Esecurity: secure internet & e-cash, summer 2012

MICHAEL NÜSKEN, RAOUL BLANKERTZ

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 $\mathrm{sig}(m)$ 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 $u_r(\mathrm{sig}(b_r(m))) = \mathrm{sig}(m)$ 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 (ie. for given $\tilde{m}$ it is easy to compute m such that $\tilde{m} = b_r(m)$) then S is EUF-KSA insecure (ie. existential forgeable under know signature attacks). $\boxed{2}$

(ii) Build a blind signature scheme from RSA-FDH. $\boxed{2}$

(iii) Is your scheme EUF-KSA secure? Why is this no contradiction to (i). $\boxed{1}$

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

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

(i) Show that h^* is not collision resistant. $\boxed{1}$

(ii) Let $k = 2$ and assume that for uniformly chosen m the hash values $h(m)$ are uniformly distributed. We consider pairs $(m_1 \| m_2, m_2 \| m_1)$ 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. $\boxed{2+4}$

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. $\boxed{+4}$

(iv) How can Alice use an algorithm from (iii) to cheat in the Chaum-Fiat-Naor protocol? $\boxed{2}$

Exercise 11.3 (Brands' electronic cash). (10 points)

(i) Read Brands (1994).

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

3 (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.

4 (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)

4+6 Think about what you have learned during the semester. Formulate and answer at least one appropriate exam exercise.

References

STEFAN BRANDS (1994). Untraceable Off-Line Cash in Wallets with Observers. In *Advances in Cryptology: Proceedings of CRYPTO '93*, Santa Barbara, CA, DOUGLAS R. STINSON, editor, number 773 in Lecture Notes in Computer Science. Springer-Verlag, New York. ISBN 0-387-57766-1. ISSN 0302-9743. URL `http://link.springer.de/link/service/series/0558/bibs/0773/07730302.htm`.