Fundamentals of Cryptography: Problem Set 10

Due Wednesday Dec 11, 3PM

Collaboration is permitted (and encouraged); however, you must write up your own solutions and acknowledge your collaborators.

Problem 0 Read section Proving properties in zero-knowledge of Boneh & Shoup, or lecture 14, 15, 16 of course 6.875 in `mit6875.org`.

Problem 1 (18pt) Let p be a prime such that $p = 2^{O(n)}$, where n is the security parameter. Let $\mathbb{G}$ be a group of order p. Let g be a generator of $\mathbb{G}$.

Part A. Linear Relation Consider boolean formulas ϕ of the following type:

$$\phi(x_1, ..., x_n) := \left\{ \prod_{j=1}^{n} g_{1j}^{x_j} = u_1 \ \wedge \ \prod_{j=1}^{n} g_{2j}^{x_j} = u_2 \ \ldots \ \wedge \ \prod_{j=1}^{n} g_{mj}^{x_j} = u_m \right\}.$$

That is, the formula is satisfied if the m linear constraints are all satisfied. In such a formula ϕ, the g_{ij}'s and u_i's are elements of the group $\mathbb{G}$. Some of these group elements could be system parameters or even constants, while others are specific to the formula. The x_i's are the formal variables of the formula.

Let L be the language

$$L = \{(g_{1,1}, \ldots, g_{m,n}, u_1, \ldots, u_m) : \exists (x_1, \ldots, x_n) \text{ s.t. } \phi(x_1, \ldots, x_n) = \text{true}\}.$$

Design a three-message proof system which allows an efficient prover P to convince a verifier V that the given $(g_{1,1}, \ldots, g_{m,n}, u_1, \ldots, u_m)$ is in L. The prover is given the witness $(x_1, \ldots, x_n)$. The proof system should have completeness error 0 (the honest prover is always accepted by the honest verifier). The soundness error (the probability that a cheating prover can fool the verifier) should be $O(\frac{1}{p})$. And the proof system should be *honest-verifier* perfect zero-knowledge.

You should state your construction, and prove its completeness, soundness, and zero-knowledge.

Part B. Prove that your construction in part A is actually a proof of knowledge system. That is, you shoud design an efficient extractor, such that, given any prover whose completeness error is small, your extractor can extract the witness from the given prover.

Part C. DH triple Let L be the language

$$L = \{(a, b, c) : \exists (x, y) \text{ s.t. } a = g^x, b = g^y, c = g^{xy}\}.$$

Use the construction in Part A to design a three-message proof system which allows an efficient prover P to convince a verifier V that a given $(a, b, c) \in \mathbb{G}^3$ is in L. The prover is given the witness (x, y).

Part D. Encrypted DH Triple Suppose Alice is given x, y and encrypts each of g^x, g^y, g^{xy} under Bob's public key $u \in \mathbb{G}$, producing three ciphertexts $(v_1, e_1), (v_2, e_2), (v_3, e_3)$,

$$(v_1, e_1) = \mathsf{Enc}(u, g^x) = (g^{\beta_1}, u^{\beta_1} g^x)$$
$$(v_2, e_2) = \mathsf{Enc}(u, g^y) = (g^{\beta_2}, u^{\beta_2} g^y)$$
$$(v_3, e_3) = \mathsf{Enc}(u, g^{xy}) = (g^{\beta_3}, u^{\beta_3} g^{xy})$$

where $\beta_1, \beta_2, \beta_3 \in \mathbb{Z}_p$ are uniformly generated by Alice during each time of encryption. Alice, as a prover, presents these ciphertexts to a verifier Charlie, and wants to convince him that these ciphertexts really do encrypt a DH-triple, without revealing anything else.

Design a three-message proof system for Alice. (Since u is generated by Bob, no one in the proof system, including the prover (Alice), the verifier (Charlie), the simulator, is given the discrete logarithm of u.)

Part D. Encrypted Polynomial Suppose Alice has two ciphertexts (v, e) and (v', e') under Bob's public key u. The first ciphertext encrypts a group element g^x and the second encrypts $g^{x'}$. Alice wants to convince Charlie that $x' = f(x)$ for some specific polynomial $f(x) = \sum_{i=0}^{d} \lambda_i x^i$. We shall assume that the degree d and the coefficients $\lambda_0, \ldots, \lambda_d$ are fixed, public values.

Design a three-message proof system for Alice.

Part E. Encrypted Bit Suppose Alice wants to prove to Charlie that a ciphertext (v, e) is the encryption of a bit g^b under Bob's public key u for some $b \in \{0, 1\}$.

Design a three-message proof system for Alice.

Hint: See Boneh & Shoup

Problem 2 (4pt) The common reference string model is similar to the common random string model. In the common reference string model, a trusted external party samples a public string from a specific distribution (rather than from the uniform distribution).

In this problem, we construct a commitment scheme in the common reference string (CRS) model. The CRS is $\mathsf{crs} = (\mathbb{G}, g)$ where $\mathbb{G}$ is a DDH-hard group and g is a generator of $\mathbb{G}$.

The commitment phase of the commitment scheme is defined as follows:

1. The sender $\mathcal{S}$ is given a message $m \in \mathbb{Z}_p$;
2. The receiver $\mathcal{R}$ sends $h \in \mathbb{G}$ to the sender;
3. The sender $\mathcal{S}$ samples random $r \in \mathbb{Z}_p$, and sends $h^m g^r$.

Finish the protocol by describe the opening phase. Prove that this commitment protocol exhibits perfect hiding and computational binding properties.

Remark: The need of CRS can be eliminated by letting the receiver samples a DDH-hard group and proves $\exists t, h = g^t$ using a ZKP protocol.