A Game-Theoretic Perspective on Oblivious Transfer

Kenji Yasunaga (ISIT)

Joint work with Haruna Higo, Akihiro Yamada, Keisuke Tanaka (Tokyo Inst. of Tech.)

2012.5.8 Crypto Seminar @ Kyusyu University

Cryptography and Game Theory

- Cryptography:
  Design protocols in the presence of adversaries
- Game theory:
  Study the behavior of rational players

Cryptography and Game Theory

- **Cryptography:**
  Design protocols in the presence of adversaries
- **Game theory:**
  Study the behavior of rational players

- **Rational cryptography:**
  Design cryptographic protocols for rational players
  - Rational Secret Sharing [HT04, GK06, ADG$^+$06, KN08a, KN08b, MS09, OPRV09, FKN10, AL11]

Asharov, Canetti, Hazay (Eurocrypt 2011)

- Game-theoretically characterize properties of two-party protocols
  - Protocol π satisfies a “certain” property
    ⇔ A “certain” game defined by π
    has a “certain” solution concept
    with “certain” utility functions
    - Properties: Correctness, Privacy, Fairness
    - Adversary model: Fail-stop adversaries
  - Equivalent defs. for correctness and privacy
  - New def. for fairness

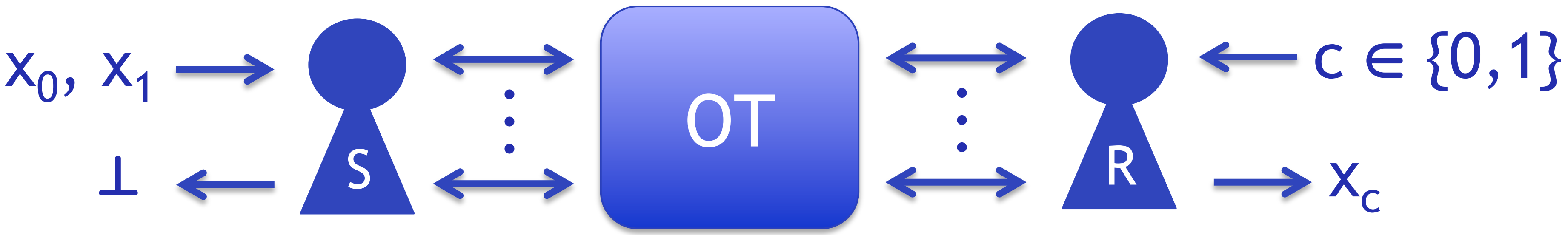
This work

- Game-theoretically characterize properties of "two-message" Oblivious Transfer (OT)
- Advantages compared to [ACH11]

1. Game between two rational players
    - Essentially played by a single player in [ACH11]
2. Characterize correctness and privacy by a single game
3. Malicious adversaries

Oblivious Transfer

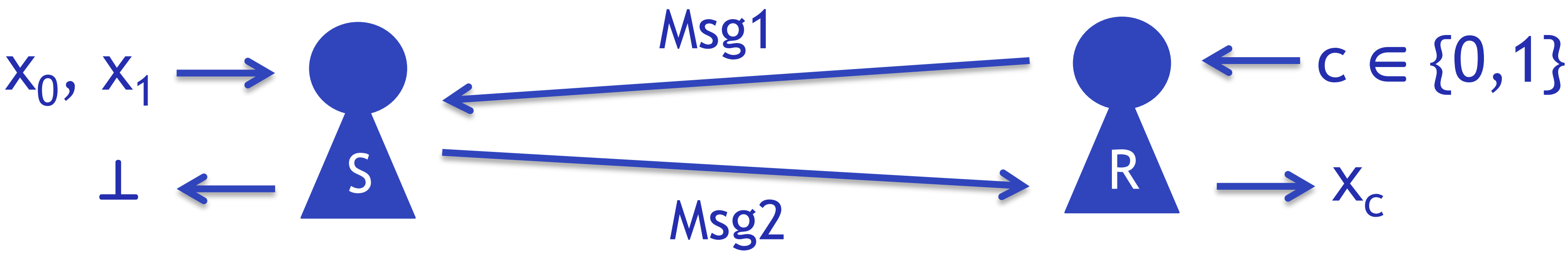
- A protocol between sender S and receiver R



- Correctness: After running the protocol, R obtains x_c and S obtains nothing (or $\perp$)
- Privacy
  - Privacy for S: R learns nothing about x_{1-c}
  - Privacy for R: S learns nothing about c

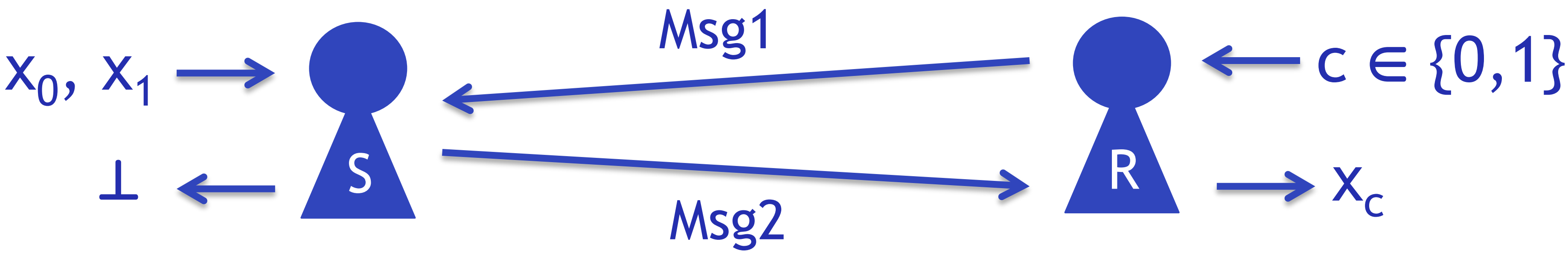
Why “two-message” OT ?

Two-message OT



Why "two-message" OT ?

Two-message OT



- IND based privacy fits for GT framework
  - Utility is high ⇔ Prediction is correct
- Exit IND based privacy for two-message OT

Our results

- Protocol π for two-message OT satisfies "correctness" and "privacy"

  ⇔ A "certain" game defined by π
  has a "certain" solution concept
  with "certain" utility functions

Our results

- Protocol π for two-message OT satisfies "correctness" and "privacy"

  ⇔ A "certain" game defined by π has a "certain" solution concept with "certain" utility functions

  ⇔ A game Game^{π} defined by π has a Nash equilibrium with utility functions $U = (U_S, U_R)$

Cryptographic Correctness of OT

- Protocol $\pi = (S, R)$

Correctness

- $\forall\ x_0, x_1 \in \{0,1\}^*$ s.t. $|x_0| = |x_1|$, $c \in \{0,1\}$,
  $\Pr[\ \mathrm{output}_R(S(x_0, x_1), R(c)) = x_c\ ] \geq 1 - \mathrm{negl}$

Cryptographic Privacy of two-message OT

Privacy for R

- $\forall$ PPT S^* and $x_0, x_1 \in \{0,1\}^*$,
  $\{view_{S^*}(S^*(x_0, x_1), R(0))\} =_c \{view_{S^*}(S^*(x_0, x_1), R(1))\}$

Privacy for S

- $\exists$ a function Choice: $\{0,1\}^* \rightarrow \{0,1\}$ s.t.
  $\forall$ determ. poly-time R^*, $x_0, x_1, x, z \in \{0,1\}^*$, $c \in \{0,1\}$,
  $\{view_{R^*}(S(X^0), R^*(c, z))\} =_c \{view_{R^*}(S(X^1), R^*(c, z))\}$
  where $X^0 = (x_0, x_1)$, and
  $X^1 = (x_0, x)$ if $Choice(R^*, c, z) = 0$, $X^1 = (x, x_1)$ otherwise
  - Choice indicates the choice bit of R^*

Game^{π}

- Protocol: $\pi = (S^{\pi}, R^{\pi})$,
  Input: $x_0, x_1, x, z \in \{0,1\}^*, c \in \{0,1\}$
  Players: Sender (S, G_S), Receiver (R, G_R)
- $\text{Game}^{\pi}((S, G_S), (R, G_R), \text{Choice}, x_0, x_1, x, c, z_S, z_R)$:
  1. $X^0 = (x_0, x_1)$,
     $X^1 = (x_0, x)$ if $\text{Choice}(R, c, z) = 0$, $X^1 = (x, x_1)$ o.w.
  2. $b \leftarrow_R \{0, 1\}$ and set z to be empty if $R = R^{\pi}$
  3. Execute $(S(X^b), R(c, z))$ $(\rightarrow \text{output}_R)$
     Set fin = 1 $\Leftrightarrow$ Protocol finished without abort
  4. G_S guesses c from view_S $(\rightarrow \text{guess}_S)$
     G_R guesses b from view_R $(\rightarrow \text{guess}_R)$
  5. Output $(\text{fin}, \text{output}_R, \text{guess}_S, \text{guess}_R)$

Utility functions $U = (U_S, U_R)$

- $U_S((S, G_S), (R, G_R))$
  $= (-\alpha_S) \cdot (\Pr[\text{guess}_R = b] - 1/2)$
  $+ \beta_S \cdot (\Pr[\text{fin}=0 \vee (\text{fin}=1 \wedge \text{output}_R = x_c)] - 1)$
  $+ \gamma_S \cdot (\Pr[\text{guess}_S = c] - 1/2)$
  - α_S, β_S, γ_S are some positive constants
  - U_S is low if G_R's guess is correct
    or finish w/o abort and output is incorrect
    or G_S's guess is incorrect
- $U_R((S, G_S), (R, G_R))$
  $= (-\alpha_R) \cdot (\Pr[\text{guess}_S = c] - 1/2)$
  $+ \beta_R \cdot (\Pr[\text{fin}=0 \vee (\text{fin}=1 \wedge \text{output}_R = x_c)] - 1)$
  $+ \gamma_R \cdot (\Pr[\text{guess}_R = b] - 1/2)$

Nash equilibrium

- Protocol (S, R) is a Nash equilibrium for Game^{π}

  $\Leftrightarrow$

  $\exists$ Choice s.t. $\forall$ PPT G_S, G_R, S^*, (determ.) R^*, $\forall$ x_0, x_1, x, $z \in \{0,1\}^*$, $c \in \{0,1\}$,

  $U_S((S^*,G_S), (R,G_R)) \leq U_S((S,G_S), (R,G_R)) + \mathrm{negl}$

  and

  $U_R((S,G_S), (R^*,G_R)) \leq U_R((S,G_S), (R,G_R)) + \mathrm{negl}$

Game-theoretic characterization

- Main Theorem:

  Protocol $\pi = (S^{\pi}, R^{\pi})$ for two-message OT satisfies cryptographic correctness and privacy

  if and only if

  $\pi = (S^{\pi}, R^{\pi})$ is a Nash equilibrium for Game^{π} with utility functions $U = (U_S, U_R)$

Proof ("Crypto → Game")

Assume π is not game-theoretically secure

$\Leftrightarrow$ $\pi = (S^\pi, R^\pi)$ is not NE for Game^π

$\Leftrightarrow$ $\forall$ Choice, $\exists\, G_S^*, G_R^*, S^*, R^*, x_0, x_1, x, z, c$ s.t.

- Case 1:
  $U_S((S^*,G_S), (R^\pi,G_R)) > U_S((S^\pi,G_S), (R^\pi,G_R)) + \varepsilon_S$

  or

- Case 2:
  $U_R((S^\pi,G_S), (R^*,G_R)) > U_R((S^\pi,G_S), (R^\pi,G_R)) + \varepsilon_R$

Proof (“Crypto → Game”)

- Case 1:
  $U_S((S^*, G_S), (R^\pi, G_R)) > U_S((S^\pi, G_S), (R^\pi, G_R)) + \varepsilon_S$
  - Recall that
    $U_S((S^\pi, G_S), (R^\pi, G_R))$
    $= (-\alpha_S) \cdot (\Pr[\text{guess}_R = b] - 1/2)$
    $+ \beta_S \cdot (\Pr[\text{fin}=0 \vee (\text{fin}=1 \wedge \text{output}_R = x_c)] - 1)$
    $+ \gamma_S \cdot (\Pr[\text{guess}_S = c] - 1/2)$
- When $S^\pi \rightarrow S^*$
  Case 1-a: $\Pr[\text{guess}_R = b]$ is lower
  Case 1-b: $\Pr[\text{fin}=0 \vee (\text{fin}=1 \wedge \text{output}_R = x_c)]$ is higher
  Case 1-c: $\Pr[\text{guess}_S = c]$ is higher

Proof ("Crypto → Game")

- Case 1-a: Pr[guess_R = b] is lower
  - ➔ Since Pr[guess_R = b] ≤ 1/2 + negl when S*, (R^π, G_R) breaks the privacy for S
- Case 1-b: Pr[fin=0 ∨ (fin=1 ∧ output_R=x_c)] is higher
  - ➔ Pr[fin=0 ∨ (fin=1 ∧ output_R=x_c)] < 1 − ε when S^π
  - ➔ Not cryptographically correct
- Case 1-c: Pr[guess_S = c] is higher
  - ➔ Pr[guess_S = c] ≠ 1/2 ± negl when S*
  - ➔ (S*, G_S) breaks the privacy for R

Proof (“Game → Crypto”)

Assume π is not cryptographically secure

$\Leftrightarrow$

- Case 1: Not cryptographically correct
- Case 2: Cryptographically correct
  - Case 2-a: Not private for S when R^{π}
  - Case 2-b: Private for S when R^{π}, not private for R
  - Case 2-c: Private for R, not private for S when R^{*}

Proof ("Game → Crypto")

- Case 1: Not cryptographically correct
  - ➔ $\exists\ x_0, x_1, c$ s.t. $\Pr[\ \mathrm{output}_R = x_c] < 1 - \varepsilon_1$
  - ➔ $U_S((S^\pi, G_S), (R^\pi, G_R)) < -\beta_S \cdot \varepsilon_1$
    $U_S((S^{def}, G_S), (R^\pi, G_R)) = 0$
  - ➔ U_S is higher when $S^\pi \to S^{def}$
    - S^{def}: Abort before start
    - $\Pr[\mathrm{fin}=0 \vee (\mathrm{fin}=1 \wedge \mathrm{output}_R=x_c)]$ is higher when $S^\pi \to S^{def}$

Proof ("Game → Crypto")

- Case 2: Cryptographically correct
  - Case 2-a: Not private for S when R^{π}

→ $\exists$ D_1 who distinguishes $\mathrm{view}_{R\pi}$

→ $U_S((S^{\pi}, G_S), (R^{\pi}, G_R)) < -\alpha_S \cdot \varepsilon_2$
$U_S((S^{stop}, G_S), (R^{\pi}, G_R)) = 0$ (when G_R uses D_1)

→ U_S is higher when $S^{\pi} \to S^{stop}$

- S^{stop}: Abort after receiving a message
- $\Pr[\ \mathrm{guess}_R = b\ ]$ is higher when $S^{\pi} \to S^{stop}$

Proof ("Game → Crypto")

- Case 2: Cryptographically correct
  - Case 2-b: Private for S when R^π, not for R

  ➔ $\exists$ S^* and D_2 who distinguishes $view_{S^*}$

  ➔ $\exists$ D_2 who distinguishes $view_{S^\pi}$ (since two-message OT)

  ➔ $U_R((S^\pi, G_S), (R^\pi, G_R)) < -\alpha_R \cdot \varepsilon_3$
  $U_R((S^\pi, G_S), (R^{def}, G_R)) = 0$ (when G_S uses D_2)
    - R^{def}: Abort before start
    - Pr[$guess_S = c$] is higher when $R^\pi \rightarrow R^{def}$

Proof (“Game $\rightarrow$ Crypto”)

- Case 2: Cryptographically correct
  - Case 2-c: Private for R, not for S when R*

$\Rightarrow$ $\exists$ R* and D_3 who distinguishes $view_{R^*}$

$\Rightarrow$ $U_R((S^\pi,G_S), (R^\pi,G_R)) < negl$
$U_R((S^\pi,G_S), (R^*,G_R)) = \gamma_R \cdot \varepsilon_4$ (when G_R uses D_3)

$\Rightarrow$ U_R is higher when $R^\pi \rightarrow R^*$

- Pr[$guess_R = b$] is higher when $R^\pi \rightarrow R^*$

Notes

- Main theorem holds even if $\gamma_S = 0$ or $\beta_R = 0$
  - $U_S((S, G_S), (R, G_R))$
    $= (-\alpha_S) \cdot (\Pr[\, \mathrm{guess}_R = b \,] - 1/2)$
    $+ \ \beta_S \cdot (\Pr[\, \mathrm{fin}=0 \vee (\mathrm{fin}=1 \wedge \mathrm{output}_R = x_c)] - 1)$
    $+ \ \gamma_S \cdot (\Pr[\, \mathrm{guess}_S = c \,] - 1/2)$
  - $U_R((S, G_S), (R, G_R))$
    $= (-\alpha_R) \cdot (\Pr[\, \mathrm{guess}_S = c \,] - 1/2)$
    $+ \ \beta_R \cdot (\Pr[\, \mathrm{fin}=0 \vee (\mathrm{fin}=1 \wedge \mathrm{output}_R = x_c)] - 1)$
    $+ \ \gamma_R \cdot (\Pr[\, \mathrm{guess}_R = b \,] - 1/2)$

Conclusions (1/2)

- Game-theoretically characterize “two-message” OT

  Protocol $\pi = (S^\pi, R^\pi)$ for two-message OT satisfies cryptographic correctness and privacy

  $\Leftrightarrow$ $\pi = (S^\pi, R^\pi)$ is a Nash equilibrium for Game^π with utility functions $U = (U_S, U_R)$

- Advantages compared to [ACH ‘11]

  1. Game between two rational players
  2. Characterize correctness and privacy by a single game
  3. Malicious adversaries

Conclusions (2/2)

- The first step toward understanding how OT protocols work for rational players
- Future work
  - Characterize OT with the ideal/real simulation-based security
  - Characterize other protocols
  - Explore good examples of rational cryptography