Quantum Key Recycling

Joint work with
Ivan Damgård and Louis Salvail

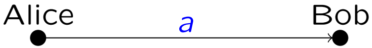
Thomas B. Pedersen

Department of Computer Science
University of Aarhus, Denmark

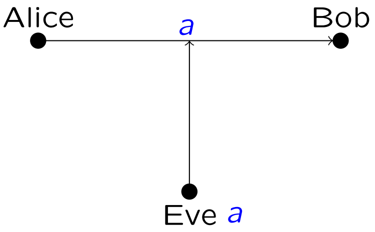
CRYPTO 2005
August 18

Outline

Motivation and Previous Work

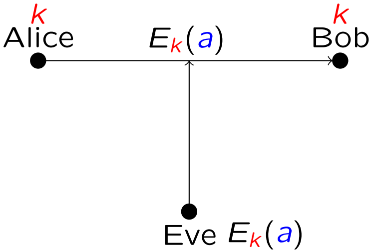


Motivation and Previous Work



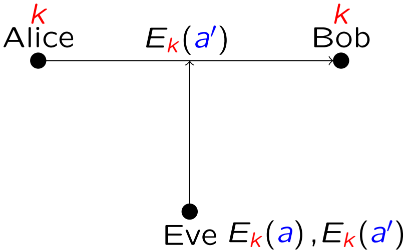
- Alice and Bob want *unconditional* confidentiality.

Motivation and Previous Work

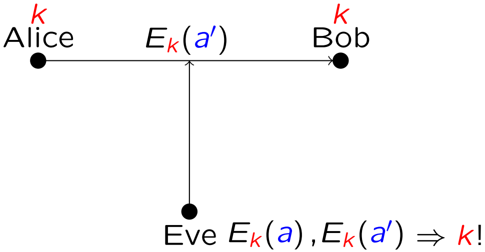


- Alice and Bob want *unconditional* confidentiality.

Motivation and Previous Work

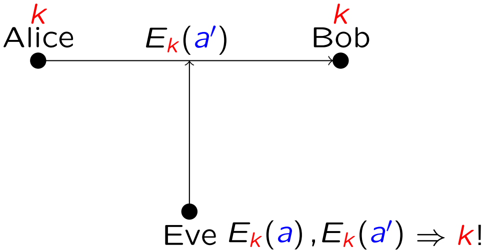


- Alice and Bob want *unconditional* confidentiality.



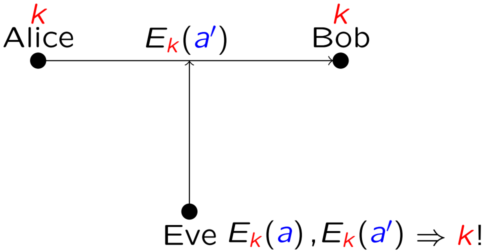
- Alice and Bob want *unconditional* confidentiality.
- When Eve has enough messages she can guess the key.

Motivation and Previous Work



- Alice and Bob want *unconditional* confidentiality.
- When Eve has enough messages she can guess the key.
- If no eavesdropping occurs, the key can be recycled.

Motivation and Previous Work



- Alice and Bob want *unconditional* confidentiality.
- When Eve has enough messages she can guess the key.
- If no eavesdropping occurs, the key can be recycled.
- Is there a way to detect eavesdropping?

Quantum Authentication

- Detects eavesdropping.

Motivation and Previous Work

Using Quantum Mechanics

Quantum Authentication

- Detects eavesdropping.
- Is an encryption scheme (Barnum, Crépeau, Gottesman, Smith, and Tapp).

Quantum Authentication

- Detects eavesdropping.
- Is an encryption scheme (Barnum, Crépeau, Gottesman, Smith, and Tapp).

Recycling Scheme by Oppenheim and Horodecki

- Uses standard quantum authentication.

Quantum Authentication

- Detects eavesdropping.
- Is an encryption scheme (Barnum, Crépeau, Gottesman, Smith, and Tapp).

Recycling Scheme by Oppenheim and Horodecki

- Uses standard quantum authentication.
- Key size $2(m + s)$.

Quantum Authentication

- Detects eavesdropping.
- Is an encryption scheme (Barnum, Crépeau, Gottesman, Smith, and Tapp).

Recycling Scheme by Oppenheim and Horodecki

- Uses standard quantum authentication.
- Key size $2(m+s)$.
- $2m+s$ bits recycled when authentication succeeds.

Quantum Authentication

- Detects eavesdropping.
- Is an encryption scheme (Barnum, Crépeau, Gottesman, Smith, and Tapp).

Recycling Scheme by Oppenheim and Horodecki

- Uses standard quantum authentication.
- Key size $2(m+s)$.
- $2m+s$ bits recycled when authentication succeeds.
- $m+s$ bits recycled when authentication fails.

Motivation and Previous Work

Using Quantum Mechanics

Quantum Authentication

- Detects eavesdropping.
- Is an encryption scheme (Barnum, Crépeau, Gottesman, Smith, and Tapp).

Recycling Scheme by Oppenheim and Horodecki

- Uses standard quantum authentication.
- Key size $2(m+s)$.
  - Key size $2(m+s')+m$.
- $2m+s$ bits recycled when authentication succeeds.
- $m+s$ bits recycled when authentication fails.

Quantum Authentication

- Detects eavesdropping.
- Is an encryption scheme (Barnum, Crépeau, Gottesman, Smith, and Tapp).

Recycling Scheme by Oppenheim and Horodecki

- Uses standard quantum authentication.
- Key size $2(m+s)$.
  - Key size $2(m+s')+m$.
- $2m+s$ bits recycled when authentication succeeds.
  - Entire key recycled.
- $m+s$ bits recycled when authentication fails.

Quantum Authentication

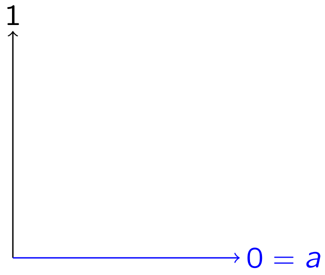
- Detects eavesdropping.
- Is an encryption scheme (Barnum, Crépeau, Gottesman, Smith, and Tapp).

Recycling Scheme by Oppenheim and Horodecki

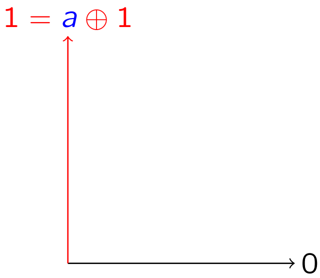
- Uses standard quantum authentication.
- Key size $2(m+s)$.
  - Key size $2(m+s')+m$.
- $2m+s$ bits recycled when authentication succeeds.
  - Entire key recycled.
- $m+s$ bits recycled when authentication fails.
  - $2m+s'$ bits recycled.

- Message: $a = 0$.
- Key: $(z, b) = (1, 1)$.

- Message: $a = 0$. (A vector in $\mathbb{F}_2^n$)
- Key: $(z, b) = (1, 1)$.

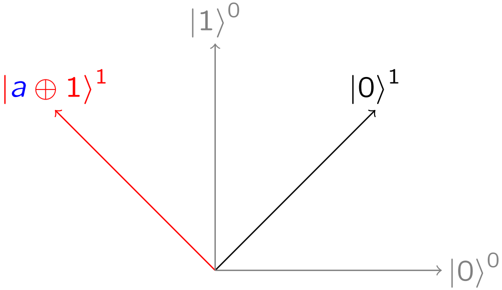


- Message: $a = 0$. (A vector in $\mathbb{F}_2^n$)
- Key: $(z, b) = (1, 1)$.



- Perform "one-time-pad" with 1.

- Message: $a = 0$. (A vector in $\mathbb{F}_2^n$)
- Key: $(z, b) = (1, 1)$.



- Perform "one-time-pad" with 1.
- Change quantum representation to basis 1.

- Wootters and Fields: $2^n + 1$ MUBs for n bits.

- Wootters and Fields: $2^n + 1$ MUBs for n bits.

Encrypting

$\mathcal{E}_{(z,b)}(a) = U_b|a \oplus z\rangle$ (basis change U_b).

- Wootters and Fields: $2^n + 1$ MUBs for n bits.

Encrypting

$\mathcal{E}_{(z,b)}(a) = U_b|a \oplus z\rangle\langle a \oplus z|U_b^\dagger$ (basis change U_b).

- Wootters and Fields: $2^n + 1$ MUBs for n bits.

Encrypting

$\mathcal{E}_{(z,b)}(a) = U_b|a \oplus z\rangle\langle a \oplus z|U_b^\dagger$ (basis change U_b).

Data hiding property

$$\rho_a = \sum_{(z,b)} p_{(z,b)}\mathcal{E}_{(z,b)}(a),$$

$$\|\rho_a - \rho_{a'}\| < \epsilon(n).$$

- Wootters and Fields: $2^n + 1$ MUBs for n bits.

Encrypting

$\mathcal{E}_{(z,b)}(a) = U_b|a \oplus z\rangle\langle a \oplus z|U_b^\dagger$ (basis change U_b).

Data hiding property

$$\rho_a = \sum_{(z,b)} p_{(z,b)}\mathcal{E}_{(z,b)}(a),$$

$$\|\rho_a - \rho_{a'}\| < \epsilon(n).$$

Theorem

$H(K|a, \mathcal{E}_{(z,b)}(a)) \geq 2n - 1$ *(EUROCRYPT 04)*.

- Eavesdropping introduce almost random noise.

- Eavesdropping introduce almost random noise.
- Wegman Carter one-time authentication ($h_u \in \mathcal{H}$).

- Eavesdropping introduce almost random noise.
- Wegman Carter one-time authentication ($h_u \in \mathcal{H}$).

Encrypting

$$\mathcal{E}'_{(z,b,u)}(a) = \mathcal{E}_{(z,b)}(a, h_u(a)).$$

- Eavesdropping introduce almost random noise.
- Wegman Carter one-time authentication ($h_u \in \mathcal{H}$).

Encrypting

$$\mathcal{E}'_{(z,b,u)}(a) = \mathcal{E}_{(z,b)}(a, h_u(a)).$$

Recycling

- Bob decrypts, verifies authentication, and send $\mathrm{acc}/\mathrm{rej}$ to Alice.

- Eavesdropping introduce almost random noise.
- Wegman Carter one-time authentication ($h_u \in \mathcal{H}$).

Encrypting

$$\mathcal{E}'_{(z,b,u)}(a) = \mathcal{E}_{(z,b)}(a, h_u(a)).$$

Recycling

- Bob decrypts, verifies authentication, and send $\mathrm{acc}/\mathrm{rej}$ to Alice.
- If Bob accepts the key is reused unmodified.

Our Encryption with Key Recycling

- Eavesdropping introduce almost random noise.
- Wegman Carter one-time authentication ($h_u \in \mathcal{H}$).

Encrypting

$$\mathcal{E}'_{(z,b,u)}(a) = \mathcal{E}_{(z,b)}(a, h_u(a)).$$

Recycling

- Bob decrypts, verifies authentication, and send $\mathrm{acc}/\mathrm{rej}$ to Alice.
- If Bob accepts the key is reused unmodified.
- If Bob rejects z is replaced.

- Two families of *hash functions* $\mathsf{R}^{n,s}_{\mathrm{acc}}$ and $\mathsf{R}^{n,t}_{\mathrm{rej}}$.

- Two families of *hash functions* $\mathsf{R}_{\mathrm{acc}}^{n,s}$ and $\mathsf{R}_{\mathrm{rej}}^{n,t}$.
- Bob announces $R \in \mathsf{R}_{\mathrm{acc}}^{n,s}$ or $R \in \mathsf{R}_{\mathrm{rej}}^{n,t}$.

- Two families of *hash functions* $\mathrm{R}_{\mathrm{acc}}^{n,s}$ and $\mathrm{R}_{\mathrm{rej}}^{n,t}$.
- Bob announces $R \in \mathrm{R}_{\mathrm{acc}}^{n,s}$ or $R \in \mathrm{R}_{\mathrm{rej}}^{n,t}$.
- $\hat{k} = R(k)$ is recycled.

- Two families of *hash functions* $\mathrm{R}^{n,s}_{\mathrm{acc}}$ and $\mathrm{R}^{n,t}_{\mathrm{rej}}$.
- Bob announces $R \in \mathrm{R}^{n,s}_{\mathrm{acc}}$ or $R \in \mathrm{R}^{n,t}_{\mathrm{rej}}$.
- $\hat{k} = R(k)$ is recycled.

Indistinguishability property

Give a, $\mathcal{E}_k(a)$, and R to Eve.

- Two families of *hash functions* $\mathrm{R}_{\mathrm{acc}}^{n,s}$ and $\mathrm{R}_{\mathrm{rej}}^{n,t}$.
- Bob announces $R \in \mathrm{R}_{\mathrm{acc}}^{n,s}$ or $R \in \mathrm{R}_{\mathrm{rej}}^{n,t}$.
- $\hat{k} = R(k)$ is recycled.

Indistinguishability property

Give a, $\mathcal{E}_k(a)$, and R to Eve.

$$\rho_{\hat{k}} = \sum_{k \in R^{-1}(\hat{k})} p_{k|\hat{k}} \mathcal{E}_k(a),$$

- Two families of *hash functions* $\mathrm{R}_{\mathrm{acc}}^{n,s}$ and $\mathrm{R}_{\mathrm{rej}}^{n,t}$.
- Bob announces $R \in \mathrm{R}_{\mathrm{acc}}^{n,s}$ or $R \in \mathrm{R}_{\mathrm{rej}}^{n,t}$.
- $\hat{k} = R(k)$ is recycled.

Indistinguishability property

Give a, $\mathcal{E}_k(a)$, and R to Eve.

$$\rho_{\hat{k}} = \sum_{k \in R^{-1}(\hat{k})} p_{k|\hat{k}} \mathcal{E}_k(a),$$

$$\|\rho_{\hat{k}} - \rho_{\hat{k}'}\| < \delta(n).$$

- Two families of *hash functions* $\mathrm{R}_{\mathrm{acc}}^{n,s}$ and $\mathrm{R}_{\mathrm{rej}}^{n,t}$.
- Bob announces $R \in \mathrm{R}_{\mathrm{acc}}^{n,s}$ or $R \in \mathrm{R}_{\mathrm{rej}}^{n,t}$.
- $\hat{k} = R(k)$ is recycled.

Indistinguishability property

Give a, $\mathcal{E}_k(a)$, and R to Eve.

$$\rho_{\hat{k}} = \sum_{k \in R^{-1}(\hat{k})} p_{k|\hat{k}} \mathcal{E}_k(a),$$

$$E[\|\rho_{\hat{k}} - \rho_{\hat{k}'}\|] < \delta(n).$$

- Two families of *hash functions* $\mathrm{R}_{\mathrm{acc}}^{n,s}$ and $\mathrm{R}_{\mathrm{rej}}^{n,t}$.
- Bob announces $R \in \mathrm{R}_{\mathrm{acc}}^{n,s}$ or $R \in \mathrm{R}_{\mathrm{rej}}^{n,t}$.
- $\hat{k} = R(k)$ is recycled.

Indistinguishability property

Give a, $\mathcal{E}_k(a)$, and R to Eve.

$$\rho_{\hat{k}} = \sum_{k \in R^{-1}(\hat{k})} p_{k|\hat{k}} \mathcal{E}_k(a),$$

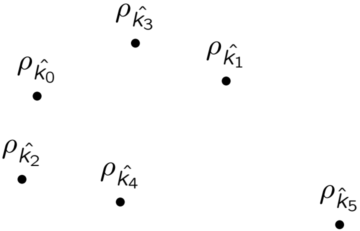
$$E[\|\rho_{\hat{k}} - \rho_{\hat{k}'}\|] < \delta(n).$$

Theorem

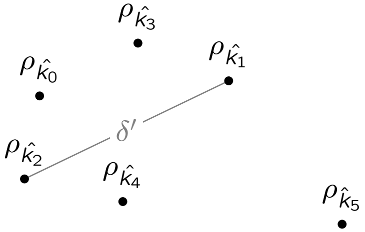
Under eavesdropping $t \leq n - m + 1$ *bits are recycled.*

- Assume $n - m + 2$ bits are recycled.

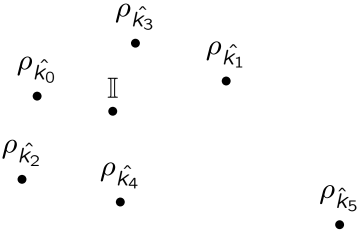
- Assume $n - m + 2$ bits are recycled.



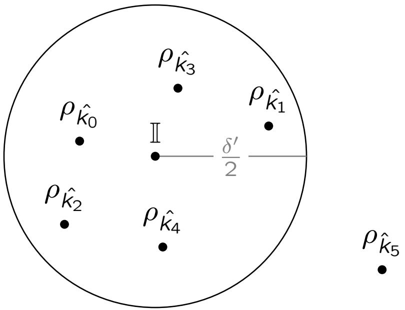
- Assume $n - m + 2$ bits are recycled.



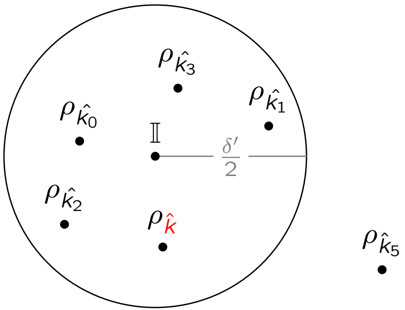
- Assume $n - m + 2$ bits are recycled.



- Assume $n - m + 2$ bits are recycled.

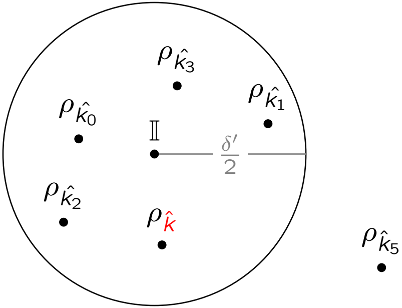


- Assume $n - m + 2$ bits are recycled.



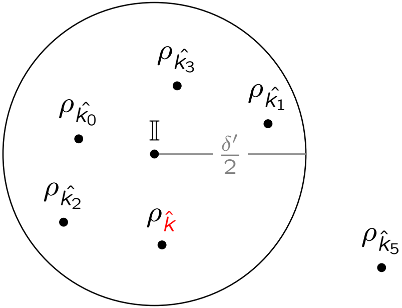
- $\hat{k}$ has small pre-image

- Assume $n - m + 2$ bits are recycled.



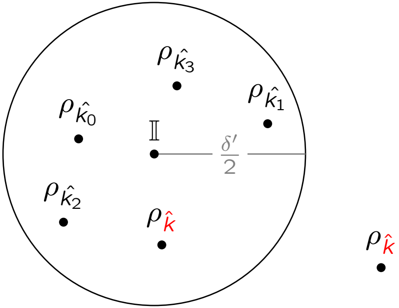
- $\hat{k}$ has small pre-image $\Rightarrow$ $\rho_{\hat{k}}$ has low rank.

- Assume $n - m + 2$ bits are recycled.



- $\hat{k}$ has small pre-image $\Rightarrow$ $\rho_{\hat{k}}$ has low rank.
- $\mathbb{I}$ has high rank.

- Assume $n - m + 2$ bits are recycled.



- $\hat{k}$ has small pre-image $\Rightarrow$ $\rho_{\hat{k}}$ has low rank.
- $\mathbb{I}$ has high rank.
- The result follows by contradiction.

Proof of Our Protocol

- Eve's action: $E = c_1\mathbb{I} + c_2\sigma_2 + \cdots + c_{4^n}\sigma_{4^n}$.

Proof of Our Protocol

- Eve's action: $E = c_1\mathbb{I} + c_2\sigma_2 + \cdots + c_{4^n}\sigma_{4^n}$.
- Lawrence, Brukner and Zeilinger: Partitions define MUBs.

Proof of Our Protocol

- Eve's action: $E = c_1\mathbb{I} + c_2\sigma_2 + \cdots + c_{4^n}\sigma_{4^n}$.
- Lawrence, Brukner and Zeilinger: Partitions define MUBs.

$$
2^n{+}1 \left\{ \begin{array}{cccc} \multicolumn{4}{c}{\overbrace{\hphantom{\mathbb{I} \quad \sigma_{(2^n+1,2)} \quad \cdots \quad \sigma_{(2^n+1,2^n)}}}^{2^n}} \\ \mathbb{I} & \sigma_{(1,2)} & \cdots & \sigma_{(1,2^n)} \\ \mathbb{I} & \sigma_{(2,2)} & \cdots & \sigma_{(2,2^n)} \\ \mathbb{I} & \sigma_{(3,2)} & \cdots & \sigma_{(3,2^n)} \\ \vdots & & & \vdots \\ \mathbb{I} & \sigma_{(2^n+1,2)} & \cdots & \sigma_{(2^n+1,2^n)} \end{array} \right.
$$

Proof of Our Protocol

- Eve's action: $E = c_1\mathbb{I} + c_2\sigma_2 + \cdots + c_{4^n}\sigma_{4^n}$.
- Lawrence, Brukner and Zeilinger: Partitions define MUBs.

$$2^n{+}1\left\{\overbrace{\begin{matrix} \mathbb{I} & \sigma_{(1,2)} & \cdots & \sigma_{(1,2^n)} \\ \mathbb{I} & \sigma_{(2,2)} & \cdots & \sigma_{(2,2^n)} \\ \mathbb{I} & \sigma_{(3,2)} & \cdots & \sigma_{(3,2^n)} \\ \vdots & & & \vdots \\ \mathbb{I} & \sigma_{(2^n+1,2)} & \cdots & \sigma_{(2^n+1,2^n)} \end{matrix}}^{2^n}\right.$$

Proof of Our Protocol

- Eve's action: $E = c_1\mathbb{I} + c_2\sigma_2 + \cdots + c_{4^n}\sigma_{4^n}$.
- Lawrence, Brukner and Zeilinger: Partitions define MUBs.

$$
2^n{+}1 \left\{ \begin{array}{cccc} \multicolumn{4}{c}{\overbrace{\hphantom{\mathbb{I} \quad \sigma_{(2^n+1,2)} \quad \cdots \quad \sigma_{(2^n+1,2^n)}}}^{2^n}} \\ \mathbb{I} & \sigma_{(1,2)} & \cdots & \sigma_{(1,2^n)} \\ \mathbb{I} & \sigma_{(2,2)} & \cdots & \sigma_{(2,2^n)} \\ \mathbb{I} & \sigma_{(3,2)} & \cdots & \sigma_{(3,2^n)} \\ \vdots & & & \vdots \\ \mathbb{I} & \sigma_{(2^n+1,2)} & \cdots & \sigma_{(2^n+1,2^n)} \end{array} \right.
$$

Proof of Our Protocol

- Eve's action: $E = c_1\mathbb{I} + c_2\sigma_2 + \cdots + c_{4^n}\sigma_{4^n}$.
- Lawrence, Brukner and Zeilinger: Partitions define MUBs.

$$2^n{+}1\left\{\overbrace{\begin{array}{cccc} \mathbb{I} & \sigma_{(1,2)} & \cdots & \sigma_{(1,2^n)} \\ \mathbb{I} & \sigma_{(2,2)} & \cdots & \sigma_{(2,2^n)} \\ \mathbb{I} & \sigma_{(3,2)} & \cdots & \sigma_{(3,2^n)} \\ \vdots & & & \vdots \\ \mathbb{I} & \sigma_{(2^n+1,2)} & \cdots & \sigma_{(2^n+1,2^n)} \end{array}}^{2^n}\right.$$

Proof of Our Protocol

- Eve's action: $E = c_1\mathbb{I} + c_2\sigma_2 + \cdots + c_{4^n}\sigma_{4^n}$.
- Lawrence, Brukner and Zeilinger: Partitions define MUBs.

$$
2^n{+}1 \left\{ \overbrace{\begin{array}{cccc}
\mathbb{I} & \sigma_{(1,2)} & \cdots & \sigma_{(1,2^n)} \\
\mathbb{I} & \sigma_{(2,2)} & \cdots & \sigma_{(2,2^n)} \\
\mathbb{I} & \sigma_{(3,2)} & \cdots & \sigma_{(3,2^n)} \\
\vdots & & & \vdots \\
\mathbb{I} & \sigma_{(2^n+1,2)} & \cdots & \sigma_{(2^n+1,2^n)}
\end{array}}^{2^n} \right.
$$

- $(0 \leq |c_1|^2 \leq 1)$ probability of no eavesdropping.

Proof of Our Protocol

- Eve's action: $E = c_1\mathbb{I} + c_2\sigma_2 + \cdots + c_{4^n}\sigma_{4^n}$.
- Lawrence, Brukner and Zeilinger: Partitions define MUBs.

$$2^n{+}1\left\{\overbrace{\begin{matrix} \mathbb{I} & \sigma_{(1,2)} & \cdots & \sigma_{(1,2^n)} \\ \mathbb{I} & \sigma_{(2,2)} & \cdots & \sigma_{(2,2^n)} \\ \mathbb{I} & \sigma_{(3,2)} & \cdots & \sigma_{(3,2^n)} \\ \vdots & & & \vdots \\ \mathbb{I} & \sigma_{(2^n+1,2)} & \cdots & \sigma_{(2^n+1,2^n)} \end{matrix}}^{2^n}\right.$$

- $(0 \leq |c_1|^2 \leq 1)$ probability of no eavesdropping.
- $p_{\mathrm{acc}} \leq |c_1|^2 + \mathrm{negligible}(n)$.

Conclusion

- Detecting eavesdropping.
- Worst case quantum = classical.
- Best case: entire key can be reused.