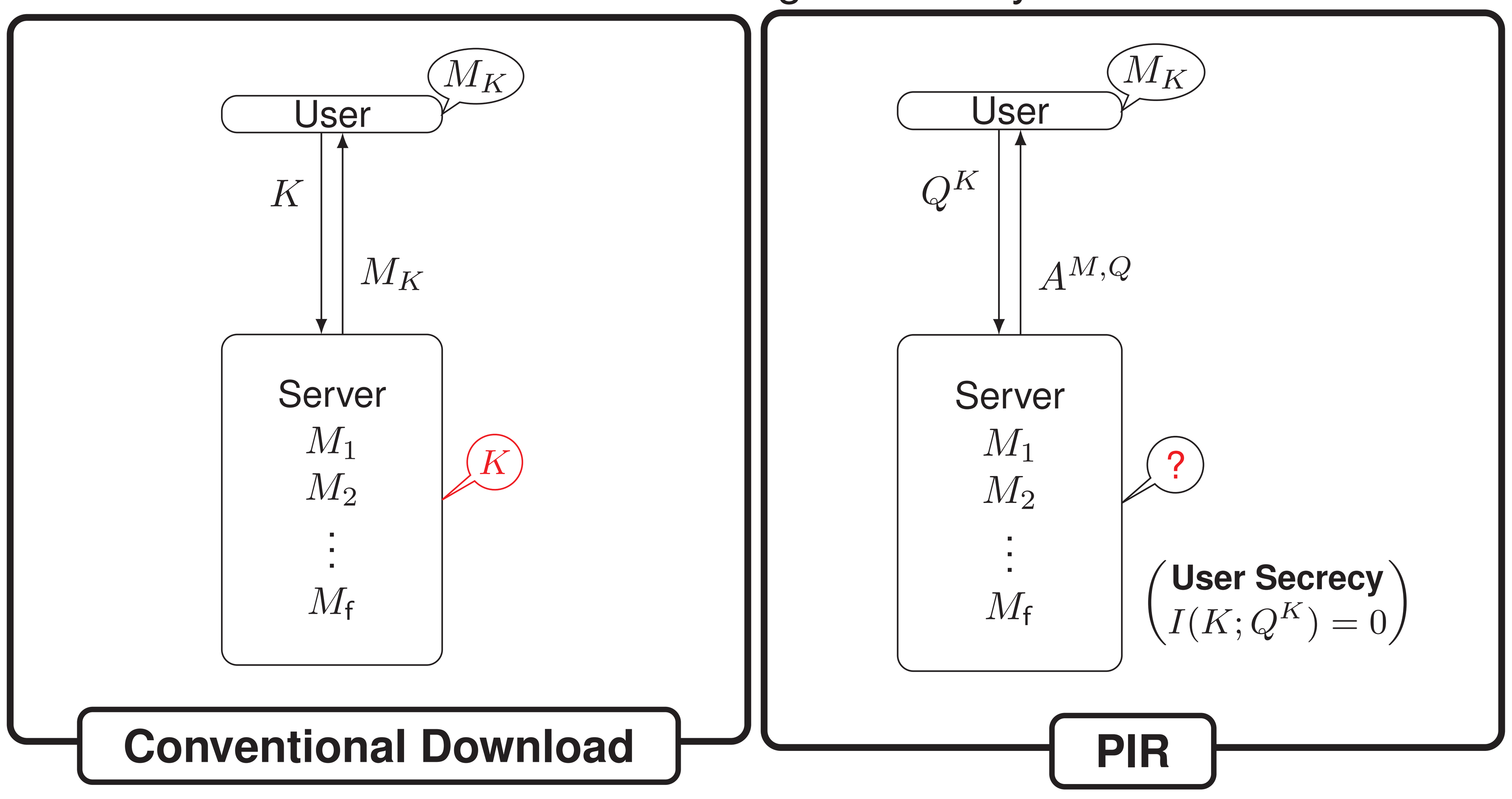
Capacity of Quantum Private Information Retrieval with Colluding Servers

Seunghoan Song[1], Masahito Hayashi[2,1] **(arXiv:2001.04436)**

[1]Nagoya University, [2]Southern University of Science and Technology

I. Private Information Retrieval (PIR)

Private Information Retrieval (PIR) is the problem to retrieve one of f classical files from servers without revealing the identity of the retrieved file.



Existing Results and Our Result

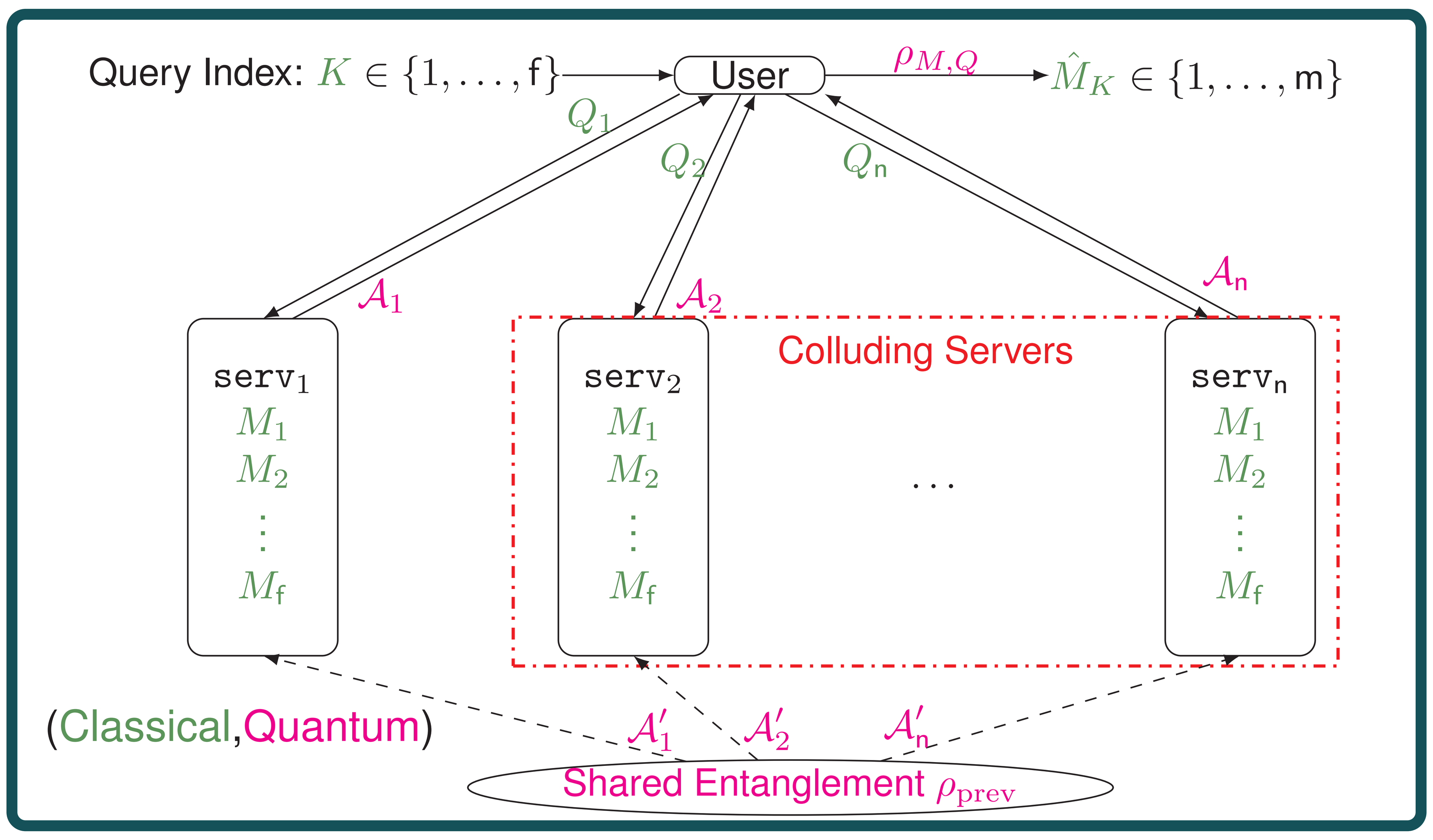
- Existing Quantum PIR (QPIR) studies mainly focused on one-server PIR with finite-bit files. [Le Gall12], [Aharonov et al.19], $\cdots$
- **Capacities** of n-server PIR with arbitrary size files: $C = \sup \frac{\text{(File size)}}{\text{(Communication)}}$

	Classical PIR	Quantum PIR our result
PIR Capacity	$\dfrac{1-\mathsf{n}^{-1}}{1-\mathsf{n}^{-\mathsf{f}}}$ [Sun-Jafar16]	1 § [SH, arXiv:1903.10209]
- with t-collusion	$\dfrac{1-\mathsf{t}/\mathsf{n}}{1-(\mathsf{t}/\mathsf{n})^{\mathsf{f}}}$ [Sun-Jafar18]	$\min\left\{1, \dfrac{2(\mathsf{n}-\mathsf{t})}{\mathsf{n}}\right\}$ §

§ With server secrecy and by strong converse. $*$ n servers and f files.

II. QPIR Model with Multiple and Colluding Servers

QPIR Model



- User and servers are honest but colluding servers (at most t, unknown to user) communicate to reveal K.

Evaluation of QPIR Protocol $\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}$

- **Error Probability** $P_{\mathrm{err}}^{(\mathsf{m})} := \Pr[\hat{M}_K = M_K]$
- **User Secrecy** $S_{\mathrm{user}}^{(\mathsf{m})} := \max_{\pi:\mathrm{perm}(\mathsf{n})} I(K;(Q_{\pi(1)},\dots,Q_{\pi(\mathsf{t})}))$
- **Server Secrecy** $S_{\mathrm{serv}}^{(\mathsf{m})} := I(M\setminus\{M_K\}; Q_{[\mathsf{n}]}, \bigotimes_{i=1}^{\mathsf{n}}\mathcal{A}_i | K)_{\rho_{M,Q}}$
- **QPIR Rate** $R^{(\mathsf{m})} = \frac{\text{(File size)}}{\text{(Download size)}} = \frac{\log \mathsf{m}}{\sum_{i=1}^{\mathsf{n}}\log\dim\mathcal{H}_i}$

QPIR Capacity For n servers and f files, QPIR capacity is defined as

$$C_{\mathrm{exact}}^{\alpha,\beta,\gamma} := \sup_{\substack{\mathsf{m}_\ell\to\infty,\\ \{\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}\}_{\ell=1}^\infty}} \left\{ \lim_{\ell\to\infty} R^{(\mathsf{m}_\ell)} \,\middle|\, P_{\mathrm{err}}^{(\mathsf{m}_\ell)} \le \alpha,\ S_{\mathrm{user}}^{(\mathsf{m}_\ell)} \le \beta,\ S_{\mathrm{serv}}^{(\mathsf{m}_\ell)} \le \gamma \right\},$$

$$C_{\mathrm{asymp}}^{\alpha,\beta,\gamma} := \sup_{\substack{\mathsf{m}_\ell\to\infty,\\ \{\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}\}_{\ell=1}^\infty}} \left\{ \lim_{\ell\to\infty} R^{(\mathsf{m}_\ell)} \,\middle|\, \lim_{\ell\to\infty} P_{\mathrm{err}}^{(\mathsf{m}_\ell)} \le \alpha,\ \lim_{\ell\to\infty} S_{\mathrm{user}}^{(\mathsf{m}_\ell)} \le \beta,\ \lim_{\ell\to\infty} S_{\mathrm{serv}}^{(\mathsf{m}_\ell)} \le \gamma \right\}.$$

III. Main Result

Theorem 1 *For any $\alpha \in [0,1)$ and $\beta,\gamma \in [0,\infty]$, the QPIR capacity with $\mathsf{f}\ge 2$ files, $\mathsf{n}\ge 2$ servers, and $1 \le \mathsf{t} < \mathsf{n}$ colluding servers is*

$$C_{\mathrm{exact}}^{\alpha,\beta,\gamma} = C_{\mathrm{asymp}}^{\alpha,\beta,\gamma} = 1 \ \text{ for } \mathsf{t} \le \frac{\mathsf{n}}{2}, \qquad C_{\mathrm{exact}}^{\alpha,0,0} = C_{\mathrm{exact}}^{0,\beta,0} = \frac{2(\mathsf{n}-\mathsf{t})}{\mathsf{n}} \ \text{ for } \mathsf{t} > \frac{\mathsf{n}}{2}.$$

IV. Preliminaries

Lemma 1: Let n,t be $\mathsf{n}/2 \le \mathsf{t} < \mathsf{n}$. There exists a $2\mathsf{n}\times 2\mathsf{t}$ matrix $D = (\mathbf{v}_1,\dots,\mathbf{v}_{2\mathsf{t}}) = (\mathbf{w}_1^\top,\dots,\mathbf{w}_{2\mathsf{n}}^\top)^\top$ over a finite field $\mathbb{F}_q$ s.t.

(a) $\langle \mathbf{v}_i, J\mathbf{v}_j\rangle = 0$ for any $i\in\{1,\dots,2(\mathsf{n}-\mathsf{t})\}$ and $j\in\{1,\dots,2\mathsf{t}\}$, where $J = \begin{pmatrix} 0 & -I_\mathsf{n} \\ I_\mathsf{n} & 0\end{pmatrix}$, and

(b) $\mathbf{w}_{\pi(1)},\dots,\mathbf{w}_{\pi(\mathsf{t})},\mathbf{w}_{\pi(1)+\mathsf{n}},\dots,\mathbf{w}_{\pi(\mathsf{t})+\mathsf{n}}$ are linearly independent for any perm $\pi \in \mathrm{perm}(\mathsf{t})$.

Stabilizer Formalism by Condition **(a)**

- $\mathrm{V} := \mathrm{span}\{\mathbf{v}_1,\dots,\mathbf{v}_{2(\mathsf{n}-\mathsf{t})}\}$ defines a **stabilizer**.
  ($\because$ Self-orthogonality $\mathrm{V}\subset\mathrm{V}^\perp := \{\mathbf{v}\in\mathbb{F}_q^{2n} \mid \langle \mathbf{v}, J\mathbf{v}'\rangle = 0\ \forall \mathbf{v}'\in\mathrm{V}\}$)
- Let $\mathcal{A} = \mathrm{span}\{|i\rangle \mid i\in\mathbb{F}_q\}$. For $a,b\in\mathbb{F}_q$ and $\mathbf{v}=(v_1,\dots,v_{2n})\in\mathbb{F}_q^{2n}$,

$$\mathsf{X}(a) := \sum_{i\in\mathbb{F}_q} |i+a\rangle\langle i|, \qquad \mathsf{Z}(b) := \sum_{i\in\mathbb{F}_q} \omega^{\mathrm{tr}\, bi}|i\rangle\langle i| \quad \text{on } \mathcal{A},$$

$$\mathbf{W}(\mathbf{v}) := \mathsf{X}(v_1)\mathsf{Z}(v_{n+1})\otimes\mathsf{X}(v_2)\mathsf{Z}(v_{n+2})\otimes\cdots\otimes\mathsf{X}(v_n)\mathsf{Z}(v_{2n}) \quad \text{on } \mathcal{A}^{\otimes n},$$

where $\omega := \exp(2\pi\sqrt{-1}/p)$.

- $\mathcal{A}^{\otimes n}$ is decomposed as $\mathcal{H}^{\otimes n} = \mathcal{W}\otimes\mathbb{C}^{q^{n-\dim\mathrm{V}}}$, where $\mathcal{W} = \mathrm{span}\{|[\mathbf{v}]\rangle \mid \underbrace{[\mathbf{v}] := \mathbf{v}+\mathrm{V}^\perp}_{\text{coset}} \in \mathbb{F}_q^{2n}/\mathrm{V}^\perp\}$.

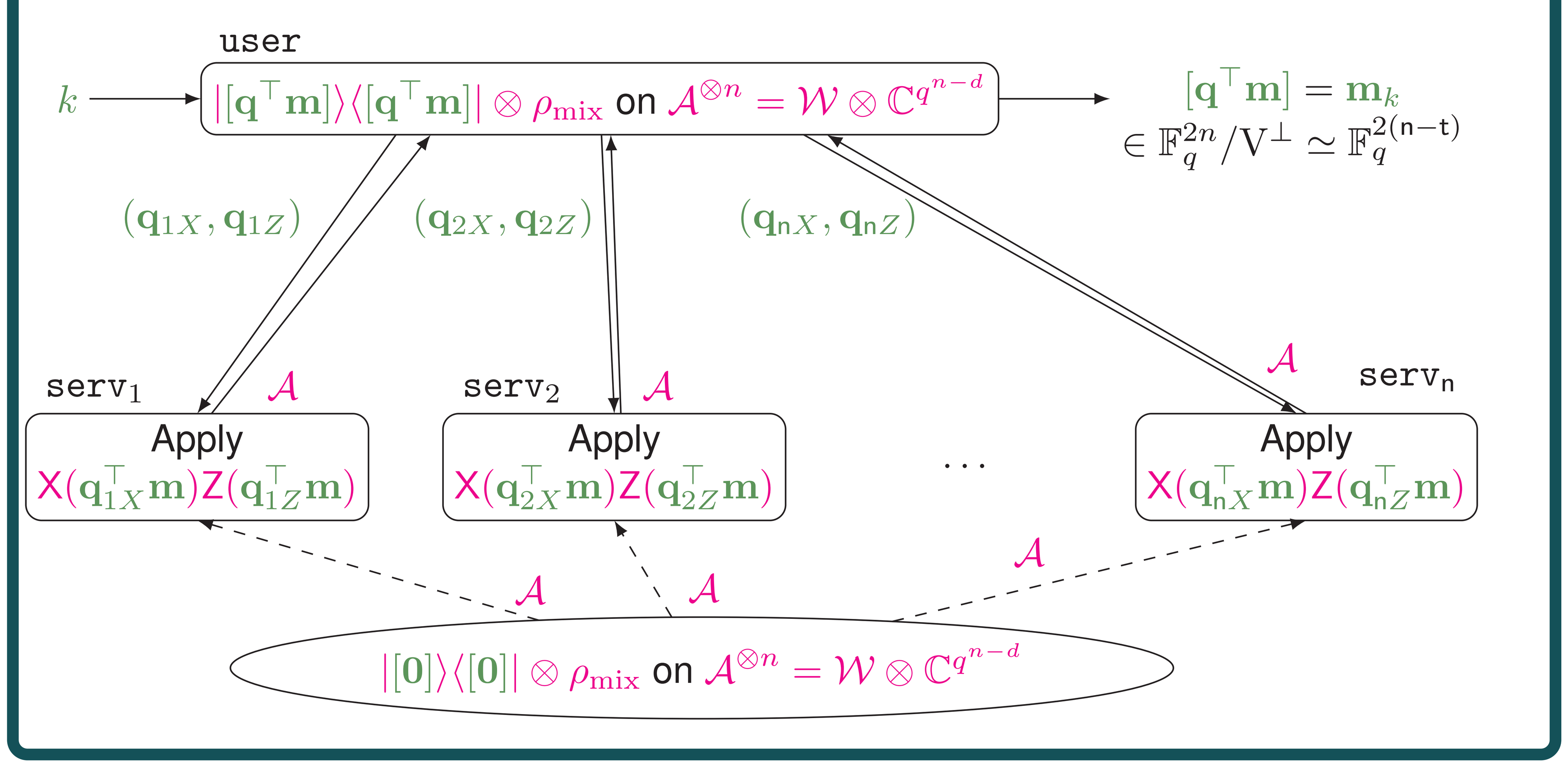
Lemma 2: . For any $\mathbf{v},\mathbf{v}'\in\mathbb{F}_q^{2n}$, we have

$$|[\mathbf{v}]\rangle\langle[\mathbf{v}]|\otimes\rho_{\mathrm{mix}} \xrightarrow{\mathbf{W}(\mathbf{v}')} |[\mathbf{v}+\mathbf{v}']\rangle\langle[\mathbf{v}+\mathbf{v}']|\otimes\rho_{\mathrm{mix}}. \tag{1}$$

V. Our QPIR Protocol

Protocol for n servers, f files, $\mathsf{t}\ge\frac{\mathsf{n}}{2}$ colluding servers

- Files $\mathbf{m} := (\mathbf{m}_1,\mathbf{m}_2,\dots,\mathbf{m}_\mathsf{f}) \in \mathbb{F}_q^{2(\mathsf{n}-\mathsf{t})}\times\cdots\times\mathbb{F}_q^{2(\mathsf{n}-\mathsf{t})} = \mathbb{F}_q^{2(\mathsf{n}-\mathsf{t})\mathsf{f}}$.
- The target file is $\mathbf{m}_k\in\mathbb{F}_q^{2(\mathsf{n}-\mathsf{t})}$.
- Choose $\mathbf{v}_{2\mathsf{t}+1},\dots,\mathbf{v}_{2\mathsf{n}}\in\mathbb{F}_q^{2n}$ s.t. $\{\mathbf{v}_1,\dots,\mathbf{v}_{2\mathsf{n}}\}$ is a basis of $\mathbb{F}_q^{2n}$.
- For secret random $R\in\mathbb{F}_q^{2\mathsf{t}\times2(\mathsf{n}-\mathsf{t})\mathsf{f}}$ and $E_k = (0,\dots,0,I,0,\dots,0)^\top$, $(\mathbf{q}_{1X},\dots,\mathbf{q}_{\mathsf{n}X},\mathbf{q}_{1Z},\dots,\mathbf{q}_{\mathsf{n}Z})^\top := (\mathbf{v}_1,\dots,\mathbf{v}_{2\mathsf{t}})R + (\mathbf{v}_{2\mathsf{t}+1},\dots,\mathbf{v}_{2\mathsf{n}})E_k$



Analysis of Protocol

- $R^{(\mathsf{m})} = \frac{\text{(Size of } \mathbf{m}_k)}{\text{(Download size)}} = \frac{2(\mathsf{n}-\mathsf{t})}{\mathsf{n}}$.
- $P_{\mathrm{err}}^{(\mathsf{m})} = 0$ and $S_{\mathrm{serv}}^{(\mathsf{m})} = 0$ ($\because$ the received state is $|[\mathbf{m}_k]\rangle\langle[\mathbf{m}_k]|\otimes\rho_{\mathrm{mix}}$).
- $S_{\mathrm{user}}^{(\mathsf{m})} = 0$ ($\because$ queries of any t servers are uniform random by **(b)**).

VI. Proof Sketch of $C_{\mathrm{exact}}^{\alpha,0,0} = C_{\mathrm{exact}}^{0,\beta,0} \le 2(\mathsf{n}-\mathsf{t})/\mathsf{n}$

- By secrecy, colluding servers generate t ebits b/w user and other servers,
- With shared ebits, non-colluding $(\mathsf{n}-\mathsf{t})$ servers can send at most $2(\mathsf{n}-\mathsf{t})$ bits to the user.