Tabitha Ogilvie

Research Associate in Cryptography, Department of Informatics, King's College London
tabitha.l.ogilvie@gmail.com · tabog.github.io · github.com/TabOg · dblp · Google Scholar

Research

I work on lattice based cryptography, particularly the security of homomorphic encryption (HE). My PhD considered how HE can be deployed securely in practice, and my thesis is built on three sole-author papers. Alongside my PhD, I worked on deploying HE at Intel, and interned at Apple. This has led me to many aspects of applied lattice cryptography, including security notions, privacy-enhancing technologies and practical performance. I am interested in cryptanalysis and the concrete hardness of lattice problems, for HE and for post-quantum cryptography more widely. I contribute to the Lattice Estimator and to HE standardisation.

Positions

May 2026 – present	**Research Associate in Cryptography**, King's College London. I work on lattice based cryptography in KCL's Cryptography Group, funded by the ERC Consolidator Grant *Advanced Practical Post-Quantum Cryptography from Lattices* (PI: Martin Albrecht).
Jan – May 2026	**Research Intern**, King's College London. I joined KCL's Cryptography Group to work on the Lattice Estimator (see Software), funded by a Zama cryptanalysis grant.
Sep 2023 – Mar 2024	**PhD Intern**, Apple. I completed an internship at Apple Park in California, as part of the Systems Intelligence Machine Learning department. My former team's work is described in the Wally preprint (below), an Apple blog post and their RWC 2025 talk.
Jan – Jun 2023	**PhD Intern**, Intel Labs. I completed a research internship in the Security and Privacy Research group, working on homomorphic encryption and differential privacy.
Jun – Dec 2022	**PhD Intern**, Intel. I completed a software internship, working on the design and implementation of homomorphic encryption solutions for clients.
2021 – 2023	**External Researcher**, The Alan Turing Institute. I worked with the Privacy Preserving Data Analysis group.

Education

2019 – 2026	**PhD in Information Security**, Royal Holloway, University of London. Information Security Group; EPSRC CDT in Cyber Security for the Everyday. Thesis: *On the Security and Privacy of Approximate Homomorphic Encryption*, awarded Aug 2026. Supervisor: Elizabeth Quaglia.
2017 – 2018	**MMath Mathematics**, Exeter College, University of Oxford. First Class Honours, ranked 9th in the year. Dissertation: *A Comparison of the Approaches to Foundations of Statistical Inference of Fisher, Neyman, and Jeffreys*.
2014 – 2017	**BA Mathematics**, Exeter College, University of Oxford. First Class Honours.

Awards and funding

2019 – 2026	EPSRC-funded PhD studentship, CDT in Cyber Security for the Everyday, Royal Holloway.
2022	Finalist, Meta Research PhD Fellowship, Security and Privacy category.
2018	Runner-up, British Society for the History of Mathematics essay prize.
2017, 2018	Fitzgerald Prize for Excellence in Final Honour School, Oxford (BA and MMath).

Publications

Authors in alphabetical order, as is standard in cryptography.

Conference papers

CRYPTO 2026 — Jianhua Hou, Haodong Jiang, **Tabitha Ogilvie**. *Careful with the Ring! Concrete Hardness Gaps Between LWE and MLWE.* In *CRYPTO 2026, Part III*, LNCS 16802, pp. 462–497. Springer, Cham, 2026. [Springer]
Merger of my single-author submission (ePrint 2026/279, below) with concurrent work by Hou and Jiang (ePrint 2026/366).

ASIACRYPT 2025 — **Tabitha Ogilvie**. *IND-CPA-D and KR-D Security with Reduced Noise from the HintLWE Problem.* In *ASIACRYPT 2025, Part VII*, LNCS 16251, pp. 263–295. Springer, Singapore, 2025. [DOI] [ePrint]

CT-RSA 2024 — **Tabitha Ogilvie**. *Differential Privacy for Free? Harnessing the Noise in Approximate Homomorphic Encryption.* In *CT-RSA 2024*, LNCS 14643, pp. 292–315. Springer, Cham, 2024. [DOI] [ePrint]

SAC 2023 — Anamaria Costache, Benjamin R. Curtis, Erin Hales, Sean Murphy, **Tabitha Ogilvie**, Rachel Player. *On the Precision Loss in Approximate Homomorphic Encryption.* In *SAC 2023*, LNCS 14201, pp. 325–345. Springer, Cham, 2024. [DOI] [ePrint]

WAHC 2020 — **Tabitha Ogilvie**, Rachel Player, Joe Rowell. *Improved Privacy-Preserving Training using Fixed-Hessian Minimisation.* In *WAHC 2020*, pp. 6–18, 2020. [DOI] [ePrint]

Preprints and full versions

ePrint 2026 — **Tabitha Ogilvie**. *On the Concrete Hardness Gap Between MLWE and LWE.* Cryptology ePrint Archive, Report 2026/279. [ePrint]
Single-author submission, merged with ePrint 2026/366 to form the CRYPTO 2026 paper above.

arXiv 2024 — Hilal Asi, Fabian Boemer, Nicholas Genise, Muhammad Haris Mughees, **Tabitha Ogilvie**, Rehan Rishi, Kunal Talwar, Karl Tarbe, Akshay Wadia, Ruiyu Zhu, Marco Zuliani. *Wally: Batched Private Nearest Neighbor Search at Scale.* arXiv preprint, 2024. [arXiv]

Thesis

PhD thesis 2026 — **Tabitha Ogilvie**. *On the Security and Privacy of Approximate Homomorphic Encryption.* PhD thesis, Royal Holloway, University of London, 2026. [Pure]

Software

2025 – present — **Contributor**, Lattice Estimator.
The Lattice Estimator is a widely used tool for estimating the security of lattice based schemes. I extended it to handle sparse secrets, which it previously could not estimate effectively, improved the accuracy and speed of its hybrid attacks, and added parameter sets from HE standards and libraries. I also help maintain it, addressing issues and reviewing pull requests, and presented this work at the 2026 HomomorphicEncryption.org Standards Meeting.

2022 – 2023 — **Contributor**, HElib.
During my internships at Intel, I extended HElib's private set intersection and database lookup logic to support more expressive queries.

Talks

Invited talks

Nov 2026 — *Concrete Hardness Gaps Between MLWE and LWE.* London Crypto Day 2026, Royal Holloway, University of London.

Mar 2026 — *Lattice Estimator Updates and the Concrete Hardness Gap Between LWE and RLWE.* 9th HomomorphicEncryption.org Standards Meeting, Seoul.

Mar 2026	*On the Concrete Hardness Gap Between MLWE and LWE.* Cryptology Group seminar, CWI, Amsterdam.
Jun 2023	*Differential Privacy for Free? Harnessing the Noise in Approximate Homomorphic Encryption.* FHE.org meetup series, online. [video]
May 2022	*An Introduction to Homomorphic Encryption.* Privacy-Preserving Data Analysis Workshop, Digital Futures, University of Manchester.

Conference presentations

Aug 2026	*Careful with the Ring! Concrete Hardness Gaps Between LWE and MLWE.* CRYPTO 2026, Santa Barbara. [slides]
Dec 2025	*IND-CPA-D and KR-D Security with Reduced Noise from the HintLWE Problem.* ASIACRYPT 2025, Melbourne.
May 2024	*Differential Privacy for Free? Harnessing the Noise in Approximate Homomorphic Encryption.* CT-RSA 2024, RSA Conference, San Francisco.
Dec 2020	*Improved Privacy-Preserving Training using Fixed-Hessian Minimisation.* WAHC 2020, online.

Service and leadership

2026 – present	Member, Sparse Secret Working Group, HomomorphicEncryption.org.
2021 – present	Subreviewer: CRYPTO 2026, Communications in Cryptology 2025, EUROCRYPT 2025, ISC 2024, ASIACRYPT 2022, PQCrypto 2021, SAC 2021, CODASPY 2021.
2026 – 2027	Aurora leadership development programme for women in higher education, Advance HE.
2020 – 2022	Co-president, WISDOM, Royal Holloway: a student society in Mathematics, Computer Science, Information Security and Electronic Engineering supporting under-represented groups. Organised panel events and chaired a cross-department research showcase.
2014 – 2018	Outreach ambassador for the Oxford mathematics department and the university, encouraging students from under-represented backgrounds to consider STEM and higher education.

Teaching and supervision

Supervision

2026 – 2027	Co-supervisor (with Ngoc Khanh Nguyen), BSc final-year projects, King's College London.

Teaching

Oct – Dec 2026	Teaching Assistant, undergraduate (BSc) cryptography, King's College London.
2025	Teaching Assistant, Information Privacy, University of London MSc in Cyber Security (distance learning).
2021	Teaching Assistant, Security Management, Royal Holloway, University of London.

Referees

Available on request.