23rd Crypto-Day

ESCRYPT GmbH

December 10 and 11, 2015

Berlin, Germany

Agenda Crypto Day 23

Thursday, December 10th			Room
13:00	14:00	Registration	Lobby
14:00	14:10	Welcome	107
14:10	14:35	A. Krestiachine (ESCRYPT) *Automotive Security Crash Course*	107
14:35	15:00	S. Tajik (TU Berlin): *Laser Fault Attack on Physically Unclonable Functions*	107
15:00	15:25	C. Reuter (Uni Mannheim): *SMAUG – Secure Mobile Authentication Using Gestures*	107
15:25	15:55	**Coffee Break & ESCRYPT Demos**	Lobby
15:55	16:20	Z. Dyka (IHP): *Successful simple power analysis of GALS ECC design*	107
16:20	16:45	M. Krause (Uni Mannheim): *Analyzing stream ciphers security against time-memory -data tradeoff attacks*	107
16:45	17:10	J. Malchow (FU Berlin): *Why SSL/TLS still fails*	107
17:10	17:40	**Coffee Break & ESCRYPT Demos**	Lobby
17:40	18:05	C. Wittke (IHP): *Probe comparison for EM-measurement in terms of side channel analysis*	107
18:05	18:30	K. ievgen (IHP): *Secure homomorphic data aggregation for smart energy consumption infrastructure*	107
18:30	18:55	C. Müller (Uni Mannheim): *Privacy In Smart Buildings – The Dark Side Of The Sensor*	107
20:00		**Christmas Market** (meet outside Bosch building)	

Friday, December 11th			
		Coffe & Croissants	107
8:30	8:55	G. Faterneh (TU Berlin): *Dispelling the myth: cloning the Physically Unclonable Functions (PUFs)*	107
8:55	9:20	M Strand (NTNU Norway): *Fully homomorphic encryption must be fat or ugly*	107
9:20	9:45	F. De Santis (TU München): *High-Speed Curve25519 Scalar Multiplication on ARM Cortex-M4 Microcontrollers*	107
9:45	10:10	**Coffee Break**	107
10:10	10:35	J. Vetter (TU Berlin): *Fault-Attacks on RSA*	107
10:35	11:00	D. Kreiser (IHP): *Bitwise key agreement using wireless channel parameters (work in progress)*	107
11:00	11:25	J. Krämer (TU Darmstadt): *The LWE Challenge*	107
11:25	11:50	**Coffee Break**	107
11:50	12:15	A. Bock (IHP): *Efficient and Power Analysis Resistant Implementation of the Montgomery kP-Algorithm*	107
12:15	12:35	S. Schmidt (ESCRYPT) *Work & Life at Escrypt*	107
12:35		**Lunch & Mingling**	217

Laser Fault Attack on Physically Unclonable Functions

Shahin Tajik[1], Heiko Lohrke[2], Fatemeh Ganji[1], Jean-Pierre Seifert[1], Christian Boit[2]

[1] Security in Telecommunications
Technische Universitt Berlin
Germany

[2] Semiconductor Devices
Technische Universitt Berlin
Germany

Physically Unclonable Functions (PUFs) [1] are introduced to remedy the shortcomings of traditional methods of secure key storage and random key generation on Integrated Circuits (ICs). Due to their effective and low-cost implementations, intrinsic PUFs are popular PUF instances employed to improve the security of different applications on reconfigurable hardware. In this work we introduce a novel laser fault injection attack on intrinsic PUFs by manipulating the configuration of logic cells in a programable logic device. We present two fault attack scenarios, where not only the effectiveness of modeling attacks can be dramatically increased, but also the entropy of the targeted PUF responses are drastically decreased. In both cases, we conduct detailed theoretical analyses by considering XOR arbiter PUFs and RO PUFs as the examples of PUF-based authenticators and PUF-based random key generators, respectively. Finally we present our experimental results based on conducting laser fault injection on real PUFs, implemented on a common complex programmable logic device manufactured in 180 nm technology.

References

[1] Gassend, Blaise and Clarke, Dwaine and Van Dijk, Marten and Devadas, Srinivas Silicon Physical Random Functions. Proceedings of the 9th ACM conference on Computer and communications security, 2002.

SMAUG – Secure Mobile Authentication Using Gestures

Frederik Armknecht, Christian A. Reuter

University of Mannheim, Germany

Mobile devices such as mobile phones or tablets companion our everyday living and often store valuable personal data. Consequently, there is a strong need for secure and usable authentication schemes. The most popular approach is based on proving certain knowledge (“What I know”), i.e., the user has to insert a PIN or a pattern to gain access to the device. However, there is the usual problem that the user often cannot choose and/or memorize strong passwords. A further problem is that using strong passwords strongly reduces usability.

Looking at the authentication methods used today, mostly PINs (Apple iOS), pattern (Google Android), and maybe graphical passwords (Microsoft Windows 8) ar being used. Each variant has been attacked successfully using procedures like brute force. Furthermore, they are all subject to shoulder-surfing or smudge-attacks. While this is true for any type of devices, these attacks are particularly dangerous for mobile devices where users have to frequently log-in while being outside of any secure environments like home or offices. An alternative approach may be to use additional devices like smart-cards (“What I possess”). If one of the devices gets stolen, no authentication is possible. Also, it gets cumbersome to use everyday and also comes with relatively high costs. An interesting alternative is to base authentication on biometric properties (“What I am”). These can be physiological attributes like fingerprints, iris recognition, and face recognition. Apart of the fact that these methods often have their own security problems, a further drawback is that this requires additional hardware.

Therefore we researched how to authenticate using biometric data without requiring new hardware. Nearly every smartphone has a gyrosensor and an accelerometer, and also a touch screen. We developed a new secure mobile authentication scheme using only these three sensors and overcome all earlier mentioned problems. A user authenticates by re-drawing a gesture that he registered during the enrollment phase. During the registration a number of sensor data are collected. Our algorithm combines these information to enable multi-factor authentication: a user needs to know what gesture has to be made but also how the gesture is being done. Our scheme exhibits a number of remarkable features as follows: no dedicated hardware required, fully flexible input, efficient feature extraction and detection, high security and usability. Compared to existing work, our scheme provides the richest set of capabilities: It allows an arbitrary amount of freely drawn gestures (multi-gesture, free-form-gesture), multi-touch (arbitrary amount of fingers used at the same time), multi-stroke (each finger can draw an arbitrary amount independent of other fingers), multi-factor (combining biometric data with knowledge), multi-sensor (touch sensor, gyroscope, accelerometer), sensor-fusion (combining gyroscope and accelerometer data), and graphical password support (background images for gestures) at the same time. Moreover, our scheme provides security with respect to the strongest attacker model considered so far, i.e., an attacker who has full knowledge on how the gesture looks like and how it has been drawn. It works without any operating system constraints and without continuous authentication.

In this talk, we will present the SMAUG algorithm in detail. We will explain which features are extracted and how the recognition-algorithm decides between the legitimate user and an impostor. Finally, we will show experimental results (98% user identification, 100% impostor detection) and give the possibility to test SMAUG on a device.

Successful simple power analysis of GALS ECC design

Zoya Dyka, Frank Vater, Dan Kreiser und Peter Langendoerfer

System dept. IHP
Frankfurt (Oder), Germany

Side channel analysis attacks are significant threat for implementing cryptographic algorithms. A lot of countermeasures based on the randomization of the secret (private) key [1], inputs [1], steps of algorithms [2] or influence of the circuit [3] are published. In [4] the implementation of ECC (Elliptic Curve Cryptography) design as a GALS (Global Asynchronous Locally Synchronous) design was introduced as a possible countermeasure against side channel analysis (SCA) attacks.

We performed a simple power analysis (SPA) attack against the original synchronous IHP ECC design and against its GALS-ified version. In this work we analysed simulated power traces of both ECC designs. To ensure a fair comparison exactly the same manufacturer library of elements, the same inputs, private key and simulation tools were used for obtaining the power traces of both hardware implementations. The private key can be extracted successfully for both designs. This shows clearly that a straight forward GALS-ification of a synchronous ECC design that is vulnerable to SPA is also vulnerable to SPA. Also we explain here why the GALS design is even more vulnerable to other SCA attacks for example to differential power analysis than a synchronous ECC design.

Acknowledgement

The authors would like to thank the Dr. Milos Krstic from System department of IHP for providing the GALS-ified version of IHP ECC design.

References

[1] J. Coron: Resistance against Differential Power Analysis for Elliptic Curve Cryptosystems. Proceedings of the First International Workshop CHES 1999, August 12-13, 1999, Worcester, MA, USA, LNCS Vol. 1717, pp. 292-302, Springer Berlin Heidelberg, 1999

[2] E. Oswald, M. Aigner: Randomized Addition-Subtraction Chains as a Countermeasure against Power Attacks. Proceedings of the Third International Workshop - CHES 2001, May 14-16, 2001, Paris, France, LNCS Vol. 2162, pp. 39-50, Springer Berlin Heidelberg, 2001

[3] Z. Dyka, Ch. Wittke and P. Langendoerfer: Clockwise Randomization of the Observable Behaviour of Crypto ASICs to Counter Side Channel Attacks. Proceedings of Euromicro Conference on Digital System Design (DSD), 26-28 Aug. 2015, pp. 551-554, IEEE,

[4] Xin Fan, S. Peter and M. Krstic: GALS design of ECC against side-channel attacks A comparative study. Proceedings of 24th International Workshop on Power and Timing Modeling, Optimization and Simulation (PATMOS), Sept. 29-Oct. 1 2014, pp. 1-6, IEEE,

Analyzing Stream Cipher Security against Time-Memory-Data Attacks

Matthias Krause

Universitt Mannheim

Due to the close relation to modern block cipher designs, in the last years, much research work has been invested into the security analysis of iterated Even-Mansour ciphers. These are pseudorandom permutations (PRPs) defined by alternatingly adding n-bit sub-keys k_i and calling public n-bit permutations P_i.

With this paper, we suggest to study similar constructions for pseudorandom functions (PRFs), where, additionally, access to a public preimage resistant n-bit function F is allowed. Our practical motivation is that the security of certain stream ciphers w.r.t. to generic time-memory-data (TMD) tradeoff attacks can be modeled in a natural way by analyzing the security of such PRF-constructions in an extended random oracle model.

Our main technical result is a sharp $\frac{2}{3}n$-security bound for the $FP(1)$-construction $F(P(x \oplus k) \oplus k)$, which contrasts with a sharp bound of the same order for the Even-Mansour PRP $P(P(x \oplus k) \oplus \pi(k)) \oplus k$, recently proved by Chen, Lampe, Lee, Seurin, Steinberger (Crypto 2014).

We obtain a method for designing stream ciphers which generate the keystream packet-wise (like the E_0-cipher of the Bluetooth system) in such a way that a beyond-the-birthday-bound security w.r.t. generic time-memory-data tradeoff attacks can be proved. This allows for designing new stream ciphers with smaller inner state lengths. Moreover, we demonstrate that a slight hardware-friendly change in the state initialization algorithm used by the E_0-cipher raises the security from $\frac{1}{2}n$ to $\frac{2}{3}n$, where n denotes the inner state length of the underlying keystream generator.

References

[1] Gassend, Blaise and Clarke, Dwaine and Van Dijk, Marten and Devadas, Srinivas Silicon Physical Random Functions. Proceedings of the 9th ACM conference on Computer and communications security, 2002.

Why CAs Must Fail - A Change of Perspective

Jan-Ole Malchow and Volker Roth

Freie Universität Berlin
Secure Identity Research Group
Berlin, Germany

The general problem addressed in the CA model is the placement of trust in remote entities. Even if a connection is encrypted it is not clear that the remote host belongs to the desired entity. An additional authentication has to be performed. It is generally assumed that users cannot carry out an identity verification for each entity. As a solution a third party is introduced to perform the validations. Therefore users have to trust a single third party only. In the classic trust model (including extended validation) CAs are the trusted third party. Fig. 1 compares the flow of money to trust and selection of trust anchors. It is especially worrisome that flows of money and trust do not correspond. As a result CAs have an incentive to behave honest regarding their customers only. This problem is intensified by the fact that large CAs are seen as “too big to fail” [1]. Combining public data and results from Durumeric et al. [2] we found that seven organizations control 99.9% of browser trusted certificates. This means removing one large CA from the truststore renders a browser practically useless. Therefore browser vendors should not be trusted by users. Fig. 1 shows that the user trusts both CAs and browser vendors where we just argued that he should not.

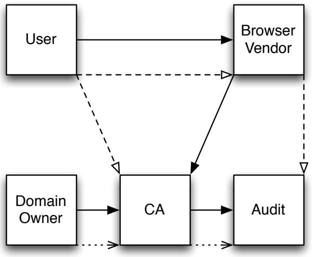

Figure 1: Selection (solid), flow of money (dotted) and trust (dashed).

Existing security extensions (Key pinning, TACK, DANE, Perspectives, Sovereign Keys, Certificate Transparency and Accountable Key Infrastructure) address the relation between CA and domain owner. We believe the reason they do not fully solve the problem is that they ignore the existing risk/reward balance. In our talk, we will discuss the trust problem and proposed slutions in greater detail. In our talk, we will discuss the trust problem and proposed solutions in greater detail and we will motivate an approach of our own to address the problem.

References

[1] A. Arnbak, H. Asghari, M. Van Eeten, and N. Van Eijk, “Security collapse in the https market,” *Queue*, vol. 12, no. 8, pp. 30:30–30:43, Aug. 2014. [Online]. Available: `http://doi.acm.org/10.1145/2668152.2673311`

[2] Z. Durumeric, J. Kasten, M. Bailey, and J. A. Halderman, “Analysis of the https certificate ecosystem,” in *Proceedings of the 2013 conference on Internet measurement conference*. ACM, 2013, pp. 291–304.

Probe comparison for EM-measurement in terms of side channel analysis

Christian Wittke, Zoya Dyka and Peter Langendoerfer

System dept.,
IHP
Frankfurt(Oder), Germany

Side channel analysis is an effective method for attacking cryptographic implementations. The most attacks are based on (statistical) analysis of the power or electromagnetic (EM) traces. These traces are measured while the device is executing cryptographic operations using its private (secret) key. The benefit of electromagnetic analysis attacks (EMA) is the feasibility to do local measurements, i.e. the activity of some blocks of a cryptographic design can be analysed separately. Different EM probes, for example commercial manufactured as well as self-made probes, can be used for measurements. Their size, form, position and orientation influence the shape and the quality of the measured traces significantly. But the focus in scientific publications is usually set on the statistical analysis of already measured traces.

In this work we explain how and why the size, position and orientation of EM probe influence the measurement results. Therefore we compare 7 different EM field probes from Langer [1], Riscure [2] and a self-made probe.

We analysed a hardware accelerator for elliptic curve point multiplication kP for elliptic curve *B-233* [3] over the extended binary Galois field $GF(2^{233})$. The kP operation was implemented using the Montgomery algorithm in projective Lopez-Dahab coordinates as described in [4]. This version of kP design is vulnerable against simple power and electromagnetic analysis attacks [5]. We selected this version since its vulnerabilities can easily be seen, i.e. it is a very helpful example to illustrate the influence of different EM probes on the measured traces. The device under attack, the analysed cryptographic operations and processed inputs are always the same in our experiments. These measurement conditions allow a fair comparison of the probes and show the influence of the probes on the shape of the measured traces.

We performed the measurements of the EM field at two positions on our FPGA Board. First we measured the EM field on the die and second at an interconnect on the PCB. In particular the EM traces measured on the die differ substantially. But also the EM traces measured at the PCB interconnect are different. The measurement results are showing a large difference between the traces of each probe. The impact is much higher for horizontal EM probes than for vertical EM probes. The presented results can be helpful in preparation of electromagnetic analysis attacks, i.e. for choosing the most appropriate EM probe and its orientation at measurement points.

References

[1] LANGER EMV-Technik GmbH, http://www.langer-emv.de/

[2] Riscure Security Lab, https://www.riscure.com/

[3] NIST, “Digital Signature Standard (DSS),” FIPS PUB 186-4, Tech. Rep., July 2013.

[4] S. Peter, “Evaluation of Design Alternatives for Flexible Elliptic Curve Hardware Accelerators,” Master’s thesis, Brandenburg University of Technology Cottbus, 2006.

[5] IHP Project TAMPRES, from http://www.ihp-microelectronics.com/de/forschung/drahtlose-systeme-und-anwendungen/abgeschlossene-projekte/tampres.html

Secure homomorphic data aggregation for smart energy consumption infrastructure

Ievgen Kabin, Krzysztof Piotrowski and Peter Langendoerfer

System dept.
IHP
Frankfurt (Oder), Germany

This work is a part of the EU E-balance project [1], which aims at integration of energy customers into the future smart-grid. The goal of the system is to adapt the time at which energy is caused to the time when it is produced in order to reduce number and level of energy peaks in the energy grid. The main entities in the system are customer management units (CMU) (representing end users), top level management units and intermediate management units at different levels the smart grid. Intermediate management units collect data about energy consumption from CMUs, calculate the sum, i.e. aggregate the data, and send the result to the next higher level in the hierarchy in order to allow energy balancing. Most customers are concerned about their privacy i.e. they dont want that anybody has access to their personal data about consumed energy. But to participate in the system they need to provide data about their energy consumption. In order to provide a certain level of privacy the data needs to be encrypted. This requires that the intermediate nodes decrypt data from clients before any aggregation and then re-encrypt the result before sending it. These multiple decryptions and encryptions reduce lifetime of sensor nodes due to high energy consumption of the cryptographic operations. In addition the data of the end users is available in plain in the intermediate units which to a certain extend violates the users privacy. If the intermediate units are empowered to aggregate encrypted data from all customers the energy consumption of wireless sensor networks would decrease significantly and maybe even more important the privacy of the end users would be by far better protected.

Homomorphic encryption is an approach that allows different types of operations to be carried out on encrypted data for example addition multiplication or both.

We implemented additively homomorphic data encryption according to [2] for our own sensor nodes based on the MSP430 microcontroller. Aggregators are able to process encrypted data. Nevertheless some information about customers can be retrieved even from encrypted data. If energy consumption of some customer is known its possible to make conclusions about his private life. This is also possible even if the energy consumption averaged over time is known. For example if nobody is at home (vacation or trip) the energy consumption is reduced significantly. For this reason options to make aggregation more secure were examined, such as averaging by the set of customers or by the time and to make personal data of each customer even more blurred for third parties. The aggregation result is the sum of the data from different customers. As additional feature this sum can be averaged over time. It will be hard to obtain information about each person separately. We measured the time for encryption, aggregation and decryption processes with different key sizes and compared the results.

References

[1] The e-balance Project, http://www.e-balance-project.eu/

[2] C. Castelluccia, E. Mykletun and G. Tsudik: *"Efficient Aggregation of Encrypted Data in Wireless Sensor Networks"*, in Proceedings of ACM/IEEE Mobiquitous: pp. 109-117, San Diego, 2005.

Privacy In Smart Buildings – The Dark Side Of The Sensor

Frederik Armknecht and Christian Müller

Theoretical Computer Science & IT-Security,
University of Mannheim,
Germany

With the Internet of Things on the rise, an increasing number of lightweight devices are fitted with wireless communication equipment and may even have access to the internet. This enables the development of new business models and applications, *e.g.*, in the field of building automation, also referred to as Smart Buildings.

In Smart Buildings, the control of utilities and facilities, *e.g.*, Heating, Ventilation, and Air Conditioning (HVAC) or lighting, is based on decentralized sensing and performed in an automatic fashion. Effectively, this control is dedicated to improve occupant comfort and convenience, while also increasing energy efficiency. To realize such a building automation system, all involved devices need to have access to a shared communication channel. Often, a wireless solution is preferred since a different form of installation would incur massive modifications to an existing building due to required wiring. The deployed devices usually form a wireless sensor network with constraints in terms of computing power, power supply, cost, and (physical) size per device. Therefore, instead of utilizing WLAN, ZigBee or similar protocols are used which target low-energy and low-range use cases.

Nowadays, different service providers offer cloud-enhanced solutions for building management, *i.e.*, a provider may have access to reported measurements of detailed room climate data. Generally, and considering the source of origin of such values, it could be tempting to state that room climate data is sensitive personal data and falls under the data protection law. However, it is questionable whether there is a need to enforce strong cryptographic protection of sensor data at all.

In this work, we investigate whether indoor temperature and relative humidity data divulge information about the presence of people in a room. We conducted an agile experiment in our workgroup's offices which revealed that visual inspection of the temperature and relative humidity graphs already provides a rough indication of presence patterns. As a matter of fact, we can clearly determine the timeframe in which our offices are tended to by the cleaning personnel, thus supporting the hypothesis that even sensor measurements require protection from unauthorized access.

Dispelling the myth: cloning the Physically Unclonable Functions (PUFs)

Fatemeh Ganji, Shahin Tajik, Jean-Pierre Seifert

Security in Telecommunications
Technische Universität Berlin / Telekom Innovation Laboratories

Nowadays, commercial piracy (i.e., counterfeiting of designs and infringements of patents) as well as industrial espionage have become rife. To combat these issues, the concept of hardware fingerprints has emerged, which stems from the human fingerprints. One of the most promising candidates for representing a hardware fingerprint is the Physically Unclonable Functions (PUFs) family [1, 2].

From a general perspective, PUFs are mappings, which generate a response for a given, arbitrarily chosen challenge. This mapping can be realised by implementing concrete circuits in the hardware (i.e., an integrated circuit, IC). When feeding such a circuit with an enable signal and the challenge, the circuit generates a response depending on the physical characteristics of the IC. Several different PUF realisations have been proposed, for instance, arbiter PUFs [3], XOR arbiter PUFs [4], and ring-oscillator PUFs [4]. While the IC manufacturers have been investing in these families, adversaries have proposed successful attacks ranging from invasive to non-invasive attacks [5, 6, 7]. Although the former attacks can successfully characterise a PUF [5, 6], non-invasive attacks are widely accepted and launched due to their cost-effectiveness [7].

In order to develop a mathematical framework for the assessment of the effectiveness of non-invasive attacks, the following steps are necessary: (a) Establishing fit-for-purpose mathematical representations of different physically unclonable functions as hardware security primitives. (b) Developing approaches to assess the security of physically unclonable functions under the proposed representation.

First, we have considered the family of arbiter PUFs that is widely accepted and studied in the security community. The principle behind the design of these PUFs is that the delay differences between symmetrically designed electrical paths on an IC can be utilised to generate a random response, when the IC is fed by a challenge. We have demonstrated that under a well-established deterministic finite automaton (DFA) representation these PUFs can be learned for given levels of accuracy and confidence [8]. Secondly, we have studied XOR arbiter PUFs as a modified structure of arbiter PUFs, in which non-linear effects are added to the PUF in order to impair the effectiveness of machine learning attacks. At the beginning of the XOR arbiter PUFs era it was assumed that xoring a large number of arbiter chains to generate the response of the PUF, the PUF would be more robust against machine learning attacks. In [9] we have established a theoretical upper bound on the number of arbiter chains of an XOR arbiter PUF, beyond which the PUF cannot be characterised by applying pure machine learning methods.

Although we have explained why the number of arbiter chains cannot be unlimitedly increased, for the sake of completeness, we have taken into account a scenario, where the number of arbiter chains can be arbitrarily large [10]. Furthermore, in our attack scenario we have considered the case that the attacker cannot have access to the challenges (so called controlled PUFs). This means that neither the attacker can apply the challenges selectively nor the challenges can be eavesdropped. This notion has been introduced by the manufacturer to prevent the non-invasive attacks. Nevertheless, we have proved that none of these countermeasures can be helpful to protect the PUF from hybrid attacks. As the name implies, these attacks are a combination of semi-invasive and non-invasive attacks. Our proposed attack leverages the strength of an attack proposed in [6].

Moreover, by extending the lattice basis reduction attack discussed in [11] and combining it with the results of [6] we have successfully launched our attack against a controlled XOR arbiter PUF with a large number of arbiter chains.

Finally, we conclude that PUF families studied by us cannot be an ultimate solution for the problems concerning the IC fingerprinting. Last but not least, we would like to stress that our study can provide an insight not only into the academic research but also the design and manufacturing of PUFs.

References

[1] Gassend, Blaise and Clarke, Dwaine and Van Dijk, Marten and Devadas, Srinivas Silicon Physical Random Functions. Proceedings of the 9th ACM conference on Computer and communications security, 2002.

[2] Pappu, Ravikanth and Recht, Ben and Taylor, Jason and Gershenfeld, Neil Physical One-way Functions. Science, Vol.297, No. 5589, 2002.

[3] Lee, Jae W and Lim, Daihyun and Gassend, Blaise and Suh, G Edward and Van Dijk, Marten and Devadas, Srini A Technique to Build a Secret Key in Integrated Circuits for Identification and Authentication Applications. Proceedings of Digest of Technical Papers. Symp. on VLSI Circuits, 2004.

[4] Suh, G Edward and Devadas, Srinivas Physical Unclonable Functions for Device Authentication and Secret Key Generation. Proceedings of the 44th annual Design Automation Conf., 2007.

[5] Helfmeier, Clemens and Boit, Christian and Nedospasov, Dmitry and Seifert, Jean-Pierre Cloning Physically Unclonable Functions. Proceedings of IEEE Intl. Symp. on Hardware-Oriented Security and Trust (HOST), 2013.

[6] Tajik, Shahin and Dietz, Enrico and Frohmann, Sven and Seifert, Jean-Pierre and Nedospasov, Dmitry and Helfmeier, Clemens and Boit, Christian and Dittrich, Helmar Physical Characterization of Arbiter PUFs. Proceedings of Cryptographic Hardware and Embedded Systems CHES 2014, 2014.

[7] Rührmair, Ulrich and Sehnke, Frank and Sölter, Jan and Dror, Gideon and Devadas, Srinivas and Schmidhuber, Jürgen Modeling Attacks on Physical Unclonable Functions. Proceedings of the 17th ACM Conf. on Computer and Communications Security, 2010.

[8] Ganji, Fatemeh and Tajik, Shahin and Seifert, Jean-Pierre PAC Learning of Arbiter PUFs. Proceedings of Security Proofs for Embedded SystemsPROOFS 2014, 2014.

[9] Ganji, Fatemeh and Tajik, Shahin and Seifert, Jean-Pierre Why attackers win: on the learnability of XOR arbiter PUFs. Proceedings of 8th International Conference on Trust and Trustworthy Computing, 2015.

[10] Ganji, Fatemeh and Krämer, Juliane and Seifert, Jean-Pierre and Tajik, Shahin Lattice Basis Reduction Attack against Physically Unclonable Functions. 22nd ACM Conference on Computer and Communications Security, 2015.

[11] Nguyen, Phong and Stern, Jacques The Hardness of the Hidden Subset Sum Problem and Its Cryptographic Implications. Advances in CryptologyCRYPTO99, 1999.

Fully homomorphic encryption must be fat or ugly

Martin Strand[1]
Norwegian University of Technology and Science
Department of Mathematical Sciences

In 1978, Rivest, Adleman and Dertouzos asked for algebraic systems for which useful privacy homomorphisms exist. To date, the only known result is noise based encryption combined with bootstrapping. Before that, there were several failed attempts.

We prove that fully homomorphic schemes are impossible for several algebraic structures, and propose a conjecture stating that FHE schemes must either have a significant ciphertext expansion or use unusual algebraic structures.

The first contribution is an analysis of the concept of fully homomorphic encryption. It generalises a characterisation in Gentry's PhD dissertation [2] and Armknecht et al.'s notion of shift type homomorphic encryption [1]. Essentially, it says that a FHE encryption consists of a deterministic mapping into the ciphertext space, and then adding a random encryption of 0. It turns out that the security of the scheme is equivalent to being able to distinguish encryptions of 0 from a random encryption.

The second part is more concrete. We consider the possibility of schemes between groups, vector spaces, fields, rings and modules. For groups, there obviously exist secure homomorphic schemes. For vector spaces (over the same field) and fields, we give a negative answer – there simply cannot be any secure schemes that preserve the structure if both the plaintext space and the ciphertext space have the same kind of structure.

The question is more complicated for rings. We give a bound on the key space for automorphic schemes on finite semisimple reduced rings and k-algebras. For more general rings, we have no results, but we propose the conjecture that a scheme must either have an "ugly" structure, or feature a huge ciphertext expansion ("fat"). Therefore, it might not support useful computations or either require much storage

Our results suggest that the contemporary development (which one could say satisfies at least one of the above adjectives) is the right way to go. The plaintext space is usually the field with two elements, whereas the much bigger ciphertext space lacks a named structure. In particular, the operations are often not even associative.

References

[1] Frederik Armknecht, Stefan Katzenbeisser, and Andreas Peter. Shift-type homomorphic encryption and its application to fully homomorphic encryption. In Aikaterini Mitrokotsa and Serge Vaudenay, editors, *Progress in Cryptology – AFRICACRYPT 2012*, volume 7374 of *Lecture Notes in Computer Science*, pages 234–251. Springer, 2012.

[2] Craig Gentry. *A fully homomorphic encryption scheme*. PhD thesis, Stanford University, 2009. `crypto.stanford.edu/craig`.

[1] Parts of the work was done while visiting Frederik Armknecht, University of Mannheim

High-Speed Curve25519 Scalar Multiplication on ARM Cortex-M4 Microcontrollers

Fabrizio De Santis, Omar Grati, Patrick Kresmer,
Hermann Seuschek and Georg Sigl

Technische Universität München
{desantis,patrick.kresmer,omar.grati}@tum.de
{hermann.seuschek,sigl}@tum.de

Curve25519 is a 255-bit Montgomery curve introduced by Daniel J. Bernstein in 2006 for use with the Elliptic Curve Diffie-Hellman (ECDH) key exchange at the 128-bit security level [BJD06]. In the past few years, Curve25519 has received increasing attention from both academia and industry, due to its high-performance and transparency regarding the selection of its parameters. Recently, ECDH-Curve25519 scalar multiplication has been implemented on a variety of embedded devices such as 8-bit AVR ATmega, 16-bit MSP430, and 32-bit ARM Cortex-M0 microcontrollers [DHH15]. In this work, we take a step forward by implementing Curve25519 on 32-bit ARM Cortex-M4 microcontrollers and setting new constant-time speed and size records. Our implementation executes in less than 1.5 million clock cycles and requires less than 4 kB non-volatile memory for one variable base-point Curve25519 scalar multiplication, thus representing the fastest and smallest ECDH-Curve25519 software implementation for embedded devices to date.

References

[BJD06] Daniel J. Bernstein. Curve25519: new Diffie-Hellman speed records. *Public Key Cryptography*, Springer, 207–228, 2006.

[DHH15] Michael Düll and Björn Haase and Gesine Hinterwälder and Michael Hutter and Christof Paar and Ana Helena Sánchez and Peter Schwabe. High-speed Curve25519 on 8-bit, 16-bit, and 32-bit microcontrollers. https://eprint.iacr.org/2015/343.pdf, April 2015.

Bitwise key agreement using wireless channel parameters (work in progress)

Zoya Dyka, Dan Kreiser and Peter Langendoerfer

System dpt. IHP
Frankfurt (Oder), Germany

Generation, distribution and re-freshing of secret keys in wireless sensor networks are important and not simple tasks. There are many different possibilities to achieve this, for example the common secret key can be pre-distributed, or the Kerberos and Diffie-Hellmann key agreement protocols can be used, or the key can be transmitted encrypted using the public key of the receivers. In 1993 a new possibility to agree a secret key was introduced. It was proposed to use a common randomness for example caused from the location of the sender and the receiver for the key agreement. If a node A sends a signal to a node B, B receives a distorted signal due to the distance between A and B and the geometry of the room (i.e. the indoor environment) causing multi-path signal replicas at the receiver. If A and B can send an identical signal to each other in a static environment, they both receive a signal identically distorted according to the reciprocity theorem. An attacker at different position as A or B can listen to their communication but he receives signals that differ significantly from those A and B receive, since the parameters of the received signal depend on the location. So A and B can use parameters of received signals, for example the middle value of the received signal strength (RSS), for secure key agreement. Thus, one key bit can be agreed per a probe signal. To agree about a 128 bit long key at least 128 probe signals need to be exchanged between A and B. In practice a lot more probe signals need to be exchanged because A and B receive a similar but not identical signals. After A and B calculated their secret keys using all collected RSS values, these keys have to be compared to verify that they are identical. For this a hash of the new keys can be calculated and compared or A can encrypt a message with its new key and send it to B. If B can decrypt the message correctly, than both have an identical secret key.

The security strength of the key generated using channel parameters is discussed in literature because this approach is vulnerable for example to manipulation of the environment and jamming attacks. But also the key generation rate is low. The collection of RSS values, their processing and the key acknowledgement phases take relatively long. If the keys generated by A and B are different the procedure will be repeated from the beginning. Energy and time consumption are also critical parameters for WSN. To improve these parameters we propose to re-fresh secret keys bitwise after each communication using the channel parameters of the communication.

Our assumption is: during the initialization phase all sensor nodes of a WSN agree pairwise to first (initial) secret keys and a key-bit hopping scheme. The key-bit hopping scheme is a sequence of N key-bit positions. This sequence is a plan for A and B to update their secret key bitwise. The number of elements in the sequence, the distance between the elements should be different for each pair of sensor nodes. Changing the sequence according to a certain algorithm is an additional option. During the communication only one of the nodes, for example node B, obtains a new key-bit value using channel parameters. The first number in the key-bit hopping scheme defines the key-bit position that will be updated. The next message from B to A will be encrypted with the updated key. A decrypts the received message at first with the old key. If the decryption was not successful, A obtains the updated key by inversion of the key bit at the first position in the bit hopping scheme. Now A can decrypt the message with the updated key. By this approach, A and B have updated their secret key. This procedure can be repeated for the next key update at the next position the key-bit hopping scheme.

The LWE Challenge

Juliane Krämer
TU Darmstadt
Kryptographie und Computeralgebra
Germany

The learning with errors problem (LWE) is one of the most important problems in lattice-based cryptography. The security of many cryptographic schemes is directly based on the hardness of an underlying LWE instance. Understanding the concrete hardness of LWE is therefore necessary to select parameters for these lattice-based schemes. However, this hardness is not sufficiently well understood at this point in time, and the known hardness results are based on theoretic considerations rather than practical experiments. Therefore, we propose an LWE challenge that provides LWE instances in various dimensions as targets for current LWE solvers.

The LWE Challenge will help to determine the practical hardness of the LWE problem and hence to choose parameters for future lattice-based cryptographic primitives. This is especially relevant since lattice-based cryptography promises to be a secure and efficient post-quantum alternative for current schemes based on the discrete logarithm problem and integer factorization, which will not remain secure once large quantum computers are developed. Furthermore, the LWE challenge will give insight into the scope of applicability of different algorithms to solve the LWE problem, since they are expected to perform not equally well for different parameters. Hence, the LWE challenge will not only determine the practical hardness of the LWE problem, but also provide information about the practical applicability of different LWE solvers.

TU Darmstadt hosts similar challenges for other lattice problems since several years. However, a certain aspect of LWE prohibited an LWE challenge so far: An LWE instance is created by picking a uniformly random matrix $\vec{A} \in \mathbb{Z}_q^{m \times n}$, a uniformly random secret vector $\vec{s} \in \mathbb{Z}_q^n$, and a small error vector $\vec{e} \in \mathbb{Z}_q^m$, calculating $\vec{b} = \vec{A}\vec{s} + \vec{e} \in \mathbb{Z}_q^m$ and publishing $\vec{A}$ and $\vec{b}$. As of today, it is not known how to create a problem instance without knowing the solution. We have solved this problem by using secure multi-party computation (MPC). MPC allows several parties to jointly create problem instances, without any party gaining additional knowledge about the solution. We are currently implementing the MPC protocol. As soon as we are finished, we will run the protocol together with TU Eindhoven and UC San Diego and then publish the LWE Challenge website[1], which is currently password-protected.

[1] https://www.latticechallenge.org/lwe_challenge/challenge.php

Efficient and Power Analysis Resistant Implementation of the Montgomery kP-Algorithm

Estuardo Alpirez Bock, Zoya Dyka and Peter Langendoerfer

System dept.
IHP
Frankfurt (Oder), Germany

Cryptographic algorithms implemented in hardware are devices that generate, besides the processing results, additional data which is linked to the calculation. Some of this data, for example the power consumption or electromagnetic radiation, can be measured, saved and analysed for attacking the implementation with the goal to extract the cryptographic key. Such attacks are known as side channel analysis attacks. The Montgomery kP-algorithm based on [LD99] is an efficient method for performing the elliptic curve point multiplication, which is the basic operation in elliptic curve crypto-systems (ECC). With this algorithm, each bit of the key k is processed in the same way, i. e. the number of the performed mathematical operations and their sequence are independent of the processed bit value. ECC hardware implementations using this algorithm are robust against simple power analysis attacks, but not against differential power analysis (DPA) attacks.

In this work we present a method for a time and energy optimized implementation of the Montgomery kP-algorithm. Our two implemented kP-designs are resistant against a horizontal DPA attack using the *difference-of-means* test.

In our implementation not only the type, number and sequence of mathematical operations are the same for each key bit, but we also take their energy consumption into account. The processing of each bit of the key in the Montgomery kP-algorithm consists of 6 multiplications, 5 squarings and 3 additions. The number of multiplications defines the shortest possible number of clock cycles needed for processing one key bit. This minimal number can be achieved only if all other operations are performed parallel to the multiplications. Our area-optimized multipliers need 9 clock cycles in our first and 6 clock cycles in our second ECC designs to calculate the product of two 233 bit long elements of $GF(2^{233})$. All other operations, including the writing of data to registers, are performed in our new designs parallel to the multiplications and are regularly performed during the bit processing time. This way, the calculation time and energy consumption of our implemented ECC designs were reduced, while their resistance against DPA attacks was increased.

We performed the horizontal DPA attack using the difference-of-means test against our two implementations and against our old ECC design, which is a straight forward implementation of the Montgomery kP-algorithm. The old ECC design delivered 57 key-candidates. Four of these candidates were extracted with a correctness of about 90%; one candidate was extracted with 100% correctness. The first of our new implementations delivered only 54 key-candidates and none of them was extracted with a correctness higher than 70%. The second implementation delivered only 36 key-candidates, from which none was extracted with a correctness higher than 76%. Our fastest ECC design has the area of 0.3 mm^2 (IHP 130nm technology) and consumes only 1.61 μJ for the performance of a complete kP-operation.

References

[LD99] Julio Lopez and Ricardo Dahab. Fast multiplication on elliptic curves over $GF(2^m)$ without precomputation. *Proceedings of the First International Workshop CHES*, Springer, 1999.

Doktoranden-Forum "Sicherheit 2016”

Im Rahmen der Fachtagung

GI SICHERHEIT 2016 Sicherheit – Schutz und Zuverlässigkeit,
5. bis 7. April 2016, Universität Bonn.

Beitragsaufruf

Im Rahmen der Konferenz Sicherheit 2016, die vom 5.-7.4.2016 in Bonn stattfindet, wird erstmals ein Doktoranden-Forum angeboten. Es bietet Doktoranden die Gelegenheit ihre Forschungs- und Dissertationsvorhaben zu Aspekten der Sicherheit informationstechnischer Systeme zu präsentieren, sich mit anderen Doktoranden sowie erfahrenen Wissenschaftlern auszutauschen und Kontakte über die eigene Universität hinaus zu knüpfen.

In einem Workshop am Tag vor der Konferenz Sicherheit 2016 präsentieren die Teilnehmer des Doktoranden-Forums Ihre Arbeiten in einem Vortrag und haben die Möglichkeit sich mit anderen Doktoranden auszutauschen sowie Probleme und Lösungswege zu diskutieren. Im Rahmen der Poster-Session der Konferenz Sicherheit 2016 stellen die Teilnehmer Ihre Arbeiten mit einem Poster einem breiteren Publikum vor und können diese mit erfahrenen Wissenschaftlern und Industrievertretern diskutieren sowie weitere Kontakte knüpfen.

Doktoranden sind deshalb eingeladen, Extended Abstracts im Umfang von 4-6 Seiten zu Ihren Forschungsarbeiten einzusenden. Einreichungen dürfen zum Zeitpunkt der Tagung nicht in identischer oder sehr ähnlicher Form zitierfähig veröffentlicht worden sein. Im Sinne eines Doktoranden-Forums wird ausdrücklich gebeten, dass die Beiträge in Allein-Autorenschaft der Doktoranden erstellt werden. Eingereichte Beiträge werden nach den Kriterien Relevanz, Innovation, Interesse für ein größeres Publikum und Qualität der Darstellung bewertet. Angenommene Beiträge werden im Tagungsband der Sicherheit 2016 als GI-Edition Lecture Notes in Informatics (LNI) veröffentlicht. Autoren angenommener Beiträge müssen sich zur Konferenz Sicherheit 2016 registrieren, Ihren Beitrag in einem Vortrag im Doktoranden-Workshop am 4.4.2016 sowie als Poster auf der Konferenz Sicherheit 2016 vorstellen.

Die Qualität jedes Beitrags sowie seine Präsentation vor Ort als Vortrag und als Poster werden durch das Programmkomitee des Doktoranden-Forums bewertet. Für den Beitrag mit der besten Bewertung wird eine besondere Anerkennung vergeben.

Beiträge

Doktoranden sind eingeladen, einen Extended Abstract von 4 bis 6 Seiten in deutscher oder englischer Sprache einzureichen. Die Veröffentlichung im Tagungsband setzt zwingend voraus, dass eine der unter https://www.gi.de/service/publikationen/lni/ verfügbaren Formatvorlagen verwendet wurde. Autoren von akzeptieren Beiträgen müssen garantieren, dass ihr Beitrag auf der Konferenz als Vortrag und Poster (DIN A0 Hochformat) präsentiert wird.

Einreichung

Bitte kennzeichnen Sie Einreichungen für das Doktoranden-Forum mit dem Präfix **PhD:** vor dem angegebenen Beitragstitel.
Alle Beiträge müssen hier eingereicht werden:
https://easychair.org/conferences/?conf=sicherheit16

Wichtige Termine

Einreichungen: 14.12.2015
Benachrichtigung über die Annahme: 18.1.2016
Abgabe der druckfähigen Manuskripte: 1.2.2016
Anmeldung: 1.2.2016
Doktoranden-Workshop: 4.4.2016
Konferenz Sicherheit 2016: 5.-7. 4.2016

Chair

Delphine Reinhardt, Rheinische Friedrich-Wilhelms-Universität Bonn und Fraunhofer FKIE

Komitee des Forums

Frederik Armknecht, Universität Mannheim
Rainer Böhme, Universität Innsbruck
Hannes Federrath, Universität Hamburg
Felix Freiling, Friedrich-Alexander-Universität Erlangen-Nürnberg
Thorsten Holz, Ruhr-Universität Bochum
Stefan Katzenbeisser, Technische Universität Darmstadt
Michael Meier, Rheinische Friedrich-Wilhelms-Universität Bonn und Fraunhofer FKIE
Ulrike Meyer, Rheinisch-Westfälische Technische Hochschule Aachen
Joachim Posegga, Universität Passau
Alexander Pretschner, Technische Universität München
Kai Rannenberg, Goethe-Universität Frankfurt
Konrad Rieck, Georg-August-Universität in Göttingen
Jörg Schwenk, Ruhr-Universität Bochum
Matthew Smith, Rheinische Friedrich-Wilhelms-Universität Bonn und Fraunhofer FKIE

Webseite

https://sicherheit2016.de/DokForum.html

24th Crypto-Day

Bonn-Aachen International Center for Information Technology
4 April 2016
Bonn, Germany

On 4 April 2016, the interest group “Angewandte Kryptographie” of Gesellschaft für Informatik e. V. will host the twenty-fourth *Crypto-Day*.

Ambition and Program: The Crypto-Day aims at providing an opportunity for early-stage researchers in the field of cryptography and IT-security to exchange knowledge and establish networks to universities as well as to industry (e.g. for collaboration across Germany, or to find out about research internships and post-doc positions). Therefore, we invite students, doctoral candidates, and experienced researchers to present their research results or research ideas in the form of 20 minute presentations on this upcoming Crypto-Day.
The B-IT will host the event, co-located to the conference GI Sicherheit 2016.

Topics: The presented talks shall cover a broad spectrum from the field of cryptography or IT-security. We invite presentations of work-in-progress, contributions, which may be submitted to a conference, or summarize findings from a thesis or dissertation.
Submitted articles corresponding to the presentations will be arranged in a technical report. Therefore, submissions will be quotable publications and will be published on the web page. Observe that this does not forbid the publication of the result at other conferences or journals.

Attendance: There are **no participation fees**.

Submission: Please submit an abstract of your talk (**one DIN A4 page**). To simplify generation of the technical report, we request you to only use the LaTeX template of the cryptography group and to provide the PDF file additionally to the LaTeX sources.

Further information related to the venue, as well as to the registration and submission process will be provided timely on the web page https://cosec.bit.uni-bonn.de/students/events/kryptotag24/.

Further Information (Program, Venue, LaTeX-template): http://www.kryptotag.de

Submission:	Until **20 March 2015** per email
Registration:	Until **20 March 2015** per email
Organisation:	Frederik Armknecht, Universität Mannheim Michael Nüsken, b-it, Universität Bonn
Contacts:	armknecht@uni-mannheim.de nuesken@bit.uni-bonn.de