ISSN 2186-7437

NII Shonan Meeting Report

No. 2014-11

Design Methods for Secure Hardware

Kazuo Sakiyama
Patrick Schaumont
Ingrid Verbauwhede

September 15–19, 2014

National Institute of Informatics
2-1-2 Hitotsubashi, Chiyoda-Ku, Tokyo, Japan

Design Methods for Secure Hardware

Organizers:
Kazuo Sakiyama (The University of Electro-Communications, JP)
Patrick Schaumont (Virginia Tech, US)
Ingrid Verbauwhede (KU Leuven, BE)

September 15–19, 2014

The objective of the NII Shonan Workshop on Design Methods for Secure Hardware addressed the secure implementation of hardware cryptography in chips. The workshop assembled a group of researchers from industry and academia with a common interest in cryptographic engineering, but with a diverse background including chip design, cryptography, and implementation attacks. Over the course of the workshop, we tried to address challenges of common interest, such as how to identify the correct metrics in hardware security, and how to design hardware-friendly cryptographic algorithms.

The organizers prepared a general outline for the workshop, which is illustrated in the schedule below. The discussions and presentations were structured around three common activities in secure hardware design. The workshop devoted one day to each of these activities.

- Design of Secure Hardware, including chip designs for cryptography, key memories, chip identifiers and PUFs, random number generators, as well as the integration of cryptographic modules in larger designs. The typical conference venue associated with this activity can be the International Solid State Circuits Conference (ISSCC).
- Design of Cryptographic Algorithms, including the design of novel cryptographic primitives for public-key and symmetric-key cryptography, advanced primitives for privacy, hash-functions, and leakage-resilient or fault-tolerant designs. The typical conference venue associated with this activity can be CRYPTO or several other venues associated with the International Association for Cryptology Research (IACR).
- Design of Implementation Attacks, including side-channel analysis, fault-analysis and various forms of physical tampering with the implementation. The typical conference venue associated with this activity can be the Cryptographic Hardware and Embedded Systems (CHES) Workshop.

For each of these activities, the organizers identified three design concepts of interest. These three design concepts were used to structure the discussions and sessions of individual workshop days. The three design concepts are as follows, and each of them applies to the activities listed above (chips, algorithms, and attacks).

- Design Examples, which illustrate current state-of-the-art and common practice by means of actual examples.
- Design Methods, which collect the common wisdom of problem-solving within a particular area of interest.
- Design Metrics, which evaluate a design quality within a particular area of interest.

The following table shows, by means of examples, how design activities and design concepts are related. The workshop discussions were not restricted to these examples.

	Design of Secure Hardware	Design of Cryptographic Algorithms	Design of Implementation Attacks
Design Examples	Chip Designs, Smart Card Implementations, FPGA Prototypes, ...	Hash Algorithms, PRNG Designs, PKC Algorithms, ...	Side-channel Analysis of FPGA, ...
Design Methods	Pipelining, Design for low-leakage, design for low-power-variation, ...	S-BOX Optimization, Metrics for diffusion, ...	Alignment of side-channel traces, fault-injection methodology, ...
Design Metrics	Power estimation, EM leakage estimation, Timing analysis, ...,	Attack Complexity, Leakage resiliency, ...,	Fault sensitivity, Measurements-to-Disclosure, ...

The workshop also allowed time for participants to introduce themselves in a brief presentation. In addition, there was a common lunch-time and dinner-time for additional discussion, as well as an excursion.

The workshop did not create an official proceedings.

Participants

- Lejla Batina, Radboud University Nijmegen, NL
- Chen-Mou Cheng, Kyushu University, JP / National Taiwan University, TW
- Joan Daemen, STMicroelectronics, CH
- Jean-Luc Danger, Télécom ParisTech, FR
- Thomas Eisenbarth, Worcester Polytechnic Institute (WPI), US
- Benedikt Gierlichs, KU Leuven, BE
- Sylvain Guilley, Télécom ParisTech, FR
- Masanori Hashimoto, Osaka University, JP
- Yu-ichi Hayashi, Tohoku University, JP
- Naofumi Homma, Tohoku University, JP
- Shinichi Kawamura, Toshiba / AIST, JP
- Shugo Mikami Hitachi, Ltd., JP
- Noriyuki Miura, Kobe University, JP
- Shiho Moriai, NICT, JP
- Makoto Nagata, Kobe University, JP
- Kazuo Sakiyama, The University of Electro-Communications, JP
- Patrick Schaumont, Virginia Tech, US
- Takeshi Sugawara, Mitsubishi Electric Corp., JP
- Berk Sunar, Worcester Polytechnic Institute (WPI), US
- Ingrid Verbauwhede, KU Leuven, BE
- Dai Yamamoto, Fujitsu Laboratories Ltd., JP

Workshop Schedule

Sunday 14th September, 2014

- 15:00 Check-in
- 19:00 – 21:00 Welcome Reception

Monday 15th September, 2014: CHIP DESIGN DAY

- 7:30 – 8:30 Breakfast
- 8:30 – 9:00 Welcome
- 9:00 – 9:45 Introductions
- 9:45 – 10:15 Tea Break
- 10:15 – 11:00 Patrick Schaumont: Current State of Design and Design Methods for Secure Hardware
- 11:00 – 11:45 Masanori Hashimoto: Towards Robust Ultra-low Voltage Circuit Design
- 11:45 – 14:00 Lunch
- 14:00 – 14:45 Chen-Mou Cheng: Hydra, Programmable PKC Accelerator
- 14:45 – 15:30 Noriyuki Miura: Slightly Analog Integrated Circuit Countermeasures
- 15:30 – 16:15 Tea Break
- 16:15 – 17:00 Dai Yamamoto: Using PUFs to Protect Circuit Layout against Reverse Engineering
- 17:00 – 17:45 Jean-Luc Danger: Tree-based FPGA
- 18:00 – 19:30 Dinner

Tuesday 16th September, 2014: CRYPTOGRAPHY DAY

- 7:30 – 9:00 Breakfast
- 9:00 – 9:45 Introductions
- 9:45 – 10:15 Tea Break
- 10:15 – 11:00 Naofumi Homma: Formally-proofed Cryptographic Processor Design
- 11:00 – 11:45 Joan Daemen: Anti-DPA Threshold Implementations
- 11:45 – 13:30 Lunch
- 13:30 – 14:30 Shugo Mikami, Kazuo Sakiyama: Secure RFID Hardware

- 14:30 – 15:15 Thomas Eisenbarth: Quantifiable Side-channel Leakage
- 15:15 – 16:00 Tea Break
- 16:00 – 16:45 Shinichi Kawamura: Recent topics on secure implementation of cryptography
- 16:45 – 17:30 Nele Mentens: Lightweight Cryptography
- 18:00 – 19:30 Dinner

Wednesday 17th September, 2014: ADVERSARY DAY

- 7:30 – 9:00 Breakfast
- 9:00 – 9:45 Introductions
- 9:45 – 10:15 Tea Break
- 10:15 – 11:00 Takeshi Sugawara: What can we see in a chip
- 11:00 – 11:45 Lejla Batina: Threats and Countermeasures for Side Channel Analysis
- 11:45 – 13:30 Lunch
- 13:30 – 14:15 Makoto Nagata: On and Off Chip Diagnosis of Leakage with Examples
- 14:15 – 15:00 Benedikt Gierlichs: Implementing Threshold Implementations
- 15:00 – 15:45 Tea Break
- 15:45 – 16:30 Yuichi Hayashi: Information Leakage from Actual Commercial Products Caused by EM
- 16:30 – 17:15 Sylvain Guilley: Metrics to Assess the Protection provided by a Chip
- 18:00 – 19:30 Dinner

Thursday 18th September, 2014: FUTURE DAY

- 7:30 – 9:00 Breakfast
- 9:00 – 9:45 Introductions
- 9:45 – 10:15 Tea Break and Group Photo
- 10:15 – 11:00 Berk Sunar: Limits in Cryptographic Engineering
- 11:00 – 11:45 Shiho Moriai: Lightweight Cryptography for the Connected Car/ITS Security
- 11:45 – 13:30 Lunch
- 13:30 – 18:00 Excursion
- 19:00 – 21:30 Banquet

Friday 19th September: CONCLUSIONS

- 7:00 – 7:30 Check-out
- 7:30 – 9:00 Breakfast
- 9:00 – 9:45 Introductions
- 9:45 – 10:15 Tea Break
- 10:15 – 11:45 Ingrid Verbauwhede: Design Methods for Secure Hardware: Lessons Learned
- 11:45 – 13:30 Lunch
- 13:30 – 14:00 Good-Bye

Summary of Talks

Patrick Schaumont: Current State of Design and Design Methods for Secure Hardware

First of all, Patrick recalled some personal experience about the very early designs of Rijndael block cipher (before it was elected AES). At that time, the first chip was 173,000 gates equivalent in size and ran at 100 MHz. Since then, drastic improvements have been made. The reason for this progress is, according to Patrick, the existence of metrics. Second, Patrick analyses the nature of metrics. Hardware design consists in decomposing intelligently a design into elementary hardware primitives such as gates and flip-flops. However, what is"secure hardware design"? A first attempt of definition is given hereafter: achieve "hardware design" under a given set of threats (probing, faults, side-channel leakage, physical tampering, optical inspection, interfere with manufacturing). Clearly, as of today, metrics for secure hardware are not consensual. It is noted by the audience that such definition could also apply to embedded software. Similarly, "secure hardware design" could also consist in designing new threat-aware cryptographic primitives. However, the structure of abstraction layers is slightly different than in software design, since the weakest link can make the whole construction fail. Then Patrick investigates some insightful use cases. The computing landscape today concerns two opposite applications:

- The cloud with servers, backbone networking, bulk storage, and
- The swarm of devices in personal media, home environment, infrastructure.

Here, the threats are different. Protecting the swarm is more challenging, as it requires both more specialization and flexibility. Patrick notes that the design abstraction for security applications is domain specific. It typically looks like this (from top to bottom):

- Secure protocols,
- Crypto kernel,
- Architecture,
- Netlist.

Within this hierarchy, the designer can play with the design using three different techniques: Refinement (top-down), Integration (bottom-up), Transformation (horizontal optimization, within a given layer).

Besides, the designer must be aware of cross-layer threats (such as stealthy dopant hardware trojan horses, common (p,q) factors in RSA, etc.) Finally, Patrick makes a proposal about "capturing the possible trade-off in secure hardware design". Any secure hardware design aims at implementing an application (whose refinement can be represented on a Z axis), under three constraints (represented on the X,Y axes): Flexibility, Performance, and Risk.

The risk is the potential for loss, and can be expressed as the product of two factors: Risk = (probability of incident) x (cost of incident). For example,

in side-channel analysis, the risk is the product between the information contained per trace (It) and the number of traces (Nt) to break the key. Using an information hiding technique, such as WDDL, the "It" parameter is reduced. Using leakage resilient protection, the "Nt" parameter is reduced. Then, Patrick summarizes the metrics for design methods for secure hardware.

Things we understand well are:

- Classic hardware optimization paradigms
- Dealing with threats by integrating protected modules
- Transformation methods for single, selected threats

Things we do not understand:

- Generic risk assessment for a RANGE of threats
- Effects of composition and integration
- Cross-layer

As a conclusion, the Shonan group is solicited to continue thinking about the definition of "risk" and of "cost".

Masanori Hashimoto: Towards Robust Ultra-low Voltage Circuit Design

Sub-/near-threshold circuits operating at ultra-low VDD (¡ or Vth) are drawing attention due to the emerging applications driven by battery maintenance-free devices such as BAN and infrastructure monitoring. Sub-threshold circuits become slow (1/3k) yet ultra low power (1/100k) and can operate at some MHz in recent technologies. He introduce two types of perspectives towards robust ultra-low voltage circuit design (Variation perspective and Soft error perspective).

One major problem of sub-threshold circuits is that they are extremely sensitive to PVT variations. For example, it is 20x sensitive to manufacturing variability. Timing margin of a chip significantly varies chip by chip. This suggest that the conventional worst case design is inefficient and post???silicon speed control (e.g., body biasing and supply voltage scaling) is promising. As a result, run-time timing sensing techniques including Critical path replica and Razor are introduced in this research area. But critical path replica may has large delay mismatch between the replica and actual critical path due to within-die variation and aging.Razor can detect timing errors by FF inserted in actual paths, but the error recovery must be accompanied. To solve such issues, Run-Time Adaptation w/ TEP-FFs technique is presented. The major advantages are (1) simple structure, w/o error recovery, no test pattern preparation, (2) applicable to general sequential logics, and (3) detectability of process and environmental variations and aging.

His open question related to (Variation perspective is as follows: ???Error detection and correction??? or ???error prediction and avoidance??? might be introduced. What will happen when error injection attack via voltage scaling is given? On the other hand, his open question related to Soft error perspective is as follows: Will anything change in laser attack? Or nothing will change.

Chen-Mou Cheng: Hydra, Programmable PKC Accelerator

Chen-Mou Cheng introduced an energy-efficient programmable cryptographic coprocessor for ECC over GF(p) and post-quantum cryptography such as LWE-based key exchanges, NTRUEncrypt, multivariate signature schemes. The accelerator is called Hydra. The Hydra's programming code is one of the high-abstraction languages. The compilation process is as follows:

1. Algorithm programmed in Haskell
2. Algebraic Structure Expansion
3. Optimization
4. Code Generation A fixed architecture is assumed.

It is based on load-store machine with data cache, instruction cache, and arithmetic logic unit called Axpy engine. The compiler can optimize the code based on the configuration of the AXpy engine. It takes about 4 minutes to compile optimal ate paring over BN curves takes 4 minutes. 300 lines of code compiled to 2,000,000 instructions. For LWE-based key exchange, a few tens of the code generates a correct C++ code. For Energy-efficient implementation, the computation finishes quickly. The chip implementation was done with 90nm CMOS with the design methodology. One paring computation finishes in about 3ms (@200MHz, 14.2mW, 116Kgates), which is comparative to the previous hand-coded designs. Future work includes a way to observing and manipulating computation process. Side-channel attacks and verification of "correctness" and security also includes.

Noriyuki Miura: Slightly Analog Integrated Circuit Countermeasures

Noriyuki Miura presented some of his ongoing research work on building countermeasures at circuit level. The idea is to get 'almost analog' solutions that fit with a standard cell design flow. Countermeasures should resist EM attacks and even LEMA attacks (T. Sugawara, CHES 2013).

His target attack circuit is an 128 bit AES implementation. This implementation uses a Composite field representation of the Sbox.

In his presentation, he showed that it is possible to implement circuits that are only slightly analog and still have good resistance to attacks. He presented 3 types of countermeasures.

- Countermeasure 1: On-chip monitor for leakage path analysis
  An on-chip monitoring circuit is connected to the power supply of the cryptographic core. The experiment is to check if on-chip more information (at higher frequencies) for DPA is available.
- Countermeasure 2: Core supply isolator
  This idea has been published before (Adi Shamir Patent and PhD student at Michigan (Tokunaga ISSCC09). The idea is that a cryptographic circuit operates from a power supply that is isolated from the external power

supply. This is implemented by a capacitor which switches between 3 phases: charge - use as supply - discharge. There is about 30% overhead for the circuitry, mostly the capacitance compared to AES core 80% power increase because of high switching. 100mmx100mm is size of caps.

  - Discussion - Miura: to reduce the power consumption, this trick would only be applied to the first and the last round.

- Countermeasure 3. Reactive sensor approach against LEMA
  This countermeasure consists of one or multiple coils on chip. These coils will 'sense' if an EM probe comes close to the chip as the mutual inductance will change, which results in a frequency shift. Instead of one coil, a differential set-up with two coils is implemented. The coils are hidden in metal layers of device.

  - Q; calibration needs to know reference value Calibration is know at design time, thus freq. is know at design time and integrated into calibration So, attack with power-up with probe onto it, will not work. Diff frequency measurement circuit is turn-on and off, only operational in between AES operations
  - Q: don't lots of EM attacks, but most useful info is not necessary on top of the core Not sure why, but sometimes it is e.g. on narrow supply wire.

Dai Yamamoto: Using PUFs to Protect Circuit Layout against Reverse Engineering

First, Dr. Yamamoto explained this research background. Recently, semiconductor industry is specialized. Design have been done in fabless and manufacturing is in foundry. In this process, there are problem. For example, leakage of IP (Circuit structure, logic design, two leakage paths) might be caused. So, the Leakage is caused though foundry. Leakage is caused through IC chip itself: reverse engineering of IC chip, or attacker can reveal IP in IC chip.

In this presentation, he proposed the following method in order to prevent information leakage. The proposed mechanism combines split fabrication with PUFs.

- To prevent leakage, they employed split fabrication (separating IC design into two parts and each part are manufactured in different foundries).
- To prevent leakage, they also employed Physically Unclonable Function (PUF) (Proposing a new application of PUFs, Circuit structure is concealed by PUFs tolerant to reverse engineering).

Next, after he showed conventional split fabrication, he explained advantages of their proposal method. Finally, he summarized this presentation and showed the following open questions related to this proposal.

- Outputs of HCI-SA PUCs are really controllable?

- HCI-SA PUCs are really tolerant to reverse engineering? Advanced technique for reverse engineering, Secret information = Existence of hot carriers in HCI-SA cells, If an attacker can overwrite the HCI effect, she may obtain the information about responses of HCI-SA cells.

Q. How is different from FPGA designs?
A. Performance is different (Target is ASIC).
Q. How do we measure hot careers?
A. We might observe optical emission from back side depending on preparation.

Jean-Luc Danger: Tree-based FPGA

Danger-san presented a novel FPGA architecture that relies on a tree-based interconnect mechanism. In this architecture, the LUTs are at the leaves of a tree, and interconnect goes across branches of the tree. Depending on the logical distance between the leaves, the interconnect will travel several levels of the tree.

The advantages of the tree-based FPGA architecture include reduced routing complexity (log(N) switches need to be crossed to connect any among N cells); easier dynamic configuration; and the use of two independent routing networks (upward and downward) which reduces routing conflicts.

The Tree-based FPGA testchip uses 65nm ST technology, offers 2048 LUT4 cells on a tree with 4 hierarchical levels. The configuration is stored in latches and supports dynamic reconfiguration. The chip area is 4 square mm. The application of a tree-based FPGA is to implement symmetric, hiding based netlist for DPL. Besides the prototype chip, Danger-san presented measurement results for the DPL efficiency. He demonstrated how CAD tools can achieve placement symmetry. An open issue is that perfect symmetry still cannot be achieved using the tree-based FPGA. Therefore, a next-iteration of the tree-based FPGA prototype should apply systematic routing symmetry.

Naofumi Homma: Formally-proofed Cryptographic Processor Design

Homma-san presented a technique to verify the design of complex arithmetic circuit that use Galois Field Arithmetic. The verification is based on equivalence checking of a high level specification against a structural specification that includes additional modeling detail. The equivalence verification exploits the hierarchical nature of the design, and works by demonstrating equivalence in a bottom-up fashion. This is the key to make the overall solution scalable.

The technique uses a data structure called GF-ACF, a Galois Field Arithmetic Computation Flow Graph. It is a data flow graph that holds in sub-circuit inside of each node. The GC-ACF captures a Galois Field in terms of its basis, an irreducible polynomial and vector coefficient sets.

The technique works through a systematic decomposition of the high-level specification on lowe-level operations, and then comparing the resulting structure to the low-level design. The decomposition is done using a technique that guarantees a unique solution, namely by reducing the high-level polynomial using a Gröbner basis.

An application of the method is the verification of a 128-bit AES processor design: this design can be verified within 858 seconds. Open problems include: the application on other cryptographic algorithms such as ECC and CLEFIA, the verification of designs with built-in countermeasures fir side-channel leakage, and the verification of non-structured (non-hierarchical) circuits.

Joan Daemen: Anti-DPA Threshold Implementations

Keccak can be used in keyed modes in hostile environments and protection against side-channel (DPA, DEMA) is relevant. On the 1st order DPA countermeasure based on masking, linear functions are separately on shares, non-linear functions are scheduled carefully to avoid correlations, and scheduling is infeasible in hardware due to glitches.

Threshold scheme is a solution for hardware and the following conditions are required in the threshold scheme for Keccak: 3 shares, incompleteness that is each combinational block only takes 2 shares, uniformity that is if input is uniform output is uniform.

In the setting of a shared implementation of round function F, two problems occur. One is randomness evaporate until finally note is left in long term. The other is that input to next round is not uniform in short term. Two approaches to tackle these problems are tweaking architecture to restore uniformity and studying non-uniformity to see how bad it is. The focus of this presentation is studying how large is total imbalance.

For Keccak-f[b], imbalance ranges from 2^{11} to 2^{16} in case of b=100. When b=1600, the imbalance ranges from 2^{176} to 2^{256}. From the analysis of non-uniformity, threshold sharing of Keccak, the entropy loss is no problem.

In discussion, the following contents are discussed. If uniformity is not achieved, it cannot be proven that a Keccak threshold implementation offers immunity against first-order DPA. In the presentation, higher order is not considered. F is a round function. Mask is bit selected.

Shugo Mikami, Kazuo Sakiyama: Secure RFID Hardware

Summary: In this presentation, the motivation is to make clear the appropriate cryptographic algorithms/architecture for RFID systems. Also, it is important how performance of UHF RFID tag can achieve. Therefore, we implemented various hash function and performed fairly comparison of their performance. Further, we fabricated test chips for RFID tags including not only cryptographic functions but also various circuits such as interface circuit and antenna circuit, etc.
Discussion:

- Q. Is control part included? (Patrick)
  A. This is roughly sketch.
- Q. How many parallel implementations? (Ingrid)
  A. 8 parallels.
- Q. Evaluation results shown in table come from other papers? (Benedikt)
  A. YES

- C. Why don't you choose light-weight Keccak? (Joan)

- C. Is it possible to produce 800KHz from 920MHz?
  A. I suppose, maybe yes, but much power consumption is caused. Better option is to have another oscillator with smaller frequency. (Makoto)
- Q. Analog-clock generator is free-run?
  A. No.
- Q. 920MHz UHF is a standard in Japan? (Takeshi)
  A. Yes.
- Q. Is it possible to use lower frequency?
  A. Maybe, yes.
- Q. How many are power domains?
  A. Two.
- Q. CPU is included?
  A. No. This is complete hardware.
- Q. Why is the efficiency of RFID Tag worsen than expected?
  A. We suppose that this is because grand level of RFID Tag is not stable.
- Q. If we can supply stable voltage, tag and reader seem to communicate with each other stably. Is this understanding correct? (Prof. Hashimoto)
  A. Yes.
- Q. Actually, you supply voltage from reader to Tag? (Benedikt)
  A. Yes.
- Q. If we connect the ground level of tag with that of reader, what will happen?
  A. Not yet done. We will try.
- Q. How much is the power consumption of EEPROM? (Makoto)
  A. 600mW.
- Q. Random number generator is included in the test chip?
  A. Hash-based pseudo random number generator is implemented in the chip. Physical random number generator is not implemented.
- Q. Is it necessary to update ID and seed whenever authentication is done? (Benedikt)
  A. yes

Thomas Eisenbarth: Quantifiable Side-channel Leakage

This talk considered the issues of leakage resilience and quantification from the application perspective. Some relevant ideas were revisited such as: key update and stateless designs that also suffer from particular problems e.g. synchronization when key updates take place.

Leakage resilient signatures are one example where one-time signature keys are used to prevent exploitable leakages. In this case Merkle-Winternitz Hash

based Signatures can be used, but they also come at cost of large keys and signatures and in general efficiency is a problem. Hence, key storage and leakage quantification remain open problems.

As another example, leakage resilient PRG, as proposed by Dziembowski and Pietrzak, was discussed. The main point here was that, the design was broken by SCA, although provably secure.

Concrete examples with SCA on AVRXMEGA were discussed, where 2 independent experimental studies lead to different results.

The following research question was posed: How to quantify SC security when leakage is weak?

Methods proposed that could lead us to answer this question include: max-likelihood principle, sub-key/full key ranking and optimizing search algorithms. As a conclusion, there are many problems to solve.

Shinichi Kawamura: Recent topics on secure implementation of cryptography

Kawamura-san presented four different topics in the secure implementation of cryptography. One topic dicusses the Japanese cryptographic module certification program; a second topic describes the design of a standard evaluation platform; a third topic discusses an attack database; a final topic describes new attacks and countermeasures. He also presented several open questions for discussion.

- The ICSS-JC (IC System Security Japan Consortium) is the organization that works on certification according to the Common Criteria program. They coordinate the activities between certification body (IPA), vendors, and testing labs (ECSEC). The present effort is to define testing criteria for new attacks including physical attacks, laser/glitch, power/EM leakage and software analysis.

- The design of standard evaluation platform has a long history. Before SASEBO, there was the INSTAC-8 and INSTAC-32 testing boards, which were made for evaluation of side-channel leakage on microprocessor platforms.

- ICSS-JC maintains a database that lists attacks. Recently, four new attacks were added based on papers selected from the SCIS 2014 conference. The four new attacks were contributed by Mitsubishi, Ritsumeikan University and Tohoku University, and they exploit side-channel leakage.

- Finally, Kawamura-san discussed two open questions. First, what can be expected once there is dramatically faster cryptography available. Second, can we make a testing lab substantially unnecessary through a systematic approach to certify security of cryptographic LSI.

Takeshi Sugawara: What can we see in a chip

- Conclusion: Stealthy dopant-level circuits (c.f. Becker et al., CHES'13) are visible

- Using SEM (scanning electron microscopy) and FIB, measured a chip of various dopant levels by Shiozaki et al.
- Dual: Can embed secrets in ROM via DPD (dopant-programmable device), which can be used to control, e.g., FPGAs
- Hashimoto: Need to analyze costs of reverse engineering vs. DPD
- Ingrid: Can be more useful for camouflage than trojan if we have full-coverage tests
- DPD-LE: dopant-programmable device logic elements
- Nagata and Sugawara: It's possible (and even promising, Sugawara said) to attack using information from dynamic electrical characteristics, some of which can be linked to, e.g., amount of switching in a small area of the circuit
- Berk: It's very tricky to put a price on the cost of reverse engineering because there's a lot of business decisions involved
- Patrick: It's also different between the two applications, trojan detection vs. key hiding
- Kazuo: How to automate the design of DPD-LE and detection, e.g., using information from design compilers and such, as they always try to reduce redundancy?
- Berk: Is using DPD-LE to protect IP cost-effective, compared with, e.g., the state of the art in IP obfuscation?
- Sugawara: Can use triple well processes to give the hider an edge in hiding DPD-LE (!) at the cost of one or two extra masks (Hashitmoto)
- Sugawara: PVC (passive voltage contrast) + FIB can allow measuring surface voltage on metal; also can use AVC (active voltage contrast) to enhance resolution (?)

Lejla Batina: Threats and Countermeasures for Side Channel Analysis

Lejla presented a new 'online template attack' that can recover the ephemeral key of ECDSA in a single observation. The attack creates reference measurements, i.e. templates, adaptively after the single target trace has been observed. The attack is generic, as it applies to a wide range of ECDSA implementations, in particular also to implementations with some protection, e.g. Montgomery ladder implementations.

Attacks on ECDSA try to recover ephemeral key used in point multiplication, i.e. attack must succeed in a single shot. The presented Online Template Attack is a generic attack on the EC point multiplication that defeats countermeasures like Montgomery ladder. Templates are created after the attack and are adaptively created. Only one observation of target device suffices, e.g. for ECC on 8-bit processor.

The attack exploits a Key dependent assignment (e.g. in double and add always, or Montgomery ladder). In fact, the key dependency is detected in the subsequent step: i.e. one detects 2P vs. 3P by templating on 4P and 6P, because one of them will be computed. Detection is done by comparing the observed trace to a trace that computes on 2P and 3P. The method of comparison is correlation: the power trace is correlated to the template trace.

Attack also works for projective coordinates, but becomes more complex. In fact, fully randomizing projective coordinates is a working countermeasure, possibly also random isomorphisms. Future work: binary right-to-left add always Algorithm for Lucas Recurrences is key-independent double, but key-dependent add. How expensive is attacking this countermeasure?

Discussions:

- Naofumi: How about Windowing algorithm?
  A: might make attack more complex, but the attack also applies in that case.
- Patrick: why does the key-dependent assignment leak:
  A(Ingrid): it does not leak, the following operation on the result leaks
- Thomas: is it collision attack?
  A: detection method is similar, but the attack method is significantly different from a collision attack

Makoto Nagata: On and Off Chip Diagnosis of Leakage with Examples

- One of the goals is to realize ???analog techniques assisting trusted digital systems??? Note that the role of digital and analog is reverse compared to the case ???Digital assisted analog???— This is a standard way which is already wide spread.
- PSN = Power supply noise
  SN = Substrate noise
- LSI???s die is very small on board so if we can measure voltage deviation as close as possible to the die, we can monitor the deviation far more accurate than usual way.
- First Makoto showed a result of on-board PSN evaluation, captured by a usual measurement: EM probe captured EM field around a target chip. Upper part of die emits a lot of noise.
- Then, model of board is prepared to simulate how noise is added on board (namely, off chip).
- Since the noise added on board is so huge, on-chip PSN/SN measurements seem very important to see the original wave form on chip, which is the origin of leakage of secret information on chip.
- Expected merit of on-chip monitoring (OCM): It provides wave form very accurate. It must be less dependent to external environment.

- OCM system consist of
  - Analog frontend
  - Timing generator
  - Voltage generator
  - Data processing unit
  - Control registers.

- Analog frontend (AFE) : It captures the target voltage level as accurate as possible. Front end includes an amplifier with reference voltage supplied form voltage generator, which will be increased with small steps.

- On chip monitored signal is digitized and transferred to outside of chip via FPGA part.

- Need to isolate the monitor system from the die. Decoupling of GND is important for accurate measurement. Capacity decoupling is applied

- Experiment:
  1. Vdd, Vss, Vsub of AES module are monitored.
  2. Example: 32-bit uP core, monitored. (Embedding PSN/SN monitors to SoC) Probing points are shown as red dot.

- Vdd Noise graph, Vss Noise graph, Vsub Noise graph are shown. Those wave forms are very clear as expected.
  Positive drop of Vdd corresponds to negative drop of Vss
  Negative drop of Vss corresponds to negative drop of Vsub

- On the other hand, on board measured graphs have very high frequency noises (20 nSec frequency noise). Off chip monitor fluctuation of reflection or something is shown. Oscillation was observed. (Resonance caused by wave reflection.) OCM is without resonance.

- SN as leakage channel: In addition to Vss and Vdd, Vsub is a leakage source. SPACES Explorer, OCM is compared with off chip monitor at SASEBO-W. AES power trace is compared with on/off chip monitors

- Low-pass filtered off chip monitored wave gives similar result to OCM w.r.t. DPA.
  Q: Why FPGA do not have huge memory?
  A: Because measurement is executed in iterative manner and the data is read out immediately after it is captured.

- Q: It seems difference between on/off chip monitorings is small.
  A: Off chip monitoring needs amplifier. OCM doesn't. That is the difference.

- Countermeasure:
  From on-chip monitoring, to suppress leakage from AES module, isolator (equalizer) should be placed between AES module power supply.

- Measured SN waveform: (Results are shown)
  CPA on SN leakage: (Results are shown)

- IC chip should be in Assembly.
  Flip chip assembly = Face of chip faced to board, namely, back side is faced to outside.
  SN leak is easy to use from back side of chip by attaching probing needle.
- Q: What happen when SOI technology employed?
  A: It could be a countermeasure but it is expensive.
- Q: Did you find some relationship between EM measurement and OCM.
  A: Since origin is the same, so they have strong relationship.
- C: Fault injection from the back side, such as laser attack, is popular. Countermeasure against Flip chip could be applied to such attacks, too.
- Q: 3D implementation could be a solution.
- Q: What do you suggest backside attack?
  A: Sensor is a candidate.
- Q: How about utilizing sense amplifier of SRAM?

Benedikt Gierlichs: Implementing Threshold Implementations

Masking is an effective countermeasure against DPA. Two-share Boolean masking, if well implemented, can offer resistance against first-order DPA. In hardware, the combinatorial logic poses a problem due to the presence of glitches and the inevitable nonlinear functions that require performing computations on both shares.

An effective technique to build hardware implementations that offer resistance against first-order DPA are so-called threshold implementations. They have as distinguishing property of incompleteness: each share at the output of the non-linear (round, or sub-round) function is independent of at least one share. The number of shares depends on the non-linear function at hand and is at least 3. With a simple information-theoretic argument one can prove that if the input to a combinatorial circuit for computing a share is uniformly shared, its computation is independent of the native value. This gives provable security against first-order DPA. Most ciphers are iterated and for the information-theoretical security of a corresponding TI scheme there is the additional requirement of uniformity. For TI implementations of invertible functions this simply corresponds with invertibility of the mapping of the shares.

A TI scheme was employed in a very compact implementation of AES by Moradi et al. This implementation has 3 shares and uses a pipelined implementation of the SubBytes S-box based on tower fields down to $GF(2^2)$ to reduce the degree of the functions to be shared. The loss of uniformity is compensated by the injection of 48 random bits per S-box evaluation. An effort was undertaken to make a lighter (smaller area and fewer random bits) implementation by taking other choices for the sharing. A circuit with considerable smaller size and slightly less random bits per S-box evaluation ("only" 44) was obtained by making the number of shares variable (2 in the linear part and up to 5 in the S-box) and going only down to $GF(2^4)$ in the S-box representation. The solution was implemented on FPGA and tests using a Sasebo board showed no

first-order leakage up to 10 million traces. Considerable second-order leakage was detected, but here we must take into account that the circumstance s are very advantageous for the attacker: no additional noise or jitter. Finally, a comparison was given of current work, including two variants of the proposed architecture: one even more compact and one that is expected to offer better resistance against 2nd order attacks.

Yu-ichi Hayashi: Information Leakage from Actual Commercial Products Caused by EM

Background

Possibility of information leakage via EM emission, and possibility of meaningful fault injection caused by EMI are discussed in his presentation with approximately 50 slides. Coupling between simple micro strip lines are demonstrated with full-wave simulation. A signal driving one of the lines is coupled to another one in parallel, and then emitted from parasitic antenna such as a cable connecting to this line. This can happen on any lines on a PCB. Modeled by Source - Path - Antenna.

- The 1st part – Information leakage threat via EM emanation for tablet PCs (AMS CCS 2014)

  Software keyboards on a display can be viewed by another people when typing secret keys. While polarization filter protects this type of attack, display is still stolen by measuring unintentional EM fields. A portable setup for EM display stealing is introduced, and targeting tablet PCs. Skew correction and keystroke detection by investigating reconstructed images from EM leakage. Horizontal and vertical scanning frequency, leakage frequency are captured in data profiling step. Leakage EM waves are received, amplified, and analog-to-digital converted for the post processing. Keystrokes on a software keyboard are detected in a demo. Yagi-antenna in a suitcase is to be directed to the tablet PC to capture. The dominant source of leakage was found on the cable connecting to LCD panel, which were emitted from wires surrounding the panel. The level of EM emission is sufficiently within the CISPR regulation. This can be protected by the shielding with a transparent conductive film. The leakage frequency may be defined as the frequency of resonance determined by the size of antenna.

- The 2nd part – Fault injection method based on IEMI

  Incident of faults with 170 MHz sinusoid waves, larger faults with higher injection voltage and larger errors as well. The secret key was completely revealed from 13,497 faulty outputs among 340,000 different plaintexts. Incident of faults with 200 MHz sinusoid waves, not effectively caused faults. Countermeasure: enhancing EM immunity of cryptographic module.

Sylvain Guilley: Metrics to Assess the Protection provided by a Chip

Sylvain began by explaining that applying state-of-the-art attacks to test a chip's security is laborious and time consuming. His talk was about attempts to find alternative methods.

Sylvain recalled that one can compute the signal to noise ratio (SNR) of side channel measurements and use it to quantify the information leakage. One can further use it to estimate the success rate of first-order attacks, under some conditions. In particular, if the leakage behavior of the chip is known, the success rate depends only on the SNR and the number of measurements.

Sylvain then introduced a normalized notion of SNR (NICV) and argued that it is advantageous because it is bounded in [0, 1]. Just like the SNR, the NICV can be used to estimate the success rate of first-order attacks. Looking at side channel analysis as a communication problem, Sylvain explained how SNR metrics can be used to derive optimal attacks (distinguishers) for a given situation. This of course requires to know the situation in advance, and is therefore mainly useful for evaluation purposes.

Next, Sylvain explained four successive notions of statistical dependence, from correlated to independent. He used these notions to discuss the relationship between SNR/NICV and the success rate of higher-order attacks.

Berk Sunar: Limits in Cryptographic Engineering

- Intro: Distributed Computing (Cloud, Storage-Centric). Massive data growth (Cloud data is getting increasing very rapidly more than 60Data center data means privately managed but cloud is not (no one knows where the data is processed).
- Problems: Generating data is too huge so has to be moved to remote huge storage (you can not have it locally) We have to download it fast, leakage is still a problem.
- Dream: We want to perform operation deirectly on encrypted data on the cloud server.
- Wish list:
  Medical records, financial database → Encrypted database
  Media server → File system functions (search replacement)
  Media processing → Blinded computations
  Financial transactions → Blinded negotiations
- What is Homomorphic Encryption:
  You can do some computations on ciphertext (equivalent to perform the computations on plain text)
  Don't need to trust cloud server anymore.
  There is somewhat homomorphic encryption (not perfect).
  e.g. addition unlimited but multiplication only a few.
  All the existing schemes are noisy.

- Q. How attack-resilient?
  A. Long-time computations may be cost increase for the side-channel attack. Trafic analysis may be a problem.

- Recent study in 5 years:
  Improved very rapidly (2 orders of magnitude improvement per year).
  2008 Gentry bootstrapping idea to reduce noise for increasing the number of computations possible.
  2010 Gentry-Halevi first FHE implementation → 30 seconds for 1-bit multiplication.
  Lots of other techniques → LWE, Batching, Module switching/reduction for improving performance.
  2013 Gentry-Halevi-Smart first HE AES evaluation → 10 minutes per AES block computation
  2014 Doroz-Hu-Sunar NTRU-based FHE GPU (reduced public kay 20GB, polynomial computation 5MB) → 7 seconds per AES block

- 2012 Alt-Lopez
  Based on NTRU variant by Stehle/Steinfeld
  Addition increases noise slowly no problem in addition
  Multiplication increases noise rapidly
  So after each multiplication do Re-linearization for noise removal.

- Batching (Encode message vector first then encrypt message polynomial)

- Fully Homomorphic Encryption:
  2 NSF CISE grants Sunar, Martin to solve efficiency bottleneck
  Implementations in 2011 (Re-encryption)
  CPU 17.8sec GPU 0.93sec (per bit operation)

- Closing the efficiency gap:
  AES → 10^8x RSA, Paillier NTRU (public key) → 10^7x MG, BGN, → 10 FHE (original)
  FHE-LWE 10^2, FHE-NTRU 10^4 custom hardware would increase 10^6-10^7

- Circuit is leaked during HE.
  If/loops need to be unrolled.

- How to handle
  Encrypt the circuit description itself
  Addition and multiplication do same time parallel and then MUX (select result)
  Full tree redundancy too much (still the circuit depth is leaked)

- Do some HE operation several times and then decrypt and refresh noise and return.

- Actual implementation (module board co-operate with blade server) connected with PCI express.

Shiho Moriai: Lightweight Cryptography for the Connected Car/ITS Security

Dr. Shiho Moriai introduced the recent trend of lightweight cryptography for constrained devices. Projects of ECRYPT-I and -II in Europe and a project of CRYPTREC in Japan were and are working toward standardization and promotion. An example of output of CRYPTREC was a list on e-Government recommended ciphers list.

Dr. Moriai told that lightweight cryptography is on the next step; that is the step of deployment for new emerging applications. One representative application is connected car. Car has more attack surfaces and much data to be protected. On the other hand, CAN bus is just a 32-bit conventional bus. To make it secure, we need to develop a secure higher layer, such as protocols. Some companies are interested in the secure CAN bus, but the others are not. Our community needs to tell the automotive community how secure CAN is important and provide a solution.

Ingrid Verbauwhede: Design Methods for Secure Hardware: Roadmap

- Central Question: What is a Design Method for Secure Hardware? as opposed to: What is a Design Method for Throughput/Speed ? (We understand Q2 very well, but Q1 not at all)
- Different Types of Drivers: Business, Individual, Society, Civic, Public. Business Drivers: DRM, Cars, Counterfeit, Medical, Bank Card, Gaming. Individual Drivers: Storage, Subscriptions, Tracking, Access, Credentials. Public Drives: Passport, Travel Docs, Money, Voting, Government, Health.
- versus Different Types of Technologies
- Given:
  fancy cryptographic algorithm (results in computational security)
  performance: lightweight, high throughput (metric for light weight)
  secure: resistant to physical attacks (metric for resistance)
- What is design?

  Link between system specs and implementation:
  Specifications,
  Refine,
  Translate to SoC,
  Memory Optimizations,
  Algorithm Transformations,
  Arithmetic Optimizations,
  Partitioning,
  Architecture Selection
- Design abstraction levels:
  Protocol,

Algorithm,
Architecture,
Netlist

- Design method:
  Refinement,
  Transformation,
  Integration/Verification
- Example: works very well RTL to tape-out for ASIC design because they had metrics at every abstraction level:
  operations w partial ordering;
  operations w clock tick;
  operations w clock tick and logical depth;
  operations w clock frequency.
- Metrics work because
  - we have them at each abstraction layer
  - ignore details of the lower levels
  - metrics give worst case
  - works well for area, time, less accurate for power, energy
- Metrics for security?
  Eg metrics for side channel resistance
  metrics for HW security?
  pyramid for SCA, pyramud for fault resistance, pyramid for countermeasures
- Nagata: can we have one pyramid or multiple pyramid
- Berk: this is a long term issue
  Ingrid: yes, first DES chip was custom design
- Sylvain: we have many pyramids
  Ingrid; they integrate to one
- Sylvain: depending on the property we need, we want high speed
  properties go top-down or bottom up
  Ingrid time is measured bottom up, best opportunities at the top
- Assignment: what is metric at your design level? what would be metric at one layer up or down?

Conclusions

All attendees considered this a very fruitful and interesting seminar. Each participant made contributions from their own background. At the end, we concluded that this seminar is a first step towards a roadmap to design secure electronic circuits. Only when we have clear metrics at each level of abstraction, will we be able to develop design methods and tools.

As a follow-up, we plan to submit a proposal for a special session at the DAC (Design Automation conference). We also plan a follow-up seminar maybe in one year time in Dagstuhl and in two years time again at Shonan.

The organizers thank the participants for their very positive and open attitude during this seminar. The organizers also thank the National Institute of Informatics to set-up Shonan meetings and supporting us in our research.