AICR · OPEN PROBLEM

A Safe Two-Scheme Key Cycle for Every Encryption Scheme

Can every public-key encryption scheme be paired with a partner that makes a 2-cycle safe to publish?

Status. Statement: AI-written from Daniele Micciancio, *Fully Composable Homomorphic Encryption*, IACR ePrint 2024/1545 (2 October 2024); published in IACR Communications in Cryptology 2(1), 8 April 2025. Not yet checked by a human. Open in both directions: the known circular-security counterexamples are all of the opposite quantifier shape, exhibiting particular pairs of schemes whose cycle is insecure, and the source paper says explicitly that they do not rule this out.

Category. *Public-Key Encryption*, *Foundations*.

Conjecture (informal). *Publishing an encryption of a secret key under its own public key — a key cycle — is not safe in general: there are schemes that are perfectly secure until the cycle is published and completely broken afterwards. This conjecture asks for something weaker and, as far as anyone knows, still possible. Take any public-key encryption scheme* E*. May one always find a second, possibly quite different scheme* E' *such that the two-step cycle —* E*'s secret key encrypted under* E'*, and* E'*'s secret key encrypted under* E *— can be published without harming* E*? The partner scheme is chosen after seeing* E *and is not required to be homomorphic or to be good for anything else. The known counterexamples do not settle this, because they build a* pair *of schemes that break each other, whereas here the pair is chosen to cooperate.*

1 The setting

Gentry's bootstrapping [Geno9] makes a homomorphic encryption scheme composable by publishing $\mathsf{Enc}_{pk}(sk)$: an encryption of the secret key under its own public key. Its security therefore rests on a circular security assumption, and the source paper's Theorem 6 isolates exactly that dependency by recasting bootstrapping as a

transformation from a circular-secure, non-composable scheme into a fully composable one.

Circular security does not come for free. A long line of work [KRW15, KW16, AP16, GKW17a, GKW17b, HK17] constructs IND-CPA secure schemes that are broken as soon as a key cycle involving them is published — for cycles of length 1, of length 2, and of arbitrary length. The source paper draws the consequence for bootstrapping in one sentence: "Previous results have shown how to build encryption schemes Enc such that publishing such a cycle is insecure. So, one cannot achieve full composability generically by publishing such an encryption cycle for any scheme Enc".

The gap those counterexamples leave. Theorem 6 generalizes from a 1-cycle $\mathsf{Enc}_{pk}(sk)$ to longer cycles $\mathsf{Enc}_{pk_1}(sk_2), \ldots, \mathsf{Enc}_{pk_n}(sk_1)$, and — this is the observation the conjecture rests on — the schemes at the different steps of the cycle need not be the same one. The source paper: "However, for the purpose of applying (a generalization of) Theorem 6 it is not necessary to use the same encryption scheme at every step of the cycle". It also notes that the second scheme carries no homomorphic burden: "Note that the new (existentially quantified) scheme Enc′ is not required to be homomorphic".

Concretely, for bootstrapping it would be enough to publish a 2-cycle $\mathsf{Enc}_{pk}(sk')$, $\mathsf{Enc}'_{pk'}(sk)$ across two schemes. Given those two ciphertexts as key material and an input ciphertext $c'' = \mathsf{Enc}_{pk}(m)$, one bootstraps c'' by homomorphically evaluating, on $\mathsf{Enc}_{pk}(sk')$, the map $sk' \mapsto \mathsf{Dec}_{\mathsf{Dec}_{sk'}(c')}(c'')$. The source paper's argument that the known separations do not apply is a distributional one: this "is different from computing a simple cycle $\mathsf{Enc}_{pk}(sk)$ directly, because the evaluated ciphertext follows a different distribution. So, it is not ruled out by previous separation results, and we conjecture the following".

Quantifier shape is the whole difficulty. The counterexamples in the literature are of the form: *there exists* a scheme (or a pair of schemes) whose cycle is insecure. The conjecture is: *for every* scheme *there exists* a partner making the cycle secure. Neither implies anything about the other. To refute the conjecture one would

have to construct a single scheme E that is poisoned against *every* possible partner E' — a universally uncooperative scheme — and no technique for that is known. To prove it one would have to build, from an arbitrary E, a partner tailored to it; the natural attempts run into the same self-reference that makes circular security hard in the first place.

What settling it would give. The source is careful about what a proof would and would not deliver: "Note that this Conjecture does not by itself imply the existence of composable FHE schemes. The reason is that for any homomorphic encryption scheme Enc (capable of evaluating functions in a given set $\mathcal{F}$), one may select a scheme Enc′ such that the required computation $sk' \mapsto \mathsf{Dec}_{\mathsf{Dec}_{sk'}(c')}(c'')$ is not in $\mathcal{F}$". The partner might, in other words, be too complicated to bootstrap with. What a proof *would* give is stated in the next sentence — "interesting information about the feasibility of achieving circular security in a generic way" — and one concrete corollary: "if the starting scheme Enc is (non-composable) fully homomorphic (i.e., $\mathcal{F}$ is the set of all possible functions), this would be enough to achieve full composability". That is, for a scheme that can already evaluate everything, the conjecture closes the gap to composable FHE.

Variants the source records. "Several variants of this conjecture are possible. For example, one may consider cycles of length greater than 2, or set Enc′ to a private key encryption scheme where the side information is $\mathsf{Enc}'_{sk'}(sk), \mathsf{Enc}_{pk}(sk')$, or consider the special case of encryption schemes that encrypt their messages bit by bit". Only the 2-cycle public-key form is stated below; the variants are separate statements, and choosing one of them is not the same problem.

2 Notation and parameters

- κ is the security parameter. A scheme's message space $\mathcal{M}$ is finite and of fixed length; $\mathcal{K}$ is its secret-key space.
- Enc^* is the componentwise extension of Enc to message vectors, $\mathsf{Enc}^*(pk, (m_1, \ldots, m_w)) = (\mathsf{Enc}(pk, m_1), \ldots, \mathsf{Enc}(pk, m_w))$,

so that a secret key encoded as a vector of messages can be encrypted.

- $\psi : \mathcal{K} \to \mathcal{M}^k$ and $\psi' : \mathcal{K}' \to (\mathcal{M}')^{k'}$ are injective key encodings: ψ encodes E's secret key as a vector of E′-messages, ψ' encodes E′'s secret key as a vector of E-messages. The source writes $\mathsf{Enc}'_{pk'}(sk)$ and $\mathsf{Enc}_{pk}(sk')$ and leaves the encodings implicit; they are named here only so that the two ciphertexts are well typed.
- Advantages are asymptotic in κ and "negligible" has its usual meaning; see Remark 3 for the source's own concrete measure of advantage.

3 The conjecture

Definition 1 (Encryption scheme, valid). A public key encryption scheme with message space $\mathcal{M}$ is a triple of probabilistic polynomial-time algorithms $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ where $(sk, pk) \leftarrow \mathsf{Gen}(\kappa)$, $c \leftarrow \mathsf{Enc}(pk, m)$ for $m \in \mathcal{M}$, and $\mathsf{Dec}(sk, c) \in \mathcal{M} \cup \{\perp\}$. It is *valid* if $\mathsf{Dec}(sk, \mathsf{Enc}(pk, m)) = m$ holds with probability 1 for every $m \in \mathcal{M}$ and every $(sk, pk) \leftarrow \mathsf{Gen}(\kappa)$.

Definition 2 (IND-CPA). $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is IND-CPA secure if every probabilistic polynomial-time adversary has negligible advantage in the game: sample $b \leftarrow \{0,1\}$ and $(sk, pk) \leftarrow \mathsf{Gen}(\kappa)$; the adversary, given pk, outputs $m_0, m_1 \in \mathcal{M}$ of equal length, receives $c \leftarrow \mathsf{Enc}(pk, m_b)$, and outputs a guess for b.

Definition 3 (The two-scheme cycle). Let $\mathsf{E} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ and $\mathsf{E}' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ be encryption schemes with message spaces $\mathcal{M}$, $\mathcal{M}'$ and secret-key spaces $\mathcal{K}$, $\mathcal{K}'$, and let $\psi : \mathcal{K} \to (\mathcal{M}')^k$ and $\psi' : \mathcal{K}' \to \mathcal{M}^{k'}$ be injective encodings. The $(\mathsf{E}, \mathsf{E}')$-*cycle scheme* is $(\widehat{\mathsf{Gen}}, \widehat{\mathsf{Enc}}, \mathsf{Dec})$ where

$$\widehat{\mathsf{Gen}}(\kappa) = \big(sk,\ (pk,\ pk',\ \mathsf{Enc}^*(pk, \psi'(sk')),\ (\mathsf{Enc}')^*(pk', \psi(sk)))\big),$$

with $(sk, pk) \leftarrow \mathsf{Gen}(\kappa)$ and $(sk', pk') \leftarrow \mathsf{Gen}'(\kappa)$ drawn independently, and $\widehat{\mathsf{Enc}}$ ignores everything but pk: $\widehat{\mathsf{Enc}}(\cdot, m) = \mathsf{Enc}(pk, m)$. Decryption is E's own Dec.

Conjecture 1 (Micciancio, as printed). *For any (public key) encryption scheme* Enc *there is a (possibly different) encryption scheme* Enc′ *such that* $\mathsf{Enc}(pk, \cdot)$ *is secure in the presence of side information* $\mathsf{Enc}'_{pk'}(sk), \mathsf{Enc}_{pk}(sk')$ *for a randomly chosen key pair* (pk', sk').

Conjecture 2 (One formalization). *For every valid, IND-CPA secure public key encryption scheme* E *there exist a valid encryption scheme* E′ *and injective encodings* ψ, ψ' *such that the* $(\mathsf{E}, \mathsf{E}')$*-cycle scheme of Definition 3 is IND-CPA secure.*

Remark 1 (A degenerate reading to exclude). Conjecture 1 is trivially true if E′ is allowed to be an arbitrary triple of algorithms in the sense of Definition 1 without the validity requirement: take Enc′ to output a constant. Then $\mathsf{Enc}'_{pk'}(sk)$ carries no information about sk, and $\mathsf{Enc}_{pk}(sk')$ is an encryption of an independent random string, which IND-CPA security of E already covers. Nothing is cyclic about it. Conjecture 2 therefore requires E′ to be *valid* — so that $\mathsf{Enc}'_{pk'}(sk)$ really does determine sk to a holder of sk' — which is also what the intended application needs, since bootstrapping has to recover sk by decrypting that ciphertext. The source does not spell this out, and a reader should treat the requirement as part of the statement rather than as pedantry.

Remark 2 (Two more choices made here). The printed conjecture says "for any (public key) encryption scheme Enc", with no security hypothesis on Enc; Conjecture 2 restricts to IND-CPA secure E, without which the conclusion is false for trivial reasons. And the printed conjecture requires nothing of E′ beyond validity: in particular it is not required to be IND-CPA secure, though any E′ witnessing the conjecture must at least not leak sk outright.

Remark 3 (The source's advantage convention). The source measures IND-CPA advantage as $\delta = (\beta - \bar{\beta})^2/(\beta + \bar{\beta})$, where $\beta = \Pr[b' = b]$ and $\bar{\beta} = \Pr[b' = 1 - b]$, following the bit-security

definition of Micciancio and Walter, and lets the adversary output $\perp$ to express low confidence. For adversaries that always output a bit this is the square of the usual distinguishing gap, so the conjecture is the same statement under either convention.

4 Bibliography

[AP16] Navid Alamati and Chris Peikert. *Three's compromised too: circular insecurity for any cycle length from (ring-)LWE.* CRYPTO 2016, Part II, LNCS 9815, pp. 659–680. Springer, 2016.

[Gen09] Craig Gentry. *Fully homomorphic encryption using ideal lattices.* STOC 2009, pp. 169–178. ACM, 2009.

[GKW17a] Rishab Goyal, Venkata Koppula and Brent Waters. *Separating IND-CPA and circular security for unbounded length key cycles.* PKC 2017, Part I, LNCS 10174, pp. 232–246. Springer, 2017.

[GKW17b] Rishab Goyal, Venkata Koppula and Brent Waters. *Separating semantic and circular security for symmetric-key bit encryption from the learning with errors assumption.* EUROCRYPT 2017, Part II, LNCS 10211, pp. 528–557. 2017.

[HK17] Mohammad Hajiabadi and Bruce M. Kapron. *Toward fine-grained blackbox separations between semantic and circular-security notions.* EUROCRYPT 2017, Part II, LNCS 10211, pp. 561–591. 2017.

[KRW15] Venkata Koppula, Kim Ramchen and Brent Waters. *Separations in circular security for arbitrary length key cycles.* TCC 2015, Part II, LNCS 9015, pp. 378–400. Springer, 2015.

[KW16] Venkata Koppula and Brent Waters. *Circular security separations for arbitrary length cycles from LWE.* CRYPTO 2016, Part II, LNCS 9815, pp. 681–700. Springer, 2016.

[Mic24] Daniele Micciancio. *Fully composable homomorphic encryption.* IACR Cryptology ePrint Archive, Report 2024/1545, 2024. Published in IACR Communications in Cryptology 2(1), 2025.