Tel Aviv University 31/12/2016

Introduction to Modern Cryptography (0368.3049) – Ex. 5

Benny Chor and Orit Moskovich

Submission in singles or pairs to Orr Fischer's Schreiber mailbox (289) until 16/1/2017, 23:59 (IST)

- Appeals/missing grade issues: bdikacs AT gmail.com
- Issues regarding missing/unchecked assignments will be addressed only if a soft copy will be submitted on time to: crypto.f16 AT gmail.com.
Subject of the email: Ex.5, ID

1. **Signatures and One Way Permutations.** Let f be a one-way permutation. Consider the following signature scheme for messages in the set $\{1, ..., n\}$:

   - Key generation algorithm Gen: choose random $x \leftarrow \{0,1\}^n$ and set $y = f^n(x)$, where $f^n(x) = f(f^{n-1}(x))$ and $f^0(x) = x$. The public key is $pk = y$, and the private key is $sk = x$.
   - To sign message $m \in \{1, ..., n\}$ output $\sigma = f^{n-m}(x)$.
   - To verify signature σ on message $m \in \{1, ..., n\}$ with respect to public key y, check whether $y = f^m(\sigma)$.

   (a) Show that the above is not a one-time signature scheme. Given a signature on a message m, for what messages $m' \neq m$ can an adversary efficiently produce a forgery?

   (b) Prove that if $f : \{0,1\}^n \to \{0,1\}^n$ is a OWP, and k is polynomial in n, then f^k is also a OWP.

   (c) Prove that no PPT adversary, given as input a signature of m, can output a forgery on any message $m' > m$ (except with negligible probability).

   (d) Suggest how to modify the scheme to obtain a one-time signature scheme. Supply a short textual argument explaining the correctness of your construction (no formal proof required) .

   Hint: Include two values y, y' in the public key.

2. **One Time Signatures.** A strong one-time signature scheme satisfies the following (informally): given a signature on a message m, it is infeasible to output $(m', \sigma') \neq (m, \sigma)$ for which σ' is a valid signature on m' (note that $m = m'$ is now allowed, as long as $\sigma' \neq \sigma$).

   Show a one-way function f for which Lamport's scheme is not a strong one-time signature scheme.

3. **Signatures.** Recall the sequential multi-message stateful signature scheme described in the recitation and in class 9, based on a one-time signature scheme $(Gen, Sign, Ver)$.

- Initially one-time keys are sampled $(sk_0, vk_0) \leftarrow Gen$.
- Before signing a message the ith message m_i, the signer's state $state_{i-1}$ includes:
  (a) All previous messages $m_1, ..., m_{i-1}$
  (b) Previous one-time signing and verification keys $sk_0, ..., sk_{i-1}$ and $vk_0, ..., vk_{i-1}$
  (c) Previous one-time signatures $\sigma_1, ..., \sigma_{i-1}$

  To sign m_i, the signer first samples a new pair of one-time keys (sk_i, vk_i). Then, it computes a signature $\sigma_i = Sign_{sk_{i-1}}(m_i, vk_i)$. It then publishes as the signature $\{vk_j, m_j, \sigma_j\}_{j \le i}$ and adds $(sk_i, vk_i, m_i, \sigma_i)$ to the current state $state_{i-1}$, resulting in a new state $state_i$.
- The signature is verified by verifying all signatures along the chain: $\{Ver_{pk_{j-1}}(m_j, vk_j, \sigma_j)\}_{j \le i}$

Show that any attacker A that breaks (ε, t)-existential-unforgeability of the scheme, can be converted to A' that runs roughly in the same time as A, breaks $(\varepsilon/(t+1), 1)$-existential-unforgeability of the underlying one-time scheme.

4. **Zero-knowledge for Quadratic-Residousity.** Let $N = pq$ be a product of two primes, and let $QR = \{r^2 : r \in \mathbb{Z}_N^*\}$ denote the subgroup of quadratic residues in $\mathbb{Z}_N^*$. Consider the following protocol for proving quadratic-residousity.

   A protocol for proving quadratic residousity $(P(x), V)(y)$

   Common Input: $y \in QR$.

   Private Input of P: x such that $y = x^2 \mod N$.

   - $P \to V$: P samples a uniformly random $r \leftarrow \mathbb{Z}_N^*$, and sends $z = r^2 \pmod N$ to V.
   - $P \leftarrow V$: V samples a uniformly random bit $b \leftarrow \{0, 1\}$, and sends b to P.
   - $P \to V$: If $b = 0$, P sends $a_0 = r$ to V. If $b = 1$, P sends $a_1 = xr \pmod N$ to V.
   - If $b = 0$, V accepts iff $a_0^2 = z \pmod N$. If $b = 1$, V accepts iff $a_1^2 = zy \pmod N$.

   (a) **Soundness:** Assume $y \notin QR$. Show that for any prover P^* (even computationally unbounded) , the probability that V accepts is $\le 1/2$.

   (b) **Zero-knowledge against honest verifiers:** Show how to efficiently generate a perfect simulation of the view of an honest verifier. Concretely, show that there exists a polytime algorithm $S(y, b)$ that given $y \in QR$, and $b \in \{0, 1\}$, efficiently samples a first message $\tilde{z}$ and a third message $\tilde{a}_b$, such that $(\tilde{z}, b, \tilde{a}_b)$ has the exact same distribution as the messages (z, b, a_b) produced in a real execution of the protocol, where V uses the coin b.

5. **Shamir's Secret Sharing.** Using Sage, set up a system for 3-out-of-6 secret sharing scheme over the finite field $\mathbb{Z}_{11}$. Generate two different quadratic polynomials $f(x), g(x)$ that have different free terms $f(0) \neq g(0)$, yet $f(i) = g(i)$ for $i = 1, 2$. In class 11, we argued that the secret can be expressed as a linear combination of the shares. Demonstrate this for two sets of participants: $\{1, 2, 4\}$ and $\{1, 2, 5\}$. For each set, compute explicitly the coefficients for extracting the secret. For example, in case of the first set, you should find the coefficients b_1, b_2, b_4 such that $h(0) = b_1 h(1) + b_2 h(2) + b_4 h(4)$ for every degree 2 polynomial. Find such coeffcients c_1, c_2, c_5 for the second set of participants as well. Demonstrate that for the specific $f(x), g(x)$ chosen above, your linear combinations indeed work.

6. **ElGamal encryption and Secret Sharing.** The ElGamal public-key encryption system (presented in lecture 8) operates over $\mathbb{Z}_p^*$, where p is a large prime, the factorization of $p-1$ is known, and $p-1$ has a large prime factor. The secret key is an integer, a, chosen uniformly at random in the interval $[0, p-2]$. Let g be a multiplicative generator of $\mathbb{Z}_p^*$, and $\beta = g^a \pmod{p}$. The public key is $p, g, \beta = g^a \pmod{p}$. A (probabilistic) encryption of $m \in Z_p$, using a randomly chosen integer $k \leftarrow [0, p-2]$, is of the form $E_{p,g,\beta}(m; k) = (g^k \pmod{p}, m \cdot \beta^k \pmod{p})$.

   (a) The owner of the secret key, $sk = a$, wishes to delegate decryption to his n class mates, by giving each of them a share sk_i of the secret key. It is required that, for each and every encrypted message, decryption is possible only if **all** n class mates are actively involved in the process. Specifically, to decrypt a given ciphertext c, each classmate i create (using the public key, c, sk_i, and possibly some locally generated random bits) a c-*designated* decryption key $sk_{i,c}$, such that given all $\{sk_{i,c}\}_{i \in [n]}$, it is possible to decrypt c. Any proper subset of classmates, $S \subsetneq [n]$, should not be able to break the encryption, even given their shares $\{sk_i\}_{i \in S}$. Furthermore, the decryption values $\{sk_{i,c}\}_{i \in [n]}$ for a given ciphertext, should not break the security of a new independent cipher c'.

   Describe how the El-Gamal encryption system can be extended to meet this requirement. There is no need to prove security, but only describe the construction.

   (b) **Bonus:** Describe how to achieve the same in the case that any t out of n classmates should be able to decrypt. You can use the fact that $\mathbb{Z}_p$ is a field.

We wish you all a great new 2017!