University of Maryland
CMSC858K — Cryptography
Professor Jonathan Katz

Problem Set 5

Due at *beginning* of class on April 29

1. **The Fiat-Shamir signature scheme.** Let N be a product of two large, distinct primes, let $x_1, ..., x_k \in \mathbb{Z}_N^*$ be randomly chosen, and let $y_i = x_i^2 \bmod N$ for $1 \leq i \leq k$. Consider the following public-key identification scheme in which the public key is N and $\{y_i\}$ and the secret key consists of $\{x_i\}$:

   > The prover $\mathcal{P}$ begins by choosing a random value $r \in \mathbb{Z}_N^*$ and sending $A = r^2 \bmod N$ to the verifier. The verifier chooses a challenge $b \in \{0,1\}^k$ at random. Let b_i denote the i^{th} bit of b (so $b = b_1 \cdots b_k$). The prover responds by computing $C = r \cdot \prod_{i=1}^k x_i^{b_i} \bmod N$. The verifier accepts iff $C^2 \stackrel{?}{=} A \cdot \prod_{i=1}^k y_i^{b_i} \bmod N$.

   (a) Show that verification always succeeds for an honest prover/verifier.

   (b) Prove that the identification scheme is secure against "weak" attacks if k is large (express your result as a function of k). What assumption is your proof based on?

   (c) Prove that the identification scheme is secure against passive attacks. What assumption is your proof based on?

   (d) Show how to use the Fiat-Shamir transformation to obtain a *signature scheme* from the above identification scheme.

2. **The Fiat-Shamir transformation for non-canonical identification schemes.** In class we showed that the Fiat-Shamir transformation converts a 3-round identification scheme to a signature scheme that is secure in the random oracle model.

   (a) Generalize the Fiat-Shamir transform so that it converts a 5-round identification scheme to a signature scheme. Sketch or give a full proof of security that your conversion results in a signature scheme that is secure in the random oracle model.

   (b) Generalize the Fiat-Shamir transform for $O(k)$-round identification schemes (where k is the security parameter). Note that this does *not* result in a secure signature scheme (in general). In particular, recall that we showed an $O(k)$-round identification scheme in class that was secure against a passive adversary and in which the verifier sent a 1-bit challenge each time. Show an explicit attack on the signature scheme that results if the generalized-Fiat-Shamir transformation is applied to this protocol.

   (c) Discuss why your proof from part (a) does not extend to part (b).

3. **Identity-based signatures.** In class we showed how to obtain an *identity-based* signature scheme: the master public key is a modulus N and an exponent e; the master secret key is d such that $ed = 1 \bmod \varphi(N)$. A user with identity ID is given secret key $SK_{ID} = H(ID)^d \bmod N$ (where H is modeled as a random oracle); this user can now sign messages with respect to his identity by using the Guillou-Quisquater (GQ) signature scheme (this was the scheme from Homework 4, problem 1; note that you do not actually need any details of this scheme other than to recall that the public key is N, e, y and the secret key is x for which $x^e = y$). Prove that this is indeed a secure identity-based scheme when H is a random oracle. More formally, show that an adversary who obtains the secret keys for users $ID_1, \ldots, ID_\ell$ cannot forge a signature for a user $ID' \notin \{ID_1, \ldots, ID_\ell\}$. (*Hint*: Show that an adversary who does so can be used to break the underlying GQ signature scheme.)

4. **A one-time signature scheme.** Consider the following one-time signature scheme, where f is a one-way permutation. The public key consists of ℓ values $y_1, \ldots, y_\ell$ and the secret key consists of values $x_1, \ldots, x_\ell$ where $f(x_i) = y_i$ for $1 \leq i \leq \ell$. To sign an ℓ-bit message $m_1, \ldots, m_\ell$ the signer simply sends $\{x_j\}_{m_j=1}$ (i.e., the signature contains all x_j for which the j^{th} bit of the message is 1).

   (a) Show that this is not a secure one-time signature scheme.

   (b) Classify the message pairs (m, m') for which an adversary who obtains a signature on message m *can* forge a signature on message m'. Prove that for *other* pairs (m, m') an adversary *cannot* forge a signature on m' given a signature on m.

   (c) Can you suggest a way to make the scheme secure as a one-time signature scheme using *one* additional element in the public key (and no random oracle). You should sketch why your proposed scheme is secure, but a proof is not necessary. (*Hint*: make use of the fact that f is a permutation...)