Improving the Security of Quantum Protocols via Commit&Open

Ivan Damgård (Aarhus University, DK)
Serge Fehr (CWI, NL)
Carolin Lunemann (Aarhus University, DK)
Louis Salvail (Université de Montréal, CA)
Christian Schaffner (CWI, NL)

CRYPTO '09, Santa Barbara, USA
Wednesday, August 19, 2009
Main Results

\[ \pi \]

Compiler

Computational security against Bob
Unconditional security against Alice

Only constant increase of qubits and rounds
Preservation of sequential composability

BB84-type protocol
Benign security against Bob
Unconditional security against Alice

Commit&Open
(with special properties)
Main Results

Compiler

\[ \pi \]

**BB84-type protocol**

- *Benign security* against Bob
- *Unconditional security* against Alice

- BQSM-security

\[ C^\alpha(\pi) \]

**Computational security**

- Unconditional security against Bob

- Unconditional security against Alice

Only constant increase of qubits and rounds
Preservation of sequential composability

**Hybrid security**

Commit&Open
(with special properties)
Intuition

Compiler

$\pi$

BB84-type protocol

Benign security against Bob

Unconditional security against Alice

$C^a(\pi)$

Computational security against Bob

Unconditional security against Alice

Only constant increase of qubits and rounds
Preservation of sequential composability

Commit & Open
(with special properties)
**BB84-type protocols**

**Intuition**

- Preparation (quantum):
  - $x \in_R \{0, 1\}^n$
  - $\theta \in_R \{+, \times\}^n$

**Post-processing (classical):**

- $\hat{\theta} \in_R \{+, \times\}^n$
- $\hat{\theta}$
- $\hat{x} : 0 \quad R \quad R \quad 1$

**Notation:** C. Schaffner
BB84-type protocols

$x \in \mathbb{R} \{0, 1\}^n \quad 0 \quad 0 \quad 1 \quad 1$

$\theta \in \mathbb{R} \{+, \times\}^n$

post-processing (classical)

$\hat{\theta} \in \mathbb{R} \{+, \times\}^n$

$\hat{\theta}$

$\hat{x} \quad 0 \quad R \quad R \quad 1$

arbitrary classical messages and local computations

preparation (quantum)
Security

- Bob measures in random bases:
  - He knows $x_i$ whenever $\theta_i = \hat{\theta}_i$.
  - For $\theta_i \neq \hat{\theta}_i$ his uncertainty is high (privacy amplification).
- We must ensure that Bob measures most of his qubits before Alice announces further information (e.g. her bases).
BB84-type protocols

\[ x \in \mathbb{R} \{0, 1\}^n \quad 0 \quad 0 \quad 1 \quad 1 \]

\[ \theta \in \mathbb{R} \{+, \times\}^n \]

post-processing (classical)

arbitrary classical messages and local computations

\[ \theta \]

\[ \hat{x} \quad 0 \quad 0 \quad 1 \quad 1 \]
Security

- Bob measures in **random bases**:
  - He knows $x_i$ whenever $\theta_i = \hat{\theta}_i$.
  - For $\theta_i \neq \hat{\theta}_i$ his uncertainty is high (privacy amplification).
- We must ensure that Bob measures most of his qubits **before** Alice announces further information (e.g. her bases).
- Security against **benign** Bob ('almost' honest in preparation phase).
- Unconditional security against dishonest Alice.
Improvement

\[ \pi \]

BB84-type protocol

\begin{itemize}
  \item Benign security against Bob
  \item Unconditional security against Alice
\end{itemize}

Compiler

\[ C^\alpha(\pi) \]

\begin{itemize}
  \item Computational security against Bob
  \item Unconditional security against Alice
  \item Only constant increase of qubits and rounds
  \item Preservation of sequential composability
\end{itemize}

Commit & Open
(with special properties)
Security

$x \in_R \{0, 1\}^m \quad 0 \quad 0 \quad 1 \quad 1$

$\theta \in_R \{+, \times\}^m \quad \text{arbitrary classical messages and local computations}$

\[ T \subset \{1, \ldots, m\}, \quad |T| = \alpha m \]

for all $i \in T$: $x_i = \hat{x}_i$

whenever $\theta_i = \hat{\theta}_i$

$n = (1 - \alpha)m$

preparation (quantum)

verification (classical)

post-processing (classical)

Intuition | Improvement | Proof Sketch | Results | Summary
Commit&Open

- Idea already in 1-2 QOT [BBCS91].
- **Intuition**: If Bob passes the measurement test, he must have measured most of his qubits (also in the remaining subset).
- Partial results for QOT, e.g. [Yao95, Mayers96, CDMS04].
- **Formal characterization** of what Commit&Open achieves in a quantum world ⇒ **Benignity**


Commit&Open

⇒ Computational Security

• Commitment can only be computationally binding.

• Standard reduction from computational security of protocol to computational binding property of commitment would require rewinding.

• Quantum rewinding is only possible in limited settings [Watrous06].
Benignity

- Bob treats the qubits *almost* honestly in preparation phase.

- Two conditions are satisfied after preparation phase:
  
  \[ x|_I = (x_i)_{i \in I}; \quad d_H(\theta, \hat{\theta}) := \left|\{i : \theta_i \neq \hat{\theta}_i\}\right|; \quad \beta \geq 0 \]

- Bob’s *quantum storage* is small:
  
  \[ H_0(\rho_B) \leq \beta n \]

- There exists a \( \hat{\theta} \), such that the *uncertainty* about \( x_i \) is (essentially) 1 whenever \( \theta_i \neq \hat{\theta}_i \):
  
  \[ H_\infty(X|_I \mid X|_{\bar{I}} = x|_{\bar{I}}) \geq d_H(\theta|_I, \hat{\theta}|_I) - \beta n \]

  for any \( I \subseteq \{1, \ldots, n\} \); for any fixed \( \theta, \hat{\theta}, \hat{x} \); for any \( x|_{\bar{I}} \)
Computational Security

- Simulation-based proof in the common-reference-string model.
- Commitment scheme with special properties and secure against quantum adversaries (e.g. [Regev05]).
- **Keyed dual-mode commitment scheme**
  - Unconditionally binding key $pk_B$.
  - Unconditionally hiding key $pk_H$.
  - **Indistinguishability of keys** (also for quantum algorithms).
Indistinguishability

\[ \text{out}[C^\alpha(\pi)]_{A,B'} = \text{out}[C^\alpha_{pkH}(\pi)]_{A,B'} \approx_q \text{out}[C^\alpha_{pkB}(\pi)]_{A,B'} = \text{out}[\pi]_{A_o,B'_o} \]
Indistinguishability

\[ \text{out}[C^\alpha(\pi)]_{A,B'} \approx^q \text{out}[\pi]_{A_0,B'_0} \]
General Compiler

Main Theorem:

If the original protocol $\pi$ is unconditionally secure against a $\beta$-benign adversary, then the compiled protocol $C^\alpha(\pi)$ is (quantum-) computationally secure against any adversary for const. $0 < \alpha < 1$, $0 < \beta$. Unconditional security against Alice is maintained.
General Compiler

- Benignity is (relatively) **weak assumption**.
- Compilation only requires an increase of qubits and rounds by a **constant factor**.
- Compilation preserves **sequential composability** [FS09].
Hybrid Security

Compiler

$\pi$

BB84-type protocol

Benign security against Bob

Unconditional security against Alice

BQSM-security

Commit&Open
(with special properties)

$C^α(\pi)$

Computational security against Bob

Unconditional security against Alice

Only constant increase of qubits and rounds
Preservation of sequential composability

Hybrid security

Intuition | Improvement | Proof Sketch | Results | Summary
Hybrid Security

Bob needs large quantum memory and large quantum computing power.

Theorem:

If $\pi$ is unconditionally secure against $\gamma$-BQSM Bob, then $C^\alpha(\pi)$ is computationally secure against a dishonest Bob and unconditionally secure against $\gamma(1 - \alpha)$-BQSM Bob for const. $0 < \alpha < 1, 0 < \gamma < 1$.

Unconditional security against Alice is maintained.
Summary

- **General compiler** to additionally achieve computational security.
- Characterization of commit&open in quantum settings (*benignity*).
- Protocols with **hybrid security**, e.g. QOT [BBCS91] and QID [DFSS07].
- Hybrid security against **man-in-the-middle attacks** for QID.
- Extensions for **noisy** quantum communication.
• Full Version: arXiv: 0902.3918

• Quantum-Secure Coin-Flipping and Applications (Damgård and Lunemann; to appear at Asiacrypt'09, arXiv: 0903.3118)

• Sampling in a Quantum Population, and Applications (Bouman and Fehr; arXiv: 0907.4246)

Thank You!