Birthday Attack on Dual EWCDM

Mridul Nandi

Indian Statistical Institute

Abstract. In CRYPTO 2017, Mennink and Neves showed almost n-bit security for a dual version of EWCDM. In this paper we describe a birthday attack on this construction which violates their claim.

1 Introduction

We briefly recall the construction EWCDM [CS16] and its dual version EWCDMD [MN17a,MN17b]. Let π_1 and π_2 be two independent random permutations over $\{0,1\}^n$. Let $\mathscr{H}$ be an ϵ-AXU over a message space $\mathscr{M}$. For a permutation π, we denote $\pi(x) \oplus x$ as $\pi^{\oplus}(x)$. For a nonce $\nu \in \{0,1\}^n$ and a message $m \in \mathscr{M}$, we define

$$\mathrm{EWCDM}(\nu, m) = \pi_2(\pi_1^{\oplus}(\nu) \oplus \mathscr{H}(m)) \tag{1}$$

$$\mathrm{EWCDMD}(\nu, m) = \pi_2^{\oplus}(\pi_1(\nu) \oplus \mathscr{H}(m)) \tag{2}$$

If there is no message we define them as

$$\mathrm{EDM}(\nu) = \pi_2(\pi_1^{\oplus}(\nu)) \tag{3}$$

$$\mathrm{EDMD}(\nu) = \pi_2^{\oplus}(\pi_1(\nu)) \tag{4}$$

These are called EDM and EDMD respectively. In [CS16], author proved PRF (pseudorandom function) and MAC (message authentication security) for EWCDM in a nonce respecting model. The original security is proved to be at least $2n/3$-bit. In CRYPTO 2017, Mennink and Neves showed almost n-bit PRF security for EWCDMD, the dual version of EWCDM.

Our Observation. In this paper we describe a PRF attack against EWCDMD in query complexity $2^{n/2}$. Thus, it violates the claim. The main idea of the attack is simple. Note that the EWCDMD can be viewed as a composition of two keyed *non-injective functions* (and so it follows birthday paradox), namely $\pi_2^{\oplus}$ and a function f mapping (ν, m) to $\pi_1(\nu) \oplus \mathscr{H}(m)$. Thus we expect that the collision probability of the composition $\pi_2^{\oplus} \circ f$ is almost double of the collision probability for the random function. Thus, by observing a collision we can distinguish EWCDMD from a random function. Note that EWCDM is a composition of a permutation and a non-injective keyed function. Hence our observation is not applicable to it. The same argument applies for EDM and EDMD.

2 Distinguishing Attack

In this section we provide details of a nonce respecting distinguishing attack on EWCDMD. For better understanding we consider a specific hash function $\mathscr{H}(m) = K \cdot m$ where K is a nonzero random key chosen uniformly from $\{0,1\}^n \setminus \{0\}$ and $m \in \mathscr{M} := \{0,1\}^n$. Here $K \cdot m$ means the field multiplication with respect to a fixed primitive polynomial. Clearly, $\mathscr{H}$ is $\frac{1}{2^n-1}$ AXU hash. Moreover it is injective hash. In other words, for distinct messages $m_1, \ldots, m_q$, $\mathscr{H}(m_1), \ldots, \mathscr{H}(m_q)$ are distinct.

Distinguishing Attack. $\mathscr{A}$ choses $(\nu_1, m_1), \ldots, (\nu_q, m_q) \in \{0,1\}^n \times \mathscr{M}$ where all ν_i's are distinct and all m_i's are distinct. Suppose $T_1, \ldots, T_q$ are all responses. $\mathscr{A}$ returns 1 if there is a collision among T_i values, otherwise returns zero.

When $\mathscr{A}$ is interacting with a random function, $\Pr[\mathscr{A} \to 1] \leq q(q-1)/2^{n+1}$ (by using the union bound). Now we provide lower bound of $\Pr[\mathscr{A} \to 1]$ while $\mathscr{A}$ is interacting with EWCDMD in which π_1, π_2 are two independent random permutations and $\mathscr{H}$ is the above hash function whose key is chosen independently. To obtain a lower bound we first prove the following lemma. Let $N = 2^n$.

Lemma 1. *Let $x_1, \ldots, x_q \in \{0,1\}^n$ be q distinct values. Let π be a random permutation. Then, for all distinct $\nu_1, \ldots, \nu_q$, let C denote the event that there is a collision among values of $\pi(\nu_i) \oplus x_i$, $1 \leq i \leq q$. Then,*

$$\alpha(1-\beta) \leq \Pr[C] \leq \alpha$$

where $\alpha = \frac{q(q-1)}{2(N-1)}$ and $\beta = \frac{(q-2)(q+1)}{4(N-3)}$.

Proof.Let $E_{i,j}$ denote the event that $\pi(\nu_i) \oplus \pi(\nu_j) = x_i \oplus x_j$. So for all $i \neq j$, $\Pr[E_{i,j}] = 1/(N-1)$. Let $C = \cup_{i \neq j} E_{i,j}$ denote the collision event. By using union bound we can easily upper bound

$$\Pr[C] \leq \alpha := \frac{q(q-1)}{2(N-1)}.$$

Now, we show the lower bound. For this, we apply Boole's inequality and we obtain lower bound of collision probability as

$$\Pr[C] \geq \alpha - \sum \Pr[E_{i,j} \cap E_{k,l}]$$

here the sum is taken over all possible choices of $\{\{i,j\},\{k,l\}\}$. Hence there are $q(q-1)(q+1)(q-2)/8 = \binom{q(q-1)/2}{2}$ choices. Note that for each such choice i, j, k, l,

$$\Pr[E_{i,j} \cap E_{k,l}] \leq \frac{1}{(N-1)(N-3)}.$$

Hence,

$$\Pr[C] \geq \alpha - \frac{q(q-1)(q+1)(q-2)}{8(N-1)(N-3)} \tag{5}$$

$$= \alpha\left(1 - \frac{(q-2)(q+1)}{4(N-3)}\right) = \alpha(1-\beta). \tag{6}$$

This completes the proof. □

Advantage Computation. Using the above Lemma we now show that the probability that $\mathscr{A}$ returns 1 while interacting EWCDMD is significant when $q = O(2^{n/2})$.

Let C_1 denote the event that there is a collision among the values $z_i := \pi_1(\nu_i) \oplus \mathscr{H}(m_i)$. We can apply our lemma as $\mathscr{H}(m_i)$'s are distinct due to our choice of the hash function. Thus, $\Pr[C_1] \geq \alpha(1-\beta)$. Moreover, $\Pr[\neg C_1] \geq (1-\alpha)$. Hence,

$$\Pr[\mathscr{A} \to 1] \geq \Pr[C_1] + \Pr[\text{ collision in } T \text{ values } \mid \neg C_1] \times \Pr[\neg C_1].$$

By simple algebra, one can obtain that $\Pr[\mathscr{A} \to 1] \geq 2\alpha - 2\alpha\beta - \alpha^2$. Thus, the advantage of the adversary is at least $\alpha - 2\alpha\beta - \alpha^2$. Now when $q \leq c2^n$ for some suitable constant c (one can easily find c from the expression) such that $1 - 2\beta - \alpha \leq 1/2$ then the advantage is at least $\alpha/2$, i.e. $q(q-1)/4(N-1)$.

3 Conclusion and Possible Future Research Work

We have demonstrated a distinguishing attack on EWCDMD. We would like to note that this attack does not work for EDM, EWCDM and EDMD as we can not write them as a composition of two non-injective functions.

1. We would like to note that our attack is PRF attack and it is not easy to extend for forging attack in a nonce respecting situation. On the other hand, we usually prove MAC security through the PRF advantage. In [MN17b] authors only proved PRF security for EWCDMD. However, in a nonce respecting model only proving PRF security is not worth as one can easily design PRF as PRF(ν) by completely ignoring the message m.
2. One can consider other dual variants. E.g.,

$$\pi_2(\pi_1(\nu) \oplus \mathscr{H}(m)) \oplus \pi_1(\nu). \tag{7}$$

   This is very close to the sum of permutations. However, the presence of $\mathscr{H}(m)$ makes it very difficult to prove (without using the Patarin's claim or conjecture on the interpolation probability of sum of random permutations [Pat08]). Moreover, it can not be expressed as a composition function with n-bit outputs. Hence it is a potential dual candidate of EWCDM.
3. The other possibility is to use three independent random permutations. As mentioned in [CS16], we can consider

$$\pi_3\big(\pi_1(\nu) \oplus \pi_2(\nu) \oplus \mathscr{H}(m)\big).$$

   This will give 2^n security in nonce respecting model assuming that the sum of permutations would give n-bit PRF security. However, we don't know trade off between the number of allowed repetition of nonce and the security bound.

References

CS16. Benoît Cogliati and Yannick Seurin. EWCDM: an efficient, beyond-birthday secure, nonce-misuse resistant MAC. In *CRYPTO 2016, Proceedings, Part I*, pages 121–149, 2016.

MN17a. Bart Mennink and Samuel Neves. Encrypted davies-meyer and its dual: Towards optimal security using mirror theory. Cryptology ePrint Archive, Report 2017/473, 2017. http://eprint.iacr.org/2017/473.

MN17b. Bart Mennink and Samuel Neves. Encrypted davies-meyer and its dual: Towards optimal security using mirror theory. In *CRYPTO 2017, Proceedings (To appear)*, pages xxx–xxx, 2017.

Pat08. Jacques Patarin. A proof of security in $o(2^n)$ for the xor of two random permutations. In *ICITS 2008*, volume 5155 of *LNCS*, pages 232–248. Springer, 2008.