Fälschungssichere Chips

Zum Schutz vor Plagiaten entwickelten Forscher des Fraunhofer-Instituts für Sichere Informationstechnologie (SIT) fälschungssichere Chips, deren Prinzip dem eines digitalen Fingerabdrucks ähnelt.

Produktplagiate verursachen einen enormen finanziellen Schaden, nicht nur in der Konsumgüterbranche, sondern auch in der Industrie. In vielen Bereichen wie Auto- oder Flugzeugbau können Plagiate gefährlich werden. Produktfälschern gelingt es, mit modernsten Analysemethoden Sicherheitsschlüssel auszuspionieren.

Ein neues Prinzip, das dem eines digitalen Fingerabdrucks ähnelt, soll den Produktpiraten das Fälschen erschweren. Bei Mikrochips gibt es minimale Unterschiede in der Dicke und Länge ihrer Leiterbahnen – das nutzen die Forscher. Das Taktsignal vieler Oszillatoren in einem Chip gibt über genaue Materialeigenschaften Auskunft und führt über eine Messschaltung zu einem spezifischen Schlüssel.

Forscher des *Fraunhofer-Instituts für Sichere Informationstechnologie (SIT)* in München beschäftigen sich mit der Implementierung in die Praxis, Weiterentwicklung und Analyse dieser Technologie. „Wie ein Mensch einen einzigartigen Fingerabdruck hat, so sind auch Mikrochips einzigartig“, erläutert Dominik Merli, Entwickler des Prototypen. „Diese Einzigartigkeit entsteht beim Menschen durch Merkmale der Hautoberfläche, bei den Chips steckt sie in Variationen der verwendeten Materialien und Strukturen.“

Ein Beispiel dafür sind die Leiterbahnen in einem Chip. Sie sind sehr klein, aber ihre Geometrie wie Länge, Breite und auch ihre Materialdichte unterliegen statistischen Variationen.

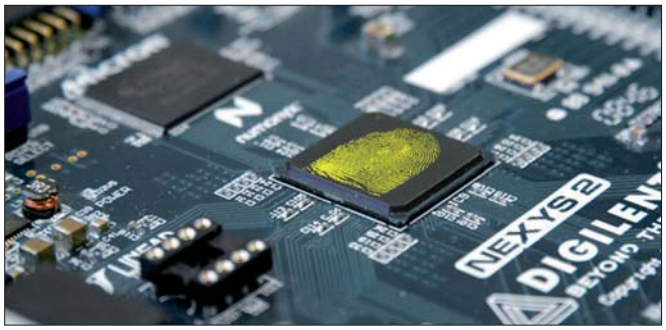

Foto: SIT (Symbolbild)

Das Prinzip des fälschungssicheren Chips ähnelt dem eines digitalen Fingerabdrucks.

Diese Eigenschaften sind bei jedem Chip zufällig und einzigartig und es ist nicht möglich, einen zweiten Chip mit identischen Merkmalen herzustellen. Auch andere Materialeigenschaften erlauben den Schutz von Mikrochips, etwa auf Basis kleiner Partikel, die mit einem Laser angeregt werden und dadurch ein einzigartiges Schattenmuster erzeugen.

Funktion. „Bei unserem Prototyp messen wir die Materialeigenschaften mit Hilfe von Ringoszillatoren. Das kann man sich wie ein Signal vorstellen, das im Kreis läuft“, erklärt Merli. „Je nach Materialabweichungen kann sich das Signal schneller oder langsamer bewegen. Dadurch entstehen höhere oder niedrigere Frequenzen, die wir im Chip messen.“

Wenn man eine größere Anzahl dieser Ringoszillatoren miteinander vergleicht, lässt sich ein binärer „Fingerabdruck“ ableiten. Diese Bit-Folge kann verwendet werden, um einen Schlüssel zu generieren, der nur in der Struktur „gespeichert“ ist. Somit kann er nicht mit invasiven Methoden ausgelesen werden, da diese die Struktur verändern und dadurch das Geheimnis zerstören würden. *Die Physical Unclonable Function (PUF)* wird in einen Chip integriert oder in einem *Field Programmable Gate Array (FPGA),* einem integrierten Schaltkreis implementiert.

Die Einsatzgebiete sind vielfältig. Mögliche Produkte sind alle Arten von Smartcards wie Bankkarten, Zutrittssysteme usw., ebenso programmierbare Hardware (FPGAs-Bausteine), die unter anderem für Steuerungen oder im Automobil eingesetzt wird. Auch Sicherheitschips in RFID-Etiketten könnten damit abgesichert werden. PUFs ermöglichen jedenfalls einen starken Produktschutz.

Entwicklung. „Bei den fälschungssicheren Chips handelt sich noch um eine Technologie, die erstmals 2002 in der Wissenschaft vorgeschlagen wurde und seitdem ständig analysiert und weiterentwickelt wird. Es gibt viele verschiedene Umsetzungen dieser Technologie“, sagt Merli. Einige Unternehmen bieten das PUF-Know-how bereits kommerziell an: *Verayo* aus den USA und die Philips-Ausgründung *Intrinsic ID*. Die niederländische Firma *NXP* hat angekündigt, in der nächsten Smartcard Generation PUFs zu integrieren.“

Bei der Forschung im Bereich Sicherheits-Chips gibt es noch viel zu tun. „Wir beschäftigen uns mit der Verbesserung und praktischen Umsetzung der vorgeschlagenen Ideen. Eine Hauptaufgabe sehen wir auch in der Analyse der Sicherheitseigenschaften von PUFs“, betont Merli. Jede Art von eingebettetem System könnte davon profitieren und Mikrochips bzw. FPGAs mit PUFs einsetzen.

Vom 1. bis 3. März 2011 zeigten die Experten auf der „Embedded-World“-Messe in Nürnberg FPGA-Boards, die mit einem Ringoszillator einen individuellen kryptografischen Schlüssel generieren können. Damit lassen sich angriffsresistente Sicherheitslösungen in eingebetteten Systemen umsetzen. Viele technisch interessierte Messebesucher waren fasziniert, dass die Einzigartigkeit von Mikrochips messbar und verwendbar ist.

Aus der Industrie war Interesse zu der FPGA Lösung zu erkennen, da einige Hersteller von eingebetteten Systemen keine eigenen Chips produzieren, aber FPGAs einsetzen.

„Da wir ein weitaus breiteres Spektrum an Produktschutz-Maßnahmen anbieten, PUFs sind nur eine spezielle Lösung für den High-Security Bereich, konnten wir auch reges Interesse an Produktschutz allgemein feststellen, da viele Branchen direkt oder indirekt bereits Probleme mit Plagiaten haben“, betont Merli. „Es waren viele Branchen vertreten wie beispielsweise Mess-, Steuer- und Regelungsmodule für Industrieanlagen.“

Sonja Berger