Separations in Circular Security for Arbitrary Length Key Cycles

Venkata Koppula
University of Texas at Austin
kvenkata@cs.utexas.edu

Kim Ramchen
University of Texas at Austin
kramchen@cs.utexas.edu

Brent Waters
University of Texas at Austin
bwaters@cs.utexas.edu *

Abstract

While standard notions of security suffice to protect any message supplied by an adversary, in some situations stronger notions of security are required. One such notion is *n-circular security*, where ciphertexts $\mathsf{Enc}(\mathsf{pk}_1, \mathsf{sk}_2), \mathsf{Enc}(\mathsf{pk}_2, \mathsf{sk}_3), \ldots, \mathsf{Enc}(\mathsf{pk}_n, \mathsf{sk}_1)$ should be indistinguishable from encryptions of zero.

In this work we prove the following results for n-circular security:

- For any n there exists an encryption scheme that is IND-CPA secure but not n-circular secure.
- There exists a bit encryption scheme that is IND-CPA secure, but not 1-circular secure.
- If there exists an encryption system where an attacker can distinguish a key encryption cycle from an encryption of zeroes, then in a transformed cryptosystem there exists an attacker which recovers secret keys from the encryption cycles.

Our first two results apply a novel utilization of indistinguishability obfuscation. The last result is generic and applies to any such cryptosystem.

*Supported by NSF CNS-0915361 and CNS-0952692, CNS-1228599 DARPA through the U.S. Office of Naval Research under Contract N00014-11-1-0382, DARPA N11AP20006, Google Faculty Research award, the Alfred P. Sloan Fellowship, Microsoft Faculty Fellowship, and Packard Foundation Fellowship. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of Defense or the U.S. Government.

1 Introduction

The classical notion of secure encryption, due to Goldwasser and Micali [GM84] demands that random encryptions of two messages submitted by the adversary should be indistinguishable. However this security notion makes no guarantees about the security of encrypting messages which the adversary is unable to generate - indeed this was observed by Goldwasser and Micali. Of particular interest is when an adversary can receive encryptions of messages which depend upon the *secret key*. The resulting notion of security against *key dependent message* attacks was first studied by Black et al [BRS01].

A particularly prominent special case of KDM security, introduced by Camenisch and Lysyanskaya [CL01], is *n-circular security*. Let $\mathsf{pk}_1, \ldots, \mathsf{pk}_n$ be public keys. An encryption scheme is said to be n-circular secure, if an adversary is unable to distinguish $\mathsf{Enc}(\mathsf{pk}_1, \mathsf{sk}_2), \mathsf{Enc}(\mathsf{pk}_2, \mathsf{sk}_3), \ldots, \mathsf{Enc}(\mathsf{pk}_n, \mathsf{sk}_1)$ from corresponding zero encryptions. Camenisch and Lysyanskaya used circular secure encryption to build an anonymous credentials scheme with "all or nothing" sharing [CL01]. In fact, circular security for $n \geq 1$ arises naturally in many other applications. A common scenario is when a disk utility is used to encrypt a partition on which the secret key has carelessly been stored. Another situation is Gentry's "bootstrapping" of a somewhat homomorphic encryption to a fully homomorphic encryption [Gen09]. In this case the decryption circuit associated with the secret key is encrypted and published in the public parameters and used to "refresh" a ciphertext periodically. Finally, circular security is used in formal methods to prove the soundness of symbolic protocols [ABHS05, Lau02].

There have been several postive results on circular security and more generally KDM security. In the random oracle model, Black et al. [BRS01] and independently Camenisch and Lysyanskaya [CL01] gave constructions for KDM secure encryption. Some time later Boneh, Hamburg, Halevi and Ostrovsky gave the first construction of circular secure encryption in the standard model [BHHO08]. Their construction provided instantiations of n-circular secure encryption for arbitrary n and in fact provided security for a broader class of key dependent messages - namely all affine functions of the secret key. Continuing in this vein, Applebaum et al [ACPS09] presented efficient constructions for affine functions under the LWE and LPN assumptions - the former for public key encryption and both for symmetric key encryption. Later works [HH09, BG10, BHHI10, BGK11, App11, MTY11, BV11, ASP12] focussed on extending the class of functions and improving efficiency of the constructions.

While there have been many positive advances for circular secure encryption and related functionalities, fewer negative results are known. *One fundamental question is whether it might be possible that circular security is implied by semantic security?* If this held, then it would have important consequences for the design of cryptographic primitives. In particular, an affirmative answer for *any* n would imply a method to construct secure fully homomorphic encryption from mildly or leveled homomorphic encryption. For small n concrete negative results are known. Indeed for $n = 1$, a folklore counterexample exists. For $n = 2$, Acar et al. [ABBC10] presented a counterexample under the SXDH assumption. Cash et al. [CGH12] showed how to strengthen this result, with a counterexample for $n = 2$ under a weaker definition of circular security. Despite these advances, for $n > 2$ the problem has largely remained open.

A related question is whether bit-by-bit encryption might suffice for protecting the secret key, i.e. ensure 1-circular security. Again there is partial negative information in that Rothblum [Rot13] has showed, interestingly, that if there exist l-multilinear groups of order p, with $p \leq 2^l$, in which the SXDH assumption holds, then there exists a semantically secure encryption scheme which is not 1-circular secure. Unfortunately, existing candidates for multilinear group schemes [GGH13a, CLT13] do not meet the SXDH requirement. Consequently there are no existing candidates for the Rothblum counterexample. As Rothblum observes, if bit by bit encryption implied circular security, this would give another avenue for utilizing Gentry's bootstrapping.

1.1 Our Contribution

We present the following results:

Counterexample for n-circular security We construct an encryption scheme that is IND-CPA secure

but not n-circular secure.

Bit encryption counterexample We construct a bit encryption scheme that is IND-CPA secure, but not circular secure.

Key recovery from n-circular insecurity Suppose there exists an IND-CPA secure encryption system where there exists an adversary that can distinguish an encryption cycle from the encryption of zeroes. We show how to transform this into an IND-CPA security cryptosystem where the adversary can recover the secret keys from the encryption cycle.

Both the constructions utilize the recent construction of *indistinguishability obfuscation* for polynomial sized circuits by Garg et al. [GGH+13b]. An indistinguishability obfuscation of a program g is a program $i\mathcal{O}(g)$ with a weaker security guarantee: if two programs g and g' have the same input-output behavior, then $i\mathcal{O}(g)$ and $i\mathcal{O}(g')$ are computationally indistinguishable. As argued by [GGH+13b, SW13], indistinguishability obfuscation is the weakest definition of obfuscation, and unlike black box obfuscation, there are no known impossibility results for indistinguishability obfuscation.

Counterexample for n-circular security: We begin by giving intuition for our encryption scheme. Let us consider any IND-CPA secure encryption scheme $\mathcal{PKE} = (\mathsf{Keygen}, \mathsf{Encrypt}, \mathsf{Decrypt})$. We show how this encryption scheme can by modified by providing some *auxiliary information* as part of the *ciphertext*, so that the scheme is n-circular insecure, and at the same time, remains IND-CPA secure. We approach the problem in two steps. We first design an approach that works with black box obfuscation. Then we design new techniques to move our construction and proof of security to use indistinguishability obfuscation.

To construct our counterexample we begin with a standard encryption system and then modify the encryption algorithm. When encrypting a message m, in addition to the $\mathcal{PKE}$ ciphertext c, we also give out a *cycle detection program* g^m which can be used to detect whether a cycle is present or not. The program g^m has m hardwired, takes n inputs $c_1, \ldots, c_n$, and works as follows: It decrypts, if possible, c_2 using m to obtain m_2, c_3 using m_2 to obtain m_3 and so on. If any decryption fails, it aborts and outputs 0. If it reaches the end of cycle, it outputs 1.

Let us consider a polynomial time adversary who is given n ciphertexts $\mathsf{ct}_1, \ldots, \mathsf{ct}_n$, where each ct_i consists of a $\mathcal{PKE}$ ciphertext c_i and a program g_i. The adversary runs program g_1 with inputs $c_1, \ldots, c_n$. If these are encryptions of secret keys $\mathsf{sk}_2, \ldots, \mathsf{sk}_n, \mathsf{sk}_1$ respectively, then g_1 runs to completion outputting 1, else it outputs 0. Therefore, using this additional information, we can detect whether there is a cycle or not. However, this scheme in itself is not IND-CPA secure since g^m may leak the value m. Therefore, as part of the ciphertext, we publish black box obfuscation of g^m: $\mathcal{O}(g^m)$. One can then argue that black box obfuscation ensures that the value m is not leaked, and hence it is IND-CPA secure.

Unfortunately, as shown by [BGI+01], it is not possible to achieve general black box obfuscation even for simple functionalities;[1] therefore, we modify our construction so as to use the weaker indistinguishability obfuscation. Our key idea is to have a set of *valid* and *invalid* public keys for each secret key such that the valid and invalid public keys are computationally indistinguishable from just the public key, *but validity is discernible given a secret key.* In our system we use such keys. In addition, at the end of the cycle detection program, we add a validity check, to ensure that pk_1 is a valid public key corresponding to m_n.

While this modification still ensures that the scheme is n-circular insecure, we need to prove IND-CPA security. Our proof of this proceeds in two hybrid steps. First, since the valid and invalid keys are indistinguishable, the real IND-CPA security game is computationally indistinguishable from one in which we substitute in invalid public keys for the real ones. Next, we observe that these invalid public keys must necessarily fail the validity check at the end of the cycle detection program, and therefore the program *always outputs 0.* Therefore, instead of outputting obfuscation of the cycle detection program, if we output the obfuscation of a program that always outputs 0, the two hybrids remain indistinguishable by property of indistinguishability obfuscation. Finally, a program that always aborts leaks no information about m, and therefore the scheme is IND-CPA secure.

[1] It is of course possible that black box obfuscation is obtainable for this particular functionality. However, we view obtaining our negative result under indistinguishability obfuscation as an important goal.

One potential view of this is as a novel and extreme application of punctured programming [SW13]. Once we alter the keys to be invalid, we can completely gut the obfuscated program to be one that simply outputs 0. In indepedent and concurrent work Boneh and Zhandry [BZ13] apply a notion similar to our invalid/valid key structure (although do not use that terminology) to building multi-party key exchange, broadcast and traitor tracing systems. An important contribution of both papers is that they demonstrate the power of altering the structure of public keys in combination with indistinguishability obfuscation.

Bit encryption counterexample: We now consider the problem of bit encryption. We first observe that the aforementioned 'chasing the cycle' technique cannot be used for bit encryption. However, in this case, all encryptions use the same public key. As a result, we can now give out useful *auxiliary cryptographic material* as part of the *public key*. Here we again use the valid-invalid public keys technique. In particular, we modify the Keygen algorithm. Suppose we have a Keygen algorithm for a valid-invalid PKE system as described above that outputs pk, sk. Let pk' be the part of pk used for checking whether pk is a valid public key corresponding to sk, and sk' the part of sk used for decrypting ciphertexts. Now consider the program $g^{\mathsf{pk}',\mathsf{sk}'}$ that has $\mathsf{pk}', \mathsf{sk}'$ hardwired, and takes l inputs $c_1, \ldots, c_l$. Program $g^{\mathsf{pk}',\mathsf{sk}}$ decrypts each of the inputs using sk' and checks (using pk') whether pk is a valid public key corresponding to the resulting string. In our modified encryption scheme, in addition to pk, we also give out an indistinguishability obfuscation of program $g^{\mathsf{pk}',\mathsf{sk}'}$.

Clearly, this encryption scheme is not bit circular secure. To prove $\mathsf{IND\text{-}CPA}$ security, we use similar hybrids as before. In the first hybrid experiment, we switch from valid to invalid public keys. Since the valid and invalid public keys are computationally indistinguishable, these hybrid experiments are computationally indistinguishable. Finally, we output an obfuscation of a program that always aborts, thereby ensuring that no information about the secret key sk is leaked by the program obfuscation.

Key recovery from n-circular insecurity: One interesting question posed in the setting of circular security is what is the right definition of security. While preventing against cycle detection is seemingly the strongest notion, in many applications such as Gentry's bootstrapping it might be sufficient if the system remained semantically secure (for other messages) in the presence of a key cycle, even if the key cycle itself were detectable. Likewise, a counterexample for such a weaker notion of security would be a stronger result. Cash et al. [CGH12] improved upon the work of Acar et al. [ABBC10] by giving a such a stronger counterexample which allowed for an attacker to completely recover private keys for the case of key cycles of length two.

The key-recovery from cycles technique of Cash et. al. was tailored specifically to the case of bilinear maps. In this work, we show that if for any n there exists an encryption system where an attacker can distinguish a key encryption cycle from a encryption of zeroes, then we can create a transformed cryptosystem where there exists an attacker which recovers secret keys from the encryption cycles. Thus, for obtaining a strong key recovery counterexample, one only needs to work to obtain a cycle detection counterexample.

Our methods here are in spirit similar to Rothblum's result in [Rot13] for the bit encryption case. When encrypting a message, we also publish a *hint* for each bit of the message, indicating whether the bit is 0 or 1. To determine the bit, we use the cycle detection algorithm. As a consequence, this hint works if and only if we have a cycle of secret keys, therefore ensuring both $\mathsf{IND\text{-}CPA}$ security and key recovery.

2 Preliminaries

Definition 1 (Public Key Encryption)**.** A public key encryption scheme $\mathcal{PKE}$ is a set of three algorithms (Keygen, $\mathsf{Encrypt}$, $\mathsf{Decrypt}$) satisfying the following properties :

- **Key Generation** $\mathsf{Keygen}(1^\lambda)$ is a randomized algorithm that takes as input the security parameter λ and outputs public key pk and secret key sk.
- **Encryption** $\mathsf{Encrypt}(\mathsf{pk}, m)$ is a randomized algorithm that takes as input a public key pk, message m and outputs a ciphertext ct.

- **Decryption** $\mathsf{Decrypt}(\mathsf{sk}, ct)$ is a deterministic algorithm that takes as input a secret key sk, a ciphertext ct and outputs m.

For correctness, we require that for all m,

$$\Pr[\mathsf{Decrypt}(\mathsf{sk}, \mathsf{Encrypt}(\mathsf{pk}, m)) \neq m : (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Keygen}(1^\lambda)] \leq \mathrm{negl}(\lambda).$$

A public key cryptosystem is called a *bit encryption scheme* if its message space is $\{0, 1\}$.

We define various security notions for public key cryptosystems.

Definition 2 (IND-CPA Security)**.** Let $\mathcal{PKE} = (\mathsf{Keygen}, \mathsf{Encrypt}, \mathsf{Decrypt})$ be a public key cryptosystem. Consider the following game between challenger $\mathcal{C}$ and adversary $\mathcal{A}$:

IND-CPA :

1. $\mathcal{C}$ computes $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Keygen}(1^\lambda)$ and sends pk to $\mathcal{A}$.
2. $\mathcal{A}$ sends challenge plaintext messages m_0, m_1 such that $|m_0| = |m_1|$ to $\mathcal{C}$.
3. $\mathcal{C}$ chooses a bit $b \xleftarrow{\$} \{0, 1\}$, computes $ct \leftarrow \mathsf{Encrypt}(\mathsf{pk}, m_b)$ and sends ct to $\mathcal{A}$.
4. $\mathcal{A}$ outputs a bit b'

The advantage of $\mathcal{A}$ is $Adv_\mathcal{A} = \Pr[b = b'] - \frac{1}{2}$.
$\mathcal{PKE}$ is said to be IND-CPA secure if for all PPT algorithms $\mathcal{A}$, $Adv_\mathcal{A} \leq \mathrm{negl}(\lambda)$.

2.1 Circular Security

Definition 3 (n-Circular Security [CL01])**.** Let $\mathcal{PKE} = (\mathsf{Keygen}, \mathsf{Encrypt}, \mathsf{Decrypt})$ be a public key cryptosystem. Consider the following game between challenger $\mathcal{C}$ and adversary $\mathcal{A}$:

n-Circular Security :

1. $\mathcal{C}$ computes $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{Keygen}(1^\lambda)$ for $1 \leq i \leq n$
2. $\mathcal{C}$ chooses a bit $b \xleftarrow{\$} \{0, 1\}$.
   - If $b = 0$, $\mathcal{C}$ computes $y_i = \mathsf{Encrypt}(\mathsf{pk}_i, \mathsf{sk}_{(i \bmod n)+1})$ for $1 \leq i \leq n$
   - Else $\mathcal{C}$ computes $y_i = \mathsf{Encrypt}(\mathsf{pk}_i, 0^{|\mathsf{sk}_{(i \bmod n)+1}|})$ for $1 \leq i \leq n$
3. $\mathcal{C}$ sends $(\mathsf{pk}_1, \ldots, \mathsf{pk}_n, y_1, \ldots, y_n)$ to $\mathcal{A}$.
4. $\mathcal{A}$ outputs b'.

The advantage of $\mathcal{A}$ is $Adv_\mathcal{A} = \Pr[b = b'] - \frac{1}{2}$.
$\mathcal{PKE}$ is said to be n-circular secure if for all PPT algorithms $\mathcal{A}$, $Adv_\mathcal{A} \leq \mathrm{negl}(\lambda)$

A *weak* notion of circular security was defined in [CGH12] as follows :

Definition 4 (n-Weak Circular Security)**.** Let $\mathcal{PKE} = (\mathsf{Keygen}, \mathsf{Encrypt}, \mathsf{Decrypt})$ be a public key cryptosystem. Consider the following game between challenger $\mathcal{C}$ and adversary $\mathcal{A}$:

n-**Weak Circular Security** :

1. $\mathcal{C}$ computes $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{Keygen}(1^\lambda)$ for $1 \leq i \leq n$.
   Next, it computes $y_i = \mathsf{Encrypt}(\mathsf{pk}_i, \mathsf{sk}_{(i \bmod n)+1})$ for $1 \leq i \leq n$.
   It sends $(\mathsf{pk}_1, \ldots, \mathsf{pk}_n, y_1, \ldots, y_n)$ to $\mathcal{A}$.
2. $\mathcal{A}$ sends challenge plaintext messages m_0, m_1 such that $|m_0| = |m_1|$ and $j \in [1, n]$ to $\mathcal{C}$
3. $\mathcal{C}$ chooses a bit $b \xleftarrow{\$} \{0, 1\}$ and sends $\mathsf{Encrypt}(\mathsf{pk}_j, m_b)$ to $\mathcal{A}$.
4. $\mathcal{A}$ outputs b'

The advantage of $\mathcal{A}$ is $Adv_{\mathcal{A}} = \Pr[b = b'] - \frac{1}{2}$.
$\mathcal{PKE}$ is said to be n-weak circular secure if for all PPT algorithms $\mathcal{A}$, $Adv_{\mathcal{A}} \leq \text{negl}(\lambda)$

Definition 5 (n-Circular Security with respect to Key Recovery)**.** Let $\mathcal{PKE} = (\mathsf{Keygen}, \mathsf{Encrypt}, \mathsf{Decrypt})$ be a public key cryptosystem. Consider the following game between challenger $\mathcal{C}$ and adversary $\mathcal{A}$:

n-**Circular Security with respect to Key Recovery** :

1. $\mathcal{C}$ computes $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{Keygen}(1^\lambda)$ for $1 \leq i \leq n$.
   Next, it computes $y_i = \mathsf{Encrypt}(\mathsf{pk}_i, \mathsf{sk}_{(i \bmod n)+1})$ for $1 \leq i \leq n$.
   It sends $(\mathsf{pk}_1, \ldots, \mathsf{pk}_n, y_1, \ldots, y_n)$ to $\mathcal{A}$.
2. $\mathcal{A}$ outputs sk'_1.

The advantage of $\mathcal{A}$ is $Adv_{\mathcal{A}} = \Pr[sk_1 = sk'_1]$.
$\mathcal{PKE}$ is said to be n-circular secure with respect to key recovery if for all PPT algorithms $\mathcal{A}$, $Adv_{\mathcal{A}} \leq \text{negl}(\lambda)$

Remark. If a public key encryption scheme is n-circular secure, then it is also n-weak circular secure. Similarly, if a scheme is n-weak circular secure, then it is also n-circular secure with respect to key recovery.

The notion of circular security can be extended to bit encryption schemes. The following definition is actually equivalent to Definition 3 in the case that $n = 1$, but will be slightly more convenient to work with.

Definition 6 (1-Circular Security of Bit-by-bit Encryption)**.** Let $\mathcal{PKE} = (\mathsf{Keygen}, \mathsf{Encrypt}, \mathsf{Decrypt})$ be a bit encryption scheme. Consider the following game between challenger $\mathcal{C}$ and adversary $\mathcal{A}$:

1-**Circular Security of Bit-by-bit Encryption** :

1. $\mathcal{C}$ chooses $b \xleftarrow{\$} \{0, 1\}$. $\mathcal{C}$ generates the public key and secret key $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Keygen}(1^\lambda)$ and sends pk to $\mathcal{A}$.
2. For a polynomial number of queries
   (a) $\mathcal{A}$ queries for encryption of j_i^{th} bit of sk.
   (b) If $b = 1$, $\mathcal{C}$ sends $ct \leftarrow \mathsf{Encrypt}(\mathsf{pk}, \mathsf{sk}_{j_i})$. Else $\mathcal{C}$ sends $ct \leftarrow \mathsf{Encrypt}(\mathsf{pk}, 0)$.
3. $\mathcal{A}$ outputs b'

The advantage of $\mathcal{A}$ is $Adv_{\mathcal{A}} = \Pr[b = b'] - \frac{1}{2}$.
$\mathcal{PKE}$ is said to be *bit circular secure* if for all PPT algorithms $\mathcal{A}$, $Adv_{\mathcal{A}} \leq \text{negl}(\lambda)$

Rothblum in [Rot13] showed that this notion of bit circular security, which he called circular security with respect to indistinguishability of oracles, is equivalent to the seemingly stronger notion where the adversary must extract the entire secret key, given encryptions of the secret key bits. Therefore, it suffices to restrict our attention to this notion of bit circular security.

2.2 Indistinguishability Obfuscation

Next, we recall the definition of indistinguishability obfuscation from [GGH+13b, SW13]

Definition 7. (Indistinguishability Obfuscation) A uniform PPT machine $i\mathcal{O}$ is called an indistinguishability obfuscator for a circuit class $\{\mathcal{C}_\lambda\}$ if it satisfies the following conditions:

- (Preserving Functionality) If for all security parameters $\lambda \in \mathbb{N}$, for all $C \in \mathcal{C}_\lambda$, for all inputs x, we have that $C'(x) = C(x)$ where $C' \leftarrow i\mathcal{O}(\lambda, C)]$
- (Indistinguishability of Obfuscation) For any (not necessarily uniform) PPT distinguisher $(Samp, D)$, there exists a negligible function $\mathrm{negl}(\cdot)$ such that the following holds: if for all security parameters $\lambda \in \mathbb{N}, \Pr[\forall x, C_0(x) = C_1(x) : (C_0; C_1; \sigma) \leftarrow Samp(1^\lambda)] > 1 - \mathrm{negl}(\lambda)$, then

$$|\Pr[D(\sigma, i\mathcal{O}(\lambda, C_0)) = 1 : (C_0; C_1; \sigma) \leftarrow Samp(1^\lambda)] - \Pr[D(\sigma, i\mathcal{O}(\lambda, C_1)) = 1 : (C_0; C_1; \sigma) \leftarrow Samp(1^\lambda)]| \leq \mathrm{negl}(\lambda)$$

In a recent work, [GGH+13b] showed how indistinguishability obfuscators can be constructed for the circuit class $P/poly$.

3 Counter Example for n-Circular Security

In this section, we describe how to build for any n, a cryptosystem $\mathcal{PKE}$ that is IND-CPA secure, but not n-circular secure.

Let $\mathcal{PKE}_A = (\mathsf{Keygen}_A, \mathsf{Encrypt}_A, \mathsf{Decrypt}_A)$ be a public key encryption scheme with message space $\mathcal{M}_A = \{0,1\}^{2l}$, key space $\mathcal{K}_A \subseteq \{0,1\}^l$ and ciphertext space $\mathcal{C}_A$. Let $G : \{0,1\}^l \to \{0,1\}^{2l}$ be a PRG family. We construct cryptosystem $\mathcal{PKE} = (\mathsf{Keygen}, \mathsf{Encrypt}, \mathsf{Decrypt})$ as follows:

- $\mathsf{Keygen}(1^\lambda)$**:** Let $(\mathsf{sk}_A, \mathsf{pk}_A) \leftarrow \mathsf{Keygen}_A(1^\lambda)$. Let $r \xleftarrow{\$} \{0,1\}^l$ and $t = G(r)$. Set $\mathsf{sk} = (\mathsf{sk}_A, r)$. Set $\mathsf{pk} = (\mathsf{pk}_A, t)$.
- $\mathsf{Encrypt}(\mathsf{pk}, m, r)$**:** Parse $\mathsf{pk} = (\mathsf{pk}_A, t)$. Let $C \leftarrow \mathsf{Encrypt}_A(\mathsf{pk}_A, m)$.

  Let CycleFind be a circuit defined as follows :

  CycleFind :
  Inputs : $C_1, \ldots, C_n \in \mathcal{C}_A$
  Constants : $m, t, 0^w$ for an appropriately chosen w
  1. Parse $m = (\mathsf{sk}_2, r)$.
  2. For i=2 to n
     (a) Let $(\mathsf{sk}_{(i \bmod n)+1}, r_{(i \bmod n)+1}) = \mathsf{Decrypt}_A(\mathsf{sk}_i, C_i)$ or output $\perp$ if $\mathsf{Decrypt}_A$ fails.
  3. If $G(r_1) = t$ output 1, else output $\perp$.

  The circuit CycleFind takes as input n ciphertexts $C_1, \ldots, C_n$, and has constants $m, t, 0^w$ hardwired, where the length of the zero padding w is chosen appropriately.
  Compute obfuscation of circuit CycleFind as $O \leftarrow i\mathcal{O}(\lambda, \mathsf{CycleFind})$. The ciphertext $ct = (C, O)$.
- $\mathsf{Decrypt}(\mathsf{sk}, ct)$**:** Parse $\mathsf{sk} = (\mathsf{sk}_A, r)$ and $ct = (C, O)$. Output $\mathsf{Decrypt}_A(\mathsf{sk}_A, C)$. String O is ignored.

Correctness follows immediately from the correctness of the original scheme $\mathcal{PKE}_A$.

3.1 The Attack

Proposition 1. *The above construction is n-circular insecure.*

Proof. We construct a polynomial time adversary $\mathcal{A}$ that breaks the n-circular security of the above construction as follows. $\mathcal{A}$ receives $(\mathsf{pk}_1, \ldots, \mathsf{pk}_n, y_1, \ldots, y_n)$ from the challenger. $\mathcal{A}$ parses y_i as $(C_i, \mathcal{O}_i)$ where $\mathcal{O}_i$ is a circuit. $\mathcal{A}$ outputs the value $b \leftarrow \mathcal{O}_1(C_1, \ldots, C_n)$. By construction this is 1 iff $(y_1, \ldots, y_n)$ is an encryption cycle with respect to $\mathcal{PKE}$. □

3.2 IND-CPA Security

In order to show that our construction is IND-CPA secure, we construct a series of hybrid experiments as follows.

Game 0: IND-CPA **Game**

1. Choose $r \xleftarrow{\$} \{0,1\}^l$ and set $t = G(r)$.
2. Let $(\mathsf{sk}_A, \mathsf{pk}_A) \leftarrow \mathsf{Keygen}_A(1^\lambda)$.
3. Let $\mathsf{sk} = (\mathsf{sk}_A, r)$ and $\mathsf{pk} = (\mathsf{pk}_A, t)$.
4. Suppose $\mathcal{A}$ sends $m_0, m_1 : |m_0| = |m_1|$.
5. Choose $b \xleftarrow{\$} \{0,1\}$.
6. Let $C = \mathsf{Encrypt}_A(\mathsf{pk}_A, m_b)$.
7. Let $O = i\mathcal{O}(\lambda, \mathsf{CycleFind})$ where CycleFind is the circuit described above.
8. Let $ct_b = (C, O)$. Send ct_b to $\mathcal{A}$.
9. Let $b' \leftarrow \mathcal{A}_2(\delta, ct_b)$.

$\mathcal{A}$ wins if $b = b'$ and has advantage $Adv_{\mathcal{A}} = \Pr[b = b'] - 1/2$.

Game 1: This game proceeds identically as the IND-CPA game, except we modify Step 1 as follows.
1. Choose $r \xleftarrow{\$} \{0,1\}^l$ and choose $t \xleftarrow{\$} \{0,1\}^{2l}$. Note that r is information theoretically hidden in this experiment.

Game 2: This game proceeds identically as **Game 1**, except we modify Step 7 as follows.
Let CycleReject be the following circuit:

CycleReject :
Inputs : $C_1, \ldots, C_n \in \mathcal{C}_A$
Constants : $0^{w'}$

1. Output $\perp$

The circuit CycleReject takes as input n ciphertexts $C_1, \ldots, C_n$, has zero padding of length w'. The constant w in circuit CycleFind and w' in circuit CycleReject are chosen such that the size of circuits CycleFind and CycleReject are equal.
Let $O = i\mathcal{O}(\lambda, \mathsf{CycleReject})$.

Proposition 2. *Suppose that there exists a polynomial time adversary $\mathcal{A}$ such that $Game_0 Adv_{\mathcal{A}} - Game_1 Adv_{\mathcal{A}} = \epsilon$. Then there exists a polynomial time adversary $\mathcal{B}$ who distinguishes the output of G from random with advantage $\epsilon_{PRG} = \epsilon$.*

Proof. The only modification is that t is computed as random $2l$-bit string rather than the output of G. The algorithm $\mathcal{B}$ is defined as follows :

1. $\mathcal{B}$ receives $t \in \{0,1\}^{2l}$ from PRG Challenger $\mathcal{C}$, where t is either a pseudorandom string generated by G or a truly random string.
2. $\mathcal{B}$ computes $(\mathsf{sk}_A, \mathsf{pk}_A) \leftarrow \mathsf{Keygen}_A(1^\lambda)$. It sets $\mathsf{pk} = (\mathsf{pk}_A, t)$ and sends it to $\mathcal{A}$.
3. $\mathcal{A}$ sends challenge messages m_0, m_1.
4. $\mathcal{B}$ chooses $b \xleftarrow{\$} \{0,1\}$. It sets $C = \mathsf{Encrypt}_A(\mathsf{pk}_A, m_b)$. Next, it defines circuit $\mathsf{CycleFind}$, which has m_b and t hard-wired. Therefore, $\mathcal{B}$ can define $\mathsf{CycleFind}$, and hence compute $O \leftarrow i\mathcal{O}(\lambda, \mathsf{CycleFind})$. Hence it sets $ct = (C, O)$ and sends it to $\mathcal{A}$.
5. $\mathcal{A}$ outputs a bit b'. If $(b = b')$ $\mathcal{B}$ outputs that the string was pseudorandom. Else $\mathcal{B}$ outputs the string was random.

If $\mathcal{C}$ sends an output of G, then this experiment corresponds to Game 0. If $\mathcal{C}$ sends a truly random string t, then this corresponds to Game 1. Therefore, if $\mathcal{A}$ can distinguish between Game 0 and Game 1 with advantage ϵ, then $\mathcal{B}$ distinguishes a pseudorandom string form a truly random string with advantage ϵ. □

Proposition 3. *Suppose that there exists a polynomial time adversary $\mathcal{A}$ such that $Game_1Adv_{\mathcal{A}}$ - $Game_2Adv_{\mathcal{A}}$ $= \epsilon$. Then there exists a polynomial time adversary $\mathcal{B}$ who breaks the indistinguishability obfuscation with advantage $\epsilon_{iO} = \epsilon$.*

Proof. Recall that $\mathcal{B}$ should comprise a pair of adversaries $(Samp, D)$ as in Definition 2.2. We construct these adversaries as follows.
$Samp(1^\lambda)$:

1. Choose $r \xleftarrow{\$} \{0,1\}^l$ and $t \xleftarrow{\$} \{0,1\}^{2l}$.
2. Let $(\mathsf{sk}_A, \mathsf{pk}_A) \leftarrow \mathsf{Keygen}_A(1^\lambda)$.
3. Let $\mathsf{sk} = (\mathsf{sk}_A, r)$ and $\mathsf{pk} = (\mathsf{pk}_A, t)$.
4. Let $(m_0, m_1) \leftarrow \mathcal{A}(\mathsf{pk}) : |m_0| = |m_1|$.
5. Choose $b \xleftarrow{\$} \{0,1\}$.
6. Let $\mathsf{CycleFind}$ be the circuit described in our construction with constants (m_b, t, 0^w) hardwired.
   Let $\mathsf{CycleReject}$ be the circuit described in Game 2 with constant $0^{w'}$ hardwired.
7. Output ($g_0 = \mathsf{CycleFind}, g_1 = \mathsf{CycleReject}$).
8. Set $\sigma = (b, m_0, m_1, \mathsf{pk})$.

$D(\sigma, i\mathcal{O}(\lambda, g_z))$:

1. Let $C = \mathsf{Encrypt}_A(\mathsf{pk}_A, m_b)$, let $O = i\mathcal{O}(\lambda, g_z)$.
2. Let $ct = (C, O)$.
3. Let $b' \leftarrow \mathcal{A}(ct, \mathsf{pk})$.
4. D guesses 1 if $b = b'$.

We first prove that $\mathcal{B}$ produces circuits g_0, g_1 which are equivalent on all inputs, with overwhelming probability. Observe that with overwhelming probability t is not in the range of G since $t \xleftarrow{\$} \{0,1\}^{2l}$ and hence $\mathsf{CycleFind}(x)$ outputs $\perp$ for all x. Thus $Samp$ produces circuits $\mathsf{CycleReject}$ and $\mathsf{CycleFind}$ which are equivalent on all inputs with overwhelming probability, by the random choice of t.

All that remains is to show $Adv_{\mathcal{B}} = \epsilon$. Let $p_z = \Pr[D(\sigma, i\mathcal{O}(\lambda, g_z)) = 1]$ for $z = 0, 1$. Note that $g_0 = \mathsf{CycleFind}$, hence when $z = 0$ the event $b = b'$ occurs iff $\mathcal{A}$ wins **Game 1**. Similarly $g_1 = \mathsf{CycleReject}$, hence when $z = 1$, the event $b = b'$ occurs iff $\mathcal{A}$ wins **Game 2**. Then $p_0 = 1/2 + Game_1Adv_{\mathcal{A}}$, while $p_1 = 1/2 + Game_2Adv_{\mathcal{A}}$. Thus $Adv_{\mathcal{B}} = p_0 - p_1 = Game_1Adv_{\mathcal{A}} - Game_2Adv_{\mathcal{A}} = \epsilon$. □

Finally, we need to show that any polynomial time adversary has only negligible advantage in Game 2. This follows from the fact that $\mathcal{PKE}_A$ is IND-CPA secure.

Proposition 4. *If there exists a polynomial time adversary $\mathcal{A}$ with non negligible advantage ϵ in Game 2, then there exists a polynomial time algorithm $\mathcal{B}$ that can break the* IND-CPA *security of $\mathcal{PKE}_A$ with advantage $\epsilon_A = \epsilon$.*

Proof. Suppose $\mathcal{A}$ has advantage ϵ in Game 2. We define $\mathcal{B}$ as follows :

1. $\mathcal{B}$ receives pk_A from the IND-CPA Challenger $\mathcal{C}$. It chooses $t \xleftarrow{\$} \{0,1\}^{2l}$ and sends public key $\mathsf{pk} = (\mathsf{pk}_A, t)$ to $\mathcal{A}$.
2. $\mathcal{A}$ sends challenge messages m_0, m_1, which are passed on to $\mathcal{C}$, and receives ciphertext C.
3. $\mathcal{B}$ computes $O \leftarrow i\mathcal{O}(\lambda, \mathsf{CycleReject})$ and sends ciphertext $ct = (C, O)$ to $\mathcal{A}$.
4. $\mathcal{A}$ sends bit b', which $\mathcal{B}$ passes on to $\mathcal{C}$.

Note that if $\mathcal{A}$ wins Game 2, then $\mathcal{B}$ wins the IND-CPA game. Hence the result follows. □

The advantage of any polynomial time IND-CPA adversary against $\mathcal{PKE}$ is at most $\epsilon_{PRG} + \epsilon_{iO} + \epsilon_A$. Therefore we have the following theorem.

Theorem 1. *Assuming that G is a secure PRG family, $i\mathcal{O}$ is an indistinguishability obfuscator and $\mathcal{PKE}_A$ is an* IND-CPA *secure encryption scheme, $\mathcal{PKE}$ is* IND-CPA *secure but not n-circular secure.*

4 Counter Example for 1-Circular Security of Bit-by-bit Encryption

In this section, we describe a bit encryption scheme that is IND-CPA secure, but is not 1-circular secure. Let $\mathcal{PKE}_A = (\mathsf{Keygen}_A, \mathsf{Encrypt}_A, \mathsf{Decrypt}_A)$ be a bit encryption cryptosystem with key space $\mathcal{K}_A \subseteq \{0,1\}^l$. Let $G : \{0,1\}^l \to \{0,1\}^{2l}$ be a PRG. We construct a bit encryption cryptosystem $\mathcal{PKE} = (\mathsf{Keygen}, \mathsf{Encrypt}, \mathsf{Decrypt})$ as follows :

- $\mathsf{Keygen}(1^\lambda)$: Let $(\mathsf{pk}_A, \mathsf{sk}_A) \leftarrow \mathsf{Keygen}_A(1^\lambda)$. Choose $r \xleftarrow{\$} \{0,1\}^l$ and compute $t = G(r)$. Define a circuit BitCycleFind as follows :

  BitCycleFind :
  Inputs : $C_1, \ldots, C_l \in \mathcal{C}_A$
  Constants : $\mathsf{sk}_A, t, 0^w$ for an appropriately chosen w
  1. For $i = 1$ to l
     (a) Let $x_i = \mathsf{Decrypt}_A(\mathsf{sk}_A, C_i)$ or output $\perp$ if $\mathsf{Decrypt}_A$ fails.
  2. Let $x = x_1 \ldots x_l$. If $G(x) = t$ output 1, else output $\perp$.

  The circuit takes as input l ciphertexts, and has constants sk_A, t and 0^w hardwired. As in the multi-bit encryption, the zero padding is required for the security proof.
  Compute obfuscation of circuit BitCycleFind as $O \leftarrow i\mathcal{O}(\lambda, \mathsf{BitCycleFind})$. Set $\mathsf{pk} = (\mathsf{pk}_A, t, O)$ and $\mathsf{sk} = (\mathsf{sk}_A, r)$.

- $\mathsf{Encrypt}(\mathsf{pk}, m)$: Parse $\mathsf{pk} = (\mathsf{pk}_A, t, O)$. Compute ciphertext $ct \leftarrow \mathsf{Encrypt}_A(\mathsf{pk}_A, m)$.

- $\mathsf{Decrypt}(\mathsf{sk}, ct)$: Parse $\mathsf{sk} = (\mathsf{sk}_A, r)$. Output $\mathsf{Decrypt}(\mathsf{sk}_A, ct)$.

The correctness of $\mathcal{PKE}$ follows directly from the correctness of $\mathcal{PKE}_A$.

4.1 The Attack

Proposition 5. *The above construction is not bit circular secure.*

Proof. We construct a polynomial time adversary $\mathcal{A}$ that breaks the *bit circular security* of the above construction as follows. $\mathcal{A}$ receives public key $\mathsf{pk} = (\mathsf{pk}_A, t, O)$. Next, it queries for encryptions of the last l bits of the secret key, and receives $ct_1, \ldots, ct_l$. $\mathcal{A}$ outputs $b = O(ct_1, \ldots, ct_l)$. By construction, it follows that $\mathcal{A}$ outputs 1 iff the challenger outputs encryptions of the bits of the secret key sk. □

4.2 IND-CPA Security

In this section, we show that our construction $\mathcal{PKE} = (\mathsf{Keygen}, \mathsf{Encrypt}, \mathsf{Decrypt})$ is IND-CPA secure.
As before we construct a sequence of hybrid experiments, and show that the outputs of the hybrid experiments are computationally indistinguishable.

Game 0: IND-CPA

1. Choose $r \xleftarrow{\$} \{0,1\}^l$ and set $t = G(r)$.
2. Let $(\mathsf{pk}_A, \mathsf{sk}_A) \leftarrow \mathsf{Keygen}_A(1^\lambda)$.
3. Let $O = i\mathcal{O}(\lambda, \mathsf{BitCycleFind})$ as described in the construction.
4. Let $\mathsf{sk} = (\mathsf{sk}_A, r)$ and $\mathsf{pk} = (\mathsf{pk}_A, t, O)$. Send pk to $\mathcal{A}$.
5. Choose $b \xleftarrow{\$} \{0,1\}$.
6. Let $ct_b \leftarrow \mathsf{Encrypt}_A(\mathsf{pk}_A, b)$. Send ct to $\mathcal{A}$.
7. Let $b' \leftarrow \mathcal{A}(ct_b)$.

$\mathcal{A}$ wins if $b = b'$ and has advantage $Adv_{\mathcal{A}} = \Pr[b = b'] - 1/2$.

Game 1: This game proceeds identically as the IND-CPA game, except we modify Step 1 as follows.
1. Choose $r \xleftarrow{\$} \{0,1\}^l$ and choose $t \xleftarrow{\$} \{0,1\}^{2l}$. Note that r is information theoretically hidden in this experiment.

Game 2: This game proceeds identically as **Game 1**, except we modify Step 3 as follows.
Let BitCycleReject be the following circuit:

BitCycleReject :
Inputs : $C_1, \ldots, C_l \in \mathcal{C}_A$
Constants : $0^{w'}$

1. Output $\perp$

The circuit BitCycleReject takes as input l ciphertexts $C_1, \ldots, C_l$, has zero padding of length w'. The constants w in circuit BitCycleFind and w' in circuit BitCycleReject are chosen such that $|\mathsf{BitCycleFind}| = |\mathsf{BitCycleReject}|$
Let $O = i\mathcal{O}(\lambda, \mathsf{BitCycleReject})$.

The proofs of the following indistinguishability results are similar to those of the previous section and are included in Appendix A.

Proposition 6. *Suppose that there exists a polynomial time adversary $\mathcal{A}$ such that $Game_0 Adv_{\mathcal{A}}$ - $Game_1 Adv_{\mathcal{A}}$ $= \epsilon$. Then there exists a polynomial time adversary $\mathcal{B}$ who distinguishes the output of G from random with advantage $\epsilon_{PRG} = \epsilon$.*

Proposition 7. *Suppose that there exists a polynomial time adversary $\mathcal{A}$ such that $Game_1 Adv_{\mathcal{A}}$ - $Game_2 Adv_{\mathcal{A}}$ $= \epsilon$. Then there exists a polynomial time adversary $\mathcal{B}$ who breaks the indistinguishability obfuscation with advantage $\epsilon_{iO} = \epsilon$.*

Proposition 8. *If there exists a polynomial time adversary $\mathcal{A}$ with non-negligible advantage ϵ in Game 2, then there exists a polynomial time algorithm $\mathcal{B}$ that can break the* IND-CPA *security of $\mathcal{PKE}_A$ with advantage $\epsilon_A = \epsilon$.*

Then, combining the above results, we have the following theorem.

Theorem 2. *Assuming that G is a secure PRG family, $i\mathcal{O}$ is an indistinguishability obfuscator and $\mathcal{PKE}_A$ is an* IND-CPA *secure bit encryption scheme, $\mathcal{PKE}$ is* IND-CPA *secure but not* 1*-circular secure.*

5 Key Recovery From Circular Insecurity

In this section we show how to transform any IND-CPA encryption scheme which is n-circular insecure into a new IND-CPA scheme which is n-circular insecure *with respect to key recovery*. An interesting point of comparison is a result of Cash et al. [CGH12]. As described in the introduction their counterexample is particular to a specific construction for $n = 2$ length key cycles. We show how to generically 'leap' from any cycle detection insecure construction to one which is insecure against key recovery, but maintains IND-CPA security.

Our generic transformation proceeds in two steps. We begin with a IND-CPA encryption system that is insecure against cycle detection attacks. That is there exists a polynomial $p(\cdot)$ and an infinite set $S \subseteq \mathbb{N}$ where the advantage of the attacker is greater than $1/p(\lambda)$ for all $\lambda \in S$. We show that if such a system exists, then there exists a cryptosystem with an attacker that has advantage of $1/2 - \text{negl}(\lambda)$ for all $\lambda \in S$. (i.e. the probability of winning the game is $1 - \text{negl}(\lambda)$ for all $\lambda \in S$.) This effectively amplifies the probability of winning within that restricted set. Our amplification technique is just a simple repetition.

Next, we show how such an amplified cycle detection encryption system can be transformed into one where a key recovery attack is possible. Our approach is to create an encryption system where the encryption algorithm will go through the message M bit by bit and encode each 1 as a M and each 0 and a string of 0's. Then if there is a key cycle, the underlying cycle detection algorithm can recover the bits of M one by one using the cycle detection algorithm/attacker of the underlying scheme.

5.1 A Circular Key Recoverable Cryptosystem

Amplification We first state our amplification lemma which is proved in Appendix B.1.

Claim 1. *Let $\mathcal{PKE}'_A$ be an* IND-CPA *secure public key cryptosystem that is n-circular secure i.e. there exists a polynomial time algorithm $\mathcal{D}'$ and a polynomial $p(\cdot)$ such that for infinitely many $\lambda \in \mathbb{N}$, $Adv_{\mathcal{D}'}(\lambda) > 1/p(\lambda)$. Then there exists an* IND-CPA *secure public key cryptosystem $\mathcal{PKE}_A$, which is constructed using $\mathcal{PKE}'_A$ as a black box, for which there exists an n-circular security adversary $\mathcal{D}$ with advantage $1/2 - \text{negl}(\lambda)$ (i.e. with probability $1 - \text{negl}(\lambda)$) for all such $\lambda \in \mathbb{N}$.*

Our Transformation Let $\mathcal{PKE}_A$ be an IND-CPA encryption scheme for which there exists an n-circular security adversary $\mathcal{D}$ with $Adv_{\mathcal{D}}(\lambda) \geq 1/2 - \text{negl}(\lambda)$ for infinitely many $\lambda \in \mathbb{N}$. Let $\mathcal{M}_A = \{0,1\}^l$ be the message space. For an l-bit message M, we will let $M[i]$ denote the i-th bit of M where $i \in [l]$. We construct an IND-CPA encryption scheme $\mathcal{PKE}$ which is n-circular insecure with respect to key recovery as follows.

IND-CPA **n-Circular key recoverable** $\mathcal{PKE}$:
Inputs : IND-CPA n-Circular insecure $\mathcal{PKE}_A$.

- $\mathsf{Keygen}(1^\lambda)$: Let $(sk_A, pk_A) \leftarrow \mathsf{Keygen}_A(1^\lambda)$. Let $sk = sk_A$, $pk = pk_A$. Output (sk, pk).
- $\mathsf{Encrypt}(\mathsf{pk}, M)$:
  - Let $C_H = \mathsf{Encrypt}_A(pk, M)$.
    1. For $i = 1 \ldots l$
       Let $C_i = \mathsf{Encrypt}_A(pk, M)$ if $M[i] = 1$, else $C_i = \mathsf{Encrypt}_A(pk, 0^{|M|})$.
    2. Output $ct = (C_H, C_1, \ldots, C_l)$.
- $\mathsf{Decrypt}(\mathsf{sk}, ct)$: Compute $M \leftarrow \mathsf{Decrypt}_A(sk, C_H)$ and $M'_i \leftarrow \mathsf{Decrypt}_A(sk, C_i)$ for $i = 1, \ldots, l$. If $\forall i \in [l]$ $M'_i = M \cdot M[i]$ output M, otherwise output $\perp$.

The proof of the following claim is straightforward and is included in Appendix B.2.

Claim 2. *$\mathcal{PKE}$ is* IND-CPA *secure if $\mathcal{PKE}_A$ is* IND-CPA .

We now formally show that if the old cryptosystem $\mathcal{PKE}_A$ is n-circular insecure, the new cryptosystem $\mathcal{PKE}$ is n-circular insecure *with respect to key recovery*. We rely on the following result which is proved in Appendix B.3. Claim 3 states that any circular security adversary can be used to distinguish an encryption cycle from a modified encryption cycle in which a zero encryption has been substituted in the last position. The proof utilizes a hybrid argument.

Claim 3. *Let $\mathcal{PKE}_A$ be an* IND-CPA *public key cryptosystem. Suppose that $\mathcal{D}$ has advantage $Adv_{\mathcal{D}}(\lambda)$ in the circular security game against $\mathcal{PKE}_A$. Then $\mathcal{D}$ distinguishes the following distributions with advantage $Adv_{\mathcal{D}}(\lambda) - \text{negl}(\lambda)$.*

$$[\mathsf{pk}_1, \ldots, \mathsf{pk}_n, \mathsf{Encrypt}_A(\mathsf{pk}_1, \mathsf{sk}_2), \ldots, \mathsf{Encrypt}_A(\mathsf{pk}_{n-1}, \mathsf{sk}_n), \mathsf{Encrypt}_A(\mathsf{pk}_n, \mathsf{sk}_1) : (\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{Keygen}_A(1^\lambda)]$$

$$[\mathsf{pk}_1, \ldots, \mathsf{pk}_n, \mathsf{Encrypt}_A(\mathsf{pk}_1, \mathsf{sk}_2), \ldots, \mathsf{Encrypt}_A(\mathsf{pk}_{n-1}, \mathsf{sk}_n), \mathsf{Encrypt}_A(\mathsf{pk}_n, 0^{|\mathsf{sk}_1|}) : (\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{Keygen}_A(1^\lambda)]$$

Armed with the above claims we are now ready to prove the following lemma.

Lemma 1. *Suppose there exists an algorithm $\mathcal{D}$ with advantage $Adv_{\mathcal{D}}(\lambda) = 1/2 - \text{negl}(\lambda)$ in the n-circular security game against $\mathcal{PKE}_A$ for infinitely many $\lambda \in \mathbb{N}$. Then there exists an algorithm $\mathcal{R}$ with advantage at least $1/2 - \text{negl}(\lambda)$ in the n-circular key recovery security game against $\mathcal{PKE}$ for all such $\lambda \in \mathbb{N}$.*

Proof. Let $\mathcal{D}$ be an algorithm such with advantage in the n-circular security game against $\mathcal{PKE}_A$ at least $1/2 - \text{negl}(\lambda)$ for infinitely many $\lambda \in \mathbb{N}$. Consider the following algorithm $\mathcal{R}$ interacting with the n-circular security with respect to key recovery challenger $\mathcal{C}$:

1. $\mathcal{C}$ runs $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{Keygen}(1^\lambda)$.
2. $\mathcal{C}$ computes $y_i = \mathsf{Encrypt}(\mathsf{pk}_i, \mathsf{sk}_{(i \bmod n)+1})$ for $1 \leq i \leq n$.
3. $\mathcal{C}$ sends $(\mathsf{pk}_1, \ldots, \mathsf{pk}_n, y_1, \ldots, y_n)$ to $\mathcal{R}$.
4. $\mathcal{R}$ parses $y_i = (C_{i,H}, C_{i,1}, \ldots C_{i,l})$ for $1 \leq i \leq n$.
5. $\mathcal{R}$ for $j = 1 \ldots l$.
   (a) Forms the vector $w_j = (C_{1,H}, \ldots, C_{n-1,H}, C_{n,j})$.
   (b) Lets $\mathsf{sk}_1[j] \leftarrow \mathcal{D}(\mathsf{pk}_1, \ldots, \mathsf{pk}_n, w_j)$.
6. $\mathcal{R}$ output sk_1.

Fix any such $\lambda \in \mathbb{N}$. Note that $C_{n,j}$ is either a random encryption of sk_1 or 0. Note that $\mathcal{D}$ distinguishes an n-encryption cycle from n zero encryptions with advantage at least $1/2 - \text{negl}(\lambda)$. Thus Claim 3 implies that $\mathcal{D}$ on input $(\mathsf{pk}_1, \ldots, \mathsf{pk}_n, w_j)$ distinguishes whether $C_{n,j}$ is an encryption of sk_1 or 0 with advantage at least $Adv_{\mathcal{D}'}(\lambda) - \text{negl}(\lambda) = 1/2 - \text{negl}(\lambda)$. Thus $\mathcal{D}$ fails to recover the j-th bit of sk_1 with probability at most $\text{negl}(\lambda)$. Then $\mathcal{R}$ recovers sk_1 correctly except with probability atmost $n \cdot \text{negl}(\lambda)$, which is negligible. □

Combining Claim 1 and Lemma 1, we get the following theorem.

Theorem 3. *Suppose there exists an algorithm $\mathcal{D}$ with non-negligible advantage in the n-circular security game against $\mathcal{PKE}'_A$ for infinitely many $\lambda \in \mathbb{N}$. Then there exists an algorithm $\mathcal{R}$ with advantage at least $1/2 - \text{negl}(\lambda)$ in the n-circular key recovery security game against $\mathcal{PKE}$ for all such $\lambda \in \mathbb{N}$.*

References

[ABBC10] Tolga Acar, Mira Belenkiy, Mihir Bellare, and David Cash. Cryptographic agility and its relation to circular encryption. In *Proceedings of the 29th Annual international conference on Theory and Applications of Cryptographic Techniques*, EUROCRYPT'10, pages 403–422, Berlin, Heidelberg, 2010. Springer-Verlag.

[ABHS05] Pedro Adão, Gergei Bana, Jonathan Herzog, and Andre Scedrov. Soundness of formal encryption in the presence of key-cycles. In SabrinadeCapitani Vimercati, Paul Syverson, and Dieter Gollmann, editors, *Computer Security ESORICS 2005*, volume 3679 of *Lecture Notes in Computer Science*, pages 374–396. Springer Berlin Heidelberg, 2005.

[ACPS09] Benny Applebaum, David Cash, Chris Peikert, and Amit Sahai. Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In Shai Halevi, editor, *Advances in Cryptology - CRYPTO 2009*, volume 5677 of *Lecture Notes in Computer Science*, pages 595–618. Springer Berlin Heidelberg, 2009.

[App11] Benny Applebaum. Key-dependent message security: generic amplification and completeness. In *Proceedings of the 30th Annual international conference on Theory and applications of cryptographic techniques: advances in cryptology*, EUROCRYPT'11, pages 527–546, Berlin, Heidelberg, 2011. Springer-Verlag.

[ASP12] Jacob Alperin-Sheriff and Chris Peikert. Circular and kdm security for identity-based encryption. In Marc Fischlin, Johannes Buchmann, and Mark Manulis, editors, *Public Key Cryptography PKC 2012*, volume 7293 of *Lecture Notes in Computer Science*, pages 334–352. Springer Berlin Heidelberg, 2012.

[BG10] Zvika Brakerski and Shafi Goldwasser. Circular and leakage resilient public-key encryption under subgroup indistinguishability. In *Proceedings of the 30th annual conference on Advances in cryptology*, CRYPTO'10, pages 1–20, Berlin, Heidelberg, 2010. Springer-Verlag.

[BGI+01] Boaz Barak, Oded Goldreich, Russell Impagliazzo, Steven Rudich, Amit Sahai, Salil Vadhan, and Ke Yang. On the (im)possibility of obfuscating programs. In *Lecture Notes in Computer Science*, pages 1–18. Springer-Verlag, 2001.

[BGK11] Zvika Brakerski, Shafi Goldwasser, and Yael Tauman Kalai. Black-box circular-secure encryption beyond affine functions. In Yuval Ishai, editor, *Theory of Cryptography*, volume 6597 of *Lecture Notes in Computer Science*, pages 201–218. Springer Berlin Heidelberg, 2011.

[BHHI10] Boaz Barak, Iftach Haitner, Dennis Hofheinz, and Yuval Ishai. Bounded key-dependent message security. In Henri Gilbert, editor, *Advances in Cryptology EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 423–444. Springer Berlin Heidelberg, 2010.

[BHHO08] Dan Boneh, Shai Halevi, Mike Hamburg, and Rafail Ostrovsky. Circular-secure encryption from decision diffie-hellman. In *Proceedings of the 28th Annual conference on Cryptology: Advances in Cryptology*, CRYPTO 2008, pages 108–125, Berlin, Heidelberg, 2008. Springer-Verlag.

[BRS01] John Black, Phillip Rogaway, and Thomas Shrimpton. Encryption-scheme security in the presence of key-dependent messages. Manuscript, 2001.

[BV11] Zvika Brakerski and Vinod Vaikuntanathan. Fully homomorphic encryption from ring-lwe and security for key dependent messages. In Phillip Rogaway, editor, *Advances in Cryptology CRYPTO 2011*, volume 6841 of *Lecture Notes in Computer Science*, pages 505–524. Springer Berlin Heidelberg, 2011.

[BZ13] Dan Boneh and Mark Zhandry. Multiparty key exchange, efficient traitor tracing, and more from indistinguishability obfuscation. Cryptology ePrint Archive, Report 2013/642, 2013. `http://eprint.iacr.org/`.

[CGH12] David Cash, Matthew Green, and Susan Hohenberger. New definitions and separations for circular security. In *Proceedings of the 15th international conference on Practice and Theory in Public Key Cryptography*, PKC'12, pages 540–557, Berlin, Heidelberg, 2012. Springer-Verlag.

[CL01] Jan Camenisch and Anna Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In Birgit Pfitzmann, editor, *Advances in Cryptology EUROCRYPT 2001*, volume 2045 of *Lecture Notes in Computer Science*, pages 93–118. Springer Berlin Heidelberg, 2001.

[CLT13] Jean-Sébastien Coron, Tancrède Lepoint, and Mehdi Tibouchi. Practical multilinear maps over the integers. In *CRYPTO (1)*, pages 476–493, 2013.

[Gen09] Craig Gentry. *A fully homomorphic encryption scheme*. PhD thesis, Stanford University, 2009. `crypto.stanford.edu/craig`.

[GGH13a] Sanjam Garg, Craig Gentry, and Shai Halevi. Candidate multilinear maps from ideal lattices. In *EUROCRYPT*, pages 1–17, 2013.

[GGH+13b] Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Amit Sahai, and Brent Waters. Candidate indistinguishability obfuscation and functional encryption for all circuits. Cryptology ePrint Archive, Report 2013/451, 2013.

[GM84] Shafi Goldwasser and Silvio Micali. Probabilistic Encryption. *J. Comput. Syst. Sci.*, 28(2):270–299, 1984.

[HH09] Iftach Haitner and Thomas Holenstein. On the (im)possibility of key dependent encryption. In Omer Reingold, editor, *Theory of Cryptography*, volume 5444 of *Lecture Notes in Computer Science*, pages 202–219. Springer Berlin Heidelberg, 2009.

[Lau02] Peeter Laud. Encryption cycles and two views of cryptography. In *NORDSEC 2002 - Proceedings of the 7th Nordic Workshop on Secure IT Systems (Karlstad University Studies 2002:31*, pages 85–100, 2002.

[MTY11] Tal Malkin, Isamu Teranishi, and Moti Yung. Efficient circuit-size independent public key encryption with kdm security. In *Proceedings of the 30th Annual international conference on Theory and applications of cryptographic techniques: advances in cryptology*, EUROCRYPT'11, pages 507–526, Berlin, Heidelberg, 2011. Springer-Verlag.

[Rot13] Ron Rothblum. On the circular security of bit-encryption. In *TCC*, pages 579–598, 2013.

[SW13] Amit Sahai and Brent Waters. How to use indistinguishability obfuscation: Deniable encryption, and more. Cryptology ePrint Archive, Report 2013/454, 2013.

A Counter Example for 1-Circular Security of Bit-by-bit Encryption

Proposition 6. Suppose that there exists a polynomial time adversary $\mathcal{A}$ such that $Game_0Adv_{\mathcal{A}}$ - $Game_1Adv_{\mathcal{A}}$ $= \epsilon$. Then there exists a polynomial time adversary $\mathcal{B}$ who distinguishes the output of G from random with advantage $\epsilon_{PRG} = \epsilon$.

Proof. In Game 0, t is an output of G, while in Game 1, t is a truly random $2l$-bit string. The algorithm $\mathcal{B}$ is defined as follows :

1. $\mathcal{B}$ receives $t \in \{0,1\}^{2l}$ from PRG Challenger $\mathcal{C}$, where t is either a pseudorandom string generated by G or a truly random string.
2. $\mathcal{B}$ computes $(\mathsf{pk}_A, \mathsf{sk}_A) \leftarrow \mathsf{Keygen}_A(1^\lambda)$. Next, it computes $O = i\mathcal{O}(\lambda, \mathsf{BitCycleFind})$ as described in Game 0. It sets $\mathsf{pk} = (\mathsf{pk}_A, t, O)$ and sends it to $\mathcal{A}$.
3. $\mathcal{B}$ chooses $b \xleftarrow{\$} \{0,1\}$. It sets $ct_b \leftarrow \mathsf{Encrypt}_A(\mathsf{pk}_A, b)$ and sends it to $\mathcal{A}$.
4. $\mathcal{A}$ outputs a bit b'. If $(b = b')$ $\mathcal{B}$ outputs that t was pseudorandom. Else $\mathcal{B}$ outputs that t was random.

Clearly, as shown in Proposition 2, if $\mathcal{A}$ wins the game with non negligible probability, then so does $\mathcal{B}$. □

Proposition 7. Suppose that there exists a polynomial time adversary $\mathcal{A}$ such that $Game_1Adv_{\mathcal{A}}$ - $Game_2Adv_{\mathcal{A}}$ $= \epsilon$. Then there exists a polynomial time adversary $\mathcal{B}$ who breaks the indistinguishability obfuscation with advantage $\epsilon_{iO} = \epsilon$.

Proof. $\mathcal{B}$ comprises a pair of adversaries $(Samp, D)$ as in Definition 7. We construct these adversaries as follows.
$Samp(1^\lambda)$:

1. Choose $r \xleftarrow{\$} \{0,1\}^l$ and $t \xleftarrow{\$} \{0,1\}^{2l}$.
2. Let $(\mathsf{sk}_A, \mathsf{pk}_A) \leftarrow \mathsf{Keygen}_A(1^\lambda)$.
3. Let $\mathsf{BitCycleFind}$ be the circuit described in our construction with constants $(\mathsf{sk}_A, t, 0^w)$ hardwired and $\mathsf{BitCycleReject}$ be the circuit described in Game 2 with constant $0^{w'}$ hardwired.
4. Output $(g_0 = \mathsf{BitCycleFind}, g_1 = \mathsf{BitCycleReject})$.
5. Set $\sigma = (\mathsf{pk}_A, t)$.

$D(\sigma, i\mathcal{O}(\lambda, g_z))$:

1. Parse $\sigma = (\mathsf{pk}_A, t)$. Set $\mathsf{pk} = (\mathsf{pk}_A, t, i\mathcal{O}(\lambda, g_z))$
2. Let $b \xleftarrow{\$} \{0,1\}$. $ct \leftarrow \mathsf{Encrypt}_A(\mathsf{pk}_A, b)$.
3. Let $b' \leftarrow \mathcal{A}(\mathsf{pk}, ct)$.
4. D guesses 1 if $b = b'$.

Note that since t is chosen uniformly at random, except with negligible probability, t is not in the range of G. Hence $\mathsf{BitCycleFind}(x)$ outputs $\perp$ for all x. Thus $Samp$ produces circuits $\mathsf{BitCycleReject}$ and $\mathsf{BitCycleFind}$ which are equivalent on all inputs with overwhelming probability, by the random choice of t.

Similar to the proof for Proposition 3, we can argue that if $\mathcal{A}$ distinguishes between the outputs of Game 1 and Game 2 with advantage ϵ, then $\mathcal{B}$ breaks the indistinguishability obfuscation with advantage ϵ. □

Proposition 8. If there exists a polynomial time adversary $\mathcal{A}$ with non-negligible advantage ϵ in Game 2, then there exists a polynomial time algorithm $\mathcal{B}$ that can break the $\mathsf{IND\text{-}CPA}$ security of $\mathcal{PKE}_A$ with advantage $\epsilon_A = \epsilon$.

Proof. Suppose $\mathcal{A}$ has advantage ϵ in Game 2. We define $\mathcal{B}$ as follows :

1. $\mathcal{B}$ receives pk_A, ct from the $\mathsf{IND\text{-}CPA}$ Challenger $\mathcal{C}$. It chooses $t \xleftarrow{\$} \{0,1\}^{2l}$ and computes $O \leftarrow i\mathcal{O}(\lambda, \mathsf{BitCycleReject})$. It sends public key $\mathsf{pk} = (\mathsf{pk}_A, t, O)$ and ciphertext ct to $\mathcal{A}$.
2. $\mathcal{A}$ sends bit b', which $\mathcal{B}$ passes on to $\mathcal{C}$.

Note that if $\mathcal{A}$ wins Game 2, then $\mathcal{B}$ wins the $\mathsf{IND\text{-}CPA}$ game. Hence the result follows. □

B Key Recovery From Circular Insecurity

B.1

Claim 1. Let $\mathcal{PKE}'_A$ be an $\mathsf{IND\text{-}CPA}$ secure public key cryptosystem that is n-circular secure i.e. there exists a polynomial time algorithm $\mathcal{D}'$ and a polynomial $p(\cdot)$ such that for infinitely many $\lambda \in \mathbb{N}$, $Adv_{\mathcal{D}'}(\lambda) > 1/p(\lambda)$. Then there exists an $\mathsf{IND\text{-}CPA}$ secure public key cryptosystem $\mathcal{PKE}_A$, which is constructed using $\mathcal{PKE}'_A$ as a black box, for which there exists an n-circular security adversary $\mathcal{D}$ with advantage $1/2 - \mathrm{negl}(\lambda)$ (i.e. with probability $1 - \mathrm{negl}(\lambda)$) for all such $\lambda \in \mathbb{N}$.

Proof. Let $\mathcal{PKE}'_A = (\mathsf{Keygen}'_A, \mathsf{Encrypt}'_A, \mathsf{Decrypt}'_A)$. Let $t(\lambda) = \lambda \cdot p(\lambda)^2$ be the amplification factor. We now define $\mathcal{PKE}_A = (\mathsf{Keygen}_A, \mathsf{Encrypt}_A, \mathsf{Decrypt}_A)$ as follows.

- $\mathsf{Keygen}_A(1^\lambda)$: Compute t public key, secret key pairs. $(\mathsf{pk}_i, \mathsf{sk}_i) \xleftarrow{\$} \mathsf{Keygen}'_A(1^\lambda)$ for $1 \le i \le t$. The public key $\mathsf{pk} = (\mathsf{pk}_1, \ldots, \mathsf{pk}_t)$ and the secret key is $(\mathsf{sk}_1, \ldots, \mathsf{sk}_t)$.
- $\mathsf{Encrypt}_A(\mathsf{pk}, m)$: Parse $\mathsf{pk} = (\mathsf{pk}_1, \ldots, \mathsf{pk}_t)$ and $m = (m_1, \ldots, m_t)$ such that $|m_i| = |m_j|$ for all i, j. Compute t ciphertexts $ct_1, \ldots, ct_t$, where $ct_i \xleftarrow{\$} \mathsf{Encrypt}'_A(\mathsf{pk}_i, m_i)$. The ciphertext $ct = (ct_1, \ldots, ct_t)$.

- $\mathsf{Decrypt}_A(\mathsf{sk}, ct)$: Parse $\mathsf{sk} = (\mathsf{sk}_1, \ldots, \mathsf{sk}_t)$ and $ct = (ct_1, \ldots, ct_t)$. Output $\mathsf{Decrypt}'_A(\mathsf{sk}_1, ct_1)$.

IND-CPA security of $\mathcal{PKE}_A$ follows from hybrid argument. We need to show that there exists an algorithm $\mathcal{D}$ such that for infinitely many λ, $Adv_{\mathcal{D}}(\lambda) > 1/2 - \text{negl}(\lambda)$ in the n-circular security game. Note that each ciphertext ct_i consists of t ciphertexts $(ct_{i1}, \ldots, ct_{it})$, and for all $1 \leq j \leq t$, either $(ct_{1j}, \ldots, ct_{nj})$ is an encryption cycle or an encryption of zeroes. By construction, it follows that each of these cycles is independent, since we have t independent invocations of Keygen'_A during Keygen_A.

$\mathcal{D}$ is defined as follows :

$\mathcal{D}'$:

1. For $1 \leq i \leq t$, compute $d_i \xleftarrow{\$} \mathcal{D}'(ct_{1i}, \ldots, ct_{ni})$
2. Output majority of $\{d_1, \ldots, d_t\}$.

If we have an encryption cycle, then, for each $1 \leq j \leq t$, we have $\Pr[\mathcal{D}'(ct_{1i}, \ldots, ct_{ni}) = 1] > 1/2 + 1/p(\lambda)$. Since we have $t = \lambda \cdot p(\lambda)^2$ invocations, using Chernoff bounds, it follows that $\Pr[\mathcal{D}(ct_1, \ldots, ct_n) = 1] > 1 - \text{negl}(\lambda)$.
Similarly, if we have encryptions of zeroes, then for each $1 \leq j \leq t$, $\Pr[\mathcal{D}'(ct_{1i}, \ldots, ct_{ni}) = 1] < 1/2 - 1/p(\lambda)$. Using Chernoff bounds, we get that $\Pr[\mathcal{D}(ct_1, \ldots, ct_n) = 1] < \text{negl}(\lambda)$. □

B.2

Claim 2. $\mathcal{PKE}$ is IND-CPA secure if $\mathcal{PKE}_A$ is IND-CPA .

Proof. To prove this claim it will be convenient to define $C_0 =: C_H$ and $M[0] =: 1$. Suppose that adversary $\mathcal{A}$ has advantage $\epsilon(\lambda)$ in the IND-CPA game against $\mathcal{PKE}$. We construct an adversary $\mathcal{B}$ which has advantage $\epsilon(\lambda)/(l+1)$ in the IND-CPA game against $\mathcal{PKE}_A$.

1. $\mathcal{B}$ receives pk_A from the challenger and forwards it to $\mathcal{A}$.
2. $\mathcal{A}$ makes some ciphertext queries to $\mathsf{Encrypt}$ which are answered using $\mathsf{Encrypt}_A$.
3. $\mathcal{B}$ receives two l-bit message M_0, M_1 from $\mathcal{A}$.
4. $\mathcal{B}$ chooses $i^* \xleftarrow{\$} \{0, \ldots, l\}$ and forms $M'_0 = M_0 \cdot M_0[i^*]$ and $M'_1 = M_1 \cdot M_1[i^*]$. If $M'_0 = M'_1$ it aborts, otherwise it sends M'_0 and M'_1 to the challenger.
5. $\mathcal{B}$ receives $ct'_b = \mathsf{Encrypt}_A(M'_b)$ from the challenger.
6. $\mathcal{B}$ forms the ciphertext $ct = (C_0, \ldots C_l)$ where

$$C_i = \begin{cases} \mathsf{Encrypt}_A(pk, M_0 \cdot M_0[i]) & : i < i^* \\ ct'_b & : i = i^* \\ \mathsf{Encrypt}_A(pk, M_1 \cdot M_1[i]) & : i > i^* \end{cases}$$

   and forwards ct to $\mathcal{A}$.
7. $\mathcal{B}$ receives bit z from $\mathcal{A}$.
8. Step 2 may be repeated.
9. $\mathcal{B}$ sends guess $b' = z$ to the challenger.

Define for $i = 0 \ldots l$, $p_i = \Pr[b' = 0 | i^* = i, b = 0]$ and $q_i = \Pr[b' = 0 | i^* = i, b = 1]$. Since $\mathcal{A}$ has advantage ϵ in the IND-CPA game against $\mathcal{PKE}$, we have $\epsilon = 1/2 \cdot (p_l - q_0)$. By inspection $p_{i-1} = q_i$ hence $\epsilon = 1/2 \cdot (\sum_{i=0}^{l} (p_i - q_i))$. Then $\epsilon = 1/2 \cdot (\sum_{i=0}^{l} p_i - \sum_{i=0}^{l} q_i) = 1/2 \cdot (\Pr[b' = 0 | b = 0] - \Pr[b' = 0 | b = 1]) \cdot (l+1) = Adv_{\mathcal{B}} \cdot (l+1)$. Thus $\mathcal{B}$ has advantage $\epsilon/(l+1)$ which is non-negligible if ϵ is non-negligible. □

B.3

Claim 3. Let $\mathcal{PKE}_A$ be an IND-CPA public key cryptosystem. Suppose that $\mathcal{D}$ has advantage $Adv_{\mathcal{D}}(\lambda)$ in the circular security game against $\mathcal{PKE}_A$. Then $\mathcal{D}$ distinguishes the following distributions with advantage

$Adv_{\mathcal{D}}(\lambda) - \text{negl}(\lambda)$.

$$[\mathsf{pk}_1, \ldots, \mathsf{pk}_n, \mathsf{Encrypt}_A(\mathsf{pk}_1, \mathsf{sk}_2), \ldots, \mathsf{Encrypt}_A(\mathsf{pk}_{n-1}, \mathsf{sk}_n), \mathsf{Encrypt}_A(\mathsf{pk}_n, \mathsf{sk}_1) : (\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{Keygen}_A(1^\lambda)]$$
$$[\mathsf{pk}_1, \ldots, \mathsf{pk}_n, \mathsf{Encrypt}_A(\mathsf{pk}_1, \mathsf{sk}_2), \ldots, \mathsf{Encrypt}_A(\mathsf{pk}_{n-1}, \mathsf{sk}_n), \mathsf{Encrypt}_A(\mathsf{pk}_n, 0^{|\mathsf{sk}_1|}) : (\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{Keygen}_A(1^\lambda)]$$

Proof. In order to prove this result, we define n intermediate hybrid experiments $H_j : 1 \leq j \leq n$, and show that $\mathcal{D}$ has overwhelming advantage in each of the hybrids. Hybrid H_j is defined as follows :

H_j :

1. $\mathcal{C}$ computes $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{Keygen}_\mathsf{A}(1^\lambda)$ for $1 \leq i \leq n$
2. $\mathcal{C}$ chooses a bit $b \xleftarrow{\$} \{0, 1\}$.
   - If $b = 0$, $\mathcal{C}$ computes $y_i = \mathsf{Encrypt}_\mathsf{A}(\mathsf{pk}_i, \mathsf{sk}_{(i \bmod n)+1})$ for $1 \leq i \leq n$
   - Else $\mathcal{C}$ computes $y_i = \mathsf{Encrypt}_\mathsf{A}(\mathsf{pk}_i, \mathsf{sk}_{(i \bmod n)+1})$ for $i < j$ and $y_i = \mathsf{Encrypt}_\mathsf{A}(\mathsf{pk}_i, 0^{|\mathsf{sk}_{(i \bmod n)+1}|})$ for $i \geq j$
3. $\mathcal{C}$ sends $(\mathsf{pk}_1, \ldots, \mathsf{pk}_n, y_1, \ldots, y_n)$ to $\mathcal{D}$.
4. $\mathcal{D}$ outputs b'.

H_1 corresponds to the n-circular security game, while H_n corresponds to the case where an encryption cycle might be modified by substituting a zero encryption in the last position. Let $Adv_{\mathcal{D}}(H_j)$ denote the advantage of $\mathcal{D}$ in hybrid experiment H_j. Suppose $Adv_{\mathcal{D}}(H_j) - Adv_{\mathcal{D}}(H_{j+1})$ is non-negligible. Then there exists a polynomial time adversary $\mathcal{A}$ that can break the IND-CPA security of $\mathcal{PKE}$ using $\mathcal{D}$.

1. $\mathcal{A}$ receives public key pk from the IND-CPA challenger $\mathcal{C}$.
2. A generates $n-1$ public key, secret key pairs $(\mathsf{pk}_i, \mathsf{sk}_i) \xleftarrow{\$} \mathsf{Keygen}(1^\lambda)$ for $2 \leq i \leq n$.
3. A sends $\mathsf{sk}_{j+1}, 0^{|sk_{j+1}|}$ as challenge messages to $\mathcal{C}$ and receives ct as the ciphertext.
4. $\mathcal{A}$ computes the remaining $n-1$ ciphertexts $(ct_1, \ldots, ct_{j-1}, ct_{j+1}, \ldots, ct_n)$ as in the hybrids, and then runs $\mathcal{D}$ on this input.
5. Depending on the output of $\mathcal{D}$, A sends its guess to $\mathcal{C}$.

Note that the advantage of $\mathcal{A}$ is equal to $Adv_{\mathcal{D}}(H_j) - Adv_{\mathcal{D}}(H_{j+1})$. We have $Adv_{\mathcal{D}}(H_1) = \epsilon$. Therefore, the advantages of $\mathcal{D}$ in each of the successive hybrids is $\epsilon - \text{negl}(\lambda)$, and in particular, its advantage in H_n is $\epsilon - \text{negl}(\lambda)$. □