Applied Cryptography

Public Key Cryptography, Assignment 6, Monday, May 13, 2024

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: Sunday, May 26, 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 SIGMA protocols.

1. **(25 points)** In the last 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, $\mathcal{D}$, that is in possession of a large universal quantum computer. How much processing time does $\mathcal{D}$ need to break a password of length 10 character characters, 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 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 if we want to achieve 128 bits of security?

   (g) What is the required length of RSA keys against quantum adversaries if we want to achieve 128 bits of security?

   (h) Choose of the of the following problems: LWE, MQ or Syndrome decoding. State the definition of the problem and explain how it can be used to construct a public key cryptosystem. Use at most 250-300 words

2. **(25 points)** In the lecture, we have seen SIGMA-protocols and how these prevent identity misbinding attacks.

   (a) Provide two 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. describe 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 (a) 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 not. Does removing the identities sent in the clear change the situation?