Asymmetrische Kryptographie

Lorenz Panny

Technische Universität München

Youth Science Club, München, 26. Januar 2024

Dieser Vortrag

Was ist asymmetrische Kryptographie?

Geschichte

Der Diffie–Hellman-Schlüsselaustausch im Detail

Anwendungen

Das Q-Wort

Was ist asymmetrische Kryptographie?

"Klassische" Kryptographie (seit tausenden Jahren):

- Geheime Schlüssel müssen im Vorhinein auf sicherem Weg ausgetauscht werden.

Was ist asymmetrische Kryptographie?

"Klassische" Kryptographie (seit tausenden Jahren):

- Geheime Schlüssel müssen im Vorhinein auf sicherem Weg ausgetauscht werden.
- Alle Teilnehmer haben gleich viele Möglichkeiten.
  Zum Beispiel: Verschlüsseln und Entschlüsseln.

Was ist asymmetrische Kryptographie?

"Klassische" Kryptographie (seit tausenden Jahren):

- Geheime Schlüssel müssen im Vorhinein auf sicherem Weg ausgetauscht werden.
- Alle Teilnehmer haben gleich viele Möglichkeiten.
  Zum Beispiel: Verschlüsseln und Entschlüsseln.
- Also symmetrisch.

Was ist asymmetrische Kryptographie?

"Klassische" Kryptographie (seit tausenden Jahren):

- Geheime Schlüssel müssen im Vorhinein auf sicherem Weg ausgetauscht werden.
- Alle Teilnehmer haben gleich viele Möglichkeiten.
  Zum Beispiel: Verschlüsseln und Entschlüsseln.
- Also symmetrisch.

Asymmetrische Kryptographie *(public-key cryptography)*:

- Schlüssel bestehen (typischerweise) aus Paaren:
  Ein privater Schlüssel und ein öffentlicher Schlüssel.

Was ist asymmetrische Kryptographie?

"Klassische" Kryptographie (seit tausenden Jahren):

- Geheime Schlüssel müssen im Vorhinein auf sicherem Weg ausgetauscht werden.
- Alle Teilnehmer haben gleich viele Möglichkeiten.
  Zum Beispiel: Verschlüsseln und Entschlüsseln.
- Also symmetrisch.

Asymmetrische Kryptographie *(public-key cryptography)*:

- Schlüssel bestehen (typischerweise) aus Paaren:
  Ein privater Schlüssel und ein öffentlicher Schlüssel.
- Sie statten die Besitzer mit verschiedenen Fähigkeiten aus.

Was ist asymmetrische Kryptographie?

"Klassische" Kryptographie (seit tausenden Jahren):

- Geheime Schlüssel müssen im Vorhinein auf sicherem Weg ausgetauscht werden.
- Alle Teilnehmer haben gleich viele Möglichkeiten.
  Zum Beispiel: Verschlüsseln und Entschlüsseln.
- Also symmetrisch.

Asymmetrische Kryptographie *(public-key cryptography)*:

- Schlüssel bestehen (typischerweise) aus Paaren:
  Ein privater Schlüssel und ein öffentlicher Schlüssel.
- Sie statten die Besitzer mit verschiedenen Fähigkeiten aus.
- Also asymmetrisch.

Beispiel: Digitale Signaturen

Beispiel: Digitale Signaturen

- Alice nutzt ihren privaten Schlüssel, um ein (digitales) Dokument zu unterschreiben.

Beispiel: Digitale Signaturen

- Alice nutzt ihren privaten Schlüssel, um ein (digitales) Dokument zu unterschreiben.
- Jeder kann dann mit Alices öffentlichem Schlüssel die Korrektheit der Unterschrift prüfen.

Beispiel: Digitale Signaturen

- Alice nutzt ihren privaten Schlüssel, um ein (digitales) Dokument zu unterschreiben.
- Jeder kann dann mit Alices öffentlichem Schlüssel die Korrektheit der Unterschrift prüfen.

Das ist etwa so, wie eine "echte" Unterschrift sein *sollte*.

Beispiel: Asymmetrische Verschlüsselung

Beispiel: Asymmetrische Verschlüsselung

- Jeder kann mit Bobs öffentlichem Schlüssel eine Nachricht so verschlüsseln, dass nur er sie entschlüsseln kann.

Beispiel: Asymmetrische Verschlüsselung

- Jeder kann mit Bobs öffentlichem Schlüssel eine Nachricht so verschlüsseln, dass nur er sie entschlüsseln kann.
- Bob gebraucht dann seinen privaten Schlüssel, um die Nachricht zu entschlüsseln.

Beispiel: Asymmetrische Verschlüsselung

- Jeder kann mit Bobs öffentlichem Schlüssel eine Nachricht so verschlüsseln, dass nur er sie entschlüsseln kann.
- Bob gebraucht dann seinen privaten Schlüssel, um die Nachricht zu entschlüsseln.

Das ist etwa so wie eine offene Kiste mit einem offenen Vorhängeschloss daran, für das nur Bob den Schlüssel hat.

Kernkonzept: *one-way functions*

- Moment mal: Wenn alle wissen, wie verschlüsseln geht, wieso können dann nicht auch alle entschlüsseln?

Kernkonzept: *one-way functions*

- Moment mal: Wenn alle wissen, wie verschlüsseln geht, wieso können dann nicht auch alle entschlüsseln?

- Manche Rechnungen sind viel schwerer umzukehren, als sie "vorwärts" durchgeführt werden können.

Kernkonzept: *one-way functions*

- Moment mal: Wenn alle wissen, wie verschlüsseln geht, wieso können dann nicht auch alle entschlüsseln?

- Manche Rechnungen sind viel schwerer umzukehren, als sie "vorwärts" durchgeführt werden können.

- Beispiel (nur für die Vorstellung):
  Die meisten Menschen finden Malnehmen leichter als Teilen.
  (Computer können beides ungefähr gleich schnell!)

Kernkonzept: *one-way functions*

- Moment mal: Wenn alle wissen, wie verschlüsseln geht, wieso können dann nicht auch alle entschlüsseln?

- Manche Rechnungen sind viel schwerer umzukehren, als sie "vorwärts" durchgeführt werden können.

- Beispiel (nur für die Vorstellung):
  Die meisten Menschen finden Malnehmen leichter als Teilen.
  (Computer können beides ungefähr gleich schnell!)

- Es gibt aber Rechenaufgaben, für die auch Computer in eine Richtung nur ein paar *Mikro*sekunden brauchen, in die andere aber über eine Milliarde Milliarden Jahre.
  (...zumindest nach aktuellem Wissensstand...)

Das Kerckhoffs-Prinzip

- Moment mal: Wenn alle wissen, wie verschlüsseln geht, wieso können dann nicht auch alle entschlüsseln?

Das Kerckhoffs-Prinzip

- Moment mal: Wenn alle wissen, wie verschlüsseln geht, wieso können dann nicht auch alle entschlüsseln?

Auguste Kerckhoffs, « La cryptographie militaire », Journal des sciences militaires, vol. IX, pp. 5–38, Janvier 1883, pp. 161–191, Février 1883.

> 2° Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi ;

Das Kerckhoffs-Prinzip

- Moment mal: Wenn alle wissen, wie verschlüsseln geht, wieso können dann nicht auch alle entschlüsseln?

Auguste Kerckhoffs, « La cryptographie militaire », Journal des sciences militaires, vol. IX, pp. 5–38, Janvier 1883, pp. 161–191, Février 1883.

> 2° Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi ;

- Die Sicherheit soll einzig und allein von der Geheimhaltung der Schlüssel abhängen! Das Verfahren dürfen alle kennen.

Dieser Vortrag

Was ist asymmetrische Kryptographie?

Geschichte

Der Diffie–Hellman-Schlüsselaustausch im Detail

Anwendungen

Das Q-Wort

Die Geschichte

...begann in den frühen 1970er Jahren.

Zu jener Zeit fanden noch viele Menschen, dass *das hier* eine gute Methode ist, um Kommunikation zu sichern.

Geschichte

1969+: Das Internet entsteht.

Geschichte

1969+: Das Internet entsteht.

- Bisher: Einzelne Punkt-zu-Punkt-Verbindungen.

Geschichte

1969+: Das Internet entsteht.

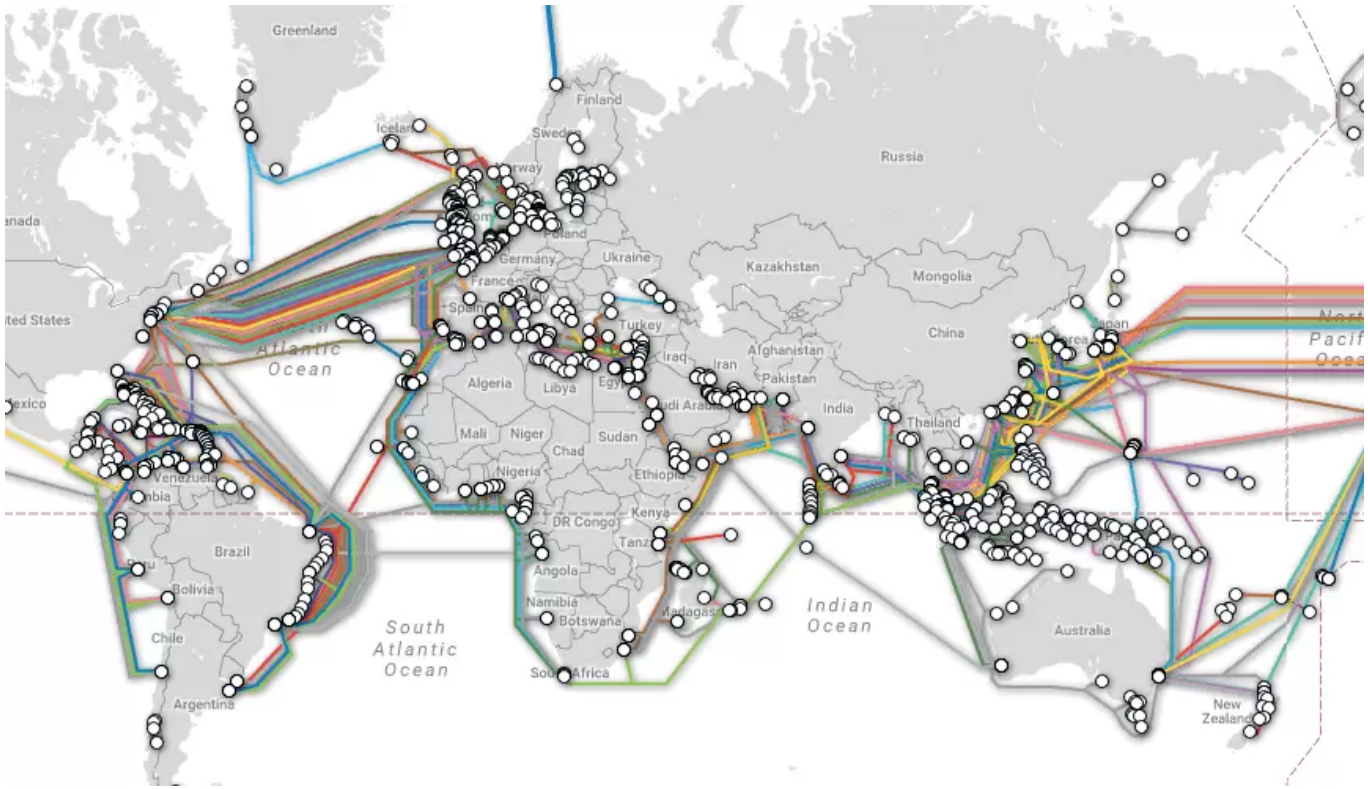
- Bisher: Einzelne Punkt-zu-Punkt-Verbindungen.
- Fortan: Fast vollständige weltweite Vernetzung.

The ARPANET in December 1969

Geschichte

1969+: Das Internet entsteht.

- Bisher: Einzelne Punkt-zu-Punkt-Verbindungen.
- Fortan: Fast vollständige weltweite Vernetzung.



Geschichte

- **1976**: Whitfield Diffie & Martin Hellman erfinden die asymmetrische Kryptographie.

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

Geschichte

- **1976**: Whitfield Diffie & Martin Hellman erfinden die asymmetrische Kryptographie.

***Abstract*—Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.**

I. Introduction

WE STAND TODAY on the brink of a revolution in cryptography.

Geschichte

- **1976**: Whitfield Diffie & Martin Hellman erfinden die asymmetrische Kryptographie.

> The best known cryptographic problem is that of privacy: preventing the unauthorized extraction of information from communications over an insecure channel. In order to use cryptography to insure privacy, however, it is currently necessary for the communicating parties to share a key which is known to no one else. This is done by sending the key in advance over some secure channel such as private courier or registered mail. A private conversation between two people with no prior acquaintance is a common occurrence in business, however, and it is unrealistic to expect initial business contacts to be postponed long enough for keys to be transmitted by some physical means. The cost and delay imposed by this key distribution problem is a major barrier to the transfer of business communications to large teleprocessing networks.

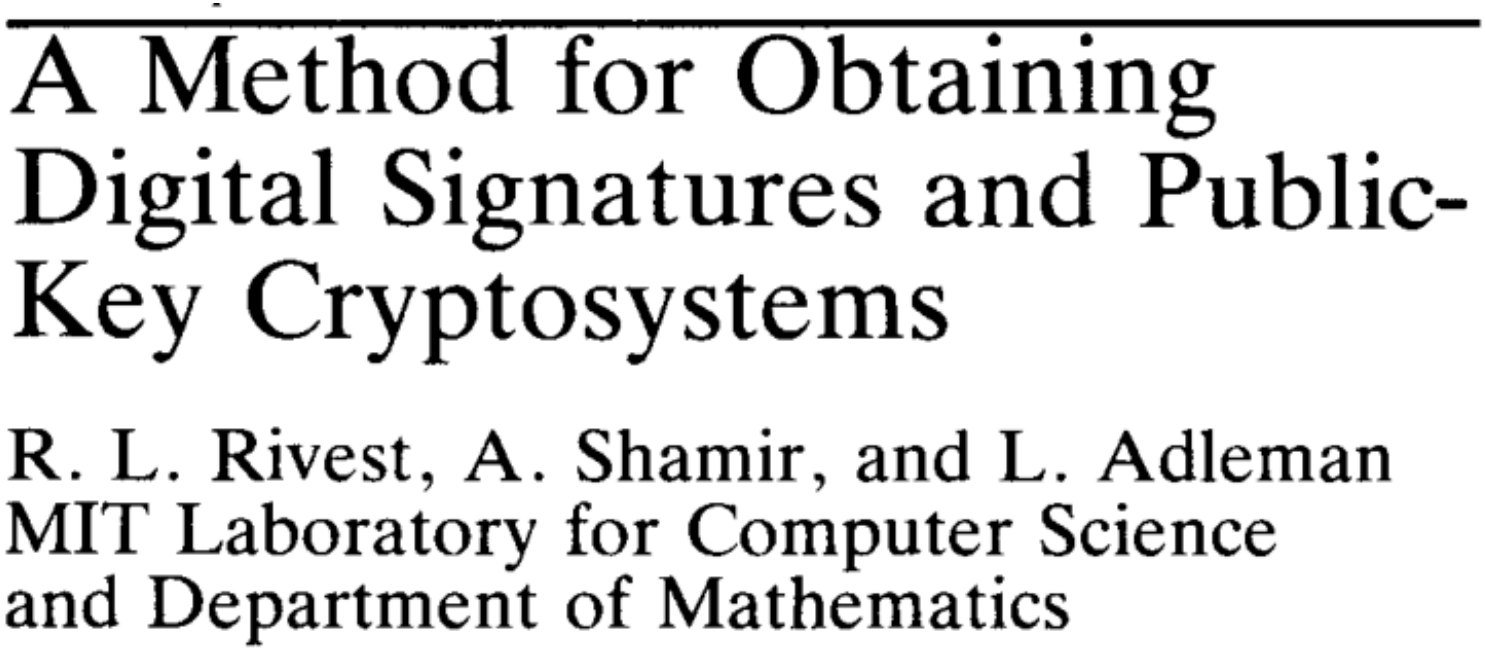
Geschichte

- **1976**: Whitfield Diffie & Martin Hellman erfinden die asymmetrische Kryptographie.

> In current business, the validity of contracts is guaranteed by signatures. A signed contract serves as legal evidence of an agreement which the holder can present in court if necessary. The use of signatures, however, requires the transmission and storage of written contracts. In order to have a purely digital replacement for this paper instrument, each user must be able to produce a message whose authenticity can be checked by anyone, but which could not have been produced by anyone else, even the recipient. Since only one person can originate messages but many people can receive messages, this can be viewed as a broadcast cipher. Current electronic authentication techniques cannot meet this need.

Geschichte

- **1977**: Ron Rivest & Adi Shamir & Len Adleman lösen offene Fragestellungen der asymmetrischen Kryptographie.



A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

R. L. Rivest, A. Shamir, and L. Adleman
MIT Laboratory for Computer Science
and Department of Mathematics

Geschichte

- **1977**: Ron Rivest & Adi Shamir & Len Adleman lösen offene Fragestellungen der asymmetrischen Kryptographie.

An encryption method is presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. This has two important consequences:
(1) Couriers or other secure means are not needed to transmit keys, since a message can be enciphered using an encryption key publicly revealed by the intended recipient. Only he can decipher the message, since only he knows the corresponding decryption key.
(2) A message can be "signed" using a privately held decryption key. Anyone can verify this signature using the corresponding publicly revealed encryption key. Signatures cannot be forged, and a signer cannot later deny the validity of his signature. This has obvious applications in "electronic mail" and "electronic funds transfer" systems.

Geschichte

- **1977**: Ron Rivest & Adi Shamir & Len Adleman lösen offene Fragestellungen der asymmetrischen Kryptographie.

I. Introduction

The era of "electronic mail" [10] may soon be upon us; we must ensure that two important properties of the current "paper mail" system are preserved: (a) messages are *private*, and (b) messages can be *signed*. We demonstrate in this paper how to build these capabilities into an electronic mail system.

At the heart of our proposal is a new encryption method. This method provides an implementation of a "public-key cryptosystem", an elegant concept invented by Diffie and Hellman [1]. Their article motivated our research, since they presented the concept but not any practical implementation of such a system. Readers familiar with [1] may wish to skip directly to Section V for a description of our method.

Geschichte

- **1970**: James H. Ellis (GCHQ )

THE POSSIBILITY OF SECURE NON-SECRET DIGITAL ENCRYPTION

J. H. Ellis, January 1970

Introduction

1. It is generally regarded as self-evident, that, in order to prevent an interceptor from understanding a message which is intelligible to the authorised recipient, it is necessary to have some initial information known to the sender and to the recipient but kept secret from the interceptor. This information can take many forms, such as the method of encipherment itself, the construction of a cipher machine, a key setting or a one-time tape. All these methods require that there is a route by which this secret information can be sent without fear of interception. Only then can the cipher text be sent safely in a non-secret manner, and large quantities of cipher text of high security thus tend to need the parallel transmission of smaller, but still substantial quantities of secret information.

2. This report demonstrates that this secret information is not theoretically necessary and that, in principle, secure messages can be sent even though the method of encipherment and all transmissions between the authorised communicators are known to the interceptor. This is what is meant by "non-secret encryption". It must be emphasised however that this demonstration has only the status of an existence theorem. It shows only that such a system is theoretically possible, and not that a practical form exists. The demonstration consists of showing that a particular, but unfortunately as yet highly impractical, system has the desired properties.

Geschichte

- **1973**: Clifford C. Cocks (GCHQ )

A NOTE ON 'NON-SECRET ENCRYPTION'
by C C Cocks, 20 November 1973

A possible implementation is suggested of J H Ellis's proposed method of encryption involving no sharing of secret information (key lists, machine set-ups, pluggings etc) between sender and receiver.

Note on "Non–Secret Encryption"

1. In [1] J H Ellis describes a theoretical method of encryption which does not necessitate the sharing of secret information between the sender and receiver. The following describes a possible implementation of this.

    a. The receiver picks 2 primes P, Q satisfying the conditions

        i. P does not divide Q-1.

        ii. Q does not divide P-1.

    He then transmits N = PQ to the sender.

    b. The sender has a message, consisting of numbers C1, C2, ... Cr with 0 < Ci < N

    He sends each, encoded as Di where Di = CiN reduced modulo N.

Dieser Vortrag

Was ist asymmetrische Kryptographie?

Geschichte

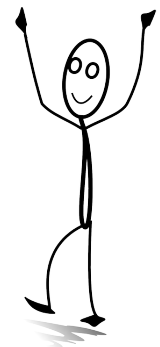
Der Diffie–Hellman-Schlüsselaustausch im Detail

Anwendungen

Das Q-Wort

Schlüsselaustausch über einen unsicheren Kanal

- Alice und Bob möchten gerne über einen unsicheren Kanal ein gemeinsames Geheimnis zu vereinbaren.
  (Danach können sie symmetrische Verfahren verwenden, um sicher zu kommunizieren.)



Schlüsselaustausch über einen unsicheren Kanal

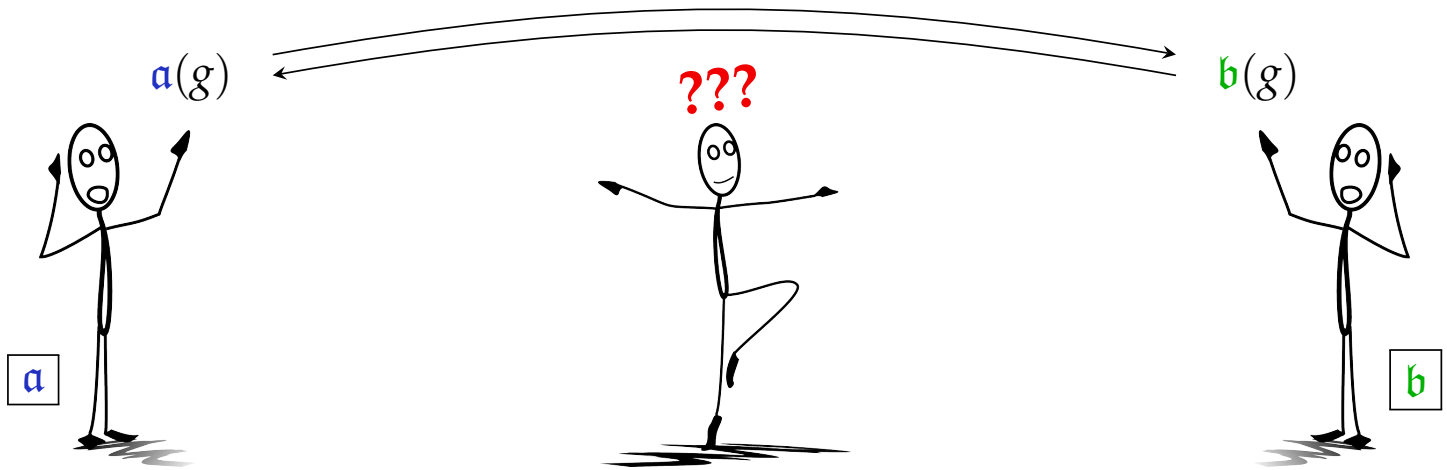
- Alice und Bob möchten gerne über einen unsicheren Kanal ein gemeinsames Geheimnis zu vereinbaren.
  (Danach können sie symmetrische Verfahren verwenden, um sicher zu kommunizieren.)

Schlüsselaustausch über einen unsicheren Kanal

- Alice und Bob möchten gerne über einen unsicheren Kanal ein gemeinsames Geheimnis zu vereinbaren.
  (Danach können sie symmetrische Verfahren verwenden, um sicher zu kommunizieren.)

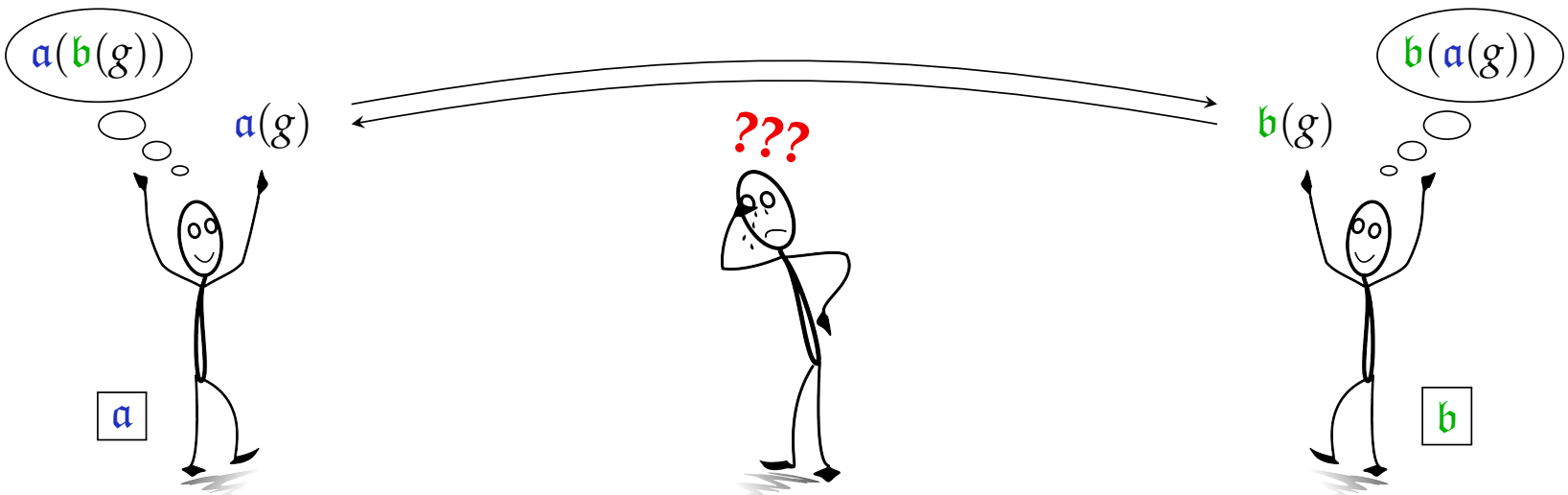
Schlüsselaustausch über einen unsicheren Kanal

- Alice und Bob möchten gerne über einen unsicheren Kanal ein gemeinsames Geheimnis zu vereinbaren.
  (Danach können sie symmetrische Verfahren verwenden, um sicher zu kommunizieren.)



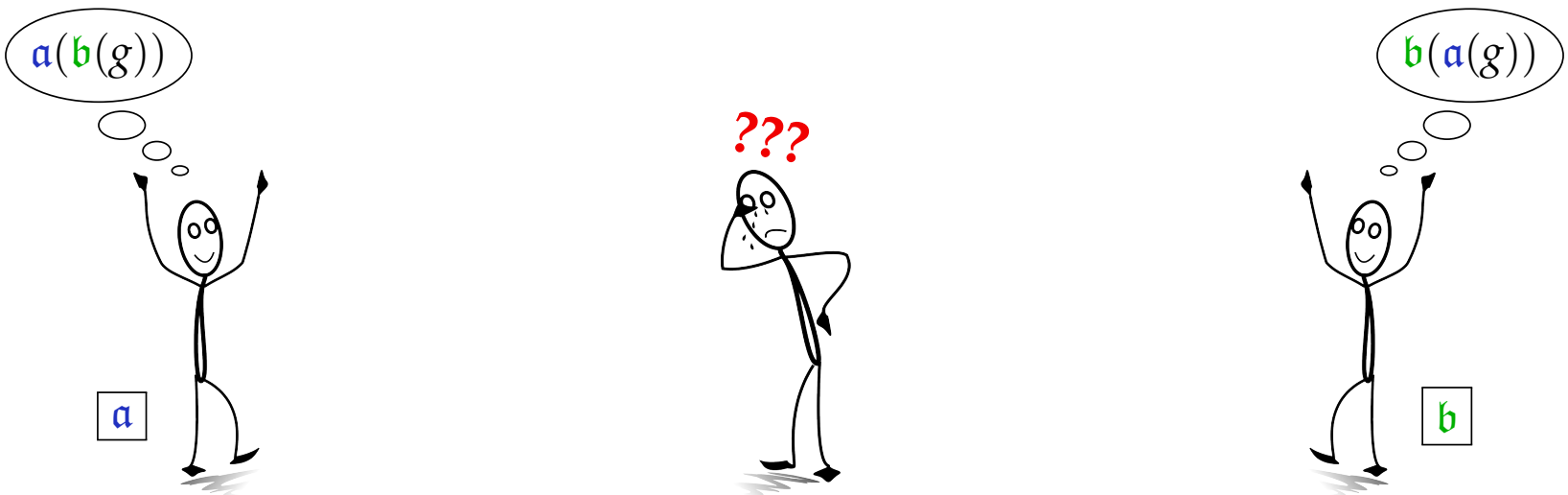
Schlüsselaustausch über einen unsicheren Kanal

- Alice und Bob möchten gerne über einen unsicheren Kanal ein gemeinsames Geheimnis zu vereinbaren.
  (Danach können sie symmetrische Verfahren verwenden, um sicher zu kommunizieren.)



Schlüsselaustausch über einen unsicheren Kanal

- Alice und Bob möchten gerne über einen unsicheren Kanal ein gemeinsames Geheimnis zu vereinbaren.
  (Danach können sie symmetrische Verfahren verwenden, um sicher zu kommunizieren.)



Schlüsselaustausch: Erste Ideen

- Wir brauchen *vertauschbare* “one-way functions” $\mathfrak{a}$ und $\mathfrak{b}$.

Schlüsselaustausch: Erste Ideen

- Wir brauchen *vertauschbare* "one-way functions" $\mathfrak{a}$ und $\mathfrak{b}$.
- Idee: Einfach mit einer geheimen Zahl multiplizieren?
  Das "funktioniert" ($g \cdot a \cdot b = g \cdot b \cdot a$), ist aber unsicher.
  (Die Angreiferin kann ja einfach $(g \cdot a)/g = a$ ausrechnen.)

Schlüsselaustausch: Erste Ideen

- Wir brauchen *vertauschbare* "one-way functions" $\mathfrak{a}$ und $\mathfrak{b}$.
- Idee: Einfach mit einer geheimen Zahl multiplizieren?
  Das "funktioniert" ($g \cdot a \cdot b = g \cdot b \cdot a$), ist aber unsicher.
  (Die Angreiferin kann ja einfach $(g \cdot a)/g = a$ ausrechnen.)
- Bessere Idee: "hoch" einer geheimen Zahl nehmen?
  Das "funktioniert" ($(g^a)^b = (g^b)^a$), ist aber unsicher
  und außerdem sehr unhandlich: absurd große Zahlen.

Schlüsselaustausch: Erste Ideen

- Wir brauchen *vertauschbare* "one-way functions" $\mathfrak{a}$ und $\mathfrak{b}$.
- Idee: Einfach mit einer geheimen Zahl multiplizieren?
  Das "funktioniert" ($g \cdot a \cdot b = g \cdot b \cdot a$), ist aber unsicher.
  (Die Angreiferin kann ja einfach $(g \cdot a)/g = a$ ausrechnen.)
- Bessere Idee: "hoch" einer geheimen Zahl nehmen?
  Das "funktioniert" ($(g^a)^b = (g^b)^a$), ist aber unsicher
  und außerdem sehr unhandlich: absurd große Zahlen.
- Wir können das aber in anderen Zahlsystemen machen!
  Dann "funktioniert" es weiterhin und ist sicher und effizient.

Die “modulo”-Operation

Sei q eine bestimmte natürliche Zahl.

- Wir rechnen normal, aber wir tun einfach so, als wäre $q = 0$.

Die “modulo”-Operation

Sei q eine bestimmte natürliche Zahl.

- Wir rechnen normal, aber wir tun einfach so, als wäre $q = 0$.
- Beispiel ($q = 5$): Es ist $\overline{11} = \overline{1 + 5 \cdot 2} = \overline{1 + 0 \cdot 2} = \overline{1}$.
  (Der Querstrich heißt, dass wir für diese Zahl einfach so tun, als wäre $q = 0$.)

Die “modulo”-Operation

Sei q eine bestimmte natürliche Zahl.

- Wir rechnen normal, aber wir tun einfach so, als wäre $q = 0$.
- Beispiel ($q = 5$): Es ist $\overline{11} = \overline{1 + 5 \cdot 2} = \overline{1 + 0 \cdot 2} = \overline{1}$.
  (Der Querstrich heißt, dass wir für diese Zahl einfach so tun, als wäre $q = 0$.)

Das “funktioniert”: Die üblichen Rechenregeln gelten!
(Der Beweis ist eine schöne Übung. Alternativ: Später mit Python ausprobieren ☺.)

Die “modulo”-Operation

Sei q eine bestimmte natürliche Zahl.

- Wir rechnen normal, aber wir tun einfach so, als wäre $q = 0$.
- Beispiel ($q = 5$): Es ist $\overline{11} = \overline{1 + 5 \cdot 2} = \overline{1 + 0 \cdot 2} = \overline{1}$.
  (Der Querstrich heißt, dass wir für diese Zahl einfach so tun, als wäre $q = 0$.)

Das “funktioniert”: Die üblichen Rechenregeln gelten!
(Der Beweis ist eine schöne Übung. Alternativ: Später mit Python ausprobieren ☺.)

Für Schlüsselaustausch löst es beide Probleme auf einmal!

Der Diffie–Hellman-Schlüsselaustausch (DH, 1976)

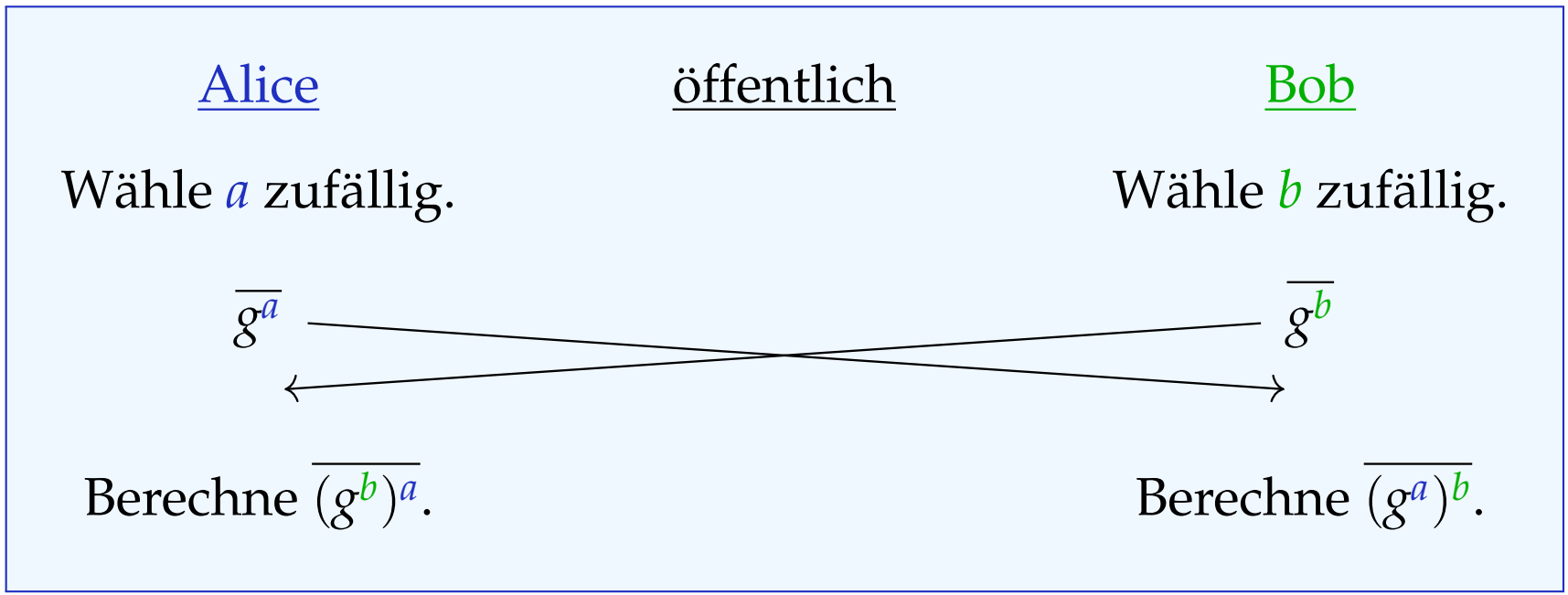
Für immer festgelegte, öffentliche Werte des Systems:

- Eine natürliche Zahl q (mit gewissen Eigenschaften...)
- Eine weitere natürliche Zahl g (mit gewissen Eigenschaften...)

Der Diffie–Hellman-Schlüsselaustausch (DH, 1976)

Für immer festgelegte, öffentliche Werte des Systems:

- Eine natürliche Zahl q (mit gewissen Eigenschaften...)
- Eine weitere natürliche Zahl g (mit gewissen Eigenschaften...)



(Hier steht der Querstrich wieder für "modulo q".)

Moderne Variante: ECDH (mit elliptischen Kurven)

- Es ist praktisch schneller und kleiner, Diffie–Hellman mit noch komplizierteren Formeln zu machen.

Moderne Variante: ECDH (mit elliptischen Kurven)

- Es ist praktisch schneller und kleiner, Diffie–Hellman mit noch komplizierteren Formeln zu machen.
- Die Rede ist von elliptischen Kurven: *Die* wichtigste Zutat moderner asymmetrischer Kryptographie.

Moderne Variante: ECDH (mit elliptischen Kurven)

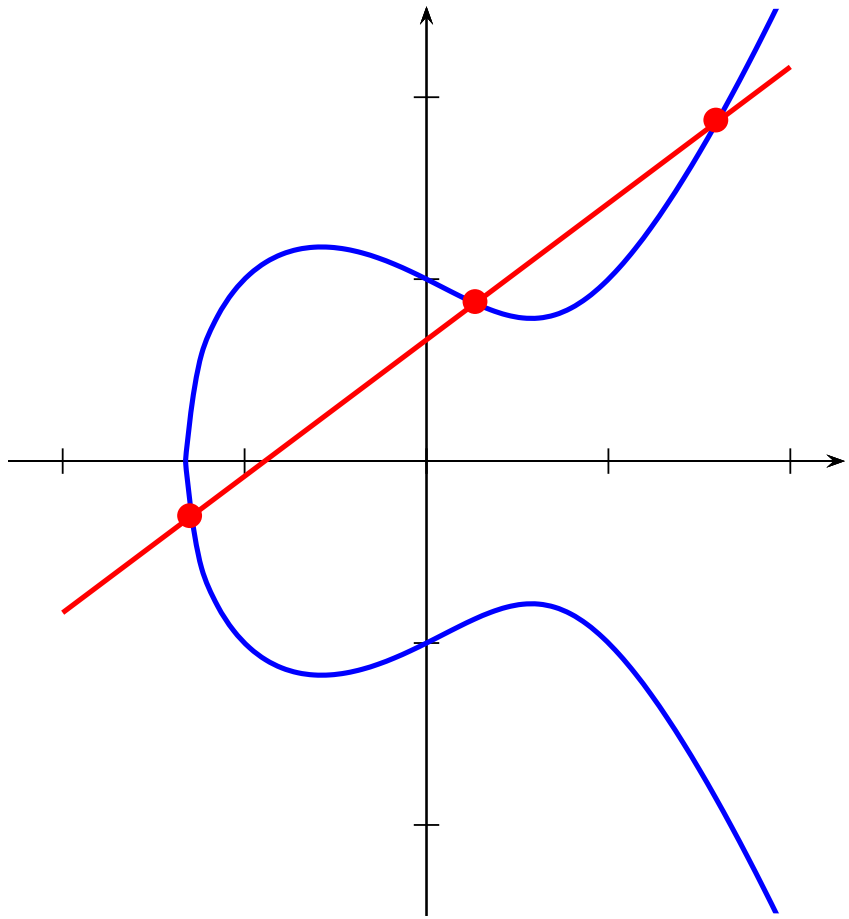
- Es ist praktisch schneller und kleiner, Diffie–Hellman mit noch komplizierteren Formeln zu machen.
- Die Rede ist von elliptischen Kurven: *Die* wichtigste Zutat moderner asymmetrischer Kryptographie.
- Im Prinzip nur die Lösungsmenge einer bestimmten Form von Gleichung: Paare (x, y) sodass $y^2 = x^3 + \alpha x + \beta$ ist.

Moderne Variante: ECDH (mit elliptischen Kurven)

- Es ist praktisch schneller und kleiner, Diffie–Hellman mit noch komplizierteren Formeln zu machen.
- Die Rede ist von elliptischen Kurven: *Die* wichtigste Zutat moderner asymmetrischer Kryptographie.
- Im Prinzip nur die Lösungsmenge einer bestimmten Form von Gleichung: Paare (x, y) sodass $y^2 = x^3 + \alpha x + \beta$ ist.

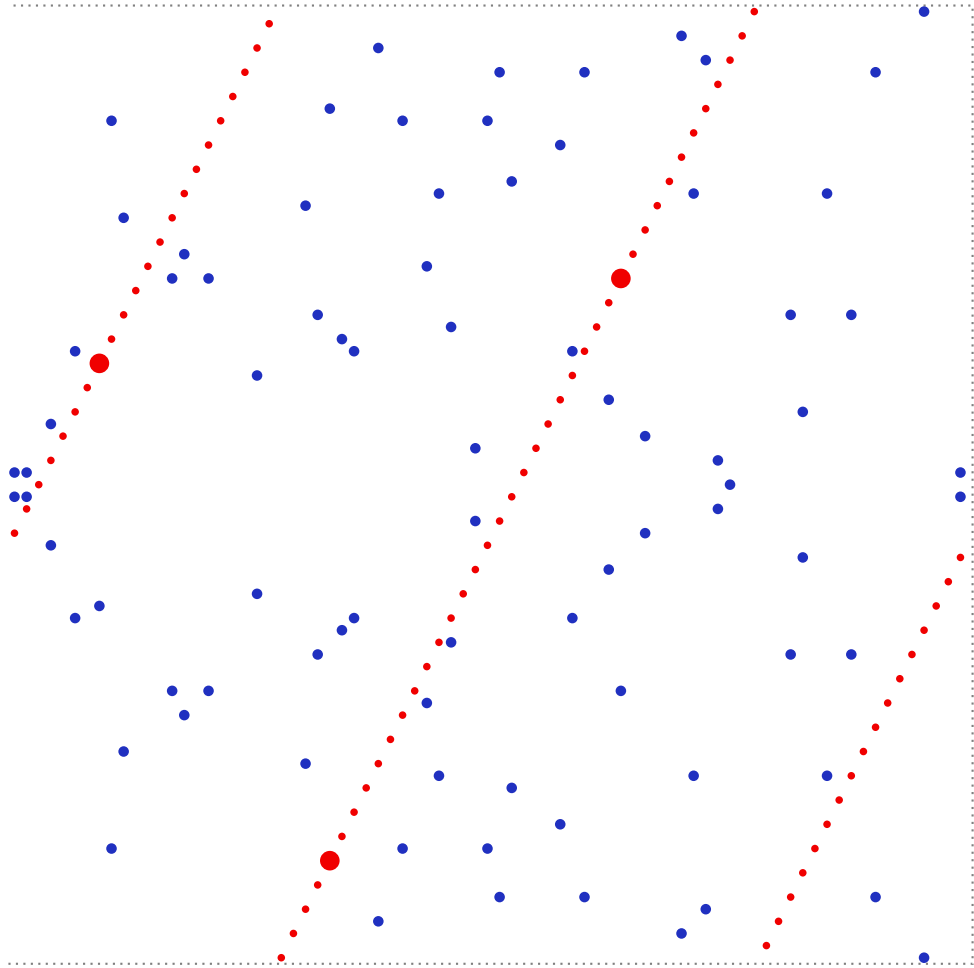
Wir können auch hiermit so rechnen, dass $(g^a)^b = (g^b)^a$ gilt.

Elliptische Kurven (ideale Welt)



Elliptische Kurven (kryptographische Realität)

Wir rechnen aus ähnlichen Gründen wieder "modulo q".



Dieser Vortrag

Was ist asymmetrische Kryptographie?

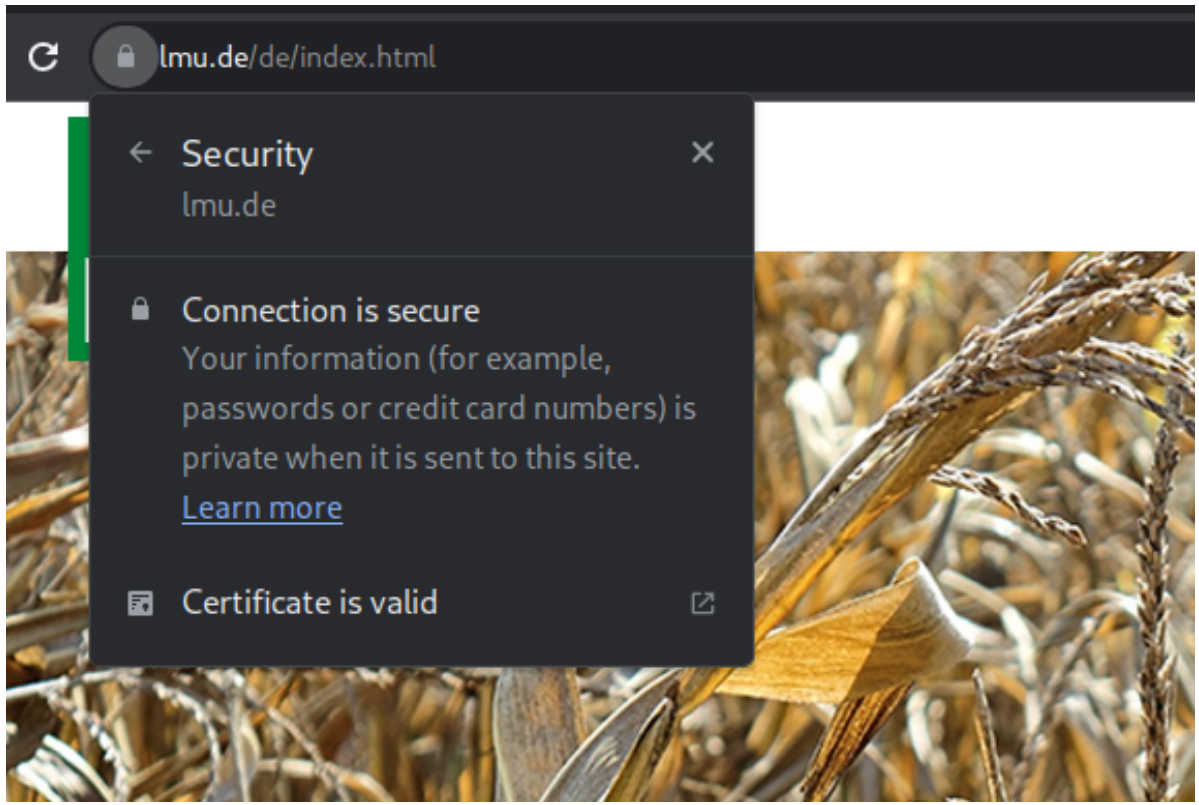
Geschichte

Der Diffie–Hellman-Schlüsselaustausch im Detail

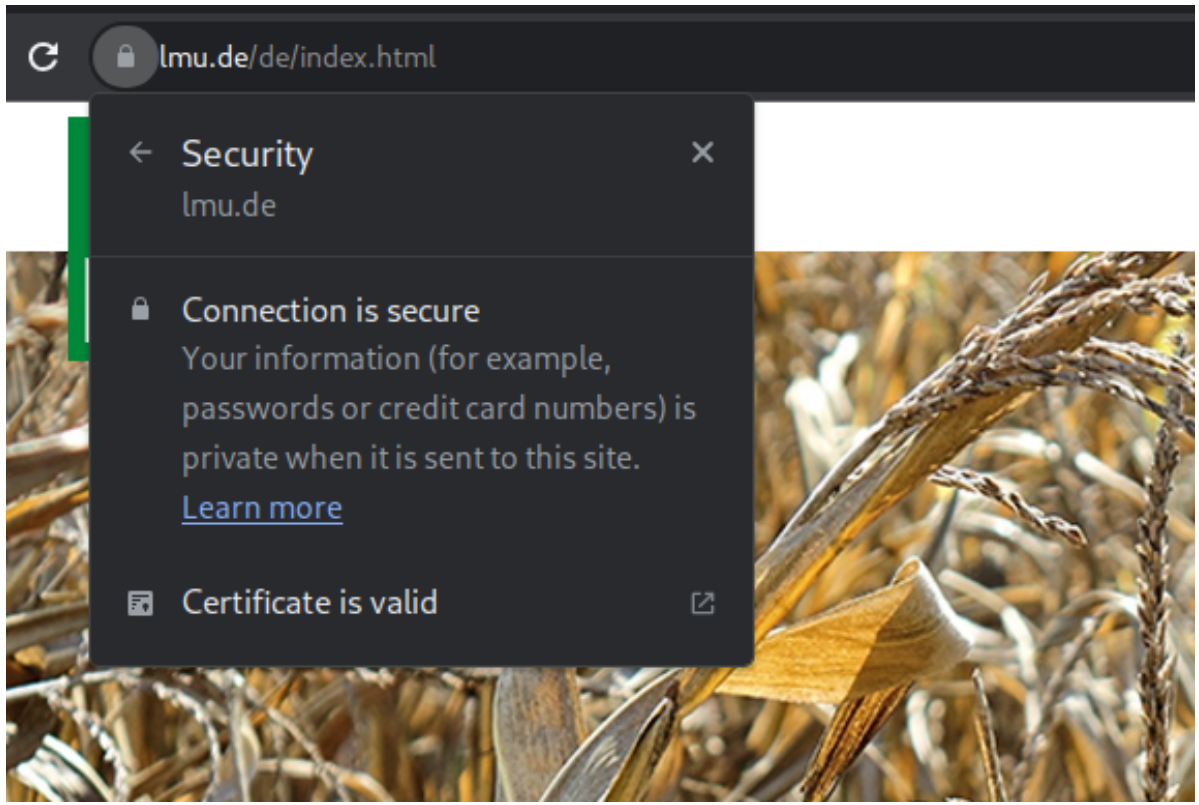
Anwendungen

Das Q-Wort

Anwendung: Das Internet (SSL/TLS)

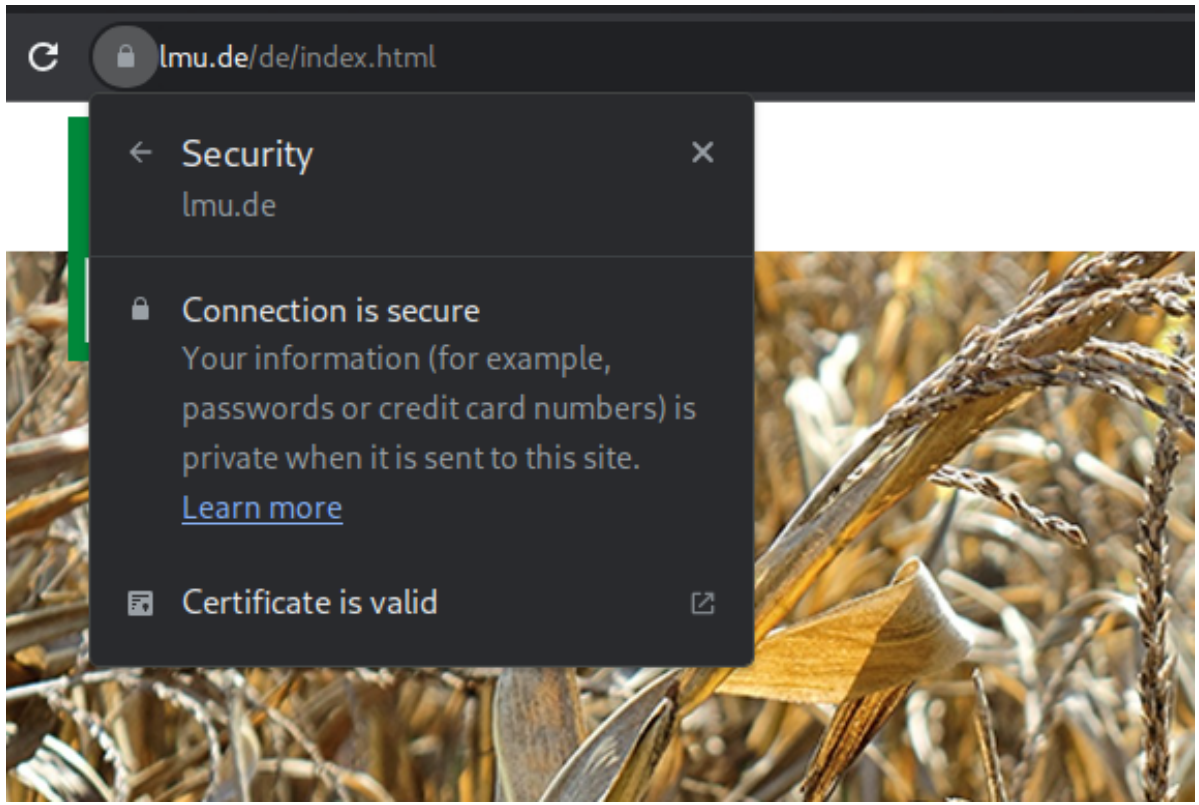


Anwendung: Das Internet (SSL/TLS)



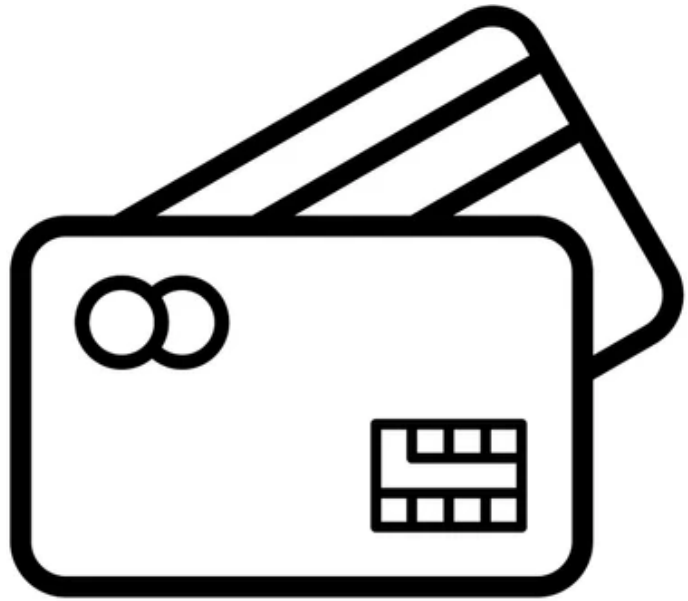
- Das Zertifikat bestätigt dem Besucher, dass die Seite auch wirklich die gewünschte ist (mit einer digitalen Signatur).

Anwendung: Das Internet (SSL/TLS)

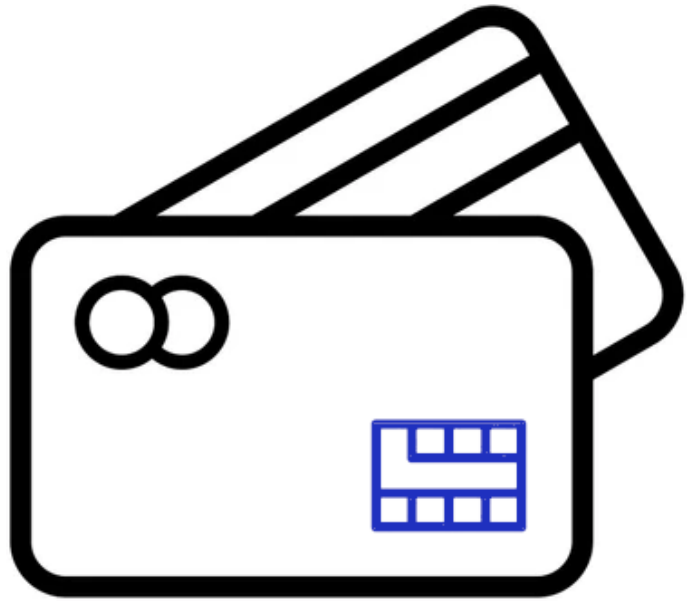


- Das Zertifikat bestätigt dem Besucher, dass die Seite auch wirklich die gewünschte ist (mit einer digitalen Signatur).
- Außerdem kommunizieren Webserver und -browser sicher: Niemand kann mitlesen oder Inhalte unterwegs verändern.

Anwendung: Mit Karte zahlen

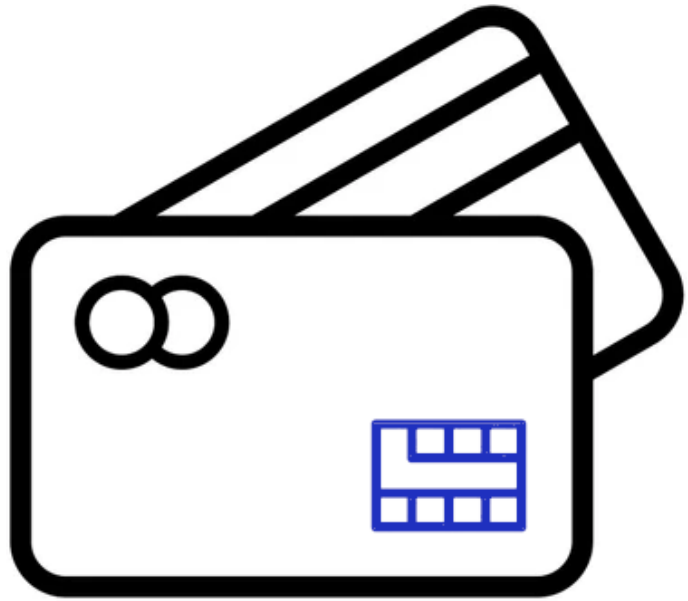


Anwendung: Mit Karte zahlen



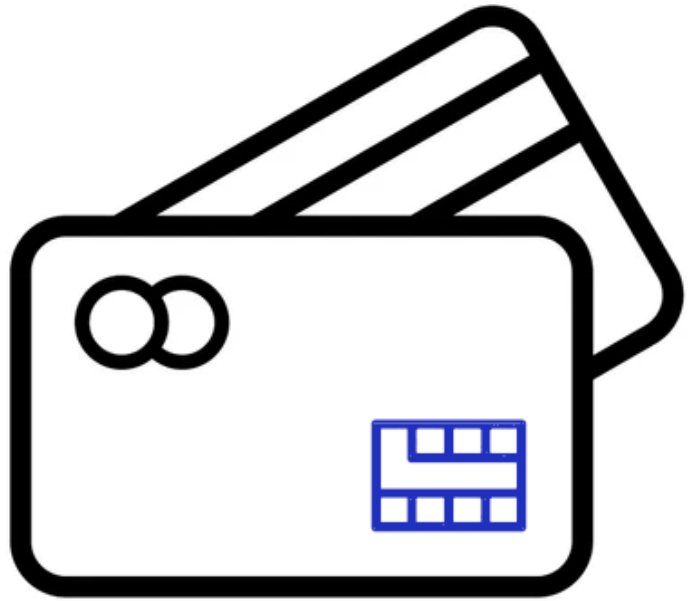
- Die Bezahlkarte enthält einen Mikrochip, mit dem für jeden Bezahlvorgang eine digitale Signatur erzeugt wird.

Anwendung: Mit Karte zahlen



- Die Bezahlkarte enthält einen Mikrochip, mit dem für jeden Bezahlvorgang eine digitale Signatur erzeugt wird.
- Die Bank kann damit prüfen, dass wirklich mit der Karte bezahlt wurde und nicht etwa nur jemand die Nummer auf der Karte abgeschrieben hat.

Anwendung: Mit Karte zahlen



- Die Bezahlkarte enthält einen Mikrochip, mit dem für jeden Bezahlvorgang eine digitale Signatur erzeugt wird.
- Die Bank kann damit prüfen, dass wirklich mit der Karte bezahlt wurde und nicht etwa nur jemand die Nummer auf der Karte abgeschrieben hat.
- (Achtung: Der PIN-Code ist nicht der private Schlüssel. Er ist viel zu kurz.)

Anwendung: Sichere Chats (E2EE)

In another exchange leaked to Silicon Alley Insider, Zuckerberg explained to a friend that his control of Facebook gave him access to any information he wanted on any Harvard student:

> ZUCK: yea so if you ever need info about anyone at harvard
>
> ZUCK: just ask
>
> ZUCK: i have over 4000 emails, pictures, addresses, sns
>
> FRIEND: what!? how'd you manage that one?
>
> ZUCK: people just submitted it
>
> ZUCK: i don't know why
>
> ZUCK: they "trust me"
>
> ZUCK: dumb fucks

(The New Yorker, 2010)

Anwendung: Sichere Chats (E2EE)

In another exchange leaked to Silicon Alley Insider, Zuckerberg explained to a friend that his control of Facebook gave him access to any information he wanted on any Harvard student:

> ZUCK: yea so if you ever need info about anyone at harvard
>
> ZUCK: just ask
>
> ZUCK: i have over 4000 emails, pictures, addresses, sns
>
> FRIEND: what!? how'd you manage that one?
>
> ZUCK: people just submitted it
>
> ZUCK: i don't know why
>
> ZUCK: they "trust me"
>
> ZUCK: dumb fucks

(The New Yorker, 2010)

- Kern des Problems: Zentraler Server kann alles mitlesen.

Anwendung: Sichere Chats (E2EE)

In another exchange leaked to Silicon Alley Insider, Zuckerberg explained to a friend that his control of Facebook gave him access to any information he wanted on any Harvard student:

> ZUCK: yea so if you ever need info about anyone at harvard
>
> ZUCK: just ask
>
> ZUCK: i have over 4000 emails, pictures, addresses, sns
>
> FRIEND: what!? how'd you manage that one?
>
> ZUCK: people just submitted it
>
> ZUCK: i don't know why
>
> ZUCK: they "trust me"
>
> ZUCK: dumb fucks

(The New Yorker, 2010)

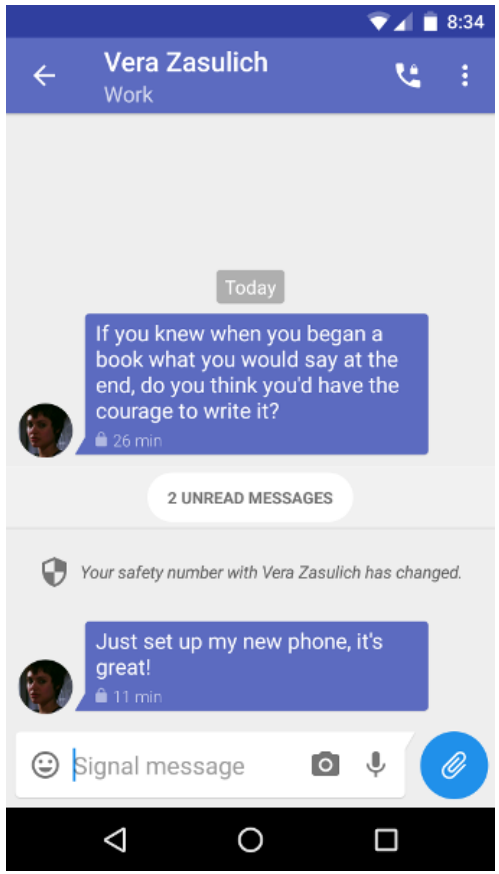
- Kern des Problems: Zentraler Server kann alles mitlesen.
- "Briefgeheimnis" wird oft nicht technisch erzwungen.

Anwendung: Sichere Chats (E2EE)

- Kern des Problems: Zentraler Server kann alles mitlesen.
- "Briefgeheimnis" wird oft nicht technisch erzwungen.
- Das geht aber — mit (asymmetrischer) Kryptographie!

Anwendung: Sichere Chats (E2EE)

- Kern des Problems: Zentraler Server kann alles mitlesen.
- “Briefgeheimnis” wird oft nicht technisch erzwungen.
- Das geht aber — mit (asymmetrischer) Kryptographie!



Anwendung: Software-Updates

- Wenn wir über das Internet Updates runterladen, könnte uns unter Umständen jemand unterwegs Malware unterjubeln.

Anwendung: Software-Updates

- Wenn wir über das Internet Updates runterladen, könnte uns unter Umständen jemand unterwegs Malware unterjubeln.

- Daher sind Software-Updates heutzutage digital signiert.
  Die Signatur garantiert: Das Update kommt wirklich vom Hersteller.

Anwendung: Software-Updates

- Wenn wir über das Internet Updates runterladen, könnte uns unter Umständen jemand unterwegs Malware unterjubeln.

- Daher sind Software-Updates heutzutage digital signiert.
  Die Signatur garantiert: Das Update kommt wirklich vom Hersteller.

- Fun Fact: Die PlayStation 3 konnte 2010 entsperrt werden, weil Sony beim Signieren einen fatalen Fehler gemacht hat.

Anwendung: “Neuer” Personalausweis

Anwendung: “Neuer” Personalausweis

- (Grundsätzliche) Möglichkeit zur Erstellung einer “qualifizierten elektronischen Unterschrift”.

Anwendung: “Neuer” Personalausweis

- (Grundsätzliche) Möglichkeit zur Erstellung einer “qualifizierten elektronischen Unterschrift”.
- Das ist eine digitale Signatur, also asymmetrische Kryptographie!

Dieser Vortrag

Was ist asymmetrische Kryptographie?

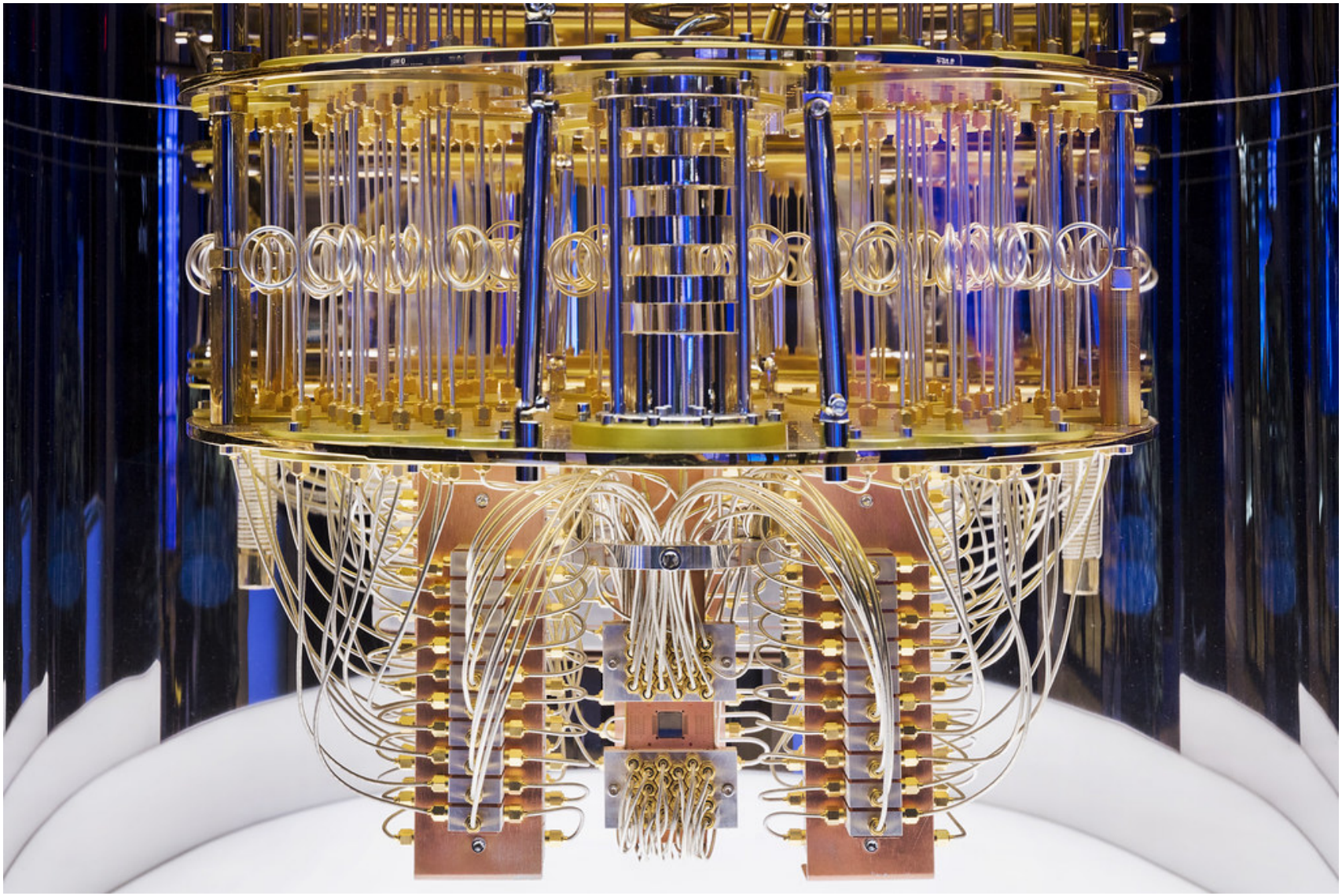
Geschichte

Der Diffie–Hellman-Schlüsselaustausch im Detail

Anwendungen

Das Q-Wort

Quantencomputer



Quantencomputer vs. Kryptographie

Entgegen landläufiger Meinung:

- ***Quantencomputer können nicht alles besser.***

Quantencomputer vs. Kryptographie

Entgegen landläufiger Meinung:

- ***Quantencomputer können nicht alles besser.***
- Für viele Aufgaben sind sie genau gleich schlecht wie "normale" Rechner — und um Größenordnungen teurer.

Quantencomputer vs. Kryptographie

Entgegen landläufiger Meinung:

- ***Quantencomputer können nicht alles besser.***
- Für viele Aufgaben sind sie genau gleich schlecht wie "normale" Rechner — und um Größenordnungen teurer.

(...zumindest nach aktuellem Wissensstand...)

Quantencomputer vs. Kryptographie

Entgegen landläufiger Meinung:

- ***Quantencomputer können nicht alles besser.***
- Für viele Aufgaben sind sie genau gleich schlecht wie "normale" Rechner — und um Größenordnungen teurer.

(...zumindest nach aktuellem Wissensstand...)

Aber..:

- Quantencomputer brechen zufällig(?) just die am meisten genutzten asymmetrischen Verfahren.
  - Diffie–Hellman (auch mit elliptischen Kurven)
  - RSA (sowohl Verschlüsselung als auch Signatur)
  - DSA (auch mit elliptischen Kurven)
  - usw.

Quantencomputer vs. Kryptographie

Entgegen landläufiger Meinung:

- ***Quantencomputer können nicht alles besser.***
- Für viele Aufgaben sind sie genau gleich schlecht wie "normale" Rechner — und um Größenordnungen teurer.

(...zumindest nach aktuellem Wissensstand...)

Aber..:

- Quantencomputer brechen zufällig(?) just die am meisten genutzten asymmetrischen Verfahren.
  - Diffie–Hellman (auch mit elliptischen Kurven)
  - RSA (sowohl Verschlüsselung als auch Signatur)
  - DSA (auch mit elliptischen Kurven)
  - usw.
- Für symmetrische Verfahren ist der Schaden geringer.

Quantencomputer: Funktionsprinzip

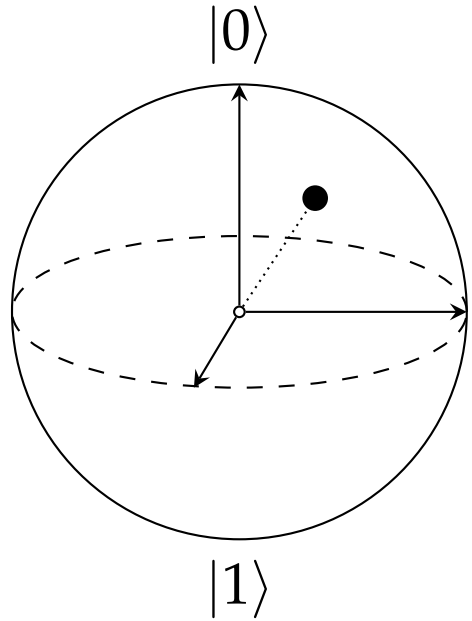
- “Normaler” Computer: Jedes Bit ist stets entweder 0 oder 1.

Quantencomputer: Funktionsprinzip

- "Normaler" Computer: Jedes Bit ist stets entweder 0 oder 1.
- Quantencomputer: "Qubits" können **auf eine bestimmte Art und Weise** "zugleich" ein bisschen 0 und ein bisschen 1 sein.

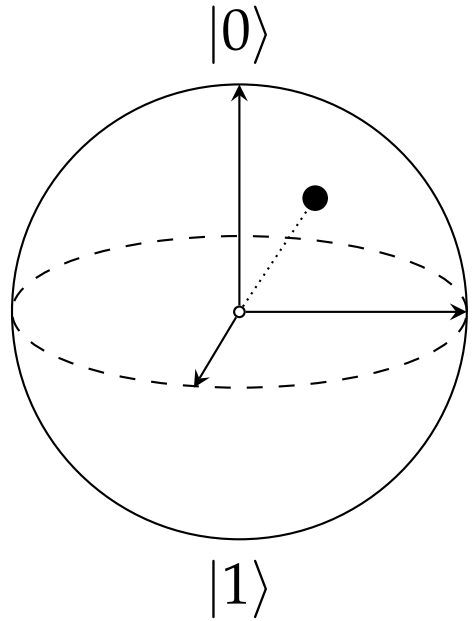
Quantencomputer: Funktionsprinzip

- "Normaler" Computer: Jedes Bit ist stets entweder 0 oder 1.
- Quantencomputer: "Qubits" können **auf eine bestimmte Art und Weise** "zugleich" ein bisschen 0 und ein bisschen 1 sein.



Quantencomputer: Funktionsprinzip

- "Normaler" Computer: Jedes Bit ist stets entweder 0 oder 1.
- Quantencomputer: "Qubits" können **auf eine bestimmte Art und Weise** "zugleich" ein bisschen 0 und ein bisschen 1 sein.



Das bedeutet **nicht**, dass "Quantencomputer einfach alle privaten Schlüssel gleichzeitig durchprobieren können".

Post-Quanten-Kryptographie

!! Es gibt viele asymmetrische Verfahren, die weiterhin sicher zu sein scheinen — auch gegen Quantencomputer.

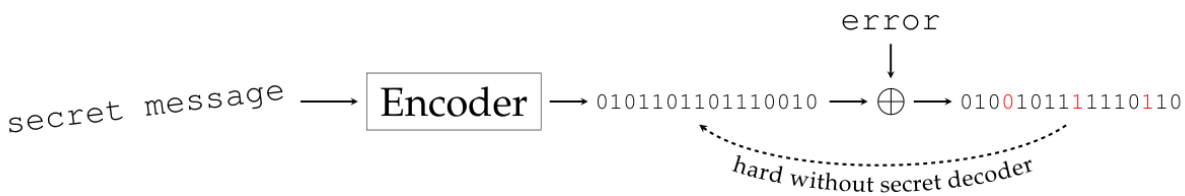
Post-Quanten-Kryptographie

!! Es gibt viele asymmetrische Verfahren, die weiterhin sicher zu sein scheinen — auch gegen Quantencomputer.

Code-based crypto

Main application: **Encryption**.

Underlying problem: Correct errors in a codeword of a random-looking code.



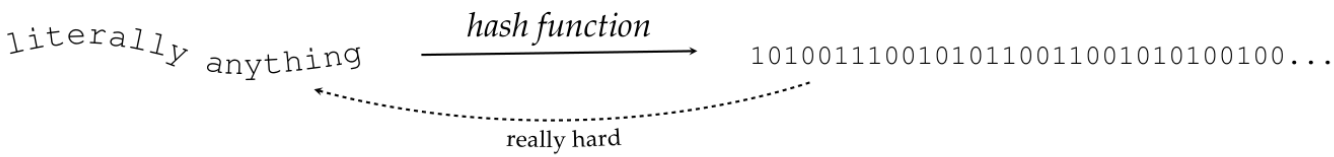
Oldest proposal: McEliece 1978. Still *essentially unbroken* [2].

Post-Quanten-Kryptographie

!! Es gibt viele asymmetrische Verfahren, die weiterhin sicher zu sein scheinen — auch gegen Quantencomputer.

Hash-based signatures

Hash functions are random-looking functions that compress arbitrary data to short bitstrings. They should be hard to invert.



An individual can tie a hash value to their identity and later identify themself by revealing the corresponding input.
Selectively revealing inputs depending on a message leads to a signature scheme.

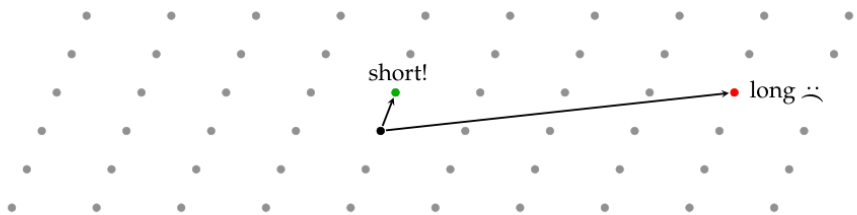
Post-Quanten-Kryptographie

!! Es gibt viele asymmetrische Verfahren, die weiterhin sicher zu sein scheinen — auch gegen Quantencomputer.

Lattice-based crypto

Main applications: **Encryption**, **signatures**, and beyond.

Underlying problem: Find short vectors in a discrete additive subgroup of $\mathbb{R}^n$.



Post-Quanten-Kryptographie

!! Es gibt viele asymmetrische Verfahren, die weiterhin sicher zu sein scheinen — auch gegen Quantencomputer.

Multivariate crypto

Main application: **Signatures**.

Underlying problem: Solve systems of quadratic equations over a finite field.

$$10x^2 + 15z^2 + 19xy + 7xz + 27yz + 20x + y \equiv 14 \pmod{31}$$
$$25x^2 + 30y^2 + 17z^2 + 30xy + 23xz + 27yz + 15x + 4y + 16z \equiv 5 \pmod{31}$$
$$15x^2 + 9y^2 + 11z^2 + 18xy + 24xz + 16yz + 28x + 9y + 3z \equiv 6 \pmod{31}$$
$$27x^2 + 10y^2 + 17z^2 + 7xz + 28yz + 4x + 13y + 27z \equiv 12 \pmod{31}$$

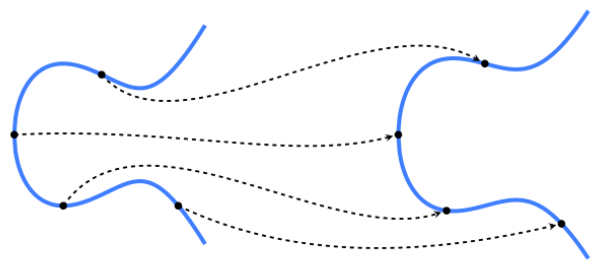
Post-Quanten-Kryptographie

!! Es gibt viele asymmetrische Verfahren, die weiterhin sicher zu sein scheinen — auch gegen Quantencomputer.

Isogeny-based crypto

Main application: **Key exchange**.

Underlying problem: Find an isogeny between two elliptic curves.
An *isogeny* is a surjective group homomorphism given by rational functions.



Dieser Vortrag

Was ist asymmetrische Kryptographie?

Geschichte

Der Diffie–Hellman-Schlüsselaustausch im Detail

Anwendungen

Das Q-Wort

Empfehlung: Veritasium über Post-Quanten-Kryptographie

https://youtu.be/-UrdExQW0cs

Empfehlung: CryptoHack

https://cryptohack.org

Fragen?

Gerne auch jederzeit per Email: `lorenz@yx7.cc`