Applied Cryptography

Symmetric Cryptography, Assignment 2, Monday, September 17, 2024

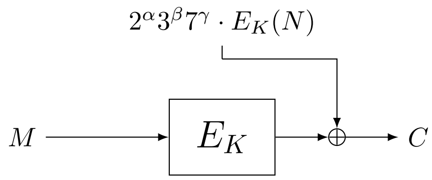
Remarks:

- 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, September 29, 23.59

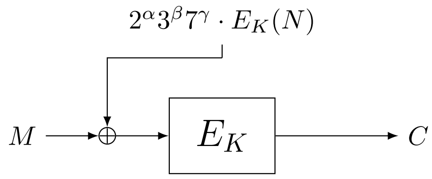
1. **(10 points)** During lecture 3, we considered the XEX tweakable block cipher construction. We now consider what would happen if we were to remove one of the blindings.

   (a) Consider the construction EX, described below, where we have removed the first blinding:

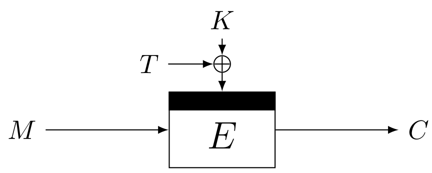
   That is, $\mathsf{EX}((\alpha,\beta,\gamma,N),M) = E_K(M) \oplus (2^\alpha 3^\beta 7^\gamma \cdot E_K(N))$, where (α,β,γ,N) is the tweak. Explain why EX is TPRP **insecure**.

   (b) Consider the tweakable block cipher XE, described below, where we have removed the second blinding:

   That is, $\mathsf{XE}((\alpha,\beta,\gamma,N),M) = E_K(M \oplus (2^\alpha 3^\beta 7^\gamma \cdot E_K(N)))$, where (α,β,γ,N) is the tweak. Explain why XE is STPRP **insecure**. (In fact, XE **is** TPRP secure, and is used in some applications.)

2. **(20 points)** Consider a tweakable block cipher $\widetilde{E} : \{0,1\}^k \times \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$, taking a k-bit key, k-bit tweak and n-bit message, built from an n-bit block cipher $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ as follows:

   Suppose you are allowed to query the construction $\widetilde{E}_K$ and the primitive E separately. Then, 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.

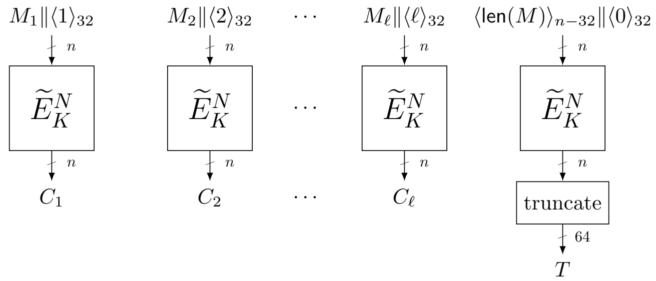
   Explain how. Here, you may assume that $k \ll n$, i.e., that k is much smaller than n.

   Hint: Can you find some kind of collision?

3. **(20 points)** Let $k = 128$, $t = 64$, $n = 128$, $a = 32$, $b = 64$ and let $\widetilde{E} : \{0,1\}^k \times \{0,1\}^t \times \{0,1\}^n \to \{0,1\}^n$ be a tweakable block cipher. Consider the following nonce-based authenticated encryption scheme CrAp (for $\mathsf{Applied}$ $\mathsf{Cryptography}$), that gets as input a key K of k bits, a nonce N of t bits, and a message M of arbitrary length, and that generates a ciphertext C and a tag T:

- The message M is first padded with a sufficiently many number of 0s so that it is of length a multiple of $n - a$ bits. It is then partitioned into $(n-a)$-bit blocks $M_1, \ldots, M_\ell$.
- Each block is encrypted as $C_i \leftarrow \widetilde{E}_K(N, M_i \| \langle i \rangle_a)$, where $\langle i \rangle_a$ is the encoding of i as an a-bit string.
- The tag is computed as $T \leftarrow \mathsf{trunc}_b\big(\widetilde{E}(K, N, \langle \mathsf{len}(M) \rangle_{n-a} \| \langle 0 \rangle_a)\big)$, where $\langle \mathsf{len}(M) \rangle_{n-a}$ encodes the bit length of M as an $(n-a)$-bit string, and trunc_b truncates its input to b bits.

The operation of CrAp is also described in the picture below:



(a) Describe how CrAp_K^{-1} operates algorithmically: what are the inputs and their sizes, the outputs and their sizes, and how are the outputs computed from the inputs?

(b) CrAp_K accepts messages M of arbitrary length, however, strictly seen there is a limit on the maximum message size due to the fact that we use a counter. What is the maximum length of M in bits?

(c) What security property do we require of $\widetilde{E}$ in order to be able to prove security of CrAp as an authenticated encryption scheme? Concisely explain your answer informally.

(d) Assume one does not implement CrAp_K with unique nonces, but rather with random nonces. In other words, for each new evaluation (for a new, or possibly repeated, message M) the implementation selects a random t-bit nonce N and evaluates $\mathsf{CrAp}_K(N, M)$. What is the expected number of evaluations an attacker must make in order to obtain a repeated nonce?

(e) One can break the authenticity of CrAp with high probability in 1 encryption query and 2^a forgery attempts. Describe the corresponding distinguisher $\mathcal{D}$.