Esecurity: secure internet & e-cash, summer 2012

MICHAEL NÜSKEN, RAOUL BLANKERTZ

10. Exercise sheet
Hand in solutions until Sunday, 24 June 2012, 23:59

Exercise 10.1 (Blind signatures). (8+4 points)

As seen in the lecture it is sometimes required that a signature protocol between two parties ALICE and BOB runs in such way that BOB signs *implicitly* a message m on behalf of ALICE, but does not know explicit by the message he is signing. Thus BOB cannot associate the signature to the user ALICE. Such protocols are called *blind signatures* and play a key role in electronic cash schemes and voting protocols.

We describe a blinding protocol based on the RSA signature scheme. Let BOB have the secret and public RSA keys sk $= (N, d)$ and pk $= (N, e)$. In order to receive blind signatures from BOB, ALICE uses her own *blinding key* $k \in \mathbb{Z}_N$ with $\gcd(k, N) = 1$.

Suppose that ALICE wants to have BOB sign the message $m \in \mathbb{Z}_N$ so that the signature can be verified but BOB cannot recover the value of m. Consider the following protocol.

1. ALICE sends $M = m \cdot k^e \in \mathbb{Z}_N$ to BOB.
2. BOB produces the signature $\sigma = \mathrm{sig}_{\mathrm{sk}}(M) = M^d \in \mathbb{Z}_N$ and sends it to ALICE.
3. ALICE recovers $\mathrm{sig}_{\mathrm{sk}}(m) = k^{-1} \cdot \sigma \in \mathbb{Z}_N$.

(i) Show that the above protocol produces a valid signature and fulfills the requirements for a blind signature scheme. $\boxed{4}$

(ii) Consider the first ecash protocol from the lecture with this RSA blind signature scheme. Alice chooses 100 messages m_i (all with the same amount but with different serial numbers) and 100 blinding keys k_i. The Bank chooses j and ask Alice to reveal all k_i with $i \neq j$. Then the Bank computes a signature σ of M_j and sends it back to Alice. Can Alice recover a valid signature from σ for another message m'? If yes, how much control does Alice have on the message m' (say, can she change the amount to a certain value)? $\boxed{4}$

(iii) Design a blind signature scheme based on the ElGamal signature algorithm and explain why it has the properties of a blinding scheme. +4

Exercise 10.2 (Coin flipping by telephone). (10 points)

(i) Read Blum (1983).

1 (ii) What are the properties of a coin-flipping protocol? What additional properties does the proposed protocol fulfill?

1 (iii) On which assumptions does the protocol rely?

2 (iv) Which conditions should the modulus n satisfy? How can these conditions be checked by Alice?

4 (v) Describe the proposed protocol and prove that the first of the properties of a coin-flipping protocol holds.

2 (vi) How could Alice cheat if she knows a factorization of n?

Hint: Extracting square roots modulo a composite number n is computational as hard as factoring n.

Exercise 10.3 (Compositions of hash functions). (6 points)

Consider to functions $g\colon \{0,1\}^n \to \{0,1\}^m$ and $f\colon \{0,1\}^m \to \{0,1\}^\ell$ with $n > m > \ell$ and their composition $f \circ g\colon \{0,1\}^n \to \{0,1\}^\ell$. Prove the following.

1 (i) If f is one way then $f \circ g$ is one way.

1 (ii) If $f \circ g$ is collision resistant then g is collision resistant.

2 (iii) If $f \circ g$ is collision resistant then f is collision resistant or g is one way.

2 (iv) If f and g are both collision resistant then $f \circ g$ is collision resistant.

References

MANUEL BLUM (1983). Coin flipping by telephone - A protocol for solving impossible problems. *SIGACT News* **15**(1), 23–27. ISSN 0163-5700. URL `http://doi.acm.org/10.1145/1008908.1008911`.