Session 2: Physical Attack Protections

Preventing Distinguishability between Multiplication and Squaring Operations

Alkistis Aikaterini Sigourou (Leibniz IHP), Zoya Dyka (Leibniz IHP and BTU Cottbus-Senftenberg), Peter Langendoerfer (BTU Cottbus-Senftenberg), Ievgen Kabin (Leibniz IHP)

Abstract: Scalar multiplication kP is a critical operation in Elliptic Curve Cryptosystems (ECC), often targeted by Side-Channel Analysis (SCA). Despite strategies based on atomic patterns to enhance security, the binary kP algorithms remain susceptible to simple SCA due to energy consumption variations in field multipliers during passing two different or two identical operands. This vulnerability arises independent of the multiplication method used. We implemented and analysed two mitigation techniques: one involving data redirection and another focusing on bus reloading.

Logic Locking with Lightweight Cryptography

Levent Aksoy (TU Tallinn), Muhammad Sohaib Munir (TU Tallinn), Sedat Akleylek (U Tartu)

Abstract: In the globalized integrated circuit (IC) manufacturing supply chain era, the hardware security threats, such as overproduction and piracy, have been causing serious damage to the IC design industry. Many techniques proposed to mitigate these threats have been broken since they do not rely on provably secure algorithms, and the ones using cryptography algorithms increase the hardware complexity significantly and have been vulnerable to removal and power analysis attacks. In this paper, we integrate a lightweight cryptography algorithm into a prominent logic locking technique and introduce a computer-aided design tool called LINDA, which automates the logic encryption process. Experimental results show that the secure designs generated by LINDA have significantly less hardware complexity when compared to those generated by previously proposed techniques using cryptography algorithms and are resilient to existing removal, algebraic, and logic locking attacks.

Lifecycle Protecting Integrated Circuits Using Physical Unclonable Functions

Michael Pehl, Carl Riehm, Tim Music (TU Munich), Valentin Huber, Matthias Hiller (FhG AISEC), Ralf Brederlow (TU Munich)

Abstract: In globalized markets, protecting chips throughout the supply chain and their entire lifecycles becomes increasingly difficult. In this extended abstract, we propose a novel concept to protect chips along the supply chain and over their entire lifetime. The key to protection is a strain-based Physical Unclonable Function (PUF) and a cryptography-based authentication scheme. Both together protect the particularly critical chip transport. This work also discusses the security properties of the scheme.