TCC 2022

On the Optimal Communication Complexity of Error-Correcting Multi-Server PIR

Nov 10, 2022

Reo Eriguchi (The University of Tokyo/AIST)

Kaoru Kurosawa (Chuo University/AIST)

Koji Nuida (Kyushu University/AIST)

Private Information Retrieval (PIR) [CGKS98]

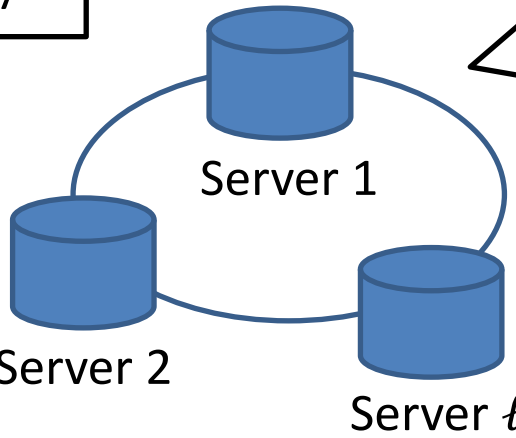
Private index τ

Stock price a_τ of Company τ

Client

Query

Answer



Database $\boldsymbol{a} = (a_1, \ldots, a_n)$

Stock-market database

Name	Price
Company 1	$ 2,720
⋮	
Company τ	$ 190
⋮	

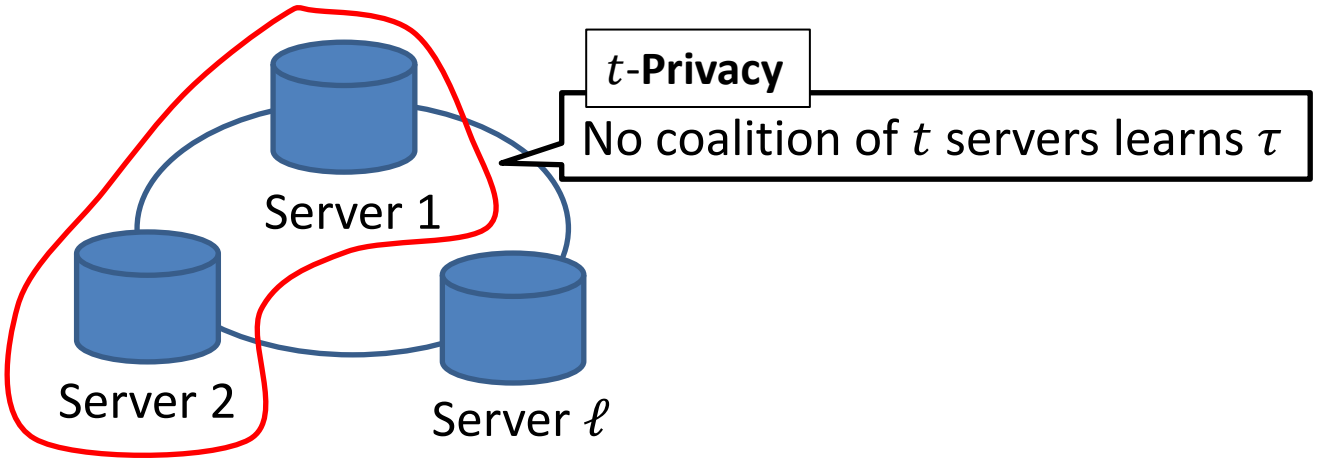
Trivial solution: Download the whole database

High communication cost $O(n)$ → Secure but **inefficient**

Multi-server PIR

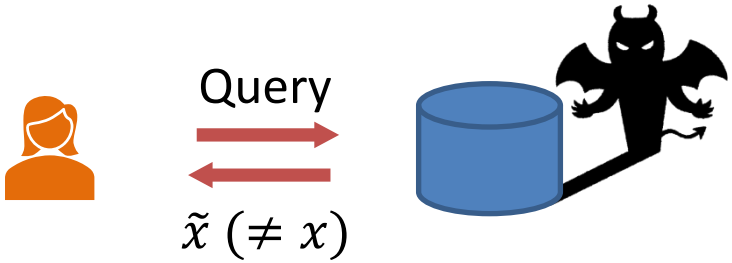
- Can achieve communication cost $o(n)$.

Scheme	# of servers ℓ	t-Privacy	Communication
[WY05]	$\ell \geq 2$	$t \leq \ell - 1$	$n^{O(t/\ell)}$
[IS10],[Efr12], [CFL+13],[DG16]	$\ell \geq 2$	$t = 1$	$n^{o(1)}$

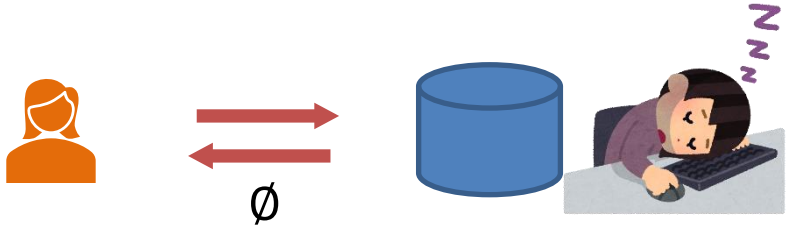


Dealing with Errors

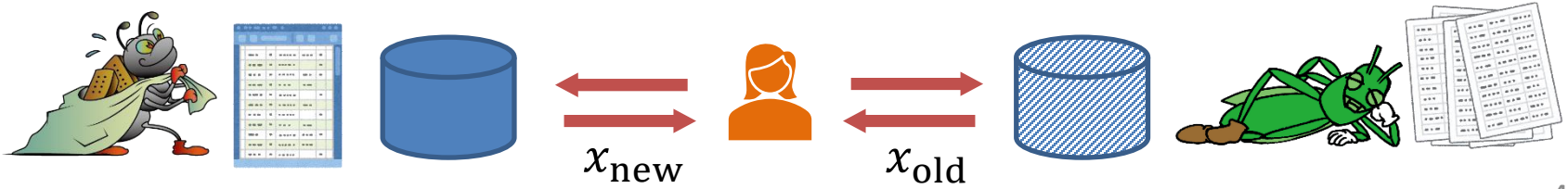
- Servers may return **incorrect** answers if
  - They are **malicious**



  - Return **nothing**



  - Have **inconsistent** databases



Error-Correcting PIR [BS07]

- Client obtains a_τ **correctly** even if at most b servers return *incorrect* answers.

Error-Correcting PIR [BS07]

- Client obtains a_τ **correctly** even if at most b servers return *incorrect* answers.

What is the optimal communication complexity $\mathrm{EC\text{-}PIR}_{\ell,b,t}(n)$ *of* t*-private* b*-error-correcting* ℓ*-server PIR?*

Error-Correcting PIR [BS07]

- Client obtains a_τ **correctly** even if at most b servers return *incorrect* answers.

What is the optimal communication complexity $\mathrm{EC\text{-}PIR}_{\ell,b,t}(n)$ *of* t*-private* b*-error-correcting* ℓ*-server PIR?*

[BS07]: b-Error correction is possible only if $\ell > 2b$.

Generic construction from any regular $(\ell - 2b)$-server PIR

Error-Correcting PIR [BS07]

- Client obtains a_τ **correctly** even if at most b servers return *incorrect* answers.

What is the optimal communication complexity $\text{EC-PIR}_{\ell,b,t}(n)$ *of* t*-private* b*-error-correcting* ℓ*-server PIR?*

[BS07]: b-Error correction is possible only if $\ell > 2b$.

Generic construction from any regular $(\ell - 2b)$-server PIR

$$\Rightarrow \quad \text{EC-PIR}_{\ell,b,t}(n) \leq c_\ell \cdot \text{PIR}_{\ell-2b,t}(n)$$

$\text{PIR}_{k,t}(n)$: Optimal comm. of t-private regular k-server PIR

c_ℓ : Constant independent of n (exponential in ℓ)

Error-Correcting PIR [BS07]

- Client obtains a_τ **correctly** even if at most b servers return *incorrect* answers.

What is the optimal communication complexity $\mathrm{EC\text{-}PIR}_{\ell,b,t}(n)$ *of* t*-private* b*-error-correcting* ℓ*-server PIR?*

[BS07]: b-Error correction is possible only if $\ell > 2b$.

Generic construction from any regular $(\ell - 2b)$-server PIR

$$\Rightarrow \quad \mathrm{EC\text{-}PIR}_{\ell,b,t}(n) \leq c_\ell \cdot \mathrm{PIR}_{\ell-2b,t}(n)$$

$\mathrm{PIR}_{k,t}(n)$: Optimal comm. of t-private regular k-server PIR
c_ℓ : Constant independent of n (exponential in ℓ)

- Related work

[Kur19, ZWW22]: *Non-generic* constructions of error-correcting PIR

⇒ Improves the *computational* complexity of [BS07]
but give no better upper bound on *communication* complexity.

Our Results

✓ **Lower bound** on $\mathrm{EC\text{-}PIR}_{\ell,b,t}(n)$ asymptotically matching the upper bound [BS07]

[BS07]

$$\mathrm{PIR}_{\ell-2b,t}(n) \leq \mathrm{EC\text{-}PIR}_{\ell,b,t}(n) \leq c_\ell \cdot \mathrm{PIR}_{\ell-2b,t}(n)$$

Upper and lower bounds on *statistical* error-correcting PIR

$$\mathrm{PIR}^*_{\ell-b,t}(n) \leq \mathrm{EC\text{-}PIR}^*_{\ell,b,t}(n) \leq c'_{\ell,\kappa} \cdot \mathrm{PIR}^*_{\ell-b,t}(n)$$

$\mathrm{EC\text{-}PIR}^*_{\ell,b,t}(n)$: Optimal comm. of t-private b-error-correcting ℓ-server PIR *with correctness error* $2^{-\kappa}$

$\mathrm{PIR}^*_{k,t}(n)$: Optimal comm. of t-private regular k-server PIR *with negligible correctness error*

$c'_{\ell,\kappa}$: Constant independent of n (exponential in ℓ and polynomial in κ)

Our Results

- ✓ **Lower bound** on $\mathrm{EC\text{-}PIR}_{\ell,b,t}(n)$ asymptotically matching the upper bound [BS07]

[BS07]

$$\mathrm{PIR}_{\ell-2b,t}(n) \leq \mathrm{EC\text{-}PIR}_{\ell,b,t}(n) \leq c_\ell \cdot \mathrm{PIR}_{\ell-2b,t}(n)$$

- ✓ **Upper and lower bounds** on *statistical* error-correcting PIR

$$\mathrm{PIR}^*_{\ell-b,t}(n) \leq \mathrm{EC\text{-}PIR}^*_{\ell,b,t}(n) \leq c'_{\ell,\kappa} \cdot \mathrm{PIR}^*_{\ell-b,t}(n)$$

$\mathrm{EC\text{-}PIR}^*_{\ell,b,t}(n)$: Optimal comm. of t-private b-error-correcting ℓ-server PIR *with correctness error* $2^{-\kappa}$
$\mathrm{PIR}^*_{k,t}(n)$: Optimal comm. of t-private regular k-server PIR *with negligible correctness error*
$c'_{\ell,\kappa}$: Constant independent of n (exponential in ℓ and polynomial in κ)

Our Results

✓ **Lower bound** on $\mathrm{EC\text{-}PIR}_{\ell,b,t}(n)$ asymptotically matching the upper bound [BS07]

[BS07]

$$\mathrm{PIR}_{\ell-2b,t}(n) \leq \mathrm{EC\text{-}PIR}_{\ell,b,t}(n) \leq c_\ell \cdot \mathrm{PIR}_{\ell-2b,t}(n)$$

✓ **Upper and lower bounds** on *statistical* error-correcting PIR

$$\mathrm{PIR}^*_{\ell-b,t}(n) \leq \mathrm{EC\text{-}PIR}^*_{\ell,b,t}(n) \leq c'_{\ell,\kappa} \cdot \mathrm{PIR}^*_{\ell-b,t}(n)$$

$\mathrm{EC\text{-}PIR}^*_{\ell,b,t}(n)$: Optimal comm. of t-private b-error-correcting ℓ-server PIR *with correctness error* $2^{-\kappa}$

$\mathrm{PIR}^*_{k,t}(n)$: Optimal comm. of t-private regular k-server PIR *with negligible correctness error*

$c'_{\ell,\kappa}$: Constant independent of n (exponential in ℓ and polynomial in κ)

The optimal communication complexity of error-correcting PIR is characterized by that of ***regular PIR.***

Corollaries

✓ **Separation** between perfect and statistical error-correcting PIR

$(\ell - 2b)$-private *perfect* error-correcting PIR has $\Omega(n)$ communication:

$$\text{EC-PIR}_{\ell,b,\ell-2b}(n) \geq \text{PIR}_{\ell-2b,\ell-2b}(n) = \Omega(n) \text{ [CGKS98]}$$

But $(\ell - 2b)$-private *statistical* error-correcting PIR achieves $o(n)$ communication:

$$\text{EC-PIR}^*_{\ell,b,\ell-2b}(n) \leq c'_{\ell,\kappa} \cdot \text{PIR}^*_{\ell-b,\ell-2b}(n) = o(n) \text{ [WY05]}$$

Corollaries

✓ **Separation** between perfect and statistical error-correcting PIR

$(\ell - 2b)$-private *perfect* error-correcting PIR has $\Omega(n)$ communication:

$$\text{EC-PIR}_{\ell,b,\ell-2b}(n) \geq \text{PIR}_{\ell-2b,\ell-2b}(n) = \Omega(n) \text{ [CGKS98]}$$

But $(\ell - 2b)$-private *statistical* error-correcting PIR achieves $o(n)$ communication:

$$\text{EC-PIR}^*_{\ell,b,\ell-2b}(n) \leq c'_{\ell,\kappa} \cdot \text{PIR}^*_{\ell-b,\ell-2b}(n) = o(n) \text{ [WY05]}$$

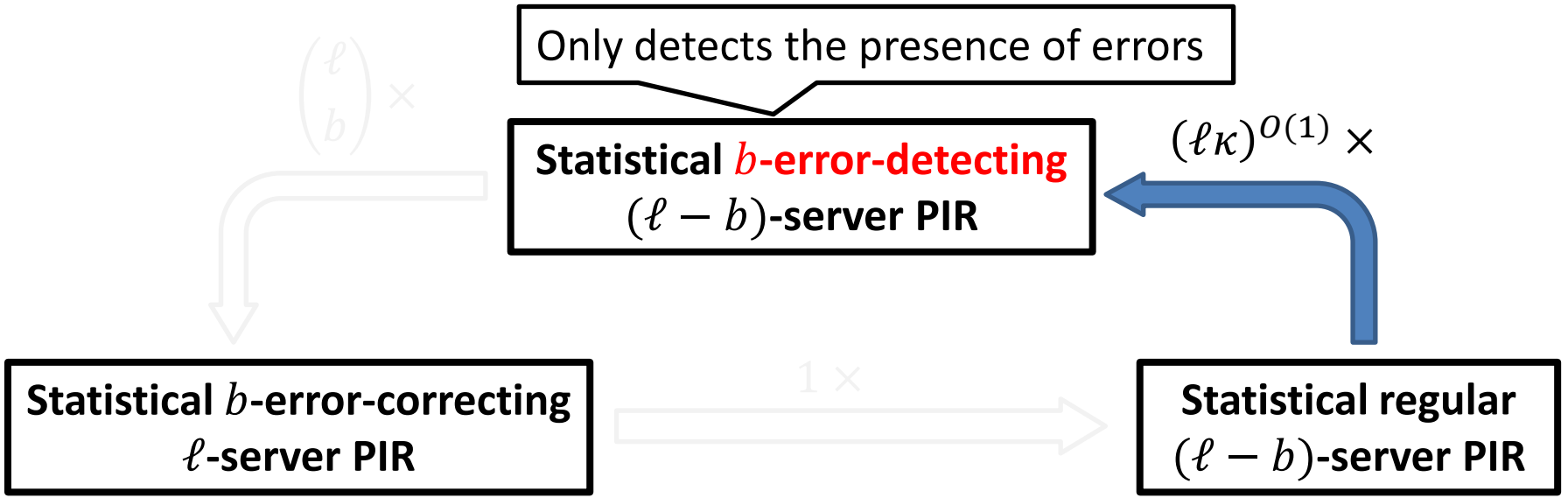
✓ **More communication-efficient** error-correcting PIR schemes

Method	Communication	Error correction
[BS07] + [Efr12]	$\mathcal{L}_n[r^{-1}, O(1)], r = \log(\ell - 2b)$	Perfect
Ours + [Efr12]	$\mathcal{L}_n[r^{-1}, O(1)], r = \log(\ell - b)$	Statistical

$$\mathcal{L}_n[u, v] = \exp(v(\log n)^u(\log\log n)^{1-u})$$

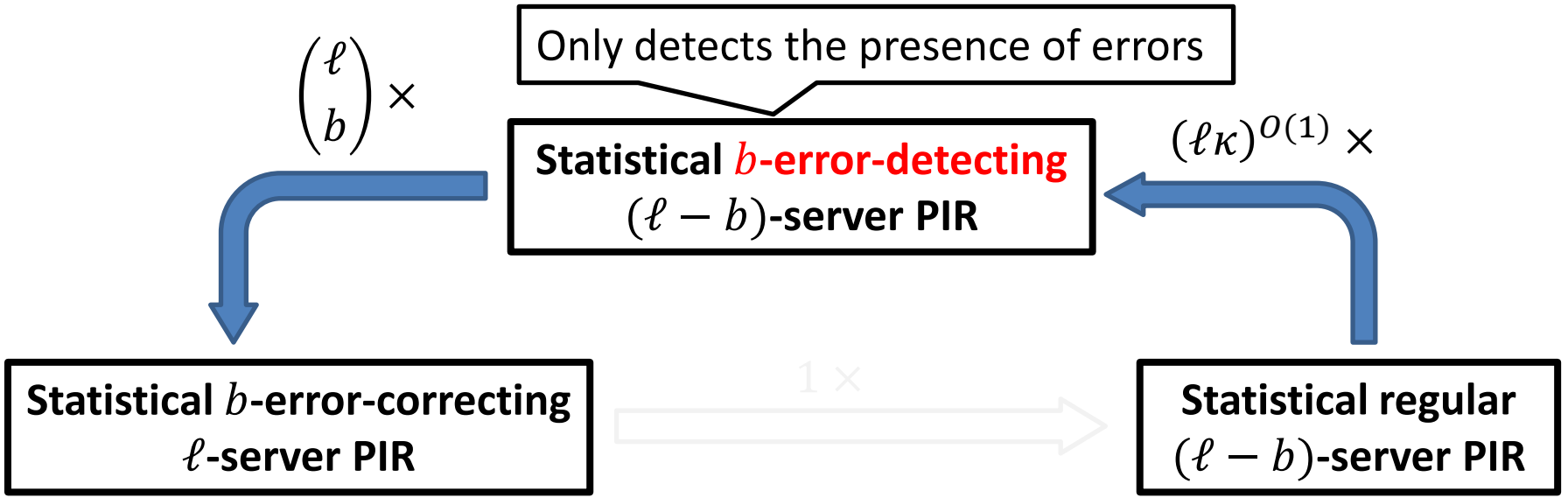
Statistical Error-Correcting PIR

Overview of Our Technique



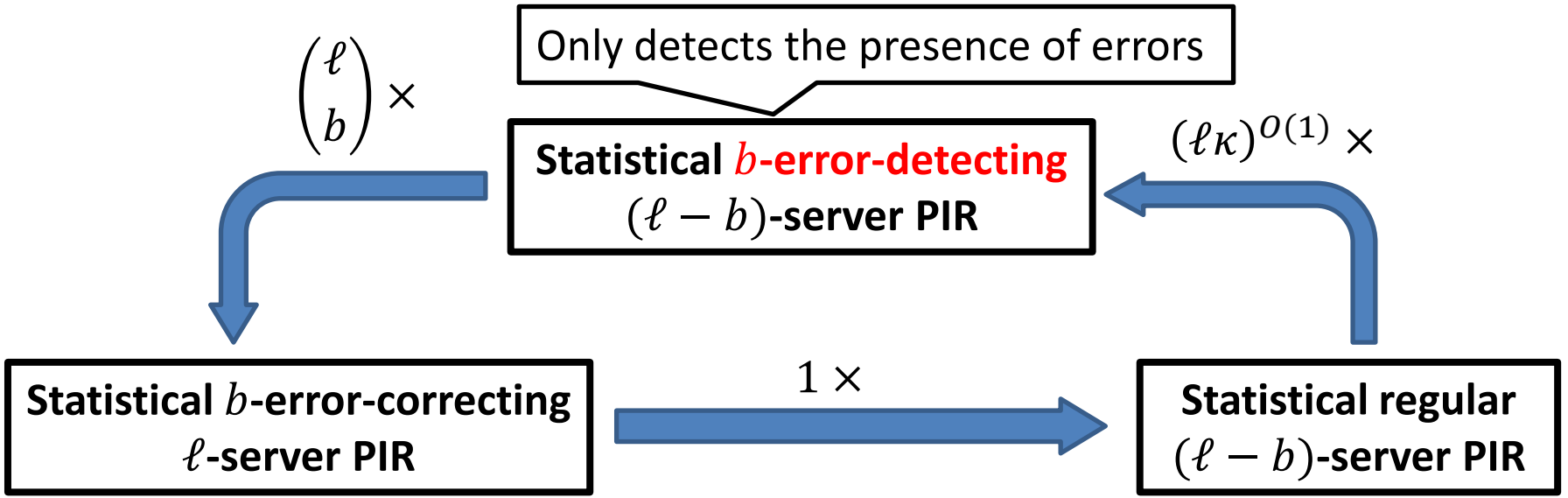
$$\mathrm{PIR}^*_{\ell-b,t}(n) \le \text{EC-PIR}^*_{\ell,b,t}(n) \le \binom{\ell}{b} \cdot \text{ED-PIR}^*_{\ell-b,b,t}(n) \le \binom{\ell}{b}(\ell\kappa)^{O(1)} \cdot \mathrm{PIR}^*_{\ell-b,t}(n)$$

Overview of Our Technique



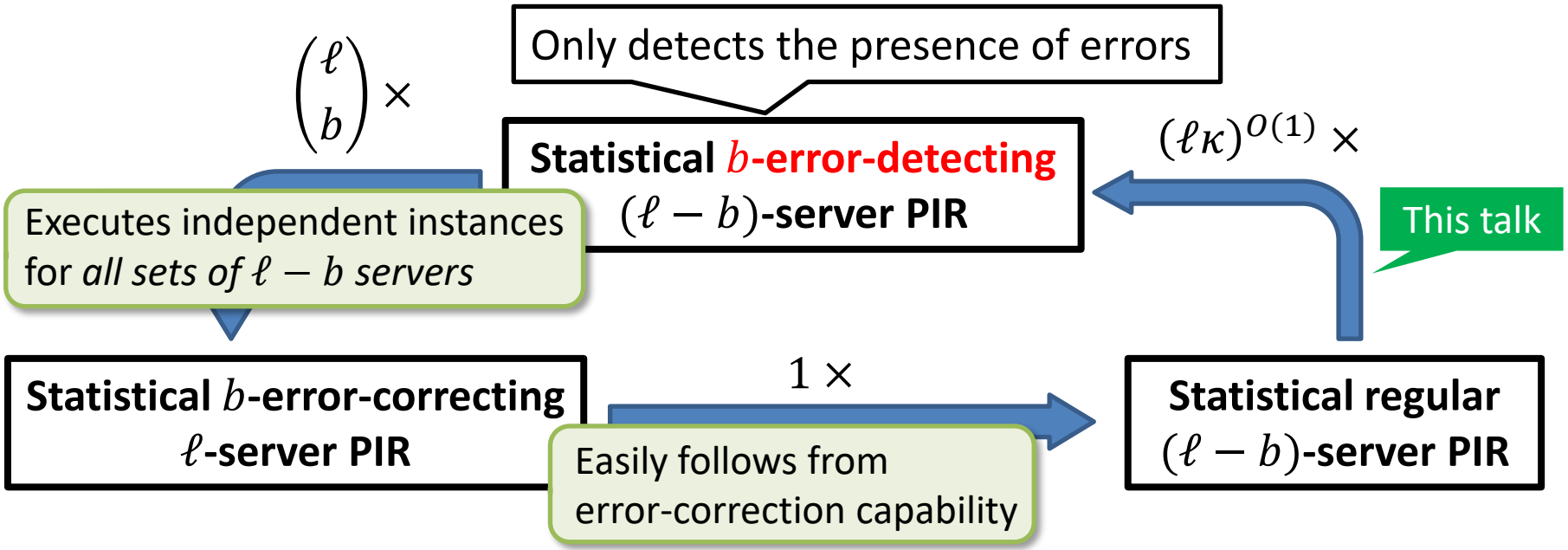
$$\mathrm{PIR}^*_{\ell-b,t}(n) \leq \text{EC–PIR}^*_{\ell,b,t}(n) \leq \binom{\ell}{b} \cdot \text{ED-PIR}^*_{\ell-b,b,t}(n) \leq \underbrace{\binom{\ell}{b}(\ell\kappa)^{O(1)}}_{\text{independent of } n} \cdot \mathrm{PIR}^*_{\ell-b,t}(n)$$

Overview of Our Technique



$$\mathrm{PIR}^*_{\ell-b,t}(n) \leq \mathrm{EC\text{-}PIR}^*_{\ell,b,t}(n) \leq \binom{\ell}{b} \cdot \mathrm{ED}\text{-}\mathrm{PIR}^*_{\ell-b,b,t}(n) \leq \underbrace{\binom{\ell}{b}(\ell\kappa)^{O(1)}}_{\text{independent of } n} \cdot \mathrm{PIR}^*_{\ell-b,t}(n)$$

Overview of Our Technique



$$\mathrm{PIR}^*_{\ell-b,t}(n) \leq \mathrm{EC\text{-}PIR}^*_{\ell,b,t}(n) \leq \binom{\ell}{b} \cdot \mathrm{ED}\text{-}\mathrm{PIR}^*_{\ell-b,b,t}(n) \leq \underbrace{\binom{\ell}{b}(\ell\kappa)^{O(1)}}_{\text{independent of } n} \cdot \mathrm{PIR}^*_{\ell-b,t}(n)$$

Two-server Case (Idea)

$\Pi_0 = (\mathcal{Q}_0, \mathcal{A}_0, \mathcal{D}_0)$: 2-server PIR with correctness error $\epsilon_0 \ll 1$

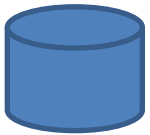
$\Longrightarrow \Pi = (\mathcal{Q}, \mathcal{A}, \mathcal{D})$: 1-error-detecting 2-server PIR

Assume (for now) that a client knows that the *first* server is honest

Still non-trivial since the client should detect it
if the second server actually submits an incorrect answer.

Honest

S_1



Malicious

S_2

Two-server Case (Idea)

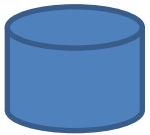
$\Pi_0 = (\mathcal{Q}_0, \mathcal{A}_0, \mathcal{D}_0)$: 2-server PIR with correctness error $\epsilon_0 \ll 1$

$\Longrightarrow$ $\Pi = (\mathcal{Q}, \mathcal{A}, \mathcal{D})$: 1-error-detecting 2-server PIR

Assume (for now) that a client knows that the *first* server is honest

Still non-trivial since the client should detect it
if the second server actually submits an incorrect answer.

Honest

S_1  $\mathrm{que}_1(\mathrm{C})$, $\mathrm{que}_2(\mathrm{V})$

Malicious

S_2  $\mathrm{que}_2(\mathrm{C}), \mathrm{que}_2(\mathrm{V})$

Query for computation

$\left(\mathrm{que}_1(\mathrm{C}), \mathrm{que}_2(\mathrm{C})\right) \leftarrow \mathcal{Q}_0(\tau)$

Query for verification

$\left(\mathrm{que}_1(\mathrm{V}), \mathrm{que}_2(\mathrm{V})\right) \leftarrow \mathcal{Q}_0(\tau)$

Two-server Case (Idea)

$\Pi_0 = (\mathcal{Q}_0, \mathcal{A}_0, \mathcal{D}_0)$: 2-server PIR with correctness error $\epsilon_0 \ll 1$

$\Longrightarrow$ $\Pi = (\mathcal{Q}, \mathcal{A}, \mathcal{D})$: 1-error-detecting 2-server PIR

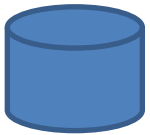
Assume (for now) that a client knows that the *first* server is honest

Still non-trivial since the client should detect it
if the second server actually submits an incorrect answer.

Simulate the answer of S_2

Honest

S_1



$\mathrm{que}_1(\mathrm{C})$, $\mathrm{que}_2(\mathrm{V})$

$\Rightarrow$ $\mathrm{ans}_1(\mathrm{C})$, $\mathrm{ans}_2(\mathrm{V})$

Malicious

S_2

$\mathrm{que}_2(\mathrm{C}), \mathrm{que}_2(\mathrm{V})$

$\Rightarrow$ $\widetilde{\mathrm{ans}}_2(\mathrm{C}), \widetilde{\mathrm{ans}}_2(\mathrm{V})$

Query for computation

$\left(\mathrm{que}_1(\mathrm{C}), \mathrm{que}_2(\mathrm{C})\right) \leftarrow \mathcal{Q}_0(\tau)$

Query for verification

$\left(\mathrm{que}_1(\mathrm{V}), \mathrm{que}_2(\mathrm{V})\right) \leftarrow \mathcal{Q}_0(\tau)$

If $\widetilde{\mathrm{ans}}_2(\mathrm{V}) = \mathrm{ans}_2(\mathrm{V})$,
outputs $\mathcal{D}_0\left(\mathrm{ans}_1(\mathrm{C}), \widetilde{\mathrm{ans}}_2(\mathrm{C})\right)$

Two-server Case (Idea)

$\Pi_0 = (\mathcal{Q}_0, \mathcal{A}_0, \mathcal{D}_0)$: 2-server PIR with correctness error $\epsilon_0 \ll 1$

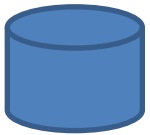
$\Longrightarrow$ $\Pi = (\mathcal{Q}, \mathcal{A}, \mathcal{D})$: 1-error-detecting 2-server PIR

Assume (for now) that a client knows that the *first* server is honest

Still non-trivial since the client should detect it
if the second server actually submits an incorrect answer.

Simulate the answer of S_2

Honest

S_1 

$\mathrm{que}_1(\mathrm{C})$, $\mathrm{que}_2(\mathrm{V})$

$\Rightarrow$ $\mathrm{ans}_1(\mathrm{C})$, $\mathrm{ans}_2(\mathrm{V})$

Query for computation

$\left(\mathrm{que}_1(\mathrm{C}), \mathrm{que}_2(\mathrm{C})\right) \leftarrow \mathcal{Q}_0(\tau)$

Query for verification

$\left(\mathrm{que}_1(\mathrm{V}), \mathrm{que}_2(\mathrm{V})\right) \leftarrow \mathcal{Q}_0(\tau)$

Shuffles the two queries

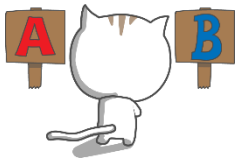
Malicious

S_2 

$\mathrm{que}_2(\mathrm{C}), \mathrm{que}_2(\mathrm{V})$

$\Rightarrow$ $\widetilde{\mathrm{ans}}_2(\mathrm{C}), \widetilde{\mathrm{ans}}_2(\mathrm{V})$

If $\widetilde{\mathrm{ans}}_2(\mathrm{V}) = \mathrm{ans}_2(\mathrm{V})$,
outputs $\mathcal{D}_0\left(\mathrm{ans}_1(\mathrm{C}), \widetilde{\mathrm{ans}}_2(\mathrm{C})\right)$



S_2 needs to guess the query for computation.

Probability of failure $\leq 1/2$

Two-server Case (Construction)

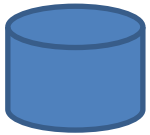
$\Pi_0 = (\mathcal{Q}_0, \mathcal{A}_0, \mathcal{D}_0)$: 2-server PIR with correctness error $\epsilon_0 \ll 1$

$\Longrightarrow \Pi = (\mathcal{Q}, \mathcal{A}, \mathcal{D})$: 1-error-detecting 2-server PIR

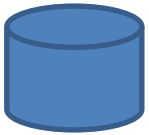
$\left(\mathrm{que}_1(\mathrm{C}), \mathrm{que}_2(\mathrm{C})\right) \leftarrow \mathcal{Q}_0(\tau)$

$\left(\mathrm{que}_1(\mathrm{V}), \mathrm{que}_2(\mathrm{V})\right) \leftarrow \mathcal{Q}_0(\tau)$

S_1



S_2

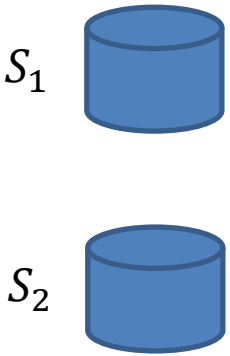


Two-server Case (Construction)

$\Pi_0 = (\mathcal{Q}_0, \mathcal{A}_0, \mathcal{D}_0)$: 2-server PIR with correctness error $\epsilon_0 \ll 1$

$\Longrightarrow$ $\Pi = (\mathcal{Q}, \mathcal{A}, \mathcal{D})$: 1-error-detecting 2-server PIR

If $S_i = S_1$:



$\left(\mathrm{que}_1(\mathrm{C}), \mathrm{que}_2(\mathrm{C})\right) \leftarrow \mathcal{Q}_0(\tau)$

$\left(\mathrm{que}_1(\mathrm{V}), \mathrm{que}_2(\mathrm{V})\right) \leftarrow \mathcal{Q}_0(\tau)$

$S_i \leftarrow_{\$} \{S_1, S_2\}$

Guess that S_i is honest

Two-server Case (Construction)

$\Pi_0 = (\mathcal{Q}_0, \mathcal{A}_0, \mathcal{D}_0)$: 2-server PIR with correctness error $\epsilon_0 \ll 1$

$\Longrightarrow$ $\Pi = (\mathcal{Q}, \mathcal{A}, \mathcal{D})$: 1-error-detecting 2-server PIR

If $S_i = S_1$:

Shuffles the two queries

$\left(\mathrm{que}_1(\mathrm{C}), \mathrm{que}_2(\mathrm{C})\right) \leftarrow \mathcal{Q}_0(\tau)$

$\left(\mathrm{que}_1(\mathrm{V}), \mathrm{que}_2(\mathrm{V})\right) \leftarrow \mathcal{Q}_0(\tau)$

$S_i \leftarrow_{\$} \{S_1, S_2\}$

Guess that S_i is honest

S_1

$\mathrm{que}_1(\mathrm{C})$, $\mathrm{que}_2(\mathrm{V})$

$\Rightarrow$ $\widetilde{\mathrm{ans}}_1(\mathrm{C})$, $\widetilde{\mathrm{ans}}_{21}(\mathrm{V})$

S_2

$\mathrm{que}_2(\mathrm{C}), \mathrm{que}_2(\mathrm{V})$

$\Rightarrow$ $\widetilde{\mathrm{ans}}_2(\mathrm{C}), \widetilde{\mathrm{ans}}_{22}(\mathrm{V})$

Two-server Case (Construction)

$\Pi_0 = (\mathcal{Q}_0, \mathcal{A}_0, \mathcal{D}_0)$: 2-server PIR with correctness error $\epsilon_0 \ll 1$

$\Longrightarrow$ $\Pi = (\mathcal{Q}, \mathcal{A}, \mathcal{D})$: 1-error-detecting 2-server PIR

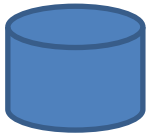
Shuffles the two queries

$\left(\mathrm{que}_1(\mathrm{C}), \mathrm{que}_2(\mathrm{C})\right) \leftarrow \mathcal{Q}_0(\tau)$

$\left(\mathrm{que}_1(\mathrm{V}), \mathrm{que}_2(\mathrm{V})\right) \leftarrow \mathcal{Q}_0(\tau)$

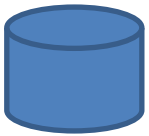
$S_i \leftarrow_{\$} \{S_1, S_2\}$

If $S_i = S_1$:

S_1 

$\mathrm{que}_1(\mathrm{C})$, $\mathrm{que}_2(\mathrm{V})$

⇨ $\widetilde{\mathrm{ans}}_1(\mathrm{C})$, $\widetilde{\mathrm{ans}}_{21}(\mathrm{V})$

S_2 

$\mathrm{que}_2(\mathrm{C}), \mathrm{que}_2(\mathrm{V})$

⇨ $\widetilde{\mathrm{ans}}_2(\mathrm{C}), \widetilde{\mathrm{ans}}_{22}(\mathrm{V})$

Guess that S_i is honest

If $\widetilde{\mathrm{ans}}_{21}(\mathrm{V}) = \widetilde{\mathrm{ans}}_{22}(\mathrm{V})$,
outputs $\mathcal{D}_0\left(\widetilde{\mathrm{ans}}_1(\mathrm{C}), \widetilde{\mathrm{ans}}_2(\mathrm{C})\right)$

Two-server Case (Construction)

$\Pi_0 = (\mathcal{Q}_0, \mathcal{A}_0, \mathcal{D}_0)$: 2-server PIR with correctness error $\epsilon_0 \ll 1$

$\Longrightarrow$ $\Pi = (\mathcal{Q}, \mathcal{A}, \mathcal{D})$: 1-error-detecting 2-server PIR

Shuffles the two queries

$\left(\mathrm{que}_1(\mathrm{C}), \mathrm{que}_2(\mathrm{C})\right) \leftarrow \mathcal{Q}_0(\tau)$

$\left(\mathrm{que}_1(\mathrm{V}), \mathrm{que}_2(\mathrm{V})\right) \leftarrow \mathcal{Q}_0(\tau)$

$S_i \leftarrow_{\$} \{S_1, S_2\}$

Guess that S_i is honest

If $S_i = S_1$:

S_1 $\mathrm{que}_1(\mathrm{C})$, $\mathrm{que}_2(\mathrm{V})$

⇨ $\widetilde{\mathrm{ans}}_1(\mathrm{C})$, $\widetilde{\mathrm{ans}}_{21}(\mathrm{V})$

S_2 $\mathrm{que}_2(\mathrm{C})$, $\mathrm{que}_2(\mathrm{V})$

⇨ $\widetilde{\mathrm{ans}}_2(\mathrm{C})$, $\widetilde{\mathrm{ans}}_{22}(\mathrm{V})$

If $\widetilde{\mathrm{ans}}_{21}(\mathrm{V}) = \widetilde{\mathrm{ans}}_{22}(\mathrm{V})$,
outputs $\mathcal{D}_0\left(\widetilde{\mathrm{ans}}_1(\mathrm{C}), \widetilde{\mathrm{ans}}_2(\mathrm{C})\right)$

Probability of failure $\leq O(\epsilon_0) + \frac{1}{2} + \frac{1}{2} \times \frac{1}{2} = \frac{3}{4} + \mathrm{negl.} < 1$

Fail to guess a honest server

Verification fails

Amplification by parallel execution

Conclusion

✓ **Lower bound** on $\mathrm{EC\text{-}PIR}_{\ell,b,t}(n)$ asymptotically matching the upper bound [BS07]

[BS07]

$$\mathrm{PIR}_{\ell-2b,t}(n) \leq \mathrm{EC\text{-}PIR}_{\ell,b,t}(n) \leq c_\ell \cdot \mathrm{PIR}_{\ell-2b,t}(n)$$

$\mathrm{EC\text{-}PIR}_{\ell,b,t}(n)$: Optimal comm. of t-private b-error-correcting ℓ-server PIR *with perfect correctness*
$\mathrm{PIR}_{k,t}(n)$: Optimal comm. of t-private regular k-server PIR *with perfect correctness*

✓ **Upper and lower bounds** on *statistical* error-correcting PIR

$$\mathrm{PIR}^*_{\ell-b,t}(n) \leq \mathrm{EC\text{-}PIR}^*_{\ell,b,t}(n) \leq c'_{\ell,\kappa} \cdot \mathrm{PIR}^*_{\ell-b,t}(n)$$

$\mathrm{EC\text{-}PIR}^*_{\ell,b,t}(n)$: Optimal comm. of t-private b-error-correcting ℓ-server PIR *with correctness error* $2^{-\kappa}$
$\mathrm{PIR}^*_{k,t}(n)$: Optimal comm. of t-private regular k-server PIR *with correctness error* $2^{-\kappa}$

The optimal communication complexity of error-correcting PIR is characterized by that of ***regular PIR.***

Thank you!

Please see https://eprint.iacr.org/2022/1206 for the full paper.