Quantum Cyber Security
Lecture 13: Quantum Encryption & Authentication

Petros Wallden

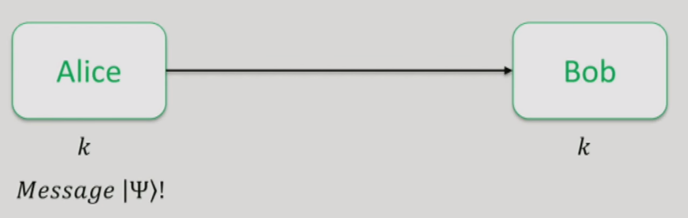
University of Edinburgh

11th March 2025

This Lecture

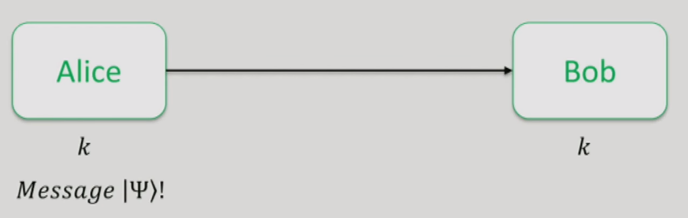
1. Encrypting Quantum Information
2. The Quantum One-Time-Pad
3. Authenticated Quantum Messages
4. A Trap-Based Quantum Authentication Scheme

Can we encrypt a qubit or a general quantum state?



Encrypting Quantum Information

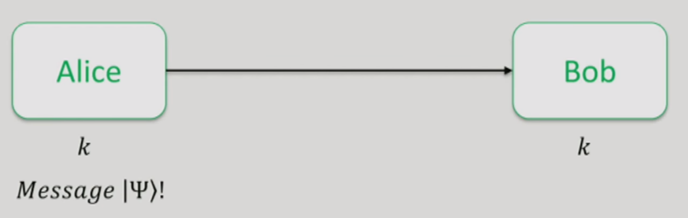
Can we encrypt a qubit or a general quantum state?



- Anyone intercepting the quantum communication (without the key k) should not learn anything about the message!
- Bob should be able to extract the message

Encrypting Quantum Information

Can we encrypt a qubit or a general quantum state?



- Anyone intercepting the quantum communication (without the key k) should not learn anything about the message!
- Bob should be able to extract the message
- Motivation: Protocols that involve communicating private quantum information.
  E.g. as part of a secure quantum computation

Task: Encrypting Quantum Information

Send a **quantum state** $|\psi\rangle$ (from Alice to Bob), through an untrusted quantum channel $\mathcal{E}_C(\cdot)$ such that: (i) Any Eavesdropper intercepting **cannot extract *any* information**, and (ii) Bob can "decrypt" and (if no Eavesdropping) **recover the correct quantum state**.

Encrypting Quantum Information

Task: Encrypting Quantum Information

Send a **quantum state** $|\psi\rangle$ (from Alice to Bob), through an untrusted quantum channel $\mathcal{E}_C(\cdot)$ such that: (i) Any Eavesdropper intercepting **cannot extract *any* information**, and (ii) Bob can "decrypt" and (if no Eavesdropping) **recover the correct quantum state**.

- Quantum Plaintext: $|\psi\rangle$
- Secret (classical) key: k
- Quantum Ciphertext: $\rho_k(\psi)$
- **Encryption Algorithm**: $\mathtt{Enc}_k(|\psi\rangle) = \rho_k(\psi)$
- Crossing Channel: $\mathcal{E}_C(\rho_k(\psi)) = \rho$
- **Decryption Algorithm**: $\mathtt{Dec}_k(\rho)$

Task: Encrypting Quantum Information

Send a **quantum state** $|\psi\rangle$ (from Alice to Bob), through an untrusted quantum channel $\mathcal{E}_C(\cdot)$ such that: (i) Any Eavesdropper intercepting **cannot extract *any* information**, and (ii) Bob can “decrypt” and (if no Eavesdropping) **recover the correct quantum state**.

1. **Correctness:** $\mathtt{Dec}_k\left(\mathtt{Enc}_k\left(|\psi\rangle\right)\right) = |\psi\rangle$; (cf $\mathcal{E}_C = \mathbb{I}$)

Encrypting Quantum Information

Task: Encrypting Quantum Information

Send a **quantum state** $|\psi\rangle$ (from Alice to Bob), through an untrusted quantum channel $\mathcal{E}_C(\cdot)$ such that: (i) Any Eavesdropper intercepting **cannot extract *any* information**, and (ii) Bob can "decrypt" and (if no Eavesdropping) **recover the correct quantum state**.

1. **Correctness:** $\texttt{Dec}_k\left(\texttt{Enc}_k\left(|\psi\rangle\right)\right) = |\psi\rangle$; (cf $\mathcal{E}_C = \mathbb{I}$)
2. **Security ITS:** Given any two distinct states $|\psi_1\rangle, |\psi_2\rangle$ *any* adversary $\mathcal{A}$ cannot distinguish between the two (averaged over secret key) quantum ciphertexts

$$T\left(\sum_k \rho_k(\psi_1), \sum_k \rho_k(\psi_2)\right) = 0 \ ; \ \sum_k \rho_k(\psi_1) = \sum_k \rho_k(\psi_2)$$

where $T(,)$ is trace-distance and we have:
Perfect Information-Theoretic Security

Task: Encrypting Quantum Information

Send a **quantum state** $|\psi\rangle$ (from Alice to Bob), through an untrusted quantum channel $\mathcal{E}_C(\cdot)$ such that: (i) Any Eavesdropper intercepting **cannot extract *any* information**, and (ii) Bob can "decrypt" and (if no Eavesdropping) **recover the correct quantum state**.

1. **Correctness:** $\texttt{Dec}_k(\texttt{Enc}_k(|\psi\rangle)) = |\psi\rangle$; (cf $\mathcal{E}_C = \mathbb{I}$)
3. **Security General:** Given two states $T(|\psi_1\rangle, |\psi_2\rangle) = p$, the prob that *any* $\mathcal{A}$ can distinguish between the average q-ciphertexts is bounded by $\epsilon(n) \cdot p$

$$Pr[\mathcal{A}(\sum_k \rho_k(\psi_1)) = 1] - Pr[\mathcal{A}(\sum_k \rho_k(\psi_2)) = 1] \leq \epsilon(n) \cdot p$$

where $\epsilon(n)$ is the security level and the distinguisher is either computational (poly-time) or ITS (trace-distance)

The Quantum One-Time-Pad (QOTP)

Focus: Information Theoretic Security (ITS)

- (Classical) Secret Key: two classical bits per qubit ($k = (a, b)$)
- "One-Time-Pad" means keys cannot be reused
- We consider a **single qubit** message (generalise later)
- We assume pure message state $\rho_\psi = |\psi\rangle\langle\psi|$

The Quantum One-Time-Pad (QOTP)

Focus: Information Theoretic Security (ITS)

- (Classical) Secret Key: two classical bits per qubit ($k = (a, b)$)
- "One-Time-Pad" means keys cannot be reused
- We consider a **single qubit** message (generalise later)
- We assume pure message state $\rho_\psi = |\psi\rangle\langle\psi|$
- **Encryption Algorithm:** $\mathtt{Enc}_{a,b}(\rho_\psi) = X^a Z^b \rho_\psi Z^b X^a$

The Quantum One-Time-Pad (QOTP)

Focus: Information Theoretic Security (ITS)

- (Classical) Secret Key: two classical bits per qubit ($k = (a, b)$)
- "One-Time-Pad" means keys cannot be reused
- We consider a **single qubit** message (generalise later)
- We assume pure message state $\rho_\psi = |\psi\rangle \langle\psi|$
- **Encryption Algorithm:** $\texttt{Enc}_{a,b}(\rho_\psi) = X^a Z^b \rho_\psi Z^b X^a$
- **Decryption Algorithm:** $\texttt{Dec}_{a,b}(\rho) = Z^b X^a \rho X^a Z^b$

The QOTP

- **Correctness:**

$$\mathtt{Dec}_{a,b}(\mathtt{Enc}_{a,b}(\rho_\psi)) = Z^b X^a \left(X^a Z^b (\rho_\psi) Z^b X^a \right) X^a Z^b = \rho_\psi$$

The QOTP

- **Correctness:**

$$\texttt{Dec}_{a,b}(\texttt{Enc}_{a,b}(\rho_\psi)) = Z^b X^a \left(X^a Z^b (\rho_\psi) Z^b X^a \right) X^a Z^b = \rho_\psi$$

- Any eavesdropper, without knowing a, b, intercepts the "average" ciphertext: $\rho_E(\psi) := \frac{1}{4}\sum_{a,b} X^a Z^b \rho_\psi Z^b X^a$

The QOTP

- **Correctness:**
$$\texttt{Dec}_{a,b}(\texttt{Enc}_{a,b}(\rho_\psi)) = Z^b X^a \left(X^a Z^b (\rho_\psi) Z^b X^a \right) X^a Z^b = \rho_\psi$$

- Any eavesdropper, without knowing a, b, intercepts the "average" ciphertext: $\rho_E(\psi) := \frac{1}{4} \sum_{a,b} X^a Z^b \rho_\psi Z^b X^a$

- **Security:** We need to prove that $\rho_E(\psi_1) = \rho_E(\psi_2) \; \forall \; \psi_1 \neq \psi_2$

- We will use the Pauli Decomposition (form basis for Hermitian matrices)

Pauli Decomposition: Single Qubit

Recall the Pauli matrices (including identity) are:

$$\mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} := P_0 \quad ; \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} := P_1$$

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} := P_2 \quad ; \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} := P_3$$

Pauli Decomposition: Single Qubit

Recall the Pauli matrices (including identity) are:

$$\mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} := P_0 \quad ; \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} := P_1$$

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} := P_2 \quad ; \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} := P_3$$

- Any (single qubit) density matrix can be written as:

$$\rho = \frac{1}{2}\mathbb{I} + a_1 X + a_2 Y + a_3 Z = \frac{1}{2}\mathbb{I} + \sum_{i=1}^{3} a_i P_i$$

  for some complex numbers a_1, a_2, a_3.

Pauli Decomposition: Single Qubit

Recall the Pauli matrices (including identity) are:

$$\mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} := P_0 \quad ; \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} := P_1$$

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} := P_2 \quad ; \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} := P_3$$

- Any (single qubit) density matrix can be written as:

$$\rho = \frac{1}{2}\mathbb{I} + a_1 X + a_2 Y + a_3 Z = \frac{1}{2}\mathbb{I} + \sum_{i=1}^{3} a_i P_i$$

  for some complex numbers a_1, a_2, a_3.
- Coefficients can be evaluated:

$$a_i = \frac{1}{2}\mathrm{Tr}(P_i \rho)$$

The QOTP: Security Proof

Commutation Relations: $P_i P_j = -P_j P_i$ for $i \neq j$ and $i, j \in \{1, 2, 3\}$.

$XZ^bX^a = (-1)^b Z^bX^aX$; $YZ^bX^a = (-1)^{b+a} Z^bX^aY$; $ZZ^bX^a = (-1)^a Z^bX^aZ$

Other property: $\sum_{a\in\{0,1\}}(-1)^a(\text{Anything}) = 0$

The QOTP: Security Proof

Commutation Relations: $P_i P_j = -P_j P_i$ for $i \neq j$ and $i, j \in \{1, 2, 3\}$.

$XZ^b X^a = (-1)^b Z^b X^a X$; $YZ^b X^a = (-1)^{b+a} Z^b X^a Y$; $ZZ^b X^a = (-1)^a Z^b X^a Z$

Other property: $\sum_{a \in \{0,1\}} (-1)^a (\text{Anything}) = 0$

- We now prove that $\rho_E(\psi)$ is independent of ψ:

$$\rho_E(\psi) = \frac{1}{4} \sum_{a,b} X^a Z^b \rho_\psi Z^b X^a = \frac{1}{4} \sum_{a,b} X^a Z^b \left(\frac{1}{2} \mathbb{I} + \sum_{i=1}^{3} a_i P_i \right) Z^b X^a$$

The QOTP: Security Proof

Commutation Relations: $P_iP_j = -P_jP_i$ for $i \neq j$ and $i, j \in \{1, 2, 3\}$.

$XZ^bX^a = (-1)^b Z^bX^aX$; $YZ^bX^a = (-1)^{b+a} Z^bX^aY$; $ZZ^bX^a = (-1)^a Z^bX^aZ$

Other property: $\sum_{a\in\{0,1\}} (-1)^a (\text{Anything}) = 0$

- We now prove that $\rho_E(\psi)$ is independent of ψ:

$$\rho_E(\psi) = \frac{1}{4}\sum_{a,b} X^aZ^b\rho_\psi Z^bX^a = \frac{1}{4}\sum_{a,b} X^aZ^b\left(\frac{1}{2}\mathbb{I} + \sum_{i=1}^{3} a_iP_i\right)Z^bX^a$$

- The first term: $\frac{1}{4}\sum_{a,b} X^aZ^b\left(\frac{1}{2}\mathbb{I}\right)Z^bX^a = \frac{1}{8}\sum_{a,b}\mathbb{I} = \frac{1}{2}\mathbb{I}$
- The second term: $\frac{1}{4}\sum_{a,b} X^aZ^b(a_1X)Z^bX^a = \frac{a_1}{4}\sum_{a,b}(-1)^bX = 0$
- The third term: $\frac{1}{4}\sum_{a,b} X^aZ^b(a_2Y)Z^bX^a = \frac{a_2}{4}\sum_{a,b}(-1)^{b+a}Y = 0$
- The forth term: $\frac{1}{4}\sum_{a,b} X^aZ^b(a_3Z)Z^bX^a = \frac{a_3}{4}\sum_{a,b}(-1)^aZ = 0$

The QOTP: Security Proof

Commutation Relations: $P_iP_j = -P_jP_i$ for $i \neq j$ and $i, j \in \{1, 2, 3\}$.

$XZ^bX^a = (-1)^b Z^bX^aX$; $YZ^bX^a = (-1)^{b+a} Z^bX^aY$; $ZZ^bX^a = (-1)^a Z^bX^aZ$

Other property: $\sum_{a\in\{0,1\}}(-1)^a(\text{Anything}) = 0$

- We now prove that $\rho_E(\psi)$ is independent of ψ:

$$\rho_E(\psi) = \frac{1}{4}\sum_{a,b} X^aZ^b\rho_\psi Z^bX^a = \frac{1}{4}\sum_{a,b} X^aZ^b\left(\frac{1}{2}\mathbb{I} + \sum_{i=1}^{3} a_iP_i\right)Z^bX^a$$

- The first term: $\frac{1}{4}\sum_{a,b} X^aZ^b\left(\frac{1}{2}\mathbb{I}\right)Z^bX^a = \frac{1}{8}\sum_{a,b}\mathbb{I} = \frac{1}{2}\mathbb{I}$
- The second term: $\frac{1}{4}\sum_{a,b} X^aZ^b(a_1X)Z^bX^a = \frac{a_1}{4}\sum_{a,b}(-1)^bX = 0$
- The third term: $\frac{1}{4}\sum_{a,b} X^aZ^b(a_2Y)Z^bX^a = \frac{a_2}{4}\sum_{a,b}(-1)^{b+a}Y = 0$
- The forth term: $\frac{1}{4}\sum_{a,b} X^aZ^b(a_3Z)Z^bX^a = \frac{a_3}{4}\sum_{a,b}(-1)^aZ = 0$
- Putting together: $\rho_E(\psi) = \frac{1}{2}\mathbb{I}$. **Independent of ψ** $\square$

Pauli Decomposition: Multiple (n)-Qubits

- Any n-qubit state can be written as:

$$\rho = \sum a_{i_1,\ldots,i_n} P_{i_1} \otimes \cdots \otimes P_{i_n}$$

for some complex numbers $a_{i_1,\ldots,i_n}$.

Pauli Decomposition: Multiple (n)-Qubits

- Any n-qubit state can be written as:

$$\rho = \sum a_{i_1,\ldots,i_n} P_{i_1} \otimes \cdots \otimes P_{i_n}$$

  for some complex numbers $a_{i_1,\ldots,i_n}$.

- Coefficients can be evaluated:

$$a_{i_1,\ldots,i_n} = \frac{1}{2^n} \mathrm{Tr}\left(P_{i_1} \otimes \cdots \otimes P_{i_n} \cdot \rho\right)$$

- Note that, since $\mathrm{Tr}(\rho) = 1$, the term with identity everywhere is: $\frac{1}{2^n} \mathbb{I} \otimes \cdots \otimes \mathbb{I}$

The QOTP: Multiple (n)-Qubits

- Secret Key: $2n$-bits ($\vec{k} = \left(\vec{a}, \vec{b}\right) = ((a_1, b_1), \ldots, (a_n, b_n))$)
- Encryption and Decryption qubit-by-qubit
- $\mathtt{Enc}_{\vec{k}}(\rho_\psi) = X^{a_1} Z^{b_1} \otimes \cdots \otimes X^{a_n} Z^{b_n} \left(\rho_\psi\right) Z^{b_1} X^{a_1} \otimes \cdots \otimes Z^{b_n} X^{a_n}$
- $\mathtt{Dec}_{\vec{k}}(\rho) = Z^{b_1} X^{a_1} \otimes \cdots \otimes Z^{b_n} X^{a_n} \left(\rho\right) X^{a_1} Z^{b_1} \otimes \cdots \otimes X^{a_n} Z^{b_n}$

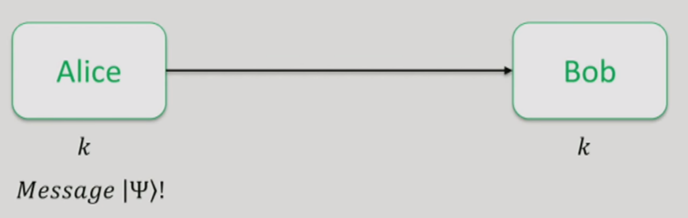
The QOTP: Multiple (n)-Qubits

- Secret Key: $2n$-bits ($\vec{k} = \left(\vec{a}, \vec{b}\right) = ((a_1, b_1), \ldots, (a_n, b_n))$)
- Encryption and Decryption qubit-by-qubit
- $\mathtt{Enc}_{\vec{k}}(\rho_\psi) = X^{a_1} Z^{b_1} \otimes \cdots \otimes X^{a_n} Z^{b_n} (\rho_\psi) Z^{b_1} X^{a_1} \otimes \cdots \otimes Z^{b_n} X^{a_n}$
- $\mathtt{Dec}_{\vec{k}}(\rho) = Z^{b_1} X^{a_1} \otimes \cdots \otimes Z^{b_n} X^{a_n} (\rho) X^{a_1} Z^{b_1} \otimes \cdots \otimes X^{a_n} Z^{b_n}$
- **Correctness:** $\mathtt{Dec}_{\vec{k}}\left(\mathtt{Enc}_{\vec{k}}(\rho_\psi)\right) = \rho_\psi$

- Secret Key: $2n$-bits ($\vec{k} = \left(\vec{a}, \vec{b}\right) = ((a_1, b_1), \ldots, (a_n, b_n))$)
- Encryption and Decryption qubit-by-qubit
- $\mathtt{Enc}_{\vec{k}}(\rho_\psi) = X^{a_1} Z^{b_1} \otimes \cdots \otimes X^{a_n} Z^{b_n} \, (\rho_\psi) \, Z^{b_1} X^{a_1} \otimes \cdots \otimes Z^{b_n} X^{a_n}$
- $\mathtt{Dec}_{\vec{k}}(\rho) = Z^{b_1} X^{a_1} \otimes \cdots \otimes Z^{b_n} X^{a_n} \, (\rho) \, X^{a_1} Z^{b_1} \otimes \cdots \otimes X^{a_n} Z^{b_n}$
- **Correctness:** $\mathtt{Dec}_{\vec{k}}\left(\mathtt{Enc}_{\vec{k}}(\rho_\psi)\right) = \rho_\psi$
- **Security:** $\rho_E(\psi) = \frac{1}{4^n} \sum_{\vec{a},\vec{b}} \mathtt{Enc}_{\vec{a},\vec{b}}(\rho_\psi) = \frac{1}{2^n} \mathbb{I} \otimes \cdots \otimes \mathbb{I}$

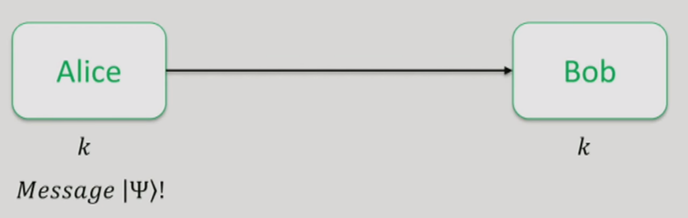
  All terms in the Pauli decomposition of ρ_ψ, except the $\mathbb{I} \otimes \cdots \otimes \mathbb{I}$ pick-up a $(-1)^{a_i}$ or $(-1)^{b_i}$ from the commutations, which when averaged over key values, vanish.

Can we authenticate a qubit (or a general quantum state)?



Authentication of Quantum Messages

Can we authenticate a qubit (or a general quantum state)?



- Alice sends (quantum) message with a "tag"
- Bob can check the tag and if he outputs `accept`, he received (whp) the intended state $|\psi\rangle$
- Is called ϵ-QAS if the probability `accept` **and** wrong state, is bounded by ϵ.

Authentication of Quantum Messages

Task: Authenticating Quantum Information

Send a **quantum state** $|\psi\rangle$ (Alice to Bob), through an untrusted quantum channel, such that Bob either (i) **accepts and recovers** the correct state $|\psi\rangle$ or (ii) **rejects**. The probability of accepting a wrong state is bounded by ϵ.

Authentication of Quantum Messages

Task: Authenticating Quantum Information

Send a **quantum state** $|\psi\rangle$ (Alice to Bob), through an untrusted quantum channel, such that Bob either (i) **accepts and recovers** the correct state $|\psi\rangle$ or (ii) **rejects**. The probability of accepting a wrong state is bounded by ϵ.

- Secrecy is not a-priori required (in classical authentication the messages are public)
- Can be proven that **quantumly authentication implies encryption**!
  (cf no-cloning/cannot "overhear" without disturbing)

Authentication of Quantum Messages

Task: Authenticating Quantum Information

Send a **quantum state** $|\psi\rangle$ (Alice to Bob), through an untrusted quantum channel, such that Bob either (i) **accepts and recovers** the correct state $|\psi\rangle$ or (ii) **rejects**. The probability of accepting a wrong state is bounded by ϵ.

- Secrecy is not a-priori required (in classical authentication the messages are public)
- Can be proven that **quantumly authentication implies encryption**!
  (cf no-cloning/cannot "overhear" without disturbing)
- Quantum Plaintext: $|\psi\rangle$
- Secret (classical) key: k
- **Authentication Algorithm**: $\texttt{Auth}_k(|\psi\rangle \otimes |0\rangle) = \rho_k(\psi)$
- **Verif. Algorithm**: $\texttt{Ver}_k(\cdot) = \rho \otimes \texttt{accept}$ or $\sigma \otimes \texttt{reject}$

Task: Authenticating Quantum Information

Send a **quantum state** $|\psi\rangle$ (Alice to Bob), through an untrusted quantum channel, such that Bob either (i) **accepts and recovers** the correct state $|\psi\rangle$ or (ii) **rejects**. The probability of accepting a wrong state is bounded by ϵ.

1. **Correctness:** $\mathtt{Ver}_k\left(\mathtt{Auth}_k\left(|\psi\rangle \otimes |0\rangle\right)\right) = |\psi\rangle \otimes \mathtt{accept}$

Authentication of Quantum Messages

Task: Authenticating Quantum Information

Send a **quantum state** $|\psi\rangle$ (Alice to Bob), through an untrusted quantum channel, such that Bob either (i) **accepts and recovers** the correct state $|\psi\rangle$ or (ii) **rejects**. The probability of accepting a wrong state is bounded by ϵ.

1. **Correctness:** $\mathtt{Ver}_k\left(\mathtt{Auth}_k\left(|\psi\rangle \otimes |0\rangle\right)\right) = |\psi\rangle \otimes \mathtt{accept}$

2. **Security:** Let $\sum_k \mathtt{Ver}_k\left(\mathcal{E}\left(\mathtt{Auth}_k\left(|\psi\rangle \otimes |0\rangle\right)\right)\right) = \rho \otimes \mathtt{flag}$

   We call the scheme ϵ-secure QAS if:

   $\mathrm{Tr}\left(\left[\left(|\psi\rangle\langle\psi| \otimes \mathtt{accept}\right) + \left(\mathbb{I} \otimes \mathtt{reject}\right)\right]\left(\rho \otimes \mathtt{flag}\right)\right) \geq 1 - \epsilon$

- This ϵ is the **probability** that the flag is **accept but fails to return the intended state**

A Trap-Based Quantum Authentication Scheme (TQAS)

- By Broadbent, Gutoski, Stebila (Crypto 2013)
- Singe qubit, simplified version

A Trap-Based Quantum Authentication Scheme (TQAS)

- By Broadbent, Gutoski, Stebila (Crypto 2013)
- Singe qubit, simplified version
- Secret Key $k = k_1 \parallel k_2$: where k_1 six random bits; k_2 a random 3-elements permutation (one-out-of six)
- Let $\mathtt{Enc}_{k_1}$ be QOTP for 3-qubits, using six bits of secret key
- Let $\Pi_{k_2}(\cdot)$ be a 3-element permutation
- Message: $\rho_\psi = |\psi\rangle \langle\psi|$

A Trap-Based Quantum Authentication Scheme (TQAS)

- By Broadbent, Gutoski, Stebila (Crypto 2013)
- Singe qubit, simplified version
- Secret Key $k = k_1 \parallel k_2$: where k_1 six random bits; k_2 a random 3-elements permutation (one-out-of six)
- Let $\texttt{Enc}_{k_1}$ be QOTP for 3-qubits, using six bits of secret key
- Let $\Pi_{k_2}(\cdot)$ be a 3-element permutation
- Message: $\rho_\psi = |\psi\rangle\langle\psi|$
- **Authentication Algorithm:**
  $\texttt{Auth}_k\left(|\psi\rangle \otimes |0\rangle \otimes |+\rangle\right) := \texttt{Enc}_{k_1}\left(\Pi_{k_2}\left(|\psi\rangle \otimes |0\rangle \otimes |+\rangle\right)\right)$

A Trap-Based Quantum Authentication Scheme (TQAS)

- By Broadbent, Gutoski, Stebila (Crypto 2013)
- Singe qubit, simplified version
- Secret Key $k = k_1 \parallel k_2$: where k_1 six random bits; k_2 a random 3-elements permutation (one-out-of six)
- Let $\mathtt{Enc}_{k_1}$ be QOTP for 3-qubits, using six bits of secret key
- Let $\Pi_{k_2}(\cdot)$ be a 3-element permutation
- Message: $\rho_\psi = |\psi\rangle\langle\psi|$
- **Authentication Algorithm:** $\mathtt{Auth}_k(|\psi\rangle \otimes |0\rangle \otimes |+\rangle) := \mathtt{Enc}_{k_1}(\Pi_{k_2}(|\psi\rangle \otimes |0\rangle \otimes |+\rangle))$
- **Ver. Algor.:** Let $P_{acc} := \mathbb{I} \otimes |0\rangle\langle 0| \otimes |+\rangle\langle +|$ and $P_{rej} := \mathbb{I} - P_{acc}$ and let $\tilde{\rho} := \Pi_{k_2}^{-1}(\mathtt{Dec}_{k_1}(\rho))$.

A Trap-Based Quantum Authentication Scheme (TQAS)

- By Broadbent, Gutoski, Stebila (Crypto 2013)
- Singe qubit, simplified version
- Secret Key $k = k_1 \| k_2$: where k_1 six random bits; k_2 a random 3-elements permutation (one-out-of six)
- Let $\mathtt{Enc}_{k_1}$ be QOTP for 3-qubits, using six bits of secret key
- Let $\Pi_{k_2}(\cdot)$ be a 3-element permutation
- Message: $\rho_\psi = |\psi\rangle\langle\psi|$
- **Authentication Algorithm:**
  $\mathtt{Auth}_k(|\psi\rangle \otimes |0\rangle \otimes |+\rangle) := \mathtt{Enc}_{k_1}(\Pi_{k_2}(|\psi\rangle \otimes |0\rangle \otimes |+\rangle))$
- **Ver. Algor.:** Let $P_{acc} := \mathbb{I} \otimes |0\rangle\langle 0| \otimes |+\rangle\langle +|$ and $P_{rej} := \mathbb{I} - P_{acc}$ and let $\tilde{\rho} := \Pi_{k_2}^{-1}(\mathtt{Dec}_{k_1}(\rho))$.

  $\mathtt{Ver}_k(\rho) :=$ computes $\tilde{\rho}$; measures $\{P_{acc}, P_{rej}\}$ and if P_{acc} outputs the first register and `accept`. If P_{rej} outputs reject.

The TQAS

- **Correctness:** $\mathtt{Ver}_k\left(\mathtt{Auth}_k\left(|\psi\rangle \otimes |0\rangle \otimes |+\rangle\right)\right) = |\psi\rangle \otimes \mathtt{accept}$
- **Security:** Proof is complicated, but essentially the adversary cannot affect the state without some chance of affecting the "trap" qubits because he is ignorant of the permutation.
- Using Pauli decomposition can show that all attacks reduce to "Pauli" attacks which can be detected with either the $|0\rangle$ or the $|+\rangle$ trap.
- Probability of corruption and not detection is non-zero (but bounded below 1). There are techniques (using quantum error-correction codes) to boost this security to exponentially close to zero.