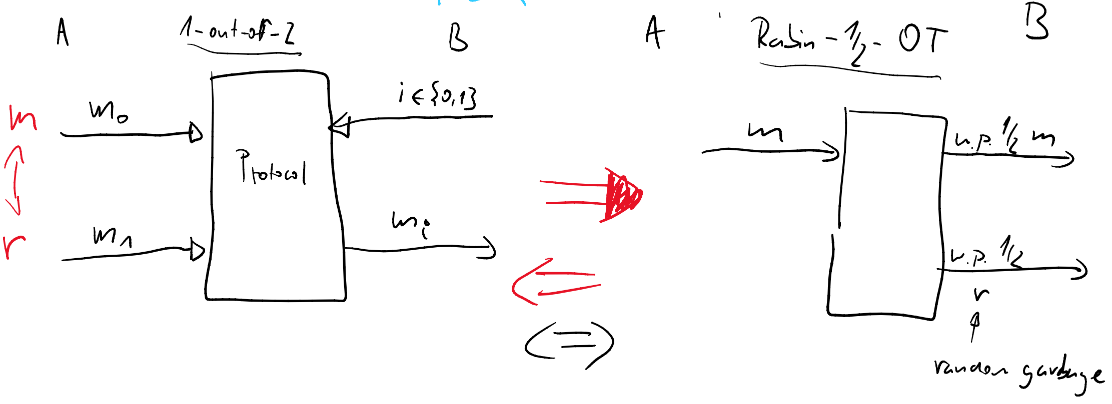
Tutorial 11 ENG

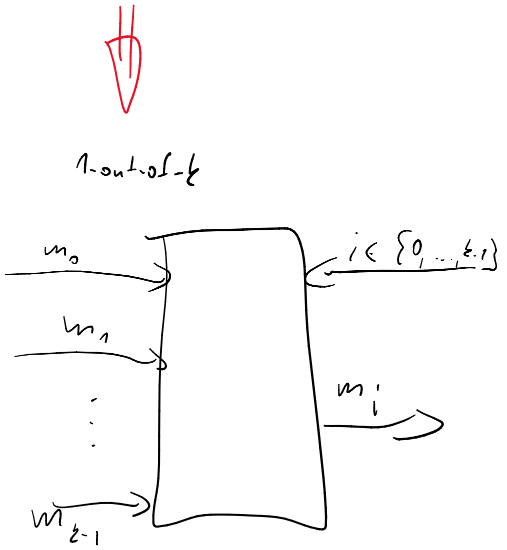
01 December 2021 13:59

TWO-PARTY CRYPTOGRAPHY 2

- → OBLIVIOUS TRANSFER
- → 1-out-of-2 OT vs. Rabin ½-OT
- → An example of 1-out-of-n OT use

OBLIVIOUS TRANSFER





1-out-of-k can be used to build protocols for

SMC - secure multiparty computation

SFE - secure function evaluation

→ n users and each user has an input x_i and they want to calculate $f(x_1, \dots, x_n)$

and they want to calculate $f(x_1, \dots, x_n)$
in such a way that they do not reveal x_i

VOTING: function that outputs the most common input

Security properties of 1-out-of-2 OT

1.) Alice does not learn Bob's choice i.

2.) Bob learns only one message

1-out-of-2 protocol using PKE (public key encryption)

1.) Alice generates two pairs of PKE keys (secret key, public key) (s_0, p_0) and (s_1, p_1)

sends p_0 and p_1 to Bob.

2.) Bob choses a random string k with a key of his choice
(p_0 if he wants to learn m_0 and p_1 if he wants to learn m_1)
and sends $B = e_{p_i}(k)$ to Alice

3.) Alice calculates $A_0 = dec_{s_0}(B)$ and $A_1 = dec_{s_1}(B)$
and she sends $M_0 = m_0 \oplus A_0$ and $M_1 = m_1 \oplus A_1$
to Bob

4.) Bob decrypts M_i of his choice, while the other message
is not available

Security
Can Alice guess Bob's choice? B is either $e_{p_0}(k)$ or $e_{p_1}(k)$, k is
a random string => they are statistically indistinguishable. => IT security
Can Bob find both messages? Yes, by breaking PKE => c...

... indistinguishable. => II security

Can Bob find both messages? Yes, by breaking PKE => Computational security

Rabin $\frac{1}{2}$ - OT protocol

1.) Alice chooses primes p and q and sends $n = p \cdot q$ to Bob

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

3.) Alice calculates $\{x_1, x_2, x_3, x_4 \mid x_i^2 = y \mod n\}$ she then sends one at random to Bob

$\boxed{\gcd(x_1 - x_3, n) = p}$

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

2.) Bob knows two square roots $(x, -x)$

3.) Bob learns a new square root w.p. $\frac{1}{2}$ = he learns p and q

3.5) Alice can use RSA to send a message and then $\frac{1}{2}$-OT to disclose private keys to Bob.

4.) Alice doesn't know if he learned a new square root.

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

$\Leftarrow$ easy

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

1.) Alice sends $3n$ randomly chosen bit messages $(x_1, \ldots, x_{3n})$ to Bob using Rabin OT.

2.) Bob chooses n indices of the messages he received I $\varnothing$

and $\frac{n}{2}$ indices of the messages he did not receive J $\varnothing$

3.) Bob sends (I, J) if he wants to learn m_0

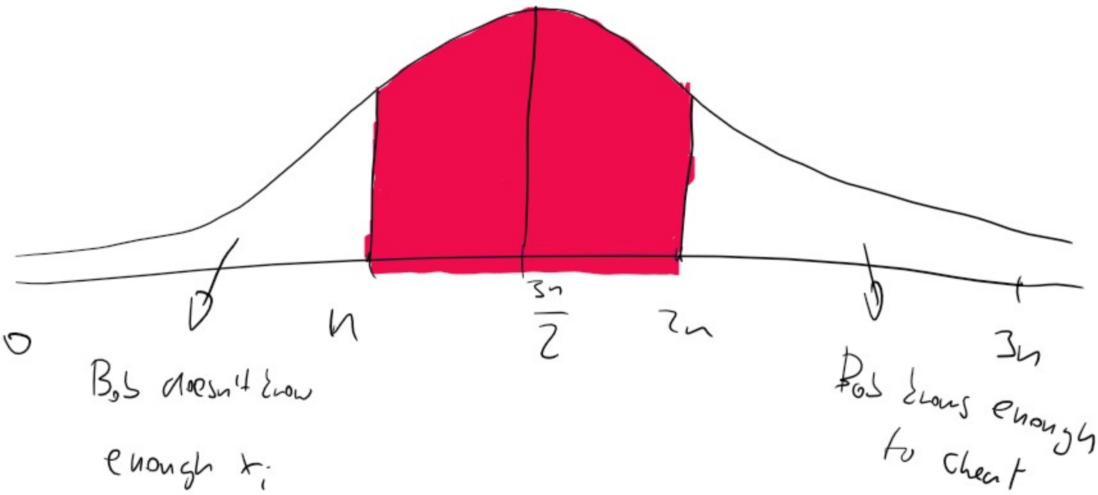
or (J, I) if he wants to learn m_1

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

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

$$m_0 \bigoplus_{i \in S_1} x_i \quad \text{and} \quad m_1 \bigoplus_{i \in S_2} x_i$$

5.) Bob decrypts the message of his choice and the other one is not available.



Chernoff tail inequalities - claim that the probability of receiving less than n messages or more than $2n$ messages decreases exponentially with n.

Example of interesting use of 1-out-of-2 OT

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

Requirements: 1.) they are hard to forge

2.) they are anonymous (Alice cannot match a voucher to a person who bought it)

1.) Alice creates a message x = "voucher for 100 CZK"

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

PROBLEM: Voucher can be reused.

$\boxed{\text{This is anonymous}}$

2.) Alice creates a message

id is a counter

x_i = "Voucher for 100 CZK, id: i"

Voucher is (x_i, s_i), where s_i is her signature

PROBLEM: Alice can keep a record of who bought which voucher

3.) 1-of-n OT

Alice creates a (large) number of vouchers

$(x_1, s_1), (x_2, s_2) \dots (x_n, s_n)$

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

Later if voucher is used to pay, it is removed from her database

PROBLEM: Alice can sell a voucher multiple times.