- Scribes?
- OT preprocessing + extension
- Malicious security (2-party setting)
- WI, ZK, PoK
- The GMW compiler (2-party setting)

Preprocessing

$$P_1 \xleftarrow{x_0,\, x_1} \boxed{rOT} \xrightarrow{b,\, x_b} P_2$$

---

s_0, s_1 $\qquad\qquad \xleftarrow{\quad b \oplus c \quad}$ $\qquad\qquad c$

$r_0 = s_0 \oplus x_{b \oplus c}$

$r_1 = s_1 \oplus x_{1 \oplus b \oplus c}$ $\qquad \xrightarrow{\quad r_0,\, r_1 \quad}$ $\qquad s_c = r_c \oplus x_b$

$$= (s_c \oplus x_{\underbrace{c \oplus b \oplus c}}) \oplus x_b$$

$$= s_c \oplus x_b \oplus x_b$$

$$= s_c$$

OT extension

parties will generate m OTs on k-bit strings

from

k OTs on m-bit strings — base OTs

$m >> k$, $\quad k \sim$ security parameter

Total Cost $= O(k)$ public-key operations $+ O(m)$ private-key operations

Aside: given k-bit OT, easy to gen m-bit OT for any $m > k$

$P_1(X_0, X_1)$ | $P_2(b)$

$k_0, k_1 \leftarrow \{0,1\}^k$

$k_0, k_1 \rightarrow \boxed{} \leftarrow b$

$\rightarrow k_b$

$\xrightarrow{\mathrm{Enc}_{k_0}(X_0),\ \mathrm{Enc}_{k_1}(X_1)}$

P_1 | P_2

$r = r_1 \cdots r_m$

(wants x_{i,r_i} for all i)

$x_{1,0}$

$x_{1,1}$

$\vdots$

$x_{m,0}$

$x_{m,1}$

$\underbrace{\qquad\qquad}_{k}$

$m \left\{ \begin{array}{c} T_1 \\ t_1 \cdots t_k \\ T_m \end{array} \right.$

base OTs

$s_i \rightarrow \boxed{OT} \leftarrow t_i,\ t_i \oplus r$

$\leftarrow t_i \oplus s_i \cdot r$

$s \leftarrow \{0,1\}^k$

q_1

$t_1 \oplus s_1 \cdot r \quad \cdots \quad t_k \oplus s_k \cdot r$

q_m

$T_i = q_i \oplus r_i \cdot s$

$\xrightarrow{X_{i,0} \oplus H(q_i),\ X_{i,1} \oplus H(q_i \oplus s)}$

$c_{i,0} \qquad c_{i,1}$

$x_{i,r_i} = c_{i,r_i} \oplus H(T_i)$

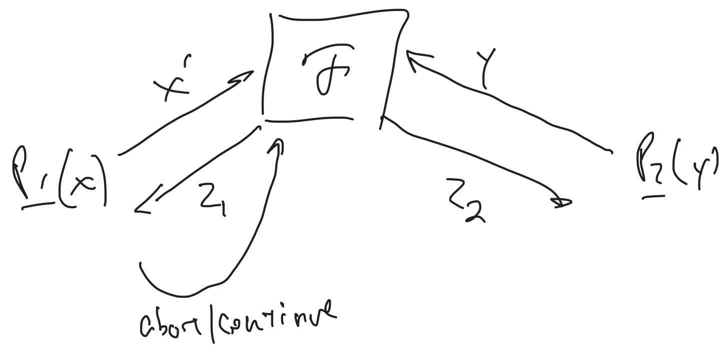
$q_i = T_i \oplus r_i \cdot s$

Malicious security (2-party)

- real-world execution of protocol Π w/ some adversary A

  (Output of honest party, view of A)

- ideal-world evaluation of $\mathcal{F}$



Zero-knowledge (proofs of knowledge)

NP language L

i.e., there exists an efficient R_L s.t. $x \in L$ iff $\exists w$ s.t. $R_L(x,w)=1$

I.e., $L =$ SAT $= \{$boolean formulas ϕ that are satisfiable$\}$

$R_{SAT}(\phi, x) = 1$ iff $\phi(x) =$ true

I.e., $L =$ HAM $= \{$directed graph G s.t. G has a Ham. cycle$\}$

$R_{HAM}(G, v_1 v_2 \cdots v_n) = 1$ iff $v_1 \cdots v_n$ is a Ham cycle in G

$b = 1 \iff x = x'$
and $R_L(x,w) = 1$

Zero-Knowledge proofs – evaluating $\mathcal{F}_{ZK}$ against a malicious V

proofs of Knowledge – evaluating $\mathcal{F}_{ZK}$ against a malicious P

ZKPoK – securely evaluating $\mathcal{F}_{ZK}$

Show ZKPoK protocol for an NP-complete language

$\Rightarrow$ ZKPoK protocol for all of NP

$\underline{P}(G, \text{cycle})$ $\qquad\qquad\qquad\qquad$ $\underline{V}(G)$

$$A = \begin{pmatrix} \square & \cdots & \square \\ \vdots & \ddots & \vdots \\ \square & \cdots & \square \end{pmatrix} \longrightarrow$$

$b \leftarrow \{0,1\}$

$$\xleftarrow{\quad b \quad}$$

if $b=0$

prove that A corresponds to G

if $b=1$

prove the A has a Ham cycle

if $b=0$

open everything $\longrightarrow$

show isomorphism to G

if $b=1$

open Ham cycle only $\longrightarrow$

verify