A Short Proof of the PRP/PRF Switching Lemma

Donghoon Chang[1]* and Mridul Nandi[2]

[1] Center for Information Security Technologies (CIST)
Korea University, Seoul, Korea
dhchang@cist.korea.ac.kr
[2] CINVESTAV-IPN, Mexico City
mridul.nandi@gmail.com

Abstract. In Eurocrypt 2006, Bellare and Rogaway [2] gave a proof of the PRP/PRF switching Lemma using their game-based proof technique. In the appendix of the same paper, they also gave an proof without games. In this paper, we give another proof of the switching lemma, which is simple and mathematically-clear and easy to uderstand. Our proof is based on *the strong interpolation theorem*.

Keywords : PRF, PRP, Switching Lemma.

1 Some Notations and Results

This section is almost same as that of [3].

Counting. Let $\mathcal{F} := \text{Func}(n, n)$, the set of all functions $f : \{0,1\}^n \to \{0,1\}^n$. And let $\mathcal{P} := \text{Perm}(n, n)$, the set of all permutations $f : \{0,1\}^n \to \{0,1\}^n$. It is easy to see that $|\mathcal{F}| = 2^{n2^n}$ and $|\mathcal{P}| = 2^n!$. Now, for any distinct a_i's and any distinct z_i's, the number of functions f such that $f(a_1) = z_1, \cdots, f(a_q) = z_q$ is exactly $2^{n(2^n-q)}$ because, the outputs of q elements are fixed and the rest $(2^n - q)$ many outputs can be chosen in $(2^n)^{(2^n-q)}$ many ways. Similarly, for any distinct a_i's and any distinct z_i's, the number of permutations f such that $f(a_1) = z_1, \cdots, f(a_q) = z_q$ is exactly $(2^n-q)!$. Thus, $\Pr_{\mathtt{u}}[\mathtt{u}(a_1) = z_1, \cdots, \mathtt{u}(a_q) = z_q] = \frac{1}{2^{nq}}$ where $\mathtt{u}$ is the uniform random function on $\mathcal{F}$ (an uniform random variable taking values on $\mathcal{F}$). And $\Pr_{\pi}[\pi(a_1) = z_1, \cdots, \pi(a_q) = z_q] = \frac{1}{2^n} \times \frac{1}{2^n-1} \cdots \frac{1}{2^n-q+1}$ where π is the uniform random permutation on $\mathcal{P}$ (an uniform random variable taking values on $\mathcal{P}$).

View. In this paper we consider a distinguisher $\mathcal{A}$ which has access of an oracle $\mathcal{O}$. We assume that $\mathcal{A}$ is deterministic and computationally unbounded. We

* The first author was supported by the MIC(Ministry of Information and Communication), Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Advancement) (IITA-2008-(C1090-0801-0025))

assume that all queries are distinct and it makes at most q queries to the oracle $\mathcal{O}$. Suppose $\mathcal{A}$ makes a_i as $\mathcal{O}$-query and obtains responses z_i, $1 \le i \le q$. The tuple $v = ((a_1, z_1), \cdots, (a_q, z_q))$ is called as the *view* of $\mathcal{A}$. We also denote $v_{\mathcal{O}}$ to specify that the view is obtained after interacting with $\mathcal{O}$. We define the first i query-response pairs of the tuple v by $v_i = ((a_1, z_1), \cdots, (a_i, z_i))$.

Advantage. Let $\mathtt{F}, \mathtt{G}$ be probabilistic oracle algorithms. We define advantage of the distinguisher $\mathcal{A}$ at distinguishing $\mathtt{F}$ from $\mathtt{G}$ as

$$\mathbf{Adv}_{\mathcal{A}}(\mathtt{F}, \mathtt{G}) = |\Pr[\mathcal{A}^{\mathtt{F}} = 1] - \Pr[\mathcal{A}^{\mathtt{G}} = 1]|.$$

Theorem 1. (Strong Interpolation Theorem) *If there is a set of good views $\mathcal{V}_{\text{good}}$ such that*

1. *for all $v \in \mathcal{V}_{\text{good}}$, $\Pr[v_{\mathtt{F}} = v] \ge (1 - \varepsilon) \times \Pr[v_{\mathtt{G}} = v]$ and*
2. $\Pr[v_{\mathtt{G}} \in \mathcal{V}_{\text{good}}] \ge 1 - \varepsilon'$

then for any $\mathcal{A}$ we have $\mathbf{Adv}_{\mathcal{A}}(\mathtt{F}, \mathtt{G}) \le \varepsilon + \varepsilon'$.

Proof. This is directly from the idea explained in [1]. ■

2 a short proof of PRP/PRF Switching Lemma

Lemma 1 (PRP/PRF Switching Lemma). *Let $n \ge 1$ be an integer. Let $\mathcal{A}$ be a distinguisher that asks at most q oracle queries. Then*

$$|\Pr[\mathcal{A}^{\mathtt{u}} = 1] - \Pr[\mathcal{A}^{\pi} = 1]| \le \frac{q(q-1)}{2^{n+1}},$$

where $\mathtt{u}$ is the uniform random function on $\mathcal{F}$ and π is the uniform random permutation on $\mathcal{P}$.

Proof. Our proof is based on *the strong interpolation theorem*. The organization of our proof is as follows. First, we define a set of good views $\mathcal{V}$good and give a lower bound of $\Pr[v_{\mathtt{F}} = v]$ for all $v \in \mathcal{V}_{\text{good}}$, where $\mathtt{F}$ is $\mathtt{u}$. And we give an upper bound of $\Pr[v_{ttG} = v]$ for all $v \in \mathcal{V}_{\text{good}}$, where $\mathtt{G}$ is π. Then, we compute ε and ε' such that for all $v \in \mathcal{V}_{\text{good}}$, $\Pr[v_{\mathtt{F}} = v] \ge (1 - \varepsilon) \times \Pr[v_{\mathtt{G}} = v]$ and $\Pr[v_{\mathtt{G}} \in \mathcal{V}_{\text{good}}] \ge 1 - \varepsilon'$. Finally, based on Theorem 1 (strong interpolation theorem), we conclude that $|\Pr[\mathcal{A}^{\mathtt{u}} = 1] - \Pr[\mathcal{A}^{\pi} = 1]| \le \varepsilon' + \varepsilon$.

- $\mathcal{V}$good is a set of good views $v = ((a_1, z_1), \cdots, (a_q, z_q))$ such that a_i's are distinct and z_i's are also distinct.
- For all $v \in \mathcal{V}_{\text{good}}$, $\Pr[v_{\mathtt{u}} = v] = \frac{1}{2^{nq}}$.
- For all $v \in \mathcal{V}_{\text{good}}$, $\Pr[v_{\pi} = v] = \frac{1}{2^n} \times \frac{1}{2^n - 1} \cdots \frac{1}{2^n - q + 1} = 2^{-nq} \times \frac{1}{1 - \frac{1}{2^n}} \times \cdots \times \frac{1}{1 - \frac{q-1}{2^n}} \le 2^{-nq} \times \frac{1}{1 - \frac{1 + 2 + \cdots + (q-1)}{2^n}} = 2^{-nq} \times \frac{1}{1 - \frac{q(q-1)}{2^{n+1}}}$.

- For all $v \in \mathcal{V}_{\text{good}}$, $\Pr[v_{\mathtt{u}} = v] \geq (1-\varepsilon) \times \Pr[v_{\pi} = v] \Leftarrow \frac{1}{2^{nq}} \geq (1-\varepsilon) \times 2^{-nq} \times \frac{1}{1-\frac{q(q-1)}{2^{n+1}}} \Leftrightarrow 1 - \frac{q(q-1)}{2^{n+1}} \geq 1 - \varepsilon \Leftarrow \varepsilon = \frac{q(q-1)}{2^{n+1}}$.
- $\Pr[v_{\pi} \in \mathcal{V}_{\text{good}}] = 1 \Leftrightarrow \varepsilon' = 0$

Therefore $|\Pr[\mathcal{A}^{\mathtt{u}} = 1] - \Pr[\mathcal{A}^{\pi} = 1]| \leq \varepsilon' + \varepsilon = \frac{q(q-1)}{2^{n+1}}$. ■

References

1. D. J. Bernstein. A short proof of the unpredictability of cipher block chaining. http://cr.yp.to/antiforgery/easycbc-20050109.pdf , 2005.
2. M. Bellare and P. Rogaway, *Code-Based Game-Playing Proofs and the Security of Triple Encryption*, Advances in Cryptology - Eurocrypt'06, LNCS 4004, Springer-Verlag, pp. 409-426, 2006.
3. D. Chang and M. Nandi, *Improved Indifferentiability security analysis of chopMD Hash Function*, Appears in FSE'08.