Master's Thesis Engineering Technology

2024-2025

Side Channel Analysis on Complementary Flexible Thin-Film Transistor Technologies

Max-émile Meylaerts

Master of Electronics and ICT Engineering Technology

1. Introduction

Thin-film transistors (TFTs) represent a significant area of research in the development of new semiconductor technologies. They can be integrated onto flexible substrates, which allows for the creation of flexible circuits, as shown in Figure 1. The potential future adoption of this technology into security-sensitive applications, such as healthcare monitors, requires a thorough evaluation of their susceptibility to side channel attacks (SCAs). These attacks bypass the mathematical security of a cryptographic device by exploiting physical information leakage to extract sensitive data. This master's thesis examines the feasibility of power analysis attacks (PAAs) and their countermeasures on a circuit created with Low-Temperature Polycrystalline Oxide (LTPO). This technology combines the fast switching and low leakage power of the underlying technologies. Figure 2 shows an attacker measuring the power consumption of a device for use in a PAA.

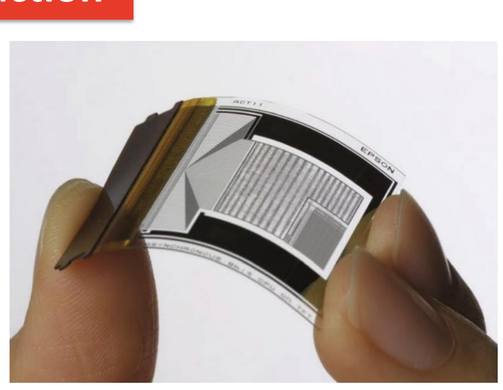

Figure 1: A flexible TFT-based microprocessor [1]

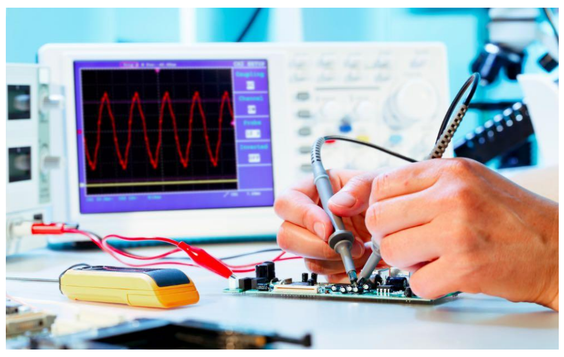

Figure 2: Example of a power analysis attack [2]

2. Side Channel Analysis

A test circuit was designed for the S-box of the Ascon algorithm. An S-box is a component of many cryptographic algorithms that obscures the relationship between the input and output data by performing substitutions. The circuit is composed of standard cells that were created using device models of LTPO transistors.
Subsequently, a PAA is performed on the circuit, which uses the variations in power consumed by the circuit to retrieve the secret key. Figure 3 displays ten power traces: each trace shows the power over time during a single clock pulse. This data is used by a Python script in a Correlation Power Analysis (CPA). The relative expected power consumption for each pulse is calculated by taking the Hamming weight of the expected output of the S-box, which is calculated using the known plaintext during that clock cycle and a key-guess. This is done for each possible key. Finally, the correlation coefficient is calculated between the expected power consumption and the actual power consumption over all traces for each key. The result is shown in Figure 4: the red bar indicates the actual secret key, which has the highest correlation coefficient.

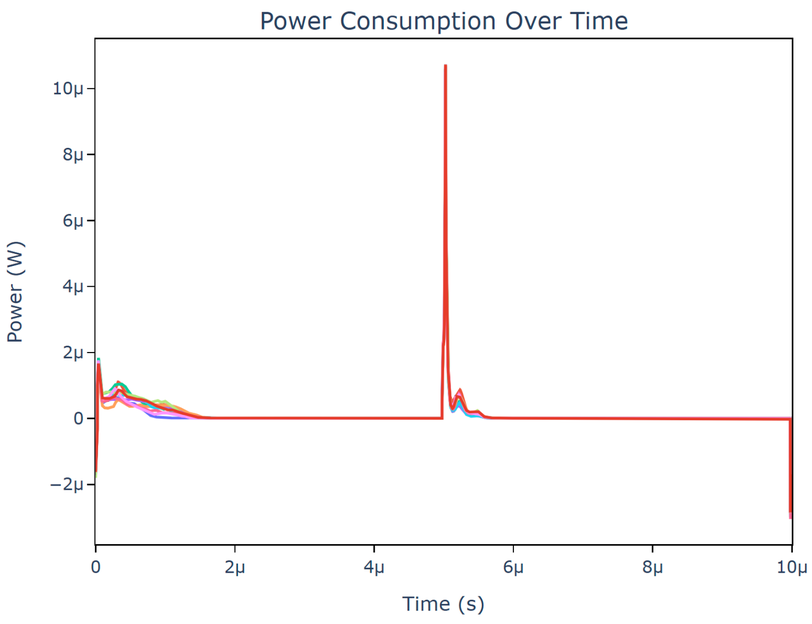

Figure 3: A sample of ten power traces from the test circuit

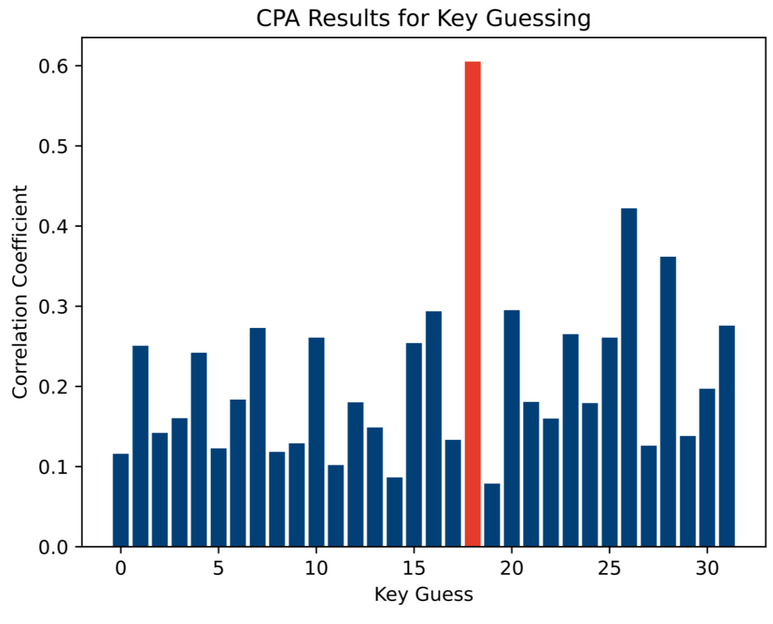

Figure 4: The correlation coefficient for each guess

3. Countermeasures

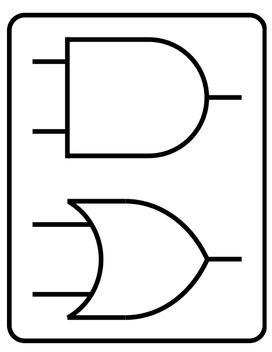

Figure 5: Symbol for a WDDL AND-cell

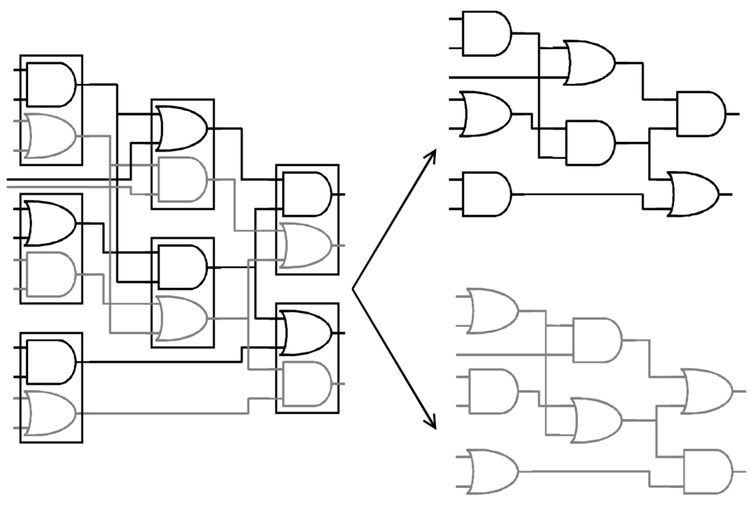

Figure 6: The WDDL circuit (left) and the derived subcircuits (right) [3]

In this master's thesis Wave Dynamic Differential Logic (WDDL) was used to protect against power analysis attacks. WDDL is a hiding technique: it attempts to reduce the information leakage by forcing the circuit to consume constant power, independent of the data being processed. It is a dual-rail logic style in which each bit of data is represented by two complementary wires. Each WDDL cell consists of two complementary gates, as shown in Figure 5. The required AND gate is combined with its complementary OR gate, which is given complementary inputs. The WDDL circuit can be divided into two subcircuits, as shown in Figure 6.
Before every clock cycle, a precharge signal is applied, which sets every input bit throughout the circuit to zero. This precharge propagates throughout the circuit in a wave. During the next clock cycle, exactly one gate will switch in every WDDL cell.

4. Conclusion and Future Work

WDDL was insufficient in preventing a CPA. This is due to the imbalance between the p-type low-temperature polycrystalline silicon TFTs and n-type indium–gallium–zinc-oxide TFTs that make up the LTPO. This complicates the balancing of the complementary gates that make up each WDDL cell, which results in a difference in input and output capacitances as well as pull-up and pull-down speeds between the gates. Eliminating all these differences poses a significant challenge. Future research should study other countermeasures that would not suffer from similar balancing difficulties, such as Sense Amplifier Based Logic or masking techniques. The effectiveness of these countermeasures, including WDDL, should also be evaluated for other TFT technologies.

Supervisors / Co-supervisors / Advisors: Prof. Dr. Ing. Kris Myny
Prof. Dr. Ir. Nele Mentens
Ing. Jelle Biesmans

[1] K. Myny, "The development of flexible integrated circuits based on thin-film transistors," *Nature Electronics*, vol. 1, no. 1, pp. 30–39, Jan. 2018.
[2] Rambus Press. (2018, May 24). *An Introduction to Side-Channel Attacks*. Rambus. [Online]. Available: https://www.rambus.com/blogs/an-introduction-to-side-channel-attacks/. (Accessed: Aug. 1, 2025).
[3] K. Tiri and I. Verbauwhede, "A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation," in *Proceedings of the 41st Annual Design Automation Conference*, 2004, pp. 246-251.