Privacy and Communication Complexity

The Hardness of Being Private [ACC+12]

Matrix M_f has entries $M_f[x, y] = f(x, y)$.
A submatrix is **monochromatic** if f is constant on inputs in the submatrix.
A deterministic protocol computing f repeatedly partitions M_f into **rectangles** (submatrices) until every rectangle is monochromatic.

Matrix M_f has entries $M_f[x, y] = f(x, y)$.
A submatrix is **monochromatic** if f is constant on inputs in the submatrix.
A deterministic protocol computing f repeatedly partitions M_f into **rectangles** (submatrices) until every rectangle is monochromatic.

Vickrey auction

The 2-player Vickrey auction is defined as $f : X \times Y \to Z$ where
$X = Y = [2^n]$, $Z = [2^{n+1}]$ and $f(x, y) = \begin{cases} (x, B), & \text{if } x \leq y \\ (y, A) & \text{if } y < x \end{cases}$

Matrix M_f has entries $M_f[x, y] = f(x, y)$.
A submatrix is **monochromatic** if f is constant on inputs in the submatrix.
A deterministic protocol computing f repeatedly partitions M_f into **rectangles** (submatrices) until every rectangle is monochromatic.

Vickrey auction

The 2-player Vickrey auction is defined as $f : X \times Y \to Z$ where $X = Y = [2^n]$, $Z = [2^{n+1}]$ and $f(x,y) = \begin{cases} (x, B), & \text{if } x \leq y \\ (y, A) & \text{if } y < x \end{cases}$

	1	2	3	4	$\dots$	$2^n - 1$	2^n
1	$(1, B)$	$(1, B)$	$(1, B)$	$(1, B)$	$\dots$	$(1, B)$	$(1, B)$
2	$(1, A)$	$(2, B)$	$(2, B)$	$(2, B)$	$\dots$	$(2, B)$	$(2, B)$
3	$(1, A)$	$(2, A)$	$(3, B)$	$(3, B)$	$\dots$	$(3, B)$	$(3, B)$
4	$(1, A)$	$(2, A)$	$(3, A)$	$(4, B)$	$\dots$	$(4, B)$	$(4, B)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
$2^n - 1$	$(1, A)$	$(2, A)$	$(3, A)$	$(4, A)$	$\dots$	$(2^n - 1, B)$	$(2^n - 1, B)$
2^n	$(1, A)$	$(2, A)$	$(3, A)$	$(4, A)$	$\dots$	$(2^n - 1, A)$	$(2^n, B)$

Matrix M_f has entries $M_f[x, y] = f(x, y)$.
A submatrix is **monochromatic** if f is constant on inputs in the submatrix.
A deterministic protocol computing f repeatedly partitions M_f into **rectangles** (submatrices) until every rectangle is monochromatic.

Vickrey auction

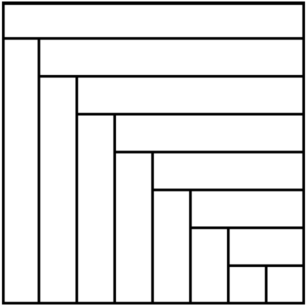
The 2-player Vickrey auction is defined as $f : X \times Y \to Z$ where $X = Y = [2^n]$, $Z = [2^{n+1}]$ and $f(x, y) = \begin{cases} (x, B), & \text{if } x \leq y \\ (y, A) & \text{if } y < x \end{cases}$

	1	2	3	4	...	$2^n - 1$	2^n
1	$(1, B)$	$(1, B)$	$(1, B)$	$(1, B)$	...	$(1, B)$	$(1, B)$
2	$(1, A)$	$(2, B)$	$(2, B)$	$(2, B)$	...	$(2, B)$	$(2, B)$
3	$(1, A)$	$(2, A)$	$(3, B)$	$(3, B)$	...	$(3, B)$	$(3, B)$
4	$(1, A)$	$(2, A)$	$(3, A)$	$(4, B)$	...	$(4, B)$	$(4, B)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	...	$\vdots$	$\vdots$
$2^n - 1$	$(1, A)$	$(2, A)$	$(3, A)$	$(4, A)$	...	$(2^n - 1, B)$	$(2^n - 1, B)$
2^n	$(1, A)$	$(2, A)$	$(3, A)$	$(4, A)$	...	$(2^n - 1, A)$	$(2^n, B)$

Matrix M_f has entries $M_f[x, y] = f(x, y)$.
A submatrix is **monochromatic** if f is constant on inputs in the submatrix.
A deterministic protocol computing f repeatedly partitions M_f into **rectangles** (submatrices) until every rectangle is monochromatic.

Vickrey auction

The 2-player Vickrey auction is defined as $f : X \times Y \to Z$ where $X = Y = [2^n]$, $Z = [2^{n+1}]$ and $f(x, y) = \begin{cases} (x, B), & \text{if } x \leq y \\ (y, A) & \text{if } y < x \end{cases}$



Matrix M_f has entries $M_f[x, y] = f(x, y)$.
A submatrix is **monochromatic** if f is constant on inputs in the submatrix.
A deterministic protocol computing f repeatedly partitions M_f into **rectangles** (submatrices) until every rectangle is monochromatic.

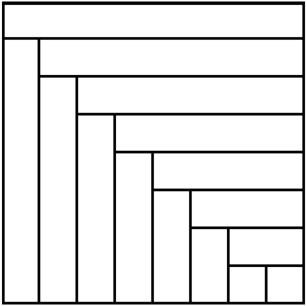
Vickrey auction

The 2-player Vickrey auction is defined as $f : X \times Y \to Z$ where
$X = Y = [2^n]$, $Z = [2^{n+1}]$ and $f(x, y) = \begin{cases} (x, B), & \text{if } x \leq y \\ (y, A) & \text{if } y < x \end{cases}$

Regions (preimages)

region $R_{x,y} = \{(x', y') \in X \times Y \mid f(x, y) = f(x', y')\}$

defined by **function** $\longrightarrow$



Matrix M_f has entries $M_f[x, y] = f(x, y)$.
A submatrix is **monochromatic** if f is constant on inputs in the submatrix.
A deterministic protocol computing f repeatedly partitions M_f into **rectangles** (submatrices) until every rectangle is monochromatic.

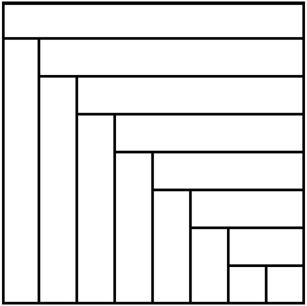
Vickrey auction

The 2-player Vickrey auction is defined as $f : X \times Y \to Z$ where
$X = Y = [2^n]$, $Z = [2^{n+1}]$ and $f(x,y) = \begin{cases} (x, B), & \text{if } x \leq y \\ (y, A) & \text{if } y < x \end{cases}$

Regions (preimages)

region $R_{x,y} = \{(x', y') \in X \times Y \mid f(x, y) = f(x', y')\}$

defined by **function** $\longrightarrow$



Rectangles

rectangle $P_{x,y} = \{(x', y') \in X \times Y \mid f(x, y) = f(x', y')$ and $\pi(x, y) = \pi(x', y')\}$

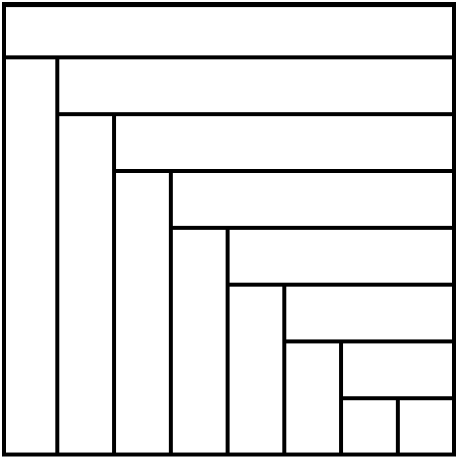
defined by **protocol**

Privacy against eavesdroppers

Can an eavesdropper learn about x and y, aside from $z = f(x, y)$?

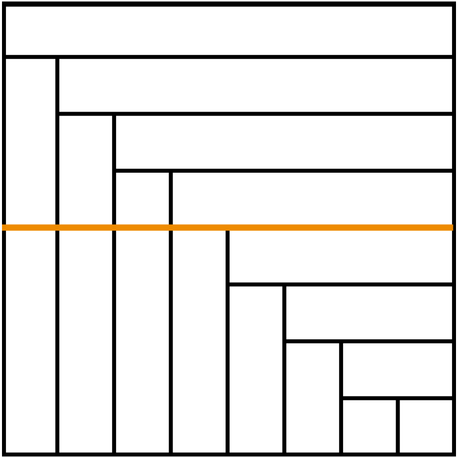
Privacy against eavesdroppers

Can an eavesdropper learn about x and y, aside from $z = f(x, y)$?



Privacy against eavesdroppers

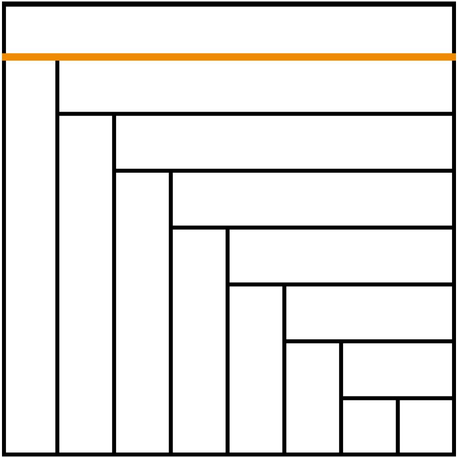
Can an eavesdropper learn about x and y, aside from $z = f(x, y)$?



Alice's first move? NO, loses privacy for Alice!

Privacy against eavesdroppers

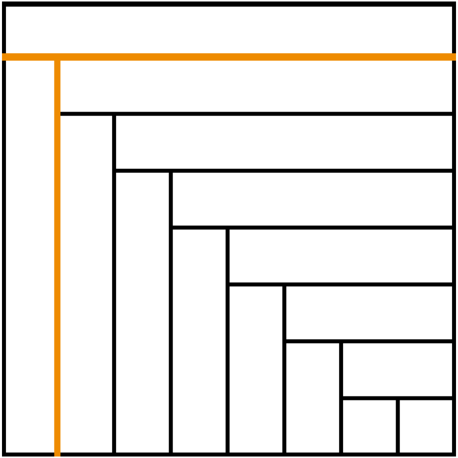
Can an eavesdropper learn about x and y, aside from $z = f(x, y)$?



Alice's only choice for a privacy-preserving first message.

Privacy against eavesdroppers

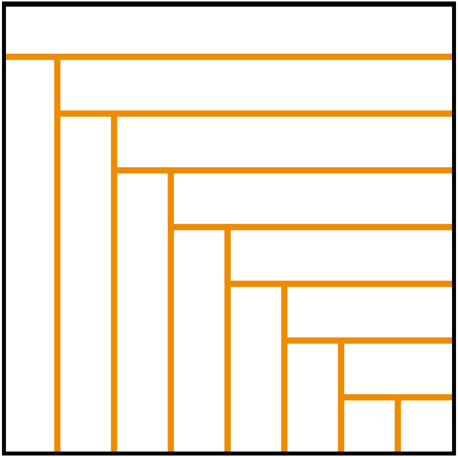
Can an eavesdropper learn about x and y, aside from $z = f(x, y)$?



Bob's only privacy-preserving first message.

Privacy against eavesdroppers

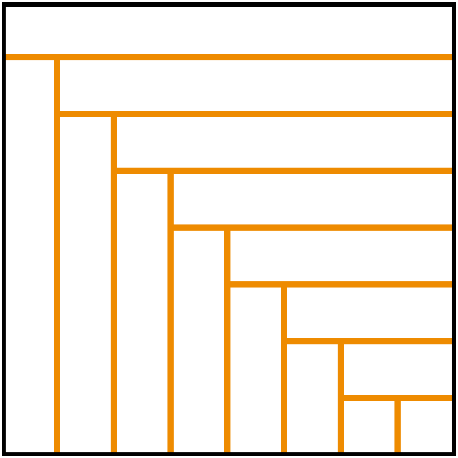
Can an eavesdropper learn about x and y, aside from $z = f(x, y)$?



. . . and so on . . .

Privacy against eavesdroppers

Can an eavesdropper learn about x and y, aside from $z = f(x, y)$?



Ascending English bidding is the *only* perfectly private protocol. Lengthy!

Perfect privacy

A protocol for 2-player function $f : X \times Y \to Z$ is **perfectly private** if every two inputs in the same **region** are partitioned into the same **rectangle**.

Perfect privacy

A protocol for 2-player function $f : X \times Y \to Z$ is **perfectly private** if every two inputs in the same **region** are partitioned into the same **rectangle**.

Characterizing perfect privacy [Kus89]

The perfectly private functions of 2 inputs are fully characterized combinatorially. A private deterministic protocol for such functions is given by "decomposing" M_f.

Perfect privacy

A protocol for 2-player function $f : X \times Y \to Z$ is **perfectly private** if every two inputs in the same **region** are partitioned into the same **rectangle**.

Characterizing perfect privacy [Kus89]

The perfectly private functions of 2 inputs are fully characterized combinatorially. A private deterministic protocol for such functions is given by "decomposing" M_f.

But perfect privacy is unattainable for many functions!
This leads us to a relaxation...

Approximate privacy

Let's relax our requirement from one **big** rectangle to simply grouping inputs in the same preimage into large*ish* rectangles.

Approximate privacy

Privacy approximation ratio [FJS10]

A protocol for f has **worst-case privacy approximation ratio**:

$$\text{worst-case PAR} = \max_{(x,y)} \frac{|R_{x,y}|}{|P_{x,y}|}$$

$$\text{average-case PAR} = \mathbb{E}_{(x,y)} \frac{|R_{x,y}|_{\mathcal{U}}}{|P_{x,y}|_{\mathcal{U}}} \text{ over distribution } \mathcal{U}$$

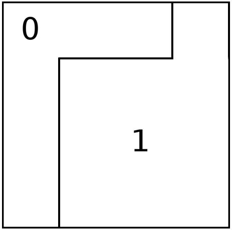
Approximate privacy

Privacy approximation ratio [FJS10]

A protocol for f has **worst-case privacy approximation ratio**:

$$\text{worst-case PAR} = \max_{(x,y)} \frac{|R_{x,y}|}{|P_{x,y}|}$$

$$\text{average-case PAR} = \mathbb{E}_{(x,y)} \frac{|R_{x,y}|_{\mathcal{U}}}{|P_{x,y}|_{\mathcal{U}}} \text{ over distribution } \mathcal{U}$$



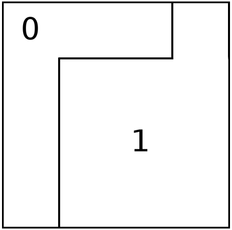
Approximate privacy

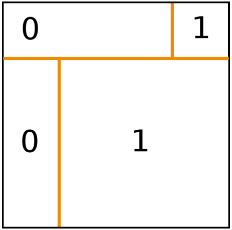
Privacy approximation ratio [FJS10]

A protocol for f has **worst-case privacy approximation ratio**:

$$\text{worst-case PAR} = \max_{(x,y)} \frac{|R_{x,y}|}{|P_{x,y}|}$$

$$\text{average-case PAR} = \mathbb{E}_{(x,y)} \frac{|R_{x,y}|_{\mathcal{U}}}{|P_{x,y}|_{\mathcal{U}}} \text{ over distribution } \mathcal{U}$$





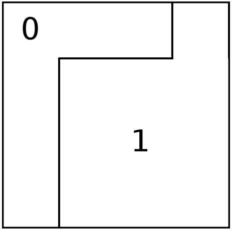
Approximate privacy

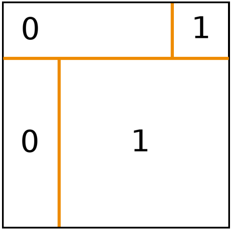
Privacy approximation ratio [FJS10]

A protocol for f has **worst-case privacy approximation ratio**:

$$\text{worst-case PAR} = \max_{(x,y)} \frac{|R_{x,y}|}{|P_{x,y}|}$$

$$\text{average-case PAR} = \mathbb{E}_{(x,y)} \frac{|R_{x,y}|_{\mathcal{U}}}{|P_{x,y}|_{\mathcal{U}}} \text{ over distribution } \mathcal{U}$$

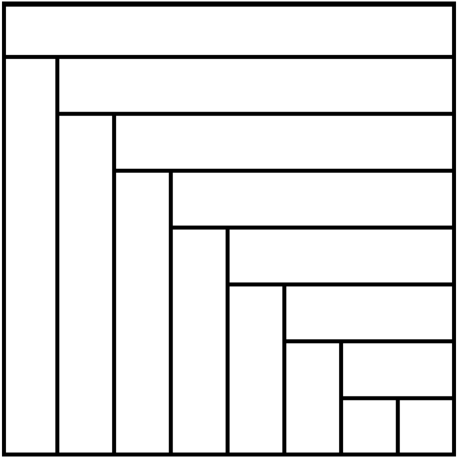




worst-case $\mathrm{PAR} = 10$
average-case $\mathrm{PAR} = 2$

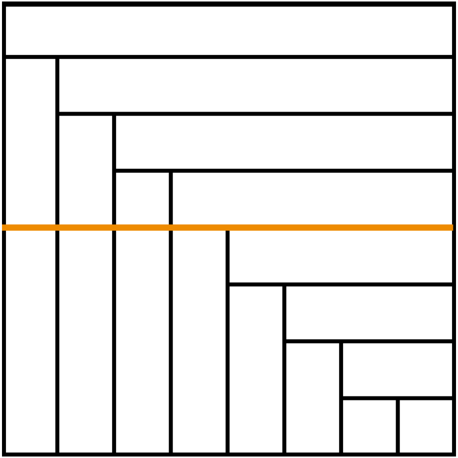
Two-player Vickrey auction

How short can we make a protocol for Vickrey auction?



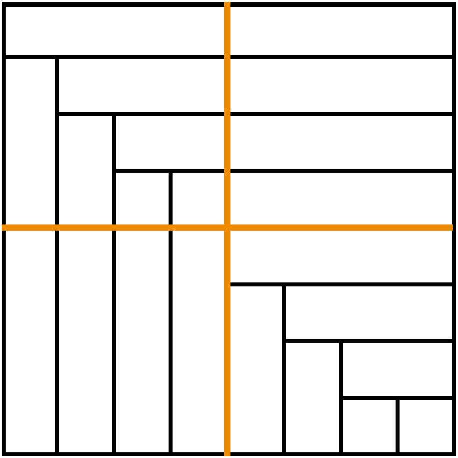
Two-player Vickrey auction

How short can we make a protocol for Vickrey auction?



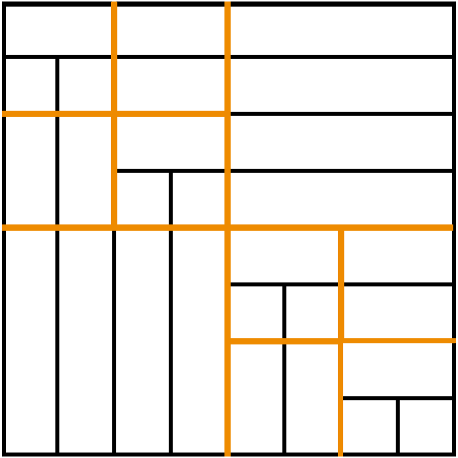
Two-player Vickrey auction

How short can we make a protocol for Vickrey auction?



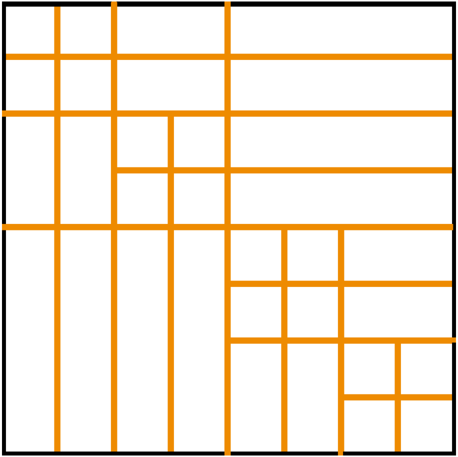
Two-player Vickrey auction

How short can we make a protocol for Vickrey auction?



Two-player Vickrey auction

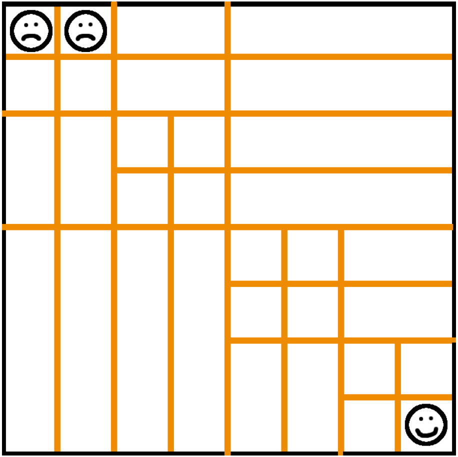
How short can we make a protocol for Vickrey auction?



Bisection protocol.

Two-player Vickrey auction

How short can we make a protocol for Vickrey auction?



Bisection protocol.

Upper bounds for Vickrey auctions [FJS10]

	English bidding	bisection protocol
communication cost	2^n	$O(n)$
worst-case PAR	1	2^n
average-case PAR	1	$O(1)$

Upper bounds for Vickrey auctions [FJS10]

	English bidding	bisection protocol
communication cost	2^n	$O(n)$
worst-case PAR	1	2^n
average-case PAR	1	$O(1)$

Worst-case lower bound (our work)

For all n, for all p, $2 \leq p \leq n/4$, any deterministic protocol for the n-bit two-player Vickrey auction obtaining PAR less than 2^{p-2} has length at least $2^{n/4p}$.

Upper bounds for Vickrey auctions [FJS10]

	English bidding	bisection protocol
communication cost	2^n	$O(n)$
worst-case PAR	1	2^n
average-case PAR	1	$O(1)$

Worst-case lower bound (our work)

For all n, for all p, $2 \leq p \leq n/4$, any deterministic protocol for the n-bit two-player Vickrey auction obtaining PAR less than 2^{p-2} has length at least $2^{n/4p}$.

Average-case lower bound (our work)

For all $n, r \geq 1$, any deterministic protocol of length at most r for the n-bit two-player Vickrey auction has average-case PAR greater than $\Omega(\frac{n}{\log(r/n)})$.

Upper bounds for Vickrey auctions [FJS10]

	English bidding	bisection protocol
communication cost	2^n	$O(n)$
worst-case PAR	1	2^n
average-case PAR	1	$O(1)$

Worst-case lower bound (our work)

For all n, for all p, $2 \leq p \leq n/4$, any deterministic protocol for the n-bit two-player Vickrey auction obtaining PAR less than 2^{p-2} has length at least $2^{n/4p}$.

Average-case lower bound (our work)

For all $n, r \geq 1$, any deterministic protocol of length at most r for the n-bit two-player Vickrey auction has average-case PAR greater than $\Omega(\frac{n}{\log(r/n)})$.

These are *trade-offs*: good privacy for short communication.

Worst-case lower bound

For all n, for all p, $2 \leq p \leq n/4$, any deterministic protocol for the n-bit two-player Vickrey auction problem obtaining PAR less than 2^{p-2} has length at least $2^{n/4p}$.

The parameter p lets us fix either the PAR or the communication cost which we want a protocol to achieve, and determines the other.

Worst-case lower bound

For all n, for all p, $2 \leq p \leq n/4$, any deterministic protocol for the n-bit two-player Vickrey auction problem obtaining PAR less than 2^{p-2} has length at least $2^{n/4p}$.

The parameter p lets us fix either the PAR or the communication cost which we want a protocol to achieve, and determines the other.

The proof proceeds as follows.

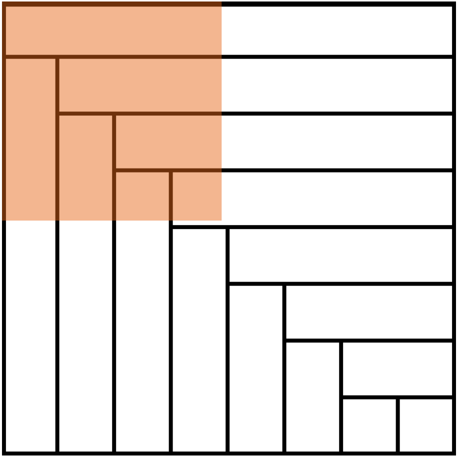
Fix any protocol π for Vickrey auction.
This proof will find some input pair (x, y) which either

- loses enough privacy (has $\text{PAR}_{x,y}(\pi) \geq 2^{p-2}$), or
- takes communication at least $2^{n/4p}$ in protocol π.

We'll track the "small" inputs (x, y) from the upper left-hand corner:

$$\{(x, y) \mid x, y \leq 2^{n-p}\}$$

These inputs stand to lose the most privacy.



The rest of the inputs will be called "large."

Let v be some vertex in the protocol tree for π.

- inputs which reach node v:
  $T(v) = T_A(v) \times T_B(v) = \{(x, y) \mid \text{ input } (x, y) \text{ reaches } v \text{ during } \pi\}$
- the square of small inputs $S(v) \times S(v)$ which reach v:
  $S(v) = T_A(v) \cap T_B(v) \cap [2^{n-p}]$
- the "large" inputs for each player:
  $A^L(v) = T_A(v) \cap \{2^{n-p}, \ldots, 2^n - 1\}$
  $B^L(v) = T_B(v) \cap \{2^{n-p}, \ldots, 2^n - 1\}$

We want a square of small inputs which reach v because every square of inputs *resembles* the entire Vickrey auction (has no quick, private protocol).

At root node r:

- $T_A(r) = T_B(r) = [2^n]$
- $S(r) = [2^{n-p}]$
- $A^L(r) = B^L(r) = \{2^{n-p}, \ldots, 2^n - 1\}$

Inputs only lose privacy as the protocol continues.

For any node v in the protocol tree and any $(x, y) \in T(v)$,

$$\mathrm{PAR}_{x,y}(\pi) = \frac{|R_{x,y}|}{|P_{x,y}|} o \geq \frac{|R_{x,y}|}{|R_{x,y} \cap T(v)|} = \mathrm{PAR}^{v}_{x,y}(\pi)$$

In particular, consider some $(x, y) \in T(v)$ where $x > y$ (Alice wins).

$$\mathrm{PAR}_{x,y}(\pi) \geq \mathrm{PAR}^{v}_{x,y}(\pi) \geq \frac{2^n - 2^{n-p}}{|A^L(v)| + 2^{n-p}} \tag{1}$$

Set $\alpha = 1 - 2^{-n/4p}$.

Our strategy for finding (x, y)

1. Start at the root with $S(r)$, $A^L(r)$, and $B^L(r)$ as defined.
2. At node v, say it's Alice's turn to speak (the case is symmetric for Bob). Alice sends bit b which partitions $T_A(v)$ into two pieces, inducing partitions of $S(v)$ and $A^L(v)$.
   - **progress**: if
     $$(1-\alpha)|S(v)| \leq |S_0(v)| \leq \alpha|S(v)|$$
     then follow the branch such that $|A_i^L(v)| \leq \frac{1}{2}|A_i^L(v)|$.
   - **useless**: if for some i,
     $$|S_i(v)| \geq \alpha|S(v)|$$
     then follow that branch of the protocol tree.
3. Repeat step 2 until one player has made p progress steps, or v is a leaf.

Progress steps make the protocol short-but-not-private (bisection-like); useless steps make the protocol private-but-not-short (English-like).

Case 1: Alice makes p progress steps (WLOG – symmetric for Bob)

We know that:

- $|R_{x,y}| \geq 2^n - 2^{n-p}$ for every $(x, y) \in S(v) \times S(v)$
- $|A^L(r)| = 2^n - 2^{n-p}$

For every progress step Alice made from vertex u to w in the protocol, we know that $|A^L(w)| \leq \frac{1}{2}|A^L(u)|$. Thus $|A^L(v)| \leq \frac{1}{2^p}|A^L(r)|$.
Thus for any $(x, y) \in S(v) \times S(v)$, by equation (1)

$$\mathrm{PAR}^v_{x,y}(\pi) \geq \mathrm{PAR}_{x,y}(\pi) \geq \mathrm{PAR}^v_{x,y}(\pi) \geq \frac{2^n - 2^{n-p}}{|A^L(v)| + 2^{n-p}} \geq 2^{p-2}$$

Case 2: We reach a leaf v, so $|S(v)| = 1$

Let q be the total number of useless steps made. Fewer than $2p$ progress steps were made. $|S(r)| = 2^{n-p}$.

$$1 = |S(v)| \geq 2^{n-p}(1-\alpha)^{2p}\alpha^q$$

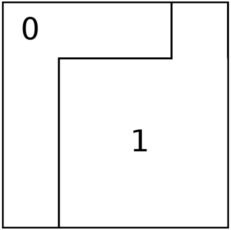
Thus $q \geq 2^{n/4p}$.

Privacy against players

Can Bob learn anything about Alice's private input x, beyond the fact that $z = f(x, y)$? Can Alice learn anything about Bob's private input y?

Privacy against players

Can Bob learn anything about Alice's private input x, beyond the fact that $z = f(x, y)$? Can Alice learn anything about Bob's private input y?



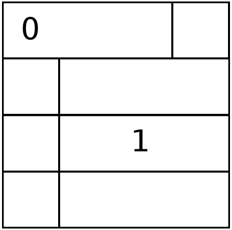
Privacy against players

Can Bob learn anything about Alice's private input x, beyond the fact that $z = f(x, y)$? Can Alice learn anything about Bob's private input y?

Subjective regions

region $R^A_{x,y} = \{(x, y') \in X \times Y \mid f(x,y) = f(x,y')\}$

defined by **function** Alice sees



Privacy against players

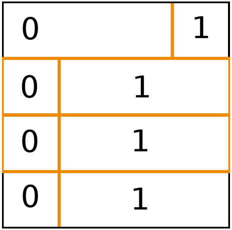
Can Bob learn anything about Alice's private input x, beyond the fact that $z = f(x, y)$? Can Alice learn anything about Bob's private input y?

Subjective regions

region $R^A_{x,y} = \{(x, y') \in X \times Y \mid f(x, y) = f(x, y')\}$

defined by **function**

Alice sees



Subjective rectangles

rectangle $P^B_{x,y} = \{(x, y') \in X \times Y \mid f(x, y) = f(x, y'), \pi(x, y) = \pi(x, y')\}$

defined by **protocol**

Alice sees

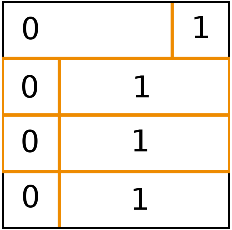
Privacy against players

Can Bob learn anything about Alice's private input x, beyond the fact that $z = f(x, y)$? Can Alice learn anything about Bob's private input y?

Subjective regions

region $R^A_{x,y} = \{(x, y') \in X \times Y \mid f(x, y) = f(x, y')\}$

defined by **function** Alice sees



Subjective rectangles

rectangle $P^B_{x,y} = \{(x, y') \in X \times Y \mid f(x, y) = f(x, y'), \pi(x, y) = \pi(x, y')\}$

defined by **protocol** Alice sees

Subjective privacy approximation ratio (Feigenbaum Jaggard Schapira '10)

$$\text{average-case } \mathrm{PAR}^{\text{sub}} = \max_{v=A,B} \mathbb{E}_{(x,y)} \frac{|R^v_{x,y}|}{|P^v_{x,y}|}$$

Information cost (Braverman et al.)

$$IC_\mu(\pi) = I(\mathbf{X} : \pi(\mathbf{X}, \mathbf{Y})|\mathbf{Y}) + I(\mathbf{Y} : \pi(\mathbf{X}, \mathbf{Y})|\mathbf{X})\}$$

Informational privacy (Klauck '02)

$$\mathrm{PRIV}_\mu(\pi) = \max\{I(\mathbf{X} : \pi(\mathbf{X}, \mathbf{Y})|\mathbf{Y}, f(\mathbf{X}, \mathbf{Y})), I(\mathbf{Y} : \pi(\mathbf{X}, \mathbf{Y})|\mathbf{X}, f(\mathbf{X}, \mathbf{Y}))\}$$

Information cost (Braverman et al.)

$$IC_\mu(\pi) = I(\mathbf{X} : \pi(\mathbf{X},\mathbf{Y})|\mathbf{Y}) + I(\mathbf{Y} : \pi(\mathbf{X},\mathbf{Y})|\mathbf{X})\}$$

Informational privacy (Klauck '02)

$$\mathrm{PRIV}_\mu(\pi) = \max\{I(\mathbf{X} : \pi(\mathbf{X},\mathbf{Y})|\mathbf{Y}, f(\mathbf{X},\mathbf{Y})), I(\mathbf{Y} : \pi(\mathbf{X},\mathbf{Y})|\mathbf{X}, f(\mathbf{X},\mathbf{Y}))\}$$

Theorem (us '12): $\mathrm{PRIV}_\mu - \log|Z| \le IC \le 2(\mathrm{PRIV}_\mu + \log|Z|)$

Information cost (Braverman et al.)

$$IC_\mu(\pi) = I(\mathbf{X} : \pi(\mathbf{X}, \mathbf{Y})|\mathbf{Y}) + I(\mathbf{Y} : \pi(\mathbf{X}, \mathbf{Y})|\mathbf{X})\}$$

Informational privacy (Klauck '02)

$$\mathrm{PRIV}_\mu(\pi) = \max\{I(\mathbf{X} : \pi(\mathbf{X}, \mathbf{Y})|\mathbf{Y}, f(\mathbf{X}, \mathbf{Y})), I(\mathbf{Y} : \pi(\mathbf{X}, \mathbf{Y})|\mathbf{X}, f(\mathbf{X}, \mathbf{Y}))\}$$

Theorem (us '12): $\mathrm{PRIV}_\mu - \log|Z| \leq IC \leq 2(\mathrm{PRIV}_\mu + \log|Z|)$
Theorem (us '12): $\mathrm{PRIV}_\mu(P) \leq \log(\mathrm{avg}_\mu \mathrm{PAR}^{sub}(P))$

Information cost (Braverman et al.)

$$IC_\mu(\pi) = I(\mathbf{X} : \pi(\mathbf{X},\mathbf{Y})|\mathbf{Y}) + I(\mathbf{Y} : \pi(\mathbf{X},\mathbf{Y})|\mathbf{X})\}$$

Informational privacy (Klauck '02)

$$\mathrm{PRIV}_\mu(\pi) = \max\{I(\mathbf{X} : \pi(\mathbf{X},\mathbf{Y})|\mathbf{Y}, f(\mathbf{X},\mathbf{Y})), I(\mathbf{Y} : \pi(\mathbf{X},\mathbf{Y})|\mathbf{X}, f(\mathbf{X},\mathbf{Y}))\}$$

Theorem (us '12): $\mathrm{PRIV}_\mu - \log|Z| \leq IC \leq 2(\mathrm{PRIV}_\mu + \log|Z|)$
Theorem (us '12): $\mathrm{PRIV}_\mu(P) \leq \log(\mathrm{avg}_\mu \mathrm{PAR}^{sub}(P))$
Theorem (Braverman '11): $\mathrm{IC}_{\mathcal{U}}(\mathrm{DISJ}) = \Omega(n)$.

Information cost (Braverman et al.)

$$IC_\mu(\pi) = I(\mathbf{X} : \pi(\mathbf{X}, \mathbf{Y})|\mathbf{Y}) + I(\mathbf{Y} : \pi(\mathbf{X}, \mathbf{Y})|\mathbf{X})\}$$

Informational privacy (Klauck '02)

$$\mathrm{PRIV}_\mu(\pi) = \max\{I(\mathbf{X} : \pi(\mathbf{X}, \mathbf{Y})|\mathbf{Y}, f(\mathbf{X}, \mathbf{Y})), I(\mathbf{Y} : \pi(\mathbf{X}, \mathbf{Y})|\mathbf{X}, f(\mathbf{X}, \mathbf{Y}))\}$$

Theorem (us '12): $\mathrm{PRIV}_\mu - \log|Z| \leq IC \leq 2(\mathrm{PRIV}_\mu + \log|Z|)$
Theorem (us '12): $\mathrm{PRIV}_\mu(P) \leq \log(\mathrm{avg}_\mu \mathrm{PAR}^{sub}(P))$
Theorem (Braverman '11): $\mathrm{IC}_{\mathcal{U}}(\mathrm{DISJ}) = \Omega(n)$.

Theorem 3

Any protocol P computing the n-bit Set Intersection $\mathrm{INTERSEC}_n$ has exponential average-case subjective PAR:

$$\mathrm{avg}_{\mathcal{U}} \mathrm{PAR}^{sub}(P) = 2^{\Omega(n)}$$

Observation

For a region R, define $cut_\pi(R) = |\{P_{x,y} \mid (x,y) \in R\}|$.

$$\begin{aligned}
\operatorname{avg}\mathrm{PAR}_\mu(\pi) = \mathbb{E}_\mu \frac{|R_{x,y}|}{|P_{x,y}|} &= \sum_{(x,y)\in X\times Y} \mu(x,y)\frac{|R_{x,y}|}{|P_{x,y}|} \\
&= \sum_{R \text{ region}} \sum_{(x,y)\in R} \mu(x,y)\frac{|R|}{|P_{x,y}|} \\
&= \sum_{R \text{ region}} |R|\Big(\sum_{(x,y)\in R} \frac{\mu(x,y)}{|P_{x,y}|} \\
&= \sum_{R \text{ region}} |R| \cdot cut_\pi(R)
\end{aligned}$$

Theorem (us '12): $\mathrm{PRIV}_\mu(P) \leq \log(\mathrm{avg}_\mu \mathrm{PAR}^{sub}(P))$

Proof:

$$\begin{aligned}
&\mathbf{I}(\mathbf{X};\pi(\mathbf{X},\mathbf{Y})|\mathbf{Y}, f(\mathbf{X},\mathbf{Y})) \\
&= \mathbf{H}(\mathbf{X};\pi(\mathbf{X},\mathbf{Y})|\mathbf{Y}, f(\mathbf{X},\mathbf{Y})) - \mathbf{H}(\mathbf{X}|\mathbf{Y}, f(\mathbf{X},\mathbf{Y}), \pi(\mathbf{X},\mathbf{Y})) \\
&\leq \mathbf{H}(\mathbf{X};\pi(\mathbf{X},\mathbf{Y})|\mathbf{Y}, f(\mathbf{X},\mathbf{Y})) \\
&= \sum_{y,z} Pr[\mathbf{Y}=y, \mathbf{Z}=z] \cdot \mathbf{H}(\pi(\mathbf{X},\mathbf{Y})|\mathbf{Y}=y, f(\mathbf{X},\mathbf{Y})=z) \\
&= \sum_{y,z} |R_z \cap \mathbb{X} \times \{y\}|_\mu \cdot \mathbf{H}(\pi(\mathbf{X},\mathbf{Y})|\mathbf{Y}=y, f(\mathbf{X},\mathbf{Y})=z) \\
&= \sum_{y,z} |R_z \cap \mathbb{X} \times \{y\}|_\mu \cdot \log(cut_\pi(R_z \cap X \times \{y\})) \\
&\leq \log \sum_{y,z} |R_z \cap \mathbb{X} \times \{y\}|_\mu \cdot (cut_\pi(R_z \cap X \times \{y\})) \\
&\leq \log(\mathrm{avg}\,\mathrm{PAR}^{\mathsf{sub}}(\pi))
\end{aligned}$$

Next time: differential privacy. Yet another definition of privacy!

References

Anil Ada, Arkadev Chattopadhyay, Stephen A Cook, Lila Fontes, Michal Koucký, and Toniann Pitassi.
The Hardness of Being Private.
In *Conference on Computational Complexity*, 2012.

Joan Feigenbaum, Aaron D Jaggard, and Michael Schapira.
Approximate Privacy: Foundations and Quantification.
ACM Conference on Electronic Commerce, pages 167–178, 2010.

Eyal Kushilevitz.
Privacy and communication complexity.
IEEE Symposium on Foundations of Computer Science, pages 416–421, 1989.