EECS 575: Advanced Cryptography
Fall 2021
Lecture 23

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Recap from last time
- Secure two-party computation (2PC): model
- Security definition for 2PC
- Secure 2PC for arbitrary circuits
- Oblivious transfer

Agenda for this lecture

- Announcements
- Recap from last time
- Secure two-party computation (2PC): model
- Security definition for 2PC
- Secure 2PC for arbitrary circuits
- Oblivious transfer

Announcements

- Take-home exam 2 will be released tonight, due next Monday

Recap from last time

* zero-knowledge proofs:
  - basics (PS and ZKPs, soundness, ZK, HVZK
  - all very large proofs
    - graph iso. non-iso
    - Graph 3Col
    - sigma protocols, Schnorr
* Last ~10 years:
  - GGPR Gennaro et al.
  - "succinct" zero-knowledge
    3 group elements of Groth16 ZKP
  - Privacy in cryptocurrencies
  - other applications (see my paper)
  - Take my 498/598

Agenda for this lecture

- Announcements
- Recap from last time
- Secure two-party computation (2PC): model
- Security definition for 2PC
- Secure 2PC for arbitrary circuits
- Oblivious transfer

Secure Two-party computation

Jim
1M or 2M

[1A > 2M]

Ryan
1.5M

Yao Millionaires problem

Model for 2PC

Honest-but-curious: only infer info from honest protocol run

Deterministic

↳ $f(\cdot,\cdot)$

$\text{view}_{P_i}[P_1(x_1) \leftrightarrow P_2(x_2)]$ is randomness of P_i, x_i, msgs exchanged

$\text{out}_{P_i}[P_1(x_1) \leftrightarrow P_2(x_2)]$

$P_1(x_1)$ — $P_2(x_2)$

2PC

$f(x_1, x_2)$ $f(x_1, x_2)$

Same output given to both parties

(can modify F to meet this)

Agenda for this lecture

- Announcements
- Recap from last time
- Secure two-party computation (2PC): model
- Security definition for 2PC
- Secure 2PC for arbitrary circuits
- Oblivious transfer

Really complicated! 2PC security

- What if abort?
- How to guarantee both parties receive output?
- How to ensure composability?
  - (>2 parties) what if collusion?
  - etc.

2PC security

Static, semi-honest security model

Pair (P_1, P_2) is a secure 2PC for $F(\cdot,\cdot)$ (def. poly time) if:

* Completeness $\forall i \in \{1,2\}$, $\forall x_1, x_2$,
$$Out_{P_i}[P_1(x_1) \leftrightarrow P_2(x_2)] = F(x_1, x_2); r$$

* Privacy $\forall i \in \{1,2\}$ $\exists$ $\$_i$ $\forall x_1, x_2$
$$View_{P_i}[P_1(x_1) \leftrightarrow P_2(x_2)] \stackrel{c}{\approx} \$_i(x_i, F(x_1, x_2))$$

(ZKPs can be viewed as 2PCs)

Important: $\$_i$ doesn't get other party's input!

2PC security

Randomized functions:

$f(x_1, x_2; r)$ ← this is a distribution

Fix random string r. Both parties get $f(x_1, x_2; r)$ for fixed r.

(see notes.)

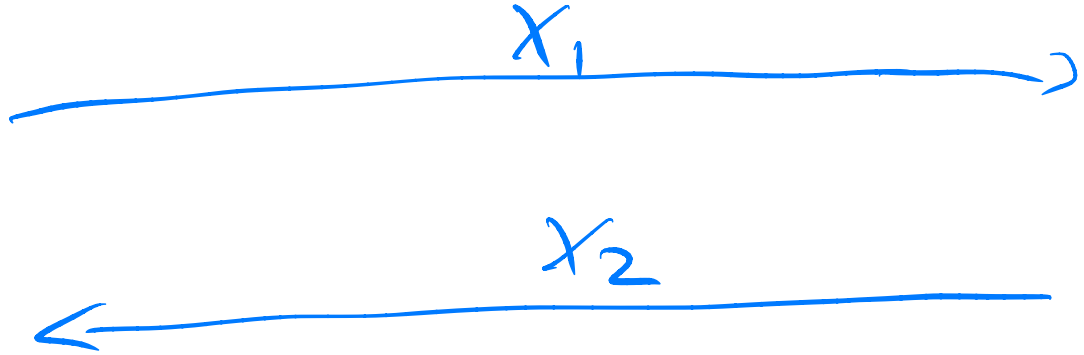
Agenda for this lecture

- Announcements
- Recap from last time
- Secure two-party computation (2PC): model
- Security definition for 2PC
- Secure 2PC for arbitrary circuits
- Oblivious transfer

~~Yao's garbled circuits~~

Addition 2PC

$P_1(x_1)$ $F(x_1, x_2) := x_1 + x_2$ $P_2(x_2)$



Output $x_1 + x_2$

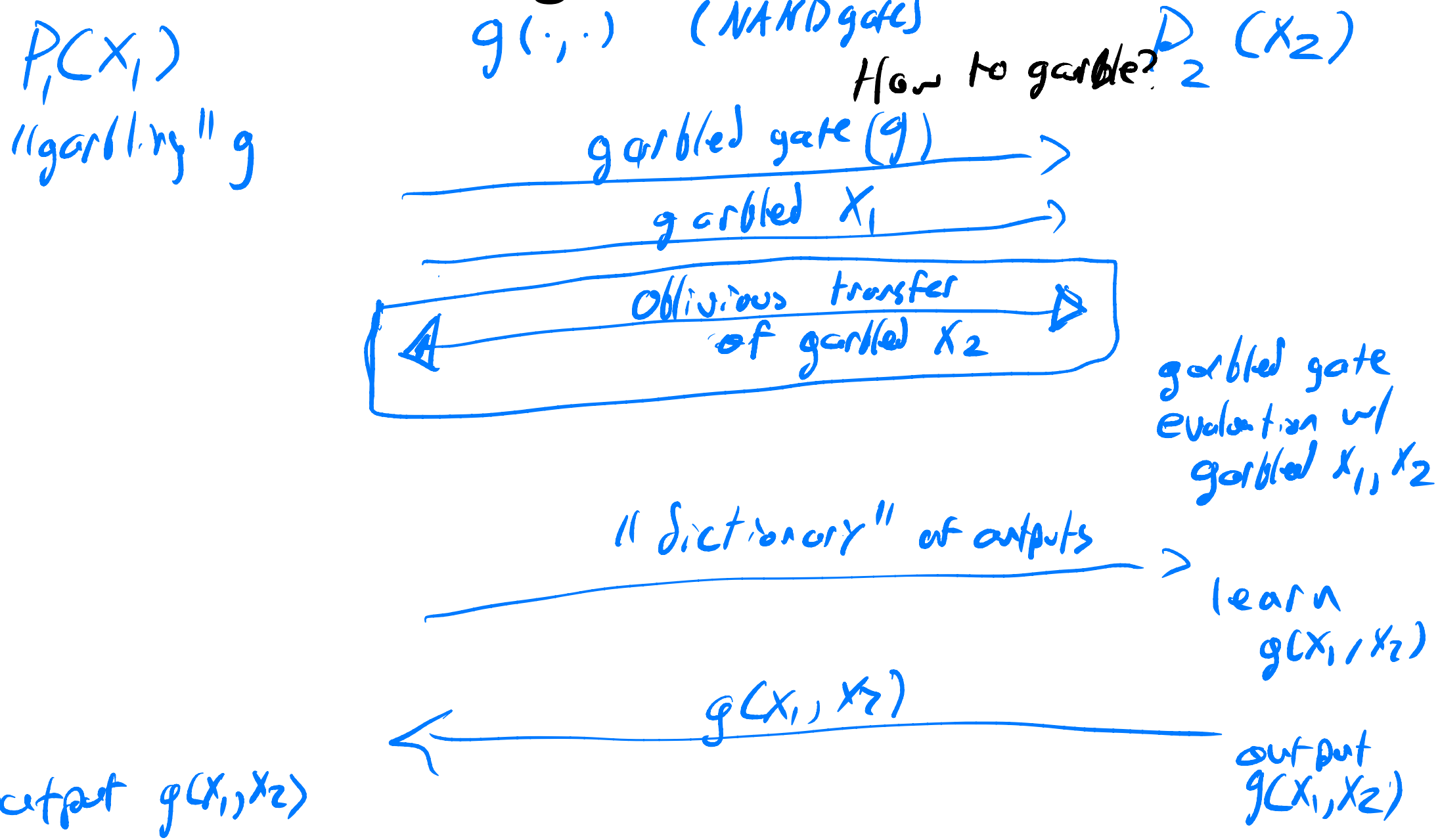
Output $x_1 + x_2$

* completeness: trivial
* privacy: simulator $S(x_i, x_1 + x_2)$:

Ret x_i, $x_1 + x_2 - x_i$, $x_1 + x_2$

Output reveals other party's input

Yao's garbled circuits



Yao's garbled circuits

1. Assign random symmetric keys to input/output values

(k_0^0, k_1^0) for wire 0

(k_0^1, k_1^1) for wire 1

(K_0^f, K_1^f) for "final" wire

2. P_2 has only $K_{x_1}^0$ and $K_{x_2}^1$

3. Scramble

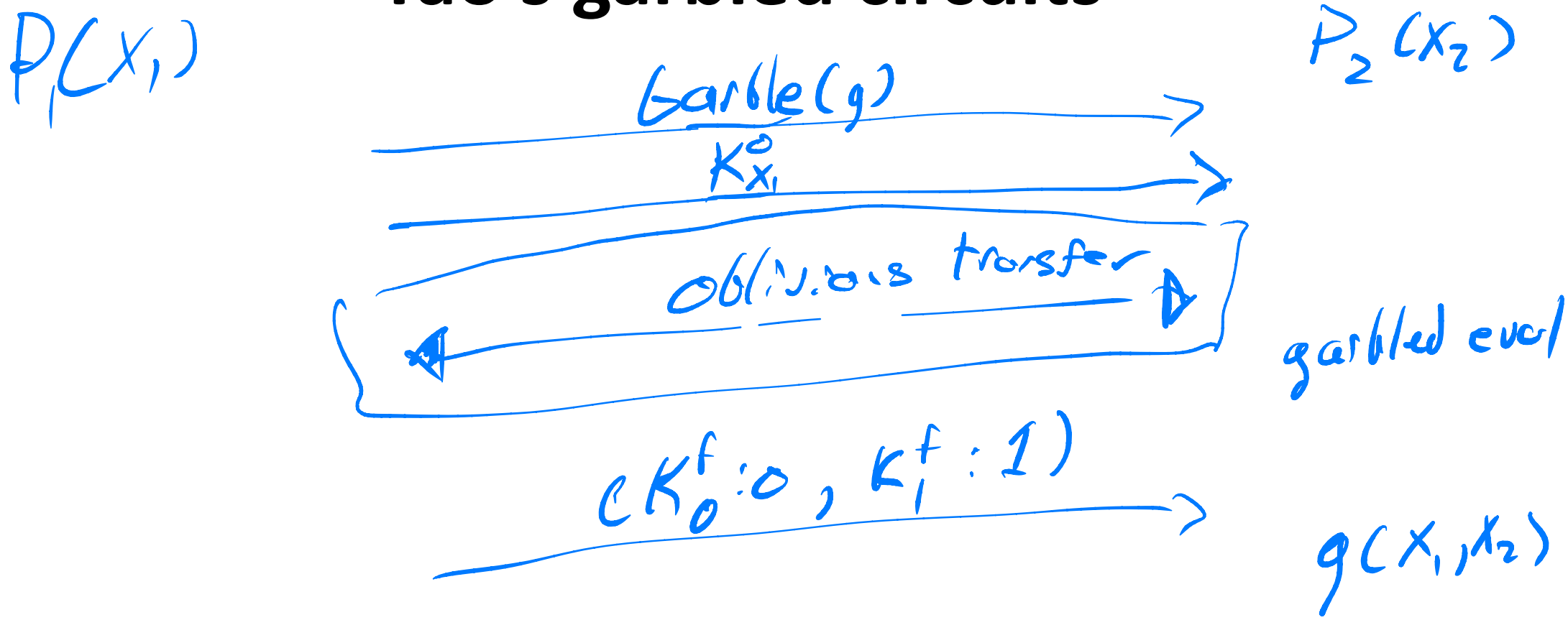
$$Enc_{k_0^0}(Enc_{k_0^1}(k^f_{g(0,0)}))$$

$$Enc_{k_0^0}(Enc_{k_1^1}(k^f_{g(1,0)}))$$

$$Enc_{k_0^0}(Enc_{k_1^1}(k^f_{g(0,1)}))$$

$$Enc_{k_1^0}(Enc_{k_1^1}(k^f_{g(1,1)}))$$

Yao's garbled circuits



Agenda for this lecture

- Announcements
- Recap from last time
- Secure two-party computation (2PC): model
- Security definition for 2PC
- Secure 2PC for arbitrary circuits
- Oblivious transfer

Oblivious Transfer

Two 6.ts

$P_1(X_0, X_1)$

Can't learn b

$g((X_0, X_1), b) : X_b$

To learn K'_{X_2},

P_1/P_2 do n OTs.

P_1 doesn't learn X_2,

P_2 doesn't learn K'_{1-X_2}

Selection b.t

$P_2(b)$ ←

Can't learn

X_{1-b}.

Oblivious Transfer

$P_1(x_0, x_1)$

$(f_S, f_S^{-1}) \leftarrow \$(1^n)$

(S, t)

$P_2(b)$

S

$v_b \leftarrow \{0,1\}^n$

$w_b \leftarrow f_S(v_b)$

$w_{1-b} \leftarrow \{0,1\}^n$

Indep. of b

w_b, w_{1-b}

$z_0 \leftarrow f^{-1}(w_0)$

$z_1 \leftarrow f^{-1}(w_1)$

$r_0 = h(z_0) \oplus x_0, \; r_1 = h(z_1) \oplus x_1$

x_{1-b} is hidden by TDP security

$z_b = h(v_b)$

$x_b = z_b \oplus r_b$