Applied Cryptography

Symmetric Cryptography, Assignment 1, Wednesday, February 16, 2022

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: Wednesday, March 2, 23.59

Goals: After completing these exercises you should have understanding in lower and upper bounding advantages, in performing generic attacks, and in authenticated encryption.

1. **(10 points)** This question is about the non-tightness of the equation of lecture 2 slide 12. In other words, it is about the existence of a MAC function that is unforgeable but not PRF-secure. Suppose we are given a pseudorandom function $F : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$. Consider MAC function

$$\mathsf{MAC}_K(M) = F_K(M) \parallel F_K(M)\,.$$

   (a) Prove that MAC is unforgeable up to bound $q_v/2^n$, i.e., that

$$\mathbf{Adv}^{\mathrm{unf}}_{\mathsf{MAC}}(q_m, q_v) \leq \frac{q_v}{2^n} + \mathbf{Adv}^{\mathrm{prf}}_{F}(q_m + q_v)\,.$$

   You do *not* have to *explicitly* write a reduction from the unforgeability of MAC to the PRF-security of F.

   (b) For PRF-security, we consider the setup of a distinguisher that has access to either $\mathsf{MAC}_K : M \mapsto T$ or to a random oracle $\mathsf{RO} : M \mapsto T$. Consider the following distinguisher $\mathcal{D}$:

   - Fix an arbitrary M and query the oracle on M to receive a tag T;
   - If the left and right half of T are equal, return 1. If the left and right half of T are unequal, return 0.

   Determine the exact PRF-advantage of this particular distinguisher $\mathcal{D}$, $\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{MAC}}(\mathcal{D})$.

2. **(5 points)** Consider the function $H : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ defined as $H_L(M) = L \otimes M$, i.e., defined as finite-field multiplication over $\mathrm{GF}(2^n)$.

   (a) Prove that this function is 2^{-n}-XOR-universal.

   (b) If plugged into the Wegman-Carter MAC function of lecture 2 slide 14, we obtain

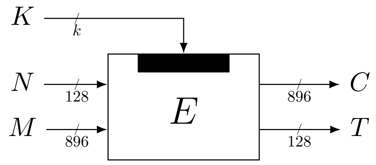
$$\mathbf{Adv}^{\mathrm{unf}}_{\mathsf{WC}}(q_m, q_v) \leq q_v/2^n + \mathbf{Adv}^{\mathrm{prf}}_{F}(q_m + q_v)\,,$$

   provided that the adversary does not query WC_K for repeated nonces. Assume you can evaluate this function for repeated nonces. Mount a forgery attack in $q_m = 3$ MAC queries and $q_v = 1$ VFY query.

3. **(10 points)** Suppose we are given a block cipher $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ for large n, in this case $n = 1024$. 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 security of this construction in the model of lecture 3 slide 4, $\mathbf{Adv}^{\mathrm{ae}}_{\mathsf{AE}}(q_e, q_v)$, *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:

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

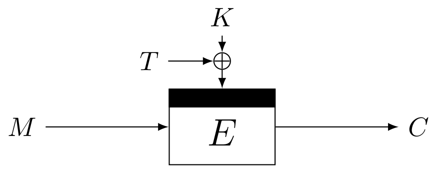
Explain your answer in words.

(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. Derive a bound on the second distance of (1), $\Delta_{\mathcal{D}}\left(\mathsf{AE}[p], \perp \ ; \ \$, \perp\right)$.

4. **(5 points)** Consider a tweakable block cipher $\widetilde{E} : \{0,1\}^k \times \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$, i.e., with k-bit key and tweak and n-bit data path, built from a 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 in $2^{k/2}$ evaluations of $\widetilde{E}_K$ and $2^{k/2}$ offline evaluations of E. Describe the attack. You can assume that $k \ll n$, i.e., there is no need to make additional queries to eliminate false positives.

5. **(10 points)** Let $n = 128$, take $E : \{0,1\}^{128} \times \{0,1\}^{128} \to \{0,1\}^{128}$ to be your favorite block cipher, and consider the XEX construction XEX_K of lecture 3 slide 24. As this question is particularly about the masking, we will have to explicitly define what multiplication means in this context. To any string $a = a_{127}a_{126}\dots a_0 \in \{0,1\}^{128}$, we associate its polynomial $a(X) = a_{127}X^{127} + a_{126}X^{126} + \cdots + a_0$. Addition of bit strings is defined as the bitwise XOR, as usual. Multiplication of two bit strings is defined as the multiplication of the two polynomials in $\mathrm{GF}(2^{128})$ modulo $q(X) = X^{128} + X^7 + X^2 + X + 1$.

(a) The masking is of the form $2^\alpha 3^\beta 7^\gamma \cdot E_K(N)$. Give the polynomials associated with "2", "3", and "7".

(b) Suppose that for a certain value of N, $E_K(N) = \underbrace{0\dots0}_{123}10101$. Compute $2^3 \cdot E_K(N)$ and $2^3 3 \cdot E_K(N)$.

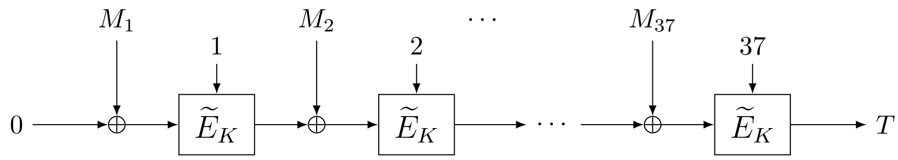
(c) Suppose that for a certain value of N, $E_K(N) = 1\underbrace{0\ldots0}_{127}$. Compute $2 \cdot E_K(N)$.

(d) It is rather weird that XEX_K uses $2, 3, 7$ as masks and not $2, 3, 5$. Try to find out why. (Hint: admissible domains.)

6. **(10 points)** Let $\widetilde{E} : \{0,1\}^k \times [1, 37] \times \{0,1\}^n \to \{0,1\}^n$ be a tweakable block cipher. Consider the PRF construction

$$F : \{0,1\}^k \times (\{0,1\}^n)^{37} \to \{0,1\}^n$$

that operates by first splitting the $37n$-bit message into 37 n-bit chunks $M_1 \| \cdots \| M_{37}$ and then processing this message as follows:



For this assignment, it is important to note that F generates authentication tags for messages that are of size *EXACTLY* $37n$ bits.

(a) We will consider the PRF security of F against any distinguisher that can make q construction queries of $37n$ bits. Prove that F is a secure PRF up to the following bound:

$$\mathbf{Adv}_F^{\mathrm{prf}}(q) \leq 2 \cdot 37 \binom{q}{2} / 2^n + \mathbf{Adv}_{\widetilde{E}}^{\mathrm{tprp}}(37q)\,.$$

We have seen proofs in earlier assignments, but this one is a little bit harder. Therefore, we will give you some hints:

- It is easier to reason about the construction if the underlying primitives behave as random functions. The first two steps will move you from above construction to a construction based on random functions.
- Then, note that if for two *different* queries (i.e., with $M^{(i_1)} \neq M^{(i_2)}$) the input to the last random function never collides, we are fine as the output tags are independently generated using a random function.
- So, the big question is to upper bound a *non-trivial* (i.e., with $M^{(i_1)} \neq M^{(i_2)}$) collision at the last random function, and here you will have to apply induction.
- There is no page limit, but as a reference: in the solutions of this assignment the proof takes around 1 page including two figures.
- Remark: it is possible to derive a slightly stronger bound. In particular, if you would opt for the so-called "H-coefficient technique", this is possible and you will get a slightly tighter bound, but the analysis is a bit more cumbersome.

Good luck!

(b) Suppose we would stretch the usage of F and allow it for all messages of size a positive multiple of n bits, up to $37n$ bits. In other words, for an n-bit message M_1, one generates tag $T = \widetilde{E}_K(1, M_1)$, for a $2n$-bit message $M_1 \| M_2$ one generates tag $T = \widetilde{E}_K(2, \widetilde{E}_K(1, M_1) \oplus M_2)$, etc. Then, the scheme is vulnerable to a trivial distinguishing attack. Describe the attack. You do not have to derive a success probability.