Institut for Matematik og Datalogi
Syddansk Universitet

December 5, 2016
JFB

Cryptology – E16 – Assignment 4

Assignment due Monday, December 21, 12:15

Note that this is part of your exam project, so it must be approved in order for you to take the exam in January, and you may not work with others not in your group. If it is late, it will not be accepted (though it could become an assignment you redo). You may work in groups of two (or three). Turn in the assignment through the SDU Assignment system in Blackboard, and remember to keep your receipt. Turn in one PDF file per group.

1. In class we used the Goldwasser-Micali encryption scheme to implement bit commitments, as follows: Assume that a modulus N, which is the product of two large, equal length primes is given, along with an element $y \in \mathbb{Z}_N^*$ such that $\left(\frac{y}{N}\right) = 1$, but y is a quadratic nonresidue modulo N.

   To commit to a bit $b \in \{0, 1\}$, choose a random $r \in \mathbb{Z}_N^*$ and set $C(b, r) = y^b \cdot r^2 \pmod{N}$.

   To open a commitment $c \in J_N$ as a zero, reveal $r \in \mathbb{Z}_N^*$ such that $c = r^2 \pmod{N}$. To open a commitment $c \in J_N$ as a one, reveal $r \in \mathbb{Z}_N^*$ such that $c = y \cdot r^2 \pmod{N}$.

   (a) Show that, assuming the hardness of the QUADRES problem, these bit commitments are computationally concealing.

   (b) Show that these bit commitments are information-theoretically binding.

   (c) Show how a prover can show that two of these bit commitments are commitments to different bits, without revealing which is a commitment to a one and which is a commitment to a zero.

      i. What does the prover reveal and how does the verifier check it?

ii. Call the output revealed when showing that commitments are to different bits r. Argue that the distribution of r is the same when $(b_1, b_2) = (0, 1)$ as when $(b_1, b_2) = (1, 0)$. This means that V learns nothing except that $b_1 \neq b_2$ (assuming the quadratic residuosity assumption).

iii. Argue that if P has in fact committed in c_1, c_2 to the bit pairs $(0, 0)$ or $(1, 1)$, she cannot use this method to show that they are commitments to different bits.

(d) Show how a prover can show that two of these bit commitments are commitments to the same bit. What does the prover reveal and how does the verifier check it? (It's OK to skip writing the security arguments, but convince yourself that it is secure.)

2. Suppose that a Prover wants to convince a Verifier that it knows the factorization of a number n, which is the product of two primes p and q. Consider the following protocol repeated $\lceil \log_2 n \rceil$ times:

Prover		Verifier
		Choose random $v \in \mathbb{Z}_n^*$. Let $u \equiv v^4 \pmod{n}$.
	$\xleftarrow{u}$	
Compute a square root x of u such that x is a quadratic residue.	$\xrightarrow{x}$	
		Check that $x = v^2 \pmod{n}$. If so, continue. Otherwise, reject.

The Verifier accepts if it has not rejected in any round.

(a) Given that u is computed as $v^4 \pmod{n}$ for some $v \in \mathbb{Z}_n^*$, how many of its four square roots are also quadratic residues? Consider three cases separately:

- $p \equiv q \equiv 3 \pmod 4$.
- Exactly one of p and q is congruent to $1 \pmod 4$, and the other is congruent to $3 \pmod 4$.
- $p \equiv q \equiv 1 \pmod 4$.

For the following subproblems, assume that $p \equiv q \equiv 3 \pmod 4$.

(b) Suppose both the Prover and the Verifier follow the protocol. Can the Prover who knows the factorization of n, but otherwise can only compute using probabilistic polynomial time, efficiently find an x which is a square root of u and is a quadratic residue? If so, how? If not, why not?

(c) Why do we believe that the Verifier will reject if the Prover cannot factor n? (Give a brief answer.)

(d) Is this protocol zero-knowledge? Explain your answer.

3. Let n be the product of two large primes, p and q, where $p \equiv 1 \pmod 3$, and let $y \in \mathbb{Z}_n^*$. Suppose the Prover knows x such that $x^3 \equiv y \pmod n$. The Prover convinces the Verifier that there exists an x satisfying $x^3 \equiv y \pmod n$ by repeating the following protocol $\lceil \log_2 n \rceil$ times:

Prover		Verifier
Choose random $u \in \mathbb{Z}_n^*$. Let $v \equiv u^3 \pmod n$.		
	$\xrightarrow{v}$	
		Choose a random $c \in \{0, 1\}$.
	$\xleftarrow{c}$	
Let $z = u \cdot x^c \pmod n$.		
	$\xrightarrow{z}$	
		Check that $z^3 \equiv v \cdot y^c \pmod n$. If so, continue. Otherwise, reject.

The Verifier accepts if it has not rejected in any round.

(a) Prove that the above protocol is an interactive proof system, showing both completeness and soundness.

(b) Prove that the above protocol is perfect zero-knowledge, defining a simulator and showing that it produces the required transcripts in expected polynomial time.