QUANTUM OBLIVIOUS TRANSFER AND QUANTUM ONE-WAY FUNCTIONS

Takeshi Koshiba (Saitama Univ.)
Preliminary
Bit Commitment

In Commit Phase, Alice commits to a bit while keeping it hidden.

In Reveal Phase, Alice reveals the committed bit.

$\mathbf{b} \in \{0, 1\}$
Bit Commitment

In Commit Phase, Alice commits to a bit while keeping it hidden.

In Reveal Phase, Alice reveals the committed bit.
Security for Bit Commitment

**Hiding**

Bob cannot know the secret contents of the received data in Commit Phase before Reveal Phase.

**Binding**

Alice cannot replace the contents after Commit Phase.
Oblivious Transfer

**Alice**

\[ b_0, b_1 \]

**Bob**

\[ c, b_c \]

**Sender’s Privacy**

Bob cannot know the bit which Bob does not choose.

**Receiver’s Privacy**

Alice cannot know Bob’s choice.
Background and Motivation
Impagliazzo's Five Worlds (1995)

- **Algorithmica**
  P = NP or something "morally equivalent" like fast probabilistic algorithms for NP.

- **Heuristica**
  NP problems are hard in the worst case but easy on average.

- **Pessiland**
  NP problems hard on average but no one-way functions exist.

- **Minicrypt**
  One-way functions exist but we do not have public-key cryptography.

- **Cryptomania**
  Public-key cryptography is possible, i.e. two parties can exchange secret messages over open channels.
Minicrypt versus Cryptomania

- **Minicrypt**
  - One-Way Functions
  - PseudoRandom Generators [Håstad-Impagliazzo-Levin-Luby 99]
  - Statistically binding Bit Commitment [Naor 91]
  - Statistically hiding Bit Commitment [Haitner-Nguyen-Ong-Reingold-Vadhan 2009]
  - Signature Scheme [Naor-Yung 89 + Rompel 90]
  - Zero-Knowledge Proofs/Arguments [Goldreich-Micali-Wigderson 91 / Brassard-Chaum-Crépeau 88]

- **Cryptomania**
  - Public-Key Cryptosystem

- **Another World: Secretica?**
  - Oblivious Transfer
  - Secure Computation (Secure Function Evaluation)
How about Quantum World?

- Unconditional QBC $\rightarrow$ Unconditional QOT
  
  [Yao 1995]

- Statistically binding QBC
  $\rightarrow$ Statistically sender-secure QOT
  $\rightarrow$ Statistically hiding QBC

  [Crépeau-Légaré-Salvail 2001]

- Computationally $f$-binding QStringC
  $\rightarrow$ QMeasurementC
  $\rightarrow$ Statistically receiver-secure QOT

  [Crépeau-Dumais-Mayers-Salvail 2004]

$Q$ Secretica may be merged into $Q$ Minicrypt?
Statistically Sender-secure (private) QOT

Naor’s construction of statistically binding BC from PRG can be adapted to the quantum case.

CLS2001

- Statistically binding QBC $\Rightarrow$ statistically sender-secure QOT

Open ?

- Quantum version of HILL99 OWF $\Rightarrow$ PRG
- Quantum version of OT symmetry [Wolf, Wullscheleger 2006]

Statistically Receiver-secure (private) QOT

CDMS2004: $f$-binding QStringC $\Rightarrow$ QMC $\Rightarrow$ SR-QOT

Open ?

- Construction of $f$-binding QStringC
Results

**QOWP/QOWF-based non-interactive statistically hiding QBC** → **computationally \( F \)-binding QSC**

+ **QOWP/QOWF** → **non-interactive statistically hiding QBC** [DMS 2000/KO 2009]
+ **Computationally \( F \)-binding QSC** → **Statistically Receiver-secure QOT** [CDMS 2004]

**Corollary:**
**QOWF** → **Statistically Receiver-secure QOT**

*Q Secretica* is merged into *Q Minicrypt* (in a sense)
QBC based on QOWP [DMS2000]

Alice

Commit Phase
① If \( b = 0 \) then use \( + \) basis.
   If \( b = 1 \) then use \( \times \) basis.
② Randomly choose \( x \).
③ Send \( |\psi\rangle = |f(x)\rangle_b \) to Bob.

Reveal Phase
④ Send \( b, x \) to Bob.

Bob

⑤ Measure \( |\psi\rangle \) w.r.t. \( b \)-basis. Accept if the observed value is equal to \( f(x) \).
QOWP-based QBC: Properties

- Except a negligible fraction of keys (i.e., inputs $x$ to QOWP $f$), the binding is guaranteed. (If the binding is violated for a non-negligible fraction of keys, $f$ can be invertible for the inputs.

- Parallel composition is possible due to the non-interactivity.

- The parallel composition constitutes a non-interactive string commitment scheme.

- The scheme satisfies the $f$-binding property.
 Cheating Alice against NI-QBC

- In Commit Phase, Alice sends a malicious state to Bob.
- In Reveal Phase, Alice executes some local operations either $O_0$ or $O_1$.
- After $O_0$, the malicious state is changed into $S_0$
  - $b_0 = \Pr[\text{Bob accepts and obtains } 0]$
- After $O_1$, the malicious state is changed into $S_1$
  - $b_1 = \Pr[\text{Bob accepts and obtains } 1]$
- If $b_0 + b_1 > 1 + 1/poly$, cheating succeeds. (Weak Def.)
- Even honest Alice can achieve $b_0 + b_1 = 1$ by sending a superposition of 0-commitment state and 1-commitment state in Commit Phase. In Reveal Phase, she just executes the identity operator regardless of the committed bit.
For QBC
- $b_0 + b_1 < 1 + 1/poly$

For QSC of $n$-bit string, a naïve extension is as follows.
- $b_0 + b_1 + \cdots + b_{2^n-1} < 1 + 1/poly$
- For each $i$, $E[b_i] = 1/2^n (1 + 1/poly)$
- This is indistinguishable from the honest behavior if $n$ is large.

So, consider the following
- Let $g: \{0,1\}^n \rightarrow \{0,1\}^m$, $m = O(polylog n)$
- Set $B_s = \sum_{x: g(x) = s} b_x$
- $B_0 + B_1 + \cdots + B_{2^m-1} < 1 + 1/poly$ ($g$-binding)
- There exists a good function (family)
Quantum Measurement Commitment

Alice

| $b_1 >_{\theta_1} b_2 >_{\theta_2} \ldots | b_n >_{\theta_n}$ |

$\hat{\theta}_1, \ldots, \hat{\theta}_n, \hat{b}_1, \ldots, \hat{b}_n$

QSC_Com($\hat{\theta}_1, \ldots, \hat{\theta}_n, \hat{b}_1, \ldots, \hat{b}_n$)

c $\in \{0, 1\}$

QSC_Open($\hat{\theta}_1, \ldots, \hat{\theta}_n, \hat{b}_1, \ldots, \hat{b}_n$) if $c = 0$

$\theta_1, \theta_2, \ldots, \theta_n$ if $c = 1$

Bob

Guess the parity

Check!
QSC for 2n-bit string $x_1x_2 \cdots x_ny_1y_2 \cdots y_n$
- 1$^{st}$ half is for basis selection for QMC
- 2$^{nd}$ half is for information to be sent

$g$ in $\mathcal{F}$ is one of the following forms:
- $x_i$
- $y_i$
- $x_i \oplus y_i$

For each $g$ in $\mathcal{F}$, $g$-binding must be satisfied.

The above $\mathcal{F}$ is enough to construct QMC, i.e., SR-QOT.
Construction of QSC

- 2n parallel executions of non-interactive QBC

- Reduction
  - Assume that QSC is violated (w.r.t. g) for a non-negligible fraction of keys
  - Random guess $i$
    - $\Pr[\text{the guess is correct}] = 1/n$
  - Random guess from $x_i, y_i$, or $x_i \oplus y_i$
    - $\Pr[\text{the guess is correct}] = 1/3$
  - The process above is same as
    - Random choice of $j$ from $\{1, \ldots, 2n\}$
    - $j^{\text{th}}$ execution of QBC is violated
Concluding Remarks

- QOT is constructible from QOWF
  - How about 2-party secure computation?
  - How about multi-party secure computation?

- The weak definition for QBC is useful to construct cryptographic protocols