



Elliptic-Curve KryptoProzessor

für hohen Durchsatz mit variabler Schlüssellänge

Viele E-Commerce Anwendungen sind u. a. dadurch gekennzeichnet, daß vertrauliche Informationen über öffentliche Kommunikationsnetze (z. B. das Internet) ausgetauscht werden. Diese Informationen müssen vor dem unberechtigten Zugriff Dritter geschützt werden. Die Basistechnologie, um diesen Schutz zu gewährleisten, ist die Public-Key Kryptographie. Neben dem weit verbreiteten RSA-Verfahren gewinnen Public-Key-Verfahren auf der Basis Elliptischer Kurven (EC) zunehmend an Bedeutung.

Die Sicherheit dieser Verfahren hängt im wesentlichen von der verwendeten Schlüssellänge ab (1024 RSA-Bits entsprechen ca. 160 EC-Bits). Im Vergleich zu RSA bedeutet dies, daß beim Einsatz von EC-Verfahren das gleiche Sicherheitsniveau bereits mit wesentlich kürzeren Schlüsseln erreicht werden kann. Die geringere Schlüssellänge ermöglicht wiederum effizientere Implementierungen und somit höheren Durchsatz.

Die Operation $K \cdot P$, d. h. die Multiplikation eines Punktes $P(x,y)$ auf der Kurve mit einer natürlichen Zahl K , stellt die Basisoperation im Bereich der EC-Kryptographie dar. Sie ist sehr aufwendig und entsprechend rechenzeitintensiv. Die zur Berechnung von $K \cdot P$ benötigte Zeit bestimmt im wesentlichen das Laufzeitverhalten von EC-Implementierungen. Der am Institut für Integrierte Schaltungen und Systeme der TU Darmstadt entwickelte *Elliptic-Curve* Krypto-Prozessor führt genau diese Operation in Hardware durch. Die Performanz von EC-Anwendungen kann durch den Einsatz des Prozessors um mehrere Größenordnungen gesteigert werden.

Hardwareplattform

Die Implementierung des *Elliptic-Curve* Krypto-Prozessors basiert auf der Standard PCI-Karte *microEnable* der Fa. Silicon Software GmbH. Diese Karte ist mit einem rekonfigurierbaren



Prof. Dr.-Ing. Sorin A. Huss
huss@iss.tu-darmstadt.de
Dipl.-Inform. Markus Ernst
ernst@iss.tu-darmstadt.de
Dipl.-Inform. Stephan Klaus
klaus@iss.tu-darmstadt.de

Technische Universität Darmstadt
Fachbereich Informatik
Integrierte Schaltungen
und Systeme
Alexanderstraße 10
D-64283 Darmstadt
Telefon +49 (0) 61 51/16-48 82
Telefax +49 (0) 61 51/16-48 10
www.vlsi.informatik.
tu-darmstadt.de

Logikbaustein (FPGA) der Fa. Xilinx Inc. bestückt, in dem die Funktionalität des Kryptoprozessors implementiert wird. Es gibt diese Karte in mehreren Bestückungsvarianten mit FPGA-Bausteinen unterschiedlicher Komplexität. Da das verwendete Verfahren zur Berechnung von $K \cdot P$ voll parallelisierbar ist, können die jeweils verfügbaren FPGA-Ressourcen optimal ausgenutzt werden, was wiederum die Voraussetzung zum Erreichen der maximalen Performanz ist. Weiterhin wird es erst durch den Einsatz rekonfigurierbarer Logik ermöglicht, EC-Verfahren mit variablen Schlüssellängen auf derselben Hardware zu unterstützen. Über die PCI-Schnittstelle kann der Kryptoprozessor auch in bereits bestehende Kryptosysteme (z. B. *Online-Banking Server*) einfach eingebunden werden, wodurch sich die Performanz derartiger Systeme erheblich steigern läßt.

Elliptic-Curve CryptoProcessor

for High Throughput with Variable Key Size

Many E-Commerce applications are characterized, for instance, by their demand for confidential data exchange via public communication networks (e. g., internet). These data exchanges must be protected from illegal access by third parties. The basic technology, which can warrant this kind of protection, is known as Public-Key Cryptography. Besides the widely-used RSA method, Public-Key methods based on Elliptic Curves (EC) have gained more and more importance.

The security for these methods depends on the utilized key size (1024 RSA-bits are equivalent to 160 EC-bits). EC methods can achieve the same level of security with substantially smaller key sizes than RSA. This smaller key size permits more efficient implementations and thus higher throughputs.

The operation $K \cdot P$ (i. e., the multiplication of a point $P(x,y)$ on a curve with a natural number K) is the basic operation in the area of EC cryptography. This is a very complex operation, and thus computation is very time consuming. The time required for the computation of $K \cdot P$ basically determines the performance of EC implementations. The *Elliptic-Curve CryptoProcessor*, which was developed at the Integrated Circuits and Systems Lab. at Darmstadt University of Technology, implements this specific operation within hardware. The performance of EC applications can be enhanced significantly by the use of this processor.

Prozessorarchitektur und Entwurfsablauf

Für den Entwurf und die Implementierung der Kryptoprozessoren wird ein VHDL-gestützter Entwurfsablauf eingesetzt. VHDL ist der *de-facto* Standard für die abstrakte Modellierung digitaler Schaltungen. Die Architektur des Kryptoprozessors ist variabel in Bezug auf die Schlüssellänge und den Parallelisierungsgrad, d. h. der Ergebnis-Bits, die parallel berechnet werden. Für eine konkrete Implementierung müssen diese beiden Parameter allerdings festgelegt werden. Zur Erzeugung einer solchen spezifischen Variante des Kryptoprozessors wurde am Institut ein spezielles VHDL-Generatorprogramm entwickelt. Das automatisch generierte VHDL-Modell des Prozessors bildet die Grundlage für die anschließende Hardware-Synthese und die weiteren Entwurfsschritte zur Erzeugung der FPGA-Konfigurationsdatei.

Hardware platform

The implementation of the *Elliptic-Curve CryptoProcessor* is based on the *microEnable* standard PCI card from Silicon Software GmbH. This card is equipped with a reconfigurable logic device (FPGA) from Xilinx Inc., in which the CryptoProcessor's functionality is implemented. The card is available with FPGA devices of different complexities. The available FPGA resources can be used at an optimum because the used method for the computation of $K \cdot P$ can be run in parallel. This in turn is the prerequisite to achieve maximal performance. Furthermore, the use of reconfigurable logic enables EC methods with variable key sizes on the same hardware. The integration of the CryptoProcessor into existing crypto systems (e. g., online banking servers) can be accomplished easily via the PCI interface, thus enhancing the performance of such systems immensely.

Processor architecture and design flow

A VHDL based design flow is used for the design and implementation of the CryptoProcessor. VHDL is the *de-facto* standard for the abstract modeling of digital circuits. The architecture of the CryptoProcessor is flexible with regard to the key size and degree of parallelization – that is, the number of bits which are computed in parallel. For a specific implementation of the processor these two parameters must be defined. A special VHDL generator program was developed at the institute in order to create such a specific version of the CryptoProcessor. This VHDL model, which is generated automatically, is the basis for the subsequent hardware synthesis and the following design steps for the generation of the FPGA configuration file.