Secure Multiparty Computations

CSG 252 Lecture 11

December 9, 2008

Riccardo Pucella

Oblivious Transfer

Suppose Alice has two messages m0 and m1

- Suppose Bob has a bit b
- Bob wants to have mb

Constraints:

- Bob does not want Alice to know b
  - Or, equivalently, which mb he wants
- Alice does not want Bob to know both m0 and m1

1-2 Oblivious Transfer

(The RSA-based version)

Alice generates an RSA key: N, public e, private d

A		B
	N, e, x_0, x_1 →	
msgs m_0, m_1		bit b
random x_0, x_1	← q	random k
$t_0 = m_0+(q-x_0)^d$		$q = k^e+x_b \pmod N$
$t_1 = m_1+(q-x_1)^d$	t_0, t_1 →	Bob computes
		t_b-k
		$(= m_b)$

1-N Oblivious Transfer

- Alice has N messages
- Bob has an index i
- Bob wants to receive i-th message without Alice learning i
- Alice wants Bob to receive only one message

Related to private information retrieval

- Added database's privacy requirement

K-N Oblivious Transfer

- Alice has N messages
- Bob wants K of those messages without Alice learning which
- Alice wants Bob to receive only K messages

Two possibilities:

- messages requested simultaneously (non-adaptive)
- messages requested sequentially (adaptively)
    - can depend on previous requests

The Millionaires Problem

(Andrew Yao, 1982)

Alice and Bob are both millionaires

- Alice has I million dollars
- Bob has J million dollars
- Alice and Bob both want to know who's richer
- But they don't want the other to know how much money they have
- For simplicity, assume 1 <= I,J <= 4

The Protocol

(The RSA-based version)

Alice generates an RSA key: N, public e, private d

A | **B**

A → B: N, e

B: J

B: M-bits random x

B: $C = x^e \pmod N$

B → A: $C - J + 1 \pmod N$

A: I

A: M/2-bits random prime P

A → B: $P, Z_1, \ldots Z_I, Z_{I+1}+1, \ldots, Z_4+1$

Bob receives $P, R_1, \ldots, R_4$:

If $R_J = x \bmod P$

then $I >= J$ (o/w $I < J$)

The Proto

(The RSA-based version)

Alice generates an RSA k

$$Z_1 = (C-J+1)^d \pmod{P}$$
$$Z_2 = (C-J+2)^d \pmod{P}$$
$$Z_3 = (C-J+3)^d \pmod{P}$$
$$Z_4 = (C-J+4)^d \pmod{P}$$

A

N

I

$C-J+1$

dom x

(mod N)

M/2-bits random prime P

$P, Z_1, \ldots Z_I,$
$Z_{I+1}+1, \ldots, Z_4+1$

Bob receives $P, R_1,\ldots,R_4$:
If $R_J = x \bmod P$
then $I>=J$ (o/w $I<J$)

Secure Multiparty Computation

Given a publicly known function F of N inputs and producing N outputs

- $F(x_1,\ldots,x_n) = (y_1,\ldots,y_n)$

Suppose N parties, each party i with a private value a_i

- Goal: compute $F(a_1,\ldots,a_n) = (r_1,\ldots,r_n)$
- Each party i wants to know r_i
- No party want others to learn their private value

Secure Multiparty Computation

Oblivious Transfer as a secure multiparty computation:

- Function $F(<m_0,m_1>,b) = (nil,m_b)$
  - Alice has $<m_0,m_1>$, Bob has b
  - Bob wants m_b (don't care about Alice)

Millionaires Problem as a secure multiparty computation:

- Function F(I,J) = (Alice,Alice) if I>=J

  = (Bob,Bob) if I<J
  - Alice has I, Bob has J
  - Alice and Bob want to know who's richer