

QRL Backs University of Manchester Cryptographers to Strengthen Post-Quantum Signature Infrastructure

Grant supports Dr Bernardo Magri, Dr Tako B. Fouotsa and Dr Trey Li, investigating isogeny-based cryptography, blockchain and post-quantum hardness assumptions

ZUG, SWITZERLAND, October 15, 2026 /EINPresswire.com/ -- The Quantum Resistant Ledger (QRL) has awarded a research grant to the University of Manchester in support of post-quantum cryptography. The grant supports Dr Bernardo Magri, Senior Lecturer in Cryptography and Principal Investigator; Dr Tako Boris Fouotsa, Lecturer in Cryptography and Co-Investigator; and Dr Trey Li, Research Fellow and Co-Investigator, all within the Systems Security (S2) group in the Department of Computer Science.

The grant targets the signature layer of the post-quantum transition. Digital signatures authorise every blockchain transaction, every software update and every TLS certificate on the internet. The schemes in use today, ECDSA, EdDSA and RSA, can all be broken by a cryptographically relevant quantum computer running Shor's algorithm. Replacing them is the most exposed and most technically demanding part of the migration, and the researchers supported by this grant work at the heart of that challenge.

The researchers

The three researchers bring complementary expertise across post-quantum cryptography.

Dr Bernardo Magri works across the foundations of blockchain, secure multi-party computation and subversion-resilient cryptography. Before joining Manchester he was a postdoctoral researcher in the cryptography group at Aarhus University.

Dr Tako Boris Fouotsa specialises in isogeny-based cryptography and is the author of several



isogeny-based key exchange, encryption and signature schemes. He is a contributor to SQIsign, the most compact post-quantum signature scheme in NIST's additional signatures process. He joined Manchester in January 2026 from the Security and Cryptography Laboratory at EPFL.

Dr Trey Li is a mathematician working on arithmetic geometry and quantum computing, with interests in post-quantum cryptography and mathematical physics. He is the originator of the Hecke problems, the noisy subset product problem, and unknown-coefficient multivariate exponential equations. His work brings new mathematical ideas to cryptographic applications, including digital signatures, key exchange, and obfuscation. His research also explores existing post-quantum directions, including lattices, isogenies, codes, and multivariate systems. He joined the University of Manchester as a Research Fellow in June 2024.

All outputs will be published openly, with reference implementations released as open-source code.

Why post-quantum signature infrastructure matters now

The standards exist; the infrastructure does not yet. NIST published its first post-quantum signature standards, ML-DSA (FIPS 204) and SLH-DSA (FIPS 205), in August 2024. The UK's National Cyber Security Centre has set 2035 as the date by which migration should be complete, with priority systems moved by 2031.

Standardisation is the start of the work, not the end of it. The current standards carry real costs. An ML-DSA-87 signature is 4,627 bytes against roughly 64 bytes for ECDSA, and its public key is 2,592 bytes against 33. For a blockchain, that is a direct cost in block space, bandwidth and storage on every node, for every transaction, permanently.

The gap is wider still for the advanced functionality that wallets, custodians and consensus protocols depend on. Threshold signing, aggregation and blind signatures are mature for elliptic curves and immature for post-quantum schemes. Until they catch up, institutions face a choice between quantum security and the operational tooling they already rely on.

Blockchains feel this first. Public keys are exposed on-chain, assets cannot be re-secured without the owner acting, and a forged signature is final. QRL has run on hash-based XMSS signatures since its 2018 launch and uses ML-DSA-87 in QRL 2.0. Funding the research that makes post-quantum signatures smaller, faster and more capable is a direct investment in the infrastructure QRL and the wider industry will run on.

"Post-quantum security is not a future problem for QRL. It has been our foundation from day one. Supporting world-class cryptographers is how we make sure the next generation of post-quantum tooling is built openly and for everyone. Manchester's team is exactly the right group to do it." Dr Joseph Kearney, Technical Advisor, QRL

“We are very excited to collaborate with the QRL Foundation on advancing the cryptographic foundations of post-quantum secure blockchains. Our main goal is to enable the advanced cryptographic functionality that real-world blockchain applications require. Through this collaboration, we hope to help bridge the gap between theoretical advances in post-quantum cryptography and their practical deployment in blockchain systems.” Dr Bernardo Magri (PI), Dr Tako Boris Fouotsa (Co-Investigator), University of Manchester.

“Blockchain is full of hard, real-world problems that pure mathematics can solve. This collaboration gives us the opportunity to turn abstract mathematical ideas into practical tools for post-quantum blockchains.” - Dr Trey Li, Research Fellow and Co-Investigator, University of Manchester.

About The Quantum Resistant Ledger

The Quantum Resistant Ledger (QRL) is a post-quantum blockchain secured by hash-based XMSS signatures since its mainnet launch in 2018. QRL 2.0, now on public testnet, adds proof-of-stake consensus, NIST-approved ML-DSA signatures and EVM-compatible smart contracts written in the Hyperion language.

More information is available at <https://www.theqrl.org>.

About the University of Manchester

The University of Manchester is recognised globally for its pioneering research, outstanding teaching and learning, and commitment to social responsibility. Part of the Russell Group, we're ranked 35th in the QS World University Rankings, 2025 (6th in the UK) and 52nd in the Academic Ranking of World Universities, 2024. Our Department of Geography is ranked 9th in the world by QS. The power of our social and environmental impact has been recognised on a global scale as the only university in the top ten in both the QS World University Sustainability Rankings and Times Higher Education Impact Rankings, for our contribution towards the United Nations' Sustainable Development Goals (SDGs).

More information is available at <https://www.manchester.ac.uk/about/>.

Media contact

Quantum Resistant Ledger: press@theqrl.org

University of Manchester: jessica.shaw@manchester.ac.uk

Joseph Kearney
Quantum Resistant Ledger
press@theqrl.org

Visit us on social media:

[X](#)

[LinkedIn](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/949841100>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.