CS 346 Class Notes

Mark Lindberg

May 2, 2016

Last Time:
LSB = Least Significant Bit.
Theorem 11.31. If RSA is hard relative to GenRSA, then for all PPT $\mathcal{A}$,

$$\Pr[\mathsf{RSA\text{-}LSB}_{\mathcal{A},\mathsf{GenRSA}}(n) = 1] \leq \frac{1}{2} + \mathtt{negl}(n).$$

Saw how to compute the 2SB of x when $\mathrm{LSB}(x) = 0$.
Given N, e, y, with $y = x^e$. Then let $z = \frac{x}{2}$. Then $y' = z^e = y \cdot 2^{-e}$.
This Time:
2 more days...
Recommended exercises.
Today: When $\mathrm{LSB}(x) = 1$... Formulas.
PKE for single-bit messages. (Without using the random oracle model.)
Construction 11.32.

- Gen: As in plain RSA. $\mathsf{GenRSA} \to (N, e, d)$, $pk = (N, e)$, $sk = (N, d)$.
- Enc: Input $pk, m \in \{0, 1\}$. Pick a random $r \in \mathbb{Z}_N^*$ such that $\mathrm{LSB}(r) = m$. Set $c = r^e$.
- Dec: Input sk, c. Get $r = c^d$. Output $m := \mathrm{LSB}(r)$.

Theorem 11.33: If RSA problem is hard relative to GenRSA, then construction 11.32 is CPA-secure. This follows easily from theorem 11.31.
Main result of this section:
CPA-secure KEM based on the RSA assumption, with no random oracle needed.
Construction 11.14.

- Gen: Run $\mathsf{GenRSA}(1^n)$ to get (N, e, d) and $\phi(N)$. Compute $d' = d^n \mod \phi(N)$. Set $pk = (N, e)$, $sk = (N, d')$.
- Encaps: On input pk and 1^n, choose c, uniformly at random, from $\mathbb{Z}_N^*$. For $i = 1$ to n

    1. Compute $k_i = \mathrm{LSB}(c_i)$.

2. Set $c_{i+1} = c_i^e$

Output ciphertext c_{n+1}, and $k = k_1 \dots k_n$.

- Decaps: On input $sk = (N, d')$ and ciphertext c, let $c_1 = c^{d'}$. For $i = 1$ to N

  1. $k_i = \text{LSB}(c_i)$.
  2. $c_{i+1} = c_i^e$.

  Output $k = k_1 \dots k_n$.

  Reason for correctness: $c_1 = c_2^d = c_3^{d^2} = \dots = c_{n+1}^{d^n} = c_{n+1}^{d^n \bmod \phi(N)} = c_{n+1}^{d'}$.

Theorem 11.35. If RSA is hard relative to GenRSA, then construction 11.34 is CPA-secure.
Chapter 12: Digital Signature Schemes.

- Public-key analogue of a MAC.
- Provides integrity.
- Provides other important properties such as
  - Public verifiability.
  - Transferability.
  - Non-repudiation.

12.2 Definitions.
(Gen, Sign, Vrfy). Key Generation, signing, verification.

- Gen: On input 1^n produces (pk, sk) (Even number $\geq n$ bits).
- Sign: On input $\underline{sk}$, and a message m, produces A signature σ. $\sigma \leftarrow \text{Sign}_{sk}(m)$.
- Vrfy: On input pk, message m, and signature σ, $\text{Vrfy}_{pk}(m, \sigma)$ outputs 1 if it accepts the message, and 0 else.

Definition of sigforge.
Definition 12.2
Section 12.3.
Theorem 12.4.
Section 12.4.
12.4.1. Plain RSA (NOT secure.)