

# Quantum Cyber Security

## Lecture 13: Quantum Encryption & Authentication

Petros Wallden

University of Edinburgh

5th March 2026



- 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?



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

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**.

## 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:**  $\text{Enc}_k(|\psi\rangle) = \rho_k(\psi)$
- Crossing Channel:  $\mathcal{E}_C(\rho_k(\psi)) = \rho$
- **Decryption Algorithm:**  $\text{Dec}_k(\rho)$

## 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:**  $\text{Dec}_k(\text{Enc}_k(|\psi\rangle)) = |\psi\rangle$ ; (cf  $\mathcal{E}_C = \mathbb{I}$ )

## 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:**  $\text{Dec}_k(\text{Enc}_k(|\psi\rangle)) = |\psi\rangle$ ; (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

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

where  $T(\cdot)$  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:**  $\text{Dec}_k(\text{Enc}_k(|\psi\rangle)) = |\psi\rangle$ ; (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)

## 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  $\rho_\psi = |\psi\rangle\langle\psi|$

## 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:**  $\text{Enc}_{a,b}(\rho_\psi) = X^a Z^b \rho_\psi Z^b X^a$

## 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:**  $\text{Enc}_{a,b}(\rho_\psi) = X^a Z^b \rho_\psi Z^b X^a$
- **Decryption Algorithm:**  $\text{Dec}_{a,b}(\rho) = Z^b X^a \rho X^a Z^b$

- **Correctness:**

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

- **Correctness:**

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

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

- **Correctness:**

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

- 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:

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

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

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:

$$\rho = \frac{1}{2}\mathbb{I} + a_1X + a_2Y + a_3Z = \frac{1}{2}\mathbb{I} + \sum_{i=1}^3 a_iP_i$$

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:

$$\rho = \frac{1}{2}\mathbb{I} + a_1X + a_2Y + a_3Z = \frac{1}{2}\mathbb{I} + \sum_{i=1}^3 a_iP_i$$

for some complex numbers  $a_1, a_2, a_3$ .

- Coefficients can be evaluated:

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

# The QOTP: Security Proof

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

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

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

# 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  $\psi$ :

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

# The QOTP: Security Proof

**Commutation Relations:**  $P_i P_j = -P_j P_i$  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  $\psi$ :

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

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

# 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  $\psi$ :

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

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

- Any  $n$ -qubit state can be written as:

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

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

- Any  $n$ -qubit state can be written as:

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

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

- Coefficients can be evaluated:

$$a_{i_1, \dots, i_n} = \frac{1}{2^n} \text{Tr}(P_{i_1} \otimes \dots \otimes P_{i_n} \cdot \rho)$$

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

# The QOTP: Multiple ( $n$ )-Qubits

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

# The QOTP: Multiple ( $n$ )-Qubits

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

# The QOTP: Multiple ( $n$ )-Qubits

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

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

# Authentication of Quantum Messages

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



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  $\epsilon$ -QAS if the probability **accept** and wrong state, is bounded by  $\epsilon$ .

## 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  $\epsilon$ .

## 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  $\epsilon$ .

- 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)

## 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  $\epsilon$ .

- 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:**  $\text{Auth}_k(|\psi\rangle \otimes |0\rangle) = \rho_k(\psi)$
- **Verif. Algorithm:**  $\text{Ver}_k(\cdot) = \rho \otimes \text{accept}$  or  $\sigma \otimes \text{reject}$

## 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  $\epsilon$ .

- 1 **Correctness:**  $\text{Ver}_k(\text{Auth}_k(|\psi\rangle \otimes |0\rangle)) = |\psi\rangle \otimes \text{accept}$

## 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  $\epsilon$ .

- 1 **Correctness:**  $\text{Ver}_k(\text{Auth}_k(|\psi\rangle \otimes |0\rangle)) = |\psi\rangle \otimes \text{accept}$
- 2 **Security:** Let  $\sum_k \text{Ver}_k(\mathcal{E}(\text{Auth}_k(|\psi\rangle \otimes |0\rangle))) = \rho \otimes \text{flag}$

We call the scheme  $\epsilon$ -secure QAS if:

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

- This  $\epsilon$  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)
- Single qubit, simplified version

# A Trap-Based Quantum Authentication Scheme (TQAS)

- By Broadbent, Gutoski, Stebila (Crypto 2013)
- Single 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  $\text{Enc}_{k_1}$  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)
- Single 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  $\text{Enc}_{k_1}$  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:**  
 $\text{Auth}_k(|\psi\rangle \otimes |0\rangle \otimes |+\rangle) := \text{Enc}_{k_1}(\Pi_{k_2}(|\psi\rangle \otimes |0\rangle \otimes |+\rangle))$

# A Trap-Based Quantum Authentication Scheme (TQAS)

- By Broadbent, Gutoski, Stebila (Crypto 2013)
- Single 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  $\text{Enc}_{k_1}$  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:**  
$$\text{Auth}_k(|\psi\rangle \otimes |0\rangle \otimes |+\rangle) := \text{Enc}_{k_1}(\Pi_{k_2}(|\psi\rangle \otimes |0\rangle \otimes |+\rangle))$$
- **Ver. Algor.:** Let  $P_{acc} := \mathbb{I} \otimes |0\rangle\langle 0| \otimes |+\rangle\langle +|$  and  $P_{rej} := \mathbb{I} - P_{acc}$  and let  $\tilde{\rho} := \Pi_{k_2}^{-1}(\text{Dec}_{k_1}(\rho))$ .

# A Trap-Based Quantum Authentication Scheme (TQAS)

- By Broadbent, Gutoski, Stebila (Crypto 2013)
- Single 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  $\text{Enc}_{k_1}$  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:**  
 $\text{Auth}_k(|\psi\rangle \otimes |0\rangle \otimes |+\rangle) := \text{Enc}_{k_1}(\Pi_{k_2}(|\psi\rangle \otimes |0\rangle \otimes |+\rangle))$
- **Ver. Algor.:** Let  $P_{acc} := \mathbb{I} \otimes |0\rangle\langle 0| \otimes |+\rangle\langle +|$  and  $P_{rej} := \mathbb{I} - P_{acc}$  and let  $\tilde{\rho} := \Pi_{k_2}^{-1}(\text{Dec}_{k_1}(\rho))$ .  
 $\text{Ver}_k(\rho) :=$  computes  $\tilde{\rho}$ ; measures  $\{P_{acc}, P_{rej}\}$  and if  $P_{acc}$  outputs the first register and accept. If  $P_{rej}$  outputs reject.

- **Correctness:**  $\text{Ver}_k(\text{Auth}_k(|\psi\rangle \otimes |0\rangle \otimes |+\rangle)) = |\psi\rangle \otimes \text{accept}$
- **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.