


# Circular Insecure Encryption: from Long Cycles to Short Cycles

Zehou Wu 

Department of Computer Science, University of Victoria, Canada  
wuzehouw@uvic.ca

**Abstract.** We prove that the existence of a CPA-secure encryption scheme that is insecure in the presence of key cycles of length  $n$  implies the existence of such a scheme for key cycles of any length less than  $n$ . Equivalently, if every encryption scheme in a class is  $n$ -circular secure and this class is closed under our construction, then every encryption scheme in this class is  $n'$ -circular secure for  $n' > n$ .

## 1 Introduction

The question of whether encryption security is maintained in the presence of self-encryption was identified during the early stages of modern cryptography [17], and in general, remains unanswered.

Theoretical considerations of circular security arise in a number of areas. One is the study of symbolic (formal) encryption [14], where a syntax is defined on sets of symbols to form expressions, these expressions combined with an entailment relation are used to model the ideal functionality of encryption functions. Abadi and Rogaway [1] sought to reconcile this symbolic approach of cryptography with the computational approach, highlighting the gap between them introduced by circular encryption. This gap is further studied in [3, 13, 20, 25, 27–30]. Without additional constraints on the symbolic side, circular security is crucial to the completeness of a logic. Another area in which circular security has become significant is the construction of various primitives whose security relies on underlying primitives with circular security properties. For example, LWE-based encryption with an additional circular security assumption is used to construct homomorphic encryption [11, 16] and indistinguishability obfuscation [15]. A well-known example of how circular encryption arises in practice is Windows BitLocker [31], where a key may be used to encrypt a disk that the key is stored on as data.

Given its potential for application in a variety of areas, there have been numerous works dealing with the (im)possibility of circular security under different scenarios, [2, 4, 7, 9, 12, 18, 19, 21, 24, 26, 32]. A particularly intriguing line of work involves finding relations between various key-cycle lengths and message spaces for circular secure schemes [5, 6, 10, 23]. Recently, it was shown in [34] that Key Dependent Message security, a more demanding notion than that of circular security [8], is reducible to 1-circular bit encryption.

Motivated by this, we are interested in finding other relations between notions of circular security. In this paper, we show that the existence of a longer-length circular insecure encryption scheme implies the existence of a shorter-length circular insecure encryption scheme. Equivalently, if every encryption scheme in a class is  $n$ -circular secure and this class is closed under our construction, then every encryption scheme in this class is  $n'$ -circular secure for  $n' > n$ .

### 1.1 Our Contribution

We present a newfound relationship for circular insecurity. To be more precise, we show that if an  $(n + 1)$ -circular insecure CPA secure encryption scheme exists, then a  $(1 \text{ to } n)$ -circular insecure CPA secure encryption scheme exists. This result applies to both public key and private key encryption schemes. We present the proof of the public key setting, which, with slight modification, can serve as proof in the symmetric key setting.

The proof uses a circular insecure encryption scheme as a black-box to construct another encryption scheme. In Construction 1, we present a construction that does not preserve the message space of the initial encryption scheme. In Construction 2, we construct an encryption scheme that preserves the message space of the base encryption scheme if the message space of the base scheme consists of only one bit. The techniques used in Construction 2 can be modified to preserve message spaces for a variety of base schemes.

Intuitively, the idea is to use an  $n + 1$ -circular insecure encryption  $\Pi$  to create an encryption scheme  $\Pi'$  so that a key of  $\Pi'$  consists of multiple keys in  $\Pi$ . This is done in a way so that from any length  $\ell$  encryption cycle where  $0 < \ell < n + 1$  of  $\Pi'$ , we can extract an encryption cycle with length  $n + 1$  of  $\Pi$ .

## Organization.

We will present the notation and definitions in Section 2. In Section 3, we present Construction 1, a message length non-preserving black-box construction. Its analysis follows in Section 4. Section 5 contains Construction 2, in which we discuss how to preserve a message space of only one bit in the black-box technique. We present a concise discussion on how to modify the results of this paper into the symmetric key setting in Section 6.

## 2 Preliminaries

We use PPT to denote probabilistic polynomial time. For a set  $S$ , we write  $s \leftarrow \$S$  to indicate that  $s$  is sampled uniformly from  $S$ . For a randomized function  $f$  with input  $x$ , we write  $y \leftarrow f(x)$  to indicate that  $y$  is the output of  $f(x)$  with fresh randomness.

**Definition 1.** A public key encryption scheme consists of three efficiently computable randomized functions: a key generating function  $\mathcal{G}$ , encryption function  $\mathcal{E}$ , and decryption function  $\mathcal{D}$ .

- The key generating function  $\mathcal{G}$  takes a unary string  $1^\eta$ , where  $\eta$  is the security parameter and outputs a public key, secret key pair  $(\text{pk}, \text{sk})$ . We assume for any  $(\text{pk}_i, \text{sk}_i) \leftarrow \mathcal{G}(1^\eta)$  and  $(\text{pk}_j, \text{sk}_j) \leftarrow \mathcal{G}(1^\eta)$  that  $|\text{pk}_i| = |\text{pk}_j|$  and  $|\text{sk}_i| = |\text{sk}_j|$ .
- The encryption function  $\mathcal{E}$  takes a public key  $\text{pk}$  and a message  $m$  and outputs a cipher text  $c$ .
- The decryption function  $\mathcal{D}$  takes a secret key  $\text{sk}$  and a ciphertext  $c$  and outputs a message  $m$  or  $\perp$ .

As usual, we require that for any  $(\text{pk}, \text{sk}) \leftarrow \mathcal{G}(1^\eta)$  and any message  $m$ ,  $\mathcal{D}(\text{sk}, \mathcal{E}(\text{pk}, m)) = m$ .

A (public key) bit encryption scheme has message space  $\{0, 1\}$ . For a bit encryption scheme and a message  $m$  where  $|m| > 1$ , we write  $\mathcal{E}(\text{pk}, m)$  to denote that bit-by-bit encryption of  $m$  using  $\mathcal{E}(\text{pk}, \cdot)$ , each encryption using fresh randomness. More definitions of bit-encryption in circular settings can be found [32].

The definition of CPA experiment and CPA-security follows that of [22].

**Definition 2.** Let  $\Pi = (\mathcal{G}, \mathcal{E}, \mathcal{D})$  be a public key encryption scheme. The CPA experiment for  $\Pi$  and adversary  $\mathcal{A}$  denoted by  $\text{CPA}_{\mathcal{A}, \Pi}(\eta)$  is defined as follows:

$\text{CPA}_{\mathcal{A}, \Pi}(\eta)$  :

1.  $\text{pk}, \text{sk} \leftarrow \mathcal{G}(1^\eta)$ . Give  $\eta$  and  $\text{pk}$  to  $\mathcal{A}$ .
2.  $b \leftarrow \$\{0, 1\}$ .
3.  $\mathcal{A}$  outputs two equal length challenge messages  $m_0, m_1$ .
4. Compute  $c^b \leftarrow \mathcal{E}(\text{pk}, m_b)$  and return  $c^b$  to  $\mathcal{A}$ .
5.  $\mathcal{A}$  outputs  $b'$  and the experiment results in 1 if  $b = b'$ , 0 otherwise.

We say  $\Pi$  is CPA secure if for every PPT adversary  $\mathcal{A}$ ,

$$\Pr[\text{CPA}_{\mathcal{A}, \Pi}(\eta) = 1] \leq \frac{1}{2} + \text{negl}(\eta).$$

The definition of  $n$ -circular experiment and  $n$ -circular-security follows that of [12].

**Definition 3.** Let  $\Pi = (\mathcal{G}, \mathcal{E}, \mathcal{D})$  be a public key encryption scheme. The  $n$ -circular experiment for  $\Pi$  and adversary  $\mathcal{A}$  denoted by  $\text{CIRC}_{\mathcal{A}, \Pi}(n, \eta)$  is defined as follows:

$\text{CIRC}_{\mathcal{A}, \Pi}(n, \eta)$  :

1.  $\text{pk}_0, \text{sk}_0 \leftarrow \mathcal{G}(1^\eta), \dots, \text{pk}_{n-1}, \text{sk}_{n-1} \leftarrow \mathcal{G}(1^\eta)$ . Give  $\eta$  and  $\text{pk}_0, \dots, \text{pk}_{n-1}$  to  $\mathcal{A}$ .
2.  $b \leftarrow \$\{0, 1\}$ .

3. Compute for  $i \in \{0, \dots, n-1\}$ :

$$c_i^b \leftarrow \begin{cases} \mathcal{E}(\text{pk}_i, \text{sk}_{i+1 \bmod n}) & \text{If } b = 1 \\ \mathcal{E}(\text{pk}_i, 0^{|\text{sk}_i|}) & \text{If } b = 0 \end{cases}$$

Send  $c_0^b, \dots, c_{n-1}^b$  to  $\mathcal{A}$ .

4. When  $\mathcal{A}$  outputs  $b'$ , the experiment results in 1 if  $b = b'$ , 0 otherwise.

We say  $\Pi$  is  $n$ -circular secure if for every PPT adversary  $\mathcal{A}$ ,

$$\Pr[\text{CIRC}_{\mathcal{A}, \Pi}(n, \eta) = 1] \leq \frac{1}{2} + \text{negl}(\eta).$$

An encryption scheme is  $n$ -circular insecure if it is not  $n$ -circular secure. An encryption scheme is  $(1$  to  $n)$ -circular insecure if it is  $\ell$ -circular insecure for any  $\ell \in \{1, \dots, n\}$ .

### 3 Construction of $n$ -Circular Insecure Encryption

We show how to construct a CPA secure  $n$ -circular insecure public key encryption from a CPA secure  $(n+1)$ -circular insecure public key encryption.

**Construction 1** Given a CPA secure  $(n+1)$ -circular insecure public key encryption scheme  $\Pi = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ . We obtain  $\Pi' = (\mathcal{G}', \mathcal{E}', \mathcal{D}')$  as follows:

$\Pi'$ :

–  $\mathcal{G}'(1^n)$ : Compute

$$(\text{pk}[0], \text{sk}[0]) \leftarrow \mathcal{G}(1^n), \dots, (\text{pk}[n], \text{sk}[n]) \leftarrow \mathcal{G}(1^n).$$

Compute  $\mathbf{s} \leftarrow \mathcal{E}(\text{pk}[0], \text{sk}[n])$ . For  $3 \leq i \leq n$  compute  $h[i] \leftarrow \mathcal{E}(\text{pk}[i], \text{sk}[i-1])$ . Return public key

$$\text{pk} = \text{pk}[0], \dots, \text{pk}[n], \mathbf{s}, h[n], h[n-1], \dots, h[3].$$

and secret key

$$\text{sk} = \text{sk}[0], \dots, \text{sk}[n-1].$$

We note that when  $n < 3$ , the public key has nothing after  $\mathbf{s}$ .

–  $\mathcal{E}'(\text{pk}, m)$ : Parse  $\text{pk}$  to

$$\text{pk}[0], \dots, \text{pk}[n], \mathbf{s}, h[n], \dots, h[3].$$

If  $|m| \neq |\text{sk}|$ , compute  $c \leftarrow \mathcal{E}(\text{pk}[1], m)$  and return

$$\langle 0, c \rangle.$$

Otherwise, parse  $m$  to  $m[0], \dots, m[n-1]$  where  $|m[i]| = |\text{sk}[i]|$  for  $0 \leq i \leq n-1$ . For  $0 \leq i \leq n-1$  compute  $c[0] \leftarrow \mathcal{E}(\text{pk}[i+1], m[i])$ , return

$$\langle 1, c[0], \dots, c[n-1] \rangle.$$

–  $\mathcal{D}'(\text{sk}, c)$ : Parse  $\text{sk}$  to

$$\text{sk}[0], \dots, \text{sk}[n-1].$$

If  $c = \langle 0, c' \rangle$ , return  $\mathcal{D}(\text{sk}[1], c)$ . Else parse  $c$  into  $\langle x, c[0], \dots, c[n-1] \rangle$ , compute  $\text{sk}[n] \leftarrow \mathcal{D}(\text{sk}[0], \mathbf{s})$  and return

$$\mathcal{D}(\text{sk}[1], c[0]) \parallel \dots \parallel \mathcal{D}(\text{sk}[n], c[n-1]).$$

One can observe that if all functions of  $\Pi$  are efficiently computable, so are the functions of  $\Pi'$ . Similarly, one can observe that if  $\Pi$  is correct, then so is  $\Pi'$ .

**Theorem 1.** *If there exists a CPA secure  $(n+1)$ -circular insecure public key encryption scheme  $\Pi$ , then there exists a CPA secure  $(1$  to  $n)$ -circular insecure encryption scheme  $\Pi'$ .*

The following section shows this theorem via Lemma 1 and Lemma 2.

## 4 Analysis of Construction 1

In this section, we will show that if  $\Pi$  is  $(n+1)$ -circular insecure and CPA secure, then  $\Pi'$  is  $(1 \text{ to } n)$ -circular insecure and CPA secure.

### 4.1 Circular Insecurity Example

Before we show the circular insecurity of  $\Pi'$  we will give an example by setting  $n = 2$ .

Let  $\Pi$  be a 3-circular insecure and CPA secure public key encryption scheme and suppose  $\Pi'$  is constructed from  $\Pi$  via Construction 1. We can show that  $\Pi'$  is both 1-circular insecure and 2-circular insecure.

Fix a security parameter  $\eta$ . Consider some adversary  $\mathcal{A}$  such that

$$\Pr[\text{CIRC}_{\mathcal{A},\Pi}(3, \eta) = 1] \geq \frac{1}{2} + \epsilon(\eta).$$

To see  $\Pi'$  is 1-circular insecure, let  $(\text{pk}, \text{sk}) \leftarrow \mathcal{G}'(1^\eta)$ . Define adversary  $\mathcal{A}'_1$  as follows:

$\mathcal{A}'_1$ :

1. Receive  $\eta$  and  $\text{pk} = \text{pk}[0], \text{pk}[1], \text{pk}[2], \text{s}$ . Send  $\text{pk}[0], \text{pk}[2], \text{pk}[1]$  to  $\mathcal{A}$ .
2. Receive  $c^b = \langle 1, c^b[0], c^b[1] \rangle$ . Send  $\text{s}, c^b[1], c^b[0]$  to  $\mathcal{A}$ .
3. When  $\mathcal{A}$  outputs  $b'$ , output  $b'$ .

In the event  $b = 1$ ,  $\mathcal{A}'_1$  has sent ciphertexts

$$\begin{aligned} \text{s} &\leftarrow \mathcal{E}(\text{pk}[0], \text{sk}[2]) \\ c^1[1] &\leftarrow \mathcal{E}(\text{pk}[2], \text{sk}[1]) \\ c^1[0] &\leftarrow \mathcal{E}(\text{pk}[1], \text{sk}[0]) \end{aligned}$$

to  $\mathcal{A}$ , which simulates  $\text{CIRC}_{\mathcal{A},\Pi}(3, \eta)$  when its internal coin is 1.

In the event  $b = 0$ ,  $\mathcal{A}'_1$  has sent ciphertexts

$$\begin{aligned} \text{s} &\leftarrow \mathcal{E}(\text{pk}[0], \text{sk}[2]) \\ c^0[1] &\leftarrow \mathcal{E}(\text{pk}[2], 0^{|\text{sk}[1]|}) \\ c^0[0] &\leftarrow \mathcal{E}(\text{pk}[1], 0^{|\text{sk}[0]|}) \end{aligned}$$

to  $\mathcal{A}$ , which by Lemma 3, simulates  $\text{CIRC}_{\mathcal{A},\Pi}(3, \eta)$  when its internal coin is 0 except with negligible probability. Therefore we conclude that  $\text{CIRC}_{\mathcal{A}'_1,\Pi'}(1, \eta) = \text{CIRC}_{\mathcal{A},\Pi}(3, \eta)$  except with negligible probability.

To see  $\Pi'$  is 2-circular secure. Consider  $(\text{pk}_0, \text{sk}_0) \leftarrow \mathcal{G}'(1^\eta), (\text{pk}_1, \text{sk}_1) \leftarrow \mathcal{G}'(1^\eta)$ . Define adversary  $\mathcal{A}'_2$  as follows:

$\mathcal{A}'_2$ :

1. Receive  $\eta$  and  $\text{pk}_0 = \text{pk}_0[0], \text{pk}_0[1], \text{pk}_0[2], \text{s}_0$  and  $\text{pk}_1 = \text{pk}_1[0], \text{pk}_1[1], \text{pk}_1[2], \text{s}_1$ . Send  $\text{pk}_1[0], \text{pk}_1[2], \text{pk}_0[1]$  to  $\mathcal{A}$ .
2. Receive  $c_0^b = \langle 1, c_0^b[0], c_0^b[1] \rangle$  and  $c_1^b = \langle 1, c_1^b[0], c_1^b[1] \rangle$ . Send  $\text{s}_1, c_1^b[1], c_0^b[0]$  to  $\mathcal{A}$ .
3. When  $\mathcal{A}$  outputs  $b'$ , output  $b'$ .

In the event  $b = 1$ ,  $\mathcal{A}'_2$  has sent ciphertexts

$$\begin{aligned} \text{s}_1 &\leftarrow \mathcal{E}(\text{pk}_1[0], \text{sk}_1[2]) \\ c_1^1[1] &\leftarrow \mathcal{E}(\text{pk}_1[2], \text{sk}_0[1]) \\ c_0^1[0] &\leftarrow \mathcal{E}(\text{pk}_0[1], \text{sk}_1[0]) \end{aligned}$$

to  $\mathcal{A}$ , which simulates  $\text{CIRC}_{\mathcal{A},\Pi}(3, \eta)$  when its internal coin is 1.

In the event  $b = 0$ ,  $\mathcal{A}'_2$  has sent ciphertexts

$$\begin{aligned} \text{s}_1 &\leftarrow \mathcal{E}(\text{pk}_1[0], \text{sk}_1[2]) \\ c_1^0[1] &\leftarrow \mathcal{E}(\text{pk}_1[2], 0^{|\text{sk}_0[1]|}) \\ c_0^0[0] &\leftarrow \mathcal{E}(\text{pk}_0[1], 0^{|\text{sk}_1[0]|}) \end{aligned}$$

By Lemma 3 we conclude that  $\text{CIRC}_{\mathcal{A}'_2,\Pi'}(2, \eta) = \text{CIRC}_{\mathcal{A},\Pi}(3, \eta)$  except with negligible probability.

## 4.2 Circular Insecurity

**Lemma 1.** *If  $\Pi$  is  $(n + 1)$ -circular insecure and CPA secure, then  $\Pi'$  is  $(1$  to  $n)$ -circular insecure.*

*Proof.* Let  $\Pi$  be  $(n + 1)$ -circular insecure and CPA secure. Then there exists an adversary  $\mathcal{A}$  such that

$$\Pr[\text{CIRC}_{\mathcal{A},\Pi}(n + 1, \eta) = 1] \geq \frac{1}{2} + \epsilon(\eta).$$

Consider an arbitrary  $\ell \in \{1, \dots, n\}$ . We can define an adversary  $\mathcal{A}'_\ell$  as follows.

$\mathcal{A}'_\ell$ :

1. Receive  $\eta$  and  $\text{pk}_0, \dots, \text{pk}_{\ell-1}$  where for  $0 \leq x \leq \ell - 1$

$$\text{pk}_x = \text{pk}_x[0], \dots, \text{pk}_x[n], \text{s}_x, h_x[n], \dots, h_x[3].$$

Send the following keys to  $\mathcal{A}$  in the order described:

- (a)  $\text{pk}_{\ell-1}[0]$
  - (b) for  $\ell + 1 \leq i \leq n$  in descending order,  $\text{pk}_{\ell-1}[i]$
  - (c) for  $0 \leq j \leq \ell - 1$  in ascending order,  $\text{pk}_{(\ell-1+j) \bmod \ell}[\ell - j]$ .
2. Receive  $c_0^b, \dots, c_{\ell-1}^b$  where for  $0 \leq x \leq \ell - 1$

$$c_x^b = c_x^b[0], \dots, c_x^b[n - 1].$$

Send the following ciphertexts to  $\mathcal{A}$  in the order described:

- (a)  $\text{s}_{\ell-1}$
  - (b) for  $\ell + 1 \leq i \leq n$  in descending order,  $h_{\ell-1}[i]$
  - (c) for  $0 \leq j \leq \ell - 1$  in ascending order,  $c_{(\ell-1+j) \bmod \ell}^b[\ell - 1 - j]$ .
3. When  $\mathcal{A}$  outputs  $b'$ , output  $b'$ .

When  $b = 1$ , we observe that

$$\text{s}_{\ell-1} \leftarrow \mathcal{E}(\text{pk}_{\ell-1}[0], \text{sk}_{\ell-1}[n])$$

For  $\ell + 1 \leq i \leq n$

$$h_{\ell-1}[i] \leftarrow \mathcal{E}(\text{pk}_{\ell-1}[i], \text{sk}_{\ell-1}[i - 1])$$

For  $0 \leq j \leq \ell - 1$

$$c_{(\ell-1+j) \bmod \ell}^1[\ell - 1 - j] \leftarrow \mathcal{E}(\text{pk}_{(\ell-1+j) \bmod \ell}[\ell - j], \text{sk}_{\ell+j \bmod \ell}[\ell - 1 - j])$$

which is a  $n + 1$  encryption cycle of  $\Pi$ , which means  $\mathcal{A}'_\ell$  simulates  $\text{CIRC}_{\mathcal{A},\Pi}(n + 1, \eta)$  when the internal coin of  $\text{CIRC}_{\mathcal{A},\Pi}(n + 1, \eta)$  is 1.

When  $b = 0$ , we observe that

$$\text{s}_{\ell-1} \leftarrow \mathcal{E}(\text{pk}_{\ell-1}[0], \text{sk}_{\ell-1}[n])$$

For  $\ell + 1 \leq i \leq n$

$$h_{\ell-1}[i] \leftarrow \mathcal{E}(\text{pk}_{\ell-1}[i], \text{sk}_{\ell-1}[i - 1])$$

For  $0 \leq j \leq \ell - 1$

$$c_{(\ell-1+j) \bmod \ell}^0[\ell - 1 - j] \leftarrow \mathcal{E}(\text{pk}_{(\ell-1+j) \bmod \ell}[\ell - j], 0^{\text{sko}[0]})$$

and by Lemma 3, this simulates  $\text{CIRC}_{\mathcal{A},\Pi}(n + 1, \eta)$  when the internal coin of  $\text{CIRC}_{\mathcal{A},\Pi}(n + 1, \eta)$  is 0 except with negligible probability.

This implies that if  $\epsilon(\eta)$  is not negligible, then  $\Pi'$  is not  $\ell$ -circular secure.

Therefore we conclude if  $\Pi$  is  $(n + 1)$ -circular insecure and CPA secure, then  $\Pi'$  is  $(1$  to  $n)$ -circular secure.  $\square$

### 4.3 CPA security

Let  $\Pi$  be a CPA secure public key encryption scheme. We show  $\Pi'$  obtained from  $\Pi$  via construction 1 is a CPA secure public key encryption scheme via a sequence of games [33].

Without loss of generality, we fix an efficient adversary  $\mathcal{A}'$  to play in  $\text{CPA}_{\mathcal{A}',\Pi'}(\eta)$ .

**Game 0.** This is just the game  $\text{CPA}_{\mathcal{A}',\Pi'}(\eta)$  with each step stated explicitly.

1.  $(\text{pk}[0], \text{sk}[0]) \leftarrow \mathcal{G}(1^\eta), \dots, (\text{pk}[n], \text{sk}[n]) \leftarrow \mathcal{G}(1^\eta)$ .  
Compute  $\mathbf{s} \leftarrow \mathcal{E}(\text{pk}[0], \text{sk}[n])$ , for  $3 \leq i \leq n$  compute  $h[i] \leftarrow \mathcal{E}(\text{pk}[i], \text{sk}[i-1])$ .  
Give  $\eta$  and  $\text{pk}[0], \dots, \text{pk}[n], \mathbf{s}, h[n], \dots, h[n-1]$  to  $\mathcal{A}'$ .
2.  $b \leftarrow \mathcal{S}\{0, 1\}$
3.  $(m_0, m_1) \leftarrow \mathcal{A}'$ .
4. If  $m_b \neq |\text{sk}[0], \dots, \text{sk}[n-1]|$ , then compute  $c^b \leftarrow \langle 0, \mathcal{E}(\text{pk}[1], m_b) \rangle$ .  
Otherwise,  
(a) Parse  $m_b$  into  $m_b[0], \dots, m_b[n-1]$ .  
(b) For  $0 \leq i \leq n-1$ , compute  $c^b[i] \leftarrow \mathcal{E}(\text{pk}[i+1], m_b[i])$ .  
Return  $c_b = \langle 1, c^b[0], \dots, c^b[n-1] \rangle$  to  $\mathcal{A}'$ .
5.  $\mathcal{A}'$  outputs  $b'$ . The experiment outputs 1 if  $b = b'$ , 0 otherwise.

Let  $S_0$  denote the event that Game 0. results in 1.

**Game 1.** Here, we modify how the public key is generated in step 1 of Game 0. In Game 1.  $\text{sk}[n], \dots, \text{sk}[2]$  is not encrypted.

1.  $(\text{pk}[0], \text{sk}[0]) \leftarrow \mathcal{G}(1^\eta), \dots, (\text{pk}[n], \text{sk}[n]) \leftarrow \mathcal{G}(1^\eta)$ .  
Compute  $\mathbf{s} \leftarrow \mathcal{E}(\text{pk}[0], 0^{|\text{sk}[n]|})$ , for  $3 \leq i \leq n$  compute  $h[i] \leftarrow \mathcal{E}(\text{pk}[i], 0^{|\text{sk}[i-1]|})$ .  
Give  $\eta$  and  $\text{pk}[0], \dots, \text{pk}[n], \mathbf{s}, h[n], \dots, h[n-1]$  to  $\mathcal{A}'$ .

We let  $S_1$  denote the event that the result of Game 1 is 1.

*Claim.*

$$|\Pr[S_0] - \Pr[S_1]| \leq \text{negl}(\eta).$$

*Proof.* We show this by applying Lemma 3. We define an adversary  $\mathcal{A}$  that plays  $\text{ZERO}_{\mathcal{A},\Pi}(n, 2, \eta)$  as follows.

$\mathcal{A}$ :

1. Receive  $\eta, \text{pk}_0, \dots, \text{pk}_{n-1}$  and  $c_0^b, \dots, c_{n-1}^b$ .
2. Send the following to  $\mathcal{A}'$  in the order described.  
(a) for  $0 \leq i \leq n-1$  in descending order,  $\text{pk}_{i+3 \bmod n}$   
(b) for  $i \in \{2, \dots, n-1\}$  in descending order,  $c_i^b$ .
3. Flip a coin  $d$ .
4. When  $\mathcal{A}'$  queries two equal length challenge messages,  $m_0, m_1$ , if  $|m_d| \neq n|\text{sk}_0|$ , compute  $c^d \leftarrow \mathcal{E}(\text{pk}[1], m_d)$  and send  $\langle 0, c^d \rangle$  to  $\mathcal{A}'$ . Else parse  $m_d$  to  $m_d[0], \dots, m_d[n-1]$ , for  $0 \leq i \leq n-1$  compute  $c^d[i] \leftarrow \mathcal{E}(\text{pk}_{i+3 \bmod n}, m_d[i])$ . Send  $\langle 1, c^d[0], \dots, c^d[n-1] \rangle$  to  $\mathcal{A}'$ .
5. When  $\mathcal{A}'$  outputs  $d'$ ,  $\mathcal{A}$  outputs 1 if  $d = d'$ , output 0 otherwise.

Since  $\mathcal{A}$  simulates Game 0. when  $b = 1$  and Game 1. when  $b = 0$ , this means when  $b = 1$   $\mathcal{A}$  wins if  $\mathcal{A}'$  loses, and when  $b = 0$ ,  $\mathcal{A}$  wins if  $\mathcal{A}'$  loses. Therefore, we have the following.

$$\begin{aligned} \Pr[\text{ZERO}_{\mathcal{A},\Pi}(n, 2, \eta) = 1] &= \frac{1}{2} \Pr[\neg S_0] + \frac{1}{2} \Pr[S_1] \\ &= \frac{1}{2}(1 + \Pr[S_1] - \Pr[S_2]) \end{aligned}$$

which is either  $\geq \frac{1+\epsilon(\eta)}{2}$  or  $\leq \frac{1-\epsilon(\eta)}{2}$ . This concludes the proof.  $\square$

**Game 2.j** We let Game 2.0 be Game 1. In Game 2.j where  $j > 0$ , we modify how the query is answered in step 4 of Game 2.(j-1).

4. If  $m_b \neq \langle \text{sk}[0], \dots, \text{sk}[n-1] \rangle$ , then compute  $c^b \leftarrow \langle 0, \mathcal{E}(\text{pk}[1], m_b) \rangle$ .  
Otherwise,
  - (a) Parse  $m_b$  into  $m_b[0], \dots, m_b[n-1]$ .
  - (b) For  $0 \leq i \leq n-j-1$ , compute  $c^b[i] \leftarrow \mathcal{E}(\text{pk}[i+1], m_b[i])$ .
  - (c) For  $n-j \leq i \leq n-1$ , compute  $c^b[i] \leftarrow \mathcal{E}(\text{pk}[i+1], 0^{|\text{sk}[0]|})$ .
Return  $c_b = \langle 1, c^b[0], \dots, c^b[n-1] \rangle$  to  $\mathcal{A}'$ .

We let  $S_{2,j}$  denote the event that Game 2. $j$ . results in 1.

*Claim.*

$$|\Pr[S_{2,j}] - \Pr[S_{2.(j+1)}]| \leq \text{negl}(\eta).$$

*Proof.* We defined an adversary  $\mathcal{A}$  to play  $\text{CPA}_{\mathcal{A},\Pi}(\eta)$  as follows.

$\mathcal{A}$ :

1. Receive  $\eta$  and  $\text{pk}$ . Label this  $\text{pk}$  as  $\text{pk}_{n-j}$ .
2. For  $i \in \{0, \dots, n\} \setminus \{n-j\}$ , compute  $\text{pk}_i, \text{sk}_i \leftarrow \mathcal{G}(1^\eta)$ . Compute  $\mathbf{s} \leftarrow \mathcal{E}(\text{pk}_0, 0^{|\text{sk}_0|})$ . For  $3 \leq i \leq n$ , compute  $h[i] \leftarrow \mathcal{E}(\text{pk}_i, 0^{|\text{sk}_i|})$ . Send

$$\text{pk}_0, \dots, \text{pk}_n, \mathbf{s}, h[n], \dots, h[3]$$

to  $\mathcal{A}'$ .

3. Flip a coin  $d$ .
4. When receive two equal length challenge messages  $m_0, m_1$  from  $\mathcal{A}'$ , if  $|m_d| \neq n \cdot |\text{sk}_0|$ , compute  $c^d \leftarrow \mathcal{E}(\text{pk}[1], c^d)$  and send  $\langle 0, c^d \rangle$  to  $\mathcal{A}'$ . Else create and query challenge messages  $m'_0 = m_d[n-(j+1)], m'_1 = 0^{|\text{sk}_0|}$  to receive  $c^b[n-(j+1)] \leftarrow \mathcal{E}(\text{pk}_{n-j}, m'_b)$ . For  $i \in \{0, n-1\} \setminus \{n-(j+1)\}$  compute

$$c^d[i] = \begin{cases} \mathcal{E}(\text{pk}[i+1], m[i]) & \text{if } i \leq n-(j+1) \\ \mathcal{E}(\text{pk}[i+1], 0^{|\text{sk}[i]|}) & \text{otherwise.} \end{cases}$$

Send  $\langle 1, c^d[0], c^d[1], \dots, c^d[n-1] \rangle$  to  $\mathcal{A}'$ .

5. When  $\mathcal{A}'$  outputs  $d'$ ,  $\mathcal{A}$  outputs 1 if  $d = d'$ , output 0 otherwise.

When  $b = 0$ ,  $\mathcal{A}$  simulates Game 2. $j$  when the internal coin is  $d$ , and when  $b = 1$ ,  $\mathcal{A}$  simulates Game 2. $(j+1)$  when the internal coin is  $d$ . Therefore

$$\begin{aligned} \text{CPA}_{\mathcal{A},\Pi}(\eta) &= \frac{1}{2} \Pr[\neg S_{2,j}] + \frac{1}{2} \Pr[S_{2.(j+1)}] \\ &= \frac{1}{2} (1 + \Pr[S_{2.(j+1)}] - \Pr[S_{2,j}]). \end{aligned}$$

Therefore, if  $\Pi$  is CPA secure, then  $|\Pr[S_{2,j}] - \Pr[S_{2.(j+1)}]|$  is negligible.  $\square$

**Lemma 2.** *If  $\Pi$  is CPA secure, then  $\Pi'$  is CPA secure.*

*Proof.* This is shown via the sequence of games above. Let  $\Pi$  be CPA secure, then for any adversary  $\mathcal{A}'$ , it would have only negligible advantage in Game 2. $(n)$ . The probability of the event that  $\mathcal{A}'$  wins in Game 2. $(n)$  differs from the probability of the event that  $\mathcal{A}'$  wins in Game 0 by a negligible amount. Therefore, we conclude that  $\Pi'$  is CPA secure.  $\square$

## 5 Bit Encryption Construction

**Construction 2** *Given a CPA secure  $(n+1)$ -circular insecure public key bit encryption scheme  $\Pi = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ . We obtain  $\Pi^b = (\mathcal{G}^b, \mathcal{E}^b, \mathcal{D}^b)$  as follows.*

$\Pi^b$ :

–  $\mathcal{G}^b$ : Compute

$$(\mathbf{pk}[0], \mathbf{sk}[0]) \leftarrow \mathcal{G}(1^n), \dots, (\mathbf{pk}[n], \mathbf{sk}[n]) \leftarrow \mathcal{G}(1^n).$$

Compute  $\mathbf{s} \leftarrow \mathcal{E}(\mathbf{pk}[0], \mathbf{sk}[n])$  (bit by bit). For  $3 \leq i \leq n$  compute  $h[i] \leftarrow \mathcal{E}(\mathbf{pk}[i], \mathbf{sk}[i-1])$  (bit by bit).  
Return public key

$$\mathbf{pk} = \mathbf{pk}[0], \dots, \mathbf{pk}[n], \mathbf{s}, h[n], h[n-1], \dots, h[3].$$

and secret key

$$\mathbf{sk} = \mathbf{sk}[0], \dots, \mathbf{sk}[n-1].$$

–  $\mathcal{E}^b(\mathbf{pk}, m)$ : Note that  $m \in \{0, 1\}$ . Parse  $\mathbf{pk}$  to

$$\mathbf{pk}[0], \dots, \mathbf{pk}[n], \mathbf{s}, h[n], \dots, h[3].$$

For  $0 \leq i \leq n-1$ . For  $0 \leq i \leq n-1$  compute  $c[0] \leftarrow \mathcal{E}(\mathbf{pk}[i+1], m)$ , return

$$c[0], \dots, c[n-1]$$

–  $\mathcal{D}^b(\mathbf{sk}, c)$ : Parse  $c$  into  $\langle x, c[0], \dots, c[n-1] \rangle$ , return

$$\mathcal{D}(\mathbf{sk}[1], c[0]).$$

The proof of CPA security for this construction is similar to the previous proof. In the Games, instead of parsing  $m$  to  $n$  strings each of length  $|\mathbf{sk}[0]|$ , we will instead duplicate  $n$  copies of  $m$  as  $m$  is just a bit.

Now, to show this scheme is  $(1$  to  $n)$ -circular insecure. We first remind the readers that for bit encryption, when we say  $\mathcal{E}(k, m)$  for  $|m| > 1$ , we mean encrypting each bit of  $m$  in order, each time with fresh randomness. Consider an arbitrary  $\ell \in \{1, \dots, n\}$ . Given  $(\mathbf{pk}_0, \mathbf{sk}_0) \leftarrow \mathcal{G}^b(1^n), \dots, (\mathbf{pk}_\ell, \mathbf{sk}_\ell) \leftarrow \mathcal{G}^b(1^n)$ , for  $0 \leq i < \ell$  let

$$c_i^b \leftarrow \begin{cases} \mathcal{E}^b(\mathbf{pk}_i, \mathbf{sk}_{i+1 \bmod n}) & \text{if } b = 1 \\ \mathcal{E}^b(\mathbf{pk}_i, 0^{|\mathbf{sk}_0|}) & \text{otherwise.} \end{cases}$$

To keep the notation tidy, let  $p = |\mathbf{sk}_0[0]|$ .

An adversary  $\mathcal{A}_\ell^b$  receiving  $c_0^b, \dots, c_{\ell-1}^b$  can do the following. First for  $0 \leq i < \ell$ , parse  $c_i^b$  into

$$c_i^b[0], \dots, c_i^b[n-1]$$

where for  $0 \leq j \leq n-1$ ,  $c_i^b[j]$  is sampled from  $\mathcal{E}^b(\mathbf{pk}_i, m_b)$  for  $m_1 = \mathbf{sk}_{i+1 \bmod \ell}[j]$ , where  $m_0 = 0^p$ . For  $0 \leq j \leq n-1$ ,  $c_i^b[j]$  can be parsed into

$$c_i^b[j][0], c_i^b[j][1], \dots, c_i^b[j][p-1]$$

where for  $0 \leq x \leq p$ ,  $c_i^b[j][x]$  is samples from  $\mathcal{E}^b(\mathbf{pk}_i, m'_b)$  where  $m'_1 = \mathbf{sk}_{i+1 \bmod \ell}[j][x]$  (the  $x$ th bit of  $\mathbf{sk}_{i+1 \bmod n}[j]$ ) and  $m'_0 = 0$ . We remind the reader that  $p = |\mathbf{sk}_0[0]|$ .

For  $0 \leq x \leq p-1$ ,  $c_i^b[j][x]$  can be parsed to

$$c_i^b[j][x][0], \dots, c_i^b[j][x][n-1]$$

where for  $0 \leq y \leq n-1$ ,  $c_i^b[j][x][y]$  is samples from  $\mathcal{E}(\mathbf{pk}[i][y+1], m''_b)$  where  $m''_1 = \mathbf{sk}_{i+1 \bmod \ell}[j][x]$  and  $m''_0 = 0$ .

Now that the ciphertext has been parsed, the adversary can extract the following in the order described:

1.  $\mathbf{s}_{\ell-1}$
2. for  $\ell+1 \leq i \leq n$  in descending order  $h_{\ell-1}[i]$
3. for  $0 \leq j \leq \ell-1$  in ascending order:
  - (a) for  $0 \leq x \leq p-1$  in ascending order:  $c_{(\ell-1+j) \bmod \ell}^b[\ell-1-j][x][\ell-1-j]$ .



Since

$$\begin{aligned}
& c_{(\ell-1+j) \bmod \ell}^b[\ell-1-j][0][\ell-1-j], \dots, c_{(\ell-1+j) \bmod \ell}^b[\ell-1-j][p-1][\ell-1-j] \\
& \leftarrow \mathcal{E}(\mathbf{pk}_{(\ell-1+j) \bmod i}[\ell-j], \mathbf{sk}_{(\ell+j) \bmod \ell}[\ell-1-j][0]), \\
& \quad \vdots \\
& \mathcal{E}(\mathbf{pk}_{(\ell-1+j) \bmod i}[\ell-j], \mathbf{sk}_{(\ell+j) \bmod \ell}[\ell-1-j][p-1]) \\
& = \mathcal{E}(\mathbf{pk}_{(\ell-1+j) \bmod i}[\ell-j], \mathbf{sk}_{(\ell+j) \bmod \ell}[\ell-1-j])
\end{aligned}$$

the ciphertexts that the adversary has extracted when  $b = 1$  are sampled from:

1.  $s_{\ell_1} \leftarrow \mathcal{E}(\mathbf{pk}_{\ell}[0], \mathbf{sk}_{\ell}[n])$
2. for  $\ell+1 \leq i < n$  in descending order,  $h_{\ell-1}[i] \leftarrow \mathcal{E}(\mathbf{pk}_{\ell-1}[i], \mathbf{sk}_{\ell-1}[i-1])$
3. for  $0 \leq j \leq \ell-1$  in ascending order,

$$c_{(\ell-1+j) \bmod \ell}^1[\ell-1-j][0, \dots, p-1][\ell-1-j] \leftarrow \mathcal{E}(\mathbf{pk}_{(\ell-1+j) \bmod i}[\ell-j], \mathbf{sk}_{(\ell+1) \bmod \ell}[\ell-1-j]).$$

which is a  $n+1$ -cycle with the following keys in  $\Pi$ ,

1.  $\mathbf{pk}_{\ell-1}[0], \mathbf{sk}_{\ell-1}[0]$
2. for  $\ell+1 \leq i < n$ ,  $\mathbf{pk}_{\ell-1}[i], \mathbf{sk}_{\ell-1}[i]$
3. for  $0 \leq j \leq \ell-1$ ,  $\mathbf{pk}_{(\ell-1+j) \bmod \ell}[\ell-j], \mathbf{sk}_{(\ell-1+j) \bmod \ell}[\ell-j]$ .

And in the event where  $b = 0$ , by Lemma 3, is indistinguishable from encryptions of zeros.

## 6 Symmetric Encryption Scheme

This section discusses how to modify the construction to work in the symmetric key setting. There are two changes to be made. The first change in the construction required is to compute the  $\mathbf{s}$  and  $h[n], \dots, h[3]$  in the encryption function and output the result as part of the ciphertext. i.e. each time the encryption function computes  $\mathbf{s} \leftarrow \mathcal{E}(\mathbf{sk}[0], \mathbf{sk}[n]), h[n] \leftarrow \mathcal{E}(\mathbf{sk}[n], \mathbf{sk}[n-1]), \dots, h[3] \leftarrow \mathcal{E}(\mathbf{sk}[3], \mathbf{sk}[2])$  and append this at the end of the ciphertext. The second change is that in the event where the message space equals the key space, the symmetric encryption function needs to create an additional ciphertext, say with  $\mathbf{sk}[1]$ , as now the length of the (secret) key is longer.

**Acknowledgement.** I thank Bruce Kapron for his helpful comments.

## References

1. Abadi, M., Rogaway, P.: Reconciling two views of cryptography. *Theoretical Computer Science: Exploring New Frontiers of Theoretical Informatics* p. 3–22 (2000). [https://doi.org/10.1007/3-540-44929-9\\_1](https://doi.org/10.1007/3-540-44929-9_1)
2. Acar, T., Belenkiy, M., Bellare, M., Cash, D.: Cryptographic agility and its relation to circular encryption. In: *Advances in Cryptology—EUROCRYPT 2010: 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30–June 3, 2010. Proceedings 29.* pp. 403–422. Springer (2010). [https://doi.org/doi.org/10.1007/978-3-642-13190-5\\_21](https://doi.org/doi.org/10.1007/978-3-642-13190-5_21)
3. Adao, P., Bana, G., Herzog, J., Scedrov, A.: Soundness and completeness of formal encryption: The cases of key cycles and partial information leakage. *Journal of Computer Security* **17**(5), 737–797 (2009). <https://doi.org/10.3233/JCS-2009-0358>
4. Alamedi, N., Peikert, C.: Three’s compromised too: Circular insecurity for any cycle length from (ring-) lwe. In: *Annual International Cryptology Conference.* pp. 659–680. Springer (2016). [https://doi.org/10.1007/978-3-662-53008-5\\_23](https://doi.org/10.1007/978-3-662-53008-5_23)
5. Applebaum, B.: Key-dependent message security: Generic amplification and completeness. *Journal of cryptology* **27**(3), 429–451 (2014). <https://doi.org/10.1007/s00145-013-9149-6>

6. Barak, B., Haitner, I., Hofheinz, D., Ishai, Y.: Bounded key-dependent message security. In: *Advances in Cryptology—EUROCRYPT 2010: 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, French Riviera, May 30–June 3, 2010. *Proceedings 29*. pp. 423–444. Springer (2010). [https://doi.org/10.1007/978-3-642-13190-5\\_22](https://doi.org/10.1007/978-3-642-13190-5_22)
7. Bishop, A., Hohenberger, S., Waters, B.: New circular security counterexamples from decision linear and learning with errors. In: *International Conference on the Theory and Application of Cryptology and Information Security*. pp. 776–800. Springer (2015). [https://doi.org/10.1007/978-3-662-48800-3\\_32](https://doi.org/10.1007/978-3-662-48800-3_32)
8. Black, J., Rogaway, P., Shrimpton, T.: Encryption-scheme security in the presence of key-dependent messages. In: *Selected Areas in Cryptography: 9th Annual International Workshop, SAC 2002 St. John’s, Newfoundland, Canada, August 15–16, 2002 Revised Papers 9*. pp. 62–75. Springer (2003). [https://doi.org/10.1007/3-540-36492-7\\_6](https://doi.org/10.1007/3-540-36492-7_6)
9. Boneh, D., Halevi, S., Hamburg, M., Ostrovsky, R.: Circular-secure encryption from decision diffie-hellman. In: *Advances in Cryptology—CRYPTO 2008: 28th Annual International Cryptology Conference*, Santa Barbara, CA, USA, August 17–21, 2008. *Proceedings 28*. pp. 108–125. Springer (2008). [https://doi.org/10.1007/978-3-540-85174-5\\_7](https://doi.org/10.1007/978-3-540-85174-5_7)
10. Brakerski, Z., Goldwasser, S., Kalai, Y.T.: Black-box circular-secure encryption beyond affine functions. In: *Theory of Cryptography: 8th Theory of Cryptography Conference, TCC 2011, Providence, RI, USA, March 28–30, 2011*. *Proceedings 8*. pp. 201–218. Springer (2011). [https://doi.org/10.1007/978-3-642-19571-6\\_13](https://doi.org/10.1007/978-3-642-19571-6_13)
11. Brakerski, Z., Vaikuntanathan, V.: Efficient fully homomorphic encryption from (standard) lwe. *SIAM Journal on computing* **43**(2), 831–871 (2014). <https://doi.org/10.1109/F0CS.2011.12>
12. Cash, D., Green, M., Hohenberger, S.: New definitions and separations for circular security. In: *International Workshop on Public Key Cryptography*. pp. 540–557. Springer (2012). [https://doi.org/10.1007/978-3-642-30057-8\\_32](https://doi.org/10.1007/978-3-642-30057-8_32)
13. Cortier, V., Zălinescu, E.: Deciding key cycles for security protocols. In: *Logic for Programming, Artificial Intelligence, and Reasoning: 13th International Conference, LPAR 2006, Phnom Penh, Cambodia, November 13–17, 2006*. *Proceedings 13*. pp. 317–331. Springer (2006). [https://doi.org/10.1007/11916277\\_22](https://doi.org/10.1007/11916277_22)
14. Dolev, D., Yao, A.: On the security of public key protocols. *IEEE Transactions on information theory* **29**(2), 198–208 (1983). <https://doi.org/10.1109/TIT.1983.1056650>
15. Gay, R., Pass, R.: Indistinguishability obfuscation from circular security. In: *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*. pp. 736–749 (2021). <https://doi.org/10.1145/3406325>
16. Gentry, C., Sahai, A., Waters, B.: Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In: *Advances in Cryptology—CRYPTO 2013: 33rd Annual Cryptology Conference*, Santa Barbara, CA, USA, August 18–22, 2013. *Proceedings, Part I*. pp. 75–92. Springer (2013). [https://doi.org/10.1007/978-3-642-40041-4\\_5](https://doi.org/10.1007/978-3-642-40041-4_5)
17. Goldwasser, S., Micali, S.: Probabilistic encryption. *Journal of Computer and System Sciences* **28**(2), 270–299 (1984). [https://doi.org/10.1016/0022-0000\(84\)90070-9](https://doi.org/10.1016/0022-0000(84)90070-9), <https://www.sciencedirect.com/science/article/pii/0022000084900709>
18. Goyal, R., Koppula, V., Waters, B.: Separating semantic and circular security for symmetric-key bit encryption from the learning with errors assumption. In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. pp. 528–557. Springer (2017). [https://doi.org/10.1007/978-3-319-56614-6\\_18](https://doi.org/10.1007/978-3-319-56614-6_18)
19. Green, M., Hohenberger, S.: Cpa and cca-secure encryption systems that are not 2-circular secure (2010). [https://doi.org/10.1007/978-3-642-30057-8\\_32](https://doi.org/10.1007/978-3-642-30057-8_32)
20. Hajiabadi, M., Kapron, B.M.: Computational soundness of coinductive symbolic security under active attacks. In: *Theory of Cryptography: 10th Theory of Cryptography Conference, TCC 2013, Tokyo, Japan, March 3–6, 2013*. *Proceedings*. pp. 539–558. Springer (2013). [https://doi.org/10.1007/978-3-642-36594-2\\_30](https://doi.org/10.1007/978-3-642-36594-2_30)
21. Hajiabadi, M., Kapron, B.M.: Toward fine-grained blackbox separations between semantic and circular-security notions. In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. pp. 561–591. Springer (2017). [https://doi.org/10.1007/978-3-319-56614-6\\_19](https://doi.org/10.1007/978-3-319-56614-6_19)
22. Katz, J., Lindell, Y.: *Introduction to modern cryptography: principles and protocols*. Chapman and hall/CRC (2007)
23. Kitagawa, F., Matsuda, T.: Circular security is complete for kdm security. In: *Advances in Cryptology—ASIACRYPT 2020: 26th International Conference on the Theory and Application of Cryptology and Information Security*, Daejeon, South Korea, December 7–11, 2020, *Proceedings, Part I 26*. pp. 253–285. Springer (2020). [https://doi.org/10.1007/978-3-030-64837-4\\_9](https://doi.org/10.1007/978-3-030-64837-4_9)
24. Koppula, V., Ramchen, K., Waters, B.: Separations in circular security for arbitrary length key cycles. In: *Theory of Cryptography: 12th Theory of Cryptography Conference, TCC 2015, Warsaw, Poland, March 23–25, 2015*, *Proceedings, Part II 12*. pp. 378–400. Springer (2015). [https://doi.org/10.1007/978-3-662-46497-7\\_15](https://doi.org/10.1007/978-3-662-46497-7_15)
25. Laud, P.: Encryption cycles and two views of cryptography. In: *Proceedings of the 7th Nordic Workshop on Secure IT Systems (NORDSEC)*. vol. 31, pp. 85–100. Citeseer (2002)

26. Marcedone, A., Orlandi, C.: Obfuscation  $\rightarrow$  (ind-cpa security  $\not\rightarrow$  circular security). In: International Conference on Security and Cryptography for Networks. pp. 77–90. Springer (2014). [https://doi.org/10.1007/978-3-319-10879-7\\_5](https://doi.org/10.1007/978-3-319-10879-7_5)
27. Micciancio, D.: Computational soundness, co-induction, and encryption cycles. In: Advances in Cryptology–EUROCRYPT 2010: 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30–June 3, 2010. Proceedings 29. pp. 362–380. Springer (2010). [https://doi.org/10.1007/978-3-642-13190-5\\_19](https://doi.org/10.1007/978-3-642-13190-5_19)
28. Micciancio, D.: Symbolic encryption with pseudorandom keys. In: Advances in Cryptology–EUROCRYPT 2019: 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19–23, 2019, Proceedings, Part III 38. pp. 64–93. Springer (2019). [https://doi.org/10.1007/978-3-030-17659-4\\_3](https://doi.org/10.1007/978-3-030-17659-4_3)
29. Micciancio, D., Panjwani, S.: Adaptive security of symbolic encryption. In: Theory of Cryptography Conference. pp. 169–187. Springer (2005). [https://doi.org/10.1007/978-3-540-30576-7\\_10](https://doi.org/10.1007/978-3-540-30576-7_10)
30. Micciancio, D., Warinschi, B.: Completeness theorems for the abadi–rogaway language of encrypted expressions. *Journal of Computer Security* **12**(1), 99–129 (2004). <https://doi.org/10.3233/jcs-2004-12105>
31. Microsoft: (2024), <https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/faq#key-management>
32. Rothblum, R.D.: On the circular security of bit-encryption. In: Theory of Cryptography: 10th Theory of Cryptography Conference, TCC 2013, Tokyo, Japan, March 3–6, 2013. Proceedings. pp. 579–598. Springer (2013). [https://doi.org/10.1007/978-3-642-36594-2\\_32](https://doi.org/10.1007/978-3-642-36594-2_32)
33. Shoup, V.: Sequences of games: a tool for taming complexity in security proofs, 2004. URL: <http://eprint.iacr.org/2004/332> (2006)
34. Waters, B., Wichs, D.: Universal amplification of kdm security: From 1-key circular to multi-key kdm. In: Annual International Cryptology Conference. pp. 674–693. Springer (2023). [https://doi.org/10.1007/978-3-031-38545-2\\_22](https://doi.org/10.1007/978-3-031-38545-2_22)

## A Zero Encryption Equivalence Lemma

Although CPA security does not imply circular security, it provides indistinguishability on ciphertexts that are “almost” an encryption cycle. We formally describe what we mean by “almost” in the following experiment.

$\text{ZERO}_{\mathcal{A}, \Pi}(n, t, \eta)$ :

1.  $(\text{pk}_0, \text{sk}_0) \leftarrow \mathcal{G}(1^\eta), \dots, (\text{pk}_{n-1}, \text{sk}_{n-1}) \leftarrow \mathcal{G}(1^\eta)$ . Send  $\eta$  and  $\text{pk}_0, \dots, \text{pk}_{n-1}$  to  $\mathcal{A}$ .
2. A random coin  $b$  is flipped.
3. For  $i \in \{0, \dots, n-1\}$  compute

$$c_i^b \leftarrow \begin{cases} \mathcal{E}(\text{pk}_i, \text{sk}_{i+1 \bmod n}) & \text{if } b = 1 \text{ and } i \geq t, \\ \mathcal{E}(\text{pk}_i, 0^{|\text{sk}_1|}) & \text{otherwise.} \end{cases}$$

Send  $c_0^b, \dots, c_{n-1}^b$  to  $\mathcal{A}$ .

4. When  $\mathcal{A}$  outputs  $b'$ , the experiment result in 1 if  $b = b'$ , 0 otherwise.

**Lemma 3.** *If a public key encryption scheme  $\Pi = (\mathcal{G}, \mathcal{E}, \mathcal{D})$  is CPA secure. Then for any PPT adversary  $\mathcal{A}$ , any  $n \geq 1$ , and any  $t \geq 1$ ,*

$$\Pr[\text{ZERO}_{\mathcal{A}, \Pi}(n, t, \eta) = 1] \leq \frac{1}{2} + \text{negl}(\eta)$$

for all but finitely many  $\eta$ .

Applying the soundness result from [27] is an easy method to show this. However, we provide the following proof to keep this paper self-contained without elaborating on symbolic encryption.

*Proof.* Assume that  $\Pi$  is CPA secure. We will show that for any PPT adversary  $\mathcal{A}$ ,

$$|\Pr[\text{ZERO}_{\mathcal{A}, \Pi}(n, t, \eta) = 1] - \Pr[\text{ZERO}_{\mathcal{A}, \Pi}(n, t+1, \eta) = 1]| \leq \text{negl}(\eta)$$

for any  $n, t \geq 1$ . Then the statement follows since for any  $t' \geq n$  it must be the case that

$$\Pr[\text{ZERO}_{\mathcal{A}, \Pi}(n, t', \eta) = 1] = \frac{1}{2}.$$

Consider an arbitrary adversary  $\mathcal{A}$  such that

$$|\Pr[\text{ZERO}_{\mathcal{A}, \Pi}(n, t, \eta) = 1] - \Pr[\text{ZERO}_{\mathcal{A}, \Pi}(n, t+1, \eta) = 1]| > \frac{1}{2} + \epsilon(\eta).$$

Now consider an adversary  $\mathcal{A}'$  to play in  $\text{CPA}_{\mathcal{A}', \Pi}(\eta)$  defined as follows.

$\mathcal{A}'$ :

1. Receive  $\eta$  and  $\text{pk}$ . Label this  $\text{pk}$  as  $\text{pk}_t$ .
2. For  $i \in \{0, \dots, n-1\} \setminus \{t\}$  compute  $(\text{pk}_i, \text{sk}_i) \leftarrow \mathcal{G}(1^\eta)$ . Give  $\text{pk}_0, \dots, \text{pk}_{n-1}$  to  $\mathcal{A}$ .
3. Query challenge messages  $m_0 = 0^{|\text{sk}|}$  and  $m_1 = \text{sk}_{t+1}$  to receive  $c_t^b \leftarrow \mathcal{E}(\text{pk}_t, m_b)$ .
4. For  $i \in \{0, \dots, n-1\} \setminus \{t\}$  compute

$$c_i \leftarrow \begin{cases} \mathcal{E}(\text{pk}_i, 0^{|\text{sk}|}) & \text{if } i < t \\ \mathcal{E}(\text{pk}_i, \text{sk}_{i+1 \bmod n}) & \text{otherwise.} \end{cases}$$

Give  $c_0, \dots, c_t^b, \dots, c_n$  to  $\mathcal{A}$ .

5. When  $\mathcal{A}$  outputs  $b'$ , output  $b'$ .

It can be observed that when  $b = 0$ ,  $\mathcal{A}'$  has simulated  $\text{ZERO}_{\mathcal{A}, \Pi}(n, t+1, \eta)$  and when  $b = 1$ ,  $\mathcal{A}'$  has simulated  $\text{ZERO}_{\mathcal{A}, \Pi}(n, t, \eta)$ . Therefore we conclude that if  $\epsilon(\eta)$  is not negligible, then  $\Pi$  is not CPA secure.  $\square$