Cryptography
Lecture 5

Lecture by Dr. Alon Rosen
Typeset by Steven Karas

2019-04-02
Last edited 18:11:37 2019-04-02

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

Last week we covered pseudorandom generators that provide computational security:

An encryption scheme (G, E, D) satisfies computational security if for any probabilistic polytime adversary A there exists some negligible function ε such that:

$$|\Pr[A(G(U_n)) = 1] - \Pr[A(U_{\ell(n)}) = 1| < \varepsilon(n)$$

Where $\ell(n)$ is the expansion of the original n-bit key of the PRG to $\ell(n)$-bit output.

PRGs as one-way functions PRGs can be considered to be one-way functions. Define the following language:

$$L_G = \{y \in \{0,1\}^{\ell(n)} \mid \exists x \in \{0,1\}^n,\ G(x) = y\}$$

Note that L_G is in $\mathcal{NP}$, because if we are given x, it serves as a witness.

2 Agenda

- One way functions
- Number theory

3 One way functions

A one-way function f is a function where:

$$x \overset{\text{"easy"}}{\longmapsto} f(x)$$
$$f(x) \overset{\text{"hard"}}{\longmapsto} f^{-1}(f(x))$$

As such, when we are given $(x, f(x))$, we can easily verify the computation, yet when only given $f(x)$, it is not easy.

3.1 Formal Definition

$f : \{0,1\}^* \to \{0,1\}^*$ is a one-way function if:

1. f can be evaluated in polytime[1].
2. For any PPT A there exists a negligible ε such that:

$$\Pr[A(f(U_n), 1^n) \in f^{-1}(f(U_n))] \leq \varepsilon(n)$$

[1]This is the asymptotic version. The concrete version is that a function is t, ε one-way function if it runs in concrete time t

3.2 Inverting OWFs

The following are sufficient definitions of

1. Find some preimage (not necessarily the same input as the original)
2. with probability $1/\operatorname{poly}(n)$
3. For infinitely many ns

Observations:

1. $|f(x) \leq \operatorname{poly}(|x|)$
2. $A(f(x)) = x$ is too demanding for A. e.g for $f(x) = |x|$,

$$\Pr[A(f(x)) = x] \leq 2^{-n}$$

.

3. We need to give A a second input: 1^n. For example, $f(x) = |x|$ would not succeed because it wouldn't be able to even write x, because $\operatorname{poly}(|x|) \ll |x|$.

3.3 Candidate OWFs

No one really has a good idea of a sufficient characteristic of a OWF, but low-degree functions are pretty well known to be bad.

3.3.1 Multiplication

$$f(x, y) = x \cdot y \qquad |x| = |y|$$

In this case, note that the inputs must be padded to conform to input length restrictions.

Factoring assumption For any PPT A, there exists a negligible ε such that:

$$\Pr[A(N) \in \{P, Q\}] \leq \varepsilon(n)$$

Where P, Q are random n-bit primes and $N = PQ$.
If the factoring assumption holds, then multiplication is a OWF.

3.3.2 Subset sum

$$f(\overset{\{0,1\}^n}{x_1}, \ldots, x_n, S) = (x_1, \ldots, x_n, \sum_{i \in S} x_i \mod 2^n)$$

Note that because the expected unpadded length of any x_i is $n-1$, we expect the sum to wrap around on average $n/2$ times.

3.3.3 Others

$$f(k) = \mathrm{DES}_k(0^{64})$$

$$f(k) = \mathrm{AES}_k(0^{128})$$

3.4 Limitations of OWFs

1. if $f : \{0,1\}^n \to \{0,1\}^\ell$ is computable in time t_0 then it is not $(O(2^n t_0), 1)$-one-way
2. $f : \{0,1\}^n \to \{0,1\}^\ell$ cannot be $(O(n), \max\{\frac{1}{2^n}, \frac{1}{2^\ell}\})$-one-way

Consider a random guessing adversary: $A(z)$ outputs $y \in_R \{0,1\}^n$:

$$\begin{aligned}
\Pr[A(f(x)) \in f^{-1}(f(x))] &= \Pr_{x,y}[y \in f^{-1}(f(x))] \\
&= \Pr_{x,y}[f(x) = f(y)] \\
&\geq \frac{1}{2^n} \text{ (prob that } x = y)
\end{aligned}$$

$$\begin{aligned}\Pr_{x,y}[f(x)=f(y)] &= \sum_{z\in\{0,1\}^\ell} \Pr[f(x)=z \;\&\; f(y)=z] \\ &= \sum_{z\in\{0,1\}^\ell} \Pr[f(x)=z]\cdot\Pr[f(y)=z] \\ &= \sum_{z\in\{0,1\}^\ell} \Pr[f(x)=z]^2 \\ &\geq \frac{1}{2^\ell}\end{aligned}$$

This shows why it's a good idea for both the input and output to be long.

4 Computational Number Theory

4.1 Sampling random prime numbers

The naive approach is to simply randomly sample numbers and check if they are prime. Fortunately, prime numbers are common, and we can efficiently check if they are prime. As a matter of fact, the number of primes smaller than x is approximately $\frac{x}{\ln x}$.

So how do we sample a random n-bit prime number in poly(n) time?

1. $x \xleftarrow{R} \{2^{n-1},\ldots,2^n-1\}$
   (a) $x' \xleftarrow{R} \{0,1\}^{n-1}$
   (b) $x \leftarrow 1x'$
2. Test if x is prime.
   (a) $\Pr[\text{success}] = x/\ln x/x = \frac{1}{\ln 2^n} = \Omega(\frac{1}{n})$
   (b) $L = [\#\text{ attempts}] = O(n)$

4.2 Modular arithmetic

$x \equiv y \mod n$ iff $^N|(x-y)$

$$x \bmod N \stackrel{\text{def}}{=} [\text{unique } x' \in \{0,\ldots,N-1\}\ x \equiv x' \pmod N]$$

$\mathbb{Z}_N = \{0,\ldots,N-1\}$ with arithmetic $(+,\cdot)$ mod$N$

4.3 Greatest common divisor

$\gcd(a,b)$ every divisor of a and b divides $\gcd(a,b)$.

For example, if we consider $A = PQ$ and $B = QR$, then $\gcd(A,B) = Q$.

The extended GCD is: $\forall x,y \in \mathbb{N}\ \exists a,b \in \mathbb{Z}$ such that $ax+by = gcd(x,y)$. This can be found in polytime.

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

These are the elements in $\mathbb{Z}_N$ with multiplicative inverses. If $\gcd(x,N) = 1$, then $\exists a,b \in \mathbb{Z}$ such that $ax+bN = 1$. Take $x^{-1} = a$ then $ax = 1 \mod N$.

Example:

$$N = 15 = 5\cdot 3$$

$$8 \in \mathbb{Z}_{15}^*$$

$$8^{-1} = 2 \mod 15$$

$$8\cdot 2 = 16 = 1 \mod 15$$

$$a\cdot 8 + b\cdot 15 = 1$$

$$2\cdot 8 + -1\cdot 15 = 1$$

4.4 Euler phi function

$$\phi(N) = |\mathbb{Z}_N^*| = N \cdot \prod_{\text{primes}^P | N} (1 - \frac{1}{P}) \geq \frac{N}{6 \log\log N}$$

For any prime number P, $\phi(P) = P - 1$. For any prime numbers P, Q:

$$\begin{aligned}\phi(PQ) &= \phi(P) \cdot \phi(Q) = (P-1)(Q-1) \\ &= N - 1 - (P-1) - (Q-1) \\ &= PQ - P - Q + 1\end{aligned}$$

We don't have enough time to cover the rest of this section, so check the official lecture notes.

4.5 Chinese Remainder Theorem

Let $N = PQ$ with $\gcd(P, Q) = 1$. Then the map $x \mapsto (x \bmod P, x \bmod Q)$ from $\mathbb{Z}_N$ to $\mathbb{Z}_P \times \mathbb{Z}_Q$ is 1-1 and onto.

In particular, $\forall y, z \in \mathbb{Z}_P \times \mathbb{Z}_q$, $\nexists x \in \mathbb{Z}_N$ such that $x \equiv y \mod P$ and $x \equiv z \mod Q$. Moreover, note that $|\mathbb{Z}_P \times \mathbb{Z}_Q| = PQ = N = |\mathbb{Z}_N|$.

Proof We will describe the inverse mapping. By extended gcd we can find $a, b \in \mathbb{Z}$ such that $\underbrace{aP}_{c} + \underbrace{bQ}_{d} = 1$.

$$\begin{array}{llll} c \equiv 1 & (\text{mod } P) & d \equiv 0 & (\text{mod } P) \\ c \equiv 0 & (\text{mod } Q) & d \equiv 1 & (\text{mod } Q) \end{array}$$

Inverse map $(y, z) \mapsto x = cy + dz \mod N$:

$$\begin{aligned} cy + dz \equiv 1 \cdot y + 0 \cdot z \equiv y \quad (\text{mod } P) \\ cy + dz \equiv 0 \cdot y + 1 \cdot z \equiv z \quad (\text{mod } Q) \end{aligned}$$

5 Next lecture

There will not be a lecture next week due to national elections. There will not be a lecture for the two weeks after due to holidays.

References

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