CONJURA · OPEN PROBLEM

Every Fully Composable Homomorphic Encryption Scheme Yields a Circular-Secure One

Is circular security necessary for full composability?

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. The converse direction is a theorem of the source paper (its Theorem 6, the bootstrapping construction); this direction is open in both senses, with no partial result and no counterexample known.

Category. *Homomorphic Encryption*, *Foundations*.

Conjecture (informal). *Every known way of building fully homomorphic encryption goes through bootstrapping, and bootstrapping needs a circular security assumption: one publishes an encryption of the secret key under its own public key. Micciancio's reformulation of bootstrapping makes it possible to ask whether that assumption is avoidable without mentioning lattice noise at all. His Theorem 6 is one half of the answer — circular security plus a limited amount of homomorphism gives full composability. The conjecture is the other half: that a fully composable scheme can always be turned back into a circular-secure one, so that the two properties stand or fall together. It is not the claim that a composable scheme is* already *circular secure, which the paper says is most likely false; the circular-secure scheme is allowed to be a different scheme built from the first.*

1 The setting

An encryption scheme is $\mathcal{F}$-homomorphic, in the standard sense, if decrypting $\mathsf{Eval}(pk, f, \mathsf{Enc}^*(pk, \mathbf{m}))$ returns $f(\mathbf{m})$ for every $f \in \mathcal{F}$ and every message vector $\mathbf{m}$. As Gentry, Halevi and Vaikuntanathan observed [GHV10], this says nothing about what happens when a second evaluation is applied to the output of the first: the ciphertexts

Eval accepts and the ciphertexts it produces need not even have the same shape, so $\mathsf{Eval}(pk, g, \mathsf{Eval}(pk, f, c))$ may be meaningless.

The source paper's response is a definition that quantifies over *all* ciphertexts rather than over the freshly encrypted ones: Eval commutes with Dec (Definition 5). This is syntactically no more complicated than the standard definition and it implies arbitrary composition, so a scheme satisfying it supports homomorphic evaluation of any circuit whose gates lie in $\mathcal{F}$ (its Theorem 2).

Bootstrapping, restated as a transformation. Fix an injective key encoding $\psi : \mathcal{K} \to \mathcal{M}^k$. For $f \in \mathcal{F}$ and a ciphertext vector c, let $f_c^{\circlearrowleft} : \mathcal{M}^k \to \mathcal{M}$ send $\psi(sk)$ to $f(\mathsf{Dec}^*(sk, c))$ and everything else to $\perp$, and let $\mathcal{F}_\psi^{\circlearrowleft}$ be the set of all such functions. Gentry's bootstrapping [Gen09] is then exactly the following construction: given a scheme that is $\mathcal{F}_\psi^{\circlearrowleft}$-homomorphic, append $pk' = \mathsf{Enc}^*(pk, \psi(sk))$ to the public key and define $\mathsf{Eval}^{\circlearrowleft}((pk, pk'), f, c) = \mathsf{Eval}(pk, f_c^{\circlearrowleft}, pk')$ — that is, evaluate the function selected by c on the fixed ciphertext sitting in the public key. The source paper's Theorem 6 proves that the result is valid, $\mathcal{F}$-homomorphic and *fully composable*, and that it inherits IND-CPA security whenever the scheme one started from was ψ-circular IND-CPA secure.

So circular security (together with a limited homomorphic capability) *suffices* for full composability. The question the paper then poses, printed as a displayed question on its page 19, is whether it is also necessary:

> *Question: Is circular security necessary necessary to achieve full composability?*

(The repeated word is the source's.) The paper's own comment on why the question is well posed is that it "does not make any reference to encryption noise, and all concepts (circular security, homomorphic encryption and full composability) have well formalized abstract cryptographic definitions". This is the point of the reformulation: the recurring informal question of whether "noisy" ciphertexts are necessary for fully homomorphic encryption is, as the paper says, "not really well posed", because being noisy is a property of particular constructions rather than of encryption schemes as abstract objects.

Why the naive version is false. One might ask instead whether a fully composable scheme is already circular secure. The paper rules that out: "this is most likely false as one can adapt the simple counterexamples demonstrating the existence of circular insecure encryption schemes to the fully composable setting". There is a substantial body of such counterexamples [KRW15, KW16, AP16, GKW17a, GKW17b, HK17]. Hence the conjecture's "can be modified into": the circular-secure scheme is allowed to differ from the composable one, while still being built from it.

What settling it would give. The source paper states the consequence itself: "Given that circular security implies full composability (Theorem 6), proving the conjecture would show that circular security and full composability are essentially equivalent (assuming the existence of a non-composable encryption scheme with limited homomorphic properties, as those that can be built from lattices.)" A refutation would be at least as interesting, since it would exhibit a world in which arbitrary homomorphic computation composes and yet no circular-secure encryption exists — that is, a route to fully homomorphic encryption that provably does not pass through a circular security assumption.

What is *not* claimed. Nothing here says that a fully composable scheme can be built without circular security, nor that it cannot. Both directions are open, and the source paper offers no partial result towards either: this is a conjecture stated in a concluding section, not a theorem with a missing case.

2 Notation and parameters

- κ is the security parameter; $\mathcal{M}$ is a finite, fixed-length message space, $\mathcal{C}$ the ciphertext space and $\mathcal{K}$ the secret-key space, all possibly depending on κ.
- Enc^* and Dec^* are the componentwise extensions of Enc and Dec to vectors: $\mathsf{Enc}^*(pk, (m_1, \ldots, m_w)) = (\mathsf{Enc}(pk, m_1), \ldots, \mathsf{Enc}(pk, m_w))$ and likewise for Dec.
- $\mathcal{F} \subseteq \bigcup_{w \geq 0} \{f : \mathcal{M}^w \to \mathcal{M}\}$ is the set of functions a homomorphic scheme supports; w is the arity of the function under

discussion.

- $\psi : \mathcal{K} \to \mathcal{M}^k$ is an injective encoding of secret keys as message vectors, so that a secret key can be encrypted componentwise.
- $\perp \notin \mathcal{M}$ is the decryption-failure symbol.
- Correctness is required to hold with probability 1, following the source; the source notes this can be relaxed to a negligible failure probability but that perfect correctness is much more convenient in the homomorphic setting.

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 $\mathsf{Dec}(sk, c)$ outputs an element of $\mathcal{M} \cup \{\perp\}$. The scheme is *valid* if $\mathsf{Dec}(sk, \mathsf{Enc}(pk, m)) = m$ for all $m \in \mathcal{M}$ and all $(sk, pk) \leftarrow \mathsf{Gen}(\kappa)$.

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 $b' \in \{0, 1, \perp\}$. See Remark 3 for the source's measure of advantage.

Definition 3 (ψ-circular IND-CPA security). Let $\psi : \mathcal{K} \to \mathcal{M}^k$ be a (possibly randomized) key encoding. Define

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

where $(sk, pk) \leftarrow \mathsf{Gen}(\kappa)$ and $pk' \leftarrow \mathsf{Enc}^{*}(pk, \psi(sk))$. Then $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is *ψ-circular IND-CPA secure* if $(\mathsf{Gen}^{\psi}, \mathsf{Enc}^{\psi}, \mathsf{Dec})$ is IND-CPA secure. In words: the scheme stays secure when an encryption of its own secret key is published alongside the public key.

Definition 4 (Homomorphic encryption). A homomorphic encryption scheme with message space $\mathcal{M}$ and function set $\mathcal{F}$ is an encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ together with an algorithm Eval that on input pk, a function $f : \mathcal{M}^w \to \mathcal{M}$ in $\mathcal{F}$ and a vector $c \in C^w$ outputs a ciphertext $\mathsf{Eval}(pk, f, c) \in C$.

Definition 5 (Full composability). $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Eval})$ is a *fully composable $\mathcal{F}$-homomorphic* encryption scheme if $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is a valid encryption scheme and

$$\mathsf{Dec}\big(sk, \mathsf{Eval}(pk, f, c)\big) = f\big(\mathsf{Dec}^*(sk, c)\big)$$

for all $(sk, pk) \leftarrow \mathsf{Gen}(\kappa)$, all $f : \mathcal{M}^w \to \mathcal{M}$ in $\mathcal{F}$, and all $c \in C^w$ such that $\mathsf{Dec}^*(sk, c) \in \mathcal{M}^w$. The quantification over *all* such c, rather than over freshly encrypted ones, is the whole of the definition's content.

Conjecture 1 (Micciancio, as printed). *Any fully composable homomorphic encryption scheme can be modified into a circular secure one.*

Conjecture 2 (One formalization). *Let $\mathcal{F}$ be a set of functions. If there exists a valid, IND-CPA secure, fully composable $\mathcal{F}$-homomorphic encryption scheme, then there exist an injective encoding ψ and a valid, ψ-circular IND-CPA secure encryption scheme. The latter may be constructed from, and depend on, the former.*

Remark 1 (Conjecture 2 is the page's reading, not the source's). The source states only Conjecture 1, in one English sentence, and does not say what "modified into" quantifies over. Conjecture 2 makes three choices the source does not make explicit: that the conclusion is the existence of a circular secure scheme rather than a property of the original one; that ψ is existentially rather than universally quantified; and that the constructed scheme is not required to be homomorphic. The first is forced by the source's own remark that the modified scheme "can be different from (but still depend on) the original composable FHE scheme"; the third is consistent with the source's parenthetical that the reverse implication is what

needs "a non-composable encryption scheme with limited homomorphic properties". The second is a guess. A reader who intends to work on this should decide these for themselves before starting.

Remark 2 (Why the formalization is not vacuous). Circular secure encryption is known to exist under concrete assumptions such as LWE [ACPS09], so in the world we believe we live in the conclusion of Conjecture 2 holds outright. The content of the conjecture is the implication itself, in the usual sense in which one primitive is said to imply another: it asserts that no world contains fully composable homomorphic encryption and no circular secure encryption. That is exactly the claim that circular security is necessary, and it is not settled by any construction from a specific assumption. A reader who prefers a sharper form should read the implication as asking for a construction of the circular secure scheme from the composable one.

Remark 3 (The source's advantage convention). The source measures the advantage of an IND-CPA adversary 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 allows the adversary to output $\perp$. For adversaries that always output a bit, $\beta + \bar{\beta} = 1$ and δ is the square of the usual distinguishing gap, so nothing in this conjecture turns on the choice. The source says as much.

4 Bibliography

[ACPS09] Benny Applebaum, David Cash, Chris Peikert and Amit Sahai. *Fast cryptographic primitives and circular-secure encryption based on hard learning problems.* CRYPTO 2009, LNCS 5677, pp. 595–618. Springer, 2009.

[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.

[GHV10] Craig Gentry, Shai Halevi and Vinod Vaikuntanathan. *i-Hop homomorphic encryption and rerandomizable Yao circuits.* CRYPTO 2010, LNCS 6223, pp. 155–172. Springer, 2010.

[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. Springer, 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.