Exercise Sheet 11

Prof. Kenny Paterson, F. Günther
M. Backendal, M. Filić

Discussion Questions (Attacks).

(a) How would you compare Bleichenbacher's attack on PKCS#1 v1.5 encryption with the attacks on MAC-then-Encrypt schemes seen earlier in the lecture?

Suggested focus. Attempt these problems

before class: Problem 1, Problem 2 (a) & (c) 1),
in class: Problem (c) 2), Problem 3,
in your own time: Problem 2 (b).

Suggested reading. Reading the following sections in the Boneh-Shoup book [1] might help with the problems on this exercise sheet: Section 10.3 (for RSA basics), Sections 13.1-13.1.1 (signature schemes), Section 13.1.1 (DSKS attack), Sections 13.3-13.3.1 (RSA Full Domain Hash).

Problem 1 (Insecure RSA-style signature scheme). Consider the following signature scheme DS based on RSA. The public key is a tuple (N, e, a) containing three integer values such that: modulus $N = pq$ is computed for random primes p, q, encryption exponent e is co-prime to $\phi(N) = (p-1) \cdot (q-1)$, and $\gcd(a, N) = 1$. The private key is the inverse of e modulo $\phi(N)$ as usual. Let H be a collision-resistant hash function. The signature on a message $m \in \{0,1\}^*$ is a residue s such that

$$s^e \equiv a^{H(m)} \bmod N$$

where $H(m)$ is interpreted as an integer.

(a) Explain how the signer can (efficiently) generate signatures.

(b) Let $\mathsf{GetCoprime}$ be a function returning two messages $m_1, m_2 \in \{0,1\}^*$ such that $H(m_1)$ and $H(m_2)$ are coprime. Build an adversary breaking the UF-CMA security of the signature scheme with advantage 1. You may use $\mathsf{GetCoprime}$.

Problem 2 (Duplicate Signature Key Selection (DSKS)). Let $\mathsf{DS} = (\mathrm{KGen}, \mathrm{Sign}, \mathrm{Vfy})$ be a signature scheme and let (m, σ) be a valid message-signature pair with respect to some verification key vk. The signature scheme DS is said to be vulnerable to **DSKS** if an attacker, who sees (m, σ), can generate a key pair (vk', sk') such that (m, σ) is also valid with respect to the verification key vk'. We require that the attacker can produce both vk' and sk'.

(a) Define a security game capturing the fact that a signature scheme is secure against DSKS attacks: the attacker mounts a chosen message attack on some vk and wins if it outputs a pair (vk', sk'), such that

- $vk' \neq vk$,
- at least one of the given message-signature pairs verifies under vk', and
- sk' is a valid signing key for vk' (for this, assume that you have an algorithm $T(vk', sk')$ that returns accept only when sk' is a valid signing key for vk').

(b) **Bonus:** Show that the RSA Full Domain Hash (FDH) signature scheme is vulnerable to the DSKS attack. More precisely, let (N, e) be Alice's public key and $\sigma \in \mathbb{Z}_N$ be a signature on some message m. Then $\sigma^e = H(m) \bmod N$ for a hash function $H(.) : \{0,1\}^* \mapsto \mathbb{Z}_N$. Sketch an adversary that can efficiently come up with a new public key $vk' = (N', e')$ and the corresponding secret key, such that (m, σ) is a valid message-signature pair w.r.t. vk'.

Hint: For some primes p, the discrete-log problem (DLP) in the multiplicative group $\mathbb{Z}_p^*$ is easy (e.g., when $p = 2^\ell + 1$ is prime, the DLP problem in $\mathbb{Z}_p^*$ can be solved efficiently using the *Pohlig-Hellman algorithm*). Show that by forming N' as a product of two such primes, the adversary can come up with an e' such that $\sigma^{e'} = H(m) \bmod N'$. You can assume that, given any two integers x, y, there is an efficient way to generate sufficiently many primes p where the DLP problem in $\mathbb{Z}_p^*$ is easy, such that $x \bmod p$ and $y \bmod p$ are generators of $\mathbb{Z}_p^*$.

(c) There is a quite easy way to immunize a signature scheme $\mathsf{DS} = (\mathrm{KGen}, \mathrm{Sign}, \mathrm{Vfy})$ against DSKS attacks: the signer simply attaches his or her public key to the message before signing the message.

1) Describe the corresponding "immunized" signature scheme $\mathsf{DS}' = (\mathrm{KGen}', \mathrm{Sign}', \mathrm{Vfy}')$ formally.
2) Given any signature scheme, prove that this approach when applied to DS satisfies the security definition from part (a).

Problem 3 (Derandomization of signature schemes). Let $\mathsf{DS}_0 = (\mathrm{KGen}_0, \mathrm{Sign}_0, \mathrm{Vfy}_0)$ be a signature scheme defined over some message space $\mathcal{M}$, such that the signing algorithm Sign_0 is probabilistic. Assume that DS_0 is UF-CMA secure. Let algorithm Sign_0 use random coins chosen from some randomness space $\mathcal{R}$. We let $\mathrm{Sign}_0(sk, m; r)$ denote the execution of algorithm Sign_0 with randomness $r \in \mathcal{R}$. Let $F\colon \{0,1\}^k \times \mathcal{M} \to \mathcal{R}$ be a secure PRF, defined for some key length $k \in \mathbb{N}$. Show that the following signature scheme $\mathsf{DS} = (\mathrm{KGen}, \mathrm{Sign}, \mathrm{Vfy})$ is UF-CMA secure:

Algorithm KGen	Algorithm Sign(sk, m)	Algorithm Vfy(vk, m, σ)
$(sk_0, vk_0) \leftarrow\!\!\$\ \mathrm{KGen}_0$	$(sk_0, \mathsf{K}) \leftarrow sk$	Return $\mathrm{Vfy}_0(vk, m, \sigma)$
$\mathsf{K} \leftarrow\!\!\$\ \{0,1\}^k$	$r \leftarrow F(\mathsf{K}, m)$	
$sk \leftarrow (sk_0, \mathsf{K})$	$\sigma \leftarrow \mathrm{Sign}_0(sk, m; r)$	
Return (sk, vk_0)	Return σ	

Note that the new signing algorithm Sign is deterministic.

Acknowledgements. This exercise sheet is in part inspired by (and adapted from) problems by Simon Blackburn, Daniel Slamanig, and Mihir Bellare, as well as the book "A Graduate Course in Applied Cryptography" by Dan Boneh and Victor Shoup.

References

[1] D. Boneh and V. Shoup. *A Graduate Course in Applied Cryptography.* Online, version 0.6 edition, Jan. 2023.