Advanced crypto
DM

"For XMAS, I'd like to have a PRP-to-PRF construction that is secure beyond the birthday bound"

2023-12-21

Instructions. This homework is graded as part of the *contrôle continu*. You must send a written report (in a portable format) detailing your answers to the questions by 2024-01-26T18:00+0100 to:

pierre.karpman@univ-grenoble-alpes.fr.

N.B. Working in teams is *not* allowed.

For XMAS, F. asks for a construction of a PRF from a PRP that would be secure beyond the birthday bound. Since F. was very nice for the whole year and this is his only wish, Santa tasks the North Pole elves to find such a construction.

Q.1: Let $E : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher with n-bit keys and blocks. The first elf is a bit lazy, and suggests to build the family of functions $\mathrm{FF}[E]$ derived from E as $\mathrm{FF}[E](k, x) = E(k, x) \oplus x$.

1. Show that $\mathbf{Adv}^{\mathrm{PRF}}_{\mathrm{FF}[E]}(t, q) = \mathbf{Adv}^{\mathrm{PRF}}_{E}(t', q)$, with $t' \propto t$.
2. Justify the informal sentence: "The first elf was not successful".

Q.2: The second elf strayed a bit far from the assignment, and forgot that the PRF should be built from a PRP, and not just a block cipher.

Assume now that E (as above) is an *ideal block cipher* in the sense that the 2^n permutations $\{E(0,\cdot), \ldots, E(2^n - 1, \cdot)\}$* are sampled uniformly and independently (with replacement) from the set of all permutations over $\{0,1\}^n$. The second elf then suggests to use the family of functions $\mathrm{SI}[E]$ derived from E and defined as $\mathrm{SI}[E](k, x) = E(x, k)$.

1. Show that *when the relevant probabilities are computed over the universe that includes the sampling of* E, one has $\mathbf{Adv}^{\mathrm{PRF}}_{\mathrm{SI}[E]}(t, q) = 0$.

We now return to the case where E is not necessarily ideal, but assume an *(n-bit) ideal permutation model* (that is, every security definition is augmented with an additional oracle uniformly sampled from the permutations over $\{0,1\}^n$).

2. Show that one may have a block cipher E s.t. $\mathbf{Adv}^{\mathrm{PRF}}_{\mathrm{SI}[E]}(t, q) \gg \mathbf{Adv}^{\mathrm{PRF}}_{E}(t, q)$.
3. Was the second elf successful? Comment on the advantages and disadvantages of the $\mathrm{SI}[E]$ construction.

*In this notation, we freely use integers to denote the n-bit strings corresponding to their respective n-bit binary representations.

Q.3: Let now $\mathcal{P}$ denote the uniform distribution over permutations over $\{0,1\}^n$; for $P : \{0,1\}^n \to \{0,1\}^n$ a permutation, let $\mathrm{X}[P] : \{0,1\}^{n-1} \to \{0,1\}^n$ be the function defined as $P(0\|x) \oplus P(1\|x)$ (where $\cdot\|\cdot$ is the operator for string concatenation), and let $\mathrm{X}[\mathcal{P}]$ denote the corresponding distribution for uniform P; let $\mathcal{F}$ denote the uniform distribution over functions from $\{0,1\}^{n-1} \to \{0,1\}^n$.

The third elf believes that a suitable present could be the function family $\mathrm{X}[E]$, derived from a block cipher E as $\mathrm{X}[E](k,x) = E(k,0\|x) \oplus E(k,1\|x)$. To determine whether this is the case, a possible strategy is to find an upper-bound for the distinguishing advantage $\mathbf{Adv}^{\mathrm{X}[\mathcal{P}],\mathcal{F}}$ of an adversary with access to one oracle that is sampled from either $\mathrm{X}[\mathcal{P}]$ or $\mathcal{F}$.

Let τ be an (unordered) transcript obtained by a distinguisher for $\mathrm{X}[\mathcal{P}]$ and $\mathcal{F}$. We say that τ is *bad* if it includes an oracle answer equal to 0 (the all-zero n-bit string). We write ${p_{\mathrm{bad}}}^{\mathcal{X}}(q)$ the probability that a bad transcript of q queries is produced when the oracle is sampled from the distribution $\mathcal{X} \in \{\mathrm{X}[\mathcal{P}], \mathcal{F}\}$

1. Show that for all q, ${p_{\mathrm{bad}}}^{\mathrm{X}[\mathcal{P}]}(q) = 0$.
2. Give an exact expression for ${p_{\mathrm{bad}}}^{\mathcal{F}}(q)$, and show that it is upper-bounded by $q/2^n$.

   Hint: The third elf suggests to use the inequality $(1-x)^q \geqslant 1 - qx$ (when $0 \leqslant x \leqslant 1$).

We now consider *good* (not bad) transcripts τ, and write $\#\,\mathrm{comp}^{\mathrm{X}[\mathcal{P}]}(\tau)$ the *number* of permutations P such that $\mathrm{X}[P]$ is compatible with τ.

3. Show that for τ made of q queries, $\#\,\mathrm{comp}^{\mathrm{X}[\mathcal{P}]}(\tau) \geqslant (2^n - 2q)! \prod_{i=0}^{q-1}(2^n - 4i)$.

   Hint: The third elf suggests to use an induction. (In slightly more details, the suggestion is to find a lower-bound on the number of values P may take to satisfy the q^{th} query, provided that it satisfies the $(q-1)^{\mathrm{th}}$ first ones.)

The third elf has shown that for $n \geqslant 13$ and $q \leqslant 2^{3n/4}$.[†]

$$\frac{(2^n)^q \prod_{i=0}^{q-1}(2^n - 4i)}{(2^n)_{2q}} \geqslant 1 - \frac{4q^3}{2^{2n} - 4q2^n + 4q^2} \geqslant 1 - \frac{5q^3}{2^{2n}} \tag{1}$$

4. Use this upper-bound and the result of the previous questions to give an upper-bound for $\mathbf{Adv}^{\mathrm{X}[\mathcal{P}],\mathcal{F}}(q)$.
5. Use this to derive an upper-bound for $\mathbf{Adv}^{\mathrm{PRF}}_{\mathrm{X}[E]}(t,q)$.
6. Justify the informal sentence: "The third elf was successful".
7. (Bonus) Show (1) (or similar).

N.B. The above analysis of $\mathrm{X}[E]$ is partly inspired by Iwata's analysis of his CENC mode of operation. It is in fact not tight: one may show that the generic term in the PRF security of this construction is $\Theta(q/2^n)$ (cf. for instance Dai, Hoang and Tessaro, 2017).

[†] This choice of upper-bound for q is somewhat arbitrary but is without loss of generality since the overall lower-bound becomes vacuous around $q \approx 2^{2n/3}$.