WASP Project Course 2025

Mitigating Power Analysis Side-Channel Vulnerabilities in Embedded Fully Homomorphic Encryption Implementations

Background

Fully Homomorphic Encryption (FHE) offers a powerful way to compute on encrypted data, enabling privacy in areas like cloud computing and machine learning. However, implementing advanced FHE schemes (e.g., CKKS, TFHE) on resource-constrained embedded systems like microcontrollers or FPGAs introduces significant security risks. While mathematically secure, the physical act of performing cryptographic operations on these devices can leak secret key information through side channels, such as variations in power consumption, thereby defeating the purpose of FHE.

This project directly addresses the threat of power analysis side-channel attacks against FHE implementations on embedded platforms. Students will investigate these vulnerabilities by implementing FHE schemes on target hardware, using tools like ChipWhisperer to detect power leakage, and then designing, implementing, and evaluating countermeasures. A key aspect is analyzing the trade-off between the achieved security improvement and the performance impact (speed, resource usage) of the implemented protections.

Constraints:

- Requires working with specific embedded hardware platforms (MCUs/FPGAs).
- Requires using the ChipWhisperer side-channel analysis toolchain.
- Focuses on power analysis side channels.
- Must consider embedded system resource limitations.

Participants

Industrial partner: Erik Mårtensson

Industrial supervisor: Erik Mårtensson, erik.martensson@advenica.com

Academic supervisor: Thomas Johansson, thomas.johansson@eit.lth.se, LTH; **:** Qian Guo,

qian.guo@eit.lth.se, LTH;

Coordinating WARA representative: no

Suggested WASP PhD students: Maggie Trân, Markus Berthilsson, Karim Khalil

Challenges to investigate

- Efficiently implementing FHE on target embedded hardware.
- Identifying power analysis leakage points using ChipWhisperer.
- Designing and implementing effective side-channel countermeasures.
- Evaluating the effectiveness of implemented countermeasures.
- Quantifying the performance overhead vs. security level trade-off.

Resources

- Target embedded hardware platforms (MCUs/FPGAs).
- ChipWhisperer side-channel analysis platform.
- Relevant FHE libraries and literature.
- Academic supervisor expertise.
- Industrial supervisor expertise.

Deliverables

- Baseline and Protected FHE Implementations (Code).
- Side-Channel Analysis & Countermeasure Evaluation Report.
- Final Project Presentation.

References

- Cheon, J. H., Kim, A., Kim, M., & Song, Y. (2017). Homomorphic encryption for arithmetic of approximate numbers. *ASIACRYPT 2017*. (CKKS Scheme)
- Chillotti, I., Gama, N., Georgieva, M., & Izabachène, M. (2020). TFHE: Fast fully homomorphic encryption over the torus. *Journal of Cryptology*, *33*(1). (TFHE Scheme)
- Microsoft SEAL GitHub Repository: https://github.com/microsoft/SEAL (FHE Library)
- OpenFHE GitHub Repository: https://github.com/openfheorg/openfhe-development (FHE Library)
- ChipWhisperer GitHub Repository: https://github.com/newaetech/chipwhisperer (Side-Channel Tool)

Keywords

Homomorphic encryption, side-channel attacks, embedded security, hardware security, privacy-preserving machine learning.