MTAT.07.003 Cryptology II
Spring 2008 / Homework 8

1. Recall that the soundness proof for the Schnorr identification protocol reduced to the task of finding two ones in the same row in a large zero one matrix. Assume that the matrix has m rows and n columns and there are at least ε-fraction of non-zero entries. Establish the following properties of the Rewind algorithm.

   (a) If the fraction of nonzero entries $\varepsilon \leq \frac{1}{n}$, there exists a matrix configuration such that no algorithm can find two ones in the same row.

   (b) Let $\mathsf{nz}(r)$ denote the number of non-zero entries in the rth row. What is the conditional probability that the Rewind algorithm halts with failure in the rth row, i.e. the output is $(r, c, \overline{c})$ and $c = \overline{c}$? What is the corresponding average failure probability $\Pr[\mathsf{Failure}]$?

   (c) Sometimes the knowledge extraction may fail even for $c \neq \overline{c}$. Let $\mathsf{bad}(r, c)$ denote the number of locations $\overline{c}$ that lead to an useless triple $(r, c, \overline{c})$. Again, express the failure probability as an averaged conditional probability such that $\Pr[\mathsf{Failure}] \leq \frac{\kappa}{\varepsilon}$, where the knowledge error κ is a solution to combinatorial optimisation problem involving only functions $\mathsf{nz}(\cdot)$ and $\mathsf{bad}(\cdot)$.

   ($\star$) Give an alternative interpretation to κ such that it can be computed more naturally without considering the optimisation task. Can it be expressed as a maximal fraction of non-zero entries such that there are no triples $(r, c, \overline{c})$ that can be used for knowledge extraction.

   (d) Consider the AND-composition of two Schnorr protocols with different secret keys. What triples reveal both secret keys? What is the corresponding knowledge error κ.

2. Consider a setting, where an adversary $\mathcal{A}$ must succeed only in one out of d proofs to cause a serious damage. Let us denote the corresponding advantage with respect to a fixed pk by

$$\mathsf{Adv}^{\mathsf{ea}}_{\mathsf{pk}}(\mathcal{A}) = \Pr[\mathcal{V}_{\mathsf{pk}} \text{ accepts a protocol instance}] \enspace ,$$

   where the instances of Schnorr protocols are executed in parallel. Namely, the prover $\mathcal{P}_*$ sends out $\alpha_1, \ldots, \alpha_d$ and honest verifier $\mathcal{V}$ replies $\beta_1, \ldots, \beta_d$ and $\mathcal{P}_*$ completes the interaction with $\gamma_1, \ldots, \gamma_d$.

   (a) Formalise the underlying extraction problem by encoding various end states with values $\{0, 1, \ldots, d\}$. What is the underlying search task in the corresponding matrix?

   (b) Modify the Rewind algorithm so that it provides solution to the problem specified above. Estimate the running time.

   (c) Estimate the failure probability of the modified Rewind algorithm. What is the expected number of probes needed to find necessary transcripts for knowledge extraction?

3. Consider a setting, where an adversary $\mathcal{A}$ must succeed only in one out of d proofs to cause a serious damage. Let us denote the corresponding advantage with respect to a fixed pk by

$$\mathsf{Adv}^{\mathsf{ea}}_{\mathsf{pk}}(\mathcal{A}) = \Pr\left[\mathcal{V}_{\mathsf{pk}} \text{ accepts a protocol instance}\right] \enspace ,$$

where the instances of Schnorr protocols are executed one by one. As a result, we can rewind the prover $\mathcal{P}_*$ algorithm in d places. We can switch each individual challenge β_i to get the revealing transcript.

   (a) Formalise the underlying extraction problem by encoding various end states with values $\{0, 1, \ldots, d\}$. Let $\mathsf{A}(r, \beta_1, \ldots, \beta_d)$ be the corresponding array. What is the underlying search task now?

   (b) Modify the Rewind algorithm so that it provides solution to the problem specified above. Estimate the running time.

   (c) Estimate the failure probability of the modified Rewind algorithm. What is the expected number of probes needed to find necessary transcripts for knowledge extraction?

4. The Guillou-Quisquater identification scheme is directly based on the RSA problem. The identification scheme is a honest verifier zero-knowledge proof that the prover knows x such that $x^e = y \mod n$ where n is an RSA modulus. More precisely, the public information $\mathsf{pk} = (n, e, y)$ and the corresponding secret is x. The protocol is following:

   1. $\mathcal{P}$ chooses $r \xleftarrow[u]{} \mathbb{Z}_n^*$ and sends $\alpha \leftarrow r^e$ to $\mathcal{V}$.
   2. $\mathcal{V}$ chooses $\beta \xleftarrow[u]{} \{0, 1\}$ and sends it to $\mathcal{P}$.
   3. $\mathcal{P}$ computes $\gamma \leftarrow rx^\beta$ and sends it to $\mathcal{V}$.
   4. $\mathcal{V}$ accepts the proof if $\gamma^e = \alpha y^\beta$.

   Prove the following facts about the Guillou-Quisquater identification scheme.

   (a) The GQ identification scheme is functional.

   (b) The GQ identification scheme has the zero-knowledge property.

   (c) The GQ identification protocol is specially sound.

   (d) Amplify the security by parallel composition. Derive the corresponding knowledge bound.
   Hint: When does the knowledge extraction fail?

5. Let $\mathbb{G}$ be a cyclic group with prime number of elements q and let g_1 and g_2 be generators of the group. Now consider a honest verifier zero-knowledge proof that the prover knows x such that $g_1^x = y_1$ and $g_2^x = y_2$. More precisely, the public information $\mathsf{pk} = (g_1, g_2, y_1, y_2)$ and the secret is x. The proof is following:

   1. $\mathcal{P}$ chooses $r \xleftarrow[u]{} \mathbb{Z}_q$ and sends $\alpha_1 \leftarrow g_1^r$ and $\alpha_2 \leftarrow g_2^r$ to $\mathcal{V}$.

2. $\mathcal{V}$ chooses $\beta \xleftarrow[u]{} \mathbb{Z}_q$ and sends it to $\mathcal{P}$.
3. $\mathcal{P}$ computes $\gamma \leftarrow x\beta + r$ and sends it to the verifier $\mathcal{V}$.
4. $\mathcal{V}$ accepts the proof if $g_1^\gamma = \alpha_1 y_1^\beta$ and $g_2^\gamma = \alpha_2 y_2^\beta$.

Prove the following facts about the sigma protocol.

(a) The protocol is functional and has the zero-knowledge property.

(b) The protocol is specially sound and two colliding transcripts indeed reveal x such that $g_1^x = y_1$ and $g_2^x = y_2$.

(c) Construct a honest verifier zero knowledge proof that the ElGamal encryption $(c_1, c_2) = \mathsf{Enc}_{\mathsf{pk}}(1)$.

($\star$) Let $\mathbb{G}$ be a cyclic group with prime number of elements q as in the previous exercise. Design a honest verifier zero-knowledge proof that the prover knows x_1 and x_2 such that $y = g_1^{x_1} g_2^{x_2}$. The latter is often used together with the lifted ElGamal encryption $\overline{\mathsf{Enc}}_{\mathsf{pk}}(x) = \mathsf{Enc}(g^x)$ that is additively homomorphic. Construct honest verifier zero-knowledge proofs for the following statements.

(a) An encryption c is $\overline{\mathsf{Enc}}_{\mathsf{pk}}(m)$ and m is known or publicly fixed.

(b) An encryption c_2 is computed as $c \cdot \mathsf{Enc}_{\mathsf{pk}}(1)$.

(c) An encryption c_2 is computed as $c_1^y \cdot \mathsf{Enc}_{\mathsf{pk}}(1)$.

(d) An encryption c_3 is computed as $c_1 \cdot c_2 \cdot \mathsf{Enc}_{\mathsf{pk}}(1)$.

6. Normally, one uses the entire message space $\mathcal{M}$ in the coin flipping protocol. That is, parties first choose $b_1, b_2 \xleftarrow[u]{} \{0,1\}^\ell \subseteq \mathcal{M}$. Next, $\mathcal{P}_1$ computes $(c, d) \leftarrow \mathsf{Com}_{\mathsf{pk}}(b_1)$ and sends c to $\mathcal{P}_2$, who replies b_2. Finally, $\mathcal{P}_1$ releases d and both parties compute $b_1 \oplus b_2$. Obviously, a malicious $\mathcal{P}_1^*$ may give different decommitment values for different replies b_2. Under the assumption that the commitment scheme is (t, ε)-binding prove the following facts.

(a) No $\frac{t}{2}$-time adversary $\mathcal{P}_1^*$ can achieve $\Pr[b_1 \oplus b_2 = 0] \geq 2^{-\ell} + \sqrt{\varepsilon}$.
Hint: Consider a simple strategy, where you provide $b_2^0, b_2^1 \leftarrow \{0,1\}^\ell$ to extract a double opening.

(b) Show that for fixed target value $y = b_1 \oplus b_2$ we can encode the search for a double opening as a matrix game. What is the difference between the standard knowledge extraction and this setting? Does it affect possible security guarantees?

(c) What happens with the success probability if one rewinds the adversary k times? What do you think which strategy is better: blind rewinding with fixed random coins or the Rewind algorithm?

(d) Let A be an efficiently detectable subset of $\{0,1\}^\ell$. Show that no $\frac{t}{2}$-time adversary $\mathcal{P}_1^*$ can achieve

$$\Pr[b_1 \oplus b_2 = 0] \geq \Pr\left[x \xleftarrow[u]{} \{0,1\}^\ell : x \in A\right] + \sqrt{\varepsilon}\ .$$