ITG news
INFORMATIONSTECHNISCHE GESELLSCHAFT IM VDE

3/2021

Liebe ITG Mitglieder,

nach langer Zeit gibt es endlich Licht am Horizont. Die COVID-19-Pandemie wird uns zwar noch länger begleiten; es gibt aber Hoffnung auf eine schrittweise Rückkehr zu mehr Normalität. Im Herbst plant die ITG auch wieder Präsenztreffen. Ich denke, wir freuen uns alle darauf, endlich auch mal wieder unbelastet „zusammen“ feiern zu dürfen.

Mit dem Nachlassen der Pandemie drängen sich andere Themen wieder in den Vordergrund: Eine sinnvolle Klimapolitik wird nicht ohne Unterstützung durch eine nachhaltige Digitalisierung umsetzbar sein. Die geopolitischen Spannungen manifestieren sich zunehmend als Technologiewettkampf mit einem gewissen Fokus auf Mikroelektronik und Mobilfunk, Cyberkriminalität hat Konjunktur und unsere technologische Souveränität, aber auch die Sicherheit unserer Versorgungsketten erfordern höchste Aufmerksamkeit.

VDE und ITG sind in diesen Bereichen aktiv. Wir konnten in den letzten Monaten durch wissenschaftliche Analysen und Positionspapiere etwas zur Lösung dieser Probleme beitragen. Die einschlägigen Positionspapiere der ITG (Technologische Souveränität, Hidden Electronics) stehen allen Mitgliedern unentgeltlich zur Verfügung.

Wir geben Ihnen in dieser Ausgabe der ITG News Einblicke in verschiedene Aspekte der Quantentechnologie, die die Zukunft der Kommunikation, Verschlüsselung und des Computing prägen könnte.

Über die 6. Mobilfunkgeneration (6G) haben wir bereits berichtet. Die ITG wird hierzu eine Fokusgruppe einrichten, damit alle Interessierten sich von Anfang an in die Diskussionen zur Bildung einer 6G-Vision und damit unserer digitalen Welt ab 2030 einbringen können.

Es warten viele Herausforderungen auf uns – und die ITG ist wie immer am Puls der Zeit …

Es warten viele Herausforderungen auf uns – und die ITG ist wie immer am Puls der Zeit …

In diesem Sinne,
viel Spaß beim Lesen der ITG News und bleiben Sie gesund,
Ihr

PROF. DR.-ING. HANS D. SCHOTTEN
ITG Vorsitzender

ITG FOKUSPROJEKT 6G

Call for 6G Experts

Wegen der großen Bedeutung des Themas 6G hat der ITG Vorstand beschlossen, ein Fokusprojekt zum Thema 6G ins Leben zu rufen. Angedacht ist die gremienübergreifende Arbeit an diesem Zukunftsthema. Interessierte Experten werden aufgerufen, ihre Bereitschaft zur Mitarbeit an die Geschäftsstelle der ITG zu melden.

// www.vde.com/itg

Inhalt

Meldungen 02
Thema
Quantenkommunikation / Quantenschlüsselaustausch 04
Personalia / Termine 12

2. VDE FACHTAGUNG „INTERNET OF THINGS/INDUSTRIE 4.0“

Neue Entwicklungen im Bereich Energiewirtschaft und 5G

Am 22. und 23. April 2021 fand zum zweiten Mal die VDE Fachtagung „Internet of Things/Industrie 4.0“ als interdisziplinäre Gemeinschaftsveranstaltung von ETG, ITG und VDE Dresden unter Leitung von Dr. Jörg Benze statt.

Keynote von Prof. Dr. Rainer M. Speh

Keynote Dr. Johannes Springer (T-Systems)

2018 auf Initiative der Mitglieder des gleichnamigen Fachausschusses KT6 der ITG ins Leben gerufen, wurde die 2. Fachtagung ursprünglich für September 2020 geplant. Pandemiebedingt verschob der Programmausschuss den Termin auf April 2021 und entschied, als eine Präsenzveranstaltung in Dresden nicht möglich war, die Tagung als ein Online-Event durchzuführen.

Steuerung der Web-Conference-Plattform aus dem Homeoffice

Mit der Keynote von Prof. Dr. Rainer M. Speh zum Thema „Der zellulare Ansatz für eine erfolgreiche Energiewende“ und der Keynote von Dr. Johannes Springer (T-Systems) zum Thema „5G und darauf basierte Anwendungen am Beispiel der Mobilität und Automotive“ konnten für die fachlichen Einleitungen in die beiden Tagungstage zwei herausragende Experten gewonnen werden, die diese hochaktuellen Themen in der Energiewirtschaft und der IKT-Branche eindrucksvoll dargestellt haben.

Darüber hinaus wurde das Themenfeld an zwei Tagungstagen mit 13 Beiträgen in den vier nachfolgend genannten Sessions sehr breit behandelt:

- Energieversorgung 4.0 im zellularen Energiesystem,
- Internet of Things, juristische und gesellschaftliche Aspekte,
- 5G-Kommunikation, Maschinelles Lernen, Künstliche Intelligenz sowie
- Innovationen auf der Schiene, Sichere Datenübertragung in KRITIS, Energiewirtschaft.

Das Formatelement der offenen Paneldiskussion am Ende jedes Tages gab den Teilnehmern ausreichend Gelegenheit, mit den Referenten und untereinander zu diskutieren. Dank der von der T-Systems MMS bereitgestellten professionellen Web-Conference-Plattform und der erfahrenen Systembedienung konnte eine lebhafte Onlinediskussion sichergestellt werden. Mit über 80 angemeldeten Teilnehmern war die Fachtagung sehr gut besucht.

DR.-ING. JÖRG BENZE
Leiter VDE ITG Fachausschuss „Internet der Dinge/Industrie 4.0“ (KT6)
T-Systems Multimedia Solutions GmbH, Dresden

TUZ 2021

33. ITG/GI/GMM Workshop Testmethoden und Zuverlässigkeit von Schaltungen und Systemen

Zum 33. Mal versammelten sich Experten der Mikroelektronik auf dem deutschsprachigen Forum, das von der Hochschule Nordhausen und der Hochschule Hamm-Lippstadt veranstaltet wurde. 52 Teilnehmer aus Industrie und von Forschungseinrichtungen kamen – aufgrund der Corona-Pandemie virtuell – zusammen, um Ideen, Trends und Herausforderungen im informellen Rahmen auszutauschen.

Teilnehmer aus Deutschland, Estland und Italien diskutierten sowohl Themen aus dem digitalen Bereich, die sich mit Fehlertoleranz, funktionaler Sicherheit und Security beschäftigten, als auch analoge Themen mit dem Fokus auf Stimuligenerierung und Selbsttest. Insgesamt umfasste das Programm unter der Leitung von Prof. Dr. René Krenz-Baath von der Hochschule Hamm-Lippstadt zwei Keynotes, vierzehn Fachvorträge und fünf Poster. Die Organisationsleitung hatte Prof. Dr. Mario Schölzel von der Hochschule Nordhausen inne.

In der ersten Keynote mit dem Titel „More Compute Performance under the Hood: New Applications and Complexity Challenges for Automotive Microcontrollers“ diskutierte Dr. Christian Pacha von der Infineon Technologies AG die speziellen Herausforderungen der ansteigenden Komplexität im Bereich zukünftiger heterogener Systems-on-Chip (SoC).

In der zweiten Keynote mit dem Titel „Low cost solutions for increasing system reliability on multi-core based safety-critical applications“ stellte Assoc. Prof. Dr. Ernesto Sanchez effiziente Testmethoden für die Anwendung von In-field-Tests in sicherheitskritischen Bereichen vor. Weitere interessante Beiträge wurden unter anderem in den Bereichen Test Standards, Safety & Security und Analog und Mixed-Signal Test vorgestellt.

Trotz der coronabedingten Einschränkungen waren zahlreiche interessante Diskussionen möglich. Das Social Event wurde mit einem virtuellen Rundgang durch Erfurt eröffnet und auf der Basis des Tools gather.town fortgesetzt. Hierbei fand ein guter Austausch zwischen den Teilnehmern statt.

Im Jahr 2022 soll der nächste TuZ-Workshop in Bremerhaven stattfinden. Dann wird die Tagung von Dr. Sebastian Thun vom Deutschen Forschungszentrum für Künstliche Intelligenz (DFKI) organisiert. Die Leitung des Programmkomitees übernimmt Prof. Dr. Görschwin Fey von der Technischen Universität Hamburg (TUH). Die Informationen über den Tagungsort und Einreichungsfristen werden wie gewohnt nach Abschluss der Planung unter www.tuz-workshop.de bereitgestellt.

PROF. DR. RENÉ KRENZ-BAATH
Hochschule Hamm-Lippstadt
Technische Informatik Embedded Systems

KONRAD-ZUSE-GESELLSCHAFT

80 Jahre Zuse-Computer Z3

Dieses Jahr jährt sich zum 80. Mal der Tag der Vorführung der Rechenmaschine Zuse Z3 in der Methfesselstr. 7 in Berlin Kreuzberg. Die Zuse Z3 gilt heute als der erste funktionsfähige Computer der Welt.

Die Zuse Z3 ist eine Maschine, die frei programmierbar ist und mit binären Gleitkommazahlen arbeitet. Um dem Ingenieur die Arbeit mit einer solchen Maschine zu erleichtern, erfolgten die Eingabe und Ausgabe der Zahlen im Dezimalsystem. Das Bild zeigt Konrad Zuse vor dem Nachbau der Maschine Z3 (ca. 1980).

Lesen Sie weitere spannende Details über die Rechenmaschine Zuse Z3 mit historischem Überblick der 1988 gegründeten Konrad-Zuse-Gesellschaft unter
http://horst-zuse.homepage.t-online.de/z3-detail.html

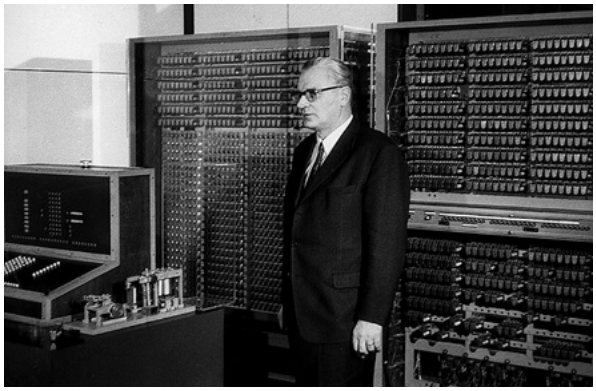

Bild: Professor Dr.-Ing. habil. Horst Zuse

PROFESSOR DR.-ING. HABIL. HORST ZUSE
Universtät Cottbus

QUANTENKOMMUNIKATION / QUANTENSCHLÜSSELAUSTAUSCH

Berliner Testbett für quantensichere Kommunikation im Europäischen Verbundprojekt OpenQKD

Die Existenz hinreichend leistungsfähiger universeller Quantencomputer wird die gesamte heute verwendete asymmetrische Kryptographie zur Absicherung sensibler Kommunikation, wie beispielsweise der Fernzugriff auf das Bankkonto, unbrauchbar machen. Die sogenannte Quantenschlüsselverteilung (QKD) ist die quantentechnische Antwort auf diese Herausforderung, aber es gibt auch algorithmische Ansätze, die einen relativ nahtlosen Ersatz für aktuelle Schlüsselaustausch-Algorithmen bieten können. Im OpenQKD-Testbett Berlin wird das Zusammenspiel beider Verfahren erprobt.

Die asymmetrische (public-key) Kryptographie ist wahrscheinlich der wichtigste Baustein, um die Sicherheit von elektronischer Kommunikation in unserer vernetzten Welt zu gewährleisten. Obwohl die Verschlüsselung von Daten zum Schutz vor unbefugtem Lesen aus Effizienzgründen in der Regel mit symmetrischen Algorithmen, wie z.B. dem AES256-Verfahren (Advanced Encryption Standard mit 256-bit-Schlüssel) erfolgt, ist die asymmetrische Kryptographie beim Austausch des Schlüssels für die symmetrische Verschlüsselung unerlässlich. Wenn eine Nachricht mit dem öffentlichen Schlüssel eines Empfängers verschlüsselt wird, kann nur der rechtmäßige Empfänger diese Nachricht mit dem eigenen privaten Schlüssel entschlüsseln. Die Berechnung des privaten Schlüssels aus dem öffentlichen (d.h. das Brechen des kryptographischen Systems) erfordert die Lösung eines schwierigen mathematischen Problems. Auf diese Weise wird die Sicherheit durch die Komplexität des Problems und die endlichen Rechenressourcen eines Angreifers gewährleistet.

Zur Konstruktion von asymmetrischen Verfahren können mathematische Funktionen verwendet werden, die relativ einfach zu berechnen, aber sehr schwer zu invertieren sind. Der bekannteste und am weitesten verbreitete Algorithmus dieser Art ist der RSA-Algorithmus, benannt nach seinen Erfindern Rivest, Shamir und Adleman. Seine Sicherheit beruht auf der Schwierigkeit, große ganze Zahlen in ihre Primfaktoren zu zerlegen, während die Berechnung des Produkts der Primzahlen einfach ist. Im Fall von RSA ist kein klassischer Algorithmus bekannt, der es ermöglichen würde, große ganze Zahlen in angemessener Zeit zu faktorisieren. Die starke Zunahme der Komplexität für die Faktorisierung von zunehmend größeren Zahlen ist fundamental für die Skalierbarkeit des Verfahrens. Falls die zunehmende Rechenleistung von klassischen Computern die Sicherheit gefährdet, kann durch eine Verdopplung der Schlüssellänge die Komplexität der Faktorisierung wieder um mehrere Größenordnungen erhöht werden.

Die Bedrohung durch Quantencomputer

Die potenzielle Bedrohung durch Quantencomputer ist seit 1999 bekannt, als Peter Shor einen Quantenalgorithmus veröffentlichte, der die Primfaktorzerlegung und die Berechnung diskreter Logarithmen mit

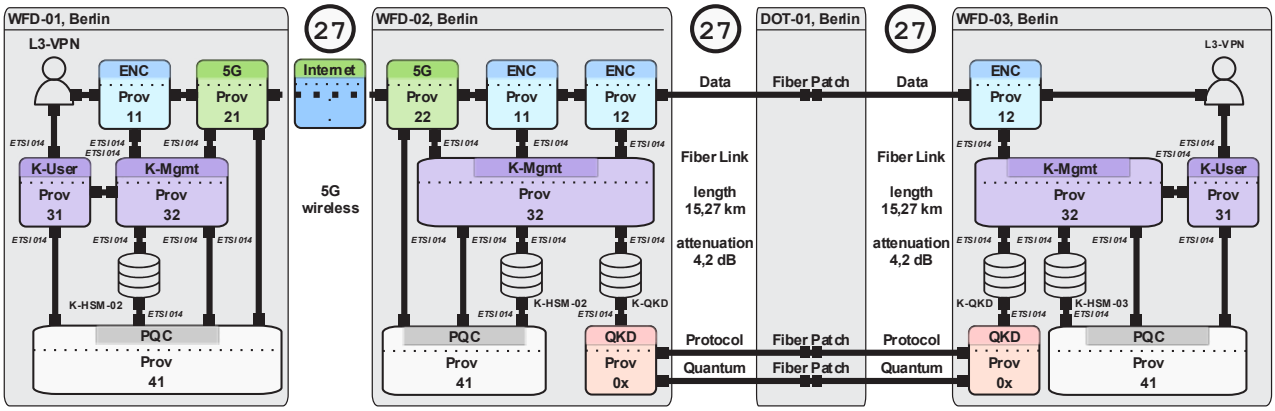

Bild 1: Aufbau eines Nutzerszenarios im Berliner OpenQKD-Testbett, das eine Faserverbindung und 5G-Access mit dem Ziel kombiniert, das Zusammenspiel von QKD und Post-Quanten-Kryptographie zu optimieren. Die realisierte Architektur folgt einem Schichtenmodell, bestehend aus einer Quantenebene, einer Key-Management-Ebene und einer Applikationsebene.

einer Komplexität ermöglicht, die nur noch moderat mit der Größe des Problems wächst. Sobald es universelle Quantencomputer hinreichender Größe gibt, wird der Algorithmus von Shor letztendlich alle Protokolle zur Authentifizierung und zum Schlüsselaustausch, die auf diesen Problemen basieren, unsicher machen. Dies gilt u.a. für RSA, ElGamal, DSA (Digital Signature Algorithm), Diffie-Hellman und die Varianten mit elliptischen Kurven von DSA und Diffie-Hellman.

Allerdings wird Shors Algorithmus erst seit wenigen Jahren als relevante Bedrohung wahrgenommen, da namhafte Firmen, wie Google, Intel und IBM, Quantenprozessoren mit mehr und mehr Qubits bauen und darum ringen, für erste spezielle Probleme die Überlegenheit des Quantencomputers zu demonstrieren. Dennoch sind aktuelle Quantencomputer noch viel zu klein, um moderne asymmetrische Algorithmen zu brechen, und selbst Fachleute sind sich nicht einig, ob die Skalierung auf sehr viel mehr Qubits und eine höhere Zuverlässigkeit lediglich eine Frage der Technik ist oder noch weitere wissenschaftliche Durchbrüche erfordert.

Auch wenn es noch viele Jahre dauern sollte, bis Quantencomputer tatsächlich asymmetrische Verfahren bedrohen, ist es bereits jetzt möglich, verschlüsselte Kommunikation aufzuzeichnen und zu einem späteren Zeitpunkt mit leistungsfähigen Quantencomputern zu entschlüsseln (Harvesting-Angriff). Das bedeutet, dass sensible Daten, je nachdem, wie lange sie geheim gehalten werden müssen, bereits jetzt gefährdet sind.

Quantenschlüsselverteilung und Post-Quantenprotokolle

Die quantentechnische Lösung für einen sicheren Schlüsselaustausch ist die sogenannte Quantenschlüsselverteilung (quantum key distribution, QKD), dessen Sicherheit nicht auf Annahmen hinsichtlich der Komplexität bestimmter mathematischer Probleme oder der Rechenleistung des Angreifers beruht. Deshalb wird QKD auch oft als langzeitsicher bezeichnet. Ein Nachteil von QKD ist allerdings, dass das Verfahren Zugang zu einem optischen Kanal (eine Faser oder eine Freistrahlverbindung) für die Übertragung von Quanteninformationen benötigt und die natürliche Dämpfung des Quantensignals die Reichweite ohne weitere Maßnahmen stark limitiert.

Die sogenannte Post-Quanten-Kryptographie (PQC) bietet eine weitere Lösung und basiert auf mathematischen Problemen, die kein bekannter Quantenalgorithmus sehr viel schneller lösen kann. Da bei diesem Konzept die Sicherheit immer noch von der Komplexität bestimmter mathematischer Probleme abhängt, ist es möglich, dass Fortschritte bei der Lösung der zugrunde liegenden Probleme die Sicherheit entscheidend schwächen können. PQC ist wie bisher ein rein algorithmisches Verfahren und benötigt somit keinen speziellen Quantenkanal. Das National Institute of Standards and Technology (NIST, USA) ist federführend bei den Bemühungen, quantensichere Schlüsselaustauschalgorithmen innerhalb der nächsten zwei bis drei Jahre zu standardisieren. In einem mehrstufigen Auswahlprozess werden die vorgeschlagenen Verfahren von vielen internationalen Experten einer rigorosen Analyse unterzogen. Aktuell wurden vier Schlüsselaustauschverfahren in die engere Wahl gezogen und es wird erwartet, dass mindestens zwei davon den Weg in die Standardisierung finden, um den Anforderungen für verschiedene Anwendungen gerecht zu werden. Erste kommerzielle Implementierungen sind, noch bevor die Standardisierung abgeschlossen ist, zu erwarten.

Sowohl das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) als auch NIST empfehlen für die Umstellung auf quantensichere Verfahren, die bewährten Algorithmen nicht sofort zu ersetzen, sondern mit Post-Quanten-Kryptographie zu ergänzen. QKD kann darüber hinaus als zusätzliches Schlüsselaustauschverfahren verwendet werden. Damit reduziert man das Risiko, das die neuen Verfahren mit sich bringen, und kann insbesondere für hohe Sicherheitsanforderungen die Sicherheit auf ganz unterschiedliche Mechanismen stützen. Neue Produkte sollten möglichst schon heute quantensichere Verfahren unterstützen oder zu einem späteren Zeitpunkt zumindest entsprechend aktualisiert werden können (crypto agility).

Quantensicheres Testbett in Berlin

Im Rahmen des Europäischen Flaggschiffprojekts OpenQKD werden in verschiedenen Testbetts zahlreiche Nutzerszenarien hinsichtlich ihrer Leistungsfähigkeit, Skalierbarkeit und der operativen Auswirkungen evaluiert. Die Deutsche Telekom T-Labs hat mit Unterstützung von ADVA und anderen Projektpartnern ein OpenQKD-Testbett in Berlin aufgebaut, das verschiedene Nutzerszenarios unterstützen kann. Bild 1 zeigt eines der im Testbett realisierten Szenarios.

Der Austausch von Schlüsseln erfolgt quantensicher über QKD-Strecken der Konsortialpartner ID Quantique und Toshiba Europe Ltd.

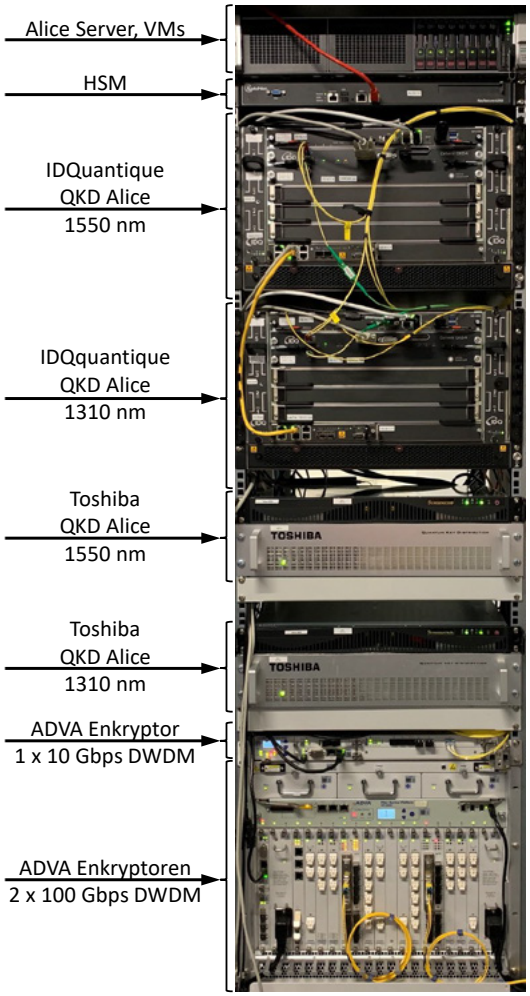

Bild 2: Knoten Alice im Berliner Testbett

Zusätzlich lassen sich Schlüssel über PQC-Verschlüsselung und Authentifizierung netzagnostisch übertragen, beispielsweise über drahtlose 5G-, Faser- oder Kupfernetze ohne Distanzlimitierungen. Alle erzeugten Schlüssel werden sofort vom Schlüsselmanagement in einen sicheren Schlüsselspeicher überführt, einem Hardware Security Module (HSM). Das HSM dient als Single Point of Trust für quantensichere Schlüssel. Applikationen bzw. Enkryptoren können über das Schlüsselmanagement die quantensicheren Schlüssel an unterschiedlichen Standorten verwenden. Die Architektur unterscheidet zwischen Nutzer- und Provider-Schlüsselmanagement, das die Schlüssel netzseitig verwaltet und im HSM speichert. Das Nutzer-Schlüsselmanagement fordert vom Provider-Schlüsselmanagement quantensichere Schlüssel für ihre spezifischen Applikationen an.

Im Gegensatz zu den aktuellen ETSI-Standards wurde, soweit beide Endpunkte dies unterstützten, das Schlüsselmanagement PQC verschlüsselt und authentifiziert aufgebaut. Dies beinhaltet insbesondere die Übergabe von Schlüsseln an die Benutzer und die Schlüsselweiterleitung über zwischengeschaltete QKD-Knoten. Somit wird eine signifikante Erhöhung der Sicherheit einer QKD-Architektur erreicht, deren größter Kritikpunkt bisher eine mögliche Offenlegung von Geheimnissen während der Schlüsselweiterleitung über intermediäre QKD-Knoten war.

Im weiteren Forschungsprogramm des Berliner OpenQKD-Testbetts werden nun die QKD-Systeme hinsichtlich ihrer Schlüsselaustauschraten in Abhängigkeit von verschiedenen Transportschemata unter möglichst realistischen und produktivitätsnahen Bedingungen untersucht.

Die Endpunkte von verschlüsselten Nachrichtenverbindungen werden gemeinhin als Alice, Bob und Charlie bezeichnet. In Bild 2 ist der Aufbau eines zentralen Knotens (Alice) des Testbetts mit verschiedenen Systemen dargestellt. Im Key-Management-Layer (K-Mgmt) steuern Virtuelle Maschinen (VM), die auf einem Server installiert sind, die einzelnen Netzelemente, einschließlich dem Hardware Security Module (HSM), in dem die Schlüssel sicher gespeichert werden, zwei Cerberis3-QKD-Systeme von ID Quantique mit Quantenkanälen jeweils bei 1550 nm und 1310 nm, zwei QKD-Systeme von Toshiba Europe Ltd. mit Quantenkanälen ebenfalls bei 1550 nm und 1310 nm, die sich auf der QKD- bzw. PQC-Ebene befinden, sowie zwei DWDM-Systeme ADVA FSP3000R7 mit 10-Gbit/s- und 100-Gbit/s-Enkryptoren, die der Enkryption-Ebene (ENC) zugeordnet sind.

Der dargestellte Netzknoten Alice ist über feldverlegte Glasfasern mit den Knoten Bob und Charlie verbunden sowie über drahtlose 5G-Verbindungen an das Internet angebunden. Mit diesem Berliner OpenQKD-Testbett können diverse Szenarien untersucht und demonstriert werden, einschließlich der Verkettung von leitungsgebundenen Glasfaserstrecken mit drahtlosen Funknetzen, über die quantensichere Netzverbindungen und Services für anwenderspezifische Ende-zu-Ende-Services und Applikationen geschaltet werden können.

Referenzen

[1] Der Aufbau des Testbetts wird vom Forschungs- und Innovationsprogramm Horizon 2020 der Europäischen Union unter der Fördervereinbarung Nr. 857156 (OpenQKD) unterstützt. Für weitere Details zum OpenQKD-Projekt: https://openqkd.eu

DR. HELMUT GRIESSER
ADVA Optical Networking SE

DR. RALF-PETER BRAUN
Deutsche Telekom AG

DR. MARC GEITZ
Deutsche Telekom AG

Kostenloses Lehrmaterial für Cyber-physikalische Systeme

Wenn man IKT-Systeme mit der physikalischen Umgebung verbindet, dann entstehen sog. Cyber-physikalische Systeme. Zu diesen gehören beispielsweise alle modernen Fahrzeuge. Das Vermitteln der Fähigkeit, solche Systeme zu entwickeln, ist aufgrund der erforderlichen Interdisziplinarität besonders schwierig. Anforderungen und Lösungsmöglichkeiten für die Lehre in diesem Gebiet wurden in einem kürzlich erschienenen Sonderheft der Zeitschrift IEEE Design & Test [1] beschrieben. Zur Unterstützung der Lehre steht ebenfalls seit Kurzem ein Lehrbuch für dieses Gebiet über eine Open-Access-Lizenz zunächst in einer englischen Fassung zum kostenlosen Download zur Verfügung [2]. Mit dem kostenlosen Download sollen Studierende gerade in Pandemie-Zeiten in ihrem Lernen unterstützt werden. Eine deutsche, ebenfalls kostenlos zugängliche Fassung sollte Anfang Mai dieses Jahres erschienen sein. Die Finanzierung der Open-Access-Gebühr erfolgte mit Mitteln des SFB 876 (und damit indirekt der Deutschen Forschungsgemeinschaft) sowie des Informatik Centrums Dortmund e. V. (ICD).

[1] Marwedel, P.; Mitra, T.; Grimheden, M. E.; Andrade, H. A. (Hrsg.): Special Issue on Education for Cyber-Physical Systems. IEEE Design & Test, November/Dezember 2020

[2] Marwedel, P.: Embedded System Design – Embedded Systems Foundations of Cyber-Physical Systems, and the Internet of Things. Springer International Publishing, 4. Auflage, 2021. DOI 10.1007/978-3-030-60910-8, www.springer.com/de/book/9783030609092

Bilder: www.dlr.de/RB

QUANTENKOMMUNIKATION / QUANTENSCHLÜSSELAUSTAUSCH

DLR Quantum Space Operations Center – Anwendung von Quantenschlüsseln im Satellitenbetrieb

Das German Space Operation Center (GSOC) am Deutschen Zentrum für Luft- und Raumfahrt (DLR) in Oberpfaffenhofen bei München blickt auf eine über 50-jährige Geschichte im Missionsbetrieb von Satelliten und in der bemannten Raumfahrt zurück. Zur Kommunikation mit den erdnahen und geostationären Satelliten greift das GSOC dabei auf ein weltumspannendes Netzwerk von Bodenstationen zurück. Eine wichtige Anforderung des sicheren Betriebs ist dabei die Verschlüsselung bzw. Signierung von Daten und Kommandos auf dem Weg von und zu den Satelliten. So kann die Kommandierung des Satelliten vor dem Zugriff unbefugter Dritter geschützt, die Vertraulichkeit und Integrität von gewonnen Mess- und Bilddaten gewahrt, sowie gesetzliche und vertragliche Auflagen erfüllt werden.

Ein zentrales Problem der klassischen Kryptographie besteht darin, dass gängige Verschlüsselungsverfahren auf die extrem geringe Wahrscheinlichkeit vertrauen, einen Schlüssel in überschaubarer Zeit mittels Numerik herkömmlicher Computer zu erraten. Klassische asymmetrische Kryptographieverfahren, wie beispielsweise RSA, generieren ein Schlüsselpaar mit einem öffentlichen und einem privaten Teil. Eine Nachricht wird nun mit dem frei zugänglichen, öffentlichen Schlüssel verschlüsselt und der Empfänger wendet den nur ihm bekannten privaten Schlüssel an, um die Nachricht zu entschlüsseln. Um die Nachricht ohne die Kenntnis des privaten Teils des Schlüssels zu entschlüsseln, muss der private Schlüssel aus dem öffentlichen Schlüssel rekonstruiert werden, was eine aufwendige mathematische Operation beinhaltet, namentlich die Faktorisierung einer Primzahl. Bei angemessener Größe dieser Faktoren wird jeder Nutzen aufgrund der immensen Dauer der Entschlüsselung mittels derzeitig verfügbarer Computerhardware zunichtegemacht.

Dieses Szenario ändert sich drastisch mit der Entwicklung von leistungsfähigen, universellen Quantencomputern. Diese sind besonders effizient darin eine bestimmte Art von mathematischen Problemen, wie die oben erwähnte Faktorisierung, innerhalb von kurzen Zeiträumen zu lösen. Derzeitige Quantencomputer sind noch nicht leistungsfähig genug, gängige Verschlüsselungen zu brechen. Bei fortschreitender Entwicklung besteht allerdings die Möglichkeit, dass gegenwärtige public-private-key-Verschlüsslungsverfahren langfristig gebrochen werden könnten.

Die beiden verfolgten Ansätze bei der Entwicklung von quanten-sicheren Kryptographiemethoden sind zum einen neue klassische Methoden, wie zum Beispiel Post-Quantum-Cryptographie, welche die Vorteile der Quantenalgorithmen bei der Entschlüsselung durch Faktorisierung nivellieren,

Kontrollraum des Satellitenkontrollzentrums

zum anderen ein physikalisch sicherer Schlüsselaustausch welcher aufgrund quantenmechanischer Gesetzmäßigkeiten weder unbemerkt mitgelesen noch verändert werden kann.

Im Rahmen eines Forschungsprojektes untersuchen wir am GSOC künftig die Anforderungen für die Integration von Quantum-Key-Distribution (QKD) in den Satellitenbetrieb. Mit Kooperationspartnern wie der Universität der Bundeswehr München, der Ludwig-Maximilians-Universität und anderen soll dafür eine hochsichere Quantum-Communication-Infrastructure (QCI) in Form eines Prototypen aufgebaut werden. Als Informationsträger für die auszutauschenden Schlüssel dienen hierbei die Quantenzustände von übermittelten Photonen. Diese werden hierbei mittels Glasfaser oder Freistrahlstrecke (sprich: Laser und optischen Detektor) übertragen. Aufgrund von Dispersionsverlusten in Glasfaserleitungen oder Luft, geografischen und lokalen Begebenheiten ist eine direkte Verbindung zwischen Schlüsselsender und Empfänger üblicherweise auf wenige 100 km beschränkt. Dies kann je nach Länge der Übertragungsstrecke den Aufbau eines Netzes sogenannter vertrauenswürdiger Kommunikationsknoten (engl. trusted nodes) bedingen.

Ziel dieser Forschungsarbeit ist, die technischen Anforderungen zu spezifizieren, welche für eine QKD-basierte Verschlüsselung zwischen Kontrollzentrum und Bodenstation notwendig sind. Hierbei müssen verfügbare Hardware-Optionen validiert werden. Dies beinhaltet, neben der Validierung verschiedener Verschlüsselungs-Geräte, die Integration in raumfahrtspezifische Daten- und Netzwerkprotokolle sowie die Formulierung von Anforderungen an künftige Satelliten, Quantenschlüssel empfangen, verarbeiten und für externe Verbindungen zwischen beliebigen Partnern verteilen zu können. Entlang aller Teilstrecken im Kontrollzentrum und zur Bodenstation sollen verschlüsselte Telemetrie- und Kommandodaten übermittelt werden, um so die Komplettverschlüsselung im Missionsbetrieb zu simulieren.

Im Ausblick für die zukünftig anstehenden Arbeiten stehen vor allem die Formulierung der technologischen Anforderungen an die Beschaffenheit und den Betrieb entsprechender Satellitenmissionen, bei denen auch der betriebene Satellit in der Lage ist, Quantenschlüssel zu empfangen und entsprechend Missionsdaten zu ver- und entschlüsseln. Darüber hinaus sollen Betriebskonzepte entworfen werden für Satelliten, die im Orbit Quantenschlüssel erzeugen und per Laser an verschiedene Bodenstationen verteilen.

Bis dahin bleibt die spannende Arbeit am leichter zugänglichen Bodensegment und die Herausforderung an dieses große notwendige Teilstück der gesamten Datenstrecke, damit die Tür in Richtung quantensicherer Satellitenbetrieb zum passenden Zeitpunkt aufzusperren. Mit einem Quantenschlüssel, versteht sich …

DR. JAN PITANN
DR. ANDREAS SPÖRL
Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR)

Security in the quantum computing era – Should we be worried today?

Imagine that in a few years from now on full-scale, practical quantum computer hits the headlines. In this scenario, the world of cryptography will be in a state of shock, since almost everything we know as the foundations of current security will collapse. Indeed, the presence of a quantum computer would render state-of-the-art, public-key cryptography useless, simply because all the underlying assumptions about the intractability of mathematical problems that offer confident levels of security today no longer apply in the presence of a quantum computer. But are we really doomed? Well, luckily not. This paper examines the technologies that will enable crypto to survive the post-quantum world. There are many things yet to be done to offer an equivalently safe environment as current crypto does, but the tools are there. It is now a game of engineering, pro-active standardization, and careful development approach to pave a safe way through what otherwise could turn out to be a "qubits inferno"

Introduction

Quantum computing no longer exists in the wild imagination and dusty drawers of some "unconventional" scientists. Considerable research efforts and enormous corporate and government funding for the development of practical quantum computing systems are being mobilized at this time. In fact, Google only recently announced quantum supremacy and although the underlying application might not be very practical (checking the outputs from a quantum random-number generator), it signifies that we are heading full speed to practical quantum computing platforms. The existence of a quantum computer as such would mark a cornerstone in mankind's technological evolution, as it would mean that computational problems which are currently considered intractable for conventional computers would be tractable for quantum ones.

Unfortunately, the intractability of some of these problems offers the foundations of state-of-the-art cryptography, hence they affect the trustworthiness and security of our digital world as a whole. This in turn implies that if a practical quantum computer was developed, much of today's public-key cryptography infrastructure such as RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography) would need to be replaced by algorithms that can offer the same – if not better – levels of security and of course resistance against cryptanalysis carried out by quantum computers.

Much to everyone's relief, modern cryptography does offer the tools to realize such quantum-safe cryptosystems; we present these solutions very

Scheme	Algorithm	Encryption	Signatures	Keys (bytes)	Remarks
Lattice-based	NTRUEncrypt, NTRUSign	✓	✓	1495 – 2062	Fast, short keys and signatures, 20 years of analysis
Code-based	McEliece, McBits	✓	✓	~958.482 – 1.046.739	Large keys, fast, 30 – 40 years of analysis
Multivariate	Rainbow, Gui, HFEv-	✓	✓	500.000 – 1.000.000	Short signatures, more analysis required
Hash-based	XMSS SPHINCS		✓	64 1056	High confidence, large signatures, state management
Elliptic Curve isogenies	SIKE, SIDH	✓	✓	564	Smallest keys and resources but no confidence yet

Table 1: The table contains indicative examples of post-quantum cryptographic solutions and associated features. Details can be found in [2] and the references therein

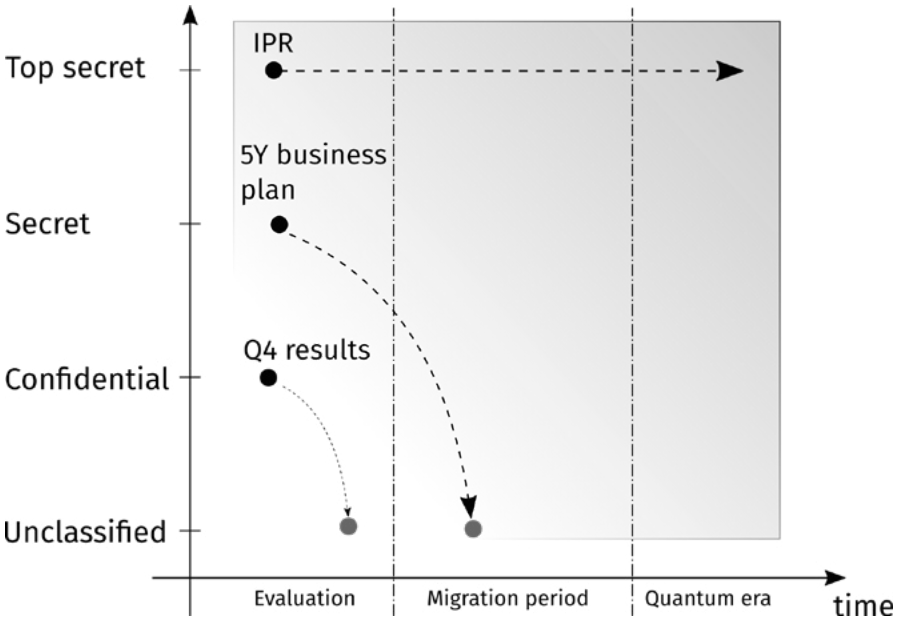

Fig. 1: Data retention and criticality as assessment criteria for switching to quantum-safe crypto

briefly and we highlight their basic strengths and pitfalls. Finally, we offer an outlook on future research and some suggestions when considering early deployments of quantum-safe cryptography.

Cryptography in the Post-Quantum Era

Before we proceed, an important clarification regarding the term "Quantum Cryptography" needs to be made. The term is often misinterpreted with the terms "Quantum-Safe Cryptography" or "Post-Quantum Cryptography". The latter two terms are basically the same thing and refer to cryptographic schemes based on the intractability of certain mathematical problems, just like current crypto does. Quantum Cryptography on the other side, refers to techniques utilizing the laws of physics and quantum mechanical properties to establish secure connections. The most important scheme is Quantum Key Distribution (QKD) which establishes a common key between two parties. This, in turn, has generated yet another misconception; QKD is not a solution to quantum computing cryptanalysis, but rather an alternative way to generate a shared secret key.

Regarding QKD there are important limitations since it requires authenticated channels, i.e., the use of traditional cryptography. This somehow contraposes the scope and the problems that quantum cryptography attempts to solve.

Furthermore, while QKD is secure in theory, it doesn't offer information encryption in real time. In addition, noise and attenuation in the quantum channel plague the key generation rates and transmission distances. While these challenges are being addressed actively by the research community as well as by commercial QKD solution providers, it is envisioned that "post-quantum cryptography" will undertake the main load of providing security – at least for a majority of applications.

Asymmetric Crypto

Research has produced some remarkable asymmetric cryptography constructions which are considered to be safe against quantum computers. A high-level overview is offered in Table 1 and actually many of those primitives have made it to the 3rd evaluation round of the NIST quantum-safe call [3]. In general, quantum-safe primitives currently evaluated implement public-key encryption, key-establishment schemes, and digital signatures, i.e., a full-scope portfolio of new asymmetric crypto solutions for the quantum era.

Symmetric Crypto

In a typical asymmetric cryptography setup, two parties that wish to establish a connection do not need to pre-agree to a common symmetric key; each party generates its own private and public key-pairs and at the end of the process the algorithms generate a common key based on the available key-pairs and underlying mathematics. This key is subsequently used in symmetric ciphers, which typically take care of fast payload encryption. Most prominent example is the AES symmetric algorithm.

Things are much easier for these primitives. Analysis has shown that they are immune by design to quantum analysis, hence, there is no need to devise new mechanisms. What is required is an increase in key-lengths (for example more than 256 bits), which, in any case, is already a safe security practice even by today's standards.

Way Forward

There are probably more open questions than answers at this point of time on what a quantum computer reality will look like. If quantum supremacy proves to be merely an engineering problem, then a practical quantum computer could be expected within the next 10–30 years, with the first releases targeting small-scale, engineering applications. This brings us to the topic of availability. Probably we will never see a quantum computer on our desks. We envision that such platforms will be hosted on an enter-

prise, educational/research, or government organization which can sustain the required resources to run and maintain a quantum computer. At the beginning the modus operandi will be probably via leasing time to end-users who would like to run their applications on these platforms; very similar to what is happening today with High Performance Computers.

Currently, not only NIST is evaluating quantum-safe key exchange and signatures algorithms (at the time of this writing the 3rd round is ongoing), but also IETF and ETSI are promoting standardization of post-quantum schemes. In 3GPP similar topics are actively being discussed in TR 33.841.

For the coming years, the deprecation strategy of current cryptography may be a challenge. Obsolete cryptographic primitives are still an issue, so if a quantum computer were to be released in a few years' time, discontinuing weak crypto would not be as straightforward as it sounds. Moreover, backdoors and vulnerabilities are still being published for generally proven and mature schemes, so it would be safe to assume that new algorithms might initially be found prone to vulnerabilities. This would call for immediate corrections, so alternatives need to be "deploy-ready" by that time. Finally, there is always the concern of "store now – decrypt later", i.e., adversaries with adequate resources who can intercept and store sensitive data today, will be able to decrypt them as soon as a quantum computer becomes available. In fact, this observation is rather important for security practitioners, CISOs and CIOs today. As demonstrated in Fig. 1, top management needs to assess the data retention vs. data criticality dynamics. As an example, Q4 results that will be published in a few days or even mid-term business plans that might be obsolete in a few years from now might not require quantum-safe encryption today. For business-critical data that need to be retained for many years to come, it would be unwise to switch to quantum-safe algorithms late along the process, as this would expose it to the risk of decryption by an adversary with access to a quantum computing platform. In fact, Fig. 1 illustrates indicative migration period before a practical quantum computer is announced. This timeframe is crucial for industries, hardware manufacturers, government organizations, regulators, etc. to evaluate and test quantum-safe cryptography and develop migration policies early enough.

On the practical side, our analysis suggests that lattice-based systems and elliptic curve isogenies could constitute the first practical deployments. After all, lattice-based systems are already part of hybrid or quantum-safe TLS (Transport Layer Security) and Internet Key Exchange (IKE) protocols. Thanks to their small keys and speed, they are suitable for constrained environments and fast communications, but cryptanalysis needs to step up to increase confidence towards these systems, especially for EC isogenies. Code-based solutions are also nice candidates since they are already quite mature, and they exhibit high speeds. Even though their keys are large, they could still be acceptable for applications that can host them and do not require frequent key-exchanges.

When it comes to implementation, we see great prospects for engineering and innovation. Industry needs to understand and encompass all the latest advances in this vibrant field. This will allow enterprises to develop safe interfaces between pre- and post-quantum schemes and tackle hardware/software compatibility issues that are likely to arise. Subsequently, we will need new performance benchmarks for applications switching to quantum-safe cryptography. The landscape around constrained IoT devices also seems quite challenging, since most of the primitives we examine require large keys, which suggests significant resources. Apparently, key players in hardware security need to enable their portfolio of safe security modules such as Trusted Platform Module (TPM), Trusted Execution Environment (TEE), Hardware Security Module (HSM) or tailored crypto-processors to support post-quantum crypto.

Finally, fundamental security protocols like TLS will need to be revised, and we expect incremental adaptations to quantum-safe algorithms as soon as their cryptanalysis is finalized. Until a full-fledged quantum-safe TLS is available, it would be safe to assume that hybrid versions will be rolled-out (i.e., supporting both quantum-safe algorithms and fallback options). Obviously, this poses yet another challenge for system administrators, as it will be rather challenging to implement and maintain a fully secure TLS infrastructure. Awareness on the latest advances in cryptanalysis is required in order to fallback promptly to safer algorithms supported by TLS.

A Final Word

While quantum computers will not change our lives at the flick of a switch a post-quantum-world holds both promise and risk. Notwithstanding, we need to have solid schemes to assure trustworthiness and security in a post-quantum world and crypto-experts around the world need to push for the best possible solutions. What is really required is proper awareness and education on what quantum computers can and cannot do. Not all problems are efficiently solved by quantum computers and dissolving quantum technology related myths is probably the best starting point towards building a safe and secure post quantum world.

References

[1] Arute, F.; Arya, K.; Babbush, R. et al.: Quantum supremacy using a programmable superconducting processor. Nature 574 (2019) pp. 505–510 (2019)

[2] Schoinianakis, D.; Martín-López, E.: Quo Vadis Qubit? Bell Labs Technical Journal 23 (December 2018), pp. 1–17

[3] NIST Post Quantum Cryptography: https://csrc.nist.gov/projects/post-quantum-cryptography

DR. DIMITRIOS SCHOINIANAKIS

Senior Security Researcher, NOKIA Bell Labs, Munich, Germany

Personalia

NEU GEWÄHLTER ITG FACHBEREICHSLEITER

Foto: Privat

Mit Wirkung zum 1.1.2021 hat der ITG Fachbereich „Dienste und Anwendungen“ (DA) seinen Leiter und Stellvertreter neu gewählt. Zum neuen Leiter wurde Professor Dr.-Ing. Sebastian Möller von der TU Berlin (Institut für Softwaretechnik und Theoretische Informatik, Quality and Usability Lab) berufen. Professor Möller leitet bereits den Fachausschuss DA 1 „Usability, Usable Security & Privacy“ und war bis 2020 Mitglied des ITG Vorstands. Er tritt die Nachfolge des langjährigen Fachbereichsleiters Dr.-Ing. Hans-Peter Quadt an. Erfreulicherweise steht Dr.-Ing. Quadt dem Fachbereich weiterhin als Stellvertreter zur Verfügung. Er übernimmt damit das Amt von Prof. Dr.-Ing. Volker Wittpahl.

Veranstaltungen

Hinweis: Weitere Veranstaltungen finden Sie auf den Seiten 46 und 47 des VDE dialog.

11.–16.07.2021, virtuell
27th International Congress on Sound and Vibration
// www.icsv27.org

19.–22.07.2021, virtuell
SMACD 2021 + PRIME 2021
ITG, IMMS GmbH, TU Ilmenau
// prime-conference.org
//smacd-conference.org

15.–18.08.2021, Wien und virtuell
DAGA 2021 – 47. Jahrestagung für Akustik
ISF, DEGA
// www.daga2021.eu

05.09.2021, Ingolstadt
7. Usable Security und Privacy Workshop
ITG, UPA, GI MCI, Projekt TrUSD
// www.vde.com/de/itg/veranstaltungen

06.–10.09.2021, Berlin
Summer School on AI for Optical Networks & Neuromorphic Photonics for AI Acceleration
ITG, Fraunhofer HHI
// www.vde.com/de/itg/veranstaltungen

13.09.2021, Lübeck / hybrid
MaLeNe 2021
Machine Learning in Networking
// www.vde.com/de/itg/veranstaltungen

13.–16.09.2021, Lübeck / hybrid
The Conference on Networked Systems (NetSys 2021) and ZdN 2021
ITG, Universität zu Lübeck, Technische Hochschule Lübeck
// www.netsys2021.org

22.09.2021, virtuell
Smart Sys Tech 2021
ITG, IEEE
// www.smart-systech.eu

23.–25.09.2021, Karlsruhe
MFI 2021 – IEEE International Conference on Multisensor Fusion and Integration
ITG
// mfi2021.org

29.09.–01.10.2021, Kiel
14. ITG Conference on Speech Communication
ITG
// www.vde.com/de/itg/veranstaltungen

09.–10.11.2021, virtuell
Wireless Congress 2021: Systems & Applications
ITG, Elektronik, elektroniknet.de
// www.vde.com/de/itg/veranstaltungen

10.–12.11.2021, Verona
26th European Wireless –Virtualization paradigms and satellite integration in future generation wireless communications (EW2021)
cnit, IEEE ComSoc, VTS, ITG
// ew2020.european-wireless.org

10.–12.11.2021, EURECOM, franz. Riviera, ggf. virtuell
25th International ITG Workshop on Smart Antennas (WSA 2021)
ITG, IMT, TUM, EURECOM
// www.wsa2021.org

Call for Papers

28.–30.09.2021, Miltenberg
Kleinheubacher Tagung 2021
Es wird gebeten, reguläre Tagungsbeiträge bis spätestens zum **13. Juli 2021** über www.kh2021.de/ einzureichen. Ein zusätzliches Konferenz-Paper kann zur Publikation auf IEEE Xplore bis zum **04.10.2021** über **www.kh2021.de/** eingereicht werden.

03.–04.11.2021, Osnabrück
25. ITG Fachtagung Mobilkommunikation
Bitte reichen Sie Ihre Präsentationen ein unter www.hs-osnabrueck.de/index.php?id=62646
Einreichungsfrist für Beiträge: 6. September 2021

14.–15.12.2021, Köln
28. ITG Fachtagung Kommunikationskabelnetze
Bitte reichen Sie Ihre Präsentationen ein unter www.vde.com/kkn-2021
Einreichungsfrist für Beiträge: 10. Juli 2021

27.02.–01.103.2022, Bremerhaven
TuZ 2022
Bitte reichen Sie Ihre Präsentationen ein unter www.tuz-workshop.de
Einreichungsfrist für Beiträge: 5. November 2021

Impressum

ITG news

Herausgeber: Informationstechnische Gesellschaft im VDE, Frankfurt am Main

Redaktion: Dr. Volker Schanz, Franziska Bienek

Telefon: 069/6308-360/-362
E-Mail: itg@vde.com
Internet: www.vde.com/itg

Konzept und Realisation: HEALTH-CARE-COM GmbH, ein Unternehmen der VDE VERLAG GmbH, Projektleitung: Anne Wolf

Druck: Heenemann GmbH & Co. KG, Berlin