Tutorial XI group 2

28 November 2019 16:05

Two party cryptography part two

→ Coin tossing

→ Rabin - OT

↳ Rabin - OT ⇔ 1-out-of-2 - OT

→ Example of practical use of 1-out-of-n OT

Coin tossing (slide 9)

Elements: Alice knows two large primes p, q

Bob knows $n = p \cdot q$ (but not p and q)

1. → Bob chooses $x_B < \frac{n}{2}$ and sends $y = x^2 \bmod n$ to Alice

2. → Alice calculates $x_i \in \{x_1, x_2, x_3, x_4 \mid x_i^2 = y \bmod n\}$

$x_1 < x_2 < x_3 < x_4$ $\quad x_1 = -x_4$

$< \frac{n}{2}$ $\quad x_2 = -x_3$

$x_1 = x$

$x_4 = n - x$ $\quad x + (n-x) = n \Rightarrow x < \frac{n}{2}$ or $n - x < \frac{n}{2}$

3. → Alice chooses $x_A \in \{x_1, x_2\}$ at random and discloses A to Bob

(e.g. by sending the least significant bit where binary representations of x_1 and x_2 differ

4. → Both Alice and Bob reveal all their information $A = \{x_1, x_2, x_3, x_4\}$ $B = \{x_B\}$ they use it to verify

$A = \{x_1, x_2, x_3, x_4\}$ $B = \{x_B\}$ they use it to verify whether Alice guessed x correctly

5. → if Alice won outcome is 1
if Alice lost outcome is 0

Assume in step 3 Alice discloses x_A instead of her guess

→ $x_A = x_B$ Bob can't cheat
(he doesn't learn anything new)

→ $x_A \neq x_B$ Bob now can cheat

He can say she guessed correctly and in step 4 reveal $x_B = x_A$

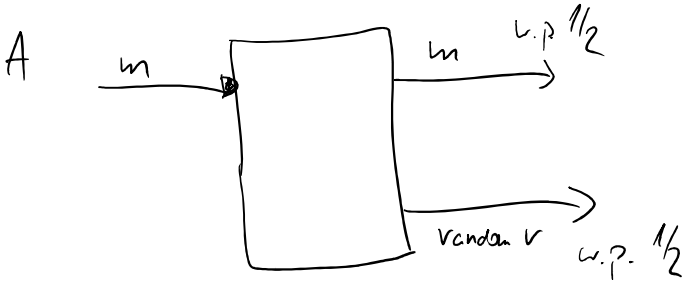
He can say she didn't guess correctly and in step 4 reveal $x_B \neq x_A$

Revealing only LSB of her choice can be used to verify her guess in step 4 without revealing x_A.

Security against Alice — IT

Security against Bob — Computational

Rabin - OT



→ Alice doesn't learn what happened

- Bob knows if he got r or m

Rabin OT protocol

1.) Alice chooses large primes p and q and sends $n = pq$ to Bob

2.) Bob chooses x and sends $y = x^2 \bmod n$

3.) Alice calculates $\{x_1, x_2, x_3, x_4 \mid x_i^2 = y\}$, chooses one at random (x_A) and sends it to Bob

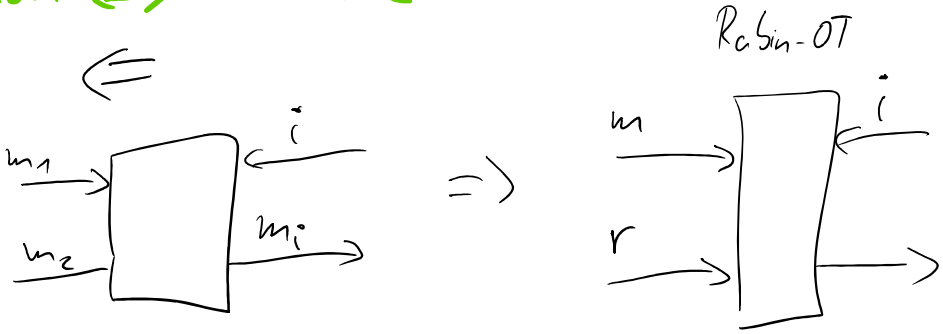
1.) Information (m) Alice is sending is p and q

2.) Bob knows two square roots (x_1, x_4) or (x_2, x_3)

3.) Bob learns a new root w.p. $1/2$

4.) Alice doesn't know if she disclosed the factors

Rabin $\Leftarrow$ 1-out-of-2



Rabin $\Rightarrow$ 1-2

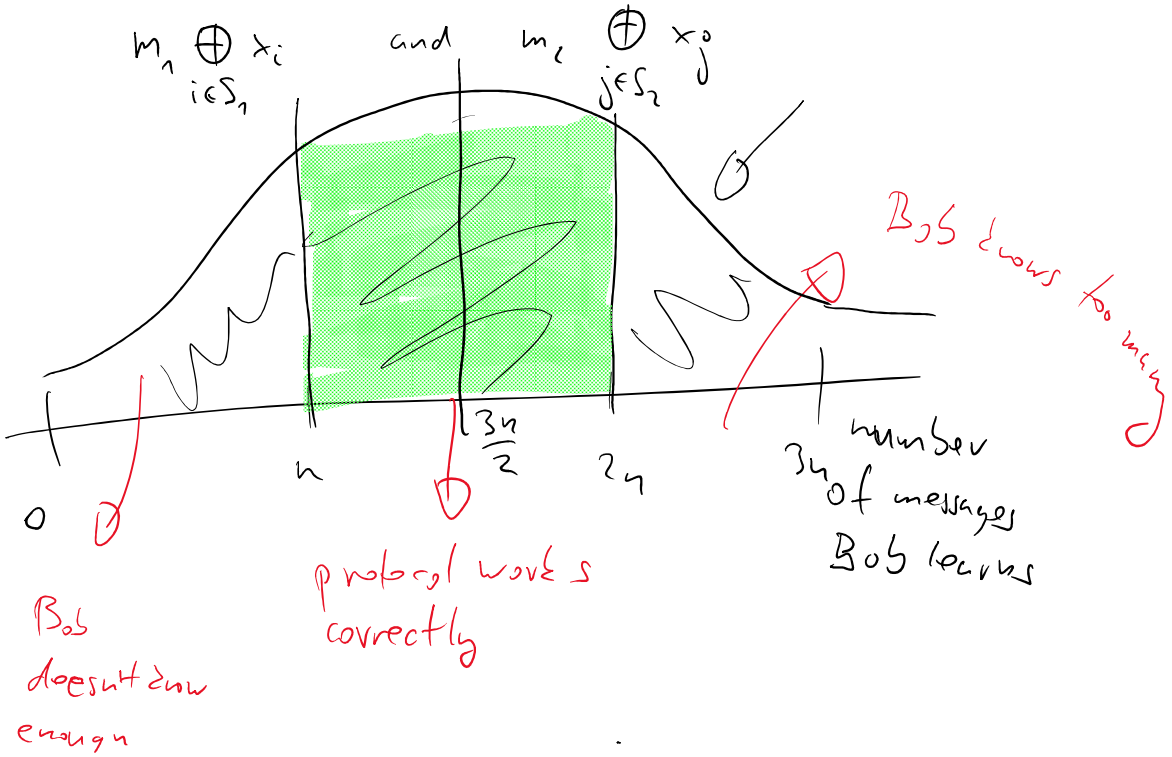
1.) Alice sends $3n$ randomly chosen bit messages $(x_{11}, \ldots, x_{3n})$ to Bob using Rabin OT

2.) Bob chooses n indices of the messages he received I and n indices of the messages he did not receive J

3.) Bob sends (I, J) if he wants to learn m_1

sends (I, I) if he wants to learn m_2

4.) Alice receives (S_1, S_2) and sends



Chernoff tail inequalities claim that the probability of receiving $< n$ messages drops exponentially with n, or $> 2n$

Example of interesting use of 1-out-of-n OT

Scenario: Alice is selling vouchers for her online shop which can be used to pay.

Requirements: 1.) they are hard to forge

2.) they are anonymous (Alice cannot match a voucher to a person she sold it to)

1.) Alice creates a message

$x =$ "Voucher for 100 kč"

and the voucher (x, S), where S is Alice's signature.

PROBLEM: Users can copy (t, S) and pay with them

This is anonymous:

2.) Alice creates a message — id. is a counter

$x_i =$ "Voucher for 100 kč, id: i"

Voucher is a pair (x_i, S_i) S_i is her signature.

PROBLEM: Not anonymous voucher can be matched to its buyer.

3.) 1-of-n OT

Alice creates a (huge) database of vouchers

$(x_1, S_1)\ (x_2, S_2) \ldots (x_n, S_n)$

if Bob buys a voucher Alice sends it via 1-of-n OT

Later if voucher is used to pay it is removed from the database

PROBLEM: Alice can sell the same voucher twice.