Centrum Wiskunde & Informatica

Quantum Authentication and Encryption with Key Recycling

Or: How to Re-use a One-Time Pad Even if P = NP — Safely & Feasibly

Serge Fehr
CWI Amsterdam

Louis Salvail
University of Montréal

Encryption & Authentication

- Schemes with **information theoretic security**
  - One-time pad: $E_k(m) = m + k$
  - Universal hashing, e.g.: $MAC_{A,b}(m) = Am + b$

Encryption & Authentication

- Schemes with **information theoretic security**
  - One-time pad: $E_k(m) = m + k$
  - Universal hashing, e.g.: $MAC_{A,b}(m) = Am + b$

- Well-known disadvantage: key cannot be re-used

- Reason:
  - Eve can learn info on key by observing cipher
  - Even worse: **such attack remains undetected**

Encryption & Authentication

- Schemes with **information theoretic security**
  - One-time pad: $E_k(m) = m + k$
  - Universal hashing, e.g.: $MAC_{A,b}(m) = Am + b$

- Well-known disadvantage: key cannot be re-used
  - Reason:
    - Eve can learn info on key by observing cipher
    - Even worse: **such attack remains undetected**
  - Thus, key has to be refreshed **even if not under attack**

General Idea

- To use a **quantum** ciphertext (or tag) instead so that any eavesdropping attack will **disturb** it

General Idea

- To use a **quantum** ciphertext (or tag) instead so that

  any eavesdropping attack will **disturb** it

- We may hope for:
  - Encode ciphertext (or tag) c into a quantum state $|c\rangle$
  - Check upon arrival if $|c\rangle$ is still in “good form”
  - Conclude: no eavesdropping took place

General Idea

- To use a **quantum** ciphertext (or tag) instead so that

  any eavesdropping attack will **disturb** it

- We may hope for:
  - Encode ciphertext (or tag) c into a quantum state $|c\rangle$
  - Check upon arrival if $|c\rangle$ is still in “good form”
  - Conclude: no eavesdropping took place

- Would allow for:
  - unbounded safe re-use of the key
  - as long as not under attack

Known Results - and our Results

General idea goes back to

- [Bennett, Brassard & Breidbart 1982]:
  - proposed a simple scheme
  - gave hand-wavy arguments for its security

Quantum Cryptography II:
How to re-use a one-time pad safely even if P=NP

Charles H. Bennett (IBM Yorktown) *
Gilles Brassard (Univ. de Montreal) †
Seth Breidbart (Box 1526, NY 10268)

November 1982

Abstract

When elementary quantum systems, such as polarized photons, are used to transmit digital information, the uncertainty principle gives rise to novel cryptographic phenomena unachievable with traditional transmission media, e.g. a communications channel on which it is impossible in principle to eavesdrop without a high probability of being detected. With such a channel, a one-time pad can safely be reused many times as long as no eavesdrop is detected, and, planning ahead, part of the capacity of these uncompromised transmissions can be used to send fresh random bits with which to replace the one-time pad when an eavesdrop finally is detected. Unlike other schemes for

Known Results - and our Results

General idea goes back to

- [Bennett, Brassard & Breidbart 1982]:
  - proposed a simple scheme
  - gave hand-wavy arguments for its security

Their paper got rejected, and idea was abandoned - until...

Known Results - and our Results

General idea goes back to

- [Bennett, Brassard & Breidbart 1982]:
  - proposed a simple scheme
  - gave hand-wavy arguments for its security

Their paper got rejected, and idea was abandoned - until...

- [Damgård, Pedersen, Salvail 2005]:
  - proposed a new scheme with rigorous security proof
  - But: honest users need quantum computing capabilities

Known Results - and our Results

General idea goes back to

- [Bennett, Brassard & Breidbart 1982]:
  - proposed a simple scheme
  - gave hand-wavy arguments for its security

Their paper got rejected, and idea was abandoned - until...

- [Damgård, Pedersen, Salvail 2005]:
  - proposed a new scheme with rigorous security proof
  - But: honest users need quantum computing capabilities

Our result:

- new simple scheme, based on BB84 qubits
- rigorous security proof

Known Results - and our Results

General idea goes back to

Related line of work:

encryption/authentication of **quantum messages**

Some also offer key recycling and/or other features (see e.g. Portmann's talk)

But, in all of those: honest users need quantum computer (even when restricting to classical messages)

Our result:

- new simple scheme, based on BB84 qubits
- rigorous security proof

Encryption with Key-Recycling vs QKD

- Allow for almost the same
- There **are** subtle differences

Encryption with Key-Recycling vs QKD

- Allow for almost the same
- There **are** subtle differences

- Encryption with key recycling:
  - non-interactive (up to the ``feedback")
  - only a 1-bit message is to be authenticated, offline
  - potential for better efficiency

Encryption with Key-Recycling vs QKD

- Allow for almost the same
- There **are** subtle differences

- Encryption with key recycling:
  - non-interactive (up to the ``feedback")
  - only a 1-bit message is to be authenticated, offline
  - potential for better efficiency

- QKD:
  - adaptively adjust to the noise

Encryption with Key-Recycling vs QKD

- Allow for almost the same
- There **are** subtle differences

- Encryption with key recycling:
  - non-interactive (up to the ``feedback")
  - only a 1-bit message is to be authenticated, offline
  - potential for better efficiency

- QKD:
  - adaptively adjust to the noise

- Our main motivation: intellectual interest

Road Map

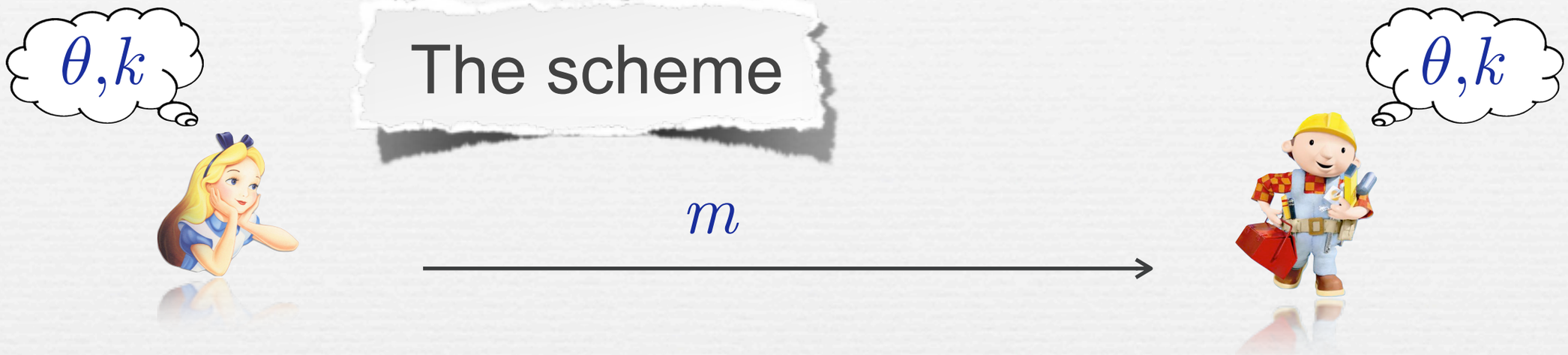
- Introduction
- The basic scheme and its analysis
- Extensions and open problem(s)

Authentication with Key-Recycling

The scheme

m

Authentication with Key-Recycling



Authentication with Key-Recycling

The scheme

$x \leftarrow \{0,1\}^n$

m

$H^\theta |x\rangle$

Authentication with Key-Recycling

The scheme

$x \leftarrow \{0,1\}^n$

m

$H^\theta |x\rangle$

θ	+	×	×	+	×	+	⋯	×	×	+
x	1	1	0	0	1	0	⋯	1	0	1
$H^\theta \|x\rangle$	↕	↘	↙	↔	↘	↔	⋯	↘	↙	↕

Authentication with Key-Recycling

The scheme

$x \leftarrow \{0,1\}^n$

m

$H^\theta |x\rangle \ , \ t = MAC_k(m \| x)$

Authentication with Key-Recycling

The scheme

$x \leftarrow \{0,1\}^n$

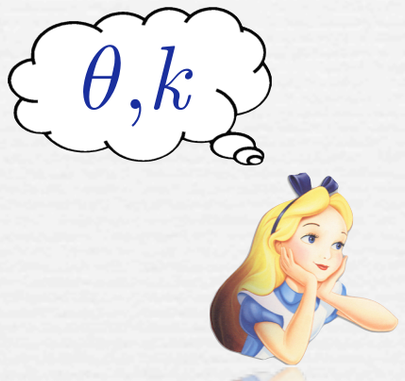
m

$H^\theta |x\rangle \ , \ t = MAC_k(m \| x)$

$= A\left[\frac{m}{x}\right] + b$

Authentication with Key-Recycling

The scheme



$x \leftarrow \{0,1\}^n$

m

$H^\theta |x\rangle \ , \ t = MAC_k(m \| x)$

$= A\left[\frac{m}{x}\right] + b$

recover x

check t

Authentication with Key-Recycling

The scheme

$x \leftarrow \{0,1\}^n$

m

$H^\theta |x\rangle \ , \ t = MAC_k(m \| x)$

$= A\left[\frac{m}{x}\right] + b$

recover x

check t

Claims (informal)

- Offers authentication security

Authentication with Key-Recycling

$x \leftarrow \{0,1\}^n$

The scheme

m

$H^\theta |x\rangle \ , \ t = MAC_k(m \| x)$

$= A\left[\frac{m}{x}\right] + b$

recover x

check t

Claims (informal)

- Offers authentication security obviously

Authentication with Key-Recycling

$x \leftarrow \{0,1\}^n$

The scheme

m

$H^\theta |x\rangle \ , \ t = MAC_k(m \| x)$

$= A\left[\frac{m}{x}\right] + b$

recover x

check t

Claims (informal)

- Offers authentication security
- If Bob accepts then key (θ, k) can be safely re-used

Authentication with Key-Recycling

$x \leftarrow \{0,1\}^n$

The scheme

m

$H^\theta |x\rangle \ , \ t = MAC_k(m \| x)$

$= A\left[\frac{m}{x}\right] + b$

recover x

check t

Claims (informal)

- Offers authentication security
- If Bob accepts then key (θ, k) can be safely re-used
- If Bob rejects then θ (only) must be refreshed

Authentication with Key-Recycling

The scheme

$x \leftarrow \{0,1\}^n$

m

$H^\theta|x\rangle\ ,\ t = MAC_k(m\|x)$

$= A\left[\frac{m}{x}\right] + b$

recover x

check t

Intuition:

If Eve gets to see authentication tags

$$t_i = MAC_k(m_i) = Am_i + b$$

for **known** messages $m_1, m_2, \ldots$ and a fixed key $k = (A,b)$,
and so accumulates (linear) info on k and can solve for it.

Authentication with Key-Recycling

The scheme

$x \leftarrow \{0,1\}^n$

m

$H^\theta|x\rangle\ ,\ t = MAC_k(m\|x)$

$= A\left[\frac{m}{x}\right] + b$

recover x

check t

Intuition:

If Eve gets to see authentication tags

$$t_i = MAC_k(m_i) = Am_i + b$$

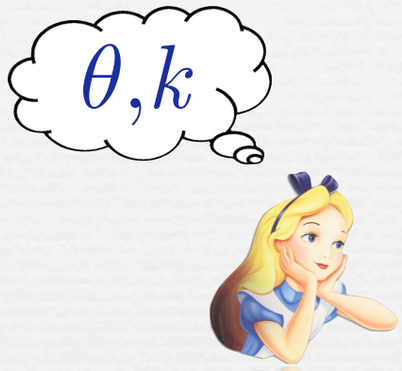
for **known** messages $m_1, m_2, \ldots$ and a fixed key $k = (A,b)$, and so accumulates (linear) info on k and can solve for it.

But **here**: authenticated message $m\|x$ is partly **unknown**, since $H^\theta|x\rangle$ **hides** x (to some extent) when θ is unknown.

An “Attack”


θ, k
$x \leftarrow \{0,1\}^n$
m
$H^{\theta_1}|x_1\rangle \otimes H^{\theta_2}|x_2\rangle \otimes \cdots$, t
θ, k
recover x
check t

An “Attack”



$x \leftarrow \{0,1\}^n$

m

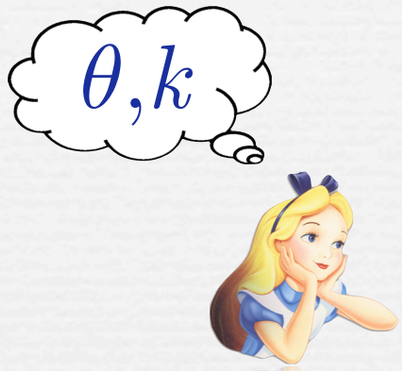
$H^{\theta_1}|x_1\rangle \otimes H^{\theta_2}|x_2\rangle \otimes \cdots \quad , \; t$

recover x

check t

Eve measures 1st qubit as if $\theta_1 = 0$

An "Attack"



$x \leftarrow \{0,1\}^n$

m

$H^{\theta_1}|x_1\rangle \otimes H^{\theta_2}|x_2\rangle \otimes \cdots \quad , \; t$

recover x

check t

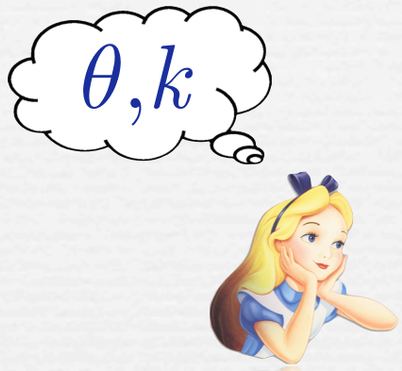
Eve measures 1st qubit as if $\theta_1 = 0$

Effect:

If $\theta_1 = 0$ then

- she learns x_1,
- $H^{\theta_1}|x_1\rangle$ is unaffected
- Bob accepts

An "Attack"



$x \leftarrow \{0,1\}^n$

m

$H^{\theta_1}|x_1\rangle \otimes H^{\theta_2}|x_2\rangle \otimes \cdots \quad , \; t$

recover x

check t

Eve measures 1st qubit as if $\theta_1 = 0$

Effect:

If $\theta_1 = 0$ then

- she learns x_1,
- $H^{\theta_1}|x_1\rangle$ is unaffected
- Bob accepts

If $\theta_1 = 1$ then

- she does not learn x_1,
- $H^{\theta_1}|x_1\rangle$ gets disturbed
- Bob rejects with prob. $\approx 1/2$

An “Attack”

Effect:

If $\theta_1 = 0$ then

- she learns x_1,
- $H^{\theta_1}|x_1\rangle$ is unaffected
- Bob accepts

If $\theta_1 = 1$ then

- she does not learn x_1,
- $H^{\theta_1}|x_1\rangle$ gets disturbed
- Bob rejects with prob. $\approx 1/2$

An “Attack”

Effect:

If $\theta_1 = 0$ then

- she learns x_1,
- $H^{\theta_1}|x_1\rangle$ is unaffected
- Bob accepts

If $\theta_1 = 1$ then

- she does not learn x_1,
- $H^{\theta_1}|x_1\rangle$ gets disturbed
- Bob rejects with prob. $\approx 1/2$

Eve’s conclusion:

If Bob rejects then $\theta_1 = 1$ (but now θ gets refreshed!)

An “Attack”

Effect:

If $\theta_1 = 0$ then

- she learns x_1,
- $H^{\theta_1}|x_1\rangle$ is unaffected
- Bob accepts

If $\theta_1 = 1$ then

- she does not learn x_1,
- $H^{\theta_1}|x_1\rangle$ gets disturbed
- Bob rejects with prob. $\approx 1/2$

Eve’s conclusion:

If Bob rejects then $\theta_1 = 1$ (but now θ gets refreshed!)

If Bob accepts: θ_1 is likely to be 0 ($\Rightarrow$ Eve learned info on θ)

An “Attack”

Effect:

If $\theta_1 = 0$ then

- she learns x_1,
- $H^{\theta_1}|x_1\rangle$ is unaffected
- Bob accepts

If $\theta_1 = 1$ then

- she does not learn x_1,
- $H^{\theta_1}|x_1\rangle$ gets disturbed
- Bob rejects with prob. $\approx 1/2$

Eve’s conclusion:

If Bob rejects then $\theta_1 = 1$ (but now θ gets refreshed!)

If Bob accepts: θ_1 is likely to be 0 ($\Rightarrow$ Eve learned info on θ)

No need to worry:

The more info she tries to learn the more likely she fails

Insight Gained

- **Cannot** expect to prove:

  "If Bob accepts then key remains (close to) random"

Insight Gained

- **Cannot** expect to prove:

  "If Bob accepts then key remains (close to) random"

- But then:
  - may not be necessary for the key to stay random
  - high uncertainty might be sufficient

Formal Statement - Informally Stated

Theorem. If before the execution:

$$\text{Guess}(\theta | \textit{Eve's view}) \approx 0 \quad \& \quad \delta(k, \textit{unif} | \theta, \textit{Eve's view}) \approx 0$$

Formal Statement - Informally Stated

Theorem. If before the execution:

$$\mathrm{Guess}(\theta|\mathit{Eve's\ view}) \approx 0 \quad \& \quad \delta(k, \mathit{unif}\,|\theta, \mathit{Eve's\ view}) \approx 0$$

then after the execution:

$$\mathrm{Guess}(\theta'|\mathit{Eve's\ view}) \approx 0 \quad \& \quad \delta(k, \mathit{unif}\,|\theta', \mathit{Eve's\ view}) \approx 0$$

where $\theta' := \theta$ if Bob accepted and freshly chosen otherwise.

Formal Statement - Informally Stated

Theorem. If before the execution:

$$\mathrm{Guess}(\theta|\mathit{Eve's\ view}) \approx 0 \quad \& \quad \delta(k, \mathit{unif}\,|\theta, \mathit{Eve's\ view}) \approx 0$$

then after the execution:

$$\mathrm{Guess}(\theta'|\mathit{Eve's\ view}) \approx 0 \quad \& \quad \delta(k, \mathit{unif}\,|\theta', \mathit{Eve's\ view}) \approx 0$$

where $\theta' := \theta$ if Bob accepted and freshly chosen otherwise.

Thus: starting off with a, say, uniformly random key (θ,k) , the (possibly refreshed) key can be re-used over and over.

Proof - The Easy Part

Note: Eve's view E' after the execution consists of

- her old view E
- the tag $t = A\left[\frac{m}{x}\right] + b$
- whatever she kept of $H^\theta|x\rangle$, call it Q
- Bob's decision, call it d

Proof - The Easy Part

Note: Eve's view E' after the execution consists of

- her old view E
- the tag $t = A\left[\frac{m}{x}\right] + b$
- whatever she kept of $H^\theta|x\rangle$, call it Q
- Bob's decision, call it d

Thus:

$$\text{Guess}(\theta'|E') = \text{Guess}(\theta'|E, Q, t, d)$$

Proof - The Easy Part

Note: Eve's view E' after the execution consists of

- her old view E
- the tag $t = A\left[\frac{m}{x}\right] + b$
- whatever she kept of $H^\theta|x\rangle$, call it Q
- Bob's decision, call it d

Thus:

$$\mathrm{Guess}(\theta'|E') = \mathrm{Guess}(\theta'|E, Q, t, d)$$

$$= \mathrm{P}[d=0]\,\mathrm{Guess}(\theta'|E,Q,t,d=0) + \mathrm{P}[d=1]\,\mathrm{Guess}(\theta'|E,Q,t,d=1)$$

Proof - The Easy Part

Note: Eve's view E' after the execution consists of

- her old view E
- the tag $t = A\left[\frac{m}{x}\right] + b$
- whatever she kept of $H^\theta|x\rangle$, call it Q
- Bob's decision, call it d

Thus:

$$\mathrm{Guess}(\theta'|E') = \mathrm{Guess}(\theta'|E, Q, t, d)$$

$$= \mathrm{P}[d=0]\,\mathrm{Guess}(\theta'|E,Q,t,d=0) + \mathrm{P}[d=1]\,\mathrm{Guess}(\theta'|E,Q,t,d=1)$$

freshly chosen

$= \theta$

Proof - The Easy Part

Note: Eve's view E' after the execution consists of

- her old view E
- the tag $t = A\left[\frac{m}{x}\right] + b$
- whatever she kept of $H^\theta|x\rangle$, call it Q
- Bob's decision, call it d

Thus:

$$\begin{aligned}
&\mathrm{Guess}(\theta'|E') = \mathrm{Guess}(\theta'|E, Q, t, d) \\
&= \mathrm{P}[d=0]\,\mathrm{Guess}(\theta'|E,Q,t,d=0) + \mathrm{P}[d=1]\,\mathrm{Guess}(\theta'|E,Q,t,d=1) \\
&\leq \frac{1}{\#\theta} + \mathrm{Guess}(\theta|E,Q,t)
\end{aligned}$$

freshly chosen

$= \theta$

Proof - The Easy Part

Note: Eve's view E' after the execution consists of

- her old view E
- the tag $t = A\left[\frac{m}{x}\right] + b$
- whatever she kept of $H^\theta|x\rangle$, call it Q
- Bob's decision, call it d

Thus:

$$\begin{aligned}
&\mathrm{Guess}(\theta'|E') = \mathrm{Guess}(\theta'|E, Q, t, d) \\
&= \mathrm{P}[d=0]\,\mathrm{Guess}(\theta'|E,Q,t,d=0) + \mathrm{P}[d=1]\,\mathrm{Guess}(\theta'|E,Q,t,d=1) \\
&\leq \frac{1}{\#\theta} + \mathrm{Guess}(\theta|E,Q,\cancel{t})
\end{aligned}$$

freshly chosen

$= \theta$

Proof - The Easy Part

Note: Eve's view E' after the execution consists of

- her old view E
- the tag $t = A\left[\frac{m}{x}\right] + b$
- whatever she kept of $H^\theta|x\rangle$, call it Q
- Bob's decision, call it d

Thus:

$$\begin{aligned}
&\mathrm{Guess}(\theta'|E') = \mathrm{Guess}(\theta'|E, Q, t, d) \\
&= \mathrm{P}[d=0]\,\mathrm{Guess}(\theta'|E,Q,t,d=0) + \mathrm{P}[d=1]\,\mathrm{Guess}(\theta'|E,Q,t,d=1) \\
&\leq \frac{1}{\#\theta} + \mathrm{Guess}(\theta|E,\not{Q},\not{t})
\end{aligned}$$

freshly chosen

$= \theta$

$H^\theta|x\rangle$

Proof - The Easy Part

Note: Eve's view E' after the execution consists of

- her old view E
- the tag $t = A\left[\frac{m}{x}\right] + b$
- whatever she kept of $H^\theta|x\rangle$, call it Q
- Bob's decision, call it d

Thus:

$$\mathrm{Guess}(\theta'|E') = \mathrm{Guess}(\theta'|E, Q, t, d)$$

freshly chosen

$$= \mathrm{P}[d=0]\,\mathrm{Guess}(\theta'|E,Q,t,d=0) + \mathrm{P}[d=1]\,\mathrm{Guess}(\theta'|E,Q,t,d=1)$$

$= \theta$

$$\leq \frac{1}{\#\theta} + \mathrm{Guess}(\theta|E,Q,t)$$

$H^\theta|x\rangle$

Proof - The Easy Part

Note: Eve's view E' after the execution consists of

- her old view E
- the tag $t = A\left[\frac{m}{x}\right] + b$
- whatever she kept of $H^\theta|x\rangle$, call it Q
- Bob's decision, call it d

Thus:

$$\mathrm{Guess}(\theta'|E') = \mathrm{Guess}(\theta'|E, Q, t, d)$$

freshly chosen

$$= \mathrm{P}[d=0]\,\mathrm{Guess}(\theta'|E,Q,t,d=0) + \mathrm{P}[d=1]\,\mathrm{Guess}(\theta'|E,Q,t,d=1)$$

$$\leq \frac{1}{\#\theta} + \mathrm{Guess}(\theta|E,Q,t) \approx 0$$

θ' = θ

$H^\theta|x\rangle$

Proof - The Easy Part

Note: Eve's view E' after the execution consists of

- her old view E
- the tag $t = A[m]$
- whatever she kept of $H^\theta|x\rangle$, call it Q
- Bob's decision, call it d

Proving $\delta(k, unif\,|\theta', E') \approx 0$ is more involved. Builds up on techniques from [Tomamichel,Fehr,Kaniewski,Wehner '13].

Thus:

$$\mathrm{Guess}(\theta'|E') = \mathrm{Guess}(\theta'|E, Q, t, d)$$

freshly chosen

$$= \mathrm{P}[d=0]\,\mathrm{Guess}(\theta'|E,Q,t,d=0) + \mathrm{P}[d=1]\,\mathrm{Guess}(\theta'|E,Q,t,d=1) \quad (\theta' = \theta)$$

$$\leq \frac{1}{\#\theta} + \mathrm{Guess}(\theta|E,Q,t) \quad \approx 0$$

$H^\theta|x\rangle$

Road Map

- Introduction
- The basic scheme and its analysis
- Extensions and open problem(s)

Extensions

- **Encryption** with key-recycling
  - Idea: extract randomness from x for one-time-pad key
  - Can mix-and-match with authentication

Extensions

- **Encryption** with key-recycling
  - Idea: extract randomness from x for one-time-pad key
  - Can mix-and-match with authentication

- Tolerate **noise** in the quantum communication
  - Straightforward error-correction does not work
  - Error-correction "*without leaking partial info*" by Dodis and Smith comes to the rescue

The Trouble with Error Correction

Obvious “solution”:

send along the syndrome $s = \mathrm{syn}(x)$ of x

The Trouble with Error Correction

Obvious “solution”:

send along the syndrome $s = \mathrm{syn}(x)$ of x

The problem: in the analysis

$$\mathrm{Guess}(\theta'|E') = \mathrm{Guess}(\theta'|E, Q, t, s, d)$$

$$\cdots$$

$$\leq \frac{1}{\#\theta} + \mathrm{Guess}(\theta|E, \cancel{Q}, \cancel{t}, s)$$

$H^\theta|x\rangle$

The Trouble with Error Correction

Obvious “solution”:

send along the syndrome $s = \mathrm{syn}(x)$ of x

The problem: in the analysis

$$\mathrm{Guess}(\theta'|E') = \mathrm{Guess}(\theta'|E, Q, t, s, d)$$

$$\cdots$$

$$\leq \frac{1}{\#\theta} + \mathrm{Guess}(\theta|E, Q, t, s)$$

$$H^\theta|x\rangle$$

*We still **expect** this to be small, but cannot **prove** it*

Conclusion

What we did:

- Considered one of the very first ideas for quantum crypto (suggested >30 ago, even before QKD)
- First provably-secure solution w/o quantum computer

Conclusion

What we did:

- Considered one of the very first ideas for quantum crypto (suggested >30 ago, even before QKD)
- First provably-secure solution w/o quantum computer

Open problems / future directions:

- To do the error correction in a better way (Dodis-Smith technique works only for small error)
- Minimize amount of quantum communication

Conclusion

What we did:

- Considered one of the very first ideas for quantum crypto (suggested >30 ago, even before QKD)
- First provably-secure solution w/o quantum computer

Open problems / future directions:

- To do the error correction in a better way (Dodis-Smith technique works only for small error)
- Minimize amount of quantum communication

Thank you!