

Physik | Technologie-Angebot

Verfahren und Vorrichtung zur Erzeugung von reproduzierbaren geheimen Schlüsseln in lithographischen Herstellungsprozessen

Marktlücke

Die Innovation zur Verschlüsselung besteht darin, dass sie ohne die Speicherung oder Weitergabe von geheimen Schlüsseln auskommt und das Verfahren somit ein neues Maß an Sicherheit bietet.

Herkömmliche Methoden der Verschlüsselung erzeugen einen geheimen Schlüssel über einen Zufallsgenerator und speichern diesen Schlüssel innerhalb des Kryptosystems, beispielsweise auf einer Festplatte oder in einem EEPROM. Solche Kopien können durch Analyseverfahren ermittelt und ausgelesen werden. Auch stellt die häufig notwendige Weitergabe des geheimen Schlüssels ein erhebliches Sicherheitsrisiko dar.

Um diesen Risiken zu begegnen sind Verfahren erforderlich, die z.B. ständig neue Schlüssel generieren oder den Schlüssel a priori und getrennt vom Kryptosystem zu erzeugen. Diese Verfahren sind i.d.R. aufwändig, teuer und dennoch nicht ausreichend sicher. Die hier vorgestellte Technologie bietet eine Alternative.

Zum Verfahren

Die Erfindung besteht in einer Methode zur Erzeugung von reproduzierbaren geheimen Schlüsseln in Produkten, die mittels lithographischer Herstellungsprozesse entstanden sind, wie z.B. Chips.

In der ersten Variante wird ein Zufallsgenerator realisiert, der sich beim Herstellungsprozess eines Chips aus den physikalischen Eigenschaften ergibt, die Schwankungen und damit dem Zufall unterworfen sind. Die Reproduzierbarkeit basiert auf der Unveränderlichkeit der physikalischen Eigenschaften jedes einzelnen Produkts über die Betriebsdauer.

Es handelt sich um einen Zufallsgenerator mit der Eigenschaft, dass der Zufallswert reproduzierbar ist und dennoch von außerhalb sehr schwer einsehbar, messbar, simulierbar oder ermittelbar ist. Die Reproduzierbarkeit ist unabhängig von Versorgungsspannung, Temperatur, Alter und Beanspruchung.

Diese Idee kann bevorzugt in Form einer mikroelektronischen Schaltung auf einem Chip realisiert werden. Die parasitären Kapazitäten zwischen bestimmten Bereichen der Topographie des Chips (Layout-abhängig) werden in ein Bitmuster überführt, aus dem ein geheimer Schlüssel abgeleitet wird.

Vorteile der Innovation

- Keine lokale Kopien des geheimen Schlüssels nötig
- Kein Austausch des geheimen Schlüssels nötig
- Große Schlüssellängen realisierbar, geeignet für Public-Key-Verfahren (> 1024 Bit)
- Einfaches Prinzip
- Schlüssel ist auch mit vollständiger Kenntnis des Generierungsverfahrens nur mit sehr hohem Aufwand zu ermitteln
- erfolgreiche Angriffe durch Hacker können ausgeschlossen werden

Sehr weites Anwendungsgebiet

- Autorisation und Zugangkontrolle (All-Chips Key)
- Smart-Card Anwendungen
- Übertragung und Verteilung von Multimedia-Inhalten/Single Chip Keys)
- Schutz von Software und Trusted-Computing (All Chips Key und Single-Chip Keys)
- Konfiguration in FPGAs

Die bevorzugte Schaltung ist so ausgelegt, dass dieses Bitmuster sehr sensibel auf Schwankungen der Kapazitäten reagiert. Eine geringfügige Differenz in der Kapazität zwischen zwei beliebigen Chips der bevorzugten Ausgestaltung erzeugt ein jeweils anderes Bitmuster (**Single Chip Keys**). Dies ist aufgrund der statistischen Prozessschwankungen bei der Herstellung der Produkte unvermeidlich.

Soll für alle Chips immer derselbe Schlüssel erzeugt werden, so reagiert die Auswerteschaltung bei geeigneter Wahl der Kapazitäten dagegen nicht auf Prozessschwankungen. In dieser Variante handelt es sich nicht um einen Zufallsgenerator, sondern um ein Verfahren zum Einprägen eines festen, nicht einsehbaren Schlüssels in allen Chips einer Serie (**All Chips Key**).

Anwendungsgebiete im Sicherheitsbereich

Anwendung findet die Erfindung in der Halbleiter- und Chipindustrie, die mit lithographischen Herstellungsprozessen arbeitet.

Autorisation und Zugangskontrolle

Eine Beispielanwendung ist ein elektronischer Schlüssel, z.B. für PKW in Form einer Fernbedienung. Zusammen mit der Seriennummer ergibt sich für jedes Paar aus Schlüssel und Fernbedienung ein gemeinsamer geheimer Schlüssel. Dieser verschlüsselt eine zufällige Bitfolge im Schloss und in der Fernbedienung. Die Autorisierung wird realisiert, in dem die Bitfolge bei jedem Öffnen und Schließen von Neuem erzeugt und ausgetauscht wird.

Smart-Card-Anwendungen

Das Verfahren eignet sich für alle Anwendungen, in denen eine Autorisationsprüfung bzw. Zugangskontrolle realisiert werden soll. Durch Einsatz eines All-Chips-Keys kann die Echtheit von Smart-Cards überprüft werden.

Als Beispiel ist das vom digitalen Fernsehen (Premiere) bekannte Verfahren zu nennen, bei dem eine Smart-Card im Digitalreceiver einen festen Schlüssel zur Entschlüsselung der Videodaten enthält.

Übertragung und Verteilung von Multimedia-Inhalten (Single Chip Keys)

Hier sichert die Erfindung die Übertragung und die Verteilung von Multimedia-Inhalten (z.B. Musik oder Videostreams aus dem Internet) dahingehend, dass die Inhalte nur auf einem bestimmten Gerät abspielbar sind, nicht jedoch auf dem Gerät eines Dritten.

Mit einer Authentizitätsprüfung kann sichergestellt werden, dass alle öffentlichen Schlüssel, die an den Contentanbieter geschickt werden, tatsächlich aus dem Multimedia-Gerät stammen und nicht vom Anwender selbst erstellt wurden (All Chips Key).

Schutz von Software und Trusted-Computing (All Chips Key und Single Chip Keys)

In diesen Anwendungsgebieten geht es darum, Software auf einem System nur dann auszuführen, wenn diese autorisiert wurde. Mit dem Single-Chip Key kann ein solcher Kopierschutz realisiert werden.

Der Idealfall bezüglich Flexibilität und Sicherheit ist die Kombination von All-Chips Keys und Single-Chips Keys. Single Chips Keys kennzeichnen jeden Prozessor in eindeutiger Weise, sodass Programme und insbesondere Multimedia-Inhalte nur auf den autorisierten Prozessoren lauffähig sind.

Der All-Chips Key stellt dagegen die Authentizität des Prozessors (d.h. Single-Chip Keys) sicher und ermöglicht es, Softwareteile vor dem Anwender geheim zu halten und damit vor Reverse-Engineering und Manipulation zu schützen.

Konfiguration in FPGAs

Soll bei FPGAs die interne realisierte Schaltung vor Einsichtnahme geschützt werden, so kann dies mit der hier vorgestellten Erfindung sicherer als mit herkömmlichen Verfahren geschehen. Die Programmierung eines EPGA wäre im Konfigurationsspeicher immer nur verschlüsselt hinterlegt und würde erst im FPGA selbst entschlüsselt werden.

Patent-Portfolio

Deutsche Patentanmeldung DE 10 2005 024 379 A1
Internationale Anmeldungen
EP 1 897 139 und US 2009/0304181 A1

Technologietransfer

Die Erfindung stammt aus dem Institut für Technische Informatik der Universität Mannheim. Die TLB GmbH ist mit der Verwertung beauftragt und bietet Unternehmen die Möglichkeit der Lizenznahme für Fertigung und Vertrieb.

Labormuster

Ein Prototyp wird momentan erstellt. Eine Weiterentwicklung mit dem Institut ist möglich.

Weitere Informationen:

Dr.-Ing. Florian Schwabe
fchwabe@tlb.de
Technologie-Lizenz-Büro (TLB)
der Baden-Württembergischen Hochschulen GmbH
Ettlinger Straße 25, D-76137 Karlsruhe
Tel. 0721 79004-0, Fax 0721 79004-79
info@tlb.de, www.tlb.de