MTAT.07.003 Cryptology II
Spring 2009 / Exercise session X

Examples of Sigma Protocols

1. The Guillou-Quisquater identification scheme (GQ 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, i.e., the public information $\mathsf{pk} = (n, e, y)$ and the secret is x. The protocol itself 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 that the Guillou-Quisquater identification scheme is sigma protocol.

    (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 soundness guarantees with parallel and sequential composition and derive the corresponding knowledge bounds.

2. 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 sigma protocol for proving the knowledge of x such that $g_1^x = y_1$ and $g_2^x = y_2$, i.e., the public information is (g_1, g_2, y_1, y_2) and the secret knowledge is x. The protocol 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 that the protocol is indeed a 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 $g_2^x = y_2$.

    As a concrete application of this protocol construct a proof that the ElGamal encryption (c_1, c_2) is an encryption of $\mathsf{Enc}_{\mathsf{pk}}(1)$.

Applications of Sigma Protocols

3. Recall that in the first step of certified computations the prover $\mathcal{P}$ commits bit by bit to his or inputs $x_1, \ldots, x_n$ and uses sigma protocol to prove the validity of commitments. Use Pedersen commitments and the Schnorr protocol $\text{POK}_x\left[y = g^x\right]$ to implement this strategy.

   (a) Construct a sigma protocol $\text{POK}_{c,g}\left[\exists r : c = y^x g^r\right]$.

   (b) Construct a sigma protocol $\text{POK}_{c,g}\left[\exists d : \mathsf{Open}(c,d) \in \{0,1\}\right]$.

   (c) Use homomorphic properties of the Pedersen commitment to construct a sigma protocol for proving $x_1 + \cdots + x_n = 1$ and $x_i \in \{0,1\}$.

4. In the second phase of certified computations the prover reveals commitments to all intermediate values in the Boolean circuit. As in the previous exercise use Pedersen commitments and the Schnorr protocol $\text{POK}_x\left[y = g^x\right]$ to construct sigma protocols to prove the following facts

   (a) Values c_u and c_v are the commitments of u and v such that $v = \neg u$.

   (b) Commitments c_u, c_v c_w of u, v and w are such that $w = u \wedge v$.

   (c) Commitment c_f of f is such that $f = x_0 \wedge \neg x_1 \vee \neg x_3 \wedge x_4$.

5. Many e-voting protocols use sigma protocols to prove the correctness of several crucial steps. In particular, one often needs to prove

   (a) c is an ElGamal encryption of 0 or 1;

   (b) c is an ElGamal encryption of $x \in \left\{0, \ldots 2^\ell\right\}$;

   (c) $(c_{ij})_{i,j=1}^n$ is an Pedersen commitment to a permutation matrix.

   Use the Schnorr protocol $\text{POK}_x\left[y = g^x\right]$ and properties of ElGamal and Pedersen commitments to construct the corresponding sigma protocols.

(⋆) Let $\mathbb{G}$ be a cyclic group with prime number of elements q as in the previous exercise. Design a sigma 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 sigma protocols 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. Recall that a generic Schnorr signature $(m, \alpha, \beta, \gamma)$ is defined as follows $\alpha \leftarrow g^r$ for $r \xleftarrow[u]{} \mathbb{Z}_q$, $\beta \leftarrow h(m, \alpha)$ and $\gamma = x\beta + r$ where $y = g^x$ is the public key of a signer and x is the secret key. Consider the security of the Schnorr signature scheme against existential forgeries, where the function h is replaced with a random oracle $\mathcal{O}_h(\cdot)$ that computes uniformly chosen function from $\mathcal{F}_{\text{all}} = \{h : \mathbb{G} \times \mathcal{M} \to \mathbb{Z}_q\}$.

(a) Convert an adversary that makes at most q_h queries to random oracle $\mathcal{O}_h(\cdot)$ and succeeds with the probability ε in the key only model can be converted to an adversary $\mathcal{A}_*$, which queries each message only once from $\mathcal{O}_h$ and returns only valid signatures or halts. Show that the running times of $\mathcal{A}$ and $\mathcal{A}_*$ are comparable and $\mathcal{A}_*$ makes at most $q_h + 1$ queries.

(b) Convert $\mathcal{A}_*$ to an adversary $\mathcal{B}$ that initiates up to $q_h + 1$ Schnorr identification protocols and then finishes successfully one these identification protocols with the same probability than $\mathcal{A}_*$ succeeds in existential forgery.

(c) Look at the second type of matrix games we considered in the lectures and provide the expected number of probes needed to extract the secret key from $\mathcal{B}$ and $\mathcal{A}$.

(d) It is common to consider security in the model where adversary can use signing oracle up to g_s times. Show that each of the queries $\mathsf{Sign}(m)$ can be simulated by choosing $\beta, \gamma \leftarrow \mathbb{Z}_q$ and computing $\alpha \leftarrow g^{\gamma} y^{-\beta}$ and then defining $\mathcal{O}_h(m, \alpha) = \beta$. Why and when is this assignment consistent with the definition of random oracle?