The Relation Between CENC and NEMO

Bart Mennink

Digital Security Group, Radboud University, Nijmegen, The Netherlands
b.mennink@cs.ru.nl

Abstract. Counter mode encryption uses a blockcipher to generate a key stream, which is subsequently used to encrypt data. The mode is known to achieve security up to the birthday bound. In this work we consider two approaches in literature to improve it to beyond birthday bound security: CENC by Iwata (FSE 2006) and its generalization NEMO by Lefranc et al. (SAC 2007). Whereas recent discoveries on CENC argued optimal security, the state of the art of NEMO is still sub-optimal. We draw connections among various instantiations of CENC and NEMO, and particularly prove that the improved optimal security bound on the CENC family carries over to a large class of variants of NEMO. We further conjecture that it also applies to the remaining variants, and discuss bottlenecks in proving so.

Keywords: CENC, NEMO, optimality, linear codes

1 Introduction

The most well-known blockcipher based encryption mode is counter mode encryption: given an n-bit keyed blockcipher E_k, a message M of (without loss of generality) length $\ell \cdot n$ bits is encrypted by generating a random looking key stream of ℓ blocks,

$$E_k(N) \,\|\, E_k(N+1) \,\|\, \cdots \,\|\, E_k(N+\ell-1)\,, \tag{1}$$

and XORing this key stream to the message M. Here, N is an initial value that needs to meet certain criteria irrelevant for the current treatment. This mode is known to be birthday bound secure: as E is a blockcipher, the generated key stream does not expose collisions whereas after the generation of around $2^{n/2}$ blocks a truly random key stream would expose collisions.

Beyond birthday bound encryption modes aim to achieve security beyond this bound. A simple way of achieving beyond birthday bound security for counter mode is by implementing it with a PRF, the most logical choice being the sum of permutations, where every key stream block is constituted of the sum of two blockcipher calls. For example, the first key stream block would be

$$E_k(N\|0) \oplus E_k(N\|1)\,, \tag{2}$$

where the nonce is now an $(n-1)$-bit string. After a long line of research [2, 3, 10, 14], Patarin [15] and later Dai et al. [5] proved that this construction is

secure up to 2^n key stream block generations. Unfortunately, the construction is expensive, requiring two blockcipher calls per data block.

In 2006, Iwata introduced CENC, an elegant and relatively cheap adjustment of counter mode that also achieves security beyond the birthday bound. At a high level, for a predetermined value $w \geq 1$, in every chunk of $w+1$ blockcipher calls, the first one is "sacrificed:" it is not used as key stream but rather used to mask the remaining w chunks. It only allows for nonces of size m bits with $m < n$, and generates its first w key stream blocks as

$$E_k(N\|0_s) \oplus E_k(N\|1_s) \,\|\, \cdots \,\|\, E_k(N\|0_s) \oplus E_k(N\|w_s)\,, \tag{3}$$

after which N is incremented and w new blocks are generated. Here, i_s denotes the encoding of i as an $s = (n-m)$-bit string. Iwata proved security of CENC$[w]$ for $w \geq 1$ up to around $2^{2n/3}$ key stream block generations, and conjectured security up to around $2^n/w$ key stream block generations. Only recently, Iwata et al. [7] confirmed this bound, pointing out that it was a direct consequence of Patarin's Mirror Theory [11–13, 15]. Bhattacharya and Nandi [4] derived a comparable bound using the Chi Squared Theory [5]. See also Section 3.1.

Soon after the introduction of CENC, Lefranc et al. [9] introduced a generalization called NEMO. Rather than being parametrized by w and using $w+1$ blockcipher outputs per w keystream blocks, NEMO$[\boldsymbol{G}]$ is instantiated using a matrix $\boldsymbol{G}$ of size $w \times v$ and it generates w keystream blocks using v blockcipher outputs as

$$\boldsymbol{G} \cdot \begin{pmatrix} E_k(N\|0_s) \\ E_k(N\|1_s) \\ \cdots \\ E_k(N\|(v-1)_s) \end{pmatrix}. \tag{4}$$

Lefranc et al. proved that if $\boldsymbol{G}$ is the generator matrix of a $[v, w, d]$ code, where d is the distance of the code (see Section 2.4), then the resulting scheme achieves security up to approximately $(2^n/v)^{d/(d+1)}$ key stream block generations (simplified, assuming that $w \approx v^{d/(d+1)}$). See also Section 3.2. The term is quite complicated, but important is the exponent $d/(d+1)$, where for small d it gives suboptimal security. For larger d the bound goes to optimal security, but the mode becomes less efficient: by the Singleton bound [16], one requires $v \geq w + d - 1$ blockcipher evaluations to generate w blocks with distance d.

1.1 Equivalences

One can consider counter mode with the sum of permutations as a special case of CENC (with $w = 1$). What is more, one can consider the general CENC$[w]$ as a special case of NEMO, namely with generator matrix

$$\boldsymbol{G}_{\mathsf{CENC}[w]} = \left[\begin{array}{c|ccc} 1 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \cdots & 1 \end{array}\right]. \tag{5}$$

Table 1: Rate (key stream blocks per blockcipher evaluations) and security (up to the number of key stream blocks) and for all variants of counter mode. $\mathsf{NEMO}[v, w, d]$ is short for $\mathsf{NEMO}[\boldsymbol{G}]$ for generator matrix $\boldsymbol{G}$ of a binary $[v, w, d]$ code. For state of the art, only the most recent citations are given.

mode	rate	security	reference
plain counter (1)	1	$2^{n/2}$	[1]
sum of permutation (2)	1/2	2^n	[5, 15]
$\mathsf{CENC}[w]$ (3)	$w/(w+1)$	$2^n/w$	[4, 7]
$\mathsf{NEMO}[v, w, d]$ (4)	w/v	$(2^n/v)^{d/d+1}$	[9]
		$2^n/v$	Section 4.1*
		$2^n/v$	Section 4.2**

* for even-weight code only
** conjectured bound for arbitrary code

In light of this, the state of the art on NEMO appears to be outdated.

In this work, we further explore the connection between the generalized $\mathsf{CENC}[w]$ (for arbitrary w) and $\mathsf{NEMO}[\boldsymbol{G}]$ (for arbitrary generator matrix $\boldsymbol{G}$). First, noting that for efficiency reasons, one would prefer $\boldsymbol{G}$ to be binary and Maximum Distance Separable (MDS). Textbook results dictate that only three such codes exist, namely the trivial $[v, v, 1]$, $[v, 1, v]$, and $[v, v-1, 2]$ codes [17, Prop. 9.2].

- Binary $[v, v, 1]$ MDS code. This code corresponds to plain counter mode of (1), giving tight $2^{n/2}$ birthday bound security.
- Binary $[v, 1, v]$ MDS code. This code corresponds to counter mode based on the sum of permutations of (2),[1] giving tight 2^n security.
- Binary $[v, v-1, 2]$ MDS code. This code, finally, is generated among others by $\boldsymbol{G}_{\mathsf{CENC}[w]}$ of (5), i.e., corresponds to CENC.

Inspired by this, one may argue that any other implementation of $\mathsf{NEMO}[\boldsymbol{G}]$ performs sub-optimally compared with state of the art.

We further investigate the security of $\mathsf{NEMO}[\boldsymbol{G}]$ for arbitrary matrices and derive two results. First, in Section 4.1 we prove that for any $\boldsymbol{G}$ generating a binary $[v, w, d]$ code with even-weight codewords only, $\mathsf{NEMO}[\boldsymbol{G}]$ is at least as secure as $\mathsf{CENC}[v-1]$. Second, in Section 4.2 we explore the possibilities for arbitrary generator matrices $\boldsymbol{G}$ (that have odd-weight codewords) and conjecture that a similar bound can be obtained. The state of the art and the new bounds are compared in Table 1.

[1] This follows from looking at the modes at a pseudorandom function level, i.e., isolating the pseudorandom function $F_k(N) = E_k(N\|0) \oplus E_k(N\|1)$ from the mode.

1.2 Understanding the Equivalences

In Section 5 we elaborate on possible alternatives of $\mathsf{CENC}[w]$, where a different generator matrix of the $[v, v-1, 2]$ code is applied. A particularly interesting approach would be to use

$$\boldsymbol{G}_{\mathsf{CENC}'[w]} = \begin{bmatrix} 1\,1\,0 \cdots 0\,0 \\ 0\,1\,1 \cdots 0\,0 \\ \vdots\;\vdots\;\vdots\;\ddots\;\vdots\;\vdots \\ 0\,0\,0 \cdots 1\,1 \end{bmatrix} \tag{6}$$

instead of $\boldsymbol{G}_{\mathsf{CENC}[w]}$ of (5). This diagonalized version of $\mathsf{CENC}[w]$ gives the exact same level of security (by Lemma 1 in Section 4.1), but may allow for more elegant implementations and easier interpretations. In addition, it allows for drawing a different connection between $\mathsf{CENC}[w]$ and counter mode based on the sum of permutations of (2), as the latter can be obtained from $\mathsf{CENC}'[w]$ by discarding every second key stream block.

2 Preliminaries

For $m, n \in \mathbb{N}$, we denote by $\{0,1\}^n$ the set of all n-bit strings. We denote by $\mathsf{P}(n)$ the set of all permutations on $\{0,1\}^n$, $\mathsf{F}(m,n)$ the set of all functions from $\{0,1\}^m$ to $\{0,1\}^n$, and m_n the encoding of the number m as an n-bit string. For a set $\mathcal{S}$, $s \xleftarrow{\$} \mathcal{S}$ denotes uniformly random sampling of s from $\mathcal{S}$.

2.1 Blockcipher

A blockcipher $E : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$ is a family of permutations indexed by a key $k \in \{0,1\}^\kappa$. We denote by $\mathbf{Adv}^{\mathrm{prp}}_E(\mathcal{D})$ the advantage of a distinguisher $\mathcal{D}$ in distinguishing E from an ideal permutation $\pi \xleftarrow{\$} \mathsf{P}(n)$:

$$\mathbf{Adv}^{\mathrm{prp}}_E(\mathcal{D}) = \mathbf{Pr}\left(k \xleftarrow{\$} \{0,1\}^\kappa \;:\; \mathcal{D}^{E_k} \to 1\right) - \mathbf{Pr}\left(\pi \xleftarrow{\$} \mathsf{P}(n) \;:\; \mathcal{D}^{\pi} \to 1\right). \tag{7}$$

We denote $\mathbf{Adv}^{\mathrm{prp}}_E(q,t) = \sup_{\mathcal{D}} \mathbf{Adv}^{\mathrm{prp}}_E(\mathcal{D})$, where the supremum is taken over all distinguishers that can make q queries and operate in t time.

2.2 Pseudorandom Function

A pseudorandom function $F : \{0,1\}^\kappa \times \{0,1\}^m \to \{0,1\}^n$ is a family of functions in $\mathsf{F}(m,n)$ indexed by a key $k \in \{0,1\}^\kappa$. We denote by $\mathbf{Adv}^{\mathrm{prf}}_F(\mathcal{D})$ the advantage of a distinguisher $\mathcal{D}$ in distinguishing F from an ideal function $\rho \xleftarrow{\$} \mathsf{F}(m,n)$:

$$\mathbf{Adv}^{\mathrm{prf}}_F(\mathcal{D}) = \mathbf{Pr}\left(k \xleftarrow{\$} \{0,1\}^\kappa \;:\; \mathcal{D}^{F_k} \to 1\right) - \mathbf{Pr}\left(\rho \xleftarrow{\$} \mathsf{F}(m,n) \;:\; \mathcal{D}^{\rho} \to 1\right). \tag{8}$$

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

2.3 Encryption

A nonce based encryption scheme $\mathcal{E} : \{0,1\}^\kappa \times \{0,1\}^n \times \{0,1\}^* \to \{0,1\}^*$ is a function that operates on a secret key k. On input of a nonce N and an arbitrarily length message M, it 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 a random function \$ that for every query (N, M) returns a random ciphertext C of size $|M|$:

$$\mathbf{Adv}^{\mathrm{cpa}}_{\mathcal{E}}(\mathcal{D}) = \mathbf{Pr}\left(k \xleftarrow{\$} \{0,1\}^\kappa \ : \ \mathcal{D}^{\mathcal{E}_k} \to 1\right) - \mathbf{Pr}\left(\$ \xleftarrow{\$} \mathsf{F}(n+*,*) \ : \ \mathcal{D}^{\$} \to 1\right),$$

where, with abuse of notation, $\mathsf{F}(n+*,*)$ is the set of all functions that get as input an n-bit block and an arbitrarily length block, and output a string of the same size as the arbitrarily length block. Distinguisher $\mathcal{D}$ is required to be nonce-respecting, meaning that it should not repeat nonces. We denote $\mathbf{Adv}^{\mathrm{cpa}}_{\mathcal{E}}(q,\ell,t) = \sup_{\mathcal{D}} \mathbf{Adv}^{\mathrm{cpa}}_{\mathcal{E}}(\mathcal{D})$, where the supremum is taken over all distinguishers that can make q queries of length ℓ n-bit blocks and operate in t time.

2.4 Linear Codes

Let $v, w \in \mathbb{N}$ be such that $v \geq w$. A binary linear code of length v and rank w transforms vectors in $\{0,1\}^w$ into vectors in $\{0,1\}^v$ using a generator matrix $\boldsymbol{G} \in \{0,1\}^{w \times v}$.[2] The distance of the code is defined as

$$d := \min_{\substack{\boldsymbol{x} \in \{0,1\}^w \\ \boldsymbol{x} \neq 0}} \left|\boldsymbol{x}^\top \cdot \boldsymbol{G}\right| . \tag{9}$$

The code C is referred to as a $[v, w, d]$ code. We call a code *even-weight* if all code words have even weight (hence the name). The rows of the generator matrix form a basis of the code, and hence, for any generator matrix $\boldsymbol{G} \in \{0,1\}^{w \times v}$ and invertible $\boldsymbol{P} \in \{0,1\}^{w \times w}$, the generator matrices $\boldsymbol{G}$ and $\boldsymbol{G'} = \boldsymbol{P} \cdot \boldsymbol{G}$ correspond to the same code.

According to the well-known Singleton bound [16], the code necessarily satisfies $v - w \geq d - 1$. A Maximum Distance Separable (MDS) code is a code that achieves equality in the Singleton bound. An elementary result [17, Prop. 9.2] states that the only binary MDS codes are the trivial $[v, v, 1]$, $[v, 1, v]$, and $[v, v-1, 2]$ codes. The second of the two is the repetition code (encode a bit by a v-fold repetition of that bit) and the latter is its dual that can be generated by the following matrix:

$$\boldsymbol{G}^\star_{v-1} := \left[\begin{array}{ccc|c} 1 & 0 & \cdots & 0 & 1 \\ 0 & 1 & \cdots & 0 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 1 \end{array}\right] \in \{0,1\}^{(v-1)\times v} . \tag{10}$$

[2] In this work we are only concerned with *binary* linear codes.

3 CENC and NEMO

Let $\kappa, m, n, v, w \in \mathbb{N}$ such that $v \geq w$ and $m + s = n$ for $s = \lceil \log_2(v) \rceil$. Let $E \in \mathsf{B}(\kappa, n)$. Both CENC and NEMO can be described by a pseudorandom function $F : \{0,1\}^\kappa \times \{0,1\}^m \to \{0,1\}^{wn}$ based on v evaluations of E_k. This pseudorandom function is then evaluated in counter mode, in such a way that F_k is never evaluated twice for the same input. The following theorem is a straightforward exercise.

Theorem 1. *Let $F : \{0,1\}^\kappa \times \{0,1\}^m \to \{0,1\}^{wn}$ be a pseudorandom function (in this work, F is either the pseudorandom function of* CENC *or of* NEMO*), and let $\mathcal{E}$ be counter mode encryption based on F. We have,*

$$\mathbf{Adv}^{\mathrm{cpa}}_{\mathcal{E}}(q, \ell, t) \leq \mathbf{Adv}^{\mathrm{prf}}_{F}(\lceil \ell / w \rceil q, t)\,. \tag{11}$$

The proof is trivial and henceforth omitted. We proceed discussing the pseudorandom function of CENC and NEMO.

3.1 CENC Pseudorandom Function

CENC was introduced by Iwata [6], but we rephrase it in our terminology. The pseudorandom function $\mathsf{CENC}[w] : \{0,1\}^\kappa \times \{0,1\}^m \to \{0,1\}^{wn}$ has $v = w + 1$, hence it makes $w + 1$ calls to the underlying blockcipher, and is defined as

$$\mathsf{CENC}[w]_k(x) = \underbrace{\left[\begin{array}{c|ccc} 1 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \cdots & 1 \end{array}\right]}_{=: \boldsymbol{G}_{\mathsf{CENC}[w]}} \cdot \begin{pmatrix} E_k(x \| 0_s) \\ E_k(x \| 1_s) \\ \cdots \\ E_k(x \| w_s) \end{pmatrix}, \tag{12}$$

recalling that $s = \lceil \log_2(w + 1) \rceil$ and $m + s = n$. Note that $\boldsymbol{G}_{\mathsf{CENC}[w]}$ can be obtained from $\boldsymbol{G}^\star_w$ of (10) by left multiplication with an invertible matrix, and hence, the two matrices generate the same code.

Iwata et al. [7] derived the following bound on $\mathsf{CENC}[w]$ using the Mirror Theory [11–13, 15]:

Theorem 2 (Iwata et al. [7]). *We have, provided $wq \leq 2^n/67$,*

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{CENC}[w]}(q, t) \leq \frac{w^2 q}{2^n} + \mathbf{Adv}^{\mathrm{prp}}_{E}((w+1)q, t)\,. \tag{13}$$

Bhattacharya and Nandi [4] derived a comparable bound using the Chi Squared Theory [5]:

Theorem 3 (Bhattacharya and Nandi [4]). *We have,*

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{CENC}[w]}(q, t) \leq \frac{(1+\sqrt{2})(w+1)^2 q}{2^n} + \mathbf{Adv}^{\mathrm{prp}}_{E}((w+1)q, t)\,. \tag{14}$$

3.2 NEMO Pseudorandom Function

NEMO was introduced by Lefranc et al. [9]. Let $\boldsymbol{G}$ be the generator matrix of a $[v, w, d]$ code. Then the pseudorandom function $\mathsf{NEMO}[\boldsymbol{G}] : \{0,1\}^\kappa \times \{0,1\}^m \to \{0,1\}^{wn}$ makes v calls to the underlying blockcipher, and is defined as

$$\mathsf{NEMO}[\boldsymbol{G}]_k(x) = \boldsymbol{G} \cdot \begin{pmatrix} E_k(x\|0_s) \\ E_k(x\|1_s) \\ \cdots \\ E_k(x\|v-1_s) \end{pmatrix}, \tag{15}$$

recalling that $s = \lceil \log_2(v) \rceil$ and $m + s = n$.

Lefranc et al. [9] derived the following bound on $\mathsf{NEMO}[\boldsymbol{G}]$ for any generator matrix of binary $[v, w, d]$ code:

Theorem 4. *Let $\boldsymbol{G}$ be the generator matrix of a binary $[v, w, d]$ code. We have,*

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{NEMO}[\boldsymbol{G}]}(q, t) \le \frac{v^2 q}{2^n} + \frac{v^{2d} q^{d+1}}{2^{dn}} + \mathbf{Adv}^{\mathrm{prp}}_E(vq, t)\,. \tag{16}$$

4 Equivalences

It is obvious from the definitions of the pseudorandom functions of CENC in (12) and NEMO in (15) that NEMO is a direct generalization of CENC, in the sense that

$$\mathsf{NEMO}[\boldsymbol{G}_{\mathsf{CENC}[w]}] = \mathsf{CENC}[w]\,. \tag{17}$$

However, the generic security bounds on $\mathsf{CENC}[w]$ in Theorems 2 and 3 are better than that of $\mathsf{NEMO}[\boldsymbol{G}]$ in Theorem 4, regardless of the generator matrix in use. In this section, we will explore the connection further, draw equivalences and reductions among the various instantiations of $\mathsf{CENC}[w]$ and $\mathsf{NEMO}[\boldsymbol{G}]$.

First, in Section 4.1, we focus on generator matrices $\boldsymbol{G}$ for even-weight linear codes of length v, and demonstrate that their induced $\mathsf{NEMO}[\boldsymbol{G}]$'s are at least as secure as $\mathsf{CENC}[v-1]$. In Section 4.2, we look beyond even-weight codes, conjecture that a similar result can be obtained for arbitrary generator matrices, and discuss bottlenecks in the analysis.

4.1 Even-Weight Linear Code

We will reduce the security of $\mathsf{NEMO}[\boldsymbol{G}]$ for a generator matrix $\boldsymbol{G}$ of an even-weight $[v, w, d]$ code to the security of $\mathsf{CENC}[v-1]$.

Theorem 5 (Security of NEMO for even-weight binary code). *Let $\boldsymbol{G}$ be a generator matrix of a binary even-weight $[v, w, d]$ code with $v > w$. We have,*

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{NEMO}[\boldsymbol{G}]}(q, t) \le \mathbf{Adv}^{\mathrm{prf}}_{\mathsf{CENC}[v-1]}(q, t)\,. \tag{18}$$

Proof. Let $\boldsymbol{G}$ be a generator matrix of a binary even-weight $[v, w, d]$ code. Define the matrix

$$\boldsymbol{A} = \left[\boldsymbol{0}_{(v-w-1)\times w}\ \boldsymbol{G}^{\star}_{v-w-1}\right] \in \{0,1\}^{(v-w-1)\times v}\,, \tag{19}$$

where $\boldsymbol{G}^{\star}_{v-w-1}$ is the matrix of (10) corresponding to the trivial $[v-w, v-w-1, 2]$ MDS code.

First Step. As a first step, we will prove that the following two matrices are row equivalent:

$$\begin{bmatrix}\boldsymbol{G}\\ \boldsymbol{A}\end{bmatrix} \sim \boldsymbol{G}^{\star}_{v-1}\,, \tag{20}$$

where $\boldsymbol{G}^{\star}_{v-1}$ of (10) corresponds to the trivial $[v, v-1, 2]$ MDS code. To prove (20), row reduction on $\boldsymbol{G}$ demonstrates the existence of a matrix $\boldsymbol{B} \in \{0,1\}^{w\times(v-w)}$ such that $\boldsymbol{G} \sim \left[\boldsymbol{I}_w\ \boldsymbol{B}\right]$. Thus:

$$\begin{bmatrix}\boldsymbol{G}\\ \boldsymbol{A}\end{bmatrix} \sim \begin{bmatrix}\boldsymbol{I}_w & \boldsymbol{B}\\ \boldsymbol{0}_{(v-w-1)\times w} & \boldsymbol{G}^{\star}_{v-w-1}\end{bmatrix}\,. \tag{21}$$

As $\boldsymbol{G}$ is an even-weight generator matrix, every row in $\boldsymbol{B}$ has odd weight. Consider any row $[b_1\ b_2\ \ldots\ b_{v-w}]$ in $\boldsymbol{B}$. For each $i \in \{1, \ldots, v-w-1\}$ such that $b_i = 1$, add the i-th row of $\boldsymbol{G}^{\star}_{v-w-1}$ (or, equivalently, the $(w+i)$-th row of the entire matrix) to this row in $\boldsymbol{B}$. As the original row has odd weight, and each row in $\boldsymbol{G}^{\star}_{v-w-1}$ has even weight, the resulting row in $\boldsymbol{B}$ has odd weight, and is in particular of the form $[0\ 0\ \ldots\ 1]$. Performing this elimination algorithm for all rows in $\boldsymbol{B}$, we subsequently have

$$\begin{bmatrix}\boldsymbol{I}_w & \boldsymbol{B}\\ \boldsymbol{0}_{(v-w-1)\times w} & \boldsymbol{G}^{\star}_{v-w-1}\end{bmatrix} \sim \boldsymbol{G}^{\star}_{v-1}\,, \tag{22}$$

completing the proof of (20).

Second Step. The second step is to note that $\boldsymbol{G}^{\star}_{v-1}$ is row equivalent to $\boldsymbol{G}_{\mathsf{CENC}[v-1]}$ of (5):

$$\boldsymbol{G}^{\star}_{v-1} \sim \boldsymbol{G}_{\mathsf{CENC}[v-1]}\,. \tag{23}$$

This equivalence is immediate and does not require further discussion.

Third Step. Combining (20) and (23), there exists an invertible matrix $\boldsymbol{P} \in \{0,1\}^{(v-1)\times(v-1)}$ such that

$$\boldsymbol{P} \circ \boldsymbol{G}_{\mathsf{CENC}[v-1]} = \begin{bmatrix}\boldsymbol{G}\\ \boldsymbol{A}\end{bmatrix}\,. \tag{24}$$

This immediately completes the proof using Lemmas 1 and 2 below, as

$$\begin{aligned}
\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{NEMO}[\boldsymbol{G}]}(q,t) &\leq \mathbf{Adv}^{\mathrm{prf}}_{\mathsf{NEMO}[\boldsymbol{P}\circ\boldsymbol{G}_{\mathsf{CENC}[v-1]}]}(q,t) \text{ by Lemma 2 and (24)}\,, && (25)\\
&= \mathbf{Adv}^{\mathrm{prf}}_{\mathsf{NEMO}[\boldsymbol{G}_{\mathsf{CENC}[v-1]}]}(q,t) \text{ by Lemma 1}\,, && (26)\\
&= \mathbf{Adv}^{\mathrm{prf}}_{\mathsf{CENC}[v-1]}(q,t) \text{ by (17)}\,. && (27)
\end{aligned}$$

□

Lemma 1. *Let $\boldsymbol{G}, \boldsymbol{G'} \in \{0,1\}^{w\times v}$ be two generator matrices such that $\boldsymbol{G'} = \boldsymbol{P}\cdot\boldsymbol{G}$ for some invertible matrix $\boldsymbol{P} \in \{0,1\}^{w\times w}$. We have,*

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{NEMO}[\boldsymbol{G}]}(q,t) = \mathbf{Adv}^{\mathrm{prf}}_{\mathsf{NEMO}[\boldsymbol{G'}]}(q,t)\,. \tag{28}$$

Proof. The proof is a trivial consequence of the fact that $\boldsymbol{G}$ and $\boldsymbol{G'}$ generate the same code. Let $\mathcal{D}$ be a distinguisher against $\mathsf{NEMO}[\boldsymbol{G}]$, we will construct a distinguisher $\mathcal{D}'$ against $\mathsf{NEMO}[\boldsymbol{G'}]$ with at least the same success probability at $\mathcal{D}$. For each query x that $\mathcal{D}$ makes, $\mathcal{D}'$ queries x to its own oracle, receives a wn-bit string y. Treating it as a vector of w n-bit blocks $\boldsymbol{y}$, it computes $\boldsymbol{P}^{-1}\boldsymbol{y}$ and sends it to $\mathcal{D}$. Then, if $\mathcal{D}$ makes its final decision, $\mathcal{D}'$ forwards its choice. Distinguisher $\mathcal{D}'$ succeeds if $\mathcal{D}$ succeeds. This holds for any distinguisher $\mathcal{D}$, and hence, $\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{NEMO}[\boldsymbol{G}]}(q,t) \leq \mathbf{Adv}^{\mathrm{prf}}_{\mathsf{NEMO}[\boldsymbol{G'}]}(q,t)$. As $\boldsymbol{P}$ is invertible, the proof in reverse direction is symmetric. □

Lemma 2. *Let $\boldsymbol{G} \in \{0,1\}^{w\times v}$ and $\boldsymbol{G'} \in \{0,1\}^{w'\times v}$ be two generator matrices such that $\boldsymbol{G'} = \begin{bmatrix}\boldsymbol{G}\\ \boldsymbol{A}\end{bmatrix}$ for some matrix $\boldsymbol{A} \in \{0,1\}^{(w'-w)\times v}$. We have,*

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{NEMO}[\boldsymbol{G}]}(q,t) \leq \mathbf{Adv}^{\mathrm{prf}}_{\mathsf{NEMO}[\boldsymbol{G'}]}(q,t)\,. \tag{29}$$

Proof. The proof is a trivial consequence of the fact that $\boldsymbol{G}$ can be obtained from "expurgating" $\boldsymbol{G'}$ [17, Sect 5.4.2]. Let $\mathcal{D}$ be a distinguisher against $\mathsf{NEMO}[\boldsymbol{G}]$, we will construct a distinguisher $\mathcal{D}'$ against $\mathsf{NEMO}[\boldsymbol{G'}]$ with at least the same success probability at $\mathcal{D}$. For each query x that $\mathcal{D}$ makes, $\mathcal{D}'$ queries x to its own oracle, receives a $w'n$-bit string y. It forwards the first wn bits to $\mathcal{D}$. Then, if $\mathcal{D}$ makes its final decision, $\mathcal{D}'$ forwards its choice. Distinguisher $\mathcal{D}'$ succeeds if $\mathcal{D}$ succeeds. This holds for any distinguisher $\mathcal{D}$, and hence, $\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{NEMO}[\boldsymbol{G}]}(q,t) \leq \mathbf{Adv}^{\mathrm{prf}}_{\mathsf{NEMO}[\boldsymbol{G'}]}(q,t)$. □

Remark 1. We remark that, due to its generality, the bound of Theorem 5 is non-optimal. Consider, for example, generator matrix

$$\boldsymbol{G}_{\mathsf{XOP}[w]} = \begin{bmatrix} 1\,1\,0\,0\cdots 0\,0\\ 0\,0\,1\,1\cdots 0\,0\\ \vdots\,\vdots\,\vdots\,\vdots\,\ddots\,\vdots\,\vdots\\ 0\,0\,0\,0\cdots 1\,1\end{bmatrix} \in \{0,1\}^{w\times 2w}\,, \tag{30}$$

for which $\mathsf{NEMO}[\boldsymbol{G}_{\mathsf{XOP}[w]}]$ corresponds to a parallel evaluation of w sums of permutations. Patarin [15] and later Dai et al. [5] demonstrated that this construction is secure up to around $wq/2^n$. The proof of Theorem 5 augments the generator matrix to

$$\left[\begin{array}{cccccc} 1 & 1 & 0 & 0 & \cdots & 0\ 0 \\ 0 & 0 & 1 & 1 & \cdots & 0\ 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots\ \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1\ 1 \\ \hline 0 & 1 & 0 & 0 & \cdots & 0\ 1 \\ 0 & 0 & 0 & 1 & \cdots & 0\ 1 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots\ \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0\ 1 \end{array}\right] \in \{0,1\}^{(2w-1)\times 2w}\,, \tag{31}$$

which generates the same code as $\boldsymbol{G}^{\star}_{2w-1}$ of (10) and $\boldsymbol{G}_{\mathsf{CENC}[2w-1]}$ of (12), and it gives an upper bound of around $(2w)^2q/2^n$.

4.2 Arbitrary Linear Codes

We conjecture that the result of Theorem 5 extends to arbitrary binary linear codes.

Conjecture 1 (Security of NEMO *for arbitrary binary code).* Let $\boldsymbol{G}$ be a generator matrix of a binary $[v, w, d]$ code with $v > w$. We have,

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{NEMO}[\boldsymbol{G}]}(q,t) \le \mathbf{Adv}^{\mathrm{prf}}_{\mathsf{CENC}[v-1]}(q,t)\,. \tag{32}$$

The result is intuitively appealing. As $\boldsymbol{G}_{\mathsf{CENC}[v-1]}$ corresponds to a binary $[v, v-1, 2]$ MDS code, it gives the most one can get out off v blocks of randomness. Stated differently, $v-1$ output blocks are generated using v blocks of randomness. Outputting another block would degrade the security of the scheme to the birthday bound. Conversely, any other $[v, w, d]$ code for $d \ge 2$ outputs less data, hence exposes less of the v blocks of randomness, and is likely to be more secure.

The proof of Theorem 5 does not stretch to Conjecture 1, and the reason is that an arbitrary generator matrix $\boldsymbol{G}$ cannot necessarily be augmented to $\boldsymbol{G}^{\star}_{v-1}$ for binary $[v, v-1, 2]$ code. A simple example is given by

$$\boldsymbol{G}_{\mathrm{bad}} := \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}\,. \tag{33}$$

For this matrix, $\mathsf{NEMO}[\boldsymbol{G}_{\mathrm{bad}}]$ implements the function

$$\mathsf{NEMO}[\boldsymbol{G}_{\mathrm{bad}}]_k(x) = E_k(x\|0_s) \oplus E_k(x\|1_s) \oplus E_k(x\|2_s)\,, \tag{34}$$

which is seemingly more secure than

$$\mathsf{CENC}[2]_k(x) = E_k(x\|0_s) \oplus E_k(x\|1_s) \;\|\; E_k(x\|0_s) \oplus E_k(x\|2_s)\,. \tag{35}$$

Yet, there appears to be no simple reduction to argue this formally. In particularly, $\boldsymbol{G}_{\mathrm{bad}}$ cannot be augmented to $\boldsymbol{G}^{\star}_2$ of (10).

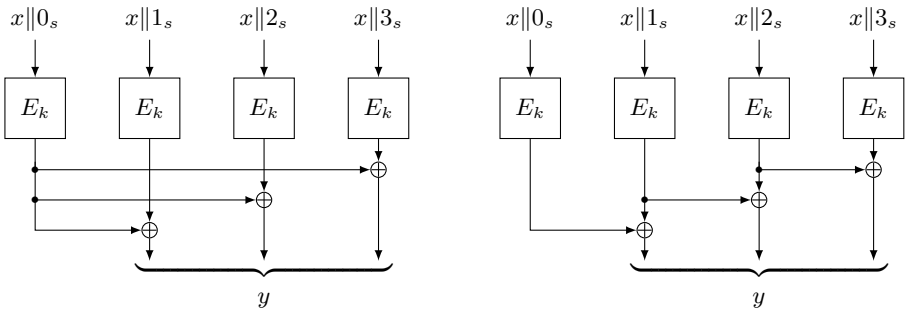

Fig. 1: $\mathsf{CENC}[3]_k$ of (12) (left) and $\mathsf{CENC}'[3]_k$ of (38) (right)

5 Understanding Equivalences

Recall $\boldsymbol{G}_{\mathsf{CENC}[w]}$ of (12):

$$\boldsymbol{G}_{\mathsf{CENC}[w]} := \begin{bmatrix} 1 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \cdots & 1 \end{bmatrix} \in \{0,1\}^{w \times (w+1)} . \tag{36}$$

By Lemma 1, left multiplication with an invertible matrix $\boldsymbol{P} \in \{0,1\}^{w \times w}$ does not decrease the security:

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{NEMO}[\boldsymbol{P} \cdot \boldsymbol{G}_{\mathsf{CENC}[w]}]}(q,t) = \mathbf{Adv}^{\mathrm{prf}}_{\mathsf{NEMO}[\boldsymbol{G}_{\mathsf{CENC}[w]}]}(q,t) = \mathbf{Adv}^{\mathrm{prf}}_{\mathsf{CENC}[w]}(q,t) , \tag{37}$$

recalling that $\mathsf{NEMO}[\boldsymbol{G}_{\mathsf{CENC}[w]}] = \mathsf{CENC}[w]$.

Note that an implementation of $\mathsf{CENC}[w]_k$ would have to compute $E_k(x\|0_s)$, store it, and add it to $E_k(x\|i_s)$ for $i = 1, \ldots, w$. See also Figure 1 (left). An alternative to $\mathsf{CENC}[w]$ would be $\mathsf{CENC}'[w]$ based on generator matrix

$$\boldsymbol{G}_{\mathsf{CENC}'[w]} := \begin{bmatrix} 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 1 \end{bmatrix} = \underbrace{\begin{bmatrix} 1 & 0 & \cdots & 0 & 0 \\ 1 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 1 \end{bmatrix}}_{=:\boldsymbol{P}} \cdot \boldsymbol{G}_{\mathsf{CENC}[w]} . \tag{38}$$

In this case, the i-th output block of $\mathsf{NEMO}[\boldsymbol{G}_{\mathsf{CENC}'[w]}]$ would be $E_k(x\|(i-1)_s) \oplus E_k(x\|i_s)$ as depicted in Figure 1 (right). This could be preferable in certain settings. The generator matrix of (38) gives another advantage: the transformation to the sum of permutations is immediate. One just needs to discard every second block to obtain a NEMO instantiation that mimics $w/2$ sums of permutations as

suggested by Remark 1 in Section 4.1:

$$\begin{bmatrix} 1 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & 1 \end{bmatrix} . \tag{39}$$

As mentioned in Remark 1, this scheme gives around $q/2^n$ security for the generation of q output blocks.

Acknowledgments. Bart Mennink is supported by a postdoctoral fellowship from the Netherlands Organisation for Scientific Research (NWO) under Veni grant 016.Veni.173.017.

References

1. Bellare, M., Desai, A., Jokipii, E., Rogaway, P.: A Concrete Security Treatment of Symmetric Encryption. In: 38th Annual Symposium on Foundations of Computer Science, FOCS '97, Miami Beach, Florida, USA, October 19-22, 1997. pp. 394–403. IEEE Computer Society (1997), https://doi.org/10.1109/SFCS.1997.646128
2. 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), http://eprint.iacr.org/1999/024
3. Bellare, M., Krovetz, T., Rogaway, P.: Luby-Rackoff Backwards: Increasing Security by Making Block Ciphers Non-invertible. In: Nyberg, K. (ed.) Advances in Cryptology - EUROCRYPT '98, International Conference on the Theory and Application of Cryptographic Techniques, Espoo, Finland, May 31 - June 4, 1998, Proceeding. Lecture Notes in Computer Science, vol. 1403, pp. 266–280. Springer (1998), https://doi.org/10.1007/BFb0054132
4. Bhattacharya, S., Nandi, M.: Revisiting Variable Output Length XOR Pseudorandom Function. IACR Trans. Symmetric Cryptol. 2018(1), 314–335 (2018), https://doi.org/10.13154/tosc.v2018.i1.314-335
5. Dai, W., Hoang, V.T., Tessaro, S.: Information-Theoretic Indistinguishability via the Chi-Squared Method. In: Katz and Shacham [8], pp. 497–523, https://doi.org/10.1007/978-3-319-63697-9_17
6. Iwata, T.: New Blockcipher Modes of Operation with Beyond the Birthday Bound Security. In: Robshaw, M.J.B. (ed.) 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), https://doi.org/10.1007/11799313_20
7. Iwata, T., Mennink, B., Vizár, D.: CENC is Optimally Secure. Cryptology ePrint Archive, Report 2016/1087 (2016), http://eprint.iacr.org/2016/1087
8. Katz, J., Shacham, H. (eds.): Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part III, Lecture Notes in Computer Science, vol. 10403. Springer (2017), https://doi.org/10.1007/978-3-319-63697-9

9. Lefranc, D., Painchault, P., Rouat, V., Mayer, E.: A Generic Method to Design Modes of Operation Beyond the Birthday Bound. In: Adams, C.M., Miri, A., Wiener, M.J. (eds.) 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), https://doi.org/10.1007/978-3-540-77360-3_21
10. Lucks, S.: The Sum of PRPs Is a Secure PRF. In: Preneel, B. (ed.) 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. 1807, pp. 470–484. Springer (2000), https://doi.org/10.1007/3-540-45539-6_34
11. Mennink, B., Neves, S.: Encrypted Davies-Meyer and Its Dual: Towards Optimal Security Using Mirror Theory. In: Katz and Shacham [8], pp. 556–583, https://doi.org/10.1007/978-3-319-63697-9_19
12. Nachef, V., Patarin, J., Volte, E.: Feistel Ciphers - Security Proofs and Cryptanalysis. Springer (2017), https://doi.org/10.1007/978-3-319-49530-9
13. Patarin, J.: On Linear Systems of Equations with Distinct Variables and Small Block Size. In: Won, D., Kim, S. (eds.) 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 (2005), https://doi.org/10.1007/11734727_25
14. Patarin, J.: A Proof of Security in $O(2^n)$ for the Xor of Two Random Permutations. In: Safavi-Naini, R. (ed.) 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), https://doi.org/10.1007/978-3-540-85093-9_22
15. 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), http://eprint.iacr.org/2010/287
16. Singleton, R.C.: Maximum distance q-nary codes. IEEE Trans. Information Theory 10(2), 116–118 (1964), https://doi.org/10.1109/TIT.1964.1053661
17. Vermani, L.R.: Elements of Algebraic Coding Theory. CRC Press (1996)