Applied Cryptography, FS2023 | Prof. Kenny Paterson, F. Günther
June 1–2, 2023 // Version 1.2 | M. Backendal, M. Filić

Exercise Sheet 14

Discussion Questions (Applying Cryptography).

(a) In the first exercise session, we asked: “What, for you, is the most important application of cryptography?” (How) Did your perspective change after having attended this course?

Suggested focus. Attempt these problems
in class: Problems 1 and 2.
in your own time: Problem 3.

Suggested reading. Reading the following sections in the Boneh-Shoup book [1] might help with the problems on this exercise sheet: Section 10.4 (Diffie–Hellman key exchange).

Problem 1 (Weakening TLS 1.3). Figure 1 shows a simplified version of the TLS 1.3 main handshake (cf. Lecture 33-34) in which only the server authenticates and the client's final messages are omitted. This protocol can be shown to be a secure key exchange protocol (with server-only authentication) assuming hardness of the DDH problem in group $\mathbb{G}$, unforgeability of the signature and MAC schemes (SIG, resp. MAC), and pseudorandomness of the key derivation function KDF.

Client	$\mathbb{G} = \langle g \rangle$ of order q	**Server** (sk_S, vk_S)
$r_C \leftarrow\$ \{0,1\}^{256}$ $x \leftarrow\$ \mathbb{Z}_q$ $X \leftarrow g^x$		$r_S \leftarrow\$ \{0,1\}^{256}$ $y \leftarrow\$ \mathbb{Z}_q$ $Y \leftarrow g^y$
	$\xrightarrow{r_C, X}$	
	$\xleftarrow{r_S, Y}$	
$\mathsf{tr} \leftarrow r_C \,\|\, X \,\|\, r_S \,\|\, Y$		$\mathsf{tr} \leftarrow r_C \,\|\, X \,\|\, r_S \,\|\, Y$ $\sigma \leftarrow\$ \mathsf{SIG}.\mathrm{Sign}(sk_S, \mathsf{tr} \,\|\, vk_S)$ $k_m \leftarrow \mathsf{KDF}(g^{xy}, \texttt{"mac"} \,\|\, \mathsf{tr} \,\|\, vk_S \,\|\, \sigma)$ $\tau \leftarrow\$ \mathsf{MAC}.\mathrm{Tag}(k_m, \mathsf{tr} \,\|\, vk_S \,\|\, \sigma)$
	$\xleftarrow{vk_S, \sigma, \tau}$	
check that vk_S belongs to S, else abort check that $\mathsf{SIG}.\mathrm{Vfy}(vk_S, \mathsf{tr} \,\|\, vk_S, \sigma) = 1$, else abort $k_m \leftarrow \mathsf{KDF}(g^{xy}, \texttt{"mac"} \,\|\, \mathsf{tr} \,\|\, vk_S \,\|\, \sigma)$ check that $\mathsf{MAC}.\mathrm{Vfy}(k_m, \mathsf{tr} \,\|\, vk_S \,\|\, \sigma, \tau) = 1$, else abort		
$k \leftarrow \mathsf{KDF}(g^{xy}, \texttt{"app"} \,\|\, \mathsf{tr} \,\|\, vk_S \,\|\, \sigma)$ peer identity: S		$k \leftarrow \mathsf{KDF}(g^{xy}, \texttt{"app"} \,\|\, \mathsf{tr} \,\|\, vk_S \,\|\, \sigma)$ peer identity: (unknown/unauthenticated)

Figure 1: A simplified version of the TLS 1.3 main handshake in which only the server authenticates.

Let us explore why these security assumptions are needed, by studying what happens when you take out one of the components. Sketch an attack on the protocol if. . .

(a) … the signature σ is omitted.

(b) … the MAC τ is omitted and the session key is computed only from the transcript, i.e., $k \leftarrow \mathsf{KDF}(g^{xy}, \texttt{"app"} \,\|\, \mathsf{tr})$.

Hint: Think about how an adversary, controlling a third party E, could fool the client to derive a shared key with the server while believing it talks to E.

How would this attack translate to the setting where the client authenticates, too (but also omits the MAC)?

(c) …the key derivation function is not completely pseudorandom, but defined as $\mathsf{KDF}(x, y) := \mathsf{KDF}'(x, y)\|0$ for a good pseudorandom key derivation function KDF'.

Problem 2 (Extended security of X3DH). In Lecture 35, we saw the initial key exchange of the Signal protocol. At its core, the extended triple Diffie–Hellman (X3DH) key exchange combines the Diffie–Hellman secret shares from (up to) four combinations of Diffie–Hellman identity keys, signed prekeys, and one-time keys, as shown in Figure 2.

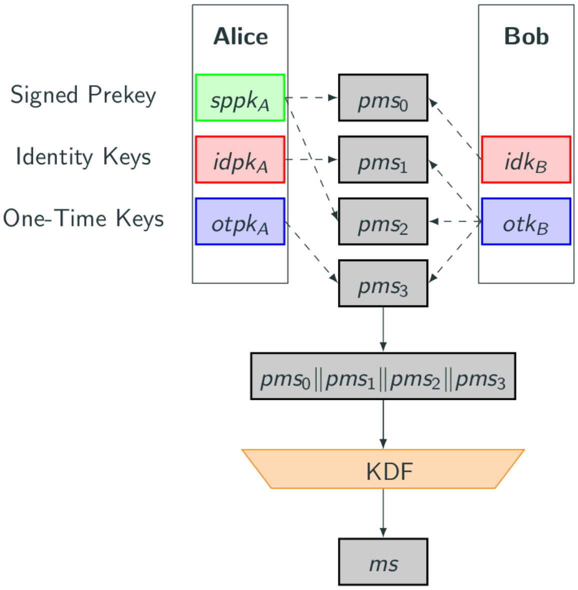

Figure 2: The master secret computation in Signal's X3DH key exchange.

Recall that:

- **Identity keys** $\mathsf{idk}_A/\mathsf{idpk}_A$ are static keys that belong to a party A and are authenticated (out-of-band); they are re-used in all Signal handshakes of that party.
- **Signed prekeys** $\mathsf{spk}_A/\mathsf{sppk}_A$ are signed by their owner (A); they are updated regularly and re-used across several Signal handshakes.
- **One-time keys** $\mathsf{otk}_A/\mathsf{otpk}_A$ are not authenticated (by A) and are uploaded to the Signal server in batches; each such key is used only once. If no one-time public key otpk_A for user Alice (A) is left on the Signal server, the X3DH handshake of Bob (B) with Alice as shown in Figure 2 omits computing pms_3 (the combination otk_A–otk_B).

When analyzing the Signal X3DH handshake, we consider a very strong adversary which not only controls the communication (i.e., can mount passive and active attacks), but which can also (selectively) compromise all types of keys of users mentioned above.

Formally, this can be captured by allowing the adversary to compromise (through oracles in a security game) **long-term keys** (idk), **medium-term keys** (the regularly updated keys sppk) as well as **session randomness** (thinking of otk keys as being generated by the individual communication sessions). We are interested in the security of the derived master secret ms as long as the two components in *at least one* Diffie–Hellman combination are *uncompromised.* It suffices to look at the individual pms_i inputs to argue security for the overall master secret ms because the key derivation function used to derive ms is assumed strong enough to extract a secret key if at least one input is unknown to the adversary.

(a) For the following security statements on Diffie–Hellman combinations from Lecture 35, Slide 35, explain informally (i) why the security statement holds, and (ii) what attack must *not* have been mounted by the adversary for this combination to remain secure.

1) pms_3: "otpk_A–otk_B provides forward secrecy."
2) pms_2: "sppk_A–otk_B provides delayed forward secrecy if no otk_A is present."
3) pms_1: "idpk_A–otk_B provides authentication of Alice."
4) pms_0: "sppk_A–idk_B provides authentication of Bob."

Problem 3 (Three-party key exchange).

(a) Propose a passively-secure key exchange protocol for three participants, Alice, Bob, and Charlie. Describe the computations performed by each participant and the messages communicated between them. Argue (informally) under which assumption the protocol is secure.

Hint: Think of an extension of the Diffie–Hellman key exchange protocol.

(b) Briefly: How would you transform this protocol into an authenticated one?

Acknowledgements. This exercise sheet is in part inspired by (and adapted from) problems by Marc Fischlin.

References

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