Publicly-Verifiable Deletion via Target-Collapsing Functions

James Bartusek (UC Berkeley)
Dakshita Khurana (UIUC)
Alexander Poremba (Caltech)

CRYPTO 2023

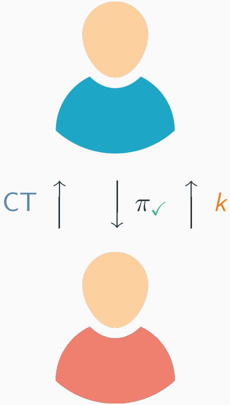
August 21, 2023

Caltech

Can we prove that data has been deleted?

Quantum Encryption with Certified Deletion (BI'20)

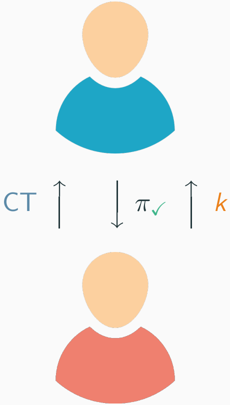
Bob



Alice $\quad \mathsf{CT} \leftarrow \mathsf{Enc}_k(m)$

Quantum Encryption with Certified Deletion (BI'20)

Bob



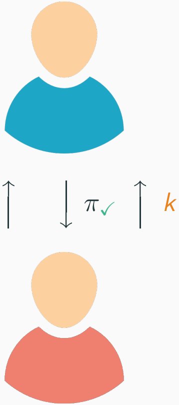
Alice $\quad \mathsf{CT} \leftarrow \mathsf{Enc}_k(m)$

Prior work:

- Broadbent and Islam (TCC '20): Private-key encryption
- Hiroka, Morimae, Nishimaki and Yamakawa (Asiacrypt '21): Public-key encryption and attribute-based encryption
- Bartusek and Khurana (CRYPTO '23): *Generic compiler* for public-key, attribute-based and homomorphic encryption

Quantum Encryption with Certified Deletion (BI'20)

Bob



Alice $\mathsf{CT} \leftarrow \mathsf{Enc}_k(m)$

Prior work:

- Broadbent and Islam (TCC '20): Private-key encryption
- Hiroka, Morimae, Nishimaki and Yamakawa (Asiacrypt '21): Public-key encryption and attribute-based encryption
- Bartusek and Khurana (CRYPTO '23): *Generic compiler* for public-key, attribute-based and homomorphic encryption

> Publicly-verifiable deletion?
>
> Anyone should be able to verify a certificate π to determine whether CT was successfully deleted.

Publicly-Verifiable Deletion

Publicly-Verifiable Deletion (PVD)

- Hiroka, Morimae, Nishimaki and Yamakawa (Asiacrypt '21): *Public-key encryption* with PVD assuming one-shot signatures and extractable witness encryption.

Publicly-Verifiable Deletion (PVD)

- Hiroka, Morimae, Nishimaki and Yamakawa (Asiacrypt '21): *Public-key encryption* with PVD assuming one-shot signatures and extractable witness encryption.
- Poremba (ITCS '23): *Public-key and fully homomorphic encryption* with PVD assuming Strong Gaussian-Collapsing Conjecture about Ajtai hash function.

Publicly-Verifiable Deletion (PVD)

- Hiroka, Morimae, Nishimaki and Yamakawa (Asiacrypt '21): *Public-key encryption* with PVD assuming one-shot signatures and extractable witness encryption.
- Poremba (ITCS '23): *Public-key and fully homomorphic encryption* with PVD assuming Strong Gaussian-Collapsing Conjecture about Ajtai hash function.
- Bartusek, Garg, Goyal, Khurana, Malavolta, Raizes, Roberts (QIP '23): *Variety of cryptosystems* with PVD assuming indistinguishability obfuscation.

Publicly-Verifiable Deletion (PVD)

- Hiroka, Morimae, Nishimaki and Yamakawa (Asiacrypt '21): *Public-key encryption* with PVD assuming one-shot signatures and extractable witness encryption.
- Poremba (ITCS '23): *Public-key and fully homomorphic encryption* with PVD assuming Strong Gaussian-Collapsing Conjecture about Ajtai hash function.
- Bartusek, Garg, Goyal, Khurana, Malavolta, Raizes, Roberts (QIP '23): *Variety of cryptosystems* with PVD assuming indistinguishability obfuscation.

THIS WORK: PVD under standard assumptions.

- Initiate the study of (certified-everlasting) target-collapsing hashes:
  - Proof of *Strong Gaussian-Collapsing Conjecture* (implies PVD under LWE/SIS)
  - Proof that the public-key encryption scheme by Hhan, Morimae, Yamawaka (Eurocrypt'23) enables PVD (implies PVD under non-abelian group actions)
- Generic compiler for cryptosystems with PVD from target-collapsing hashes (for example, assuming *almost-regular one-way functions*)

Candidate construction:

Dual-Regev public-key scheme with PVD

Poremba (ITCS '23)

Gaussian superpositions

MAIN IDEA: Quantum reduction from SIS to LWE [Reg'05,SSTX'09]. Let $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$.

$$|\psi\rangle = \sum_{\mathbf{x}\in\mathbb{Z}_q^m} \rho_\sigma(\mathbf{x}) \, |\mathbf{x}\rangle \otimes |\mathbf{A}\cdot\mathbf{x} \pmod{q}\rangle, \qquad \rho_\sigma(\mathbf{x}) = \exp(-\pi\|\mathbf{x}\|^2/\sigma^2).$$

Gaussian superpositions

Main idea: Quantum reduction from SIS to LWE [Reg'05,SSTX'09]. Let $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$.

$$|\psi\rangle = \sum_{\mathbf{x} \in \mathbb{Z}_q^m} \rho_\sigma(\mathbf{x}) \, |\mathbf{x}\rangle \otimes |\mathbf{A} \cdot \mathbf{x} \pmod{q}\rangle, \qquad \rho_\sigma(\mathbf{x}) = \exp(-\pi \|\mathbf{x}\|^2 / \sigma^2).$$

Measure the second register, which results in an outcome $\mathbf{y} \in \mathbb{Z}_q^n$.

Gaussian superpositions

Main idea: Quantum reduction from SIS to LWE [Reg'05,SSTX'09]. Let $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$.

$$|\psi\rangle = \sum_{\mathbf{x}\in\mathbb{Z}_q^m} \rho_\sigma(\mathbf{x})\,|\mathbf{x}\rangle \otimes |\mathbf{A}\cdot\mathbf{x} \pmod q\rangle, \qquad \rho_\sigma(\mathbf{x}) = \exp(-\pi\|\mathbf{x}\|^2/\sigma^2).$$

Measure the second register, which results in an outcome $\mathbf{y} \in \mathbb{Z}_q^n$.

$$|\psi_{\mathbf{y}}\rangle = \sum_{\substack{\mathbf{x}\in\mathbb{Z}_q^m:\\ \mathbf{A}\mathbf{x}=\mathbf{y} \pmod q}} \rho_\sigma(\mathbf{x})\,|\mathbf{x}\rangle$$

Coset state

Gaussian superpositions

MAIN IDEA: Quantum reduction from SIS to LWE [Reg'05,SSTX'09]. Let $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$.

$$|\psi\rangle = \sum_{\mathbf{x} \in \mathbb{Z}_q^m} \rho_\sigma(\mathbf{x}) \, |\mathbf{x}\rangle \otimes |\mathbf{A} \cdot \mathbf{x} \pmod{q}\rangle, \qquad \rho_\sigma(\mathbf{x}) = \exp(-\pi \|\mathbf{x}\|^2/\sigma^2).$$

Measure the second register, which results in an outcome $\mathbf{y} \in \mathbb{Z}_q^n$.

$$|\psi_{\mathbf{y}}\rangle = \sum_{\substack{\mathbf{x} \in \mathbb{Z}_q^m: \\ \mathbf{A}\mathbf{x} = \mathbf{y} \pmod{q}}} \rho_\sigma(\mathbf{x}) \, |\mathbf{x}\rangle$$

Coset state

Superposition of short vectors $\mathbf{x}$
subject to the constraint that

$$\mathbf{A}\mathbf{x} = \mathbf{y} \pmod{q}.$$

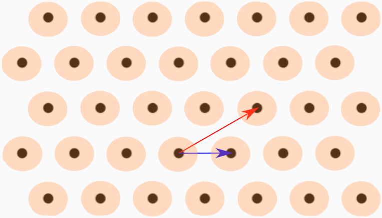
(solutions to inhomogenous SIS problem)

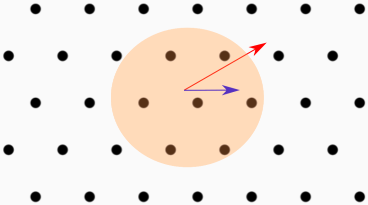
Duality of Gaussian States

$$\sum_{\mathbf{s}\in\mathbb{Z}_q^n}\sum_{\mathbf{e}\in\mathbb{Z}_q^m}\rho_{q/\sigma}(\mathbf{e})\,\omega_q^{-\langle\mathbf{s},\mathbf{y}\rangle}\,|\mathbf{s}^\mathsf{T}\mathbf{A}+\mathbf{e}^\mathsf{T}\rangle \quad\overset{\text{FT}}{\longleftrightarrow}\quad \sum_{\substack{\mathbf{x}\in\mathbb{Z}_q^m:\\ \mathbf{A}\mathbf{x}=\mathbf{y}\pmod q}}\rho_\sigma(\mathbf{x})\,|\mathbf{x}\rangle$$

Primal state

Dual state





Duality of Gaussian States

Use primal domain to *encrypt* messages.

$$\sum_{\mathbf{s}\in\mathbb{Z}_q^n}\sum_{\mathbf{e}\in\mathbb{Z}_q^m}\rho_{q/\sigma}(\mathbf{e})\,\omega_q^{-\langle\mathbf{s},\mathbf{y}\rangle}\left|\mathbf{s}^\intercal\mathbf{A}+\mathbf{e}^\intercal\right\rangle$$

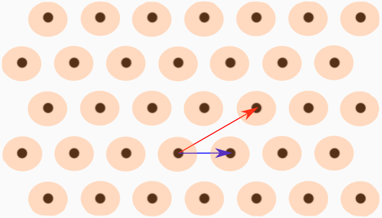
Primal state

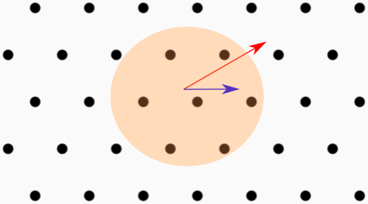
$$\xleftrightarrow{\text{FT}}$$

Use dual domain to *prove* deletion.

$$\sum_{\substack{\mathbf{x}\in\mathbb{Z}_q^m:\\ \mathbf{A}\mathbf{x}=\mathbf{y}\pmod q}}\rho_\sigma(\mathbf{x})\,|\mathbf{x}\rangle$$

Dual state





Dual-Regev public-key encryption with PVD [Poremba, ITCS'23]

- $\mathsf{KeyGen}(1^\lambda)$ generate $\mathsf{pk} = \mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and $\mathsf{sk} = \mathbf{t}$ with $\mathbf{A}\cdot\mathbf{t} = \mathbf{0} \pmod q$.
- $\mathsf{Enc}_{\mathsf{pk}}(b)$ generate a verification key $\mathsf{vk} \leftarrow (\mathbf{A}, \mathbf{y} \in \mathbb{Z}_q^n)$ and ciphertext

$$|\mathsf{CT}\rangle \leftarrow \sum_{\mathbf{s}\in\mathbb{Z}_q^n} \sum_{\mathbf{e}\in\mathbb{Z}_q^m} \rho_{q/\sigma}(\mathbf{e})\,\omega_q^{-\langle \mathbf{s},\mathbf{y}\rangle} |\mathbf{s}^\intercal\mathbf{A} + \mathbf{e}^\intercal + (0,\ldots,0,b\cdot\lfloor q/2\rfloor)\rangle.$$

- $\mathsf{Dec}_{\mathsf{sk}}(|\mathsf{CT}\rangle)$ measure the ciphertext in the computational basis with outcome $\mathbf{c} \in \mathbb{Z}_q^m$ and round $\mathbf{c}^\intercal \cdot \mathsf{sk} \in \mathbb{Z}_q$ with respect to 0 and $\lfloor \frac{q}{2} \rfloor$.

Dual-Regev public-key encryption with PVD [Poremba, ITCS'23]

- $\mathsf{KeyGen}(1^\lambda)$ generate $\mathsf{pk} = \mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and $\mathsf{sk} = \mathbf{t}$ with $\mathbf{A} \cdot \mathbf{t} = \mathbf{0} \pmod q$.
- $\mathsf{Enc}_{\mathsf{pk}}(b)$ generate a verification key $\mathsf{vk} \leftarrow (\mathbf{A}, \mathbf{y} \in \mathbb{Z}_q^n)$ and ciphertext

$$|\mathsf{CT}\rangle \leftarrow \sum_{\mathbf{s} \in \mathbb{Z}_q^n} \sum_{\mathbf{e} \in \mathbb{Z}_q^m} \rho_{q/\sigma}(\mathbf{e})\, \omega_q^{-\langle \mathbf{s}, \mathbf{y} \rangle} |\mathbf{s}^\intercal \mathbf{A} + \mathbf{e}^\intercal + (0, \dots, 0, b \cdot \lfloor q/2 \rfloor)\rangle.$$

- $\mathsf{Dec}_{\mathsf{sk}}(|\mathsf{CT}\rangle)$ measure the ciphertext in the computational basis with outcome $\mathbf{c} \in \mathbb{Z}_q^m$ and round $\mathbf{c}^\intercal \cdot \mathsf{sk} \in \mathbb{Z}_q$ with respect to 0 and $\lfloor \frac{q}{2} \rfloor$.

To delete the ciphertext, apply the quantum Fourier transform resulting in

$$|\widehat{\mathsf{CT}}\rangle = \sum_{\substack{\mathbf{x} \in \mathbb{Z}_q^m: \\ \mathbf{A}\mathbf{x} = \mathbf{y} \pmod q}} \rho_\sigma(\mathbf{x})\, \omega_q^{\langle \mathbf{x}, (0, \dots, 0, b \cdot \lfloor \frac{q}{2} \rfloor) \rangle} |\mathbf{x}\rangle$$

and measure to obtain a *short* solution π to the ISIS problem $\mathbf{A} \cdot \pi = \mathbf{y}$ (public verification!)

Security

Certified Deletion Experiment

$\text{CD-EXP}_{\mathcal{A}}(b)$:

1. Sample a matrix $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$.
2. Generate a pair $(\mathbf{y}, |\psi_{b,\mathbf{y}}\rangle)$ with

$$|\psi_{b,\mathbf{y}}\rangle = \sum_{\mathbf{x}\in\mathbb{Z}_q^m \text{ s.t. } \mathbf{Ax}=\mathbf{y}} \rho_\sigma(\mathbf{x})\ \omega_q^{\langle \mathbf{x},(0,\ldots,0,b\cdot\lfloor \frac{q}{2}\rfloor)\rangle} |\mathbf{x}\rangle.$$

3. Run $\mathcal{A}(\mathbf{A}, \mathbf{y}, |\psi_{b,\mathbf{y}}\rangle)$ to produce certificate π and residual state ρ.
4. If π is short and $\mathbf{A}\cdot\pi = \mathbf{y}$, output ρ. Else, output $|\perp\rangle\langle\perp|$.

Security: For any QPT $\mathcal{A}$: $\mathrm{TD}\big(\text{CD-EXP}_{\mathcal{A}}(0), \text{CD-EXP}_{\mathcal{A}}(1)\big) \le \text{negl}.$

(Certified-Everlasting) Target-Collapsing Hashes

Certified-Everlasting Gaussian-Collapsing

CEGC-EXP$_{\mathcal{A}}(b)$:

1. Sample a matrix $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$.
2. Generate a pair $(\mathbf{y}, |\psi_{\mathbf{y}}\rangle_{\mathsf{X}})$ with

$$|\psi_{\mathbf{y}}\rangle_{\mathsf{X}} = \sum_{\mathbf{x}\in\mathbb{Z}_q^m \text{ s.t. } \mathbf{A}\mathbf{x}=\mathbf{y}} \rho_\sigma(\mathbf{x})\,|\mathbf{x}\rangle_{\mathsf{X}}.$$

3. If $b = 1$, additionally measure register X in computational basis.
4. Run $\mathcal{A}(\mathbf{A}, \mathbf{y}, \mathsf{X})$ to produce certificate π and residual state ρ.
5. If π is short and $\mathbf{A} \cdot \pi = \mathbf{y}$, output ρ. Else, output $|\bot\rangle\langle\bot|$.

Security: For any QPT $\mathcal{A}$: $\mathsf{TD}\big(\text{CEGC-EXP}_{\mathcal{A}}(0), \text{CEGC-EXP}_{\mathcal{A}}(1)\big) \leq \text{negl.}$

Certified-Everlasting Gaussian-Collapsing

CEGC-EXP$_{\mathcal{A}}(b)$:

1. Sample a matrix $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n \times m}$.
2. Generate a pair $(\mathbf{y}, |\psi_{\mathbf{y}}\rangle_{\mathsf{X}})$ with

$$|\psi_{\mathbf{y}}\rangle_{\mathsf{X}} = \sum_{\mathbf{x} \in \mathbb{Z}_q^m \text{ s.t. } \mathbf{A}\mathbf{x} = \mathbf{y}} \rho_\sigma(\mathbf{x}) \, |\mathbf{x}\rangle_{\mathsf{X}}.$$

3. If $b = 1$, additionally measure register X in computational basis.
4. Run $\mathcal{A}(\mathbf{A}, \mathbf{y}, \mathsf{X})$ to produce certificate π and residual state ρ.
5. If π is short and $\mathbf{A} \cdot \pi = \mathbf{y}$, output ρ. Else, output $|\bot\rangle\langle\bot|$.

Proof idea:
- use entanglement via $|+\rangle_{\mathsf{C}}$: superposition of non-measured/measured register X.
- wait until $\mathcal{A}$ replies with π, then perform projective measurement on register C.

Generalization: Certified-Everlasting Target-Collapsing

Let $\mathcal{H} = \{h : \mathcal{X} \to \mathcal{Y}\}_h$ be a hash family, $\mathcal{D}$ be a distribution and $\mathcal{M}$ be a measurement.

Certified-Everlasting $(\mathcal{D}, \mathcal{M})$-Target-Collapsing

- Ajtai hash function $\to$ random hash h in $\mathcal{H}$
- Gaussian distribution $\to$ distribution specified by $\mathcal{D}$.
- Computational basis measurement of X $\to$ measurement specified by $\mathcal{M}$.

$$|\psi\rangle_{\mathsf{XY}} = \sum_{x \in \mathcal{X}} \sqrt{\mathcal{D}(x)}\, |x\rangle_{\mathsf{X}} \otimes |h(x)\rangle_{\mathsf{Y}}.$$

Generalization: Certified-Everlasting Target-Collapsing

Let $\mathcal{H} = \{h : \mathcal{X} \to \mathcal{Y}\}_h$ be a hash family, $\mathcal{D}$ be a distribution and $\mathcal{M}$ be a measurement.

Certified-Everlasting $(\mathcal{D}, \mathcal{M})$-Target-Collapsing

- Ajtai hash function $\to$ random hash h in $\mathcal{H}$
- Gaussian distribution $\to$ distribution specified by $\mathcal{D}$.
- Computational basis measurement of X $\to$ measurement specified by $\mathcal{M}$.

$$|\psi\rangle_{\mathsf{XY}} = \sum_{x \in \mathcal{X}} \sqrt{\mathcal{D}(x)}\, |x\rangle_{\mathsf{X}} \otimes |h(x)\rangle_{\mathsf{Y}}.$$

Main Theorem: If the hash function family $\mathcal{H}$ satisfies

- $(\mathcal{D}, \mathcal{M})$-target-collision-resistance
- $(\mathcal{D}, \mathcal{M})$-target-collapsing

then $\mathcal{H}$ is certified-everlasting $(\mathcal{D}, \mathcal{M})$-target-collapsing.

Generalization: Certified-Everlasting Target-Collapsing

Let $\mathcal{H} = \{h : \mathcal{X} \to \mathcal{Y}\}_h$ be a hash family, $\mathcal{D}$ be a distribution and $\mathcal{M}$ be a measurement.

Certified-Everlasting $(\mathcal{D}, \mathcal{M})$-Target-Collapsing

- Ajtai hash function $\to$ random hash h in $\mathcal{H}$
- Gaussian distribution $\to$ distribution specified by $\mathcal{D}$.
- Computational basis measurement of X $\to$ measurement specified by $\mathcal{M}$.

$$|\psi\rangle_{\mathsf{XY}} = \sum_{x \in \mathcal{X}} \sqrt{\mathcal{D}(x)}\, |x\rangle_{\mathsf{X}} \otimes |h(x)\rangle_{\mathsf{Y}}.$$

Main Theorem: If the hash function family $\mathcal{H}$ satisfies

- $(\mathcal{D}, \mathcal{M})$-target-collision-resistance $\quad$ ($\leftarrow$ quantum generalization of classical TCR)
- $(\mathcal{D}, \mathcal{M})$-target-collapsing $\quad$ ($\leftarrow$ weakening of collapsing property [Unruh'16])

then $\mathcal{H}$ is certified-everlasting $(\mathcal{D}, \mathcal{M})$-target-collapsing.

Conclusion

Conclusion

- We introduce a natural weakening of *collapsing* called target-collapsing.
- We show that hash functions which satisfy basic (non-everlasting) security properties *automatically* satisfy certified-everlasting target-collapsing.
- We use our framework to prove that the encryption schemes of Poremba (ITCS'23) and Hhan, Morimae and Yamakawa (Eurocrypt'23) enable PVD.
- We use our framework to design a generic compiler that adds PVD to a variety of schemes (commitments, PKE, ABE, FHE, WE, ...).

Conclusion

- We introduce a natural weakening of *collapsing* called target-collapsing.
- We show that hash functions which satisfy basic (non-everlasting) security properties *automatically* satisfy certified-everlasting target-collapsing.
- We use our framework to prove that the encryption schemes of Poremba (ITCS'23) and Hhan, Morimae and Yamakawa (Eurocrypt'23) enable PVD.
- We use our framework to design a generic compiler that adds PVD to a variety of schemes (commitments, PKE, ABE, FHE, WE, ...).

Open Problems:

- investigate the relationship between target-collapsing and target-collision-resistance, and related notions.
- new cryptographic applications of target-collapsing hashes.

Questions?