

Proceedings of the 11. Kryptotag

Workshop of the section “Angewandte Kryptographie” (applied cryptography) of the
“Gesellschaft für Informatik e.V.” (German Computer Science Society)

Chair of Information Security and Cryptography,
University of Trier

November 30, 2009



Inhaltsverzeichnis

Side Channel Analysis of AVR XMEGA Crypto Engines <i>Ilya Kizhvatov</i>	3
Light-weight Key Generation based on Physical Properties of Wireless Channels <i>Matthias Wilhelm, Ivan Martinovic, and Jens B. Schmitt</i>	4
A known plaintext cache-based attack against AES <i>Jean-François Gallais</i>	5
Übermittlung eines vertraulichen Passwortes mit Hilfe nicht kommutativer Verfahren <i>Henning Legell</i>	6
An Epistemic Approach to Coercion-Resistance for Electronic Voting Protocols <i>Ralf Küsters and Tomasz Truderung</i>	7
A Game-Based Definition of Coercion-Resistance and its Applications <i>Ralf Küsters and Tomasz Truderung and Andreas Vogt</i>	8
A Simulation-Based Treatment of Authenticated Message Exchange <i>Klaas Ole Kürtz, Henning Schnoor, and Thomas Wilke</i>	9
Computational Soundness for Key Exchange Protocols with Symmetric Encryption <i>Ralf Küsters and Max Tuengerthal</i>	10
Einsatz von Trusted Computing in der Automatisierung mit Schwerpunkt eingebettete Systeme <i>Nora Lieberknecht</i>	11

Side Channel Analysis of AVR XMEGA Crypto Engines

Ilya Kizhvatov

University of Luxembourg
Faculty of Science, Technology and Communication
6, rue Coudenhove-Kalergi
L-1359 Luxembourg

AVR XMEGA is the recent general-purpose 8-bit microcontroller from Atmel featuring symmetric crypto engines implementing DES and AES. Along with the other features, this makes XMEGA a promising device for embedded system developers. XMEGA is not claimed by Atmel to be a microcontroller for secure embedded applications. However, the presence of the crypto engines suggests that it may still be used in a such an application. Embedded applications are often subject to implementation attacks, in particular, attacks exploiting side channel leakage of the device.

In this practical work we look at the resistance of XMEGA crypto engines to side channel attacks. We reveal the relatively strong side channel leakage of the AES engine that enables full 128-bit AES secret key recovery in a matter of several minutes with a measurement setup cost about 1000 USD. 3000 power consumption traces are sufficient for the successful attack. Our analysis was performed without knowing the details of the crypto engine internals. Quite the contrary, it reveals that the implementation is not a parallelized one. We sketch other feasible side channel attacks on XMEGA and suggest the countermeasures that can raise the complexity of the attacks but not fully prevent them.

With this work we demonstrate how easy it is to attack an unprotected device with more or less standard techniques even without knowing the details of the actual implementation of the cryptographic algorithm. So care should be taken to use such devices either in a trusted environment or if the desired security level of the application is lower than the complexity of the implementation attacks.

The work was published in [Ki09].

References

- [Ki09] Ilya Kizhvatov. Side Channel Analysis of AVR XMEGA Crypto Engines. *WESS '09: Proceedings of the 4th Workshop on Embedded Systems Security*, ACM, New York, 2009.

Light-weight Key Generation based on Physical Properties of Wireless Channels

Matthias Wilhelm, Ivan Martinovic, and Jens B. Schmitt

disco | Distributed Computer Systems Lab
TU Kaiserslautern, Germany
{wilhelm,martinovic,jschmitt}@cs.uni-kl.de

Key management is at the heart of cryptography system designs, enabling and ensuring the overall security of such systems. There are a variety of cryptographic protocols to generate and distribute keying material, and in many applications these well-researched solutions offer good performance and security. However, when considering low-cost and low-performance devices such as wireless sensor motes used for distributed monitoring of the environment, common protocols can introduce too large computational burdens or implementation complexity.

A new approach first considered in the context of information theory offers a promising concept of generating secret keys from *correlated random variables* [MRW07]. Inspired by this idea, wireless communication researchers showed that the wireless channel connecting two devices can be used as a source of such random variables [MTM+08, AKM+07]. Wireless channels show a strong correlation of the channel states between sender and receiver, known as the *reciprocity* of the wireless channel. By exchanging sampling messages and measuring the received signal strength during movement, this property can be used to derive a shared bit string. This string is only known to the involved entities because the channel behavior decorrelates rapidly in space, making this scheme resistant to eavesdropping from other physical positions.

We introduce a new concept that does not rely on movement as the source of randomness, but on the *frequency-selectivity* of the wireless channel. We show by implementation in our wireless sensor network testbed that this approach can be used to successfully generate unpredictable bits, even in static scenarios, which match for Alice and Bob with a very high probability, simply by using only the communication and measurement capabilities of standard sensor mote hardware. We also show how to analyze the secrecy of our proposed key generation protocol by using an information-theoretical approach to quantify the entropy of the resulting bits.

References

- [MRW07] Ueli Maurer, Renato Renner, and Stefan Wolf. Unbreakable keys from random noise. Security with Noisy Data, Springer-Verlag, pp. 21-44, 2007.
- [MTM+08] Suhas Mathur, Wade Trappe, Narayan Mandayam, Chunxuan Ye, and Alex Reznik. Radio-telepathy: extracting a secret key from an unauthenticated wireless channel. MobiCom '08: Proceedings of the 14th ACM international conference on Mobile computing and networking, pp. 128-139, 2008.
- [AKM+07] Babak Azimi-Sadjadi, Aggelos Kiayias, Alejandra Mercado, and Bulent Yener. Robust key generation from signal envelopes in wireless networks. CCS '07: Proceedings of the 14th ACM conference on Computer and communications security, pp. 401-410, 2007

A known plaintext cache-based attack against AES

Jean-François Gallais

University of Luxembourg
Faculty of Science, Technology and Communication
6, rue Coudenhove-Kalergi
L-1359 Luxembourg

Cache memory is now widely used on various devices implementing cryptographic algorithms, including smart cards, in order to speed up the execution of the procedures. This fast storage placed between the processor and the main memory makes the data stored in the Non Volatile Memory (Flash, EEPROM...) more quickly accessible once they have been loaded into it. However, the use of a cache can possibly represent as explained here a threat to security, when the data fetched from the NVM to the cache is indexed by the bytes of the secret key.

Indeed, loading some data from the NVM into the cache takes more clock cycles and requires more energy than fetching the data from the cache. These differences of timing and energy consumption have an influence on the physical characteristics of the device while running a cryptographic primitive. As a consequence, the so-called **cache misses** (when a line of the NVM is loaded to the cache) and **cache hits** (when data is fetched right from the cache) can be distinguished on a power trace under certain conditions on the implementation and the measurement setup.

An adaptive approach taking advantage of the cache hits and misses occurring during an AES encryption has been described in [Tu06]. In the considered scenario, the `ByteSub` function is implemented as a lookup table with 256 entries, and the round keys pre-computed and pre-stored.

In this scenario, I describe here a non-adaptive approach, hence using non-chosen known plaintexts and the cache traces obtained from the power traces corresponding to the encryption of these plaintexts. This strategy allows an attacker to recover 60 bits of the target key out of 128 within a hundred acquisitions, using the first round of encryption. Without requiring any additional traces, this analysis may also be extended to the second round of encryption, hence allowing the recovery of the full AES key.

References

[Tu06] [Tu06] J. Fournier, M. Tunstall *Cache Based Power Analysis Attacks on AES*, ACISP 2006.

Übermittlung eines vertraulichen Passwortes mit Hilfe nicht kommutativer Verfahren

Henning Legell

Hamburg

Die Verfahren, welche sich auf das “no-key-protocol” von Shamir beziehen, erfordern für die Realisierung Algorithmen, die bezüglich der Hintereinanderausführung kommutativ sind. Kommutative Methoden sind in der Regel einfach und bieten beim 3-Wege-Verfahren nach Shamir keine Sicherheit. Die Umsetzung der Idee mit Hilfe großer Primzahlen verwendet auch einen kommutativen Algorithmus. Nur weil die Berechnung des diskreten Logarithmus für große Zahlen eine mathematische Herausforderung ist, stellt diese Methode eine ausreichende Sicherheit dar. Das hier vorgestellte 3-Wege-Verfahren greift auf nicht kommutative Algorithmen zurück. Es ist schnell, unkompliziert und sicher, weil es als perfektes System ausgeführt werden kann. Die Einzelheiten des Verfahrens sollen bei dieser Vorstellung nicht dargestellt werden. Jeder Interessent erhält aber eine zeitlich eingeschränkt lauffähige Programmversion, für ausführliche Tests.

An Epistemic Approach to Coercion-Resistance for Electronic Voting Protocols

Ralf Küsters and Tomasz Truderung

University of Trier

Germany

`{kuesters,truderun}@uni-trier.de`

Coercion resistance is an important and one of the most intricate security requirements of electronic voting protocols. Several definitions of coercion resistance have been proposed in the literature, including definitions based on symbolic models. However, existing definitions in such models are rather restricted in their scope and quite complex.

In this paper, we therefore propose a new definition of coercion resistance in a symbolic setting, based on an epistemic approach. Our definition is relatively simple and intuitive. It allows for a fine-grained formulation of coercion resistance and can be stated independently of a specific, symbolic protocol and adversary model. As a proof of concept, we apply our definition to three voting protocols. In particular, we carry out the first rigorous analysis of the recently proposed Civitas system. We precisely identify those conditions under which this system guarantees coercion resistance or fails to be coercion resistant. We also analyze protocols proposed by Lee et al. and Okamoto.

A Game-Based Definition of Coercion-Resistance and its Applications

Ralf Küsters and Tomasz Truderung and Andreas Vogt

University of Trier

Germany

`{kuesters, truderun, vogt}@uni-trier.de`

Coercion-resistance is one of the most important and intricate security requirements for voting protocols. Several definitions of coercion-resistance have been proposed in the literature, both in cryptographic settings and more abstract, symbolic models. However, unlike symbolic approaches, only very few voting protocols have been rigorously analyzed within the cryptographic setting. A major obstacle is that existing cryptographic definitions of coercion-resistance tend to be complex and limited in scope: They are often tailored to specific classes of protocols or are too demanding.

In this paper, we therefore present a simple and intuitive cryptographic definition of coercion-resistance, in the style of game-based definitions. This definition allows to precisely measure the level of coercion-resistance a protocol provides. As the main technical contribution of this paper, we apply our definition to two voting systems, namely, the Bingo voting system and ThreeBallot. The results we obtain are out of the scope of existing approaches. We show that the Bingo voting system provides the same level of coercion-resistance as an ideal voting system. We also precisely measure the degradation of coercion-resistance of ThreeBallot in case the so-called short ballot assumption is not met and show that the level of coercion-resistance ThreeBallot provides is significantly lower than that of an ideal system, even in case of short ballots.

A Simulation-Based Treatment of Authenticated Message Exchange

Klaas Ole Kürtz, Henning Schnoor, and Thomas Wilke

AG Theoretische Informatik, Institut für Informatik, Christian-Albrechts-Universität zu Kiel

Simulation-based security notions for cryptographic protocols are regarded as highly desirable, primarily because they admit strong composability and, consequently, a modular design. We give a simulation-based security definition for two-round authenticated message exchange and show that a concrete protocol, 2AMEX-1, satisfies our security definition.

Over the last years, a variety of cryptographic primitives, such as asymmetric encryption and digital signatures, have been treated following the simulation-based approach. There are, however, only few complex cryptographic protocols that have been tackled within the simulation-based framework, for instance, Kerberos and the Yahalom protocol.

We analyze the situation of 2AMEX-1, a two-round authenticated message exchange protocol which is a generic protocol reflecting the authentication mechanisms for web services discussed in various standardization documents. It consists of only a single client request and a subsequent server response and works under the realistic assumptions that the responding server is long-lived, has bounded memory, and may be reset occasionally.

The protocol was introduced and proven secure in a Bellare-Rogaway style framework in [1]. It is complex in several respects: it distinguishes between short-lived clients and long-lived servers; it requires only bounded memory; it uses digital signatures and therefore makes use of a public-key infrastructure; it uses nonces and timestamps to counter replay attacks; each client and each server has its own local clock.

To analyze this protocol in the simulation-based setting, we (i) provide an ideal functionality for two-round authenticated message exchange, (ii) provide an implementation corresponding to 2AMEX-1, and (iii) prove the implementation of 2AMEX-1 to be secure.

Several simulation-based approaches have been developed over the last decade, see, for instance, [2, 3, 4, 5]. We could have used any of these approaches, but we have adopted the one by Küsters because it provides a very flexible addressing mechanism and easy-to-use joint-state theorems.

References

- [1] Kürtz, K.O., Schnoor, H., Wilke, T.: Computationally secure two-round authenticated message exchange. Cryptology ePrint Archive, Report 2009/262 (2009) <http://eprint.iacr.org/>.
- [2] Canetti, R.: Universally composable security: A new paradigm for cryptographic protocols. In: FOCS. (2001) 136–145
- [3] Pfitzmann, B., Waidner, M.: A model for asynchronous reactive systems and its application to secure message transmission. In: IEEE Symposium on Security and Privacy. (2001) 184–201
- [4] Backes, M., Pfitzmann, B., Waidner, M.: A general composition theorem for secure reactive systems. In Naor, M., ed.: TCC. Volume 2951 of LNCS, Springer (2004) 336–354
- [5] Küsters, R.: Simulation-based security with inexhaustible interactive Turing machines. In: CSFW, IEEE Computer Society. (2006) 309–320

Computational Soundness for Key Exchange Protocols with Symmetric Encryption

Ralf Küsters and Max Tuengerthal

University of Trier

Germany

`{kuesters,tuengerthal}@uni-trier.de`

Formal analysis of security protocols based on symbolic models has been very successful in finding flaws in published protocols and proving protocols secure, using automated tools. An important question is whether this kind of formal analysis implies security guarantees in the strong sense of modern cryptography. Initiated by the seminal work of Abadi and Rogaway, this question has been investigated and numerous positive results showing this so-called computational soundness of formal analysis have been obtained. However, for the case of active adversaries and protocols that use symmetric encryption computational soundness has remained a challenge.

In this work, we show the first general computational soundness result for key exchange protocols with symmetric encryption, along the lines of a paper by Canetti and Herzog on protocols with public-key encryption. More specifically, we develop a symbolic, automatically checkable criterion, based on observational equivalence, and show that a key exchange protocol that satisfies this criterion realizes a key exchange functionality in the sense of universal composability. Our results hold under standard cryptographic assumptions.

Einsatz von Trusted Computing in der Automatisierung mit Schwerpunkt eingebettete Systeme

Nora Lieberknecht

FZI Forschungszentrum Informatik an der Universität Karlsruhe
Embedded Systems and Sensors Engineering (ESS)
Haid-und-Neu-Str. 10-14, D-76131 Karlsruhe, Germany
`lieberknecht@fzi.de`

Vor dem Hintergrund der zunehmenden Produktpiraterie in der Investitionsgüterindustrie wird in der Automatisierungsbranche der Ruf nach effizienten Software- und Datenschutzmaßnahmen lauter. Neben gefälschten Ersatzteilen und dem Nachbau komplexer Gesamtanlagen werden von Produktpiraten auch Software (z.B. aufwändige Maschinensteuerungsprogramme) und Produktionsdaten von Originalmaschinen auf Nachbauten kopiert, manipuliert oder zur unerlaubten Mehrproduktion von Waren für den Schwarzmarkt genutzt.

Um dies effizient verhindern zu können und das in Software und Daten steckende Know-How und geistige Eigentum der Maschinenhersteller vor Produktpiraten und Wettbewerbern zu schützen, werden verschiedene Schutzmechanismen benötigt, die u.a. das unberechtigte Auslesen oder Kopieren von Daten und Programmcode von einer Maschine verhindern, sichere Programm-Updates ermöglichen und die Integrität eines aus Hardware und Software bestehenden Gesamtsystems sicherstellen.

Bereits seit einigen Jahren gibt es das von der Trusted Computing Group (TCG) entwickelte Konzept des „Trusted Computings“ zur Erhöhung der Sicherheit und Vertrauenswürdigkeit von IT-Systemen. Grundlage dieses Konzepts ist ein spezieller Chip, das sogenannte Trusted Platform Module (TPM)[Gro07a], das verschiedene kryptographische Funktionen erfüllt und u.a. als Schlüsselgenerator und sicherer Schlüsselspeicher dient. Darüber hinaus kann es zur eindeutigen Identifikation einer Plattform, zur Sicherstellung der Plattformintegrität sowie zur Bindung von Software und Daten an eine bestimmte Plattform verwendet werden.

Schwerpunkt meiner Arbeit ist die Realisierung verschiedener Softwareschutzmechanismen auf in der produzierenden Industrie üblichen Plattformen mit Hilfe von TPMs. Der Fokus liegt dabei auf leistungsschwachen Embedded Systemen mit begrenzter Speicher- und Rechenkapazität. Diese haben häufig kein Betriebssystem, das den Zugriff auf das TPM regelt und keinen TPM Softwarestack [Gro07b], der eine einfache Einbindung der TPM-Funktionen in eigene Anwendungen ermöglicht.

Das Trusted Computing Konzept muss daher an die technischen Gegebenheiten von Embedded Plattformen angepasst und die Nutzung des TPMs in die bestehenden Software-Entwicklungsprozesse integriert werden [Kin06].

Literatur

[Gro07a] Trusted Computing Group. TPM Specification. Version 1.2. rev.103, 2007.

[Gro07b] Trusted Computing Group. TSS Specification. Version 1.2., 2007.

[Kin06] Steven Kinney. *Trusted Platform Module Basics: Using TPM in Embedded Systems (Embedded Technology)*. Newnes, 2006.

<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

12. Kryptotag voraussichtlich Anfang 2010, Universität Karlsruhe.

Bisherige Kryptotage

11. Kryptotag 30. November 2009, Universität Trier.

Kontakt: Ralf Küsters und Andreas Vogt.

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: MMarkus 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 für 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 (Universität Mannheim) und Christopher Wolf (K.U.Leuven, Belgien) verantwortlich für die Organisation der Kryptotage. Für eventuelle Rückfragen bitte an sie wenden.