

RITICS Newsletter



Welcome to the final RITICS newsletter of 2024

This has been an incredibly busy year, with RITICS hosting five events. One highlight was our first-ever 2-day **RITICS Fest**, which welcomed 110 attendees over the course of the event. This successful gathering provided early-career researchers with an invaluable opportunity to present their work during dynamic 5-minute "madness" sessions, gaining exposure and feedback from an engaged audience.

With this success RITICS Fest is set to return in 2025! Look out for our Spring newsletter for more information about how to get involved.

Another highlight of 2024 was the announcement of three fellowships, including our first ever Industry Fellowship. All three fellowships are currently at their midway point, and we are excited to see what their impact will be. Find out more about our activities in 2024 in our Annual Report

Looking ahead to 2025, we are gearing up for a strong start! The **RITICS Showcase** is scheduled for **Tuesday 28th January 2025**, with full details below.

In September, we announced the call for applications for the 2025 Fellowship, receiving an impressive 26 submissions. We expect to announce the successful applicants in the new year. Stay tuned for updates.

Thank you for being part of an incredible year. Here's to an even more exciting 2025!

We wish you a Merry Christmas and a Happy New Year and we look forward to welcoming you all at the RITICS Showcase.

REGISTER TO ATTEND RITICS SHOWCASE

28th January, Scale Space, White City, W12 7RZ

Join us for an exciting in-person event, the **RITICS Showcase 2025**, Discover the latest progress and findings from RITICS fellows and RITICS projects. Engage with industry leaders and experts, and immerse yourself in thought-provoking discussions and presentations. Don't miss this opportunity to connect, learn, and be inspired by the cutting-edge solutions shaping our digital future.

Featured speakers:

1. **Towards Security Assurance for Cyber Physical Systems** - *Dr. Ashraf Tantawy*, Cranfield University
2. **OT Penetration Testing** - *Dr. Ric Derbyshire*, Orange Cyber Defense
3. **Exploring Security and Motivation** - *Dr. Neetesh Saxena*, Cardiff University

We'll be announcing more speakers in the coming weeks.

: <https://www.eventbrite.co.uk/e/ritics-showcase-2025-tickets-1096100479039?aff=oddtcreator>

PROJECT UPDATE

Post-Quantum Blockchains Based on FALCON++

In recent years, blockchain technology has emerged as a transformative force in the digital landscape, best known as the foundation of cryptocurrencies such as Bitcoin and Ethereum. However, cryptocurrencies represent just one of many potential applications of blockchain. The technology's scope extends to areas such as smart contracts, e-voting, and the Internet of Things (IoT). With the NIST standardization process marking the start of a broader transition to post-quantum cryptography, our project aims to explore these advances by applying a lattice-based post-quantum digital signature scheme known as FALCON (Fast-Fourier Lattice-based Compact Signatures over NTRU). We are working on modifying the existing trapdoor sampler in FALCON to incorporate Monte Carlo Markov Chain (MCMC) sampling, enhancing its security.

A new idea of our research has been addressing HAWK, an optimized signature scheme. It is based on the equivalence problem of quadratic forms, which has become a foundational concept in lattice-based cryptography. HAWK's efficiency and simplicity make it an attractive alternative to FALCON, encouraging further cryptanalysis. Any successful cryptanalytic attack on this scheme could significantly impact related cryptosystems. Our work has focused on the spinor genus, which provides a refined classification of quadratic forms within the field of lattice-based cryptography.

Our findings have been recognized with acceptance at a prestigious cryptography conference:

Cong Ling, Jingbo Liu, and Andrew Mendelsohn, "On the Spinor Genus and the Distinguishing Lattice Isomorphism Problem," Asiacrypt 2024.

Further progress is being made in this area, with another paper submission planned for later this year.

WHAT YOU'VE MISSED SO FAR:

1. [RITICS Annual Report for 2024](#)
2. [RITICS Fest 12th and 13th September 2024 Abstracts are now available](#)