

Höchste Sicherheit auf kleinstem Raum

Erste Ergebnisse im von Seibersdorf koordinierten FIT-IT Projekt zur Entwicklung eines Quantenkryptographie-Chips

Wien, 14. September 2006, Kleiner, leichter, schneller – das ist das Motto des FIT-IT Projekts „Quantum Cryptography on a Chip – QCC“. Das Projekt setzt dort an, wo die Forschung endet: bei der Überführung von aktuellen Ergebnissen aus der Quantenkryptographie hin zu kommerziellen Produkten. Anwendungsgebiet des Chips ist der sichere Datenaustausch im Bereich Gigabit pro Sekunde.

Während die Quantenphysik aus codierten Lichtteilchen absolut zufällige Bitfolgen generiert, ist der Sicherheits-Chip für den ganzen Rest der Datenverarbeitung und Kommunikation zuständig. Das beinhaltet: Schlüsselerzeugung aus den Quanten-Bitfolgen, Verschlüsselung, Datenverarbeitung, Nachrichtenübertragung, Elektronik.

Erste Ergebnisse: Software-Prototyp für quanten-verschlüsselte Kommunikation

Projektstart von „Quantum Cryptography on a Chip – QCC“ war genau vor einem Jahr im September 2005. Das erste, große Projektergebnis steht kurz vor der Fertigstellung. Anfang Oktober 2006 steht ein kompletter Software-Prototyp zur Verfügung, der jeden Schritt, vom Bit zur verschlüsselten Nachricht bis zur Nachrichtenübertragung über ein virtuelles Netz, transparent zeigt. Für zukünftige Kunden ein Vorteil: Der Simulator bietet eine Entscheidungshilfe für den Einsatz von verschlüsselter Kommunikation mittels Quantenkryptographie.

In der zweiten Projekthälfte steht die Entwicklung des Quantenkryptographie-Chips auf dem Programm.

Chip: Meilenstein in der Markteinführung von Quantenkryptographie

Die Entwicklung des Chips mit integriertem Sicherheitsprozessor und spezieller Hardware-Firewall stellt einen Meilenstein in der Markteinführung von Quantenkryptographie dar. „Wir verwerten die Forschungsergebnisse der Quantenphysik und entwickeln daraus ein Produkt für hochsichere Kommunikation im Bereich Gigabit pro Sekunde. Am Ende soll beim Kunden nur ein Gerät stehen, das die mit Quantenkryptographie verschlüsselte Kommunikation abwickelt“ meint Dr. Christian Monyk, ARC Seibersdorf research GmbH, Projektleiter von „Quantum Cryptography on a Chip – QCC“.

Einsatzmöglichkeit für den Chip bietet etwa eine Quanten-VPN-Verbindung für die Kommunikation zwischen mehreren Firmenstandorten über das Internet. Dabei steht VPN für „virtual private network“ und beschreibt abgesicherte Verbindungen über das Internet. Im FIT-IT-Vorgängerprojekt „PRODEQUAC“ (Prototype Development for Quantum Cryptography) wurde die technische Machbarkeit demonstriert. Auf diesen Ergebnissen aufbauend, erfolgt die Entwicklung des Chips mit erweiterter Funktionalität: sämtliche Schritte zur Schlüsselerzeugung aus den Quanten-Bitfolgen sowie zur Verschlüsselung von Daten im Gigabit-Bereich sind integriert.

Die Technologie des Sicherheitsprozessors

Aus den durch Quantenphysik erzeugten zufälligen Bitfolgen werden im Chip die eigentlichen Schlüssel zur Nachrichtenverschlüsselung generiert. Aufgrund der eigens entwickelten Sicherheitsarchitektur des Chips („Hardware-Firewall“) sind jene Bereiche, die für die Erzeugung der Schlüssel zuständig sind, physisch getrennt implementiert von den Netzwerk- und Verschlüsselungsmodulen. Das garantiert höchste Sicherheit gegen Hacker.

Für die Verschlüsselung der Nachrichten wird der Algorithmus AES (Advanced Encryption Standard) verwendet. Dabei werden Datenströme mit Durchsatzraten von bis zu 1 Gigabit pro Sekunde von eigenen Modulen am Chip verschlüsselt. Diese Module sind direkt in die Hardware des Chips integriert und garantieren dadurch, dass auch bei zeitkritischer Kommunikation keine Qualitätseinbußen auftreten.

Der Sicherheits-Chip ist außerdem „Plattform unabhängig“. Das heißt: egal mit welcher Quantenkryptographie-Technologie die zufälligen Bitfolgen erzeugt werden, der Chip ist für alle Technologien geeignet.

Projekt-Partner: Seibersdorf, Siemens, TU-Graz

Drei Österreichische Partner arbeiten an der Entwicklung des Sicherheitsprozessors: Die Gruppe Quantentechnologien der ARC Seibersdorf research GmbH, die Programm- und Systementwicklung PSE der Siemens AG Österreich, sowie das Institut für Angewandte Informationsverarbeitung der TU Graz. Das Projekt hat eine Laufzeit von zwei Jahren und hat ein Volumen von ca. 580.000 Euro. Projektstart war September 2005.

Kontakt:

Julia Petschinka

Gruppe Quantentechnologien des Bereichs „smart-systems“

ARC Seibersdorf research GmbH

22; Donau City Straße 1/3.OG

Tel: 0664-8251064

Fax: 050550-4190

Web: www.quantenkryptographie.at und www.smart-systems.at