Applied Cryptography

Symmetric Cryptography, Assignment 2, Monday, February 19, 2024

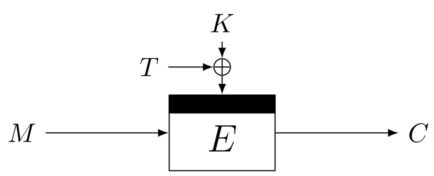
Remarks:

- 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. Also submit code used for your assignments (as separate files).
- Assure that the name of **each** group member is **in** the document (not just in the file name).

Deadline: Sunday, March 3, 23.59

Goals: After completing these exercises you should have understanding in arguing security of message authentication and authenticated encryption.

1. **(10 points)** Consider a tweakable block cipher $\widetilde{E} : \{0,1\}^k \times \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$, a tweakable block cipher taking a k-bit key, k-bit tweak and n-bit data, built from an n-bit block cipher $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ as follows:

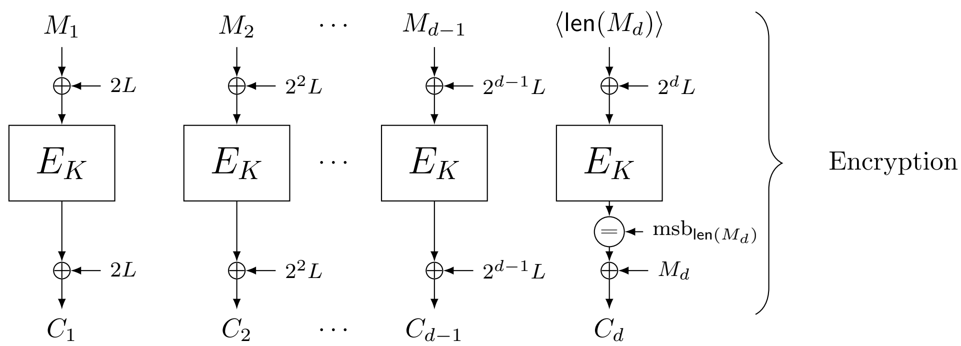


   It is possible to recover the secret key K with high probability, by making $2^{k/2}$ evaluations of $\widetilde{E}_K$ and $2^{k/2}$ offline evaluations of E. Explain how. Here, you may assume that $k \ll n$, i.e., that k is much smaller than n.

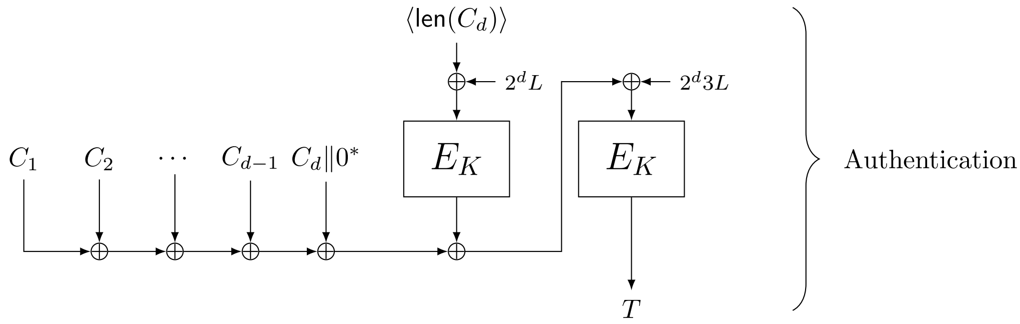
   Hint: Can you find some kind of collision?

2. **(20 points)**[1] Let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher, and consider the following variant of the $\mathsf{OCB2}$ mode of operation, which we call $\overline{\mathsf{OCB2}}$. For simplicity, we assume that associated data is always empty, hence it will be omitted from this exercise. $\overline{\mathsf{OCB2}}$ now operates as follows:

   - Firstly, $\overline{\mathsf{OCB2}}$ takes a k-bit key K, n-bit nonce N, and arbitrary length message M. The message is split into blocks $M_1, M_2, \ldots, M_d$, where $M_1, \ldots, M_{d-1}$ are all of size n bits, and M_d is of size between 1 and n bits. A subkey $L = E_K(N)$ is computed.
   - Secondly, $\overline{\mathsf{OCB2}}$ proceeds as in the picture:



[1] This exercise is based on an attack against OCB2 of Inoue et al.: `https://eprint.iacr.org/2019/311.pdf`.



Here, $\mathsf{len}(X)$ denotes the length of a bit string X, $\langle n \rangle$ is the binary representation of n, and $\ominus\!\leftarrow \mathrm{msb}_l$ denotes the truncation to the l most significant bits, i.e., the dropping of the right $n - l$ bits.

- Thirdly, it outputs ciphertext $C = C_1 \| C_2 \| \cdots \| C_d$ and tag T.

(a) Describe how the verification function of $\overline{\mathsf{OCB2}}$ works. I.e., given a k-bit key K, n-bit nonce N, arbitrary length ciphertext C, and an n-bit tag T, describe:

   i. How to determine if the tag is valid.

   ii. How to recover the plaintext M, if (N, A, C, T) is a correct authenticated ciphertext.

(b) It turns out that this version of $\overline{\mathsf{OCB2}}$ is, in fact, not secure. Consider an adversary that does the following:

   - Let N be an arbitrary nonce, and let $M = M_1 \| M_2$ be a $2n$-bit message with $M_1 = \langle n \rangle$ and M_2 any n-bit string.
   - The adversary calls the encryption oracle with input $(N, M_1 \| M_2)$, and obtains $(C_1 \| C_2, T)$.
   - The adversary takes a ciphertext $C' = C_1 \oplus \langle n \rangle$ of length n bits, and tag $T' = M_2 \oplus C_2$.
   - The adversary outputs forgery (N, C', T').

   Show that this forgery is valid. In order to do this, we recommend to proceed as follows:

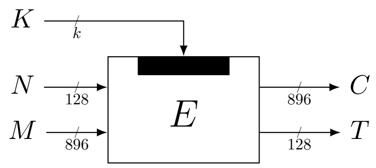
   i. Compute M', the plaintext corresponding to C'.

   ii. Compute $\overline{\mathsf{OCB2}}(N, M')$. **Hint**: Here, you need to use that in a binary field we have $2 \cdot 3 \oplus 2 = 2^2$.

3. **(10 points)** Consider a block cipher $E : \{0,1\}^k \times \{0,1\}^{1024} \to \{0,1\}^{1024}$ and consider the following authenticated encryption scheme

$$\begin{aligned} \mathsf{AE}\colon \{0,1\}^k \times \{0,1\}^{128} \times \{0,1\}^{896} &\to \{0,1\}^{896} \times \{0,1\}^{128}\,, \\ (K, N, M) &\mapsto (C, T)\,, \end{aligned}$$

defined as follows:



We will consider the nonce-misuse-resistance of this scheme. In other words, we consider the security of this construction in the model of lecture 3 slide 4, $\mathbf{Adv}^{\mathsf{ae}}_{\mathsf{AE}}(q_e, q_v)$, *with the difference that $\mathcal{D}$ may repeat nonces*. Here, q_e and q_v denote the total number of encryption and decryption queries, respectively.

(a) Describe how the authenticated decryption function AE_K^{-1} operates.

(b) The first step in the security proof of AE will be to replace the keyed block cipher E_K by a random permutation p. Apply the triangle inequality to do so, with explicitly mentioning the loss incurred by this triangle inequality:

$$\Delta_{\mathcal{D}}\left(\mathsf{AE}_K, \mathsf{AE}_K^{-1} \;;\; \$, \perp\right) \leq \Delta_{\mathcal{D}}\left(\mathsf{AE}[p], \mathsf{AE}[p]^{-1} \;;\; \$, \perp\right) + \dots$$

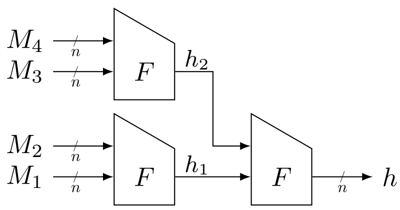
Explain your answer in words.

(c) We are left with the task of bounding $\Delta_{\mathcal{D}}\left(\mathsf{AE}[p], \mathsf{AE}[p]^{-1} \;;\; \$, \perp\right)$. We will perform another triangle inequality:

$$\Delta_{\mathcal{D}}\left(\mathsf{AE}[p], \mathsf{AE}[p]^{-1} \;;\; \$, \perp\right) \leq \Delta_{\mathcal{D}}\left(\mathsf{AE}[p], \mathsf{AE}[p]^{-1} \;;\; \mathsf{AE}[p], \perp\right) + \Delta_{\mathcal{D}}\left(\mathsf{AE}[p], \perp \;;\; \$, \perp\right) . \tag{1}$$

The first distance of (1) is a bit peculiar and will be ignored in this assignment. Derive a bound on the second distance of (1), $\Delta_{\mathcal{D}}\left(\mathsf{AE}[p], \perp \;;\; \$, \perp\right)$.

4. **(10 points)** We will cover the Merkle-Damgård and other *sequential* hashing modes in lecture 4, and this question is an introductory teaser towards this lecture.. An alternative to sequential hashing is tree-based hashing. Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a compression function, and consider the following hash function $\mathcal{H} : \{0,1\}^{4n} \to \{0,1\}^n$:



Argue (informally) that $\mathcal{H}$ is collision resistant if F is collision resistant.