Anamorphic Cryptography

Security against New Powerful Attack Models

Hieu Phan
Head of C^2 Team at Telecom Paris
https://www.di.ens.fr/~phan/

November 7, 2025

Anamorphic encryption was introduced in 2022 by Persiano, Phan, and Yung [9]. This new research direction aims to ensure security under conditions that challenge the traditional Kerckhoffs's principle, enabling private communication even when facing an exceptionally powerful adversary (e.g., a dictator) who may have access to the secret key associated with the public key or may coerce the sender into transmitting unintended messages.

Since its introduction, this primitive has been further developed in numerous works, published at flagship conferences in cryptology (CRYPTO, EUROCRYPT, ASIACRYPT) or in privacy (PoPETs) [9, 8, 7, 11, 1, 3, 10, 5, 2, 6, 4]. More works in this domain can be found at the IACR Eprint: https://www.iacr.org/search/?q=Anamorphic.

Master's Internship and PhD Project

This proposal outlines a six-month Master's internship designed to prepare a PhD project that focuses on advancing the promising field of anamorphic cryptography across various communication contexts (signatures, zero-knowledge proofs, multi-party computation, post-quantum cryptography) by developing new technical and mathematical tools.

Ultimately, the objective is to design communication systems that remain secure against exceptionally powerful adversaries, whether arising from new

technologies or new policies, extending beyond the standard models typically considered in cryptographic literature.

References

[1] Fabio Banfi, Konstantin Gegier, Martin Hirt, Ueli Maurer, and Guilherme Rito. Anamorphic encryption, revisited. In *EUROCRYPT 2024, Part II*, LNCS, pages 3–32, June 2024.

[2] Davide Carnemolla, Dario Catalano, Emanuele Giunta, and Francesco Migliaro. Anamorphic resistant encryption: the good, the bad and the ugly. In *CRYPTO 2025, Part III*, LNCS, pages 472–503, August 2025.

[3] Dario Catalano, Emanuele Giunta, and Francesco Migliaro. Anamorphic encryption: New constructions and homomorphic realizations. In *EUROCRYPT 2024, Part II*, LNCS, pages 33–62, June 2024.

[4] Amit Deo and Benoit Libert. Anamorphic signatures with dictator and recipient unforgeability for long messages. In *Advances in Cryptology – ASIACRYPT 2025*. Springer-Verlag, 2025.

[5] Xuan Thanh Do, Giuseppe Persiano, Duong Hieu Phan, and Moti Yung. Anamorphism beyond one-to-one messaging: Public-key with anamorphic broadcast mode. In *EUROCRYPT 2025, Part III*, LNCS, pages 429–455, June 2025.

[6] Yevgeniy Dodis and Eli Goldin. Anamorphic-resistant encryption; or why the encryption debate is still alive. In *CRYPTO 2025, Part III*, LNCS, pages 440–471, August 2025.

[7] Miroslaw Kutylowski, Giuseppe Persiano, Duong Hieu Phan, Moti Yung, and Marcin Zawada. Anamorphic signatures: Secrecy from a dictator who only permits authentication! In Helena Handschuh and Anna Lysyanskaya, editors, *CRYPTO 2023, Part II*, volume 14082 of *LNCS*, pages 759–790, August 2023.

[8] Miroslaw Kutylowski, Giuseppe Persiano, Duong Hieu Phan, Moti Yung, and Marcin Zawada. The self-anti-censorship nature of encryption: On the prevalence of anamorphic cryptography. *PoPETs*, 2023(4):170–183, October 2023.

[9] Giuseppe Persiano, Duong Hieu Phan, and Moti Yung. Anamorphic encryption: Private communication against a dictator. In Orr Dunkelman and Stefan Dziembowski, editors, *EUROCRYPT 2022, Part II*, volume 13276 of *LNCS*, pages 34–63, May / June 2022.

[10] Giuseppe Persiano, Duong Hieu Phan, and Moti Yung. Public-key anamorphism in (CCA-secure) public-key encryption and beyond. In *CRYPTO 2024, Part II*, LNCS, pages 422–455, August 2024.

[11] Yi Wang, Rongmao Chen, Xinyi Huang, and Moti Yung. Sender-anamorphic encryption reformulated: Achieving robust and generic constructions. In Jian Guo and Ron Steinfeld, editors, *ASIACRYPT 2023, Part VI*, volume 14443 of *LNCS*, pages 135–167, December 2023.