

LERNENDE  
MASCHINEN  
02.05.2017

INDUSTRIE  
4.0  
23.05.2017

SPRACH-  
DIALOGUE  
09.05.2017

KÜNSTLICHE  
INTELLIGENZ

**KI**

BIG  
DATA  
13.06.2017

TEAM-  
ROBOTIK  
30.05.2017

AUTONOME  
SYSTEME  
16.05.2017

ALTERS-  
ASSISTENZ

SMART  
SERVICE

**SICHER-  
HEIT**  
**20.06.2017**

EMOTION &  
VERHALTEN

Vorlesungsreihe 2017: Künstliche Intelligenz für den Menschen: Digitalisierung mit Verstand

Mainz, 20. Juni 2017



# Datensouveränität, Privatsphärenschutz und Langzeit-Sicherheit im Zeitalter Künstlicher Intelligenz

Prof. Dr. Dr. h.c.

**Johannes Buchmann**



Technische Universität Darmstadt

Fachbereich Informatik

Hochschulstraße 10

64289 Darmstadt

Herausforderung:  
Langzeitsicherheit

Barack Obama  
30. Januar 2015



*Tonight, I'm launching a new Precision Medicine Initiative to bring us closer to curing diabetes*

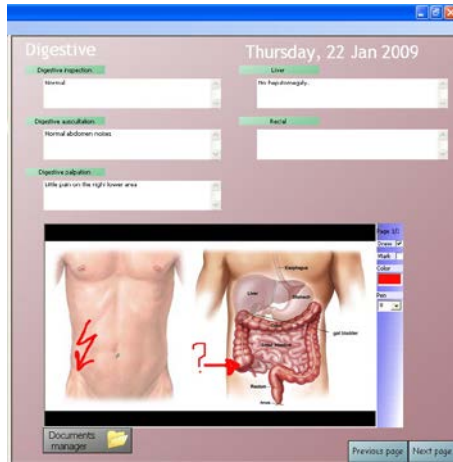
*and to give all of us access to the personalized information we need to keep ourselves and our families healthier.*

**Erfordert Langzeit-Archivierung medizinischer Daten**



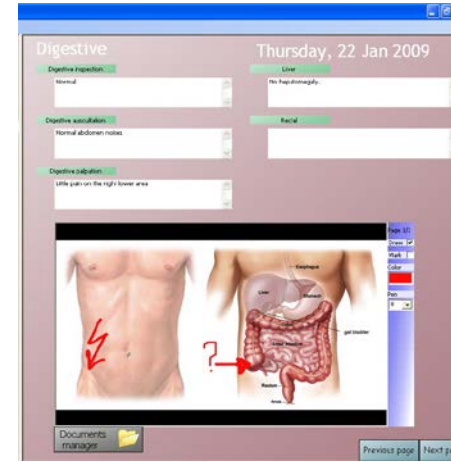
# Schutzziele für langfristig archivierte Daten

# Integrität



$t_0$

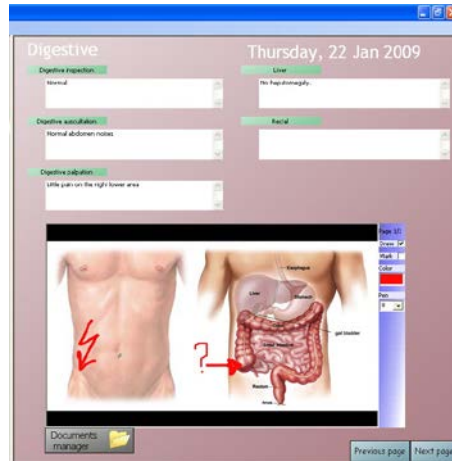
Archivierungszeitpunkt



$t$

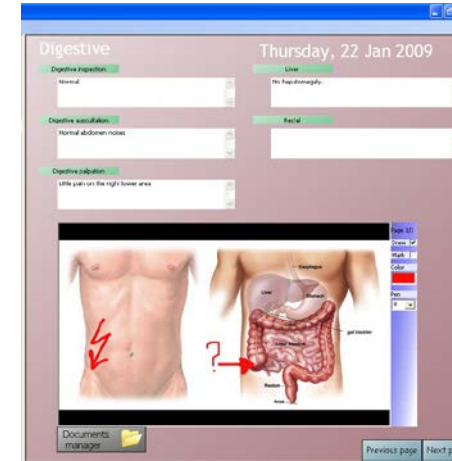
Dokument wurde seit Zeitpunkt  $t_0$  nicht geändert

# Authentizität



$t_0$

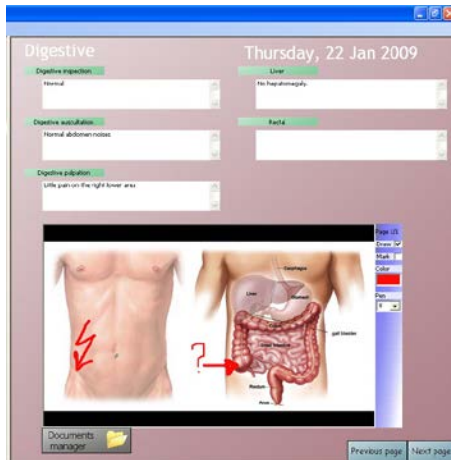
Archivierungszeitpunkt



$t$

Dokument wurde seit Zeitpunkt  
 $t_0$  nicht geändert  
und Herkunft ist verifizierbar

# Vertraulichkeit



Data in transit



Data at rest





Langzeitschutz auch für:

# Genomdatenbanken

NCBI » Genomes & Maps » Homo sapiens

Search  for

**Browse your genome**  
Click on a chromosome to show

Genes

1 2 3 4 5 6 7 8  
9 10 11 12 13 14 15 16  
17 18 19 20 21 22 X Y

**Find A Gene**  
Search for   
from

The NCBI Handbook

**Human Genome Resources**

A challenge facing researchers today is that of piecing together and analyzing the plethora of data currently being generated through the Human Genome Project and scores of smaller projects. NCBI's Web site serves an an integrated, one-stop, genomic information infrastructure for biomedical researchers from around the world so that they may use these data in their research efforts. [More...](#)

**Genes and Human Health**

- ▶ **Gene Database**  
A new database of genes and associated information is now available for searching in Entrez.
- ▶ **OMIM**  
A guide to human genes and inherited disorders maintained by Johns Hopkins University and collaborators.
- ▶ **dbSNP**
- ▶ **dbGaP**

# Steuerdaten

ELSTER. The electronic tax return.

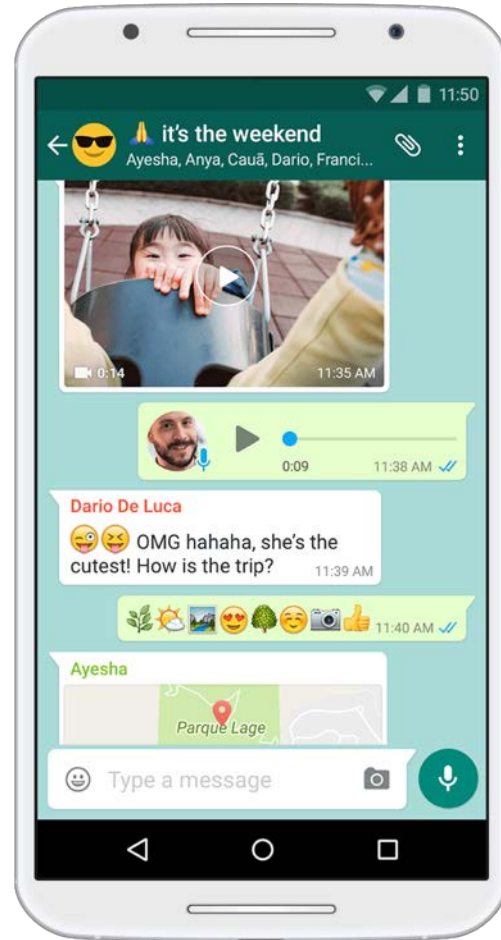
↳ [www.elster.de](http://www.elster.de)



# Hoheitliche Dokumente



# WhatsApp



Wie lange sollen Nachrichten  
vertraulich bleiben?



Loggen Sie sich in Ihr  
Konto ein.

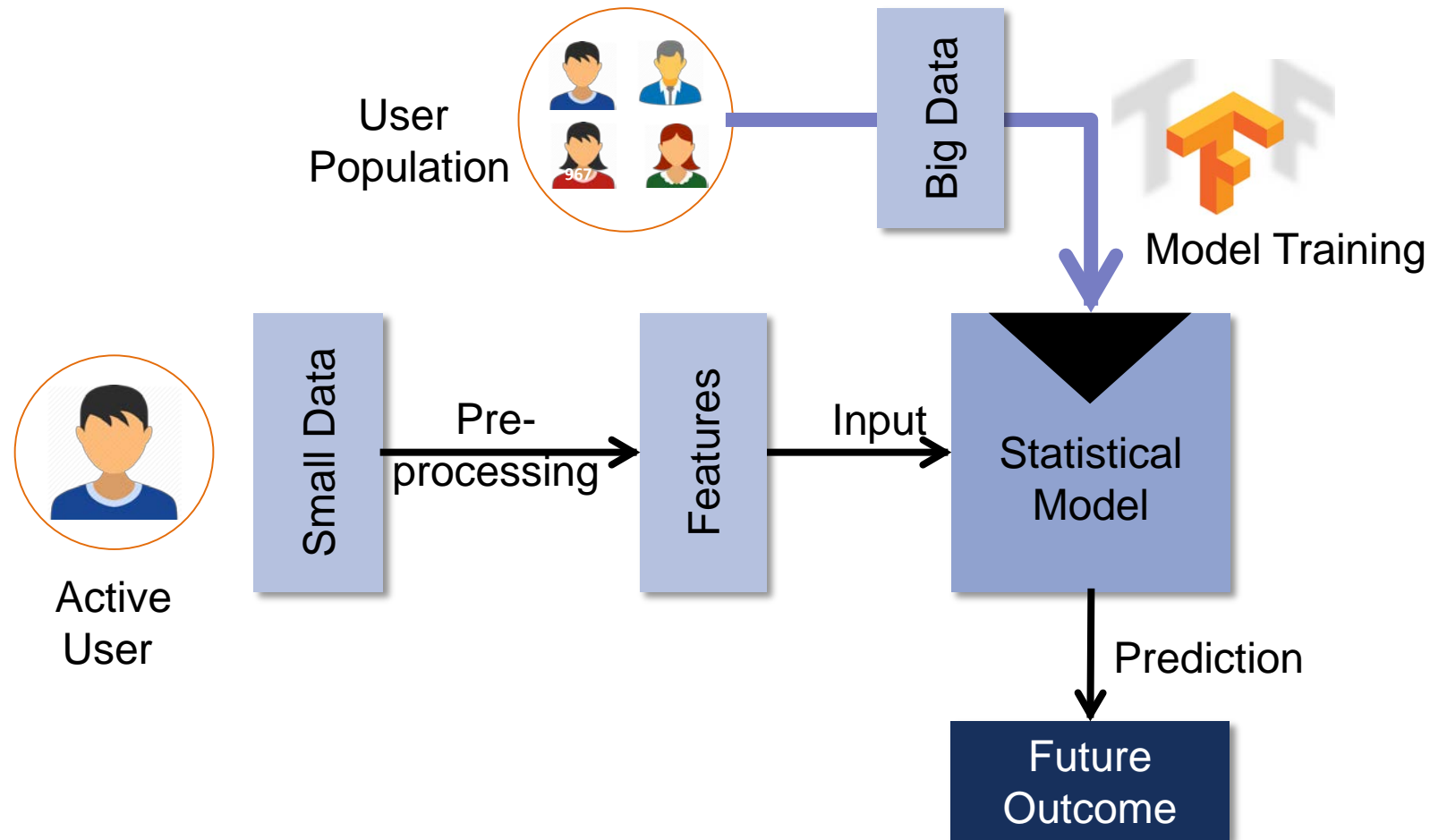
E-Mail-Adresse

Passwort

Einloggen

Wie lange sollen Transaktionen  
vertraulich bleiben?

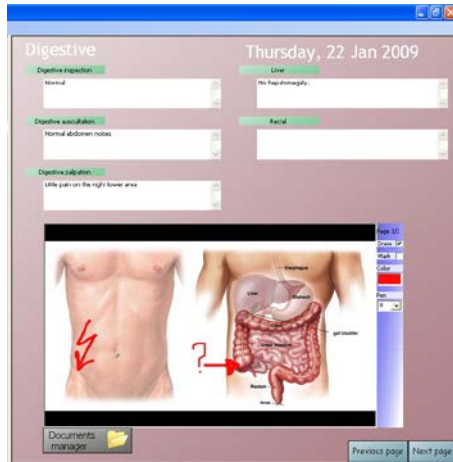
# ... in Anbetracht der künstlichen Intelligenz



# Schutz durch Kryptographie



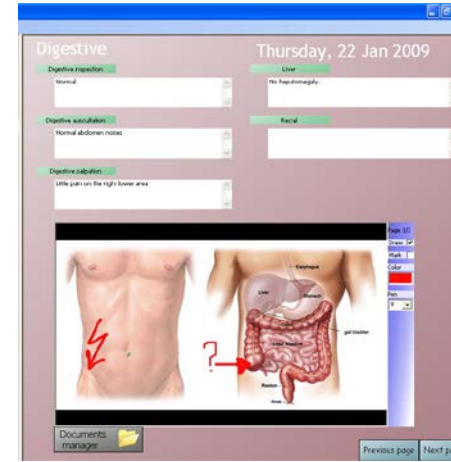
# Integrität und Authentizität



$t_0$

Archivierungszeitpunkt

Elektronische Signatur

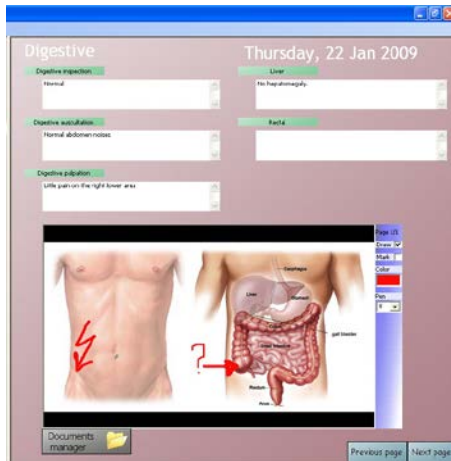


$t$

Beweis: Dokument wurde seit  $t_0$  nicht geändert und Herkunft verifizierbar

Verifikation der elektronischen Signatur

# Vertraulichkeit



Data in transit

Verschlüsselung 



Data at rest

Verschlüsselung 

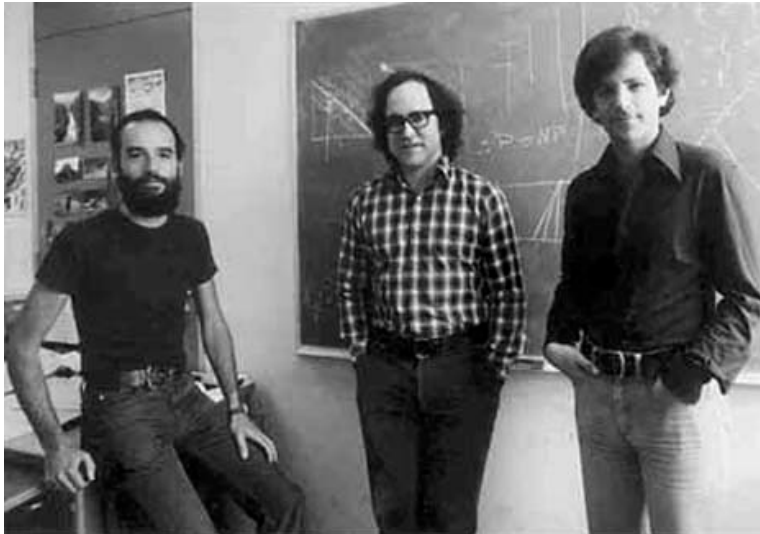
Klassische Kryptographie kann  
keinen langfristigen Schutz  
garantieren



Pierre de Fermat  
1601 - 1665

# A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

R.L. Rivest, A. Shamir, and L. Adleman\*



Turing Award 2002

# RSA-Schlüssel

Öffentlich: Produkt von zwei Primzahlen    Geheim: Primfaktoren

15

= 3 x 5

35

= 5 x 7

109869256229

= 123787 x 887567

# Öffentlicher RSA-Schlüssel von *PayPal*

3179526881036662712547379085979709839119790828652543  
5077364011285905104383826325079684464756664707367650  
3769835004073498912040835036111984436982786965149879  
6736654117936220830386313846453323800787497770622902  
0370398442691648609936395220964249973923183224282326  
2429388312437906163176507342320461004280137879967546  
1282344132598820089096699918817427772240619604850688  
2840651732990015115731765933488273881059259173651847  
3675860071778688184869496311991708023434339343863224  
1104852580095512302299147769809327477605192706038053  
1333826375120534463741477208577693040311951483520936  
6439467587236529469610751231196183098894682104613232  
94360350311459316891189249

1997

Polynomial-Time Algorithms for Prime Factorization  
and Discrete Logarithms on a Quantum Computer\*

Peter W. Shor<sup>†</sup>



www.datacenterdynamics.com/content-tracks/servers-storage/google-may-unveil-a-powerful-quantum-computer-by-end-of-2017/96880.fullarticle 133%

Welcome visitor | Sign in | Register | Magazine | Advertise

# DatacenterDynamics

The Business of Data Centers.

Search the

Home News Webinars Opinion Videos Magazine Content Tracks Events Awards Res

HOME > CONTENT TRACKS > SERVERS + STORAGE

# Google may unveil a powerful quantum computer by end of 2017

2 September 2016 | By **Sebastian Moss**



# Langfristiger Schutz ist möglich

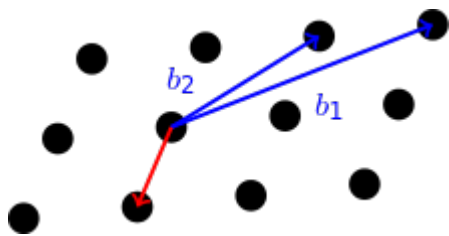
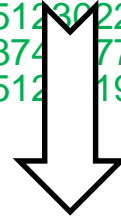


**CROSSING**

<http://www.crossing.tu-darmstadt.de>

# Post-Quantum Cryptography

317952688103666271254737908597970983911979082865254350773  
 640112859051043838263250796844647566647073676503769835004  
 073498912040835036111984436982786965149879673665411793622  
 083038631384645332380078749777062290203703984426916486099  
 363952209642499739231832242823262429388312437906163176507  
 342320461004280137879967546128234413259882008909669991881  
 742777224061960485068828406517329900151157317659334882738  
 810592591736518473675860071778688184869496311991708023434  
 339343863224110485258009551230229914776980932747760519270  
 6038053133382637512053446374772085776930403119514835209  
 3664394675872365294696107512196183098894682104613232943  
 60350311459316891189249

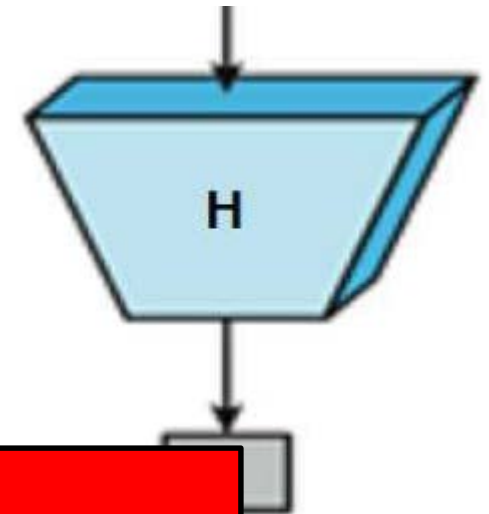
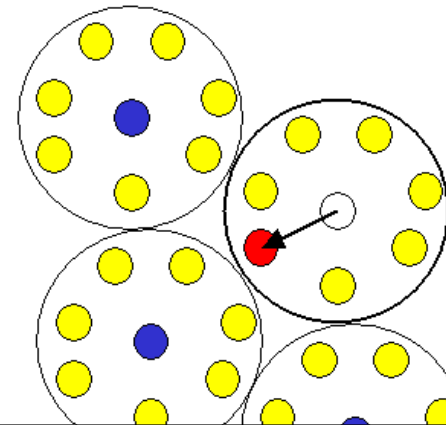


$$\bar{X}_i = \frac{1}{n_i} \sum_{j=1}^{n_i} X_{ij},$$

$$A_i = \sum_{j=1}^{n_i} (X_{ij} - \bar{X}_i)(X_{ij} - \bar{X}_i)',$$

$$S_i = \frac{1}{n_i - 1} A_i,$$

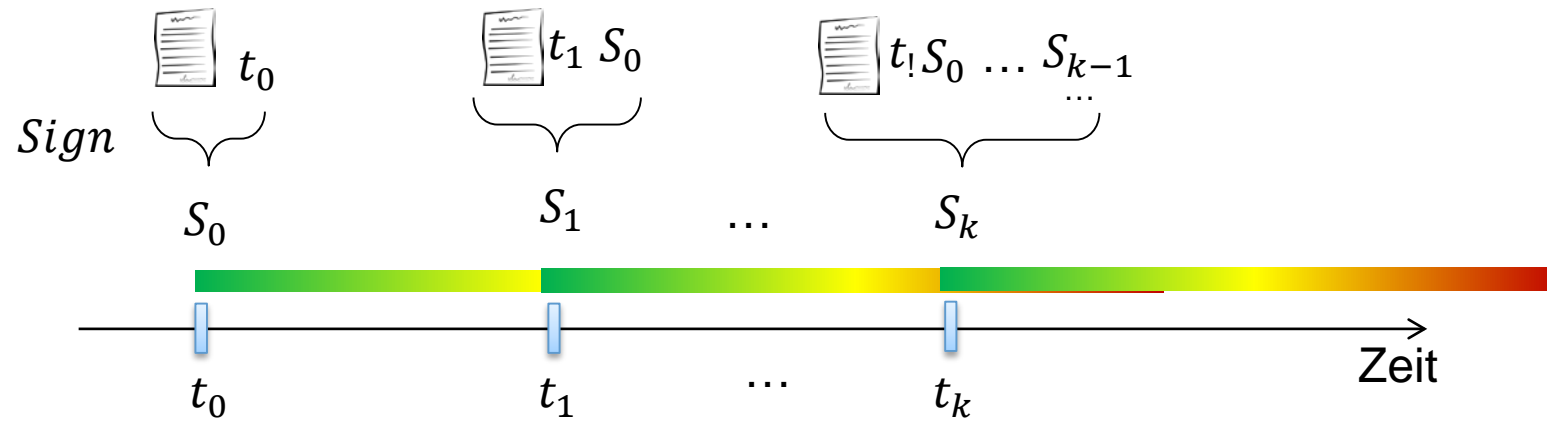
$$\tilde{S}_i = \frac{1}{n_i} S_i,$$



Kein Beweis für Quantencomputerresistenz

# Langzeit-Integrität und Authentizität

# Gültigkeit von Signaturen kann verlängert werden

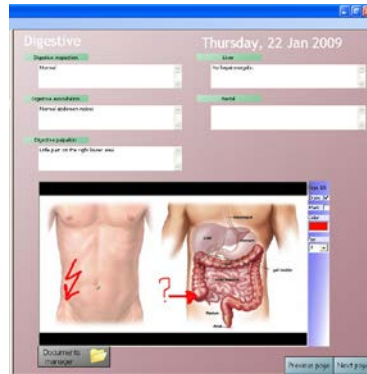


Kann Gültigkeit von  
Verschlüsselung verlängert werden?



# Langzeit-Vertraulichkeit





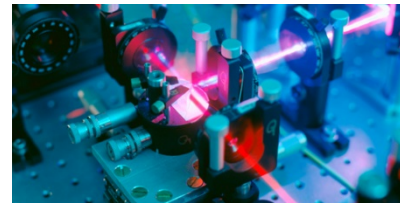
Data in transit



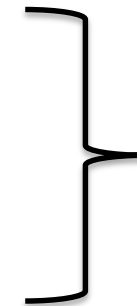
Quanten-Schlüsselaustausch  
[BB84]

+

One-Time-Pad-Verschlüsselung  
[Shannon 48]



```
03003802 996CB7BA 0E00161B 06021C06
BA7CE203 09030200 01086C00 37014D00
18122500 02480002 03030C00 AD222500
18D03C00 887525C1 01A07700 37D14D00
87122500 02480002 03030C00 AD222500
0003C000 887525C1 4F5431 53414241
4F5431 42624348 304045 6460004
16C2F4F 553D45D3 41000000 4F3D9114
425604 00130000 00000000 00000000
003042 4C000000 0248404F 00010000
125442 22400000 88038000 22878000
3ECCA CB3E888F DF038D7F A14217
2A44D 04343875 4F571C83 535C00
7DED9 157C659E CB208E07 FA49F
96DB 7D7F743D 9A36DD29 45480
014D 410800C0 9A54ED72 5A114C
```



Informationstheoretisch  
sichere Vertraulichkeit

# Caesar Chiffre 60 v. Chr.



K	R	A	N	I	C	H

# Caesar Chiffre 60 v. Chr.



K	R	A	N	I	C	H
N						

# Caesar Chiffre 60 v. Chr.



K	R	A	N	I	C	H
N	U					

# Caesar Chiffre 60 v. Chr.



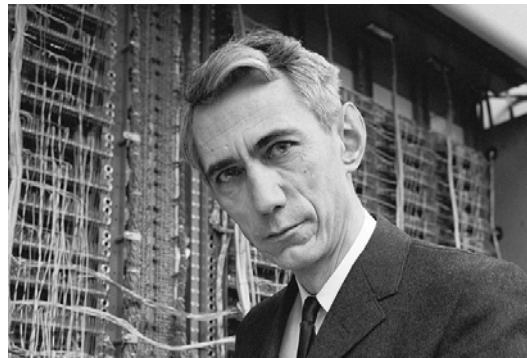
K	R	A	N	I	C	H
N	U	D				

# Caesar Chiffre 60 v. Chr.



K	R	A	N	I	C	H
N	U	D	Q	L	F	K

# Perfekt sichere Verschlüsselung 1948



Claude Shannon (1916 – 2001)

k	r	a	n	i	c	h

Schlüssel wird zufällig gewählt



k	r	a	n	i	c	h
3	13	15	3	21	20	22

Schlüssel wird zufällig gewählt

k	r	a	n	i	c	h
3	13	15	3	21	20	22
N	E	P	Q	D	W	D

Schlüssel wird zufällig gewählt

N	E	P	Q	D	W	D



N	E	P	Q	D	W	D
3	13	15	3	21	20	22



N	E	P	Q	D	W	D
3	13	15	3	21	20	22
k	r	a	n	i	c	h



N	E	P	Q	D	W	D
3	13	15	3	21	20	22
k	r	a	n	i	c	h

N	E	P	Q	D	W	D
12	10	23	24	3	5	0



N	E	P	Q	D	W	D
3	13	15	3	21	20	22
k	r	a	n	i	c	h

N	E	P	Q	D	W	D
12	10	23	24	3	5	0
b	u	s	s	a	r	d



N	E	P	Q	D	W	D
3	13	15	3	21	20	22
k	r	a	n	i	c	h

N	E	P	Q	D	W	D
12	10	23	24	3	5	0
b	u	s	s	a	r	d
24	0	4	8	19	22	16





N	E	P	Q	D	W	D
3	13	15	3	21	20	22
k	r	a	n	i	c	h

N	E	P	Q	D	W	D
12	10	23	24	3	5	0
b	u	s	s	a	r	d
24	0	4	8	19	22	16
p	e	l	i	k	a	n



N	E	P	Q	D	W	D
3	13	15	3	21	20	22
k	r	a	n	i	c	h

N	E	P	Q	D	W	D
12	10	23	24	3	5	0
b	u	s	s	a	r	d
24	0	4	8	19	22	16
p	e	l	i	k	a	n
k	o	l	i	b	r	i



N	E	P	Q	D	W	D
3	13	15	3	21	20	22
k	r	a	n	i	c	h



N	E	P	Q	D	W	D
12	10	23	24	3	5	0
b	u	s	s	a	r	d
24	0	4	8	19	22	16
p	e	l	i	k	a	n
3	16	4	8	2	5	21
k	o	l	i	b	r	i

N	E	P	Q	D	W	D
3	13	15	3	21	20	22
k	r	a	n	i	c	h

Jeder Klartext mit sieben  
Buchstaben ist möglich

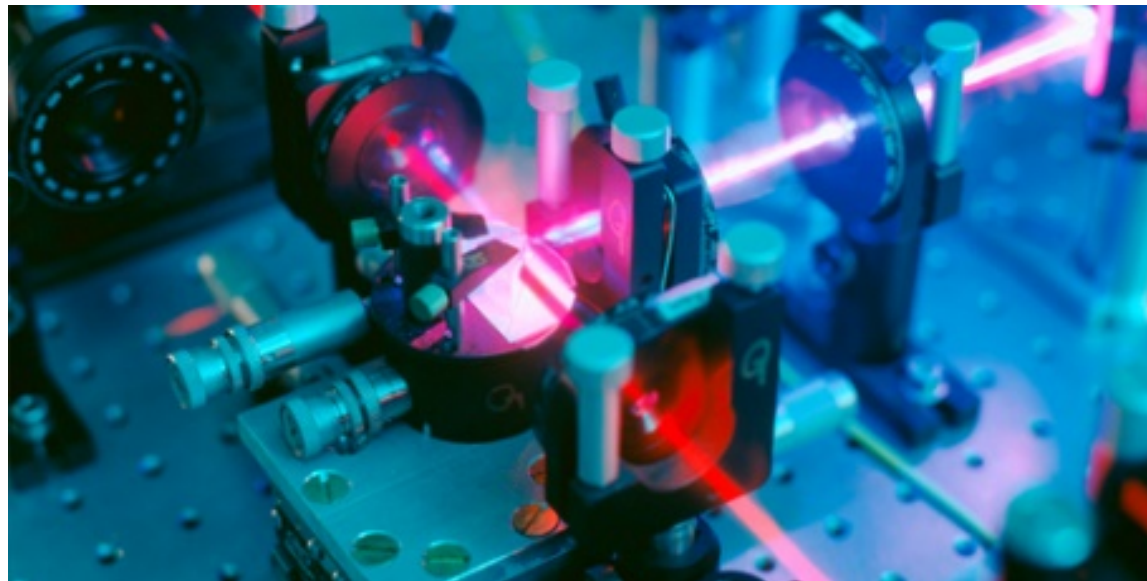
N	E	P	Q	D	W	D
12	10	23	24	3	5	0
b	u	s	s	a	r	d
24	0	4	8	19	22	16
p	e	l	i	k	a	n
3	16	4	8	2	5	21
k	o	l	i	b	r	i

N	E	P	Q	D	W	D
3	13	15	3	21	20	22
k	r	a	n	i	c	h

N	E	P	Q	D	W	D
12	10	23	24	3	5	0
b	u	s	s	a	r	d
24	0	4	8	19	22	16
p	e	l	i	k	a	n
3	16	4	8	2	5	21
k	o	l	i	b	r	i

Theorem von Shannon:  
Der Angreifer lernt nichts  
aus dem Schlüsseltext

# Quantenschlüsselaustausch



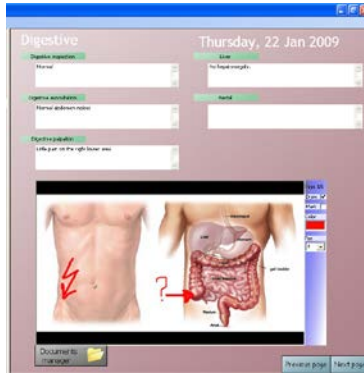


[Startseite](#) / [Nachrichten](#) / EU: Quantentechnologie-Programm mit einem Budget von 1 Mrd. Euro vorgest

## EU: Quantentechnologie-Programm mit einem Budget von 1 Mrd. Euro vorgestellt

**Das Flaggschiff-Projekt soll Anwendungen der Quantenphysik voranbringen – etwa Quantenkommunikationsnetzwerke, hochpräzise Atomuhren, Gravitationssensoren und Quantensimulatoren zur Entwicklung neuer Materialien und Quantencomputer.**

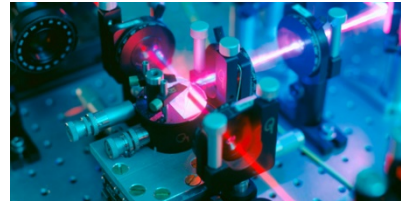




**Quanten-Schlüsselaustausch**  
[BB84]

+

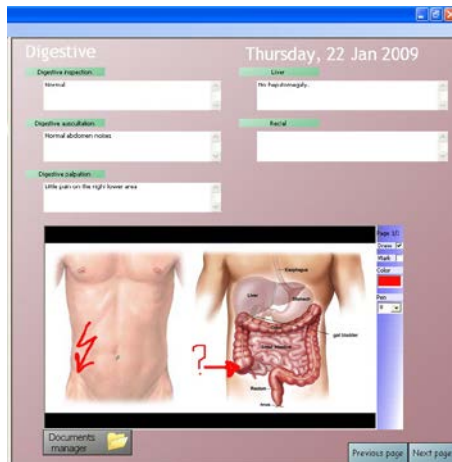
**One-Time-Pad-Verschlüsselung**  
[Shannon 48]



```
03003802 996CB7BA 0E00161B 06021C06
8A7CE203 09030200 01086C00 37014D00
18122500 02480002 03030C00 A0722500
18D03C00 887525C1 01A07700 37D14D00
87122500 02480002 03030C00 A0722500
0003C000 887525C1 4F5A31 53414241
74510001 42624348 304050 64600004
16C2F4F 553D4503 41000000 4F3D9114
825604 00130000 00000000 00000000
003042 4C000000 0248404F 00010000
125402 22400000 88038000 22807000
3ECCA CB3E8888F DF038D7F A14217
2A4E0 04343875 4F571C03 535C00
7DED9 157C659E CB208E07 FA49F
96DB 7D7F743D 9A36DD29 45480
014D 410800C0 9A54ED72 5A114C
```

Informationstheoretisch  
Sichere Vertraulichkeit

# Langzeit-Vertraulichkeit

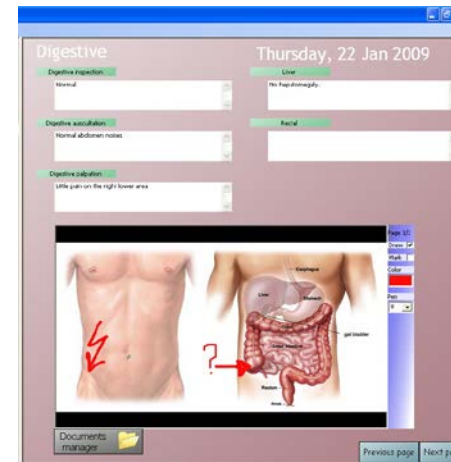


**Data at rest**

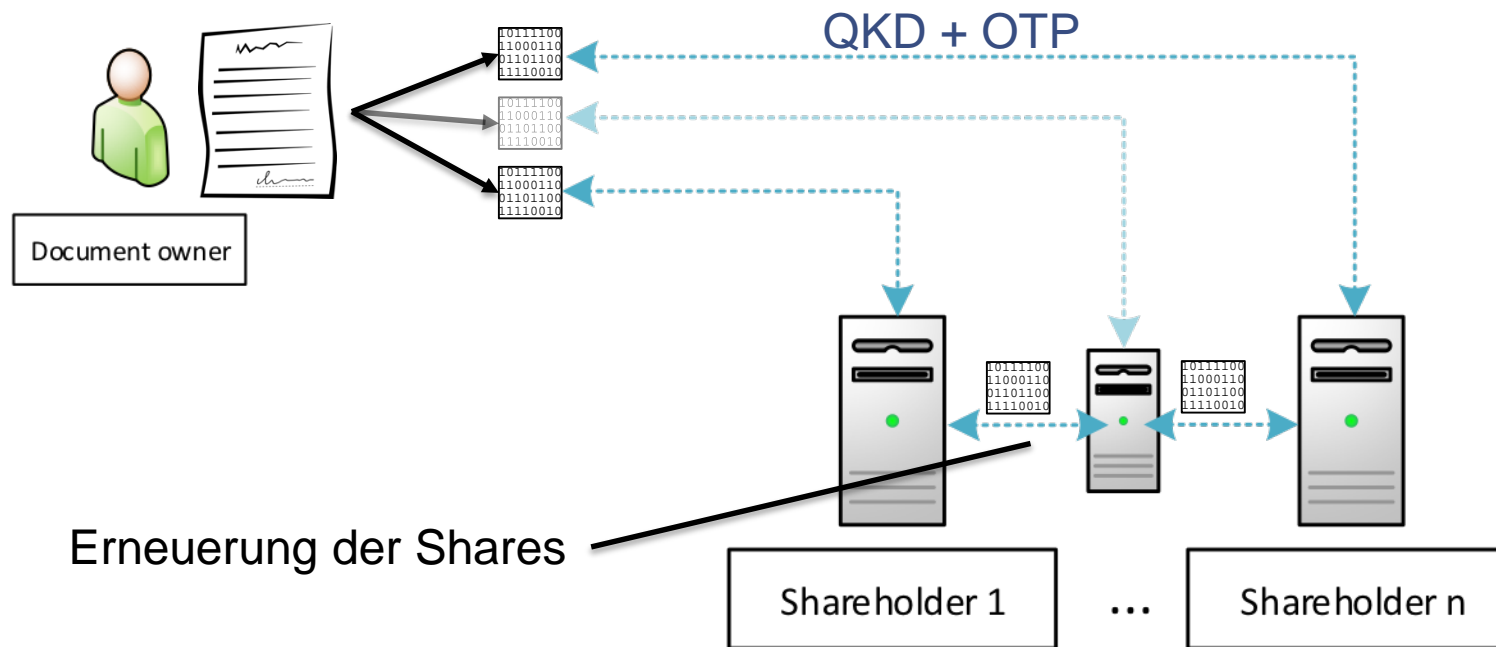
# One-time pad?

```

03003802 996CB7BA 0EG0161B G0021C06
BA7CE203 G0030200 01208600 37D14D00
1B7125G0 024FG002 53D03C00 AD722500
1BD03C00 887525C1 01A07700 37D14D00
B7125G0 024FG002 53D03C00 AD722500
BD03C00 887525C1 4F553F00 53414242
F4F3D41 4242434E 3D4A6000 64692042
16C2F4F 553D4553 4142434E 4F3D414
425604 00312E30 04241001 0003424
003042 4C000000 024E4E4F 00B1D30
1254F1 21000009 8833B0CC 2957EE
3ECAA CB3E88EF DF038D7F A14217
2AA4D 04143B75 4F571C83 535C00
7DED9 B57C659E C820EE07 FA49F
196DB 7D7F743D 9A36DD29 454E0
014D 410800C8 9A54E072 5A14C
  
```

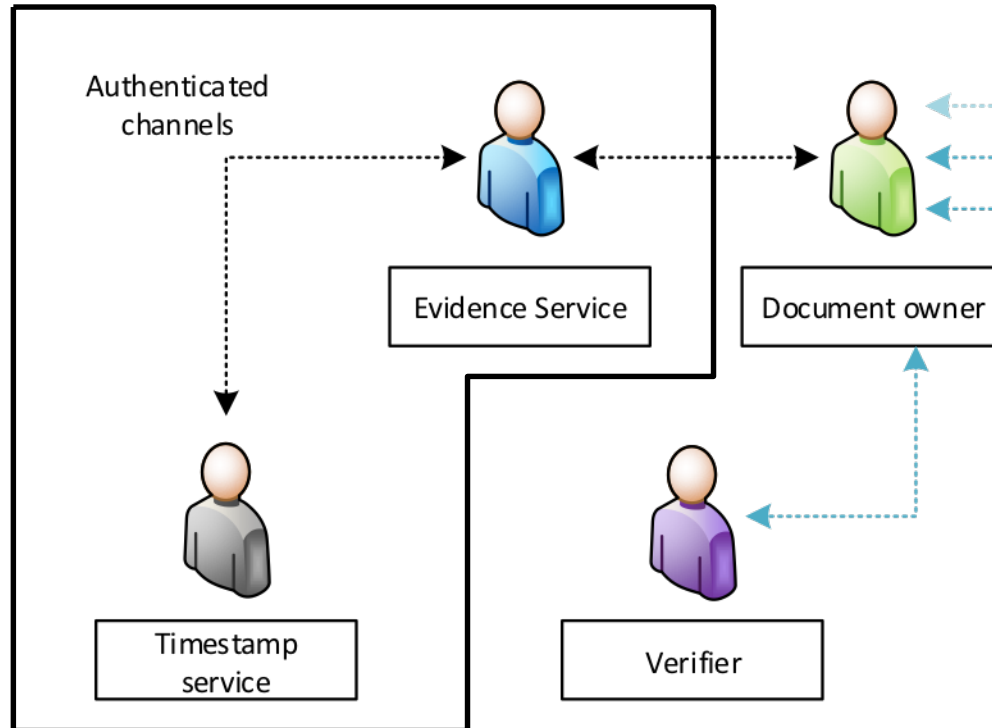


# Proactive Secret Sharing

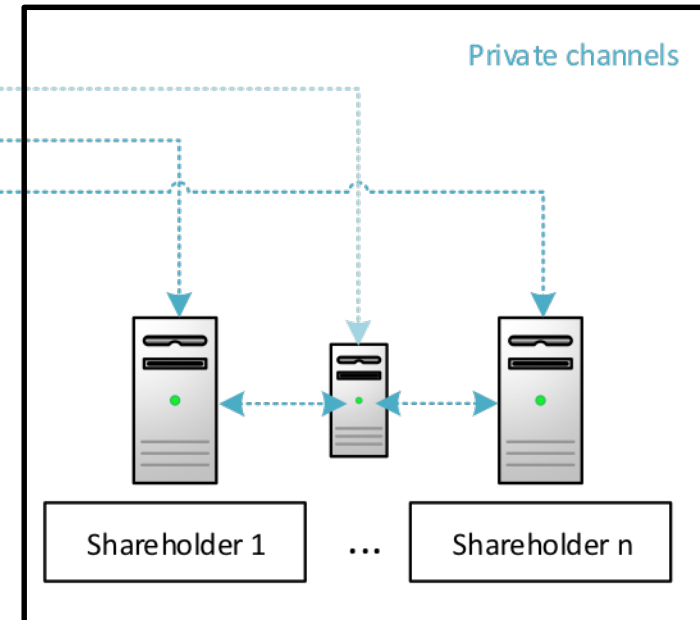


# 2016 LINCOS in Kooperation mit NICT Japan

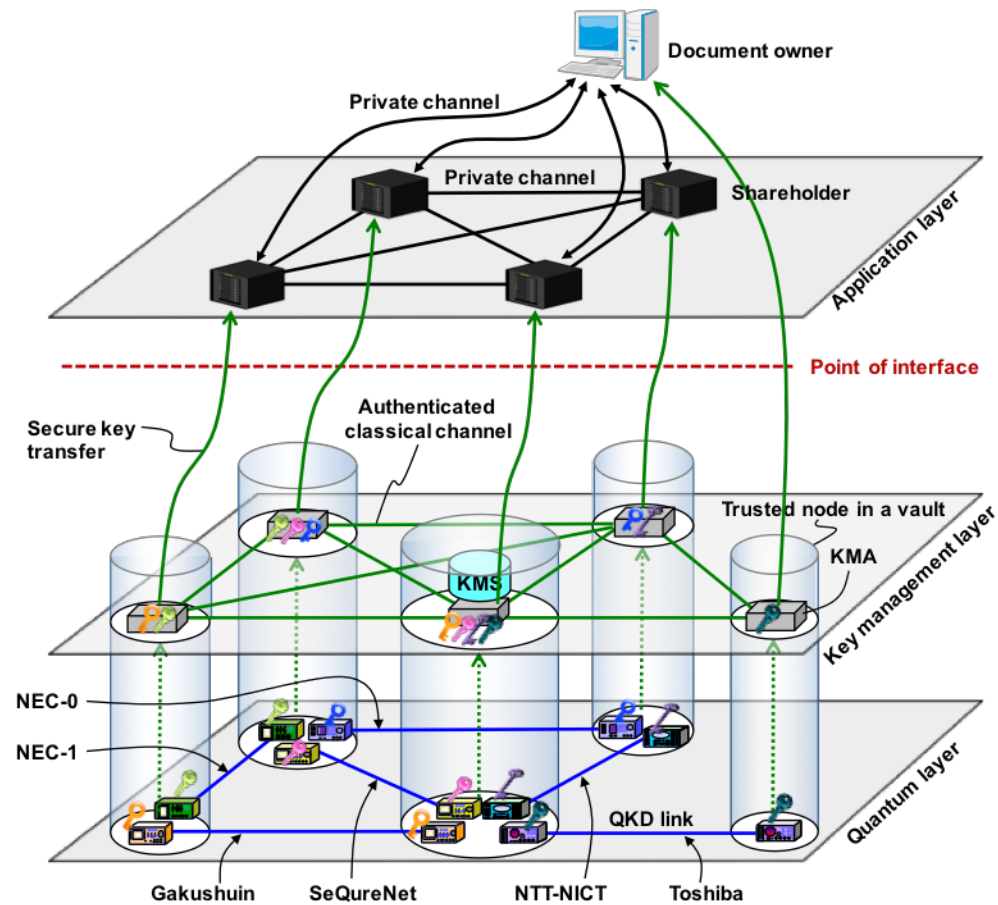
## Integrität



## Vertraulichkeit



## Tokyo QKD Network of NICT



Link	Distanz (km)	Key Rate (kbit/s)
NEC-0	50	200
NEC-1	22	200
Toshiba	45	300
NTT-NICT	90	10
Gakushuin	2	100
SeQureNet	2	10

# Zeit für Quantenschlüsselaustausch

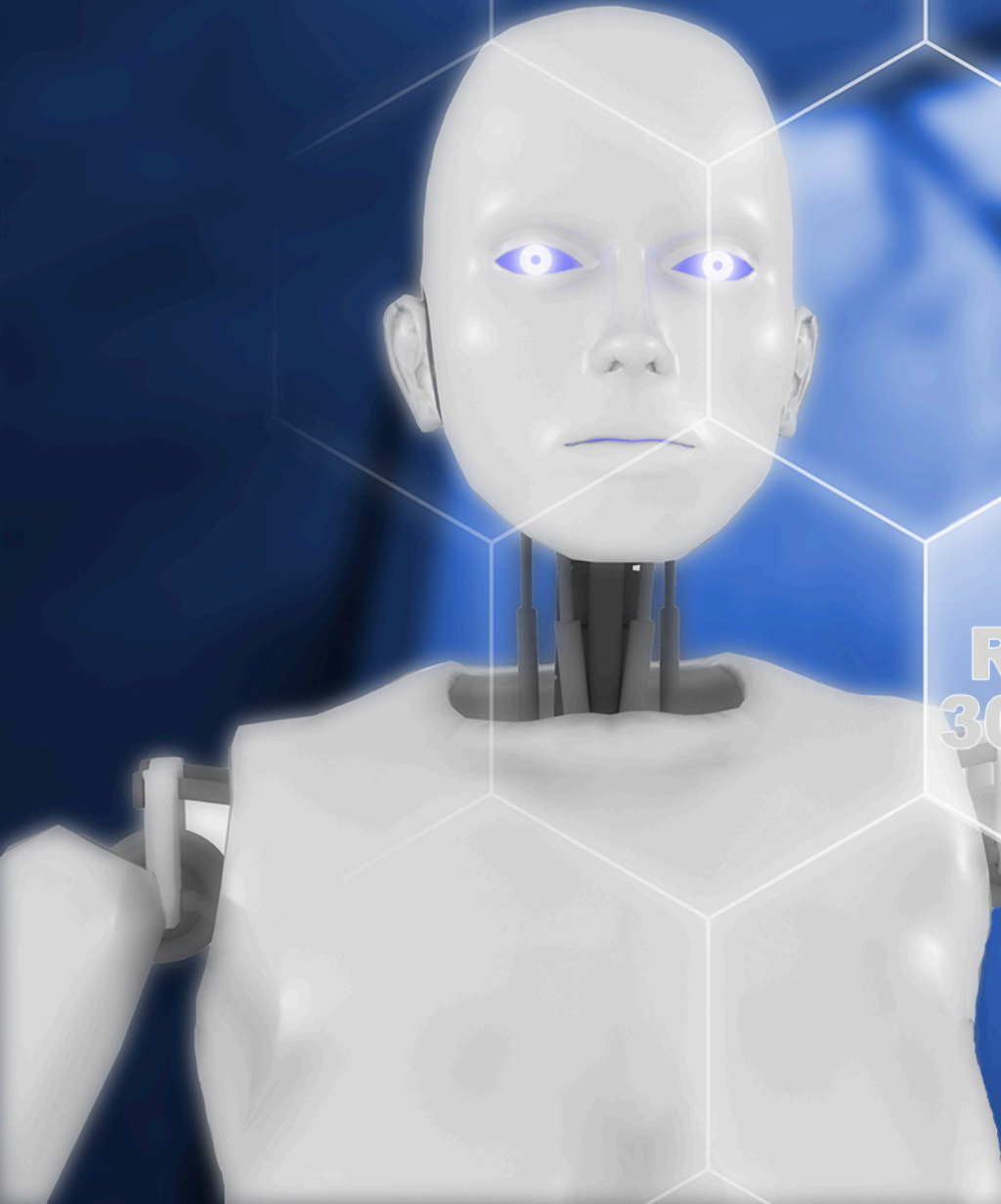
Datenmenge	Zeit
1 KB	0.027 Sekunden
1 MB	4.45 Minuten
1 GB	7.41 Stunden



Fazit:

Langzeitschutz von Integrität und Vertraulichkeit ist nötig und möglich.

Weitere Forschung ist nötig.



LERNENDE  
MASCHINEN  
02.05.2017

INDUSTRIE  
4.0  
23.05.2017

SPRACH-  
DIALOGE  
09.05.2017

KÜNSTLICHE  
INTELLIGENZ

**KI**

BIG  
DATA  
13.06.2017

TEAM-  
ROBOTIK  
30.05.2017

AUTONOME  
SYSTEME  
16.05.2017

**ALTERS-  
ASSISTENZ**

**SMART  
SERVICE  
27.06.2017**

SICHER-  
HEIT  
20.06.2017

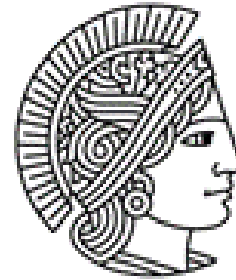
**EMOTION &  
VERHALTEN**

# Vielen Dank für Ihre Aufmerksamkeit

Johannes Gutenberg  
Stiftungsprofessur



Johannes Gutenberg  
Stiftungsprofessur



TECHNISCHE  
UNIVERSITÄT  
DARMSTADT



TECHNISCHE  
UNIVERSITÄT  
DARMSTADT