Lecture 3. Reconstruction Attacks (Part 2)

- Recap on linear reconstruction attacks.
- Reconstruction Attacks w/ less queries
- More ~~-~~ Computationally efficient attacks
- Reconstruction Attack in practice. (Reading)

Logistics: Office Hour Friday 9-10 am est

Music: What to play before class?

Linear Reconstruction Attack

- Introduced by Dinur & Nissim in 2003

Name	Postal Code	Age	Sex	Has Disease?
Alice	02445	36	F	1
Bob	02446	18	M	0
Charlie	02118	66	M	1
⋮	⋮	⋮	⋮	⋮
Zora	02120	40	F	1

Z : identifiers — Secret bit

Identifiers	Secret
z_1	s_1
z_2	s_2
z_3	s_3
⋮	⋮
z_n	s_n

← abstraction

Release count statistics : # people satisfy some property

- How many people $\underbrace{\text{are older than 40}}_{\varphi(z_j)}$ & have secret bit $=1$?

$$f(x) = \sum_{j=1}^{n} \varphi(z_j)\, s_j \qquad \text{for some } \varphi : Z \longmapsto \{0,1\}$$

$$f(x) = \underbrace{(\varphi(z_1), \varphi(z_2), \dots, \varphi(z_n))}_{\text{bit vector } \in \{0,1\}^n} \cdot \underbrace{(s_1, \dots, s_n)}_{\text{secret bits}}$$

Releasing k linear Statistics

Released Statistics

$$\begin{bmatrix} f_1(X) \\ \vdots \\ f_k(X) \end{bmatrix} = \underbrace{\begin{bmatrix} \varphi_1(z_1) & \cdots & \varphi_1(z_n) \\ \vdots & F_i & \vdots \\ \varphi_k(z_1) & \cdots & \varphi_k(z_n) \end{bmatrix}}_{F} \begin{bmatrix} s_1 \\ \vdots \\ s_n \end{bmatrix}$$

Secret bits

F : query matrix

$$f_i(X) = \underbrace{\boxed{F_i}}_{\text{query}} \cdot s$$

Examples :

$\varphi_1(z_j) = 1$: z_j is older than 40

$\varphi_2(z_j) = 1$: z_j is older than 40 and male

$\varphi_3(z_j) = 1$: z_j is older than 20 and male

First Reconstruction Attack

"You can't release all count statistics with non-trivial accuracy." if "privacy-preserving"

Queries: $\boxed{k = 2^n}$

For every $v \in \{0,1\}^n$, $F_v = v$

Reconstruction:

True answer Released answer

Suppose the answers $(a_v)_{v \in \{0,1\}^n}$, $\forall v \in \{0,1\}^n$, $\boxed{|F_v \cdot s - a_v| \le \alpha n}$

$\alpha = 5\%$

$\boxed{\text{Choose } \tilde{s} \in \{0,1\}^n}$, $\forall v$, $\boxed{|F_v \cdot \tilde{s} - a_v| \le \alpha \cdot n}$

Constraints.

Theorem. $\|s - \tilde{s}\|_1 \le 4\alpha n$

reconstruct 80% of secrets.

$\alpha = 5\%$

Theorem. If all $\boxed{2^n}$ counts are within αn error, then $s, \tilde{s}$ disagree on $\leq$ 4αn bits.

$\leq 20\%$

Reconstruction Using Fewer Queries

Released Statistics << 2^n .

Attack : Choose $\boxed{k = 20n}$ (linear in n) random $\varphi_i : Z \mapsto \{0,1\}$, $\forall i \in [k]$.

$\Rightarrow$ k random vectors/queries $F_i \in \{0,1\}^n$ $\leftarrow$ each bit is random

Suppose that answers : $\forall i \in [k], \quad |F_i \cdot s - a_i| \le \alpha n$

Find $\tilde{s} \in \{0,1\}^n$ such that: $\forall i \in [k], \quad |F_i \cdot \tilde{s} - a_i| \le \alpha n$

Theorem. $\|s - \tilde{s}\|_1 \le 256\,\alpha^2 n^2$.
with high probability

Theorem. If we ask $\boxed{O(n)}$ random queries $F \in \{0,1\}^n$ and all answers have error $\boxed{\le \alpha n}$, then reconstruct $\tilde{S}$ such that $\boxed{\|S - \tilde{S}\|_1 \le O(\alpha^2 n^2)}$.

previously $O(n)$

Implication $\rightarrow$

$\alpha n << \sqrt{n}$, then reconstruct a linear fraction of S.

$\alpha = 10\%$ $\quad \alpha n \le \frac{\sqrt{n}}{10}$

$(\alpha n)^2 = \frac{n}{100}$

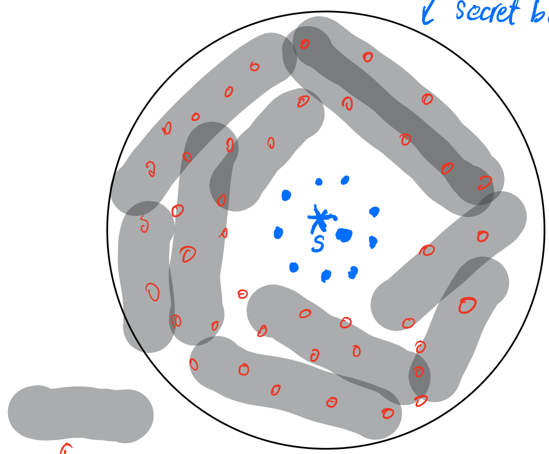
Claim: $\sqrt{n} \approx$ sampling error.

Remark: Don't exactly need random queries

Diverse / orthogonal queries

Proof Idea.

Space of secret bit vectors



given by random queries

• good $\tilde{s}$: $\|s-\tilde{s}\|_1 \le \alpha^2 n^2$

o bad $\tilde{s}$: $\|s-\tilde{s}\|_1 > \alpha^2 n^2$

Reconstruction Method

Given queries $F_1, \dots, F_k$, ← random

answers $a_1, \dots, a_k$

Find $\boxed{\tilde{s} \in \{0,1\}^n}$ that minimizes

max error → $\boxed{\max_{i \in \{1,\dots,k\}}} \; |\underbrace{F_i \cdot \tilde{s} - a_i}_{\text{error w.r.t released answer.}}|$

Output $\tilde{s}$.

Recall :

$$\max_i | F_i \cdot s - a_i | \le \alpha n$$

S is arbitrary placeholder.

Proof Idea.

① $\tilde{s}$ satisfies

$$\max_i \left| F_i \cdot \tilde{s} - a_i \right| \le \underline{\alpha n}$$

② $\tilde{s}$ is eliminated if

$\exists F_i$ s.t. $\underline{|F_i \cdot \tilde{s} - a_i|} > \alpha n$

($\tilde{s}$ is eliminated by F_i)

③ For every bad $\tilde{s}$,

Some random query eliminates $\tilde{s}$ with high probability.

Reconstruction Method

Given queries $F_1, \dots, F_k$,

answers $a_1, \dots, a_k$

Find $\tilde{s} \in \{0,1\}^n$ that minimizes

$$\max_{i \in \{1,\dots,k\}} \left| F_i \cdot \tilde{s} - a_i \right|$$

Output $\tilde{s}$.

Proof.

$$\mathbb{P}(\exists \text{ some bad } \tilde{s} \text{ not eliminated})$$

"there exists"

$$\le \sum_{\text{bad } \tilde{s}} \mathbb{P}[\tilde{s} \text{ not eliminated})$$

$$\mathbb{P}[\tilde{s} \text{ not eliminated}]$$

$$= \mathbb{P}[\forall i, \tilde{s} \text{ is not eliminated}]$$

"for all"

$$= \mathbb{P}[\tilde{s} \text{ not eliminated by } F_i]^k$$

$$\le \underbrace{\mathbb{P}[\,|F_i \cdot \tilde{s} - F_i \cdot s| \le 42n]}_{\le \frac{9}{10}}{}^k \boxed{\le} \left(\frac{9}{10}\right)^k \le 2^{-2n}$$

Key Step to be shown

Reconstruction Method

Given queries $F_1, \ldots, F_k$,

answers $a_1, \ldots, a_k$

Find $\tilde{s} \in \{0,1\}^n$ that minimizes

$$\max_{i \in \{1,\ldots,k\}} |F_i \cdot \tilde{s} - a_i|$$

Output $\tilde{s}$.

$k = 20n$.

Proof.

Key Lemma.

bad candidate

If $s, \tilde{s} \in \{0,1\}$ s.t.

$\|s - \tilde{s}\|_1 = m$ think $\gg 2^2 n^2$ (differ on m coordinates)

Let $F \in \{0,1\}^n$ be random,

then

$$\mathbb{P}\left[\,|F \cdot (s-\tilde{s})| \le \frac{\sqrt{m}}{10}\right] \le \frac{9}{10}$$

$$\mathbb{P}\left[\,\underbrace{|F \cdot (s-\tilde{s})| > \frac{\sqrt{m}}{10}}_{\text{sufficient prob. mass}}\right] > \frac{1}{10}.$$

Intuition:

$t = s - \tilde{s} \in \{-1, 0, 1\}^n$

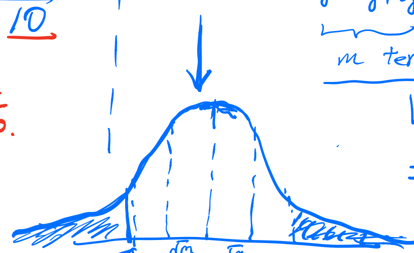
If $t_j = 1$,

$$F_j t_j = \begin{cases} 1 & \text{w.p. } \frac{1}{2} \\ 0 & \text{w.p. } \frac{1}{2} \end{cases}$$

If $t_j = -1$

$$F_j t_j = \begin{cases} -1 & \text{w.p. } \frac{1}{2} \\ 0 & \end{cases}$$

$$F \cdot t = \underbrace{\sum_{j:\, s_j \ne \tilde{s}_j}}_{m \text{ terms}} F_j t_j$$



$$\begin{aligned} &\mathrm{Var}(F \cdot t) \\ &= \mathrm{Var}\left(\sum_j F_j \cdot t_j\right) \\ &= \sum_j \underbrace{\mathrm{Var}(F_j \cdot t_j)}_{\frac{1}{4}} \\ &= \frac{m}{4} \end{aligned}$$

Efficient Reconstruction.

Reconstruction Method

Given queries $F_1, \dots, F_k$, ← linear in n

answers $a_1, \dots, a_k$

Find $\boxed{\tilde{s} \in \{0,1\}^n}$ that minimizes → 2^n search

$$\max_{i \in \{1,\dots,k\}} |F_i \cdot \tilde{s} - a_i|$$

↑ Exactly solving it is NP-hard.

Output $\tilde{s}$.

Approximation: Replace $\hat{s} \in [0,1]^n \rightarrow$ linear Program. (HW?)

Round $\hat{s} \rightarrow \tilde{s} \in \{0,1\}^n$

Linear Programming

$$\boxed{\max_{x \in \mathbb{R}^d} \; c \cdot x} \leftarrow \text{linear.}$$

s.t.

$$\boxed{\forall i \in [k], \; v_i \cdot x \le b_i}$$

↑ Can solve in $\boxed{\text{polynomial time.}}$

poly(n, d).

Attacking Diffix

private analytics product by Aircloak

Check out the Diffix Challenge!

```
SELECT COUNT(*) FROM loans
WHERE loanStatus = 'C'
AND clientId BETWEEN 2000 and 3000
```

Client ID	Loan Status
2000	1
⋮	0
⋮	⋮
3000	1

Identifiers →

Secret ← bits

```
SELECT COUNT(*) FROM loans
WHERE loanStatus = 'C'
AND (clientId = 2007
OR clientId = 2018
...
OR clientId = 2991)
```

$$\boxed{\text{Count query} \quad \sum_{iD=2000}^{3000} \text{LoanStatus}(iD)}$$

Add noise to answer according to "effective length"

$\rightarrow \Omega(\sqrt{n})$

Attack by Kobbi Nissim & Aloni Cohen 2018.

```
SELECT COUNT(clientId) FROM loans
WHERE FLOOR(100 * ((clientId * 2)^.7))
    = FLOOR(100 * ((clientId * 2)^.7) + 0.5)
AND clientId BETWEEN 2000 and 3000
AND loanStatus = 'C'
```

$(\times \text{prime})^{8}$

- "Random" Queries
- Small length.

Dick- Joseph- Schutzman. 2020.