# EECS 575: Advanced Cryptography
# Fall 2021
# Lecture 5

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

# Agenda for this lecture

- Announcements
- Recap from last time
- One-wayness of the Rabin collection
- Statistical and computational indistinguishability
- Pseudorandom generators

# Agenda for this lecture

- Announcements
- Recap from last time
- One-wayness of the Rabin collection
- Statistical and computational indistinguishability
- Pseudorandom generators

# Announcements

- Homework 2 is due ~~9/22~~ 9/20
- Lecture topic vote

Lattices
verif. comp
FHE
blockchains
zkSNARKs

# Agenda for this lecture

- Announcements
- Recap from last time
- One-wayness of the Rabin collection
- Statistical and computational indistinguishability
- Pseudorandom generators

# Recap from last time

$\mathbb{Z}_N$ : integers $+, \cdot \bmod N$

$\mathbb{Z}_N^*$ mult. subgroup. $\mathbb{Z}_N^* = \{x : \gcd(x, N) = 1\}$

$|\mathbb{Z}_N^*| = \phi(N)$ ← mult, so if $N = pq$

$QR_N^* = \{y \in \mathbb{Z}_N^* : \exists x \text{ s.t. } y = x^2 \bmod N\}$

$\phi(N) = \phi(p)\phi(q)$
$= (p-1)(q-1)$
$= 4\text{-to-}1$ function

Every elt of $QR_N^*$ has 4 square roots

$x \in \mathbb{Z}_N^* = \{(x \bmod p, x \bmod q)$
$-(x \bmod p, -x \bmod q)$
$-(-x \bmod p, x \bmod q)$
$-(-x \bmod p, -x \bmod q)\}$

All lead to $y$ when squared

CRT: $\mathbb{Z}_N^* \cong \mathbb{Z}_p^* \times \mathbb{Z}_q^*$

# One-wayness of the Rabin collection

$f_N(x) = x^2 \bmod N$ ← OWF collection

Exercise: Define as OWF coll'n

**Theorem:** Let $\mathcal{S}$ be the parameter sampler of the collection. If factoring is hard w.r.t. $\mathcal{S}$, then $f_N(x)$ is a OWF.

**Proof:** By reduction. Suppose $\mathcal{I}$ breaks Rabin with non-negl probability:

$$\Pr_{\substack{N \leftarrow \mathcal{S}(1^n) \\ x \leftarrow \mathbb{Z}_N^*}} [\mathcal{I}(y = x^2 \bmod N, N) \in \sqrt{y} \bmod N] > \frac{1}{p(n)}$$

Build $\mathcal{I}'$ that factors $N$

# One-wayness of the Rabin collection

$f_N(x) = x^2 \bmod N$

**Theorem:** Let $\mathcal{S}$ be the parameter sampler of the collection. If factoring is hard w.r.t $\mathcal{S}$, then $f_N(x)$ is a OWF.

**Proof:** $\mathcal{I}$ breaks Rabin: $\mathcal{I}(y, N) = \sqrt{y} \bmod N$ w/ non-negl prob.

Build $\mathcal{I}'$ as follows:

$\mathcal{I}'(N)$:

$x_1 \leftarrow \mathbb{Z}_N^*$

$x_2 \leftarrow \mathcal{I}(x_1^2 \bmod N, N)$

If $x_1 \neq \pm x_2$:

$p \leftarrow \gcd(x_1 - x_2, N)$

Ret $p$

Else Fail

(1) $\Pr[\mathcal{I}'(N) = p, q]$

(2) why does this work?

# One-wayness of the Rabin collection

$\mathcal{I}'(N)$:

$x_1 \leftarrow \mathbb{Z}_N^*$

$x_2 \leftarrow \mathcal{I}(x_1^2 \bmod N, N)$

If $x_1 \neq \pm x_2$:

  $p \leftarrow \gcd(x_1 - x_2, N)$

  Ret $p$

Else Fail

$\Pr[\mathcal{I}'(N) \text{ wins}] \geq \frac{\Pr[\mathcal{I}(x,N) \in \sqrt{x} \bmod N]}{2}$

$\geq \frac{1}{2 \cdot p(\eta)}$

why does this work?

we know $x_1^2 = x_2^2 \bmod N$

$\rightarrow (x_1 - x_2)(x_1 + x_2) = 0 \bmod N$

But $x_1 \neq \pm x_2 \bmod N$

$\rightarrow x_1 - x_2 \not\equiv 0 \bmod N$ and $x_1 + x_2 \not\equiv 0 \bmod N$

$N \mid (x_1 - x_2)(x_1 + x_2)$

$\gcd(N, x_1 - x_2) > 1$

So $\gcd(N, x_1 - x_2)$ is either $p$ or $q$ ☒

# Agenda for this lecture

- Announcements
- Recap from last time
- One-wayness of the Rabin collection
- Statistical and computational indistinguishability
- Pseudorandom generators

# Indistinguishability

Statistical distance between $X$ and $Y$: ← dists

$$\Delta(X,Y) := \sup_{A \subseteq \Omega} |X(A) - Y(A)|$$

$A \subseteq \Omega$ ← set of possible events

$A$: subset of events

(1) $\sup_{A \subseteq \Omega} |X(A) - Y(A)|$

$= \sup_{\bar{A} \subseteq \Omega} |X(\bar{A}) - Y(\bar{A})|$

(2) $\Delta(X,Y) = \frac{1}{2} \sum_{\omega \in \Omega} |X(\omega) - Y(\omega)|$

(3) Statistical dist. is a metric:

Reflexive: $\Delta(X,X) = 0$

Symmetric: $\Delta(X,Y) = \Delta(X,Y)$

# Indistinguishability

$U_n$ = unif. dist over $n$-bit strings

(3) Statistical dist. is a metric:

Reflexive: $\Delta(X,X)=0$ Symmetric: $\Delta(X,Y) = \Delta(Y,X)$

Subadditive: $\Delta(X,Y) \le \Delta(X,Z) + \Delta(Y,Z)$

Statistical indistinguishability: a/k/a ensembles

Let $\{X_n\}_{n\in\mathbb{N}}$ and $\{Y_n\}_{n\in\mathbb{N}}$ be sequences of dists.

Then $X$ and $Y$ are stat. ind. if

$$\Delta(X_n, Y_n) = \text{negl}(n) \quad \forall n$$

E.g. take $X_n = U_n$, $Y_n$ = unif. over $\{0,1\}^n \setminus \{0^n\}$.

Claim: Let $X = \{X_n\}$ $Y = \{Y_n\}$. Then $X \approx_s Y$.

# Computational Indistinguishability

Stat. ind. allows inefficient "tests"

Comp. ind. : restrict to efficient tests

$$Adv_{X,Y}(A) = |Pr[A(X)=1] - Pr[A(Y)=1]|$$

nuppt

output 1 is convenient

"guesses X correctly"

"guesses X incorrectly"

# Computational Indistinguishability

$$Adv_{X,Y}(A) = |Pr[A(x)=1] - Pr[A(y)=1]|$$

Let $X = \{X_n\}$ and $Y = \{Y_n\}$ be ensembles, where $X_n$ and $Y_n$ are dists over $\{0,1\}^{\ell(n)}$ for $\ell(n) = poly(n)$.

Say $X$ and $Y$ are comp. ind. [$X \approx_c Y$] if

$$Adv_{X_n,Y_n}(A) = negl(n) \quad \forall n, \forall nuppt\ A$$

(1) Composition Lemma: Let $B$ be nuppt. If $X \not\approx_c Y$, then $B(X) \not\approx_c B(Y)$

# Computational Indistinguishability

**Hybrid Lemma:** Let $X^i = \{X_n^i\}$ for $i \in [m]$, $m = poly(n)$ be ensembles. If $X^i \approx_c X^{i+1}$ for $i \in [m-1]$, then $X^1 \approx_c X^m$

"triangle inequality" for comp. ind.

extreme ensembles

# Hybrid Lemma

# Agenda for this lecture

- Announcements
- Recap from last time
- One-wayness of the Rabin collection
- Statistical and computational indistinguishability
- Pseudorandom generators

# Pseudorandom generators