

# New Definitions and Separations for Circular Security

David Cash<sup>1,\*</sup>, Matthew Green<sup>2,\*\*</sup>, and Susan Hohenberger<sup>2,\*\*\*</sup>

<sup>1</sup> IBM T.J. Watson Research Center

<sup>2</sup> Johns Hopkins University

**Abstract.** Traditional definitions of encryption security guarantee secrecy for any plaintext that can be computed by an outside adversary. In some settings, such as anonymous credential or disk encryption systems, this is not enough, because these applications encrypt messages that depend on the secret key. A natural question to ask is do standard definitions capture these scenarios? One area of interest is *n-circular security* where the ciphertexts  $E(pk_1, sk_2), E(pk_2, sk_3), \dots, E(pk_{n-1}, sk_n), E(pk_n, sk_1)$  must be indistinguishable from encryptions of zero. Acar et al. (Eurocrypt 2010) provided a CPA-secure public key cryptosystem that is not 2-circular secure due to a distinguishing attack.

In this work, we consider a natural relaxation of this definition. Informally, a cryptosystem is *n-weak circular secure* if an adversary given the cycle  $E(pk_1, sk_2), E(pk_2, sk_3), \dots, E(pk_{n-1}, sk_n), E(pk_n, sk_1)$  has no significant advantage in the regular security game, (e.g., CPA or CCA) where ciphertexts of chosen messages must be distinguished from ciphertexts of zero. Since this definition is sufficient for some practical applications and the Acar et al. counterexample no longer applies, the hope is that it would be easier to realize, or perhaps even implied by standard definitions. We show that this is unfortunately not the case: even this weaker notion is not implied by standard definitions. Specifically, we show:

- For symmetric encryption, under the minimal assumption that one-way functions exist, *n-weak circular (CPA) security* is not implied by CCA security, for any *n*. In fact, it is not even implied by authenticated encryption security, where ciphertext integrity is guaranteed.

---

\* This work was performed at the University of California, San Diego, supported in part by NSF grant CCF-0915675.

\*\* Supported in part by the Defense Advanced Research Projects Agency (DARPA) and the Air Force Research Laboratory (AFRL) under contract FA8750-11-2-0211, the Office of Naval Research under contract N00014-11-1-0470, NSF grant CNS-1010928 and HHS 90TR0003/01. Its contents are solely the responsibility of the authors and do not necessarily represent the official views of the HHS.

\*\*\* Supported in part by the Defense Advanced Research Projects Agency (DARPA) and the Air Force Research Laboratory (AFRL) under contract FA8750-11-2-0211, the Office of Naval Research under contract N00014-11-1-0470, NSF grant CNS 1154035, a Microsoft Faculty Fellowship and a Google Faculty Research Award. Applying to all authors, the views expressed are those of the authors and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

- For public-key encryption, under a number-theoretic assumption, 2-weak circular security is not implied by CCA security.

In both of these results, which also apply to the stronger circular security definition, *we actually show for the first time an attack in which the adversary can recover the secret key of an otherwise-secure encryption scheme after an encrypted key cycle is published.* These negative results are an important step in answering deep questions about which attacks are prevented by commonly-used definitions and systems of encryption. They say to practitioners: if key cycles may arise in your system, then even if you use CCA-secure encryption, your system may break catastrophically; that is, a passive adversary might be able to recover your secret keys.

**Keywords:** Encryption, Definitions, Circular Security, Counterexamples.

## 1 Introduction

Encryption is one of the most fundamental cryptographic primitives. Most definitions of encryption security [22,19,35] follow the seminal notion of Goldwasser and Micali which guarantees indistinguishability of encryptions for messages chosen by the adversary [22]. However, Goldwasser and Micali wisely warned to be careful when using a system proven secure within this framework on messages that the adversary cannot derive himself.

Over the past several years, there has been significant interest in designing schemes secure against *key-dependent message attacks*, e.g., [15,11,31,3,27,29,13,14,5,2], where the system must remain secure even when the adversary is allowed to obtain encryptions of messages that depend on the secret keys themselves. In this work, we are particularly interested in circular security [15]. A public-key cryptosystem is *n-circular secure* if the ciphertexts  $E(pk_1, sk_2), E(pk_2, sk_3), \dots, E(pk_{n-1}, sk_n), E(pk_n, sk_1)$ , as well as ciphertexts of chosen messages, cannot be distinguished from encryptions of zero, for independent key pairs. Either by design or accident, these key cycles naturally arise in many applications, including storage systems such as BitLocker [13], anonymous credentials [15], the study of “axiomatic security” [31,3] and more. See [13] for a discussion of the applications.

Until recently, few positive or negative results regarding circular security were known outside of the random oracle model. On one hand, no *n-circular secure* cryptosystems were known for  $n > 1$ . On the other hand, no counterexamples existed for  $n > 1$  to separate the definitions of circular and CPA security; that is, as far as anyone knew the CPA-security definition already captured circular security for any cycle larger than a self-loop.

Recently, this gap has been closing in two ways. On the positive side, several circular-secure schemes have been proposed [13,5,14]. The focus of the current work is on negative results – namely, investigating whether standard notions of encryption are “safe” for circular applications.

In 2008, Boneh, Halevi, Hamburg and Ostrovsky proved, by counterexample, that *one-way* security does not imply circular security [13]. Recently, Acar, Benliky, Bellare and Cash [2] proved that, under an assumption in bilinear groups, CPA-security does not imply circular security.

*Our Results.* We narrow this gap even further by studying the extent to which standard definitions (e.g., CPA, CCA) imply a *weak* form of circular security. Our results are primarily negative.

*1. Relaxing the Circular Security Notion.* Perhaps the current formulation of circular security is “too strong”; that is, perhaps there is a relaxed notion of this definition which simultaneously satisfies many practical applications and yet is also *already* captured by standard security notions. This is an area worth investigating. We begin by proposing a natural relaxation called *weak circular security* where the adversary is handed an encrypted cycle  $E(pk_1, sk_2), E(pk_2, sk_3), \dots, E(pk_{n-1}, sk_n), E(pk_n, sk_1)$  along with the public keys and then proceeds to play the CPA or CCA security game as normal (where these ciphertexts are also off-limits for the decryption oracle). We stress here that the encrypted cycle is *always* generated as described, and is never changed to encryptions of zero. This definition is intriguing, and perhaps of independent interest, for two reasons.

First, the Acar et al. [2] counterexample does *not* apply to it. That construction uses the bilinear map to test whether a sequence of ciphertexts contain a cycle or zeros. Here the adversary knows he’s getting an encrypted cycle, but then must extract some knowledge from this that helps him distinguish two messages of his choosing.

Second, this definition appears sufficient for some practical settings. Using a weak circular secure encryption scheme, Alice and Bob could exchange keys with each other over an insecure channel knowing that: (1) Eve can detect that they did so, but (2) Eve cannot learn anything about their other messages. Similarly, an adversary scanning over a user’s BitLocker storage may detect that her drive contains an encrypted cycle, but cannot read anything on her drive. In an anonymous credential system of Camenisch and Lysyanskaya [15], a user has multiple keys. To participate in the system, the user must encrypt them in a cycle, provide this cycle to the other users, and prove that she has done this correctly. Then, if she shares one key, she automatically shares all her keys. In their application, *detection* of a cycle is actually desirable, provided that subsequent encryptions remain secure.

*2. Symmetric-Key Counterexamples.* In the symmetric setting, we show that standard notions do not imply  $n$ -circular security for any positive  $n$ . Specifically, given any  $n \geq 1$ , we show how to construct a secure authenticated encryption scheme (which is necessarily CCA-secure; see Section 2) that is not  $n$ -weak circular secure, under the minimal assumption that secure authenticated encryption schemes exist, which are equivalent to one-way functions.

The main technical ingredient in our counterexample is a lemma showing that it is provably hard for an adversary to compute an encrypted key cycle itself,

assuming that the symmetric scheme under attack is a secure authenticated encryption scheme (or CCA secure). We stress that this lemma does not hold if the encryption scheme is only CPA secure.

Our lemma gives us leverage in constructing a counterexample because it means the adversary is given strictly more power in the weak circular security game than in the standard security game. Specifically, the adversary is given an encrypted key cycle in the weak circular security game that it could not have computed itself, and we design a scheme to help such an adversary without affecting regular security.

*3. Public-Key Counterexamples.* We show that neither CPA nor CCA-security imply (even) weak circular security for cycles of size 2. That is, we show secure systems that are totally compromised when the independently-generated ciphertexts  $E(pk_A, sk_B)$  and  $E(pk_B, sk_A)$  are released. This is a difficult task, because the system must remain secure if either one, but only one, of these ciphertexts are released. Moreover, this counterexample requires new ideas. We cannot use the common trick in self-loop counterexamples that test if the message is the secret key corresponding to the public key, since there is no way for the encryption algorithm with public key  $pk_A$  to distinguish, say,  $sk_B$  from any other valid message. Specifically, we show that:

If there exists an algebraic setting where the Symmetric External Diffie-Hellman<sup>1</sup> (SXDH) assumption holds, then there exists a CPA-secure cryptosystem which is *not* 2-weak circular secure. The proposed scheme is particularly interesting in that it breaks *catastrophically* in the presence of a 2-cycle — revealing the secret keys of both users.

Moreover, if simulation-sound non-interactive zero-knowledge (NIZK) proof systems exist for NP and there exists an algebraic setting where the Symmetric External Diffie-Hellman (SXDH) assumption holds, then there exists a CCA-secure cryptosystem which is *not* 2-weak circular secure. This is also the first separation of CCA security and (regular) circular security.

These results deepen our understanding of how to define “secure” encryption and which practical attacks are captured by the standard definitions. They also provide additional justification for the ongoing effort, e.g. [13,14,5], to develop cryptosystems which are provably circular secure.

## 1.1 Related Work

In 2001, Camenisch and Lysyanskaya [15] introduced the notion of *circular security* and used it in their anonymous credential system to discourage users from delegating their secret keys. They also showed how to construct a circular-secure cryptosystem from any CPA-secure cryptosystem in the random oracle model.

<sup>1</sup> The SXDH assumption states that there is a bilinear setting  $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$  where the DDH assumption holds in both  $\mathbb{G}_1$  and  $\mathbb{G}_2$ . It has been extensively studied and used e.g., [21,38,32,12,8,6,24,9,25], perhaps most notably as a setting of the Groth-Sahai NIZK proof system [25].

Independently, Abadi and Rogaway [1] and Black, Rogaway, Shrimpton [11] introduced the more general notion of *key-dependent message* (KDM) security, where the encrypted messages might depend on an arbitrary function of the secret keys. Black et al. showed how to realize this notion in the random oracle model.

Halevi and Krawczyk [27] extended the work of Black et al. to look at KDM security for deterministic secret-key functions such as pseudorandom functions (PRFs), tweakable blockciphers, and more. They give both positive and negative results, including some KDM-secure constructions in the standard model for PRFs. In the symmetric setting, Hofheinz and Unruh [29] showed how to construct circular-secure cryptosystems in the standard model under relaxed notions of security. Backes, Pfitzmann and Scedrov [7] presented stronger notions of KDM security (some in the random oracle model) and discussed the relationships among these notions.

In the public-key setting, Boneh, Halevi, Hamburg and Ostrovsky [13] presented the first cryptosystem which is simultaneously CPA-secure and  $n$ -circular-secure (for any  $n$ ) in the standard model, based on either the DDH or Decision Linear assumptions. As mentioned earlier, Boneh et al. [13] also proved, by counterexample, that *one-way* security does not imply circular security. One-way encryption is a very weak notion, which informally states that given  $(pk, E(pk, m))$ , the adversary should not be able to recover  $m$ . Given any one-way encryption system, they constructed a one-way encryption system that is not  $n$ -circular secure (for any  $n$ ). Their system generates two key pairs from the original and sets  $PK = pk_1$  and  $SK = (sk_1, sk_2)$ . A message  $(m_1, m_2)$  is encrypted as  $(m_1, E(pk_1, m_2))$ . In the event of a 2-cycle, the values  $\text{Enc}(pk_A, sk_B) = (sk_{B,1}, E(pk_{A,1}, sk_{B,2}))$  and  $\text{Enc}(pk_B, sk_A) = (sk_{A,1}, E(pk_{B,1}, sk_{A,2}))$  provide the critical secret key information  $(sk_{B,1}, sk_{A,1})$  in the clear.

Subsequently, Applebaum, Cash, Peikert and Sahai [5] adapted the circular-secure construction of [13] into the lattice setting. Camenisch, Chandran and Shoup [14] extended [13] to the first cryptosystem which is simultaneously CCA-secure and  $n$ -circular-secure (for any  $n$ ) in the standard model, by applying the “double encryption” paradigm of Naor and Yung [34]. (Interestingly, we use this same approach in Section 4.4 to extend our public-key counterexample from CPA to CCA security.)

Haitner and Holenstein [26] recently provided strong impossibility results for KDM-security *with respect to 1-key cycles* (a.k.a., self-loops.) They study the problem of building an encryption scheme where it is secure to release  $E(k, g(k))$  for various functions  $g$ . First, they show that there exists no fully-black-box reduction from a KDM-secure encryption scheme to one-way permutations (or even some families of trapdoor permutations) if the adversary can obtain encryptions of  $g(k)$ , where  $g$  is a poly( $n$ )-wise independent hash function. Second, there exists no reduction from an encryption scheme secure against key-dependent messages to, essentially, any cryptographic assumption, if the adversary can obtain an encryption of  $g(k)$  for an *arbitrary*  $g$ , as long as the security reduction treats both the adversary and the function  $g$  as black boxes. These results address

the possibility of achieving strong single-user KDM-security via reductions to cryptographic assumptions. The results in this paper study a version of KDM security that is in one sense weaker – we only allow a narrow class of functions  $g$  – but also stronger because it considers multiple users. Our results also address a different question regarding KDM security. We study whether or not KDM security is always implied by regular security while Haitner and Holenstein study the possibility of achieving strong single-user KDM security via specialized constructions.

Recently, Acar et al. [2] demonstrated both public and private key encryption systems that are provably CPA-secure and yet also demonstrably *not* 2-circular secure. Their counterexample does not apply to CCA or weak circular security.

There is also a relationship to recent work on *leakage resilient* and *auxiliary input* models of encryption, which mostly falls into the “self-loop” category. In leakage resilient models, such as those of Akavia, Goldwasser and Vaikuntanathan [4] and Naor and Segev [33], the adversary is given some function  $h$  of the secret key, not necessarily an encryption, such that it is *information theoretically* impossible to recover  $sk$ . The auxiliary input model, introduced by Dodis, Kalai and Lovett [18], relaxes this requirement so that it only needs to be difficult to recover  $sk$ .

*Self-Loops.* In sharp contrast to all  $n \geq 2$ , the case of 1-circular security is fairly well understood. A folklore counterexample shows that CPA-security does not directly imply 1-circular security. Given any encryption scheme  $(G, E, D)$ , one can build a second scheme  $(G, E', D')$  as follows: (1)  $E'(pk, m)$  outputs  $E(pk, m)||0$  if  $m \neq sk$  and  $m||1$  otherwise, (2)  $D'(sk, c||b)$  outputs  $D(sk, m)$  if  $b = 0$  and  $sk$  otherwise. It is easy to show that if  $(G, E, D)$  is CPA-secure, then  $(G, E', D')$  is CPA-secure. When  $E'(pk, sk) = sk||1$  is exposed, then there is a complete break. Conversely, given any CPA-secure system, one can build a 1-circular secure scheme in the standard model [13].

## 2 Definitions of Security

A *public-key encryption system*  $\Pi$  is a tuple of algorithms  $(\text{KeyGen}, \text{Enc}, \text{Dec})$ , where  $\text{KeyGen}$  is a key-generation algorithm that takes as input a security parameter  $\lambda$  and outputs a public/secret key pair  $(pk, sk)$ ;  $\text{Enc}(pk, m)$  encrypts a message  $m$  under public key  $pk$ ; and  $\text{Dec}(sk, c)$  decrypts ciphertext  $c$  with secret key  $sk$ . A *symmetric-key encryption system* is a public-key encryption system, except that it always outputs  $pk = \perp$ , and the encryption algorithm computes ciphertexts using  $sk$ , i.e. by running  $\text{Enc}(sk, m)$ . In the symmetric case we will sometimes write  $K$  instead of  $sk$ . As in most other works, we assume that all algorithms implicitly have access to shared public parameters establishing a common algebraic setting.

Our definitions of security will associate a message space, denoted  $M$ , with each encryption scheme. Throughout this paper, we assume that the space of possible secret keys output by  $\text{KeyGen}$  is a subset of the message space  $M$  and

$\text{IND-CPA}(\Pi, \mathcal{A}, \lambda)$ $b \xleftarrow{r} \{0, 1\}$ $(pk, sk) \leftarrow \text{KeyGen}(1^\lambda)$ $(m_0, m_1, z) \leftarrow \mathcal{A}_1(pk)$ $y \leftarrow \text{Enc}(pk, m_b)$ $\hat{b} \leftarrow \mathcal{A}_2(y, z)$ $\text{Output } (\hat{b} \stackrel{?}{=} b)$	$\text{AE}(\Pi, \mathcal{A}, \lambda)$ $b \xleftarrow{r} \{0, 1\}$ $K \leftarrow \text{KeyGen}(1^\lambda)$ $\hat{b} \leftarrow \mathcal{A}^{\mathcal{E}_{K,b}^{\text{ae}}, \mathcal{D}_{K,b}^{\text{ae}}}(\cdot)(1^\lambda)$ $\text{Output } (\hat{b} \stackrel{?}{=} b).$
--	--

**Fig. 1.** Experiments for Definitions 1 and 3

thus any secret key can be encrypted using any public key. For symmetric encryption schemes we will always have  $M \subset \{0, 1\}^*$ .

By  $\nu(k)$  we denote some *negligible* function, i.e., one such that, for all  $c > 0$  and all sufficiently large  $k$ ,  $\nu(k) < 1/k^c$ . We abbreviate probabilistic polynomial time as PPT.

### 2.1 Standard Security Definitions

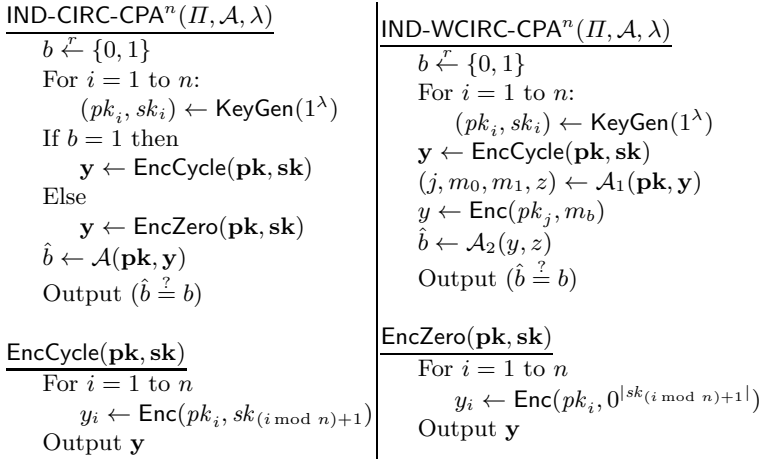
*Public-key encryption.* We recall the standard notion of indistinguishability of encryptions under a chosen-plaintext attack due to Goldwasser and Micali [22].

**Definition 1 (IND-CPA).** Let  $\Pi = (\text{KeyGen}, \text{Enc}, \text{Dec})$  be a public-key encryption scheme for the message space  $M$ . For  $b \in \{0, 1\}$ ,  $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$  and  $\lambda \in \mathbb{N}$ , let the random variable  $\text{IND-CPA}(\Pi, \mathcal{A}, \lambda)$  be defined by the probabilistic algorithm described on the left side of Figure 1. We denote the IND-CPA advantage of  $\mathcal{A}$  by  $\text{Adv}_{\Pi, \mathcal{A}}^{\text{cpa}}(\lambda) = 2 \cdot \Pr[\text{IND-CPA}(\Pi, \mathcal{A}, \lambda) = 1] - 1$ . We say that  $\Pi$  is IND-CPA secure if  $\text{Adv}_{\Pi, \mathcal{A}}^{\text{cpa}}(\lambda)$  is negligible for all PPT  $\mathcal{A}$ .

We also consider the indistinguishability of encryptions under chosen-ciphertext attacks [34,35,19].

**Definition 2 (IND-CCA).** Let  $\Pi = (\text{KeyGen}, \text{Enc}, \text{Dec})$  be a public-key encryption scheme for the message space  $M$ . Let the random variable  $\text{IND-CCA}(\Pi, \mathcal{A}, \lambda)$  be defined by an algorithm identical to  $\text{IND-CPA}(\Pi, \mathcal{A}, \lambda)$  above, except that both  $\mathcal{A}_1$  and  $\mathcal{A}_2$  have access to an oracle  $\text{Dec}(sk, \cdot)$  that returns the output of the decryption algorithm and  $\mathcal{A}_2$  cannot query this oracle on input  $y$ . We denote the IND-CCA advantage of  $\mathcal{A}$  by  $\text{Adv}_{\Pi, \mathcal{A}}^{\text{cca}}(\lambda) = 2 \cdot \Pr[\text{IND-CCA}(\Pi, \mathcal{A}, \lambda) = 1] - 1$ . We say that  $\Pi$  is IND-CCA secure if  $\text{Adv}_{\Pi, \mathcal{A}}^{\text{cca}}(\lambda)$  is negligible for all PPT  $\mathcal{A}$ .

*Symmetric-key authenticated encryption.* We recall the definition of secure authenticated (symmetric-key) encryption due to [36], except that we will not require pseudorandom ciphertexts. Bellare and Namprempre [10] showed that AE implies IND-CCA, and is in fact strictly stronger. For our counterexample, we target this very strong definition of security in order strengthen our results by showing that even this does not imply weak circular security.



**Fig. 2.** Experiments for Definitions 4 and 5. Each is defined with respect to a message space  $M$ , and we assume that  $m_0, m_1 \in M$  always. We write  $\mathbf{pk}$ ,  $\mathbf{sk}$ , and  $\mathbf{y}$  for  $(pk_1, \dots, pk_n)$ ,  $(sk_1, \dots, sk_n)$  and  $(y_1, \dots, y_n)$  respectively

**Definition 3 (AE).** Let  $\Pi = (\text{KeyGen}, \text{Enc}, \text{Dec})$  be a symmetric-key encryption scheme for the message space  $M$ . Let the random variable  $\text{AE}(\Pi, \mathcal{A}, \lambda)$  be defined by the probabilistic algorithm described on the right side of Figure 1. In the experiment, the oracle  $\mathcal{E}_{K,b}^{\text{ae}}(\cdot, \cdot)$  takes as input a pair of equal-length messages  $(m_0, m_1)$  and computes  $\text{Enc}(K, m_b)$ . The oracle  $\mathcal{D}_{K,b}^{\text{ae}}(\cdot)$  takes as input a ciphertext  $c$  and computes  $\text{Dec}(K, c)$  if  $b = 1$  and always returns  $\perp$  if  $b = 0$ . The adversary is not allowed to submit any ciphertext to  $\mathcal{D}_{K,b}^{\text{ae}}(\cdot)$  that was previously returned by  $\mathcal{E}_{K,b}^{\text{ae}}(\cdot, \cdot)$ . We denote the AE advantage of  $\mathcal{A}$  by  $\text{Adv}_{\Pi, \mathcal{A}}^{\text{ae}}(\lambda) = 2 \cdot \Pr[\text{AE}(\Pi, \mathcal{A}, \lambda) = 1] - 1$ . We say that  $\Pi$  is AE secure if  $\text{Adv}_{\Pi, \mathcal{A}}^{\text{ae}}(\lambda)$  is negligible for all PPT  $\mathcal{A}$ .

### 2.2 Circular Security Definitions

We next give definitions for circular security of public-key and symmetric-key encryption. These definitions are variants of the Key-Dependent Message (KDM) security notion of Black et al. [11]. By restricting the adversary’s power, we make it significantly harder for us to devise a counterexample and thus prove a stronger negative result.<sup>2</sup>

**Definition 4 (IND-CIRC-CPA<sup>n</sup>).** Let  $\Pi = (\text{KeyGen}, \text{Enc}, \text{Dec})$  be a public-key encryption scheme for the message space  $M$ . For  $b \in \{0, 1\}$ , integer  $n > 0$ , adversary  $\mathcal{A}$  and  $\lambda \in \mathbb{N}$ , let the random variable  $\text{IND-CIRC-CPA}^n(\Pi, \mathcal{A}, \lambda)$  be

<sup>2</sup> If we allowed the adversary to obtain encryptions of any affine function of the secret keys, as is done in [27,13], then we could devise a trivial counterexample where the adversary uses 1-cycles to break the system.



defined by the probabilistic algorithm on the left side of Figure 2. We denote the IND-CIRC-CPA<sup>n</sup> advantage of  $\mathcal{A}$  by

$$\text{Adv}_{\Pi, \mathcal{A}}^{n\text{-circ-cpa}}(\lambda) = 2 \cdot \Pr[\text{IND-CIRC-CPA}^n(\Pi, \mathcal{A}, \lambda) = 1] - 1.$$

We say that  $\Pi$  is IND-CIRC-CPA<sup>n</sup> secure if  $\text{Adv}_{\Pi, \mathcal{A}}^{n\text{-circ-cpa}}(\lambda)$  is negligible for all PPT  $\mathcal{A}$ .

One could augment this definition by modifying the IND-CIRC-CPA<sup>n</sup> experiment to allow for a challenge “left-or-right” query as in IND-CPA. While this is a quite natural modification, it only strengthens the definition, and we are interested in studying the weakest notions for which we can give a separation. Next we give a definition of weak circular security of public-key encryption.

**Definition 5 (IND-WCIRC-CPA<sup>n</sup>).** Let  $\Pi = (\text{KeyGen}, \text{Enc}, \text{Dec})$  be a public-key encryption scheme for the message space  $M$ . For  $b \in \{0, 1\}$ , integer  $n > 0$ , adversary  $\mathcal{A}$  and  $\lambda \in \mathbb{N}$ , let the random variable  $\text{IND-WCIRC-CPA}^n(\Pi, \mathcal{A}, \lambda)$  be defined by probabilistic algorithm on the center of Figure 2. We denote the IND-WCIRC-CPA<sup>n</sup> advantage of  $\mathcal{A}$  by

$$\text{Adv}_{\Pi, \mathcal{A}}^{n\text{-wcirc-cpa}}(\lambda) = 2 \cdot \Pr[\text{IND-WCIRC-CPA}^n(\Pi, \mathcal{A}, \lambda) = 1] - 1.$$

We say that  $\Pi$  is IND-WCIRC-CPA<sup>n</sup> secure if the function  $\text{Adv}_{\Pi, \mathcal{A}}^{n\text{-wcirc-cpa}}(\lambda)$  is negligible for all PPT  $\mathcal{A}$ .

Finally, we give a definition of weak circular security for symmetric encryption. We will abuse notation and also call this IND-WCIRC-CPA<sup>n</sup> security, since it will be clear from the context whether or not we mean public-key and symmetric-key.

**Definition 6 (IND-WCIRC-CPA<sup>n</sup>).** Let  $\Pi = (\text{KeyGen}, \text{Enc}, \text{Dec})$  be a symmetric-key encryption scheme for the message space  $M$ . For  $b \in \{0, 1\}$ , integer  $n > 0$ , adversary  $\mathcal{A}$  and  $\lambda \in \mathbb{N}$ , let  $\text{IND-WCIRC-CPA}^n(\Pi, \mathcal{A}, \lambda)$  be defined by the following probabilistic algorithm:

$\text{IND-WCIRC-CPA}_b^n(\Pi, \mathcal{A}, \lambda)$	$\text{EncCycle}(\mathbf{K})$
$b \xleftarrow{r} \{0, 1\}$	$\text{For } i = 1 \text{ to } n$
$\text{For } i = 1 \text{ to } n:$	$y_i \leftarrow \text{Enc}(K_i, K_{(i \bmod n)+1})$
$K_i \leftarrow \text{KeyGen}(1^\lambda)$	$\text{Output } \mathbf{y}$
$\mathbf{y} \leftarrow \text{EncCycle}(\mathbf{K})$	$\widetilde{\text{Enc}}(j, m_0, m_1)$
$\hat{b} \leftarrow \mathcal{A}^{\widetilde{\text{Enc}}(\cdot, \cdot, \cdot)}(\mathbf{y})$	$\text{Return } \text{Enc}(K_j, m_b)$
$\text{Output } (\hat{b} \stackrel{?}{=} b)$	

We denote the IND-WCIRC-CPA<sup>n</sup> advantage of  $\mathcal{A}$  by

$$\text{Adv}_{\Pi, \mathcal{A}}^{n\text{-wcirc-cpa}}(\lambda) = 2 \cdot \Pr[\text{IND-WCIRC-CPA}^n(\Pi, \mathcal{A}, \lambda) = 1] - 1.$$

We say that  $\Pi$  is IND-WCIRC-CPA<sup>n</sup> secure if  $\text{Adv}_{\Pi, \mathcal{A}}^{n\text{-wcirc-cpa}}(\lambda)$  is negligible for all PPT  $\mathcal{A}$ .

*Discussion.* In both the IND-CPA and IND-CIRC-CPA notions, the adversary must distinguish an encryption (or encryptions) of a special message from the encryption of zero. This choice of the message zero is arbitrary. We keep it in the statement of our definition to be consistent with [13]; however, it is important to note, for systems such as ours where zero is not in the message space, that zero can be replaced by any constant message for an equivalent definition. Acar et al. [2] use an equivalent definition where zero is replaced by a fresh random message.

We will not need to define a notion of security to withstand *circular and chosen-ciphertext attacks*, because we are able to show a stronger negative result. In Section 4.4, we provide an IND-CCA-secure cryptosystem, which is provably not IND-CIRC-CPA-secure. In other words, we are able to devise a peculiar cryptosystem: one that withstands all chosen-ciphertext attacks, and yet breaks under a weak circular attack which does not require a decryption oracle.

### 3 Counterexample for Symmetric Encryption

*Encryption Scheme  $\Pi_{ae}$ .* Let  $\Pi'_{ae} = (\text{KeyGen}', \text{Enc}', \text{Dec}')$  be a secure authenticated encryption scheme. To simplify our results, we assume that  $\text{KeyGen}'(1^\lambda)$  outputs a uniformly random key  $K$  in  $\{0, 1\}^\lambda$ , that the message space  $M' = \{0, 1\}^*$ , and that ciphertexts output by  $\text{Enc}'(K, m)$  are always in  $\{0, 1\}^{p(|m|)}$ , where  $p$  is some polynomial that depends on  $\lambda$ . We also assume that the first  $\lambda$  bits of a ciphertext are *never* equal to  $K$ . All of these assumptions can be removed via straightforward and standard modifications to our arguments below.

Fix a positive integer  $n$ . We now construct our counterexample scheme, denoted  $\Pi_{ae} = (\text{KeyGen}, \text{Enc}, \text{Dec})$ . We will take  $\text{KeyGen} = \text{KeyGen}'$ , i.e.,  $\Pi_{ae}$  also uses keys randomly chosen from  $\{0, 1\}^\lambda$ . The message-space of  $\Pi_{ae}$  will consist of  $M = \{0, 1\}^\lambda \cup \{0, 1\}^{np(\lambda)}$ , bit strings of length either  $\lambda$  or  $np(\lambda)$ . The algorithms  $\text{Enc}$  and  $\text{Dec}$  are defined as follows.

$\frac{\text{Enc}(K, m)}{\text{If } \text{IsCycle}(K, m) \text{ then}$ $\quad \text{Output } K \parallel m$ $\text{Else}$ $\quad \text{Output } \text{Enc}'(K, m)$ <hr style="border: 0.5px solid black;"/> $\frac{\text{Dec}(K, c)}{\text{If } c = K \parallel \tilde{m} \text{ then}$ $\quad \text{Output } \tilde{m}$ $\text{Else}$ $\quad \text{Output } \text{Dec}'(K, c)$	$\frac{\text{IsCycle}(K, m)}{\text{If }  m  \neq np(\lambda)}$ $\quad \text{Return false}$ $\text{Parse } m \text{ as } (c_1, \dots, c_n)$ $K_2 \leftarrow \text{Dec}'(K, c_1)$ $\text{For } i = 2 \text{ to } n$ $\quad K_{i \bmod n+1} \leftarrow \text{Dec}'(K_i, c_i)$ $\text{Return } (K_1 \stackrel{?}{=} K)$
---	---

Decryption is always correct. This follows from our assumption that  $\text{Enc}'$  will never output a ciphertext that contains  $K$  as a prefix. We first establish the AE security of our scheme.

**Theorem 1.** *Encryption scheme  $\Pi_{\text{ae}}$  is AE secure whenever  $\Pi'_{\text{ae}}$  is AE secure. (Proof in the full version of this work [17].)*

The proof proceeds by showing that computing an encrypted key-cycle during the AE game is equivalent to recovering the secret key. From there we can reduce the security of  $\Pi_{\text{ae}}$  to  $\Pi'_{\text{ae}}$  easily.

Curiously, Theorem 1 is no longer true if one replaces AE security with a symmetric version of IND-CPA security for both  $\Pi_{\text{ae}}$  and  $\Pi'_{\text{ae}}$ . Namely, some type of chosen-ciphertext security is required on  $\Pi'_{\text{ae}}$  to prove even chosen-plaintext security of  $\Pi_{\text{ae}}$ . Intuitively, this is because it might be possible for an adversary to compute an encrypted key-cycle on its own if the scheme is only IND-CPA-secure, but *not* if the scheme is AE-secure. In fact, the work of Boneh et al. [13] gives an explicit example of a scheme where the adversary can compute a cycle himself.

*The Attack.* We now show that  $\Pi_{\text{ae}}$  is not circular-secure for  $n$  cycles, even in a weak sense.

**Theorem 2.**  *$\Pi_{\text{ae}}$  is not IND-WCIRC-CPA<sup>n</sup> secure.*

*Proof.* We give an explicit adversary  $\mathcal{A}$  that has advantage negligibly close to 1. The adversary takes as input the encrypted key-cycle  $\mathbf{y}$  in the IND-WCIRC-CPA<sup>n</sup> game. It queries  $\widetilde{\text{Enc}}(1, m_0, m_1)$ , where  $m_0 = \mathbf{y}$  and  $m_1$  is a random message of the same length. Let  $y$  be the ciphertext returned by the oracle.

At this point, there are many ways to proceed; perhaps the simplest is to observe that the *length* of  $y$  depends on the challenge bit  $b$ . This is because, if  $b = 0$ , then  $m_0 = \mathbf{y}$  was encrypted, resulting in  $y = K \parallel \mathbf{y}$ , which is  $\lambda + np(\lambda)$  bits long. If  $b = 1$  then  $y$  was computed by running  $\text{Enc}'(K, m_1)$ , which will be  $p(|m_1|) = p(np(\lambda))$  bits long *if*  $\text{IsCycle}(K, m_1)$  returns false. Thus, as long as  $\text{IsCycle}(K, m_1)$  returns false,  $\mathcal{A}_2$  can compute the value of  $b$  by measuring  $y$ 's length.

But why should  $\text{IsCycle}(K, m_1)$  return false? This follows from the AE security of  $\Pi'_{\text{ae}}$ . Let us parse  $m_1$  into  $(c_1, \dots, c_n)$ , where each  $c_i \in \{0, 1\}^{p(\lambda)}$  is random. When  $\text{IsCycle}(K, m_1)$  returns true, it must be that  $\text{Dec}'(K, c_1)$  did not return  $\perp$ . But if this happens, then we can construct an adversary to break the AE security of  $\Pi'_{\text{ae}}$ . The adversary simply queries  $\mathcal{D}_{K,b}^{\text{ae}}(\cdot)$  at a random point, observes if it returns  $\perp$  or not, and outputs  $\hat{b} = 0$  or 1 depending on this observation.

We note that we could design an encryption scheme that does not have this type of ciphertext-length behavior by giving a different attack that abuses the fact that  $K$  is present in the ciphertext in one case, but not the other. We have chosen to present the attack this way for simplicity only.

## 4 Counterexamples for Public-Key Encryption

### 4.1 Preliminaries and Algebraic Setting

*Bilinear Groups.* We work in a bilinear setting where there exists an efficient mapping function  $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$  involving groups of the same prime order  $p$ .

Two algebraic properties required are that: (1) if  $g$  generates  $\mathbb{G}_1$  and  $h$  generates  $\mathbb{G}_2$ , then  $e(g, h) \neq 1$  and (2) for all  $a, b \in \mathbb{Z}_p$ , it holds that  $e(g^a, h^b) = e(g, h)^{ab}$ .

**Decisional Diffie-Hellman Assumption (DDH):** Let  $\mathbb{G}$  be a group of prime order  $p \in \Theta(2^\lambda)$ . For all PPT adversaries  $\mathcal{A}$ , the following probability is  $1/2$  plus an amount negligible in  $\lambda$ :

$$\Pr \left[ \begin{array}{l} g, z_0 \leftarrow \mathbb{G}; a, b \leftarrow \mathbb{Z}_p; z_1 \leftarrow g^{ab}; d \leftarrow \{0, 1\}; \\ d' \leftarrow \mathcal{A}(g, g^a, g^b, z_d) : d = d' \end{array} \right].$$

**Strong External Diffie-Hellman Assumption (SXDH):** Let  $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$  be bilinear groups. The SXDH assumption states that the DDH problem is hard in both  $\mathbb{G}_1$  and in  $\mathbb{G}_2$ . This implies that there does *not* exist an efficiently computable isomorphism between these two groups. The SXDH assumption appears in many prior works, such as [21,38,32,12,8,6,24,9,25,2].

*Indistinguishability and Pseudorandom Generators.*

**Definition 7 (Indistinguishability).** *Two ensembles of probability distributions  $\{X_k\}_{k \in \mathbb{N}}$  and  $\{Y_k\}_{k \in \mathbb{N}}$  with index set  $\mathbb{N}$  are said to be computationally indistinguishable if for every polynomial-size circuit family  $\{D_k\}_{k \in \mathbb{N}}$ , there exists a negligible function  $\nu$  such that*

$$|\Pr [x \leftarrow X_k : D_k(x) = 1] - \Pr [y \leftarrow Y_k : D_k(y) = 1]|$$

*is less than  $\nu(k)$ . We denote such sets  $\{X_k\}_{k \in \mathbb{N}} \stackrel{c}{\approx} \{Y_k\}_{k \in \mathbb{N}}$ .*

**Definition 8 (Pseudorandom Generator [30]).** *Let  $U_x$  denote the uniform distribution over  $\{0, 1\}^x$ . Let  $\ell(\cdot)$  be a polynomial and let  $G$  be a deterministic polynomial-time algorithm such that for any input  $s \in \{0, 1\}^n$ , algorithm  $G$  outputs a string of length  $\ell(n)$ . We say that  $G$  is a pseudorandom generator if the following two conditions hold:*

- (Expansion:) *For every  $n$ , it holds that  $\ell(n) > n$ .*
- (Pseudorandomness:) *For every  $n$ ,  $\{U_{\ell(n)}\}_n \stackrel{c}{\approx} \{s \leftarrow U_n : G(s)\}_n$ .*

The constructions of Section 4.2 use a PRG where the domain of the function is an exponentially-sized cyclic group.

## 4.2 Encryption Scheme $\Pi_{\text{cpa}}$

We now describe an encryption scheme  $\Pi_{\text{cpa}} = (\text{KeyGen}, \text{Enc}, \text{Dec})$ . It is set in asymmetric bilinear groups  $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$  of prime order  $p$  where we assume that the groups  $\mathbb{G}_1$  and  $\mathbb{G}_2$  are distinct and that the DDH assumption holds in both. We assume that a single set of group parameters  $(e, p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g, h)$ , where  $\mathbb{G}_1 = \langle g \rangle, \mathbb{G}_2 = \langle h \rangle$ , will be shared across all keys generated at a given security level and are implicitly provided to all algorithms.

The message space is  $\mathcal{M} = \{0, 1\} \times \mathbb{Z}_p^* \times \mathbb{Z}_p^*$ . Let  $\text{encode} : \mathcal{M} \rightarrow \{0, 1\}^{\ell(\lambda)}$  and  $\text{decode} : \{0, 1\}^{\ell(\lambda)} \rightarrow \mathcal{M}$  denote an invertible encoding scheme where  $\ell(\lambda)$  is the polynomial length of the encoded message. Let  $F : \mathbb{G}_T \rightarrow \{0, 1\}^{\ell(\lambda)}$  be a pseudorandom generator secure under the Decisional Diffie Hellman assumption. (Recall that pseudorandom generators can be constructed from any one-way function [28].)

**KeyGen**( $1^\lambda$ ). The key generation algorithm selects a random bit  $\beta \leftarrow \{0, 1\}$  and random values  $a_1, a_2 \leftarrow \mathbb{Z}_p^*$ . The secret key is set as  $sk = (\beta, a_1, a_2)$ . We note that  $sk \in \mathcal{M}$ . The public key is set as:

$$pk = \begin{cases} (0, e(g, h)^{a_1}, g^{a_2}) \in \{0, 1\} \times \mathbb{G}_T \times \mathbb{G}_1 & \text{if } \beta = 0 \\ (1, e(g, h)^{a_1}, h^{a_2}) \in \{0, 1\} \times \mathbb{G}_T \times \mathbb{G}_2 & \text{if } \beta = 1. \end{cases}$$

**Encrypt**( $pk, M$ ). The encryption algorithm parses the public key  $pk = (\beta, Y_1, Y_2)$ , where  $Y_2$  may be in  $\mathbb{G}_1$  or  $\mathbb{G}_2$  depending on the structure of the public key, and message  $M = (\alpha, m_1, m_2) \in \mathcal{M}$ . Note that  $m_1$  and  $m_2$  cannot be zero, but these values can be easily included in the message space by a proper encoding.

Select random  $r \leftarrow \mathbb{Z}_p$  and  $R \leftarrow \mathbb{G}_T$ . Set  $I = F(R) \oplus \text{encode}(M)$ .

Output the ciphertext  $C$  as:

$$C = \begin{cases} (g^r, R \cdot Y_1^r, Y_2^{rm_2} \cdot g^{m_1}, I) & \text{if } \beta = 0; \\ (h^r, R \cdot Y_1^r, Y_2^{rm_2}, I) & \text{if } \beta = 1. \end{cases}$$

We note that in the first case,  $C \in \mathbb{G}_1 \times \mathbb{G}_T \times \mathbb{G}_1 \times \{0, 1\}^{\ell(\lambda)}$ , while in the second  $C \in \mathbb{G}_2 \times \mathbb{G}_T \times \mathbb{G}_2 \times \{0, 1\}^{\ell(\lambda)}$ .

**Decrypt**( $sk, C$ ). The decryption algorithm parses the secret key  $sk = (\beta, a_1, a_2)$  and the ciphertext  $C = (C_1, C_2, C_3, C_4)$ . Next, it computes:

$$R = \begin{cases} (C_2/e(C_1, h))^{a_1} & \text{if } \beta = 0; \\ (C_2/e(g, C_1))^{a_1} & \text{if } \beta = 1. \end{cases}$$

Then it computes  $M' = F(R) \oplus C_4 \in \{0, 1\}^{\ell(\lambda)}$  and outputs the message  $M = \text{decode}(M')$ .

*Discussion.* Like the circular-secure scheme of Boneh et al. [13], the above cryptosystem is a variation on El Gamal [20]. It is a practical system, which on first glance might be somewhat reminiscent of schemes the readers are used to seeing in the literature. The scheme includes a few “artificial” properties: (1) placing a public key in either  $\mathbb{G}_1$  or  $\mathbb{G}_2$  at random and (2) the fact that the ciphertext value  $C_3$  is unused in the decryption algorithm. We will shortly see that these features are “harmless” in a semantic-security sense, but very useful for recovering the secret keys of the system in the presence of a two cycle. While it is not unusual for counterexamples to have artificial properties (e.g., [16,23]), we

can address these points as well.<sup>3</sup> In the full version of this work [17], we show that property (1) can be removed by doubling the length of the ciphertext. For property (2), we observe that many complex protocols such as group signatures (e.g., [12]) combine ciphertexts with other components that are unused in decryption but are quite important to the protocol as a whole. Thus, we believe our counterexample is not that far fetched. It is possible that such an attack could exist on one of today’s commonly-used encryption algorithms.

We first show that  $\Pi_{\text{cpa}}$  meets the standard notion of CPA security.

**Theorem 3.** *Encryption scheme  $\Pi_{\text{cpa}}$  is IND-CPA secure under the Decisional Diffie-Hellman Assumption in  $\mathbb{G}_1$  and  $\mathbb{G}_2$  (SXDH).*

The proof is given in the full version of this work [17]. It is relatively standard and involves repeated applications of the DDH assumption and PRG security.

### 4.3 The Attack

Despite being IND-CPA-secure, cryptosystem  $\Pi_{\text{cpa}}$  is not even weakly circular secure for 2-cycles. Specifically, given a circular encryption of two keys, we show that an adversary can distinguish another ciphertext with advantage  $1/2$ . Our adversary actually does much more than this: with probability  $1/2$  over the coins used in key generation, *it can recover both secret keys*.

This is the first circular attack that allows the adversary to recover the secret keys. (In the full version of this work [17], we discuss how to improve these probabilities to almost 1.) Our attack combines elements of both ciphertexts in an attempt to recover  $sk_A$ , which can then be used to decrypt the first ciphertext and obtain  $sk_B$ . It is counterintuitive that this is possible, given that it is easy to see that IND-CPA-security guarantees that it is safe for *one* of them to send their message.

**Theorem 4.**  *$\Pi_{\text{cpa}}$  is not IND-WCIRC-CPA<sup>2</sup>-secure.*

*Proof.* We give PPT adversary  $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$  such that  $\text{Adv}_{\Pi_{\text{cpa}}, \mathcal{A}}^{2\text{-wcirc-cpa}}(\lambda)$  is equal to  $1/2$ . Since IND-WCIRC-CPA security requires that this advantage be negligible, this attack breaks security. The adversary proceeds as follows. The first stage of the adversary,  $\mathcal{A}_1$ , obtains the two public keys, which we will write as  $pk_A$  and  $pk_B$ , and an encrypted cycle, which we will write as  $(C_A, C_B)$ .

If both keys have  $\beta = 0$  or  $\beta = 1$  (call this event  $E_1$ ), the adversary aborts and instructs the second stage ( $\mathcal{A}_2$ ) to output a random bit. Since the two keys are independently generated by the challenger, this event will occur with probability exactly  $1/2$ . Below we will condition on  $E_1$  not happening, and wlog assume that  $pk_A = (0, e(g, h)^{a_1}, g^{a_2})$  and  $pk_B = (1, e(g, h)^{b_1}, h^{b_2})$ . The corresponding secret keys  $sk_A = (0, a_1, a_2)$ ,  $sk_B = (1, b_1, b_2)$  are not known to the adversary.

---

<sup>3</sup> While our scheme is different from that of Acar et al. [2], that scheme also has similar artificial properties such as the presence of values that are not used in decryption.

We write the given ciphertexts  $C_A = (c_{A,1}, c_{A,2}, c_{A,3}, c_{A,4})$  and  $C_B = (c_{B,1}, c_{B,2}, c_{B,3}, c_{B,4})$ .  $\mathcal{A}_1$  will output two arbitrary distinct messages, and request that the challenge use  $pk_A$ . For the state passed to  $\mathcal{A}_2$ , it now computes:

$$X := c_{B,2} \cdot \frac{e(c_{A,1}, c_{B,3})}{e(c_{A,3}, c_{B,1})}.$$

$\mathcal{A}_1$  sets  $\hat{sk}_A = \text{decode}(c_{B,4} \oplus F(X))$  and passes this with the challenge messages as state to  $\mathcal{A}_2$ .

$\mathcal{A}_2$  receives a ciphertext  $y$  and the passed state. It parses  $\hat{sk}_A$  as a secret key for  $\Pi_{\text{cpa}}$  and computes  $\text{Dec}(\hat{sk}_A, y)$ , and tests if this is equal to either of the challenge messages. If so, it outputs the corresponding bit. Otherwise it outputs a random bit.

Let's explore why this test works. Write  $C_A = \text{Enc}(pk_A, sk_B)$  and  $C_B = \text{Enc}(pk_B, sk_A)$ . Then:

$$\begin{aligned} C_A &= (c_{A,1}, c_{A,2}, c_{A,3}, c_{A,4}) \\ &= (g^r, R \cdot e(g, h)^{ra_1}, g^{ra_2b_2+b_1}, F(R) \oplus \text{encode}(sk_B)) \\ C_B &= (c_{B,1}, c_{B,2}, c_{B,3}, c_{B,4}) \\ &= (h^s, S \cdot e(g, h)^{sb_1}, h^{sa_2b_2}, F(S) \oplus \text{encode}(sk_A)) \end{aligned}$$

for some  $r, s \in \mathbb{Z}_p$  and  $R, S \in \mathbb{G}_T$ . Then we have that:

$$\begin{aligned} X &:= c_{B,2} \cdot \frac{e(c_{A,1}, c_{B,3})}{e(c_{A,3}, c_{B,1})} = S \cdot e(g, h)^{sb_1} \cdot \frac{e(g^r, h^{sa_2b_2})}{e(g^{ra_2b_2+b_1}, h^s)} \\ &= S \cdot e(g, h)^{sb_1} \cdot \frac{e(g, h)^{rsa_2b_2}}{e(g, h)^{rsa_2b_2} \cdot e(g, h)^{sb_1}} = S. \end{aligned}$$

Thus,  $\mathcal{A}_1$  recovers  $\hat{sk}_A = sk_A$  as  $\text{decode}(c_{B,4} \oplus F(S))$ , and  $\mathcal{A}_2$  will correctly guess bit  $b$  in this case.

Write  $\hat{b}$  for the output of  $\mathcal{A}_2$ . We have

$$\begin{aligned} \text{Adv}_{\Pi_{\text{cpa}}, \mathcal{A}}^{2\text{-wcirc-cpa}}(\lambda) &= 2 \Pr[\hat{b} = b] - 1 \\ &= 2(\Pr[\hat{b} = b | E_1] \Pr[E_1] + \\ &\quad \Pr[\hat{b} = b | \neg E_1] \Pr[\neg E_1]) - 1 \\ &= 2(1 \cdot 1/2 + 1/2 \cdot 1/2) - 1 \\ &= 1/2 \end{aligned}$$

This completes the proof.

#### 4.4 Extension: A Counterexample for CCA Security

We show that there exists an IND-CCA-secure cryptosystem, which suffers a complete break when Alice and Bob trade secret keys over an insecure channel;

i.e., transmit the two-key cycle  $E(pk_A, sk_B)$  and  $E(pk_B, sk_A)$ . Our construction follows the “double-encryption” approach to building IND-CCA systems from IND-CPA systems as pioneered by Naor and Yung [34] and refined by Dolev, Dwork and Naor [19] and Sahai [37]. Our building blocks will be:

1. The IND-CPA-secure cryptosystem  $\Pi_{\text{cpa}} = (G, E, D)$  from Section 4. Let  $E(pk, m; r)$  be the encryption of  $m$  under public key  $pk$  with randomness  $r$ .
2. An adaptively non-malleable non-interactive zero-knowledge (NIZK) proof system with unpredictable simulated proofs and uniquely applicable proofs for the language  $L$  of consistent pairs of encryptions, defined as:

$$L = \left\{ (e_0, e_1, c_0, c_1) : \begin{array}{l} \exists m, r_0, r_1 \in \{0, 1\}^* \text{ s.t.} \\ c_0 = E(e_0, m; r_0) \text{ and } c_1 = E(e_1, m; r_1) \end{array} \right\}.$$

A proof system for  $L$  can be realized under relatively mild assumptions, such as the difficulty of factoring Blum integers (e.g., [37]). One complication is that the secret keys for this cryptosystem now change and the construction must be adapted accordingly, so that the secret key can still be recovered by the adversary during a circular attack. We show that this is possible.

## 5 Conclusion and Open Problems

In this work, we presented a natural relaxation of the circular security definition, which may prove interesting for positive results in its own right. We demonstrated that its guarantees are *not* already captured by standard definitions of encryption. To do this, we presented symmetric and public-key encryption systems that are secure in the IND-CPA and IND-CCA sense, but fail catastrophically in the presence of an encrypted cycle. This provides the first answer to the foundational question on whether IND-CCA-security captures (weak or regular) circular security for all cycles larger than self-loops. In either case, it does not.

Our work leaves open the interesting problem of finding a public-key counterexample for cycles of size  $\geq 3$ . Secondly, while our symmetric counterexample depended only on the existence of AE-secure symmetric encryption, our public-key counterexample, like that of Acar et al. [2], required a specific bilinear map assumption. It would be highly interesting to find a counterexample assuming only that IND-CPA- or IND-CCA-secure systems exist.

Finally, we observe that our public-key counterexample contains a novel and curious property – *certain combinations of independently generated ciphertexts trigger the release of their underlying plaintext*. From Rabin’s  $\frac{1}{2}$ -OT system to DH-DDH gap groups, the cryptographic community has a strong history of turning such oddities to an advantage. If we view a cryptosystem with this property as a new primitive, what new functionalities can be realized using it?

**Acknowledgments.** The authors thank Ronald Rivest for the suggestion to view the public key counterexample in Section 4 as a potential building block for other functionalities.



## References

1. Abadi, M., Rogaway, P.: Reconciling two views of cryptography (the computational soundness of formal encryption). *J. Cryptology* 15(2), 103–127 (2002)
2. Acar, T., Belenkiy, M., Bellare, M., Cash, D.: Cryptographic Agility and Its Relation to Circular Encryption. In: Gilbert, H. (ed.) *EUROCRYPT 2010*. LNCS, vol. 6110, pp. 403–422. Springer, Heidelberg (2010)
3. Adão, P., Bana, G., Herzog, J., Scedrov, A.: Soundness of Formal Encryption in the Presence of Key-Cycles. In: de Capitani di Vimercati, S., Syverson, P.F., Gollmann, D. (eds.) *ESORICS 2005*. LNCS, vol. 3679, pp. 374–396. Springer, Heidelberg (2005)
4. Akavia, A., Goldwasser, S., Vaikuntanathan, V.: Simultaneous Hardcore Bits and Cryptography against Memory Attacks. In: Reingold, O. (ed.) *TCC 2009*. LNCS, vol. 5444, pp. 474–495. Springer, Heidelberg (2009)
5. Applebaum, B., Cash, D., Peikert, C., Sahai, A.: Fast Cryptographic Primitives and Circular-Secure Encryption Based on Hard Learning Problems. In: Halevi, S. (ed.) *CRYPTO 2009*. LNCS, vol. 5677, pp. 595–618. Springer, Heidelberg (2009)
6. Ateniese, G., Camenisch, J., de Medeiros, B.: Untraceable RFID tags via insubvertible encryption. In: *CCS 2005*, pp. 92–101 (2005)
7. Backes, M., Pfizmann, B., Scedrov, A.: Key-dependent message security under active attacks -BRSIM/UC-soundness of Dolev-Yao-style encryption with key cycles. *J. of Comp. Security* 16(5), 497–530 (2008)
8. Ballard, L., Green, M., de Medeiros, B., Monrose, F.: Correlation-resistant storage. Technical Report TR-SP-BGMM-050705, Johns Hopkins University, CS Dept, 2005. <http://spar.isi.jhu.edu/~mgreen/correlation.pdf>.
9. Belenkiy, M., Chase, M., Kohlweiss, M., Lysyanskaya, A.: P-signatures and Noninteractive Anonymous Credentials. In: Canetti, R. (ed.) *TCC 2008*. LNCS, vol. 4948, pp. 356–374. Springer, Heidelberg (2008)
10. Bellare, M., Namprempre, C.: Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. *J. Cryptology* 21(4), 469–491 (2008)
11. Black, J., Rogaway, P., Shrimpton, T.: Encryption-Scheme Security in the Presence of Key-Dependent Messages. In: Nyberg, K., Heys, H.M. (eds.) *SAC 2002*. LNCS, vol. 2595, pp. 62–75. Springer, Heidelberg (2003)
12. Boneh, D., Boyen, X., Shacham, H.: Short Group Signatures. In: Franklin, M. (ed.) *CRYPTO 2004*. LNCS, vol. 3152, pp. 41–55. Springer, Heidelberg (2004)
13. Boneh, D., Halevi, S., Hamburg, M., Ostrovsky, R.: Circular-Secure Encryption from Decision Diffie-Hellman. In: Wagner, D. (ed.) *CRYPTO 2008*. LNCS, vol. 5157, pp. 108–125. Springer, Heidelberg (2008)
14. Camenisch, J., Chandran, N., Shoup, V.: A Public Key Encryption Scheme Secure against Key Dependent Chosen Plaintext and Adaptive Chosen Ciphertext Attacks. In: Joux, A. (ed.) *EUROCRYPT 2009*. LNCS, vol. 5479, pp. 351–368. Springer, Heidelberg (2009)
15. Camenisch, J.L., Lysyanskaya, A.: An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. In: Pfizmann, B. (ed.) *EUROCRYPT 2001*. LNCS, vol. 2045, pp. 93–118. Springer, Heidelberg (2001)
16. Canetti, R., Goldreich, O., Halevi, S.: The random oracle methodology, revisited. *J. of the ACM* 51(4), 557–594 (2004)
17. Cash, D., Green, M., Hohenberger, S.: New definitions and separations for circular security. *Cryptology ePrint Archive*, Report 2010/144 (2012), <http://eprint.iacr.org/2010/144>

18. Dodis, Y., Kalai, Y.T., Lovett, S.: On cryptography with auxiliary input. In: STOC 2009, pp. 621–630 (2009)
19. Dolev, D., Dwork, C., Naor, M.: Nonmalleable cryptography. *SIAM J. Computing* 30(2), 391–437 (2000)
20. El Gamal, T.: A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 10–18. Springer, Heidelberg (1985)
21. Galbraith, S.D.: Supersingular Curves in Cryptography. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 495–513. Springer, Heidelberg (2001)
22. Goldwasser, S., Micali, S.: Probabilistic encryption. *J. Comput. Syst. Sci.* 28(2), 270–299 (1984)
23. Goldwasser, S., Kalai, Y.T.: On the (In)security of the Fiat-Shamir Paradigm. In: FOCS 2003, p. 102 (2003)
24. Green, M., Hohenberger, S.: Universally Composable Adaptive Oblivious Transfer. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 179–197. Springer, Heidelberg (2008)
25. Groth, J., Sahai, A.: Efficient Non-interactive Proof Systems for Bilinear Groups. In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 415–432. Springer, Heidelberg (2008)
26. Haitner, I., Holenstein, T.: On the (Im)Possibility of Key Dependent Encryption. In: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, pp. 202–219. Springer, Heidelberg (2009)
27. Halevi, S., Krawczyk, H.: Security under key-dependent inputs. In: ACM CCS 2007, pp. 466–475 (2007)
28. Hastad, J., Impagliazzo, R., Levin, L.A., Luby, M.: A pseudorandom generator from any one-way function. *SIAM J. Computing* 28(4), 1364–1396 (1999)
29. Hofheinz, D., Unruh, D.: Towards Key-Dependent Message Security in the Standard Model. In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 108–126. Springer, Heidelberg (2008)
30. Katz, J., Lindell, Y.: *Introduction to Modern Cryptography*. Chapman & Hall/CRC (2008)
31. Laud, P., Corin, R.: Sound Computational Interpretation of Formal Encryption with Composed Keys. In: Lim, J.-I., Lee, D.-H. (eds.) ICISC 2003. LNCS, vol. 2971, pp. 55–66. Springer, Heidelberg (2004)
32. McCullagh, N., Barreto, P.S.L.M.: A New Two-Party Identity-Based Authenticated Key Agreement. In: Menezes, A. (ed.) CT-RSA 2005. LNCS, vol. 3376, pp. 262–274. Springer, Heidelberg (2005)
33. Naor, M., Segev, G.: Public-Key Cryptosystems Resilient to Key Leakage. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 18–35. Springer, Heidelberg (2009)
34. Naor, M., Yung, M.: Public-key cryptosystems provably secure against chosen ciphertext attacks. In: STOC 1990, pp. 427–437 (1990)
35. Rackoff, C., Simon, D.R.: Non-interactive Zero-Knowledge Proof of Knowledge and Chosen Ciphertext Attack. In: Feigenbaum, J. (ed.) CRYPTO 1991. LNCS, vol. 576, pp. 433–444. Springer, Heidelberg (1992)
36. Rogaway, P., Shrimpton, T.: A Provable-Security Treatment of the Key-Wrap Problem. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 373–390. Springer, Heidelberg (2006)
37. Sahai, A.: Non-malleable non-interactive zero knowledge and adaptive chosen-ciphertext security. In: FOCS 1999, pp. 543–553 (1999)
38. Scott, M.: Authenticated id-based key exchange and remote log-in with simple token and pin number (2002), <http://eprint.iacr.org/2002/164>