Testumfeld nutzen. Außerdem kooperiert man eng mit Gruppen anderer Forschungseinrichtungen laufenden Betrieb nicht getestet werden, ohne Störungen zu verursachen.

fließt nicht mehr nur in eine Richtung. Die Kapazität vorhandener Netze muss durch geschicktes Management erhöht werden.

Sonne oder indische Feuchte auf einen Wechselrichter auswirkt, sagt Kupzog.

zum Jahr 2030 insgesamt 100 Prozent des Stroms aus erneuerbarer Energie kommen.

Wie Autos in Zukunft sicher miteinander sprechen

Kommunikation. Eine heute sichere Verschlüsselung von Daten im Straßenverkehr könnte der Quantencomputer einmal mit Leichtigkeit knacken. Dem beugen Wiener Forscher mit einem speziellen kryptografischen Schlüssel vor.

VON DANIEL POHSELT

Bedrohungslagen richtig einzuschätzen zählt zum Rüstzeug eines IT-Sicherheitsforschers. Ernst Piller hat dafür ein besonderes Gespür entwickelt: „Der Quantencomputer, der modern verschlüsselte Kommunikationsnetzwerke auch wirklich knacken kann, wird wohl noch eine Weile auf sich warten lassen", sagt Piller.

Realist zu sein heißt aber auch, die Fortschritte bei Rechnern, die den Gesetzen der Quantenphysik folgen, nicht unter den Teppich zu kehren, weiß der Leiter des Instituts für IT-Sicherheitsforschung an der FH St. Pölten. Fast im Monatstakt wird die Bestmarke bei der maximal realisierten Zahl an Quantenbits – der Rechen- und Speichereinheit von Quantenrechnern – nach oben korrigiert. „Schon heute braucht es also Ideen für eine künftige Verschlüsselung von Daten, wenn der Quantenrechner einmal mehrere Tausend Quantenbits Leistung hat und damit zum echten Bedrohungsszenario wird", sagt Piller. Er denkt vor allem an sensible Bereiche wie das autonome Fahren, an Industrieanlagen und sowie an Kommunikationsnetzwerke wie das Internet.

Der Schlüssel wird zu lang

Bisher kommt hier zur Verschlüsselung von Daten die sogenannte asymmetrische Kryptografie zum Einsatz. Das mathematische Verfahren arbeitet mit einem Schlüsselpaar, das aus einem privaten und einem öffentlichen Schlüssel besteht. Das Prinzip ist simpel: Wer den öffentlichen Schlüssel hat, kann die Daten verschlüsseln; wer den privaten Schlüssel besitzt, kann sie entschlüsseln. Um gegen die Rechenleistung künftiger Quantencomputer zu bestehen, brauchte es aber sehr lange Schlüssel, die aus Milliarden von Bits zusammengesetzt sind. „Dies würde viel zu lang dauern", erklärt Piller.

Neuere Ansätze zur sicheren Verschlüsselung setzen daher auf komplexe Algorithmen. Einen alternativen Ansatz ganz ohne mathematische Kniffe verfolgt Pillers Arbeitsgruppe im vom Technologieministerium geförderten Projekt „KIF – Kryptografie für kabellose Kommunikation". „Wir setzen auf eine Verschlüsselung auf Basis gemessener Funkkanaldaten einer hochfrequenten Funkübertragung", so Piller.

Die Forscher nutzen dabei das Phänomen der Umkehrbarkeit der Funkübertragung. Egal, ob gerade A oder B sendet oder empfängt: Laufzeit, Signalstärke und Phasenverschiebung der Funksignale an beiden Orten sind ident. „Aus den beiderorts identen Messwerten lassen sich geeignete kryptografische Schlüssel bilden", lautet die These im Projektteam. Unter anderem im Projekt mit an Bord: der Straßenbetreiber Asfinag sowie der IT-Sicherheitsdienstleister Cryptas.

IN ZAHLEN

72 **Quantenbits** Rechenleistung erreicht Googles neuer Quantenrechnerchip Bristlecone. Erzielt wird die Leistung über 72 supraleitende Leiterschleifen. Damit nähert man sich dem Punkt, an dem Quantencomputer die besten Supercomputer übertreffen.

8000 **Quantenbits** Rechenleistung brauchte es nach Forschermeinung, um die heutige asymmetrische Kryptografie zu knacken. Bei diesem Verschlüsselungsverfahren nutzen die Kommunikationspartner zwei Schlüssel: einen öffentlichen und einen privaten.

Tests im Straßenverkehr

Erste Livetests mit Fahrzeugen auf St. Pöltens Straßen stimmen jedenfalls zuversichtlich. „Wir sammelten Daten für unterschiedliche Fahrgeschwindigkeiten in wechselnder Verkehrsdichte in Funknetzen über zwei Gigahertz", schildert Ernst Piller.

Seit ein paar Monaten dreht sich nun alles um die Auswertung und Optimierung der Daten sowie die optimale Schlüsselerzeugung. Nächste Etappe: Die Fertigstellung eines Prototyps mit Sender, Empfänger und Messeinheit ist bis April 2019 geplant.

Neues Bild des Universums

Physiker erklären Messung mit Dunklen Photonen.

Messungen eines australischen Radioteleskops stehen im Widerspruch zum gängigen Bild des frühen Universums. Sie zeigten Anfang des Jahres, dass das sogenannte 21-Zentimeter-Signal, eine kosmologische Messgröße, deutlich vom erwarteten Wert abweicht. Wiener Wissenschaftler arbeiteten an einer Erklärung des Phänomens mit. Die Erkenntnisse wurden im Fachjournal „Physical Review Letters" veröffentlicht.

„Unsere Theorie beruht auf der Annahme Dunkler Photonen, die nur eine minimale Erweiterung des Standardmodells darstellen", sagt Josef Pradler vom Institut für Hochenergiephysik der Österreichischen Akademie der Wissenschaften. Demnach können Dunkle Photonen unter bestimmten Umständen in normale Lichtteilchen umgewandelt werden. Das würde letztendlich die unerwartete Stärke des gemessenen Signals erklären. (APA)