Side Channel Attacks And Countermeasures For Embedded Systems

This book constitutes revised selected papers from the 11th International Workshop on Constructive Side-Channel Analysis and Secure Design, COSADE 2020, held in Lugano, Switzerland, in April 2020. Due to COVID-19, the workshop was held online. The 15 papers presented in this volume were carefully reviewed and selected from 36 submissions. The workshop covers subjects from wide ranges such as secure design, side channel attacks and countermeasures, and architectures and protocols.

This Special Issue provides an opportunity for researchers in the area of side-channel attacks (SCAs) to highlight the most recent exciting technologies. The research papers published in this Special Issue represent recent progress in the field, including research on power analysis attacks, cache-based timing attacks, system-level countermeasures, and so on.

This book constitutes the refereed proceedings of the Third International Workshop on Constructive Side-Channel Analysis and Secure Design, COSADE 2012, held in Darmstadt, Germany, May 2012. The 16 revised full papers presented together with two invited talks were carefully reviewed and selected from 49 submissions. The papers are organized in topical sections on practical side-channel analysis; secure design; side-channel attacks on RSA; fault attacks; side-channel attacks on ECC; different methods in side-channel analysis.

In the 1970s researchers noticed that radioactive particles produced by elements naturally present in packaging material could cause bits to flip in sensitive areas of electronic chips. Research into the effect of cosmic rays on semiconductors, an area of particular interest in the aerospace industry, led to methods of hardening electronic devices designed for harsh environments. Ultimately various mechanisms for fault creation and propagation were discovered, and in particular it was noted that many cryptographic algorithms succumb to so-called fault attacks. Preventing fault attacks without sacrificing performance is nontrivial and this is the subject of this book. Part I deals with side-channel analysis and its relevance to fault attacks. The chapters in Part II cover fault analysis in secret key cryptography, with chapters on block ciphers, fault analysis of DES and AES, countermeasures for symmetric-key ciphers, and countermeasures against attacks on AES. Part III deals with fault analysis in public key cryptography, with chapters dedicated to classical RSA and RSA-CRT implementations, elliptic curve cryptosystems and countermeasures using fault detection, devices resilient to fault injection attacks, lattice-based fault attacks on signatures, and fault attacks on pairing-based cryptography. Part IV examines fault attacks on stream ciphers and how faults interact with countermeasures used to prevent power analysis attacks. Finally, Part V contains chapters that explain how fault attacks are implemented, with chapters on fault injection technologies for microprocessors, and fault injection and key retrieval experiments on a widely used evaluation board. This is the first book on this topic and will be of interest to researchers and practitioners engaged with cryptographic engineering.

This book constitutes revised selected papers from the 8th International Workshop on Constructive Side-Channel Analysis and Secure Design, COSADE 2017, held in Paris, France, in April 2017. The 17 papers presented in this volume were carefully reviewed and selected from numerous submissions. They were organized in topical sections named: Side-Channel Attacks and Technological Effects; Side-Channel Countermeasures; Algorithmic Aspects in Side-Channel Attacks; Side-Channel Attacks; Fault Attacks; Embedded Security; and Side-Channel Tools.

The transfer of information has always been an integral part of military and civilian operations, and remains so today. Because not all information we share is public, it is important to secure our data from unwanted parties. Message encryption serves to prevent all but the sender and recipient from viewing any encrypted information as long as the key stays hidden. The Advanced Encryption Standard (AES) is the current industry and military standard for symmetric-key encryption. While AES remains computationally infeasible to break the encrypted message stream, it is susceptible to side-channel attacks if an adversary has access to the appropriate hardware. The most common and effective side-channel attack on AES is Differential Power Analysis (DPA). Thus, countermeasures to DPA are crucial to data security. This research attempts to evaluate and combine two hiding DPA countermeasures in an attempt to further hinder side-channel analysis of AES encryption. Analysis of DPA attack success before and after the countermeasures is used to determine effectiveness of the protection techniques. The results are measured by evaluating the number of traces required to attack the circuit and by measuring the signal-to-noise ratios. Annotation This book constitutes the refereed proceedings of the 12th International Workshop on Cryptographic Hardware and Embedded Systems, CHES 2010, held in Santa Barbara, USA during August 17-20, 2010. This year it was co-located with the 30th International Cryptology Conference (CRYPTO). The book contains 2 invited talks and 30 revised full papers which were carefully reviewed and selected from from 108 submissions. The papers are organized in topical sections on low cost cryptography, efficient implementation, side-channel attacks and countermeasures, tamper resistance, hardware trojans, PUFs and RNGs.

The 1st International Conference on “Applied Cryptography and Network Se- rity” (ACNS 2003) was sponsored and organized by ICISA (International C- munications and Information Security Association), in cooperation with MiAn Pte. Ltd. and the Kunming government. It was held in Kunming, China in - tober 2003. The conference proceedings was published as Volume 2846 of the Lecture Notes in Computer Science (LNCS) series of Springer-Verlag. The conference received 191 submissions, from 24 countries and regions; 32 of these papers were accepted, representing 15 countries and regions (acceptance rate of 16.75%). In this volume you will ?nd the revised versions of the - cepted papers that were presented at the conference. In addition to the main track of presentations of accepted papers, an additional track was held in the conference where presentations of an industrial and technical nature were given. These presentations were also carefully selected from a large set of presentation proposals. This new international conference series is the result of the vision of Dr. Yongfei Han. The conference concentrates on current developments that advance the - eas of applied cryptography and its application to systems and network security. The goal is to represent both academic research works and developments in - dustrial and technical frontiers. We thank Dr. Han for initiating this conference and for serving as its General Chair.

This book constitutes the thoroughly refereed post-conference proceedings of the 6th International Workshop, COSADE 2015, held in Berlin, Germany, in April 2015. The 17 revised full papers presented were carefully selected from 48 submissions. the focus of this workshop was on following topics: side-channel attacks, FPGA countermeasures, timing attacks and countermeasures, fault attacks, countermeasures, and Hands-on Side-channel analysis.

This thesis deals with side channel attacks against hardware implementations of cryptographic algorithms. Studies conducted in this document are therefore in place where an adversary has access to noisy observations of intermediate results of a cryptographic computation. In this context, many attacks are dedicated with their countermeasures, but their relevance and their implementation are still unclear. This thesis initially focuses on the relevance of existing attacks and potential links between them. A formal classification is proposed as well as selection criteria. Based on this study, a generic efficient attack is described and analyzed in depth. In a second step, the implementation of common countermeasures is studied, leading to the creation of an application scheme mixing them to achieve a better efficiency / security trade off.

Side-channel Attacks on FPGAs and Related Countermeasures

With wide adoption of embedded systems, the security aspect of embedded systems is becoming significantly important. Especially, power analysis side-channel attack, which is a type of attack on embedded hardware encryption/decryption systems, is a substantive security threat. Since power information has a correlation with the sensitive data that have to be protected from adversaries, the power consumption data become the ``side-channel'' of crypto-hardware. Power analysis side-channel attacks find such a correlation from collected many power consumption sample data. Countermeasures against the power analysis side-channel attacks are available; however, conventional countermeasures incur area, power, and performance overheads. Furthermore, hardware designers need to make trade-off decisions between the countermeasure resistivity and those overheads. This thesis proposes PARADE (Power Analysis Resistive Architecture DEsign) techniques to overcome such difficulties in designing secure embedded systems against power analysis side-channel attacks. In particular, the proposed method reduces the risk of power analysis side-channel attacks and the overhead of countermeasure by covering three key approaches of countermeasures: randomization, balancing, time-shifting. The first contribution in PARADE techniques is ExCCel (Exploration of Complementary Cells) that helps generating randomizing hardware countermeasure. ExCCel automates selective insertion of complementary cells that simultaneously improves attack resistivity while lowering the area and energy overheads in a simulated annealing manner. The second contribution, HDRL (Homogeneous Dual-Rail Logic), provides a power balancing technique. HDRL theoretically guarantees fully balanced power consumption using only standard cells and significantly improves power analysis side-channel attack resistivity. The third contribution, LRCG (Latch-based Random Clock-Gating), achieves realization of the time-shifting hardware in ASIC design. LRCG casts the problem of power analysis attacks as a retiming problem of circuits and automate latch-based circuit design process. Latch-based circuit, retiming, and clock-gating are traditionally used for performance and low power design, however LRCG randomly change the clock timing (time-shifting) using clock-gating techniques on latch-based circuit to obfuscate the power signature of crypto-hardware. Accordingly, the PARADE covers the three key directions of countermeasures. This thesis theoretically and experimentally demonstrates that the proposed PARADE techniques reduce the area, energy, performance overheads as well as enhancing the power analysis resistivity. The advantages of low overheads and better resistivity makes the proposed contributions promising approaches for designing smart cards and mobile devices.

Cryptography plays a vital role in digital communications, working to ensure the privacy and integrity of the users and their data. However, in the last decade, attacks have emerged that target physical implementations of cryptographic algorithms. In particular, side-channel attacks are of concern. It is the task of the hardware engineer to ensure that implementations of these algorithms do not introduce weaknesses in the form of side-channel information, that could compromise the integrity of the cryptosystem. This thesis investigates side-channel attacks on FPGA implementations of cryptographic algorithms. The vulnerability of cryptographic hash functions to side-channel attacks is not usually considered in the literature. However, in protocols such as HMAC, hash functions are used to process secret key information, which can be recovered via a side-channel attack. Here, using a commercial FPGA, the vulnerability of the SHA-2 and Whirlpool hash functions to Differential Power Analysis (DPA) is proven. In response to such vulnerability, masking is a common DPA countermeasure used in academia and industry. New masking schemes are presented for both hash functions, and a novel method of converting from Boolean to arithmetic masks is developed. Secure logic styles ensure that the cryptographic device consumes a constant amount of power in each clock cycle, and represent a general countermeasure to side-channel attacks. The Double Wave Dynamic Differential Logic (DWDDL) secure logic style for FPGAs is examined, and leveraged to develop an alternative logic style, Isolated WDDL (IWDDL). Using laboratory experiments, a flaw in the DWDDL design flow is highlighted, and rectified. Another general side-channel attack countermeasure is proposed in the form of All-or-Nothing Transforms (AONTs). In this thesis, it is shown that All-or-Nothing Encryption and Decryption are inherently resistant to DPA attacks. This resistance is then further increased using a novel extension to the AONE protocol. Various AONT constructions are considered, and the performance of these schemes is analysed. The thesis concludes with a comparison of general side-channel attack countermeasures, to determine the most effective method of protecting cryptosystems against side-channel at-tacks. It is shown that a ryptosystem using the All-or-Nothing countermeasure can match the performance of (and, in certain cases, outperform) an unprotected implementation.

Side-Channel Analysis plays an important role in cryptology, as it represents an important class of attacks against cryptographic implementations, especially in the context of embedded systems such as hand-held mobile devices, smart cards, RFID tags, etc. These types of attacks bypass any intrinsic mathematical security of the cryptographic algorithm or protocol by exploiting observable side-effects of the execution of the cryptographic operation that may exhibit some relationship with the internal (secret) parameters in the device. Two of the main types of side-channel attacks are timing attacks or timing analysis, where the relationship between the execution time and secret parameters is exploited; and power analysis, which exploits the relationship between power consumption and the operations being executed by a processor as well as the data that these operations work with. For power analysis, two main types have been proposed: simple power analysis (SPA) which relies on direct observation on a single measurement, and differential power analysis (DPA), which uses multiple measurements combined with statistical processing to extract information from the small variations in power consumption correlated to the data. In this thesis, we propose several countermeasures to these types of attacks, with the main themes being timing analysis and SPA. In addition to these themes, one of our contributions expands upon the ideas behind SPA to present a constructive use of these techniques in the context of embedded systems debugging. In our first contribution, we present a countermeasure against timing attacks where an optimized form of idle-wait is proposed with the goal of making the observable decryption time constant for most operations while maintaining the overhead to a minimum. We show that not only we reduce the overhead in terms of execution speed, but also the computational cost of the countermeasure, which represents a considerable advantage in the context of devices relying on battery power, where reduced computations translates into lower power consumption and thus increased battery life. This is indeed one of the important themes for all of the contributions related to countermeasures to side- channel attacks. Our second and third contributions focus on power analysis; specifically, SPA. We address the issue of straightforward implementations of binary exponentiation algorithms (or scalar multiplication, in the context of elliptic curve cryptography) making a cryptographic system vulnerable to SPA. Solutions previously proposed introduce a considerable performance penalty. We propose a new method, namely Square-and-Buffered- Multiplications (SABM), that implements an SPA-resistant binary exponentiation exhibiting optimal execution time at the cost of a small amount of storage -- O(\sqrt(\ell)), where \ell is the bit length of the exponent. The technique is optimal in the sense that it adds SPA-resistance to an underlying binary exponentiation algorithm while introducing zero computational overhead. We then present several new SPA-resistant algorithms that result from a novel way of combining the SABM method with an alternative binary exponentiation algorithm where the exponent is split in two halves for simultaneous processing, showing that by combining the two techniques, we can make use of signed-digit representations of the exponent to further improve performance while maintaining SPA-resistance. We also discuss the possibility of our method being implemented in a way that a certain level of resistance against DPA may be obtained. In a related contribution, we extend these ideas used in SPA and propose a technique to non-intrusively monitor a device and trace program execution, with the intended application of assisting in the difficult task of debugging embedded systems at deployment or production stage, when standard debugging tools or auxiliary components to facilitate debugging are no longer enabled in the device. One of the important highlights of this contribution is the fact that the system works on a standard PC, capturing the power traces through the recording input of the sound card.

This book constitutes the thoroughly refereed post-conference proceedings of the 12th International Conference on Smart Card Research and Advanced Applications, CARDIS 2013, held in Berlin, Germany, in November 2013. The 17 revised full papers presented in this book were carefully reviewed and selected from 47 submissions. The papers are organized in topical sections on security technologies; attacks on masking; side channel attacks; software and protocol

analysis; side channel countermeasures; and side channel and fault attacks.
This book constitutes the proceedings of the 14th International Workshop on Cryptographic Hardware and Embedded Systems, CHES 2012, held in Leuven, Belgium, in September 2012. The 32 papers presented together with 1 invited talk were carefully reviewed and selected from 120 submissions. The papers are organized in the following topical sections: intrusive attacks and countermeasures; masking; improved fault attacks and side channel analysis; leakage resiliency and security analysis; physically unclonable functions; efficient implementations; lightweight cryptography; we still love RSA; and hardware implementations.
This book constitutes the refereed proceedings of the 5th International Workshop on Cryptographic Hardware and Embedded Systems, CHES 2003, held in Cologne, Germany in September 2003. The 32 revised full papers presented were carefully reviewed and selected from 111 submissions. The papers are organized in topical sections on side channel attack methodology, hardware factorization, symmetric cypher attacks and countermeasures, secure hardware logic, random number generators, efficient multiplication, efficient arithmetics, attacks on asymmetric cryptosystems, implementation of symmetric cyphers, hyperelliptic curve cryptography, countermeasures to side channel leakage, and security of standards.

Hardware implementations of mathematically secure algorithms unintentionally leak side channel information, that can be used to attack the device. Such attacks, known as side channel attacks, are becoming an increasingly important aspect of designing security systems. In this thesis, power analysis attacks are discussed along with existing countermeasures. In the first part of the thesis, the theory and practice of side-channel attacks is introduced. In particular, it is shown that plain implementations of block ciphers are highly susceptible to power-analysis attacks. Dual rail precharge (DRP) circuits have already been proposed as an effective countermeasure against power analysis attacks. DRP circuits suffer from an implementation problem; balancing the routing capacitance of differential signals. In this thesis we propose a new countermeasure, path switching, to address the routing problem in DRP circuits which has very low overheads compared to existing methods. The proposed countermeasure is tested with simulations and experimentally on an FPGA board. Results from these tests show a minimum of 75 times increase in the power traces required for a first order DPA attack. Some of the existing countermeasures to address the routing problem in DRP circuits do not consider coupling capacitance between differential signals. In this thesis we propose a new method, divided backend duplication that effectively addresses balanced the routing problem of DRP circuits. The proposed countermeasure is tested with simulations and results show a minimum of 300 times increase in the power traces required for a first order DPA attack. Randomisation as a

DPA countermeasure is also explored. It is found that randomising the power consumption of the cryptographic device itself has little impact on DPA. Randomising the occurrence of intermediate results, on which DPA relies on, has better effect at mitigating DPA.

After two decades of research and development, elliptic curve cryptography now has widespread exposure and acceptance. Industry, banking, and government standards are in place to facilitate extensive deployment of this efficient public-key mechanism. Anchored by a comprehensive treatment of the practical aspects of elliptic curve cryptography (ECC), this guide explains the basic mathematics, describes state-of-the-art implementation methods, and presents standardized protocols for public-key encryption, digital signatures, and key establishment. In addition, the book addresses some issues that arise in software and hardware implementation, as well as side-channel attacks and countermeasures. Readers receive the theoretical fundamentals as an underpinning for a wealth of practical and accessible knowledge about efficient application. Features & Benefits: * Breadth of coverage and unified, integrated approach to elliptic curve cryptosystems * Describes important industry and government protocols, such as the FIPS 186-2 standard from the U.S. National Institute for Standards and Technology * Provides full exposition on techniques for efficiently implementing finite-field and elliptic curve arithmetic * Distills complex mathematics and algorithms for easy understanding * Includes useful literature references, a list of algorithms, and appendices on sample parameters, ECC standards, and software tools This comprehensive, highly focused reference is a useful and indispensable resource for practitioners, professionals, or researchers in computer science, computer engineering, network design, and network data security.

This book constitutes revised selected papers from the 10th International Workshop on Constructive Side-Channel Analysis and Secure Design, COSADE 2019, held in Darmstadt, Germany, in April 2019. The 14 papers presented together with one keynote and one invited talk in this volume were carefully reviewed and selected from 34 submissions. They were organized in topical sections named: Side-Channel Attacks; Fault-Injection Attacks; White-Box Attacks; Side-Channel Analysis Methodologies; Security Aspects of Post-Quantum Schemes; and Countermeasures Against Implementation Attacks.

Embedded Systems are ubiquitous, used in various applications, ranging from low-end electronic appliances to high-end rockets. Security on such systems is a major concern where any useful insight gained by the adversary is harmful. Side Channel Attacks (SCAs) are performed by observing properties such as power usage, processing time and electro magnetic(EM) emissions, to correlate these external manifestations with internal computations. These properties are used to obtain critical information, such as a secret key of a secure application. Power analysis has been the most effective technique to extract secret keys during the execution of cryptographic algorithms using

SCAs. This book elaborates on power analysis based side channel attacks detailing all the common attacks and the countermeasures proposed in the past. It also presents novel processor designs to combat against such attacks.

This book constitutes the proceedings of the 15th International Workshop on Cryptographic Hardware and Embedded Systems, CHES 2013, held in Santa Barbara, CA, USA, in August 2013. The 27 papers presented were carefully reviewed and selected from 132 submissions. The papers are organized in the following topical sections: side-channel attacks; physical unclonable function; lightweight cryptography; hardware implementations and fault attacks; efficient and secure implementations; elliptic curve cryptography; masking; side-channel attacks and countermeasures.

A lot of devices which are daily used (i.e., credit card, pay-tv card, e-passport) have to guarantee the retention of sensible data. Sensible data are ciphered by a secure key by which only the key holder can get the data. For this reason, to protect the cipher key against possible attacks becomes a main issue. Many research activities have been directed in developing countermeasures to enhance the device resistance against attacks and, on the other side, many contributions aimed to enhance the attack itself have been reported in the technical literature. This book is a collection of the main results of a PhD in hardware cryptography about side-channel attacks and countermeasures in the design of secure IC's devices. About hardware countermeasures against power analysis, three new logic families for cryptographic applications are designed. With respect to the contributions aimed to enhance the attack methodologies, an active circuit which promises to improve the power attacks is proposed. Besides, a new side channel and a novel methodology to attack cryptographic circuits is studied. Finally, two activities focused on Random Numbers Generators are briefly described.

This book constitutes the refereed proceedings of the 4th International Conference on Security, Privacy, and Applied Cryptography Engineering held in Pune, India, in October 2014. The 19 papers presented together with two invited papers were carefully reviewed and selected from 66 submissions. The papers are organized in topical sections on cryptographic building blocks; mini tutorial; attacks and countermeasures; tools and methods; and secure systems and applications.

This book provides the foundations for understanding hardware security and trust, which have become major concerns for national security over the past decade. Coverage includes security and trust issues in all types of electronic devices and systems such as ASICs, COTS, FPGAs, microprocessors/DSPs, and embedded systems. This serves as an invaluable reference to the state-of-the-art research that is of critical significance to the security of, and trust in, modern society’s microelectronic-supported infrastructures.

Our world is increasingly driven by sophisticated networks of advanced computing technology, and the basic operation of everyday society is becoming increasingly vulnerable to those networks’ shortcomings. The implementation and upkeep of a strong network defense is a substantial challenge, beset not only by economic disincentives, but also by an inherent logistical bias that grants advantage to attackers. Network Security Attacks and Countermeasures discusses the security and optimization of computer networks for use in a variety of disciplines and fields. Touching on such matters as mobile and VPN security, IP spoofing, and intrusion detection, this edited collection emboldens the efforts of researchers, academics, and network administrators working in both the public and private sectors. This edited compilation includes chapters covering topics such as attacks and countermeasures, mobile wireless networking, intrusion detection systems, next-generation firewalls, and more.

This book constitutes revised selected papers from the 9th International Workshop on Constructive Side-Channel Analysis and Secure Design, COSADE 2018, held in Singapore, in April 2018.The 14 papers presented in this volume were carefully reviewed and selected from 31 submissions. They were organized in topical sections named: countermeasures against side-channel attacks; tools for side-channel analysis; fault attacks and hardware trojans; and side-channel analysis attacks.

Cryptographic algorithms are being applied to various kinds of embedded devices such as credit card, smart phone, etc. Those cryptographic algorithms are designed to be resistant to mathematical analysis, however, passive Side Channel Attack (SCA) was demonstrated to be a serious security concern for embedded systems. These attacks analyzed the relationship between the side channel leakages (such as the execution time or power consumption) and the cryptographic operations in order to retrieve the secret information. Various countermeasures were proposed to thwart passive SCA by hiding this relationship. Another different type of SCA, known as the active SCA is Fault Injection Attack (FIA). FIA can be divided into two phases. The first one is the fault injection phase where the attacker aims at injecting a fault to a target circuit with a specific timing and spatial accuracy. The second phase is the fault exploitation phase where the attacker exploits the induced fault and forms an attack. The major targets for the fault exploitation phase are the cryptographic algorithms and the application-sensitive processes. Over the last one and a half decades, FIA has attracted expanding research attention. There are various techniques which could be used to conduct an FIA such as laser, Electromagnetic (EM) pulse, voltage/clock glitch, etc. EM FIA achieves a moderate spatial resolution and a high timing resolution. Moreover, since the EM pulse can pass through the package of the chip, the chip does not need to be fully decapsulated to run the attack. However, there remains a lack of understanding of the fault injected to the cryptographic devices and the countermeasures to protect them. Therefore, it is important to conduct in-depth research on EM FIA. This dissertation concentrates on the study of EM FIA by analyzing the experimental results on two different devices, PIC16F687 and LPC1114. The PIC16F687 applies a two-stage pipeline with a Harvard structure. Faults injected to the PIC16F687 resulted in instruction replacement faults. After analysis of detailed experiments, two new Advanced Encryption Standard (AES)-128 attacks were proposed and empirically verified using a two-step attack approach. These new AES attacks were proposed with lower computational complexity unlike previous Differential Fault Analysis (DFA) algorithms. Instruction specific countermeasures were designed and verified empirically for AES to prevent known attacks and provide fault tolerant protection. The second target chip was the LPC1114, which utilizes an ARM Cortex-M0 core with a three-stage pipeline and a Von Neumann structure. Fault injection on multiple LDR instructions were analyzed indicating both address faults and data faults were found. Moreover, the induced faults were investigated with detailed timing analysis taking the pipeline stall stage into consideration. Fault tolerant countermeasures were also proposed and verified empirically unlike previous fault tolerant countermeasures which were designed only for the instruction skip fault. Based on empirical results, the charge-based fault model was proposed as a new fault model. It utilizes the critical charge concept from single event upset and takes the supply voltage and the clock frequency of the target microcontroller into consideration. Unlike previous research where researchers suggested that the EM pulse induced delay or perturbation to the chip, the new fault model has been empirically verified on both PIC16F687 and LPC1114 over several frequencies and supply voltages. This research contributes to state of the art in EM FIA research field by providing further advances in how to inject the fault, how to analyze the fault, how to build an attack with the fault, and how to mitigate the fault. This research is important for improving resilience and countermeasures for fault injection attacks for secure embedded microcontrollers.

This book constitutes the refereed proceedings of the Third International Conference on Security, Privacy and Applied Cryptography Engineering held in Kharagpur, India, in October 2013. The 12 papers presented were carefully reviewed and selected from 39 submissions. The papers are organized in topical sections on implementations and protocols, side channel attacks and countermeasures, identity-based identification schemes, and signatures.

This thesis describes implementation of an Advanced Encryption Standard (AES) Smart Card, a highly tamper resistant to Side Channel Attacks. Smart Cards are gaining popularity in applications that require high security and store sensitive information. Modern smart Cards, highly capable of complicated cryptography, provide a high assurance of tamper resistance and thus commonly used in payment application. However, advanced Smart Cards can not protect attackers from being defrauded by different side channel attacks (DSCA). Small, embedded integrated circuits (ICs) such as smart cards are vulnerable to side channel Attacks (SCAs) The development of such attacks describes how to perform different kinds of side channel Attack on an AES implementation by using simulated power traces. Working in a simulated environment brings relevant advantages, e.g., eventual weakness to Differential power Attack(DPA) may be detected at device designing phase, so that satisfactory countermeasures can be adopted before the physical realization. The security prevention from such corresponding attacks is a randomized masking technique for implementing in software and hardware, which has been discussed here

Papers from a recent workshop cover all aspects of fault injection- based side channel attacks on cryptographic devices and the corresponding countermeasures for both secret and public key cryptosystems. Work is arranged in sections on side channel attacks and countermeasures, differential fault analysis, fault security of hardware and software, fault security of elliptic curve cryptography, and fault security of public key cryptography. Some specific areas examined include silicon-level solutions to counteract passive and active attacks, comparative analysis of robust fault attack resistant architectures for public and private cryptosystems, exploiting hardware performance, counters, and a generic fault countermeasure providing data and program flow integrity.

This book is for engineers and researchers working in the embedded hardware industry. This book addresses the design aspects of cryptographic hardware and embedded software. The authors provide tutorial-type material for professional engineers and computer information specialists.

This book constitutes the thoroughly refereed post-workshop proceedings of the 16th International Workshop on Information Security Applications, WISA 2015, held on Jeju Island, Korea, in August 2015. The 35 revised full papers presented in this volume were carefully reviewed and selected from 78 submissions. The papers are organized in topical sections such as hardware security; cryptography, side channel attacks and countermeasures; security and threat analysis; IoT security; network security; cryptography; application security.

This book presents two practical physical attacks. It shows how attackers can reveal the secret key of symmetric as well as asymmetric cryptographic algorithms based on these attacks, and presents countermeasures on the software and the hardware level that can help to prevent them in the future. Though their theory has been known for several years now, since neither attack has yet been successfully implemented in practice, they have generally not been considered a serious threat. In short, their physical attack complexity has been overestimated and the implied security threat has been underestimated. First, the book introduces the photonic side channel, which offers not only temporal resolution, but also the highest possible spatial resolution. Due to the high cost of its initial implementation, it has not been taken seriously. The work shows both simple and differential photonic side channel analyses. Then, it presents a fault attack against pairing-based cryptography. Due to the need for at least two independent precise faults in a single pairing computation, it has not been taken seriously either. Based on these two attacks, the book demonstrates that the assessment of physical attack complexity is error-prone, and as such cryptography should not rely on it. Cryptographic technologies have to be protected against all physical attacks, whether they have already been successfully implemented or not. The development of countermeasures does not require the successful execution of an attack but can already be carried out as soon as the principle of a side channel or a fault attack is sufficiently understood.

Power side-channel attacks are a very effective cryptanalysis technique that can infer secret keys of security ICs by monitoring a chip's power consumption. Since the emergence of practical attacks in the late 90s, they have been a major threat to many cryptographic-equipped devices including smart cards, encrypted FPGA designs, and mobile phones. Designers and manufacturers of cryptographic devices have in response developed various countermeasures for protection. Attacking methods have also evolved to counteract resistant implementations. This paper reviews foundational power analysis attack techniques and examines a variety of hardware design mitigations. The aim is to highlight exposed vulnerabilities in hardware-based countermeasures for future more secure implementations.

Intel Software Guard eXtensions (SGX) provides software applications shielded execution environments to run private code and operate sensitive data, where both the code and data are isolated from the rest of the software systems. Despite of its security promises, today’s SGX design has been demonstrated to be vulnerable to various side-channel attacks, and countermeasures have been proposed to mitigate these attacks. However, current understanding of the attack vectors and the corresponding countermeasures is insufficient. This dissertation explores new attacks when the adversary could exploit hardware features, such as Hyper-Threading and speculative execution, and aims to design comprehensive defense mechanisms that could address existing threats. Specifically, we first demonstrate how to abuse Hyper-Threading to launch attacks that could bypass existing AEX-based mitigations. Then, we introduce SgxPectre Attacks, the SGX-variants of the recently disclosed Spectre attacks, that exploit speculative execution vulnerabilities to subvert the confidentiality of SGX enclaves. On the defense side, we first design and implement HyperRace, an LLVM-based tool for instrumenting SGX enclave programs to eradicate all side-channel threats due to Hyper-Threading. Then, to address the limitations of existing mitigations, we extend the idea of HyperRace and propose the concept of verifiable execution contracts, which request the privileged software to provide a benign execution environment for enclave within which launching attacks becomes infeasible.