Advanced crypto
TD#1

2023-W48/49

Security of an iterated random permutation (Adapted from the Final Exam 2022)

This exercise is based on the article: The Iterated Random Permutation Problem with Applications to Cascade Encryption *(Minaud & Seurin, CRYPTO 2015).*

Preliminaries

In all of the following, except specified otherwise, distinguishers are deterministic algorithms that have access to an oracle and make their oracle queries adaptively.

We give and recall the following notation, definitions and results.

Advantage. We write $\mathbf{Adv}_{A_{\mathsf{q}}^{\mathbb{O}}}^{\mathcal{D},\mathcal{D}'} := \left|\Pr\left[A_{\mathsf{q}}^{\mathbb{O}} = 1 : \mathbb{O} \sim \mathcal{D}\right] - \Pr\left[A_{\mathsf{q}}^{\mathbb{O}} = 1 : \mathbb{O} \sim \mathcal{D}'\right]\right|$ the advantage that a distinguisher A that makes q queries to its oracle $\mathbb{O}$ has of distinguishing between $\mathbb{O} \sim \mathcal{D}$ and $\mathbb{O} \sim \mathcal{D}'$.

We then further write $\mathbf{Adv}^{\mathcal{D},\mathcal{D}'}(\mathsf{q})$ for $\max_{A_{\mathsf{q}}^{\mathbb{O}}} \ \mathbf{Adv}_{A_{\mathsf{q}}^{\mathbb{O}}}^{\mathcal{D},\mathcal{D}'}$, where the maximum is over all distinguishers (with unbounded computational cost) that make q queries to their oracle.

H-coefficients method. Let T^{q} be the set of all unordered transcripts that can be produced by any distinguisher making q queries to an oracle sampled from $\mathcal{D}$ or $\mathcal{D}'$, and $\mathsf{T}^{A} \subseteq \mathsf{T}^{\mathsf{q}}$ the set of transcripts that can be produced by a given distinguisher A. Further let $\mathsf{p}_{\tau}^{\mathcal{D}}$ (resp. $\mathsf{p}_{\tau}^{\mathcal{D}'}$) be the probability with which $\tau \in \mathsf{T}^{\mathsf{q}}$ may be produced by A when the oracle is sampled from $\mathcal{D}$ (resp. $\mathcal{D}'$).[1] Further let $\mathsf{T}_{\mathsf{good}}^{\mathsf{q}}$ and $\mathsf{T}_{\mathsf{bad}}^{\mathsf{q}}$ define a partition of T^{q} and ε be such that $\tau \in \mathsf{T}_{\mathsf{good}}^{\mathsf{q}} \Rightarrow \mathsf{p}_{\tau}^{\mathcal{D}}/\mathsf{p}_{\tau}^{\mathcal{D}'} \geqslant 1-\varepsilon$; then if $\mathsf{p}_{\mathsf{bad}}$ is such that for all A, the probability that A produces a transcript $\tau \in \mathsf{T}_{\mathsf{bad}} \cap \mathsf{T}^{A}$ when $\mathbb{O} \sim \mathcal{D}'$ is less than $\mathsf{p}_{\mathsf{bad}}$, one has the upper-bound $\mathbf{Adv}^{\mathcal{D},\mathcal{D}'}(\mathsf{q}) \leqslant \varepsilon + \mathsf{p}_{\mathsf{bad}}$.

(Iterated) (cyclic) permutations. We write P for a permutation sampled uniformly from all the permutations over $[\![1,\mathsf{N}]\!]$, P^2 for $P \circ P$ (where P is as previously), and for $\mathsf{r} > 2$, $P^{\mathsf{r}} := P \circ P^{\mathsf{r}-1}$ (that is, P^{r} is the r-time composition of P). We write C for a permutation sampled uniformly from all the cyclic permutations over $[\![1,\mathsf{N}]\!]$ (that is, permutations with a single cycle of size N. In other words, $C(1), C(C(1)), \ldots, C^{\mathsf{N}-1}(1)$ are pairwise distinct), and define C^{r} similarly as P^{r}. Finally we write $\mathcal{P}$ (resp. $\mathcal{P}^{\mathsf{r}}$, $\mathcal{C}$, $\mathcal{C}^{\mathsf{r}}$) for the uniform distribution underlying P (resp. P^{r}, C, C^{r}).

Questions

The goal of this exercise is to (partially) derive an upper-bound for $\mathbf{Adv}^{\mathcal{P},\mathcal{P}^{\mathsf{r}}}(\mathsf{q})$.

Q.1: Show that if $\mathbf{Adv}^{\mathcal{P},\mathcal{C}}(\mathsf{q}) \leqslant \alpha$, $\mathbf{Adv}^{\mathcal{C},\mathcal{C}^{\mathsf{r}}}(\mathsf{q}) \leqslant \beta$, $\mathbf{Adv}^{\mathcal{C}^{\mathsf{r}},\mathcal{P}^{\mathsf{r}}}(\mathsf{q}) \leqslant \gamma$, then $\mathbf{Adv}^{\mathcal{P},\mathcal{P}^{\mathsf{r}}}(\mathsf{q}) \leqslant \alpha+\beta+\gamma$.

[1] Recall that this probability is the same for every distinguisher A that produces τ with non-zero probability.

Q.2: Show that $\mathbf{Adv}^{\mathcal{C}^r,\mathcal{P}^r}(q) \leqslant \mathbf{Adv}^{\mathcal{C},\mathcal{P}}(rq)$.
HINT: Show that any distinguisher for $\mathcal{C}^r$ and $\mathcal{P}^r$ can be converted into a distinguisher for $\mathcal{C}$ and $\mathcal{P}$.

Q.3:

1. Show that the number of cyclic permutations over $[\![1, N]\!]$ is equal to $(N-1)!$.
2. Show that the number of cyclic permutations over $[\![1, N]\!]$ that map 1 to 2 is equal to $(N-2)!$.
3. Show that the number of cyclic permutations over $[\![1, N]\!]$ that map 1 to 2, 2 to 3, …, q to $(q+1)$ is equal to $(N-1-q)!$.

   We say that those permutations *define* q points in a single *chain* of size q.[2]
4. Show that the number of cyclic permutations over $[\![1, N]\!]$ that map 1 to 2 and 3 to 4 is equal to $(N-3)!$.

   We say that those permutations define 2 points in two chains of size 1.
5. Show that the number of cyclic permutations over $[\![1, N]\!]$ for which q points are *defined* (in any number of chains) is equal to $(N-1-q)!$.
   HINT: You may show this "directly", or by using an induction showing that the number of permutations that define $q = q_1 + q_2$ points in two chains of size q_1 and q_2 (i.e. with $q_1 + 1$ and $q_2 + 1$ points respectively) is equal to the number of permutations that define q points in one chain of size q.
6. Show that the number of (non-necessarily cyclic) permutations over $[\![1, N]\!]$ for which q points are defined (in any number of chains) is equal to $(N-q)!$.

Q.4: Show that $\mathbf{Adv}^{\mathcal{P},\mathcal{C}}(q) \leqslant q/N$, using the H-coefficients method.
HINT. Use bad transcripts T_{bad} such that $\tau \in T_{\mathsf{bad}} \Rightarrow p^{\tau}_{\mathcal{C}} = 0$.

Q.5: Suppose $r \leqslant N$, and let $d = \gcd(r, N) \leqslant r$ and $N' := N/d$. Show that C^r is a permutation with *cycle structure* $[N']^d$, i.e. a permutation with d cycles of size N'.

We now admit that $\mathcal{C}^r$ uniformly samples permutations over the ones with cycle structure $[N']^d$.

Q.6: Let again $d = \gcd(r, N)$, $N' = N/d$.

1. Specify an adaptive distinguisher A for $\mathcal{C}$ and $\mathcal{C}^r$ such that $d > 1 \land q \geqslant N' \Rightarrow \mathbf{Adv}^{\mathcal{C},\mathcal{C}^r}_{A^{\mathbb{O}}_q} = 1$.
2. Explain why there is no *non-adaptive* distinguisher A' such that $d > 1 \land q \geqslant N' \Rightarrow \mathbf{Adv}^{\mathcal{C},\mathcal{C}^r}_{A'^{\mathbb{O}}_q} = 1$.

Q.7: One can show that for all distinguisher A, $q < N' \Rightarrow \mathbf{Adv}^{\mathcal{C},\mathcal{C}^r}_{A^{\mathbb{O}}_q} = 0$. Give an upper-bound for $\mathbf{Adv}^{\mathcal{P},\mathcal{P}^r}(q)$.

[2] Be advised that here, what we call the *size* of the chain is one less than the *number of points* it contains.