HPC and Modern Cryptography: The Race Against Quantum

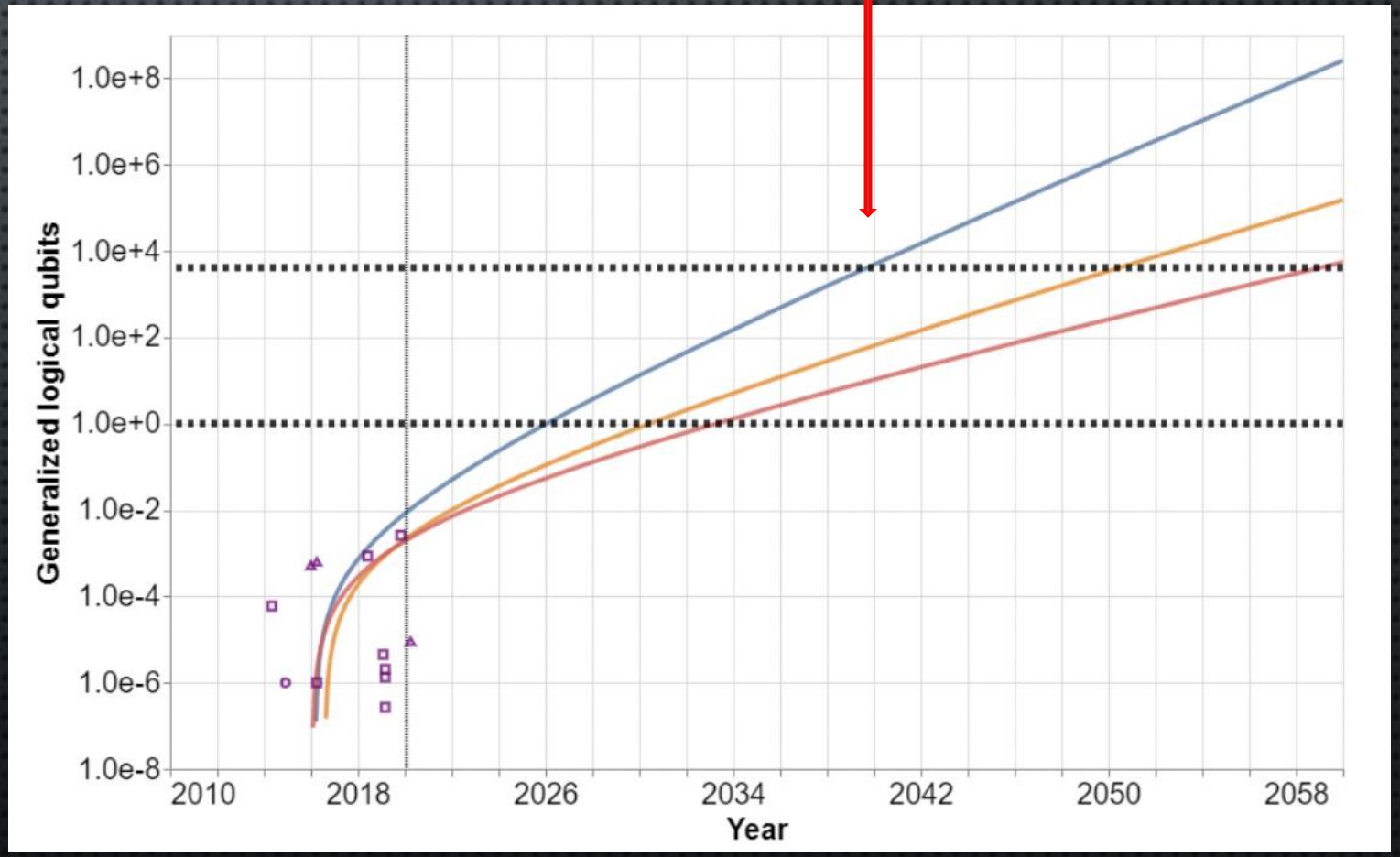
Brian Rosca

YOUR SECRETS HAVE AN EXPIRATION DATE

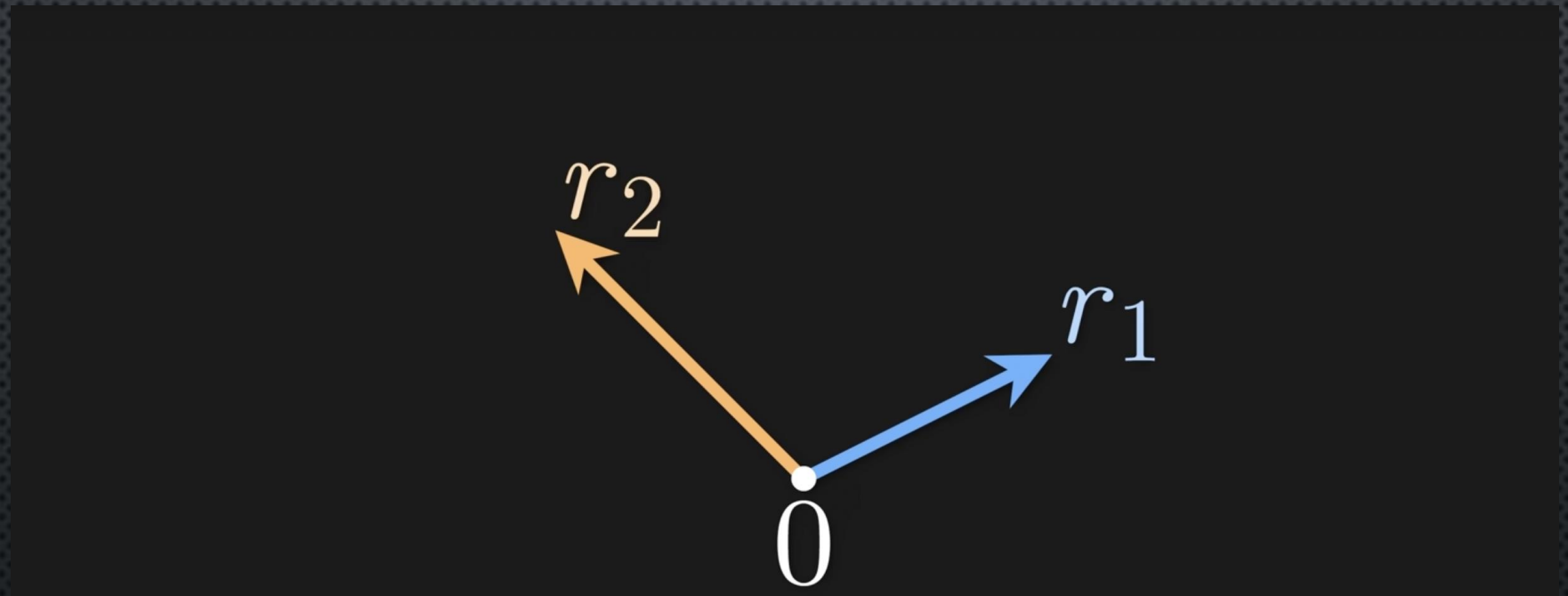
THE QUANTUM THREAT TO CLASSICAL CRYPTOGRAPHY

Shor's Algorithm:
RSA / Diffie-Hellman

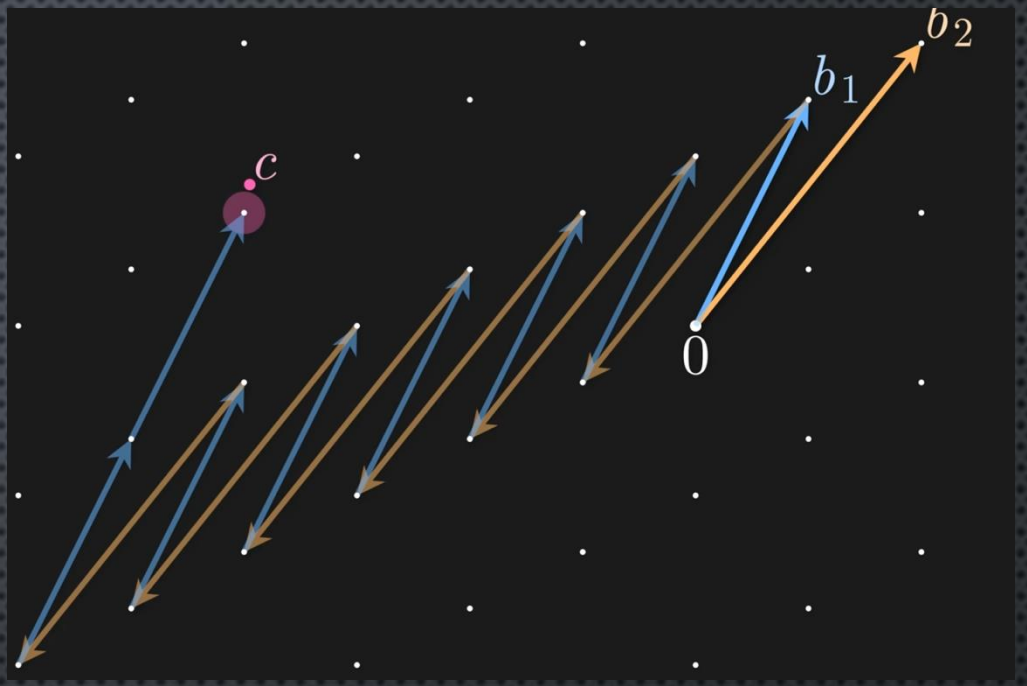
Grover's Algorithm:
AES-128

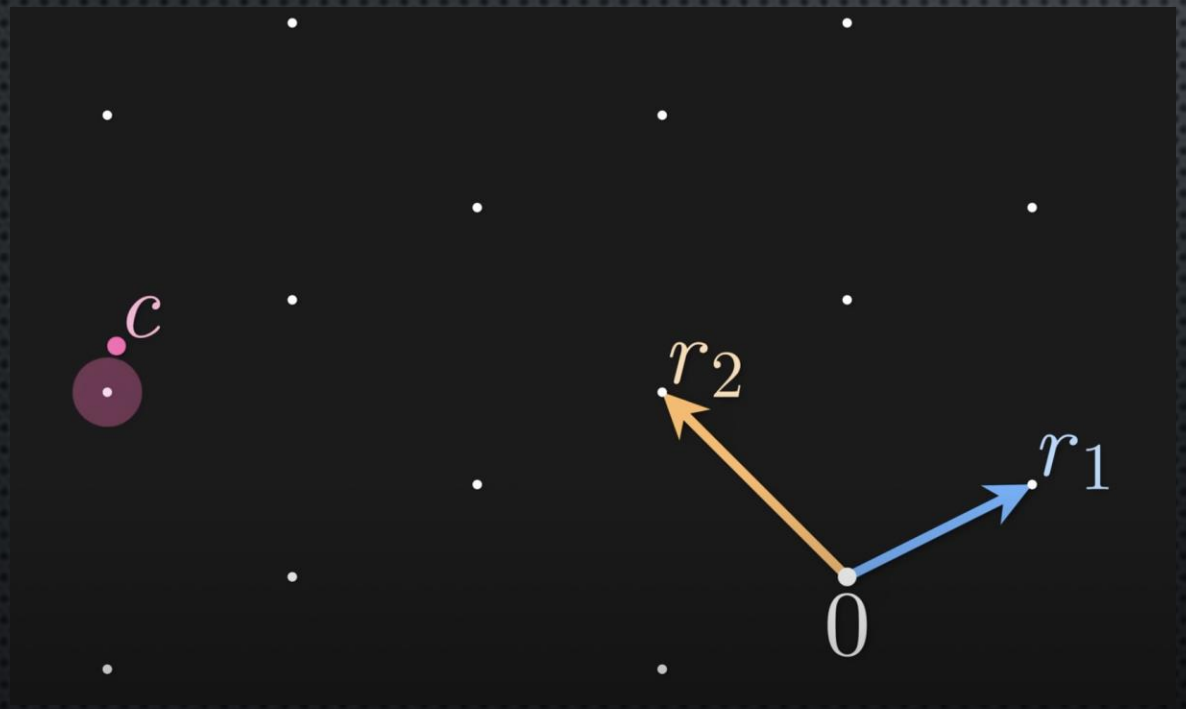


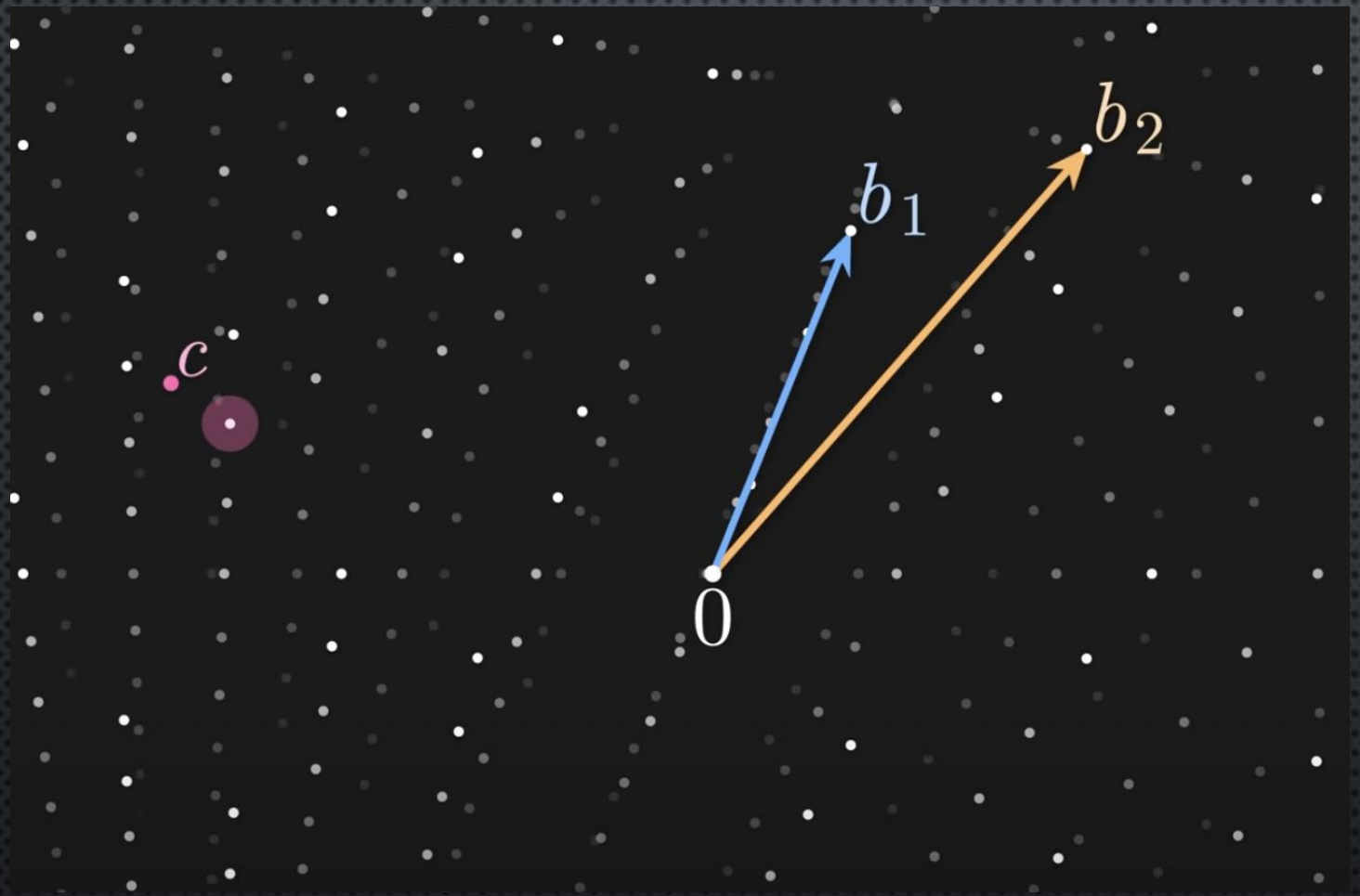
LATTICE-BASED CRYPTOGRAPHY



One application: CVP (Closest vector)







How do you know you have the closest point? You must check everything exhaustively!

Where does HPC come in? Security benchmarks

- Most computers can solve up to 200 dimensions, HPC can go to 900+
- Cryptanalysis algorithms targeting SVP/CVP: Lattice Reduction (LLL, BKZ)
- Direct solving (Enumeration, Sieving)

Performance challenges: implementation-dependent, memory-intensive

DISCUSSION

- – LUSA
- – NIST
- – INCREASE HARDWARE, INCREASE QUBITS
- – SECURE ENCRYPTION

REFERENCES

"How Quantum Computers Break The Internet... Starting Now." YouTube, uploaded by Veritasium, 18 May 2022, www.youtube.com/watch?v=-UrdExQW0cs

Chi, D. P., et al. "Lattice Based Cryptography for Beginners." IACR Cryptology ePrint Archive, 2015, p. 938, eprint.iacr.org/2015/938.

Mariano, A. "LUSA: the HPC Library for Lattice-Based Cryptanalysis." Cryptology ePrint Archive, Paper 2020/605, 2020, eprint.iacr.org/2020/605.

Mariano, A. "High Performance Algorithms for Lattice-Based Cryptanalysis." Technische Universität Darmstadt, 2016.

Bonnetain, X., et al. "Quantum Security Analysis of AES." IACR Transactions on Symmetric Cryptology, vol. 2019, no. 2, June 2019, pp. 55-93. doi:10.46586/tosc.v2019.i2.55-93.

Regev, O. "On Lattices, Learning with Errors, Random Linear Codes, and Cryptography." arXiv, 2024, arxiv.org/pdf/2401.03703.

Sevilla, J., and C. J. Riedel. "Forecasting Timelines of Quantum Computing." arXiv, Dec. 2020, arxiv.org/abs/2009.05045.

Barker, E., and A. Roginsky. "Transitioning the Use of Cryptographic Algorithms and Key Lengths." National Institute of Standards and Technology, Special Publication 800-131Ar2, Mar. 2019. doi:10.6028/NIST.SP.800-131Ar2.