CSE 575: Advanced Cryptography
Fall 2024
Lecture 5

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Rabin’s OWF collection
- Proving one-wayness of Rabin
- Computational indistinguishability

Agenda for this lecture

- Announcements
- Rabin's OWF collection
- Proving one-wayness of Rabin
- Computational indistinguishability

Announcements

- Say hello to Luke!
- HW1 now due TONIGHT at 11:59
- My office hours will be Wednesday from 10:30-11:30am

Agenda for this lecture

- Announcements
- Rabin's OWF collection
- Proving one-wayness of Rabin
- Computational indistinguishability

Rabin's function

OWF collection

$F = \{ f_s : D_s \to R_s \}_s$

- Sampler for s $\$$
- Domain Sampler $D(s) \in D_s$
- Evaluator $F(s, x) = f_s(x) \quad \forall s, x$

- Easy to sample $s + x$
- Easy to evaluate
- $\forall$ nuPPT $\mathcal{I}$,

$$\left\{ \Pr_{\substack{s \leftarrow \$ \\ x \leftarrow D(s)}} [\mathcal{I}(s, f_s(x)) \in f_s^{-1}(f_s(x))] = \text{negl}(n) \right\}$$

Thm:

$\exists$ OWFs iff $\exists$ owf collections

Rabin's function

- Sampler $S(1^n)$:

  $p, q \leftarrow \Pi_n$

  Ret $p \cdot q$

  $\Pi_n = \{x \text{ prime and } x < 2^n\}$

- Sampler $D(N)$:

  $X \leftarrow \{1, \ldots, N-1\}$

  Ret X

- Evaluator $f_N(X)$: $X^2 \bmod N$

Four Properties:

1. Easy to sample S
2. Easy to sample $D(S)$
3. Easy to evaluate
- Hard to invert

Agenda for this lecture

- Announcements
- Rabin's OWF collection
- Proving one-wayness of Rabin
- Computational indistinguishability

Factoring => Rabin is OWF

- Sampler $\$(1^n)$:
  $p, q \leftarrow \Pi_n$
  Ret $p \cdot q$
- Sampler $D(N)$:
  $X \leftarrow \{1, \ldots, N-1\}$
  Ret X
- Evaluator $f_N(x)$: $x^2 \bmod N$

$\forall$ nuPPT $\mathcal{F}$
$\Pr[\mathcal{F}(N) = (p,q) \text{ s.t. } N = pq] = \text{negl}(n)$
$N \leftarrow \$$

Lemma: Let $N = pq$.
Given $x_1, x_2 \in \mathbb{Z}_N^*$
such that $x_1^2 = x_2^2 \bmod N$
but $x_1 \neq \pm x_2$,
can factor.

Thm: If factoring is hard w/r/t $\$$, then Rabin is owf collection for $\$$

Proof:
By reduction:
Assume $\exists$ inverter for Rabin that wins w/ non-negl prob.
use this inverter to factor

Factoring => Rabin is OWF

Lemma: Let $N = pq$.

Given $x_1, x_2 \in \mathbb{Z}_N^*$ such that $x_1^2 = x_2^2 \bmod N$ but $x_1 \neq \pm x_2$, can factor. (compute $\gcd(x_1 + x_2, N)$)

Proof:

$x_1^2 = x_2^2 \Rightarrow$

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

$$(x_1 - x_2)(x_1 + x_2) = 0 \bmod p$$

$$(x_1 - x_2)(x_1 + x_2) = 0 \bmod q$$

(a, b) x_1

$(-a, b)$ x_2 $x_1 = x_2 \bmod q$ So,

$(a, -b)$

$(-a, -b)$

a^2, b^2

$(p \mid (x_1 - x_2)$ or $p \mid (x_1 + x_2))$

and $(q \mid (x_1 - x_2)$ or $q \mid (x_1 + x_2))$

Take $p \mid (x_1 + x_2) \Rightarrow \gcd(x_1 + x_2, N) = p$ ☒

Factoring => Rabin is OWF

Assume Rabin not owf. $\exists \mathcal{I}, p$ s.t. $\Pr_{\substack{s \leftarrow \$ \\ x \leftarrow D(s)}}[\mathcal{I}(s, f_s(x)) \in f_s^{-1}(f_s(x))] = \text{negl}(n)$

$\Pr[\mathcal{I} \text{ wins inversion game}] \geq 1/p(n)$

Build the following $F^{\mathcal{I}}$ to factor:

$F^{\mathcal{I}}(N)$:

$x_1 \leftarrow \{1, \ldots, N-1\}$

$y = x_1^2 \bmod N$

$x_2 \leftarrow \mathcal{I}(y, N)$

if $x_1 \neq \pm x_2$:

  Ret $\gcd(x_1 + x_2, N)$

Ret $\perp$

$\Pr[F^{\mathcal{I}}(N) = (p, q) \text{ s.t. } N = pq]$

$N \leftarrow \$$

$\geq \Pr[F^{\mathcal{I}} \text{ wins} \mid \mathcal{I} \text{ wins}] \Pr[\mathcal{I} \text{ wins}]$

$\Pr[F^{\mathcal{I}} \text{ wins} \mid \mathcal{I} \text{ wins}] = 1/2$

$\Pr[\mathcal{I} \text{ wins}] \geq 1/p(n)$

$\geq \frac{1}{2p(n)}$

$\square$

Factoring => Rabin is OWF

If Rabin owF, then factoring hard

¬Factoring hard => ¬Rabin owF

Exercise

2^{n}

$2^{\sqrt[3]{n}}$

Agenda for this lecture

- Announcements
- Rabin's OWF collection
- Proving one-wayness of Rabin
- Computational indistinguishability

Indistinguishability

Computational Indistinguishability

Pseudorandom generators