# An authentication scheme for QKD protocols

Minh-Dung Dang

TELECOM PARIS
école nationale supérieure des télécommunications

2006

# Outline

# Outline

# Unconditionally secure QKD links

## Usual communication with QKD

1. Alice and Bob exchange via QKD a random key which cannot be eavesdropped
2. Alice enciphers the confidential message, using Vernam cipher with the shared key

# QKD links without Authentication

## Man-in-the-middle attack

1. Eve impersonates Bob and exchange a key $k_a$ with Alice
2. Eve impersonates Alice and exchange a key $k_b$ with Bob
3. Whenever Alice sends a message, ciphered with $k_a$, Eve deciphers; reads; ciphers with $k_b$ and sends to Bob
4. Eve's actions are transparent and not recognized by Alice and Bob

# Authentications for QKD

- *Approach 1*: applying authentication to the key, after running QKD.
  - Classical authentication: public-key, secret-key using Universal Hashing.
  - Quantum authentication: using shared EPR pairs
- *Approach 2*: inserting authentication codes into *qubits* during QKD run.

# Classical authentication

- Alice and Bob want to communicate messages in a set $M$
- They agree on rules of producing authenticators for messages: the set of these is $T$
- The sender sends a message with its authenticator
- The receiver always accepts if the message and its authenticator come from the true sender, not from the other.
- Impersonating attack: Eve produces a pair $m, t$ that is accepted by the receiver
- Substituting attack: Eve receives $m, t$ from the sender, and can make $m' \neq m, t'$ which is accepted by the receiver.

# Outline

1. Problems
2. **Universal hashing**
3. Authentication for ideal QKD link
4. For a practical use

# Universal hashing and authentication

## Definition

An ensemble $H$ of hash functions $M \mapsto T$ is $\epsilon$ *almost strongly universal* ($\epsilon$-ASU) if

- For any message $m \in M$ and tag $t \in T$, there are $|H|/|T|$ functions of $H$ that map $m \rightarrow t$
- $\forall m_1 \neq m_2 \in M$ and $\forall t_1, t_2 \in T$, there exist at most $\epsilon|H|/|T|$ functions of $H$ that map both $m_i \rightarrow t_i$

- Probability of successful impersonating: $pd_0 = 1/|T|$
- Probability of successful substituting: $1/|T| \leq pd_1 \leq \epsilon$ $(\epsilon \geq 1/|T|)$

# Some good ASU

- $a = log(|M|)$, $b = log(|T|)$, $k = log(|H|)$
- Wegman-Carter
  - $s = b + log(log(a))$, $k = 4s * log(a)$
  - $pd_1 \leq 2/|T| = 1/2^{b-1}$
- Bierbrauer et al.
  - $a = (b + s)(2^s + 1)$, $k = 3b + 2s$
  - $pd_1 \leq 1/2^{b-1}$

# Counter-based Multiple Authentication

## Wegman-Carter method

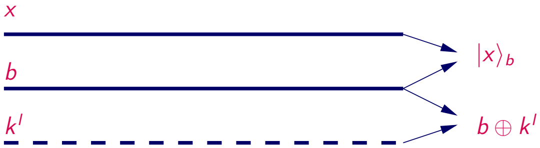
- Let $H$ an $\epsilon$-ASU: Alice and Bob have to share a key $k$ of $log(|H|)$ bits
- Alice and Bob share still $n-1$ strings of $b$ bits, indexed from $2$ to $n$: $\omega_2, .., \omega_n$
- Alice and Bob can authenticate $n$ messages
  - $t_1 = H_k(m_1)$
  - $t_i = H_k(m_i) \oplus \omega_i$
- The probability for Eve of producing a good pair $m', t'$ after receiving $0 \leq i \leq n$ is $pd_i \leq \epsilon$

# Outline

# The proposed scheme

## … for ideal BB84 link

- Alice and Bob preposition random $k$.
- Alice creates $x$ - raw key, $b$ - bases: $|x| = |b| = n$.
- Alice sends qubits encoding $x$ in $b$ to Bob.
- Alice sends $b \oplus k^l$ to Bob: $n = l * |k|$.
- Bob deciphers $b$ and decodes the qubits for $x$.
- $m$ rounds mutually:
  - Alice sends a random string $s$ to Bob; who sends back the parity bit $x \odot s = \bigoplus_i x_i.s_i$; Alice computes $x \odot s$ on his own $x$, compares and rejects if it's different
  - Bob's turn to verify



# Impersonating attack

- Eve tries to produce authentication codes to pass
- $H(b/b \oplus k^l) = |k|$
- $I(x; |x\rangle_b, b \oplus k^l, |x\rangle_b / b \oplus k^l)$: Holevo bound
    - $= l * \delta$ if Eve measures each photons individually
    - $= l - 1$ if Eve can measure $l$ photons collectively
- Let $g(l) = l - (x; |x\rangle_b, b \oplus k^l, |x\rangle_b / b \oplus k^l)$
- $\Rightarrow H(x/ |x\rangle_b, b \oplus k^l) > |k| * g(l) \geq |k|$
- High probability of being detected in $m$ parity check rounds

# Impersonating attack

- Authentication-key revelation
    - By observing only $|x\rangle_b$, Eve has no information about $b$ and thus $k$.
    - Eve gets $m$ parity bits from Alice: discovering no more than $m$ bits of $k$.
- $H(x) \geq (|k| - m) * g(l)$
- High probability of being detected in $m$ parity check rounds

# Substituting attack

- Eve can modify the exchanged key without knowing it
  - When received a qubit at position $i$, Eve inverse it by the NOT operator and resends to Bob
  - In each parity check round, if the key bit at $i$ is selected, Eve flip also the parity bit
- This attack is eliminated by classical authentication
- But this attack is not important in QKD protocol
- It has the same effect as
  - After Alice and Bob have exchanged a key, they apply Vernam cipher to exchange a message
  - Eve flip the ciphertext at position $i$

# For practical BB84: post-correction

- Because of errors, one needs Error Correction
  - Channel noise
  - Noise caused by presence of Eve
- Eve can correct all of the noises ?
- With actual technology, Eve can only measure each photon individually. $H(x) = |k| * g(l)$ is important, and BER is high
- Channel BER is much smaller than BER caused by wrong authentication keys.
- We can use thresholds on BER to prevent Man-in-the-middle attacks
- But it's difficult to compute how much information of the key Eve can get

# Outline

# For more advanced technology

## Pre-correction of errors

- Lo & Chau proposed a method for establishing noiseless quantum channel over noisy one
  - Sending half of EPR pairs via the noisy channel
  - Using entanglement purification protocol to extract nearly perfect EPR pairs from them
  - Applying QKD upon noiseless EPR channel
- This pre-correction is convenient for our authentication scheme

# Parity check for EPR pairs I

## Quantum hashing

Denote EPR pairs by 2-bits string

$$(|00\rangle + |11\rangle)/\sqrt{2} \rightarrow 00$$
$$(|01\rangle + |10\rangle)/\sqrt{2} \rightarrow 01$$
$$(|00\rangle - |11\rangle)/\sqrt{2} \rightarrow 10$$
$$(|01\rangle - |10\rangle)/\sqrt{2} \rightarrow 11$$

- Suppose Alice and Bob share $n$ pairs, represented by a string $R$ of $2n$ bits where $R[2i, 2i+1]$ stands for $i^{th}$ pair
- Alice and Bob agree on a subset index string $s$ of $2n$ bit.

# Parity check for EPR pairs II

## Quantum hashing

- With local operations, they can compute $s \odot R$, and the result is stored in a target pair (eg. the first pair of $R$)
- They communicate (quantum or classical measurement outcome) to verify this target pair

# Authentication for EPR based QKD

- Suppose that after running Lo-Chau method, Alice and Bob share $n$ perfect $00$ EPR pairs $(|00\rangle + |11\rangle)/\sqrt{2}$
- Each user runs $m \in O(log(1/\epsilon))$ verification round
  - Verifier generates a random $n$-bits string $s_1$, and flips his own bit of the pair $i$ if $s_1[i] = 1$, i.e. the $i^{th}$ pair is $01$ EPR state $(|01\rangle + |10\rangle)/\sqrt{2}$
  - Verifier generates $2n$ bit subset index string $s_2$, announces it to Prover and they compute the parity of EPR pairs into the first pair.
  - Only the Verifier can know the state of the target pair
  - Prover measures his own qubit of the first pair, XOR the result with a bit of the authentication key, and sends to Verifier

# Comparison

- The probability of cheating is $1/2^{b-1}$
- Classical authentication needs
  - A good ASU - not optimal $k = C * b$: $C > 2$
  - And a key of $b$ bit for each message more
  - Ie. $C * b + (n-1)b$ bits for $n$ sessions
- Our quantum authentication (for EPR scheme) needs
  - At most $b$ key bits for each verification
  - Ie. $2b + (n-1)b$ bits for $n$ sessions : optimal

## The End!

Thank you for your attention!