Looking for an Optimal Authentication Scheme in Quantum Key Distribution

Romain. Alléaume, Minh-Dung Dang, Patrick Bellot

Get/ENST

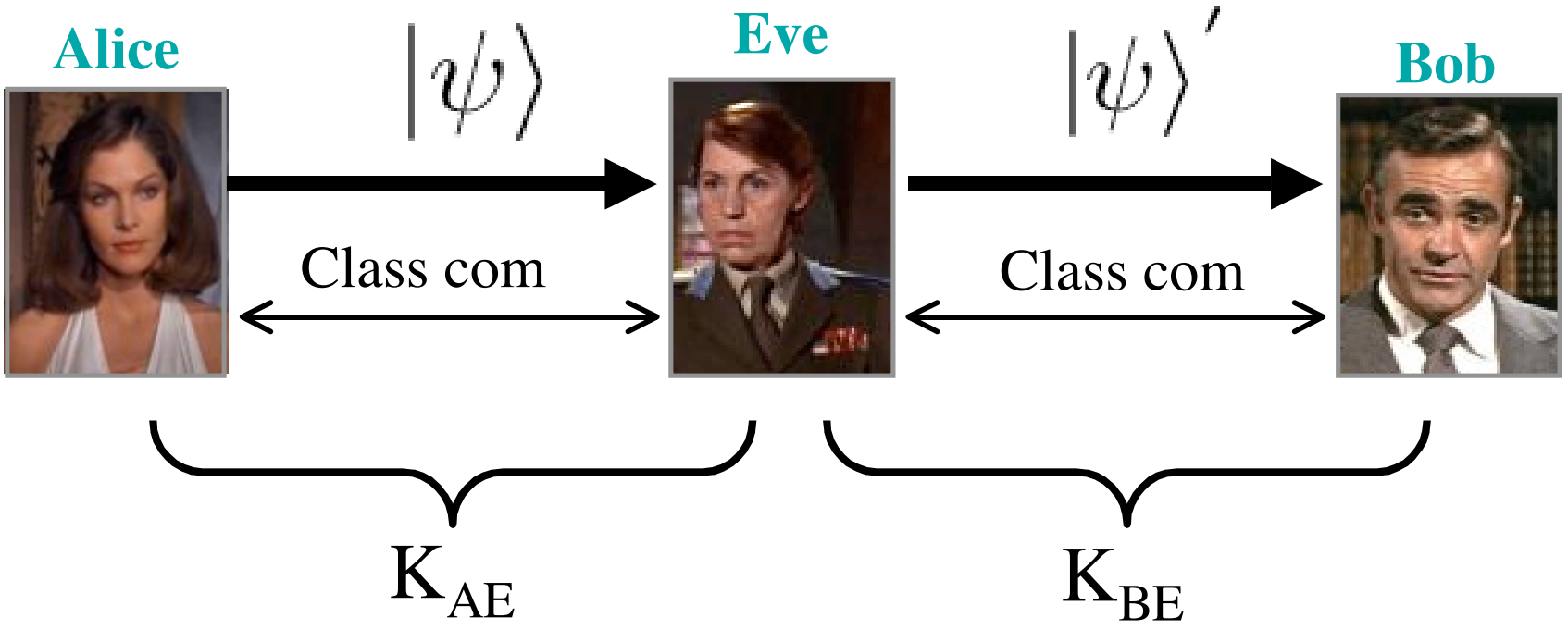
Ecole Nationale Supérieure des Télécommunications

LTCI-UMR 5141 CNRS, Paris, France.

Corresponding author : romain.alleaume@enst.fr

Motivations (1)

QKD protocols taken alone do not provide authentication, that is however needed so that they are not vulnerable to man in the middle attacks



Authentication is needed to prevent **impersonation** or **substitution** attacks ***on the key***

Motivations (2)

Authentication has to be done via information-theoretic schemes.

These schemes need a previously prepositionned symmetric secret.

Quantum Key Distribution should in this perspective be considered as ***Quantum Key Growing.*** *(Bennett, Brassard).*

Our question is :

Is there a way to minimize, for a given security level, the amount of secret needed for authentication ?

=> optimal authentication schemes ?

Motivations (3)

Authentication schemes relying on a prepositionned symmetric secret key are vulnerable to Denial of Service attacks (DoS).

With DoS, a third party, could exhaust prepositionned key material that has been securely and costly exchanged among legitimate users.

Is it possible to devise authentication scheme for QKD that is resistant to DoS attacks ?

Generic phases of a QKD protocol

1. Distribution of correlated quantum data through the physical exchange of a string of single qubits from Alice to Bob. This distribution can be reduced to classical correlations + a control parameter (error rate, etc…) according to the projective measurements performed by Bob

2. Reconciliation : Secret-Key agreement over an unauthenticated public channel (cf [Maurer & Wolf])

What could an optimal authentication scheme be ?

Information-theoretic bound of the probability of success of Impersonation and Substitution attack

Require as little secret material necessary, ideally none (greater resistance to DoS attack)

[Renner Wolf 04] ***The assumption that Alice and Bob share a short key initally is unnecessarily strong***

Question : How to design such a scheme in the case of BB84 ?

Almost Strongly Universal class of Hash functions

Definition :

Let $\epsilon > 0$. A class H of functions from A to B is called ϵ almost strongly universal (ϵ -ASU) if :

1) For every $x \in A$ and $y \in B$

$$|\{h \in H : h(x) = y\}| = \frac{|H|}{|B|}$$

2) For every $x_1, x_2 \in A, x_1 \neq x_2, \quad y_1, y_2 \in B,$

$$|\{h \in H : h(x_1) = y_1, h(x_2) = y_2\}| \leq \epsilon . \frac{|H|}{|B|}$$

A class is strongly universal is it $1/|B|-$ ASU.

Information-theoretically secure authentification

When using an ϵ -ASU class of function for authentication :

Pimpersonation = 1/|B|
Psubstition $\leq \epsilon$

Example : Wegman-Carter (81)
Length of the authenticator tag : t
Length of the message : m
Cost (secret bits) :

$$4(t + log_2 \, log_2 \, m) log_2 \, m$$

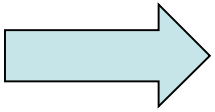
Exact cost of continuous authentication : Cf [Gilbert, Hamrick] quant-ph 009027

(Simple) Idea :
One Time Pad encryption of the basis

Idea: exploit the randomness of the encoding basis to perform one-time pad encoding :
If M is a random message of size m, H(M) = m

$$H(K|C) = H(M) + H(K) - H(C)$$

For OTP, H(C) = m, H(K) = m



$$H(K|C) = H(K)$$

Our - incomplete - authenticated BB84 protocol

Authentication scheme for the QKD.

1. Alice generates a random bit string and, for presenting each bit, uses a quantum eigen state in a random basis $\{\oplus, \otimes\}$. Alice sends these quantum states to Bob.
2. Bob uses a random basis to measure each received quantum states.
3. Bob uses a bit string b_b to present his bases: 0 for $\oplus$; 1 for $\otimes$, encrypts this string with the key k_b , and sends to Alice $(b_b \oplus k_b)$ using the classical channel.
4. Alice uses a bit string b_a to present her bases, and sends her used bases encrypted with the key k_a to Bob, i.e. $(b_a \oplus k_a)$ on the classical channel.
5. Alice and Bob decrypt the bases used by each other and could then find out $(b_a \oplus b_b)$. They discard the results at all positions i with $b_a[i] \oplus b_b[i] = 1$ and interpret the rest of results to two strings x_a and x_b.
6. Alice and Bob can compare some distilled bits from x_a and x_b to detect the presence of Eve or to validate the authentication

First Elements of analysis

Usual BB84 + Wegman Carter

Distribution of correlations
QBER check
Key distillation
Equivalence check **authenticated**

Our protocol

Distribution of correlations
Encryption of sifting
QBER check
Key distillation
Equivalence check (**non-auth**)

How can it lead to an improvement ? :

Wegman-Carter + OTP allow for reuse of secret material (polynomial number of time).

Our scheme should allow to calculate extensively the information learnt by Eve for one instance of the protocol => optimisation