

Siemens IT Solutions and Services

Für die Fachpresse

München, 14. Juli 2008

Siemens baut Lichtschlösser: Datenaustausch mit Quantenkryptografie

Die elektronische Kommunikation wird weltweit sicherer, denn: Siemens IT Solutions and Services, die Austrian Research Centers und die Technische Universität Graz haben den ersten Quantenkryptografie-Chip für den industriellen Gebrauch entwickelt. Der Chip ersetzt die bislang gängige Schlüsselverteilung mit mathematischen Algorithmen und generiert stattdessen aus Lichtteilchen eine absolut zufällige Zahlenfolge zum Schutz der Daten.

Der Prototyp des Quantenkryptografie-Chips ist bereits fertig. Ein entsprechendes Glasfasernetz für die Nutzung des Chips im Rahmen eines absolut sichereren Datenaustauschs wird bei Siemens IT Solutions and Services in Wien im Oktober 2008 vorgestellt.

Und so funktioniert es: Die Quantenkryptografie arbeitet mit einzelnen Lichtteilchen, den so genannten Photonen, die von einem optischen Gerät generiert und codiert werden. Die Sicherheit der Daten gewährleisten dabei Naturgesetze, denn durch Photonen entstehen absolut zufällige Schlüssel. Bisherige mathematische Formeln, die mit entsprechendem Aufwand entschlüsselt werden können, haben bald ausgedient. Nachdem das optische Gerät die Lichtteilchen über Glasfaserkabel an den Empfänger der Nachricht geschickt hat, misst jeder Kommunikationspartner bestimmte Eigenschaften der Photonen mittels eines Detektors. Anschließend werden die Werte über ein Kommunikationsprotokoll via Internet miteinander verglichen. Stimmen die Werte überein, übernimmt der Chip die Verarbeitung und erzeugt aus den

1/2

Messergebnissen die abhörsicheren Schlüssel. Erst mit einem sicheren Schlüssel wird die Nachricht übertragen. Jeder Abhörversuch bei der Schlüsselgenerierung wird erfasst, da Photonen dabei verändert oder zerstört werden. Wenn der Chip registriert, dass jemand mitgehört hat, erzeugt er einfach einen neuen Schlüssel. Dies wiederholt er solange, bis sicher ist, dass niemand mithört. Die Schlüssel werden gleich im Chip zum Ver- bzw. Entschlüsseln von Daten verwendet und danach gelöscht. Sie verlassen den Chip nie. Bis zur Serienreife des Verfahrens wird es allerdings noch zwei Jahre dauern.

Pressebilder finden Sie hier: <http://www.siemens.com/it-solutions/bilder/14070801>

Siemens IT Solutions and Services ist ein international führender Anbieter von IT-Lösungen und -Services und liefert entlang der IT-Dienstleistungskette alles aus einer Hand: vom Consulting mit spezifischem Branchenwissen über die Systemintegration bis zum Management komplexer IT-Infrastrukturen. Darüber hinaus vervollständigt Siemens IT Solutions and Services die Angebotspalette der Siemens-Sektoren mit Software-Entwicklungen und IT-Lösungen. Die Siemens-Division erwirtschaftete im Geschäftsjahr 2007 mit etwa 43.000 Mitarbeitern rund 5,4 Mrd. EUR Umsatz – rund 70 Prozent davon werden außerhalb des Siemens-Konzerns erzielt. Mehr Informationen unter: www.siemens.com/it-solutions