Power of a Public Random Permutation and its Application to Authenticated-Encryption

Kaoru Kurosawa

Department of Computer and Information Sciences,
Ibaraki University,
4-12-1 Nakanarusawa, Hitachi, Ibaraki, 316-8511, Japan
Tel/Fax. +81-294-38-5135
E-mail. kurosawa@mx.ibaraki.ac.jp

Abstract

In this paper, we first show that *many* independent pseudorandom permutations over $\{0,1\}^n$ can be obtained from a single *public* random permutation and *secret* n bits. We next prove that a slightly modified IAPM is secure even if the underlying block cipher F is publicly accessible (as a blackbox). We derive a similar result for OCB mode, too. The security proofs are based on our first result and are extremely simple. We finally show that our security bound is tight within a constant factor.

Keywords: authenticated-encryption, DESX, IAPM, OCB mode, pseudorandom permutation

1 Introduction

DESX was proposed by Rivest in order to strength the security of DES. It is defined for a block cipher F over $\{0,1\}^n$ as

$$P(x) = F(x \oplus S) \oplus S, \tag{1}$$

where S is a secret mask randomly chosen from $\{0,1\}^n$. Assume that F is ideal. Then Even and Mansour showed that DESX is secure even if the underlying block cipher F is publicly accessible (as a blackbox) [2].

Kilian and Rogaway [7] showed that its effective key length increases from $n - \log_2 \mu$ bits to $n + \kappa - \log_2 \mu$ bits if the key K of F is kept secret, where κ is the bit length of K and μ bounds the number of queries the adversary can ask to the encryption oracle.

On the other hand, Jutla [5] recently proposed an authenticated-encryption scheme, called IAPM, which consists of many DESX together with a simple checksum. Its computational cost is significantly lower than trivial schemes which just concatenate an encryption scheme with a MAC scheme. Jutla proved that IAPM and his another scheme IACBC are secure against chosen plaintext attack in the sense of indistinguishability (IND-CPA) and satisfy authenticity of ciphertexts. (It is known that this combination implies indistinguishability under the strongest form of chosen ciphertext attack (IND-CCA) [1, 6].)

Some variants of IAPM and IACBC were suggested by Gligor and Donsecu (XECB and XCBC) [3] and by Rogaway et al. (OCB mode) [9]. Halevi showed that universal hash functions can be used for mask generation in these schemes [4].

In this paper, we first show that *many* independent pseudorandom permutations $P_1, \cdots, P_m$ can be obtained from a single *public* random permutation F and *secret* n bits. Note that Even and Mansour [2] showed that a *single* pseudorandom permutation $P(x)$ is obtained from the same cryptographic resource by eq.(1).

We next prove that a slightly modified IAPM is secure even if the underlying block cipher F is publicly accessible (as a blackbox). The security proofs are based on our first result and are extremely simple. No extra cost is required in this modification. We derive a similar result for OCB mode, too.

We finally prove that our security bound is tight within a constant factor under some condition.

(Related work:) Independently of our work, Listov, Rivest and Wagner introduced a new cryptographic prmitive "tweakable block cihphers" recently [8] which contains a notion of variability. A tweakable block cipher takes a tweak as well as a key and a message. Their second construction of tweakable block ciphers [8, Sec.3.1] is the same as ours (of Sec.2.1 below) except for that the underlying block cipher F is publicly accessible (as a blackbox) in ours. In other words, our construction can be used as a tweakable block cipher such that the underlying block cipher F is publicly accessible. Further, their security bound [8, Thorem 2] is obtained as a special case of ours (Theorem 2.1 and its proof below). (The complexity theoretic bound is obtained easily from the information theoretic bound by using a standard technique.)

2 Power of a Public Random Permutation

Even and Mansour [2] showed that a *single* pseudorandom permutation P can be obtained from a public random permutation F over $\{0,1\}^n$ and a secret n bits mask S by eq.(1).

This section shows that we can construct *many* independent pseudorandom permutations $P_1, \cdots, P_m$ over $\{0,1\}^n$ from the same cryptographic resource, that is, a *single* public random permutation F over $\{0,1\}^n$ and secret n bits.

2.1 How to construct many pseudorandom permutations

Definition 2.1 *Let H be a set of hash functions $h : X \to \{0,1\}^n$. We say that H is an (ϵ, δ)-*almost XOR universal *((ϵ,δ)-AXU) hash function family if*

1. *for any element $x \in X$ and any element $y \in \{0,1\}^n$,*

$$\Pr_h(h(x) = y) \leq \delta$$

2. *for any two distinct elements $x, x' \in X$ and any element $y \in \{0,1\}^n$,*

$$\Pr_h(h(x) \oplus h(x') = y) \leq \epsilon.$$

We show some examples.

1. Let $H_1 = \{h_a(x) = a \cdot x \text{ over } \mathrm{GF}(2^n)\}$. Then H_1 is a $(1/2^n, 1/2^n)$-AXU hash function family from $\{0,1\}^n \setminus \{0^n\}$ to $\{0,1\}^n$.

2. Let $H_2 = \{h_a(x_1, x_2) = ax_1 + a^2 x_2 \text{ over } \mathrm{GF}(2^n)\}$. Then H_2 is a $(1/2^{n-1}, 1/2^{n-1})$-AXU hash function family from $\{0,1\}^{2n} \setminus \{0^{2n}\}$ to $\{0,1\}^n$.

Now define m permutations $P_1, \cdots, P_m$ as follows. Let H be a (ϵ, δ)-AXU hash function family from X to $\{0,1\}^n$. For any distinct $i_1, \cdots, i_m \in X$, let

$$\begin{aligned} S_j &= h(i_j) \\ P_j(x) &= F(x \oplus S_j) \oplus S_j \end{aligned}$$

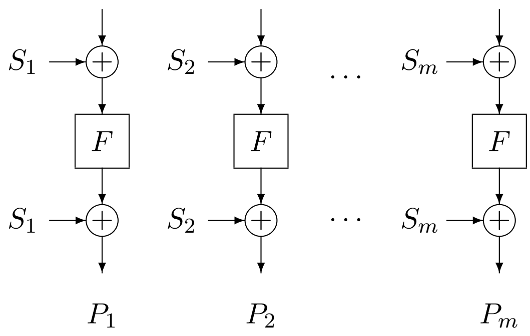

Figure 1: $P_1, P_2, \ldots, P_m$

for $i = 1, \cdots, m$, where h is randomly chosen from H. (See Fig.1.)

We will show that $P_1, \cdots, P_m$ are indistinguishable from m independently chosen random permutations $Q_1, \cdots, Q_m$ over $\{0,1\}^n$ even if distinguishers have oracle access to F and F^{-1}. For example, let $H = H_1$. Then note that $P_1, \cdots, P_m$ are constructed from a single public random permutation F and a secret n bit a.

Let D be an adaptive distinguisher which has $2m+2$ oracles. In $Game0$, D has oracle access to $Q_1, Q_1^{-1}, \cdots, Q_m, Q_m^{-1}$ and F, F^{-1}. In $Game1$, D has oracle access to $P_1, P_1^{-1}, \cdots, P_m, P_m^{-1}$ and F, F^{-1}. In each game, suppose that D makes at most q_1 queries to F, F^{-1} in total and at most q_0 queries to the other oracles in total. Define

$$Adv_D(q_0, q_1) \stackrel{\triangle}{=} |\Pr(D = 1 \text{ in } Game0) - \Pr(D = 1 \text{ in } Game1)|$$

and $Adv(q_0, q_1) \stackrel{\triangle}{=} \max_D Adv_D(q_0, q_1)$. Then we prove the following theorem.

Theorem 2.1

$$Adv(q_0, q_1) \le 2\binom{q_0}{2}\epsilon + 2q_0q_1\delta + \frac{q_0(q_0 + 2q_1 - 1)}{2^n}.$$

Note that the right hand side of the above equation is independent of m.

2.2 Proof of Theorem 2.1

Suppose that a distinguisher D makes at most q_1 queries to F, F^{-1} in total and at most q_0 queries to the other oracles in total. Let ϕ_0 denote the event that $D = 1$ in $Game0$ and ϕ_1 denote the event that $D = 1$ in $Game1$.

In $Game1$, let GOOD denote the event that the inputs to F are all distinct and the outputs of F are all distinct. Let $\mathsf{BAD} = \neg\mathsf{GOOD}$. Then we have

$$\begin{aligned}
\Pr[\phi_1] &= \Pr[\phi_1 \wedge \neg\mathsf{BAD}] + \Pr[\phi_1 \wedge \mathsf{BAD}] \\
&= \Pr[\phi_1 \mid \neg\mathsf{BAD}] \Pr[\neg\mathsf{BAD}] + \Pr[\phi_1 \mid \mathsf{BAD}] \Pr[\mathsf{BAD}] \\
&= \Pr[\phi_1 \mid \neg\mathsf{BAD}](1 - \Pr[\mathsf{BAD}]) + \Pr[\phi_1 \mid \mathsf{BAD}] \Pr[\mathsf{BAD}] \\
&= \Pr[\phi_1 \mid \neg\mathsf{BAD}] + \Pr[\mathsf{BAD}](\Pr[\phi_1 \mid \mathsf{BAD}] - \Pr[\phi_1 \mid \neg\mathsf{BAD}])
\end{aligned}$$

Hence

$$\begin{aligned}
Adv_D(q_0, q_1) &= |\Pr[\phi_1] - \Pr[\phi_0]| \\
&\leq |\Pr[\phi_1 \mid \neg\mathsf{BAD}] - \Pr[\phi_0]| \\
&\quad + |\Pr[\mathsf{BAD}](\Pr[\phi_1 \mid \mathsf{BAD}] - \Pr[\phi_1 \mid \neg\mathsf{BAD}])| \\
&\leq |\Pr[\phi_1 \mid \neg\mathsf{BAD}] - \Pr[\phi_0]| + \Pr[\mathsf{BAD}]
\end{aligned}$$

We first show that

$$|\Pr[\phi_1 \mid \neg\mathsf{BAD}] - \Pr[\phi_0]| \leq \frac{q_0(q_0 + 2q_1 - 1)}{2^{n+1}}.$$

Suppose that D queries $X = (x_1, \cdots, x_{q_0+q_1})$ to the oracles, and receives $Y = (y_1, \cdots, y_{q_0+q_1})$ from the oracles. Since D is deterministic, each of her query x_{i+1} is completely determined by the previous answers $y_1, \cdots, y_i$ from the oracles. Similarly, the final output of D (0 or 1) is determined by the all answers $Y = (y_1, \cdots, y_{q_0+q_1})$ which D received from the oracles. Let Γ denote the set of Y such that $D = 1$.

Let $\mathcal{Y}_0$ be the random variable induced by Y in $Game0$, and $\mathcal{Y}_1$ be the random variable induced by Y in $Game1$. Then

$$\Pr[\phi_0] = \sum_{Y \in \Gamma} \Pr[\mathcal{Y}_0 = Y] \tag{2}$$

$$\Pr[\phi_1 \mid \neg\mathsf{BAD}] = \sum_{Y \in \Gamma} \Pr[\mathcal{Y}_1 = Y \mid \neg\mathsf{BAD}] \tag{3}$$

Define

$$N(q) = 2^n(2^n - 1) \cdots (2^n - q + 1).$$

Lemma 2.1

$$\begin{aligned}\Pr[\mathcal{Y}_0 = Y] &\le \frac{1}{N(q_0)} \times \frac{1}{N(q_1)} \qquad (4)\\ \Pr[\mathcal{Y}_0 = Y] &\ge \frac{1}{(2^n)^{q_0}} \times \frac{1}{N(q_1)} \qquad (5)\end{aligned}$$

(Proof) Fix $Y = (y_1, \cdots, y_{q_0+q_1})$ arbitrarily. Then $X = (x_1, \cdots, x_{q_0+q_1})$ is determined by D as shown above.

Suppose that D queries $x_1, \cdots, x_{q_0}$ to Q_1-oracle and $x_{q_0+1}, \cdots, x_{q_0+q_1}$ to F-oracle. Then $y_i = Q_1(x_i)$ for $i = 1, \cdots q_0$, and $y_{q_0+i} = F(x_{q_0+i})$ for $i = 1, \cdots q_1$. Hence

$$\begin{aligned}\Pr[\mathcal{Y}_0 = Y] &= \Pr_{Q_1,F}[y_i = Q_1(x_i) \text{ for } i = 1, \cdots q_0 \text{ and}\\ &\qquad y_{q_0+i} = F(x_{q_0+i}) \text{ for } i = 1, \cdots q_1]\\ &= \frac{1}{N(q_0)} \times \frac{1}{N(q_1)}\end{aligned}$$

It is easy to see that this is the maximum value of $\Pr[\mathcal{Y}_0 = Y]$. In other words, eq.(4) holds for any D.

Similarly, it is easy to see that eq.(5) holds for any D.

Q.E.D.

Lemma 2.2

$$\Pr[\mathcal{Y}_1 = Y \mid \neg\mathsf{BAD}] = \frac{1}{N(q_0 + q_1)} \qquad (6)$$

(Proof) Fix $Y = (y_1, \cdots, y_{q_0+q_1})$ arbitrarily. Then $X = (x_1, \cdots, x_{q_0+q_1})$ is determined by D as shown above.

Suppose that D queries $x_1, \cdots, x_{q_0}$ to P_1-oracle and $x_{q_0+1}, \cdots, x_{q_0+q_1}$ to F-oracle. We first show a proof for this case. Note that

$$\begin{aligned}y_i &= P_1(x_i)\\ &= F(x_i \oplus h(i_1)) \oplus h(i_1)\end{aligned}$$

for $i = 1, \cdots q_0$, and

$$y_{q_0+i} = F(x_{q_0+i})$$

for $i = 1, \cdots q_1$. Let $a_i = x_i \oplus h(i_1)$ for $i = 1, \cdots, q_0$ and $a_{q_0+i} = x_{q_0+i}$ for $i = 1, \cdots, q_1$. Let $b_i = y_i \oplus h(i_1)$ for $i = 1, \cdots, q_0$ and $b_{q_0+i} = y_{q_0+i}$ for $i = 1, \cdots, q_1$. Then we have

$$F(a_i) = b_i$$

for $i = 1, \cdots, q_0 + q_1$. We say that h is good if all a_i are distinct. Fix a good h arbitrarily. Then we obtain that

$$\begin{aligned} \Pr[\mathcal{Y}_1 = Y \mid h \text{ is } \textit{good}] &= \Pr_F[F(a_i) = b_i \text{ for } i = 1, \cdots, q_0 + q_1] \\ &= \frac{1}{N(q_0 + q_1)} \end{aligned}$$

Finally $\neg\mathsf{BAD}$ is the event such that h is good. Hence we can see that

$$\Pr[\mathcal{Y}_1 = Y \mid \neg\mathsf{BAD}] = \frac{1}{N(q_0 + q_1)}$$

It is not hard to see that such a proof holds for any D.

Q.E.D.

Lemma 2.3

$$\Pr[\phi_0] \le \Pr[\phi_1 \mid \neg\mathsf{BAD}]$$

(Proof) From eq.(4) and eq.(6), we have

$$\frac{\Pr[Y_0 = y]}{\Pr[\mathcal{Y}_1 = Y \mid \neg\mathsf{BAD}]} \le \frac{N(q_0 + q_1)}{N(q_0)N(q_1)} \le 1.$$

Hence

$$\Pr[Y_0 = y] \le \Pr[\mathcal{Y}_1 = Y \mid \neg\mathsf{BAD}]$$

Therefore from eq.(2) and eq.(3), we have

$$\begin{aligned} \Pr[\phi_0] &= \sum_{Y \in \Gamma} \Pr[\mathcal{Y}_0 = Y] \\ &\le \sum_{Y \in \Gamma} \Pr[\mathcal{Y}_1 = Y \mid \neg\mathsf{BAD}] \\ &= \Pr[\phi_1 \mid \neg\mathsf{BAD}] \end{aligned}$$

Q.E.D.

Lemma 2.4

$$\Pr[\phi_1 \mid \neg\mathsf{BAD}] - \Pr[\phi_0] \le \frac{q_0(q_0 + 2q_1 - 1)}{2^{n+1}}$$

(Proof) From eq.(5) and eq.(6), we have

$$\begin{aligned}\frac{\Pr[Y_0 = y]}{\Pr[\mathcal{Y}_1 = Y \mid \neg\mathsf{BAD}]} &\geq \frac{N(q_0+q_1)}{(2^n)^{q_0} N(q_1)} \\ &= \left(1 - \frac{q_1}{2^n}\right) \cdots \left(1 - \frac{q_1+q_0-1}{2^n}\right)\end{aligned}$$

Let

$$p_i \triangleq \frac{q_1+i}{2^n}$$

for $0 \leq i \leq q_0 - 1$. Then we have

$$\begin{aligned}(1-p_0)(1-p_1)\cdots(1-p_{q_0-1}) &\geq 1 - (p_0 + p_1 + \cdots + p_{q_0-1}) \\ &= 1 - \frac{1}{2^n}(q_0 q_1 + \frac{q_0(q_0-1)}{2}) \\ &= 1 - \frac{q_0(q_0+2q_1-1)}{2^{n+1}}.\end{aligned}$$

Therefore

$$\Pr[Y_0 = y] \geq \Pr[\mathcal{Y}_1 = Y \mid \neg\mathsf{BAD}]\left(1 - \frac{q_0(q_0+2q_1-1)}{2^{n+1}}\right)$$

Hence from eq.(2) and eq.(3), we have

$$\begin{aligned}\Pr[\phi_0] &= \sum_{Y\in\Gamma} \Pr[\mathcal{Y}_0 = Y] \\ &\geq \sum_{Y\in\Gamma} \Pr[\mathcal{Y}_1 = Y \mid \neg\mathsf{BAD}]\left(1 - \frac{q_0(q_0+2q_1-1)}{2^{n+1}}\right) \\ &= \Pr[\phi_1 \mid \neg\mathsf{BAD}]\left(1 - \frac{q_0(q_0+2q_1-1)}{2^{n+1}}\right)\end{aligned}$$

Consequently we obtain that

$$\begin{aligned}\Pr[\phi_1 \mid \neg\mathsf{BAD}] - \Pr[\phi_0] &\leq \Pr[\phi_1 \mid \neg\mathsf{BAD}]\frac{q_0(q_0+2q_1-1)}{2^{n+1}} \\ &\leq \frac{q_0(q_0+2q_1-1)}{2^{n+1}}\end{aligned}$$

Q.E.D.

From Lemma 2.3 and Lemma 2.3, we obtain that

$$|\Pr[\phi_1 \mid \neg\mathsf{BAD}] - \Pr[\phi_0]| \leq \frac{q_0(q_0+2q_1-1)}{2^{n+1}}$$

We next estimate $\Pr[\mathsf{BAD}]$. Note that BAD is the event in $Game1$ that there exist a pair of inputs (u, v) to F or there exist a pair of outputs (u, v) of F such that $u = v$. It is easy to see that there exist $\binom{q_0}{2} + q_0 q_1$ input pairs to F and $\binom{q_0}{2} + q_0 q_1$ output pairs of F. Therefore, we have

$$\Pr[\mathsf{BAD}] \leq 2\binom{q_0}{2}\epsilon + 2q_0q_1\delta$$

from Def.2.1.

Consequently, we obtain that

$$\begin{aligned} Adv_D(q_0, q_1) &\leq |\Pr[\phi_1 \mid \neg\mathsf{BAD}] - \Pr[\phi_0]| + \Pr[\mathsf{BAD}] \\ &\leq 2\binom{q_0}{2}\epsilon + 2q_0q_1\delta + \frac{q_0(q_0 + 2q_1 - 1)}{2^n}. \end{aligned}$$

for any D.

3 Public Block Cipher Authenticated-Encryption

In this section, we first present a slight modification of IAPM. No extra cost is required in this modification. We next, by using Theorem 2.1, prove that the modified scheme satisfies confidentiality and message integrity even if adversaries have oracle access to the underlying block cipher F and F^{-1} as well as the encryption oracle $\mathcal{E}_{scheme}$. We call such security *enhanced* security.

Our security proofs are extremely simple. From Theorem 2.1, it is shown that each block of the modified IAPM can be viewed as an independent random permutation even against our strong adversaries. Then it is clear that it satisfies IND-CPA. Similarly, the proof of authenticity is very simple and intuitive.

Formally, we consider an adversary A such that $A^{\mathcal{E}_{scheme}, F, F^{-1}}$.

3.1 Modified IAPM

Let H be an (ϵ, δ)-AXU hash function family from $\{0,1\}^{2n} \setminus \{0^{2n}\}$ to $\{0,1\}^n$. For example, we can use H_2 shown in Sec.2.1. An encryptor and a decryptor share $h \in H$ secretly.

To encrypt an L-block plaintext $M = M_1||M_2||\cdots||M_L$ (with $M_j \in \{0,1\}^n$), the encryptor first picks a new nonce IV. Wlog, we assume that this nonce was never used before. The encryptor then generates $L+1$ masks $S_1, \cdots, S_L$ and T_L as follows.

$$\begin{aligned} S_i &= h(2i-1, IV) \text{ for } 1 \leq i \leq L, \\ T_L &= h(2L, IV) \end{aligned}$$

The ciphertext $C = C_0||C_1|| \cdots ||C_{L+1}$ is computed by setting $C_0 = IV$, $C_j = S_j \oplus F(S_j \oplus M_j)$ for $1 \leq j \leq L$, and

$$C_{L+1} = T_L \oplus F(T_L \oplus \sum_{j=1}^{L} M_j). \tag{7}$$

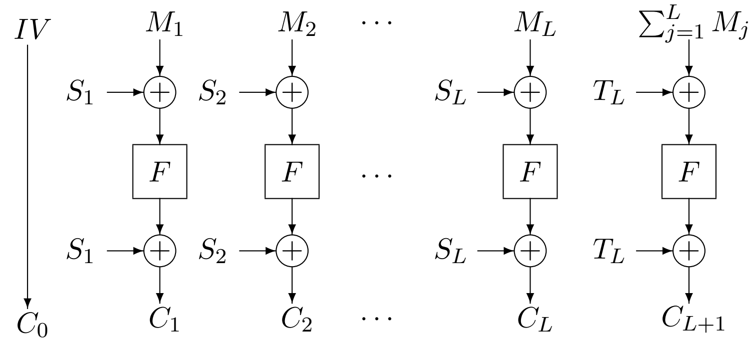

Figure 2: Modified IAPM

(See Fig. 2.) To decrypt a ciphertext of $L+2$ blocks, $C = C_0||C_1|| \cdots ||C_{L+1}$, the decryptor first computes the masks $S_1, \ldots, S_L$ and T_L. He then recovers $M_j = S_j \oplus F^{-1}(S_j \oplus C_j)$ for $1 \leq j \leq L$. He next check if eq.(7) holds. If the check passes, the plaintext is $M_1||M_2|| \cdots ||M_L$. Otherwise, the ciphertext is deemed invalid.

(Remark) In Jutla's IAPM,

$$C_{L+1} = S_0 \oplus F(S_{L+1} \oplus \sum_{j=1}^{L} M_j).$$

$S_0, S_1, \ldots, S_L + 1$ are generated by using a block cipher.

3.2 Random World

To prove the enhanced security of the modified IAPM by using Theorem 2.1, we introduce a *random* world as follows.

For each (j, IV), two random permutations $Q_{(j,IV)}$ and $R_{(j,IV)}$ are chosen independently. Both the encryptor and the decryptor have oracle access to them.

To encrypt an L-block plaintext $M = M_1||M_2||\cdots||M_L$, the encryptor first picks a new nonce IV. The encryptor computes the ciphertext $C = C_0||C_1||\cdots||C_{L+1}$ as $C_0 = IV,\ C_j = Q_{(j,IV)}(M_j)$ for $1 \leq j \leq L$, and

$$C_{L+1} = R_{(L,IV)}(\sum_{j=1}^{L} M_j). \tag{8}$$

To decrypt a ciphertext of $L+2$ blocks, $C = C_0||C_1||\cdots||C_{L+1}$, the decryptor computes $M_j = Q^{-1}_{(j,IV)}(C_j)$ for $1 \leq j \leq L$. The decryptor next checks if eq.(8) holds. If the check passes, the plaintext is $M_1||M_2||\cdots||M_L$. Otherwise, the ciphertext is deemed invalid.

It is clear that our scheme of 3.1 is indistinguishable from the random world from Theorem 2.1. This means that the security proofs are reduced to those in the random world, which makes our proofs extremely easy.

We denote the encryption oracle in the random world by $\mathcal{E}_{random}$.

3.3 Enhanced Confidentiality

We will show that no adversary can distinguish two encryption oracles, $\mathcal{E}_{scheme}$-oracle and $\mathcal{E}_{random}$-oracle, even if he has oracle access to F, F^{-1}. The adversary works as a distinguisher between them in this subsection.

Theorem 3.1 *Suppose that an adversary A asks at most α queries to the encryption oracle, totaling at most μ blocks, and asks at most q_1 queries to F and F^{-1}. Let $q_0 = \alpha + \mu$. Then*

$$\begin{aligned} & |\Pr(A^{\mathcal{E}_{scheme},F,F^{-1}} = 1) - Pr(A^{\mathcal{E}_{random},F,F^{-1}} = 1)| \\ \leq \;& 2\binom{q_0}{2}\epsilon + 2q_0 q_1 \delta + \frac{q_0(q_0 + 2q_1 - 1)}{2^n}. \end{aligned} \tag{9}$$

(Proof) It is easy to see that we can use A as a distinguisher of Theorem 2.1. Therefore, we have eq.(9) from Theorem 2.1. Q.E.D.

3.4 Enhanced Message Integrity

We say that an adversary A forges if A outputs a valid C' (that is, C' satisfies eq.(7) in the real world, or it satisfies eq.(8) in the random world) and A never queried the corresponding plaintext M' to the encryption oracle. We will show that this probability is negligible.

Lemma 3.1 *In the random world, suppose that an adversary A asks at most α queries to the encryption oracle and asks at most q_1 queries to F and F^{-1}. Then*

$$\Pr(A \textit{ forges in the random world}) \leq \frac{1}{2^n - 1}.$$

(Proof) Suppose that A queried $M^i = M_1^i || \cdots || M_L^i$ and received $C^i = C_0^i || C_1^i || \cdots || C_{L^i}^i || C_{L^i+1}^i$ from the encryption oracle $\mathcal{E}_{random}$ for $1 \leq i \leq q_0$, where $C_0^i = IV_i$.

Let U be the set of all random permutations invoked by $\mathcal{E}_{random}$ in this process.

Next suppose that A output $C' = C_0' || C_1' || \cdots || C_{L'}' || C_{L'+1}'$ finally, where $C_0' = IV'$. Then A succeeds in forging iff

$$C_{L'+1}' = R_{(L',IV')}(\sum_j M_j'), \tag{10}$$

where $M_j' = Q_{(j,IV')}^{-1}(C_j')$ for $1 \leq j \leq L'$.

(Case 1) Suppose that $IV' \notin \{IV_1, \ldots, IV_m\}$. Then $R_{(L',IV')}$ of eq.(10) is a random permutation chosen independently of U and $Q_{(1,IV')}, \ldots, Q_{(L',IV')}$. Therefore,

$$\Pr[\text{eq.(10) holds}] = 1/2^n.$$

(Case 2) Suppose that $IV' = IV_i$ for some $i \in \{1, \ldots, q_0\}$,

(Case 2-a) If $L' \neq L^i$, then $R_{(L',IV')}$ of eq.(10) is a random permutation chosen independently of U and $Q_{(1,IV')}, \ldots, Q_{(L',IV')}$. (Especially, it is independent of $R_{(L^i,IV_i)}$.) Therefore,

$$\Pr[\text{eq.(10) holds}] = 1/2^n.$$

(Case 2-b) If $L' = L^i$, then it must be that $(C_0', C_1', \ldots, C_{L'}', C_{L'+1}') \neq (C_0^i, C_1^i, \ldots, C_{L'}^i, C_{L'+1}^i)$. Let j_0 be the smallest j such that $C_j' \neq C_j^i$.

If $j_0 = L' + 1$, then $(C_0', C_1', \ldots, C_{L'}') = (C_0^i, C_1^i, \ldots, C_{L'}^i)$ and $C_{L'+1}' \neq C_{L'+1}^i$. In this case, $\sum_j M_j' = \sum_j M_j^i$ and

$$C_{L'+1}^i = R_{(L',IV')}(\sum_j M_j').$$

Therefore, eq. (10) does not hold clearly.

Suppose that $1 \leq j_0 \leq L'$. Fix

$$Q_{(1,IV')}, \cdots, \overset{j_0}{\vee}, \cdots, Q_{(L',IV')}, R_{(L',IV')}$$

arbitrarily. Then $Q_{(j_0,IV')}$ is chosen independently of them under the condition such that

$$Q^{-1}_{(j_0,IV')}(C^i_{j_0}) = M^i_{j_0}.$$

Therefore, $M'_{j_0} = Q^{-1}_{(j_0,IV')}(C'_{j_0})$ is uniformly distributed over $\{0,1\}^n \setminus \{M^i_{j_0}\}$ because $C'_{j_0} \neq C^i_{j_0}$. Then $\sum_j M'_j$ in eq.(10) can take $2^n - 1$ possible values. Hence

$$\Pr[\text{eq.(10) holds}] = 1/(2^n - 1).$$

Q.E.D.

Theorem 3.2 *In our scheme of Sec.3.1, suppose that an adversary A asks at most α queries to the encryption oracle, totaling at most μ blocks, and asks at most q_1 queries to F and F^{-1}. Let $q_0 = \alpha + \mu$. Then*

$$\Pr(A \textit{ forges}) \leq \frac{1}{2^n - 1} + 2\binom{q_0}{2}\epsilon + 2q_0q_1\delta + \frac{q_0(q_0 + 2q_1 - 1)}{2^n}.$$

(Proof) We can construct a distinguisher D for Theorem 2.1 from the adversary A as follows. Note that D can simulate $\mathcal{E}_{scheme}/\mathcal{E}_{random}$ and verify eq.(7)/eq.(8) if it is a distinguisher of Theorem 2.1. Then D outputs 1 if A succeeds in forging and 0 otherwise.

Therefore, it holds that

$$\begin{aligned} & |\Pr(A \text{ forges in the real world}) - \Pr(A \text{ forges in the random world})| \\ \leq \; & 2\binom{q_0}{2}\epsilon + 2q_0q_1\delta + \frac{q_0(q_0 + 2q_1 - 1)}{2^n} \end{aligned}$$

from Theorem 2.1. Then we obtain Theorem 3.2 from lemma 3.1.

Q.E.D.

4 Extension to OCB mode

OCB mode was proposed by Rogaway et al. [9]. It is a refinement of IAPM such that it works for messages of any bit length and therefore returns a ciphertext of minimal length.

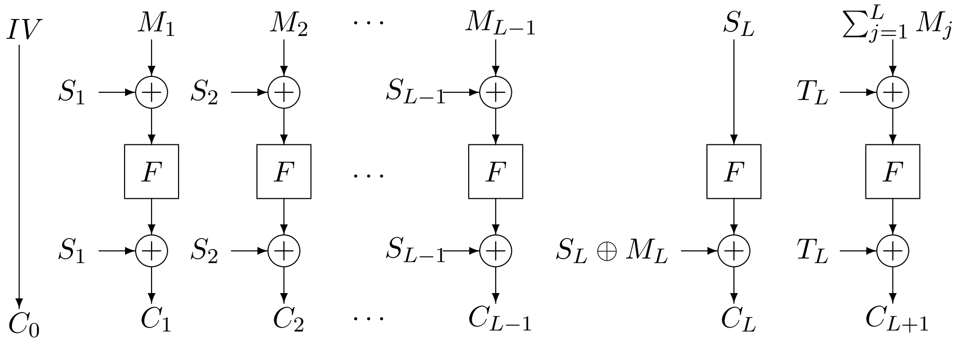

Figure 3: Modified OCB

In this subsection, we present a slight modification of OCB mode and prove its enhanced security.

Let H be an (ϵ, δ)-AXU hash function family from $\{0,1\}^{3n} \setminus \{0^{3n}\}$ to $\{0,1\}^n$. An encryptor and a decryptor share $h \in H$ secretly.

To encrypt an L-block plaintext $M = M_1||M_2||\cdots||M_L$ (with $M_j \in \{0,1\}^n$), the encryptor first picks a new nonce IV. Wlog, we assume that this nonce was never used before. The encryptor then generates $L+1$ masks $S_1, \cdots, S_L$ and T_L as follows.

$$\begin{aligned} S_i &= h(IV, 2i-1, n) \text{ for } 1 \leq i \leq L-1, \\ S_L &= h(IV, 2i-1, |M_L|), \\ T_L &= h(IV, 2L, n), \end{aligned}$$

where $|M_L|$ denotes the bit length of M_L. The ciphertext $C = C_0||C_1||\cdots||C_{L+1}$ is computed by setting $C_0 = IV,\ C_j = S_j \oplus F(S_j \oplus M_j)$ for $1 \leq j \leq L-1$, and

$$\begin{aligned} C_L &= \text{the first } |M_L| \text{ bits of } S_L \oplus F(S_L) \oplus M_L \\ C_{L+1} &= T_L \oplus F(T_L \oplus \sum_{j=1}^{L} M_j). \end{aligned} \tag{11}$$

To decrypt a ciphertext of $L+2$ blocks, $C = C_0||C_1||\cdots||C_{L+1}$, the decryptor first computes the masks $S_1, \ldots, S_L$ and T_L. He then recovers

$M_j = S_j \oplus F^{-1}(S_j \oplus C_j)$ for $1 \le j \le L-1$ and

$$M_L = C_L \oplus (\text{the first } |C_L| \text{ bits of } S_L \oplus F(S_L)).$$

He next check if eq.(11) holds. If the check passes, the plaintext is $M_1||M_2||\cdots||M_L$. Otherwise, the ciphertext is deemed invalid.

(Remark) In the original OCB mode,

$$\begin{aligned} C_L &= \text{the first } |M_L| \text{ bits of } F(T_L) \oplus M_L, \\ C_{L+1} &= F(S_L \oplus \sum_{j=1}^{L} M_j), \end{aligned}$$

$S_1, \ldots, S_L$ and T_L are generated by using a block cipher.

We can define a random world similarly to Sec.3.2. Then we can prove the following enhanced security. Suppose that an adversary A asks at most α queries to the encryption oracle, totaling at most μ blocks, and asks at most q_1 queries to F and F^{-1}. Let $q_0 = \alpha + \mu$. Then

Theorem 4.1 *If A works as a distinguisher, then*

$$\begin{aligned} & |\Pr(A^{\mathcal{E}_{scheme}, F, F^{-1}} = 1) - Pr(A^{\mathcal{E}_{random}, F, F^{-1}} = 1)| \\ \le\ & 2\binom{q_0}{2}\epsilon + 2q_0 q_1 \delta + \frac{q_0(q_0 + 2q_1 - 1)}{2^n}. \end{aligned} \tag{12}$$

Theorem 4.2 *If A tries to make a forgery, then*

$$\Pr(A \textit{ forges}) \le \frac{1}{2^n - 1} + 2\binom{q_0}{2}\epsilon + 2q_0 q_1 \delta + \frac{q_0(q_0 + 2q_1 - 1)}{2^n}.$$

The proofs will be given in the final paper.

5 Lower Bound

In this section, we prove that Theorem 2.1 is tight within a constant factor if $q_1 = 0$ and H satisfies some property. This means that Theorem 3.1 and Theorem 4.1 are tight within a constant factor under the same condition.

Definition 5.1 *Let H be a set of hash functions $h : X \to \{0,1\}^n$. We say that H is an XOR universal hash function family if for any two distinct elements $x, x' \in X$ and any element $y \in \{0,1\}^n$,*

$$\Pr_h(h(x) \oplus h(x') = y) = 1/2^n.$$

Theorem 5.1 *In the model of Sec.2.1, suppose that H is an XOR universal hash function family. If*

$$\binom{q_0}{2}\frac{1}{2^n} < 0.158,$$

then

$$Adv(q_0, 0) \geq cq_0^2/2^n$$

for some constant c.

A proof is given in Appendix A. Then we obtain the following corollary.

Corollary 5.1 *In each of IAPM, the modified IAPM, OCB mode and the modified OCB mode, suppose that an XOR universal hash function family is used. If an adversary A asks at most μ blocks to the encryption oracle, where*

$$\binom{\mu}{2}\frac{1}{2^n} < 0.158,$$

then

$$|\Pr(A^{\mathcal{E}_{scheme}} = 1) - Pr(A^{\mathcal{E}_{random}} = 1)| \geq c\mu^2/2^n$$

for some constant c.

Acknowledgement

The author would like to thank Tetsu Iwata of Ibaraki University and, Wakaha Ogata and Toshihiko Matsuo of Tokyo Insitute of Tecnhology for useful discussion.

References

[1] M.Bellare and C.Namprempre. "Relations among notions and analysis of the generic composition paradigm", Asiacrypt'00, LNCS 1976, pp.531–545 (2000)

[2] S. Even and Y. Mansour. "A Construction of a Cipher from a Single Pseudorandom Permutation " *Journal of CRYPTOLOGY vol.10 no.3,* pp. 151-161, Springer-Verlag, 1997.

[3] V. Gligor, and P. Donescu. Fast encryption and authentication: XCBC encryption and XECB authentication modes. Preproceedings of *Fast Software Encryption, FSE 2001, to appear in LNCS,* pp. 97–111, Springer-Verlag.

[4] Shai Halevi, "An observation regarding Jutla's modes of operation ", IACR e-prit archive.

[5] Charanjit S. Jutla, "Encryption Modes with Almost Free Message Integrity ", B.Pfitzmann (Ed.): EUROCRYPT 2001, LNCS 2045, pp. 529-544, 2001.

[6] J.Katz and M.Yung. "Unforgeable encryption and adaptively secure modes of operation", FSE'00, pp.284–299 (2000)

[7] J. Kilian and P. Rogaway. "How to Protect DES Against Exhaustive Key Search (An Analysis of DESX) " *Journal of CRYPTOLOGY vol.14 no.1,* pp. 17-35, Springer-Verlag, 2001.

[8] M.Liskov, R.Rivest and D.Wagner, Tweakable Block Ciphers. *Crypto'2002*

[9] P. Rogaway, M. Bellare, J. Black, and T. Krovetz. OCB: a block-cipher mode of operation for efficient authenticated encryption. *Proceedings of ACM Conference on Computer and Communications Security, ACM CCS 2001,* pp. 196-205, ACM press, 2001.

A Proof of Theorem 5.1

We consider a distinguisher D who asks the ith query x_i to $P_{i'}$-oracle/$Q_{i'}$-oracle such that $i' = i \bmod m$ for $1 \le i \le q_0$, where x_i is randomly chosen. Let y_i denote the answer from the oracle. For simplicity, we show a proof for $q_0 \le m$. The proof for $q_0 > m$ is similar.

In *Game*1, let a_i denote the input to F in the ith query. Then

$$\begin{aligned} a_i &= x_i \oplus S_i \\ F(a_i) &= y_i \oplus S_i. \end{aligned}$$

If $a_i = a_j$, then $F(a_i) = F(a_j)$. In this case,

$$\begin{aligned} x_i \oplus S_i &= x_j \oplus S_j, \\ y_i \oplus S_i &= y_j \oplus S_j. \end{aligned}$$

Hence

$$x_i \oplus y_i = x_j \oplus y_j. \tag{13}$$

Equivalently,

$$F(a_i) \oplus F(a_j) = a_i \oplus a_j.$$

Now our distinguisher D outputs 1 if and only if eq.(13) holds.

First in *Game*0, it is easy to see that

$$\Pr(D = 1 \text{ in } Game0) \leq \binom{q_0}{2} \frac{1}{2^n}.$$

Next in *Game*1, let E_0 denote the event that $a_i = a_j$ for some $i \neq j$. Then $\Pr(D = 1 \mid E_0) = 1$. Therefore,

$$\begin{aligned} \Pr(D = 1 \text{ in } Game1) &= \Pr(D = 1 \mid E_0) \Pr(E_0) + \Pr(D = 1 \mid \neg E_0) \Pr(\neg E_0), \\ &= \Pr(E_0) + (1 - \Pr(E_0)) \Pr(D = 1 \mid \neg E_0). \end{aligned}$$

Proppposition A.1 *If $xy \geq 0$, then*

$$(1 - x)(1 - y) \geq 1 - x - y.$$

Proppposition A.2 *If $0 \leq x \leq 1$, then*

$$1 - x \leq e^{-x} \leq 1 - (1 - 1/e)x.$$

Theorem A.1 *Let $E_1, \cdots, E_k$ be any events. Define*

$$p_i \stackrel{\triangle}{=} \Pr(\neg E_i \mid E_1, \cdots, E_{i-1}).$$

If $p_1 + p_2 + \cdots + p_k \leq 1$, then

$$0.632(p_1 + \cdots + p_k) \leq \Pr(\neg E_1 \vee \cdots \vee \neg E_k) \leq p_1 + \cdots + p_k.$$

(Proof) It is clear that

$$\begin{aligned} \Pr(E_1 \wedge \cdots \wedge E_k) &= \Pr(E_1) \Pr(E_2 \mid E_1) \cdots \Pr(E_k \mid E_1, \cdots, E_{k-1}) \\ &= (1 - p_1)(1 - p_2) \cdots (1 - p_k) \end{aligned}$$

First from Proposition A.1, we have that

$$(1-p_1)(1-p_2)\cdots(1-p_k) \geq 1-(p_1+\cdots+p_k).$$

Next from Proposition A.2, we have that

$$\begin{aligned}(1-p_1)(1-p_2)\cdots(1-p_k) &\leq e^{-p_1}e^{-p_2}\cdots e^{-p_k}\\ &= e^{-(p_1+p_2+\cdots+p_k)}\\ &\leq 1-(1-1/e)(p_1+\cdots+p_k)\end{aligned}$$

Therefore,

$$0.632(p_1+\cdots+p_k) \leq \Pr(\neg E_1 \vee \cdots \vee \neg E_k) \leq p_1+\cdots+p_k$$

because $\Pr(\neg E_1 \vee \cdots \vee \neg E_k) = 1-\Pr(E_1 \wedge \cdots \wedge E_k)$.

Q.E.D.

We first compute $\Pr(D=1 \mid \neg E_0)$.

Lemma A.1

$$\Pr(D=1 \mid \neg E_0) \geq 0.632\binom{q_0}{2}\frac{1}{2^n}.$$

(Proof) Suppose that $\neg E_0$ occurs. That is, $a_i \neq a_j$ for any $i \neq j$. Let E_{ij} be the event that

$$F(a_i) \oplus F(a_j) \neq a_i \oplus a_j.$$

Let

$$p_{ij} = \Pr(\neg E_{ij} \mid E_{12}, \cdots, E_{i,j-1}).$$

Then it is easy to see that

$$\begin{aligned}p_{ij} &= \Pr(F(a_i) \oplus F(a_j) = a_i \oplus a_j \mid E_{12}, \cdots, E_{i,j-1})\\ &\geq 1/2^n.\end{aligned}$$

Therefore, from Theorem A.1,

$$\Pr(\neg E_{12} \vee \cdots \vee \neg E_{q_0,q_0-1}) \geq 0.632\binom{q_0}{2}\frac{1}{2^n}.$$

Hence

$$\Pr(D=1 \mid \neg E_0) \geq 0.632\binom{q_0}{2}\frac{1}{2^n}.$$

Q.E.D.

We next compute $\Pr(E_0)$.

Lemma A.2 *If $\epsilon = 1/2^n$ and*

$$\binom{q_0}{2}\frac{1}{2^n} < 0.136,$$

then

$$0.632\binom{q_0}{2}\frac{1}{2^n} \le \Pr(E_0) \le \binom{q_0}{2}\frac{1}{2^n}.$$

(Proof) Let E_{ij} be the event that $a_i \ne a_j$ for $i \ne j$. Note that $a_i = a_j$ if and only if

$$x_i \oplus S_i = x_j \oplus S_j.$$

Therefore, E_{ij} is the event that

$$S_i \oplus S_j \ne x_i \oplus x_j.$$

Let

$$p_{ij} = \Pr(\neg E_{ij} \mid E_{12}, \cdots, E_{i,j-1}).$$

Then

$$\begin{aligned} p_{ij} &= \Pr(S_i \oplus S_j = x_i \oplus x_j \mid S_1 \oplus S_2 \ne x_1 \oplus x_2, \cdots, S_i \oplus S_{j-1} \ne x_i \oplus x_{j-1}) \\ &\ge \Pr(S_i \oplus S_j = x_i \oplus x_j) \\ &= 1/2^n. \end{aligned}$$

On the other hand,

$$p_{ij} \le \frac{\Pr(\neg E_{ij})}{\Pr(E_{12}, \cdots, E_{i,j-1})}.$$

$$\Pr(\neg E_{12} \vee \cdots \vee \neg E_{i,j-1}) \le \binom{q_0}{2}\frac{1}{2^n}.$$

Hence

$$\Pr(E_{12}, \cdots, E_{i,j-1}) \ge 1 - \binom{q_0}{2}\frac{1}{2^n} \ge 0.864.$$

Therefore,

$$p_{ij} \le \frac{1}{1-0.864}\frac{1}{2^n} \le 1.16\frac{1}{2^n}.$$

Finally from Theorem A.1,

$$0.632\binom{q_0}{2}\frac{1}{2^n} \le \Pr(E_0) \le 1.16\binom{q_0}{2}\frac{1}{2^n}.$$

Q.E.D.

Consequently, in Game1,

$$\begin{aligned}\Pr(D=1) &\geq 0.632\binom{q_0}{2}\frac{1}{2^n}+(1-1.16\binom{q_0}{2}\frac{1}{2^n})0.632\binom{q_0}{2}\frac{1}{2^n}\\ &= 1.264\binom{q_0}{2}\frac{1}{2^n}-0.733(\binom{q_0}{2}\frac{1}{2^n})^2.\end{aligned}$$

Therefore,

$$\begin{aligned}Adv(q_0,0) &= |\Pr(D=1 \text{ in } Game1)-\Pr(D=1 \text{ in } Game0)|\\ &\geq 0.264\binom{q_0}{2}\frac{1}{2^n}-0.733(\binom{q_0}{2}\frac{1}{2^n})^2\\ &= \binom{q_0}{2}\frac{1}{2^n}(0.264-0.733\binom{q_0}{2}\frac{1}{2^n}).\end{aligned}$$

If

$$\binom{q_0}{2}\frac{1}{2^n}<0.136,$$

then

$$Adv(m,0)\geq 0.164\binom{q_0}{2}\frac{1}{2^n}.$$