Research Statement

Karsten Nohl
nohl@virginia.edu
www.cs.virginia.edu/~kn5f

The need for trusted hardware grows as computer technology converges with every day life in form of payment, authentication, and communication devices. Basic security functions such as encryption need to be performed in highly distributed systems with limited power and computing resources. The set of tools available for security reviews grows constantly. Therefore, ad-hoc defenses are not effective against the increasingly sophisticated adversaries and systems must derive trust from valid security assumptions. Two aspects of trusted hardware have proven to be particularly challenging: key storage and the correct use of cryptography. Hence, my current and future research solves open questions in hardware security and focuses on microchip security and cryptanalysis.

Microchip Security

The challenge of storing cryptographic keys in microchips is typically addressed through complex networks of on-chip encryption and chip obfuscation. The techniques differ across chip vendors and have for the most part never been discussed in an academic context. My research analyzes the existing techniques, describes the underlying design trade-offs, and proposes improvements. This research stream involves reverse-engineering protection measures on state-of-the-art microchips.

I developed simple techniques to reverse-engineer algorithms from their silicon implementation [1]. My approach is to lay bare, open, and take pictures of microchips using only simple tools and an optical microscope. I then use a set of pattern recognition and logic checking scripts to automatically reconstruct an electrical circuit from the chip images such as the one shown in Figure 1. These circuits encode the algorithms implemented on a chip. As first results, some proprietary ciphers such as Mifare Classic's Crypto-1 stream cipher and the DECT standard cipher (DSC) were shown to be cryptographically weak. Furthermore, several research groups started applying and extending our techniques and the "common criteria" evaluation standard for smart cards is currently being updated to give a stronger weight to reverse-engineering attacks.

My future research will create a toolbox of techniques for securing microchips. First, I will reverse-engineer commonly used security measures including obfuscation, meshes, current scramblers and memory encryption. Then, I intend to make the techniques known and accessible in the academic domain by analyzing them in light of a realistic attacker model. Following the documentation of existing microchip security measures, I will investigate how the different measures can be combined to span a design space with trade-offs between higher security and lower cost, power consumption and design overhead. The design space will guide chip designers in

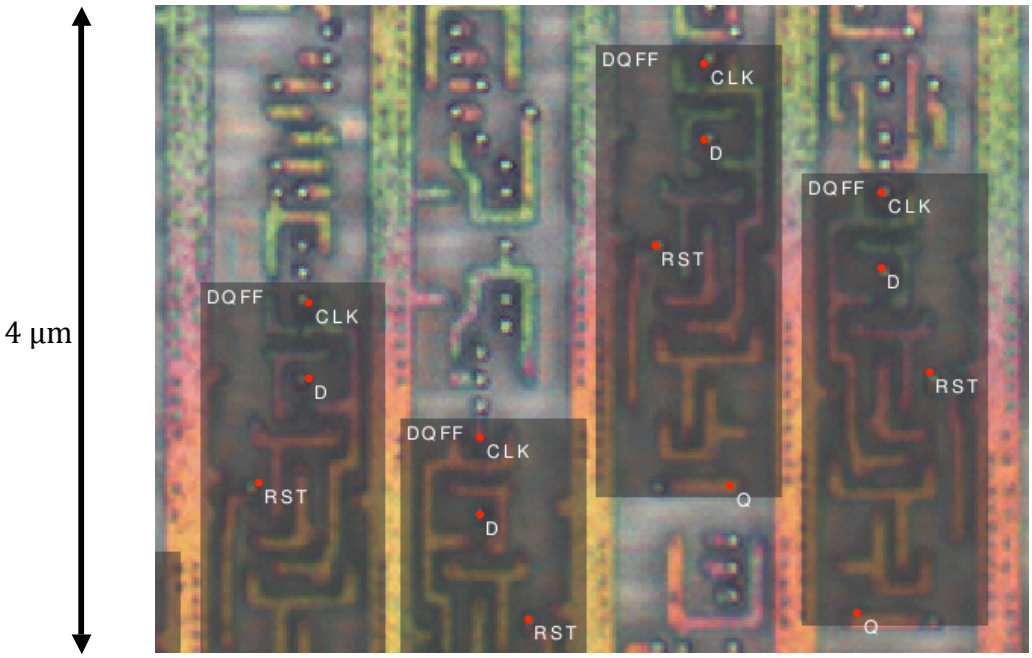

Figure 1. Transistor layer of a microchip with annotated logic gates.

choosing the right combination of measures for a given set of implementation constraints.

Security techniques that are currently a "dark art" with no open analysis will be categorized, analyzed and replaced with stronger designs where needed as happened when the field of cryptography was reclaimed for academia in the 70s and 80s. As the ultimate goal of this research, I want to bring back to the academic community discussion of how secret information can be securely stored in hardware.

Cryptanalysis

When secret keys can be securely stored, the cryptographic protocols become the next weakest link of embedded security systems. Some of the most widely used computing systems have been broken because of cryptographic flaws. The de-facto standards in cell phone encryption, GSM A5/1, cordless telephony, DECT, and RFID payment tickets, Mifare Classic, use proprietary ciphers that are weak. The most widely used access control system, HID, as well as toll collect system, FasTrak, do not implement any encryption. Besides the choice of encryption function, system security depends on the cryptographic protocol, the quality of random numbers, as well as the hardware's resistance to side-channel and fault attacks. Despite the existing insecurities in widely deployed systems on all of these layers, weaknesses are often only discovered when systems have grown too large to be upgraded. My reverse-engineering and cryptanalysis techniques will accelerate the public review of systems and contribute to the evolution of embedded security.

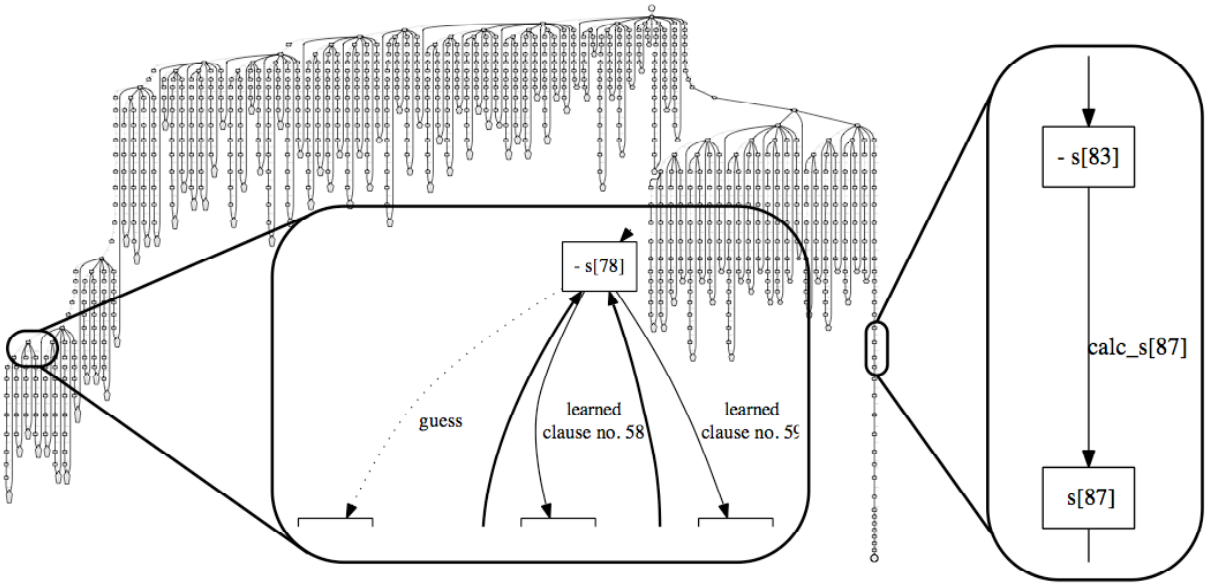

Figure 2. "Smart brute force" key search for finding a Crypto-1 key using SAT solvers. Each node represents one guessed key bit.

The functions disclosed through reverse-engineering undergo cryptanalysis to test their strength. In cryptanalysis, my current work challenges the limits of lightweight cryptography from two directions: breaking ciphers with insufficient complexity and developing design metrics for finding new candidate functions that are strong, yet lightweight.

In my current research in collaboration with INRIA Rhone-Alpes we repurposed satisfiability solvers—mathematical tools mostly used in hardware and software verification—to inverse cryptographic functions. These SAT solvers work on systems of equations, which describe a cryptographic function. The solvers execute a "smart brute force" search in which each wrong guess cuts the search tree until only the correct solution is left. In the example shown in Figure 2, only a tiny fraction of the 2^{48} possible keys are tried until enough information is accumulated inside the SAT solvers to smartly guess the right key. Our SAT solver optimized for cryptographic problems breaks weak stream ciphers trivially [2] and is able to solve the eStream-selected ciphers Trivium and Grain faster than other known attacks. The attack time is directly related to the complexity of a function's system of equations and, therefore, can be used as a design metric to find better functions.

A related metric developed in collaboration with Sean O'Neil is the randomness of a cipher's algebraic representation. We are using this metric in the design of cryptographic primitives by automatically testing the algebraic structure of all possible primitives in a large design space [3][4]. A design space could, for instance, consist of any combination of functions that can be implemented cheaply on a given microcontroller. The goal of this research is to develop and automate an approach for finding the best possible cryptographic function for a highly constrained platform,

thereby enabling security and privacy in applications such as long-range RFID tags where they are currently considered too expensive. Even when no perfect protection can be achieved, the level of protection can often be increased enough to discourage any reasonable attacker, which is one of the main results of my dissertation [4][5][6].

Outlook

My past research has encouraged discussion across the domains of academia, white-hat hackers and industry about the level of trust we should have in hardware devices. I want to continue bridging these three worlds with research that is both inspiring and relevant for real world applications. With the tools I have created, the security of microchips and cryptographic primitives can be evaluated more easily. My work will continue to make knowledge about chip security and cryptographic strength more accessible and easier to apply in the design of new security systems.

References

[1] Karsten Nohl, Starbug, Henryk Plötz, and David Evans. *Reverse-Engineering a Cryptographic RFID Tag*. USENIX Security, August 2008

[2] Mate Soos, Karsten Nohl, and Claude Castelluccia. *Extending SAT Solvers to Cryptographic Problems*. Theory and Applications of Satisfiability Testing (SAT), July 2009

[3] Sean O'Neil and Karsten Nohl. *EnRupt* – a submission to the NIST SHA-3 Hashing Competition, August 2008

[4] Karsten Nohl. *Implementable Privacy for RFID Systems*. PhD Dissertation. January 2009.

[5] Karsten Nohl and David Evans. *Hiding in Groups: On the Expressiveness of Privacy Distributions*. 23rd International Information Security Conference (SEC), Sep. 2008

[6] Karsten Nohl and David Evans. *Design Trade-Offs for Realistic Privacy* (Book Chapter). Paris Kitsos and Yan Zhang (Ed.): RFID Security: Techniques, Protocols and System-On-Chip Design.