CS 120: Introduction to Cryptography

Salil Vadhan and Alon Rosen Oct. 19, 2006

Lecture Notes 9:

Collections of One-Way Functions

Recommended Reading.

- Katz-Lindell 8.4.4, 8.5.4, 8.5.5

1 Definition

Definition 1 $\mathcal{F} = \{f_{\mathsf{key}} : D_{\mathsf{key}} to R_{\mathsf{key}}\}_{\mathsf{key} \in \mathcal{K}}$ *is a* collection of one-way functions *if:*

1. *There is a PPT $G(1^n)$ which outputs a key* $\mathsf{key} \in \mathcal{K}$
2. *Given* key*, one can sample uniformly from D_{key} in polynomial time.*
3. *Given* key *and $x \in D_{\mathsf{key}}$, one can evaluate $f_{\mathsf{key}}(x)$ in polynomial time.*
4. *For every (nonuniform) PPT A, there is a negligible function ε such that*

$$\Pr\left[A(1^n, K, f_K(X)) \in f_K^{-1}(f_K(X))\right] \leq \varepsilon(n) \qquad \forall n$$

where the probability is taken over $K \xleftarrow{R} G(1^n)$, $X \xleftarrow{R} D_{\mathsf{key}}$, and the coin tosses of A.

If for every key*, $D_{\mathsf{key}} = R_{\mathsf{key}}$ and f_{key} is a permutation, then we call $\mathcal{F}$ a* collection of one-way permutations.

- (1) = we can choose a function of the family efficiently by choosing a key key. (Note that the keys are not necessarily integers.)
- (2) = we can select an input at random. (Note that this condition wasn't necessary for a OWF because a OWF takes strings as inputs.)
- (3) = each function is easy to compute in the forward direction.
- (4) = each function is hard to invert on a random input. The key key is given to the adversary since it should also be able to evaluate the function f_{key}.

2 The RSA Functions

Keys $\mathcal{K} = \{(N, e) : N = p \cdot q$ where p and q are primes, $||p|| = ||q||$ and $e \in \mathbb{Z}^*_{\phi(N)}\}$

Generation The PPT $G(1^n)$ does as follows :

- Generate random n-bit primes p, q
- Let $N = pq$

- Generate random $e \stackrel{R}{\leftarrow} \mathbb{Z}^*_{\phi(N)}$, i.e. $gcd(e, \phi(N)) = 1$
- Output (N, e)

Function $f_{N,e} : \mathbb{Z}^*_N \to \mathbb{Z}^*_N$ given by $f_{N,e}(x) = x^e \bmod N$.

Proposition 2 *RSA is a collection of permutations*

Proof: For each $\mathsf{key} = (N, e)$, $D_{\mathsf{key}} = R_{\mathsf{key}}$. To show that each $f_{N,e}$ is a permutation, we will give the inverse map. $e \in \mathbb{Z}^*_{\phi(N)}$ so there exists d such that $ed \equiv 1 \pmod{\phi(N)}$. We claim that $y \mapsto y^d \bmod N$ is the inverse map:

$$(f_{N,e}(x))^d \equiv (x^e)^d \equiv x^{ed} \equiv x \pmod{N}.$$

The key point is that exponents work modulo $\phi(N)$. ■

Proposition 3 *RSA is a collection of one-way functions* only if *the Factoring Assumption holds.*

The Factoring Assumption is therefore a necessary condition for RSA to be a collection of one-way functions. The converse ("if the Factoring Assumption holds, then RSA is a collection of OWFs") is still open.

3 Rabin's Functions

Keys $\mathcal{K} = \{N : N = p \cdot q$ where p and q are primes and $||p|| = ||q||\}$

Generation The PPT $G(1^n)$ generates random n-bit primes p, q and outputs $N = p \cdot q$.

Function $f_N : \mathbb{Z}^*_N \to \mathbb{Z}^*_N$ given by $f_N(x) = x^2 \bmod N$.

Note that this is *not* a special case of RSA because 2 and $\phi(N)$ are *not* relatively prime.

Proposition 4 *Rabin's collection is a collection of one-way functions* if and only if *the Factoring Assumption holds.*

Proof: We'll show the "if" direction. Suppose there were a PPT adversary A inverting Rabin's collection with nonnegligible probability $\varepsilon(n)$, where the probability is taken over the choice of N, x and the coin tosses of A. We'll convert A into a PPT adversary A' which factors with probability $\varepsilon(n)/2$.

Define $A'(N)$ as follows:

1. Choose $x \stackrel{R}{\leftarrow} \mathbb{Z}^*_N$.
2. Let $z = x^2 \bmod N$.
3. Let $y \stackrel{R}{\leftarrow} A(z, N)$.
4. Output $\gcd(x - y, N)$.

When N is the product of two random n-bit primes, then $A'(N)$ feeds A the same distribution as when trying to invert Rabin's collection. When A succeeds, we have

$$(x + y)(x - y) \equiv x^2 - y^2 \equiv 0 \pmod{N} \Rightarrow N | (x - y)(x + y)$$

This means that:

- both p and q are factors of $x+y$, i.e. $N|(x+y)$
- OR both p and q are factors of $x-y$, i.e. $N|(x-y)$.
- OR one is a factor of $x+y$ and the other is a factor of $x-y$.

Hence $\gcd(x-y, N) \in \{p, q\}$ provided that $y \not\equiv \pm x \pmod{N}$. This event happens with probability $1/2$ if A has found a square root of z (because there are four square roots of z and A has no information about which one is x). This analysis shows that A' factors a random N with probability $\varepsilon(n)/2$.

■

Note that Rabin's functions are *not* permutations because the map f_N is 4 to 1. We can obtain permutations by restricting to $p \equiv q \equiv 3 \pmod{4}$ and considering $f_N : \mathrm{QR}_N \to \mathrm{QR}_N$.

4 Modular Exponentiation

Keys $\mathcal{K} = \{(p, g) : p \text{ is prime and } g \text{ is a generator of } \mathbb{Z}_p^*\}$.

Generation $G(1^n)$ generates a random n-bit prime p together with a random generator g of $\mathbb{Z}_p^*$ and outputs (p, g).

Function $f_{p,g} : \mathbb{Z}_{p-1} \to \mathbb{Z}_p^*$ given by $f_{p,g}(x) = g^x \bmod p$.

The inversion problem is : given (p, g, y), output x such that $x = \log_g y$. This is the Discrete Log Problem, for which the fastest known algorithm has running time $\exp\left(O(n^{1/3}(\log n)^{2/3})\right)$.

Note that $f_{p,g}$ is a permutation if we identify $\mathbb{Z}_{p-1}$ and $\mathbb{Z}_p^*$ (e.g. treat $0 \in \mathbb{Z}_{p-1}$ as $p-1$).

5 Single one-way functions vs. collections

Proposition 5 *A collection of one-way functions exists iff one-way functions exist.*

Proof: $\Rightarrow$ The idea is to define $g(\mathsf{key}, x) = (\mathsf{key}, f_{\mathsf{key}}(x))$, but as a OWF takes a string as input, we will actually use coin tosses of $G(1^n)$ and D_{key}-sampler as input to g.
Let r_1 be the coin tosses of $G(1^n)$ ($\mathsf{key} = G(1^n, r_1)$). Let r_2 be the coin tosses of D_{key}-sampler (x is the output of D_{key}-sampler with coin tosses r_2). We define $f(r_1, r_2) = (\mathsf{key}, f_{\mathsf{key}}(x))$
$\Leftarrow$ Exercise. ■