COMS W4261 Introduction to Cryptography **October 11, 2005**

Lecture 11: Introduction to Cryptography

Lecturer: Tal Malkin *Scribes: Kate McCarthy, Adam Vartanian*

Summary

In this lecture we will prove that Rabin's collection and the RSA collection are both collections of one-way functions, given that the proper assumptions hold.

1 Rabin Squaring Function and the Factoring Assumption

Recall Rabin's collection $\{f_n\}_{n \in I}$ where

$I = \{n \mid n = pq, |p| = |q|, p \neq q \text{ odd primes}\}$
$f_n : \mathbb{Z}_n^* \to \mathbb{Z}_n^*$
$f_n(x) \equiv x^2 \pmod{n}$

Theorem 1 *Rabin's collection is a collection of one-way functions if and only if the Factoring Assumption holds.*

Proof:

If the Factoring Assumption does not hold, then it is not a one-way function by the corollary proven last lecture.

Assume Rabin's collection is not a collection of one-way functions.

Then there is a probabilistic polynomial time algorithm A such that

$$Prob[p, q \leftarrow \{\text{k-bit primes}\}, n = pq, x \leftarrow \mathbb{Z}_n^*, y \equiv x^2 \pmod{n}, x' \leftarrow A(n, y, 1^k) : x'^2 \equiv y \pmod{n}] \geq \delta(k)$$

where $\delta(k)$ is non-negligible.

We will construct a probabilistic polynomial time algorithm A' such that

$$Prob[p, q \leftarrow \{\text{k-bit primes}\}, n = pq \ : \ A'(n, 1^k) \in \{p, q\}] \geq \frac{\delta(k)}{2}$$

where $\delta(k)$ is non-negligible, and thus the Factoring Assumption does not hold.

Define $A'(1^k, n)$ as:

- Choose $x \in Z_n^*$ uniformly at random.
- Let $y \equiv x^2 \pmod{n}$.
- Run $A(n, y, 1^k)$ and call the output x'.
- If ${x'}^2 \equiv y \pmod{n}$, and $x' \neq \pm x \pmod{n}$, then output $gcd(x - x', n)$.
- Otherwise, output "Fail".

It is easy to see that A' is a probabilistic polynomial time algorithm.

Claim 2 *If A' does not output "Fail" then the output is a factor of n.*

Proof:

If A' does not output "Fail", then $x' \not\equiv \pm x \pmod{n}$ and ${x'}^2 \equiv y \pmod{n}$. Thus, the four roots of y are $\{x, -x, x', -x'\}$. From this, we can see that

$0 \equiv y - y \equiv x^2 - {x'}^2 \equiv (x - x')(x + x') \pmod{n}$

Which in turn shows that $n|(x - x')(x + x')$. Since $n = pq$ and p and q are primes, we have that $p|(x - x')(x + x')$ which implies that $p|(x - x')$ or $p|(x + x')$ since if a prime divides a product it must divide one of the terms. Similarly, we have that $q|(x - x')$ or $q|(x + x')$.

But it must be that p divides one and q the other:

Case 1: $p|(x + x'), q|(x - x') \implies gcd(x - x', n) = q$

Case 2: $q|(x + x'), p|(x - x') \implies gcd(x - x', n) = p$

Case 3: $p, q|(x + x') \implies n|(x + x') \implies x + x' = 0 \pmod{n}, x' = -x \pmod{n}$

Case 4: $p, q|(x - x') \implies n|(x - x') \implies x' = x \pmod{n}$

We can see that if case 3 or 4 occurs, $x \equiv \pm x' \pmod{n}$, which contracts the assumption that A' did not output "fail". Thus, one of cases 1 or 2 must occur, in which case A' will output a factor of n. Thus if A' does not output "fail" then it will output a factor of n.

■

Claim 3 *With probability* $\geq \frac{\delta(k)}{2}$*, A' does not output "Fail".*

Proof:

If $x'^2 \equiv y \pmod{n}$ (which happens with probability $\delta(k)$), then since x was chosen at random, x has equal probability to be $\pm x'$, or to be one of the other two roots.

$$Prob[A' \text{ succeeds}] = Prob[A \text{ succeeds}] \cdot Prob[A' \text{ succeeds}|A \text{ succeeds}] + Prob[A \text{ does not succeed}] \cdot Prob[A' \text{ succeeds}|A \text{ does not succeed}]$$

$Prob[A' \text{ succeeds}|A \text{ does not succeed}] = 0$, so the second term is zero. Thus we have $Prob[A' \text{ succeeds}] = Prob[A \text{ succeeds}] \cdot Prob[A' \text{ succeeds}|A \text{ succeeds}]$. Since x has equal probability to be $\pm x'$ or to be one of the other two roots, the probability that A' succeeds given that A succeeds is $\frac{1}{2}$. So, we get that

$Prob[A' \text{ succeeds}] = Prob[A \text{ succeeds}] \cdot \frac{1}{2} \geq \frac{\delta(k)}{2}$

■

By claims 2 and 3, A' outputs a factor with probability at least $\frac{\delta(k)}{2}$. Since $\delta(k)$ is non-negligible, $\frac{\delta(k)}{2}$ is also non-negligible. Therefore, Rabin's collection is a one-way function if and only if factoring is hard.

■

Note: Rabin's function is not a permutation in general, because squaring $n = pq$ is a 4-to-1 function.

If we use $p \equiv 3 \pmod{4}$, $q \equiv 3 \pmod{4}$ (in which case $n = pq$ is called a Blum integer) and restrict $f_n : QR_n \to QR_n$, then it turns out that it is a permutation. This is because, in this case, exactly one of the four square roots is itself a square.

2 RSA Candidate for One-Way Function

Definition 1 *RSA collection*

$F = \{f_{n,e}\}_{(n,e \in I)}$

$I = \{(n, e) \mid n = pq, |p| = |q|, p \neq q \text{ odd primes}, gcd(e, \phi(n)) = 1\}$

$f_{n,e} : \mathbb{Z}_n^* \to \mathbb{Z}_n^*$

$f_{n,e}(x) \equiv x^e \pmod{n}$

Note that an RSA function uses $n = pq$ as in Rabin, but a different exponent e, chosen at random such that $gcd(e, \phi(n)) = 1$, or equivalently, $e \in \mathbb{Z}_{\phi(n)}^*$. Note that e cannot be 2 (because $2|\phi(n)$), so Rabin's function is not a special case of RSA.

Claim 4 *RSA is a collection of permutations.*

Proof:

We'll show that for all (n, e), $f_{n,e}$ has an inverse function $f_{n,e}^{-1}$.

$f_{n,e}^{-1}(y) \equiv y^d \pmod{n}$ where d is such that $de \equiv 1 \pmod{\phi(n)}$ (since $e \in \mathbb{Z}_{\phi(n)}^*$, d exists and can be found efficiently given $\phi(n)$).

$f_{n,e}^{-1}$ is an inverse function:

$f_{n,e}^{-1}(f_{n,e}(x)) \equiv f_{n,e}^{-1}(x^e) \equiv (x^e)^d \equiv x^{ed} \equiv x^1 \pmod{n}$

So, RSA is a permutation.

■

It is believed to be hard to efficiently compute the inverse given only n and e. This is captured in the following.

Definition 2 *RSA Assumption*

For all probabilistic polynomial time algorithms A, there exists a negligible $\epsilon(k)$ such that

$$Prob[p, q \leftarrow \{\text{k-bit primes}\}, e \leftarrow \mathbb{Z}^*_{\phi(n)}, x \leftarrow \mathbb{Z}^*_n, y \equiv x^e \pmod{n} \\ : A(n, y, 1^k) = x] \leq \epsilon(k)$$

We remark that sometimes instead of choosing e at random, the RSA function is used with $e = 3$. This requires a stronger RSA assumption using $e = 3$.

Theorem 5 *RSA is a collection of one-way permutations if the RSA Assumption holds.*

Proof:

As proven above, RSA is a collection of permutations, and by the RSA assumption, RSA is a collection of one-way functions.

■

Theorem 6 *If the Factoring Assumption is false, then RSA is not a one-way permutation.*

Proof:

If the Factoring Assumption is false, then n may be efficiently factored into p and q (with non-negligible probability). Given p and q, $\phi(n) = (p-1)(q-1)$ can be computed efficiently, and thus d such that $de \equiv 1 \pmod{\phi(n)}$ can be computed efficiently and the function can be inverted.

■

Note that the RSA assumption is not known to be equivalent to the Factoring Assumption. This is, as far as we know, it is possible that the Factoring Assumption holds (ie, it is hard to factor) but the RSA assumption doesn't (ie, it is easy to take eth roots). This is in contrast to the Rabin collection, which we proved in Theorem 1 is equivalent to factoring.