Exercise Sheet 7

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

Discussion Questions (Generic Decomposition and AEAD).

(a) We saw how to generically construct a secure AE scheme from an (IND-CPA secure) symmetric encryption scheme and a (SUF-CMA secure) MAC scheme. Can we also do the inverse, construct secure symmetric encryption and MAC schemes from a secure AE scheme?

(b) Is the associated data (AD) value included in the AEAD ciphertext or does it need to be sent along with the ciphertext?

Suggested focus. Attempt these problems
before class: Problem 1, Problem 2 part (a).
in class: Problem 2 part (b) and (c).

Suggested reading. Reading the following sections in the Boneh-Shoup book [1] might help with the problems on this exercise sheet: Sections 9.1 (Authenticated encryption: definitions) and 9.4.1. (Encrypt-then-MAC)

Problem 1 (Formalizing integrity notions). Formalize the two integrity notions for plaintext (INT-PTXT) and ciphertext (INT-CTXT) integrity by completing the following code-based games (cf. lecture 18–21, slides 10–15).

Game $\textbf{INT-PTXT}(\mathcal{A}, \mathrm{SE})$ $\boxed{\textbf{INT-CTXT}(\mathcal{A}, \mathrm{SE})}$:

$\mathsf{K} \leftarrow_{\$} \mathrm{KGen}()$
$S_P, S_C \leftarrow \emptyset$
$\mathsf{win} \leftarrow \mathsf{false}$
$\mathcal{A}^{\mathsf{enc},\mathsf{try}}()$
Return win

Oracle $\mathsf{enc}(m)$:

$\ldots$
$S_P \leftarrow \ldots$
$\boxed{S_C \leftarrow \ldots}$
Return c

Oracle $\mathsf{try}(c)$:

$\ldots$
$a \leftarrow (m \neq \perp) \wedge \ldots$
$\boxed{a \leftarrow (m \neq \perp) \wedge \ldots}$
If $a = \mathsf{true}$ then $\mathsf{win} \leftarrow \mathsf{true}$
Return a

We require that any adversary $\mathcal{A}$ playing in game **INT-PTXT** or **INT-CTXT** makes exactly *one* query to its try oracle. We define the advantange of an adversary $\mathcal{A}$ in the games as:

$$\mathbf{Adv}_{\mathrm{SE}}^{\text{INT-PTXT/CTXT}}(\mathcal{A}) = \Pr\left[\,\text{Game } \textbf{INT-PTXT/CTXT}(\mathcal{A}, \mathrm{SE}) \Rightarrow \mathsf{true}\,\right].$$

Problem 2 (Authenticated encryption security of Encrypt-then-MAC). Let $\mathrm{SE}_0 = (\mathrm{KGen}_0, \mathrm{Enc}_0, \mathrm{Dec}_0)$ be a symmetric encryption scheme. Let $\mathrm{M} = (\mathrm{KGen}_\mathrm{M}, \mathrm{Tag}, \mathrm{Vfy})$ be a MAC scheme defined for message space $\mathcal{M}_\mathrm{M} = \{0,1\}^*$ and having fixed tag length t. Let $\mathrm{SE} = (\mathrm{KGen}, \mathrm{Enc}, \mathrm{Dec})$ be the symmetric encryption scheme resulting from the *Encrypt-then-MAC* (EtM) composition of SE_0 and M.

(a) Complete the details of the code for SE.

Algorithm KGen	Algorithm $\mathrm{Enc}(\mathsf{K}, m)$	Algorithm $\mathrm{Dec}(\mathsf{K}, c)$
$\mathsf{K}_0 \leftarrow\!\!\$\ \mathrm{KGen}_0()$	$(\mathsf{K}_0, \mathsf{K}_\mathrm{M}) \leftarrow \mathsf{K}$	$(\mathsf{K}_0, \mathsf{K}_\mathrm{M}) \leftarrow \mathsf{K}$
$\mathsf{K}_\mathrm{M} \leftarrow\!\!\$\ \mathrm{KGen}_\mathrm{M}()$	$\ldots$	$\ldots$
$\mathsf{K} \leftarrow (\mathsf{K}_0, \mathsf{K}_\mathrm{M})$		
Return K		

(b) Assume that SE_0 is IND-CPA secure and M is SUF-CMA secure. Provide a formal proof that SE is a secure authenticated encryption scheme by showing that SE is

- IND-CPA secure and
- INT-CTXT secure.

In each case reduce the security of SE to that of either SE_0 or M.

(c) Now assume that the symmetric encryption scheme SE_0 and the message authentication scheme M both use the same key generation algorithm $\mathrm{KGen}_0 = \mathrm{KGen}_\mathrm{M}$ (and hence share the same key space). It might be tempting to use this fact in order to simplify the *Encrypt-then-MAC* composition, reusing the *same* key for both SE_0 and M components. Formally, let us call this scheme $\mathrm{SE}^* = (\mathrm{KGen}^*, \mathrm{Enc}^*, \mathrm{Dec}^*)$ where $\mathrm{Enc}^* = \mathrm{Enc}$ and $\mathrm{Dec}^* = \mathrm{Dec}$ (from part (a)) and key generation is defined as

Algorithm $\mathrm{KGen}^*()$
$\mathsf{K} \leftarrow\!\!\$\ \mathrm{KGen}_0()$
Return (K, K) // In notation of part (a): $\mathsf{K}_0 = \mathsf{K}_\mathrm{M} = \mathsf{K}$

We will now see that that SE^* is not guaranteed to be IND-CPA or INT-CTXT secure, even if SE_0 is IND-CPA secure and M is SUF-CMA secure. ((Re)using a shared key for multiple cryptographic primitives generally risks introducing security vulnerabilities.)

Let $\mathsf{E}\colon \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher. Let SE_0 be the CBC mode based on E, defined *only* for n-bit long messages (hence only having one complete block, not requiring any padding). Then the scheme SE_0 is defined for plaintext space $\mathcal{M}_0 = \{0,1\}^n$ and ciphertext space $\mathcal{C}_0 = \{0,1\}^{2n}$. Let M be the basic CBC-MAC defined for $\mathcal{M}_\mathrm{M} = \{0,1\}^{2n}$. Let SE^* be the proposed single-key version of *Encrypt-then-MAC* composition, based on schemes SE_0 and M as described above.

1) Build an adversary $\mathcal{A}_{\textsf{ind-cpa}}$ against the IND-CPA security of SE^*. Your adversary should make at most two queries to its $\textsf{LoR}$ oracle, and achieve $\mathbf{Adv}^{\text{IND-CPA}}_{\mathrm{SE}^*}(\mathcal{A}_{\textsf{ind-cpa}}) = 1$.
2) Build an adversary $\mathcal{A}_{\textsf{int-ctxt}}$ against the INT-CTXT security of SE^*. Your adversary should make at most one query to its $\textsf{Enc}$ oracle, and achieve $\mathbf{Adv}^{\text{INT-CTXT}}_{\mathrm{SE}^*}(\mathcal{A}_{\textsf{int-ctxt}}) \geq 1 - 2^{-n}$.

Note that under reasonable assumptions about E, SE_0 can provide IND-CPA security and M can provide SUF-CMA security. However, SE^* is not secure regardless of the choice for E.
Hint: Draw a picture of algorithm Enc^*, expanding algorithms Enc_0 and Tag to use the CBC-based primitives.

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