Tagungsband zum 24. Kryptotag
4. April 2016

Workshop der Fachgruppe Kryptographie in der Gesellschaft für Informatik

Bonn-Aachen International Center for Information Technology

Version: August 30, 2016

Program

13^{00} - 13^{50} Session I.

13^{00} Jan Bobolz & Fabian Eidens (Uni Paderborn). Expressive practical credential systems from standard techniques.

13^{25} Martin Gegenleitner (Department Sichere Informationssysteme, Hagenberg, Österreich). SPAKE und FIDO U2F zur Kerberos-Preauthentication.

13^{50} - 14^{00} Rump session.

14^{30} - 15^{45} Session II.

14^{30} Christian Wittke, Zoya Dyka, Oliver Skibitzki & Peter Langendoerfer (IHP, Frankfurt/Oder). Successfully Decapsulating BGA Packages: How To.

14^{55} Estuardo Alpirez Bock, Zoya Dyka & Peter Langendoerfer (IHP, Frankfurt/Oder). Discussing the Initialization of the Montgomery kP-Algorithm in the Light of SCA.

15^{20} Peter Samarin, Kerstin Lemke-Rust & Christof Paar (Hochschule Bonn-Rhein-Sieg, RUBochum). IP Core Protection using Voltage-Controlled Side-Channel Receivers.

15^{45} Good bye and invitation to the Panel of the Doktoranden-Forum at GI Sicherheit 2016.

17^{00} - 18^{30} Panel Discussion Doktorandenforum.

Expressive practical credential systems from standard techniques

Jan Bobolz and Fabian Eidens
Paderborn University
Germany

In anonymous credential systems, there are two types of entities: users and organizations. Users are known to organizations only by pseudonyms. An organization may issue *credentials* certifying a set of *attributes* to a user. Furthermore, an organization may offer services where access is restricted to users with certain attributes. To gain access, a user can *show* an organization his credential and a chosen subset of his attributes. In secure anonymous credential systems, users stay anonymous and credentials are unforgeable. More specifically:

- Organizations only learn as much about a user and his attributes as he is willing to reveal when showing credentials
- Organizations cannot link two pseudonyms of the same user
- Users can only show credentials (and attributes) that they have been issued

While there are several alternative approaches to constructing credential systems, constructions usually follow the ideas of Camenisch and Lysyanskaya [Lys02, CL02]. They show how to construct anonymous credential systems from a signature scheme that admits certain protocols.

Our goal is to construct *simple* and practical credential systems based on recent results. As a first step, we present a concrete construction, using the recent signature scheme by Pointcheval and Sanders [PS16]. In a second step, we extend the basic show protocol such that users are not restricted to revealing a subset of attributes, but may more generally prove that their attributes fulfill some boolean formula. Finally, we discuss design choices for credential systems that should be considered when constructing a scheme for specific use cases.

This work is partially supported by the German Research Foundation (DFG) within the Collaborative Research Centre ,,On-The-Fly Computing” (SFB 901).

References

[CL02] Jan Camenisch and Anna Lysyanskaya. A signature scheme with efficient protocols. In *Security in communication networks*, pages 268–289. Springer, 2002.

[Lys02] Anna Lysyanskaya. *Signature schemes and applications to cryptographic protocol design.* PhD thesis, Massachusetts Institute of Technology, 2002.

[PS16] David Pointcheval and Olivier Sanders. Short randomizable signatures. In *Topics in Cryptology - CT-RSA*, pages 111–126. Springer, 2016.

SPAKE und FIDO U2F zur Kerberos-Preauthentication

Martin Gegenleitner

FH OÖ Fakultät für Informatik, Kommunikation und Medien
Department Sichere Informationssysteme
Softwarepark 11, 4232 Hagenberg/Mühlkreis
Österreich

Die Masterarbeit mit dem Thema „Multifaktorauthentisierung und Single-Sign-On für Inter- und Intranet-Anwendung mit FIDO U2F über Kerberos und SAML“ hat als Ziel ein Konzept, welches externen und internen Benutzergruppen multifaktor-gesicherten Single-Sign-On-Prozesse ermöglicht.

Zur Umsetzung der Multifakorauthentisierung für Kerberos wurde SPAKE [AP05, LA16] als neue Preauthentication-Methode in Kombination mit dem Signaturverfahren von FIDO U2F [FA15] verwendet. Diese Kombination erschwert bzw. verhindert, dass Angreifer einerseits Offline-Bruteforce-Attacken auf das Passwort des Benutzers durchführen und andererseits als Man-In-The-Middle aktiv in die Kommunikation eingreifen.

Für den Vortrag werden das Masterarbeitskonzept und das Kerberosprotokoll erläutert. Im Zuge der Behandlung der Kerberospreauthentication werden die Protokollschritte und die Funktionsweise von SPAKE und im Anschluss die Integration von FIDO U2F präsentiert. Am Ende werden mögliche Angreiferszenarien durchgespielt.

SPAKE steht für „Simple Password-Based Encrypted Key Exchange“ und beschreibt einen passwortgeschützten Diffie-Hellman-Schlüsselaustausch. Durch die Aushandlung eines Schlüssels wird ein sicherer Kanal geschaffen, über den weitere Authentisierungsfaktoren gesendet werden können.

Als zweiter Faktor bietet sich FIDO U2F an. Das Challenge-Response-Verfahren kann dazu genutzt werden als Challenge den Hash des vom Server gesendeten SPAKE-Parameters zu setzen. Überprüft der Client den Hash des zuvor erhaltenen Parameters und den Wert der U2F-Challenge bzw. der Server die Signatur der U2F-Challenge, können Man-In-The-Middle-Angriffe erkannt und die Kommunikation terminiert werden.

Das Konzept wurde im Zuge der Masterarbeit prototypisch mit Hilfe des MIT-Kerberosprojekts [MK16] umgesetzt und kann den Ablauf der Authentisierung demonstrieren.

Literatur

[AP05] Michel Abdalla, David Pointcheval. *Simple Password-Based Encrypted Key Exchange Protocols*, CT-RSA 2005, Volume 3376 of Lectures Notes in Computer Science, pages 191-208, San Francisco, CA, USA, Feb. 14-18, 2005. Springer-Verlag, Berlin, Germany.

[LA16] W. Ladd. *SPAKE2, a PAKE.* draft-irtf-cfrg-spake2-03.txt, URL: https://www.ietf.org/id/draft-irtf-cfrg-spake2-03.txt, 13. Februar 2016.

[FA15] FIDO Alliance. *FIDO U2F Raw Message Formats.* URL: https://fidoalliance.org/specs/fido-u2f-v1.0-nfc-bt-amendment- 20150514/fido-u2f-raw-message-formats.html, Mai 2015.

[MK16] MIT Kerberos. *Kerberos: The Network Authentication Protocol.* URL: http://web.mit.edu/kerberos/, Dezember 2015

Successfully Decapsulating BGA Packages: How To

Christian Wittke, Zoya Dyka, Oliver Skibitzki and Peter Langendoerfer

IHP
Im Technologiepark 25
Frankfurt (Oder), Germany

Some types of physical attacks e.g. optical inspection, fault injections, etc. require the device under attack (DUA) to be decapsulated. But also more common attacks such as analysis of electromagnetic (EM) traces are benefiting from decapsulations since the amplitude of the measured signal is higher and by that allows simpler analysis and better local measurements in terms of side channel attacks.

In this work we explain detailed how we successfully decapsulated a state of the art FPGA realized in a 45 nm technology and packaged in a BGA housing [1]. The challenge here is that the device needs to be fully functional after dacapsulation. When decapsulating the BGA package the acid can easily destroy the substrate that is under the die. Moreover the PCB and the mounted components need a good protection to keep the device functional. But even though the decapsulation of BGA packages is more challenging than the one of QPF packages it is doable if prepared thoroughly. As preparation steps we made a x-ray image of the device and cut the FPGA in order to learn about the dimension and placement of the die in the package. Next we run a series of experiments with different acids at different temperatures to learn which acids are suitable and how fast the plastic reacts to the acids since the manufacturer of the chip often do not reveal the material of the package. The next step is the thorough protection of the whole device since we opened the BGA package on the PCB, i.e. in-situ. For protection we used adhesive aluminum foil similar to [2]. The removal of the package material and cleaning of the die is the last step for the decapsulation of the DUA.

We destroyed only one FPGA for the preparation and successfully opened four FPGAs on PCBs which was a success rate of 100 %. As a result we tested the DUAs and recorded EM traces of an elliptic curve decryption (EC point kP operation) with the MFA-R-75 EM probe from Langer [3] to show that the die and the PCB were still fully functional and that decapsulation improves the measurement results of the EM traces.

Acknowledgments

The work presented in this paper has been partially funded by the “Ministry of Sciences, Research and Cultural Affairs (MWFK)“ from resources of the European Social Fund (ESF) and of the state Brandenburg.

References

[1] JEDEC - Global Standards for the Microelectronics Industry, www.jedec.org

[2] Loubet Moundi, P.: Cost effective techniques for chip delayering and in-situ depackaging In: COSADE 2013 Short Talks Session, https://www.cosade.org/cosade13/presentations/session5b_a.pdf

[3] LANGER EMV-Technik GmbH, MFA02 micro probe set, http://www.langer-emv.com/produkte/stoeraussendung/nahfeldsonden/set-mfa02/

Discussing the Initialization of the Montgomery kP-Algorithm in the Light of SCA

Estuardo Alpirez Bock, Zoya Dyka and Peter Langendoerfer

IHP
Im Technologiepark 25
Frankfurt (Oder), Germany

Side channel analysis (SCA) attacks have been a popular research topic in the last years. Parameters like power consumption, electromagnetic radiation and execution time of a cryptographic implementation can be analysed for identifying implementation details and based on this, extracting the private key. The Montgomery kP-algorithm using Lopez-Dahab projective coordinates [LD99] is an efficient method for performing the scalar multiplication in elliptic curve crypto-systems (ECC). This algorithm is a bitwise processing of the scalar k, which is the private key used for performing decryption in ECC. It is considered resistant against simple power analysis (SPA) since each key bit is processed by the same type, amount and sequence of operations, independently of the key bit's value. Nevertheless, its initialization phase affects this algorithm's robustness against SCA. We describe how the first iteration of the kP processing loop reveals information about the key bit being processed, i.e. bit k_{l-2}.

Using simulated power traces, we demonstrate that the power profile of the processing of k_{l-2} differs from the power profiles of the processing of all other key bits. Moreover, we demonstrate that this power profile differs significantly for the cases $k_{l-2} = 1$ and $k_{l-2} = 0$. This leads to an easy extraction of bit k_{l-2} using SPA and exposes details of the implementation of the algorithm. This can be useful for the preparation of further attacks. As a countermeasure against this vulnerability, we propose a modification of the algorithm's initialization phase and of the processing of bit k_{l-2}. We show that with this modification, the power profiles of the processings of $k_{l-2} = 1$ and $k_{l-2} = 0$ look similar to each other and similar to the processing of all remaining bits of the key, i.e. the value of the key bit k_{l-2} cannot be extracted using SPA.

Our proposed modifications increase the algorithm's robustness against SCA and even reduce the time needed for the initialization phase and for processing k_{l-2}. Compared to the original design, our new implementation needs only 0.12% additional area, while its energy consumption is almost the same, remaining by 2.09 μJ. Thus, we achieved to increase the security of our implementation without any additional costs.

Acknowledgement: The research leading to these results has received funding from the European Commission's Horizon 2020 under grant agreement from project myAirCoach – No. 643607.

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.

IP Core Protection using Voltage-Controlled Side-Channel Receivers

Peter Samarin[*,†], Kerstin Lemke-Rust[*], and Christof Paar[†]

[*] Bonn-Rhein-Sieg University of Applied Sciences
Sankt Augustin
Germany

[†] Ruhr-Universität Bochum
Bochum
Germany

We present a method for protecting netlist-based Intellectual Property (IP) cores in FPGAs using a voltage-controlled side-channel receiver. The receiver is realized by modulating the supply voltage of the chip, while at the same time detecting these changes from within the chip using a ring oscillator. The levels of the supply voltage can be determined by constantly monitoring the frequency of the ring oscillator.

The working principle of a voltage-controlled side-channel receiver is illustrated in the figure below. The analog circuit on the left is used to control the level of the supply voltage of the FPGA by setting and unsetting the wires c_0 and c_1. The digital circuit in the FPGA on the right determines the voltage level indirectly by sampling the frequency of the ring oscillator using a fixed clock. Two consecutively sampled frequencies are subtracted and compared to a fixed threshold t, in order to detect rising and falling edges. In the final step, Manchester coding is used to convert this information to one bit of data at a time.

The side-channel receiver can be used to protect any IP core individually by providing it with a unique key. To prove authorship of an IP core, the verifier first authenticates himself to the core over the voltage side-channel with the correct key, and second sends commands that limit the core's functionality. By monitoring the regular outputs of the overall system, it is possible to detect illegitimately used cores after repeatedly turning them on and off. The working principle of our method is demonstrated in a case study in which we protect several IP cores on a Spartan 3 FPGA.

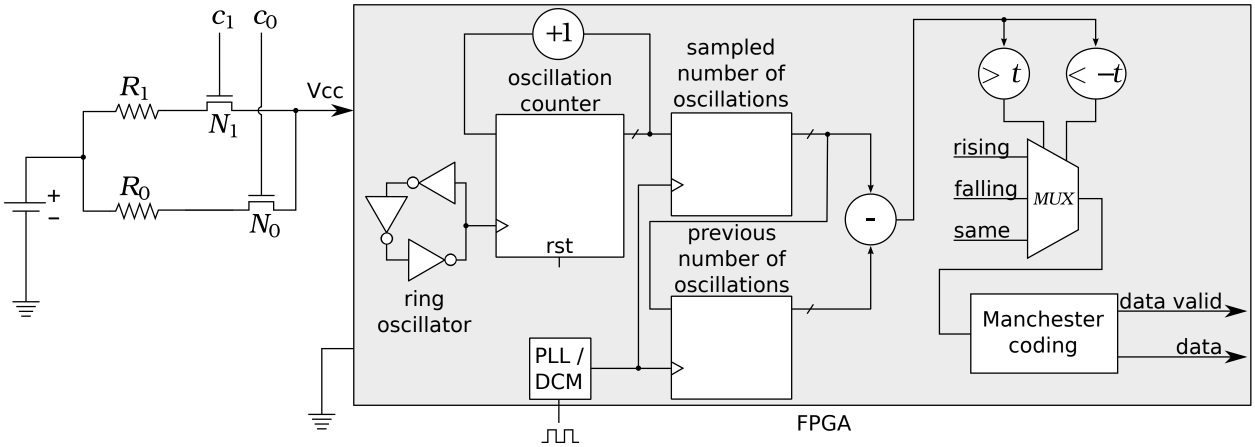

Figure 1: An example of a voltage-controlled side-channel receiver.