Oblivious Transfer 
from Weakly Random-Self-Reducible Encryption

Claude Crépeau

School of Computer Science
McGill University

joint work with Raza Ali Kazmi
Foreword
2008

Oblivious Transfer via McEliece’s PKC and Permutated Kernels

K. Kobara\(^1\), Kirill Morozov\(^1\) and R. Overbeck\(^2\)

\(^1\) RCIS, AIST
\{k-kobara,kirill.morozov\}@aist.go.jp
\(^2\) TU-Darmstadt,
Department of Computer Science,
Cryptography and Computer Algebra Group.
overbeck@cdc.informatik.tu-darmstadt.de

Oblivious Transfer Based on the McEliece Assumptions

Rafael Dowsley\(^1\), Jeroen van de Graaf\(^2\), Jörn Müller-Quade\(^3\),
and Anderson C.A. Nascimento\(^1\)
Oblivious Transfer via McEliece’s PKC and Permuted Kernels

K. Kobara¹, Kirill Morozov¹ and R. Overbeck²

¹ RCIS, AIST
{k-kobara,kirill.morozov}@aist.go.jp
² TU-Darmstadt,
Department of Computer Science,
Cryptography and Computer Algebra Group.
overbeck@cdc.informatik.tu-darmstadt.de

Oblivious Transfer Based on the McEliece Assumptions

Rafael Dowsley¹, Jeroen van de Graaf², Jörn Müller-Quade³,
and Anderson C.A. Nascimento¹
(1) two-party Cryptographic Protocols
BIT COMMITMENT

COMMIT

UNVEIL

b, 29 - 41 - 02 - 17
BIT COMMITMENT

CONCEALING

BINDING

\(-b, 39 - 21 - 12 - 27\)
Classically (information theoretical)

Folklore
Quantumly
(information theoretical)

Mayers, Lo-Chau
Classically

BIT COMMITMENT

COMMIT

UNVEIL

One-way Function

b, 29 - 41 - 02 - 17
Classically

Oblivious Transfer

B₀ → 1/2-OT → Bcampo C

BIT COMMITMENT

COMMIT

UNVEIL

x → f(x, y) → y

f(x, y) → g(x, y)
Oblivious Transfer (message multiplexing)

B₀ \rightarrow 1/2-OT \rightarrow B_c

B₁ \rightarrow C
Oblivious Transfer

$B_0 \rightarrow 1/2$-$OT \rightarrow B_0$

$B_1 \rightarrow 1/2$-$OT \rightarrow B_1$
Oblivious Transfer

B_0 \rightarrow 1/2-OT \rightarrow B_0(+)B_1 \rightarrow B_1
Oblivious Transfer
Oblivious Function Evaluation

\[ f(x, y) \]

\[ f(g(x, y)) \]

\[ g(x, y) \]
Oblivious Function Evaluation

f, g

f'(x, y)
Oblivious Function Evaluation

\[ x \rightarrow f,g \rightarrow y \leftarrow g'(x,y) \]
Mutual Identification

x = y?

x = y?
Oblivious DB query

Q \rightarrow Q \subseteq DB \rightarrow DB

data[Q]/no
Classically

Oblivious Transfer

B₀ → 1/2-OT → Bₙ

B₁ → C

One-way Function

BIT COMMITMENT

COMMIT

UNVEIL

b, 29 - 11 - 02 - 17

Oblivious Function Evaluation

x → f(x, y) → g(x, y) → y

© Claude Crépeau 2002-2010
Classically

Oblivious Transfer

B₀ → Bₙ

1/2-OT

B₁ → C

Enhanced Trapdoor One-way Permutation

One-way Function

Oblivious Function Evaluation

x → y

f(x,y) → g(x,y)
INGREDIENTS

a public-key block cipher: $(\text{enc}_B, \text{dec}_B)$

a public predicate: $\pi$
\[ \text{enc}_B(\mathbb{R}_0) \rightarrow \mathbb{R}_1 \rightarrow U_0 \rightarrow U_1 \]
\[ \text{enc}_B(\mathcal{R}_0) \rightarrow \pi(\text{dec}_B(U_0))(+)B_0 \]

\[ \mathcal{R}_1 \rightarrow U_1 \]

\[ Z_0 \rightarrow \pi(\text{dec}_B(U_1))(+)B_1 \]

\[ Z_1 \rightarrow U_0 \]

[EG85] [GMW87]
\[ \text{enc}_B(\mathbb{R}_0) \rightarrow U_0 \rightarrow U_1 \rightarrow \pi(\text{dec}_B(U_0))(+)B_0 \rightarrow \pi(\text{dec}_B(U_1))(+)B_1 \rightarrow B_0 = \pi(\mathbb{R}_0)(+)Z_0 \]
Use ZK proofs to make sure both party follow the protocol.
Definition (Enhanced TOWP)

A TOWP enc is enhanced if there exists a PPT algorithm to select random elements from the image of enc without knowledge of the corresponding pre-image.
Classically

Oblivious Transfer

B₀ → 1/2-OT → B₁

Oblivious Function Evaluation

x, y → f,g → f(x,y), g(x,y)

One-way Function

Random-Self-Reducible Encryption Scheme

BIT COMMITMENT

 Commit

UNVEIL
INGREDIENTS
a public-key block cipher:
\((\text{enc}_B, \text{dec}_B)\)

a public predicate: \(\pi\)
$m_0 = \pi^{-1}(B_0)$

$\quad m_1 = \pi^{-1}(B_1)$
\[ \text{enc}_A(m_0) \rightarrow U_0 \]
\[ \text{enc}_A(m_1) \rightarrow U_1 \]
\[ \text{RSR}_A(\mathbb{R}, U_c) \]
Definition (RSR Encryption Scheme)

A public-key encryption scheme (enc, dec) is **Random-Self-Reducible** if there exists a pair of PPT algorithms (RSR, RSR⁻¹) such that for all ®, m,

\[ RSR^{-1}(®, \text{dec}(RSR(®, \text{enc}(m)))) = m \]

and

\[ RSR(®, \text{enc}(m)) \text{ is a uniform ciphertext} \]

when ® is uniform.
\[ \text{enc}_A(m_0) \rightarrow U_0 \]

\[ \text{enc}_A(m_1) \rightarrow U_1 \]

\[ z \rightarrow \text{RSR}_A(\mathbb{R}, U_c) \]
\[ \text{enc}_A(m_0) \rightarrow U_0 \]
\[ \text{enc}_A(m_1) \rightarrow U_1 \]
\[ z \rightarrow \text{enc}_A(\mathbb{R}^*m_c) = \text{enc}_A(\mathbb{R}) \cdot U_c \]
\[
\begin{align*}
\text{enc}_A(m_0) & \rightarrow U_0 \\
\text{enc}_A(m_1) & \rightarrow U_1 \\
& \downarrow z \\
& \text{RSR}_A(\mathbb{C},U_c) \\
\text{dec}_A(z) & \rightarrow \\
\end{align*}
\]
\[ \text{enc}_A(m_0) \rightarrow U_0 \]
\[ \text{enc}_A(m_1) \rightarrow U_1 \]
\[ RSR_A(\mathbb{R}, U_c) \rightarrow z \]
\[ \text{dec}_A(z) \rightarrow y \]

\[ B_c = \pi(RSR_A^{-1}(\mathbb{R}, y)) \]
\[ \text{enc}_A(m_0) \rightarrow U_0 \]

\[ \text{enc}_A(m_1) \rightarrow U_1 \]

\[ z \leftarrow \text{enc}_A(\mathcal{R}) \cdot U_c \]

\[ \text{dec}_A(z) \rightarrow \mathcal{R}^* m_c \]

\[ B_c = \pi(\mathcal{R}^{-1} \cdot \mathcal{R}^* m_c) \]
OT Implementations

**RSA**
\[ (* = x \mod n, \cdot = x \mod n) \]

**El-Gammal**
\[ (* = x \mod p, \cdot = x \mod p) \]

**Goldwasser-Micali**
\[ (* = (+), \cdot = x \mod n) \]

**Paillier**
\[ (* = + \mod N, \cdot = x \mod N^2) \]
Use ZK proofs to make sure both party follow the protocol.
(2.5)
Quantum Secure OT Implementations
Quantumly

Oblivious Transfer

B₀ → 1/2-OT → Bₑ

B₁ → C

Oblivious Function Evaluation

x → f(x,y) → y
g(x,y)
Quantumly

Oblivious Transfer

B₀ → B₁

1/2 - 0T

Quantum Communication

BIT COMMITMENT

COMMIT

UNVEIL

Quantum One-way Function

b, 29 - 41 - 02 - 17
Quantumly Secure
Classically Implemented

Oblivious Transfer

\[ B_0 \xrightarrow{\text{1/2-OT}} B_c \]

\[ B_1 \xrightarrow{\text{c}} C \]

Quantum Enhanced Trapdoor
One-way Permutation

Quantum One-way Function

Oblivious Function Evaluation

\[ f(x,y) \xrightarrow{\text{f,g}} g(x,y) \]

\( b, 29 - 41 - 02 - 17 \)
Quantum Enhanced Trapdoor One-way Permutation

\[ \{ \text{QETOP} \} = \emptyset ? \]
Quantum Enhanced Trapdoor One-way Permutation

Discrete Logarithm

Factoring

RSA

Elliptic Curves
Quantum Enhanced Trapdoor One-way Permutation
Quantumly Secure
Classically Implemented

Oblivious Transfer

B_0 \rightarrow B_c
B_1 \rightarrow C

BIT COMMITMENT

COMMIT

UNVEIL

Quantum Random-Self-Reducible Encryption Scheme

Quantum One-way Function

Oblivious Function Evaluation

b, 29 - 41 - 02 - 17

f(x, y) \rightarrow g(x, y)

© Claude Crépeau 2002-2010
Quantum Random-Self-Reducible Encryption Scheme
Quantum Random-Self-Reducible Encryption Schemes

- RSA
- El-Gammal
- Goldwasser
- Micali
- Paillier
- Elliptic Curves
Quantum Random-Self-Reducible Encryption Schemes

McEliece

Lattices

LWE

Integer GCD
Quantum Secure
Classically Implemented

Oblivious Transfer

\[ B_0 \rightarrow 1/2-OT \rightarrow B_c \]

\[ B_1 \rightarrow C \]

Quantum Weakly Random-Self-Reducible Encryption Scheme
Quantum Weakly Random-Self-Reducible Encryption Scheme
**THIS WORK**

A public-key encryption scheme \((\text{enc}, \text{dec})\) is *Weakly Random-Self-Reducible* if there exists a pair of PPT algorithms \((\text{Rs}R, \text{Rs}R^{-1})\) such that for all \(\mathbb{R}, m,\)

\[
\text{Rs}R^{-1}(\mathbb{R}, \text{dec}(\text{Rs}R(\mathbb{R}, \text{enc}(m)))) = m
\]

and there exists a PPT distribution on \(\mathbb{R}\) s.t. for all \(m, m'\)

\[
\text{Rs}R(\mathbb{R}, \text{enc}(m)) \sim \text{Rs}R(\mathbb{R}, \text{enc}(m')).
\]
(3) Implementation from QwRsRES
\[ \text{enc}_A(m_0) \rightarrow U_0 \]
\[ \text{enc}_A(m_1) \rightarrow U_1 \]
\[ \mathbb{Z}_c \rightarrow \text{RsR}_A(\mathbb{Z}, U_c) \]
Approximate Integer GCD

Let $p$ be a large odd integer. Define several $(k)$ $x_i$’s as follows

$$x_i = pq_i + 2r_i$$

with $x_i \gg p \gg \sum |r_i|$

w.l.o.g. assume $x_0 = \text{largest } x_i$ and $q_0$ is odd.
Approximate Integer GCD

Let \( p \) be a large odd integer. Define several \((k)\) \( x_i \)'s as follows

\[
x_i = pq_i + 2r_i \quad \text{with} \quad x_i > p > \sum |r_i|
\]

Define the following public-key encryption function:

\[
\varepsilon_x(s,e,b) = (\sum_{i>0} x_i s_i + 2e + b) \mod x_0
\]

where \( b = \text{input bit, } s = \text{rand bin vector, and rand error } |e| < p \)

\[
b = \text{parity}(\varepsilon_x(s,e,b) - \text{nearest multiple of } p)
\]
Approximate Integer GCD

Let $p$ be a large odd integer. Define several $(k)$ $x_i$’s as follows:

$$x_i = pq_i + 2r_i \quad \text{with } x_i \gg p \gg \sum |r_i|$$

Define the following public-key encryption function:

$$\varepsilon_x(s,e,b) = (\sum_{i>0} x_i s_i + 2e + b) \mod x_0$$

where $b =$ input bit, $s =$ rand bin vector, and rand error $|e| \ll p$.
Appr Int GCD

\[ \varepsilon_x(R_0, E_0, B_0) \rightarrow U_0 \]

\[ \varepsilon_x(R_1, E_1, B_1) \rightarrow U_1 \]

\[ \varepsilon_x(s, e, b) + U_c \]

Secure if \( |E_0| + |E_1| + k|r_0| + \sum |r_j| \ll |e| \)

\[ \varepsilon_x(s, e, b) + U_0 \sim \varepsilon_x(s', e, 0) \sim \varepsilon_x(s, e, b) + U_1 \]
Insecure if $|E_i| \gg \text{lel}$ or $|r_j| \gg \text{lel}$!
Prove in ZK that

\[ |E_0| + |E_1| + kr_0 + \sum r_j \leq \text{Public Bound.} \]

Use \( |el| \) » Public Bound.
\[ \varepsilon_x(R_0, E_0, B_0) \rightarrow U_0 \]
\[ \varepsilon_x(R_1, E_1, B_1) \rightarrow U_1 \]
\[ \delta_A(z) \rightarrow y \]
\[ B_c = y(+)b \]
(4) Conclusion
Open Problems
Quantum Weakly Random-Self-Reducible Encryption Scheme
Open Problem

McEliece

Find a pair of PPT algorithms \((RsR, RsR^{-1})\)
such that for all \(\mathcal{R}, m,\)

\[
RsR^{-1}(\mathcal{R}, \text{dec}(RsR(\mathcal{R}, \text{enc}(m)))) = m
\]

and there exists a PPT ditribution on \(\mathcal{R}\) s.t. for all \(m, m'\)

\[
RsR(\mathcal{R}, \text{enc}(m)) \sim RsR(\mathcal{R}, \text{enc}(m')).
\]
Oblivious Transfer from Weakly Random-Self-Reducible Encryption

Claude Crépeau

School of Computer Science
McGill University

joint work with Raza Ali Kazmi
Randomized Oblivious Transfer

\[ \mathcal{R}^0 \quad 1/2-OT \quad \mathcal{R}^\circ \]

\[ \mathcal{R}^1 \quad \mathcal{C} \]
Randomized Oblivious Transfer
Randomized Oblivious Transfer
Randomized Oblivious Transfer

\[ D = \odot(+)C \]
Randomized Oblivious Transfer

\[ Z_0 = B_0(+)\otimes D \]
\[ Z_1 = B_1(+)\otimes \neg D \]
\[ B_c = Z_c(+)\otimes \neg \]

\[ D = \otimes (+)C \]
\[ \text{if } B_0 = B_1 \text{ then } \operatorname{enc}_B(B_0) \]
if $B_0 = B_1$ then
\[
\text{enc}_B(B_0)
\]
else
\[
\text{enc}_B(B_0) \cdot U \sim \text{enc}_B(B_0^*c)
\]
This work:

\[ \begin{align*}
\text{if } B_0 &= B_1 \text{ then } \\
& \quad \text{enc}_B(B_0) \\
\text{else } & \quad \text{enc}_B(B_0) \cdot U \\
& \quad \sim \text{enc}_B(B_0 \ast c)
\end{align*} \]
\( \cup \) \hspace{1cm} \text{enc}_B(c)

if \( B_0 = B_1 \) then
\[ \text{enc}_B(B_0) \]

else
\[ \text{enc}_B(B_0) \cup \sim \text{enc}_B(B_0 \ast c) \]

z or \( \exists \)