UNSW SYDNEY

Quadseal Hardware Attack Mitigation

Quadseal is a mitigation technique to stop attackers from obtaining secret keys from block ciphers. Where a conventional encrypting device is accessible it is possible to obtain the secret key in less than 10 minutes. With Quadseal the attacker is stymied, making communications channels and other protected items far safer.

Competitive advantage

- First known countermeasure that can thwart both power and fault attacks
- Smallest power area product among all available technologies
- Embedded Systems Laboratory has over 20 years' experience in hardware–software co-design, security and design automation

Impact

- Enhanced communications security

Successful applications

- Our work in pipelined processing systems has been used extensively by Canon Inc.
- Optimised systems used within multiple other commercial environments

Capabilities and facilities

- Side channel analysis equipment for measuring power and electromagnetic radiation
- SASEBO FPGA-based boards to create circuits that can be tested
- Custom made processor boards for testing of software countermeasures

Our partners

- Canon Information Systems Research Australia
- Seeing Machines Inc.
- Defence Science and Technology (DST)

More Information

Professor Sri Parameswaran

School of Computer Science and Engineering

T: +61 (0) 2 9385 7223
E: sri.parameswaran@unsw.edu.au

UNSW Knowledge Exchange

knowledge.exchange@unsw.edu.au

www.capabilities.unsw.edu.au

+61 (2) 9385 5008