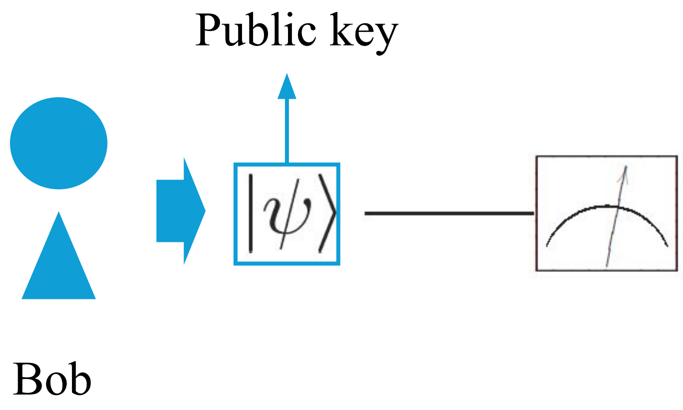
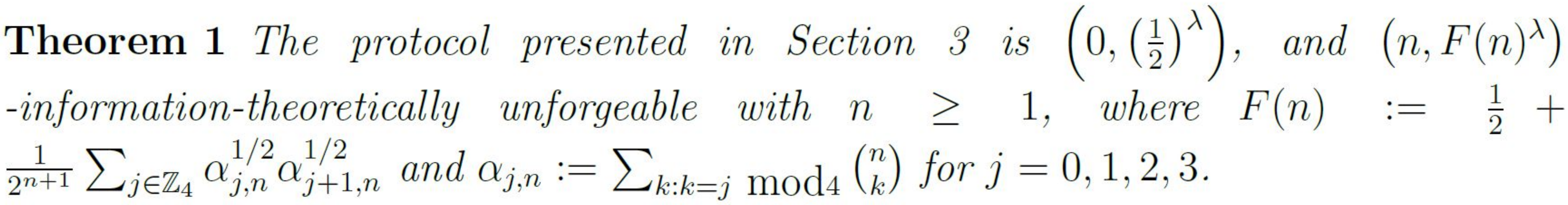


Figure 5: Verification phase. The verifier Bob makes the quantum measurement for $\{H_{ijm_i}\}_{ij}$ under the basis $\{B_{ijm_i}\}_{ij}$, respectively. If for all i, j, the corresponding measurement result is equal to $\{V_{ijm_i}\}_{ij}$, he accepts the signature; otherwise, he rejects the signature.

Security against unforgeability

- To theoretically analyze the security performance resisting unforgeability, we need to calculate the specific probability that a malicious party, Jack, succeeds forging attack. The probability is given in the following theorem.



Theorem 1 *The protocol presented in Section 3 is* $\left(0, \left(\frac{1}{2}\right)^{\lambda}\right)$, *and* $(n, F(n)^{\lambda})$ *-information-theoretically unforgeable with* $n \geq 1$, *where* $F(n) := \frac{1}{2} + \frac{1}{2^{n+1}} \sum_{j \in \mathbb{Z}_4} \alpha_{j,n}^{1/2} \alpha_{j+1,n}^{1/2}$ *and* $\alpha_{j,n} := \sum_{k:k=j \mod 4} \binom{n}{k}$ *for* $j = 0, 1, 2, 3$.

State identification

- If an adversary colludes with $n-1$ parties, he can hold at most n copies of the public key. To calculate the probability that the adversary succeeds forging attacks, we should calculate the minimum error probability in state identification. We apply covariant group method in this section.

$$\boxed{\begin{aligned} |0\rangle &= \frac{1}{\sqrt{2}}(|e_0\rangle + |e_1\rangle), & \frac{1+i}{\sqrt{2}}|+\rangle &= \frac{1}{\sqrt{2}}(|e_0\rangle + i|e_1\rangle) \\ i|1\rangle &= \frac{1}{\sqrt{2}}(|e_0\rangle - |e_1\rangle), & \frac{1-i}{\sqrt{2}}|-\rangle &= \frac{1}{\sqrt{2}}(|e_0\rangle - i|e_1\rangle). \end{aligned}}$$

$$|e_0\rangle := \tfrac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$$
$$|e_1\rangle := \tfrac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$$

⇒ state family $\{\boxed{|f_x\rangle}\}_{x\in\mathbb{Z}_4}$

$$|f_x\rangle := \frac{1}{\sqrt{2}}(|e_0\rangle + e^{x\pi i/2}\,|e_1\rangle)$$

- Our target function:

- $$1 - F(\underset{\substack{\downarrow \\ \text{The number of copies} \\ \text{of the public key}}}{\boxed{n}}) = \min_{\{\Pi_{\hat{x}}\}} \sum_{x=0}^{3} \frac{1}{4} \sum_{\hat{x}=0}^{3} \underset{\substack{\downarrow \\ \text{Error function}}}{\boxed{R(x, \hat{x})}} \operatorname{Tr} \overset{\substack{\text{POVM} \\ \uparrow}}{\boxed{\Pi_{\hat{x}}}} (|f_x\rangle\langle f_x|)^{\otimes n}$$

Theorem 2 *We have the following relation*

$$\min_{\{\Pi_{\hat{x}}\}} \sum_{x=0}^{3} \frac{1}{4} \sum_{\hat{x}=0}^{3} R(x, \hat{x}) \operatorname{Tr} \Pi_{\hat{x}} (|f_x\rangle\langle f_x|)^{\otimes n} = \frac{1}{2} - \frac{1}{2^{n+1}} \sum_{j \in \mathbb{Z}_4} \alpha_{j,n}^{1/2} \alpha_{j+1,n}^{1/2}.$$

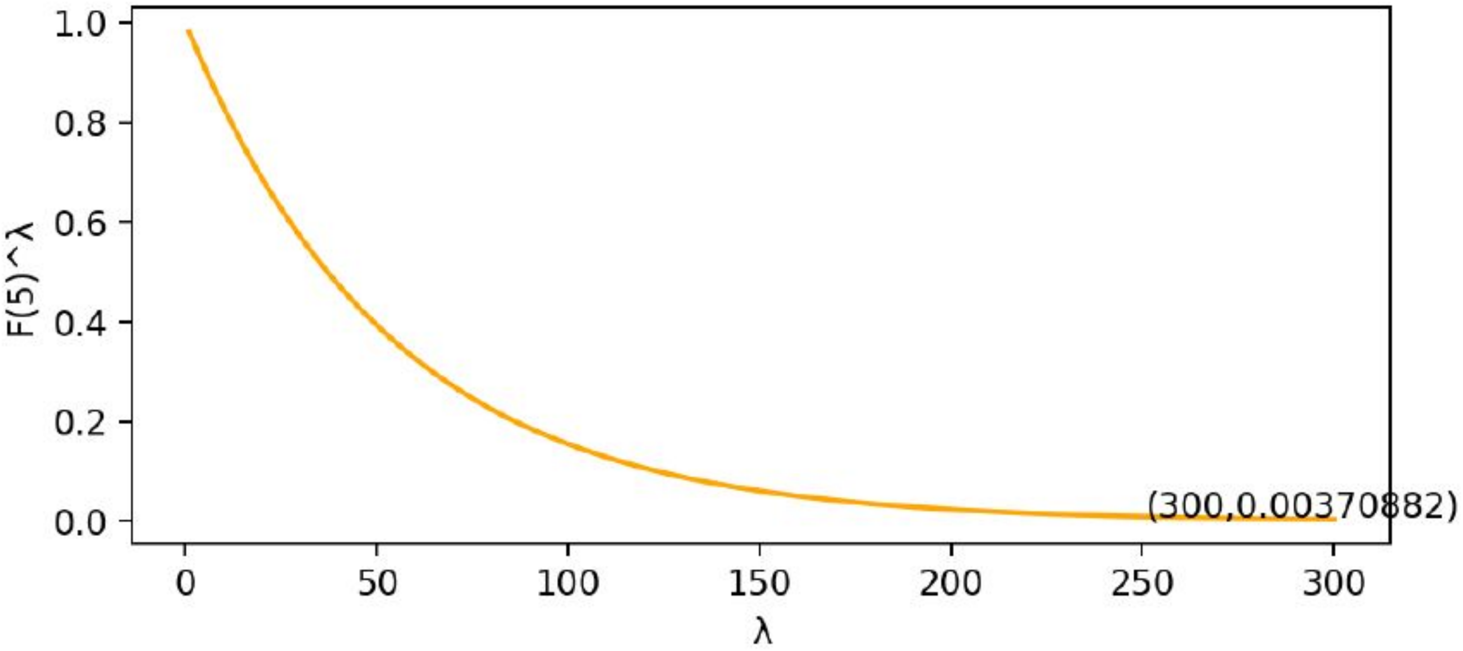


Figure 6: The probability of succeeding a forging attack in the case of $n = 5$.

Thank you for listening

A simple example

- We assume that Alice wants to send one bit message 0, $\lambda = 1$.
- Key generation phase

Alice generates a private key $\{\{0, X\}, \{1, Z\}\}$, subsequently generates its corresponding quantum public key $|+\rangle, |1\rangle$. Then she sends the public key to Bob.

- Signing phase

Alice sends the message-signature pair $\{0, \{0, X\}\}$ to Bob.

- Verification phase

Bob measures the first qubit in the public key under basis X. If the measure result is $|+\rangle$, he accepts the signature, otherwise he rejects the signature.