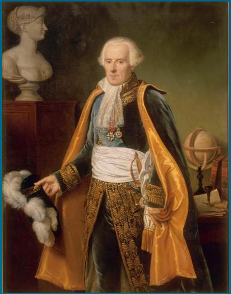
hard to get privacy



Giorgos Zirdelis
giorgos@ccs.neu.edu

April 27, 2017

Cool things we learned in class

including Chernoff bounds

- Laplace mechanism: $|Q| \approx n^2, \quad |X| = n^{\omega(1)}$
- Noisy histogram: $|X| \approx n^2, \quad |Q| = n^{\omega(1)}$
- PMW: if $|X|, |Q| \in \text{poly}(n)$

We require to be **computationally** efficient
$\rightarrow$ especially while giving this talk

Memories...

A flashback from the algo class - fa'15

Solving linear programs

- Dantzig'47: Simplex method
- Khachiyan '79: Ellipsoid method ($n^4 L$, n vars, L bits)
- ...

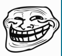
But...

- Simplex is not worst case polynomial time
- Klee-Minty polytope requires exp time

Can we "cook" hard instances for privacy?

- Yes, if you believe in crypto!
- If not, let us know ASAP of your results.

The Model

- Non-interactive setting
- Fix beforehand a query set Q
- Curator sanitizes/privatizes a dataset X^n for all $q \in Q$
  - Synthetic dataset - Can run my queries, it's a dataset!
  - Arbitrary output - Need an evaluator
- Throw away the original data and the curator 

Hardness for synthetic datasets [DNR+09]

(super-strong) Signatures from OWF [NY89, Rom90]

- Data universe X: pairs (msg, sig) = $\boxed{(m, \sigma)}$
- Query set Q: $\boxed{q_{\mathrm{vk}}(m, \sigma) = 1 \text{ iff } \mathrm{Verify}_{vk}(m, \sigma) = 1}$
- Items of Q, X are in $\{0,1\}^\lambda \implies$ both $|Q|$, $|X|$ have size 2^λ.
- Sample a dataset X^n with the **same** secret-key:
  - $m \leftarrow \{0,1\}^\lambda$
  - $\sigma \leftarrow \mathrm{Sign}(\mathsf{sk}, m)$
  - Output (m, σ)

Goal: Release a dataset that preserves some fractional count of the sigs (depending on accuracy) that verify for a key-pair $(\mathsf{sk}, \mathrm{vk})$.

Hardness for synthetic datasets [DNR+09]

A view of an alleged synthetic dataset X^m

$$X^n = \begin{array}{|c|}\hline (m_1, \sigma_1) \\ \hline (m_2, \sigma_2) \\ \hline (m_3, \sigma_3) \\ \hline \vdots \\ \hline (m_n, \sigma_n) \\ \hline \end{array} \qquad X^m = \begin{array}{|c|}\hline (m_1, \sigma_1)? \\ \hline (m_2, \sigma_2)? \\ \hline (m_3, \sigma_3)? \\ \hline \vdots \\ \hline (m_m, \sigma_m)? \\ \hline \end{array}$$

- Counting query $q(X^n) = \frac{1}{n} \sum_{i=1}^{n} q_{\mathrm{vk}}(m_i, \sigma_i) = 1$
- Counting query $q(X^m) = \frac{1}{m} \sum_{i=1}^{m} q_{\mathrm{vk}}(m_i, \sigma_i) \approx 1$
- Utility $\wedge$ $(X^n \cap X^m) \neq \emptyset$ /OR/ forge sigs (efficiently) $\rightarrow$ break crypto++

Hard-to-sanitize distribution [DNR+09]

A definition

Hard-to-sanitize distibutions on datasets:

- Sample a dataset x
- For all $q \in Q$,
- $\forall$ PPT sanitizers A with output $y = A(x) \implies$ PPT adversary T s.t.:
  - $\Pr[|q(x) - q(y)| \leq \alpha \quad \wedge \quad T(y) \cap x = \emptyset] \leq$ negl
  - $\Pr[x_i \in T(y')] \leq$ negl
    $y' = A(x')$ and $x_i \notin x$

In words:

- being accurate without leaking elements has negl prob.
- extracting an element that is not in the dataset has negl prob.

Hard-to-sanitize distribution [DNR+09]

Synthetic datasets. A TTS connection

- (super-strong) signatures: $|Q| = $ poly, $|X| = \exp$
- PRFs: $|Q| = \exp$, $|X| = $ poly
- Both assume OWFs

- What if $A(x)$ is an arbitrary output?
- Connection to traitor tracing schemes (TTS) [CFNP94]

Hardness results [DNR$^+$09]

- (super-strong) signatures: $|Q| = \text{poly}$, $|X| = \exp$
- PRFs: $|Q| = \exp$, $|X| = \text{poly}$
- Both assume OWFs

- What if $A(x)$ is an arbitrary output?
- Connection to traitor tracing schemes (TTS) first defined [CFNP94]

- TTS imply hard-to-sanitize distributions
- Hard-to-sanitize distributions imply TTS (one-shot + up to some parameters)

TTS implies hard-to-sanitize distributions [DNR+09]

TTS definition

t-resilient (private-key) TTS

- Consists of $(\mathrm{Gen}, \mathsf{Enc}, \mathsf{Dec}, \mathrm{Trace})$
- $(\mathrm{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is a semantically secure enc. scheme $(\mathsf{sk}_1, \ldots, \mathsf{sk}_n, \mathsf{pk})$
- $\leq t$ users arbitraty combine their secret-keys $\longrightarrow$ decoder D
- $\mathrm{Trace}(D)$ with black-box access $\Longrightarrow$ trace back at least one user

Can assume $t = n$.

TTS implies hard-to-sanitize distributions [DNR+09]

The reduction

- Data universe X = Secret-Keys: $\{0,1\}^{\mathrm{size}_{\mathrm{sk}}(n,\lambda)}$
- Query set Q = Ciphertexts: $q_c(x_i) =$ Dec(c, x_i)
  (output LSB for counting queries)
- Both $|Q|, |X| = \exp(n, \lambda)$
- "Loose" utility $\alpha < 1/2 \Rightarrow \lceil 0 \pm \alpha \rfloor = 0$ and $\lceil 1 \pm \alpha \rfloor = 1$

- Utility $\Rightarrow$ Decoder $\Rightarrow$ Trace $\Rightarrow$ No-privacy
- Trace $\rightarrow x'_i \notin x \Rightarrow$ Decoder $= x'_i \Rightarrow$ Blame innocent user

TTS implies hard-to-sanitize distributions [DNR+09]

Instatiate with [BSW06]

- Secret-Key and Ciphertext $\Rightarrow$ size of X, Q
- Full collusion resilience [BSW06]
- $\mathrm{size}_{\mathrm{sk}} = O(\lambda)$ and $\mathrm{size}_{\mathrm{c}} = O(\sqrt{n}\lambda)$
- $|X| = 2^{\mathrm{size}_{\mathrm{sk}}}$ and $|Q| = 2^{\mathrm{size}_{\mathrm{c}}}$

Smaller TTS parameters [KMUZ16]

What is an iO scheme?

Definition

A PPT algorithm iO is an indistinguishability obfuscator for a family of circuits $\{C_\lambda\}$ that satisfies the following properties:

- **Correctness:** For all λ, $C \in \{C_\lambda\}$ and x

$$\Pr_{iO \text{ coins}}[iO(C)(x) = C(x)] = 1$$

- **Security:** For all $C_0, C_1 \in \{C_\lambda\}$ such that for all x, $C_0(x) = C_1(x)$ and poly sized adversaries Adv,

$$|\Pr[\mathsf{Adv}(iO(C_0(x)) = 1] - \Pr[\mathsf{Adv}(iO(C_1(x)) = 1]| \leq \mathsf{negl}(\lambda)$$

We note that we are interested only in families of polynomial sized circuits.

Smaller TTS parameters [KMUZ16]

What is an iO scheme?

- iO(·) and iO(C(x)) are efficient (assume C(x) is efficient)
- **(correctness)** For all C: iO(C(x)) = C(x)
- **(security)** For all C_0, C_1 with
  $C_0(x) = C_1(x) \implies iO(C_0(x)) \overset{c}{\approx} iO(C_1(x))$

Smaller TTS parameters [KMUZ16]

What is an puncturable PRF?

- Allowed to evaluate on all but some “punctured” inputs
- “Punctured” inputs do not return PRF value
  Still return a pseudorandom value
- Can get them from GGM construction

Smaller TTS parameters [KMUZ16]

The old and the new

- A PRG: $\{0,1\}^{\lambda/2} \to \{0,1\}^{\lambda}$
- A puncturable PRF: $\mathrm{PRF}_{\mathsf{sk}} : [n] \to \{0,1\}^{\lambda}$
- A twice puncturable PRF: $\mathrm{PRF}_{\mathsf{Enc}} : [m] \to [n]$
- An indistinguishability obfuscator iO.

Smaller TTS parameters [KMUZ16]

Put everything together

The scheme works in the following way.

- Setup(1^λ).
  - Sample contrained $\mathrm{PRF}_{\mathsf{sk}}$ and $\mathrm{PRF}_{\mathsf{Enc}}$
  - $s_i = \mathrm{PRF}_{sk}(i)$. Let $O \leftarrow iO(\Pi_{\mathrm{PRF}_{\mathsf{sk}},\mathrm{PRF}_{\mathsf{Enc}}})$.
  - User's secret-key $\mathsf{sk}_i = (i, s_i, O)$ and the master key $\mathrm{mk} = \mathrm{PRF}_{\mathsf{Enc}}$.
- Enc(j, mk). Output $c \leftarrow \mathrm{PRF}^{-1}_{\mathsf{Enc}}(j)$.
- Dec(sk_i, c). Output $O(c, i, s_i)$.

$\Pi_{\mathrm{PRF}_{\mathsf{sk}},\mathrm{PRF}_{\mathsf{Enc}}}(c, i, s)$:
If $\mathrm{PRG}(s) \neq \mathrm{PRG}(\mathrm{PRF}_{\mathsf{sk}}(i))$, halt and output $\perp$.
Output $\mathbb{I}\{i \leq \mathrm{PRF}_{Enc}(c)\}$.

Smaller TTS parameters [KMUZ16]

The parameters

- $|\mathsf{sk}_i| = \log n + \lambda + |O| = \mathsf{poly}(\log n + \lambda)$ (bits)
- $c \in [m] \Rightarrow |c| = \log m \approx \log n^7 = \tilde{O}(\log n)$
- $\boxed{|X| = \{0,1\}^{\mathsf{poly}(\log n + \lambda)}}$ $\boxed{|Q| = m \approx n^7 = \mathsf{poly}(\lambda)}$
- Can do vice-versa

Open problems from [KMUZ16] and [BZ16]

- Replace iO with standard assumptions (i.e. LWE)
  - Contrained & Contraint Hiding PRFs (LWE [BKM17, CC17])
- Reduce degree of n^7, i.e. either $|X|$ or $|Q|$.
  - VBB gets you n^3.
  - Hard as low as $n^{2+o(1)}$ for $|Q|$ or $|X|$? (Laplace, Histogram)
- Hardness results for PAC learning from crypto using ORE
  - Threshold class. More "natural" classes?
  - iO, mmaps(functional enc.), NIZKs
  - Standard assumptions?

Open problems from [KMUZ16] and [BZ16]

- Replace iO with standard assumptions (i.e. LWE)
  - Contrained & Contraint Hiding PRFs (LWE [BKM17, CC17])
- Reduce degree of n^7, i.e. either $|X|$ or $|Q|$.
  - VBB gets you n^3.
  - Hard as low as $n^{2+o(1)}$ for $|Q|$ or $|X|$? (Laplace, Histogram)
- Hardness results for PAC learning from crypto using ORE
  - Threshold class. More "natural" classes?
  - iO, mmaps(functional enc.), NIZKs
  - Standard assumptions?

Questions? 

Bibliography I

[BKM17] Dan Boneh, Sam Kim, and Hart William Montgomery.
Private Puncturable PRFs From Standard Lattice Assumptions.
IACR Cryptology ePrint Archive, 2017:100, 2017.

[BSW06] Dan Boneh, Amit Sahai, and Brent Waters.
Fully Collusion Resistant Traitor Tracing with Short Ciphertexts and Private Keys.
In Serge Vaudenay, editor, *EUROCRYPT*, volume 4004 of *Lecture Notes in Computer Science*, pages 573–592. Springer, 2006.

[BZ16] Mark Bun and Mark Zhandry.
Order-Revealing Encryption and the Hardness of Private Learning.
In Eyal Kushilevitz and Tal Malkin, editors, *TCC (A1)*, volume 9562 of *Lecture Notes in Computer Science*, pages 176–206. Springer, 2016.

Bibliography II

[CC17] Ran Canetti and Yilei Chen.
Constraint-hiding Constrained PRFs for NC1 from LWE.
IACR Cryptology ePrint Archive, 2017:143, 2017.

[CFNP94] Benny Chor, Amos Fiat, Moni Naor, and Benny Pinkas.
Tracing Traitors, 1994.

[DNR$^+$09] Cynthia Dwork, Moni Naor, Omer Reingold, Guy N. Rothblum, and Salil P. Vadhan.
On the complexity of differentially private data release: efficient algorithms and hardness results.
In Michael Mitzenmacher, editor, *STOC*, pages 381–390. ACM, 2009.

[KMUZ16] Lucas Kowalczyk, Tal Malkin, Jonathan Ullman, and Mark Zhandry.
Strong Hardness of Privacy from Weak Traitor Tracing.
In Martin Hirt and Adam D. Smith, editors, *TCC (B1)*, volume 9985 of *Lecture Notes in Computer Science*, pages 659–689, 2016.

Bibliography III

[NY89] Moni Naor and Moti Yung.
Universal One-Way Hash Functions and their Cryptographic Applications.
In David S. Johnson, editor, *STOC*, pages 33–43. ACM, 1989.

[Rom90] John Rompel.
One-Way Functions are Necessary and Sufficient for Secure Signatures.
In Harriet Ortiz, editor, *STOC*, pages 387–394. ACM, 1990.