EE 720: An Introduction to Number Theory and Cryptography (Spring 2018)

Lecture 21 — April 6, 2018

Instructor: Saravanan Vijayakumaran *Scribe: Saravanan Vijayakumaran*

1 Lecture Plan

- El Gamal Encryption
- RSA Encryption

2 Recap

Definition. *A **public-key encryption scheme** is a triple of probabilistic polynomial-time algorithms* ($\texttt{Gen}$, $\texttt{Enc}$, $\texttt{Dec}$) *such that:*

1. *The key-generation algorithm takes 1^n as input and outputs a pair of keys (pk, sk). The first key is called the **public key** and the second key is called the **secret key** or **private key**.*
2. *The encryption algorithm $\texttt{Enc}$ generates the ciphertext $c \leftarrow \texttt{Enc}_{pk}(m)$*
3. *For ciphertext c, the decryption algorithm uses the private key sk to output a message $m = \texttt{Dec}_{sk}(c)$ or error indicator $\perp$.*

- Consider the following experiment $\texttt{PubK}^{\texttt{eav}}_{\mathcal{A},\Pi}(n)$:
  1. $\texttt{Gen}(1^n)$ is run to obtain keys (pk, sk).
  2. The adversary $\mathcal{A}$ is given pk and outputs a pair of arbitrary messages $m_0, m_1 \in \mathcal{M}$ with $|m_0| = |m_1|$.
  3. A uniform bit $b \in \{0, 1\}$ is chosen. Ciphertext $c \leftarrow \texttt{Enc}_{pk}(m_b)$ is computed and given to $\mathcal{A}$. This ciphertext c is called the *challenge ciphertext*.
  4. $\mathcal{A}$ outputs a bit b'.
  5. The output of the experiment is defined to be 1 if $b' = b$, and 0 otherwise. We write $\texttt{PubK}^{\texttt{eav}}_{\mathcal{A},\Pi}(n) = 1$ if the output of the experiment is 1 and in this case we say that $\mathcal{A}$ succeeds.

Definition. *A public-key encryption scheme $\Pi = (\texttt{Gen}, \texttt{Enc}, \texttt{Dec})$ has **indistinguishable encryptions in the presence of an eavesdropper** if for all probabilistic polynomial-time adversaries $\mathcal{A}$ there is a negligible function $\texttt{negl}$ such that, for all n,*

$$\Pr\left[\texttt{PubK}^{\texttt{eav}}_{\mathcal{A},\Pi}(n) = 1\right] \leq \frac{1}{2} + \texttt{negl}(n).$$

Proposition. *If a public-key encryption scheme has indistinguishable encryptions in the presence of an eavesdropper, it is CPA-secure.*

3 El Gamal Encryption

Define a public-key encryption scheme as follows:

- $\texttt{Gen}$: On input 1^n run $\mathcal{G}(1^n)$ to obtain (G, q, g). Then choose a uniform $x \in \mathbb{Z}_q$ and compute $h = g^x$. The public key is $\langle G, q, g, h \rangle$ and the private key is $\langle G, q, g, x \rangle$. The message space is G.
- $\texttt{Enc}$: On input a public key $pk = \langle G, q, g, h \rangle$ and message $m \in G$, choose a uniform $y \in \mathbb{Z}_q$ and output the ciphertext $\langle g^y, h^y \cdot m \rangle$.
- $\texttt{Dec}$: On input a private key $sk = \langle G, q, g, x \rangle$ and ciphertext $\langle c_1, c_2 \rangle$, output $\hat{m} = c_2 / c_1^x$.

Theorem. *If the DDH problem is hard relative to $\mathcal{G}$, then the El Gamal encryption scheme is CPA-secure.*

4 RSA Encryption

- Given a composite integer N, the factoring problem is to find integers $p, q > 1$ such that $pq = N$.
- One can find factors of N by *trial division*, i.e. exhaustively checking if p divides N for $p = 2, 3, \ldots, \lfloor \sqrt{N} \rfloor$. But trial division has running time $\mathcal{O}\left(\sqrt{N} \cdot \texttt{polylog}(N)\right) = \mathcal{O}\left(2^{\|N\|/2} \cdot \|N\|^c\right)$ which is exponential in the input length $\|N\|$.

4.1 The Factoring Assumption

- Let $\texttt{GenModulus}$ be a polynomial-time algorithm that, on input 1^n, outputs (N, p, q) where $N = pq$, and p and q are n-bit primes except with probability negligible in n.
- **The factoring experiment** $\texttt{Factor}_{\mathcal{A},\texttt{GenModulus}}(n)$:
  1. Run $\texttt{GenModulus}(1^n)$ to obtain (N, p, q).
  2. $\mathcal{A}$ is given N, and outputs $p', q' > 1$.
  3. The output of the experiment is 1 if $N = p'q'$, and 0 otherwise.
- **Definition: Factoring is hard relative to** $\texttt{GenModulus}$ if for all PPT algorithms $\mathcal{A}$ there exists a negligible function $\texttt{negl}$ such that $\Pr[\texttt{Factor}_{\mathcal{A},\texttt{GenModulus}}(n) = 1] \leq \texttt{negl}(n)$.
- The **factoring assumption** states that there exists a $\texttt{GenModulus}$ relative to which factoring is hard.

4.2 Plain RSA

- Let $\texttt{GenRSA}$ be a PPT algorithm that on input 1^n, outputs a modulus N that is the product of two n-bit primes, along with integers $e, d > 1$ satisfying $ed = 1 \bmod \phi(N)$.

- If we chose $e > 1$ such that $\gcd(e, \phi(N)) = 1$, then the multiplicative inverse d of e in $\mathbb{Z}_N^*$ will satisfy the required conditions.

- Define a public-key encryption scheme as follows:

  - `Gen`: On input 1^n run $\texttt{GenRSA}(1^n)$ to obtain N, e, and d. The public key is $\langle N, e\rangle$ and the private key is $\langle N, d\rangle$.
  - `Enc`: On input a public key $pk = \langle N, e\rangle$ and message $m \in \mathbb{Z}_N^*$, compute the ciphertext $c = m^e \bmod N$.
  - `Dec`: On input a private key $sk = \langle N, d\rangle$ and ciphertext $c \in \mathbb{Z}_N^*$, output $\hat{m} = c^d \bmod N$.

5 References and Additional Reading

- Sections 11.1,11.2.1 from Katz/Lindell
- Sections 11.4.1,8.2.3,11.5.1 from Katz/Lindell