Authentication of Quantum Messages

Daniel Gottesman
with
Howard Barnum
Claude Crepeau
Adam Smith
Alain Tapp

quant-ph/0205158

Classical Authentication

Alice sends a message to Bob. How does Bob know it really came from Alice?

Alice & Bob share secret key k

Message m

Family of hash functions σ_k

Alice sends $(m, \sigma_k(m))$

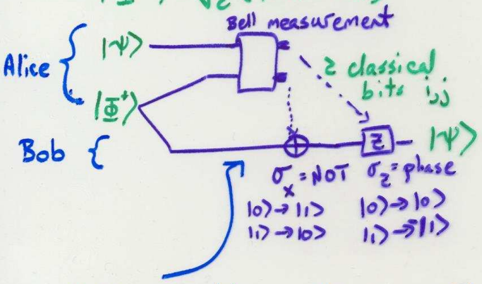
Bob accepts (m, σ) only if $\sigma = \sigma_k(m)$

Secure since only Alice knows key k.

Quantum Teleportation

Alice wants to send an unknown quantum state $|\psi\rangle$ to Bob. They have a classical communications channel and shared EPR pairs:

$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$



Bob's density matrix $\rho_B = I$ completely random.

Actually, Bob has $\sigma_{ij}|\psi\rangle$ with random ij.

Authentication of Quantum Message with <u>Quantum</u> <u>Key</u>

Alice & Bob share m Bell states $|\Phi^{+\otimes m}\rangle$

m-qubit message $|\psi\rangle$

Alice teleports $|\psi\rangle$ to Bob using Bell states:

Transmits $2m$ random classical bits (authenticated)

Bob has encrypted $|\psi\rangle$, which he can decrypt with Alice's transmission.

Quantum Error Correction

Alice wants to send Bob an unknown quantum state $|\psi\rangle$ through a noisy quantum channel. ($|\psi\rangle$ has m qubits)

$X = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Y = \sigma_Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $Z = \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

- Use n qubits ($n > m$); consider 2^m-dimensional subspace Q of full 2^n-dim. Hilbert space
- Q is eigenspace of tensor products of Pauli matrices

e.g.

$$\left.\begin{matrix} X\otimes Z\otimes Z\otimes X\otimes I \\ I\otimes X\otimes Z\otimes Z\otimes X \\ X\otimes I\otimes X\otimes Z\otimes Z \\ Z\otimes X\otimes I\otimes X\otimes Z \end{matrix}\right\} \text{generate Abelian group (stabilizer)}$$

(5-qubit code encoding 1 qubit, protecting against 1 error)

Quantum Error Correction

If $|\varphi\rangle$ is an encoded state, M is in stabilizer S, then

$M|\varphi\rangle = |\varphi\rangle$

- If E tensor product of Pauli matrices, either:
  - $\exists M \in S$ s.t. $ME = -EM$

    $\Rightarrow M(E|\varphi\rangle) = -E(M|\varphi\rangle) = -E|\varphi\rangle$

or

  - $\forall M \in S$, $ME = EM$

    $\Rightarrow E|\varphi\rangle$ is a valid codeword

Code Q detects E if

a) $\exists M \in S$ s.t. $EM = -ME$

b) $E \in S$ (so $E|\varphi\rangle = |\varphi\rangle$)

Error syndrome = pattern of +/- for generators of stabilizer

Purity Testing Code

Set of quantum codes $\{Q_k\}$

Q_k detects errors M_k

(i.e. $E \in M_k \Leftrightarrow EM = -ME$ for $M \in S$ or $E \in S$)

For fixed E, random k

Prob. of failure $= \dfrac{\#\{k \mid E \notin M_k\}}{\#\{k\}}$

Protocol:

- Encode using Q_k, k secret
- Adversary does error E
- Measure error syndrome, reject is non-zero

3 possibilities:

1) Syndrome non-zero — reject ✓
2) Syndrome zero
   a) $E \in Q_k \Rightarrow$ state correct — accept ✓
   b) $E \notin Q_k \Rightarrow$ error! — accept ✗

Interactive Quantum Authentication (with classical key)

Alice & Bob share classical key k

Family of quantum error-detecting codes Q_k

m-qubit message $|\psi\rangle$

- Alice creates n Bell states $|\Phi^{+\otimes n}\rangle$, sends 2nd halves to Bob
- Alice & Bob measure Q_k, compare coset
  - Reject if coset different
- Otherwise, decode to $|\Phi^{+\otimes m}\rangle$, use as quantum key
- Alice teleports $|\psi\rangle$, transmits x
- Bob decrypts $\sigma_x|\psi\rangle$

Given Bell state $|\Phi^+\rangle^{\otimes n}$,
when Alice measures Q_k, syndrome y

Bob gets
half of $|\Phi^+\rangle^{\otimes m}$
encoded w/ Q_k, syndrome y

Given Bell state $(I \otimes E)|\Phi^+\rangle^{\otimes n}$,
when Alice measures Q_k,
syndrome y

Bob gets
half of ?? (another Bell state)
encoded w/ Q_k, syndrome $y+e$

e is syndrome of E for Q_k

Alice teleports using $|\Phi^+\rangle^{\otimes m}$, get x

Bob has $\sigma_x|\psi\rangle$

Non-Interactive Quantum Authentication

Replace classical transmissions from interactive protocol with secret key

Alice & Bob share classical key (k,x,y)
Family of quantum codes Q_k
Message $|\psi\rangle$

- Alice encrypts message $\sigma_x|\psi\rangle$
- Alice encodes to $Q_k\sigma_x|\psi\rangle$
- Alice shifts to coset y
  $T_y Q_k \sigma_x|\psi\rangle$
- Alice sends this to Bob
- Bob decodes $|\psi\rangle$
  - Rejects if coset $\neq y$

Only Alice knows (x,y,k), so scheme secure.

Encryption is necessary

Suppose Eve can distinguish (almost) messages $|0\rangle$ and $|1\rangle$ (sent as ρ_0, ρ_1)

Then $\rho_0 = \left(\begin{array}{c|c} V_0 & 0 \\ \hline 0 & 0 \end{array}\right)$, $\rho_1 = \left(\begin{array}{c|c} 0 & 0 \\ \hline 0 & V_1 \end{array}\right)$
(or close)

$\Rightarrow$ Eve maps $V_0 \mapsto V_0$
$V_1 \mapsto (-1)V_1$

Effect: message $|0\rangle+|1\rangle$
(almost) becomes $|0\rangle-|1\rangle$

Eve can change the message.

Encryption is necessary

Suppose Eve can distinguish ρ_0 (representing $|0\rangle$) and ρ_1 (for $|1\rangle$) by ϵ. (e.g. trace distance)

$\Rightarrow \rho_0^{\otimes t}$ & $\rho_1^{\otimes t}$ are distinguishable by $\sim t\epsilon$

When $t \sim 1/\epsilon$, Eve can change message $|0^{\otimes t}\rangle + |1^{\otimes t}\rangle$ to $|0^{\otimes t}\rangle - |1^{\otimes t}\rangle$

Thm.: Encryption is necessary

Cor.: Digitally signing quantum states is impossible (info.-theoretically)

Thm.: Digitally signing quantum states is impossible, even with computational security.

Digital Signatures

Alice

private key k

classical message m $\longrightarrow \sigma_k(m)$

sends $(m, \sigma_k(m))$

Bob $\xrightarrow{(m, \sigma_k(m))}$ Charlie

Alice's public key p

m

$\sigma_k(m) \longrightarrow$ verify

Alice's public key p

m

$\sigma_k(m) \longrightarrow$ verify

- only Alice can create $\sigma_k(m)$
- anyone can verify (using public key)

Digital Signatures for Quantum States are Impossible

- Given $|\psi\rangle$, Alice produces signed state $S_k(|\psi\rangle\langle\psi|)$ (depends on private key k)
- Any recipient Bob can perform

$$U : S_k(|\psi\rangle\langle\psi|) \longmapsto |\psi\rangle\langle\psi| \otimes \rho_{k,|\psi\rangle}$$

$\rho_{k,|\psi\rangle}$ must be independent of $|\psi\rangle$!

- U can be performed efficiently

To cheat, Bob performs U,

then

$$|\psi\rangle\langle\psi| \otimes \rho_k \longmapsto |\phi\rangle\langle\phi| \otimes \rho_k$$

then

$$U^\dagger : |\phi\rangle\langle\phi| \otimes \rho_k \longmapsto S_k(|\phi\rangle\langle\phi|)$$

- $U^\dagger$ is also efficient

Any recipient can change the state

Unclonable Encryption

Alice & Bob share classical key k

Classical message M

Quantum authentication scheme A_k

Alice sends $A_k(|M\rangle)$ to Bob

Eve intercepts, attempts to copy (has state $\rho_k(M)$).

Bob receives message.

Eve learns k.

By security of quantum authentication,

1) Bob detects Eve's copying

or 2) Eve has almost no info about M

(or a superposition $\Sigma |M\rangle$ would be entangled with Eve)

Conclusions

- Efficient, non-interactive authentication is possible, using classical key
- Quantum authentication requires encryption (auth. in one basis needs encrypt. in other)
- Unclonable encryption of classical messages

(authentication related to BB84 quantum key distribution)