26th Crypto-Day

June 01 and 02, 2017

Nuremberg, Germany

Kryptotag SUSE, 1.-2. Juni 2017

Donnerstag, 1. Juni 2017			Art	Speaker	Affiliation	Title
13:00	13:05	0:05	Welcome			
13:05	13:35	0:30	*Keynote Talk*	Johannes Segitz	SUSE, Nürnberg	Vorstellung SUSE; security Prozess
13:35	14:05	0:30	Talk	Lars Tebelmann	Technical University Munich, Germany	EM Attack on BCH-based Error Correction for PUFs
14:05	14:35	0:30	Talk	Heiko Stamer	-	Distributed Key Generation and Threshold Decryption for OpenPGP
14:35	15:00	0:25	**Coffee Break**			
15:00	15:30	0:30	Talk	Michael Nüsken	b-it, Uni Bonn	On the Security of IPsec
15:30	16:00	0:30	Talk	Venesa Watson	University of Siegen	Optimization of Encryption for Time Sensitive Networks
16:00	16:30	0:30	Talk	Christian Gorke	Mannheim	Security Auditing for the Cloud: Cloud Storage File Recoverability
16:30	16:55	0:25	**Coffee Break**			
16:55	17:25	0:30	Talk	Nikolaos Athanasios Anagnostopoulos	TU Darmstadt; Yale University; University of Connecticut	Insights into the Potential Usage of the Initial Values of DRAM Arrays of Commercial O -the-Shelf Devices for Security Applications
17:25	18:00	0:35	GI Fachgruppe			
18:00	19:00	1:00	"Kofferpause"			
19:00			**Excursion**			
Freitag, 2. Juni 2017			**Art**	**Speaker**	**Affiliation**	**Title**
9:00	9:30	0:30	Talk	Dan Kreiser	IHP, Frankfurt/Oder	Run-time refreshing of symmetric keys in automation systems as countermeasure against real-time attacks
9:30	10:00	0:30	Talk	Ievgen Kabin	IHP, Frankfurt/Oder	Horizontal DEMA Attack as Low Cost E ective Mean to Reveal Keys
10:00	10:30	0:30	Talk	Ievgen Kabin	IHP, Frankfurt/Oder	Horizontal DPA Attacks: Low-cost and High-e ective
10:30	10:55	0:25	**Coffee Break**			
10:55	11:25	0:30	Talk	Dan Kreiser	IHP, Frankfurt/Oder	Selecting the Best Suitable EM Probe using Horizontal DEMA Attack
11:25	11:55	0:30	Talk	Edita Bajramovic	Friedrich-Alexander-University Erlangen-Nürnberg & AREVA GmbH Erlangen, Germany	Forensic Readiness Industrial Instrumentation and Control (I&C) Systems
11:55	12:55	1:00	**Lunch**			

EM Attack on BCH-based Error Correction for PUFs

Lars Tebelmann, Michael Pehl, Georg Sigl

Technical University Munich, Germany; {lars.tebelmann,m.pehl,sigl}@tum.de

Cryptographic key storage is an important requirement in embedded devices. Physical Unclonable Functions (PUFs) are security primitives based on intrinsic differences of physical objects, which can be used for this task. Key generation from PUFs provides a cost-efficient alternative to secure key storage on embedded devices. Instead of storing the secret key permanently in a non-volatile memory, which is prone to physical attacks or needs further expensive protection, the key is generated only on demand from the PUF response and is not stored permanently on the device. To ensure reliable PUF-based key generation, helper data algorithms based on error-correcting codes (ECCs) are used [1].

The helper data algorithm of the fuzzy commitment scheme [2] in combination with a concatenation of ECCs [3] has been shown to be vulnerable against a first order differential power analysis (DPA) attack in [4], where a code word masking scheme was proposed as a countermeasure.

This work transfers the original attack from [4] to the electromagnetic (EM) emissions side channel and develops a second order DPA attack on the code word masking scheme. The original correlation-based DPA attack is improved by incorporating a priori knowledge from leakage of the public helper data. Subsequently, an extension is proposed, which exploits the correlation pattern of the original attack in combination with the a priori knowledge. This extension of the original DPA attack decreases the number of traces for an attack. It is employed to successfully attack the PUF response used in the fuzzy commitment scheme. Exceeding the work in [4], the PUF response of an entire decoding cycle is recovered. Furthermore, the negative influence of bit errors in the PUF response on the DPA attack is analyzed. A second order DPA attack on the code word masking scheme is successfully conducted based on the proposed extension. Possible countermeasures to prevent the second order DPA attack are sketched.

The results proof that DPA attacks on ECCs for PUF-based key generation are possible and show the feasibility as well as the increased effort for a second order DPA attack on masked ECC implementations.

References

[1] Matthias Hiller, Michael Pehl, and Georg Sigl. Fehlerkorrekturverfahren zur sicheren Schlüsselerzeugung mit Physical Unclonable Functions. *Datenschutz und Datensicherheit - DuD*, 39(229-233), 2015.

[2] Ari Juels and Martin Wattenberg. A fuzzy commitment scheme. In *Proceedings of the 6th ACM Conference on Computer and Communications Security*, CCS '99, pages 28–36. ACM, 1999.

[3] Christoph Bösch, Jorge Guajardo, Ahmad-Reza Sadeghi, Jamshid Shokrollahi, and Pim Tuyls. Efficient helper data key extractor on FPGA. In Elisabeth Oswald and Pankaj Rohatgi, editors, *Cryptographic Hardware and Embedded Systems – CHES 2008. 10th international workshop. Washington, DC, USA, August 10 - 13, 2008. Proceedings*, pages 181–197. Springer, 2008.

[4] Dominik Merli, Frederic Stumpf, and Georg Sigl. Protecting PUF error correction by codeword masking. *IACR Cryptology ePrint Archive*, 334, 2013.

Distributed Key Generation and Threshold Decryption for OpenPGP

Heiko Stamer*

* HeikoStamer@gmx.net

We report on our experimental implementation of a distributed key generation (DKG) protocol [GJKR07] for discrete logarithm based cryptosystems and its straight-forward integration for generating ElGamal encryption keys [Elg85]. A simple and well-known reliable broadcast (RBC) protocol [CKPS01] is used as mechanism to achieve some validity, consistency, and totality of the exchanged DKG messages in a most likely asynchronous communication environment. The implemented threshold decryption [CGS97] employs non-interactive zero-knowledge proofs of knowledge in order to avoid interactiveness of the decryption process. The source code of all is released under a free software licence (GPLv2) in the most recent version 1.3.0 of LibTMCG [Sta17].

Related work [CBVK04, DCC08, KG09, KHG12] is mostly known from the areas of secure multiparty computation and electronic voting, where so-called *t-resiliance* is often required for distributing trust among the involved parties in a robust way, i.e., at most t participants can be malicious or fail to participate. However, there are also some interesting usage scenarios of DKG and threshold decryption for OpenPGP [RFC4880] that we would like to discuss in this talk.

References

[GJKR07] Rosario Gennaro, Stanislaw Jarecki, Hugo Krawczyk, and Tal Rabin. Secure Distributed Key Generation for Discrete-Log Based Cryptosystems. *Journal of Cryptology*, 20(1):51–83, 2007.

[Elg85] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. Advances in Cryptology — CRYPTO '84, LNCS 196, pp. 10–18, 1985.

[CGS97] Ronald Cramer, Rosario Gennaro, and Berry Schoenmakers. A Secure and Optimally Efficient Multi-Authority Election Scheme. Advances in Cryptology — EUROCRYPT '97, LNCS 1233, pp. 103–118, 1997.

[CKPS01] Christian Cachin, Klaus Kursawe, Frank Petzold, and Victor Shoup. Secure and Efficient Asynchronous Broadcast Protocols. Advances in Cryptology — CRYPTO '01, LNCS 2139, pp. 524–541, 2001.

[CBVK04] A. T. Chronopoulos, F. Balbi, D. Veljkovic, and N. Kolani. Implementation of distributed key generation algorithms using secure sockets. Proceedings of the Third IEEE International Symposium on Network Computing and Applications (NCA 2004), pp. 393-398, 2004.

[DCC08] Adam M. Davis, Dmitri Chmelev, and Michael R. Clarkson. Civitas: Implementation of a Threshold Cryptosystem. Computing and Information Science Technical Report, Cornell University, 2008.

[KG09] Aniket Kate and Ian Goldberg. Distributed Key Generation for the Internet. Proceedings of the 29th IEEE International Conference on Distributed Computing Systems (ICDCS 2009), pp. 119–128, 2009.

[KHG12] Aniket Kate, Yizhou Huang, and Ian Goldberg. Distributed Key Generation in the Wild. Cryptology ePrint Archive: Report 2012/377, 2012. https://eprint.iacr.org/2012/377

[RFC4880] J. Callas, L. Donnerhacke, H. Finney, D. Shaw, and R. Thayer. OpenPGP Message Format. *Network Working Group, Request for Comments*, No. 4880, November 2007.

[Sta17] Heiko Stamer. LibTMCG. http://www.nongnu.org/libtmcg/

On the security of IPsec

Michael Heußen
Universität Bonn

Daniel Loebenberger
genua GmbH, Kirchheim

Michael Nüsken
b-it, Universität Bonn

May 2017

The security of IPsec has been considered repeatedly, however a precise, complete, accessible security reduction is still missing. Paterson (2006) says 'The full IKEv2 protocol surely deserves a formal analysis.' and to our knowledge this has still not been done. So our work provides game-based security definitions suitable for this investigation, basically adapting AKE to IKEv2. We provide an explicit security reduction for IKEv2 with mutual authentication. Algorithm negotiation is part of our treatment and we use no abstractions. It turns out that we need a slightly stronger Oracle Diffie-Hellman assumption than used for TLS and we need that an extra assumption, that we call RCR security, about the signatures which for practical schemes boils down to collision-resistance of the underlying hash function with a attacker known, but unpredcitable part in the message.

This analysis is a starting point for further investigations. In particular, unilateral authentication and downgrade attacks to IKEv1 are not yet covererd. A reference implementation suitable for automatic verification and a machine assisted proof for its security is the ultimate goal.

References

TIBOR JAGER, FLORIAN KOHLAR, SVEN SCHÄGE & JÖRG SCHWENK (2011). On the Security of TLS-DHE in the Standard Model. *Cryptology ePrint Archive* **2011/219**, 41 pages. URL `http://ia.cr/2011/219`. Latest version 20 February 2013.

TIBOR JAGER, FLORIAN KOHLAR, SVEN SCHÄGE & JÖRG SCHWENK (2012). On the Security of TLS-DHE in the Standard Model. In *Advances in Cryptology: Proceedings of CRYPTO 2012*, Santa Barbara, CA, REIHANEH SAFAVI-NAINI & RAN CANETTI, editors, volume 7417 of *Lecture Notes in Computer Science*, 273–293. Springer-Verlag, Berlin, Heidelberg. ISBN 978-3-642-32008-8 (Print) 978-3-642-32009-5 (Online). ISSN 0302-9743. URL `http://dx.doi.org/10.1007/978-3-642-32009-5_17`. .

C. KAUFMAN, P. HOFFMAN, Y. NIR, P. ERONEN & T. KIVINEN (2014). Internet Key Exchange Protocol Version 2 (IKEv2). URL `http://tools.ietf.org/html/rfc7296`. RFC 7296.

KENNETH G. PATERSON (2006). A cryptographic tour of the IPsec standards. *Information Security Technical Report* **11**(2), 72–81. URL `http://dx.doi.org/10.1016/j.istr.2006.03.004`.

OLIVER SOEST (2014). *Kryptographische Analyse von IPsec*. Master thesis, Ruhr-University Bochum, Germany, Bochum, Germany.

KATRIN WEIDEN (2014). *Cryptographic Analysis of IPsec IKE*. Master thesis, Ruhr-University Bochum, Germany, Bochum, Germany.

Optimization of Encryption for Time Sensitive Networks

Venesa Watson* † and Jochen Sassmannshausen*
* University of Siegen † AREVA GmbH
Siegen, Germany Erlangen, Germany

Critical industrial networks are characterized as having complex network architectures, with each level having specific functional requirements. For example, a typical industrial network architecture will have the field level network at the lowest point, with the control level just above, followed by the management level [1]. The field level is the most time-critical of this architecture, requiring bus cycle times (time taken for the exchange of data between master and slaves or between slaves) of less than 10ms, due to the critical nature of the data communicated here [2]. At the other levels, the favourable maximum bus cycle times are far greater. Given this requirement for rapid system reaction time at specific levels, typically, such network segments do not feature security measures to preserve confidentiality and integrity, as associated security controls would introduce additional time constraints. However, the absences of these controls suggest that there are security gaps in industrial networks that cyber-attackers can exploit. This is of great concern, as attacks against critical industries, such as the power industry, can result in disruptions in significant sectors of society, such as transportation, financial institutions and medical facilities. One control that adds a significant overhead to system response time, is cryptography. This control is used in various ways to ensure confidentiality and integrity, such as by verifying and validating connected systems and users through authentication and authorization mechanisms, and verifying the trustworthiness of data through hashing techniques. However, implementing cryptographic controls require additional resources to facilitate the encryption, decryption and the verification processes, which contributes significant overhead to large complex networks.

To present cryptographic controls as favourable to time sensitive networks, this paper seeks to evaluate optimization techniques for cryptographic controls, the effort of which is to maintain system real-time responsiveness. This paper also seeks to evaluate the limitation of current or popular industrial network protocols, such as Modbus and Profibus, in supporting these controls, in comparison to more resilient protocols. In this work, we intend to evaluate the use of Counter Mode of Operation (e.g. CTR-AES) to accelerate encryption and decryption operations [3] [4] [5]. The results will then be compared to those from previous works, such as where parallelism is employed in accelerating encryption, using two cryptographic modes, namely Cipher Block Chaining (CBC) and Interleaved CBC (ICBC) [6] [7]. Modbus, Profibus, Profinet and Avionics Full-Duplex Switched Ethernet (AFDX) networks will serve as the testbed for the comparison of these techniques. In our talk, we will we discuss the selection of the Counter Mode of Operation for encryption/decryption acceleration, time sensitive networks in the industrial context, the limitations of popular protocols, and the strengths of current and emerging industrial ethernet technology in better maintaining real-time responsiveness whilst also supporting cryptographic controls.

References

[1] Knapp, E.D. and Langill, J. T., (2015). Industrial Network Security Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems (2nd ed). Syngress (Elsevier), USA.

[2] Profibus International, (2009), PROFIBUS Installation Guideline for Planning Version 1.0.

[3] Lipmaa, H., Rogaway, P. and Wagner, D., (2000), Comments to NIST concerning AES Modes of Operations: CTR-Mode Encryption. Symmetric Key Block Cipher Modes of Operation Workshop.

[4] Jonsson, J. (2002), On the Security of CTR + CBC-MAC NIST Modes of Operation Additional CCM Documentation.

[5] Mohan, H. and Reddy, A., (2012), Revised AES and its Modes of Operation. International Journal of Information Technology and Knowledge Management.

[6] Duta, C., Michiu, G. and Stoica, S., (2013), Accelerating Encryption Algorithms Using Parallelism. 19th International Conference on Control Systems and Computer Science (CSCS).

[7] Dongara, P. and Vijakumar, T., (2003), Accelerating Private-Key Cryptography via Multithreading on Symmetric Multiprocessors. IEEE International Symposium on Performance Analysis of Systems and Software (ISPASS).

Security Auditing for the Cloud: Cloud Storage File Recoverability

Christian A. Gorke*, Christian Janson†, Frederik Armknecht*, and Carlos Cid‡

* University of Mannheim, Mannheim, Germany
† Technische Universität Darmstadt, Darmstadt, Germany
‡ Information Security Group, Royal Holloway, University of London, UK

Data loss is perceived as one of the major threats for cloud storage. Consequently, the security community developed several challenge-response protocols that allow a user to remotely verify whether an outsourced file is still intact. For example, to verify availability of an outsourced file cryptographic proofs like "Proofs of Retrievability" or "Proofs of Data Possession" are being employed. However, two important practical problems have not yet been considered in this context. First, clients commonly outsource multiple files of different sizes, raising the question how to formalize such a scheme and in particular ensuring that *all* files can be simultaneously audited. And even if this is done, it needs to be efficient such that it can be executed in the form of regular audits without hindering the usual services. Second, in case auditing of the files fails, existing schemes do not provide a client with any method to prove if the original files are still recoverable. In other words, even if a small error occurs, for example due to hardware failure, the original data may still be recoverable but the client does get the information that his data is lost.

We address both problems and describe appropriate solutions. The first problem is tackled by providing a new type of "Proofs of Retrievability" scheme, enabling a client to check all files simultaneously in a compact way. Additionally, we introduce a cloud storage model in order embed practical structures into the security model. This further allows us to not only check multiple files but also multiple cloud storage instances simultaneously, such as blobs and containers. The second problem is solved by defining a novel procedure called "Proofs of Recoverability", enabling a client to obtain an assurance whether a file is recoverable or irreparably damaged. Finally, we present a combination of both schemes allowing the client to check the recoverability of all her original files, thus ensuring cloud storage file recoverability.

In this talk we further present our solution as part of security audits in the cloud environment. Security audits are cryptographic schemes which provably verify security properties of the cloud, such as availability of storage. We published our results as "Cloud Storage File Recoverability" at the Fifth International Workshop on Security in Cloud Computing (SCC), co-located to AsiaCCS, in 2017 [1]; an extended version is available on IACR Cryptology ePrint Archive [2].

References

[1] Christian A. Gorke, Christian Janson, Frederik Armknecht, and Carlos Cid. Cloud Storage File Recoverability. Proceedings of the Fifth ACM International Workshop on Security in Cloud Computing, SCC@AsiaCCS 2017, Abu Dhabi, United Arab Emirates, April 2, 2017.

[2] Christian A. Gorke, Christian Janson, Frederik Armknecht, and Carlos Cid. Cloud Storage File Recoverability. IACR Cryptology ePrint Archive, 2017:167, 2017.

Insights into the Potential Usage of the Initial Values of DRAM Arrays of Commercial Off-the-Shelf Devices for Security Applications

Nikolaos Athanasios Anagnostopoulos*, André Schaller*, Yufan Fan*, Wenjie Xiong†, Fatemeh Tehranipoor‡, Tolga Arul*, Sebastian Gabmeyer*, Jakub Szefer†, John A. Chandy‡ and Stefan Katzenbeisser*

* Security Engineering Group (CRISP-CYSEC), Technische Universität Darmstadt
† Computer Architecture and Security Lab, Yale University
‡ Department of Electrical and Computer Engineering, University of Connecticut

Several cryptographic applications entail the availability of a secure storage on a device, for instance, to store secret keys. Physical Unclonable Functions (PUFs) can be used to provide such key storage on commodity devices in a cost-efficient manner [KKR+12]. Their security is based on the existence of at least one (random but stable) output that is unique per device for some given input. Recently, a number of different PUF implementations based on DRAMs have been proposed [SXA+17, TKXC15, TKYC17, XSA+16]. We draw motivation from these recent publications in order to investigate the potential of the initial values of DRAMs found in commercial off-the-shelf devices to be used for the implementation of a PUF.

For this purpose, we test the DRAM arrays of two evaluation platforms, i.e. Intel Galileo Gen. 2 and PandaBoard ES Rev. B3. The Intel Galileo platform features a 256 (2×128) MB DDR3 SDRAM, with a row size of 16 KB, whereas the PandaBoard contains a 1 GB Low Power (LP)DDR2 SDRAM with a row size of 32 KB. To access the values of the DRAM cells, we modify the Quark EDKII firmware on the Galileo board and the U-Boot bootloader on the PandaBoard. For enabling better insights, we obtain the initial values of the DRAM at two different positions in the progression of the boot process of each evaluation platform.

On the Intel Galileo board, code position *GP1* marks the state during boot when the DRAM has been completely set up, but has not yet been written to by any user code. At this state, however, only the refresh function has been set up, while the error correction function has not yet been set

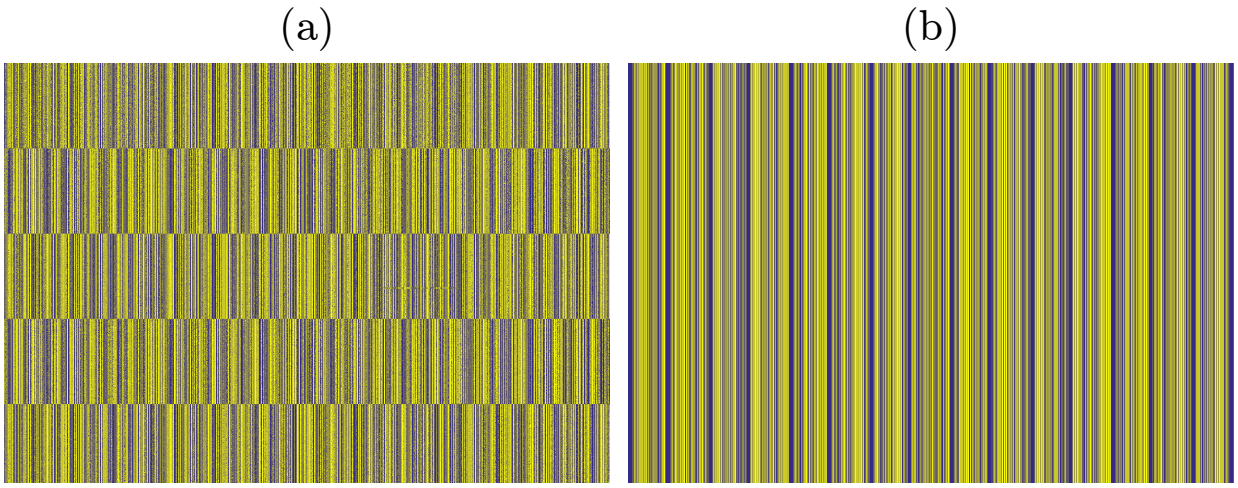


Figure 1: Patterns observed in the initial values of the DRAM of the Galileo.

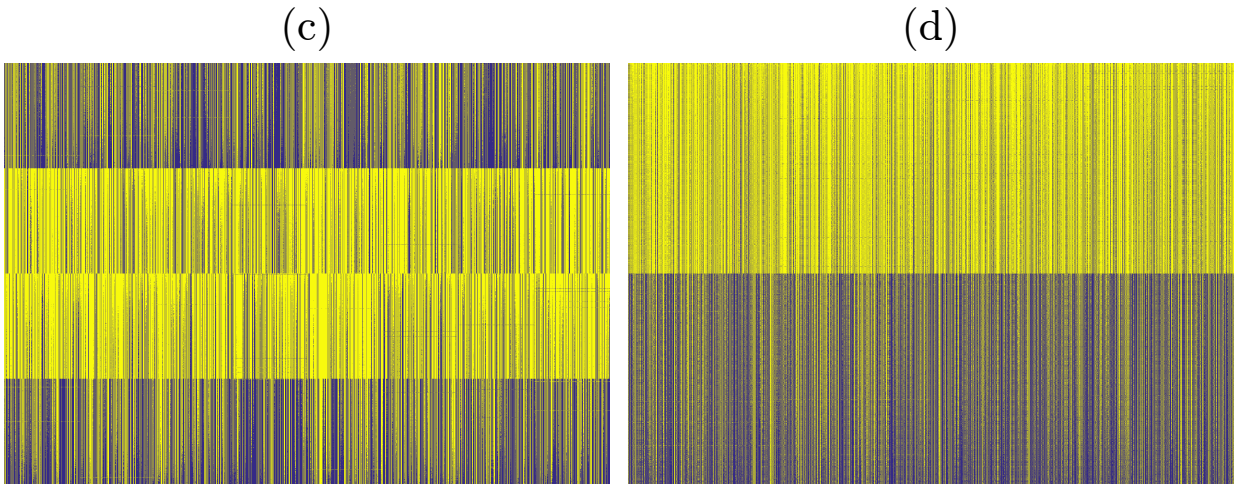


Figure 2: Patterns observed in the initial values of the DRAM of the PandaBoard.

up. Code position *GP2* refers to a prior state when the system has just enabled access to the DRAM, after setting up and initialising its addressing system. At code position *GP1*, we observe distinct pattern segments, one after the other, as shown in Figure 1a. The first four segments exhibiting a pattern have a length of 416 rows, whereas the fifth one is only 384 rows long. This behaviour is repeated in the following segments. At code position *GP2*, all of the memory follows a single pattern as shown in Figure 1b. Values at both code positions exhibit different patterns and noise between measurements, whereas changes in the firmware alter observed patterns even more radically.

On the PandaBoard, code position *PP1* marks the state during boot when the system has almost finished setting up the DRAM and all its functions, but the DRAM has not yet been written to by any user code, while, code position *PP2* refers to a prior state when the system has just enabled serial communication for transferring the initial values and only a low-level setup of the DRAM has occured, i.e. system access to the DRAM array has been enabled and its addressing system has been set up and initialised. In both cases, we observe distinct pattern segments, one after the other. However, slight modifications of the PandaBoard's U-Boot bootloader can change the segment length, e.g., from 512 rows (Figure 2c) to 1024 rows (Figure 2d).

Further analysis using relevant metrics, such as Hamming weight and intra- and inter-Hamming distances, confirms that the observed patterns prevent the usage of the obtained boot-up values of these commercial DRAMs as a PUF. Nevertheless, these patterns may provide insights into the physical layout of the DRAM arrays and into the relation between physical and logical addresses. Future research may enable access to the values of fully uninitialised cells of commercial DRAMs, which may then prove useful for security applications.

References

[KKR+12] Stefan Katzenbeisser, Ünal Kocabaş, Vladimir Rožić, Ahmad-Reza Sadeghi, Ingrid Verbauwhede, and Christian Wachsmann. PUFs: Myth, fact or busted? A security evaluation of Physically Unclonable Functions (PUFs) cast in silicon. In *Cryptographic Hardware and Embedded Systems–CHES 2012*, pages 283–301. Springer, 2012.

[SXA+17] André Schaller, Wenjie Xiong, Nikolaos A. Anagnostopoulos, Muhammad Umair Saleem, Sebastian Gabmeyer, Stefan Katzenbeisser, and Jakub Szefer. Intrinsic rowhammer PUFs: Leveraging the rowhammer effect for improved security. In *2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE, 2017.

[TKXC15] Fatemeh Tehranipoor, Nima Karimian, Kan Xiao, and John Chandy. DRAM-based intrinsic physical unclonable functions for system level security. In *25th Great Lakes Symposium on VLSI*, pages 15–20. ACM, 2015.

[TKYC17] Fatemeh Tehranipoor, Nima Karimian, Wei Yan, and John A. Chandy. DRAM-based intrinsic physically unclonable functions for system-level security and authentication. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 25(3):1085–1097, 2017.

[XSA+16] Wenjie Xiong, André Schaller, Nikolaos A. Anagnostopoulos, Muhammad Umair Saleem, Sebastian Gabmeyer, Stefan Katzenbeisser, and Jakub Szefer. Run-time accessible DRAM PUFs in commodity devices. In *Cryptographic Hardware and Embedded Systems–CHES 2016*, volume 9813 of *Lecture Notes in Computer Science (LNCS)*, pages 432–453. Springer, 2016.

Run-time refreshing of symmetric keys in automation systems as countermeasure against real-time attacks

Dan Kreiser, Zoya Dyka, and Peter Langendoerfer

IHP
Im Technologiepark 25,
Frankfurt (Oder), Germany

The demand of replacing wired automation systems (AS) by wireless systems is steadily increasing. The flexibility of wireless AS is a big advantage. To make wireless communication systems usable for automation systems, it is crucial to fulfil the strong requirements with respect to reliability and security. A secure communication between nodes can be achieved by using cryptographic methods. For automation systems the protection against manipulation of the manufacturing process is even more important than the confidentiality of the processed data.

It is always possible to listen to a wireless communication between nodes assumed that the attacker is in the range and has adequate antennas. Thus, the attacker can always find the cryptographic key by using brute-force methods, even though it can take a long time. If the attacker revealed the key and if the key is still valid then it is possible for an attacker to use the key to inject faulty messages. By using special hardware the time needed to extract the secret key can be significantly reduced. A possible countermeasure could be to change the key in short time intervals. According to the German Federal Office for Information (BSI) a session key should expire after 48 hours. But this results in many key exchanges that are usual performed with symmetric cryptographic approaches. These symmetric approaches are very time consuming and complex. That's the reason why this will lead to a lower data rate, higher latency and higher power consumption. If the attacker can extract the secret key before a new session key is used, i.e. in less than 48 hours, then the attacker can decrypt all messages from this session and can also introduce it's own malicious messages for the rest of the current session.

A potential solution fro this issue is to use a new key for each communication. But the run-time key refreshing should use significantly less power and time than a key exchange.

In this article we will describe a low complex method for a run-time key refreshing between two nodes master and slave. The proposed run-time key refreshing can prevent real-time attacks, i.e. the manipulation of the AS. The refreshment is done using a combination of a pseudo random number generator and a real random number generator. Each message will be encrypted with a refreshed cryptographic key. Even if an attacker is able to find a cryptographic key in less than the half of the loop time, it will not be able to predict the valid key for the next message. Even if the refreshing algorithm and all already applied keys are known at a certain point in time, it is not possible to predict the next valid keys. This is due to the fact that a true random variation is included in the key refreshment algorithm and that this randomness increases with each message. Another advantage of our proposed method is that it is fault tolerant, i.e. if some messages get lost or if the communication between nodes is disturbed, the keys will still be continuously refreshed and will still be the same on both nodes.

The research leading to these results has received funding from the German Federal Ministry for Education and Research under the grant agreement no. 16KIS0219 also referred as ParSec.

Horizontal DEMA Attack as Low Cost Effective Mean to Reveal Keys

Ievgen Kabin, Zoya Dyka, Christian Wittke, Dan Kreiser and Peter Langendoerfer

IHP

Im Technologiepark 25,

Frankfurt (Oder), Germany

The mostly used side channel analysis (SCA) attacks are vertical differential power (DPA) or differential electromagnetic analysis (DEMA) attacks that need a lot of measurements to be performed. In [1] 1000 measurements were needed to reveal a single key bit using DEMA.

In contrast to classical vertical attacks only one measured trace is sufficient for a successful statistical analysis in horizontal DEMA attacks. An example of a horizontal DEMA attack is described in [2]. For this attack the device under attack e.g. an FPGA needs to be decapsulated to get an appropriate amplitude and resolution of the measured signal. In addition a lot of measured traces (about 8000) was recorded to prepare the analysis of only one trace. We performed a horizontal DEMA attack against an elliptic curve hardware accelerator for the kP operation on the NIST B-233 elliptic curve over $GF(2^{233})$, implemented on an FPGA. The investigated design is an efficient and balanced implementation of the Montgomery kP algorithm. It allows to implement all operations in parallel to the field multiplications, that increases the efficiency of the design and provides some kind of additional robustness against SCA attacks [3]. We used single electromagnetic trace measured on the power decoupling capacitor to run the attack. We used the *difference of means* test for statistical analysis. We evaluated the success of the attack by comparing the key candidates with the scalar that was really processed. Many key candidates were revealed with a high correctness. 18 of 54 key candidates have a correctness of more than 80 percent. The best key candidate extracted from the electromagnetic trace has a correctness of 94 percent.

In comparison to DPA attacks, DEMA attacks don't require difficult preparations such as implantation of a probe resistor into the attacked board. The electromagnetic trace can be measured without the need to modify the device under attack, i.e. the attack can go completely undetected. Please note that in addition electromagnetic emanation can be measured not only over the IC and wires of the PCB but also over power supply capacitors [4] on the PCB. There exist currently no means to avoid the electromagnetic emanation of capacitors which makes the horizontal DEMA attacks especially dangerous. A possible countermeasure is the integration of power supply capacitors into IC, i.e. the using of supercapacitors [5].

References

[1] E. D. Mulder et al., *Electromagnetic Analysis Attack on an FPGA Implementation of an Elliptic Curve Cryptosystem*, in EUROCON 2005, vol. 2, pp. 1879-1882

[2] J. Heyszl, S. Mangard, B. Heinz, F. Stumpf, and G. Sigl, *Localized Electromagnetic Analysis of Cryptographic Implementations*, in Topics in Cryptology CT-RSA 2012, vol. 7178, pp. 231-244.

[3] Z. Dyka, E. A. Bock, I. Kabin, and P. Langendoerfer, *Inherent Resistance of Efficient ECC Designs against SCA Attacks*, Proc. of NTMS 2016, pp. 1-5.

[4] J.-J. Quisquater and D. Samyde, *Electromagnetic Attack*, in Encyclopedia of Cryptography and Security, Springer US, 2011, pp. 382-385.

[5] Vacuum carbon technologies, http://www.vctechnologies.org/en/electrode/

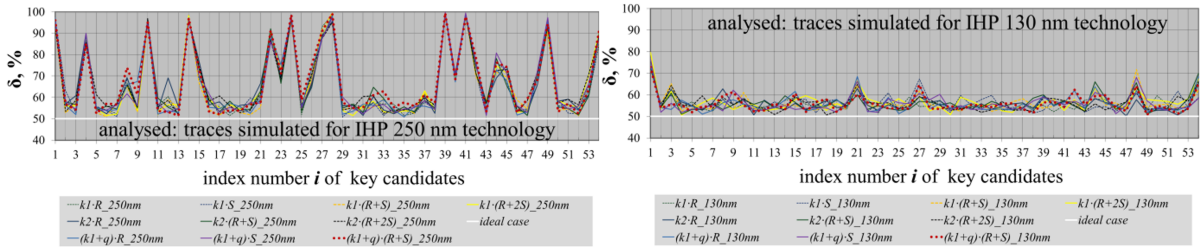
Horizontal DPA Attacks: Low-cost and High-effective

Zoya Dyka, Ievgen Kabin, Dan Kreiser and Peter Langendoerfer

IHP

Frankfurt (Oder), Germany

In this paper we evaluate the influence of different inputs such as EC point coordinates $P=(x,y)$ and scalar k on the result of our horizontal DPA attacks using the difference of means test for statistical processing of traces. We attacked our hardware implementation of the Montgomery kP accelerator for NIST EC B-233. Due to the fact that the Montgomery kP algorithm processes each key bit of the scalar k in the main loop using the same sequence of operations, it is resistant against simple SCA attacks [1]. I.e. a visual inspection of a simulated power trace of a kP of our (regular) implementation of the Montgomery ladder does not reveal the key, so our design is resistant against SPA attack. We performed horizontal DPA attacks using simulated power traces. We applied a difference of means test to reveal the scalar k. Our attack is similar to [2], but doesn't require a lot of additional measurements in the preparation step. In comparison to the horizontal correlation collision analysis attack described in [3] our attack needs by far less efforts. To evaluate the effectivity of our attack and the influence of the different inputs on the attack results we compared all obtained key candidates with the real processed scalar k. We calculated the correctness δ of each key candidate in per cent. Results of our attack show that the correctness of key candidates depends neither on the processed point P nor on the scalar k. The next graph illustrates this fact.



The results of the analysis illustrate also the fact that the well-known key randomization (traces with scalar $k1+q$) or the EC point blinding (traces with the EC points $R+S$ or $R+2S$) are not effective against horizontal DPA attacks. This statement holds true for both investigated technologies, but we admit that the designs synthesized for the 250 nm technology are more vulnerable than those synthesized for the 130 nm technology. Our experiments with the same implementation ported to a Xilinx Spartan-6 FPGA show that the FPGA implementation is even more vulnerable than the design synthesized using the IHP 250 nm technology. Using the two key candidates with the highest correctness of 99.6% and 99.1% respectively, we revealed the processed scalar 100% correctly by brute forcing the 3 not correctly revealed bits.

References

[1] T. Oliveira, J. Lopez, and F. Rodrguez-Henrquez, *The Montgomery ladder on binary elliptic curves*, Journal of Cryptographic Engineering, Apr. 2017.

[2] J. Heyszl, S. Mangard, B. Heinz, F. Stumpf, and G. Sigl, *Localized Electromagnetic Analysis of Cryptographic Implementations*, Topics in Cryptology - CT-RSA 2012. Springer. 231-244.

[3] C. Clavier, B. Feix, G. Gagnerot, M. Roussellet, and V. Verneuil, *Horizontal correlation analysis on exponentiation*, Proc. of ICICS, LNCS Vol. 6476. Springer. 46-61.

Selecting the Best Suitable EM Probe using Horizontal DEMA Attack

Christian Wittke, Ievgen Kabin, Dan Kreiser, Zoya Dyka and Peter Langendoerfer

IHP
Im Technologiepark 25
Frankfurt(Oder), Germany

Implementing cryptographic algorithms in a tamper resistant way is a complex task as the algorithm used and the target platform have a significant impact on the potential side channel leakage of the implementation. In addition the knowledge of an attacker, especially about the best suitable measurement setup and measurement point is of importance. Electromagnetic analysis (EMA) attacks are especially dangerous due to the fact that measurements of electromagnetic (EM) emanation can be done without modification of the device under attack, i.e. without being noticed that an attack occurred. A method for selecting the best measurement conditions can improve EMA attacks significantly. This method should be used by designers to evaluate the resistance of their cryptographic implementations against side channel analysis attacks before releasing them. In this work we discuss a low-cost method for comparison of measurement tools. We propose to use the results of horizontal differential electromagnetic analysis (DEMA) attacks as the criterion for determining the best suitable instruments for measurements, for example for determining the best suitable EM probe. To demonstrate the applicability of this method we performed a horizontal DEMA attack against an IHP elliptic curve cryptography (ECC) design. The design is an implementation of the Montgomery kP algorithm for NIST elliptic curve B-233 [1]. The kP design was ported to a Xilinx Spartan-6 FPGA manufactured in a 45 nm technology. The experiments were made under same measurement conditions: attacked FPGA, design, inputs, measurement point and measurement equipment, excepting the EM probes. We experimented with 7 EM probes: 2 from Riscure [2], 4 from Langer [3] and a self-made probe. Performing the horizontal DEMA attack using each EM probe results in revealing the cryptographic key - the used scalar k - with a certain correctness. We used this correctness as a criterion for the selection of the best suitable EM probe.

In our experiments the MFA-R-75 probe from Langer allowed to reveal 14 key candidates with a correctness of more than 90 per cent whereas the ICR HH 150-27 and ICR HV 150-27 microprobes from Langer dont allow to get a single key candidate with a correctness of more than 70 per cent. So, our experiments give a qualitative low-cost and low-time method for comparison of EM probes at least for a predefined measurement setup and clearly show that selecting the wrong probe for an attack may lead to a wrong impression of good resistance.

References

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

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

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

Forensic Readiness Industrial Instrumentation and Control (I&C) Systems

Edita Bajramovic* †

* Friedrich-Alexander-University Erlangen-Nuemberg
Erlangen, Germany

† AREVA GmbH
Erlangen, Germany

The vulnerability of nuclear power plants has been the research topic in the latest years. But since the disclosure of the digital worm Stuxnet and its impact on the operation of the equipment in nuclear power plants, many experts have been concerned that similar attempts to nuclear power plants could pose a severe risk.

Just this one example is suggesting that digital forensics, including digital forensic readiness, must be thoroughly planned and implemented before cybersecurity incident happens to prevent disastrous events. Forensic readiness is the state of being ready for a forensic investigation in advance of an incident occurrence. Unfortunately, even though digital forensic readiness is being established as a legal and regulatory requirement in many industries, nuclear power plants have not yet established a considerable capability in this domain.

The overall purpose of my PhD research is to address security issues in operational Instrumentation and Control (I&C) system using smart testing. The results will help to identify potential security threats in operational I&C and develop appropriate methodology to achieve appropriate level of security and implementation of forensic readiness. In addition, formalizing and implementing secure logging will support detection of unauthorized manipulations to, or tampering of, the security logs. More specifically, this PhD thesis proposes the following research question:

- How forensic readiness and secure logging can be achieved in Operational I&C systems without interfering running I&C systems? Which in turn suggests the following sub-questions:

1. How to design and implement forensic readiness?
2. How to model forensic related security controls and security properties?
3. How to formalize and implement secure logging?

The interest group Angewandte Kryptographie of Gesellschaft für Informatik e.V. hosts

27th Crypto-Day

7.-8. December 2017
Im Technologiepark 25, 15236 Frankfurt (Oder), Germany

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.

Schedule (tentative)

Thu 13:00-17:00	Talks
Thu 17:10-17:55	GI Fachgruppentreffen "Angewandte Kryptographie"
Thu 18:00-22:00	Social event
Fri 09:00-13:00	Talks

Host: The IHP is an institute of the Leibniz Association and conducts research and development of silicon-based systems and ultra high-frequency circuits and technologies including new materials. It develops innovative solutions for application areas such as wireless and broadband communication, security, medical technology, industry 4.0, automotive industry, and aerospace. The sensor networks group is working in the field of hardware accelerators for cryptographic operations for more than 10 years. Its research is embedded into national and international projects. The recent focus is on tamper resistant design approaches especially for elliptic curve cryptography. As part of the Kryptotag we will offer the opportunity of guided tours "through" our class1 clean room, HW crypto lab, focused ion beam station and test laboratory.

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

Submission/Registration:	Until **15 November 2017**, per email at kryptotag@lists.bit.uni-bonn.de
Organisation:	Zoya Dyka, IHP GmbH Michael Nüsken, b-it, Universität Bonn Frederik Armknecht, Universität Mannheim