Dipl.-Ing. Manfred Aigner
Institut für Angewandte Informationsverarbeitung
und Kommunikationstechnologie
E-Mail: manfred.aigner@iaik.tugraz.at
Tel.: 0316 873 5516

Smartcards und sichere RFID Tags

Smartcards and Secure RFID Tags

Meine Entscheidung zum Telematikstudium nach dem Einstieg ins Berufsleben als HTL Absolvent war zufällig. Vom normalen Arbeitalltag in einem Rechenzentrum einer großen Bank eher gelangweilt, beschloss ich meine berufliche Karriere zum Zwecke des Studiums zu unterbrechen. Durch ein Projekt am IAIK wurde ich das erste Mal mit dem Thema „IT-Sicherheit" konfrontiert, welches mich seitdem beschäftigt. Genauer gesagt die sichere Implementierung von kryptographischer Hardware in integrierten digitalen Schaltungen.

Schon im Rahmen meiner Diplomarbeit beschäftigte ich mich mit der Umsetzung eines Verschlüsselungsalgorithmus (DES – Data Encryption Standard) für Chipkarten. Speziell die enge Zusammenarbeit mit anderen Universitäten und Firmen im Rahmen eines EU-Projektes, war neben der technischen Herausforderung für mich besonders interessant. Nach einem Studienaufenthalt in Spanien war ich in einigen weiteren Projekten mit Firmenkooperationen am Institut für angewandte Informationsverarbeitung und Kommunikationstechnologie (IAIK) in der Hardwaregruppe tätig. In allen Projekten ging es um Implementierungen von kryptographischen Algorithmen für Smartcards, die teilweise fast direkt in kommerziellen Produkten eingesetzt wurden.

Im Jahr 2002 wurde mir die Leitung der Gruppe VLSI und Security am IAIK übertragen. Die Koordination der Gruppe nimmt einiges an Zeit für „nichttechnische" Aufgaben in Anspruch, was ich jedoch vor allem aufgrund der engen Zusammenarbeit mit Forschungspartnern von anderen Universitäten und Firmen als Bereicherung betrachte. Die Gradwanderung zwischen akademischer Forschung und kommerzieller Verwertung der Ergebnisse mit Firmenpartnern ist immer wieder spannend zu erleben.

Unsere Spezialisierung hat sich in den Jahren meiner Mitwirkung stark gewandelt. Zum Anfang meiner Tätigkeiten am Institut waren die Herausforderungen im Entwurf von kryptographischer Hardware auf Chipkarten vor allem die sehr begrenzte Chipfläche, die für die durchaus komplexen Berechnungen zur Verfügung stand. Aufgrund der kleineren Halbleiterstrukturen auf integrierten Schaltungen lassen sich nun viel komplexere Schaltungen auf Chipkarten implementieren und damit stellt die Größe unserer Entwürfe oftmals nicht das Hauptproblem dar.

Eines dieser neuen Probleme sind die sehr restriktiven Anforderungen für den Stromverbrauch von kontaktlosen Chipkarten und RFID Tags. Bislang wurde in low-cost RFID Systemen gänzlich auf Datenschutz verzichtet, weil man der Meinung war, dass der Einsatz von kryptographischen Algorithmen ohne Reduktion der Reichweite technisch nicht möglich sei. In einem von mir koordinierten Forschungsprojekt wurde ein Chip-Prototyp gefertigt, der bislang die weltweit kleinste und verbrauchärmste Implementierung des AES (Advanced Encryption Standard) darstellt und die äußerst restriktiven Anforderungen von passiven Longe-Range RFID Systemen deutlich unterbietet.

Ein weiteres sehr wichtiges Thema stellen aktuell sog. Seitenkanalattacken dar. Um diese sehr effektiven Attacken durchzuführen, misst der Angreifer während der kryptographischen Operation Seitenkanalinformation, z.B. den Stromverbrauch, und verwendet statistische Methoden um damit den auf der Karte gespeicherten Schlüssel zu berechnen. Aktuelle Chipkarten sind durch verschiedene Gegenmaßnahmen gegen solche Attacken gut geschützt, die Implementierung dieser Gegenmaßnahmen in Entwurf und Produktion ist jedoch im Vergleich zu ungeschützten Schaltungen sehr teuer. Ich bin derzeit wissenschaftlicher Leiter eines EU-Projektes mit 9 Partnern aus ganz Europa, welches sich damit befasst diese Gegenmaßnahmen effizienter zu implementieren. Obwohl wir im Zuge unseres Projektes sehr gute Fortschritte gemacht haben, wird uns das Thema sicher noch weiter beschäftigen, bis eine optimale Lösung für den kommerziellen Einsatz in Sicht ist. Bislang konnten wir als Ergebnis des 2 ½ jährigen Projektes einen Prototypenchip implementieren, der eine unsicher Referenzimplementierung und sieben verschiedene Varianten von geschützten Implementierungen eines Mikroprozessors beinhaltet. Dieser Prototyp stellt eine wichtige Basis für weiterführende Forschungen dar (siehe Abb. 1).

Für spannende Themen in der nahen Zukunft ist bereits gesorgt. Noch diesen Sommer werden wir mit drei neuen Projekten im Bereich sicherer RFID Technologie beginnen. Mein derzeitiger Tätigkeitsbereich umfasst state-of-the-art Forschung und Koordination sowohl intern als auch in internationalen Konsortien. Ständig neue Herausforderungen in einem sich schnell wandelnden Forschungsgebiet sorgen für viel Abwechslung und Spannung. Ich denke deshalb, dass mein Entschluss zum Studium vor einigen Jahren die Richtige Entscheidung für mich war.
http://www.iaik.at

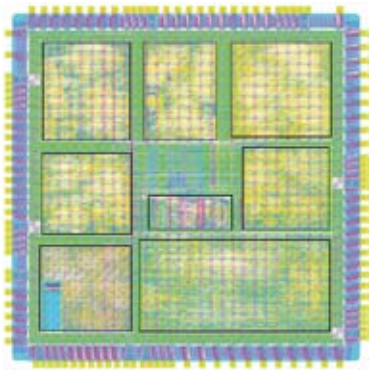

Abb. 1: (scard-chip.tif) Layout des SCARD Chips

Smartcards and Secure RFID Tags

My first contact with crypto algorithms and their efficient implementation in silicon was during my master thesis that I performed at the Institute for Applied Information Processing and Communications (IAIK). Already at that time I was very pleased that the research was performed in an international research framework. After finishing my studies I stayed with IAIK and worked in various projects that dealt with crypto-implementation for smart cards. Some of our results were nearly directly exploited in commercial products. In 2002 I became the coordinator of the research group VLSI and Security at IAIK. Our major research topics are still the specialized hardware implementations of cryptographic algorithms and protocols. Currently we are heavily involved in research projects dealing with secure RFID technology and side-channel analysis resistant smart cards. Currently I'm scientific leader of a European project with 9 partners from academia and industry. New challenges for the future are already approaching. This summer we will start with three international projects in the area of secure RFID technology, where we will deal with implementation of encryption hardware in extremely low power environments, e.g. for passively powered long range RFID tags.