Ein mathematischer Zugang zum Design und zur Analyse von effizienten kryptografischen Bausteinen

A Mathematical Approach for Designing and Evaluating Fast Cryptographic Primitives

Vincent Rijmen, Mario Lamberger

Vincent Rijmen arbeitet am Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie (IAIK). Seine Forschungsinteressen sind das Design, die Analyse und die Implementierung von schnellen Algorithmen in der Symmetrischen Kryptografie.

Vincent Rijmen is with the Institute for Information Processing and Communications Technology. He is interested in the design, evaluation and implementation of fast symmetric algorithms.

„Ambient Intelligence", „Internet der Dinge" oder „Smart Dust" sind unterschiedliche Bezeichnungen für ein und dieselbe Entwicklung, nämlich die Verschmelzung von Informationstechnologie mit immer mehr Bereichen unseres täglichen Lebens. Der Übergang zu einem digitalen Alltag bringt ganz neue Herausforderungen. Abgesehen von den bekannten Sicherheitsbedrohungen wie Viren, Phishing und Spam gibt es noch weitere unangenehme Nebenerscheinungen der neuen Technologien.

Ein herkömmlicher RFID-Transponder sendet seine gespeicherte Information an alle in der Nähe befindlichen Lesegeräte aus und kann somit missbraucht werden, um jemanden auszuspionieren. Jede digitale Transaktion hinterlässt Spuren, die in riesigen Datenbanken gespeichert werden, woraus mit statistischen Analysen auf unsere Vorlieben und Verhaltensweisen für Marketingzwecke geschlossen werden kann. Als Gegenmaßnahmen für derartige Bedrohungen stehen uns kryptografische Techniken wie Verschlüsselung, Authentifizierung oder Hash-Funktionen zur Verfügung. Bei der Verschlüsselung gibt es auf der einen Seite Algorithmen wie z. B. RSA, die auf zahlentheoretischen Grundlagen basieren. Diese sichern jedoch in der Praxis nur ca. ein Prozent der eigentlichen Daten. Auf der anderen Seite stehen Algorithmen wie der Data Encryption Standard (DES) und der Advanced Encryption Standard (AES). Diese Algorithmen sind bis zu 10.000-mal schneller als RSA, bauen jedoch auf einem weniger starken mathematischen Fundament auf. Unsere Forschung zielt darauf ab, dieses Fundament zu stärken. Wir wollen das an zwei konkreten Beispielen demonstrieren.

AES

Eine große Gefahr für industrielle kryptografische Applikationen stellen sogenannte „Seitenkanalan-

Ambient Intelligence, the Internet of Things, Smart Dust, ... are different names for the same type of development, namely that digital information processing is entering into more and more aspects of daily life. The transition to the digital economy raises increasing challenges for privacy, security, financial regulation, and intellectual property. Apart from the well-known computer viruses, spam and phishing emails, there are also more subtle threats.

For instance, RFID labels continuously broadcasting data to all listeners, thus allowing people to track all our moves. Every digital transaction leaves traces which are collected in large databases on which data mining techniques are unleashed in order to analyze our daily behavior and our reactions to various marketing techniques, etc.

The only way to counter or moderate these threats is by using cryptographic operations such as encryption, authentication and hashing. While there exist cryptographic operations, e.g. RSA, which are based on strong mathematical foundations, due to their slowness they protect in practice less than one percent of digital data. The vast majority of the data is secured by cryptographic algorithms like the Data Encryption Standard (DES) or the Advanced Encryption Standard (AES), which are up to 10000 times faster than RSA but have a lesser mathematical underpinning. In our research we aim to provide a mathematical framework for the design and evaluation of modern, fast cryptographic operations. Two specific testbeds are being used.

AES

An important threat to commercial cryptographic applications is posed by side-channel attacks, where an attacker measures the electro-magnetic

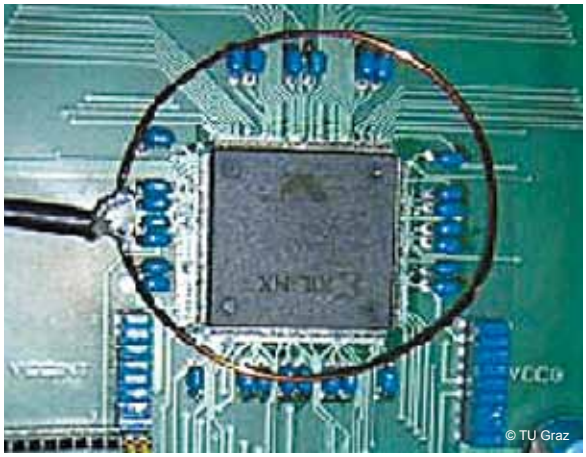

Abb. 1: Messung der elektromagnetischen Abstrahlung bei einer Smartcard mit dem Ziel, den geheimen Schlüssel herauszufinden.

Fig. 1: Electro-magnetic radiation measurement in order to determine the secret key from a smartcard.

griffe“ dar, bei denen ein Angreifer die elektromagnetische Abstrahlung misst, die z. B. eine Smartcard während einer kryptografischen Berechnung verursacht. Der momentane Grad der Abstrahlung steht in engem Zusammenhang mit der durchgeführten Operation und den verarbeiteten Daten. Dies ermöglicht dem Angreifer Rückschlüsse auf den geheimen Schlüssel, der auf diesem Chip gespeichert ist.

Im Rahmen unserer Forschung haben wir mithilfe von „Secret-Sharing“ eine Methode entwickelt, die Seitenkanalattacken vorbeugt. Dabei werden die Daten in drei oder mehrere Teile aufgeteilt, und der Chip arbeitet unabhängig mit diesen „Shares“, aus denen sich jedoch keine Rückschlüsse auf den eigentlichen Schlüssel ziehen lassen. Die Herausforderung bei dieser Methode ist, für eine Verschlüsselungsoperation jene Boole‘schen Funktionen zu finden, die aus den Input-Shares die korrekten Output-Shares berechnen.

Hash-Funktionen

Wann immer ein Dokument digital signiert wird, wird zuerst eine Hash-Funktion auf das Dokument angewandt, um die Daten zu einem digitalen „Fingerabdruck“ zu komprimieren. Aus Performancegründen wird in der Praxis nur dieser Hash-Wert signiert. Ein Sicherheitsproblem in einer Hash-Funktion hat somit gravierende Auswirkungen auf das zugehörige Signaturschema und die daran hängenden Applikationen sowie deren rechtliche Grundlagen (Signaturgesetz, E-Government-Gesetz).

Die US-Behörde NIST (National Institute of Standards and Technology) veranstaltet aktuell einen Wettbewerb mit dem Ziel, den neuen Hash-Standard SHA-3 zu finden. 64 unterschiedliche Designs wurden bis Oktober 2008 als Kandidaten für SHA-3 eingereicht. Ca. ein Drittel dieser Hash-Designs nutzt Teile des AES zur Konstruktion. Dabei konnten wir zeigen, dass ein einfaches blindes

radiation produced by a smartcard during the execution of a cryptographic operation. Because the instant amount of radiation is correlated to the operation being performed and to the logical values that are being processed, it is often possible to determine in this way the secret key used by the chip.

We developed a method based on secret-sharing techniques that counters side-channel attacks. In our method, the sensitive data is never present “in the clear” on the chip. Instead, the data is divided into three or more shares which are all perfectly uncorrelated to the sensitive data and which are processed independently. The consequence is that an attacker may be able to correlate the radiation of the chip to a share, but this doesn’t help to obtain the sensitive data. The research task here is to derive the Boolean functions that are to be applied on the shares of the input in order to obtain the shares of the correct output. Although the mathematical structure of AES facilitates this task, we are still looking for a solution that leads to a good performance at an acceptable cost in hardware.

Hash Functions

Every time a document is signed by means of a digital signature, firstly a hash function is used to compress the document to a “fingerprint.” For performance reasons, the real signature is made on the fingerprint of the document only. Consequently, every new result on the security level of hash functions has a big impact on electronic signature laws and applications, e-government and e-commerce.

The (US) National Institute for Standard and Technology (NIST) is currently running the international SHA-3 competition in order to obtain a new standard hash function. 64 submissions entered the competition in October 2008. Approximately one third of the submissions use (parts of)

Mario Lamberger arbeitet am Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie (IAIK). Sein Forschungsschwerpunkt liegt auf der mathematischen Analyse von Hash-Funktionen und Blockchiffren.

Mario Lamberger is with the Institute for Information Processing and Communications Technology. His interests are the mathematical analysis of symmetric primitives.

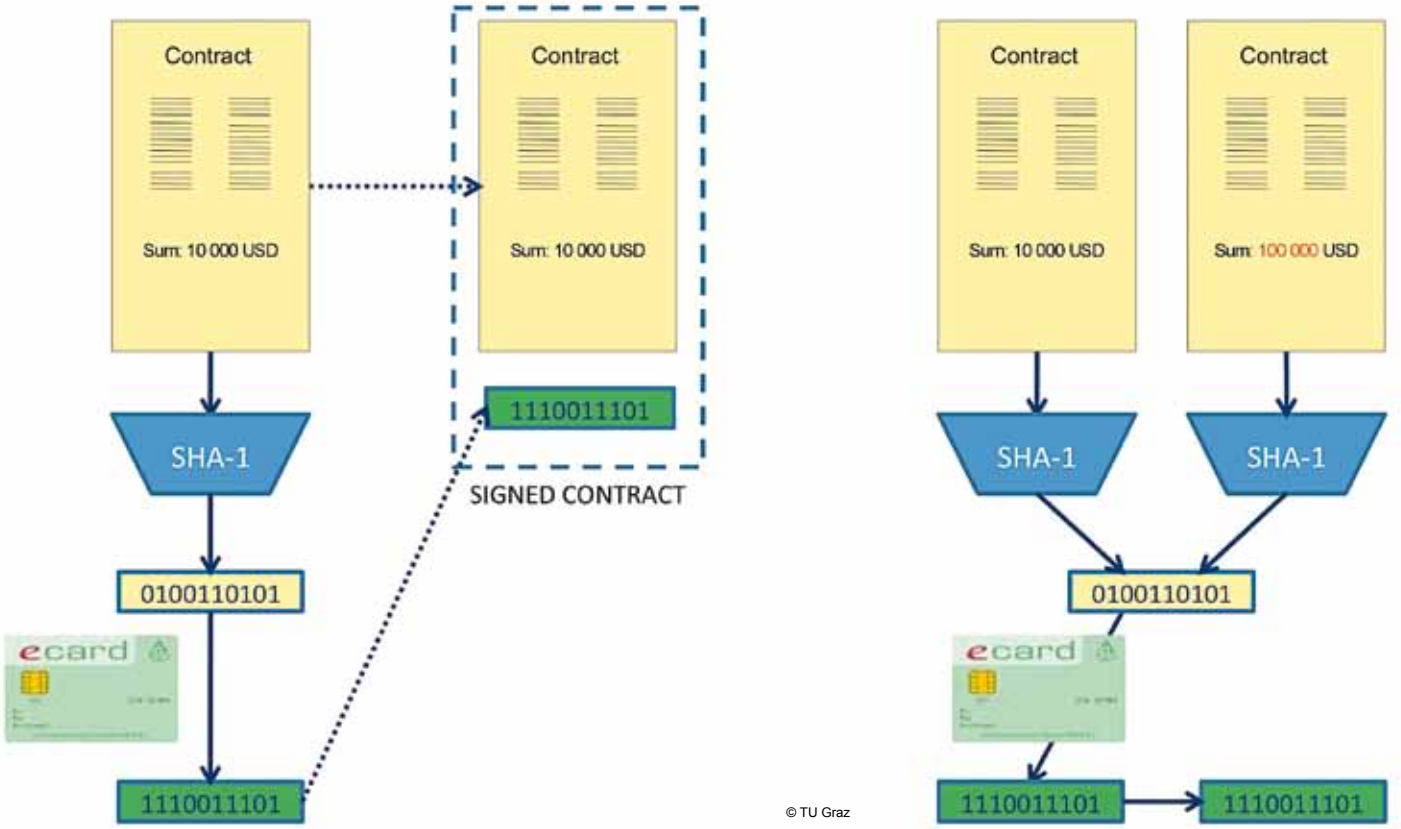

Abb. 2: Der Hash-Wert eines digitalen Vertrags wird eruiert, danach wird die Signatur berechnet (links). Haben zwei Verträge denselben Hash-Wert, sind auch ihre Signaturen gleich: Wenn man einen der Verträge signiert, gilt diese Signatur auch für den anderen (rechts).

Fig. 2: A digital contract is hashed before the digital signature is applied (left). If two different contracts hash to the same value, then their signatures are identical. If you sign one of the contracts, then your signature can be copied onto the other contract (right).

Kopieren der Bausteine des AES zu Sicherheitsproblemen führt. Der bessere Zugang ist es, die gesamte Design-Strategie, die hinter dem AES steht, in Richtung der neuen Anforderungen bei Hash-Funktionen zu adaptieren. Diese Strategie verfolgte das Design-Team der Hash-Funktion „Groestl“, das aus Forscherinnen und Forschern der TU Graz (IAIK) und der Danish Technical University (DTU) besteht. „Groestl“ befindet sich unter den verbleibenden 5 Finalisten im SHA-3-Wettbewerb.

Darüber hinaus haben wir neue mathematische Methoden für die Analyse von Hash-Funktionen entwickelt und diese dazu benutzt, Schwächen in einer Vielzahl von SHA-3-Kandidaten nachzuweisen. Durch den Zusammenhang von gewissen Schwachstellen in einer Hash-Funktion und der Existenz von Code-Wörtern mit geringem Hamming-Gewicht in speziellen linearen Codes wurden automatisierte Tools entwickelt, die die Suche nach diesen Schwachstellen erheblich vereinfachen. Momentan untersuchen wir sogenannte „Covering codes“ auf ihre Anwendbarkeit zur Verbesserung von Attacken auf Hash-Funktionen.

the AES in order to combine security with a high performance. We have shown, however, that blindly copying elements quite often leads to weaknesses. A much better approach is to reuse the AES design strategy and to adapt the components to the new requirements that are posed by the new application. This approach was followed by a joint team of researchers from IAIK and the Danish Technical University (DTU) when they developed the hash function Groestl, which is one of the 5 currently remaining finalists in the SHA-3 competition.

Furthermore, we developed new mathematical methods for the cryptanalysis of hash functions, and used them to break several of the SHA-3 submissions. By linking certain weaknesses in a hash function design to the existence of low-weight code words in a linear code derived from the hash function description, we were able to develop tools that automatically detect this type of weaknesses. Currently, we are exploring the use of covering codes in order to speed up attacks against hash functions.