21st Crypto-Day

Wincor Nixdorf International GmbH

January 22 and 23, 2015

Paderborn, Germany

On January 22&23 2015, the interest group “Angewandte Kryptographie” of Gesellschaft für Informatik e. V. will host the twenty-first *Crypto-Day*.

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

Host: The Wincor Nixdorf International GmbH will host the event and provide an insight into product security aspects and ongoing industry research. Moreover, a guided tour in the Heinz Nixdorf Museumsforum, being the world’s largest computer museum, is planned.

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**.

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

Organisation: Frederik Armknecht, Universität Mannheim
Volker Krummel, Wincor Nixdorf International GmbH

Contacts: armknecht@uni-mannheim.de

Day 1 – January 22, 2015 (Thursday)

13:30-13:55 Welcome Coffee

Talks Session 1	
13:55 – 14:00	**Welcome**
14:00 – 14:20	Wincor Nixdorf **Research & Innovation @ Wincor Nixdorf**
14:20 – 14:40	Peter Günther (Universität Paderborn, Germany) **Securing the Financial Cloud**
14:40 – 15:00	Gennadij Liske (Universität Paderborn, Germany) **Constructing CCA-Secure Predicate Key Encapsulation Mechanisms from CPA-Secure Schemes and Universal One-way Hash Functions**
15:00-15:20	Nikolas Karvelas (TU Darmstadt, Germany) **ORAM challenges in a fully sequenced DNA world**

15:20 - 15:50 Coffee Break

Talks Session 2	
15:50 – 16:10	Christian Janson (Royal Holloway, UK) **Revocation in Publicly Verifiable Outsourced Computation**
16:10 – 16:30	Christian Reuter (Universität Mannheim) **Outsourced Proofs of Retrievability**
16:30 – 16:50	Jakob Juhnke (Universität Paderborn, Germany) **Anonymous and Publicly Linkable Reputation Systems**

Visit of the Heinz Nixdorf MuseumsForum (HNF)	
17:00 – 17:30	Walk to the HNF
17:30 – 18:30	Guided tour in the HNF in English

19:30- Dinner and Get Together

Day 2 – January 23, 2015 (Friday)

Talks Session 3	
9:30 – 9:50	Wincor Nixdorf **Secure Reality - Real Security**
9:50 – 10:10	Georg Becker (Ruhr-Universität Bochum, Germany) **An Efficient Machine Learning Attack on the Slender PUF Protocol**
10:10 – 10:30	André Schaller (TU Darmstadt, Germany) **RSA with SRAM-based PUFs Found on Commodity Hardware**

10:30 - 10:50 Coffee Break

Talks Session 4	
10:50 – 11:10	Thorsten Kranz (Ruhr-Universität Bochum, Germany) **Cryptanalysis of the ASASA Structure**
11:10 – 11:30	Vasily Mikhalev (Universität Mannheim, Germany) **On Lightweight Stream Ciphers with Shorter Internal States**
11:30 – 11:50	Christof Beierle (Ruhr-Universität Bochum, Germany) **Analyzing Permutations for AES - like Ciphers : Understanding ShiftRows**

12:00 - 13:00 Lunch

Talks Session 5	
13:00 – 13:20	Angela Jäschke (Universität Mannheim, Germany) **Fully Homomorphic Encryption : A Tour Through the Definition Jungle**
13:20 – 13:40	Christina Kolb (Universität Paderborn, Germany) **Secure Credential Systems including Proofs of Partial Knowledge**
13:40 – 14:00	Wincor Nixdorf **Advanced Offline User Authentication: Design And Analysis of an Authentication Scheme for ATM-Technicians**

Securing the Financial Cloud

Peter Günther

University of Paderborn

Over the past years, cloud computing has become and important concept for offering scalable and cost-efficient services. The National Institute of Standards and Technology (NIST) defines cloud computing "as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [1]. To reduce costs, in cloud computing resources are shared between different organizations. This requests for new data security strategies [2].

In this talk we introduce the project *Securing the Financial Cloud* (SFC)[1] that has the goal to transfer financial services into a financial community cloud where different financial institutions like, e.g., banks participate.

An important service of the financial cloud is data storage. This includes sharing of data by multiple users like, for example different financial institutions. Financial services deal with very sensible data and hence confidentiality is a major concern. Furthermore, the access of users to data should be restricted according to some access policy. Hence, a fine-grained access control mechanism is required. One approach to implement access control is an access control server operated by the storage provider. But contrarily to the cloud definition from above, this increases the storage provider's interactions. Furthermore, it requires ultimate trust of the users in the provider.

A different approach that we pursue in the SFC project to implement access control is attribute based encryption (ABE) [3]. Here, data is encrypted based on attributes that describe the data. A user owns a private key that reflects the access policy of the user. Users are able to decrypt only if their policies match the attributes of the encrypted data and hence an access control server is not required. This increases scalability of services and reduces trust in the cloud provider. In this talk we will present our ongoing work about the application of ABE in the financial cloud. We will provide our basic concepts for encrypted and authenticated data storage.

Another goal of the financial cloud is to offer services that process data. Since data is encrypted, either the encryption mechanism has to allow processing on encrypted data or the data has to be decrypted prior to the processing. Within the SFC project, we apply the second approach. In the talk we will explain how we delegate access policies and the related private keys to dedicated, secured cloud services for the purpose of data processing.

References

[1] National Institute of Standards and Technology. The NIST Definition of Cloud Computing. `http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf` Accessed: 2015-01-05

[2] Cloud Security Alliance (CSA). Security Guidance for Critical Areas of Focus in Cloud Computing. `http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf` Accessed: 2015-01-05

[3] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. In *ACM Conference on Computer and Communications Security*, pages 8998. ACM, 2006.

[1]Funded by the German Federal Ministry of Education and Research, grant 16KIS0062.

Constructing CCA-secure predicate key encapsulation mechanisms from CPA-secure schemes and universal one-way hash functions

M.Sc. (Comp. Sc.) Gennadij Liske and Prof. Dr.rer.nat. Johannes Blömer

January 5, 2015

University of Paderborn

In our talk we present our transformation of chosen-plaintext secure predicate key encapsulation schemes with public index into chosen-ciphertext secure schemes. Our construction requires only an universal one-way hash function and is selectively secure in the standard model. The transformation is not generic but can be applied to various existing schemes constructed from bilinear groups. Using common structural properties of these schemes we provide an efficient and simple transformation without overhead in form of one-time signatures or message authentication codes as required in previous generic transformations.

Traditionally, encryption schemes are used to ensure confidentiality during one to one communication, whereas modern applications also require encryption schemes which can be applied in much more sophisticated scenarios. Consequently, various types of encryption schemes for different applications have been proposed during the last decades in order to meet novel demands. Many of these schemes fall into the class of predicate encryption schemes with public index, which will be considered in our talk.

The goal of predicate encryption schemes with public index is still to ensure confidentiality, but the sender does not encrypt messages for some specified receiver anymore. Rather, she encrypts the message under some ciphertext index $cInd$, whereas the user i obtains from a central authority a secret key for some key index $kInd_i$. User i will be able to decrypt a ciphertext if and only if the ciphertext index and the users key index match according to some predicate $\mathcal{R}$, that is if $\mathcal{R}(X_i, Ind) = 1$. The class of predicate encryption schemes with public index covers such schemes as identity-based encryption, attribute-based encryption, broadcast encryption and others.

It is widely accepted in the cryptographic community, that the notion of chosen-ciphertext security (CCA-security) is the right notion of security for encryption schemes. Nevertheless, novel predicate encryption schemes are usually constructed to withstand only chosen-plaintext attacks (CPAs). Achieving CCA-secure schemes is mostly considered separately due to several reasons. On the one hand, CPA-secure constructions of predicate encryption schemes are already quite complex. On the other hand, in many contexts there exist generic and quite efficient transformations of CPA-secure encryption schemes into CCA-secure encryption schemes. Hence, researchers often just propose to apply such transformations and the question of finding specific and possibly more efficient CCA-secure constructions for novel schemes is ignored.

Enhancing specific CPA-secure encryption schemes in order to achieve efficient CCA-secure constructions is a laborious but useful task as has been shown for various schemes based on bilinear groups. These schemes are the starting point of our work. Analyzing them we extract common properties that we use to provide an efficient and at the same time widely applicable transformation of CPA-secure predicate key encapsulation schemes into CCA-secure schemes. If applied to previously proposed schemes the constructions are provable secure in the selective security model under the same security assumptions as the original schemes. Note that although selective security model is a weaker notion of security than adaptive security, many recently proposed predicate encryption schemes are secure only in this security model. Furthermore, we are already able to apply our technique to some specific adaptively secure predicate encryption schemes and work on similar semi-generic transformation in adaptive security model.

ORAM challenges in a fully sequenced DNA world

Nikolaos P. Karvelas*, Andreas Peter† and Stefan Katzenbeisser*

* TU Darmstadt † University of Twente

As fully sequenced human DNA becomes an inexpensive commodity, it will not come as a surprise in the near future to see thriving business models, that will use sequenced DNA as their driving force. One can then imagine, that in such a case the data (i.e. the fully sequenced human genome) will be outsourced to a remote biobank and will be processed on demand by an authorized third party like a private physician or a researcher, which we can here call an investigator. Due to the data's sensitivity, it is vital that it be technically protected against misuse and should be allowed to be seen in plain only by the owner. In other words, the investigator should retrieve the encrypted DNA parts that he wants to process, only after authorization from the data owner and should process them without decrypting them.

A closer look at the problem however makes apparent that encryption alone is not enough to guarantee the owner's privacy: The biobank (or another investigator), can deduce enough information about previous processing on the data by merely studying the access patterns (i.e. which parts of the data have been previously accessed). In order then to preserve the data owner's privacy, a cryptographic primitive proposed by Goldreich and Ostrovsky in [GO96], known as Oblivious RAM (ORAM) seems to be a promising candidate as a building block for solutions to the above described problem. Solutions like [FWC+11, KPK+14] address the aforementioned problem in settings of environments with multiple data owners and using ideas from the ORAM literature.

Inspired by the ORAM primitive, in this talk we will revise the state-of-the-art ORAM constructions proposed in [SCSL11, SvDS+13] and explore their ability to form the building blocks for solutions, that can guarantee access pattern privacy in processing of encrypted fully sequenced human DNA. Furthermore we investigate their potential usage not only in settings where multiple clients store their encrypted DNA, but also in settings where multiple investigators are allowed to process the encrypted DNA of multiple data owners.

References

[FWC+11] Martin Franz, Peter Williams, Bogdan Carbunar, Stefan Katzenbeisser, Andreas Peter, Radu Sion, and Miroslava Sotáková. Oblivious outsourced storage with delegation. In *FC*, pages 127–140, 2011.

[GO96] Oded Goldreich and Rafail Ostrovsky. Software protection and simulation on oblivious RAMs. *J. ACM*, 43(3):431–473, 1996.

[SCSL11] Elaine Shi, T.-H. Hubert Chan, Emil Stefanov, and Mingfei Li. Oblivious RAM with o((logn)3) worst-case cost. In *Advances in Cryptology - ASIACRYPT 2011 , Seoul, South Korea, December 4-8, 2011. Proceedings*, pages 197–214, 2011.

[SvDS+13] Emil Stefanov, Marten van Dijk, Elaine Shi, Christopher W. Fletcher, Ling Ren, Xiangyao Yu, and Srinivas Devadas. Path ORAM: an extremely simple oblivious RAM protocol. In *ACM CCS*, pages 299–310, 2013.

[KPK+14] Nikolaos P. Karvelas, Andreas Peter, Stefan Katzenbeisser, Erik Tews and Kay Hamacher. Privacy Preserving Whole Genome Sequence Processing through Proxy-Aided ORAM In *ACM Workshop on Privacy in the Electronic Society, WPES 2014, Scottsdale Arizona, USA, November 4, 2014.*

Revocation in Publicly Verifiable Outsourced Computation

James Alderman, Christian Janson, Carlos Cid and Jason Crampton

Information Security Group, Royal Holloway, University of London
Egham, Surrey, TW20 0EX, United Kingdom

The combination of software-as-a-service and the increasing use of mobile devices gives rise to a considerable difference in computational power between servers and clients. Thus, there is a desire for clients to outsource the evaluation of complex functions to an external server. Servers providing such a service may be rewarded per computation, and as such have an incentive to cheat by returning garbage rather than devoting resources and time to compute a valid result. This problem, known as *Verifiable Outsourced Computation* (VC) [GGP10, PRV12], has attracted a lot of attention in the community recently. Prior work mainly focussed on detecting cheating servers but in practice a misbehaving server should not be trusted for future computations.

We introduce the notion of *Revocable Publicly Verifiable Computation* (RPVC) [AJCC14], where a cheating server is revoked and may not perform future computations (thus incurring a financial penalty). We introduce a Key Distribution Center (KDC) to efficiently handle the generation and distribution of the keys required to support RPVC. The KDC is an authority over entities in the system and enables revocation. We also introduce a notion of blind verification such that results are verifiable (and hence servers can be rewarded or punished) without learning the value of the result. We present a rigorous definitional framework, define a number of new security models and present a construction of such a scheme built upon Key-Policy Attribute-based Encryption.

This framework already provides a weak form of *access control* provided by the KDC. We can also extend this framework to achive access control policies over delegators, servers and verifiers [AJCC15].

References

[AJCC15] James Alderman, Christian Janson, Carlos Cid and Jason Crampton. Access Control in Publicly Verifiable Outsourced Computations. *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, AsiaCCS 2015 - to appear,* `full version available at eprint.iacr.org/2014/762`

[AJCC14] James Alderman, Christian Janson, Carlos Cid and Jason Crampton. Revocation in Publicly Verifiable Outsourced Computations. *Proceedings of the 10th International Conference on Information Security and Cryptology - Inscrypt 2014. Springer - to appear,* `full version available at eprint.iacr.org/2014/640`

[GGP10] Rosario Gennaro, Craig Gentry and Bryan Parno. Non-interactive Verifiable Computing: Outsourcing Computation to Untrusted Workers. *Advances in Cryptology - CRYPTO 2010, 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010. Proceedings, p. 465-482.*

[PRV12] Bryan Parno, Mariana Raykova and Vinod Vaikuntanathan. How to Delegate and Verify in Public: Verifiable Computation from Attribute-Based Encryption. *Theory of Cryptography - 9th Theory of Cryptography Conference, TCC 2012, Taormina, Sicily, Italy, March 19-21, 2012. Proceedings, p. 422-439.*

Outsourced Proofs of Retrievability – Liability in the Cloud

Frederik Armknecht*, Jens-M. Bohli†, Ghassan O. Karame†, Zongren Liu†, Christian A. Reuter*

*University of Mannheim, Germany
†NEC Laboratories Europe, Germany

Cloud storage is a popular service, being offered by a number of major companies like Dropbox, Microsoft, Amazon, Google and many more. The idea behind cloud storage is that the data will no longer be stored locally at the user, but outsourced to some service provider who makes the data available upon request. One of the major concerns though is the risk of data loss. The service provider may be malicious and delete some data, but also accidental hardware, software or human fails may cause data loss. Hence, a user should preferably be able to regularly check if his data is still stored without the need to retrieve it completely.

This problem can be solved with Proofs of Retrievability (POR). These are cryptographic proofs that enable a cloud provider to prove that a user can retrieve his data in its entirety. POR need to be frequently executed by the user to ensure that their data stored on the cloud can be fully retrieved at any point in time. To conduct and verify POR, users need to be equipped with devices that have network access, and that can tolerate the (non-negligible) computational overhead incurred by the verification process. This clearly hinders the large-scale adoption of POR by cloud users, since many users increasingly rely on portable devices that have limited computational capacity, or might not always have network access.

In our recently published paper [OPOR], we introduce the notion of *Outsourced Proofs of Retrievability* (OPOR), in which users can task an external auditor to perform and verify POR with the cloud provider. We argue that the OPOR setting is subject to security risks that have not been covered by existing POR security models. To remedy that, we propose a formal framework and a security model for OPOR. We then propose an instantiation of OPOR which builds upon the provably-secure private POR scheme due to Shacham and Waters [SW] and we show its security in our proposed security model. We implement a prototype based on our solution, and evaluate its performance in a realistic cloud setting. Our evaluation results show that our proposal minimizes user effort, incurs negligible overhead on the auditor (compared to the SW scheme), and considerably improves over existing publicly verifiable POR.

In this talk, we will present current POR schemes and their common problems which occur if the user wants to check his outsourced cloud data regularly. After that, we will explain the OPOR model and compare it to classical POR schemes. Finally, we will give an example of an OPOR scheme by presenting a concrete instantiation, called Fortress.

References

[OPOR] Frederik Armknecht, Jens-Matthias Bohli, Ghassan O. Karame, Zongren Liu and Christian A. Reuter. Outsourced Proofs of Retrievability. In: Gail-Joon Ahn, Moti Yung and Ninghui Li (eds.), *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS)*, pp. 831-843. ACM Press (2014).

[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).

Anonymous and Publicly Linkable Reputation Systems
(*to appear in FC 2015*)

Jakob Juhnke[1]

University of Paderborn
jakob.juhnke@uni-paderborn.de

Reputation systems are an increasingly popular tool to give providers and customers valuable information about previous transactions. To provide trustworthy, reliable, and honest ratings there is a need for anonymous reputation systems that also guarantee that customers rate products only once. To further increase trust in the system, everyone - even outsiders - should be able to verify the validity of ratings.

Some of the properties for reputation systems have been studied in the context of group signatures [BMW03, BSZ05]. However, the concept of group signatures does not meet all the requirements for reputation systems. In particular, reputation systems do not consist of a single group of users. Rather one can think of reputation systems as a family of group signature schemes - one for each product.

Moreover, we may have providers with several products. Hence, when looking at security and anonymity group signature schemes for different products can not be considered in isolation. Finally, known constructions of group signatures do not provide all properties that we need for a secure and anonymous reputation system and do not provide them simultaneously.

In this talk, we will present a construction of a reputation system providing anonymity, traceability, strong-exculpability, verifier-local revocation, and public linkability. Anonymity means that ratings of honest users are indistinguishable. Traceability means that it is impossible for any set of colluding users to create ratings that can not be traced back to a user of the system. Strong-exculpability means that nobody can produce ratings on behalf of honest users. A system has verifier-local revocation, if revocation messages only have to be sent to rating verifiers, but not to individual raters. Public linkability requires that anyone can decide whether or not two ratings for the same product were created by the same user, i.e. no secret key is required to link ratings.

Our construction is primarily based on the group signature schemes [BBS04] and [NF06]: we use non-interactive zero-knowledge proofs of knowledge in bilinear groups to obtain a signature scheme which is secure in the random oracle model. Then this signature scheme is extended to a reputation system that fulfills our needs.

References

[BMW03] Mihir Bellare, Daniele Micciancio, and Bogdan Warinschi. Foundations of Group Signatures: Formal Definitions, Simplified Requirements, and a Construction Based on General Assumptions, EUROCRYPT 2003

[BSZ05] Mihir Bellare, Haixia Shi, and Chong Zhang. Foundations of Group Signatures: The Case of Dynamic Groups, CT-RSA 2005

[BBS04] Dan Boneh, Xavier Boyen, and Hovav Shacham. Short Group Signatures, CRYPTO 2004

[NF06] Toru Nakanishi and Nobuo Funabiki. A Short Verifier-Local Revocation Group Signature Scheme with Backward Unlinkability, Advances in Information and Computer Security, 2006

[1]This talk is about joint work with Johannes Blömer and Christina Kolb.

An Efficient Machine Learning Attack on the Slender PUF Protocol

Georg T. Becker

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

Physical Unclonable Functions (PUFs) have emerged as a promising solution for securing resource-constrained embedded devices such as RFID tokens. PUFs use the inherent physical differences of every chip to either securely authenticate the chip or generate cryptographic keys without the need of non-volatile memory. However, PUFs have shown to be vulnerable to model building attacks if the attacker has access to challenge and response pairs. In these model building attacks, machine learning is used to determine the internal parameters of the PUF to build an accurate software model. Nevertheless, PUFs are still a promising building block and several protocols and designs have been proposed that are believed to be resistant against machine learning attacks.

In this talk we take a closer look at the Slender PUF protocol [M12, R14] that uses an XOR-Arbiter PUF as a building block for a secure PUF based authentication protocol. The Slender PUF protocol is based on pattern matching and obfuscates the individual PUF responses so that an attacker does not have direct access to challenges and responses of the used of the XOR-Arbiter PUF. Since the attacker does not have access to direct challenges and responses, the protocol is supposed to be secure against machine learning attacks. However, in this talk we will see that even these highly obfuscated responses can be used to attack the PUF using machine learning. This is achieved using an Evolution Strategies based machine learning algorithm (CMA-ES) in conjunction with a fitness function based on the hamming weight of the PUF response bits.

With this new attack strategy, it is possible to attack the protocol even when it is used with parameters that were believed to be computationally infeasible to be attack using machine learning. These attacks highlight once more how difficult it is to use Arbiter PUFs as building blocks for secure lightweight authentication protocols.

References

[R14] M. Rostami, M. Majzoobi, F. Koushanfar, D. Wallach, and S. Devadas. Robust and Reverse-Engineering Resilient PUF Authentication and Key-Exchange by Substring Matching *IEEE Transactions on Emerging Topics in Computing*, PP(99):11, 2014.

[M12] M. Majzoobi, M. Rostami, F. Koushanfar, D. Wallach, and S. Devadas. Slender PUF Protocol: A Lightweight, Robust, and Secure Authentication by Substring Matching *IEEE Security and Privacy Workshops (SPW)*, May 2012.

RSA with SRAM-based PUFs Found on Commodity Hardware

André Schaller and Stefan Katzenbeisser
{schaller,katzenbeisser}@seceng.informatik.tu-darmstadt.de
Technische Universität Darmstadt
Darmstadt, Germany

In recent years Physically Unclonable Functions (PUFs) have become a promising building block for cryptographic protocols and applications. They allow for extracting unique keys by exploiting minuscule differences among devices, which are due to manufacturing variations. In contrast to traditional secure hardware approaches like TPM the key derived from PUFs is only existent during a short period of time, increasing the efforts for an attacker to illegitimately extract it. Furthermore, intrinsic PUFs can be found on several commodity devices, such as smartphones or microcontrollers [SAvdLK14]. As they don't require additional hardware, they can be used to implement lightweight security protocols with a hardware-based anchor of trust even on low-end devices.

Numerous scenarios, which are based on PUFs have been proposed, including client authentication [RBK10], secure key storage [TSW+07], hardware-software binding [GKST07] and more. Virtually all of them extract a shared secret, which is further used during protocol execution. In this work we investigate the possibilities to combine asymmetric cryptography and PUFs. Enabling asymmetric cryptography on PUFs combines the advantages of such cryptosystems with the desired characteristics of PUFs. To the best of our knowledge, this is the first work that explores how SRAM-based PUFs can be used to derive and securely store RSA key pairs. The main focus of this work is to identify to what extent computational limitations imposed by the hardware resources restrict the security properties and performance of our proposed schemes.

In particular, we explore approaches to securely store a given RSA key pair and to derive a valid RSA key pair using the SRAM start-up patterns. We further implemented and evaluated the proposed approaches on an evaluation board exploiting the intrinsic on-chip SRAM PUF. The presented work is in progress, thus we also give an outlook on how the presented approaches could be optimized with respect to performance and security properties.

References

[SAvdLK14] André Schaller, Tolga Arul, Vincent van der Leest, and Stefan Katzenbeisser. Lightweight Anti-counterfeiting Solution for Low-End Commodity Hardware Using Inherent PUFs. In *Trust and Trustworthy Computing*, pages 83–100. Springer, 2014.

[RBK10] Ulrich Rührmair, Heike Busch, and Stefan Katzenbeisser. Strong pufs: models, constructions, and security proofs. In *Towards hardware-intrinsic security*, pages 79–96. Springer, 2010.

[TSW+07] Pim Tuyls, Geert-Jan Schrijen, Frans Willems, Tanya Ignatenko, and Boris Škorić. Secure key storage with PUFs. *Security with Noisy Data-On Private Biometrics, Secure Key Storage and Anti-Counterfeiting*, pages 269–292, 2007.

[GKST07] Jorge Guajardo, Sandeep S. Kumar, Geert Jan Schrijen, and Pim Tuyls. FPGA Intrinsic PUFs and Their Use for IP Protection. In *Proceedings of the 9th International Workshop on Cryptographic Hardware and Embedded Systems*, volume 4727 of *Lecture Notes in Computer Science*, pages 63–80, 2007.

Cryptanalysis of the ASASA Structure

Thorsten Kranz and Gregor Leander

Horst Görtz Institute for IT-Security
Ruhr-University Bochum

The alternation of S-box layers and affine mappings is frequently used in the design of cryptographic primitives. ASASA was recently suggested by Biryukov et al. [BBK14] as a building block for various cryptographic scenarios. We give an algorithm to decompose an ASASA structure on n bits in 2^{2n} steps. The algorithm is based on the idea that the number of possible output differences depends on the number of active S-boxes in the first layer of S-boxes. We sort the input differences by the number of output differences. We then use the sorted list to find the subspaces of differences which belong to the case of exactly one active S-box. Given this set of subspaces we are able to find the first layer of the ASASA structure by solving a system of linear equations. The attack can be executed in the same way for the last layer which leads to the insecure SAS structure. Our experimental results indicate a high success probability.

References

[BBK14] Alex Biryukov et al. Cryptographic Schemes Based on the ASASA Structure: Black-Box, White-Box, and Public-Key (Extended Abstract), *ASIACRYPT 2014*, December 2014.

On Lightweight Stream Ciphers with Shorter Internal States
(to appear at FSE 2015)

Frederik Armknecht and Vasily Mikhalev

University of Mannheim
Germany

During the last years several lightweight block ciphers and stream ciphers have been proposed. Stream ciphers usually allow for a higher throughput but require a larger area size compared to block ciphers. The latter is mainly caused by time-memory-data trade-off (TMDTO) attacks which aim to recover the internal state of the stream cipher [2]. The attack effort is in $O(2^{\sigma/2})$, where σ denotes the size of the internal state of a stream cipher. This results into a rule of thump that for achieving κ-bit security level, the size of internal state should be at least $\sigma = 2 \cdot \kappa$. It means that in order to implement such a cipher at least $2 \cdot \kappa$ memory gates are required. As memory gates are usually the most area and power consuming components, this implies a sever limitation with respect to possible lightweight implementations.

In this work, we investigate an extension in the common design for stream ciphers which allows to realize secure lightweight stream cipher with an area size beyond the trade-off attack bound mentioned above. The core idea is to split the set of internal states into 2^κ equivalence classes such that a TMDTO attack has to consider each of these classes at least once. To achieve this goal, we suggest to involve the key into the update process of the internal state.

Theoretically, the overall approach is still to have a sufficiently large internal state which determines the keystream bits. The main difference though is that part of this state is the secret key itself and not only a state that has been derived from this key. If one considers the case that the key is fixed for the device, one can make use of the fact that storing a fixed key is significantly less area consuming than deploying a register of the same length. In fact, a similar idea has been used in the design of KATAN/KTANTAN [3].

We demonstrate the feasibility of this approach by describing and implementing a concrete stream cipher named Sprout. It builds upon the Grain 128a [1] cipher but uses shorter registers and aims for 80 bit security. We argue that Sprout seems to inherit the strengths of Grain 128a. However, our implementation confirms that Sprout uses significantly less area size than the eStream finalisits of the hardware portfolio and also compares favorably with many lightweight block ciphers.

References

[1] Martin Ågren, Martin Hell, Thomas Johansson, and Willi Meier. Grain-128a: a new version of Grain-128 with optional authentication. *International Journal of Wireless and Mobile Computing,*5(1):4859, 2011..

[2] Alex Biryukov and Adi Shamir. Cryptanalytic time/memory/data tradeoffs for stream ciphers *In Advances in Cryptology ASIACRYPT 2000,*pages 113. Springer, 2000.

[3] Christophe De Canni‘ere, Orr Dunkelman, and Miroslav Knezevic. KATAN and KTANTAN - A family of small and ecient hardware-oriented block ciphers. In Christophe Clavier and Kris Gaj, editors, *Cryptographic Hardware and Embedded Systems - CHES 2009, 11th International Workshop, Lausanne, Switzerland, September 6-9, 2009, Proceedings,*volume 5747 of *Lecture Notes in Computer Science*, pages 272-288. Springer, 2009..

Analyzing Permutations for AES-like Ciphers: Understanding ShiftRows[1]

Christof Beierle*, Philipp Jovanovic**, Martin Lauridsen†, Gregor Leander*, Christian Rechberger†

* Ruhr University Bochum ** University of Passau † Technical University of Denmark

With the standardization of Rijndael as the AES, an astonishing number of new primitives using similar components have seen the light of day. This can largely be attributed to the seminal wide-trail design strategy which was introduced for the first time. It is an elegant way of ensuring good diffusion properties and at the same time allow designers to easily give bounds on the resistance towards differential- and linear cryptanalysis. On top, it decouples the choice of the non-linear layer and the linear layer to a large extent. For AES-like ciphers, the linear layer itself is composed of two parts, one that resembles the AES `MixColumns` operation and one that resembles the AES `ShiftRows` operation. For the former, the criteria are well understood. In stark contrast, for the operation resembling `ShiftRows`, the situation is significantly less clear. Basically, the `ShiftRows`-like operation highly influences the number of active S-boxes when considering more than two rounds only. Understanding the bounds for more than two rounds is crucial for many good designs.

In this work, we develop a structured approach to analyzing the permutation layer, i.e. the generalized `ShiftRows`-like operation. For this, we start by defining a general framework for AES-like ciphers. Note that we do not restrict to the case where permutation is identical in all rounds. Moreover, we first consider arbitrary word-wise permutations and later restrict ourselves to word-wise rotations in the rows. Word-wise rotations have the appeal of being efficiently implementable on many modern CPUs. Our following analysis consists of two parts.

First, we simplify the problem by introducing the notion of equivalent permutation parameters. It is intuitively clear that many choices of the permutation will lead to the same behavior of the cipher. One such example is changing the order of the rotation constants for the `ShiftRows` operation in the AES. Two permutation-layers will be defined to be equivalent whenever they guarantee the same lower bound on the number of active S-boxes. This is interesting theoretically, as it allows to simplify the problem. For example, we prove that a general permutation can never yield better results than a permutation that operates on the rows individually. Furthermore, using this notion of equivalence, we derive a normalized representation of any word-wise rotation in the rows. This allows to reduce the problem domain and thus the search space for a computational approach significantly.

In the second part of our analysis, we use this normalized representation in a combination with solving mixed-integer linear programs using the IBM ILOG CPLEX library. This results in optimal parameter suggestions for a wide range of AES-like ciphers. In particular, it allows us to suggest improved parameters for Rijndael-192, Rijndael-256, PRIMATEs-80 and Prøst-256 on this front.

Finally, given our extensive experimental results, we conjecture an optimal lower bound on the number of active S-boxes possible for specific parameters. Those parameters are such that they allow for an iterative version of the Four-Round Propagation Theorem of the AES. We also provide a permutation which guarantees this conjectured optimal bound. In contrast to prior work, this permutation layer is generic and, more importantly, realized with *cyclic row rotations only.*

[1]This is a summary of a paper accepted at CT-RSA 2015.

Fully Homomorphic Encryption: A Tour Through the Definiton Jungle

Frederik Armknecht*, Colin Boyd†, Chris Carr†, Kristian Gjøsteen†, Angela Jäschke*, Christian Reuter* and Martin Strand†

* University of Mannheim
Mannheim
Germany

† NTNU Trondheim
Trondheim
Norway

Fully homomorphic encryption (FHE), which means an encryption system which allows arbitrary computations on encrypted data, has been dubbed the holy grail of cryptography, an elusive goal which would solve the IT world's problems of security and trust. Research in the area exploded after 2009 when Gentry showed that it can be realised in principle [Gent09]. Since that time considerable progress has been made in finding more practical and more efficient solutions. However, as research developed, terminology and concepts became diverse and confusing so that today it can be difficult to understand what the achievements of different works actually are.

The purpose of this presentation is to give a brief overview of this complex field: On the one hand, we will take a look at possible real-world applications of FHE and examine the current state of the field in terms of efficiency, while on the other hand, we will categorize and explain different definitions and the relationships between them. While the latter does not sound very interesting at first, it turns out to be very important: For example, being able to evaluate an arbitrary circuit on encrypted data and being able to evaluate arbitrarily many circuits consecutively at first seem to be the same thing. However, if we take a closer look, this turns out not to be the case at all and makes a big difference for real-world applications. In this spirit, it is important to give a formal overview of all the definitions used in research and to examine what they imply and what they don't.

This research was sponsored by the DAAD.

References

[Gent09] Craig Gentry. *A fully homomorphic encryption scheme*, Stanford PHD Thesis, 2009.

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

[BV11] Zvika Brakerski and Vinod Vaikuntanathan. *Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages*, Advances in Cryptology – CRYPTO 2011.

[LNV11] Michael Naehrig and Kristin Lauter and Vinod Vaikuntanathan. *Can homomorphic encryption be practical?*, CCSW 2011.

Secure Credential Systems including Proofs of Partial Knowledge

Christina Kolb

Research Group: Codes and Cryptography
Universität der Informationsgesellschaft
Fürstenallee 11, 33102 Paderborn - Germany
ckolb@mail.upb.de

In credential systems, users obtain attribute-certifying credentials from trustworthy authorities. These credentials can be used to access certain locations or resources. In addition, we want the user's credentials to achieve policies before having access to the resources. This is called a proof of partial knowledge. To protect the users' privacy this must be possible without revealing their identities. Beside the users' anonymity, another security requirement is preventing users from credential sharing.
Important work on signature schemes and commitment schemes, such as the Pedersen Commitment Scheme, applied to credential systems was done by A. Lysanskaya in [Lys02] and J. Camenisch [Cam05], where a credential is considered as a digital signature on a committed value.
In our research project, we want to design access control systems realizing complicated access policies. Whereas credential systems can be viewed as access control systems for simple policies, i.e single attributes are required to get access to resources, they do not lead directly to more complicated access control systems. In this research project, we want to combine the techniques of [Lys02] and [Cam05] with the techniques of [Cramer94]. Cramer, Damgård, and Schoenmakers [Cramer94] show how to transform zero-knowledge protocols proving knowledge of witnesses for simple relations into witness indistinguishable protocols for more complicated relations, defined via secret sharing schemes (see [Beimel96] and [Beimel11]).
In this talk, we briefly define credential systems and their security properties. We mainly show the construction of the proof of partial knowledge of [Cramer94]. We also give an overview of future research work for the credential system mentioned above.

References

[Beimel96] A. Beimel; Secure Schemes for Secret Sharing and Key Distribution; Research Thesis; Israel Institute of Technology; 1996

[Beimel11] A. Beimel; Secret-Sharing Schemes: A Survey; Springer 2011

[Cam05] J. Camenisch and A. Lysyanskaya; Signature Schemes and Anonymous Credentials from Bilinear Maps; 2005

[Cramer94] R. Cramer, I. Damgård, B. Schoenmakers; Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols; CRYPTO '94

[Lys02] A. Lysyanskaya; Signature Schemes and Applications to Cryptographic Protocol Design; Massachusetts Institute of Technology; 2002

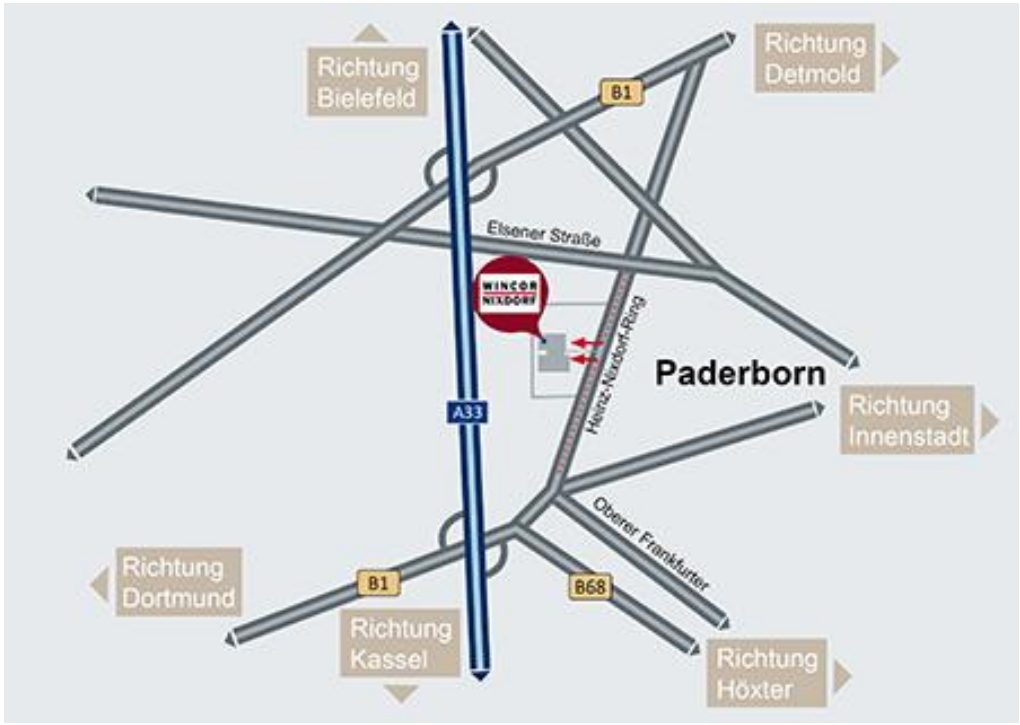
[Pedersen92] T. P. Pedersen; Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing; Springer; 1992

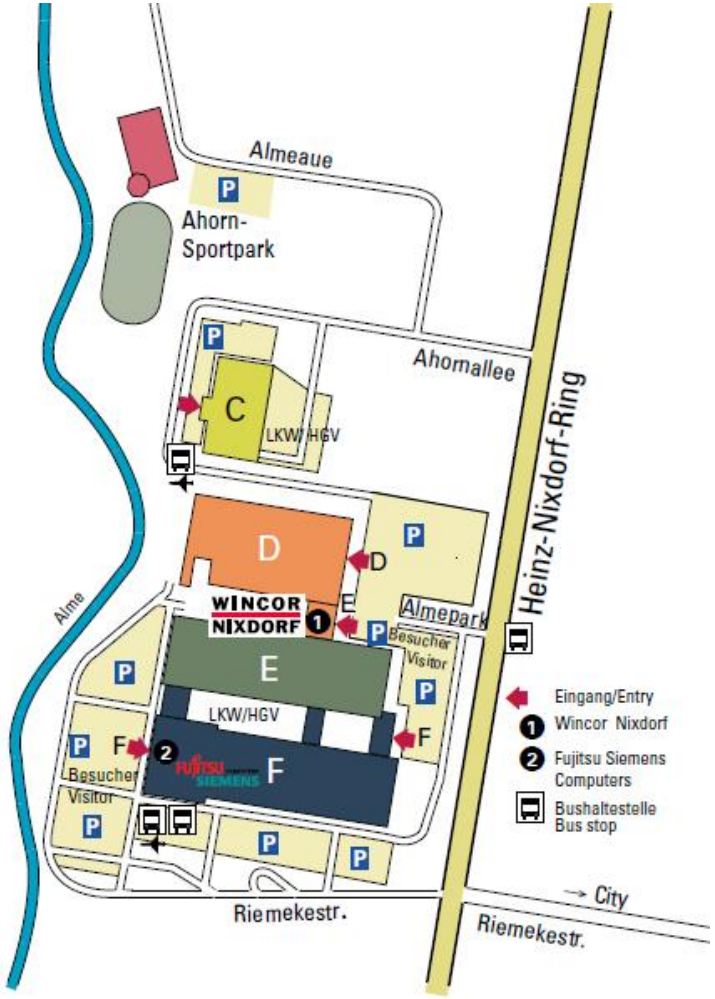
Kryptotag

WINCOR NIXDORF

EXPERIENCE MEETS VISION.

Anfahrt Wincor Nixdorf Paderborn





Wincor Nixdorf International GmbH
Heinz-Nixdorf-Ring 1
33106 Paderborn

Hotelempfehlungen in Paderborn

WINCOR NIXDORF

Name of hotel	Address	Phone (P) Fax (F)	Homepage E-Mail	Distance to WN location	No. of rooms
Hotel*+ Aspethera**	Am Busdorf 7 33098 Paderborn	P:+49 (0) 5251 2888-100 F:+49 (0) 5251 2888-101	info@hotel-aspethera.de www.hotel-aspethera.de	4 km *downtown* direct bus no. 8	57
ibis** **Paderborn**	Paderwall 1-5 33102 Paderborn	P:+49 (0)5251 1245 F:+49 (0)5251 124 888	h0718@accor.com http://www.ibis.com/de/hotel-0718-ibis-paderborn-city/index.shtml	3,2 km *downtown* direct bus no. 8	90
Hotel*** **Stadthaus**	Hathumarstraße 22 33098 Paderborn	P:+49 (0) 5251 1889 10 F:+49 (0) 5251 1889 1555	info@hotel-stadthaus.de www.hotel-stadthaus.de	2 km *downtown*	34
Hotel*+ Scherf**	Arminiusstraße 23 33175 Bad Lippspringe	P:+49 (0) 5252 204-0 F:+49 (0) 5252 204-188	www.hotel-scherf.de info@hotel-scherf.de	11 km via bus 450	58
Vital-Hotel****	Schwimmbadstr. 14 33175 Bad Lippspringe	P:+49 (0) 5252 964-100 F:+49 (0) 5252 964-170	reception@vital-hotel.de www.vital-hotel.de	11 km via bus 450	110
Waldhotel** Nachtigall**	Hatzfelder Straße 45 33104 Paderborn	P:+49 (0) 5254 8053 5-0 F:+49 (0) 5254 8053 5-144	rezeption@waldhotel-nachtigall.de www.waldhotel-nachtigall.de	5 km	52
Welcome Hotel** Paderborn**	Fürstenweg 13 33102 Paderborn	P:+49 (0)5251 288-00 F:+49 (0)5251 288-100	info.pad@welcome-hotels.com http://www.welcome-hotel-paderborn.de	2,5 km near HNF	153
Hotel**+ Best Western Premier Arosa**	Westernmauer 38 33098 Paderborn	P:+49 (0) 5251 128-0 F:+49 (0) 5251 128-806	info@arosa.bestwestern.de www.arosa.bestwestern.de	3,5 km *downtown* direct bus no. 8	121
Hotel**+ Best Western Premier Park**	Peter-Hartmann-Allee 4 33175 Bad Lippspringe	P:+49 (0) 5252 963-0 F:+49 (0) 5252 963-111	info@parkhotel-lippspringe.bestwestern.de www.parkhotel-lippspringe.bestwestern.de	11 km via bus 450	135

22nd Crypto-Day

Infineon Technologies AG
July 9 and 10, 2015
Munich, Germany

On July 9 & 10 2015, the interest group "Angewandte Kryptographie" of Gesellschaft für Informatik e. V. will host the twenty-second *Crypto-Day*.

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

Host: The Infineon Technologies AG will host the event and provide an insight into product security aspects and ongoing industry research.

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

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

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

Further information related to the venue, as well as to the registration and submission process will be provided timely on the web page.

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

Submission:	Until **June 15** per email
Registration:	Until **June 15** per email
Organisation:	Frederik Armknecht, Universität Mannheim Benedikt Driessen, Infineon Technologies AG
Contacts:	armknecht@uni-mannheim.de benedikt.driessen@infineon.com