

## Kryptographie Prinzipien und Anwendungen



### Rätsel = *Enigma*

Wie heißt der 14-jährige Komponist der Eingangsmusik (gespielt vom *Enigma Ensemble*)?

Wie lange läuft eine 3.2GHz-CPU, um alle Zustände eines 64 bit Registers zu durchlaufen?

Dr. Jörg Walter



## Geheimnisse

- ...sind eine Form der **Macht**
  - Macht, sie zu wahren
  - Macht, sie zu erschließen, zu gebrauchen
- ...können ermächtigen, schützen und verletzen
- ...werden aus guten und aus üblen Gründen geschützt und gebrochen
- ∃ große Begehrlichkeiten:
  - Militär, Diplomatie und Geschäftswelt
    - Planungs- und Verhandlungsvorteil durch Wissen z.B. um Strategien, Kostenstruktur, Risiken, Spielräume
  - Industrie F&E
    - Nichtöffentliche Forschung USA: 130 G\$/a
    - Informationen zu stehlen ist oft billiger, als sie selbst zu erzeugen, zu entdecken oder wiederzuentdecken

Dr. Jörg Walter

2

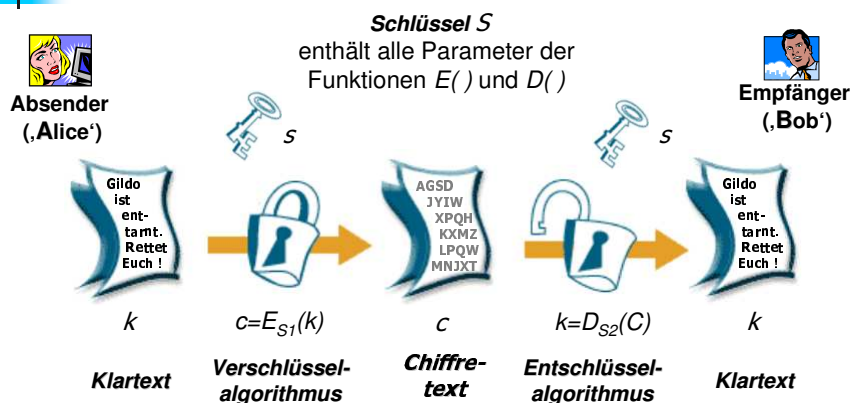
## Gliederung

- Kryptographie
  - Synopsis und Ziele
  - Wichtige Prinzipien und Verfahren
- Bedrohung durch Quantencomputing
- Lösung durch Quantenkryptographie

Dr. Jörg Walter

3

## Verschlüsselte Nachrichtenübermittlung



Dr. Jörg Walter

4

## Kryptographie

- Hauptziel:
  - Vertraulichkeit gewährleisten
    - = Geheimnis, Privatheit bewahren
    - nur autorisierter Zugang
- Weitere Ziele
  - Integrität der Nachricht  $k$ 
    - = keine unbemerkte, unauthorisierte Änderung
  - Authentifizierung = Identifikation von  $A$
  - Nichtleugbarkeit von  $k$  (*Non-repudiation*),
    - z.B. Vertragszustimmung, Bestellung
  - ...
- Kunst gute Codes und Chiffres zu entwickeln
  - „Praktische“ Funktionen  $E()$ ,  $D()$  und
  - Protokolle

Digitale  
Signaturen

Dr. Jörg Walter

5

## Kryptoanalyse

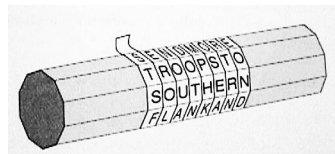
- ...ist die Kunst, die Codes und Chiffres „zu brechen“
- Systematische Attacken gegen das Chiffresystem:
  - Dechiffriere: gesucht  $k$ , gegeben  $c$ ,
    - Eventuell ist  $D()$  bekannt
  - Ermittle Schlüssel  $s$ 
    - Geg.  $\{c\}$  oder  $\{(k,c)\}$ ,
    - Eventuell Kontrolle über  $k$  oder  $c$  (Zugang zu  $E_s, D_s$ )
    - ...
- Attacken gegen das Protokoll
  - *Man-in-the-middle (impersonation)*
  - *Replay*
  - *Dictionary, forward-search*
  - ... *purchase-key (erschleichen, bestechen, erpressen, ...)*

Heute ist das  
Protokoll  
oft die  
Achillesferse

Dr. Jörg Walter

6

## Prinzip Transposition



- Skytale
  - Sparta (5. Jhd BC)

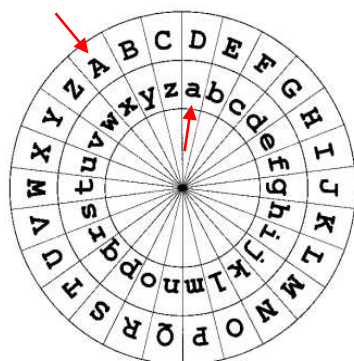
- Gittertransposition

TRANSPOSITION  
 T/A/S/O/I/I/N  
 R/N/P/S/T/O  
 TASOIINRNPSTO

Dr. Jörg Walter

7

## Prinzip Substitution (monoalphabetisch)



- Caesar Verschiebung
  - Rom (60-50 BC)
  - Ersetze jeden Buchstaben durch Nachbarn  $s=3$  Positionen weiter.
  - |Schlüsselraum  $\mathbf{S}$ | = 26
- Allgemeine Substitution
  - $s = (a, b, \dots, z) \in \mathbf{S}$
  - $|\mathbf{S}| = 26! = 4 \cdot 10^{26}$
- Kryptoanalyse
  - Al-Kindis, Bagdad, (8 Jhd.)
  - Statistik der Buchstabenhäufigkeiten



Dr. Jörg Walter

8

## Prinzip Substitution (polyalphabetisch)



- Blaise de **Vigenère** (französischer Diplomat, 1586)
- Zyklischer Tausch von Substitutions-Alphabeten,
  - hier einfache Caesare, gesteuert von einem Geheimwort



- Kryptoanalyse: **Charles Babbage** (London, 1854)
  - Ansatzpunkt: kurzer Schlüssel wird periodisch wiederholt
  - suche Schlüssellänge
  - Häufigkeitsanalyse für Einzelteile



- Enigma (griechisch: Rätsel) **Arthur Scherbius** (Berlin, 1920)
  - elektromechanischer "Rotor" = Substitutions-Alphabet
  - mehrere Rotor kaskadiert
  - komplexe Wechselfolge

- Kryptoanalyse: u.a. **Alan Turing** (Bletchley Park, 1940)

Dr. Jörg Walter

9

## Substitution extrem – Prinzip *One-Time-Pad*

- S.G. **Vernam** (USA, 1926)
  - $|k|=|s|=|c|$  und  $D_s(x) = E_s(x) = x \oplus s$
- **Unbedingt sicher**, wenn
  - **s** perfekt zufällig ist und
  - nur einmal gebraucht wird.

informations-  
theoretisch  
ultimativ sicher !

**k** Klartext: 1 1 1 1 0 1 0 1 1 1 0 0 1 0 1 0 (16 Bit)

Schlüssel: 1 0 1 0 1 1 0 1 0 0 1 0 0 0 1 0 (16 Bit)

bitweise XOR  $\oplus$

Cipher: 0 1 0 1 1 0 0 0 1 1 1 0 1 0 0 0 (16 Bit)

bitweise XOR  $\oplus$

**k** 1 1 1 1 0 1 0 1 1 1 0 0 1 0 1 0

Anwendungen  
Diplomatische Dienste, z.B.  
Kremel – White House

Dr. Jörg Walter

10

## Computer und Kryptoverfahren

- DES: *Data Encryption Standard* (NIST USA, 1977)
  - *Privacy Act 1974* zwingt US-Administration zur Sicherung und Geheimhaltung von Daten und Transaktionen
  - logische Entwicklung in der Reihe von Verschlüsselungsverfahren (symmetrisch)
  - Kombiniert
    - Substitution und Transposition
    - Kaskaden und Runden
  - NEU: Völlige Offenlegung von D(), E(), Sicherheit beruht allein auf Key!
  - $|s|=56$  bit, d.h.  $|S|=2^{56}=72'057'594'037'927'936 = 7 \cdot 10^{16}$
- *DES Challenge III, 1999*
  - 100'000 PCs + „Deep Crack“ brechen DES in 22 Stunden ±

Dr. Jörg Walter

11

## AES: *Advanced Encryption Standard*

- 1997: NIST Auslobung für neuen *Advanced Encryption Standard* (AES)
  - Symmetrischer Block Cipher
  - Effizient in SW + HW
  - Schlüssellänge variabel (128, 192, 256 bit)
  - Öffentlich und frei
- 2000: Gewinner: Rijndael
  - Von Joan Daemen + Vincent Rijmen (Belgien)
  - gegen IBM, RSA, ...
- *Animation auf Nachfrage*



Dr. Jörg Walter

12

## Symmetrische Verfahren: Schlüsselaustauschproblem



- Nur **A** und **B** teilen geheimen Schlüssel **s**
  - ⇒ sichere Kommunikation (**COM**)
  - + sichere Authentisierung (**AUTH**)
- Voraussetzung:
  - zuerst **s**-Austausch durch persönliches Treffen (oder Kurier)
  - Vertrauen in Zuverlässigkeit in Partner B
    - sonst Fälschungen möglich
- Annahme: 1000 Parteien ⇒ jeder 999 Schlüssel, ⇒ insgesamt. 499'500 Schlüssel **und** Treffen

⇒ Hinfällig falls  
Kompromittierung  
von **s**

Trusted-Third-Party Konzept (TTP oder „Big Brother“)  
Probleme: Verfügbarkeit, Sicherheit, Vertrauen

Dr. Jörg Walter

13

## Asymmetrische Verfahren Public-Key Verfahren (PK)

„SuperSafe“  
mit Doppelschloß



**S<sub>E</sub>**  
schließt  
nur

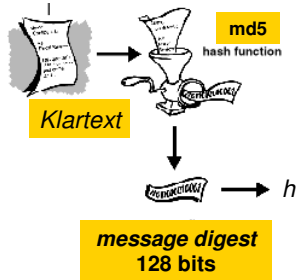
**S<sub>D</sub>**  
öffnet  
nur

- **Public-Private** Verfahren (1)
  - behalte Öffner-Schlüssel **s<sub>D</sub>** (geheim + „privat“)
  - verteile Schließ-Schlüssel **s<sub>E</sub>**
- Ergebnis (1)
  - **COM** sicher
  - **AUTH** unsicher (jeder kann senden)
- Umkehrung: (2): **s<sub>E</sub>** privat, **s<sub>D</sub>** publik
  - **AUTH** sicher
  - **COM** unsicher (jeder kann lesen)
- Kombination: zwei Schlüsselpaare (**s<sub>D1</sub>** **s<sub>E2</sub>** privat)  
Zuerst (2) dann (1);  $c = E(E(k; s_{E2}); s_{E1})$
- Oder packe Prüfcode **h** mit (2) dann (1):
  - $c = E(k + E(h; s_{E2}); s_{E1}) \Rightarrow k + h' = D(k; s_{D1}) \Rightarrow$  **COM**
  - prüfe Code  $h = D(h'; s_{D2}) ? \Rightarrow$  **AUTH**
  - $E(h; s_{E2}) =$  **Digitale Signatur**, wenn  $h = H(k)$

Dr. Jörg Walter

14

## One-Way Hash



„Einwegfunktion“  $h: X \rightarrow Y \in Y$

- $x \rightarrow y$  einfach berechenbar
- $y \rightarrow x$  „praktisch unmöglich“

- Beispiel:  
*message-digest (md5, 128 bit),*  
*secure-hash (sha1, 160bit)*

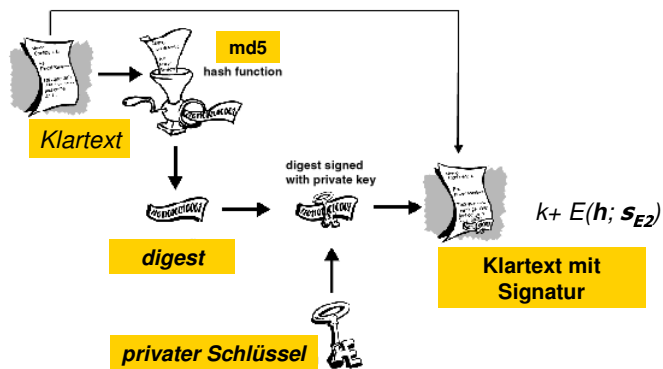
String	md5 (128 bit)
$h("1010")$	1e48c4420b7073bc11916c6c1de226bb
$h("1011")$	7f975a56c761db6506eca0b37ce6ec87

- Jedes y-bit ist von jedem x-bit abhängig

Dr. Jörg Walter

15

## Digitale Signatur mit Digest und PK



Dr. Jörg Walter

16

## Public-Private-Key (2) Beispiel RSA-System

Beispiel:  
 $n = 3233$   
 $e = 17$   
 $d = 2753$

$k = 160$   
 $c = 855$

$k = 855^{2753} \% 3233$   
 $c^d = 5.0 * 10^{8309}$

- Ronald Rivest, Adi Shamir und Leonard Adleman (1977)
- Symmetrieeigenschaft  $D() = E()$ 
  - $c = k^e \pmod n$  d.h.  $S_E = (e, n)$  mit  $c, k < n$
  - $k = c^d \pmod n$  d.h.  $S_D = (d, n)$
  - D.h. Schlüsselpaare können auch für Kommunikation in Gegenrichtung verwendet werden (also im Beisp. 1000 Paare)
- Voraussetzung: (Schlüsselgenerierung)
  - $p, q$  Primzahlen
  - $n = p * q$
  - wähle  $e < n$  so, dass ko-prim mit  $(p-1)(q-1)$
  - finde  $d$  (mit Euklidischem Algorithmus) so, dass  $(ed-1)$  teilbar durch  $(p-1)(q-1)$
- Patentende 2000, gilt heute sicherer de-facto-Standard.
- Sicherheit beruht auf der Schwierigkeit große Zahlen zu faktorisieren (hier  $n$ )

„Young man, in mathematics you don't understand things, you just get used to them.“ - John von Neumann

Dr. Jörg Walter

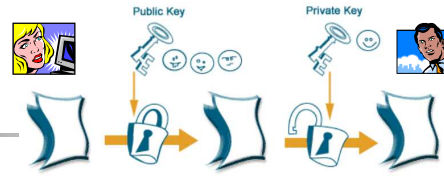
## RSA-129 Challenge (PK 3) Schlüssellänge L=129 bits

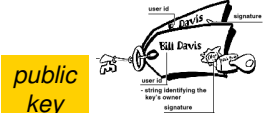
- **Teste in Sekundenbruchteilen:**  
`echo 3490529510847650949147849619903898133417764638493387843990820577 \`  
`* 32769132993266709549961988190834461413177642967992942539798288533 | bc`  
`11438162575788886766923577997614661201021829672124236256256184293570\`  
`6935245733897830597123563958705058989075147599290026879543541`
- Gegenrichtung dauerte **17 Jahren** oder 5000 MIPS-Jahre:  
*100 Quadrillion Calculations Later, Eureka!*  
 Gina Kolata, N.Y. Times, Apr. 27, 1994, Seite A13.
- Herausforderung in Sci. Am., 1977 :  
*Mathematical Games: A New Kind of Cipher That Would Take Millions of Years to Break,*  
 Martin Gardner, Sci. Am.(9) 1977, Seite 120-123.
  - Klartext "The magic words are squeamish ossifrage.."
- Heute: RSA mit  $L \geq 1024$  bits üblich

Dr. Jörg Walter

18

## Public-Key Verfahren (5)





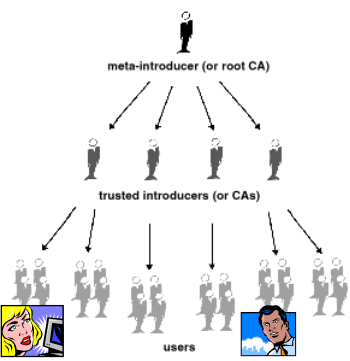
**public key**

- Liefert auch Signaturverfahren
- Löst das Schlüsselverteilungsproblem
  - Schlüsselzahl  $O(N)$  statt  $O(N^2)$

**Kritisch:** *Man-in-the-middle* Attacke bei Übertragung des öffentlichen Schlüssels  $s$

Schlüsselzertifizierung

- Zertifizierungsautorität (CA)
  - prüft Identität und signiert  $s$
  - fungiert als vertrauenswürdiger *introducer*
- Schlüsselmanagement wichtig
  - SSL (z.B. https), PGP, ...




Dr. Jörg Walter
19

## Hybridsysteme

- Schwächen
  - *Public-key* (PK) Verfahren sind relativ langsam
  - *Secrete-key* (SK) Verfahren sind latent empfindlich gegen *chosen-plaintext* Attacken (s. WLAN mit RC4)
- Bau von hybriden Systemen
  - (1) Etabliere symmetrischen *session-key*  $s_s$  mit PK
    - z.B. RSA, ECC
  - (2) Chiffriere Nutzlast effizient mit SK
    - z.B. mit AES, IDEA, 3DES, RC4, RC5, Twofish ...
  - (3) Für Kommunikationskanäle (z.B. ssh, VPN):
    - erneuere  $s_s$  regelmäßig
- Sicherheit von (1) hängt von der **unbewiesenen** Schwierigkeit bestimmter mathematischer Problem ab
  - Komplexitätstheorie  $NP \neq P$ ? (1M\$ Frage [www.claymath.org](http://www.claymath.org))

Dr. Jörg Walter
20




## Quantencomputer

---

Quantencomputer könnten einige dieser Probleme effizienter lösen.

Dr. Jörg Walter 21



## Quantencomputer

---

- Quantencomputer (QC)
  - Rechner der die Eigenschaften von quantenmechanischen Systemen (QS) nutzt.
- QS-Eigenschaft (1): **Superposition**
  - Ein QS kann sich simultan in mehreren Zuständen befinden.
- Konzept:  
Rechenoperationen massiv parallel am selben Ort
- Rechnet mit „qubits“ statt „bits“

Dr. Jörg Walter 22

## QC - Jüngste Entwicklungen

Idee


1981 – R. Feynman "*Simulating Physics With Computers*"  
klassischer Rechner langsam zur Simulation von QM-Systemen

1985 – D. Deutsch (Oxford) "*universal quantum computer*", XOR-Gatter

Äußerst wichtige Anwendung

1994 – **P. Shor** (AT&T Bell Labs, NY) **Algorithmus zur Integer-Faktorisierung in polynomialer Zeit!**

- Faktorisierung durch Reihung +
- Quanten-Fourier-Transformation
- Entzündet sehr viel Interesse



2. allgemeine Anwendung

1996 - Lov **Grover** (Bell Labs) Algorithmus für Entscheidungsprobleme (z.B. Quanten-Datenbank-Suche) statt  $O(N)$  nur  $O(\sqrt{N})$ .

Erste Demos

1998 - (UC Berkeley) Erster 2-qubit NMR Computer

2001 - (IBM's Almaden) 7-qubit NMR Computer

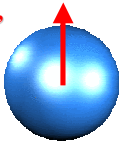
Dr. Jörg Walter 23

## Struktur des Quanten-Computers (QC)

- 1 bit
  - Klassisches Bit wird z.B. durch 2 Spannungen dargestellt.
- 1 qubit
  - Quanten-Bit "qubit" ist ein beliebiges System mit 2 Grundzuständen:  $|0\rangle$  und  $|1\rangle$
  - z.B. Photon oder Teilchen mit Spin (Atomkern, Elektron)

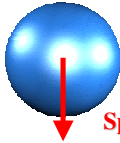
Grundzustand  $|0\rangle$

Spin Up "0"

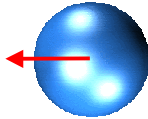


Grundzustand  $|1\rangle$

Spin Down "1"



Superposition  $\alpha |0\rangle + \beta |1\rangle$



$\alpha$  und  $\beta$  komplexe Zahlen

Dr. Jörg Walter 24

## QS-Eigenschaften 3-qubit Register in Superposition

- 3-bit Register kann 8 Zahlen codieren und erhält zu jeder Zeit genau eine (z.B. "101")
- 3-qubit Register ist eine **Superposition** von 8 simultanen Zuständen. Die Mischung wird durch 8 komplexe Amplituden  $\alpha_j$  beschrieben. Z.B.:

Zustand	Amplitude $\alpha$	Wahrscheinlichkeit $ \alpha ^2$
000	$0.37 + i 0.04$	0.14
001	$0.11 + i 0.18$	0.04
010	$0.09 + i 0.31$	0.10
011	$0.30 + i 0.30$	0.18
100	$0.35 + i 0.43$	0.31
101	$0.40 + i 0.01$	0.16
110	$0.09 + i 0.12$	0.02
111	$0.15 + i 0.16$	0.05

**|000> wird mit Wahrscheinlichkeit p=14% gemessen.**

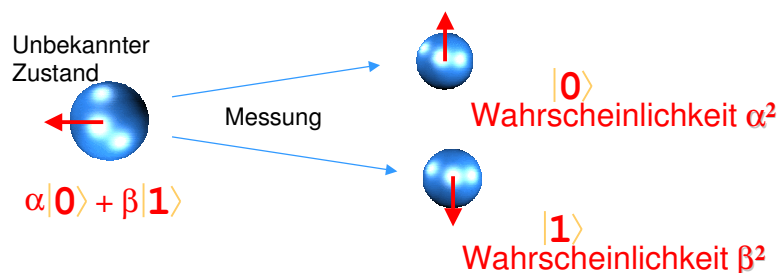
- Messergebnisse sind probabilistisch
- Ein  $n$ -qubit Register kann **simultan  $2^n$**  Zustände repräsentieren
  - massiv parallele Operationen möglich

Dr. Jörg Walter

25

## QS-Eigenschaften Messung und Nicht-Klonierbarkeit

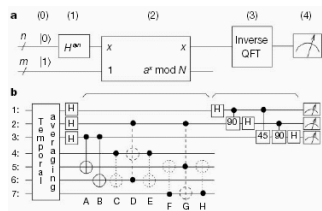
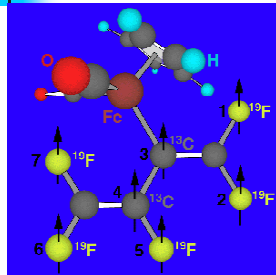
- QS-Eigenschaft (2): **Messung ergibt reinen Zustand und stört**
  - Durch Messung des QS ergibt sich genau ein Zustand.
  - Dabei wird das System unvermeidbar gestört. (Heisenbergsche Unschärferelation)
- QS-Eigenschaft (3): **Nicht-Klonierbarkeit:**
  - Es ist unmöglich eine perfekte Kopie eines unbekanntens Zustands zu erzeugen.



Dr. Jörg Walter

26

## Realisation von Shor's Algorithmus



Vandersypen et al., Nature(414) 2001

- (IBM Almaden, 2001)  
7-qubits Quanten-Computer
  - $10^{18}$  Spezialmoleküle (Perfluorobutadienyl-Eisen-Komplex,  $5 \cdot \text{Fluor} + 2 \cdot \text{C}^{13}$ )
- Präparation und Messung der 7 qubits mit NMR-Pulssequenzen
- Nach 4 Stunden Rechnen
  - $15 = 3 \cdot 5$

Dr. Jörg Walter

27

## Praktikabler Quantencomputer?

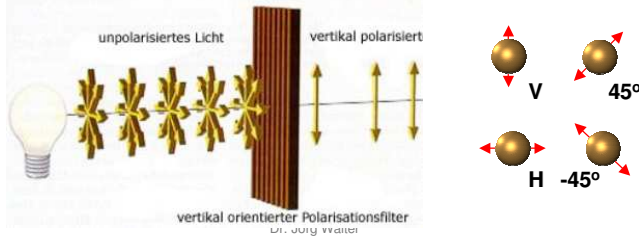
- Kriterien (David DiVincenzo)
  - Skalierbarkeit (Zahl der qubits)
  - Initialisierbarkeit
  - Auslesbarkeit
  - Universaler Satz von Q-Gattern
  - Q-Gatter schneller als Dekohärenz
- Faktorisierung von L-bit Integer benötigt
  - $2L+3$  qubits
  - $+ 16L^3$  Hadamard  $+ 8L^2$  NOT  $+ 8N^3$  C-NOT  $+ 4L^3$  phaseshift  $+ 8L^4$  C-phaseshift
- RSA sicher, solange Schlüssel lang genug
  - $L=1024$  unsicher, sobald 2051-qubits-QC realisierbar
  - Heute unklar, aber das Rennen läuft

Dr. Jörg Walter

28

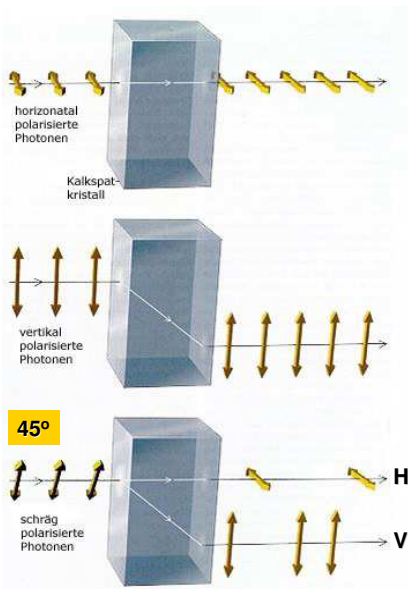
## Quantenkryptographie, oder besser *Quantum Key Distribution (QKD)*

- Durch QC und Shor's Algorithmus könnten alle heute gängigen Kryptosystem bedroht werden!
- Abhilfe: auch durch Quantenmechanik!
- Verteilung eines Zufallsschlüssels (random-bits) mittels polarisierten Photonen
  - Alice braucht Einzelphotonenquelle mit vier möglichen Polarisationsrichtungen



29

## QKD Polarisationstrennung



- Trennung der Polarisierungen mit doppelbrechendem Kristall (hier in HV-Richtung)
- Verdrehte Polarisierungen werden in die beiden Grundzustände der neuen Basis „projiziert“. D.h. 45° Photon wird
  - mit  $p=50\%$  als H Photon und
  - mit  $p=50\%$  als V Photon registriert .

Dr. Jörg Walter

30

## BB84 Protokoll (1)

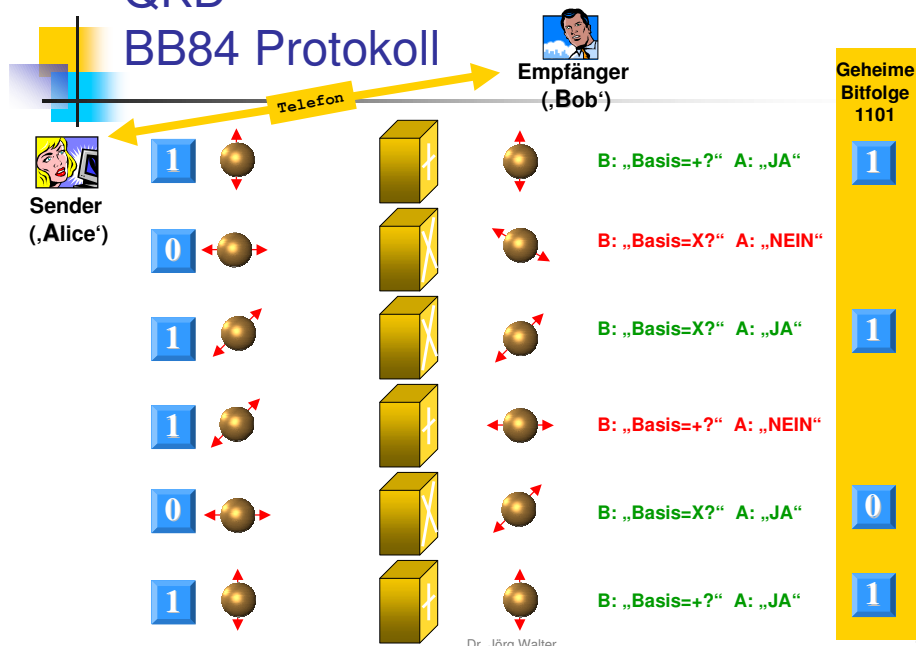
Charles Bennett und Gilles Brassard (1984)

- Phase 1:
  - Bob hat zwei Polarisationsmesseinrichtungen: HV und  $\pm 45^\circ$
  - Kodevereinbarung H,  $-45^\circ=0$  und V,  $45^\circ=1$
- Phase 2:
  - Alice sendet Zufallsfolge von H, V,  $45^\circ$ ,  $-45^\circ$
  - Er misst H/V bzw.  $45^\circ$ / $-45^\circ$ ; wechselt Messbasis in zufälliger Folge

Dr. Jörg Walter

31

## QKD BB84 Protokoll



Dr. Jörg Walter

32

## BB84 Protokoll (2)

Charles Bennett und Gilles Brassard (1984)

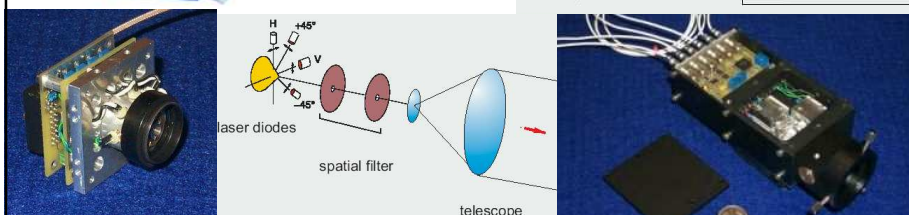
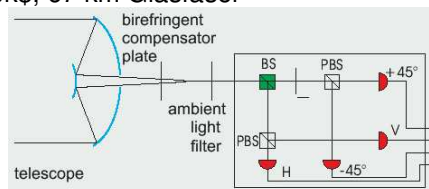
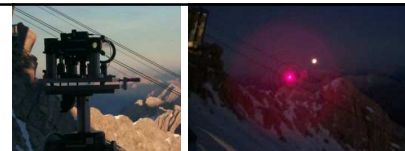
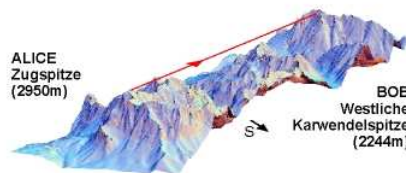
- Phase 3:
  - Öffentlicher Abgleich (Telefon) über die verwendete Basis.
  - Alle in korrekter Basis gemessenen Photonen/bits bilden den neuen Geheimschlüssel.
  - Konversation stellt für andere keinerlei Informationen dar - es sei denn, der Photonen austausch wurde beobachtet.
- Aber Beobachtung stört das QS
  - Klonen des Photons nicht perfekt; genauer:
  - jedes belauschte Photon führt mit  $p=25\%$  zu falschem Bit
- Phase 4:
  - Teste bit-Folge auf Korrektheit („Schlüsselabgleich“)
  - Wiederhole (2-4), falls Fehlerrate zu hoch, b.z.w. nutze Verfahren zur Fehlerkorrektur und *privacy-amplification*

Dr. Jörg Walter

33

## QKD Realisierungen

- 1992 „Experimental QC“ Bennett Brassard (Distanz von 32cm)
- 2002 Kurtsiefer, Weinfurter et.al (LMU) Distanz 23,4 km
  - Minaturisierte Einzelphotonenquelle + passiver Detektor, 1 kbit/s
- 2003 MagiQ.com, Genf, 100k\$, 67 km Glasfaser



34

## Zusammenfassung

- Sehr starke kryptographische Verfahren sind heute leicht verfügbar
  - Hybride Systeme: SK + PK
  - Erfordern Sorgfalt im Umgang
  - Sicherheit durch mathematische Schwierigkeit
- Falls große Quantencomputer möglich, werden die meisten heutigen Krypto-Systeme hinfällig.
- Unbedingt sicher nur
  - *One-time pad*
  - Quanten-Schlüsseletablierungsverfahren QKD
- ...Quantenkryptographie ist bereits verfügbar

Dr. Jörg Walter

35

- Danke für Ihre Aufmerksamkeit!

### Lösung:

Wie heißt der 14-jährige Komponist der Eingangsmusik (gespielt vom *Enigma Ensemble*)?

**Ludwig van Beethoven**

(C-dur Rondo Allegro, Klavierquartette WoO36)

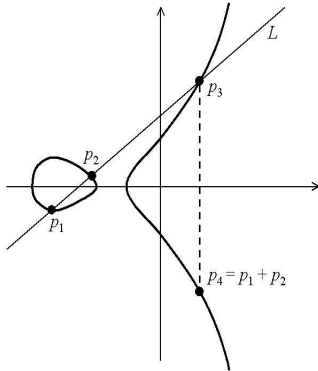
Wie lange läuft eine 3.2GHz-CPU, um alle Zustände eines 64 bit Registers zu durchlaufen?

**182 Jahre** =  $2^{64} / (3.2 \cdot 10^9 \cdot 365 \cdot 24 \cdot 3600)$

Dr. Jörg Walter

36

## Neue *Public-Key* Verfahren (4) Elliptic Curve Cryptosystems (ECC)



Victor Miller (1986) und Neal Koblitz [1987]

- Elliptische Kurven auf abgeschlossenen Feldern  
 $y^2 = x^3 + ax + b$ 
  - Addition:  $P_4 = P_1 + P_2$  (=  $P_3$  gespiegelt)
  - Produkt:  $G = k * P = P + P \dots + P + O$  (Basispunkt +  $k$ -mal)
- Hartes Problem:  $P$  und  $G$ , ges:  $k$ , ( $k=l*j$  ähnlich DH)  
*(elliptic curve discrete logarithm problem)*
- Key kürzer (160 bit ECC ~ 1024 bit RSA)  
 ... da bisher keine *shortcuts* bekannt
- Aber Zweifel, ob langfristig so hart
- Attraktiv für ressourcenbegrenzte Anwendungen  
 (z.B. Smartcards, Handy)
- Standards unterwegs: ANSI X9.62, X9.63

[ecc-faq](#)  
[cryptomathic.Demo](#)

Dr. Jörg Walter

37

## Diffie-Hellman Key-Exchange



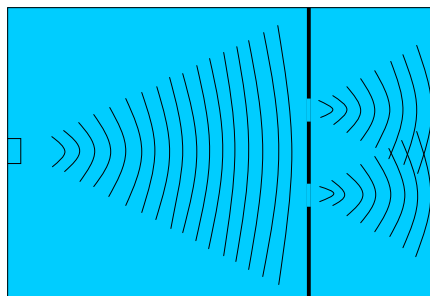
- Alice und Bob wählen  $g$  (ggf. öffentlich)
- Alice wählt random number  $a$ , schickt  $g^a$  an Bob.
- Bob wählt random number  $b$ , schickt  $g^b$  an Alice.
- Alice computes  $(g^b)^a$ .
- Bob computes  $(g^a)^b$ .
- Schlüssel ist  $g^{(ab)}$
- Diffie-Hellman Problem related to discrete logarithms in order to deduce  $a$  from  $g^a$  and  $b$  from  $g^b$ .
- Discrete logarithms are defined in group theory in analogy to ordinary logarithms.

Dr. Jörg Walter

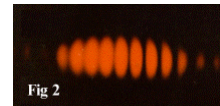
38

## QS Besonderheiten Interferenz

- Doppelspalt-Experiment (Young)
  - Lichtwelle interferiert mit sich selbst und ergibt Beugungsmuster
  - Geht auch bei geringster Intensität (Einzelphotonen)
- Welle-Teilchen-Dualismus



### Resultat

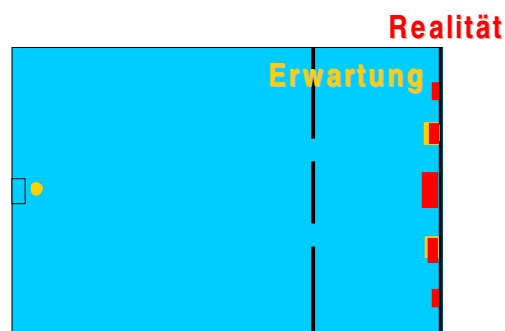


Dr. Jörg Walter

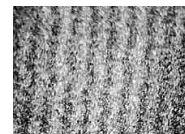
39

## QS Besonderheiten Interferenz mit Elektronen

- Doppelspalt-Experiment mit Elektronen (Young)
  - interferiert wie Lichtwelle mit sich selbst und ergibt Beugungsmuster
- Welle-Teilchen-Dualismus



Resultat: Auch Elektronen  
interferieren miteinander /  
mit sich selbst (!)



Dr. Jörg Walter

40

## QS-Eigenschaften Verschränkte Zustände (*Entanglement*)

- Durch Interaktion können QS **verschränkte Zustände** erreichen, die anders sind, als die Kombination der individuellen Zustände.
- EPR Beispiel:  
Werden zwei verschränkte qubits weit voneinander getrennt, und wird ein qubit gemessen, erreicht das andere instantan einen vorhersagbaren Zustand.
  - (Einstein, Podolsky, Rosen 1935)

Dr. Jörg Walter

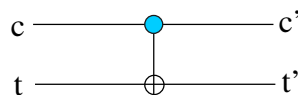
41

## QC Controlled-NOT Gatter

- Q-Gatter müssen **umkehrbar** sein (verlustloses Rechnen)
- Eines der ersten Quantengatter war das **Controlled-NOT**.
  - implementiert XOR-Gatter, aber mit zwei inputs und **zwei** outputs

c	t	c'	t'
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

Das *target*  $t'$ , wird invertiert, wenn *control*  $c = "1"$

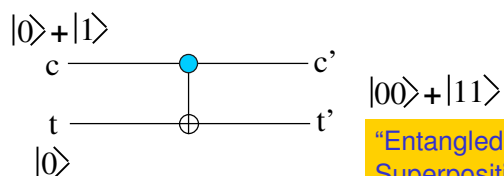


Dr. Jörg Walter

42

## Q-Gatter c-NOT zu Verschränkung

- Angenommen, *control-input*  $c$  ist in einer Superposition, flipped das *target*  $t'$  oder nicht?
- Antwort: beides, d.h.
  - $c'$  und  $t'$  werden verschränkt.



“Entangled state” = eine Superposition von  $c'$  und  $t'$ , dabei sind entweder beide  $|0\rangle$  oder beide  $|1\rangle$

Dr. Jörg Walter

43

## QC Konzepte

- Stephen Bartlett, 2003 NITP Summer School

Implementation	qubit	1 qubit operation	2 qubit operation	Max # of qubits
Ion Trap	Ion	YES	YES	10 – 100
NMR	Atom	YES	YES	10 – 100
Linear optics	Photon	YES	??	??
Superconducting	Josephson junction	YES	2003 ?	$10^6$ ?
Silicon	Atom	2003 ?	2003-2004 ?	$10^9$ ?

Dr. Jörg Walter

44

## Southampton Quantum Technology Centre Facilities



Dr. Jörg Walter

45