11. Exercise sheet
Hand in solutions until Sunday, 1 July 2012, 23:59

Exercise 11.1 (Are blind signature schemes EUF-KSA insecure?) (5 points)

(i) Consider an signature scheme $S$. Denote by $\text{sig}(m)$ a valid signature of $m$ under $S$. Assume one can build a blind signature scheme from $S$ such that there is a blinding function $b_r$ and an unblinding function $u_r$ depending on a blinding key $r$ such that $u_r(\text{sig}(b_r(m))) = \text{sig}(m)$ and it is hard or impossible to recover $m$ from $b_r(m)$ without the knowledge of $r$. Prove that if $b_r$ is invertible (i.e., for given $\tilde{m}$ it is easy to compute $m$ such that $\tilde{m} = b_r(m)$) then $S$ is EUF-KSA insecure (i.e., existential forgeable under known signature attacks).

(ii) Build a blind signature scheme from RSA-FDH.

(iii) Is your scheme EUF-KSA secure? Why is this no contradiction to (i).

Exercise 11.2 (Breaking the Chaum-Fiat-Naor protocol?) (5+8 points)

From a hash function $h: \{0, 1\}^\ell \to \mathbb{Z}_n$ we build a new hash function $h^*: \{0, 1\}^{dk} \to \mathbb{Z}_n$ by sending a message $m = m_1 \parallel \ldots \parallel m_k \in \{0, 1\}^{dk}$ with $m_i \in \{0, 1\}^\ell$ to $h^*(m) = \prod_{1 \leq i \leq k} h(m_i)$. Assume $h$ is collision resistant.

(i) Show that $h^*$ is not collision resistant.

(ii) Let $k = 2$ and assume that for uniformly chosen $m$ the hash values $h(m)$ are uniformly distributed. We consider pairs $(m_1 \parallel m_2, m_2 \parallel m_1)$ as trivial collisions. Describe an algorithm that computes a non-trivial collision of $h^*$. Is it faster than the birthday-attack? Compute its expected runtime.

   Hint: Consider the zero divisors in $\mathbb{Z}_n$. Maybe start with $n$ being prime.

(iii) Generalize your algorithm from (ii) to arbitrary $k$ and compute the expected runtime.

(iv) How can Alice use an algorithm from (iii) to cheat in the Chaum-Fiat-Naor protocol?
Exercise 11.3 (Brands’ electronic cash). (10 points)

(i) Read Brands (1994).

(ii) Describe the two concepts of ecash protocols mentioned in the paper (section 2.2). What are the differences?

(iii) Prove that the ‘representation problem in groups of prime order’ in a group $G$ and with $k = 2$ is as hard as the DLOG problem in $G$.

(iv) What are the major differences between the first protocol (section 5) and the second (section 6)?

Exercise 11.4 (What to ask?). (4+6 points)

Think about what you have learned during the semester. Formulate and answer at least one appropriate exam exercise.

References