5. Krypto-Tag – Workshop über Kryptographie Universität Kassel

Heiko Stamer (Hg.)
Universität Kassel, Fachbereich Mathematik/Informatik
Heinrich-Plett-Straße 40, D-34132 Kassel

11. September 2006

UNIKASSEL
VERSITÄT

Technical Report No. 06/06

Inhaltsverzeichnis

Performanter Krypto-CoProzessor für unterschiedliche Verfahren

Ralf Laue und Sorin A. Huss
Fachgebiet Integrierte Schaltungen und Systeme, Fachbereich Informatik
Technische Universität Darmstadt

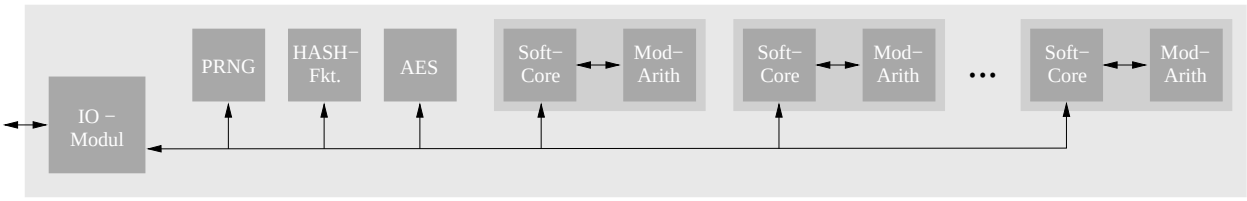
Ziel unserer Planung ist ein PKC-CoProzessor für den Servereinsatz, der verschiedene Verfahren (RSA, ECC) mit unterschiedlichen Bitlängen beherrscht. Für einen möglichst hohen Durchsatz müssen die zunehmend parallelen Strukturen heutiger Hardware kontinuierlich ausgelastet werden.

Wir unterscheiden folgende Abstraktionsebenen: Die niedrigste ist die Ebene der *modularen Arithmetik*, welche für RSA und ECC existiert. Auf diese baut ausschließlich im ECC-Fall die Ebene der *EC-Arithmetik* auf. Darüber wiederum folgt die Ebene des *Diskreten Logarithmus* (ECC) bzw. der *Integer Faktorisierung* (RSA), wobei ECC die elliptischen Kurven als Gruppe nutzt, während für RSA die modularen Arithmetik diese Rolle übernimmt. Darauf gründet sich schließlich die Abstraktionsebene der *kryptographischen Verfahren* (z. B. ECDSA Sign).

Wichtigste Elementaroperation ist die modulare Multiplikation, weshalb sie sich für Parallelisierung anbietet. Die erste Möglichkeit dafür ist in voller Bitbreite zu rechnen. Dazu muss die Hardware aber für die maximale Bitbreite ausgelegt sein und wegen der variablen Bitbreiten (> 100 bis mehrere 1000 Bit) bleiben Ressourcen oft ungenutzt. Die zweite Möglichkeit ist Pipelining, das dank frei wählbarer Anzahl der Stufen flexibler ist. Eine hohe Stufenzahl führt aber ebenfalls zu ungenutzten Ressourcen, da die Pipeline immer mit Bitlängen arbeitet, die einem Vielfachen ihrer Stufen in Wörtern entspricht. Einen guten Kompromiss stellen bei einer Wortlänge von 16 Bit Pipelines mit 2 oder 4 Stufen dar.

Oberhalb der modularen Arithmetik nehmen die Verfahren hauptsächlich Steueraufgaben wahr. Außerdem sind die Algorithmen (z. B. RSA, ECDSA, usw.) stark unterschiedlich. Deshalb bietet sich eine Implementierung in Software an, die für Steueraufgaben gut geeignet ist und durch die sich der Prozessor für die verschiedenen Algorithmen wiederverwenden lässt. Auf heutigen FPGAs können dazu Soft-Cores verwendet werden: Diese sind einfache Prozessoren, die aus den konfigurierbaren Elementen des FPGAs gebildet werden.

Wie oben beschrieben, ist Parallelisierung in der modularen Arithmetik nur beschränkt möglich, weshalb auch höhere Ebenen betrachtet werden sollten. Dabei beschränken jedoch Datenabhängigkeiten den Grad der Parallelisierung: Die EC Arithmetik lässt sinnvoll nur 2-3 parallele Multiplizierer zu, während die Exponentiation von RSA bis zu 2 nutzen kann. Um ungenutzte Ressourcen zu vermeiden, ist man also auf 2 Multiplizierer beschränkt und die eigentlich mögliche Parallelisierung innerhalb der EC Multiplikation entfällt. Das kryptographische Verfahren schließlich lässt sich dank fehlender Datenabhängigkeiten beliebig oft parallelisieren.



Die Abbildung zeigt vereinfacht eine mögliche Struktur für einen CoProzessor: Das IO-Modul kommuniziert mit der Außenwelt und überlässt die Ausführung der kryptographischen Verfahren den Soft-Cores. Diese verfügen je über ein Modul für modulare Arithmetik und teilen sich den Zugriff auf die weiteren Module wie AES- oder RNG-Core, da diese nicht so häufig benötigt werden.

Generatoren für echte Zufallszahlen auf FPGAs für eingebettete Systeme

Karl Tyss

Technische Universität Hamburg-Harburg, Institut für Rechnertechnologie
Schwarzenbergstrasse 95, D-21071 Hamburg, Germany

Die Entwicklung von ressourcenbeschränkten eingebetteten Systemen, wie z. B. RFID, hat dazu geführt, dass kryptografische Anwendungen immer mehr an Bedeutung gewinnen. Diese benötigen, zum generieren von Session-Keys, echte Zufallszahlen. Die Gewinnung von echten Zufallszahlen ist jedoch in der Regel mit einem hohen Aufwand verbunden, da die als Rauschquellen benutzte Hardware meist extern an die Andwendung gekoppelt oder als ein Full-Custom-Design realisiert wird. Die bei der Generierung von echten Zufallszahlen ausgenutzten physikalischen Phänomene verfügen nicht immer über die gewünschte Qualität und Stabilität. Diese Eigenschaften führen dazu, dass der Hardwareaufwand, um qualitativ hochwertige Zufallszahlen zu erzeugen, für solche Generatoren relativ hoch ausfällt. Im Fall von z. B. RFID-Anwendungen stehen aber nur wenige Hardwareressourcen zur Verfügung. Gebraucht werden deswegen vor allem Generatoren für echte Zufallszahlen, die mit wenig Hardwareressourcen auskommen und keine externe Hardware benötigen.

In meinem Vortrag werde ich Generatoren für echte Zufallszahlen vorstellen, die sich durch eine geringe Komplexität auszeichnen. Es werden eine Reihe von Zufallszahlengeneratoren, basierend auf dem Phasenrauschen von oszillierenden Schaltkreisen [1] und ihre Realisierung auf einem FPGA vorgestellt. Da diese Klasse der Zufallszahlengeneratoren sich jedoch unter gewissen Umständen als anfällig für Manipulation erweist, werden im Vortrag einige bewährte [2], [3] und neu entwickelte Methoden zur Stabilisierung der Zufallszahlengeneratoren vorgestellt und diskutiert. Als Abschluss werde ich eine Lösung vorstellen, die mit wenig Hardware auskommt, auf FPGAs realisierbar und stabil gegenüber Manipulationen ist.

Literatur

[1] Michael Epstein, Laszlo Hars, Raymond Krasinski, Martin Rosner, Hao Zheng. *Design and Implementation of a True Random Number Generator Based on Digital Circuit Artefacts.* Cryptographic Hardware and Embedded Systems – CHES 2003 5th International Workshop, Cologne, Germany, September 8-10, 2003, Proceedings Series: Lecture Notes in Computer Science, Vol. 2779, Seiten 152–165, Springer Verlag.

[2] Viktor Fischer, Miloś Drutarowský. *The True Random Number Generator Embedded in Reconfigurable Hardware.* Cryptographic Hardware and Embedded Systems – CHES 2002 4th International Workshop, Redwood Shores, CA, USA, August 13-15, 2002, Revised Papers Series: Lecture Notes in Computer Science, Vol. 2523, Seiten 415–430, Springer Verlag.

[3] Werner Schindler. *Efficient Online Tests for True Random Number Generators.* Cryptographic Hardware and Embedded Systems – CHES 2001 Third International Workshop, Paris, France, May 14-16, 2001, Proceedings Series: Lecture Notes in Computer Science, Vol. 2162, Seiten 103–117, Springer Verlag.

Starke kryptographische Algorithmen – eine hinreichende Sicherheitsanforderung?

Werner Schindler
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185–189
53175 Bonn

Kryptographische Algorithmen und Protokolle bilden den Kern zahlloser IT-Sicherheitsmechanismen. Die Sicherheit kryptographischer Mechanismen beruht normalerweise darauf, dass ein potentieller Angreifer nicht in der Lage ist, einen geheimen Schlüssel zu bestimmen. Es liegt unmittelbar auf der Hand, dass die Resistenz der verwendeten kryptographischen Algorithmen und Protokolle gegen algorithmische Angriffe unverzichtbar ist.

Andererseits geht es einem Angreifer nur um die Erlangung des gesuchten Schlüssels, und da ist ihm letztlich jedes Mittel recht, das zum Erfolg führt. So kann ein potentieller Angreifer den Speicherbereich eines PCs nach Schlüsseln durchsuchen, oder er könnte probieren, einen in einer Chipkarte gespeicherten Schlüssel durch einen direkten Angriff gegen die Hardware zu bestimmen oder nach einer Schwachstelle im Betriebssystem zu suchen. Wird zur Schlüsselerzeugung ein schwacher Zufallszahlengenerator verwendet, ermöglicht dies vielleicht das Errechnen oder das Erraten von Sessionkeys oder Signaturparametern, insbesondere wenn Vorgänger- oder Nachfolgerzufallszahlen bekannt sind.

Seitenkanalangriffe sind kombinierte Angriffe, die den kryptographischen Algorithmus nicht direkt attackieren, sondern zudem Eigenschaften der Implementierung ausnutzen. Seitenkanalangriffe werden seit etwa 10 Jahren sowohl in der Wissenschaft als auch von der Halbleiterindustrie mit großer Aufmerksamkeit verfolgt. Besonderes Interesse gilt der Entwicklung wirkungsvoller Gegenmaßnahmen. Seitenkanalangriffe richten sich in aller Regel gegen Chipkarten, aber selbst Remote-Angriffe gegen Server sind möglich.

Abhängig von ihrer Implementierung kann die Laufzeit kryptographischer Operationen von deren Input abhängen. Laufzeitangriffe versuchen, diesen Umstand auszunutzen, um aus einer Stichprobe von gemessenen Laufzeiten auf den gesuchten Schlüssel zu schließen. Die Ursache für Laufzeitunterschiede sind normalerweise laufzeitoptimierte arithmetische Algorithmen oder das Cacheverhalten. Bei Powerattacken misst der Angreifer den Stromverbrauch der Chipkarte, um hieraus sukzessiv Teile des Schlüssels zu bestimmen. Ziel eines Abstrahlangriffs ist es, an Hand der elektromagnetischen Abstrahlung zunächst die Aktivitäten auf dem Chip zu lokalisieren.

Die schlüsselabhängige, d. h. die für einen Angriff nutzbare Information, ist durch „Rauschen“ überlagert. Das gemeinsame Ziel von potentiellen Angreifern und Designern besteht darin, auf Basis von Messwerten optimale Entscheidungen zu treffen, wenngleich aus völlig unterschiedlichen Gründen: Angreifer wollen ihre Erfolgsaussichten optimieren, während ein Designer das Risikopotential eines Angriffs bzw. einer Klasse von Angriffen ausloten möchte, um zuverlässige Gegenmaßnahmen implementieren zu können. Zur Optimierung von Seitenkanalangriffen haben sich insbesondere stochastische Methoden als geeignet herausgestellt.

The eStream Project

Erik Zenner

Cryptico A/S
ez@cryptico.com

eStream is an EU-funded project on stream cipher cryptography. After its predecessor NESSIE was unable to recommend a secure stream cipher for public use, the need for additional research in the area was recognized, and the eStream project was born. Its purpose is to improve the understanding of stream cipher security and to identify a portfolio of ciphers that are both secure and resource-effective.

In May 2005, the surprisingly large number of 34 stream cipher candidates were submitted to the project. After one year of public evaluation (and the submission of 128 academic papers to the project), the organisers announced a first selection in March 2006. Currently, the project is in evaluation phase 2, where the cryptographic community is again requested to continue the demolition derby and help in identifying the most suitable cipher candidates.

In this talk, we will give an overview over the eStream project. We will point out new trends in stream cipher cryptography and discuss some of the most interesting cipher candidates. Finally, we will go into some of the more controversial selection criteria, like the comparison of security features or resource consumption.

Neue Algorithmen für die Modularmultiplikation

Viktor Bunimov

Institut für Informatik, Uni Kiel

In diesem Vortrag werden die wichtigsten Ergebnisse der Dissertation [1] aus dem Bereich der ganzzahligen Langzahlcomputerarithmetik für die Anwendungen vor allem aus dem Bereich der modernen Kryptographie vorgestellt. Alle hier behandelten Verfahren wurden weiterhin in Bezug auf eine Realisierung in Hardware optimiert.
Bei den neuen Algorithmen handelt es sich um drei neue Methoden zur Berechnung der Modularmultiplikation, die sich durch ein besonders günstiges Flächen-Zeit-Produkt auszeichnen. Dabei wird zunächst eine neue Version der Modularmultiplikation von Montgomery entwickelt, bei der die Anzahl der Additionseinheiten gegenüber den besten bisher bekannten Verfahren [2] halbiert werden kann. Danach wird die verschränkte Modularmultiplikation behandelt. Bezogen auf die derzeit als bester geltenden Version [3] kann hier die Anzahl der Additionseinheiten um einen Faktor drei reduziert werden. Der dritte Algorithmus ist ein neu entwickeltes Verfahren [4], bei dem nicht nur die Berechnungen, sondern auch die Eingaben in redundanter Form erfolgen. Dadurch kann die Umrechnung von redundanter in nichtredundante Form bei der mehrfachen Anwendung der Modularmultiplikation, wie z. B. bei der modularen Exponentiation, eingespart werden, ohne zusätzlichen Zeit- bzw. Flächenaufwand zu benötigen. Alle drei Algorithmen werden in Hinsicht auf ihre Komplexität evaluiert.

Literatur

[1] Bunimov, V.: Entwicklung von neuen Algorithmen der Computerarithmetik in Hinsicht auf ihre Nutzung in der Kryptographie, Dissertation, Kiel 2005.

[2] Kim, Y. S. Kang, W. S. Choi, J. R.: Implementation of 1024-bit modular processor for RSA cryptosystem, School of Electronic and Electrical Engineering, Kyungpook National University, 1370 Sankyok-Dong, Book-Gu, Taegu, Korea, `http://www.ap-asic.org/2000/proceedings/10-4.pdf`.

[3] Koc, C. K.: RSA Hardware Implementation, RSA Laboratories, RSA Data Security, Inc. August 1995, `http://security.ece.orst.edu/koc/papers/reports.html`.

[4] Schimmler, M., Bunimov, V.: Fast Modular Multiplication by Operand Changing. The International Conference on Information Technology ITCC 2004, pp. 518-524, April 5-7, 2004.

The SMS4 Block Cipher

Ralf-Philipp Weinmann

Technische Universität Darmstadt

The Wired Authentication and Privacy Infrastructure (WAPI) standard is a Chinese National Standard for securing Wireless LANs. It is an alternative to IEEE 802.11i which has become mandatory in China. Originally the block cipher SMS4 that is exclusively used in WAPI has been secret; however, due to non-acceptance of WAPI by the ISO standards organization, the Chinese government published the block cipher in January 2006 [1].

SMS4 is a 32 round unbalanced Feistel network [2] with a block and key size of 128 bits. It is source heavy, complete and homogeneous and uses a single 8-bit S-Box that has good differential and linear properties. The specification of the cipher is simple and clean: A C implementation of the cipher was finished in less than an hour.

In this talk we will demonstrate that the design of SMS4 is somewhat brittle: A small change in the key schedule (different key constants) yields a variant that exhibits a large class of weak keys. Furthermore we will show differential and linear attacks against reduced-round versions of this cipher.

References

[1] Specification of SMS4 (in Chinese)
`http://www.oscca.gov.cn/UpFile/200621016423197990.pdf`

[2] B. Schneier and J. Kelsey. *Unbalanced Feistel Networks and Block Cipher Design*. Fast Software Encryption 1996, Third International Workshop Proceedings (February 1996), Springer-Verlag, 1996, pp. 121–144.

On the Application of Merkle's Puzzle for Telemedicine and M-Health

Frederik Armknecht and Dirk Westhoff

NEC Europe, Network Laboratories, Heidelberg, Germany

Cryptography for networks with low-end devices is usually designed to meet the capabilities of the weakest party. At this we are aiming at low-priced, unprotected hardware with extremely limited computing and storage capabilities which makes modular arithmetic with large numbers unsuitable or even impossible. However, in several cases, the network has an asymmetric topology with a full functioning powerful device and an extremely limited device with only reduced functioning. This is for example true in telemedicine, or, more concretely, in an m-health scenario where the patient's biosensors form a network with a more powerful control node.

We argue that in these cases the well known Merkle's Puzzle [1] has its practical application and provide concrete parameter settings for specific device characteristics. As opposed to other mechanisms it takes advantage of the asymmetric topology by shifting most of the workload toward the more powerful device. The proposed solution has particular value in scenarios where security associations are required for a relatively short, but well-defined duration. Furthermore, no pre-installed secrets are required, making (often expensive) tamper resistance superfluous.

References

[1] R. C. Merkle. Secure communications over insecure channels. Communications of the ACM 21(4), pp. 294–299, ACM Press, 1978.

Dissecting Apple's FileVault

Ralf-Philipp Weinmann

Technische Universität Darmstadt

FileVault [1] is a security feature of Mac OS X that allows users to encrypt their home directories using their login passwords. Although Apple claims that security is achieved "by encrypting its entire contents using the Advanced Encryption Standard with 128-bit keys", publically available technical information publically available beyond that statement is scarce: the only other thing known is that encrypted volumes (so-called disk images) are employed. Unfortunately the source code for this part of the operating system (the DiskImages framework) is not available for inspection. This makes accessing the contents of such encrypted volumes from other operating systems such as Linux or *BSD a impossible at the moment.

This talk will show work in progress made by the author in reverse-engineering the the programs surrounding the Apple FileVault technology with the aim of creating a compatible driver for Linux. Being a cryptographer, the author also likes to second-guess the designers' choices: however, no glaring holes in the design have been discovered yet. Blocks are encrypted in CBC mode, the IV for each block is computed using an HMAC-SHA1 variant. This raises an obvious question: Why has the cryptographic design of FileVault not been opened up for peer review?

References

[1] Apple – Mac OS X – FileVault
`http://www.apple.com/macosx/features/filevault`

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 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

6. Kryptotag am 19. Februar 2007 (Einreichung: 19. Januar 2007, Anmeldung: 11. Februar 2007). Universität des Saarlandes, Information Security and Cryptography Group und Sirrix AG. Kontakt: Michael Backes und Ammar Alkassar.

Bisherige Kryptotage

5. Kryptotag am 11. September 2006. Universität Kassel, Fachbereich Mathematik/Informatik, Fachgebiet Theoretische Informatik. Kontakt: Heiko Stamer. 8 Einreichungen.
1. Kryptowochenende am 1.–2. Juli 2006. Tagungszentrum Kloster Bronnbach der Universität Mannheim. Kontakt: Frederik Armknecht und Dirk Stegemann. 14 Einreichungen und 21 angemeldete Teilnehmer.
4. Kryptotag am 11. Mai 2006. Ruhr Universität Bochum, Horst-Görtz Institut. Kontakt: Ulrich Greveler. 10 Einreichungen und 32 angemeldete Teilnehmer.
3. Kryptotag am 15. September 2005. Technische Universität Darmstadt, Theoretische Informatik. Kontakt: Ralf-Philipp Weinmann. 13 Einreichungen und 35 angemeldeten Teilnehmer.
2. Kryptotag am 31. März 2005. Universität Ulm, Abteilung für Theoretische Informatik. Kontakt: Wolfgang Lindner und Christopher Wolf. 10 Einreichungen und 26 angemeldeten Teilnehmer.
1. Kryptotag am 1. Dezember 2004. Universität Mannheim, Lehrstuhl für Theoretische Informatik. Kontakt: Stefan Lucks und Christopher Wolf. 15 Einreichungen und 37 angemeldeten Teilnehmer.

Innerhalb der Fachgruppe für Angewandte Kryptologie sind Stefan Lucks (Universität Mannheim) und Christopher Wolf (Ecole Normale Superieure, Paris) verantwortlich für die Organisation der Kryptotage. Für eventuelle Rückfragen bitte an sie wenden.