06/2018 NOV/DEZ

NACHRICHTEN AUS TECHNIK, NATURWISSENSCHAFT UND WIRTSCHAFT

TECHNIK IN BAYERN

Das Regionalmagazin für VDI und VDE

Kryptologie

Eventkalender & Aktuelles
Maschinelles Lernen
40 Jahre Aktuelles Forum Technik

Universität Augsburg

Professionelle Weiterbildung für Führungskräfte

MBA Universität Augsburg

ZWW Zentrum für Weiterbildung und Wissenstransfer

www.mba-augsburg.de | www.zww.uni-augsburg.de

Sicher ist sicher


Foto: Sigl

Prof. Dr.-Ing. Georg Sigl
Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC

Wer hätte vor 10 Jahren gedacht, dass wir uns heute mit Freunden darüber unterhalten, WhatsApp oder Signal Ende-zu-Ende Verschlüsselung zu unterstützen? Oder haben Sie sich schon mal gefragt, warum Banken neue Kreditkarten mit einem Chip anstelle des Magnetstreifens ausstatten?

Der Grund dafür ist die Kryptographie, die der Chip unterstützt und der Magnetstreifen eben nicht. Kryptographie ist in unserem Alltag angekommen meist ohne, dass wir es merken. Doch Sicherheit ist manchmal unbequem, manchmal auch schwer anwendbar und manchmal richtig ärgerlich, beispielsweise wenn wir es wieder mal nicht schaffen, unseren Laptop an ein verschlüsseltes WLAN anzumelden, obwohl wir den Schlüssel doch bestimmt richtig eingegeben haben. Bemerkenswert ist auch, dass jemand schon fast als Experte gilt, der es schafft, eine verschlüsselte Email zu verschicken.

Zu einem Experten werden wir Sie mit diesem Heft sicher nicht machen. Wir wollen jedoch versuchen, Ihnen ein paar interessante Einblicke in die Historie und die Prinzipien der Kryptographie zu geben. Vielleicht hilft es ja beim Lösen des nächsten Problems, wenn man den Unterschied zwischen symmetrischer und asymmetrischer Kryptographie verstanden hat.

„Der Münchner Raum ist bereits heute ein Zentrum der Sicherheitsindustrie“

Wir zeigen, wie man im Internet der Dinge das Problem der Identifikation von Maschinen über eine Art Fingerabdruck von Materialien lösen kann. Auch Anwendungsbereiche wie Industrie 4.0 oder Telekommunikation werden in Beiträgen aus der heimischen Industrie vorgestellt.

Der Münchner Raum ist bereits heute ein Zentrum der Sicherheitsindustrie in Deutschland. Über 100 Firmen haben sich vor einigen Jahren zum Sicherheitsnetzwerk München zusammengeschlossen.

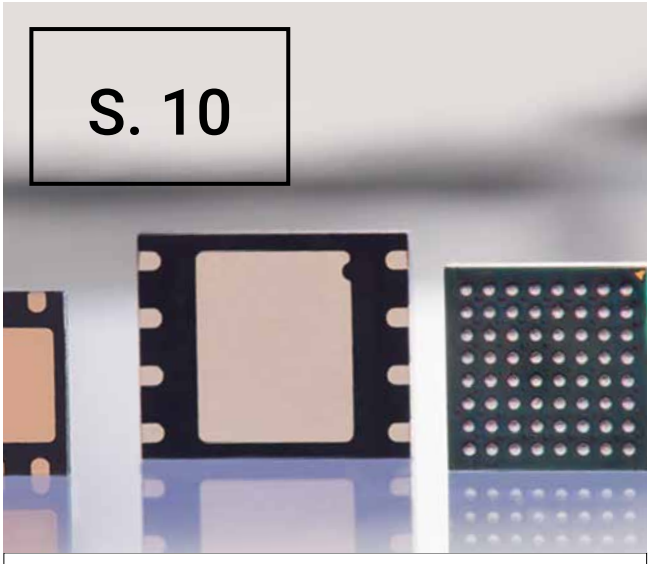
Vor 9 Jahren wurde das Fraunhofer Institut AISEC gegründet, um die Zusammenarbeit zwischen Forschung und Industrie zu stärken. In Neubiberg baut die Universität der Bundeswehr ein nationales Zentrum für Cybersicherheit auf. Es tut sich also bereits viel am IT-Sicherheits-Standort München. In naher Zukunft wird an der TUM in Garching ein neues Zentrum für Quantentechnik gebaut. Dort wird auch an Quantenkommunikation und -computing geforscht. Was geschieht, wenn der Quantencomputer realisiert wird? Dann ist ein Teil der Kryptographie gebrochen und wir sind nicht mehr in der Lage, sichere Internetverbindungen (https) aufzubauen. Deshalb forscht man an Algorithmen, die gegen Quantencomputer-Angriffe resistent sind. Absolut sicher ist auch die Quanten-Schlüsselverteilung, die Kollege Weinfurter an der LMU erforscht. Auch diese Zukunftsthemen behandeln wir in diesem Heft. Auf den kryptographischen Grundlagen dieses Heftes aufbauend, plant die TiB-Redaktion eine Ausgabe zur Cyber Security im nächsten Jahr.

Nun wünsche ich Ihnen viel Spaß bei der Lektüre dieser Ausgabe und ein paar neue Einsichten in die IT-Sicherheitsforschung und Entwicklung hier in München, die zukünftig eine weitere sichere Digitalisierung erst ermöglicht.

Kryptologie

Die Lehre des Verborgenen und des Verbergens, ist heute ein nicht mehr wegzudenkender Bestandteil der gesamten Sicherheit des Datenverkehrs.

SCHWERPUNKT



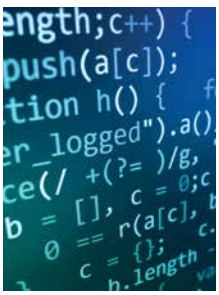
Sicherheit in der Telefonie:
eSIM-Karten zum direkten Verbauen auf Platinen

Fotos: Giesecke & Devrient

HOCHSCHULE UND FORSCHUNG

AKTUELLES

RUBRIKEN



Titelbild:
Foto: Shutterstock,
Best-Backgrounds

VDI Landesverband Bayern
VDI Bezirksverein München, Ober- und Niederbayern e.V.
Westendstr. 199, D-80686 München
Tel.: (0 89) 57 91 22 00, Fax: (0 89) 57 91 21 61
www.verein-der-ingenieure.de, E-Mail: bv-muenchen@vdi.de

VDI Bezirksverein Bayern Nordost e.V.
c/o Ohm-Hochschule, Keßlerplatz 12, D-90489 Nürnberg
Tel.: (09 11) 55 40 30, Fax: (09 11) 5 19 39 86
E-Mail: vdi@th-nuernberg.de

VDE Bayern, Bezirksverein Südbayern e.V.
Hohenlindener Straße 1, D-81677 München
Tel.: (0 89) 91 07 21 10, Fax: (0 89) 91 07 23 09
www.vde-suedbayern.de, E-Mail: info@vde-suedbayern.de

Einführung in die Kryptologie

Eine Geheimwissenschaft tritt an die Öffentlichkeit

Die Kryptologie, die Lehre von den Geheimschriften, begann Ende der sechziger Jahre aus ihrem Dasein als Geheimwissenschaft der militärischen und diplomatischen Dienste herauszutreten. Die heutige vernetzte Gesellschaft kann ohne Datensicherheit nicht mehr auskommen.

Ein entscheidender Einfluss war die rasche Entwicklung der Mikroelektronik und der damit verbundenen aufkommenden kommerziellen Informationsverarbeitung. In der heutigen vernetzten Gesellschaft stellen Informationen und die mit Informationsverarbeitung und -übermittelung verbundenen Dienstleistungen erhebliche kommerzielle Werte dar.

In zunehmendem Maße stützen sich auch wichtige Funktionen des Staates mehr und mehr auf die elektronische Informationsverarbeitung. Der Schutz der Informationen und Informationsflüsse ist deshalb mit der Stabilität von Staat, Wirtschaft und Gesellschaft eng verbunden. Die Kryptologie, als ein modernes Teilgebiet der angewandten Mathematik, liefert die Grundlagen für den Schutz von Informationen, zum Beispiel in Form von kryptographischen Basisalgorithmen, Kommunikationsprotokollen, Modellen von Angreifern, sowie Metriken für die Bewertung der Sicherheit der angewendeten Schemata.
Allerdings ist die Anwendung von Kryptographie auch ein brisantes politisches und gesellschaftliches Thema (z.B. Datenschutz und Privatsphäre versus Überwachung, Datensammeln und Vorratsspeicherung). Auch ist die korrekte und verantwortungsvolle Umsetzung ein Thema für die Industrie (z.B. Gefahr der fehlerhaften Umsetzungen mit Einfallstoren für Viren und Trojaner oder absichtlich eingebrachte Hintertüren).

Der erste Schritt: DES mit Lucifer

1977 wurde der erste Verschlüsselungsalgorithmus für nichtklassifizierte aber vertrauliche Informationen von der US-Bundesregierung als FIPS PUB 46 veröffentlicht. Dieser sogenannte „Data Encryption Standard" DES basierte auf einem von Horst Feistel (IBM) entwickelten Algorithmus namens Lucifer mit 128 Bit Schlüssellänge. Unter Beteiligung des Auslandsgeheimdienstes der Vereinigten Staaten NSA wurde daraus der DES mit einer reduzierten Schlüssellänge von 56 Bit abgeleitet. Die Veröffentlichung aller Details des Algorithmus führte zu einer enormen Weiterentwicklung der Kryptoanalyse im öffentlichen, d.h. akademischen und kommerziellen, Bereich. Der DES stellt den Prototyp einer Blockchiffre dar: Ein solcher Algorithmus wandelt in deterministischer Weise mit Hilfe eines Schlüssels Zeichenfolgen fester Länge (Nachricht) in andere Zeichenfolgen fester Länge (Chiffrat) um. Im Idealfall ist ein Dritter, der den Schlüssel nicht kennt, nicht in der Lage die ursprüngliche Nachricht aus dem Chiffrat wiederherzustellen. Aber mit Hilfe des richtigen Schlüssels kann man den Algorithmus in umgekehrter Richtung laufen lassen und die Nachricht wiedergewinnen. August Kerckhoffs Maxime (1883) folgend, soll die Sicherheit dieses Algorithmus nicht von der Geheimhaltung des Verfahrens an sich abhängen, sondern nur von der Geheimhaltung des verwendeten Schlüssels.

Public Key Verfahren

Mit der kommerziellen Verbreitung der Kryptographie entstanden viele neue Anforderungen, z.B. der Wunsch nach dem digitalen Unterschreiben von Verträgen (in diese Kategorie gehören auch Banküberweisungen und autorisierte Software-Updates), der verschlüsselten Kommunikation zwischen zwei Kommunikationspartnern ohne einen vorangegangenen persönlichen Schlüsseltausch, sowie dem Manipulationsschutz von großen Datenmengen. Ein wegweisender Meilenstein war die Entwicklung der sogenannten „asymmetrischen Schlüsselsysteme" (Public Key Kryptographie). Der Durchbruch gelang mit der Diffie-Hellman-Schlüsselvereinbarung (DH, 1976), einem Algorithmus, der es zwei Kommunikationspartnern ermöglicht, ausschließlich mit öffentlicher Kommunikation ein gemeinsames Geheimnis (Schlüssel) zu erzeugen. Die davon inspirierten Algorithmen von R. Rivest, A. Shamir und L. Adleman (RSA, 1977) und T. Elgamal (1985) versetzten die Wissenschaftler in die Lage, digitale Signaturen und die Public Key Verschlüsselung zu erzeugen. Dies ist eine Verschlüsselungsmethode mit einem geheimen und einem dazugehörigen öffentlichen Schlüssel. Dabei wird eine Nachricht mit dem öffentlichen Schlüssel verschlüsselt. Das Chiffrat kann dann ausschließlich mit dem geheimen Schlüssel entschlüsselt werden. Die Sicherheit des Verfahrens beruht darauf, dass der geheime Schlüssel aus dem öffentlichen praktisch nicht berechnet werden kann.

Schnelle Fortschritte in der öffentlichen Kryptoanalyse (z.B. differentielle und lineare Kryptoanalyse, LLL-Algorithmus) und ein enormer Zuwachs der verfügbaren Rechenkapazitäten führten sehr bald zur Erfordernis längerer Schlüssel und effizienterer Algorithmen. So ersetzte die im Jahr 2000 standardisierte Blockchiffre AES (Advanced Encryption Standard, FIPS PUB 197) mit Schlüssellängen von 128, 192 und 256 Bit den DES, da dessen kleiner Schlüsselraum von $2^{56} \approx 7x10^{16}$ heute auf Spezialrechnern aus FPGAs

oder Graphikkarten in wenigen Stunden vollständig nach dem richtigen Schlüssel durchsucht werden kann (Brute-Force Angriff). Die Mitte der 80 Jahre von V. Miller und N. Koblitz entwickelte Elliptische-Kurven-Kryptographie (ECC) ermöglicht Schlüsselvereinbarung (ECDH), Signatur (ECDSA) und Public Key Verschlüsselung mit wesentlich kürzeren Schlüsseln als bei den entsprechenden RSA/DH Algorithmen. So entspricht die Sicherheit eines RSA/DH Algorithmus mit 3072 Bit Schlüssel in etwa dem eines ECDH Algorithmus mit 256 Bit Schlüssel (was wiederum der Sicherheit einer Blockchiffre mit 128 Bit Schlüssel entspricht).

Angriff über die Anwendungen

Inzwischen werden diese Basisalgorithmen in unzähligen Anwendungen eingesetzt. Beispiele sind die Absicherung des Datenverkehrs im Internet (TCP/IP), Funknetze (GSM, WLAN), Fernwartung von Industrieanlagen, Banking, Software-Updates, Zugangskontrollen, Betriebssystemintegrität (TPM), Bezahlfunktionen (Chipkarten) und hoheitliche Dokumente (ePassport, eID). Sogenannte „kryptographische Protokolle“ regeln dabei das Zusammenspiel der oben erwähnten Basis-Algorithmen. Aufgrund der großen Zahl an funktionalen Anforderungen in den Anwendungen tendieren die Protokolle dazu, sehr komplex zu sein. Außerdem ist heute aufgrund der vielen verschiedenen Einsatzgebiete die Zahl der unterschiedlichen Protokolle schier unüberschaubar geworden. Die damit einhergehende mangelnde kryptoanalytische Evaluierungstiefe führte leider in der Vergangenheit immer wieder zu eklatanten konzeptionellen Fehlern, die gut funktionierende logische Angriffe erlaubten. Beispiele dafür sind die Angriffe auf WEP, das ehemalige Standard-Verschlüsselungsprotokoll für WLAN (FMS-Angriff), und auf S/MIME, ein weit verbreiteter E-Mail Verschlüsselungsstandard (Efail-Angriff). Eine weitere sehr große Klasse von logischen Angriffen zielt auf Fehler in der Implementierung von Protokollen. Dabei versucht der Angreifer typischerweise die Zustandsmaschine, die das Protokoll abarbeitet, gezielt mit außerhalb der Spezifikation liegenden Daten zu füttern. Das Ziel des Angreifers ist es, den Protokollablauf zu ändern, um z.B. mittels Pufferüberläufen nicht autorisierte Veränderungen am System vorzunehmen.

Angriff über Seitenkanäle

Die Implementierung von Krypto-Protokollen in unzähligen Geräten, welche für einen potentiellen Angreifer auch physikalisch direkt zugängig sein können (z.B. Kreditkarten, Ausweise, Smartphones, Automobile) ermöglicht noch weit potentere Angriffe. Im Jahr 1996 veröffentlichte P. Kocher einen Timing-Angriff (TA) auf die Implementierung von Diffie-Hellman, RSA, DSS und anderen Systemen. Er zeigte, wie kryptographisch sichere und auch korrekt implementierte Protokolle vollständig gebrochen werden können, wenn z.B. eine Abhängigkeit der Laufzeit des Algorithmus von den Bits des Schlüssels besteht – was typischerweise der Fall ist, wenn keine dedizierten Gegenmaßnahmen in die Software eingebaut werden.
Kurze Zeit später veröffentlichten P. Kocher, J. Jaffe, B. Jun (1999) die einfache und differenzielle Stromanalyse (SPA bzw. DPA), die auch Implementierungen von Algorithmen, welche gegen TA gehärtet

Quelle: Nokia

sind, brechen kann. Dabei wird, z.B. mit einem Oszilloskop, die zeitliche Stromaufnahme während der Berechnung aufgezeichnet. Die winzige Korrelation zwischen den verarbeiteten Schlüsselbits und der Stromaufnahme kann mit einer recht einfachen statistischen Analyse ausgenutzt werden um den Schlüssel zu rekonstruieren. Über diesen passiven Angriff hinausgehend, kann ein aktiver Angreifer das elektronische Gerät auch während der Ausführung des Krypto-Algorithmus stören (z.B. Spannungspuls, Lichtblitz, Laser). Der Bellcore-Angriff auf RSA (1997) und der differentielle Fehlerangriff (DFA) von G. Piret und J-J. Quisquater (2003) zeigten, dass auch die Beobachtung des Resultats eines eingebrachten Fehlers während der Berechnung sofort zur Rekonstruktion des vollständigen Schlüssels ausgenutzt werden kann. Die Mächtigkeit dieser sogenannten Seitenkanal-Angriffe hat in den letzten beiden Jahrzehnten zur Entwicklung von besonders gehärteten Sicherheitsprozessoren geführt, die heute ubiquitär eingesetzt werden – in elektronischen Personalausweisen und Pässen, in Chipkarten für den Zahlungsverkehr, in Secure Elements (SE) in Mobiltelefonen und im Automobil, in Trusted Platform Modules (TPM) im Personal Computer und vielen anderen Geräten. Mit Meltdown und Spectre haben die Seitenkanal-Angriffe nun im Jahr 2017 auch fast alle modernen Mikroprozessoren getroffen, die z.B. in Desktops, Laptops, Cloud-Servern und Mobiltelefonen eingesetzt werden und üblicherweise keine Gegenmaßnahmen gegen Seitenkanal-Angriffe enthalten. Hierbei wird ein Timing-Angriff im Zusammenspiel mit gemeinsam genutzten Prozessor-Ressourcen (z.B. Caches) ausgenutzt um die strikte Separation von Prozessen zu umgehen.

Ein weiteres praktisches Problem in der Realisierung von sicheren kryptographischen Protokollen auf realer Hardware besteht in der Erzeugung und gesicherten Speicherung eines geheimen und individuellen Schlüssels. Das ist z.B. der Fall, wenn ein Mikrocontroller in einer Logiktechnologie gefertigt werden soll, die keinen eingebetteten beschreibbaren, nichtflüchtigen und gesicherten Speicher zur Verfügung stellt. Sogenannte „Physical Unclonable Functions“ (PUF) erlauben die Extraktion von einzigartigen Merkmalen aus Fertigungsschwankungen in den Transistoren oder der Verdrahtung, sofern diese statistisch hinreichend unabhängig über den Wafer verteilt sind. Aus diesen Schwankungen können dann mit Fehlerkorrekturverfahren und Entropie-Extraktoren chip-individuelle Schlüssel mit genügend hoher Variabilität erzeugt werden.

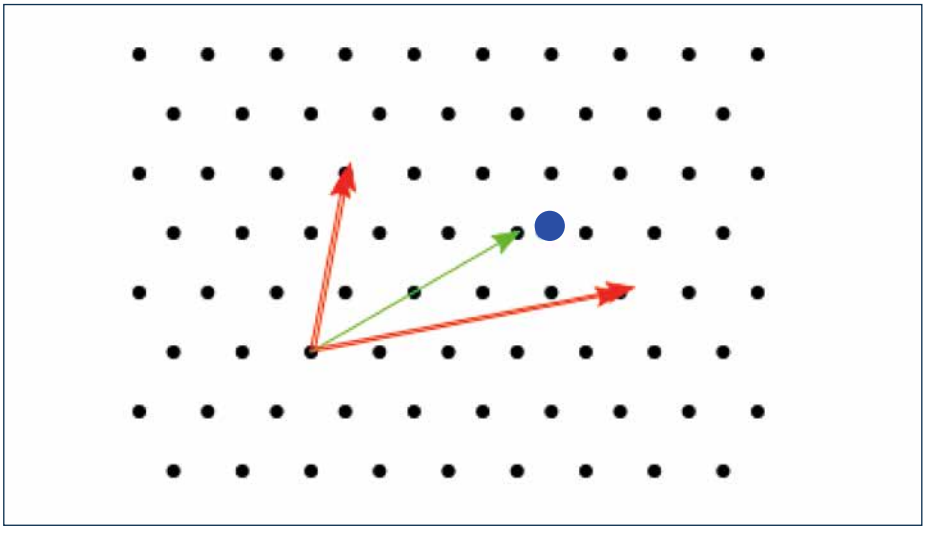
Der Quantencomputer am Horizont

Eine völlig neue Herausforderung ergibt sich für die Kryptologie durch die Möglichkeit, dass in Zukunft leistungsfähigere Quantencomputer gebaut werden könnten. Schon 1994 zeigte Peter Shor, dass die zugrunde liegenden mathematischen harten Probleme (Primfaktorisierung, diskreter Logarithmus), welche die zuvor genannten Public Key Verfahren auf einem klassischen Computer praktisch nicht brechbar machen, auf einem Quantencomputer effizient lösbar sind.

Dies führt dazu, dass man sich auf heute erstellte digitale Zertifikate und Signaturen zukünftig nicht mehr verlassen kann und, dass DH-Schlüsselvereinbarung und Publik Key Verschlüsselung nicht mehr ausreichend sicher sein werden (unabhängig von der gewählten Schlüssellänge). Aus diesem Grund hat das amerikanische National Institute of Standards and Technology (NIST) 2016 einen offenen Wettbewerb für Post-Quanten Kryptographie (PQC) ausgeschrieben, der bis ca. 2024 zu einer Auswahl von Standards für PQC-Algorithmen führen soll. Als erster PQC Internet-Standard (RFC 8391) wurde 2018 das auf Hash-Funktionen basierende XMSS-Signaturverfahren (eXtended Merkle Signature Scheme) veröffentlicht, welches als Quantencomputer-resistent gilt.

So stehen wir heute, wie vor einem halben Jahrhundert, wieder am Anfang einer neuen Ära in der Kryptologie, auch dieses Mal getrieben durch Fortschritte in Physik und Technik.

Dr. Berndt Gammel und
Dr. Wieland Fischer
Infineon Technologies AG



Quelle: TUM

Gitter bestehen aus den ganzzahligen Linearkombinationen linear unabhängiger Vektoren, den Vektoren einer sog. Gitterbasis. Wie findet man Gittervektoren, die möglichst nahe zu einem vorgegebenen Vektor liegen, der nicht zur Basis gehört, also z.B. der blaue Punkt in der Skizze? Was im Zweidimensionalen trivial erscheint, wird in Räumen mit vielen Dimensionen ein äußerst schwer lösbares mathematisches Problem, das durch diese Eigenschaft die Sicherheit entsprechender Verschlüsselungen garantiert.

Kryptologie – kurz gefasst

Eine kleine Begriffskunde

Die heute meist genutzte **asymmetrische Kryptographie**, nach ihren Erfindern Rivest, Shamir und Adleman RSA genannt, benutzt sowohl private als auch öffentliche Schlüssel, daher auch die Bezeichnung „Public Key Kryptographie". Im Kern beruht ihre Sicherheit darauf, dass man zwar große Primzahlen durch geeignete Algorithmen leicht generieren und auch leicht das Produkt aus zwei Primzahlen bilden kann. Zum Entschlüsseln einer Nachricht muss man aber die beiden Primfaktoren selbst kennen, denn es gibt bis heute kein effektives Verfahren, um sie „rückwärts" aus dem Produkt zu berechnen, ein Problem, das schon Euklid bekannt war. Diese **Faktorisierung** kann man beispielsweise für 119 = 7 *17 noch unschwer erraten, für große Zahlen mit etwa 3000 bit, wie sie heute zur Verschlüsselung verwendet werden, geht das jedoch nicht mehr. Der Quantencomputer wird diese Situation aber ändern.

Da RSA Berechnungen sehr aufwändig sind, dauert es sehr lange bis man eine umfangreiche Datenmenge, z.B. einen Vertragstext oder ein Software Update, verschlüsselt bzw. signiert hat. Deshalb hat man **Hashfunktionen** in die Kryptographie eingeführt. Eine Hashfunktion generiert aus einer langen Datei einen kurzen heute meist 256 bit langen Hashwert, der als „Fingerabdruck" der Datei bezeichnet werden kann und anstelle der gesamten Nachricht signiert wird. Ändert man die Datei auch nur ein Wenig, dann verändert sich der Hashwert drastisch. Verwendet man kryptographische Hashfunktionen, so haben unterschiedliche Dateien auch unterschiedliche Hashwerte. Ist dies nicht der Fall so spricht man von einer Kollision die nicht erwünscht ist, weil dann Änderungen der Datei nicht mehr erkannt werden können. Dann kann ein Hacker beispielsweise Malware einschleusen unter Missbrauch einer Signatur eines Softwareherstellers. Die heute meist eingesetzte kryptographische Hashfunktion SHA-2 erfüllt die Kriterien für eine sichere Hashfunktion:

- Einwegfunktion, d.h. es ist leicht y= h(x) aber extrem aufwändig und somit praktisch unmöglich die Umkehrfunktion $x=h^{-1}(y)$ zu berechnen
- Kollisionsresistenz, d.h. es ist sowohl praktisch unmöglich zu einem Paar $y_1= h(x_1)$ ein zweites Paar $y_2= h(x_2) = h(x_1)$ zu bestimmen als auch zwei beliebige Dateien x_1 und x_2 die den gleichen Hashwert liefern.

Hashfunktionen haben vielfältige Einsatzgebiete. Die Speicherung von Passwörtern in Form von Hashwerten ist vermutlich der bekannteste. Aufgrund der oben beschriebenen Einwegeigenschaft kann aus einer gestohlenen Passwortdatei das Passwort aus dem Hashwert nicht ermittelt werden. Auf dem gleichen Prinzip der Einwegfunktion beruht die Sicherheit der Postquantum sicheren Einmalsignaturen.

Gitter (engl. Lattice) sind Unterräume von reellen kontinuierlichen mehrdimensionalen Räumen. Sie entstehen durch Addieren von reellen Basisvektoren, die mit ganzen Zahlen skaliert werden. Das erzeugt einen Raum von Punkten, die wie ein Gitter angeordnet sind. In Gittern gibt es mathematisch schwierig zu lösende, sog. NP-vollständige Probleme. Dazu gehören das Finden des kürzesten Vektors im Gitter (SVP: Shortest Vector Problem) und das Finden des nächsten Gitterpunktes zu einem beliebigen Punkt im Raum der nicht auf dem Gitter liegt (CVP: Closest Vector Problem), siehe dazu die Abbildung auf S.8.

Prof. Dr.-Ing. Georg Sigl

Die TiB Redaktion empfiehlt als Einführung zur Kryptologie:
Ertl/Löhmann „Angewandte Krytografie", siehe hierzu die Rezension auf S. 48.

Kryptographie im Mobiltelefon

Authentifizierung und Verschlüsselung bei einem Alltagsgegenstand

Mobilfunknetze sind ein gutes Beispiel, um typische Anwendungen von Kryptographie, wie Authentifizierung und Verschlüsselung, an einem täglich benutzten Gegenstand zu erläutern.

Dass drahtlos übertragene Daten zu verschlüsseln sind, damit nicht schon ein geeigneter Funkempfänger zum Abhören ausreicht, leuchtet unmittelbar ein. Auch dass ein Benutzer authentifiziert werden muss, um bei der Nutzung des Systems entstehende Kosten sicher zuordnen zu können, ist nachvollziehbar.

Systemaufbau

Zunächst muss sich ein Mobilfunkteilnehmer gegenüber dem Netz authentisieren, also seine Identität und damit seine Berechtigung zum Benutzen des Netzes nachweisen. Die Identität ist durch eine weltweit eindeutige Nummer, die International Mobile Subscriber Identity (IMSI) gegeben. Der IMSI ist ein nur auf dem Subscriber Identity Module (SIM-Karte) im Mobiltelefon und im Authentisierungscenter des Netzbetreibers gespeicherter kryptographischer Schlüssel KI zugeordnet. Die SIM-Karte enthält einen speziellen Chip, der den geheimen Schlüssel sicher aufbewahren kann. Die ersten SIM-Karten wurden 1991 von der Firma Giesecke & Devrient in München entwickelt. Die Abbildung auf Seite 4 oben zeigt eine SIM Karte, die für drei Größen passt.

Die Authentisierung des Teilnehmers am Netz erfolgt mit einem Challenge-Response Verfahren. Wenn sich ein Netzteilnehmer mit einer bestimmten IMSI am Netz anmelden möchte, generiert das Authentisierungscenter eine Zufallszahl RAND (die „Challenge“) und schickt sie an den Teilnehmer. Mit Hilfe des geheimen Schlüssels KI muss der Teilnehmer daraus eine Antwort SRES („Response“) ausrechnen und zurück an das Authentisierungscenter schicken. Da es ebenfalls den Schlüssel KI besitzt, kann es prüfen, ob SRES korrekt berechnet wurde. Falls ja, wird dem Teilnehmer Zugang zum Netz gewährt. Das Protokoll ist in der Abbildung skizziert.

Mit Hilfe von KI wird außerdem aus der Zufallszahl RAND ein neuer kryptographischer Schlüssel Kc ausgerechnet. Sowohl SRES wie auch Kc werden in der SIM-Karte berechnet und dann an das Mobiltelefon weitergegeben, das SRES wie beschrieben an das Netz zur Authentisierung schickt. Kc wird als Schlüssel für die weitere Verschlüsselung des Funkverkehrs mit der Basisstation verwendet, die nicht in der SIM-Karte sondern im wesentlich rechenstärkeren Mobiltelefon stattfindet.

Der Algorithmus zum Berechnen von SRES und Kc aus RAND und KI kann vom Netzbetreiber frei gewählt werden, da er nur auf der von ihm herausgegebenen SIM-Karte und im von ihm betriebenen Authentisierungscenter implementiert sein muss. Die Sprachverschlüsselung ist stärker standardisiert, da jedes Mobiltelefon und jede Basisstation sie beherrschen muss.

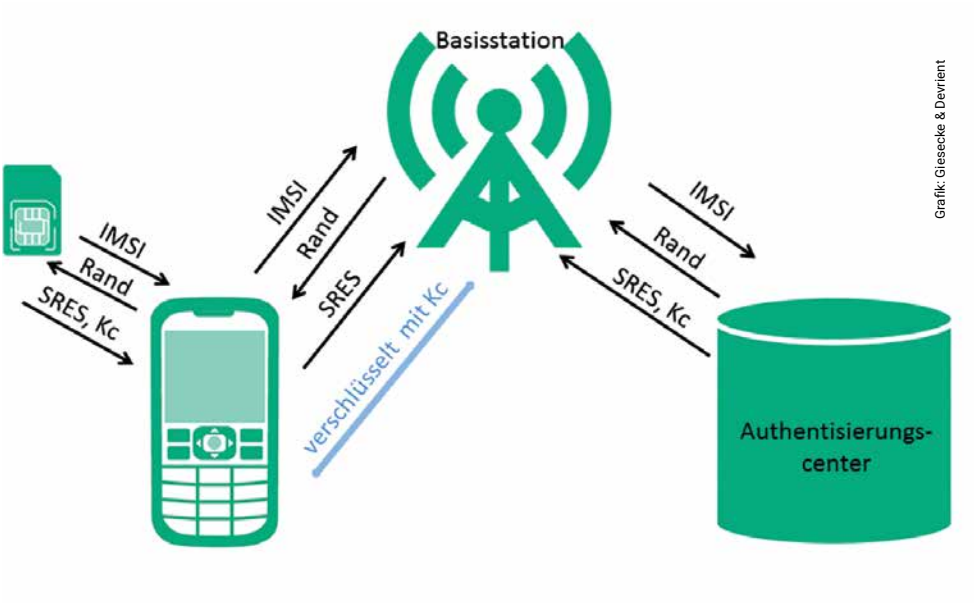
Sicherheitsaspekte

Zunächst kann man die mathematische Sicherheit der einzelnen Algorithmen zur Authentisierung, Schlüsselableitung und Verschlüsselung des Datenverkehrs betrachten. Die Algorithmen zur Authentisierung und Schlüsselableitung kann der Netzbetreiber zwar beliebig wählen, aber der UMTS-Standard schlägt zwei alternative Verfahren namens Milenage und TUAK vor. Milenage basiert auf dem Advanced Encryption Standard (AES), TUAK dagegen auf der Hash-Funktion KECCAK. Gegen beide sind keine praktikablen Angriffe bekannt.

Die anfangs bei GSM eingesetzten Algorithmen A5/1 und A5/2 zur Verschlüsselung der Datenübertragung haben inzwischen bekannte mathematische Schwächen. Auch für den neueren Verschlüsselungsalgorithmus Kasumi wurden 2010 sogenannte „related key attacks“ veröffentlicht, es ist aber noch kein daraus abgeleiteter Angriff bekannt, der das Abhören einer Verbindung ermöglicht.

Genauso wichtig wie die mathematische Sicherheit der einzelnen kryptographischen Algorithmen ist die Sicherheit des gesamten Protokolls, also die Art, wie die einzelnen Algorithmen im Gesamtsystem eingesetzt werden. Beispielsweise muss sich im GSM-Netz das Mobiltelefon gegenüber dem Netz authentisieren, also nachweisen, dass es berechtigt ist, das Netz zu nutzen. Da umgekehrt keine Authentisierung des Netzes gegenüber dem Mobiltelefon vorgesehen ist, kann ein Angreifer eine gefälschte Basisstation aufstellen, die vorgibt, keine Verschlüsselung des Datenverkehrs zu beherrschen. Mobiltelefone in der Nähe bauen dann eine unverschlüsselte Verbindung zu dieser gefälschten Funkzelle auf. Leitet der Angreifer die eingehenden Datenströme über eine eigene Verbindung weiter, kann er den unverschlüsselten Datenstrom abhören. In UMTS und LTE Netzen existieren Mechanismen, um solche Angriffe zu verhindern. Allerdings endet auch in UMTS und LTE Netzen die Verschlüsselung an der Basisstation. Dort besteht also weiterhin eine Abhörmöglichkeit. Um das Roaming in fremden Netzen zu ermöglichen, existieren außerdem Mechanismen, damit Netzbetreiber und Dienstleister untereinander Schlüssel wie Kc austauschen können. Im Jahr 2014 wurde bekannt, dass sich so über unseriöse Dienstleister auch Privatleute

Schlüssel besorgen und Datenverkehr abhören können. Für Geheimdienste sollte der Zugriff ohnehin kein größeres Problem darstellen. Geheimnisträger benutzen daher gerne Mobiltelefone, die eine verschlüsselte Verbindung bis zum Gesprächspartner aufbauen. Ein Beispiel ist das als „Merkel-Phone“ bekannte Gerät der Bundeskanzlerin. Da es für solche Lösungen keine verbreiteten Standards gibt, müssen beide Gesprächspartner über kompatible Geräte oder Software verfügen. Seit den Snowden-Enthüllungen haben auch einige weit verbreitete Messenger-Dienste wie WhatsApp eine derartige Ende-zu-Ende-Verschlüsselung eingeführt und so kostengünstig der Allgemeinheit verfügbar gemacht.



Protokolle zwischen SIM-Karte, Mobiltelefon und Netz

Ein dritter Aspekt ist die physikalische Sicherheit. Bei der Betrachtung der mathematischen Sicherheit der kryptographischen Algorithmen und der Protokollsicherheit wird außen vor gelassen, dass konkrete Geräte mit physikalischen Eigenschaften beteiligt sind. Man geht davon aus, dass ein Angreifer nur die über Funk ausgetauschten Daten mithören oder manipulieren oder eigene Daten einschleusen kann. Interessant ist aber auch die Frage, welche Möglichkeiten ein Angreifer hat, der nicht nur auf die Verbindung, sondern auch auf einen der Verbindungsendpunkte Zugriff hat. Der Sicherheitsanker im Mobiltelefon ist wie beschrieben die SIM-Karte. Da fast jeder ein Mobiltelefon in der Tasche trägt, ist es nicht zu vermeiden, dass SIM-Karten experimentierfreudigen Angreifern in die Hände fallen. Es hat sich herausgestellt, dass die Stromaufnahme eines Mikroprozessors während der Abarbeitung eines Programms vom Programm und den verarbeiteten Daten abhängt. Mit ausgeklügelten statistischen Auswertungen solcher Strommessungen ist es daher unter Umständen tatsächlich möglich, Rückschlüsse auf den in einer SIM-Karte gespeicherten geheimen Schlüssel zu ziehen. Zwar erfordert ein solcher Angriff einigen Aufwand und der wirtschaftliche Schaden für einen Netzbetreiber scheint zunächst gering. Würden solche Angriffe aber tatsächlich durchgeführt und publik werden, wäre das Kundenvertrauen, insbesondere das in die Korrektheit der eigenen Telefonrechnung, erschüttert. Daher wird bei der Implementierung der kryptographischen Software von SIM-Karten oft ein hoher Aufwand betrieben, um sicherzustellen, dass die Stromaufnahme der SIM-Karte beim Ausführen der Software keine Rückschlüsse auf die in die Berechnungen eingehenden geheimen Schlüssel möglich sind.

Jenseits des Mobiltelefons: vernetzte Geräte

Mittlerweile sind über das Mobilfunknetz nicht mehr nur Mobiltelefone verbunden. Maschinen melden zur Ferndiagnose Zustandsdaten, Verkaufsautomaten teilen dem Betreiber mit, ob neue Ware nachgefüllt werden muss und Autos setzen bei einem Unfall selbständig einen Notruf ab. Aus Sicht des Mobilfunknetzes verhalten sich alle diese Geräte wie ein Mobiltelefon. In der Regel steckt in vernetzten Maschinen keine von einem Mobilfunkbetreiber herausgegebene SIM-Karte aus Plastik, sondern es wird ein entsprechender Chip direkt auf einer Platine verbaut. Zunehmend werden diese „SIM-Karten“ auch erst nach Inbetriebnahme einem Mobilfunkbetreiber zugeordnet. Das ermöglicht der noch recht junge Standard eSIM für solche embedded SIMs.

In einem modernen Mobiltelefon wird Kryptographie noch in vielen weiteren Anwendungen eingesetzt. So werden für den Aufbau sicherer Internetverbindungen oder für die Abwicklung von Zahlungsvorgängen Authentifizierung und Verschlüsselung benötigt, die ebenfalls mit Werkzeugen der Kryptographie umgesetzt werden.

Sven Bauer und Hermann Drexler
Giesecke+Devrient Mobile Security GmbH, München

Überprüfbare Sicherheit durch Quantenschlüsselverteilung

Erstmals ist eine Schlüsselverteilung möglich, die auch gegen Angriffe eines Quantencomputers gefeit ist.

Es gibt viele Möglichkeiten, die Übermittlung von Nachrichten abzusichern. Aber, was bedeutet „sicher"? Bei allen konventionellen Verfahren sind wir auf Annahmen angewiesen: wir müssen zum Beispiel darauf vertrauen, dass unser Verfahren ohne back-door konzipiert wurde, dass Zertifikatsdaten nicht gehackt wurden, oder dass es eben noch keinen Quantencomputer gibt, mit dem die heute verwendeten public key systeme entschlüsselt werden könnten. Anders bei der Quantenschlüsselverteilung: ausgehend von physikalischen Gesetzen können wir die Information, die ein potentieller Abhörer haben könnte, messen und erhalten so erstmals wirklich überprüfbare Sicherheit.

Der Schlüssel zur sicheren Kommunikation

Das Prinzip der Quantenkryptographie, oder genauer, der Quantenschlüsselverteilung (englisch: quantum key distribution QKD), wurde 1984 von Charles Bennett und Giles Brassard vorgeschlagen. Für fast alle konventionellen Kryptographieverfahren benötigt man eine geheime, zufällige Bitfolge als Schlüssel. Zu seiner Erzeugung verwendet die Quantenschlüsselverteilung nur grundlegende, einfache Eigenschaften der Optik und Quantenmechanik, die man sich auch gut mit polarisiertem Licht veranschaulichen kann. Licht, das zum Beispiel vertikal polarisiert ist, kann ungestört durch ein vertikal orientiertes Polarisationsfilter (Abbildung 1a), wird aber vollständig durch ein horizontal orientiertes Filter absorbiert (Abbildung 1b). Das genügt bereits, um binäre Signale zu senden, zum Beispiel vertikale Polarisation für „1" und horizontale Polarisation für „0". Der Sender könnte für eine Reihe von Lichtpulsen jeweils zufällig zwischen den beiden Richtungen wählen und dem Empfänger eine zufällige Bitfolge übermitteln. Würde der Sender einzelne Lichtquanten, Photonen, senden, könnte es natürlich passieren, dass bei der Übertragung einige verloren gehen. Meldet der Empfänger an den Sender, zu welchen Zeitpunkten er ein Photon detektierte, so können die beiden die ursprüngliche Bitfolge auf diese Zeitpunkte reduzieren und eine etwas kürzere, aber noch immer zufällige Folge erhalten.

Ein Abhörer könnte sich aber noch ohne Probleme dazwischenschalten, die Polarisation der Photonen messen und an den Empfänger weitersenden. Auch wenn einzelne Photonen verwendet werden, kann eindeutig zwischen den beiden Einstellungen unterschieden werden. Dies ändert sich sofort, wenn alternativ und zufällig 4 Richtungen, nämlich horzontal/vertikal und +45° und -45° lineare Polarisation für die Kodierung verwendet werden. Horizontal oder vertikal polarisiertes Licht wird mit gleicher Wahrscheinlichkeit durch ein unter +45° orientiertes Filter gehen. Hat nun zum Beispiel der Sender horizontal/vertikal verwendet, der Abhörer (Eve in Abb.1c) aber diagonal, so wird er mit 50% Wahrscheinlichkeit ein falsches Zeichen gemessen haben. Jetzt ist es auch wichtig, dass nur ein einzelnes Photon geschickt wird, da der Abhörer dann nämlich auch nur eine einzige Messung durchführen kann, und nur in einer der zwei Alternativen. Schickt er aber nun sein Zeichen weiter an den Empfänger, und misst dieser gerade in der horizontal/vertikalen Einstellung, so ist auch dieses Resultat zufällig und, vor allem, unabhängig vom Signal des Senders (Abbildung 1c). Auf diese Weise entsteht in der Zeichenfolge zwischen Sender und Empfänger mit einer Wahrscheinlichkeit von 25% ein Fehler. Man kann nun allgemeine Angriffe formulieren und so zeigen, dass ein direkter Zusammenhang zwischen der Information, die ein Abhörer maximal haben könnte und der Fehlerwahrscheinlichkeit der vom Empfänger detektierten Bitfolge besteht. Durch entsprechendes Verkürzen des Schlüssels kann diese Information beliebig klein gemacht werden und so erstmals messbare Sicherheit für zufällige Schlüsselfolgen erhalten werden.

Grundlegende physikalische Gesetze geben uns also die Möglichkeit, nicht nur festzustellen, dass ein Abhörer einen Angriff gestartet hat, sondern sogar, wieviel Information er maximal erhalten haben könnte. Durch geeignete Verkürzung des Schlüssels kann seine Information ausradiert werden und so verlässliche Sicherheit gewährleistet werden.

Vom ersten Test zu sicheren Netzwerken

Nach einem ersten Experiment durch Bennett, Brassard und Kollegen bei IBM im Jahr 1992 begannen zahlreiche Gruppen weltweit das Konzept zu erweitern oder in Experimenten zu testen. Bereits im Jahr 2001 wurde die Firma IdQuantique durch Wissenschaftler der Universität Genf gegründet. Ihre Produkte, zum Beispiel für Punkt-zu-Punkt Verbindungen mit 100 Gbit/s, sind die ausgereiftesten Kommunikationssyteme derzeit. Daneben etablierten sich eine Reihe von jungen Spin-off und auch Startup Firmen die derzeit neue Produkte anbieten. Von größeren Firmen engagieren sich insbesondere Toshiba und HUAWEI mit sehr aktiven Forschungsgruppen.

Für die technische Umsetzung können mittlerweile auch sehr schwache Lichtpulse, im Mittel mit weniger als einem Photon, verwendet werden. Sie werden

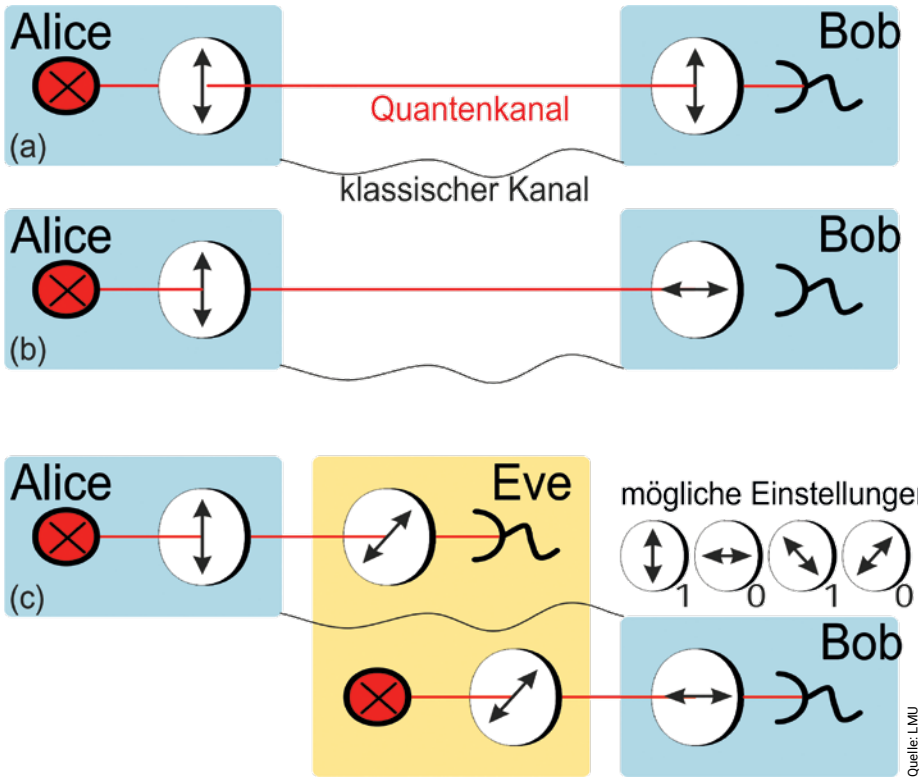


Abbildung 1:
Erzeugung eines sicheren Schlüssels mit Photonen polarisiert in unterschiedlichen Richtungen. Alice: Sender eines Schlüssels, Bob: Empfänger, Eve: Abhörer

entweder direkt durch die Luft mittels Linsen oder Teleskopen übertragen, oder durch eine Glasfaser. Wichtig dabei ist, dass das Signal nicht zum Beispiel in Repeatern gemessen oder verstärkt werden darf, da dies eine ähnliche Fehlerstatistik wie ein Abhörversuch verursachen würde. Wegen der unvermeidlichen Abschwächung entsteht so eine obere Grenze, bis zu der noch genügend viele Lichtpulse des Senders verglichen mit dem Rauschen der Detektoren oder Streulicht detektiert werden können.

Dank der Entwicklung hocheffizienter Detektoren für einzelne Lichtquanten konnte Anfang 2018 von der Universität Genf sogar noch über etwas mehr als 400 km ein Schlüssel sicher übertragen werden. Ein sogenannter Quantenrepeater wird in der Zukunft auch größere Entfernungen ermöglichen, setzt aber noch wesentliche Entwicklungen voraus wie sie im Moment zum Beispiel deutschlandweit in einem BMBF Verbund in Angriff genommen werden. Möchte man über größere Entfernung bereits heute kommunizieren, so kann ein Netz aus sogenannten sicheren Knoten aufgebaut werden. Derartige Netzwerke wurden vor etwa 10 Jahren in kleinem Stil in Europa getestet, und bilden nun eine ausgedehnte Infrastruktur in China über eine Strecke von 2000 km zwischen Peking und Shanghai mit mehr als 200 Verbindungen zu Behörden, Banken und großen Firmen in verschiedenen Städten. China ist auch führend dabei, Quantenschlüsselaustausch weltweit zu ermöglichen. Der im Jahr 2016 gestartete Satellit MICIUS konnte bereits erfolgreich Schlüssel mit Bodenstationen in China und Österreich austauschen. Als fliegender, sicherer Knoten kann er jeden beliebigen Punkt auf der Erde an Netzwerke für sichere Kommunikation anschließen.

Neben immer größeren Entfernungen geht die derzeitige Entwicklung auch zu immer höheren Raten. Hier wird der Rekord von der Gruppe der Firma Toshiba gehalten, die im Frühjahr 2018 vor allem dank einer sehr schnellen Kontroll- und Auswerteelektronik eine Rate von 10Mbit/s über eine 10 km lange Glasfaserstrecke erreichen konnte. In Bayern arbeiten wir an der LMU München zum Beispiel an nur Streichholz großen Systemen für den Sender. Am Max-Planck-Institut Erlangen (MPL) entwickelt das Team integrierte Module für Übertragungssysteme, die auch bei starker Streustrahlung in Glasfasern oder bei Tageslicht noch verwendet werden können. Generell versuchen wir, die Systeme so klein und einfach wie möglich zu machen um sie direkt in unterschiedlichsten herkömmlichen Kommunikationssystemen zu integrieren. Neben Glasfaserverbindungen sind zum Beispiel mobile Systeme denkbar, oder Komponenten für kleinere, kostengünstigere Satelliten. An einem derartigen Projekt arbeiten derzeit in Bayern MPL und LMU mit den im Satellitenbau erfahrenen Teams vom DLR und OHB in Oberpfaffenhofen und vom ZfT Würzburg zusammen.

Mit der Quantenschlüsselverteilung gibt es also nun ein System, das erstmals messbare Sicherheit gewährleistet. Es ist auch gefeit gegen Angriffe eines Quantencomputers und bildet so die erste Methode mit sogenannter post-quantum Sicherheit. Dank der immer schnelleren technologischen Entwicklungen steht in Zukunft ein System zur Verfügung, das in herkömmliche Glasfaser- oder Freiraumkommunikationssysteme integriert werden kann, und so dem Anwender auch ohne Kenntnis der Quantenmechanik sichere Kommunikation ermöglicht.

Prof. Dr. Harald Weinfurter
Department für Physik
Ludwig-Maximilians-Universität
München

Sicherheit in Industrie 4.0

Die Bedeutung der Informationssicherheit steigt kontinuierlich an

Unsere vernetzte und digitalisierte Welt schafft im Rahmen von Industrie 4.0 ein hohes Potenzial für weitere Automatisierung von Prozessabläufen und wird zu einer globalvernetzten Zusammenarbeit in vielen industriellen Bereichen führen. Gleichzeitig steigt die Bedeutung des Themas Informationssicherheit in all seinen Ausprägungen (IT-Security, Cyber Security, Industrial Security) kontinuierlich an.

Die Möglichkeiten böswilliger Angriffe auf industrielle Systeme nehmen schon auf Grund der steigenden Vernetzung zu: Vormals isolierte Anlagen werden durch Kommunikationsnetze über Ländergrenzen hinweg verbunden, die Zusammenarbeit entlang von Supply Chains wird zunehmend automatisiert. Außerdem steigen auch die Fähigkeiten potenzieller Angreifer durch eine verbreiterte Verfügbarkeit von Angriffstechnologien und Know-how, bis hin zu kommerziell buchbaren Angriffen durch kriminelle Anbieter im Darknet.
Industriefirmen müssen daher deutlich mehr Vorsorge für den Schutz der Informationssicherheit leisten, als es in der Vergangenheit üblich war. Eine adäquate Security stellt eine notwendige Voraussetzung für erfolgreiche Industrie 4.0 (I4.0) Prozesse dar. Typische Sicherheitsanforderungen für Industrie 4.0 Anlagen und deren Entwicklung sind:

Kommunikationssicherheit, Ende-zu-Ende Sicherheit in die Anwendung integriert

Die Kommunikation zwischen interagierenden Geräten (und Anwendern) muss vor dem Zugriff Unberechtigter durch kryptographische Mechanismen geschützt werden. Insbesondere für die Kommunikation zwischen unterschiedlichen Standorten sind kryptographische Schutzmechanismen unumgänglich. Dabei wird für viele Anwendungen End-to-End-Security erforderlich sein, die über eine reine Netzabschottung durch kryptographisch unterstützte VPNs (Virtual Private Networks) hinausgeht. Geräte und Anwendungen müssen über unterschiedliche Standorte hinweg sicher kommunizieren können und das Sicherheits-Niveau des jeweiligen Partners verlässlich kennen.

Authentifikation und sichere Identitäten für Geräte

Eine sichere Kommunikation setzt gegenseitige Authentifikation der beteiligten Geräte voraus. Dafür sind sichere Identitäten erforderlich, die den Gräten zugewiesen und fälschungssicher implementiert werden müssen. Verschlüsselungsmechanismen werden logisch an diese Identitäten gebunden. Pro Gerät können für verschiedene Nutzer unterschiedliche (sichere) Identitäten erforderlich sein. Auch können über fabrikationsseitig integrierte Sicherheitsparameter die Zugriffsrechte der Anwender auf ein Gerät kontrolliert werden, um z.B. Mechanismen für den Know-how-Schutz umzusetzen (Lizensierung, Echtheitsschutz).

Global verfügbare Sicherheitsinfrastruktur

Globale Zusammenarbeit benötigt eine vertrauenswürdige und robuste Sicherheitsinfrastruktur, die sich sehr resilient gegen Attacken verhält. Diese Infrastruktur muss Verschlüsselungsmechanismen unterstützen (Key Management) und sollte die beteiligten Anwender bei der Beurteilung der Vertrauenswürdigkeit unterstützen können. Hier müssen umgehend international akzeptierte Standards erarbeitet werden.

Security für den „Digitalen Zwilling"

Neben der physikalischen Implementierung einer I4.0 Produktionsumgebung existiert auch der dazugehörige „Digitale Zwilling". Dieser enthält prinzipiell sämtliche mit der Produktion und dem Produkt verbundenen Daten. Im „Digitalen Zwilling" werden Produktionsprozesse geplant, simuliert, gesteuert und auch überwacht. Vieles dwavon geschieht auf von der physikalischen Produktion getrennten Plattformen (Cloud, Office-IT). Beide Welten kommunizieren kontinuierlich miteinander und benötigen das gleiche Security-Niveau, um zu verhindern, dass erfolgreiche Attacken das Gesamtsystem beschädigen.

Adaptive Sicherheitsarchitekturen und Langlebigkeit der Lösungen

Industrie I4.0 Produktionsstätten können sich sehr agil auf veränderte Produktionsanforderungen anpassen. Diese Anpassungsfähigkeit überträgt sich als Anforderung auf die dazugehörigen Sicherheitsarchitekturen und Mechanismen. Diese müssen zudem den langen Lebenszyklen von Geräten und Maschinen in der Fabrikation gerecht werden können. Da die Fähigkeiten von Angreifern mit der Technologieentwicklung kontinuierlich zunehmen, müssen z.B. kryptographisch basierte Sicherheitsmechanismen bei Bedarf im Feld nachgebessert werden können.

Security-by-Design als übergeordnetes Prinzip entlang der Wertschöpfungskette

Sicherheit muss auch prozessmäßig in den Lebenszyklus von Produkten und Anlagen integriert werden. Nachträgliche Add-on Maßnahmen sind insgesamt ineffizient. Dies erfordert ein durchgängiges „holistisches" Security-Konzept für jede Organisation. Als Gemeinschaftsaufgabe betrifft Security alle an der Wertschöpfungskette beteiligten „Stakeholder": Lieferanten von Komponenten und Software,

Hersteller, Integratoren, Betreiber und Benutzer. Jeder Beteiligte muss seinen Anteil der Verantwortung proaktiv wahrnehmen. Auch müssen die Wege der Supply-Chain entsprechend gegen Angriffe insbesondere gegen die Echtheit und Integrität der Komponenten gesichert sein.

Standardisierung ermöglicht sichere Infrastrukturen

Um Sicherheit und Vertrauenswürdigkeit von Komponenten und Anlagen für Industrie 4.0 und deren Teilprodukte entlang der Wertschöpfungskette gewährleisten und beurteilen zu können, sind internationale Standards erforderlich.

Bei Sicherheitsmechanismen und Algorithmen kann man sich auf existierende Ergebnisse bei ISO und IEC berufen. Existierende Standards für Prozesse und Industrial Security (I3.x) werden gerade auf ihre I4.0-Tauglichkeit überprüft und bei Bedarf erweitert (ISO 27xyz, IEC 62443). In Deutschland erarbeiten die nationalen Standardisierungsgremien DKE und DIN zusammen mit Vertretern aus Industrie und Hochschulen in der Plattform Industrie 4.0 derzeit die Anforderungen an die Standardisierung zur I4.0-Security.

Erste Handlungsempfehlungen finden sich in der „DIN/DKE – ROADMAP Industrie 4.0“ [1]. Deutsche Firmen und Wissenschaftler sind in der internationalen Standardisierung sehr aktiv und leiten in wichtigen Gruppen die Security-Arbeiten (z. B. IEC TC65, ISO/IEC JTC1 SC27, ISO TC-292WG4).

Umsetzung von Industrial Security

Zur Lösung der Sicherheitsprobleme bei Industrie 4.0 genügt es nicht, die aus der Office-Welt bekannten Lösungen und Prozesse einfach auf industrielle Installationen anzuwenden. Beide Welten weisen höchst unterschiedliche Charakteristiken auf, die in den zukünftigen Standards berücksichtigt werden müssen.

Industrielle Systeme und Bürowelt haben unterschiedliche Management- und Betriebseigenschaften SIEMENS

	Industrielles System	Büro IT
Schutzziel für die Sicherheit	Produktionsressourcen, Incl. Logistik	IT- Infrastruktur
Lebensdauer der Komponete	Bis zu 20 Jahre und mehr	3-5 Jahre
Verfügbarkeit / Zuverlässigkeit (System)	24 x 365 x ...	Mittel, Verzögerungen werden akzeptiert
Integrität	Hoch	Mittel
Vertraulichkeit (Daten)	Niedrig - Mittel für Produktionsebene Hoch für geschäftsrelevantes Know-how	Hoch
Echtzeitanforderung	Kann kritisch sein	Verzögerungen werden akzeptiert
Existierende physikalische Sicherheit	Sehr unterschiedlich	Hoch (für IT Service Center)
Anwendung von Patchen	Langsam / teilweise eingeschränkt durch Regulierung	Regelmäßig / geplant
Antivirus	Gelegentlich, schwer zu implementieren, Whitelist	Häufig, weit verbreitet
Sicherheitsprüfung / Audit	Zunehmend	Geplant und beauftragt
Sicherheitsstandards	In Entwicklung, Regulierung	Existiert

Deshalb wird in der Industrie der Begriff „Industrial Security“ benutzt. Die Tabelle stellt Randbedingungen und Eigenschaften gegenüber:

Insbesondere sind die Lebenszyklen der installierten Produkte und Komponenten höchst unterschiedlich: Industriekomponenten weisen eine Lebensdauer von bis zu mehreren Jahrzehnten auf, während zum Beispiel die Laufzeit „der“ typischen Office-Komponente „Notebook“ die 5-Jahresgrenze üblicherweise nicht überschreitet.

Wartungszyklen und -prozesse unterscheiden sich in der Industrie vollkommen von denen in Büro-Umgebungen; insbesondere hat sich der normale Büro-Anwender inzwischen an unregelmäßige und individuelle Update-Zeiten seiner Systeme und die damit verbundenen Produktivpausen gewöhnt. Für eine Produktionsanlage könnte man vergleichbare Stehzeiten keinesfalls akzeptieren. Diese Unterschiede wirken sich immens auf die Anforderungen und Implementierungen der erforderlichen Sicherheitsfunktionen aus. Für die Kryptographie wird man bei I4.0 auf existierende Ergebnisse zurückgreifen. Ändern werden sich allerdings die Anforderungen an die Implementierung der Algorithmen und Mechanismen.

Zusätzlich müssen global kompatible, vertrauenswürdige und benutzerfreundliche Sicherheits-Infrastrukturen standardisiert werden. In der Umsetzung muss die Vertrauenswürdigkeit insbesondere von sicherheitskritischen Komponenten gewährleistet sein, um mögliche Angriffe durch die Nutzung versteckter Funktionen oder Schwachstellen zu vermeiden. Dies erfordert eine sichere Supply Chain und durchgehende Qualitätskontrollen.

Siemens verleiht durch die Gründung der „Charter of Trust“ diesen Forderungen besonderen Nachdruck und setzt sich besonders proaktiv für die Definition und Umsetzung von Sicherheitsstandards für die Industrie ein [2].

Dr. Wolfgang Klasen
Siemens AG, München

Informationen

[1] DIN/DKE - ROADMAP Industrie 4.0; http://easyurl.net/720ed
[2] Siemens Charter of Trust http://easyurl.net/8919b

Physical Unclonable Functions

Das Geheimnis aus der Hardware

Für die dauerhafte Speicherung kryptographische Schlüssel in Chips sind besondere Maßnahmen nötig, damit der Schlüssel nicht auf einfache Weise von einem Angreifer ausgelesen werden kann. Eine zunächst überraschend erscheinende Möglichkeit ist die Messung chipindividueller Fertigungsschwankungen bestimmter Parameter und ihre Verwendung zur sicheren und kostengünstigen Schlüsselspeicherung.

Klassische Speicher sind häufig angreifbar, da sie optisch – wie bspw. sogenannte eFuses – oder auf anderem Weg ausgelesen werden können. Vielfach sind auch für geeignete Technologien zusätzliche Fertigungsschritte nötig, was zu hohen Kosten führt, weshalb solche Technologien nicht auf jedem Chip verfügbar sind. Der grundlegende kryptographische Nachteil eines nicht-flüchtigen Speichers ist, dass der Schlüssel auch vorhanden ist, wenn der Chip ausgeschaltet ist und aktive Gegenmaßnahmen – wie Sensoren – inaktiv sind. Ein Angreifer kann dann den Chip manipulieren und den geheimen Schlüssel auslesen. Eine Alternative zu einer permanenten Spannungsversorgung für die Aufrechterhaltung der Gegenmaßnahmen und eine Lösung für Anwendungsfälle, in denen kein sicherer nicht-flüchtiger Speicher verfügbar ist, bieten Physical Unclonable Functions, kurz PUFs. Diese können nicht nur als Schlüsselspeicher sondern auch für die Authentifizierung verwendet werden wobei ihre Nutzung als Schlüsselspeicher die derzeit wichtigste Einsatzmöglichkeit darstellt, auf die sich dieser Artikel zunächst fokussiert. Hierbei werden im folgenden Abschnitt sogenannte Silicon PUFs betrachtet, also PUFs die im klassischen Halbleiterprozess integriert werden können.

Vom Zufall zum Schlüssel

Den Ursprung des von PUFs erzeugten Geheimnisses stellen im Fertigungsprozess unvermeidbare Schwankungen dar, die selbst für den Hersteller nicht kontrollierbar sind. Solche Schwankungen treten im Fall von Silicon PUFs beispielsweise bei der Dotierung oder Belichtung auf und können als Zufall modelliert werden. Ziel ist es, pro PUF einzigartige und nicht vorhersagbare Fertigungsschwankungen reproduzierbar zu messen, also gewissermaßen einen Fingerabdruck des Chips zu generieren. Die bekanntesten PUFs basieren hierbei auf der Unvorhersagbarkeit des Initialzustands einer Speicher-Zelle (z.B. SRAM-PUF) oder der Laufzeitvariation von Logikgattern (z.B. Ringoszillator PUF).

PUFs generieren das chipindividuelle Geheimnis nur bei Bedarf. Ist der Chip ausgeschaltet oder wird das Geheimnis nicht benötigt, muss es nicht vorgehalten und somit auch nicht geschützt werden. Das Auslesen der PUF ohne den Chip einzuschalten oder die chipindividuellen Eigenschaften zu verändern (also das Geheimnis zu zerstören) ist praktisch nicht durchführbar. Für PUFs werden dabei in der Regel sehr grundlegende Strukturen wie SRAM-Zellen oder Logikgatter verwendet, sodass sie in jedem Fertigungsprozess ohne großen Mehraufwand realisiert werden können.

Allerdings muss das von PUFs erzeugte Geheimnis für die spätere Nutzung aufbereitet werden. Soll die PUF etwa für die Speicherung eines Schlüssels genutzt werden, muss dieser Schlüssel zuverlässig über die gesamte Lebenszeit des Chips immer wieder hergestellt werden können. Das von der PUF durch Messung ermittelte Geheimnis variiert jedoch; nicht nur aufgrund von Rauschen, sondern auch wegen Umgebungseinflüssen und Alterungseffekten (praktische Implementierungen setzen Fehlerwahrscheinlichkeiten von bis zu 15 %-25 % pro Bit an). Das mittels PUF erzeugte Geheimnis unterscheidet sich also bei jedem Messvorgang leicht. Um einen stabilen Schlüssel zu erzeugen, sind sehr effiziente, ressourcensparende Fehlerkorrekturverfahren notwendig [1]. Hier sind in den letzten Jahren erhebliche Fortschritte gemacht worden. Allerdings sind immer noch Fragen offen. Insbesondere wird erforscht, inwieweit sicherheitskritische Information bei der Verarbeitung des Geheimnisses durch die Fehlerkorrektur preisgegeben wird.

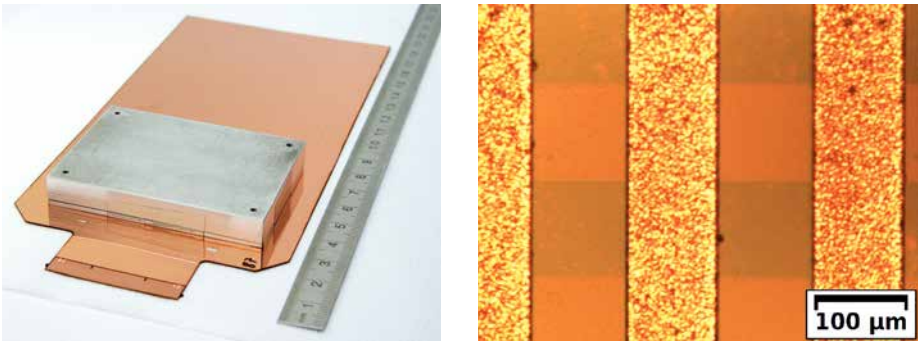


Abb. 1: Die von Fraunhofer entwickelte Schutzfolie aus feinen Leiterbahnen nutzt PUF-Eigenschaften zum Schutz ganzer Systeme

Alle Abbildungen: AISEC

Solche Leakage kann bspw. über Seitenkanäle (z. B. elektromagnetische Abstrahlung) oder durch gespeicherte Zusatzinformation für die Fehlerkorrektur (Helper Daten) entstehen.
Ein weiterer Forschungsschwerpunkt im PUF-Bereich ist die Qualitätsbewertung, insbesondere bezüglich der statistischen Vorhersagbarkeit des mit ihr gespeicherten Geheimnisses [2]. Das Finden von Maßen, die für PUFs eine statistisch belastbare Aussage über die Güte zulassen, stellt ein herausforderndes Problem dar, da in der Regel nur ein vergleichsweise kleiner Datensatz zur Verfügung steht. Auch sind Grundannahmen mancher Tests unzulässig, da etwa nicht vorausgesetzt werden kann, dass alle PUF-Antworten aus derselben Verteilung stammen. Geeignete Maße sind jedoch eine Grundvoraussetzung für eine sinnvolle Sicherheitszertifizierung von PUFs. Das Fraunhofer-Institut für Angewandte und integrierte Sicherheit AISEC und der Lehrstuhl für Sicherheit in der Informationstechnik der Technischen Universität München nutzen für die Analyse von PUF-Prototypen auf FPGA und zur Überprüfung der Eignung von PUF-Bewertungsmaßen ein am Fraunhofer AISEC befindliches FPGA Array (Abb. 2) [3] und tragen so zur Lösung dieser Aufgabenstellung bei.

PUFs als Schutz gegen Manipulationsversuche

Neben den bereits erwähnten Einsatzmöglichkeiten innerhalb von Siliziumchips können großflächigere PUFs auch genutzt werden, um Manipulationsversuche an ganzen eingebetteten Systemen zu unterbinden. Hierzu wurde am Fraunhofer AISEC in Zusammenarbeit mit Fraunhofer EMFT und IMS eine Schutzfolie mit PUF-Eigenschaften [4] entwickelt (Abb. 1): Ein engmaschiges Netz von Leiterbahnen wird in eine Folie eingebracht. Die Kapazitäten zwischen den Leiterbahnen unterliegen feinen Fertigungsschwankungen, die über eine Verstärkerschaltung gemessen werden. Wird die Folie von einem Angreifer manipuliert – z.B. entfernt oder durchbohrt – führt dies zu einer irreversiblen Veränderung von Kapazitäten. Ist das unter der Folie befindliche System – typischerweise ein eingebettetes System mit kryptographischen Geheimnissen oder schützenswerter Software – eingeschaltet, so kann der Angriff direkt aus einer Änderung zur Laufzeit detektiert werden. Ist das System ausgeschaltet, so sind alle sicherheitskritischen Informationen mit einem aus der Folie extrahierten Geheimnis verschlüsselt, welches durch den Angriff zerstört wird. Das Konzept erlaubt somit einen umfassenden Schutz aller im System gespeicherten kritischen Informationen. Anders als herkömmliche Schutzfolien erlaubt die Nutzung der PUF-Eigenschaften die Realisierung des Schutzes ohne permanente Spannungsversorgung aus einer integrierten Batterie. Dies ist z.B. im Hinblick auf Temperaturbereich und Lagerung, aber auch Größe und Gewicht vorteilhaft.

Fazit

Die in diesem Artikel vorgestellten Eigenschaften von PUFs erlauben ein hohes Sicherheitsniveau bei der Schlüsselspeicherung sowie den Schutz ganzer Systeme gegen Manipulation. Dabei können insbesondere auch leichtgewichtige Anwendungen geschützt werden, die über keine permanente Spannungsversorgung verfügen. Die Integration von PUFs ist überdies oft kostengünstig. Somit sind PUFs bspw. in Sensornetzwerken und im IoT-Bereich, aber auch darüber hinaus eine interessante und zukunftsträchtige Lösung.

Dr. Matthias Hiller und Dr. Michael Pehl
Fraunhofer AISEC und TUM Fakultät für Elektrotechnik und Informationstechnik

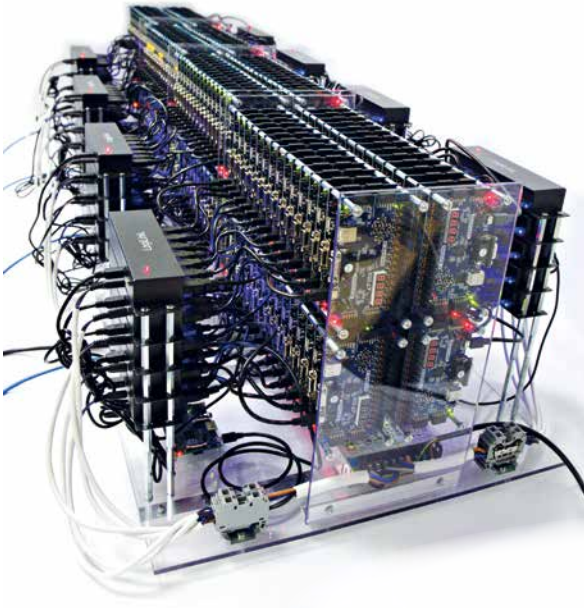


Abb. 2: Zur Bewertung von PUF-Prototypen und zum Test von Bewertungsmaßen wird ein FPGA-Array mit mehr als 200 FPGAs genutzt.

Literatur

[1] M. Pehl, M. Hiller und G. Sigl, „Secret Key Generation for Physical Unclonable Functions“, in Information Theoretic Security and Privacy of Information Systems, Cambridge University Press, 2017, pp. 362-389.
[2] F. Wilde, B. M. Gammel und M. Pehl, „Spatial Correlation Analysis on Physical Unclonable Functions“, IEEE Transactions on Information Forensics and Security, 2018.
[3] R. Hesselbarth, F. Wilde, C. Gu und N. Hanley, „Large scale RO PUF analysis over slice type, evaluation time and temperature on 28nm Xilinx FPGAs“, IEEE International Symposium on Hardware Oriented Security and Trust (HOST) , 2018.
[4] V. Immler, J. Obermaier, M. König, M. Hiller und G. Sigl, „B-TREPID: Batteryless Tamper-Resistant Envelope with a PUF and Integrity Detection“, IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 2018.

Post-Quantum Kryptographie

Der Weg in die Praxis

Public-Key-Kryptographie ist die Grundlage für den Aufbau sicherer Kommunikationskanäle. Allerdings bergen sogenannte Quantencomputer ein Risiko für diese Kommunikationssicherheit. Sobald solche Rechner ausreichend leistungsfähig sind, werden sie in der Lage sein, heute gängige asymmetrische bzw. Public-Key-Verfahren zu brechen und alle heute bekannten und genutzten symmetrischen Techniken zu schwächen. Um dieser Gefahr zu begegnen, werden sogenannte Post-Quantum Algorithmen benötigt.

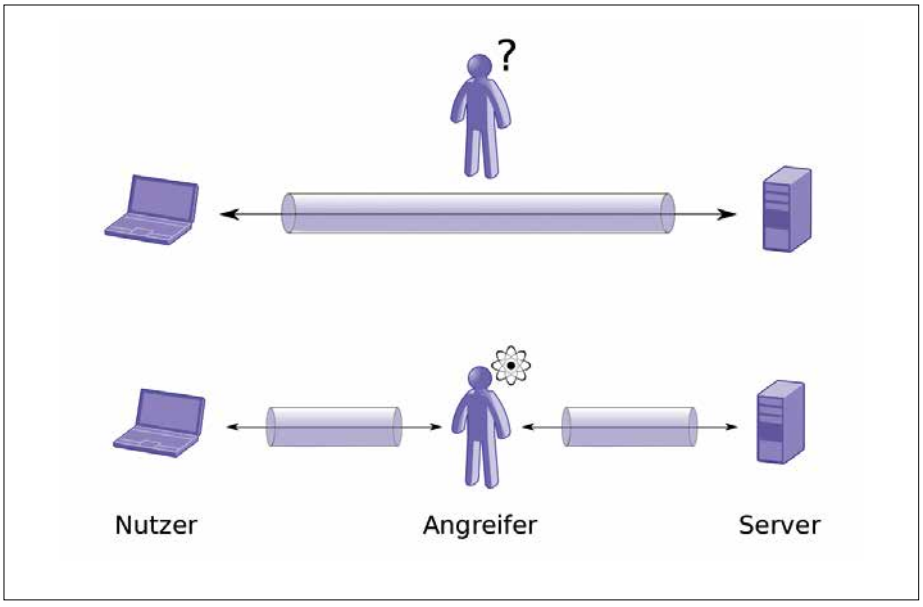
Quantencomputer erobern inzwischen selbst die Massenmedien und wissen dabei zu faszinieren. In der Presse werden sie gerne mal als Wundermaschinen dargestellt, die plötzlich alles besser können. Hinter Quantencomputern steckt jedoch keine Magie, sondern Wissenschaft. Das Grundprinzip solcher Computer beruht auf den Eigenschaften subatomarer Teilchen (den Quanten), die zu jedem Zeitpunkt potenziell in mehr als einem Zustand existieren können. Aufgrund der Art und Weise, wie sich diese kleinen Partikel verhalten, können bestimmte Rechenoperationen viel schneller als bei klassischen Computern ausgeführt werden.

Allerdings ist dieser Fortschritt auch mit einem Problem für die Sicherheit verknüpft. Bisher wissen wir dank der Arbeit von Shor [1], dass Quantencomputer effizient faktorisieren können. Das Faktorisieren großer Zahlen ist jedoch auch ein wichtiges mathematisches Problem, auf das sich die aktuelle Public-Key-Kryptographie stützt. Mit anderen Worten: Sobald die Quantencomputer über genug Rechenleistung verfügen, sind Verfahren wie RSA effizient angreifbar. Die Sicherheit symmetrischer Verschlüsselung wie AES ist ebenfalls von Quantencomputern betroffen: sie halbiert sich aus generischer Sicht, also bei Betrachtung ganzer Verfahrensarten, wie die Arbeit von Grover [2] gezeigt hat.

Im konkreten Beispiel würde das wiederum bedeuten, dass Anwendungen wie Online-Banking bzw. sichere Kommunikation über das Internet im Allgemeinen nicht mehr sicher sind, wenn ein Angreifer über einen hinreichend großen Quantencomputer verfügt, siehe Abb. 1. Deswegen ist es nicht überraschend, dass die Forschung schon länger untersucht, wie Sicherheit trotz der Gefahr durch Quantencomputer erreicht werden kann.

Post-Quantum Kryptographie

Seit mehr als 15 Jahren beschäftigen sich Kryptologen intensiv mit sog. kryptographischen Primitiven, die resistent gegen Quantencomputer sind. Als Ergebnis konnten Algorithmen gefunden werden, die auf harten Problemen im Bereich von Codes, Gittern, multivariaten Gleichungssystemen und Hashfunktionen basieren. Diese Gruppe von Algorithmen wird als Post-Quantum Kryptographie bezeichnet und ist nicht nur gegen klassische, sondern auch gegen Quantencomputer-basierte kryptanalytische Angriffe resistent. Die amerikanische Behörde für Standardisierung und Technologien, die NIST, hat deshalb Ende 2017 begonnen, im Rahmen eines Standardisierungsprozesses geeignete Kryptosysteme zu identifizieren, die für den Einsatz im Post-Quantum Zeitalter in Frage kommen. Diese sollen in den



Alle Abbildungen: genua GmbH

Abb. 1: In Anwesenheit leistungsfähiger Quantencomputer wären gängige kryptographische Mechanismen nicht mehr sicher: Klassisch abgesicherte Kommunikation (oben) kann mit solchen Rechnern gebrochen werden und ermöglicht Man-in-the-Middle-Angriffe (unten).

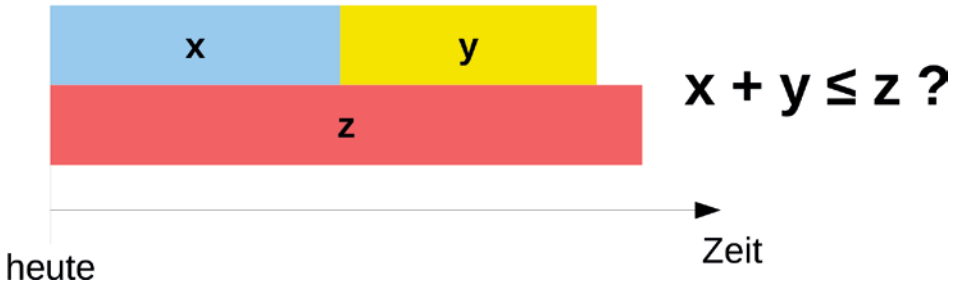


Abb. 2: Frei nach Michele Mosca [3]. Die Zeit x, die man benötigt, ein Post-Quantum Verfahren zu ersinnen plus die Zeit y, die es braucht, um das Verfahren erfolgreich in die Praxis zu bringen, darf nicht größer sein, als die Zeit z bis zur Konstruktion eines für gängige Kryptographie gefährlichen Quantencomputers.

folgenden Jahren von Experten analysiert und geeignete Verfahren letztlich dann auch standardisiert und für bestimmte Einsatzszenarien empfohlen werden.
Auch andere Gremien verfolgen ein ähnliches Ziel. So verfolgt die für Internetstandards zuständige IETF/IRTF mehrere Standards im Bereich der Post-Quantum Kryptographie, von denen ein erster auch schon im Rahmen von RFC8391 publiziert wurde [4,5].
Um diese Algorithmen in der Praxis nutzen zu können, müssen wir uns schon heute damit auseinandersetzen, wie wir den Weg entsprechend bereiten. Schon bei klassischen Verfahren hat sich gezeigt, dass für neue Verfahren von der theoretischen Beschreibung, über Analysen zur Sicherheit, die Normierung des Verfahrens bis hin zu der tatsächlichen Umsetzung und Verbreitung in der Praxis gerne 15 bis 20 Jahre vergehen, siehe Abb. 2. Dank der Forschung in den letzten Jahren wächst das Verständnis für die Sicherheit dieser Systeme weiter, aber es gibt noch viel zu tun, sowohl in der Theorie als auch in der Praxis – und die Zeit drängt:

Während die Theorie weiterhin die mathematischen Probleme untersucht, rückt potenziell der Tag näher, an dem Angriffe auf die Sicherheit mittels Quantencomputern möglich sind. Und so ist es nötig, dass gleichzeitig daran gearbeitet wird, wie die sichere Theorie auch sicher in die Praxis gebracht werden kann.

Auf dem Weg in die Praxis

Will man Post-Quantum-Verfahren in der Praxis einsetzen, so führt kaum ein Weg daran vorbei, etwaige Beschränkungen in Protokollen und Implementierungen aufzuweichen. Nichtsdestotrotz ist nicht nur die Analyse der Sicherheit, sondern auch die Optimierung der neuartigen Verfahren ein wichtiges Ziel der aktuellen Forschung. Schließlich will man übermäßigen Speicherbedarf und niedrige Geschwindigkeiten vermeiden. Sowohl der Lehrstuhl für Sicherheit in der Informationstechnik an der TU München als auch die genua GmbH sind dabei, die Post-Quantum Kryptographie auf ihrem Weg zur Praxis voranzubringen. Dabei wird am Lehrstuhl an Gitter-basierten Verfahren gearbeitet und bei genua werden Hash-basierte Verfahren schon jetzt neben den aktuellen Sicherheitsverfahren in der Praxis angewendet.

Gitter-basierte Verfahren

Dieser Ansatz ist einer der vielversprechendsten Post-Quantum-Kandidaten.
Mathematische Gitter, im Prinzip die Darstellung von Vektoren in einem mehrdimensionalen Raum, können zum Verschlüsseln, zum Austausch von Schlüsseln und zum Signieren verwendet werden und bieten gleichzeitig einen sehr guten Kompromiss zwischen Sicherheit und Effizienz. Darüber hinaus ist die Größe des Schlüssels und des Geheimtextes klein, wodurch in der Praxis Datenmengen und Ressourcenbedarf eingespart werden können.

Ein Beispiel für ein effizientes Gitter-basiertes Kryptosystem ist das sog. NTRU-Verfahren, das als IEEE 1363.1 standardisiert wurde.
Eine mögliche Grundlage für ein Kryptosystem ist das sog. Problem „Learning with Errors“ (LWE), also das Lernen mit Fehlern, bei dem die geheime Nachricht durch das Hinzufügen von zufälligen Fehlern verborgen werden kann.

Der Lehrstuhl für Sicherheit in der Informationstechnik investiert in die Entwicklung von Software- und Hardwarelösungen für eine sichere Post-Quantum-Kryptographie. Es konnten bereits die gegenwärtig kleinste und kompakteste Implementierung von NTRU und mehrere Embedded-Lösungen der verschiedenen, beim NIST-Standardisierungsprozess eingereichten Gitter-basierten Kandidaten entwickelt werden. Diese können z. B. in Industrie 4.0-Geräte integriert werden,

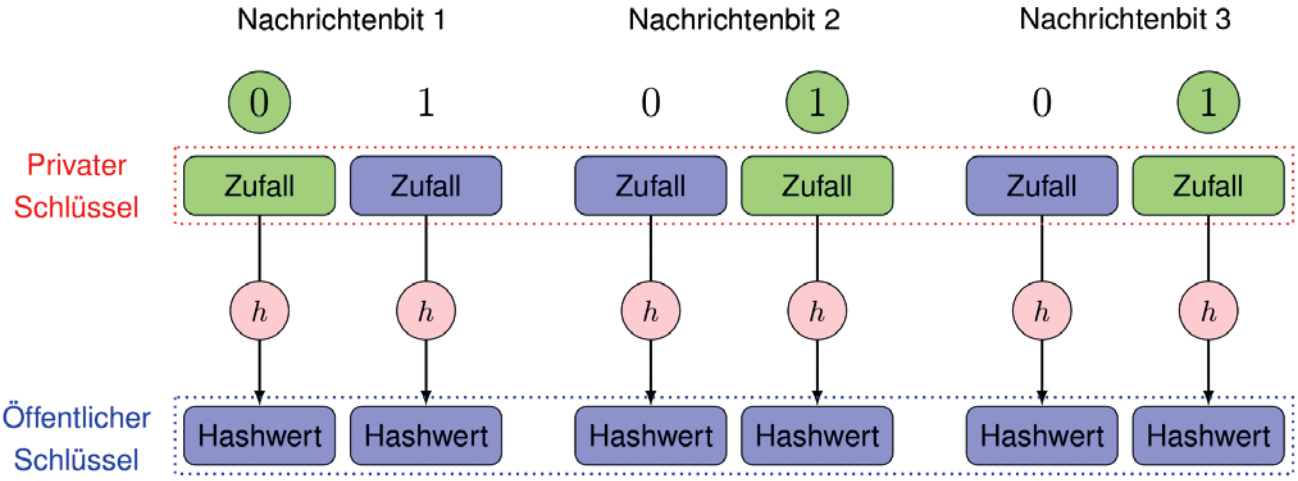


Abb. 3: Das Einmal-Signaturverfahren nach Lamport für die Nachricht 011. Pro möglichem Nachrichtenbit werden zwei Zufallszahlenblöcke erzeugt, welche dann auch den privaten Schlüssel bilden (im Bild rot). Den öffentlichen Schlüssel bilden die Ergebnisse der Anwendung einer kryptographischen Hash-Funktion h auf die einzelnen Blöcke des privaten Schlüssels.
Die Signatur (im Bild die grünen Elemente des privaten Schlüssels) kann überprüft werden, in dem man je Signatur-Block die Hashfunktion h anwendet und mit den zugehörigen Elementen des öffentlichen Schlüssels vergleicht.

einschließlich der Sensoren für drahtlose Netze. Das Ziel ist es, auch weiterhin an Methoden zum Steigern der Sicherheit und der Effizienz von Gitter-basierter Kryptographie zu forschen.

Hash-basierte Verfahren

Hash Funktionen sind Einwegfunktionen, sind also nicht umkehrbar. Hash-basierte Signaturen sind im Bereich der Post-Quantum Kryptographie eine hervorragende Wahl. Zur Erstellung solcher digitaler Unterschriften werden dabei viele, in einer Baumstruktur abgelegte Schlüssel eines Einmalsignatur-Verfahrens verwendet. Für eine Illustration eines solchen Verfahrens siehe Abbildung 3. Diese Konstruktion ist verhältnismäßig gut verstanden und das Sicherheitsniveau solide einschätzbar, da sich die verwendeten Hash-Funktionen bezüglich ihrer Sicherheit verträglich mit Quantencomputern verhalten: so kann man zeigen, dass die Verfahren nach aktuellem Kenntnisstand resistent gegenüber generischen Angriffen mithilfe von Quantencomputern sind. Die Firma genua nutzt bereits das in RFC 8391 von der IETF/IRTF (www.ietf.org) standardisierte Hash-basierte Verfahren XMSS, um einige ihrer Produkte mit einer zusätzlichen Post-Quantum Signatur auszustatten. Wird auf einem System ein neuer Softwarestand installiert, wird sowohl mit einer klassischen, als auch mit einer quantenresistenten Signatur sichergestellt, dass das Softwarepaket tatsächlich von genua stammt. Solch hybrides Vorgehen ist eine gute Lösung, um erste Erfahrungen mit Post-Quantum Kryptographie zu sammeln. So kann schon heute auf die Sicherheit beider Kryptosysteme vertraut werden.

Dr. Stefan-Lukas Gazdag und Dr. Daniel Loebenberger
genua GmbH – Kirchheim

Dr. Johanna Sepúlveda
Lehrstuhl für Sicherheit in der Informationstechnik, TUM

Literatur

[1] Shor, Peter W. (1997), „Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer“, SIAM J. Comput., 26 (5): 1484–1509, arXiv:quant-ph/9508027v2
[2] Grover, L. K.: A fast quantum mechanical algorithm for database search, Proceedings, 28th Annual ACM Symposium on the Theory of Computing, (May 1996) p. 212
[3] Michele Mosca: Cybersecurity in an era with quantum computers: will we be ready?; November 2015; https://eprint.iacr.org/ 2015/1075
[4] Andreas Huelsing, Denis Butin, Stefan-Lukas Gazdag, Joost Rijneveld und Aziz Mohaisen: RFC 8391; XMSS: eXtended Merkle Signature Scheme; IETF/IRTF; Mai 2018; https://rfc-editor.org/rfc/rfc8391.txt
[5] D. McGrew, M. Curcio, S. Fluhrer: Hash-Based Signatures; Internet-Draft; April 2018; http://easyurl.net/65237

Nahezu unbekannt – das Schlüsselgerät 41

Viele Geschichten und noch mehr Geheimnisse

Kaum ein Chiffriergerät der Sammlung des Deutschen Museums gibt so viele Rätsel auf wie das Schlüsselgerät 41. Eigentlich hätte es zum Ende des Zweiten Weltkriegs die heute so berühmte Enigma ersetzen sollen. Aber es kam anders:

- 1939: Die Chiffrierabteilung des Oberkommandos der Wehrmacht (OKW) beanstandet, dass sämtliche Verschlüsselungsmaschinen nicht mathematisch auf ihre Sicherheit geprüft wurden. Deshalb besteht der Leiter der Chiffrierabteilung Fritz Menzer – entgegen der Ignoranz einiger Heeresmitglieder – auf die sofortige Entwicklung verbesserter Chiffriergeräte und erfindet u.a. das Schlüsselgerät 41, das die NSA später als „valuable asset" bezeichnen, weil dessen Verschlüsselungsalgorithmus weitaus sicherer ist als der der Enigma. Aber das Heer blockiert.
- 1942: Es erfolgt eine zweijährige Sicherheitseinschätzung aller verwendeten Chiffrierverfahren, mit dem Ergebnis: Fast alle Chiffriergeräte, vor allem die weitverbreitete Heeres-Enigma, werden offiziell als unsicher eingestuft. Deshalb entscheidet man sich ab 1943 zur Massenproduktion des Schlüsselgeräts 41. Dokumente des Sächsischen Staatsarchivs belegen, dass die Wehrmacht rund 11.000 Maschinen bei der Wanderer Werke AG in Siegmar-Schönau bei Chemnitz bestellt. Doch durch den Mangel an Leichtmetall zu Kriegsende wiegen die Maschinen fast 15 Kilogramm – viel zu schwer für den Feldeinsatz. Nur etwa 1500 Stück werden tatsächlich hergestellt.
- 1945: Wie die meisten Chiffriergeräte müssen auch sämtliche Schlüsselgeräte 41 zu Kriegsende gemäß der „Verschlußsachen-Vorschrift" zerstört, versenkt oder verbrannt werden. Die wenigen Geräte, die tatsächlich den Krieg überdauert haben, sind in der Regel funktionsunfähig oder befinden sich für die Öffentlichkeit unzugänglich in den Depots diverser Geheimdienste. Unmittelbar nach Kriegsende protokolliert das Target Intelligence COMmitee (TICOM) der USA und Großbritannien sämtliche Aussagen deutscher Kryptologen in Kriegsgefangenschaft. Diese TICOM-Dokumente werden bis 2011 von der NSA unter Verschluss gehalten.
- 1973: Über den Erfinder des Schlüsselgeräts 41 Fritz Menzer (1908 – 2005) ist nur wenig bekannt. Nach dem Krieg gerät er in U.S.- und danach in sowjetische Kriegsgefangenschaft. Nach 1951 wird er nicht mehr in offiziellen Dokumenten erwähnt. Allerdings erhält er aus nicht-öffentlichen Gründen 1973 das Bundesverdienstkreuz der BRD.
- 1979: Der bekannte Kryptologie-Hersteller Boris Hagelin (1892 – 1983) erwähnt in seiner Biografie das Schlüsselgerät 41 als eine Kopie seiner eigenen Maschinen – nicht ganz zu Unrecht, da Menzer tatsächlich den typischen Hagelin'schen Stangenwalzen-Mechanismus kopiert hat. Aber er entwickelte interessante Verbesserungen, z.B. einen unregelmäßigen Fortschaltungsmechanismus mit interagierenden Chiffrierwalzen – eine Lösung, die erst nach dem Krieg in den Hagelin'schen Maschinen auftaucht. Doch um den Einfluss zu verstehen, den jeder Erfinder auf den anderen hatte, benötigt man mehr Informationen, die zu dieser Zeit noch nicht zugänglich sind.

Foto: Konrad Rainer, Deutsches Museum München

Bodenfund Schlüsselgerät 41

- 2011: Viele TICOM-Dokumente werden von der NSA freigegeben. Nun kann die Geschichte der Verschlüsselungsmaschinen rekonstruiert werden, die während des Kriegsverlaufs am OKW/Chi entstanden. Doch die einschlägigen Dokumente über das Schlüsselgerät 41 und die persönlichen Interviews mit Fritz Menzer bleiben weiter unter Verschluss.
- 2013: Das Deutsche Museum ersteigert den stark restaurierten Seefund eines Schlüsselgeräts 41 Modell Z bei Christie's in London. Das Gerät stammt aus einem See in Ostdeutschland und lag vermutlich 60 Jahre lang im Wasser. Wegen der Korrosion kann man keinerlei Rückschlüsse auf den Verschlüsselungsalgorithmus ziehen.
- 2017: Zwei Hobby-Schatzsucher finden im Waldboden im Münchner Umland ein Schlüsselgerät 41 und übergeben den Fund dem Deutschen Museum. Irgendjemand muss es vor circa 70 Jahren vergraben haben. Das Gerät ist ebenfalls stark korrodiert. Die Restaurierungsforscher des Deutschen Museums finden heraus, dass die Tastatur der Maschine aus Cellulose-Nitrat besteht. Diese schwierige Substanz zerfällt bei Wärme und Lichteinfall und emittiert nitrathaltige Gase, die das Exponat selbst sowie alle anderen schädigt, die in derselben Vitrine stehen. Deshalb müssen spezielle Bedingungen für die Lagerung und Ausstellung des Gerätes geschaffen werden.
- 2018: Wird es in Zukunft möglich sein, Menzers Erfindung vollständig in den Lauf der Geschichte einzuordnen und eine Simulation zu schreiben? Wahrscheinlich schon – denn in Sammlerkreisen gibt es noch funktionsfähige Schlüsselgeräte 41. Ein Stuttgarter Ingenieur hat mit viel Mühe und langjähriger Erfahrung ein Original zum Laufen gebracht und akribisch dessen Algorithmus aufgezeichnet.

Bald wissen wir hoffentlich mehr.

Dr. Carola Dahlke
Deutsches Museum, Kuratorin für Informatik und Kryptologie

VDI-AK FiB München

Maschinelles Lernen für die Produktion von Morgen

Der Umsatz der produzierenden Industrie belief sich im Jahr 2017 auf rund 2 Billionen Euro. Gleichzeitig lag der Anteil des Verbrauchs von Roh-, Hilfs- und Betriebsstoffen am Gesamtumsatz bei 42,7%. Bei diesen Zahlen wird deutlich, welchen Kostendruck die Probleme in der Fertigung für die produzierenden Firmen bedeuten. Dazu zählen beispielsweise mangelnde Fertigungsqualität und sich daraus ergebender Ausschuss oder Nacharbeit, hoher Energieverbrauch, instabile Fertigungsprozesse oder auch zu lange Anlauf- und Taktzeiten.

Ein Schlüsselelement zur Lösung dieser Probleme ist die optimale Einstellung der Fertigungsanlagen. Die Frage ist: Mit welchen Einstellungen wird die Güte des Fertigungsprozesses optimal? Die Firma IPT Insight Perspective Technologies GmbH bietet Antworten.

Bei einem Fertigungsprozess müssen sowohl die einzelnen Prozessschritte, als auch deren Kombination optimiert werden. Heute arbeiten erfahrene Prozess-Experten fortlaufend daran, die einzelnen Prozessschritte im Griff zu behalten. Schon aufgrund der menschlichen Reaktionsgeschwindigkeit im Zusammenhang mit kurzen Taktzeiten ist es dabei jedoch bestenfalls nur möglich, den gleitenden-Durchschnitt über die Zeit zu optimieren. Und eine noch größere Herausforderung besteht darin, die Kombination einzelner Schritte in einer Prozesskette aufeinander abzustimmen.

Klassische Machine-Learning-Verfahren konnten bisher aufgrund des hohen Datenbedarfs nur eingeschränkt Mehrwert liefern. Denn in der produzierenden Industrie ist es in der Regel nicht möglich, viele Trainingsdaten zu erzeugen.

Zum einen ist die Stückzahl der produzierten Teile begrenzt, zum anderen kann das Erheben der Daten sehr teuer sein; zum Beispiel, weil es sich um zerstörende Messverfahren handelt. Im Gegensatz zu klassischen Big-Data-Anwendungen ist hier also die Herausforderung nicht eine schiere Menge an Daten, sondern das Fehlen von Daten. IPT hat mit der Software IPT.Stack eine Lösung entwickelt, die mit den wenigen verfügbaren Daten auskommt, gleichzeitig jedoch so flexibel ist, dass sie der Komplexität der Realität gerecht werden kann. Der Clou daran ist, nicht nur Machine Learning mit Daten zu betreiben, sondern den Algorithmus auf das bestehende Wissen der Prozessexperten aufzubauen. Konkret bedeutet das, den Produktionsablauf in Form eines statistischen Ablaufdiagrams darzustellen. Dabei wird sowohl quantitatives, als auch qualitatives Wissen in mathematische Formeln übersetzt.

Und die Erfahrung zeigt: der Aufwand lohnt sich, denn der Prozessgraph macht den Unterschied. Der IPT.Stack ist in der Lage, mit den wenigen Daten, die in der industriellen Fertigung verfügbar sind, zu arbeiten. Das Ergebnis: stabile Produktionsprozesse, kurze Anlaufzeiten und eine optimale Produktionsgüte im Sinne von Taktzeit, Material- und Energieverbrauch und Produktqualität.

Dr. Theo Steininger und
Dr. Isabell Franck

VDI-AK Frauen im Ingenieurberuf (FiB) München

Haben Sie Lust auf einen exklusiven Einblick in dieses Thema? Dann kommen Sie zum Vortragsabend im VDI-Netzwerk der Frauen

Referentin: Dr. Isabell Franck, Gründerin + Geschäftsführerin der IPT - Insight Perspective Technologies GmbH

Anlässlich eines Themenabends des VDI-Netzwerks der Frauen im Ingenieurberuf (FiB) hält Dr. Isabell Franck, Gründerin und Geschäftsführerin der IPT – Insight Perspective Technologies GmbH, am **21. November** in der TU München einen Vortrag zum Thema Maschinelles Lernen für die Produktion von Morgen.

Eingeladen wurde sie von der stellvertretenden Vorsitzenden des BV München und FiB-Arbeitskreisleiterin Christa Holzenkamp: „Dieses Thema, das bei einem renommierten, ortsansässigen Automobilhersteller in Details des Produktionsprozesses erhebliche Einsparungen bringt, hat mich begeistert. Erfolgreiche Gründerinnen wie Dr. Isabell Franck sind das beste Beispiel dafür, wie progressiv und nachhaltig Frauen das Ingenieurwesen schon längst mitgestalten. Das wollen wir zeigen“.

Mehr Infos unter: vdi.de/fib-muenchen

VDI Bezirksverein München Ober- und Niederbayern

Hochschule München

Kryptologie im Zeitalter des Quantencomputers

Quantensimulationsexperiment mit langen Ionenkristallen

Foto: IQOQI/Knabl

Quantencomputer können gängige Verschlüsselungen brechen. Welche Kryptographie jetzt noch quantensicher ist, wie Quanteninformation verarbeitet und wie sie sicher übertragen werden kann, all dies wird an der Hochschule München gelehrt.

Mit Hilfe großer, fehlerkorrigierter Quantencomputer, wie sie aktuell von IBM, Microsoft, Google und einigen anderen Firmen mit erheblichem Aufwand entwickelt werden, wird es möglich sein, Quanteninformation zu verarbeiten und so bestimmte Algorithmen effizienter zu berechnen.
Einer dieser Algorithmen, der sogenannte Shor-Algorithmus, kann ganze Zahlen wesentlich effizienter faktorisieren (Komplexitätsklasse BQP) als jeder bekannte, klassische Algorithmus und so die RSA-Kryptografie brechen. Quantencomputer, die den heutigen Schlüssel mit 2048 bit brechen können, sind aber noch nicht in Reichweite.
Dennoch wird dringend empfohlen, schon jetzt quantensichere Verschlüsselungsmethoden zu entwickeln. Das National Institute of Standards and Technology (NIST) der USA entscheidet gerade über einen neuen, quantensicheren „public key"-Kryptographie-Algorithmus als neuen Standard. Zur abhörsicheren Schlüsselübertragung existieren bereits einige Quantenkryptographie-Protokolle. Diese sind schon weit entwickelt und kommerziell erhältlich.

Quanteninformationen verstehen und anwenden

Informatiker und Ingenieure werden in Zukunft zunehmend herkömmliche Systeme – sofern sinnvoll – mit Quantentechnologie kombinieren und sollten deshalb die neuartige Verarbeitung und Übertragung von Quanteninformation verstehen und anwenden können. An der Hochschule München wird deshalb die Lehrveranstaltung „Quanteninformatik" für Informatik-Studierende angeboten.
Die Quantentechnologie basiert auf sogenannten Qubits. Dieses sind quantenmechanische Zweizustandssysteme.
Erst wenn man den Zustand des Qubits misst, wird dieser festgelegt (0 oder 1). Der Messprozess verändert also den Zustand des Qubits. Das Messergebnis ist dabei zufällig. Auf diese Weise können z. B. echte Zufallszahlen – etwa für einen kryptologischen Schlüssel – erzeugt werden. Grundsätzlich kann ein Qubit oder eine Quantennachricht nicht einfach kopiert und weitergeschickt werden, sie kann aber quantenteleportiert werden. Diese Eigenschaften machen ein Abhören der Quanteninformation grundsätzlich unmöglich, andererseits stellen eine ggfs. notwendige Fehlerkorrektur oder ein Verstärken des Signals (Repeater) große Herausforderungen dar.

Quantensoftware

Die meisten Quantenalgorithmen nutzen quantenmechanische Effekte wie Interferenz und Verschränkung. Verschränkte Qubits sind eng gekoppelt, so dass sie ihre Zustände immer korreliert ändern, auch wenn sie weit voneinander entfernt sind.
Zur Entwicklung von Algorithmen, z. B. solchen zur Simulation von Quantenprozessen, zur Faktorisierung oder zur Teleportation von Qubits, existiert ein universeller Satz von Quantengattern. Eine fertige Quantensoftware kann dann schon heute mit Hilfe des IBM Quantencomputers oder den Simulatoren von Google und Microsoft online getestet werden.
Außerdem gibt es Testnetzwerke für ein Quanteninternet.
Obwohl unsere heutige Kryptografie in den kommenden Jahren absehbar noch nicht bedroht sein wird, müssen wir uns jetzt auf die Situation der kommenden Jahrzehnte vorbereiten. Dazu brauchen wir gut ausgebildete „Quanteninformatiker" und „Quanteningenieure".

Prof. Dr. Sabine Tornow
Hochschule München

TU München

Neues Zentrum für Quantentechnik in Garching

Auf dem Campus Garching hat sich in den letzten Jahren ein weltweit beachteter Forschungsschwerpunkt zu Quantentechnologien entwickelt. Der Wissenschaftsrat befürwortet nun ein neues Zentralinstitut der Technischen Universität München (TUM), das diesen Schwerpunkt mit den Ingenieurwissenschaften verknüpft und Quantensysteme schneller in reale Anwendungen überführen soll.

Längst haben die Quantenwissenschaften Einzug in unseren Alltag gehalten. Die gesamte moderne Mikroelektronik wäre ohne die von Forschern wie Max Planck und Albert Einstein entwickelten Grundlagen der Quantenphysik undenkbar. Kernspintomographen nutzen bereits gezielt das Wissen um eine neue Generation von Quantenphänomenen, um schärfere Bilder zu bekommen, und in naher Zukunft sollen Quantencomputer die Datenverarbeitung revolutionieren.

„Auch wenn quantenphysikalische Phänomene bereits in vielen Anwendungen unseres Alltags eine Rolle spielen, stehen wir mit der aktuellen Entwicklung, der Quantentechnologie 2.0, noch ganz am Anfang der gezielten Ausschöpfung eines völlig neuen Potenzials“, sagt Christian Pfleiderer, Professor für Experimentalphysik der TU München. „Die Quantentechnologien gehören zu den zentralen Zukunftstechnologien.“

In direkter Nachbarschaft zum Walter Schottky Institut für Halbleiterphysik der TUM, das ebenfalls eine Kooperationseinrichtung der Fakultäten für Physik und für Elektro- und Informationstechnik ist, soll nun unter Führung der Professoren Christian Pfleiderer (Physik) und Holger Boche (Elektro-und Informationstechnik) ein Zentrum für QuantumEngineering (ZQE) entstehen.

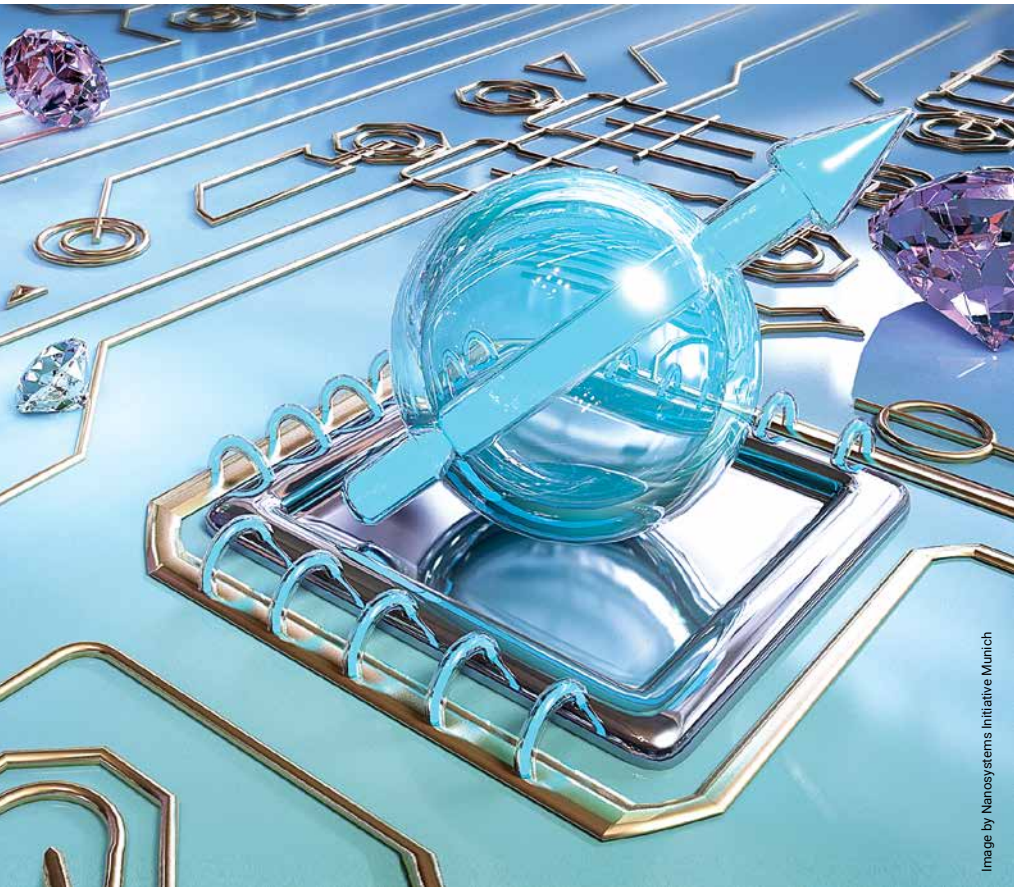
Aufbauend auf den langjährigen, sehr erfolgreichen Vorarbeiten einzelner Arbeitsgruppen der TUM ist ein wichtiges Ziel des geplanten Zentrums die zügige Überführung von Forschungsergebnissen in die Anwendung. Geplant ist dafür eine integrative Vernetzung mit Industriepartnern.

Quantentechnologie – Quantencomputer

Das neue Institut soll sich auf drei interdisziplinäre Forschungsschwerpunkte konzentrieren: Hybride Quantenbauelemente und Quantenschaltkreise, Funktionale Quantenmaterialien sowie Systemaspekte und Modellierung komplexer Quantensysteme.

„Der Forschungscampus Garching ist weltweit als ein Zentrum der Quantenforschung anerkannt. Durch seine fakultätsübergreifende Programmatik bildet das ZQE ein ideales Bindeglied zwischen den Fakultäten für Physik, Chemie, Elektro- und Informationstechnik, Informatik und Mathematik. Es schafft durch Bündelung der Kräfte neue Synergien“, sagt TUM-Präsident Prof. Wolfgang A. Herrmann. Hier zeige sich erneut, so Herrmann, wie wegweisend die Entscheidung zur Verlagerung der Fakultät für Elektro- und Informationstechnik nach Garching war und wie wichtig nun deren schnelle Realisierung ist.

Andreas Battenberg



Zukunftsvision: Quantencomputer mit Chips aus Diamant und Graphen

IHR SCHLÜSSEL ZU GUTEN ÜBERSETZUNGEN

Hilfreiche Tipps zur Vergabe von Übersetzungsaufträgen

„Sprache ist der Schlüssel zur Welt", sagte schon Wilhelm von Humboldt. Ähnlich wie in der Kryptologie werden auch mit der Sprache Informationen verschlüsselt und entschlüsselt. Denken Sie nur an medizinische Befunde, die für Laien mehr als kryptisch sein können. Oder an Ihre eigenen Fachgespräche, die für Sie selbst völlig verständlich sind, Fachfremden aber „spanisch" vorkommen. Um diese wichtigen Informationen zu verstehen oder zu übermitteln, müssen Sie in jeder Hinsicht die richtige Sprache sprechen.

Wenn Sie international kommunizieren, stehen Sie an der Schnittstelle von Sprache und Know-how. Mit Ihrer Muttersprache kommen Sie dabei häufig nicht weiter und wenn Sie Fachtexte mithilfe Ihrer eigenen Fremdsprachenkenntnisse übertragen, fehlt Ihnen diese Zeit bei der Erledigung Ihrer eigentlichen Aufgaben. Vielleicht müssen Sie auch mit Kollegen im Ausland in einer Sprache interagieren, die Sie gar nicht beherrschen. Unterlaufen Ihnen dabei Fehler, kann dies nicht nur zu Imageschäden, sondern schlimmstenfalls zu rechtlichen Konsequenzen führen.

Oft muss also ein qualifizierter Übersetzer oder Dolmetscher her – schon allein, um professionell aufzutreten und Risiken zu minimieren.

5 TIPPS ZUR VERGABE VON ÜBERSETZUNGEN

- **EXPERTENWISSEN:** Achten Sie darauf, dass Ihr Übersetzer auf das jeweilige Fachgebiet spezialisiert ist.
- **ANGEBOTSANFORDERUNG:** Geben Sie Ihrem Übersetzer Einblick in den betreffenden Text, damit ein verlässliches Angebot möglich wird – ausschlaggebend für den Preis sind die Sprachkombination und die Schwierigkeit des Textes.
- **BEI MEHREREN ANGEBOTEN:** Noch wichtiger als der Preis ist das Fachwissen des Übersetzers, damit Sie Texte hoher Qualität erhalten.
- **FRÜHZEITIGE BEAUFTRAGUNG:** Eilaufträge sind in der Regel deutlich teurer.
- **KOSTENEFFIZIENZ DURCH ENDFASSUNGEN:** Geben Sie möglichst nur Endfassungen von Texten in Auftrag, damit Ihr Übersetzer günstig und effizient für Sie arbeiten kann.

Dolmetscher- und Übersetzerdatenbank Bayern: by-suche.bdue.de

Bundesverband der Dolmetscher und Übersetzer e. V. (BDÜ) Landesverband Bayern: by.bdue.de

Expertenleistung – von Profis für Profis

Die externe Vergabe von Sprachdienstleistungen an Übersetzer und Dolmetscher ist oft auch günstiger: Ein professioneller Übersetzer braucht in der Regel weniger Zeit, als Sie selbst mühsam für eine Übersetzung aufwenden müssten – und dies zu Ihrem teuren Stundensatz als technischer Spezialist. Sie profitieren durch die Beauftragung eines Übersetzers also in doppelter Hinsicht.

Frei verfügbare maschinelle Übersetzungen mit diversen Apps wiederum sind nur auf den ersten Blick kostenlos. Sie können unbemerkt gravierende Fehler produzieren und stellen außerdem ein erhebliches Risiko im Hinblick auf Vertraulichkeit und Informationssicherheit dar.

So finden Sie qualifizierte Übersetzer und Dolmetscher

Hätten Sie es gewusst? **Übersetzer** übertragen Schriftliches von einer in die andere Sprache, **Dolmetscher** hingegen das gesprochene Wort. Es handelt sich also um zwei verschiedene Berufe, für die man jeweils ein mehrjähriges Studium oder eine staatliche Prüfung absolviert. Abgesehen von diesen Abschlüssen sind die beiden Berufsbezeichnungen in Deutschland jedoch nicht geschützt, sodass sich auch viele unqualifizierte Sprachdienstleister auf dem Markt tummeln.

Der Bundesverband der Dolmetscher und Übersetzer (BDÜ) erleichtert Ihnen die Suche nach Profis, denn in den größten deutschen Verband der Branche wird nur aufgenommen, wer eine entsprechende fachliche Qualifikation nachweisen kann.

In der kostenlos nutzbaren Online-Datenbank des BDÜ unter **by-suche.bdue.de** finden Sie Kontaktdaten von rund 1.500 Dolmetschern und Übersetzern in Bayern für mehr als 40 Sprachen und zahlreiche Fachgebiete. Die Suche kann bei Bedarf auch auf die rund 8.000 BDÜ-Mitglieder mit insgesamt 80 Sprachen in der bundesweiten Datenbank erweitert werden.

Dipl.-Übers. Manuela Wilpert

VDI-Freundeskreis Italia

Goldenes Jubiläum: 50 Jahre VDI Italia

Am 21. September 1968 wurde von den bei der damaligen Euratom-Forschungsstelle in Ispra arbeitenden VDI-Mitgliedern der VDI Freundeskreis Italien gegründet.

Die erste Versammlung fand damals im Hotel Europa statt und so wurde das 50-jährige Jubiläum mit einem Festakt auch in diesem Hotel begangen. Bei seiner Begrüßung und Eröffnung konnte der Vorsitzende Walter Brand ein Gründungsmitglied Martin Oberhofer hervorheben. Nach einem gestrafften Rückblick auf die Aktivitäten in den 50 Jahren des Freundeskreises sprachen die Grußworte an die Mitglieder:

- Claus Robert Krumrei, Generalkonsul der BRD in Mailand
- Udo Ungeheuer, Präsident des VDI in Düsseldorf
- Marinus Stroosnider, Head of JRC Department Ispra
- Katrin Oswald-Richter, Leiterin Goethe-Institut Mailand
- Peter Hotka, Vorstandsmitglied des VDI-Bezirksvereins München.

Umrahmt wurde die Feier mit klassischer Musik des Duos Willi Burger (Chromatische Mundharmonika) mit Clara Schembari (Klavier) und den Zwillingsschwestern Mailin Barbara und Silah Gabriela Göbel am Klavier.

In seinem Festvortrag stellte Roland Schmid Betrachtungen über die Zahl „50“ an. Es folgte die Übergabe der Präsente an die Vorstandsmitglieder des Freundeskreises. Der offizielle Teil endete mit einem Aperitiv.

Wie jedes Jahr gab es auch ein attraktives Rahmenprogramm: Noch am Donnerstag wurde die Reis-Herstellung „Azienda Agricola“ in Vespolate und eine Fabrik für Essig/Öl-Gemüsekonserven „Ponti“ in Ghemme besichtigt. Am Freitagmorgen besuchten wir das Forschungszentrum JRC in Ispra, zuerst im Informations-Zentrum die Vorstellung aller Aktivitäten des JRC und anschließend im Detail das Zentrum für Elektrische Fahrzeuge, Smart Grids und das Mikrowellensignaturlabor.

Bei strahlendem Sonnenschein startete am Samstag der Tagesausflug per Schiff über den Lago Maggiore von Angera bis Locarno, mit dem Zug Centovalli nach Domodossola und weiter nach Arona und per Schiff nach Angera.

Die Tagung schloss am Sonntagmorgen in Mailand mit einer Stadtrundfahrt, einem Bummel über Schloss- und Domplatz zum Porta-Nuova-Viertel.

Der Abschied schloss mit der Verabredung „Nächstes Jahr in München!“

Karl-Heinz Lohn

50 Jahre VDI Freundeskreis Italia

Foto: K-H. Lohn

Fotos: R. Schmidt und P. Hotka

70 Jahre Erfindermesse iENA Nürnberg

Ideen – Erfindungen – Neuheiten

Es erfordert Fleiß, Mut und Kreativität, um eine Idee zu verfolgen, um an sie zu glauben und sie weiterzuentwickeln, bis sie als fertiges Produkt auf den Markt kommt. Rund 30.000 Erfindungen wurden in den vergangenen 70 Jahren auf der internationalen Fachmesse „Ideen – Erfindungen – Neuheiten“ in Nürnberg präsentiert.

Internationaler Treffpunkt der Erfinderszene

Erfinderverbände und Kollektive aus der ganzen Welt treffen sich zur iENA in Nürnberg, um ihre Neuheiten vorzustellen, sich zu vernetzen und um Kontakte zu knüpfen.

Partner der iENA 2018 ist der Iran, der mit seinem Erfinderverband regelmäßig vielversprechende Innovationen, zum Beispiel aus dem medizinischen Bereich, präsentiert. Die iENA pflegt sowohl national als auch international starke Partnerschaften, die das Angebot und Potential für Erfinder vorantreiben.

Die seit 2017 bestehende Partnerschaft mit dem Verein Deutscher Ingenieure (VDI) bringt weitere Zielgruppen wie Ingenieure und professionelle Anwender auf die iENA. Auch der Erfindernachwuchs bringt beeindruckende Innovationen auf die iENA, neben den „Jugend forscht“-Gewinnern und den VDI-ZUKUNFTS-PILOTEN beweisen jedes Jahr Schüler und Studenten aus vielen Nationen stets großes Innovationspotential.

Die internationale Erfindermesse „Ideen – Erfindungen – Neuheiten“ iENA 2018 findet vom 1. bis zum 4. November statt.

Informationen unter www.iena.de

VDI-AK Aktuelles Forum Technik

40 Jahre Faszination Technik

Als ich im Januar 1977 nach München kam, meldete ich mich bei der VDI-Geschäftsstelle (Frau Anthes), um – wie man heute sagt – ein Netzwerk zu finden und suchte mir den Stammtisch der „Studenten und Jungingenieure" aus. Dieser traf sich in wechselnder Teilnehmerzahl in verschiedenen Restaurants. Schon bald kam der Wunsch auf, den Treffen ein Thema zu geben. Zuerst kamen Kurzvorträge über Berufserfahrungen aus den eigenen Reihen. Anfang 1978 wurde dann eine Wunschliste für Vortragsthemen aufgestellt, die zum Beispiel aus dem beruflichen Umfeld kamen: Patentrecht, Personalführung/-politik, Versicherungs- und Haftungsfragen, Neue Technologien: Roboterfertigung, Raumfahrt, Concorde, Transrapid, Technik in der Freizeit: Sicherheit von Seilbahnen, Skibindungen, Schifffahrt, Technikverantwortung und Ethik, Rhetorikschulungen und Fachpresse.

Alle Fotos: Karl-Heinz Lohn

Das Aktuelle Forum Technik besuchte die Baustelle des Luise-Kiesselbach-Tunnels (Bild oben), die Zeche Zollern (unten links) und flog mit dem Zeppelin NT (unten rechts)

Treffpunkt der Ingenieure

Hierzu wurden Räumlichkeiten mit den erforderlichen technischen Hilfsmitteln benötigt. Auf Vermittlung von Herrn Ergens fanden wir im Kaminzimmer des Exportclubs am Lenbachplatz eine noble Unterkunft mit Butler. Dazu gaben wir uns den Namen „Treffpunkt der Ingenieure". Zwischenzeitlich nannten wir uns AK „Mensch und Technik" analog zur VDI-Gesellschaft in Düsseldorf. Nachdem der Exportclub schließen musste, zogen wir 1982 in das Rahnstüberl des Hansahauses.

Aktuelles Forum Technik

Ab 1999 nannten wir uns dann „Aktuelles Forum Technik" und waren Gast von Pater Rupp im Akademiker Centrum, Lämmerstraße. Dieses schloss 2011 und so kehrten wir wieder zurück ins inzwischen renovierte Rahnstüberl. Der Bereich der Interessen blieb gleich, allerdings wurden für umfangreichere Themen auch Vortragsreihen geplant, getreu dem Motto: Der Ingenieur kennt zwar sein Fachgebiet – muss aber in der Öffentlichkeit oder auch nur im Freundeskreis zu aktuellen Fragen Antworten geben. So zuerst bei der Atomenergie, wo wir vom Betreiber, vom TÜV, von den Grünen und von Greenpeace Informationen über Funktion, Sicherheit und Risiken von Kernkraftwerken erhielten. Ähnlich verfuhren wir bei Fragen des Umweltschutzes, angestoßen durch die Diskussion über die Mülltrennung. So hielten wir es auch bei den dringlichen Problemen des Nah- und Fernverkehrs.
Hier luden wir Referenten ein von der Stadt München, der Bahn, des MVV, des ADAC, des ADFC, der Lufthansa und eines Automobilherstellers. Nur durch diese Vielfalt kann man sich eine eigene Meinung bilden. Ergänzt wurden die Vorträge durch Betriebsbesichtigungen.

Höhepunkte

Mehrtägige Exkursionen führten uns zu den VDI-Bezirksgruppen in Rosenheim, Passau, Deggendorf und Ingolstadt, die uns bei Firmenbesuchen unterstützten und lokale Besonderheiten näherbrachten. Ebenso machten wir Besuche bei den VDI-Bezirksvereinen in Magdeburg, Hannover, Bremen, Dortmund und Linz.

Besondere Erlebnisse waren die mehrtägigen Reisen zu technischen, lokalen, kulturellen, historischen und politischen Höhepunkten. So fuhren wir ins Elsass (Schiffshebewerk Saint-Louis/Arzviller, eine Festung der Maginot-Linie, Kloster Ste. Odile, Isenheimer Altar, Automuseum Schlumpf), besuchten das Europa-Parlament, machten uns nach Ostfriesland auf (Meyer Werft, Transrapid-Teststrecke, Kunsthalle Emden) und bereisten das Ruhrgebiet (Thyssen-Stahlwerk, Villa Hügel, Zeche Zollverein, Bergbaumuseum, Bergarbeitersiedlungen).

Neben den vielen treuen Mitgliedern – einige von 1978 an – finden auch viele jüngere Mitglieder zu unseren Veranstaltungen, wenn wir auch nie wieder den Rekord von 120 Besuchern erreichen werden wie bei der Podiumsdiskussion zum Thema „Nachdiplomierung".

Zum Schluss möchte ich mich bei allen Unterstützern bedanken, wobei ich nur drei Namen hervorheben will, auch wenn sie nicht mehr unter uns sind: Dr. Horst Lange, Prof. Dr. Hermann Linde und Dr. Ernst Hofmeister.

Karl-Heinz Lohn

VDI BV München

Tradition und Innovation verbinden

MAURER SE erhält Urkunde als Fördermitglied im VDI-Bezirksverein München, Ober- und Niederbayern

Termin überzogen – was für Ingenieure oft unangenehm ist, war am 9. Oktober ein gutes Zeichen.

Foto: MAURER

Urkundenüberreichung (von links): Dr. Jan Göpfert, Vorstandsmitglied beim VDI BV München, Dr. Christian Braun und Max Meincke, geschäftsführende Direktoren der MAURER SE, und Prof. Dr. Peter Pfeffer Vorstandsvorsitzender des VDI BV München

Die Münchner VDI Vorstände Prof. Peter Pfeffer und Dr. Jan Göpfert überreichten die Fördermitglied-Urkunde an die geschäftsführenden Direktoren der MAURER SE, Dr. Christian Braun und Max Meincke. MAURER ist seit 60 Jahren Mitglied im VDI. Gemeinsame Werte wie Tradition, Qualität und innovativer Tatendrang führten zu einem regen und ausgedehnten Austausch.

Gerahmt wurde die Urkundenverleihung durch Unternehmens- bzw. Vereinspräsentationen, und einen Werksrundgang. Eine Gemeinsamkeit ist, dass der VDI Bezirksverein München, Ober- und Niederbayern und MAURER fast gleich alt sind: 141 bzw. 142 Jahre. Diese lange Tradition verbindet – und doch ist den Gesprächspartnern bewusst: Auf Tradition darf man sich nicht ausruhen, sie muss immer die Basis für beständig gute Qualität sein. Das zeigte Fertigungsleiter Karoly Kesztyüs bei der Führung durch drei Werkshallen an zahlreichen Beispielen, von der Stahlqualität über den idealen Stahlzuschnitt und Spezialmaschinen bis hin zum Kennzeichnungssys-tem aller Teile in der Produktion.

Tradition ist zudem der Hintergrund für erfolgreiche Innovation. MAURER SE hat sich aus einer Werkstatt zum international gefragten Nischenspezialisten entwickelt. Für Schlagzeilen sorgt aktuell das 77 m hohe Riesenrad „WOM – Wheel of Munich".

In 20 Arbeitskreisen, die jährlich 330 Veranstaltungen organisieren und dabei auch stark auf Internationalität setzen, engagiert sich der VDI Bezirksverein München besonders für den Ingenieursnachwuchs. Behandelt werden aktuelle Themen, die fachlich fundiert die gesamte Bandbreite technischer Entwicklungen beleuchten.

DieGesprächspartnerentwickeltengemeinsame Themenideen, zum Beispiel Erdbebenschutz, Schwingungsdämpfung von Hochhäusern oder das WOM. Alle sind gleichermaßen spektakulär wie technisch innovativ. Konkrete Umsetzungen im Netzwerk sind in Planung.

Judith Klein

VDI-AK „Technische Führungskräfte und Unternehmer“ Bayern Nordost

Herausforderung „Digitalisierung“

Anforderungen an Führungskräfte und Mitarbeiter

Spannende und gewinnbringende Informationen vor allem unter organisationspsychologischen Gesichtspunkten lieferte der Vortrag von Hagen Böh-me, Inhaber Controlling Intelligence, zum Thema Digitalisierung.

Der Umbruch in die digitale Welt bietet viele Chancen, vor allem auf der prozessualen und finanzbuchhalterischen Seite, birgt jedoch auch so manche Risiken vor allem auf der menschlichen Seite. Gewachsene Strukturen, Selbstoptimierungen einzelner Abteilungen und Bereiche, gewohnte Prozesse und herkömmliche Technik sind Ursachen noch veralteter Prozesse, Methoden und Strukturen, jedoch nicht mehr zeitgemäß und unter Wettbewerbs- und Kostengesichtspunkten kritisch.

Foto: VDI

Hagen Böhme bei seinem Vortrag

Erfolgsstrategien und Methoden

Den teilnehmenden Unternehmern und Führungskräften zeigte der Referent Böhme anhand anschaulicher Praxis-Beispiele zahlreiche Erfolgsstrategien und Methoden zur Prozessverbesserung, Zeitreduzierung, Kosteneinsparung und effektivem Einsatz der Mitarbeiter auf.

Die meisten Methoden entwickelte und realisierte er selber in seiner Funktion als kaufmännischer Leiter in Unternehmen. Die wichtigsten Erfolgsfaktoren im Einzelnen:

- Strategie und Management
- Digitale Infrastruktur
- Produkt- und Service-Innovationen
- Organisation
- Geschäftsprozesse
- Zusammenarbeit, sowie
- Wissen und Kultur

wurden aufgezeigt und theoretisch sowie an praktischen Beispielen erläutert und zwischen den Teilnehmern ausgetauscht. Die Aspekte wie das richtige „Management-Mindset“, die Komplexität der Schnittstellenanalyse, die Entwicklung von neuen Serviceleistungen durch neue digitale und technologische Möglichkeiten, wie auch Änderung der Stellenanforderungen wurden aufgezeigt und beschrieben.

Offenheit, Transparenz, Vertrauen und verantwortungsvoller Umgang mit Daten und Menschen sind dabei elementare Erfolgskriterien. Erfahrungen und Meinungen wurden intensiv zwischen dem Referenten und den Teilnehmern ausgetauscht und noch lange beim anschließenden Imbiss diskutiert.

Ein rundum überzeugender und informativer Vortrag bereicherte die begeisterten Teilnehmer.

Hagen Böhme
Inhaber Controlling Intelligence
Bodo Ikinger

VDI-Gesellschaft Energie und Umwelt

Ehrenmedaille für Dipl.-Ing. Harald Fonfara

Der Verein Deutscher Ingenieure verleiht Herrn Dipl.-Ing. Harald Fonfara mit Dank und Würdigung seiner langjährigen, verdienstvollen ehrenamtlichen und überaus erfolgreichen Tätigkeiten im Fachbereich Energietechnik die Ehrenmedaille. Harald Fonfara hat durch seine federführende Mitarbeit und als Vorsitzender in den Richtlinienausschüssen zu den Themen Wärmepumpen und Energiespeichern maßgeblich zur Weiterentwicklung des VDI-Richtlinienwerkes beigetragen. Er hat sein Fachwissen und seine beruflichen Erfahrungen stets in engagierter Art und Weise in den VDI eingebracht und unsere Aufgaben beispielhaft vorangetrieben.

Prof. Dr.-Ing. Harald Bradke
Vorsitzender VDI-GEU

Pof. Dr.-Ing. Uwe Görisch
Stellv. Vorsitzender VDI-GEU

Technische Hochschule Deggendorf

Eine Hochschule und ihre Technologiezentren

Die Technische Hochschule Deggendorf (THD), gegründet 1994, ist eine von vier Technischen Hochschulen in Bayern und bildet heute über 6.000 Studierende aus.

Der Bereich Forschung spielt an der THD neben Lehre und Weiterbildung eine sehr wichtige Rolle, ist interdisziplinär ausgerichtet und orientiert sich an aktuellen gesellschaftlichen Herausforderungen und den Lösungsbedarfen von Wirtschaft, Gesellschaft und Industrie.

Vier Forschungsschwerpunkte stehen dabei im Fokus:

- Digitale Wirtschaft & Gesellschaft
- Nachhaltiges Wirtschaften, Innovative Werkstoffe & Energie
- Intelligente Mobilität
- Innovative Arbeitswelt & Gesundheit

Als forschungsstarke Hochschule für angewandte Wissenschaften hat die THD die Dezentralisierung von Forschung initiiert, um ländliche Regionen zu stärken. Seit 2009 betreibt sie mit großem Erfolg Forschungs- und Technologiezentren, sogenannte Technologiecampus (TCs).
Verteilt über ganz Niederbayern, die Oberpfalz und Mittelfranken, findet in regionalen Kooperationen thematisch fokussierter Wissens- und Technologietransfer statt. Zusammen mit lokalen Industrie- und Wirtschaftsunternehmen entwickeln Wissenschaftlerteams bedarfsorientierte innovative technologische Lösungen.
Laut Prof. Dr.-Ing. Andreas Grzemba, Vizepräsident für Forschung & Wissenstransfer der THD, sind die TCs bedeutende Impulsgeber für die lokale Wirtschaftsentwicklung und -förderung. Sie stärken die Innovationskapazitäten nachhaltig und verhelfen den Regionen zu überregionaler und sogar internationaler Aufmerksamkeit.
Mittlerweile gibt es bayernweit sechs Technologiecampus, vier weitere sind in Planung/im Bau.

Mit den folgenden Schwerpunkten verfolgt die THD die Zukunftsvision einer deutschland- und weltweit sichtbaren Hochschul- und Technologieregion Bayerischer Wald:

- TC Cham: Automatisierungstechnik, Robotik
- TC Freyung: Angewandte Informatik, Eingebettete Systeme, Geoinformatik, Bionik
- TC Teisnach 1: Optische Technologien, Präzisionsoptik, Hochfrequenztechnik
- TC Teisnach 2: Industrielle Sensorik für Industrie 4.0 (Gepl. Eröffnung: 2019)
- TC Grafenau: Logistik, Supply Chain Management, Data Analytics, Big Data, Räumliche Entwicklung
- Technologie- und Anwenderzentrum Spiegelau: Glasschmelz-Technologie
- kunststoffcampus bayern (mit dem Technologie- und Studienzentrum Weißenburg i. Bay. und dem TC Hutthurm [Geplante Eröffnung 2019]): Polymer-Technologien, Additive Fertigung & Leichtbau, Digitalisierte Prozesse in der Kunststofftechnik
- TC Plattling: Moderne Mobilität (Gepl. Eröffnung: 2019)
- TC Parsberg/Lupburg: Moderne Werkstoffe und ihre Verarbeitung in digitalisierten Fertigungsumgebungen (Gepl. Eröffnung: 2019)

In den letzten Jahren haben THD-Wissenschaftler zur Förderung industriegebundener Forschungsprojekte Mittel in Höhe von jährlich etwa 9,4 Mio. € eingeworben und entsprechende Labore aufgebaut (z.B. Labor Autonomes Fahren, Labor Industrie 4.0, Institut ProtectIT).
Die Zeichen stehen an der THD auch weiterhin auf Wachstum. Im Juli 2018 genehmigte der Ministerrat die Errichtung eines Zentrums für Digitalisierungstechnologien, dem eine 7. Fakultät mit innovativen Informatik-Studiengängen angegliedert werden wird. Die Fakultäten, TCs und Industriepartner werden hier mit vereinten Kompetenzen an Zukunftsthemen wie Big Data, Künstliche Intelligenz, Cyber Security und High Performance Computing forschen.
Kontakt: vp-forschung@th-deg.de

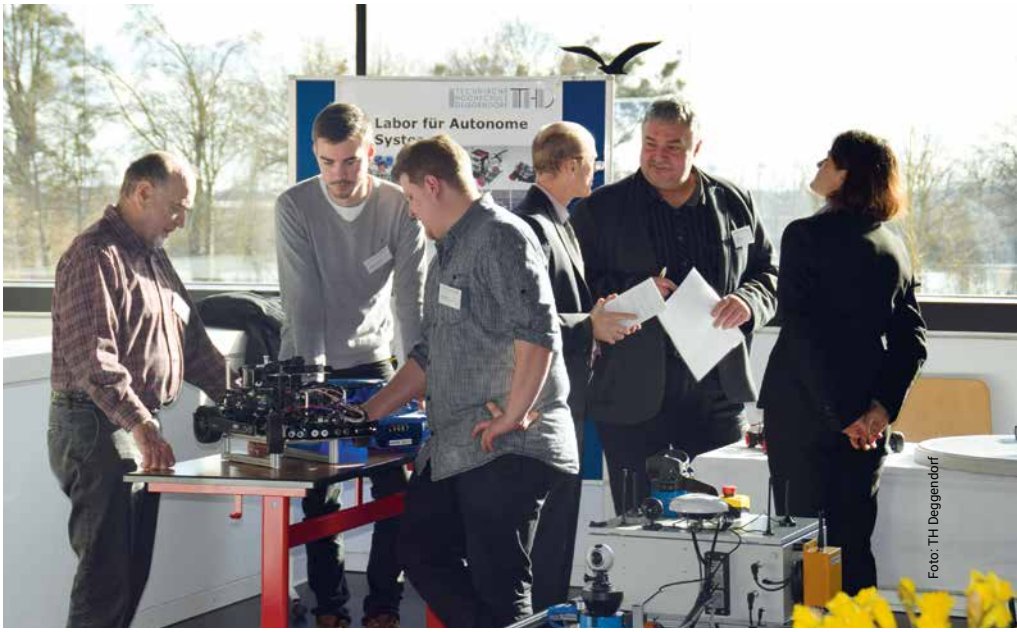


Foto: TH Deggendorf

Das Labor für Autonomes Fahren an der TH Deggendorf

VDI-AK „Technischer Vertrieb & Produktmanagement“ München

Das neue Datenschutzrecht im Vertriebsumfeld – am Beispiel IoT


Foto: Pröll

Am 16. Juli 2018 trafen sich etwa 25 Mitglieder des Arbeitskreises am Standort Garching der TUM fml, um sich über die neuen (alten?) Datenschutz-Regelungen zu informieren, und zwar am Beispiel einer echten Zukunftsbranche: dem „Internet of Things.

Der Referent Florian G. Padberg (siehe Foto), seines Zeichens Diplom-Kaufmann, Vertriebs-Consultant und Datenschutz-Experte der ituso GmbH aus Gröbenzell, schuf zunächst die nötigen Grundlagen, um das Thema „Datenschutz“ richtig einordnen und von anderen Disziplinen wie etwa der IT-Sicherheit sauber abgrenzen zu können. Denn im Datenschutz geht es um die Missbrauchsvermeidung bzgl. sog. „personenbezogener Daten“ (pbD) wie etwa Namen, Adress- und Kontaktdaten, aber auch Gesundheitsdaten oder Daten zur politischen Gesinnung. Im Sinne des Datenschutzrechts dürfen diese Daten durch Unternehmen nur auf Basis definierter Rechtsgrundlagen und unter Einhaltung bestimmter technischer und organisatorischer Maßnahmen verarbeitet werden – wobei die „Verarbeitung“ bereits bei der Erfassung anfängt und erst mit der Vernichtung der Daten endet.

Das Marktortprinzip

Die neue EU-Datenschutzgrundverordnung – kurz EU-DSGVO – die seit 25. Mai 2018 ihre Wirkung entfaltet, schafft nun einen stärker vereinheitlichten Datenschutz-Rechtsraum, der – und das ist eine der Kern-Neuerungen – nach dem „Marktortprinzip“ auch für Nicht-EU-Konzerne gilt, sobald sie in Europa aktiv sind. Die EU-DSGVO bringt insbesondere höhere Transparenz- und Informationspflichten sowie einen verschärften Strafkatalog mit sich. Saubere Einwilligungen zur Verarbeitung pbD einholen, die Dienstleister vertraglich einbinden, die Geschäftsprozesse (insbesondere den Akquise- & Vertriebsprozess) auf Datenschutz-relevante Aspekte prüfen – das sind die Hauptaufgaben, die ein Unternehmen nun priorisiert angehen muss.

Der potenzialstärkste Markt

Das „Internet of Things“ – kurz IoT – zeichnet sich dadurch aus, dass es durch die Anbindung von Geräten an das World Wide Web einen intensiven Datenaustausch ermöglicht und dadurch wiederum smarte Anwendungen rund um zeitlich und/oder lokal abgestimmte, individualisierte Dienste effizient machbar werden. In einer immer mehr technisierten und nach Individualität strebenden Welt ist IoT damit einer DER potenzialstärksten Märkte überhaupt.

Zahlreiche Stolperfallen

Dass Datenschutz auch und gerade im hochvernetzten und dynamisch wachsenden IoT-Markt immer relevanter wird, zeigt sich nicht nur durch die Bedenken der Konsumenten, bei denen die Gefährdung der Privatsphäre weit oben rangiert. Auch die immanenten Komplexitätstreiber des Geschäftsmodells – wie zahlreiche Marktbeteiligte, die Menge an möglichen Datenquellen, Transportwegen und -zielen – oder (noch) nicht vollständig geklärte Verantwortlichkeiten zeugen davon, dass in diesem Markt die eine oder andere „Stolperfalle“ droht.

Beim Smart Car beispielsweise müssen die unterschiedlichen Interessen der beteiligten Player (Autohersteller, Versicherungen, Location-based-Services-Anbieter usw.) in Einklang gebracht werden mit den Transparenz- und Schutzanforderungen der Konsumenten: Was wird mit MEINEN Daten angestellt, wo werden sie verarbeitet, wer bekommt welchen Teil davon? Hier ist bspw. ein klares, umfassendes und dennoch einfach handhabbares Einwilligungs-Management nötig. Im Smart Home hängt es davon ab, wie genau die Verbrauchsinformationen der schlauen Zähler auf einzelne Personen zurückführbar sind, denn so sind Ableitungen möglich, die man als Verbraucher ggf. nicht gerne sieht.
Der Abend wurde nach intensiver Diskussion mit dem Fazit geschlossen, dass gerade der Vertrieb durch einen offensiven und transparenten Umgang mit dem Thema Vertrauen aufbauen und so langfristige Kundenbeziehungen und damit auch Umsatzpotenziale schaffen kann.

Florian Padberg und Norbert Pröll

VDI Landesverband Bayern

Ohne Informationsaustausch geht es nicht

Nicht nur für Mitglieder, sondern auch für die ehrenamtlichen Funktionsträger und hauptamtlichen Mitarbeiter des VDI e.V. Landesverbandes Bayern ist der Informationsaustausch eine feste Größe im jährlichen Vereinsleben.
Bei zahlreichen VDI-Veranstaltungen während eines Jahres tauschen sich die Mitglieder sowie Interessierte in Arbeitskreisen der Bezirksvereine und Bezirksgruppen sowie in örtlichen Tagungen zum Thema Technik und Ingenieurwesen in Bayern aus, um auf dem aktuellen Stand zu bleiben.

Der Landesverbandsvorstand

Der Vorstand des Landesverbandes Bayern nutzt die Gelegenheit zum regen Informationsaustausch während seiner regelmäßigen jährlichen Sitzungen. Neben den Formalien und der Planung künftiger Veranstaltungen, wie beispielsweise dem kommenden VDI Forum 2018 am Dienstag, 20. November im Oskar von Miller Forum in München zum Thema „Urbane Produktion und Logistik - Leben und Arbeiten wieder vereinen“, nutzt das Gremium die Chance, aktuelle Informationen vor Ort zu erhalten.
Während ihrer diesjährigen Oktobersitzung erhielten die Vorstandsmitglieder bei einer Führung im BMW Werk Landshut interessante Einblicke in die Herstellung von Sondermotoren, dem Leichtmetallguss und der Carbon-Fertigung. Neben den aktuellen Motorbaureihen stellt BMW mit der Fertigung von Elektro- und Sondermotoren Hochleistungsmotoren bis hin zu Zwölfzylindermotoren her. An die 30.000 Elektromotoren werden hier jährlich produziert. Für das Jahr 2019 ist u.a. der Start der Produktion des Elektromotors für den vollelektrischen MINI geplant. In der Leichtmetallgießerei wurde den Teilnehmern gezeigt, wie bei BMW jährlich über 5 Millionen Gusskomponenten aus Aluminium und Magnesium herstellt werden, z.B. Zylinderköpfe oder Kurbelgehäuse. Ebenso werden in diesem BMW-Werk Karosserieteile aus Carbon gefertigt, die durch ihre vielfältigen Eigenschaften wie extremer Stabilität, Leichtigkeit aber auch Korrosionsresistenz im Fahrzeugbau eine immer wichtigere Stellung einnehmen. BMW beschäftigt derzeit über 4.300 Mitarbeiter im Landshuter Werk.
Im Anschluss an diese interessante wie aufschlussreiche Werksbesichtigung nutzten die Vorstandsmitglieder die Möglichkeit zur Durchführung ihrer zweiten Vorstandssitzung für 2018 in der Konferenzzone des BMW-Werkes Landshut.

Die Hauptamtlichen

Aber auch im hauptamtlichen Bereich des VDI e.V. ist der Informationsaustausch eine feste Größe im Jahreslauf. An die drei- bis viermal jährlich treffen sich die Geschäftsstellenleiter aller 15 VDI Landesverbände zu einer Arbeits- und Informationstagung. Hierbei sind die persönlichen Kontakte das A und O, die somit ein unkompliziertes wie einfaches Zusammenarbeiten über regionale Grenzen hinweg garantieren. Unter fachkundiger Leitung durch die Hauptgeschäftsstelle, hier dem Bereich der Mitglieder- und Regionalorganisation, erhalten die teilnehmenden Geschäftsstellenleiter Wissenswertes über Technik, zu Themen der Vereinsorganisation aber auch zu Kultur.
Unter Federführung des VDI Landesverbandes Bayern trafen sich dieses Jahr die hauptamtlichen Geschäftsstellenleiterinnen und Mitarbeiterinnen der vier bayerischen Bezirksvereine – sowie der Redaktion „Technik in Bayern“ in Nürnberg. Das Motto dieses Arbeitstreffens war der Gedankenaustausch über die jeweilig anstehenden und durchgeführten Projekte und Veranstaltungen in den Bezirksvereinen sowie der täglich zu erledigenden VDI-Geschäftsstellenarbeit.
Als Fazit ist festzuhalten: Der persönliche Kontakt und die Diskussion über die tägliche Vereinsarbeit trägt zur vereinfachten Bewältigung der Aufgaben und Ziele und einem unkomplizierten Umgang untereinander bei.

Günther Pfrogner

Foto: Silvia Stettmayer

Jetzt anmelden zum VDI Forum 2018!

Urbane Produktion und Logistik – Leben und Arbeiten wieder vereinen

Anlässlich des VDI-Jahresthemas „Urbane Produktion und Logistik“ veranstaltet der VDI Landesverband zusammen mit dem VDI BV München und dem VDI e.V. am 20. November um 18.00 Uhr im OSKAR VON MILLER FORUM in München ein Forum.

Anmeldung nur online bis Freitag, 09.11.2018 | Das Programm und weitere Infos unter **www.verein-der-ingenieure.de**

VDI-AK Technikgeschichte München

Die Fernmeldetechnische Lehrsammlung der Bundeswehr in Feldafing

Der VDI AK Technikgeschichte lud am 6. September 2018 zu einer Führung durch die Lehrsammlung für Nachrichten-, Fernmelde- und Informationstechnik der Bundeswehr ein.

Etwa 50 Teilnehmer, die meisten zwar mit grauem Haar über der Schädeldecke, aber mit jung gebliebenen grauen Zellen darunter, folgten begeistert der professionellen Führung von Hauptmann Wolfgang Schmidt, Manfred Kienzle und Stefan Becker. Eine Besonderheit dieser Sammlung ist, dass viele Exponate in funktionsfähigen Zustand gebracht wurden, mit Ergänzungen und Nachbauten, also nicht unbedingt im Originalzustand, aber „zum Anfassen".

Fernsprech- und Fernschreibtechnik

Eine Menge Exponate aus verschiedenen Epochen zogen die Besucher in ihren Bann. Beispielsweise ist ein sog. Festungsfernsprecher in eine Wand eingebaut, aus massivem Gusseisen, schuss- und explosionssicher. Über eine Handvermittlung konnte die Verbindung zu einem beliebigen Telefonapparat im Ausstellungsraum hergestellt werden. Die Technik der Zweidraht-Sprachübertragung war bei allen Geräten aus verschiedenen Ländern gleich, so dass erbeutete Geräte unschwer in das eigene Netz eingebaut werden konnten. Die ausgestellten Geräte dürfen, ja sollen von den Besuchern benützt werden, und so drehten eine ganze Menge flinker Finger an den Induktorkurbeln. Nicht-trivial ist auch heute noch die Technik der mobilen Kabelverlegung. Einige Geräte dazu waren zu sehen, und auch dazu erfuhren die Besucher Tipps aus der Praxis.

Manfred Kienzle erklärt eine nachgebaute Kodierwalze der Enigma

Fotos: Peter von Bechen

Feldfernschreiber Hell, Bj. 1941

Analoge Richtfunkgeräte für die Frequenzbereiche 1,5 GHz und 15 GHz

Foto: Peter Baier

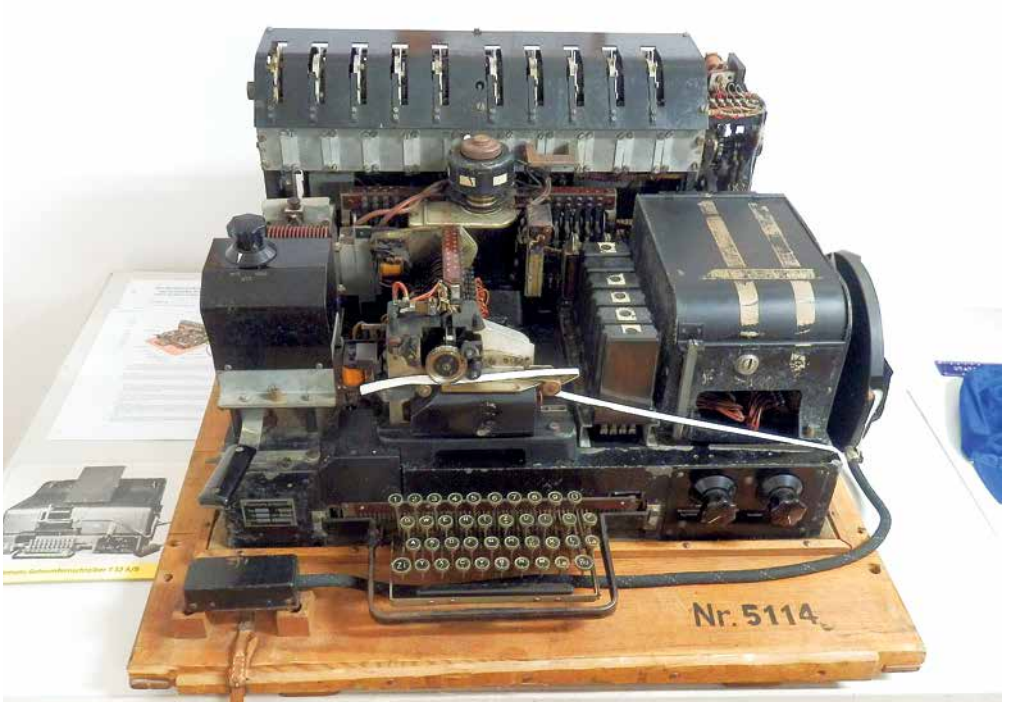
Funktechnik

Im militärischen Bereich von Anfang an äußerst wichtig, nehmen die Exponate der Funktechnik einen breiten Raum ein. Neben Sende- und Empfangsgeräten waren wichtige Einzelbauteile zu sehen wie Senderöhren bis in den Kilowatt Leistungsbereich und rauscharme Vorverstärkerröhren für Empfänger. Da die Funktechnik ursprünglich das Morsealphabet benützte, waren mehrere funktionsfähige Morsetasten ausgestellt, an denen mancher Besucher seine diesbezüglichen Fähigkeiten erproben konnte. Die mobile militärische Richtfunktechnik war mit mehreren sehr gut erhaltenen Geräten vertreten, zu denen es noch eine ausgezeichnete Spezialführung gab, denn der ehemalige Entwickler war anwesend. Die Geräte zeigten die hohe Zeit der Feinmechanik in der Funktechnik – der geniale Konstrukteur für präzise Kurbelantriebe zur Einstellung von Frequenzen und Pegeln war mindestens so wichtig wie der Entwicklungsingenieur der Hochfrequenztechnik.
Interessant sind auch Ausstellungsstücke für die optische Sprachübertragung mit moduliertem Licht, die beispielsweise für Verbindungen zwischen Schiffen eingesetzt wurden.

Kryptographie

Eine Perle der Ausstellung ist die Enigma, das berühmte Verschlüsselungsgerät der deutschen Wehrmacht. Neben einem Originalgerät ist ein funktionsfähiger Nachbau ausgestellt, den man auch benützen kann. Eine Tastatur dreht beim Eintippen eines Buchstabens die Kodierwalzen und erzeugt chiffrierte Buchstaben, die auf einem Lampenfeld an-

gezeigt werden. Herr Kienzle hat sich sehr intensiv mit der Technik und der Geschichte der Enigma beschäftigt und hielt dazu ein interessantes Tutorial. Viele Geschichten und Legenden ranken sich um dieses Gerät und seine Entschlüsselung durch die Alliierten. So führte Herr Kienzle aus, dass vor der Einführung im militärischen Bereich eine zivile Version auf dem freien Markt erhältlich gewesen sei, die u.a. der polnische Geheimdienst erwarb. Damit war das Konstruktionsprinzip frühzeitig bekannt, man konnte aber trotzdem den tagesaktuellen Schlüssel noch nicht brechen. Dazu holte man sich Mathematiker von der Universität Posen, der bekannteste war Marian Rejewski. An sie erinnert heute ein Denkmal vor dem Schloss von Posen. Sie fanden kryptologische Schwachstellen, über welche die Dechiffrierung gelang. Eine davon war die militärisch fest definierte Form von Anweisungen, eine andere die allerdings später aufgegebene Art der Übertragung eines für jeden Funkspruch individuellen Teilschlüssels, dem sog. Spruchschlüssel. Darüber hinaus bot das Verdrahtungsschema eines Steckerfeldes einen Angriffspunkt. So wurde nie ein Buchstabe in sich selbst kodiert, was kryptologische Analyseansätze erlaubte. Warum war die Konstruktion so gewählt worden? Der Legende nach waren es Kostengründe, es wäre ein zusätzlicher Kontakt notwendig gewesen. Ein Argument, das auch heute sehr modern ist.



Fernschreibgerät mit integrierter Verschlüsselung

Turing Bombe

Marian Rejewski ersann zur Entschlüsselung eine elektromechanisch betriebene Maschine, genannt die „Bombe", mit vielen der Enigma nachempfundenen schnell rotierenden Walzen, die auf Basis von kryptologischen Vorinformationen den möglichen Schlüsselraum durchsuchen konnte. Sie wurde später in England zu der sog. Turing-Bombe weiterentwickelt und erlaubte es, die Funksprüche der Deutschen innerhalb kurzer Zeit zu entziffern. Von der „Bombe" sind keine Originalexemplare erhalten geblieben, aber es gibt einen funktionsfähigen Nachbau in England.

Die Sammlung ist für die Öffentlichkeit zugänglich, es gelten jedoch bestimmte Auflagen, da sie sich im militärischen Sicherheitsbereich befindet.

Anmeldung über: Htm Wolfgang Schmidt, ITSBwLehrsammlung@bundeswehr.org, oder den Förderverein Militärhistorische Lehrsammlung Nachrichten-, Fernmeldetechnik e.V., Herr Igor Asl, Tel. 08157 – 273 2912.

Eine Zusammenarbeit mit der Volkshochschule Starnberg ist geplant.

Teilnehmer vor der Fernmeldetechnischen Lehrsammlung

Fotos: Peter Baier

Fritz Münzel

VDE/VDI-AK Informationstechnik München

Das neue spannende Programm

Es gibt ein neues Programm für den VDE/VDI Arbeitskreis Informationstechnik, diesmal bis zum Juni 2019.

Angefangen hat es im September 2018 mit dem Vortrag „Security by Design for Industrie 4.0“ mit Dr. Rainer Falk von Siemens. Der Vortrag bildete vielfach eine gute Anknüpfung an das letzte Programm, in dem es bereits sehr häufig um verschiedenste Themen der Internet-Sicherheit ging. In dem Vortrag im September ging es speziell um die Sicherheit bei Industrie 4.0. Allerdings sind dort die Prioritäten bei den Sicherheitsbedürfnissen ganz anders als in der Office-IT-Welt. Denn Verfügbarkeit und das Laufen der Produktion ist oberstes Gebot. Stillstand durch häufiges Booten aufgrund von Patchen, Problemen nach Upgrades, usw. sind nicht akzeptierbar, die Produktion darf nicht beeinflusst werden.

Werden Systeme in der Office-IT-Welt nach einigen Jahren ausgetauscht, so sind in der Produktion Lebenszeiten von 20 Jahren keine Seltenheit. Aus diesem Grund gibt es für IT-Systeme in der Fertigung ganz eigene Standards in Bezug auf Sicherheit (z. B. IEC 62443). Die allerdings auch wieder je nach Branche ganz unterschiedlich aussehen können. Während des gesamten Vortrages kam es immer wieder zu regen Diskussionen. Und genau das ist ja das, was die Abende bei den Vorträgen, Exkursionen und Workshops ausmacht. Ausgewiesene Experten auf ihren Gebieten stellen sich den Fragen der Teilnehmer.

Dr. Rainer Falk bei seinem Vortrag

Haben Sie auch Lust, wieder einmal vorbeizuschauen und mitzureden? Blicken Sie hier in den Veranstaltungskalender der Technik in Bayern oder auf unsere AKI Homepage unter http://www.vdi.de/bv-muenchen/aki. Die IT-Sicherheit ist weiterhin ein Thema bei uns. Aber auch Big Data und als nächstes am 15. November zum Thema „PPDR – Kritische Kommunikation über Mobilfunk“.

Seien Sie herzlich willkommen!

Stefan Emilius

Aktuelle Informationen unter:
www.vdi.de/bv-muenchen/aki

VDI Young Professionals Technikdinner bei Roche in Penzberg

am Montag, den 26. November 2018

Es wird ein exklusives Programm geboten: Bei einer Führung erhalten Sie spannende Einblicke in die Energiezentrale, die ein Best-Practice Beispiel für Nachhaltigkeit und Energieeffizienz ist. Außerdem berichtet Dr. Ulrich Opitz, Werkleitung Penzberg, über seine Laufbahn und gibt Einblicke in seinen Arbeitsalltag.

Ein besonderes Highlight: während des Dinners bietet sich in kleinen Runden die Möglichkeit zu direkten Gesprächen.

Interessant für Studierende der Fächer Maschinenbau, Automatisierungstechnik, Elektrotechnik, Biotechnologie, Verfahrenstechnik, Informatik, Technische Gebäudeausrüstung, etc.

Bitte bei der Anmeldung die Fachrichtung mit angeben. Zielgruppe sind Jungingenieure und Studenten kurz vor dem Abschluss.

Beginn ist um 17:45 Uhr mit der Führung. Diese ist optional. **Der offizielle Teil beginnt um 18:30 Uhr.**
Anmeldungen bei Philipp Lederer: suj-rosenheim@vdi.de
Veranstalter: VDI SuJ Rosenheim und München und die Firma Roche (Roche ist in 82377 Penzberg, Nonnenwald 2).

VDI-AK Produktionstechnik Bayern Nordost

Turbinenschaufeln und Triebwerkskomponenten

Am 25.7.2018 konnte der AK-Produktionstechnik die in Nürnberg alteingesessene Firma LEISTRITZ besuchen. Wir wurden vom Marketingleiter Herrn Thummert empfangen. Er ging in seiner Präsentation auf den Werdegang der Firma ein, die 1905 in Nürnberg von Paul Leistritz, gegründet wurde.

Waren es 1905 Turbinenschaufeln für Dampfturbinen, so sind es heute Triebwerks- und Turbinenkomponenten für Flugzeugtriebwerke, sowie Gas- und Dampfturbinen. Die Rohteile für diese Komponenten sind in großem Maß Schmiedeteile, die im Werk Remscheid und in Thailand hergestellt werden. Die Fertigbearbeitung der Teile aus Remscheid erfolgt vollständig in Nürnberg, die aus Thailand teilweise in Nürnberg. Die Bearbeitung erfolgt im Wesentlichen auf 5-Achs-Fräszentren und ECM-Maschinen (electrochemical machining).
Weltweit beschäftigt LEISTRITZ derzeit 2078 Personen, in Nürnberg gut 800.
Bereits in der Vergangenheit wurde eine hohe Flexibilität durch Mehrfachbedienung von Maschinen erreicht. Die ersten Schritte zur weiteren Optimierung – automatisiertes Be- und Entladen der Maschinen – sind getan und werden im Rahmen eines Investitionsprogramms konsequent weiter verfolgt.
Eine große Herausforderung stellt die Forderung der Flugzeugindustrie dar, den einmal festgelegten und homologierten Fertigungsprozess für alle Zeit und alle Ersatzteilanforderungen zu gewährleisten.

Das zweite Geschäftsfeld sind Schraubenspindelpumpen und -systeme. Die ersten Pumpen wurden bereits 1924 entwickelt und produziert. In diesem Bereich fällt auf, das es zwar ein umfassendes Produktprogramm gibt, aber keine Standardprodukte, die der Kunde aus einem Katalog auswählen kann.
Die besonderen Anforderungen, die kundenseitig an die Schraubenspindelpumpe gestellt werden, erfordern individuell maßgeschneiderte Lösungen.
Ca. 300 Mitarbeiter sorgen für weltweit zufriedene Kunden. Die kleinsten Aggregate finden im Kofferraum eines Kombis Platz, für die größten Systeme muss der Schwertransporter anrollen.

Ebenso kundenorientiert werden Extruder und Extrusionsanlagen für die Kunststoff- und Pharmaindustrie hergestellt. Die individuell ausgelegten gleichläufigen Doppelschneckenextruder und Extrusionsanlagen werden von ca. 200 Mitarbeitern gebaut, bei der weltweiten Kundschaft montiert und in Betrieb genommen.
LEISTRITZ ist mit seinen Extrusionsanlagen im GMP-Design (Good-Manufacturing Practice: Qualitätsrichtlinien in der Arzneimittelindustrie) Marktführer.

Der vierte Geschäftsbereich Werkzeugmaschinen, Hartmetallwerkzeuge und Rohrtechnik (früher Pkw Abgassysteme) befindet sich im Werk Pleystein, nahe der tschechischen Grenze. Die hohen Qualitätsanforderungen, die an die Fertigung, sowohl der Teile für die Luftfahrtindustrie, wie auch für die Pumpen und Extruder, gestellt werden, haben dazu geführt, dass LEISTRITZ Werkzeugmaschinen entwickelt hat, die auf dem Markt so nicht zu kaufen waren. Das Produktprogramm umfasst CNC-Wirbel- und Nutenziehmaschinen und ECM-Maschinen. Als brandneues Produkt wurde uns die neu entwickelte ECM Maschine gezeigt, die durch Pulsen eine noch höhere Produktqualität ermöglicht.
Die Hartmetall-Präzisionswerkzeuge sind schwerpunktmäßig auf die drehende Bearbeitung von Werkstücken und die Weiterbearbeitung von Drehteilen ausgelegt.
Der Bereich Rohrtechnik fertigt kundenspezifische Rohrkomponenten, z.B. Tankeinfüllstutzen, oder Abgasrohre für Premium-Automobile.

Bei einem Imbiss wurden geduldig und ausführlich viele weitere Fragen beantwortet, so dass auch diesmal der geplante Zeitrahmen überzogen wurde.

Hans-Peter Schobig

Modernste Turbinenkomponenten von Leistritz: Leichtbauschaufeln aus Titanaluminid

VDI-AK FiB München

Nachruf zum Tod von Prof. Dr. Susanne Ihsen

Prof. Dr. Susanne Ihsen verstarb plötzlich und unerwartet am 20. August 2018. Ihren viel zu frühen Tod im Alter von nur 54 Jahren bedauern wir sehr. Sie wird uns als unermüdlich engagierte Vorreiterin für die Rolle der Frauen in den Ingenieurwissenschaften im Gedächtnis bleiben.

Prof. Dr. Ihsen warf als Sozialwissenschaftlerin ihren Blick besonders auf die Ingenieurinnen und Ingenieure. Schon ihre Doktorarbeit titelte mit „Qualitätskultur in den Ingenieurwissenschaften". Das Thema Gender Diversity machte sie sich sehr zu eigen und vertrat es vehement im Beruf und in vielen Ehrenämtern. Den VDI lernte Prof. Dr. Ihsen im Jahr 1999 als Leiterin der Abteilung „Beruf und Karriere" in der Düsseldorfer Hauptgeschäftsstelle kennen. Sie beriet von dort aus die VDI-Mitglieder zu berufs- und karriererelevanten Fragen. Ende 2004 wurde sie als Professorin für Gender Studies in Ingenieurwissenschaften an die TU München berufen. Ihre wissenschaftlichen Arbeiten und ihr persönliches Engagement zu Frauen und MINT verfolgten das Ziel, mehr Chancengleichheit und Vielfalt in die technischen Berufe zu bringen.

Als Ehrenamtliche kam Prof. Dr. Ihsen wieder zum VDI – sie engagierte sich viele Jahre als stellvertretende Vorsitzende im bundesweiten VDI-Netzwerk Frauen im Ingenieurberuf. Im VDI BV München war sie in den Jahren 2010-2012 Mitglied im Vorstand und leitete den Münchener VDI-Arbeitskreis Frauen im Ingenieurberuf.

Für ihr großes Engagement für eine stärkere Rolle von Frauen in den Technikwissenschaften wurde sie im Jahr 2015 mit der Bayerischen Verfassungsmedaille in Silber ausgezeichnet.

Foto: privat

Wir danken ihr und bedauern ihren frühen Tod. Unser Mitgefühl gilt ihrer Familie und Freunden.

VDI FiB München

VDI-AK Produkt- und Prozessgestaltung Nordost

Führen von Projektteams mit 3G

Referent: Dr. Werner Bitterwolf, Ingenieur und Psychologe

Projektleiter sind Führungskräfte ohne Macht. Gerade sie müssen deshalb in der Lage sein, die Projektmitglieder zu gewinnen und dafür sorgen, dass diese ein möglichst großes Engagement für das Projekt entwickeln, dass es gewissermaßen IHR Projekt wird. Selbst wenn die Planung eines Projektes nichts zu wünschen übriglässt, kann es im Projektablauf zu Problemen kommen, weil Verhaltensweisen unkalkulierbar sind und deswegen das menschliche Miteinander nicht klappt.

Menschenführung geschieht über Kommunikation. Die Erfahrung zeigt immer wieder: Menschen sind dann am meisten bereit, sich für eine Sache einzusetzen, wenn es gelingt, sie in Ihrer Persönlichkeit anzusprechen. Freundliches und höfliches Verhalten und die Beachtung von Gesprächsregeln sind dabei selbstverständlich. Mit dem neu entwickelten 3G-Kommunikationsmodell, das 2016 in den Markt eingeführt wurde, gelingt es darüber hinaus, individuell, d. h. persönlichkeitsbezogen, zu kommunizieren. Dabei gilt: Ein und dieselbe Sache muss verschiedenen Personen auf unterschiedliche Weise nahegebracht werden, um erfolgreich zu sein.

Wie dies geschehen kann und was dies für die Führungsrolle in Projektteams bedeutet, darüber informiert Sie dieser Vortrag.

Die Teilnehmer haben die Möglichkeit, in einem Kurztest via Smartphone im Internet ihre eigene 3G-Persönlichkeitsstruktur zu ermitteln. Zudem erhalten sie eine kostenlose Lehrbroschüre zur 3G-Kommunikation.

22.11.2018, 19:00 Uhr
Technische Hochschule Nürnberg
Kesslerplatz 12, Raum KA.440b
Anmeldung per E-Mail:
ak-ekv-bno@vdi.de

Nicht verpassen!

Treffs, Vorträge und Exkursionen des VDI München/VDE Südbayern

02. November 2018 / Freitag

09:45 Exkursion

Exkursion Adelholzener Alpenquellen

Veranstalter: VDE Rosenheim, VDI Rosenheim, SuJ Rosenheim
Ort: Siegsdorf
Adresse: St.-Primus-Str. 1-5, 83313 Siegsdorf, Adelholzener Werke
Info: Für Fahrgemeinschaften von Bad Aibling, Rosenheim und ggf. weitere Orte helfen wir gerne vermittelnd. Bitte bei Anmeldung angeben, ob jemand Personen mitnehmen kann bzw. zwingend eine Fahrgemeinschaft benötigt. Anmeldung: Rainer Vogt: vde-rosenheim@vde-online.de, Tel (P. Lederer): 08034-7075955
Anmeldung: Rainer Vogt: vde-rosenheim@vde-online.de, Tel (P. Lederer): 08034-7075955

---

05. November 2018 / Montag

19:00 Treff

VDE Young Professionals Stammtisch mit Hochschulgruppe

Veranstalter: VDE YoungProf/Hochschulgruppe
Ort: München
Adresse: Milchstraße 1, 81667 München, Lollo Rosso Bar(varian) Grill
Info: Evtl. Terminänderungen entnehmen Sie bitte unserer Homepage www.vde-suedbayern.de // Um Anmeldung wird gebeten, bitte nach Möglichkeit per Mail: stammtisch@vde-muenchen.de

---

06. November 2018 / Dienstag

18:00 Vortrag

Festveranstaltung „40 Jahre Aktuelles Forum Technik“

Veranstalter: VDI-AK Aktuelles Forum Technik
Ort: München
Adresse: Brienner Str. 39, 80333 München, Hansahaus, Saal
Anmeldung: Online Anmeldung

19:00 Vortrag

Betriebsoptimierung von Kälteversorgungssystemen am Beispiel einer Kältemaschine mit Wasser als Kältemittel

Veranstalter: VDI-AK Technische Gebäudeausrüstung
Ort: München
Adresse: Lothstr. 34, 80335 München, Hochschule München, Fachbereich 05, Nr.G-1.27
Referent: M. SC Jörg Benz, Hochschule München
Info: Org.: Prof. Dr. Martin Ehlers, martin.ehlers@hm.edu, kostenlose Parkmöglichkeiten in der Tiefgarage. Wir freuen uns auf Sie!

17:30 Vortrag

Traktions- und Bordnetzaggregate für die Bahnanwendung

Veranstalter: VDI-AK Fahrzeug- und Verkehrstechnik
Ort: München
Adresse: R 1.049, 80335 München, Hochschule München
Referent: Dipl.-Ing. Jan Harthan
Info: Parken in der Tiefgarage, gutmann@hm.edu

---

07. November 2018 / Mittwoch

18:00 Vortrag

Vortrag Rosenheim vor 50 Jahren

Veranstalter: VDI BG Rosenheim, VDE Rosenheim, VDI SuJ Rosenheim
Ort: Rosenheim
Adresse: Samerstr. 17, 83022 Rosenheim, Flötzinger Bräustüberl
Referent: Harold Plesch
Info: Vortrag im Rahmen des Stammtisches

---

08. November 2018 / Donnerstag

18:00 Vortrag

Philipp von Jolly (1809-1884) – er legte die Erde auf die Waage

Veranstalter: VDI-AK Technikgeschichte
Ort: München
Adresse: Ledererstraße 5, 2. Stock (Lift), 80331 München, Akad. Gesangverein (AGV), Max-Planck-Saal 2. Stock (Lift)
Referent: Dr. rer. nat. Heinrich C. Soffel, LMU Section Geophysik
Info: 08105 4261
Anmeldung: Online Anmeldung

---

12. November 2018 / Montag

16:30 Vortrag

What Can Proposed „Negative Emissions Technologies” for Removing CO_2 from the Atmosphere Contribute towards Achieving the Paris Agreement?

Veranstalter: Münchner Zentrum für Wissenschafts- und Technikgeschichte
Ort: München
Adresse: Museumsinsel 1, 80538 München, Deutsches Museum, Bibliotheksbau, Alter Seminarraum (1402)
Referent: Prof. Dr. Mark G. Lawrence, Institute for Advanced Sustainability, Potsdam

---

18:15 Vortrag

Anatomie des Vertrauens – Ist Vertrauen ein gefährliches Gefühl?

Veranstalter: VDE-AK ML
Ort: München
Adresse: Haidenauplatz 1, 81667 München, MDK Bayern, im Haus des Bayerischen Staatsministeriums für Gesundheit und Pflege, Raum Nymphenburg, 6. OG
Referent: Prof. Dr. Jürgen Wertheimer, Deutsches Seminar, Philosophische Fakultät, Eberhard Karls Universität Tübingen

---

19:00 Treff

November Stammtisch der Studenten und Jungingenieure München

Veranstalter: VDI AK Studenten und Jungingenieure München
Ort: München
Adresse: wird noch bekanntgegeben, 80802 München

---

13. November 2018 / Dienstag

17:30 Vortrag

Hintergründe zu möglichen Fahrverboten in deutschen Städten; WLTP; RDE; Vergleich Otto/Diesel, Auswirkungen auf die AU

Veranstalter: VDI-AK FVT + Hochschule München
Ort: München
Adresse: Lothstr. 64, 80335 München, Hochschule München, Hörsaal R1.049
Referent: Dipl.-Ing. Erik Pellmann
Info: Parken in der Tiefgarage, bei Rückfragen: gutmann@hm.edu

---

19:00 Treff

VDI/VDE Treff

Veranstalter: VDI BG Landshut
Ort: Landshut
Adresse: 84030 Landshut, Gasthaus „Zur Insel"
Info: Dr. Helmut Strasser, Tel. 0871/74197

---

15. November 2018 / Donnerstag

18:00 Exkursion

Exkursion: Smart Grid Labor

Veranstalter: VDE-AKE
Ort: Garching
Adresse: Lichtenbergstraße 4a, 85748 Garching, Forschungscampus Garching
Referent: M.Sc. Franz Christange, Dr.-Ing. Peter Tzscheutschler
Anmeldung: erforderlich: www.vde-suedbayern.de

19:00 Vortrag

Public Protection Desaster Relief (PPDR) – Kritische Kommunikation über Mobilfunk

Veranstalter: VDE/VDI-AK Informationstechnik
Ort: München
Adresse: Werinherstraße 91, 81541 München, Nokia Solutions and Networks GmbH & Co. KG, Gebäude 41, Konferenzzone
Referent: Ulrich Rehfuess, Nokia Networks
Info: aki@vde-suedbayern.de

---

19. November 2018 / Montag

18:00 Vortrag

Design und Recht

Veranstalter: VDI-AK TV & PM
Ort: München
Adresse: Boltzmannstr. 15, 85748 Garching, TUM fml, Gebäude 5, MW1501
Referent: RAin Heike Zirwick & RA Arno Bernhardt
Anmeldung: ehrenamt@proell-verfahrenstechnik.de

---

20. November 2018 / Dienstag

15:00 Exkursion

3D-Druck mit Silikon

Veranstalter: VDI BG Innviertel
Ort: Burghausen
Adresse: Industriepark Lindach A12, 84489 Burghausen, A12
Referent: Dr. Vera Seitz, ACEO
Gebühr: Eintritt frei
Anmeldung: Eine vorab Anmeldung ist notwenig, da die Teilnehmerzahl begrenzt ist

---

20. November 2018 / Dienstag

17:30 Vortrag

Mobile Fluid Systeme/Kühlung

Veranstalter: VDI-AK FVT + Hochschule München
Ort: München
Adresse: Lothstr. 64, 80335 München, Hochschule München, Hörsaal R1.049
Referent: Dr.-Ing. Justin Richards
Info: Parken in der Tiefgarage, bei Rückfragen: gutmann@hm.edu

---

21. November 2018 / Mittwoch

19:00 Vortrag

Optimierung komplexer Produktionsprozesse mit KI

Veranstalter: VDI fib – Frauen im Ingenieurberuf
Ort: München
Adresse: Arcisstraße 21, 80333 München, TU München, folgt
Referent: Dr. Isabell Franck, Gründerin + Geschäftsführerin der IPT – Insight Perspective Technologies GmbH
Anmeldung: Per E-Mail: fib-muenchen@vdi.de

---

22. November 2018 / Donnerstag

14:00 Vortrag

Verborgenes Universum in der ESO Supernova

Veranstalter: VDI-AK Aktuelles Forum Technik
Ort: Garching
Adresse: Karl-Schwarzschild-Str. 2, 85748 Garching bei München, ESO Supernova Planetarium
Info: Ihre Anmeldung wird nur gültig durch Überweisung von 5,00 € auf das AV-Konto**IBAN: DE23 7025 0150 0028 1010 20
Anmeldung: Online Anmeldung

19:00 Vortrag

Ein Weg zur unternehmerischen Freiheit

Veranstalter: VDI-AK Unternehmer & Führungskräfte
Ort: München
Adresse: 80000 München
Referent: Holger Körber
Info: Den genauen Ort geben wir online bzw. über unseren Arbeitskreis-Newsletter bekannt
Anmeldung: Online Anmeldung

---

23. November 2018 / Freitag

14:00 Exkursion

Exkursion zur Fima Océ

Veranstalter: SuJ Rosenheim
Ort: Poing
Adresse: Siemensallee 2, 85586 Poing, Océ
Info: Gemeinsame Veranstaltung mit den SuJ München. Für Rosenheimer Teilnehmer besteht die Möglichkeit, gemeinsam mit dem ÖPNV von Rosenheim Bhf aus zu starten. Details dazu bei der Anmeldung, bitte mit angeben, ob die Anreise direkt, oder per ÖPNV von Ro aus.
Anmeldung: Online Anmeldung

Die tagesaktuelle Veranstaltungsliste finden Sie unter www.technik-in-bayern.de

26. November 2018 / Montag

16:30 Vortrag

Techno-diplomacy: Knowledge, Power and US Foreign Policy

Veranstalter: Münchner Zentrum für Wissenschafts- und Technikgeschichte
Ort: München
Adresse: Museumsinsel 1, 80538 München, Deutsches Museum, Bibliotheksbau, Alter Seminarraum (1402)
Referent: Prof. Dr. John Krige, Georgia Institute of Technology, Atlanta

---

17:00 Vortrag

Die Rolle von flexiblen Kraftwerken und Speichern im zukünftigen Energiesystem

Veranstalter: VDI-AK Energie
Ort: Garching
Adresse: Lichtenbergstraße 2a, 85748 Garching, Institute for Advanced Study, TU München, IAS Auditorium
Referent: Prof. Dr.-Ing. Hartmut Spliethoff, TU München
Anmeldung: Online Anmeldung

17:30 Event

VDI Young Professionals Technikdinner bei Roche

Veranstalter: VDI SuJ
Ort: Penzberg
Adresse: Nonnenwald 2, 82377 Penzberg, Roche, Tor 1
Referent: Dr. Ulrich Opitz (Werksleiter)
Info: bei der Anmeldung bitte die Fachrichtung angeben
Anmeldung: bei Philipp Lederer: suj-rosenheim@vdi.de

---

27. November 2018 / Dienstag

17:30 Vortrag

Flugerprobung des A340 Laminar Flow Blade Demonstrators

Veranstalter: VDI BV AK FVT + Hochschule München
Ort: München
Adresse: Lothstr. 64, 80335 München, Hochschule München, R 1.049
Referent: Dipl.-Ing. Karl-Heinz Mai,Testpilot Firma Airbus, Toulouse
Info: Parken in der Tiefgarage, bei Rückfragen: gutmann@hm.edu

---

18:15 Vortrag

Erkenntnisgewinn 2018 – Zwischen klinischen Studien und Big Data

Veranstalter: VDE-AK ML
Ort: München
Adresse: Haidenauplatz 1, 81667 München, MDK Bayern, im Haus des Bayerischen Staatsministeriums für Gesundheit und Pflege, Raum Nymphenburg, 6. OG
Referent: Prof. Dr. rer. nat. Gerd Antes, Co-Direktor Cochrane Deutschland, Wissenschaftlicher Vorstand Cochrane Deutschland Stiftung, Universitätsklinikum Freiburg

---

28. November 2018 / Mittwoch

19:00 Vortrag

Tiefengeothermie – Brückentechnologie oder Schlüssel zu einer erfolgreichen Energiewende

Veranstalter: VDE Rosenheim, VDI BG Rosenheim, VDI SuJ Rosenheim
Ort: Rosenheim
Adresse: Hochschulstr. 1, 83024 Rosenheim, FH-Rosenheim, E.002
Referent: Hr. Flechter, TUM

---

29. November 2018 / Donnerstag

18:00 Vortrag

Energiewende – Zweite Phase

Veranstalter: VDI-AK Technikgeschichte und Hochschule München Fakultät 03
Ort: München
Adresse: Lothstraße 64, 80335 München, Hochschule München, Hörsaal R1.049, blaue Tonne
Referent: Prof. Hermann Wagenhäuser, Hochschule München
Info: 08105 4261
Gebühr: 5 Euro, Studenten, Schüler, VDI-Mitglieder und Mitglieder der Hochschule München frei
Anmeldung: technikgeschichte@verein-der-ingenieure.de

---

03. Dezember 2018 / Montag

19:00 Treff

VDI fib Weihnachtstreffen

Veranstalter: VDI fib - Frauen im Ingenieurberuf
Ort: München
Adresse: folgt rechtzeitig, 8000 München

19:00 Treff

VDE Young Professionals Stammtisch mit Hochschulgruppe

Veranstalter: VDE YoungProf/Hochschulgruppe
Ort: München
Adresse: Milchstr. 1, 81667 München, Lollo Rosso Bar(varian)Grill
Info: Evtl. Terminänderungen entnehmen Sie bitte unserer Homepage www.vde-suedbayern.de // Um Anmeldung wird gebeten, bitte nach Möglichkeit per Mail:stammtisch@vde-muenchen.de

---

04. Dezember 2018 / Dienstag

17:30 Vortrag

Flugversuch und Zulassung des A330Neo

Veranstalter: VDI-AK Fahrzeugtechnik
Ort: München
Adresse: Lothstr. 64, 80333 München, Hochschule München, R 1.049
Referent: Dipl.-Ing. Thomas Wilhelm
Info: Parken in der Tiefgarage, bei Rückfragen: gutmann@hm.edu

---

19:00 Vortrag

TGA Festvortrag 2018: Nachhaltige Gebäudetechnik: Herausforderungen und Chancen für die Zukunft

Veranstalter: VDI-AK Technische Gebäudeausrüstung
Ort: München
Adresse: Lothstr. 34, 80335 München, Hochschule München, Fachbereich 05, Nr.G-1.27
Referent: Dipl.-Ing. (FH) Bernhard Nimbach, Nimbach Ing- u. Beratungsgesellschaft Mchn.
Info: Org.: B. Fritzsche, bernhard.fritzsche@verein-der-Ingenieure.de, kostenlose Parkmöglichkeiten in der Tiefgarage. Wir freuen uns auf Sie!

---

05. Dezember 2018 / Mittwoch

18:00 Treff

Weihnachtsfeier VDI/VDE

Veranstalter: VDI, VDE, SuJ
Ort: Rosenheim
Adresse: Samerstr. 17, 83022 Rosenheim, Flötzinger Bräustüberl
Info: bei Philipp Lederer, bg-rosenheim@vdi.de, Tel: 08034-7075955, Gäste sind uns jederzeit herzlich willkommen

10. Dezember 2018 / Montag

16:30 Vortrag

Nomography at the Crossroads of Mathematics and Engineering Sciences

Veranstalter: Münchner Zentrum für Wissenschafts- und Technikgeschichte
Ort: München
Adresse: Museumsinsel 1, 80538 München, Deutsches Museum, Bibliotheksbau, Alter Seminarraum (1402)
Referent: Prof. Dr. Dominique Tournès, Université de la Réunion, Sainte-Clotilde

---

17:00 Vortrag

Sektorkopplung auf Quartiersebene: Ein wesentlicher Beitrag zur Energieeffizienz

Veranstalter: VDI-AK Energie zusammen mit der TU MÜnchen
Ort: Garching
Adresse: Lichtenbergstraße 2a, 85748 Garching, Institute for Advanced Study, TU München, IAS Auditorium
Referent: Virginia Ahuir, Zentrum Digitalisierung Bayern
Anmeldung: Online Anmeldung

19:00 Treff

Dezember Stammtisch der Studenten und Jungingenieure München

Veranstalter: VDI AK Studenten und Jungingenieure München
Ort: München
Adresse: 80802 München

---

11. Dezember 2018 / Dienstag

17:30 Vortrag

System-und/oder Komponentenbetrachtung zur zuverlässigen, robusten Produktfunktion

Veranstalter: VDI-AK Fahrzeugtechnik
Ort: München
Adresse: Lothstaße 64, 80335 München, Hochschule München, R 1.049
Referent: Dr. Stefan Kemmler
Info: Parken in der Tiefgarage, bei Rückfragen: gutmann@hm.edu

---

11. Dezember 2018 / Dienstag

19:00 Treff

VDI/VDE Treff

Veranstalter: VDI BG Landshut
Ort: Landshut
Adresse: 84030 Landshut, Gasthaus „Zur Insel"
Info: Dr. Helmut Strasser, Tel.0871/74197

---

13. Dezember 2018 / Donnerstag

18:00 Vortrag

Karfiol und Paradeiser – Kulturgeschichte und gemeinsames Erbe der Gartenpflanzen

Veranstalter: VDI-AK Technikgeschichte
Ort: München
Adresse: Ledererstraße 5, 2. Stock (Lift), 80331 München, Akad. Gesangvereins (AGV), Max-Planck-Saal 2. Stock (Lift)
Referent: Thomas Janscheck, Gartenbauingenieur und Buchautor
Info: 08105 4261
Gebühr: 5 Euro, Studenten, Schüler, VDI-Mitglieder und AGVer frei
Anmeldung: technikgeschichte@verein-der-ingenieure.de

---

18. Dezember 2018 / Dienstag

17:30 Vortrag

Gewichtsmanagement und Leichtbau im Fahrzeug

Veranstalter: VDI-AK Fahrzeugtechnik
Ort: München
Adresse: Lothstraße 64, 80335 München, Hörsaal R1.049
Referent: Markus Pfuhler, Frank Seifert
Info: Parken in der Tiefgarage, bei Rückfragen: gutmann@hm.edu

---

20. Dezember 2018 / Donnerstag

18:00 Treff

Jahresabschluss-Treffen

Veranstalter: VDI-Arbeitskreis Unternehmer & Führungskräfte
Ort: Raum München
Adresse: folgt rechtzeitig, 8000 München
Info: Genaueres erfahren Sie online bzw. über unseren Arbeitskreis-Newsletter
Anmeldung: Online Anmeldung

Nicht verpassen!

Treffs, Vorträge und Exkursionen des VDI BV Bayern Nordost

01. November 2018 / Donnerstag

09:00 Messe

Erfindermesse iENA

Veranstalter: VDI
Ort: Nürnberg
Adresse: Messezentrum 1, 90471 Nürnberg, Messezentrum Nürnberg

---

06. November 2018 / Dienstag

17:00 Exkursion

Besichtigung Labor A I R

Veranstalter: BG Ansbach
Ort: Ansbach
Adresse: Ziegelhütte 3, 91522 Ansbach, Analytik Institut Rietzler GmbH
Referent: Dipl.-Ing. (FH) Adrian Riedel
Anmeldung: Online Anmeldung

---

07. November 2018 / Mittwoch

19:00 Treff

Treff für Studenten und Jungingenieure Regensburg

Veranstalter: VDI SuJ Regensburg
Ort: Regensburg
Adresse: Gesandtenstraße 2, 93047 Regensburg, Geflickte Trommel

08. November 2018 / Donnerstag

18:30 Vortrag

Multikanalvertrieb identischer Produkte am Beispiel der Medizintechnik

Veranstalter: VDI-AK Technischer Vertrieb und Produktmanagement
Ort: Nürnberg
Adresse: Kesslerplatz 12, 90489 Nürnberg, GSO-Hochschule Nürnberg, Raum KA.440a
Referent: Prof. Dr. Roland Schnurpfeil
Info: Prof. Dr. Roland Schnurpfeil leitet den Bachelor-Studiengang Biomedizinische Technik und den Master-Studiengang Medizintechnik an der HaW Ansbach.
Anmeldung: Online Anmeldung

19:00 Treff

Treffpunkt Technikgeschichte

Veranstalter: VDI-Arbeitskreis Technikgeschichte
Ort: Nürnberg
Adresse: Wollentorstr. 3, 90489 Nürnberg, Restaurant „KIM CHUNG"
Info: Dipl.-Ing. Klaus Jantsch, Tel. (09 11) 59 13 44

09. November 2018 / Freitag

14:00 Workshop

Forschungs AG im SFZ

Veranstalter: VDI Zukunftspiloten – Schülerforschungszentrum Richard Willstätter
Ort: Nürnberg
Adresse: Innerer Laufer Platz 11, 90403 Nürnberg, Richard Willstätter Gymnasium, Schülerforschungszentrum
Info: herwanger@willstaetter-gymnasium.de
Anmeldung: Online Anmeldung

18:30 Treff

Einladung zum Stammtisch

Veranstalter: VDI-AK Produktion
Ort: Nürnberg
Adresse: Glöckleinsgasse 2, 90403 Nürnberg, Restauration Goldenes Posthorn
Info: Sollten Sie ein dringendes Anliegen haben, teilen Sie uns dies bitte vorab mit, damit wir ausführlich antworten können.
Anmeldung: Online Anmeldung

10. November 2018 / Samstag

10:00 Event

Erstitag mit Ingenieursralley

Veranstalter: Studenten und Jungingenieure Nürnberg
Ort: Nürnberg
Adresse: Keßlerplatz 12, 90489 Nürnberg, TH Nürnberg, Haupttor, an der Seite des Keßlerplatzes
Referent: Diverse
Anmeldung: Online Anmeldung

13. November 2018 / Dienstag

17:00 Treff

Treffen für technische Gespräche

Veranstalter: VDI-Bezirksgruppe Erlangen
Ort: Erlangen-Büchenbach
Adresse: Dorfstr. 14, 91054 Erlangen-Büchenbach, Gaststätte "Zur Einkehr"
Info: Dr. Hans Buerhop, Tel. (0 91 31) 4 49 54

19:00 Treff

Monatliche Zusammenkunft mit Erfahrungsaustausch

Veranstalter: VDI-Bezirksgruppe Coburg
Ort: Coburg
Adresse: Lossaustr. 12, 96450 Coburg, Hotel Stadt Coburg
Info: Dr.-Ing. Martin Schmitt, Tel. (01 60) 91 81 24 94

19:30 Treff

Treff BG Regensburg

Veranstalter: VDI-Bezirksgruppe Regensburg
Ort: Regensburg
Adresse: Adolph-Kolping-Str. 1, 93047 Regensburg, Kolpinghaus

14. November 2018 / Mittwoch

18:00 Vortrag

Was hat das Universum mit mir zu tun?

Veranstalter: BG Ansbach
Ort: Ansbach
Adresse: Residenzstr. 8, 91522 Ansbach, Hochschule Ansbach, Hans-Maurer-Auditorium,
Referent: Dr. rer. nat. Josef M. Gaßner

19:30 Workshop

Treff für Studenten und Jungingenieure Nürnberg

Veranstalter: VDI-AK Studenten und Jungingenieure Nürnberg
Ort: Nürnberg
Adresse: Augustinerstraße 1, 90403 Nürnberg, CôCô – Indochine

16. November 2018 / Freitag

14:00 Exkursion

Exkursion bei Krones in Neutraubling

Veranstalter: VDI-BG Regensburg
Ort: Neutraubling
Adresse: Böhmerwaldstraße 5, 93073 Neutraubling
Anmeldung: ekkehard.schreiber@gmail.com

19. November 2018 / Montag

19:00 Vortrag

Die Bedeutung der Ästhetik und transdisziplinärer Prozesse bei der Digitalisierung

Veranstalter: VDI-Arbeitskreis Gesellschaft und Technik
Ort: Nürnberg
Adresse: Keßlerplatz 12, 90489 Nürnberg, Technische Hochschule Nürnberg, KA.102
Referent: Michael Schels
Anmeldung: Online Anmeldung

20. November 2018 / Dienstag

19:00 Treff

Gesprächsrunde Netzwerk Nürnberg

Veranstalter: VDI-AK Netzwerk Nürnberg
Ort: Nürnberg
Adresse: Wollentorstr. 3, 90489 Nürnberg, Restaurant „KIM CHUNG"
Info: M.Eng Herbert Gaida, Tel. (01 77) 7 23 17 41

---

22. November 2018 / Donnerstag

19:00 Vortrag

Führen von Projektteams mit 3G

Veranstalter: VDI-AK Produkt- und Prozessgestaltung
Ort: Nürnberg
Adresse: Kesslerplatz 12, 90489 Nürnberg, Technische Hochschule Nürnberg, KA.440b
Referent: Dr. Werner Bitterwolf, BITTERWOLF-KASPAR GmbH, Stein bei Nürnberg
Info: Siehe Info auf S. 38
Anmeldung: Online Anmeldung

---

23. November 2018 / Freitag

14:00 Workshop

Forschungs AG im SFZ

Veranstalter: VDI Zukunftspiloten – Schülerforschungszentrum Richard Willstätter
Ort: Nürnberg
Adresse: Innerer Laufer Platz 11, 90403 Nürnberg, Richard Willstätter Gymnasium, Schülerforschungszentrum
Info: herwanger@willstaetter-gymnasium.de
Anmeldung: Online Anmeldung

---

30. November 2018 / Freitag

14:00 Workshop

Forschungs AG im SFZ

Veranstalter: VDI Zukunftspiloten – Schülerforschungszentrum Richard Willstätter
Ort: Nürnberg
Adresse: Innerer Laufer Platz 11, 90403 Nürnberg, Richard Willstätter Gymnasium, Schülerforschungszentrum
Info: herwanger@willstaetter-gymnasium.de
Anmeldung: Online Anmeldung

---

01. Dezember 2018 / Samstag

19:00 Sonstiges

Konzert zur Weihnachtszeit

Veranstalter: Musikfreunde e.V.
Ort: Nürnberg
Adresse: Auf der Burg, 90402 Nürnberg, Rittersaal der Kaiserburg
Referent: Blechbläserquintett "brasspur"
Info: Kartenbestellung über Frau Loch, Tel. (09 11) 55 40 30 oder vdi@th-nuernberg.de
Gebühr: VDI-Mitglieder 30,- Euro, Nichtmitglieder 40,- Euro
Anmeldung: Online Anmeldung

---

05. Dezember 2018 / Mittwoch

18:00 Vortrag

Unser Bankgeheimnis: Gestaltungsfreiheit – Die Team Bank und die Anforderungen der Arbeitswelt 4.0

Veranstalter: BG Ansbach
Ort: Ansbach
Adresse: Residenzstr. 8, 91522 Ansbach, Hochschule Ansbach, Hans-Maurer-Auditorium
Referent: Dr. Christiane Decker

19:00 Treff

Treff für Studenten und Jungingenieure Regensburg

Veranstalter: VDI SuJ Regensburg
Ort: Regensburg
Adresse: Am Brückenfuß 1, 93059 Regensburg, Spital Weihnachtsmarkt

---

07. Dezember 2018 / Freitag

14:00 Workshop

Forschungs AG im SFZ

Veranstalter: VDI Zukunftspiloten – Schülerforschungszentrum Richard Willstätter
Ort: Nürnberg
Adresse: Innerer Laufer Platz 11, 90403 Nürnberg, Richard Willstätter Gymnasium, Schülerforschungszentrum
Info: herwanger@willstaetter-gymnasium.de
Anmeldung: Online Anmeldung

---

11. Dezember 2018 / Dienstag

17:00 Treff

Treffen für technische Gespräche

Veranstalter: VDI-Bezirksgruppe Erlangen
Ort: Erlangen-Büchenbach
Adresse: Dorfstr. 14, 91054 Erlangen-Büchenbach, Gaststätte „Zur Einkehr"
Info: Dr. Hans Buerhop, Tel. (0 91 31) 4 49 54

19:00 Treff

Adventsabend mit Angehörigen

Veranstalter: VDI-Bezirksgruppe Coburg
Ort: Coburg
Adresse: Lossaustr. 12, 96450 Coburg, Hotel Stadt Coburg
Info: Dr.-Ing. Martin Schmitt, Tel. (01 60) 91 81 24 94
Anmeldung: Online Anmeldung

19:30 Treff

Weihnachtsfeier der BG-Regensburg

Veranstalter: VDI-Bezirksgruppe Regensburg
Ort: Regensburg
Adresse: Adolph-Kolping-Str. 1, 93047 Regensburg, Kolpinghaus

---

Die tagesaktuelle Veranstaltungsliste finden Sie unter www.technik-in-bayern.de

12. Dezember 2018 / Mittwoch

19:00 Workshop

Treff für Studenten und Jungingenieure Nürnberg

Veranstalter: VDI-AK Studenten und Jungingenieure Nürnberg
Ort: Nürnberg
Adresse: 90403 Nürnberg, Weihnachtsmarkt, Treffpunkt: Schöner Brunnen
Info: Treffpunkt: Schöner Brunnen vor dem Standesamt

13. Dezember 2018 / Donnerstag

19:00 Treff

Treffpunkt Technikgeschichte

Veranstalter: VDI-Arbeitskreis Technikgeschichte
Ort: Nürnberg
Adresse: Wollentorstr. 3, 90489 Nürnberg, Restaurant "KIM CHUNG"
Info: Dipl.-Ing. Klaus Jantsch, Tel. (09 11) 59 13 44

14. Dezember 2018 / Freitag

14:00 Workshop

Forschungs AG im SFZ

Veranstalter: VDI Zukunftspiloten – Schülerforschungszentrum Richard Willstätter
Ort: Nürnberg
Adresse: Innerer Laufer Platz 11, 90403 Nürnberg, Richard Willstätter Gymnasium, Schülerforschungszentrum
Info: herwanger@willstaetter-gymnasium.de
Anmeldung: Online Anmeldung

19. Dezember 2018 / Mittwoch

19:00 Treff

Gesprächsrunde Netzwerk Nürnberg

Veranstalter: VDI-AK Netzwerk Nürnberg
Ort: Nürnberg
Adresse: Wollentorstr. 3, 90489 Nürnberg, Restaurant „KIM CHUNG"
Info: M.Eng Herbert Gaida, Tel. (01 77) 7 23 17 41

21. Dezember 2018 / Freitag

14:00 Workshop

Forschungs AG im SFZ

Veranstalter: VDI Zukunftspiloten – Schülerforschungszentrum Richard Willstätter
Ort: Nürnberg
Adresse: Innerer Laufer Platz 11, 90403 Nürnberg, Richard Willstätter Gymnasium, Schülerforschungszentrum
Info: herwanger@willstaetter-gymnasium.de
Anmeldung: Online Anmeldung

Musikfreunde des VDI und VDE

Festliches Konzert zur Weihnachtszeit

Die Musikfreunde des VDI und VDE laden zum „Festlichen Konzert zur Weihnachtszeit" mit brasspur in die Kaiserburg Nürnberg am 1.12.18, 19:00 Uhr mit Werken von Bach, Händel, Mozart, Pachelbel u. a. sowie adventlichen Weisen.

Das Blechbläserquintett *brasspur* begeistert seit 1984 sein Publikum im In- und Ausland. Die Solisten Harald Bschorr (Posaune), Martin Ehlich (Trompete, Piccolo, Flügelhorn), Michael Engl (Tuba), Evgeni Trambev (Horn) und Stefan Wiedemann (Trompete, Flügelhorn, Akkordeon) verleihen Kompositionen und Arrangements in technischer Perfektion ihre persönliche Note. Ihr hoher Anspruch an solistischer Virtuosität, ihr makelloses Zusammenspiel sowie ein breites musikalisches Spektrum und eigene unverwechselbare Klangvorstellungen ermöglichen eine rege Konzerttätigkeit.

Kartenkategorien:
30,- Euro (VDI/VDE-Mitglieder, max. 2 Karten);
40,- Euro (Nichtmitglieder)

Kartenbestellung:
VDI@th-nuernberg.de oder
Tel. (09 11) 55 40 30
Einlass: 18.00 Uhr; Beginn: 19.00 Uhr


Bild: brasspur

VDI-AK Systems Engineering Nordost

Neuer Arbeitskreis im VDI BV Bayern Nordost

Der Begriff Systems Engineering steht aktuell bei vielen Unternehmen auf der Agenda der Digitalisierung. Es ist ein interdisziplinärer Ansatz, um komplexe technische Systeme in Projekten zu entwickeln und zu realisieren. Systems Engineering Ansätze gibt es seit rund 60 Jahren, doch erst seit dem Einzug der Digitalisierung in den Unternehmen findet es auch in der breiten Masse der Unternehmen Anklang – vor allem bei interdisziplinären Arbeiten und großen komplexen Projekten.
Bisher gibt es vergleichsweise wenig Literatur über Systems Engineering, sei es über die System-Architektur, die Modellierung mithilfe von SysML oder der Anwendung dieser Methode. Deswegen ist vor allem der Erfahrungsaustausch gefragt – auf deutschlandweiter Ebene auf Symposien, beispielsweise von namhaften Vereinen wie der Gesellschaft für Systems Engineering (GfSE), oder auf lokaler Ebene.
Um regelmäßige regionale Treffen im Raum Nürnberg/Erlangen/Ingolstadt/Regensburg zu ermöglichen, wurde der Arbeitskreis „Systems Engineering“ im Bezirksverein Bayern Nordost ins Leben gerufen.
Wissenschaftliche Vorträge geben einen Einblick in den Stand der Forschung, und Diskussionen zeigen verschiedene Perspektiven auf ein Thema auf.
Die Teilnehmerinnen und Teilnehmer profitieren von mehr Wissen und neuen Kontakten und erhalten Anregungen für Handlungsoptionen.
In der ersten Sitzung am 29. Juni 2018, die von den Arbeitskreis-Gründern Goran Madzar, Jan Vollmar und Daniela Kaiser moderiert wurde, diskutierten Vertreterinnen und Vertreter verschiedener Unternehmen und Institutionen über Herausforderungen und Fragestellungen bei der Anwendung von Systems Engineering. Dabei wurde eine Vielzahl an Themen gemeinsam identifiziert, die in den nächsten Treffen behandelt werden sollen.

Die zweite Sitzung fand am 27. September in Erlangen-Tennenlohe statt. Dort wurde das Thema Model-based Systems Engineering (MBSE) anhand eines Erfahrungsberichtes und eines Fachvortrags aufgegriffen. Hier konnten auch zentrale Fragen der Teilnehmer geklärt werden. Wir freuen uns auf das nächste Treffen.

Goran Madzar, Jan Vollmar
und Daniela Kaiser

VDI-AK Technischer Vertrieb und Produktmanagement Nordost

Multikanalvertrieb identischer Produkte am Beispiel der Medizintechnik

Referent: Prof. Dr. Roland Schnurpfeil, u.a. Leiter Master-Studiengang Medizintechnik, HaW Ansbach

Die Gesundheitswirtschaft ist mit derzeit 5,4 Millionen Beschäftigten der größte Arbeitgeber Deutschlands, damit ist fast jeder siebte Arbeitsplatz in Deutschland in der Gesundheitswirtschaft angesiedelt. Nach einer Prognose einer Studie im Auftrag des Bundeswirtschaftsministeriums aus dem Jahr 2010 werden bis zum Jahr 2030 weitere zwei Millionen Menschen mehr in der Gesundheitswirtschaft beschäftigt sein.

Das sind im Prinzip gute Nachrichten für jedes Medizintechnik-Unternehmen. Allerdings gelten in diesem Markt andere Spielregeln als in anderen Märkten: Die Abgabe von Medizinprodukten im Rahmen der gesetzlichen und privaten Krankenversicherungen erfolgt überwiegend über Apotheken, Sanitätshäuser, orthopädietechnische sowie orthopädieschuhtechnische Betriebe, Hörgeräte-Akustiker und Augenoptiker – in Summe ca. 37.000 Betriebe in Deutschland. Diese beziehen ihre Waren entweder direkt vom Hersteller oder über einen Groß- oder Zwischenhändler. Für einige dieser Produkte, Medizinische Hilfsmittel genannt, hat der Spitzenverband der Gesetzlichen Krankenversicherungen (GKV Spitzenverband) sog. Festbeträge festgelegt.

Das bedeutet, dass die Krankenkassen nur einen Sockelbetrag für diese Produkte erstatten und die Patienten die Differenz zum Marktpreis selbst tragen müssen. Diese wirtschaftliche Zuzahlung kann in einigen Fällen deutlich höher als der Festbetrag ausfallen, wobei es den abgebenden Betrieben obliegt, diese mit den Patienten zu verhandeln.
Wie kann es Herstellern unter solchen Marktkonfigurationen gelingen, einen stabilen Endverbraucherpreis oder gar eine Unverbindliche Preisempfehlung durchzusetzen? Wie kann Einfluss auf die verschiedenen Stufen des Distributionskanals genommen werden? Im anschließenden Erfahrungsaustausch sollen Möglichkeiten zum Transfer in andere Branchen identifiziert werden.

08.11.2018, 18:45 – 20:30 Uhr
Technische Hochschule Nürnberg
Kesslerplatz 12, Raum KA.440a
Informationen unter:
mohr@mohrfriendscoaching.de


Foto: Fotolia, Urheber: xiaoliang

VDI Fotowettbewerb 2018

Wählen Sie Ihren Favoriten!

Auch dieses Jahr wurde unser Fotowettbewerb wieder gut angenommen und wir hatten zahlreiche Einsendungen zum Thema „Technische Details und Miniaturen".
Nun gilt es, den Sieger zu küren. Bitte wählen Sie Ihren Favoriten aus der Bildergalerie aus, die Sie auf der Webseite des BV München unter: www.verein-der-ingenieure.de finden.
Wir freuen uns auf Ihr Votum!
Stimmabgabe bis: 1. Dezember 2018

VDI-BG Regensburg

Große Ehre für Horst Kohl

Dipl.-Ing. (FH) Horst Kohl, stellvertretender Bezirksgruppenleiter der Bezirksgruppe Regensburg, wurde am 10.09.2018 das Ehrenzeichen des Bayerischen Ministerpräsidenten für langjähriges ehrenamtliches Engagement verliehen.
In ihrer Laudatio bot Bürgermeisterin Gertrud Maltz-Schwarzfischer einen Überblick über Herrn Kohls mannigfaltige Tätigkeiten – nicht nur im VDI. Diesem trat Horst Kohl bereits 1957 bei, 1982 übernahm er die Leitung der BG Regensburg.
Ein großes Anliegen war ihm stets, Schüler für Naturwissenschaften zu begeistern. Er gründete vor 19 Jahren ein Forum für Jugendliche, bei dem Teams verschiedener Schultypen im Rahmen eines Wettbewerbs zu einem naturwissenschaftlichen oder technischen Thema einen Vortrag erarbeiten und einer Jury vorstellen. Seine Interessen sind vielfältig, denn viele Jahre lang organisierte er auch den Ball des VDI Regensburg.
Wir gratulieren Hern Kohl zu dieser ehrenvollen Auszeichung.

VDI Bayern Nordost


Foto: Nidermayer

Bürgermeisterin Gertrud Maltz-Schwarzfischer bei der Übergabe des Ehrenzeichens des Bayerischen Ministerpräsidenten an Horst Kohl

VDI-AK FiB Bayern Nordost

Machen Sie mit!

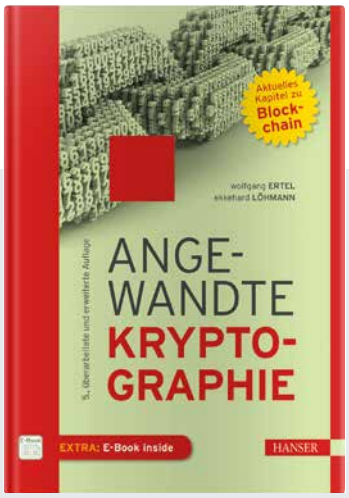
Der Arbeitskreis Frauen im Ingenieurberuf BV Bayern Nordost trifft sich an jedem 17. des Monats zum Stammtisch.
Wir planen folgende Events und möchten damit Ingenieurinnen, bzw. Frauen in technischen Berufen ansprechen, mit uns aktiv zu sein:

SEMINARE/WORKSHOPS
- „She Boss" mit Marion Knaths „Lebenslauf in der Hosentasche"

EXKURSIONEN
- Arbeitgeber in der Region
- „Kunst und Eisen" im Fembohaus
- Fürther Kirchweih

EVENTS IN DIESEM JAHR, DIE WIR GESTALTET HABEN:
- Pavillon auf der VDI Technikmeile
- 18.10. VDI Recruitingtag

VDI FIB Women are actING!
Kontakt: actING-Women@web.de



Angewandte Kryptographie
Wolfgang Ertel
Ekkehard Löhmann
Hanser, München 2018,
ISBN 978-3-446-45468-2
32,00 Euro

Wenn man auch nur etwas tiefer unter die Oberfläche der kryptologischen Algorithmen blicken will, kommt man um die Arithmetik auf endlichen Mengen wie modulares Rechnen, Ringe, Körper u.ä. nicht herum.
Den meisten Ingenieuren ist dieses Teilgebiet der Mathematik nicht geläufig, aber der Einstieg gelingt in kurzer Zeit mit Hilfe des Anhangs im Buch der beiden Autoren. Voraussetzung ist lediglich etwas Schulmathematik. Entstanden aus einem Vorlesungsskript an der Hochschule Ravensburg-Weingarten bietet dieses Lehrbuch aber auch ohne mathematischen Bezug einen guten Einstieg in die wichtigsten kryptologischen Themen, von den klassischen und modernen Blockchiffren und Public-Key-Systemen über Authentifizierung und digitale Signatur zum elektronischen Bargeld.
Ein ganzes Kapitel ist der aktuellen Blockchain Technologie und der Anwendung auf das Zahlungssystem Bitcoin gewidmet. In dem didaktisch hervorragend aufgebauten Buch findet der Leser zunächst einen „Kapitelfahrplan“ vor, der je nach Interessensgebiet zu den relevanten Informationen führt. Jedes Kapitel enthält Übungen, deren Lösungen in einem besonderen Anhang zu finden sind. Ein Schlagwortregister und ein umfangreiches Literaturverzeichnis, das zum einfachen Anklicken auch elektronisch verfügbar ist, runden das Buch ab. Darüber hinaus stellt die Printausgabe einen Code zum Download als E-Book bereit. Zu empfehlen für Studenten der Informatik und für jeden, die sich schnell in die Thematik einarbeiten möchten.

Fritz Münzel

Taumelde Giganten
Gelingt der Autoindustrie die Neuerfindung?
Weert Canzler, Andreas Knie
oekom verlag München,
2018
ISBN 978-3-96238-019-9
13,00 Euro

Die deutsche Autoindustrie hat seit drei Jahren viel Vertrauen verloren und keine verlässliche Versprechung abgegeben. Die Diskussion um Fahrverbote wegen des Dieselabgasproblems geht in die nächste Runde.
Die Sozialwissenschafler Weert Canzler und Andreas Knie haben vor 20 Jahren die „Projektgruppe Mobilität“ in Berlin gegründet und bearbeiten Mobilitätsthemen in Staat und Gesellschaft. Das vorliegende Buch ist in sechs Kapitel gegliedert, die vom Streben nach Mobilität, dem Wunsch nach dem eigenen Auto bis zum Kollaps im Berufsverkehr reichen. Die Botschaft ist daher eine schlichte: Die Stadt der Zukunft mit einer hohen Aufenthaltsqualität gibt es nur mit weniger, saubereren und leiseren Autos. Die gigantischen Mengen an Verkehrsgeräten müssen kleiner werden und sie brauchen in Zukunft eine völlig andere Orchestrierung.
Um auch bei der Mobilität der Zukunft eine bedeutsame Rolle zu spielen, müssen sich die Konzerne neu erfinden und das funktioniert nicht ohne Druck. Das Buch zeigt auf, welche Weichen neu zu stellen sind, um die überfällige Verkehrswende einzuleiten.
Alles schon mal gehört, alles aus größerer Perspektive betrachtet. Was mir als Autofan fehlt, sind Namen der Autohersteller wie Autobianchi, Buick, Chevrolet, DAF, FAUN, Glas, Hanomag-Henschel, Kaelble, Lancia, OPEL, Rolls-Royce, Rover, Saab, Trabant, Volvo, Wartburg, Wiesmann und Zündapp.
Viele haben wegen wirtschaftlicher Probleme den Fortbestand nicht geschafft.

Harold Plesch

Foto: Ulrike Myrzik / Architekturmuseum der TU München

Georg Dollmann baute für König Ludwig II. zwischen 1869 und 1872 das Königshaus auf dem Schachen

Königsschlösser und Fabriken – Ludwig II. und die Architektur

Architekturmuseum der TU München

Die anlässlich des 150-jährigen Jubiläums der TU München geplante Ausstellung beleuchtet das Architekturgeschehen im Königreich Bayern zur Zeit Ludwigs II. (reg. 1864-1886).

In der Ausstellung soll erstmals eine Gesamtschau der unter seiner Ägide errichteten Bauten und nicht realisierten Projekte präsentiert werden.
Im Fokus stehen daher nicht nur die weltberühmten Königsschlösser und die spektakulären Theaterprojekte, die im direkten Auftrag Ludwigs II. entstanden, sondern auch die öffentliche und private Bautätigkeit seiner Zeit. Dazu zählen so prominente Gebäude wie das Münchner Rathaus, die Münchner Akademie der Bildenden Künste oder das Bayreuther Festspielhaus, aber auch weniger bekannte, jedoch architektur- und kulturgeschichtlich herausragende Bauwerke wie zum Beispiel der Ursprungsbau der »Neuen Polytechnischen Schule« in München, die Synagogen in München und Nürnberg, die Fabrikbauten des Augsburger Textilviertels oder die ephemeren Architekturen für die 1882 in Nürnberg veranstaltete „Bayerische Landes-, Industrie-, Gewerbe-, und Kunstausstellung“.
Für einen tieferen Einstieg gibt es Kuratorenführungen „Aus erster Hand“ und Kanalführungen.

Weitere Informationen

Bis 13. Januar 2019
Pinakothek der Moderne
Architekturmuseum der TU München
Barer Straße 40
80799 München
https://www.pinakothek.de/besuch/pinakothek-der-moderne

TECHNIK IN BAYERN

Impressum

Herausgeber:
Verein Deutscher Ingenieure (VDI),
Bezirksverein München, Obb. u. Ndb. e.V.
Anschrift der Redaktion:
„Technik in Bayern“, Westendstr. 199 (TÜV)
80686 München

Chefredakteur: Dipl.-Ing. Friedrich Münzel (verantw.)
Tel. (0 89) 57 91 22 00, Fax (0 89) 57 91 21 61

Chefin vom Dienst: Silvia Stettmayer
Tel. (0 89) 57 91 24 56, Fax (0 89) 57 91 21 61
E-Mail: tib@bv-muenchen.vdi.de

Redaktion:
Hermann Auer Ing. (grad.); Dipl.-Ing. Wolfgang Berger; Dr. Frank Dittmann; Christina Kaufmann M.A.; Bernhard Kramer M.Sc.; Dipl.-Ing. Jochen Lösch, Dipl.-Phys. Susanne Moses; Dipl.-Ing. Harold Plesch

Verlag:
MuP Verlag GmbH
Nymphenburger Str. 20b, 80335 München
Tel. (089) 1 39 28 42-0, Fax: (089) 1 39 28 42-28
Geschäftsführer: Christoph Mattes

Anzeigenleitung: Christoph Mattes
Tel. (089) 1 39 28 42-20, Fax: (089) 1 39 28 42-28
E-Mail: christoph.mattes@mup-verlag.de

Anzeigenverkauf: Regine Urban-Falkowski
Tel. (0 89) 1 39 28 42-31, Fax: (0 89) 1 39 28 42-28
E-Mail: regine.urban@mup-verlag.de
Es gilt die Anzeigenpreisliste Nr. 21 von 01.01.2018

Vertriebsleitung: Philip Esser
Tel. (0 89) 1 39 28 42-33, Fax: (0 89) 1 39 28 42-28
E-Mail: philip.esser@mup-verlag.de

Layout und Grafik: Ines Fischer

Internet-Service: SpaceNet AG

21. Jahrgang 2018
Technik in Bayern erscheint zweimonatlich.
Der Bezugspreis ist bei VDI- und VDE-Mitgliedern der Bezirksvereine in Bayern sowie dem IDV in der Mitgliedschaft enthalten.

Jahresabonnement 36,– Euro / 72,– SFr; Einzelheft 8,– Euro / 16,– SFr. Jahresabonnement für Studenten gegen Einsendung einer entsprechenden Bestätigung 27,– Euro/ 54,– SFr. Der Euro-Preis beinhaltet die Versandkosten für Deutschland und Österreich, der SFr-Preis die Versandkosten für die Schweiz. Bei Versand in das übrige Ausland werden die Porto-Mehrkosten berechnet. Die Abodauer beträgt ein Jahr. Das Abo verlängert sich um ein weiteres Jahr, wenn es nicht zwei Monate vor Ablauf schriftlich gekündigt wird.

Druck: Mayr/Miesbach GmbH
Am Windfeld 15, 83714 Miesbach

Technik in Bayern ISSN1610-6563

Nächster Redaktionsschluss: 12.11.2018

CARTOON

Cartoon: Cornelis Jettke

VORSCHAU

Ausgabe 01/2019 erscheint am 21. Dezember 2018 mit dem Schwerpunktthema

Urbane Produktion und Logistik

Unsere nächste Ausgabe widmen wir dem VDI-Jahresthema 2018. Die VDI Fachgesellschaft für Produktion und Logistik GPL plädiert dafür, zukünftig den Fokus verstärkt auf Standortentwicklung und -sicherung von Produktions- und Logistikunternehmen im Ballungsraum zu legen. Wir beleuchten das Thema und betrachten die Realsituation im urbanen Raum.

Foto: Fotolia - Sasint

Schwerpunktthema der Ausgabe 02/2019

Tier-Technik

Schwerpunktthema der Ausgabe 03/2019

Automatisierung

18. MÜNCHNER WISSENSCHAFTSTAGE

Wissen für alle!

Spaß am Entdecken. Eintritt frei. www.muenchner-wissenschaftstage.de

arbeits-welten

10.–13. November 2018

Mit speziellem Programm für Schüler und Kinder

In der Alten Kongresshalle und im Verkehrszentrum des Deutschen Museums auf der Theresienhöhe u. a.

Gefördert durch:

Bayerische Staatsregierung

Landeshauptstadt München

Europäisches Patentamt
European Patent Office
Office européen des brevets

Medienpartner:

muenchen.de
Das offizielle Stadtportal

Büchner Hochschule