# Cryptography

Lecture 6

Lecture by Dr. Alon Rosen
Typeset by Steven Karas

2019-04-30
Last edited 18:04:30 2019-04-30

**Disclaimer** These notes are based on the lectures for the course Cryptography, taught by Dr. Alon Rosen at IDC Herzliyah in the spring semester of 2018/2019. Sections may be based on the lecture slides prepared by Dr. Alon Rosen.

## 1 Recap

## 2 Agenda

- Chinese Remainder Theorem - Quadratic Residues

## 3 Chinese Remainder Theorem - Quadratic Residues

Consider the field of $\mathbb{Z}_N$, and the subset $\mathbb{Z}_N^*$ of those elements with multiplicative inverses. The quadratic remainder $QR_N \triangleq \{x^2 \bmod N \mid x \in \mathbb{Z}_N^*\}$.

$$|QR_p| = \frac{|\mathbb{Z}_p^*|}{2} = \frac{(p-1)}{2}$$

$$N = pq \qquad |QR_N| = \frac{|\mathbb{Z}_N^*|}{4}$$

$$x \bmod N \longleftrightarrow (x \bmod p,\ x \bmod q)$$

## 4 Overview

Perfect security requires $|\mathcal{K}| = |\mathcal{C}|$. Computational security relaxes this to negligible probability. Pseudorandom generators provide computational security. One way functions provide pseudorandom generators.

## 5 Collections of OWFs

Define $F$ as:

$$F = \{f_{\text{neg}} : D_{\text{key}} \to D_{\text{key}}\}$$

$F$ is a collection of OWFs if it satisfies the following conditions:

1. there exists a PPT $G(1^n)$ that outputs $k \in \mathcal{K}$
2. given $k$ we can sample $x \leftarrow D_k$ in polytime
3. given $k$ and $x \in D_k$ we can evaluate $f_k(x)$ in polytime
4. for any PPT $A$ there is a negligible probability such that:

$$\Pr_{k \xleftarrow{R} G(1^n)} [A(1^n, k, f_k(x)) \in f_k^{-1}(f_k(x))] \leq \varepsilon(n)$$

## 5.1 RSA as a OWP

RSA is a collection of one way permutations.

$$k = \{(N, e) \mid N = p \cdot q \;\; p, q \text{ are primes } \; |p| = |q|\}$$
$$e \in \mathbb{Z}^*_{\varphi(N)}$$

The invention of RSA was based on finding a one-way function, which they had issues with until a seder pesah when Rivest went home after and invented it. Adi Shamir has had visa issues with the US in recent years, to the point of having his visa denied when he was invited to give a talk at the NSA. Notably, RSA were not the first to discover this, but the GCHQ classified the paper that discovered it first.

### 5.1.1 Key generation

1. $p, q \xleftarrow{R} n$-bit primes
2. $N = pq$
3. $e \xleftarrow{R} \mathbb{Z}^*_{\varphi(N)}$
4. output $(N, e)$

### 5.1.2 Encryption/Decryption

$$f_{N,e} : \mathbb{Z}^*_N \to \mathbb{Z}^*_N$$

$$f_{N,e}(x) = x^e \mod N$$

### 5.1.3 Proof as a OWP

$$\forall k = (N, e), \quad D_k = R_k$$

To show $f_{N,e}$ is a permutation, we give $f^{-1}_{N,e}$.
$e \in \mathbb{Z}^*_{\varphi(N)}$, so $\exists d$ such that $ed \equiv 1 \mod \varphi(N)$ so $y \mapsto y^d \mod N$ is the inverse map.

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

Note that:

$$x^{ed} = x^{k\varphi(N)+1} = x^{\varphi(N)^k} \cdot x = 1^k \cdot x$$

However, if it's easy to factorize integers, then it's easy to find $\varphi(pq)$, and from there to find $d$ given $e$. As such, our proof that RSA is a collection of OWPs is contingent on that. Note that this means that factoring is at least as hard as RSA because RSA reduces to factoring.

## 5.2 Rabin's function

Rabin was one of the founding faculty members of IDC, and taught algorithms/automata for the first two years of the CS school.

$$k = \{N \mid N = pq \;\; \ldots\}$$

$$f_N : \mathbb{Z}^*_N \to \mathbb{Z}^*_N$$

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

Rabin is a collection of OWFs iff the factoring assumption holds.

### 5.2.1 Proof of equivalence to factoring

Assume towards contradiction that a PPT $A$ exists that inverts $f_N$ with probability $\varepsilon(N)$. We will use $A$ to factor $N$ with probability $\varepsilon(N)/2$.

$A'(N)$ is defined as follows:

1. $x \xleftarrow{R} \mathbb{Z}^*_N$
2. $z = x^2 \mod N$
3. $y = A(z, N)$
4. output $\gcd(x - y, N)$

When $A$ succeeds (with probability $\varepsilon(N)$):

$$(x + y)(x - y) = x^2 - y^2 \equiv 0 \mod N$$

This implies that ${}^N|(x + y)(x - y)$. This means that one of the following is true:

1. Both $p, q$ are factors of $(x + y)$
2. Both $p, q$ are facotrs of $(x - y)$
3. one is a factor of $(x + y)$ and the other of $(x - y)$.

Hence, $\gcd(x - y, N) \in \{P, Q\}$ provided that $x \neq \pm y \mod N$.

#### 5.2.2 Example

Let $P = 3,\ Q = 5.\ N = 15.\ QR_3 = \{1\}$, and $QR_5 = \{1, 4\}$
$\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$, and $\varphi(15) = 8 = (3 - 1)(5 - 1)$.
$QR_{15} = \{1, 4\}$
Note that the mapping $\mathbb{Z}_{15}^* \to QR_{15}$ pairs off $x, y \in \mathbb{Z}_{15}^*$ such that $x + y = N$, and $f_N(x) = f_N(y)$.

# 6 Modular Exponentiation

Keys $\mathcal{K} = \{(p, q) \mid p$ is prime and $g$ is a generator of $\mathbb{Z}_p^*\}$
Let $f_{p,g} : \mathbb{Z}_{p-1} \to \mathbb{Z}_p^*$. Note that $|\mathbb{Z}_{p-1}| = p - 1 = |\mathbb{Z}_p^*|$.

$$f_{p,g}(x) = g^x \mod p$$

The fastest algorithm for this runs in $2^{n^{1/3}}$, whereas the SOTA for elliptic curves runs in $(2^{n/2})$, where $n$ is the number of bits, not the size of the field.

# 7 OWF implies PRG

Note that this is an OWF if RSA holds, yet it is not a PRG:

$$f'_{N,e}(x) = 1, x^e \mod N$$

# 8 Hard-core bits

Consider subset sum:

$$f(x_1, \ldots, x_n, S) = (x_1, \ldots, x_n, \sum_{i \in S} x_i)$$

a function $b : \{0, 1\}^* \to \{0, 1\}$ is a hardcore bit for a given OWF f if:

1. $b$ is polytime computable
2. any PPT $A$ has a negligible $\varepsilon$ such that:

$$\Pr_x[A(f(x)) = b(x)] \leq \frac{1}{2} + \varepsilon$$

**Example of real hardcore bits:**

- RSA: $lsb_{N,e} : \mathbb{Z}_N^* \to \{0, 1\}$
- RSA: $half_N(x) = \begin{cases} 0 & 0 \leq x \leq N/2 \\ 1 & \text{else} \end{cases}$
- Rabin: $lsb_N : \mathbb{Z}_N^* \to \{0, 1\}$
- modexp: $half_{p-1}(x) \qquad g^x \mod p$

## 8.1 Goldreich-Levin

Let $f$ be any OWF. Define $f'(x, r) = f(x), r$. Then $< x, r > \mod 2$ is a hardcore bit for $f'$, where:

$$< x, r >= \sum_{i=1}^{n} x_i r_i \mod 2$$

This is equivalent to the Hadamard local decoding code.

# 9 Next lecture

Next weeks lecture will be cut short due to Erev Yom HaZikaron.

# References

[1] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography, Second Edition.* Chapman & Hall/CRC, 2nd edition, 2014.