Publicly-Verifiable Deletion via Target-Collapsing Functions

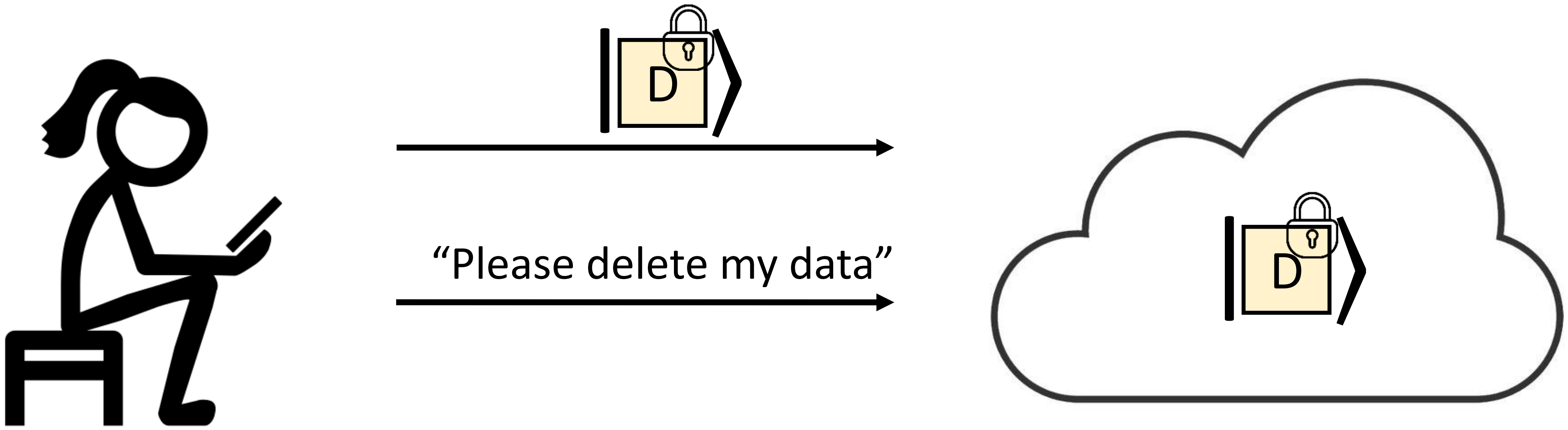
James Bartusek — UC Berkeley

Dakshita Khurana — UIUC

Alexander Poremba — Caltech

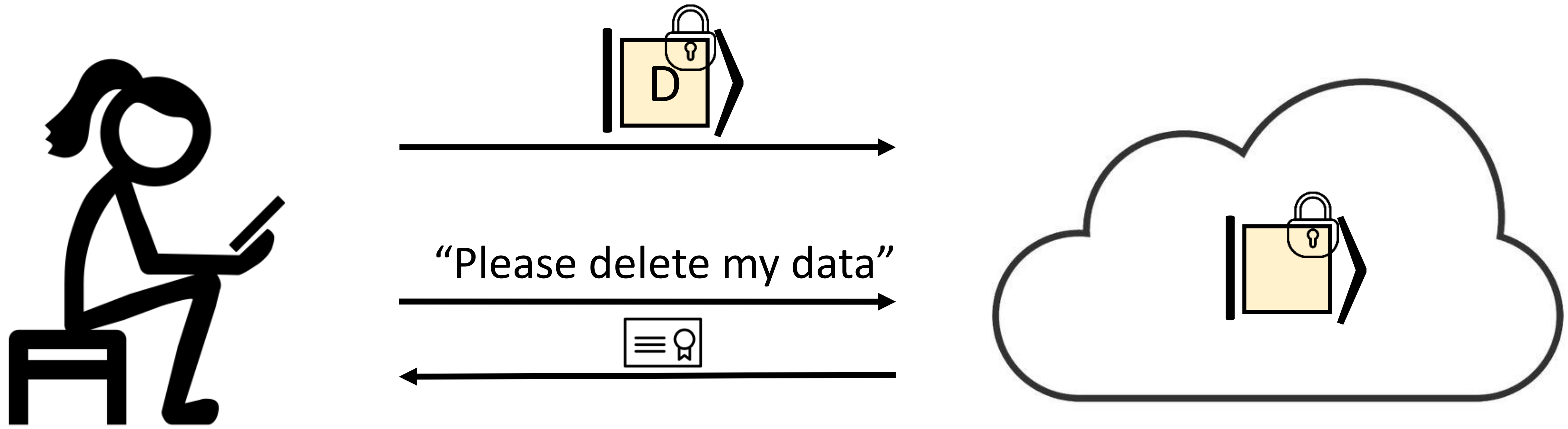
Publicly-Verifiable Deletion

Publicly-Verifiable Deletion



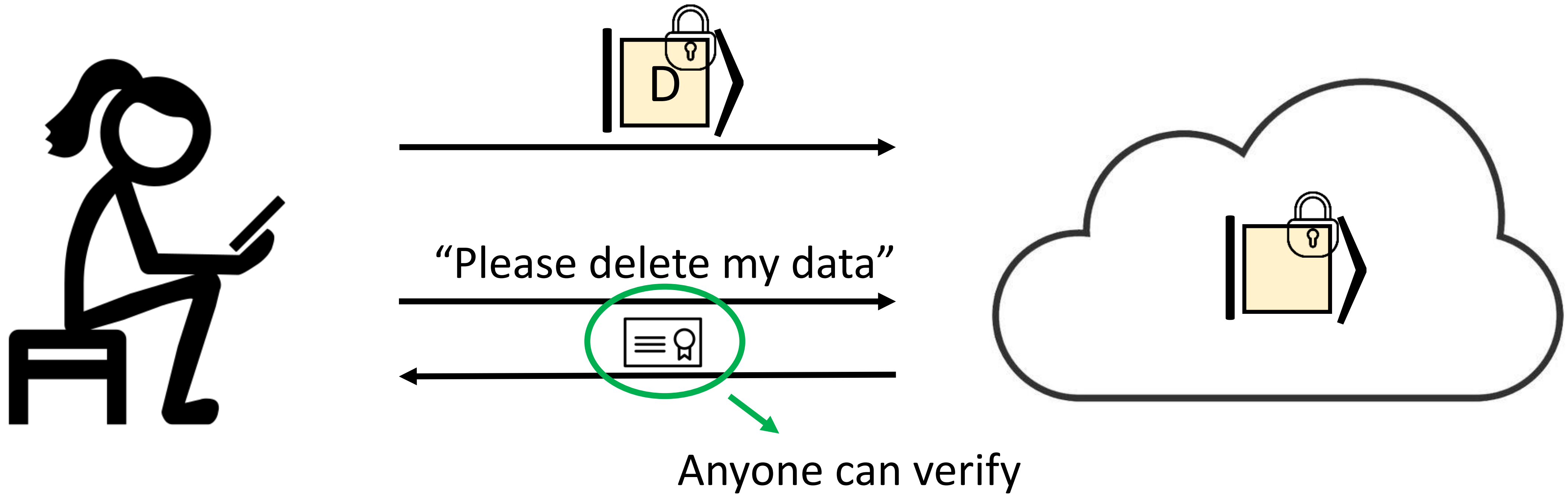
- Assumption: Malicious server cannot recover D from the encoding in polynomial time

Publicly-Verifiable Deletion



- Assumption: Malicious server cannot recover D from the encoding in polynomial time

Publicly-Verifiable Deletion



- Assumption: Malicious server cannot recover D from the encoding in polynomial time
- Goal: if is valid, the server won't be able to recover D even given and unbounded time

Prior Work

- [Broadbent, Islam 20]: Raised the question of publicly-verifiable deletion (PVD)
- [Hiroka, Morimae, Nishimaki, Yamakawa 21]: Public-key encryption with PVD assuming one-shot signatures and extractable witness encryption
- [Poremba 23]: Fully-homomorphic encryption with PVD assuming LWE and the strong Gaussian-collapsing conjecture
- [**B**, Garg, Goyal, Khurana, Malavolta, Raizes, Roberts 23]: Variety of cryptosystems with PVD assuming post-quantum indistinguishability obfuscation

Results: PVD from standard assumptions

- Prove the strong Gaussian-collapsing conjecture
  - Implies PVD from LWE via the dual-Regev-based scheme of [Por23]
- Prove that [Hhan, Morimae, Yamakawa 23] public-key encryption from non-abelian group actions satisfies PVD
- Initiate the study of *target*-collapsing hash functions and *certified-everlasting* target-collapsing hash functions
- Present a general template for obtaining PVD based on target-collapsing hash functions
  - E.g., obtain commitments with PVD from injective one-way functions
  - Follow-up works [**B**, Khurana, Malavolta, Poremba, Walter 23], [Kitagawa, Nishimaki, Yamakawa 23] further weaken the assumptions necessary for PVD

[Por 23] Candidate Scheme

$$\sum_{x \in \mathbb{Z}_q^m : A \cdot x = y} \rho_\sigma(x) \omega_q^{\langle x, b \cdot \left(0, \dots, 0, \frac{q}{2}\right) \rangle} |x\rangle$$

$$\Big\updownarrow \mathrm{FT}_q$$

$$\sum_{s, e \in \mathbb{Z}_q^n \times \mathbb{Z}_q^m} \rho_{\frac{q}{\sigma}}(e) \omega_q^{\langle s, y \rangle} \left| s \cdot A + e + b \cdot \left(0, \dots, 0, \frac{q}{2}\right) \right\rangle$$

KeyGen:

- Sample $(A, (v, 1)) \in \mathbb{Z}_q^{n \times m} \times \{0,1\}^m$ such that $A \cdot (v, 1) = 0$
- Output $pk = A, sk = v$

$\mathrm{Enc}(b)$:

- Prepare $|\psi_b\rangle = \sum_{x \in \mathbb{Z}_q^m} \rho_\sigma(x) \omega_q^{\langle x, b \cdot \left(0, \dots, 0, \frac{q}{2}\right) \rangle} |x\rangle |A \cdot x\rangle$
- Measure second register to obtain $y \in \mathbb{Z}_q^n$
- Output remaining state $|ct\rangle = \sum_{x \in \mathbb{Z}_q^m : A \cdot x = y} \rho_\sigma(x) \omega_q^{\langle x, b \cdot \left(0, \dots, 0, \frac{q}{2}\right) \rangle} |x\rangle$
- Output $vk = y$

$\mathrm{Del}(|ct\rangle)$:

- Measure in standard basis to obtain $\pi \in \mathbb{Z}_q^m$

$\mathrm{Verify}(vk, \pi)$:

- Check that π is “short” and that $A \cdot \pi = y$

Certified Deletion Experiment

$\mathrm{CDExp}_{\mathcal{A}}(b)$:

- Sample $A \leftarrow \mathbb{Z}_q^{n \times m}$
- Sample the pair $|\psi_{b,y}\rangle = \sum_{x: A \cdot x = y} \rho_\sigma(x) \omega_q^{\langle x, b \cdot \left(0, \ldots, 0, \frac{q}{2}\right) \rangle} |x\rangle, y$
- $\mathcal{A}(|\psi_{b,y}\rangle, y) \rightarrow \pi, \mathrm{st}$
- If π is "short" and $A \cdot \pi = y$, output st, and otherwise $|\bot\rangle\langle\bot|$

Claim: For any QPT $\mathcal{A}$, $\mathrm{TD}\big(\mathrm{CDExp}_{\mathcal{A}}(0), \mathrm{CDExp}_{\mathcal{A}}(1)\big) = \mathrm{negl}$

Suffices to prove that the Ajtai hash function is "certified everlasting Gaussian-collapsing"

Certified Everlasting Gaussian-Collapsing

$\mathrm{CEGCExp}_{\mathcal{A}}(b)$:

- Sample $A \leftarrow \mathbb{Z}_q^{n \times m}$
- Sample the pair $|\psi_y\rangle_X = \sum_{x:A\cdot x=y} \rho_\sigma(x)|x\rangle_X, y$
- If $b = 1$, measure register X in the standard basis
- $\mathcal{A}(X, y) \to \pi, \mathrm{st}$
- If π is "short" and $A \cdot \pi = y$, output st, and otherwise $|\perp\rangle\langle\perp|$

Claim: $\mathrm{TD}\big(\mathrm{CEGCExp}_{\mathcal{A}}(0), \mathrm{CEGCExp}_{\mathcal{A}}(1)\big) = \mathrm{negl}$

Proven by building on techniques from [**B**, Khurana 23]

Generalization: (Certified Everlasting) Target-Collapsing

Let $\mathcal{H} = \{h\colon \mathcal{X} \to \mathcal{Y}\}_h$ be a family of hash functions

<u>Target-Collapsing Experiment</u>

<u>$\mathcal{A}$</u> (QPT)

<u>$Ch(b)$</u>

Sample $h \leftarrow \mathcal{H}$

Prepare $\sum_{x\in\mathcal{X}} |x\rangle_X |h(x)\rangle_Y$

Measure Y register to obtain y

If $b = 1$, measure X register

$\mathcal{A} \xleftarrow{X, y} Ch(b)$

$\mathcal{A} \xrightarrow{b'} Ch(b)$

Output 1 if $b' = b$

Weakening of collapsing [Unruh 16] – analogous to how target collision resistance is a weakening of collision resistance

Generalization: (Certified Everlasting) Target-Collapsing

Let $\mathcal{H} = \{h: \mathcal{X} \to \mathcal{Y}\}_h$ be a family of hash functions

<u>Target-Collapsing Experiment</u>

$\underline{\mathcal{A}}$		$\underline{Ch(b)}$
		Sample $h \leftarrow \mathcal{H}$
		Prepare $\boxed{\sum_{x \in \mathcal{X}} \|x\rangle_X \|h(x)\rangle_Y}$
		Measure Y register to obtain y
		If $b = 1$, $\boxed{\text{measure } X \text{ register}}$
	$\xleftarrow{X, y}$	
(QPT)	$\xrightarrow{b'}$	
		Output 1 if $b' = b$

Can generalize the distribution over $\mathcal{X}$

Can generalize the measurement of X

Weakening of collapsing [Unruh 16] – analogous to how target collision resistance is a weakening of collision resistance

Generalization: (Certified Everlasting) Target-Collapsing

Let $\mathcal{H} = \{h: \mathcal{X} \to \mathcal{Y}\}_h$ be a family of hash functions

<u>Target-Collapsing Experiment</u>

$\underline{\mathcal{A}}$		$\underline{Ch(b)}$
		Sample $h \leftarrow \mathcal{H}$ Prepare $\sum_{x \in \mathcal{X}} \lvert x\rangle_X \lvert h(x)\rangle_Y$ Measure Y register to obtain y If $b = 1$, measure X register
	$\xleftarrow{X, y}$	
(QPT)	$\xrightarrow{b'}$	
		Output 1 if $b' = b$

Weakening of collapsing [Unruh 16] – analogous to how target collision resistance is a weakening of collision resistance

<u>Certified Everlasting Target-Collapsing Experiment</u>

$\underline{\mathcal{A}}$		$\underline{Ch(b)}$
		Sample $h \leftarrow \mathcal{H}$ Prepare $\sum_{x \in \mathcal{X}} \lvert x\rangle_X \lvert h(x)\rangle_Y$ Measure Y register to obtain y If $b = 1$, measure X register
	$\xleftarrow{X, y}$	
(QPT)	$\xrightarrow{\pi}$	
(unbounded)	$\xrightarrow{b'}$	If $h(\pi) \neq y$, output $b' \leftarrow \{0,1\}$
		Output 1 if $b' = b$

Generalization: (Certified Everlasting) Target-Collapsing

Let $\mathcal{H} = \{h: \mathcal{X} \to \mathcal{Y}\}_h$ be a family of hash functions

Main Theorem: If $\mathcal{H}$ satisfies target-collapsing and target-collision-resistance, then it satisfies *certified everlasting* target-collapsing

Conclusion

- Introduce a natural weakening of collapsing called target-collapsing
- Show that hash functions with certain non-everlasting security properties *automatically* satisfy certified everlasting target-collapsing
- Use our framework to prove that encryption schemes from [Por 23] and [HMY 23] satisfy publicly-verifiable deletion
- Use our framework design a suite of schemes with publicly-verifiable deletion based on target-collapsing hash functions
- Future directions:
  - A more thorough investigation of the relationship between target-collapsing, target-collision-resistance, and related notions
  - Other applications of target-collapsing