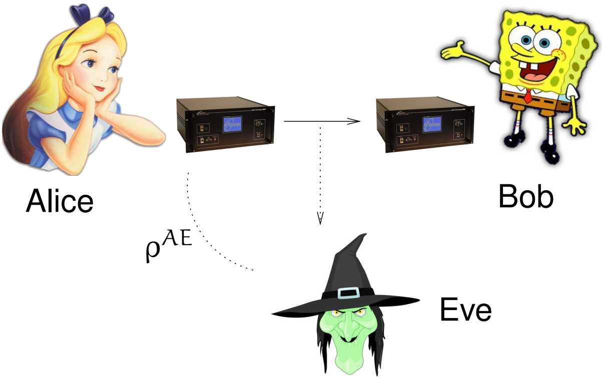
Quantum entropic security and approximate quantum encryption

Frédéric Dupuis, Université de Montréal and McGill University
joint work with Simon-Pierre Desrosiers

QIP 2008, New Delhi

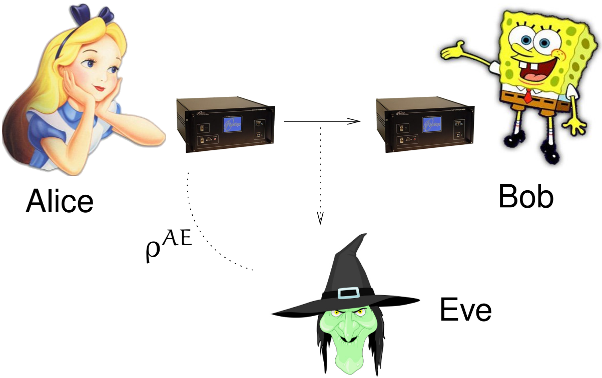
Outline

Quantum encryption



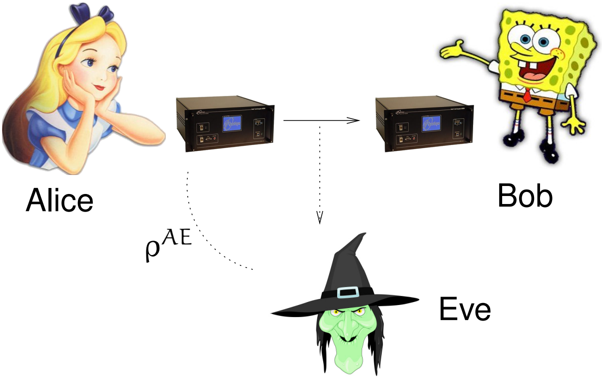
- Alice has a quantum state that she wants to send to Bob without Eve getting any information about it if she intercepts the transmission.

Quantum encryption



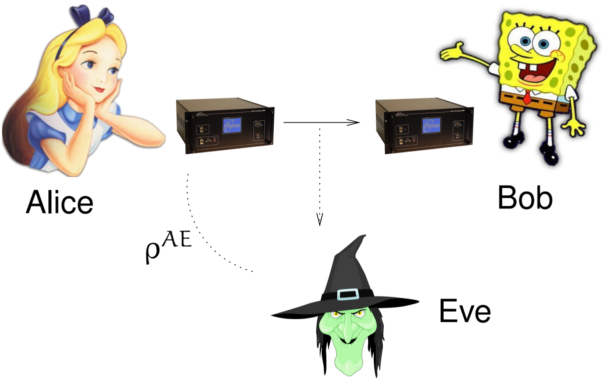
- Alice has a quantum state that she wants to send to Bob without Eve getting any information about it if she intercepts the transmission.
- Eve may have some partial quantum information about the message.

Quantum encryption



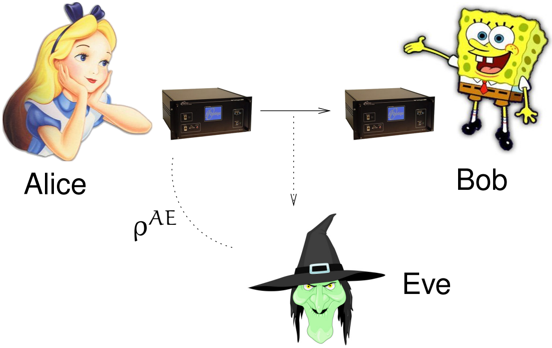
- Alice and Bob share a private classical key to encrypt the message.

Quantum encryption



- Alice and Bob share a private classical key to encrypt the message.
- In this talk, we always assume we want to encrypt n qubits.

Quantum encryption



Security criterion:

$$\forall \rho^{AE} \qquad (\mathcal{E} \otimes \mathbb{I})(\rho^{AE}) = \frac{\mathbb{I}^{A}}{d_A} \otimes \rho^{E}$$

So, no matter what the input is, all Eve ever sees is her own prior information $\Rightarrow$ Eve gains no information

Here's a simple way to do it [Ambainis, Mosca, Tapp, de Wolf]:

- Apply one of the 4 Pauli operators to each qubit to be encrypted

Here's a simple way to do it [Ambainis, Mosca, Tapp, de Wolf]:

- Apply one of the 4 Pauli operators to each qubit to be encrypted
- The key determines which operator is applied.

Here's a simple way to do it [Ambainis, Mosca, Tapp, de Wolf]:

- Apply one of the 4 Pauli operators to each qubit to be encrypted
- The key determines which operator is applied.
- How many bits do we need? 4 Pauli operators $\Rightarrow$ 2 bits per qubit $\Rightarrow 2n$ bits in total.

Here's a simple way to do it [Ambainis, Mosca, Tapp, de Wolf]:

- Apply one of the 4 Pauli operators to each qubit to be encrypted
- The key determines which operator is applied.
- How many bits do we need? 4 Pauli operators $\Rightarrow$ 2 bits per qubit $\Rightarrow 2n$ bits in total.
- It is easy to show that

$$(\mathcal{E} \otimes \mathbb{I})(\rho^{AE}) = \frac{\mathbb{I}}{d_A} \otimes \rho^{E} \qquad \forall \rho^{AE}$$

Here's a simple way to do it [Ambainis, Mosca, Tapp, de Wolf]:

- Apply one of the 4 Pauli operators to each qubit to be encrypted
- The key determines which operator is applied.
- How many bits do we need? 4 Pauli operators $\Rightarrow$ 2 bits per qubit $\Rightarrow 2n$ bits in total.
- It is easy to show that

$$(\mathcal{E} \otimes \mathbb{I})(\rho^{AE}) = \frac{\mathbb{I}}{d_A} \otimes \rho^{E} \qquad \forall \rho^{AE}$$

- So we can encrypt n qubits perfectly using $2n$ bits of key. Can we do better?

Approximate quantum encryption

- Answer: Not with this security definition. But what if we allow just a little bit of information leakage?
- Relaxed definition:

$$\forall \rho^{AE} \qquad \left\| (\mathcal{E} \otimes \mathbb{I})(\rho^{AE}) - \frac{\mathbb{I}}{d_A} \otimes \rho^{E} \right\|_1 \leqslant \varepsilon$$

  where $\|\rho - \sigma\|_1 := \mathrm{Tr}\,|\rho - \sigma|$.
- Still doesn't help: we need at least $2n - 1$ bits of key.
- Need an additional assumption.
- In the literature so far: assume ρ^{AE} is not entangled.

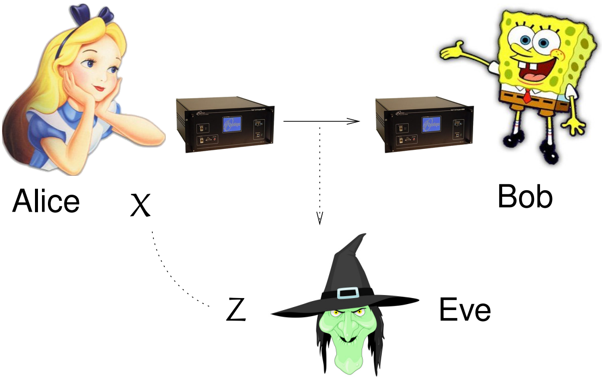
Approximate quantum encryption

Two methods for non-entangled states

- First proposal by Hayden, Leung, Shor, Winter using sets of random transformations brought it down to $n + \log n + 2\log(1/\varepsilon) + O(1)$.
- Two explicit constructions by Ambainis and Smith requiring $n + 2\log n + 2\log(1/\varepsilon)$ and $n + 2\log(1/\varepsilon)$ bits of key.
- So we have:
  - No entanglement: about n bits of key, same as classical
  - With entanglement: need $2n$ bits.
- Is there nothing in between? What if it's entangled only a little bit?

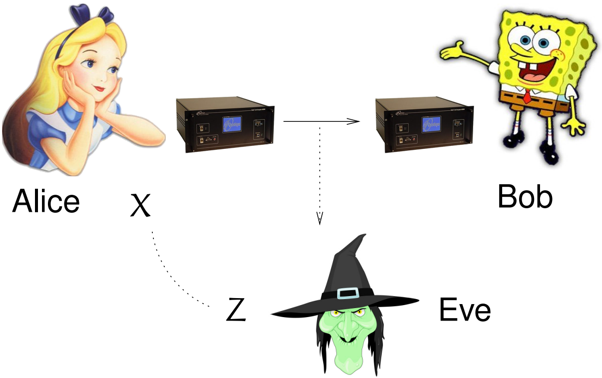
Classical encryption

Classical encryption



- Alice has a classical message that she wants to send to Bob without Eve getting any information about it if she intercepts the transmission.
- Eve may have some partial classical information about the message.

Classical encryption



- Alice and Bob share a private classical key to encrypt the message.
- With no assumption on the input state, we need at least $n - 1$ bits of key. What assumption can we make to reduce this?

- Suppose that we have a lower bound on Eve's prior knowledge of the message. Then we might be able to vary the key size based on this lower bound.
- A natural way to characterize this prior knowledge is the *conditional min-entropy* of the message X given the adversary's knowledge Z:

$$H_\infty(X|Z) := -\log\left[\max_{z\in\mathcal{Z},x\in\mathcal{X}} p(x|z)\right]$$

Note: slightly different from this morning...
This definition: in the worst-case scenario, what will be Eve's best chance of guessing the message?

Entropic security and indistinguishability

Here is a security definition based on min-entropy:

Definition (Entropic indistinguishability, from Dodis and Smith)

A probabilistic encryption scheme E *is* (t, ε)*-indistinguishable if for all message distributions such that* $H_\infty(X|Z) \geqslant t$*,*

$$D(P_{E(X),Z}, P_U P_Z) \leqslant \varepsilon$$

Here, $D(P, Q) = \sum_{x \in \mathcal{X}} |P(x) - Q(x)|$.

This definition is easy to work with, but not directly based on operational ideas.

Entropic security:

VS

$\mathcal{E}(X), Z$ $\qquad$ Z

We say $\mathcal{E}$ is secure if the Eve on the left can't eavesdrop better than the Eve on the right

Entropic security and indistinguishability

Definition (Entropic security, modified from Russell and Wang)

A probabilistic encryption scheme E *is* (t, ε)*-entropically secure if for every adversary* $\mathcal{A}$*, there exists an adversary* $\mathcal{A}'$ *such that for all functions* f*, then*

$$\left|\Pr[\mathcal{A}(E(X), Z) = f(X, Z)] - \Pr[\mathcal{A}'(Z) = f(X, Z)]\right| \leqslant \varepsilon$$

as long as $H_\infty(X|Z) \geqslant t$

Entropic indistinguishability and entropic security can be shown to be equivalent up to small variations in the parameters t and ε.

Entropic security and indistinguishability

- How much key do we need to achieve this?
- Dodis and Smith present a scheme with $n - t + 2\log(1/\varepsilon) + O(1)$ bits of key, as long as $H_\infty(X|Z) \geqslant t$.
- Can we get a quantum version of this?

Our results

- We generalize the notions of entropic security and indistinguishability to the quantum world.
- We prove that the two Ambainis-Smith schemes fit these security definitions unmodified.
- We give a simple lower bound of $n - t - 1$ bits of key.

Quantum conditional min-entropy

- How do we measure Eve's uncertainty in the quantum case?
- Quantum conditional min-entropy: again, slightly different from this morning…

$$
\begin{aligned}
H_\infty(\rho^{AE}|\rho^{E}) &= \min\left\{\lambda \in \mathbb{R} : \rho^{AE} \leqslant 2^{\lambda}\mathbb{I}^{A} \otimes \rho^{E}\right\} \\
&= -\log\left[\max_{|\psi\rangle} \frac{\langle\psi|\rho^{AE}|\psi\rangle}{\langle\psi|\mathbb{I}\otimes\rho^{E}|\psi\rangle}\right]
\end{aligned}
$$

Quantum conditional min-entropy

A few properties of quantum conditional min-entropy:

- For an n-qubit state:

  $$-n \leqslant H_\infty(\rho^{AE}|\rho^E) \leqslant n$$

  The lower bound is saturated by a maximally entangled state between A and E, and the upper bound, by the maximally-mixed state.
- If ρ^{AE} is separable, then $H_\infty(\rho^{AE}|\rho^E) \geqslant 0$.

Quantum entropic indistinguishability

We can use this to define a new notion of security:

Definition (Quantum entropic indistinguishability)

A quantum encryption system $\mathcal{E}$ is (t, ϵ)-indistinguishable if for all states ρ^{AE} such that $H_\infty(\rho^{AE}|\rho^E) \geqslant t$ we have that:

$$\left\| (\mathcal{E} \otimes \mathbb{I})(\rho^{AE}) - \frac{\mathbb{I}}{d_A} \otimes \rho^E \right\|_1 \leqslant \varepsilon$$

Quantum entropic security

How do we generalise the concept of “function on the input”?

- Consider every possible *interpretation* of ρ^{AE}:

$$\rho^{AE} = \sum_j p_j \sigma_j^{AE}$$

- We’ll consider functions on j.
- This covers information encoded in any basis.

Quantum entropic security

Quantum entropic security:

VS

$(\mathcal{E} \otimes \mathbb{I})(\rho^{AE})$ ρ^{E}

We say $\mathcal{E}$ is secure if the Eve on the left can't eavesdrop better than the Eve on the right

Quantum entropic security

Definition (Quantum entropic security)

A quantum encryption system $\mathcal{E}$ *is* (t, ε)*-entropically secure if for all states* ρ^{AE} *such that* $H_{\min}(\rho^{AE}|\rho^{E}) \geqslant t$*, all interpretations* $\{(p_j, \sigma_j^{AE})\}$ *and all adversaries* A*, there exists an* A' *such that for all functions* f*, we have*

$$\left| \Pr[A((\mathcal{E} \otimes \mathbb{I})(\sigma_i^{AE})) = f(i)] - \Pr[A'(\sigma_i^{E}) = f(i)] \right| \leqslant \varepsilon.$$

Quantum entropic security and indistinguishability

In our paper, we've shown that

- $(t-1, \varepsilon/2)$-indistinguishability implies (t, ε)-entropic security.
- (t, ε)-entropic security implies $(t-1, 6\varepsilon)$-indistinguishability as long as $t \leqslant n-1$.

Just like the classical case, despite the fact that everything here is quantum.

The Ambainis-Smith schemes

- Perfect encryption: $\mathcal{E}(\rho) = \sum_{(k_x,k_z)} X^{k_x} Z^{k_z} \rho Z^{k_z} X^{k_x}$, where

$$X^{k_x} = X^{k_x^{(1)}} \otimes X^{k_x^{(2)}} \otimes \cdots X^{k_x^{(n)}}$$
$$Z^{k_z} = Z^{k_z^{(1)}} \otimes Z^{k_z^{(2)}} \otimes \cdots Z^{k_z^{(n)}}$$

- Ambainis-Smith schemes: pick k_x and k_z from a smaller set of bitstrings that behave almost like random bitstrings.

The first Ambainis-Smith scheme

Definition (δ-biased set)

A set $S \subseteq \{0,1\}^n$ is said to be δ-biased iff for every $s' \in \{0,1\}^n, s' \neq 0^n$, we have that $\left|\mathbb{E}_{s \leftarrow S}\left[(-1)^{s \odot s'}\right]\right| \leqslant \delta$.

Picking strings from a δ-biased set is almost like choosing strings at random when it comes to taking parities.

The construction we need [Alon, Goldreich, Håstad, Peralta] yields sets of size n^2/δ^2.

The first Ambainis-Smith scheme

$$\mathcal{E}(\rho) = \sum_{(k_x, k_z)} X^{k_x} Z^{k_z} \rho Z^{k_z} X^{k_x}$$

If we pick (k_x, k_z) from a δ-biased set of $2n$-bit strings, and that $H_\infty(\rho^{AE}|\rho^E) \geqslant t$, we can show that

$$\left\| (\mathcal{E} \otimes \mathbb{I})(\rho^{AE}) - \frac{\mathbb{I}}{2^n} \otimes \rho^E \right\|_1 \leqslant \delta\sqrt{2^{n-t}}$$

So if we pick $\delta = \varepsilon/\sqrt{2^{n-t}}$, we're fine.

How many bits of key do we need for that?
$\log(2n)^2/\delta^2 = \log[2^{(n-t)}(2n)^2/\varepsilon^2] = n - t + 2\log n + 2\log(1/\varepsilon) + 2$.

The Ambainis-Smith scheme

Ambainis and Smith also give a second scheme which requires only $n - t + 2\log(1/\varepsilon)$ bits of key, but doubles the size of the ciphertext.

Connection with previous results

We can retrieve previous results from this:

- If we assume no entanglement between Alice and Eve, we implicitly have $t \geqslant 0$, and hence we need roughly $n - t = n$ bits of key.
- If we have no bound whatsoever on Eve's knowledge, our best bound is $t \geqslant -n$ and we need at least $n - t = 2n$ bits of key.

A simple lower bound on the key length

We can show that $n - t$ is essentially the optimal number of key bits. Let's assume Alice wants to encrypt a state which consists of:

- $(n-t)/2$ halves of EPR pairs, with the other halves in Eve's hands
- $(n+t)/2$ maximally mixed qubits.

It is easy to show that that $H_\infty(\rho^{AE}|\rho^E) = t$: the EPR pairs contribute $-(n-t)/2$ and the rest contributes $(n+t)/2$ to the conditional min-entropy.

To encrypt this, we have to at least be able to encrypt the halves of EPR pairs; but we can show that that takes at least $2(n-t)/2 - 1 = n - t - 1$ bits of key.

Summary

Recap of what we have done:

- Gave quantum versions of entropic security and indistinguishability
- Showed that they are equivalent
- Showed that these definitions lead to a more complete understanding of approximate quantum encryption;
- Presented encryption schemes which achieve these security definitions;
- Showed that they are nearly optimal.

The End

Thank you!