Tagungsband zum 13. Kryptotag

Workshop der Fachgruppe Angewandte Kryptologie in der Gesellschaft für Informatik

Security Engineering Group,
Technische Universität Darmstadt & CASED,
Fachbereich Informatik

14. Dezember 2010

Inhaltsverzeichnis

Forward Security for Hash-Based Signatures

Andreas Hülsing

Department of Computer Science
TU Darmstadt

Digital signature schemes are one of the most used cryptographic primitives, with a wide range of applications. The security of commonly used signature schemes is based on hard number theoretic problems. However, no reduction of the security of these schemes to the underlying problems is known. Furthermore, Shor showed that large quantum computers will be able to solve the underlying problems in polynomial time and thus break all currently used signature schemes.

This motivates research on alternative signature schemes. One candidate scheme is the Merkle Signature Scheme (MSS) ([1]). MSS uses a hash tree to authenticate many one time signature scheme (OTS) instances using one public key. Using hash-based OTS schemes like the Winternitz-OTS [1], the security of MSS can be reduced to standard properties of cryptographic hash functions, an extensively studied primitive with non number theoretic implementations.

Furthermore MSS is a key evolving signature scheme meaning that the secret key changes over time. One interesting property key evolving signature schemes can achieve is *forward security*, formally defined in [2]. Informally a key evolving signature scheme is forward secure, if an adversary gaining knowledge of the secret key at some point in time is not capable of forging a signature for any secret key used before.

MSS is per construction forward secure, if the OTS key pairs are chosen at random and each secret key is deleted directly after usage. But to reduce the key size of MSS to a practical value, a pseudo-random generator (PRG) is used to generate the OTS key pairs. This construction was studied by the authors of [4] and [3]. Both papers contain security reductions for certain constructions. We revisit these reductions. Although mathematically correct, the assumptions in both cases are problematic. The first one uses a construction, that undoes the benefit of using a PRG as a large part of the OTS keys has to be stored initially. The other one, misses the formal model of forward security as they do not release the whole secret key to the adversary during their proof. We plan to construct a MSS variant with minimized key size that is provably forward secure in the formal modell.

References

[1] Ralph Merkle. A certified digital signature. In Gilles Brassard, editor, *Advances in Cryptology - CRYPTO' 89*, volume 435 of *Lecture Notes in Computer Science*, pages 218–238. Springer Berlin / Heidelberg, 1990.

[2] Mihir Bellare and Sara Miner. A Forward-Secure Digital Signature Scheme. In Michael Wiener, editor, *Advances in Cryptology CRYPTO' 99* volume 1666 of *Lecture Notes in Computer Science*, pages 786-786. Springer Berlin / Heidelberg, 1999.

[3] L. C. Coronado Garcia. On the security and the efficiency of the merkle signature scheme. Cryptology ePrint Archive, Report 2005/192, 2005.

[4] Tal Malkin, Daniele Micciancio, and Sara Miner. Efficient generic forward-secure signatures with an unbounded number of time periods. In *Advances in Cryptology — EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 400–417. Springer Berlin / Heidelberg, 2002.

Towards a mobile eCard Client

J. Buchmann, A. Wiesmaier*, D. Hühnlein**, J. Braun, M. Horsch, F. Kiefer† and F. Strenzke††

* CASED Darmstadt ** ecsec GmbH Michelau † Technische Universität Darmstadt Darmstadt †† Flexsecure GmbH Darmstadt

Many future electronic identity cards will be equipped with a contact-less interface. Analysts expect that a significant proportion of future mobile phones support Near Field Communication (NFC) technology. Thus, it is a reasonable approach to use the cell phone as mobile smart card terminal, which in particular supports the Password Authenticated Connection Establishment (PACE) protocol to ensure user consent and to protect the wireless interface between the mobile phone and the smart card. Other than existing efficient PACE implementations on low power devices we present a platform independent solution using the Java Micro Edition (JavaME), which is supported by almost all modern mobile phones. Based on a straightforward PACE [1] implementation, we apply various optimizations realizable with existing JavaMe libraries to come up with a user friendly performance.
Since point multiplication is one of the biggest run-time consumers in the PACE protocol, we examine the elliptic curve arithmetic of the available Cryptographic Service Providers (CSP). Benchmarking [2] on PC and on the Nokia 6212 reveals the significant better performance of the FlexiProvider (FP) compared to Bouncy Castle which is the only other available CSP usable without changes. Thus, we use FP for our implementation. For further optimization we review the most common point multiplication algorithms and identify different possibilities for optimization, utilizing the advantages of the algorithms respectively. Merging different arithmetic operations of the PACE protocol allows us to utilize interleaved point multiplication and thus, reducing the total number of arithmetic operations. Furthermore we take advantage of different scalar lengths during the protocol.
Saving the domain-parameters of the used eID card at first contact allows for static and dynamic precomputations for subsequent program executions. Another optimization is changing the scheduling of the calculations needed during the protocol. Additionally, threading allows to use the time waiting for a response from the card or the user for further calculations. Further improvement is reached by avoiding heavy Java objects (which are given by the libraries) and using primitive data types and optimized data structures instead. We end up with a performance of 7.33 seconds on the first execution and 6.31 seconds when using the eID card repeatedly on the Nokia 6212, whereas the straightforward reference implementation achieves a total execution time of 9.5 seconds.
Additionally, we discuss potential side channel attacks and give advice on possible vulnerabilities. The future work discussion shows that there is more optimization potential when making changes to the existing CSPs.
All in all we succeeded in providing a platform independent efficient mobile PACE implementation [3], and also showed where and how more efficiency could be gained, thereby preparing the way for a mobile eCard client [4].

References

[1] M. Horsch. MobilePACE – Password Authenticated Connection Establishment implementation on mobile devices. Bachelor's Thesis, Department of Cryptography and Computer Algebra, Technische Universitt Darmstadt / CASED, September 2009.

[2] F. Kiefer. Effiziente Implementierung des PACE- und EAC-Protokolls fr mobile Gerte. Bachelor's Thesis, Department of Cryptography and Computer Algebra, Technische Universitt Darmstadt / CASED, July 2010.

[3] J. Buchmann, J. Braun, M. Horsch, D. Hühnlein, F. Kiefer, F. Strenzke, and A. Wiesmaier. An efficient PACE Implementation for mobile Devices. In preperation.

[4] J. Buchmann, J. Braun, M. Horsch, D. Hühnlein, T. Hühnlein, F. Kiefer and A. Wiesmaier. Mobile Authentisierung und Signatur. In preperation.

A Hybrid Encryption Technique Supporting Expressive Policies

Stefan G. Weber
Center for Advanced Security Research Darmstadt (CASED)
Mornewegstrasse 32, 64293 Darmstadt, Germany
stefan.weber@cased.de

We sketch a novel hybrid encryption technique that supports expressive policies. It is hybrid, as it combines ciphertext-policy attribute-based encryption (CP-ABE) [BSW07] with location-based encryption (LBE) [SD03] on the level of symmetric keys. It enables encryption under expressive policies, since it can efficiently handle attributes with continuous values, like location.

We use the following notation: $E_{AP}^{L^{(P_1,P_2)}}(M)$ denotes the encryption of a message M under a logical conjunction of a CP-ABE attribute policy AP and a LBE location area attribute $L^{(P_1,P_2)}$. Hereby, $L^{(P_1,P_2)}$ specifies an geographic area with the shape of an rectangle, defined by GPS coordinates $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$. Finally, $D_{\{A\}_R}^{P_R}(CT)$ denotes the decryption of a ciphertext CT initiated by a receiver R, using his private attribute set $\{A\}_R$, while being positioned at GPS coordinate $P_R = (x_R, y_R)$. Decryption succeeds if R's attribute set $\{A\}_R$ satisfies the attribute policy AP and R is positioned within $L^{(P_1,P_2)}$, i.e. if $x_2 \geq x_R \geq x_1$ and $y_2 \geq y_R \geq y_1$ hold. It employs a *location lock mapping* $f_{LL}(L^{(P_1,P_2)})$, according to the following principle: first, GPS coordinates P_1, P_2 are concatenated. Second, the resulting string $s_{LL^{(P_1,P_2)}} = x_1||y_1||x_2||y_2$ is hashed, $h(s_{LL^{(P_1,P_2)}})$, to a 128 bit string (assuming 128 bit symmetric keys), the location lock value. Our *hybrid encryption scheme* works as follows: first, a random session key Key_S is generated. Second, the message is symmetrically encrypted under Key_S, producing ciphertext CT_1. Third, Key_S is XORed with the location lock value, generating a hybrid key Key_H. Fourth, the output is concatenated with an encoding of the location area. Fifth, the resulting string is CP-AB encrypted under an attribute policy AP, producing ciphertext CT_2. CT_1 concatenated with CT_2 form the ciphertext CT. Then, CT is transferred to a receiver R. The *scheme for hydrid decryption* works as follows: first, receiver R tries to decrypt CT_2, using his private attribute set $\{A\}_R$. Second, on successful decryption, the location area $s_{LL^{(P_1,P_2)}}$ is extracted. Third, R's current GPS position P_R is verified to be inside the location area by means of a tamper-resistant GPS receiver. On success, the location lock value can be computed. It is then XORed with the recovered Key_H, in order to reconstruct Key_S. Finally, Key_S is used to symmetrically decrypt CT_1 to M.

We are currently working on applications of this techniques in the areas of *end-to-end secure attribute-based messaging* [WRM10] and *identity and access management* [WMRM10].

References

[BSW07] Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-Policy Attribute-Based Encryption. In: IEEE Symposium on Security and Privacy (SP '07). pp. 321–334. IEEE CS (2007)

[SD03] Scott, L., Denning, D.E.: A Location Based Encryption Technique and Some of Its Applications. In: ION National Technical Meeting 2003. pp. 730–740 (2003)

[WRM10] Weber, S.G., Ries, S., Mühlhäuser, M.: Concepts and Scheme for Multilaterally Secure, User-Friendly Attribute-Based Messaging. Telecooperation Report No. TR-13, ISSN 1864-0516 (2010)

[WMRM10] Weber, S.G., Martucci, L.A., Ries, S., Mühlhäuser, M.: Towards Trustworthy Identity and Access Management for the Future Internet. In: The 4th International Workshop on Trustworthy Internet of People, Things & Services (Trustworthy IoPTS 2010)

Compact Keys for Multivariate Cryptography

Albrecht Petzoldt[1] and Stanislav Bulygin[1]

[1] TU Darmstadt, CASED
Mornewegstrasse 32, 64293 Darmstadt, Germany

When quantum computers arrive, cryptosystems based on number theoretic problems such as factoring or discrete logarithms will become insecure, since such problems can be efficiently solved via Shor's algorithm. So, to guarantee the security of communication in the post-quantum world, alternatives to classical public key schemes are needed. Besides lattice-, code- and hash-based cryptosystems, multivariate public key cryptography is one of the main approaches to achieve this goal.

The basic idea behind multivariate cryptography is to choose a system $\mathcal{Q}$ of m quadratic polynomials in n variables which can be easily inverted (central map). After that one chooses two affine invertible maps $\mathcal{S}$ and $\mathcal{T}$ to hide the structure of the central map. The public key of the cryptosystem is the composed quadratic map $\mathcal{P} = \mathcal{S} \circ \mathcal{Q} \circ \mathcal{T}$ which is difficult to invert. The private key consists of $\mathcal{S}$, $\mathcal{Q}$ and $\mathcal{T}$ and therefore allows to invert $\mathcal{P}$.

Since they require only modest computational resources, multivariate schemes seem to be appropriate for the use on low cost devices like RFID's and smartcards. However, these schemes are not yet widely used, mainly because of the large size of their public and private keys. Therefore, the question of key size reduction for multivariate schemes is an important area of research.

The main topic of this talk is the reduction of the public key size of multivariate signature schemes. After a short introduction into multivariate cryptography and an overview of the different research activities in this field at CASED we present ways, how to create compact public keys for multivariate schemes.

The public key $\mathcal{P}$ of multivariate schemes is given as a set of m quadratic polynomials in n variables. After having chosen a monomial ordering, the coefficients of $\mathcal{P}$ can be written down into an $m \times \frac{(n+1)\cdot(n+2)}{2}$ matrix M_P. Our goal is to create multivariate schemes in such a way, that the corresponding coefficient matrix M_P gets a compact structure.

Our first target here is the UOV signature scheme of Kipnis and Patarin, whose public key $\mathcal{P}$ is given as the concatenation of the quadratic central map $\mathcal{Q}$ and an affine map $\mathcal{T}$, i.e. $\mathcal{P} = \mathcal{Q} \circ \mathcal{T}$. We show how, for a fixed matrix B and fixed affine map $\mathcal{T}$, one can choose the coefficients of $\mathcal{Q}$ in such a way that the coefficient matrix of the corresponding public key gets the form $M_P = (B|C)$. We present several possibilities for the choice of B, e.g. choosing B partially circulant or B generated by a Linear Feedback Shift Register (LFSR). By doing so, it is possible to reduce the public key size of the UOV scheme by up to 86! Furthermore we show how this idea can be extended to other (more advanced) multivariate signature schemes like Rainbow and enSTS, which reduces the public key size by 62! Of course, the security is a crucial point for all of these schemes with reduced key size . The talk finishes with some remarks about future research goals.

Analysing XL and its variants

Enrico Thomae* and Christopher Wolf*

*Horst Görtz Institute for IT-security
& Faculty of Mathematics
Ruhr-University of Bochum, 44780 Bochum, Germany

Solving systems of non-linear multivariate equations are at the heart of many cryptographic algorithms, in particular in the public key setting. Usually, computing the Gröbner basis of the corresponding ideal is the best choice in this context. The best known and also most efficient algorithms for this task are F_4 and F_5. Another strategy to solve such systems is called *eXtended Linearization (XL)*. Using this rather simple folklore algorithm in cryptography was suggested by Courtois et al. at Eurocrypt 2000 [1]. Unfortunately they did not provide a deep analysis of the method and many claims showed to be overly ambiguous. At least since Courtois and Pieprzyk claimed to have broken AES [2] using an XL derivate called XSL and the disproof by Cid and Leurent [3] in 2005, the community of cryptographers became increasingly reserved against this method. But thanks to Moh [4], Diem [5], Yang and Chen [6] and others, XL is understood quite well today.
At Asiacrypt 2004 it was shown that XL actually is a sub-case of Gröbner algorithms and that we hence can expect that Gröbner algorithms are always faster than XL [7, 5]. To improve XL and *maybe* obtain a faster algorithm than F_5 many derivates were proposed, such as FXL, XFL, XLF, XL', XL2, XSL and MutantXL.
We want to revisit the analysis of XL and adapt it on some of its variants. We are concerned about the connection between these variants. Can one use them in parallel? Is some variant always better than an other in some case? Many things can be evaluated only by experiments. Here, we want to start understanding the theoretical background.

References

[1] Nicolas T. Courtois, Alexander Klimov, Jacques Patarin, and Adi Shamir. Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In Advances in Cryptology — EUROCRYPT 2000, volume 1807 of Lecture Notes in Computer Science, pages 392–407. Bart Preneel, editor, Springer, 2000. Extended Version: http://www.minrank.org/xlfull.pdf.

[2] Nicolas T. Courtois and Josef Pieprzyk. Cryptanalysis of block ciphers with overdefined systems of equations. In Advances in Cryptology — ASIACRYPT 2002, volume 2501 of Lecture Notes in Computer Science, pages 267–287. Yuliang Zheng, editor, Springer, 2002.

[3] Carlos Cid and Gatan Leurent. An analysis of the xsl algorithm. In Proceedings of Asiacrypt 2005, LNCS, volume 3788 of Lecture Notes in Computer Science, pages 333–352. Bimal Roy, editor, Springer-Verlag, 2005. ISBN 3-540-30684-6.

[4] T. Moh. On the method of XL and its inefficiency to TTM, 2000.

[5] Claus Diem. The XL-algorithm and a conjecture from commutative algebra. In ASIACRYPT.

[6] Bo-Yin Yang and Jiun-Ming Chen. All in the XL family: Theory and practice. In ICISC 2004, pages 67–86. Springer, 2004.

[7] Gwénolé Ars, Jean-Charles Faugère, Hideki Imai, Mitsuru Kawazoe, and Makoto Sugita. Comparison between xl and gröbner basis algorithms. pages 338–353.

Erfolgreiche Faktorisierungsangriffe gegen RSA in der Praxis

Juliane Krämer, Benjamin Michéle

TU Berlin / T-Labs
Ernst-Reuter-Platz 7
10587 Berlin

Seifert beschrieb 2005 einen neuen Fehler-Angriff gegen eine Implementierung der RSA-Signatur-Verifikation [3]: Zunächst wird der öffentliche RSA-Modul N off-line modifiziert, indem zu den letzten b Bits des Moduls bitweise zufällige Fehlervektoren gleicher Länge addiert werden. Findet sich unter diesen modifizierten $\widehat{N}$ ein Modul, der prim und teilerfremd zu dem öffentlichen Schlüssel e ist, wird anschließend durch Fehlerinduktion in die Hardware genau dieser Modul erzeugt. Aufgrund der Eigenschaften des manipulierten Moduls kann auf diese Weise die selbsterstellte Signatur einer frei wählbaren Nachricht verifiziert werden. Muir verallgemeinerte diesen Angriff [2]. Zum einen lässt er zusammenhängende Fehlervektoren nicht nur bei den letzten Bits von N zu. Zum anderen betrachtet er nicht nur prime $\widehat{N}$, sondern allgemeiner solche, die leicht zu faktorisieren sind. Muir konnte zeigen, dass dieser Angriff für 2048-Bit-RSA und einen 6-Bit-Fehlervektor eine Erfolgswahrscheinlichkeit von mehr als 50% hat.

Während der beschriebene Fehlerangriff Fehler-Induzierung in der Hardware erfordert, untersuchen wir die Möglichkeit, den RSA-Modul durch einen Eingriff in die Software zu manipulieren: Wir betrachten zusammenhängende Teil-Bitfolgen des Moduls N verschiedener Länge und untersuchen die Wahrscheinlichkeit einer leichten Faktorisierung mittels Probedivision und dem Miller-Rabin-Test. Zusätzlich wenden wir auf alle in Frage kommenden Teil-Bitfolgen eines gegebenen 2048-Bit-RSA-Moduls diese Algorithmen tatsächlich an und bestätigen damit die theoretischen Werte, die auf einer Formel von Knuth beruhen [1]. Basierend auf diesen Ergebnissen ist ein praktisch durchführbarer Fehler-Angriff entstanden.

Literatur

[1] Donald E. Knuth. *The Art of Computer Programming.* Vol. 2. Addison-Wesley, 3d ed., 1997.

[2] James A. Muir. *Seifert's RSA Fault Attack: Simplified Analysis and Generalizations.* ICICS 2006, Lecture Notes in Computer Science 4307 (2006), 420-434.

[3] Jean-Pierre Seifert. *On authenticated computing and RSA-based authentication.* CCS 2005, Proceedings of the 12th ACM Conference on Computer and Communications Security, November 2005, 122-127.

A zero-knowledge identification scheme based on the q-ary Syndrome Decoding problem

Pierre-Louis Cayrel[1], Pascal Véron[2] and Sidi Mohamed El Yousfi Alaoui[1]

[1] CASED
Mornewegstrasse 32, 64293 Darmstadt
Germany

[2]IMATH
Université du Sud Toulon-Var.
France

Shor's quantum algorithm for integer factorization, which was published in 1994, poses a serious threat to most cryptographic systems in use today. In particular, all constructions whose security relies on number theory (such as variants of the discrete logarithm problem or integer factorization) are vulnerable to this algorithm. If quantum computers will at one point exist, such schemes can be broken in polynomial time, whereas no quantum attacks are known for lattice-based, code-based, and multivariate cryptographic systems. On the other hand, even should such number-theoretic assumptions remain hard, it is not wise to rely on a single type of hard problems. Furthermore, as the capacity of current adversaries increases, so does the key size for classical constructions; it is possible that alternative post-quantum constructions may provide a better alternative in that sense.

In this work, we consider a particular type of alternative cryptography, based on error-correcting code theory. Code-based cryptography was initiated a long time ago with the celebrated McEliece encryption algorithm. We consider the question of public key identification (ID) protocols in this context. Such schemes allow a party holding a secret key to prove its identity to any other entity holding the corresponding public key. The minimum security of such protocols should be that a passive observer who sees the interaction should not then be able to perform his own interaction and successfully impersonate the prover.

At CRYPTO'93, Stern proposed a 3-pass code-based identification scheme with a cheating probability of 2/3. In this work, we propose a 5-pass code-based protocol with a lower communication complexity, allowing an impersonator to succeed with only a probability of 1/2. Furthermore, we propose to use double-circulant construction in order to dramatically reduce the size of the public key. The proposed scheme is zero-knowledge and relies on an NP-complete coding theory problem (namely the q-ary Syndrome Decoding problem). The parameters we suggest for the instantiation of this scheme take into account a recent study of (a generalization of) Stern's information set decoding algorithm, applicable to linear codes over arbitrary fields $\mathbb{F}_q$; the public data of our construction is then 4 Kbytes, whereas that of Stern's scheme is 15 Kbytes for the same level of security.

The improvement proposed here to the Stern scheme can be applied to all the Stern-based identification and signature schemes (such as identity-based identification and signature scheme [1] for example). We believe that this type of scheme is a realistic alternative to the usual number theory identification schemes in the case of constrained environments such as, for smart cards and for applications like Pay-TV or vending machines.

References

[1] P.-L. Cayrel, P. Gaborit and M. Girault : Identity-based identification and signature schemes using correcting codes. *International Workshop on Coding and Cryptography, WCC 2007*, pp 69–78. editors : Augot, D., Sendrier, N., and Tillich, J.-P.

Quasi-dyadic CFS signatures

Paulo Barreto* and Pierre-Louis Cayrel† and Rafael Misoczki* and Robert Niebuhr‡

* Escola Politécnica, Universidade de São Paulo, Brazil
† CASED, Darmstadt, Germany
‡ Technische Universität, Darmstadt, Germany

Digital signatures are among the most useful and pervasive cryptographic primitives, either *per se* or as part of more elaborate, derived protocols. Yet the overwhelming majority of actually deployed signature schemes seem to rely on the hardness of certain computational problems that are efficiently solvable by quantum computers [Sh95]. Should quantum computers become a technological reality, the task of ensuring that suitable quantum-resistant signatures are available for deployment becomes critical.

The signature algorithm proposed by Courtois, Finiasz and Sendrier, or CFS for short [CFS01], is one of the few and most promising schemes known based on the difficulty of decoding linear error-correcting codes. However, it has the drawback that public keys tend to be exceedingly large [FS09], all the more so due to an attack due to Bleichenbacher (unpublished, but described in [FS09]).

Part of the difficulty resides in obtaining codes with high density of decodable syndromes, since the CFS signing mechanism involves sampling random syndromes until a decodable one is found. Essentially the only family of suitable codes for this purpose is that of binary Goppa codes, for which one can actually correct all t design errors, leading to a signing complexity of $O(t!)$. In comparison, for other classes of codes, no decoding method is known that is capable of efficiently correcting more than about half as many errors; since one has then to design the error correcting capacity twice as high, the CFS signing complexity becomes $O((2t)!) \approx O((t!)^2 \cdot 4^t/\sqrt{t})$, far too much for any secure parameter set.

Quasi-dyadic (QD) codes [MB09], which constitute a proper subfamily of Goppa codes, have been proposed to address the problem of key reduction in the related McEliece and Niederreiter cryptosystems. However, the original QD construction only yields codes with a fairly low density of decodable syndromes, comparable to generic alternant codes rather than to other Goppa codes.

In our paper we modify the construction algorithm for t-error correcting quasi-dyadic codes by [MB09], where the density of decodable syndromes is high, while also allowing for a reduction by a factor up to t in the key size. This yields dense binary Goppa codes as needed for practical instantiation of CFS signatures.

References

[Sh95] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26:1484–1509, 1995.

[CFS01] N. Courtois, M. Finiasz, and N. Sendrier. How to achieve a McEliece-based digital signature scheme. In *Advances in Cryptology – Asiacrypt'2001*

[FS09] M. Finiasz and N. Sendrier. Security bounds for the design of code-based cryptosystems. In *Advances in Cryptology – Asiacrypt'2009*, volume 5912 of *LNCS*, pages 88–105. Springer, 2009.

[MB09] R. Misoczki and P. S. L. M. Barreto. Compact McEliece keys from goppa codes. In *Selected Areas in Cryptography – SAC'2009*, volume 5867 of *LNCS*, pages 276–392. Springer, 2009.

Stochastische Methoden für den Entwurf von sicheren FPGA-Designs

Annelie Heuser*, Michael Kasper*, Werner Schindler*†, Marc Stöttinger*

* CASCADE - Constructive Attacks | Side-Channel Analysis | Secure Design
Center for Advanced Security Research Darmstadt (CASED),
Mornewegstraße 32,
64289 Darmstadt, Germany
email: {Annelie.Heuser,Michael.Kasper,Werner.Schindler,Marc.Stoettinger}@cased.de

† Bundesamt für Sicherheit in der Informationstechnik (BSI),
Godesberger Allee 185–189,
53175 Bonn, Germany
e-mail: Werner.Schindler@bsi.bund.de

In den letzten zehn Jahren ist der Bedarf an eingebetteten Systemen sehr stark gestiegen. Die Integration von Field-Programmable-Gate-Arrays *FPGAs* in diesen Geräten ermöglicht es, rechenintensivere und komplexere Aufgaben auf Kleinstrechnern auszuführen. Im Vergleich zu spezialisierten Co-Prozessoren sind FPGAs durch ihre Rekonfigurierbarkeit flexibler und dennoch sehr effizient in Bezug auf Rechenleistung und Stromverbrauch. Zusätzlich sind die Entwicklungskosten von Funktionsblöcken, so genannten IP-cores, auf FPGAs geringer als die Entwicklung eines spezialisierten Prozessors mit der gleichen Funktionalität. FPGAs werden auch zunehmend für sicherheitskritische Applikationen auf eingebetteten Systemen interessanter, die viel Rechenleistung benötigen. Sicherheitsmaßnahmen gegen Angriffe auf *IP-Cores* mit kryptographischen Operationen sind daher ein elementarer Bestandteil bei der Entwicklung gehärteter, FPGA-basierter eingebetteter Systeme. Diese Angriffe können analytischer Natur sein, aber auch Angriffe auf die Implementierung selbst.

Seitenkanalangriffe nutzen Schwachstellen in der Implementierung aus, um kryptographische Algorithmen (z.B.) in eingebetteten System anzugreifen. Besonders die Powerattacken sind seit 1999 ein fundamentaler Bestandteil im Bereich der Seitenkanalangriffe. Vereinfacht ausgedrückt, besteht das Ziel dieser Angriffe darin, einen Zusammenhang zwischen dem datenabhängigen Leistungsverbrauch und dem geheimen Schlüssel zu entdecken und auszunutzen.

In unserem Vortrag zeigen wir, wie die Kluft zwischen der Seitenkanalanalyse und dem Hardwareentwurf bei sicherheitskritischen FPGA-Implementierungen geschlossen werden kann. Wir stellen den so genannten *stochastischen Ansatz* vor, welcher stochastische Methoden verwendet, um den deterministischen, schlüsselabhängigen Leistungsverbrauch der kryptographischen Prozesse anhand der Transitionsaktivitäten zu bestimmen. Mit Hilfe dieser Methode können mögliche Schwachstellen in einem Design gezielt detektiert werden, um die über Seitenkanäle ausnutzbaren Informationslöcher durch konstruktive Gegenmanahmen zu reduzieren, um eine Kompromittierung geheimer Daten zu verhindern. Der stochatische Ansatz verbindet ingenieursmäßiger Expertise mit fortgeschrittenen stochastischen Methoden aus dem Gebiet der multivariaten Statistik und kann konstruktiv als Werkzeug unterstützend im Design-Prozess von gesicherten IP-Cores auf FPGAs eingesetzt werden. Im Gegensatz zu anderen Analysemethoden, die ebenfalls den datenabhängigen Leistungsverbrauch ausnutzen, wie spa, dpa oder Template Attacken, zeichnet sich die vorgestellte Methode dahingehend aus, dass sie quantitative Informationen über die Schwachstellen in der Implementierung liefert.

http://KryptoTag.de

Der Kryptotag ist eine zentrale Aktivität der GI-Fachgruppe Angewandte Kryptologie. Er ist eine wissenschaftliche Veranstaltung im Bereich der Kryptologie und von der organisatorischen Arbeit der Fachgruppe getrennt. Grundgedanke des Kryptotages ist, dass er inklusive Anreise wirklich nur einen Tag dauert und Nachwuchswissenschaftlern, etablierten Forschern und Praktikern auf dem Gebiet der Kryptologie die Möglichkeit bieten, Kontakte über die eigene Universität hinaus zu knüpfen.

Die Vorträge können ein breites Spektrum abdecken, von noch laufenden Projekten, die ggf. erstmals einem breiteren Publikum vorgestellt werden, bis zu abgeschlossenen Forschungsarbeiten, die zeitnah auch auf Konferenzen präsentiert wurden bzw. werden sollen oder einen Schwerpunkt der eigenen Diplomarbeit oder Dissertation bilden. Die eingereichten Abstracts werden gesammelt und als technischer Bericht veröffentlicht. Es handelt sich damit um eine zitierfähige Arbeit. Sie können von den Seiten der Fachgruppe herunter geladen werden.

Geplante Kryptotage

14. Kryptotag am 21. und 22. März 2011 Ruhr-Universität Bochum, Horst Görtz-Institut für IT-Sicherheit. Kontakt: Christopher Wolf.

Bisherige Kryptotage

13. Kryptotag am 5. November 2010 Security Engineering Group, Technische Universität Darmstadt & CASED. Kontakt: Andreas Peter.
12. Kryptotag am 9. April 2010 Institut für Kryptographie und Sicherheit, KIT. Kontakt: Willi Geiselmann und Jörn Müller-Quade.
11. Kryptotag am 30. November 2009 Lehrstuhl für Informationssicherheit und Kryptographie, Universität Trier. Kontakt: Ralf Küsters.
10. Kryptotag am 20. März 2009 Institut für Mathematik, Technische Universität Berlin. Kontakt: Florian Heß.
9. Kryptotag am 10. November 2008 Institut für Internet-Sicherheit, Fachhochschule Gelsenkirchen. Kontakt: Markus Linnemann.
8. Kryptotag am 11. April 2008 Universität Tübingen, WSI für Informatik, Diskrete Mathematik. Kontakt: Michael Beiter, Claudia Schmidt, Anja Korsten.
7. Kryptotag am 9. November 2007 Bonn-Aachen International Center for Information Technology. Kontakt: Michael Nüsken und Daniel Loebenberger.
6. Kryptotag am 19. Februar 2007. Universität des Saarlandes, Information Security and Cryptography Group und Sirrix AG. Kontakt: Michael Backes und Ammar Alkassar.
5. Kryptotag am 11. September 2006. Universität Kassel, Fachbereich Mathematik/Informatik, Theoretische Informatik. Kontakt: Heiko Stamer.
1. Kryptowochenende am 1. – 2. Juli 2006. Tagungszentrum Kloster Bronnbach der Universität Mannheim. Kontakt: Frederik Armknecht und Dirk Stegemann.
4. Kryptotag am 11. Mai 2006. Ruhr Universität Bochum, Horst-Görtz Institut. Kontakt: Ulrich Greveler.
3. Kryptotag am 15. September 2005. Technische Universität Darmstadt, Theoretische Informatik. Kontakt: Ralf-Philipp Weinmann.
2. Kryptotag am 31. März 2005. Universität Ulm, Abteilung fr Theoretische Informatik. Kontakt:

Wolfgang Lindner und Christopher Wolf.
1. Kryptotag am 1. Dezember 2004. Universität Mannheim, Theoretische Informatik. Kontakt: Stefan Lucks und Christopher Wolf.

Innerhalb der Fachgruppe für Angewandte Kryptologie sind Stefan Lucks (Bauhaus Universität Weimar) und Frederik Armknecht (Universität Mannheim) verantwortlich für die Organisation der Kryptotage. Für eventuelle Rückfragen bitte an sie wenden.