Advancing 6G Security: Insights, Innovations, and Collaborations from the CONFIDENTIAL6G

Welcome to the Third Issue of the CONFIDENTIAL6G Newsletter! In this edition, we bring you the latest updates on our cutting-edge research, key events, and progress towards securing the future of 6G networks.

Explore how CONFIDENTIAL6G is driving innovations in cryptography, privacy, and mobile network security.

Cryptography | Confidential Computing | Confidential Networking

About CONFIDENTIAL6G

CONFIDENTIAL6G is a project focused on ensuring secure and private computation across the cloud-edge continuum in 6G networks. By developing advanced cryptographic techniques, tools, and libraries, the project addresses the critical need for privacy preservation and data security in diverse environments. One of its key goals is to prepare for the threat of quantum computers, which could break current encryption methods, by exploring innovative cryptographic solutions.

With a consortium of 13 partners from 10 countries, including Austria, Germany, and Finland, CONFIDENTIAL6G brings together industry expertise and academic research. The project is financed by the EU Commission with a total budget of €5 million.

Learn More

CONFIDENTIAL6G News

Thomas Attema, from TNO: Confidential Computing and Post-Quantum Cryptography for 6G at Fuse5G Event

Thomas Attema from TNO, a CONFIDENTIAL6G project partner, spoke at the FUSE5G event in Utrecht on the security and privacy needs of 5G and 6G networks. He highlighted CONFIDENTIAL6G's solutions for secure communication, particularly for critical industries, and engaged with experts on building resilient wireless networks.

Learn More

Madhusanka Liyanage from UCD, CONFIDENTIAL6G Partner, Shares Insights at 6Gsec CP² Event

Madhusanka Liyanage from University Cllege Dublin, a CONFIDENTIAL6G project partner, highlighted use of advanced cryptography and privacy-preserving technologies to address these issues.
The event fostered discussions on building secure and resilient 6G infrastructures with input from leading experts.

Learn More

Telefónica and Zentrix Lab Introduce CONFIDENTIAL6G Project at OpenInfra Edge Computing Working Group

Telefónica and Zentrix Lab introduced the CONFIDENTIAL6G project at the OpenInfra Edge Computing Working Group, highlighting efforts to tackle security and privacy challenges in 6G edge computing and develop secure communication protocols for decentralized networks.

Learn More

Madhusanka Liyanage from UCD, CONFIDENTIAL6G Partner, Shares Insights at 6Gsec CP² Event

UCD researchers presented the TRUST-SPEC framework, part of CONFIDENTIAL6G, to enhance trust and security in 6G networks. TRUST-SPEC integrates advanced protocols to improve resilience and protect against emerging threats, showcasing UCD's role in advancing secure wireless communication.

Learn More

CONFIDENTIAL6G Showcases Innovations at 2024 EuCNC & 6G Summit

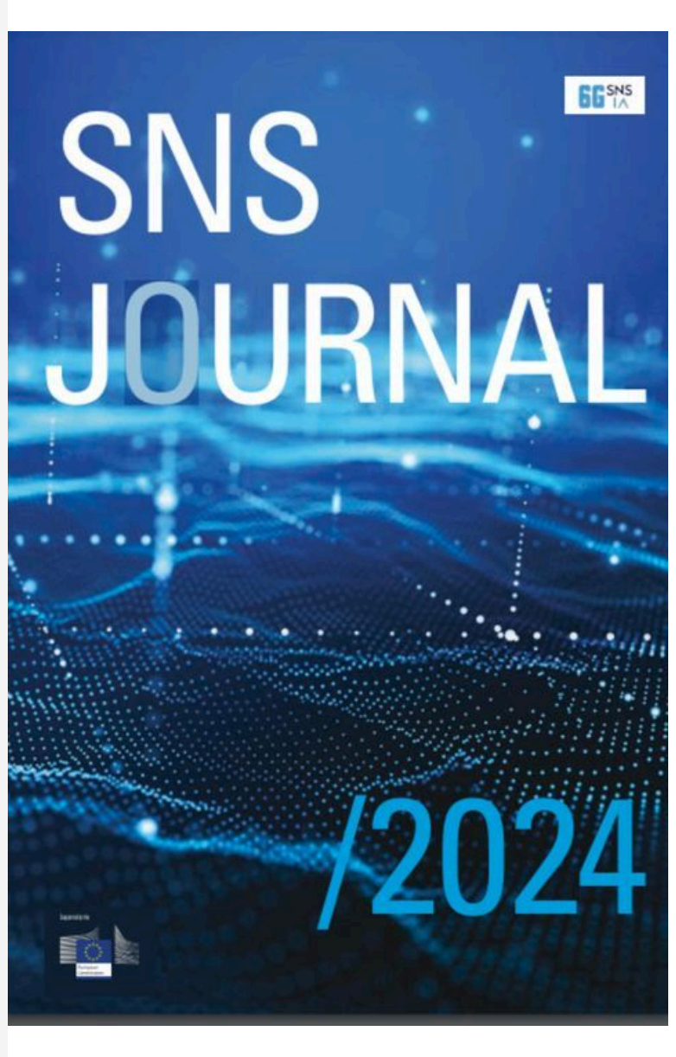
CONFIDENTIAL6G participated in the 2024 EuCNC & 6G Summit, presenting its latest innovations and engaging with the broader research and industry community. The team showcased advancements in secure 6G communication technologies, focusing on privacy, cryptography, and network security. Attendees had the opportunity to learn more about the project's ongoing work, which is aimed at addressing key security challenges in 6G networks. The summit provided a platform for open discussions, enabling valuable feedback and collaboration with other experts in the field.

Learn More

CONFIDENTIAL6G Project Meeting Held in Dublin, Ireland

The CONFIDENTIAL6G consortium recently gathered in Dublin, Ireland, for a key project meeting hosted by University College Dublin (UCD). The meeting brought together project partners to discuss progress, share insights, and plan the next phases of the project. Topics included advancements in 6G security, cryptography, and privacy-preserving technologies, as well as collaborative efforts to address the technical challenges posed by next-generation networks. This face-to-face meeting allowed partners to align their strategies and ensure smooth collaboration as the project moves forward in its mission to enhance security for future 6G networks.

Learn More



New Issue of SNS Journal Explores CONFIDENTIAL6G's Advances in 6G Security and Cryptography

Discover how the CONFIDENTIAL6G Project is advancing secure, private computation for 6G with cutting-edge cryptography to counter threats like quantum computing.

We're focused on open-source solutions, vendor compatibility, and GDPR compliance, while developing privacy-preserving AI/ML in decentralized networks.

SNS Journal 2024 highlights security, cryptography, and confidential computing in 6G.

Learn More

CONFIDENTIAL6G Publications

New Limits of Provable Security: Sven Schäge from Eindhoven University of Technology on ElGamal Encryption

Sven Schäge, a CONFIDENTIAL6G partner from Eindhoven University of Technology, has made significant strides in cryptography by proving that ElGamal encryption cannot be CCA1-secure, resolving a long-standing problem. His research uses meta-reduction techniques, extending to other cryptographic systems like Paillier and Damgård–Jurik, highlighting new security limitations. This work plays a key role in advancing secure communication technologies within the CONFIDENTIAL6G project.

Learn More

Foundations of Adaptor Signatures: Addressing Security Gaps in Blockchain Applications

Paul Gerhart and Dominique Schröder from FAU, along with Pratik Soni and Sri AravindaKrishnan Thyagarajan, revisit adaptor signatures, which extend regular signatures for blockchain applications like conditional payments. Their research uncovers security gaps in current models, particularly in coin-mixing and oracle-based payment protocols. They propose new definitions to fix these issues and present secure constructions, including the first adaptor signature schemes for Camenisch-Lysyanskaya (CL), BBS+, and Waters signatures, offering stronger security in blockchain systems and valuable tools for cryptographers.

Learn More

Blockchain-Regulated Key Refreshment Mechanism for IoT in CONFIDENTIAL6G

Madhusanka Liyanage from University College Dublin, along with co-authors, has contributed to research on a blockchain-regulated, verifiable, and automatic key refreshment mechanism for IoT systems. This mechanism addresses the challenge of ensuring security compliance in complex IoT architectures by enabling transparent, regular key updates. Utilizing blockchain and smart contracts, the solution allows verification of key freshness, enhancing trust in IoT systems. The research, supported by the CONFIDENTIAL6G project, demonstrates the viability and security of the mechanism using Ethereum and Hyperledger Fabric.

Learn More

CONFIDENTIAL6G Collaborations

CONFIDENTIAL6G at SECURENET 2024: Advancing Mobile Network Security

The SECURENET 2024 Summit, held at University College Dublin, was a landmark event organized by the UCD School of Computer Science's Network Softwarization and Security Labs (NETSLAB), the SFI Connect Center, and the Horizon Europe CONFIDENTIAL6G project.

The CONFIDENTIAL6G team shared updates on their work developing new security solutions for 6G networks, focusing on privacy protection and cryptography. The summit provided an excellent platform for exchanging ideas with other experts and addressing the security challenges of next-generation networks.

Don't miss out on our upcoming issue of the newsletter; subscribe now to stay in the loop with the latest developments in 6G technology!

Subscribe

Stay tuned!

Stay updated on all our latest news, developments, research and general information regarding the CONFIDENTIAL6G project.

Co-funded by the European Union