CENC is Optimally Secure

Tetsu Iwata[1], Bart Mennink[2], and Damian Vizár[3]

[1] Nagoya University, Nagoya, Japan
iwata@cse.nagoya-u.ac.jp
[2] Dept. Electrical Engineering, ESAT/COSIC, KU Leuven, and iMinds, Belgium
bart.mennink@esat.kuleuven.be
[3] EPFL, Lausanne, Switzerland
damian.vizar@epfl.ch

Abstract. At FSE 2006, Iwata introduced the CENC encryption mode and proved its security up to $2^{2n/3}$ plaintext blocks processed in total. He conjectured optimal security up to a constant. In this brief note, we confirm this conjecture. Rather than proving it ourselves, we point out that the conjecture's proof follows as a corollary of Patarin's "Theorem $P_i \oplus P_j$ for any $\xi_{\max}$" from 2005. This connection appears to have remained unnoticed, and the sole purpose of this brief note is to make the connection explicit.

1 Introduction

A blockcipher mode of operation for message encryption (encryption mode for short) is called *beyond birthday-bound* (BBB) secure, if the proven upper bound on the adversarial advantage is meaningful even if the adversary can process more than $2^{n/2}$ blocks of data with the same key (with n being the block size of the blockcipher). In 2006, Iwata proposed a BBB secure encryption mode CENC [3]. CENC is a nonce-based encryption mode which can be seen as a generalization of counter mode. Given a parameter w, CENC makes $w+1$ blockcipher calls to encrypt w plaintext blocks, achieving a rate $1+\frac{1}{w}$. Iwata proved CENC secure up to $2^{\frac{2n}{3}}/w$ processed blocks but conjectured that it is in fact optimally secure (i.e., secure up to $2^n/w$ processed blocks). In the same paper, Iwata also proposed CHM, a mode of operation for authenticated encryption obtained by extending CENC ciphertexts by and encrypted AXU hash.

Independently, Patarin [8] studied the PRF security of the permutation-sum construction, and proved that a single-permutation variant of this construction is indistinguishable from a random function up to $\approx 2^n$ processed blocks.[4] The core idea of his proof was to represent the transcript of adversarial queries and the oracle replies as a system of linear equalities with specific properties. Patarin also considered a generalization of his techniques to a larger class of systems of equalities: "Theorem $P_i \oplus P_j$ for any $\xi_{\max}$." The first appearance of this result was in 2003 with sub-optimal $2^{2n/3}$ security [6], optimal 2^n security was derived in 2005 [7], with a concrete bound given in 2010 [9].

In this note, we point out that the proof of Iwata's conjecture about CENC's optimal security is in fact a corollary of Patarin's generalized theorem. We do not claim any novelty of this work. Its purpose is merely to make the immediate, but not apparent, connection explicit. Pointing out the optimal security of CENC is of theoretical, but also of practical interest, as this will allow for larger data volumes to be processed with lightweight (e.g. 64-bit) blockciphers. We note that the security bound of CENC is now better than that of the scheme in [4]. The analysis of CHM is beyond the scope of this brief note, but it is conceivable that a better security bound can be obtained analogously.

2 Preliminaries

For $m, n \in \mathbb{N}$, $\{0,1\}^n$ denotes the set of all n-bit strings, $\mathsf{P}(n)$ the set of all permutations on $\{0,1\}^n$, $\mathsf{F}(m,n)$ the set of all functions from $\{0,1\}^m$ to $\{0,1\}^n$, $\langle m \rangle_n$ the encoding of m as an n-bit string, and $(m)_n$ the falling factorial. For a set $\mathcal{X}$, $x \xleftarrow{\$} \mathcal{X}$ denotes uniformly random sampling of x from $\mathcal{X}$.

[4] This problem was previously addressed also by Bellare and Impagliazzo [1] and Lucks [5].

2.1 Blockcipher

A blockcipher $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ is a function that is a permutation for every $K \in \{0,1\}^k$. We denote by $\mathsf{B}(k,n)$ the set of all blockciphers $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$. We denote by $\mathbf{Adv}^{\mathrm{prp}}_E(\mathcal{D})$ the advantage of a distinguisher $\mathcal{D}$ in distinguishing E from an ideal permutation $\pi \xleftarrow{\$} \mathsf{P}(n)$:

$$\mathbf{Adv}^{\mathrm{prp}}_E(\mathcal{D}) = \mathbf{Pr}\left[K \xleftarrow{\$} \{0,1\}^k \ : \ \mathcal{D}^{E_K} = 1\right] - \mathbf{Pr}\left[\pi \xleftarrow{\$} \mathsf{P}(n) \ : \ \mathcal{D}^{\pi} = 1\right].$$

Note that $\mathcal{D}$ only gets forward access to E. By $\mathbf{Adv}^{\mathrm{prp}}_E(q,t)$ we denote the supremum of $\mathbf{Adv}^{\mathrm{prp}}_E(\mathcal{D})$ taken over all distinguishers that can make q queries and operate in t time.

2.2 Pseudorandom Function

A pseudorandom function $F : \{0,1\}^k \times \{0,1\}^m \to \{0,1\}^n$ gets as input a key K and transforms a message X to a value Z. We denote by $\mathbf{Adv}^{\mathrm{prf}}_F(\mathcal{D})$ the advantage of a distinguisher $\mathcal{D}$ in distinguishing F from an ideal function $\rho \xleftarrow{\$} \mathsf{F}(m,n)$:

$$\mathbf{Adv}^{\mathrm{prf}}_F(\mathcal{D}) = \mathbf{Pr}\left[K \xleftarrow{\$} \{0,1\}^k \ : \ \mathcal{D}^{F_K} = 1\right] - \mathbf{Pr}\left[\rho \xleftarrow{\$} \mathsf{F}(m,n) \ : \ \mathcal{D}^{\rho} = 1\right].$$

By $\mathbf{Adv}^{\mathrm{prf}}_F(q,t)$ we denote the supremum of $\mathbf{Adv}^{\mathrm{prf}}_F(\mathcal{D})$ taken over all distinguishers that can make q queries and operate in t time.

2.3 Encryption

A nonce based encryption scheme $\mathcal{E} : \{0,1\}^k \times \{0,1\}^m \times \{0,1\}^* \to \{0,1\}^*$ gets as input a key K, a nonce N, and an arbitrarily length message M, and returns a ciphertext C of length $|M|$. We denote by $\mathbf{Adv}^{\mathrm{cpa}}_{\mathcal{E}}(\mathcal{D})$ the advantage of a distinguisher $\mathcal{D}$ in distinguishing $\mathcal{E}$ from an ideal enciphering scheme \$:

$$\mathbf{Adv}^{\mathrm{cpa}}_{\mathcal{E}}(\mathcal{D}) = \mathbf{Pr}\left[K \xleftarrow{\$} \{0,1\}^k \ : \ \mathcal{D}^{\mathcal{E}_K} = 1\right] - \mathbf{Pr}\left[\$ \xleftarrow{\$} \mathsf{F}(n+*,*) \ : \ \mathcal{D}^{\$} = 1\right].$$

Note that we are abusing notation in the drawing of \$: \$ is a function that returns a random ciphertext C of length $|M|$ for every new query (N,M). Distinguisher $\mathcal{D}$ is required to be nonce-respecting, i.e., it should not repeat nonces. By $\mathbf{Adv}^{\mathrm{cpa}}_{\mathcal{E}}(q,\ell,t)$ we denote the supremum of $\mathbf{Adv}^{\mathrm{cpa}}_{\mathcal{E}}(\mathcal{D})$ taken over all distinguishers that can make q queries of length ℓ blocks and operate in t time.

3 Pseudorandom Function

Let $k,m,n,w \in \mathbb{N}$ such that $m+s = n$ for $s = \lceil \log_2(w+1) \rceil$. Let $E \in \mathsf{B}(k,n)$. We define pseudorandom function $\mathsf{XORP}[w] : \{0,1\}^k \times \{0,1\}^m \to \{0,1\}^{wn}$ with load w as follows:

$$\mathsf{XORP}[w](K,X) = \Big|\Big|_{j=1}^{w} E_K(X \| \langle 0 \rangle_s) \oplus E_K(X \| \langle j \rangle_s). \tag{1}$$

Note that $\mathsf{XORP}[w]$ makes $w+1$ distinct blockcipher calls (the $E_K(X\|\langle 0\rangle_s)$ repeats). See Figure 1 for $\mathsf{XORP}[w]$ with $w = 1$ and $w = 3$.

For $\mathsf{XORP}[w]$, Iwata proved approximately $2^{2n/3}$ security, and as becomes clear in Section 4, this bound capped the security of CENC.

Theorem 1 (Iwata (2006) [3]). *We have*

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{XORP}[w]}(q,t) \le \frac{(w+1)^4 q^3}{2^{2n+1}} + \frac{w(w+1)q}{2^{n+1}} + \mathbf{Adv}^{\mathrm{prp}}_E((w+1)q,t). \tag{2}$$

Independently, Patarin proved approximately optimal security in [7, 9]. We follow [9] as this one includes a concrete bound. As becomes clear in Section 4, this bound implies optimal security of CENC.

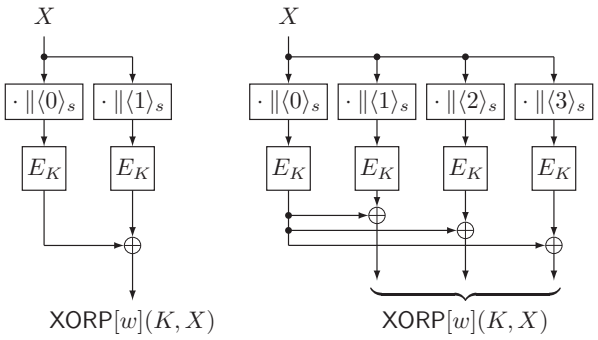

Fig. 1: $\mathsf{XORP}[w]$ for $w = 1$ (left) and $w = 3$ (right)

Theorem 2 (Patarin (2010) [9, Theorem 6]). *We have, provided* $wq \leq 2^n/67$,

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{XORP}[w]}(q,t) \leq \frac{w^2 q}{2^n} + \mathbf{Adv}^{\mathrm{prp}}_{E}((w+1)q, t)\,. \tag{3}$$

[9, Theorem 6] is in fact more general and its application to $\mathsf{XORP}[w]$ is not entirely straightforward. Therefore, we briefly discuss how to interpret $\mathsf{XORP}[w]$ in terms of [9, Theorem 6].

Proof. We will consider $\mathsf{XORP}[w]$ based on an ideal permutation $\pi \xleftarrow{\$} \mathsf{P}(n)$, and consider deterministic information-theoretic distinguishers solely measured in query complexity. The step to the standard model is straightforwardly made at the expense of $\mathbf{Adv}^{\mathrm{prp}}_{E}((w+1)q, t)$. For any X and any $j \in \{0, \ldots, w\}$, denote the variable corresponding to the evaluation $\pi(X \| \langle j \rangle_s)$ by $P_{X,j}$.

Now, consider a given transcript of q distinct evaluations $(X_1, Z_1), \ldots, (X_q, Z_q)$, where the Z_i's can be parsed into w n-bit blocks as $Z_i = Y_{i,1} \| \cdots \| Y_{i,w}$. This transcript defines equations

$$\begin{aligned} P_{X_i,0} \oplus P_{X_i,1} &= Y_{i,1}\,, \\ P_{X_i,0} \oplus P_{X_i,2} &= Y_{i,2}\,, \\ &\vdots \\ P_{X_i,0} \oplus P_{X_i,w} &= Y_{i,w}\,, \end{aligned} \tag{4}$$

for $i = 1, \ldots, q$. In other words, every of the q queries gives w equations $\mathcal{E}_i$ with $w+1$ variables $\mathcal{S}_i := \{P_{X_i,0}, P_{X_i,1}, \ldots, P_{X_i,w}\}$.

We say that the transcript is "good" if $Y_{i,j} \neq 0$ for all (i,j) and $Y_{i,j} \neq Y_{i,j'}$ for all $(i,j) \neq (i,j')$. The following observations are easily made:

(i) There is no variable $P_{X_i,j}$ occurring in two different sets. This is because all queries, and thus all values X_i, are different;
(ii) The set of equations $\mathcal{E}_1 \cup \mathcal{E}_2 \cup \cdots \cup \mathcal{E}_q$ does not generate an equation independent of any variable $P_{X_i,j}$. In the terminology of [9], this means that the set of equations does not contain a "circle." This observation follows by close inspection of (4);
(iii) The set of equations $\mathcal{E}_1 \cup \mathcal{E}_2 \cup \cdots \cup \mathcal{E}_q$ does not generate an equation $P_{X_i,j} = P_{X_{i'},j'}$ with $(i,j) \neq (i',j')$. For $i \neq i'$ this is apparent as $X_i \neq X_{i'}$. For $i = i'$, this follows by our definition of good transcripts.

Central to [9, Theorem 6] is $\xi_{\max}$, defined as the maximum number of indices that are in the same "block," i.e., the maximum number of variables that are related to each other through the set of equations. Observation (i) above shows that no variable $P_{X_i,j}$ occurs in two different sets, while on the other hand, every set contains $w+1$ variables. Thus, the set of equations defines q blocks of $w+1$ indices. We henceforth have $\xi_{\max} = w+1$.

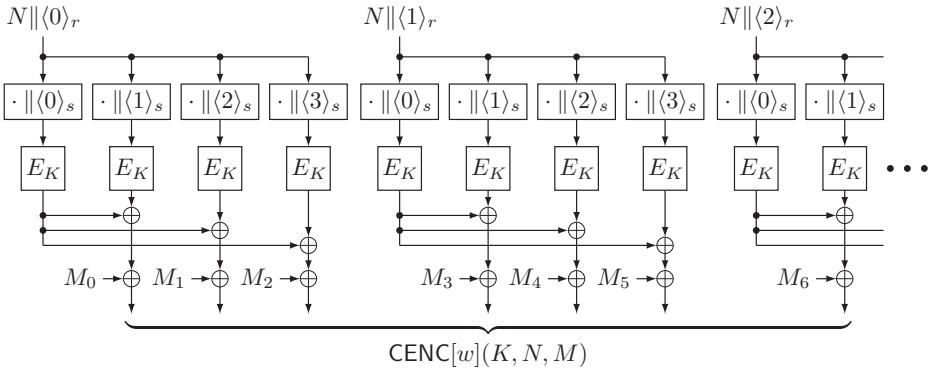

Fig. 2: $\mathsf{CENC}[w]$ for $w = 3$

[9, Theorem 6] now states that if $(\xi_{\max} - 1)q \leq 2^n/67$, then $\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{XORP}[w]}(q, \infty) \leq \beta$, where β is minimal such that[5]

$$\frac{|\text{good transcripts}|}{|\text{all transcripts}|} \geq 1 - \beta\,. \tag{5}$$

Clearly, the number of transcripts is $|\text{all transcripts}| = 2^{wnq}$ (we consider the values X_i given and count the number of possible Z_i's). The number of good transcripts is $|\text{good transcripts}| = ((2^n - 1)_w)^q$, as for every value Z_i we have $(2^n - 1)_w$ possible values. We obtain for (5):

$$\frac{|\text{good transcripts}|}{|\text{all transcripts}|} = \frac{((2^n - 1)_w)^q}{2^{wnq}} = \prod_{i=1}^{q}\prod_{j=1}^{w}\frac{2^n - j}{2^n} \geq 1 - \frac{w^2 q}{2^n}\,. \tag{6}$$

This gives $\beta = \frac{w^2 q}{2^n}$ and completes the proof. □

4 CENC

Let $k, m, n, \ell, w \in \mathbb{N}$ such that $m + r + s = n$ for $r = \lceil \log_2(\ell) \rceil$ and $s = \lceil \log_2(w+1) \rceil$. Let $E \in \mathsf{B}(k, n)$. We define encryption scheme $\mathsf{CENC}[w] : \{0,1\}^k \times \{0,1\}^m \times \{0,1\}^{\leq \ell w n} \to \{0,1\}^{\leq \ell w n}$ as

$$\mathsf{CENC}[w](K, N, M) = \Big\|_{i=0}^{\ell_m/w-1} \mathsf{XORP}[w](K, N\|\langle i\rangle_r) \oplus M_{wi}\| \cdots \|M_{w(i+1)-1}\,, \tag{7}$$

$\ell_m := \lceil M/n \rceil$ and M is parsed into $M_0\| \cdots \|M_{\ell_m - 1}$ where $|M_i| = n$ for $i = 0, \ldots, \ell_m - 2$ and $|M_{\ell_m - 1}| \leq n$. $\mathsf{CENC}[w]$ is depicted in Figure 2 for $w = 3$. Note that, compared to [3], the description of (7) simplifies the format of the blockcipher input blocks and omits the handling of incomplete last blocks for conciseness and clarity, but we see that these details do not affect the security analysis presented below.

Theorem 3. *Assume w.l.o.g. that ℓ/w is integral. We have*

$$\mathbf{Adv}^{\mathrm{cpa}}_{\mathsf{CENC}[w]}(q, \ell, t) \leq \frac{\ell w q}{2^n} + \mathbf{Adv}^{\mathrm{prp}}_E(\tfrac{w+1}{w}\ell q, t)\,. \tag{8}$$

Proof. Note that $\mathsf{CENC}[w]$ consists of ℓ/w invocations of $\mathsf{XORP}[w]$. We replace $\mathsf{XORP}[w]$ by a random function $\rho : \{0,1\}^{m+r} \to \{0,1\}^{wn}$ at the expense of

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{XORP}[w]}((\ell/w) \cdot q, t) \leq \frac{\ell w q}{2^n} + \mathbf{Adv}^{\mathrm{prp}}_E(\tfrac{w+1}{w}\ell q, t) \tag{9}$$

by Theorem 2. However, it is obvious that $\mathsf{CENC}[w]$ instantiated with ρ is perfectly secure. □

[5] We are currently adopting the notation from [9]. In the refurbished H-coefficient technique as outlined by Chen and Steinberger [2], β corresponds to the probability that an ideal world transcript is *bad*.

Acknowledgments. The authors would like to thank Farzaneh Abed, Pierre Karpman, Hristina Mihajloska, Samuel Neves, and Bart Preneel, as well as the organizers of the Lorentz workshop "HighLight: High-Security Lightweight Cryptography" for discussions that eventually lead to analyzing the optimal security of CENC. The work by Tetsu Iwata was supported by JSPS KAKENHI, Grant-in-Aid for Scientific Research (B), Grant Number 26280045, and was carried out while visiting Nanyang Technological University, Singapore. Bart Mennink is a Postdoctoral Fellow of the Research Foundation – Flanders (FWO).

References

1. Bellare, M., Impagliazzo, R.: A tool for obtaining tighter security analyses of pseudorandom function based constructions, with applications to PRP to PRF conversion. Cryptology ePrint Archive, Report 1999/024 (1999)
2. Chen, S., Steinberger, J.P.: Tight security bounds for key-alternating ciphers. In: Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings. Lecture Notes in Computer Science, vol. 8441, pp. 327–350. Springer (2014)
3. Iwata, T.: New blockcipher modes of operation with beyond the birthday bound security. In: Fast Software Encryption, 13th International Workshop, FSE 2006, Graz, Austria, March 15-17, 2006, Revised Selected Papers. Lecture Notes in Computer Science, vol. 4047, pp. 310–327. Springer (2006)
4. Lefranc, D., Painchault, P., Rouat, V., Mayer, E.: A generic method to design modes of operation beyond the birthday bound. In: Selected Areas in Cryptography, 14th International Workshop, SAC 2007, Ottawa, Canada, August 16-17, 2007, Revised Selected Papers. Lecture Notes in Computer Science, vol. 4876, pp. 328–343. Springer (2007)
5. Lucks, S.: The sum of PRPs is a secure PRF. In: Advances in Cryptology - EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceeding. Lecture Notes in Computer Science, vol. 4047, pp. 470–484. Springer (2000)
6. Patarin, J.: Luby-rackoff: 7 rounds are enough for $2^{n(1-\varepsilon)}$ security. In: Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings. Lecture Notes in Computer Science, vol. 2729, pp. 513–529. Springer (2003)
7. Patarin, J.: On linear systems of equations with distinct variables and small block size. In: Information Security and Cryptology - ICISC 2005, 8th International Conference, Seoul, Korea, December 1-2, 2005, Revised Selected Papers. Lecture Notes in Computer Science, vol. 3935, pp. 299–321. Springer (2006)
8. Patarin, J.: A proof of security in $o(2^n)$ for the xor of two random permutations. In: Information Theoretic Security, Third International Conference, ICITS 2008, Calgary, Canada, August 10-13, 2008, Proceedings. Lecture Notes in Computer Science, vol. 5155, pp. 232–248. Springer (2008)
9. Patarin, J.: Introduction to mirror theory: Analysis of systems of linear equalities and linear non equalities for cryptography. Cryptology ePrint Archive, Report 2010/287 (2010)