Applied Cryptography

Public Key Cryptography, Assignment 4, Wednesday May 11, 2022

Remarks:

- Hand in your answers through Brightspace.
- Hand in format: PDF. Either hand-written and scanned in PDF, or typeset and converted to PDF. Please, **do not** submit photos, Word files, LaTeX source files, or similar.
- Assure that the name of **each** group member is **in** the document (not just in the file name).

Deadline: Wednesday, May 25, 23.59

Goals: After completing these exercises you should have a high level understanding of post-quantum cryptography, and a more in depth understanding of hash based signatures, as well as Authenticated Key Exhange using digital signatures

1. **(15 points)** In the lecture post quantum cryptography was introduced. Using your own words, and with the help of the slides and the internet answer the following:
   (a) What is necessary for a cryptosystem to be called post-quantum?
   (b) Why are we interested in post-quantum cryptosystems?
   (c) What are the main advantages of post-quantum cryptography as opposed to quantum cryptography?
   (d) Assume a quantum adversary that is in possession of a large universal quantum computer. How much time, in processing time, does he need to break a password of length 10, uniformly chosen from the set of all passwords containing any letter A-z and any special character, but no numerical characters 0-9?
   (e) Answer the previous question in the case the adversary is not in possession of a quantum computer.
   (f) What is the required length of the keys of a symmetric cryptosystem against quantum adversaries for 128 bits of security?
   (g) What is the required length of RSA keys against quantum adversaries for 128 bits of security?
   (h) Define one of the hard problems: LWE, MQ, Syndrome decoding and explain how it can be used to construct a public key cryptosystem. Use at most 250-300 words

2. **(20 points)** Consider the following generalization of one time signatures:

- **Key generation:**
  - Generate a pair of secret and public key $(\mathsf{sk}_1, \mathsf{pk}_1)$ using Lamport's OTS for 256-bit messages and which uses SHA-256
  - Set a state to $S = ()$ and $\sigma_0 = ()$
- **Signing:** To sign a message M_i, $i = 1, 2, \ldots$ the signer
  - Generates a new key pair $(\mathsf{sk}_{i+1}, \mathsf{pk}_{i+1})$
  - Computes a signature $\sigma_i = (M_i, \mathsf{pk}_{i+1}, \mathsf{Sign}_{\mathsf{sk}_i}(H_0(M_i, \mathsf{pk}_{i+1})), \sigma_{i-1})$ where $\mathsf{Sign}_{\mathsf{sk}_i}$ is the signing algorithm of Lamport OTS using the secret key sk_i.
  - Add $(M_i, \mathsf{pk}_{i+1}, \mathsf{sk}_{i+1}, \mathsf{Sign}_{\mathsf{sk}_i}(H_0(M_i, \mathsf{pk}_{i+1})))$ to the state S
- **Verification:** To verify the signature $\sigma_i = (M_i, \mathsf{pk}_{i+1}, \sigma_{i,OTS}, \sigma_{i-1})$
  - Check $\mathsf{Vf}_{\mathsf{pk}_j}(M_j, \mathsf{pk}_{j+1}, \sigma_{j,OTS}) = 1$ for all $j \in \{1, 2, \ldots, i\}$

(a) What should be the length of the output of H_0?

(b) How long is the signature of the 12-th message? Assume the length of the i-th message is L_{M_i}.

(c) What is the advantage of this scheme compared to MSS introduced in the lectures? What is the disadvantage?

(d) Show that a forgery is possible if instead of $\mathsf{Sign}_{\mathsf{sk}_i}(H_0(M_i, \mathsf{pk}_{i+1}))$ the signer includes $\mathsf{Sign}_{\mathsf{sk}_i}(H_0(M_i))$

(e) Show that a forgery is possible, if in the signature generation of σ_i, we omit σ_{i-1}, and in the verification process we set $j \in \{i\}$, and provide the OTS public key pk_i together with the signature.

(f) Show that a forgery is possible if the adversary is able to find second preimages for H_0

(g) Can you think of a way to improve the efficiency of the scheme using Merkle trees? If yes, please describe the solution in detail, with a justification of the improved efficiency. Different solutions are possible, and will be accepted, provided there isn't an obvious security flaw.

3. **(15 points)**

(a) Provide concrete plausible practical examples for the two identity misbinding attacks (Attack 1 and 2) from the lectures.

(b) Show in detail that SIGMA-I indeed prevents the two identity misbinding attacks (Attack 1 and 2) from the lectures.

(c) Recall the ISO 9796 protocol from the lectures, in which the identity of the receiver was included in the signatures σ_A, σ_B to prevent an identity misbinding attack.

Alice's client		Bob's server
$P, G, \mathsf{pk}_B, a, \mathsf{sk}_A$		$P, G, \mathsf{pk}_A, b, \mathsf{sk}_B$
$A \leftarrow G^a$	$\xrightarrow{\text{Alice};\ A}$	
$\mathsf{Vf}_{\mathsf{pk}_B}(\sigma_B)$	$\xleftarrow{\text{Bob};\ B;\ \sigma_B}$	$B \leftarrow G^b$, $\sigma_B = \mathsf{Sign}_{\mathsf{sk}_B}(A, B, Alice)$
$K_{A,B} \leftarrow B^a$		$K_{B,A} \leftarrow A^b$
$\sigma_A = \mathsf{Sign}_{\mathsf{sk}_A}(B, A, Bob)$	$\xrightarrow{\sigma_A}$	$\mathsf{Vf}_{\mathsf{pk}_A}(\sigma_A)$

Show in detail (i.e. describing an attack) why including the identity of the sender in the signatures does not prevent identity misbinding attacks.

(d) Assume the protocol uses RSA signatures. Because the idea from (c) does not work, the designers decided to include the shared key $K_{A,B} = K_{B,A}$ in the signatures σ_A, σ_B instead of the identities. Does this idea prevent identity misbinding attacks? Explain why. (Hint: No, it doesn't. Please show an attack.) Does removing the identities sent in clear change the situation?