20th Crypto-Day

Telekom Innovation Laboratories
June 26 and 27, 2014
Berlin, Germany

On 26th and 27th June 2014, the interest group "Angewandte Kryptographie" of Gesellschaft für Informatik e. V. will host the twentieth *Crypto-Day*.

Ambition and Program: The Crypto-Day aims at providing an opportunity for early-stage researchers in the field of cryptography 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). Students, doctoral candidates, and experienced researchers present their research results or research ideas in the form of 20 minute presentations on this upcoming Crypto-Day.

Host: The Telekom Innovation Laboratories will host the event and provide an insight into product security aspects and ongoing industry research.

Topics: The presented talks cover a broad spectrum from the field of cryptography or IT-security.

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

Further information related to the venue, as well as to the registration are given below.

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

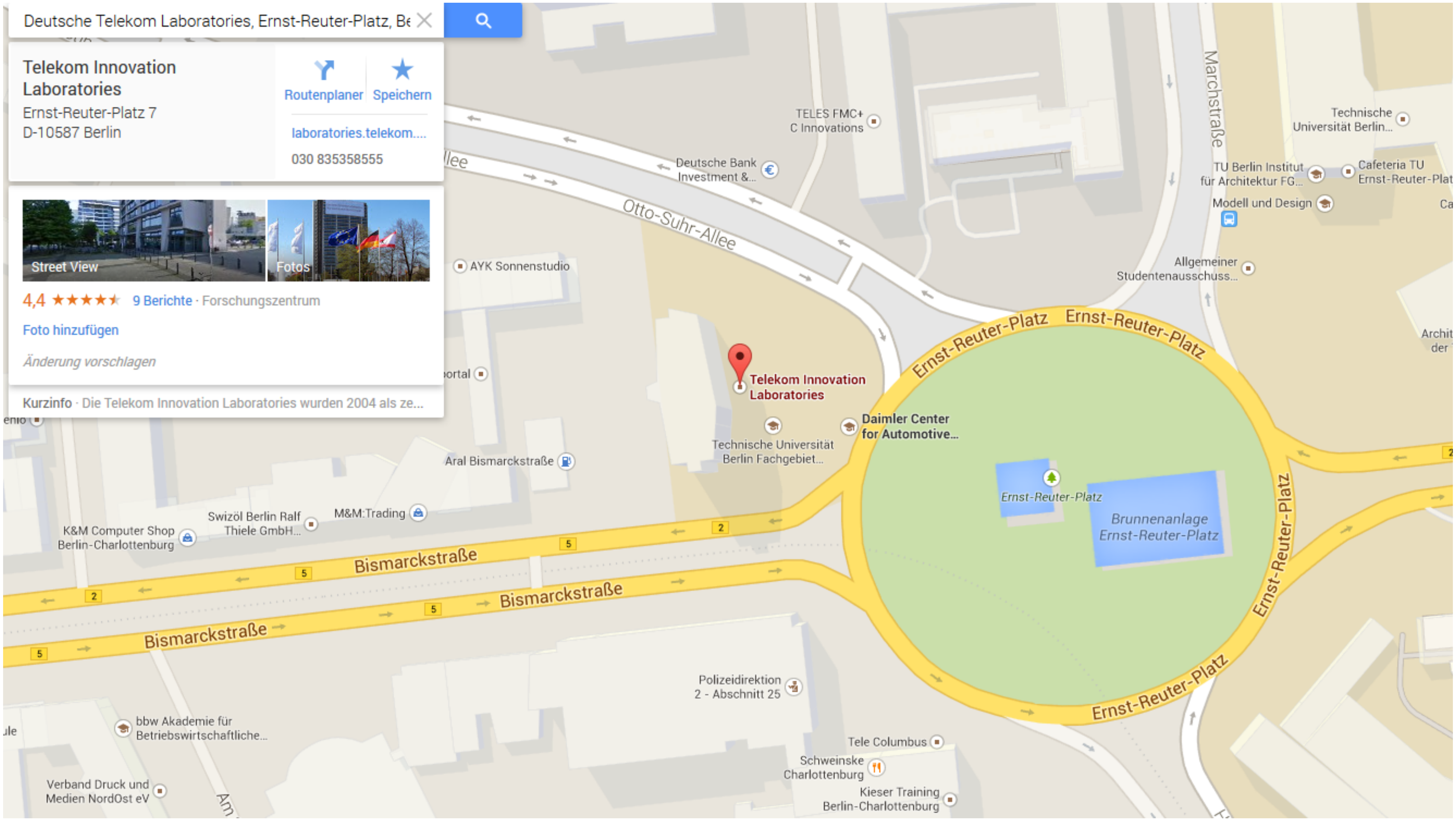
Registration: Until **June 12** under https://registration.crypto.ruhr-uni-bochum.de/conf/KryptotagBerlin20/

Venue: T-Labs, Ernst-Reuter-Platz 7, 10587 Berlin (Link)

Directions: German, English

Organisation:
Frederik Armknecht, Universität Mannheim
Christopher Wolf, Ruhr-Universität Bochum
Jean-Pierre Seifert, Technische Universität Berlin (TUB) & Deutsche Telekom Laboratories

Contacts:
armknecht@uni-mannheim.de
Christopher.Wolf@ruhr-uni-bochum.de



Deutsche Telekom Laboratories, Ernst-Reuter-Platz, Be

Telekom Innovation Laboratories
Ernst-Reuter-Platz 7
D-10587 Berlin

Routenplaner Speichern

laboratories.telekom....

030 835358555

4,4 ★★★★★ 9 Berichte · Forschungszentrum

Foto hinzufügen

Änderung vorschlagen

Kurzinfo · Die Telekom Innovation Laboratories wurden 2004 als ze...

Street View
Fotos
Telekom Innovation Laboratories
Otto-Suhr-Allee
llee
Marchstraße
Ernst-Reuter-Platz
Ernst-Reuter-Platz
Ernst-Reuter-Platz
Ernst-Reuter-Platz
Ernst-Reuter-Platz
Brunnenanlage Ernst-Reuter-Platz
Bismarckstraße
Bismarckstraße
Bismarckstraße
TELES FMC+ C Innovations
Deutsche Bank Investment &...
Technische Universität Berlin...
TU Berlin Institut für Architektur FG...
Cafeteria TU Ernst-Reuter-Plat
Modell und Design
Ca
Allgemeiner Studentenausschuss...
Archit der
AYK Sonnenstudio
ortal
Daimler Center for Automotive...
Technische Universität Berlin Fachgebiet...
Aral Bismarckstraße
M&M:Trading
Swizöl Berlin Ralf Thiele GmbH...
K&M Computer Shop Berlin-Charlottenburg
enio
Polizeidirektion 2 - Abschnitt 25
Tele Columbus
Schweinske Charlottenburg
Kieser Training Berlin-Charlottenburg
bbw Akademie für Betriebswirtschaftliche...
Verband Druck und Medien NordOst eV
ule
Am
2
5
5
2
5
5
2
5

Day 1 – June 26, 2014 (Thursday)

12:45-13:25 Welcome Coffee

Talks Session 1	
13:25 – 13:30	**Welcome**
13:30 – 13:50	Ricardo Gomes da Silva (Technische Universität Berlin / Deutsche Telekom Innovation Laboratories & Universidade Federal do Rio Grande do Sul) **Practical Implementation of Higher-Order Instruction Skips in Micro-controllers**
13:50 – 14:10	Peter Günther (Universität Paderborn) **Breaking Pairing-Based Cryptography with Second-Order Instruction Skips**
14:10 – 14:30	Matthias Hamann, Vasily Mikhalev (Universität Mannheim) **Lightweight Authentication Protocols on Ultra-Constrained RFIDs – Myths and Facts**

14:30 - 14:50 Coffee Break

Talks Session 2	
14:50 – 15:10	Ágnes Kiss (Telekom Innovation Laboratories & EIT ICT Labs Master School) **Experimenting Differential Fault Analyses on CLEFIA**
15:10 – 15:30	Elena Kirshanova (Ruhr- Universität Bochum) **Learning with Errors Decoding**
15:30 – 15:50	Ernst G Giessmann (HU Berlin) **RSA-Schlusselerzeugung in OpenSSL - Haken und Ösen**

Demo Session 1	
15:50 – 16:30	Dr. Martin Kurze, T-Labs, Director Research & Innovation, Terminals & Cross-Domain middleware **Privacy before, during and after Cryptography – A Real Life Example showing the "Future of Mobile Privacy" using FirefoxOS**

18:00 WM Public Viewing

Day 2 – June 27, 2014 (Friday)

Demo Session 2	
9:00 – 9:40	Tim Kalmer und Christoph Prieschl (trust2core) **Secure Mobile Communication – How Governments protect their Communication against Governments**

9:40-10:00 Coffee Break

Talks Session 3	
10:00 – 10:20	Tim Waage (Universität Göttingen) **Secure Structures and Adaptable Encryption for Cloud Databases**
10:20 – 10:40	Angela Jäschke (Universität Mannheim) **Fully Homomorphic Encryption over Euclidean Rings**
10:40 – 11:00	Frank Quedenfeld (Ruhr- Universität Bochum) **Kryptoanalyse mit Hilfe ähnlicher Variablen**

11:00 - 11:20 Coffee Break

Talks Session 4	
11:20 – 11:40	Stefan Hoffmann (Ruhr - Universität Bochum) **An Asymptotic Analysis of Information Set Decoding for the McEliece Cryptosystem**
11:40 – 12:00	Christian A. Reuter (Universität Mannheim) **Auditing the Cloud: Proofs of Retrievability**
12:00 – 12:20	Pascal Sasdrich (Ruhr-Universität Bochum) **Efficient Elliptic-Curve Cryptography using Curve25519 on Reconfigurable Devices**

12:20 - 13:10 Lunch

Talks Session 5	
13:10 – 13:30	Tobias Fiebig (TU Berlin) **Teaching Crypto - How to Make Teenagers Curious**
13:30 – 13:50	Shahin Tajik (Technische Universität Berlin / Deutsche Telekom Innovation Laboratories) **Physical Characterization of Arbiter PUF**
13:50 – 14:10	Bastian Richter (Ruhr-Universität Bochum) **Side-Channel Attacks on the Yubikey 2 One-Time Password Generator**

Practical implementation of higher-order instruction skips in microcontrollers

Ricardo Gomes da Silva*,†

* Technische Universität Berlin
Deutsche Telekom Innovation Laboratories
Berlin
Germany

† Universidade Federal do Rio Grande do Sul
Instituto de Informática
Porto Alegre, RS
Brazil

Microcontrollers are extremely popular nowadays, being present in numerous devices and systems. They are designed to be embedded into small systems and interact with the environment, either directly through sensors and actuators, or through other digital systems. The most common example is *smart cards*, used for numerous scenarios, such as personal identification and access control. On such devices, the software limits the device's interaction with the outside world, such as limiting how much data can be obtained from it upon request. However, such devices assume that they have not been tampered with, neither that it was previously modified in a manner that the system behaves differently than original (*i.e.*the system behaves nominally).

Clock glitching attacks are one of the different types of hardware fault injections studied nowadays. By glitching the clock, it is possible to change the target's hardware behavior, either by corrupting or simply skipping CPU instructions. Since the software is not prepared to handle a device that has been tampered with, an attacker can exploit such vulnerability and take over the control flow of the program. Multiple attacks can then be performed, such as forcing the device to exiting loops [1] or dump its own memory [2].

This work applies clock glitching attacks against a family of embedded microcontrollers (AVR XMEGA from Atmel [3]) by implementing a modular glitcher environment based on an open-source security-focused platform (Die Datenkrake [4]). Such environment allows not only for fine-tuning of attacks, but also a brute-force algorithm for finding the glitching range to be implemented. By executing multiple repeatable experiments, both on handcrafted and compiled code, we demonstrate that such architecture is vulnerable against these attacks by introducing faults that were not expected and cannot be handled by the software. The implications of this regarding the security of the program are discussed in this work.

Literatur

[1] H. Bar-El, H. Choukri, D. Naccache, M. Tunstall, and C. Whelan, The Sorcerer's Apprentice Guide to Fault Attacks. In *Proceedings of the IEEE*, 2006.

[2] R. Anderson and M. Kuhn, Tamper resistance: a cautionary note. In *Proceedings of the 2nd USENIX Workshop on Electronic Commerce. USENIX*, 1996.

[3] Atmel AVR XMEGA Microcontroller Family Product Page, http://www.atmel.com/products/microcontrollers/avr/avr_xmega.aspx, accessed: 2014-06-03.

[4] Dmitry Nedospasov and Thorsten Schroder. Introducing Die Datenkrake: Programmable Logic for Hardware Security Analysis. In *7th USENIX Workshop on Offensive Technologies*, 2013.

Practical Fault Attacks against Pairing Based Cryptography

Peter Günther [1]

University of Paderborn

Cryptographic pairings map two arguments from an elliptic curve to a finite field and are linear in both arguments. A pairing is computed in two steps. In the first step, a rational function maps the two arguments from the elliptic curve to a finite field. This function is computed with the so-called Miller algorithm. In the second step, the result is raised to a fixed power, the final exponent. Today, numerous schemes such as hierarchical identity-based encryption, attribute based encryption, and identity based signatures make use of pairings as their building blocks [2].

In cryptography, fault attacks tamper with the computation of an algorithm to learn protected secret information. For example attacks modify the program execution or the internal memory and numerous techniques are used to induce faults, e.g., clock glitching, power glitching, and laser beams [1]. Even attacks that introduce two faults within one computation, so-called second-order attacks, have been performed.

In adversarial environments smart cards are often deployed to protect the secret. Because the computation of bilinear pairings on smart cards is already feasible [4], the vulnerability of pairings to fault attacks is relevant. Several theoretical results were published in this context [2]. All of these attacks use two faults: one fault to attack the Miller algorithm and one fault to attack the final exponentiation. Because none of those theoretical approaches has been evaluated in practice to date, it is not clear that second-order faults can really be applied to the complex pairing computation.

In this talk, we will see that it is indeed possible to perform second-order attacks against practical pairing implementations. We will use clock glitches to induce two faults in the pairing computation on an AVR XMEGA A1. To physically realize our faults, we use the DDK [3], a security-focused, low-cost, open source development platform which consists of an FPGA and an ARM CPU. The faults do not directly lead to the secret and require some algebraic post-processing. Hence, we will also explain how the faults can be analyzed with Sage, an open source computer algebra system. Together, this shows that it is possible to perform fault attacks on pairing based cryptography with low-cost tools.

References

[1] H. Bar-El, H. Choukri, D. Naccache, Michael Tunstall, and C. Whelan. The Sorcerer's Apprentice Guide to Fault Attacks. *Proceedings of the IEEE*, 94(2):370–382, Feb 2006.

[2] Marc Joye and Gregory Neven, editors. *Identity-Based Cryptography*, volume 2 of *Cryptology and Information Security*. IOS Press, 2009.

[3] Dmitry Nedospasov and Thorsten Schroder. Introducing Die Datenkrake: Programmable Logic for Hardware Security Analysis. In *7th USENIX Workshop on Offensive Technologies*, 2013.

[4] Michael Scott, Neil Costigan, and Wesam Abdulwahab. Implementing Cryptographic Pairings on Smartcards. In Louis Goubin and Mitsuru Matsui, editors, *CHES*, volume 4249 of *Lecture Notes in Computer Science*, page 134147. Springer, 2006.

[1] This talk is about joint work with Johannes Blömer, Ricardo Gomes da Silva, Juliane Krämer, and Jean-Pierre Seifert.

Lightweight Authentication Protocols on Ultra-Constrained RFIDs - Myths and Facts
(to appear at RFIDSec 2014)

Frederik Armknecht, Matthias Hamann, Vasily Mikhalev

University of Mannheim
Mannheim, Germany

For economical reasons low-cost RFID tags (e.g., in the production cost range of \$0.05 to \$0.10) are particularly interesting for industry. This cost pressure directly translates into severe hardware restrictions for the targeted devices. Consequently, the search for appropriate lightweight authentication protocols has become an important topic in cryptography during the last years with high relevance for academia and industry. While there is quite a good understanding with respect to the *security* of most of these schemes, often only very little is known about their *applicability* for real-world systems. One main reason is the apparent lack of commonly accepted criteria for a scheme to be considered as lightweight. Of course one might argue that developments in technologies continuously enable *more possibilities* at the *same price.* However, experience shows that for economic reasons advances in technology are rather used for developing hardware that possesses about the *same capabilities* as existing devices but at a *lower price.* In this work, we concentrate on authentication protocols between an RFID reader and ultra-constrained tags. More precisely, we target devices in the cost range of \$0.05 to \$0.10. The reasons for this specific choice are twofold: Firstly, RFID tags which can be produced at costs of \$0.1 or cheaper, like (variants of) *Electronic Product Codes* (EPCs), have been a common motivation for existing work. Secondly, if one allows for only few additional costs, standard cryptographic primitives like AES become in fact feasible, thus practically removing the need for alternative solutions altogether. Our contributions are:

Set of Conditions. Our first contribution is that we specify and argue several conditions that need to be satisfied by authentication protocols to be suitable for ultra-constrained RFID devices. These conditions have been derived partly from open literature but most importantly from various discussions with experts from industry. Although these experts were working for different companies and were aiming for RFID-based authentication in different areas, all of them share more or less the same view on what “lightweight” means in the context of ultra-constrained devices and when a scheme can be considered to be relevant for real-word applications. As these conditions mostly result from long lasting experience in hardware production and have not (or only partly) been comprehensively described and summarized in open literature, we think that this information will be very helpful for assessing the suitability of existing protocols and for providing guidance in the development of new ones.

Evaluation of LPN-based Protocols. Our second contribution is the application of the gained knowledge for evaluating the suitability of *LPN-based protocols.* This branch of research represents the most prominent non-proprietary approach for designing lightweight authentication protocols. It has been initiated by HB and HB$^+$, which became the prototypes for a whole family of protocols that base their security on the hardness of the learning parity in the presence of noise (LPN) assumption (or variant problems). To this end, we extracted concrete parameter choices for almost 20 proposals in this work and verified whether these comply to the derived set of conditions. As it turned out, none of the existing LPN-based protocols meet the requirements, i.e., none of them can actually run on current low-cost RFID hardware.

Experimenting Differential Fault Analyses on CLEFIA

Ágnes Kiss*,†

*,† Telekom Innovation Laboratories,
EIT ICT Labs Master School
Berlin
Germany

Differential Fault Analysis is a cryptographic attack method that exploits computational errors in order to reveal the secret key of a cryptosystem. To mount such an attack, the adversary induces faults into one or more steps of the computations. Afterwards she computes the difference between the correct and faulty results, thus gaining additional information about the secret key.

CLEFIA is a 128-bit block cipher proposed by Sony Corporation in 2007 [S07] with three supported key lengths, 128, 192 and 256 bits. CLEFIA uses the four-branch generalized Feistel structure, using four 32-bit data lines through the encryption and decryption process.

Since its appearance, several Differential Fault Analysis methods were proposed on CLEFIA for all available key lengths. In chronological order they are [CWF07, TF10, ZWG10, AM13] and to the best of our knowledge, these are all published Differential Fault Analyses on CLEFIA to date. The attacks differ in their fault models, in the number of faults injected and in the analysis algorithm that used to reveal the secret key.

I implemented these methods in C and made observations based on my experimental results on these Differential Fault Analysis techniques. The focus of my research was on examining the probability of success with the minimal amount of faults for all the attacks. Due to an observation on the attack using the least fault number against CLEFIA with longer keys [AM13], I could improve on its probability for success by mixing the original technique with an other method [TF10]. This new improved method uses the same amount of faults and succeeded in 8% more of the cases than the original one in case of 2,000 random experiments.

References

[AM13] S. Ali and D. Mukhopadhyay, Improved Differential Fault Analysis of CLEFIA, in *2013 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, W. Fischer and J.-M. Schmidt, Eds., 2013, pp. 60–70.

[CWF07] H. Chen, W. Wu, and D. Feng. *Differential Fault Analysis on CLEFIA*, in ICICS, ser. Lecture Notes in Computer Science, S. Qing, H. Imai, and G. Wang, Eds., vol. 4861. Springer Berlin Heidelberg, 2007, pp. 284–295.

[S07] T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata, The 128-Bit Blockcipher CLEFIA (Extended Abstract) in *FSE*, ser. Lecture Notes in Computer Science, A. Biryukov, Ed., vol. 4593. Springer Berlin Heidelberg, 2007, pp. 181–195.

[TF10] J. Takahashi and T. Fukunaga. Differential Fault Analysis on CLEFIA with 128, 192, and 256-Bit Keys, *IEICE Transactions*, vol. 93-A, no. 1, pp. 136–143, 2010.

[ZWG10] X.-j. Zhao, T. Wang, and J. zhe Gao. Multiple Bytes Differential Fault Analysis on CLEFIA, *IACR Cryptology ePrint Archive*, vol. 2010, p. 78, 2010.

Learning with Errors Decoding

Leif Gottschling Elena Kirshanova Alexander May

Horst Görtz Institute for IT-Security
Faculty of Mathematics
Ruhr University Bochum, Germany
elena.kirshanova@rub.de

The security of most public-key encryption schemes relies on the hardness of the *learning with errors* (LWE) problem – an average-case hard lattice problem introduced by Regev ([Reg05]). While LWE has been proved to be as hard as quantumly approximating the so-called *Short Independent Vectors Problem*, the parameters used in the proof are not suitable for practical reasons. It makes difficult to assess the security of the proposed lattice-based schemes and there has been a number of attempts to address this issue ([MR09], [RS10]). In the work of Lindner and Peikert ([LP11]), the authors analyze the concrete hardness of LWE instances applying their bounded-distance decoding (with a lattice basis reduction as a preprocessing step), tailored for the structure of LWE.

Concretely, the Lindner-Peikert decoding algorithm can be viewed as the generalization of the Babai's `NearestPlane` algorithm [Bab85]. The goal of all decoding algorithms is to find the closest lattice point to a given point in space. In a nutshell, the Babai's algorithm projects this given point to a closest hyperplane of a lattice, chooses the closest lattice point to the projection and repeats the same procedure for the hyperplane and the lattice point, thus reducing the dimension by one. In [LP11], instead of iteratively projecting on *one* closest plane, we project on *several* close planes. Geometrically, the new algorithm extends the search space giving us the control over the approximation factor of the resulting output. This results in a parallelepiped-shaped search space, and we consider all lattice point that lie inside this parallelepiped as possible solutions. The main difference we propose is to transfer this parallelepiped into an ellipsoid, thus taking into an account the Gaussian nature of the LWE error and, at the same time, cutting some vectors that are unlikely the solution. We also provide the asymptotic analysis for our algorithm and compare it with the `NearestPlanes` algorithm of [LP11].

LWE decoding problem. The search-LWE problem asks to find a secret vector $\mathbf{s}$ given polynomially many 'noisy' samples of the form $(\mathbf{A}, \mathbf{t} = \mathbf{A}^t\mathbf{s} + \mathbf{e} \bmod q) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}^m$, where n is the security parameter, $q = poly(n), m = \Omega(n)$ and $\mathbf{e}$ is a relatively short noise-vector. The problem is an average-case Bounded Distance Decoding problem for a so-called q-ary lattice $\Lambda(\mathbf{A}^t) = \{\mathbf{z} \in \mathbb{Z}^m : \exists \mathbf{s} \in \mathbb{Z}_q^n \text{ s.t. } \mathbf{z} = \mathbf{A}^t\mathbf{s} \mod q\}$.

Our results. The first main result of our work is the asymptotic analysis of the Lindner-Peikert `NearestPlanes` algorithm, which turned out to be slightly sub-exponential in the lattice dimension m. We analyze the algorithm under a specific choice of parameters with a polynomial number of samples.

Our second contribution is a new `EllipticNearestPlanes` algorithm. As the name suggests, we use an ellipsoid-shaped search space to look for a candidate solution. Asymptotic analysis shows that it outperforms the Lindner-Peikert decoding attack. We also provide the complexity estimates for concrete LWE instances, which agree with our theoretical results.

References

[Bab85] László Babai. On Lovász' lattice reduction and the nearest lattice point problem (shortened version). In *STACS*, pages 13–20, 1985. (Cited on page 1.)

[LP11] Richard Lindner and Chris Peikert. Better key sizes (and attacks) for lwe-based encryption. In *CT-RSA'11*, pages 319–339, 2011. (Cited on page 1.)

[MR09] Daniele Micciancio and Oded Regev. Lattice-based cryptography. In *Post Quantum Cryptography*, pages 147–191. Springer, 2009. (Cited on page 1.)

[Reg05] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In *STOC*, pages 84–93. ACM Press, 2005. (Cited on page 1.)

[RS10] Markus Rückert and Michael Schneider. Esimating the security of lattice-based cryptosystems. *Cryptology ePrint Archive, Report 2010/137*, 2010. URL: `https://eprint.iacr.org`. (Cited on page 1.)

RSA-Schlüsselerzeugung in OpenSSL - Haken und Ösen

Ernst G Giessmann*
*Institut für Informatik
Humboldt-Universität zu Berlin
D-10099 Berlin

Die Erzeugung von RSA-Schlüsseln gehört zu den oft genutzen Routinen in OpenSSL. Falls nichts anderes angegeben wird, ist RSA mit 512 Bit und dem Exponenten 65537 der Standardalgorithmus, der bei einer Schlüsselerzeugung von OpenSSL bis zur Version 1.0.0 verwendet wird. Diese Routine ist in ihren Grundzügen seit Jahren nicht mehr verändert worden, von wenigen Anpassungen im Zusammenhang mit dem `genpkey`-Kommando einmal abgesehen.

Bei jedem `genrsa`-Kommando erkennt man leicht in der Anzeige der sich wiederholenden Symbole die Suche nach den beiden Primzahlen (Punkte) und die Miller-Rabin-Tests (Pluszeichen), die je nach Schlüssellänge unterschiedlich oft wiederholt werden. Es kann übrigens sogar auch ein Stern nach den Pluszeichen auftreten.

Dahinter verbergen sich folgende Schritte

1. Erzeugung eines zufälligen Startwerts
2. Pseudoprimzahl-Suche
3. Miller-Rabin-Tests
4. Wiederholung der Suche für die zweite Primzahl
5. Erzeugung der Schlüsselparameter

Obwohl das alles bekannt aussieht, entdeckt man doch einige unerwartete Details in den zugehörigen Prozeduren. Im Vortrag beantworten wir die folgenden Fragen.

Wie zufällig sind die erzeugten Primzahlen?
Wie sicher ist es eigentlich, dass es Primzahlen sind?
Sind die Primzahlen, die OpenSSL findet, gleichverteilt?
Welche öffentlichen Exponenten verwendet OpenSSL?
Wie lange dauert die Schlüsselerzeugung?

Wir interessieren uns aber auch für einige exotische Dinge, nach denen normalerweise niemand zu fragen sich traut:

Sind Entschlüsselungs- und Signaturschlüssel gleich?
Was ist die kürzeste RSA-Schlüssellänge und welches die längste?
Wie groß ist der größte Exponent?
Woraus besteht ein RSA-Schlüssel?
Kann man sich auf die Schlüsselprüfung verlassen?
Und wann kommt eigentlich der Stern?

Secure Structures and Adaptable Encryption for Cloud Databases

Tim Waage*, Lena Wiese*

*University of Göttingen, Institute of Computer Science
Knowledge Engineering Group

There are many strong encryption algorithms that provably provide privacy of sensitive data, but another requirement is a sufficient level of efficiency in data processing. Thus data protection and usability are two *competitive* demands. Ideally pre-processing on encrypted data should be possible in order to avoid a complete decryption, processing and then re-encryption. For applications regarding databases three methods are advisable: *searchable encryption* [Tang12], *order preserving* encryption [Xiao12] as well as *homomorphic* encryption [Gentry09].

The main objective of our work is to acquire the ability to save data in cloud databases in an encrypted form. At the same time all technical mechanisms of those databases should remain untouched, which means the database systems are supposed to keep working without any changes. Ideally only one step of encryption should be done before accessing the database and only one step of decryption should be processed on the database servers answers.

Therefore a client software runs on the users computer providing a variety of security features, most important adaptable encryption. That allows the user to determine which parts of the dataset are to be encrypted. Furthermore an appropriate key management is provided for access control.

There are a couple of proprietary as well as open source database implementations, that are used in different scenarios, e.g. cloudstorage databases, but none of the existent implementations supports any kind of encrypted storage. However, for a wider acceptance of cloud storage, data is supposed to be protected from attacks of so called honest-but-curious cloud storage providers as well as from attacks of malicious third parties.

In order to achieve that there are very few approaches like CryptDB [Popa12] for traditional SQL databases, but a variety of datamodels and -systems has been developed recently that differ from the relational view on data. One category we focus on are so called column family stores, inspired by Googles Big Table [Chang06] system. Examples for other systems, available as open source software and thus available for further development within this work, are Cassandra, HBase, Accumulo and Hypertable. RDF triple stores are taken into account as well.

Acknowledgement: We acknowledge funding by the DFG (grant number: WI 4086/2-1).

References

[Chang06] Chang, Fay, et al. “Bigtable: A distributed storage system for structured data.” *ACM Transactions on Computer Systems (TOCS) 26.2* (2008): 4.

[Tang12] Tang, Qiang. “Search in Encrypted Data: Theoretical Models and Practical Applications.” *ACR Cryptology ePrint Archive* 2012 (2012): 648.

[Xiao12] Xiao, Liangliang, and I-Ling Yen. “Security analysis for order preserving encryption schemes.” *Information Sciences and Systems (CISS)*, 2012 46th Annual Conference on. IEEE, 2012.

[Popa12] Popa, Raluca Ada, et al. “CryptDB: Processing queries on an encrypted database.” *Communications of the ACM* 55.9 (2012): 103-111.

[Gentry09] Gentry, Craig. *A fully homomorphic encryption scheme.* Diss. Stanford University, 2009.

Fully Homomorphic Encryption over Euclidean Rings

Angela Jäschke and Frederik Armknecht

University of Mannheim
Mannheim
Germany

In 2009, Gentry solved the problem of fully homomorphic encryption, i.e. encryption schemes that allow unlimited addidtions and multiplications on encrypted data [Gen09]. Other schemes soon followed, among them [DGHV10], which presents a scheme using only integer addition and multiplication and has $\{0, 1\}$ as the message space. After quickly reviewing this scheme, we present a generalization to Euclidean Rings in general, which allows us much bigger freedom in choosing plaintext spaces tailored to a specific scenario. We show correctness of this general scheme and derive a security result from [AKP10], which relates IND-CPA security to a subgroup membership problem, which will also be explained.

We then see how the original scheme [DGHV10] is a special case of our general scheme, and that with our simpler approach to security analysis, we arrive at the same hard problem as the authors do with a rather complicated method. We then present a new somewhat homomorphic instantiation of the general scheme which works over binary polynomials and has a plaintext space of $\mathbb{F}_{2^n}$ where n can be freely chosen, and explain why we believe this scheme could be beneficial for certain applications.

References

[Gen09] Craig Gentry. A fully homomorphic encryption scheme Dissertation at Stanford University, 2009

[DGHV10] Marten van Dijk, Craig Gentry, Shai Halevi and Vinod Vaikuntanathan. Fully Homomorphic Encryption over the Integers. *EUROCRYPT*, 2010.

[AKP10] Frederik Armknecht, Stefan Katzenbeisser and Andreas Peter. Group Homomorphic Encryption: Characterizations, Impossibility Results, and Applications. *DCC*, 2011.

[GHS12] Craig Gentry, Shai Halevi and Nigel P. Smart. Homomorphic Evaluation of the AES Circuit. *CRYPTO*, 2012.

Kryptoanalyse mit Hilfe ähnlicher Variablen

Frank Quedenfeld and Christopher Wolf

Ruhr-Universität Bochum

Zusammenfassung

Wir stellen eine neue algebraische Repräsentation von Trivium vor. Diese erlaubt es uns mehrere Instanzen zur gleichen Zeit zu betrachten. Darüber hinaus nutzen wir Methoden aus der linearen Algebra um die Anzahl der Zwischenvariablen zu reduzieren. So erhalten wir ein quadratisches Gleichungssystem um den gemeinsamen Schlüssel der Triviuminstanzen, die mit verschiedenen unterschiedlichen öffentlichen Werten generiert werden, zu beschreiben. Ein solches Gleichungssystem mit $15k$ Variablen und 10^6 Monomen zu lösen ist eine groe Herausforderung. Aus diesem Grund stellen wir die Methoden vor mit denen wir ein solches Gleichungssystem lösen können. Damit brechen wir eine auf 625 Runden reduzierte Variante von Trivium in $2^{42.3}$ und einer Datenkomplexität von 2^{12}.

Stromchiffren werden verwendet, um schnelle und sichere Verbindungen zu garantieren. Heutzutage ist das zum Beispiel bei mobiler Kommunikation von groer Bedeutung. Dabei sind die Stromchiffren des eSTREAM Projekts [oE08] heutiger Standard und werden regelmäig auf ihre Sicherheit hin getestet. Das in [CDC08] beschriebene Trivium werden wir betrachten.

Trivium ist eine hardware-orientierte synchrone Stromchiffre, die bis zu 2^{64} langen Schlüsselstrom von einem 80-bit langen geheimen Schlüssel und einem 80-bit langen öffentlichen Wert produziert. Dabei werden drei Schieberegister $A = [A_i, \dots, A_{i-92}], B = [B_i, \dots, B_{i-83}]$ und $C = [C_i, \dots, C_{i-110}]$ mit nichtlinearer Aktualisierungsfunktion genutzt und Ausgabe erst nach einer Anzahl von Initialisierungsrunden R gegeben. Volles Trivium benutzt $R = 1152$.

Die einfache Gestalt macht Trivium zu einem beliebten Ziel für Kryptanalysten. Bis heute ist Trivium jedoch ungebrochen.

Vorherige algebraische Angriffe hatten bisher gar keinen Erfolg. Das lag vor allem daran, dass nur eine Instanz betrachtet wurde. Wir werden eine andere algebraische Repräsentation vorstellen, die es uns erlaubt mehrere Instanzen mit dem selben Schlüssel, aber anderen öffentlichen Wert zu betrachten. Damit stellen wir ein groes Gleichungssystem auf, dass weit auerhalb der Reichweite von Groebnerbasentechniken ist. Daher stellen wir einen Solver, der mit solchen Gleichungssystemen umgehen kann.

Literatur

[CDC08] B. Prenel C. De Cannire. Trivium. In *New Stream Cipher Designs*, volume 4986 of *LNCS*, pages 84–97. Springer, 2008.

[oE08] ECRYPT Network of Excellence. The estream project, 2008. http://www.ecrypt.eu.org/stream/.

An Asymptotic Analysis of Information Set Decoding for the McEliece Cryptosystem

Stefan Hoffmann and Alexander May

Horst Görtz Institute for IT-Security
Ruhr-University Bochum

McEliece is one of the promising candidates for post-quantum encryption and it already underwent a decent amount of cryptanalytic attacks. The best known attack on McEliece regards the underlying Goppa code as a random linear code and applies Information Set Decoding (ISD). It is crucial to study ISD algorithms and how they behave on McEliece instances.

Random linear codes of constant rate $\frac{k}{n}$ admit a constant relative distance $\frac{d}{n}$. In contrast, the Goppa codes in McEliece of constant rate admit a relative distance of $\mathcal{O}(\frac{1}{\log n})$. Recent algorithmic improvements for decoding random linear codes use sophisticated enumeration techniques for error vectors with weight of error correction capability $\omega = \lfloor \frac{d-1}{2} \rfloor$. Thus, it remains unclear whether these techniques yield similar good results for Goppa codes.

In 1962, Prange [Pr62] published the original ISD algorithm that achieves worst-case complexity $2^{0.057n}$, where the worst-case is taken over all choices of k. Stern's algorithm [St89] from 1989 uses a classical Meet-in-the-Middle technique to improve the complexity to $2^{0.055n}$. Using techniques recently developed for the subset sum technique [HGJ10], eventually Becker, Joux, May, Meurer [BJMM12] were able to bring down the running time to $2^{0.049n}$.

Prange's algorithm admits for Goppa code parameters asymptotic complexity $2^{0.531\frac{n}{\log n}}$ [Pe11]. However, none of the other ISD variants has been studied in an asymptotic Goppa code setting in the literature. Such a study is crucial for a solid comparison of those algorithms that determine a secure parameter selection process for the McEliece cryptosystem.

We adapt the newer ISD algorithms to the case of Goppa codes, and analyze their complexity in an asymptotic setting. As a somewhat surprising result, we show that for rates $\frac{k}{n} < 0.87$ all recent optimizations of Information Set Decoding achieve their optimal complexity for a parameter setting that lets them collapse to the original Prange algorithm. Only for higher rates, the new algorithms can show their strength in improving the decoding complexity for Goppa codes.

References

[Pr62] Prange, Eugene. The Use of Information Sets in Decoding Cyclic Codes. *Information Theory, IRE Transactions on*, September 1962.

[St89] Stern, Jacques. A Method for Finding Codewords of Small Weight. *Coding Theory and Applications*, 1989.

[HGJ10] Howgrave-Graham, Nick and Joux, Antoine. New Generic Algorithms for Hard Knapsacks. *Advances in Cryptology EUROCRYPT 2010.*

[BJMM12] Becker, Anja and Joux, Antoine and May, Alexander and Meurer, Alexander. Decoding Random Binary Linear Codes in $2^{n/20}$: How $1 + 1 = 0$ Improves Information Set Decoding. *Advances in Cryptology EUROCRYPT 2012.*

[Pe11] Peters, Christiane. Curves, Codes, and Cryptography. 2011.

Auditing the Cloud: Proofs of Retrievability

Christian A. Reuter and Frederik Armknecht
University of Mannheim
68131 Mannheim, Germany
reuter@uni-mannheim.de, armknecht@uni-mannheim.de

Nowadays many companies, organizations and private users generate huge quantities of electronic data. While the costs for storage devices such as hard drives are very low, storing the data locally isn't the best thing to do. One reason may be the availability and reliability of the data. If the data should be available anywhere, a simple hard drive isn't enough, instead a well secured server infrastructure is needed. Furthermore, one wants to have replicated copies of the stored data in case of hardware failure, software bugs or inadvertent deletion of data. To overcome theses problems, the data is stored remotely in the "Cloud". Cloud computing in general offers its users a large amount of storage and computing resources on demand. The large-scale data centers take a lot of managing away from the users and therefore especially the financial benefits of the cloud become clear. This allows data access from nearly everywhere in the world and at the same time an assigned storage provider takes care of storing the data itself.

On the other hand, many users and companies don't trust the cloud and fear the security and operational risks. Server misconfigurations, power outages, hardware fails or even insider threats menace the availability and reliability of the stored data. The open question is: If remotely stored data is accessed rarely, how can the owner be sure that its data is stored correctly? The service provider may lose the data and won't notice its clients, hoping they will not find out. Additionally, the provider may be malicious, deleting data to save storage space.

To survey its stored data, the user may download it completely and check if it is not corrupted. Obviously, this is very inefficient for large files. To audit the remotely stored data more efficient and also provably secure, Juels and Kaliski introduced *Proofs of Retrievability* (PoR) in [JK]. A PoR is a protocol, where a user stores its data on a server and keeps locally only a very short verification string. After storing the file, the user audits the storage provider who proves the availability of the data which can be extracted and retrieved by the user later on.

We are interested in efficient schemes with low communication and computational overhead. In [SW], Shacham and Waters present compact PoR which are efficient and provably secure. They use homomorphic properties to aggregate data and their adversary model is based on the one from Juels and Kaliski. As another advantage of their scheme, the user is able to do an unbound number of verification checks.

In this talk, we explain how to build PoR and present a detailled view on the PoR scheme of Shacham and Waters. Furthermore, we compare it to other existing PoR schemes and discuss open questions regarding the extensibility and instantiation of PoR.

References

[JK] Ari Juels and Burton S. Kaliski. PORs: Proofs of Retrievability for Large Files. In: S. De Capitani di Vimercati and P. Syverson (eds.), *Proceedings of CCS 2007*, pp. 584-597. ACM Press (2007).

[SW] Hovav Shacham and Brent Waters. Compact Proofs of Retrievability. In: J. Pieprzyk (ed.) *ASIACRYPT 2008*. LNCS, vol. 5350, pp. 99–107. Springer, Heidelberg (2008).

Efficient Elliptic-Curve Cryptography using Curve25519 on Reconfigurable Devices

Pascal Sasdrich

Horst Görtz Institute for IT-Security
Ruhr-Universität Bochum
Bochum, Germany

Elliptic curve cryptography (ECC) has become the predominant asymmetric cryptosystem found in most devices during the last years. Despite significant progress in efficient implementations, computations over standardized elliptic curves still come with enormous complexity, in particular when implemented on small, embedded devices. In this context, Bernstein proposed the highly efficient ECC instance Curve25519 that was shown to achieve new ECC speed records in software providing a high security level comparable to AES with 128-bit key. These very tempting results from the software domain have led to adoption of Curve25519 by several security-related applications, such as the NaCl cryptographic library or in anonymous routing networks (nTor). In this work we demonstrate that even better efficiency of Curve25519 can be realized on reconfigurable hardware, in particular by employing their Digital Signal Processor blocks (DSP). In a first proposal, we present a DSP-based single-core architecture that provides high-performance despite moderate resource requirements. As a second proposal, we show that an extended architecture with dedicated inverter stage can achieve a performance of more than 32,000 point multiplications per second on a (small) Xilinx Zynq 7020 FPGA. This clearly outperforms speed results of any software-based and most hardware-based implementations known so far, making our design suitable for cheap deployment in many future security applications.

Teaching Crypto
How to make Teenagers Curious

Tobias Fiebig[†]

[†] Technische Universität Berlin
Ernst-Reuter Platz 7
D-10587 Berlin

Understanding how cryptography end (en)coding theory work is not necessarily a hard task. For someone who has a little bit of curiosity for how things work, the path is rather straight forward. One starts with the basic algorithms, which have long since been abandoned. Skytale, Ceasar, Railfence and so forth. There after one starts with Vigenère, Affine and Playfair. Suddenly the ciphers can not be broken with simple pen and paper guessing techniques and the first pieces of math have to be understood. When the journey then reaches Enigma and the Lorenz Machine one slowly crosses the bridge to really modern, computerized cryptography. From then on it is only a small step to RC4, DES and MD4. Ultimately one is surrounded by AES, RSA, DSA, SHAs of all sorts and so forth. And while these abbreviations may sound cryptic to most, one realizes: "I am a cryptographer."

However, this leads to the question why not more young people pick up studies in this field, if only some curiosity is necessary to start the whole endeavor. The reason is most certainly that the first steps seem rather boring from the outside. Shuffling around and counting letters with pen and paper seems more like the cross-word puzzles one's grandparents do, than the thrilling experience James Bond's Q had, when he breaks a villain's cipher. So to start up the curiosity in young people aiming at starting their academic career we have to provide them with something that requires the skills of the first, but the thrilling experience of the second.

In this talk we will introduce a small one-week block-course for students in their last year of school, aimed at providing that thrilling experience. Although they should feel like Q, performing cryptoanalysis on a real-world implementation, it should still cater to their yet developing skill-set. To this end we decided to build a course around the reverse engineering of FlickerTAN [Re14], a widely adapted home-banking security mechanism. Although it's functionality is already known in the field [CCC14], it should be sufficiently unknown to the target group. During the projects the pupils have to first investigate the optical transmission methods used to get the plain-text into the reader. Then they will cover length of encoding and hashing to figure out what the actual debit card does, while it is in the reader. In the end they should have gathered a basic understanding of the related concepts and found the little spark of curiosity to start their academic career in the field of cryptography.

References

[CCC14] Chaos Computer Club Frankfurt a.M. Vom Überweisungsauftrag zur TAN *Website, Accessed*, 2nd of June 2014 `https://wiki.ccc-ffm.de/projekte:tangenerator:start#ableitung_der_tan`

[Re14] REINER SCT Producte: Tan Generatoren *Website, Accessed*, 2nd of June 2014 `https://wiki.ccc-ffm.de/projekte:tangenerator:start#ableitung_der_tan`

Physical Characterization of Arbiter PUFs

Shahin Tajik[1], Enrico Dietz[2], Sven Frohmann[2], Jean-Pierre Seifert[1], Dmitry Nedospasov[1],
Clemens Helfmeier[3], Christian Boit[3], Helmar Dittrich[2]

[1] Security in Telecommunications
Technische Universitt Berlin
Germany

[2] Optical Technologies
Technische Universitt Berlin
Germany

[3] Semiconductor Devices
Technische Universitt Berlin
Germany

As intended by its name, Physically Unclonable Functions (PUFs) [1] are considered as an ultimate solution to deal with insecure storage, hardware counterfeiting, and many other security problems. However, many different successful attacks have already revealed vulnerabilities of certain digital intrinsic PUFs. Although settling-state-based PUFs, such as SRAM PUFs, can be physically cloned by semi-invasive and fully-invasive attacks, successful attacks on timing-based PUFs [2, 3] were so far limited to modeling attacks. Such modeling requires a large subset of challenge-response-pairs (CRP) to successfully model the targeted PUF. In order to provide a final security answer, this paper proves that all arbiter-based (i.e. controlled and XOR-enhanced) PUFs can be completely and linearly characterized by means of photonic emission analysis. Our experimental setup is capable of measuring *every* PUF-internal delay with a precision of 6 picoseconds. Due to this precision we indeed require only the theoretical minimum number of linear independent equations (i.e. physical measurements) to directly solve the underlying inhomogeneous linear system. Moreover, we neither require to know the actual PUF challenges nor the corresponding PUF responses for our physical delay extraction. On top of that devastating result, we are also able to further simplify our setup for easier physical measurement handling. We present our practical results for a real arbiter PUF implementation on a Complex Programmable Logic Device (CPLD) from Altera manufactured in a 180 nanometer process.

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] 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. Symposium on VLSI Circuits, 2004. Digest of Technical Papers, 2004.

[3] 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 conference on Computer and communications security, 2010.

Side-Channel Attacks on the Yubikey 2 One-Time Password Generator

Bastian Richter, David Oswald and Christof Paar

Horst Görtz Institute
Ruhr University Bochum, Germany

Since online services are more and more at risk, e.g., due to phishing and malware, classical authentication schemes like username and password need to be strengthened by an additional factor. For this, hardware tokens that generate One-Time Passwords (OTPs) can be used. These tokens are common in high-security commercial applications, but still not for private use, often because of the high price and the need for additional infrastructure.

The security of an OTP system not only depends on the security of the server backend and the protocols, but also on the security of the token itself. Therefore, an analysis of the hardware is needed. One (in practice often occurring) flaw is the susceptibility towards implementation attacks, especially Side-Channel Analysis (SCA). SCA utilizes information leaked through physical channels not intended by the developer, for example, power consumption or electro-magnetic (EM) emanation.

The OTP token tested in this work is the Yubikey 2 Standard [Yub] produced by Yubico Inc. It differs from most OTP tokens with a focus on simplicity and an open-source software backend. However, the question arises if high-security requirements can be fulfilled by such a low-cost device.

The Yubikey appears as a normal USB keyboard to the user's computer to enable direct input of the OTP. When the user presses the button on top of the Yubikey, it generates a proprietary OTP and enters it via the simulated keyboard. The user gives the focus to an additional input field on the login form an then presses the Yubikey's button. The generated OTP consists of counters, counting the power-ups of the device and the generated OTPs after power-up. Additionally, the OTP contains a 6-byte secret ID and a timer iterating at approx. 8 Hz. At the end, a CRC checksum is appended and the whole data encrypted with the AES algorithm. This ensures that a unique OTP is generated each time.

We present a power as well as an EM side-channel attack on the Yubikey 2. The attacks enable the attacker to extract the secret AES key used by the Yubikey. With this knowledge, the attacker is able to clone the device by generating the OTPs in software using the extracted key without keeping the Yubikey. Due to the short measurement time of approx. 1 hour for the EM analysis, the whole attack can be performed in a lunch break to stay undiscovered. Detailed information can be found in [RAID13].

References

[Yub] Yubico Inc., Yubikey Standard, http://www.yubico.com/products/yubikey-hardware/yubikey/

[RAID13] David Oswald, Bastian Richter and Christof Paar, Side-Channel Attacks on the Yubikey 2 One-Time Password Generator, Research in Attacks, Intrusions, and Defenses, 2013.