Elliptic Curve Cryptography

Erik Nellessen

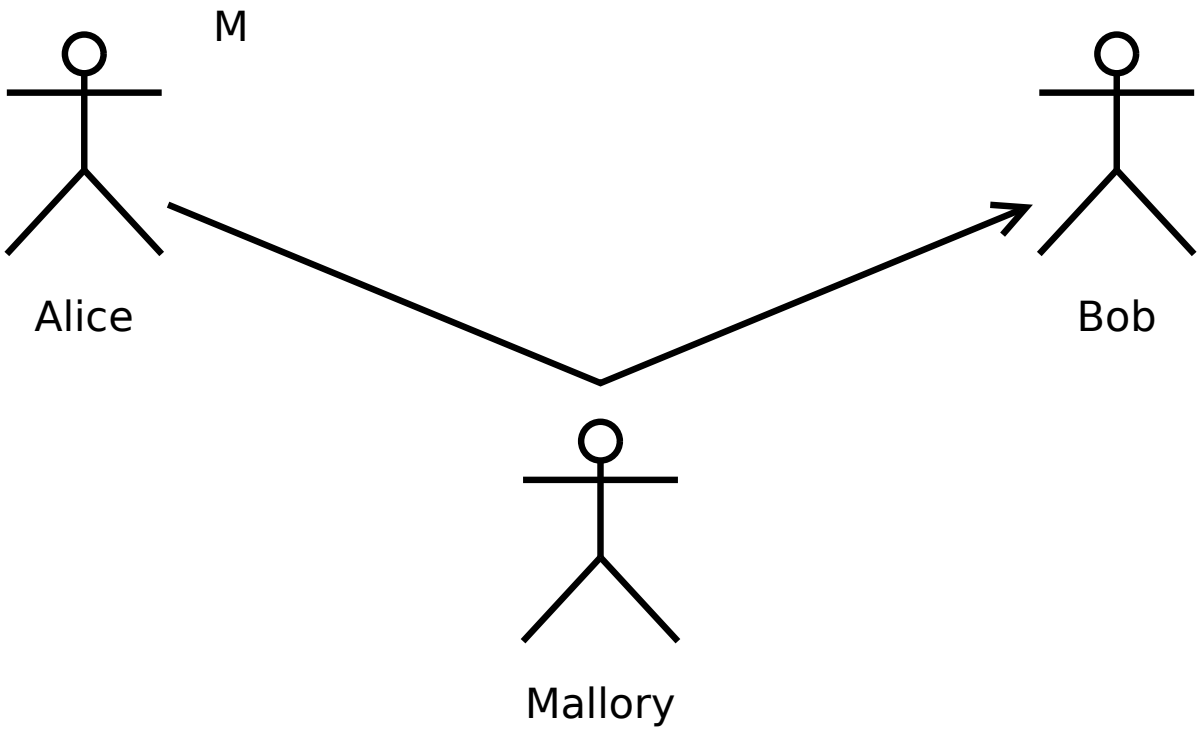
Institut für Informatik
Humboldt-Universität zu Berlin

10. November 2013

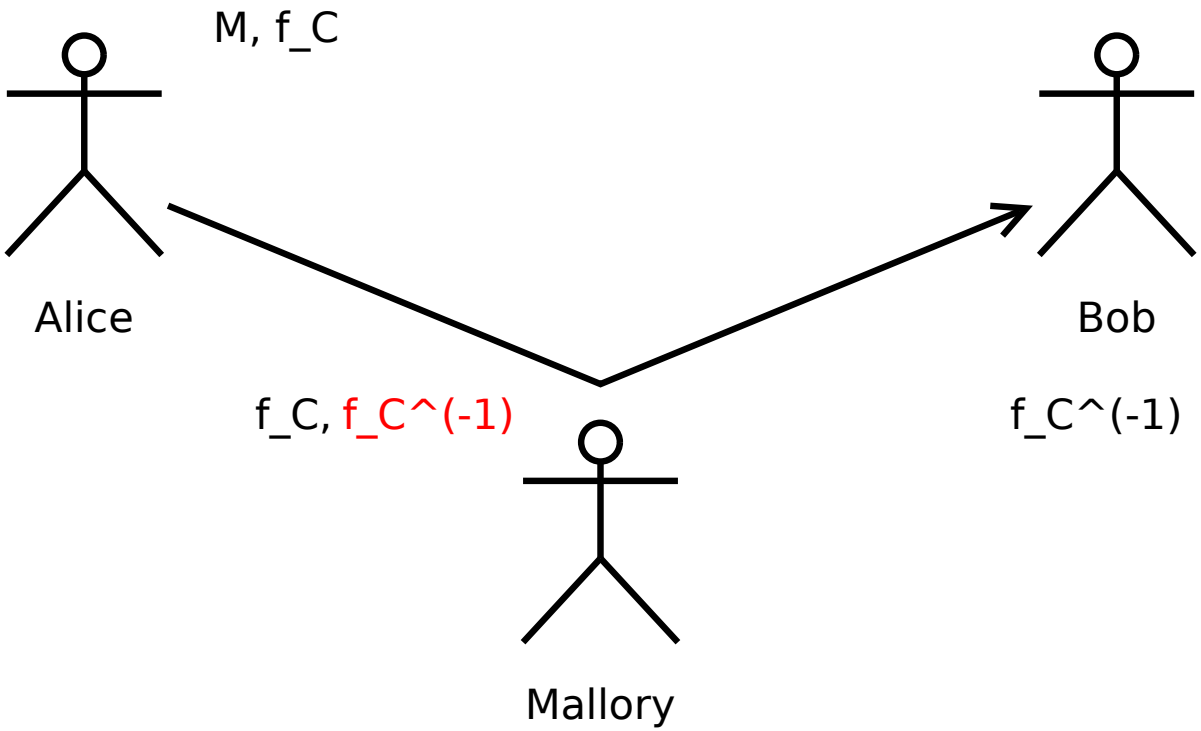
Aufbau

1. Asymmetrische Verschlüsselung im Allgemeinen
2. Elliptische Kurven über den reellen Zahlen und modulo einer Primzahl
3. Addition auf elliptischen Kurven
4. ECDLP
5. Beispiel einer ECC-verschlüsselten Kommunikation
6. Anwendung von ECC
7. ECC in Krypto-Bibliotheken
8. Vorteile von ECC
9. Woher kommen die Kurven?

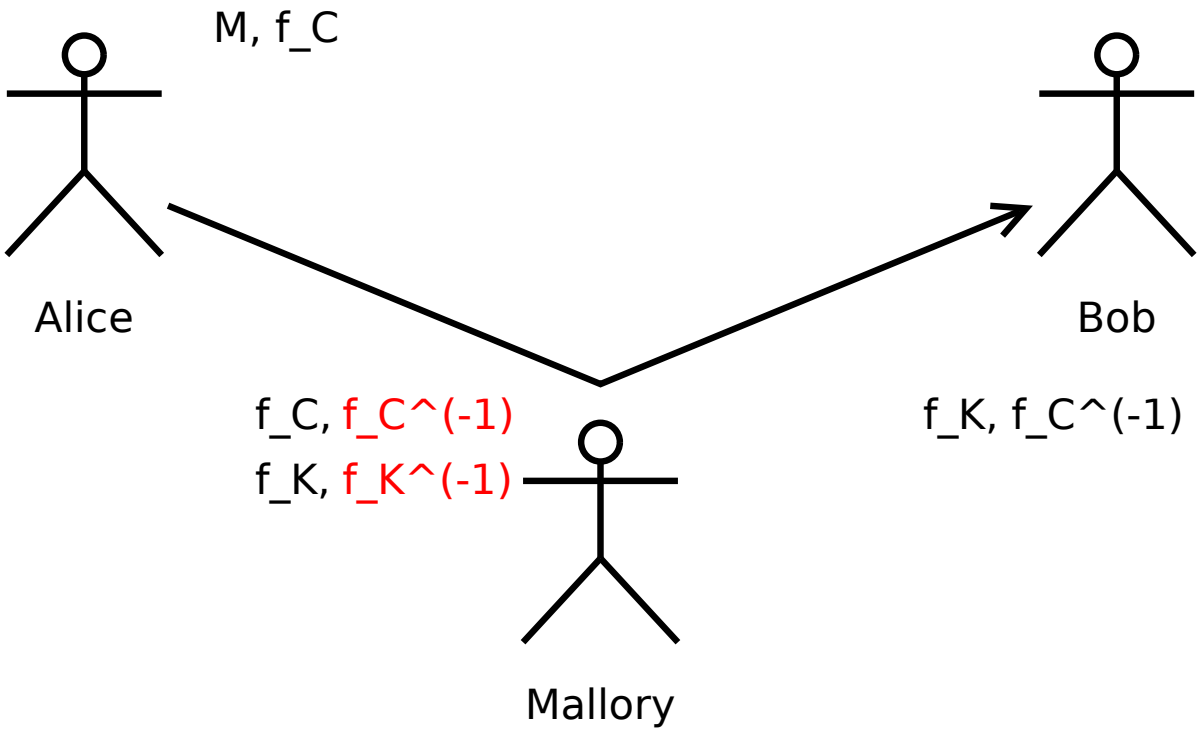
Asymmetrische Verschlüsselung (1)



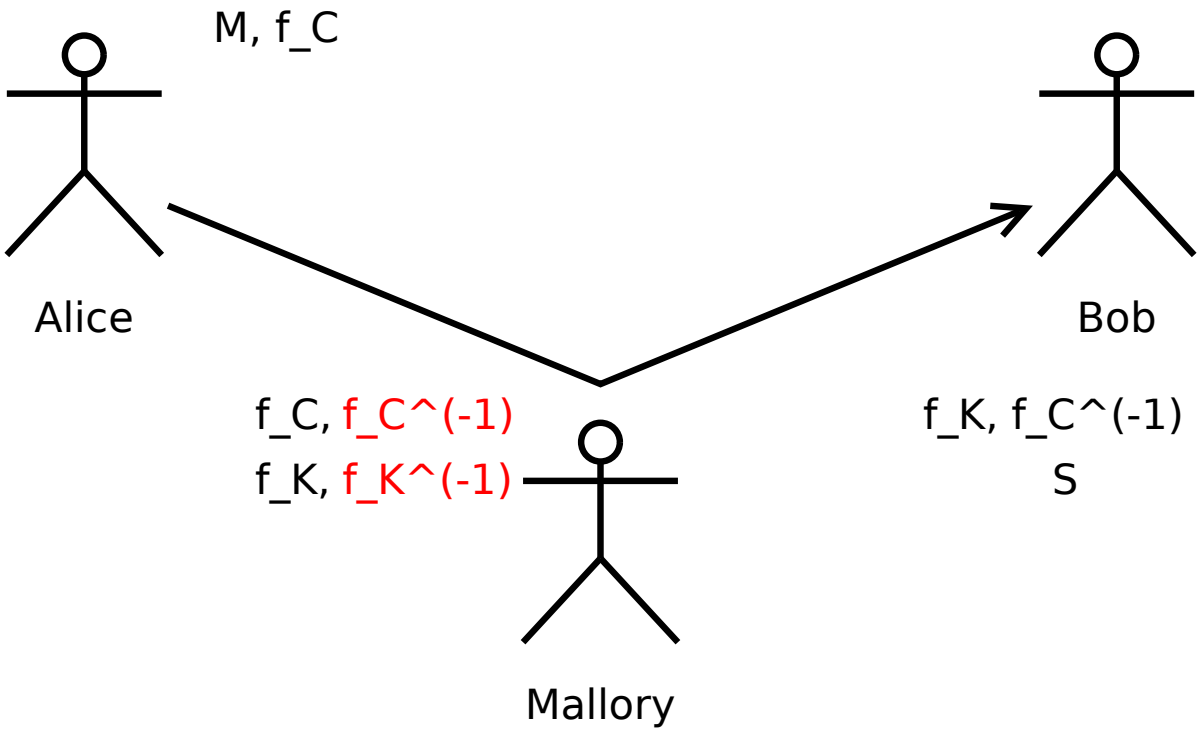
Asymmetrische Verschlüsselung (2)



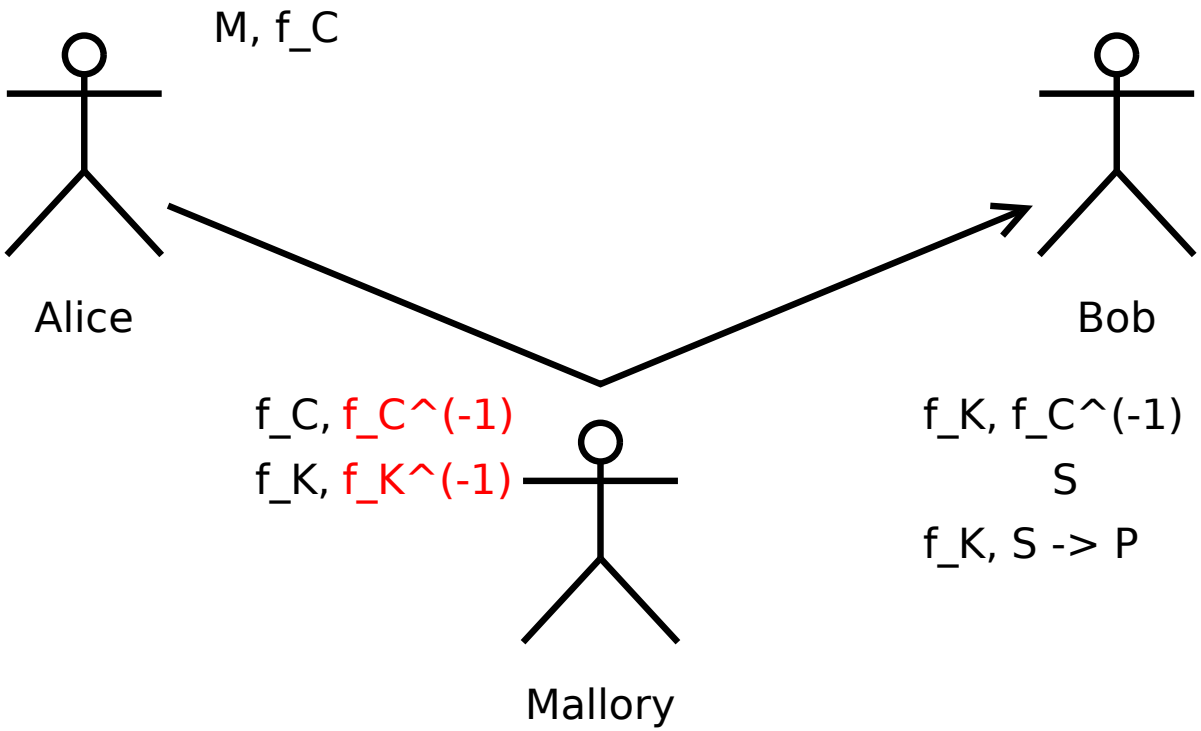
Asymmetrische Verschlüsselung (3)



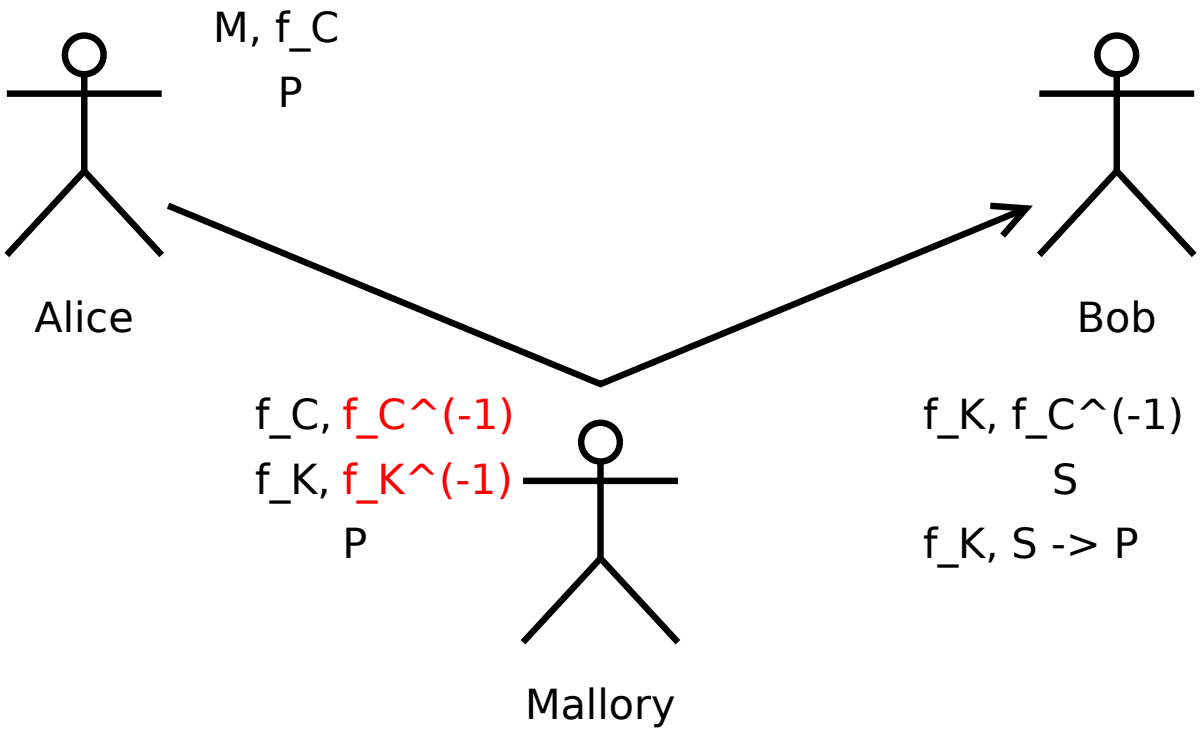
Asymmetrische Verschlüsselung (4)



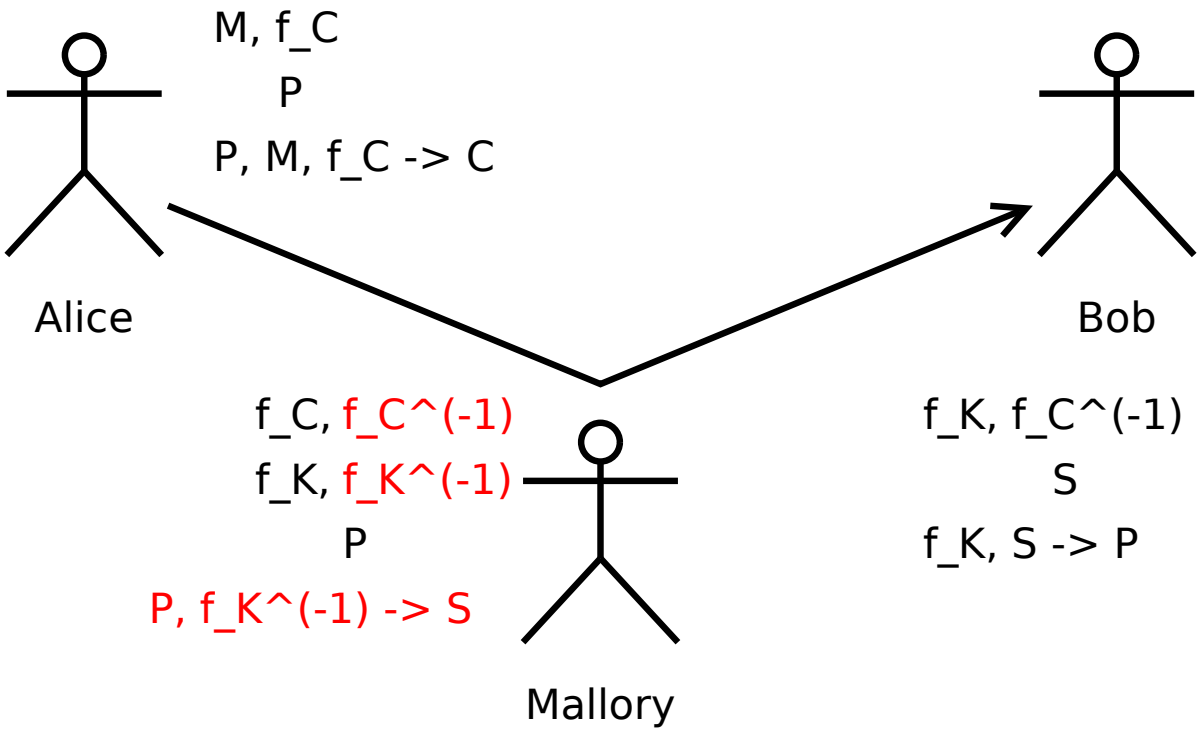
Asymmetrische Verschlüsselung (5)



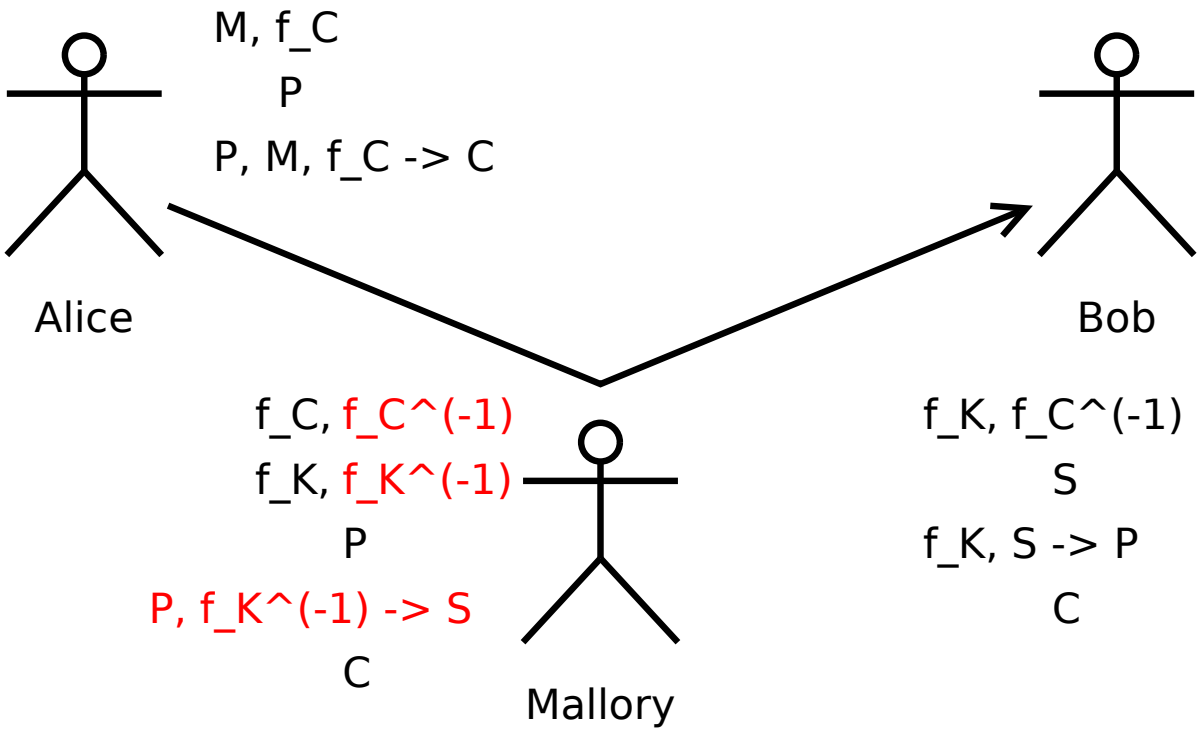
Asymmetrische Verschlüsselung (6)



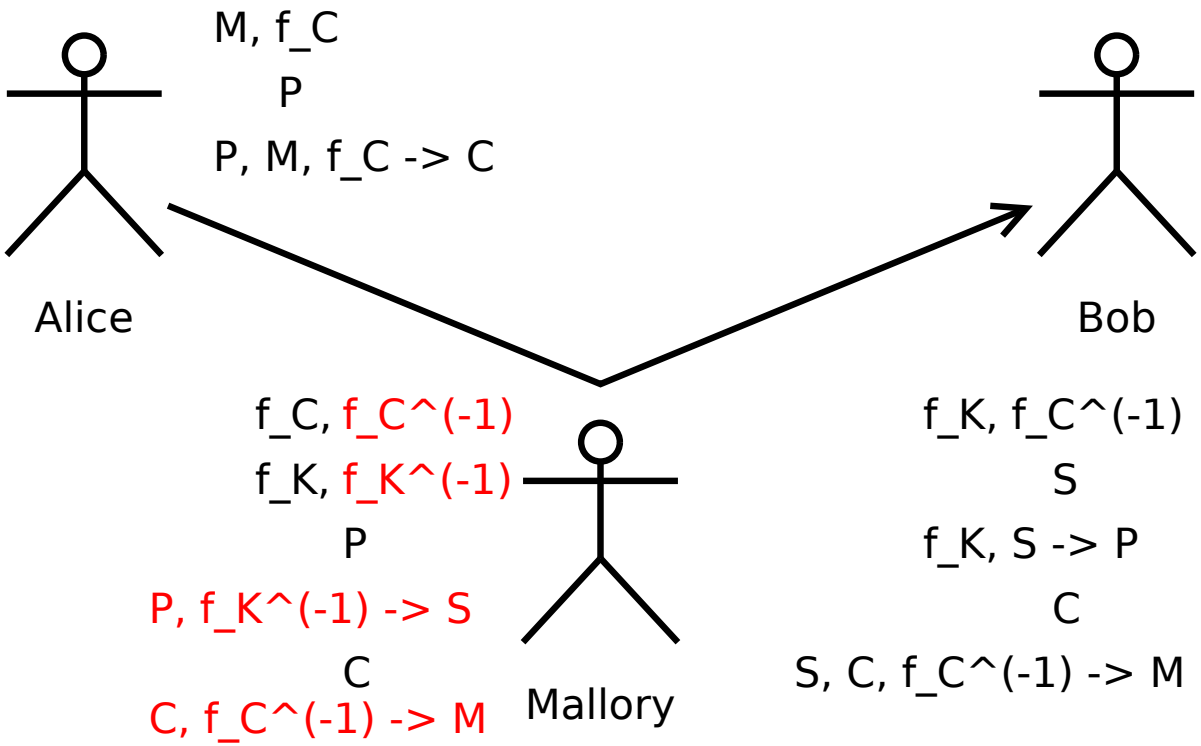
Asymmetrische Verschlüsselung (7)



Asymmetrische Verschlüsselung (8)



Asymmetrische Verschlüsselung (9)



Asymmetrische Verschlüsselung: Vorteile

- Kein Schlüsselaustausch über sicheren Kanal von Nöten.
- Jeder muss nur seinen eigenen privaten Schlüssel geheim halten.

Asymmetrische Verschlüsselung: Nachteile

- Deutlich langsamer als symmetrische Verschlüsselung.
- Sicherheit basiert auf einer **Annahme**, abgefangene Nachrichten in Zukunft vielleicht entschlüsselbar.

Asymmetrische Verschlüsselung: Grenzen

- Woher weiß Alice, dass der öffentliche Schlüssel zu Bob gehört?
- In bisher vorgestellter Form kein Schutz vor Man-in-the-Middle-Angriffen
- $\rightsquigarrow$ PKI

Elliptische Kurven (1)

- Die Multiplikation über elliptischen Kurven ist genau so eine Funktion f, wie wir sie suchen.
- Elliptische Kurven können über verschiedenen Körpern definiert werden.

Elliptische Kurven(2)

- Elliptische Kurven über $\mathbb{R}$: Für Kryptographie unwichtig, für das Verständnis der Addition anschaulich.
- Elliptische Kurven über $\mathbb{Z}_p$: Für Kryptographie wichtig, Addition nicht anschaulich.

Elliptische Kurven über den reellen Zahlen: Definition

Definition

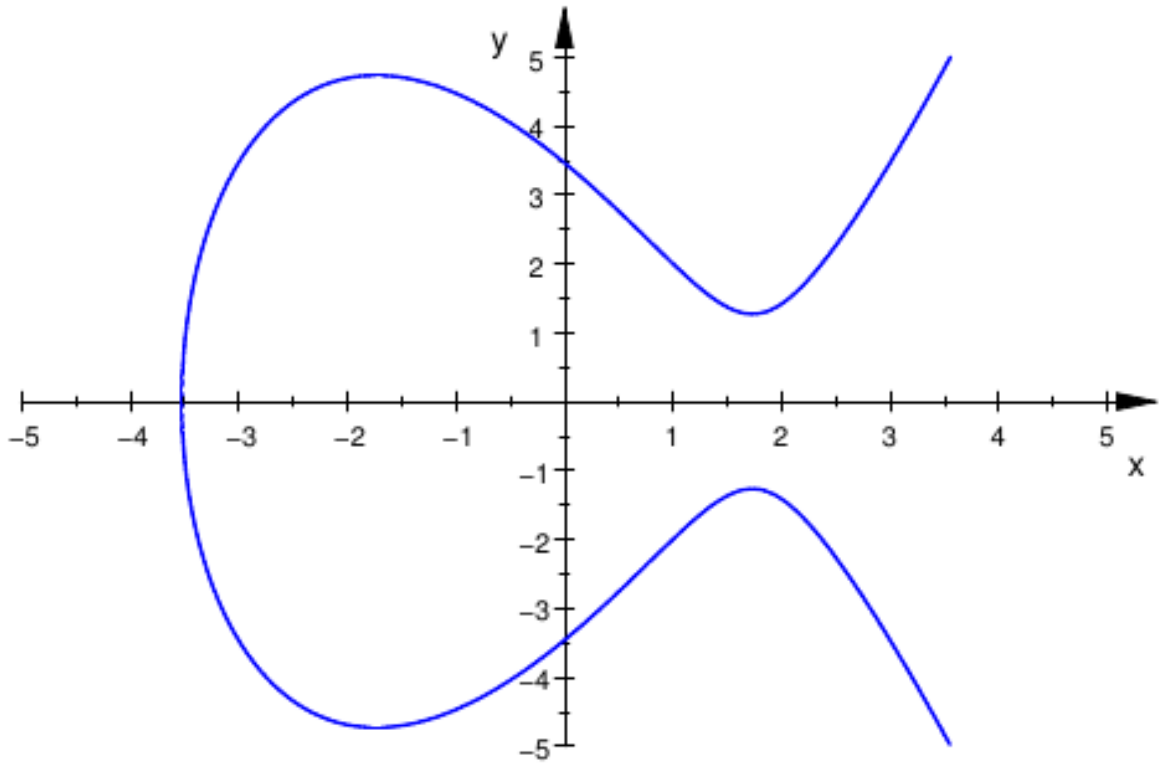
Seien $a, b \in \mathbb{R}$ *Konstanten, sodass gilt:* $4a^3 + 27b^2 \neq 0$. *Eine* **nicht-singuläre elliptische Kurve** *ist die Menge* E *der Lösungen* $(x, y) \in \mathbb{R} \times \mathbb{R}$ *der Gleichung*

$$y^2 = x^3 + ax + b$$

zusammen mit einem speziellen Punkt $\mathcal{O}$, *den man den* **Punkt im Unendlichen** *nennt.*

[3, S. 255]

Elliptische Kurven über den reellen Zahlen: Beispiel



Die elliptische Kurve $y^2 = x^3 - 9x + 12$ über $\mathbb{R}$.

Quelle: [2, S. 3]

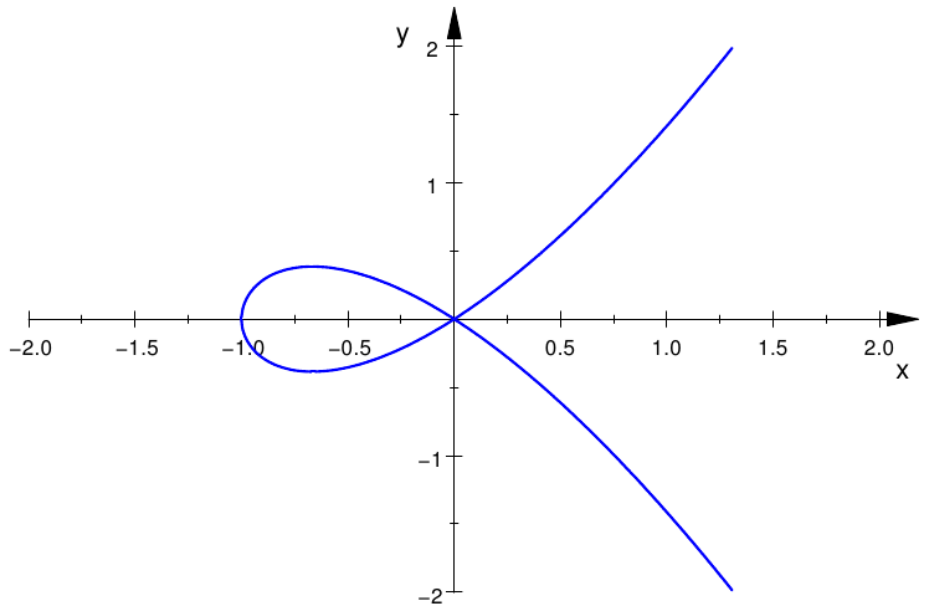
Elliptische Kurven über den reellen Zahlen: Nicht-Singularität (1)

- Ein Punkt auf einer elliptischen Kurve heißt **nicht-singulär**, wenn die Tangente des Punktes wohldefiniert ist.
- Eine elliptische Kurve ist nicht-singulär, wenn alle ihre Punkte nicht-singulär sind.

Elliptische Kurven über den reellen Zahlen: Nicht-Singularität (2)

- Nicht-Singularität ist notwendige Bedingung für die Punktverdopplung.
- Wenn eine elliptische Kurve die Bedingung $4a^3 + 27b^2 \neq 0$ erfüllt, ist sie nicht-singulär.

Elliptische Kurven über den reellen Zahlen: Nicht-Singularität (3)



Die elliptische Kurve $y^2 = x^3 + x^2$ über $\mathbb{R}$ als Beispiel für Singularität.

[2, S. 4]

Elliptische Kurven modulo einer Primzahl: Definition

Definition

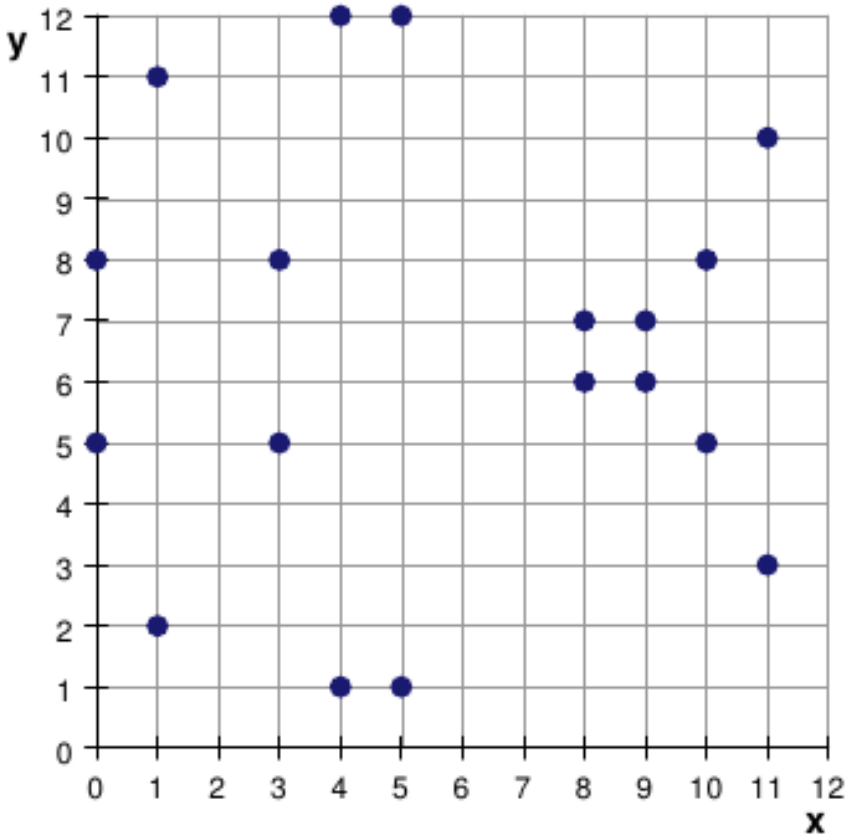
Sei $p > 3$ eine Primzahl. Die **elliptische Kurve** $y^2 = x^3 + ax + b$ *über $\mathbb{Z}_p$ ist die Menge der Lösungen $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ der Kongruenzgleichung*

$$y^2 \equiv x^3 + ax + b \ (mod\ p)$$

wobei $a, b \in \mathbb{Z}_p$ Konstanten sind, sodass $4a^3 + 27b^2 \not\equiv 0$ gilt, zusammen mit einem speziellen Punkt $\mathcal{O}$, den man den **Punkt im Unendlichen** *nennt.*

[3, S. 258]

Elliptische Kurven modulo einer Primzahl: Beispiel



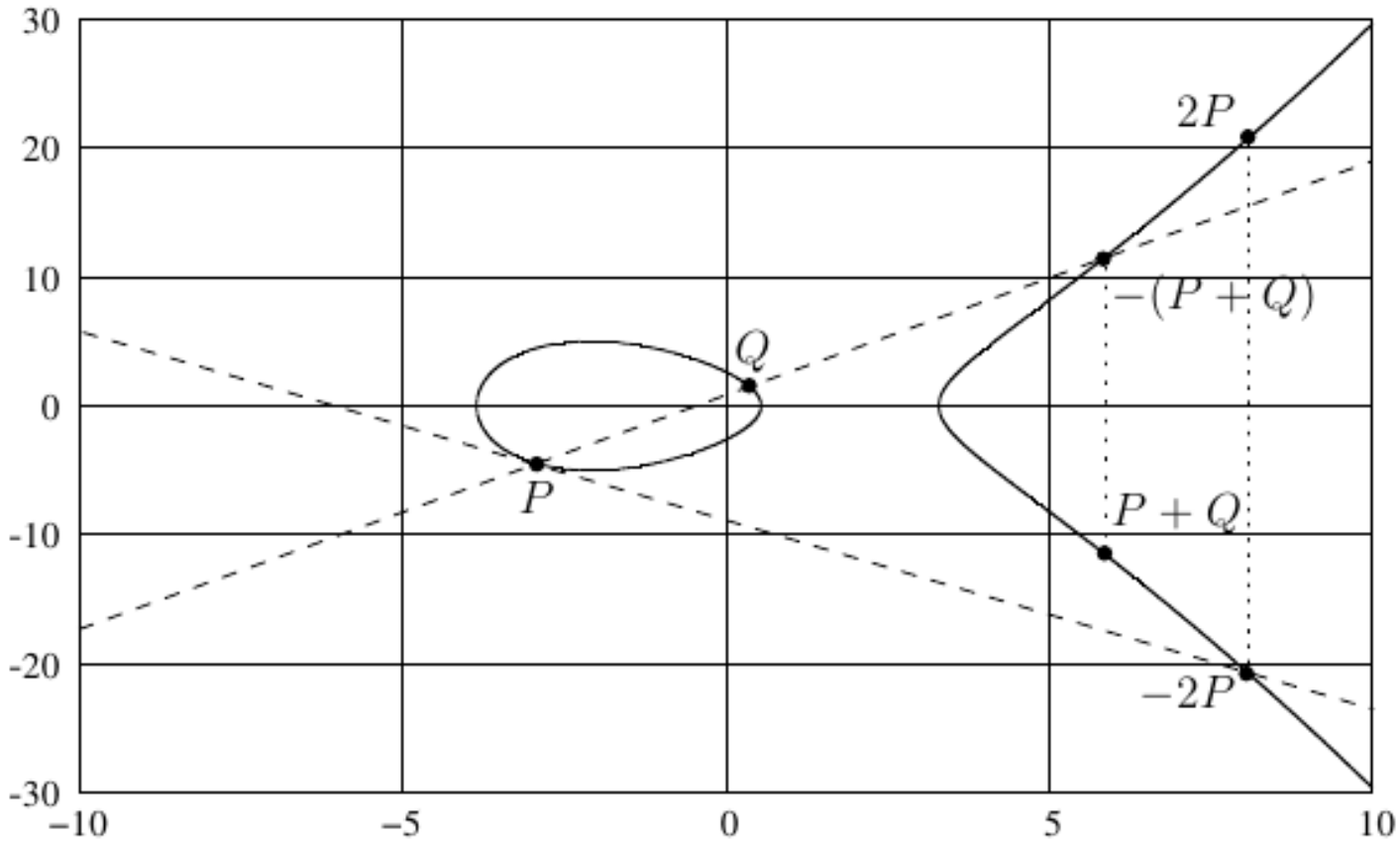
Die elliptische Kurve $y^2 = x^3 - 9x + 12$ über $\mathbb{Z}_{13}$.

Quelle: [2, S. 9]

Elliptische Kurven über den reellen Zahlen: Addition (1)

- Wir definieren: Wenn $S = (x_S, y_S)$, dann $-S := (x_S, -y_S)$.
- Wir unterscheiden 3 Fälle bei der Addition zweier beliebiger Punkte $P = (x_P, y_P)$ und $Q = (x_Q, y_Q)$:
  1. $x_P \neq x_Q$
  2. $x_P = x_Q$ und $y_P \neq y_Q$, also $P = -Q$.
  3. $P = Q$

Elliptische Kurven über den reellen Zahlen: Addition (2)



Fall 1 und 3 der Addition auf einer elliptischen Kurve über $\mathbb{R}$.

[1, S. 14]

Elliptische Kurven über den reellen Zahlen: Addition (3)

- **Fall 1**: Unwichtig für vorgestelltes Verfahren, aber anschauliche Berechnung der Formeln.
- **Fall 2**: Einfache Definition: $P + (-P) = \mathcal{O}$.
- **Fall 3**: Wichtig für vorgestelltes Verfahren, nicht so anschauliche Berechnung der Formeln wie in Fall 1.

Elliptische Kurven über den reellen Zahlen: Addition (4)

Wir betrachten Fall 1:

1. Bestimmung der Geraden $y = \lambda x + \nu$:
   - Steigung λ: $\lambda = \frac{y_Q - y_P}{x_Q - x_P}$
   - Schnittpunkt mit der y-Achse ν:
     $y_P = \lambda x_P + \nu \Leftrightarrow \nu = y_P - \lambda x_P$.

Elliptische Kurven über den reellen Zahlen: Addition (5)

Wir betrachten Fall 1:

2. Bestimmung der Schnittpunkte der Geraden und der elliptischen Kurve:
   - Einsetzen der Geradengleichung in die Gleichung der elliptischen Kurve: $(\lambda x + \nu)^2 = x^3 + ax + b$
   - Die Gerade und die elliptische Kurve haben 3 Schnittpunkte. Wir kennen bereits die Schnittpunkte P und Q. Über den Satz von Vieta kann man x_R nun wie folgt berechnen: $x_R = \lambda^2 - x_P - x_Q$.

Elliptische Kurven über den reellen Zahlen: Addition (5)

Wir betrachten Fall 1:

2. Bestimmung der Schnittpunkte der Geraden und der elliptischen Kurve:
   - Wir berechnen im Moment noch $-R = (x_R, -y_R)$.
   - Steigung λ kann durch beliebige zwei Punkte auf der elliptischen Kurve berechnet werden.
     $\lambda = \frac{-y_R - y_P}{x_R - x_P}$, und somit
     $y_R = -\lambda(x_R - x_P) - y_P = \lambda(x_P - x_R) - y_P$.

Elliptische Kurven über den reellen Zahlen: Addition (6)

Wir betrachten Fall 1:
Wir erhalten also folgende Formeln zur Berechnung von $P + Q = R$:

$$x_R = \lambda^2 - x_P - x_Q$$

$$y_R = \lambda(x_P - x_R) - y_P$$

$$\lambda = (y_Q - y_P) \cdot (x_Q - x_P)^{-1}$$

Elliptische Kurven über den reellen Zahlen: Addition (7)

Wir betrachten Fall 3 (**Punktverdopplung**):
Die Berechnungsformeln für Fall 3 ergeben sich analog zu Fall 1, nur dass die Steigung der Tangente anders berechnet wird als die der Geraden:

- Implizites Differenzieren der Gleichung $y_P^2 = x^3 + ax + b$ ergibt: $2y_P \frac{dy_P}{dx_P} = 3x_P^2 + a$. Umstellen nach $\lambda = \frac{dy_P}{dx_P}$ liefert: $\lambda = \frac{3x_P^2+a}{2y_P} = (3x_P^2 + a) \cdot (2y_P)^{-1}$.

Elliptische Kurven über den reellen Zahlen: Addition (8)

Wir betrachten Fall 3 (**Punktverdopplung**):
Wir erhalten also folgende Formeln zur Berechnung von $P + P = R$:

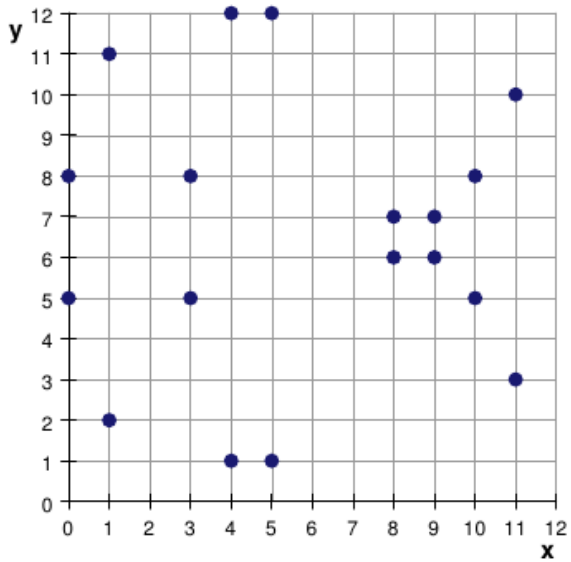
$$x_R = \lambda^2 - x_P - x_P$$

$$y_R = \lambda(x_P - x_R) - y_P$$

$$\lambda = (3x_P^2 + a) \cdot (2y_P)^{-1}$$

Elliptische Kurven modulo einer Primzahl: Addition (1)

Die Berechnungsformeln können von den elliptischen Kurven über den reellen Zahlen übernommen werden.



Die elliptische Kurve $y^2 = x^3 - 9x + 12$ über $\mathbb{Z}_{13}$.

Quelle: [2, S. 9]

Elliptische Kurven modulo einer Primzahl: Addition (2)

Beispiel für Fall 3 (**Punktverdopplung**): Verdopplung des Punkts (3,5):

$\lambda = (3x_P^2+a)\cdot(2y_P)^{-1} = (3\cdot 3^2-9)\cdot(2\cdot 5)^{-1} = (1-9)\cdot 10^{-1} = 5\cdot 10^{-1}$
$= 5 \cdot 4 = 7 \pmod{13}$

$$x_R = \lambda^2 - x_P - x_P = 7^2 - 2 \cdot 3 = 10 - 6 = 4 \pmod{13}$$

$$y_R = \lambda(x_P - x_R) - y_P = 7(3 - 4) - 5 = 1 \pmod{13}$$

ECDLP (1)

Das Problem des diskreten Logarithmus auf elliptischen Kurven ist wie folgt definiert:

Definition

Gegeben sei ein Punkt $P \in E$ der Ordnung n (d.h., die von ihm erzeugte zyklische Untergruppe hat die Größe n). Wir wollen zu einem Punkt Q in der von P erzeugten zyklischen Untergruppe diejenige Zahl k mit $kP = Q$ bestimmen.

Dieses Problem ist mit heutiger Technik und heutigem Kenntnisstand nicht effizient lösbar. [4, S. 75]

ECDLP (2)

- Naiver Ansatz: Einfach k Additionen von P auf P ausführen und jedes Mal überprüfen, ob das Ergebnis gleich Q ist. Das ist die „Brute-Force“-Methode, die zu lange dauert, also nicht effizient ist.
- Wie kann dann aber der legitime Nutzer, der k kennt, Q effizient berechnen?

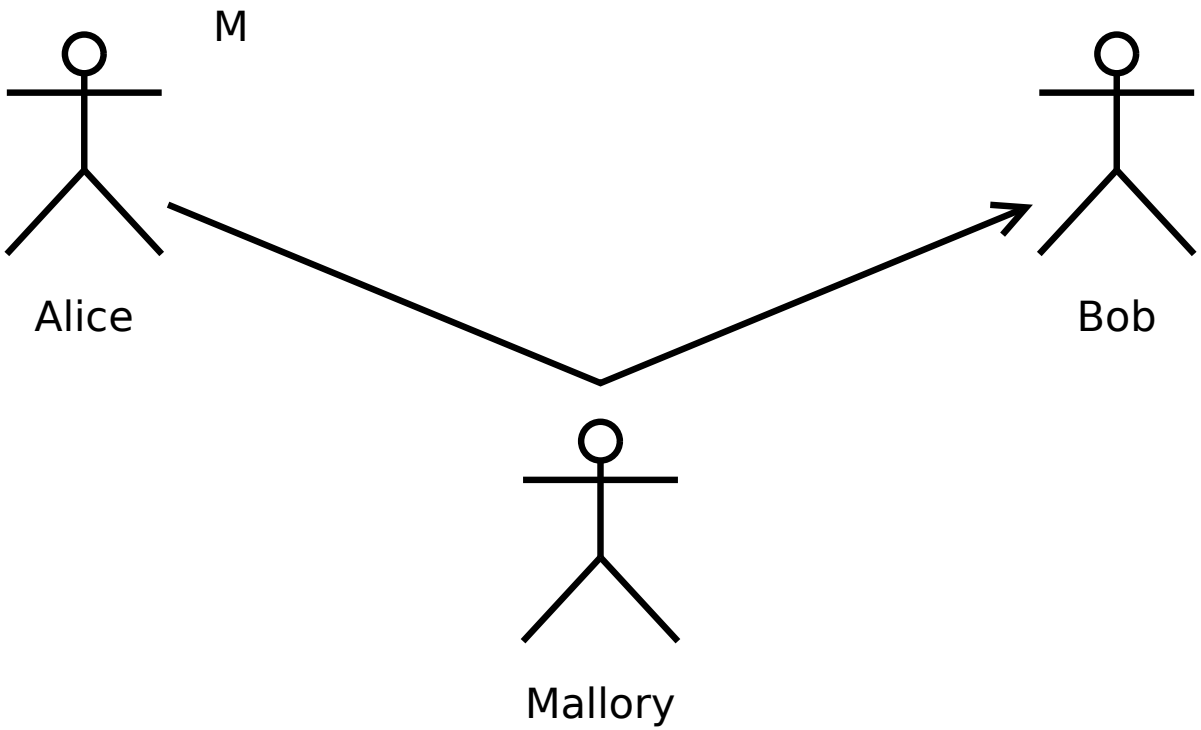
ECDLP (3)

- Idee: Wir schreiben k in Binärdarstellung $[b_z b_{z-1} ... b_2 b_1 b_0]$. Wir berechnen $2^z \cdot P$ indem wir $2 \cdot P$ berechnen, das Ergebnis speichern und wieder verdoppeln (also $2 \cdot (2 \cdot P)$), dieses Ergebnis speichern und wieder verdoppeln usw., bis wir z Verdopplungen durchgeführt haben.
- Das ist in $log_2 k$ Punktverdopplungen möglich. Eine Punktverdopplung ist in $\mathcal{O}((log_2 n)^2)$ möglich, wobei n die Anzahl der Bits ist, die benötigt werden, um P zu kodieren.

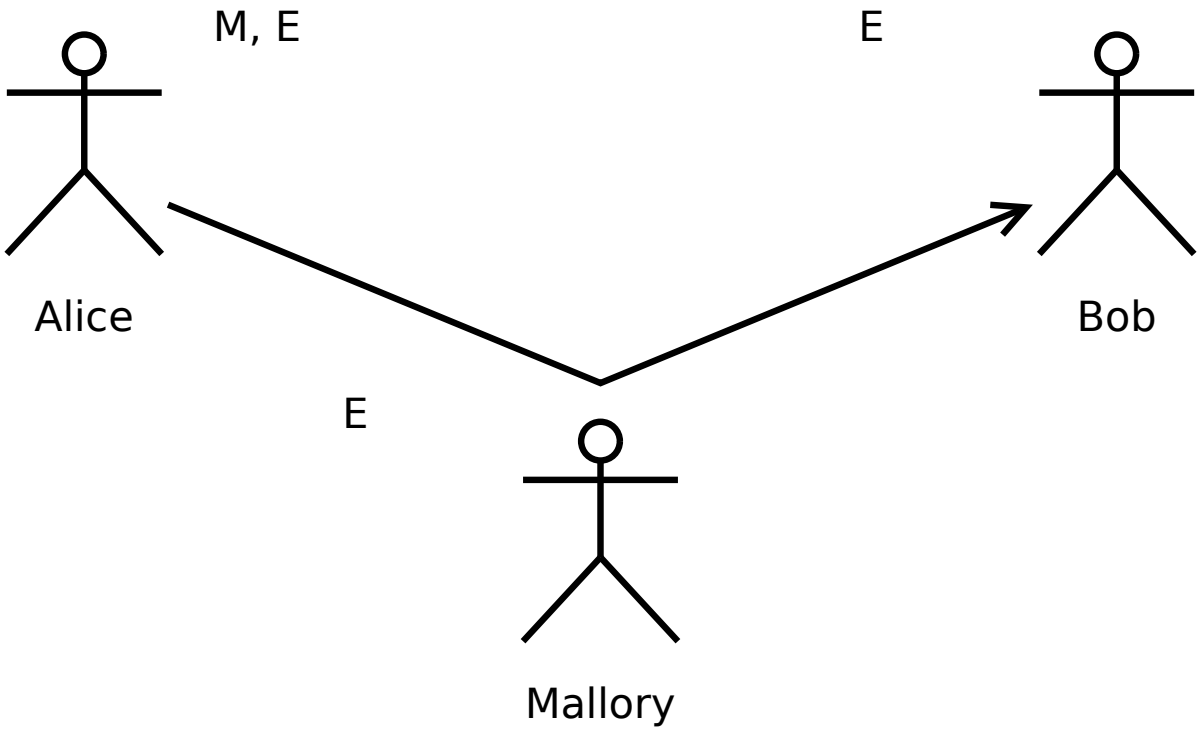
ECDLP (4)

- Wir müssen jetzt noch alle Zwischenergebnisse addieren: $kP = \sum_{i=0}^{z} b_i \cdot (2^i \cdot P)$.
- Komplexität insgesamt: $\mathcal{O}(log_2 k \cdot (log_2 n)^2)$.

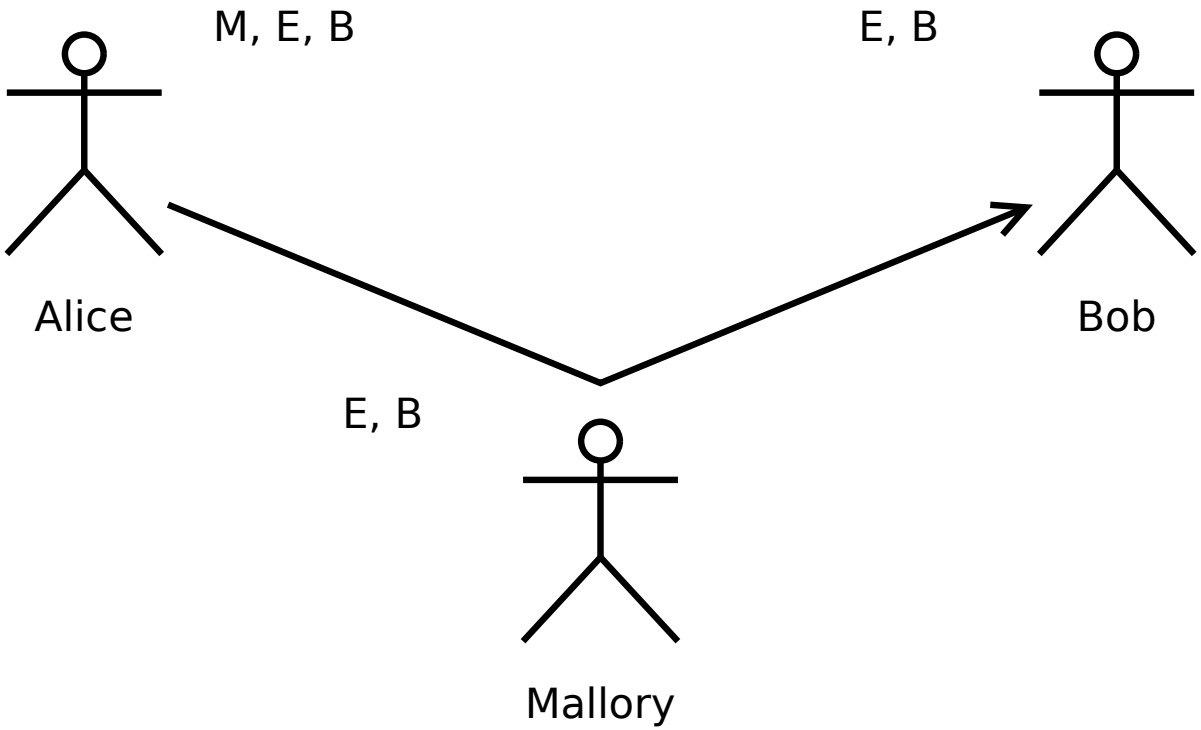
Beispiel einer ECC-verschlüsselten Kommunikation (1)



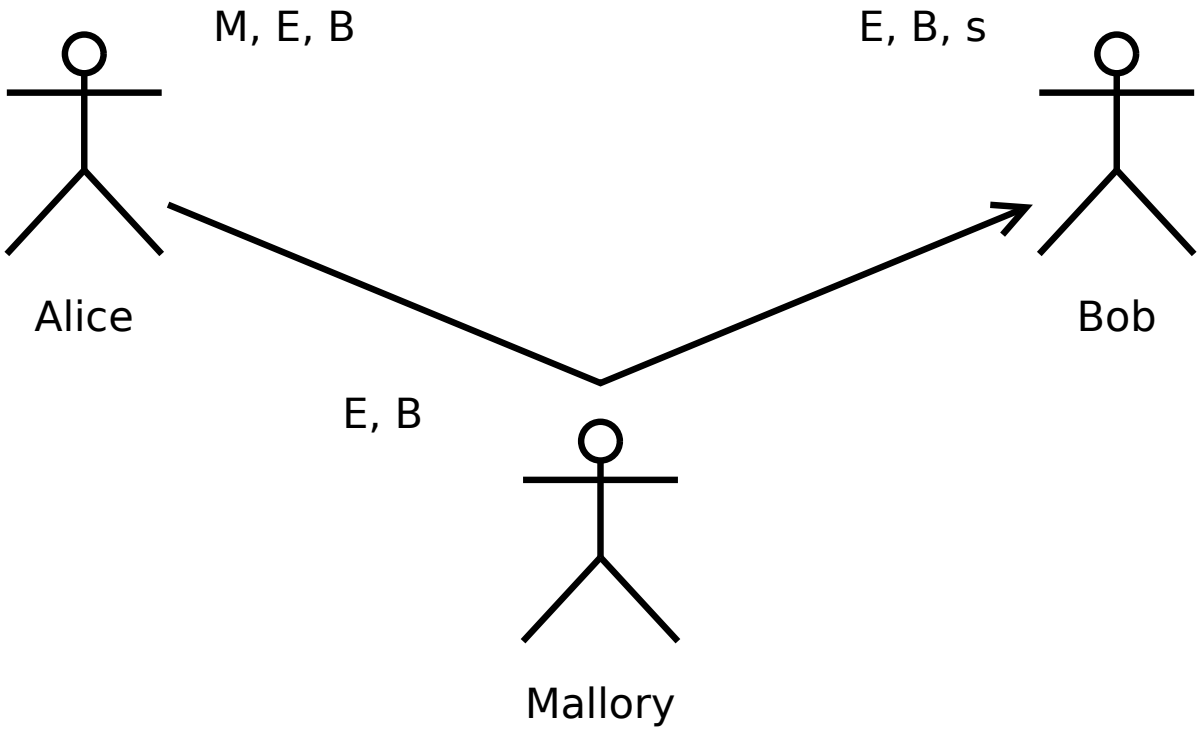
Beispiel einer ECC-verschlüsselten Kommunikation (2)



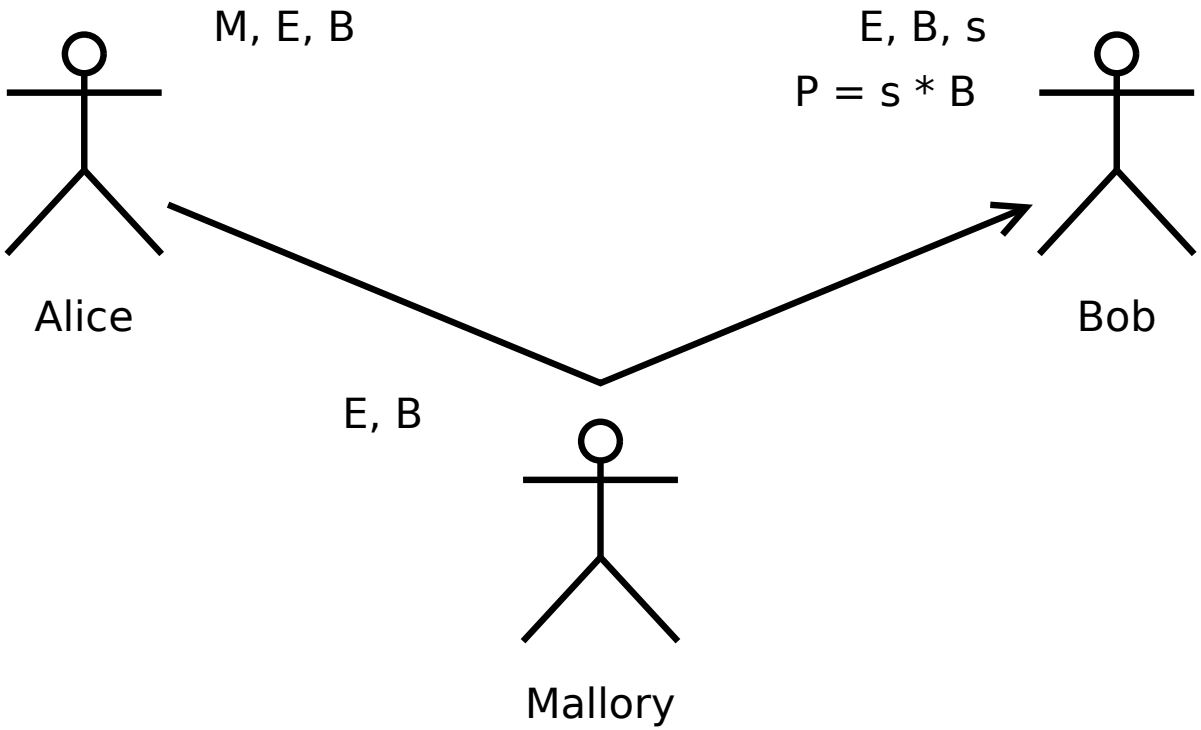
Beispiel einer ECC-verschlüsselten Kommunikation (3)



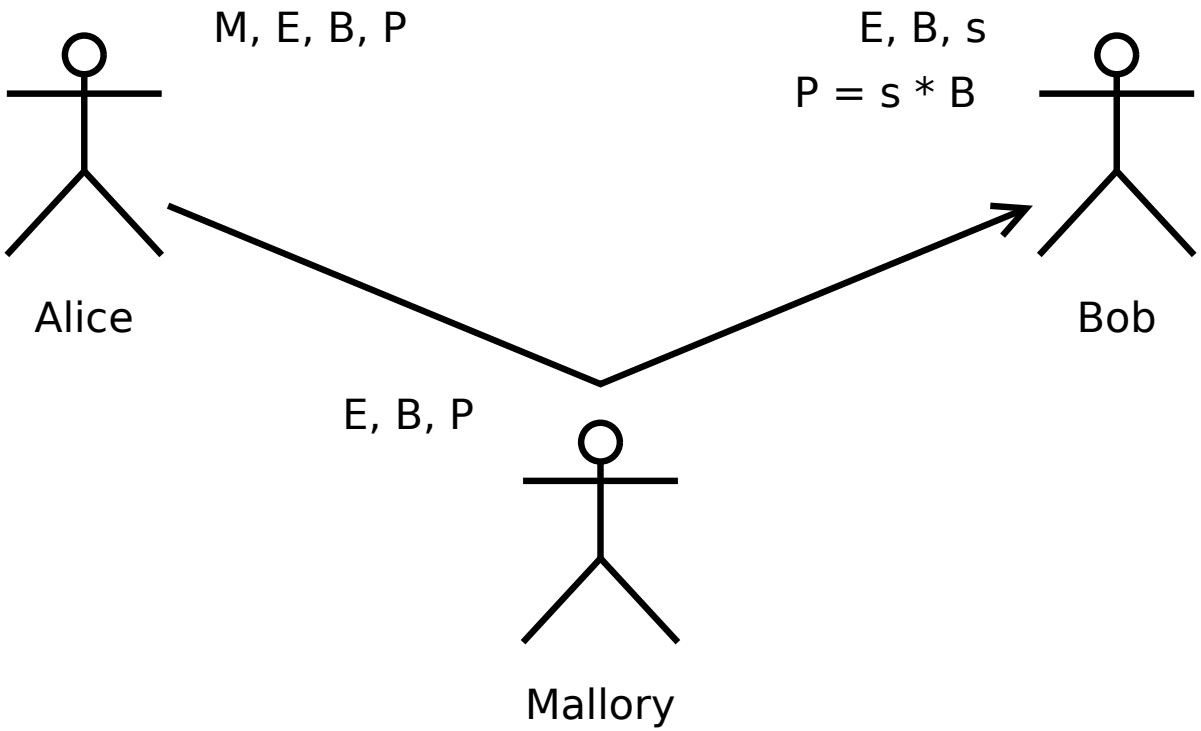
Beispiel einer ECC-verschlüsselten Kommunikation (4)



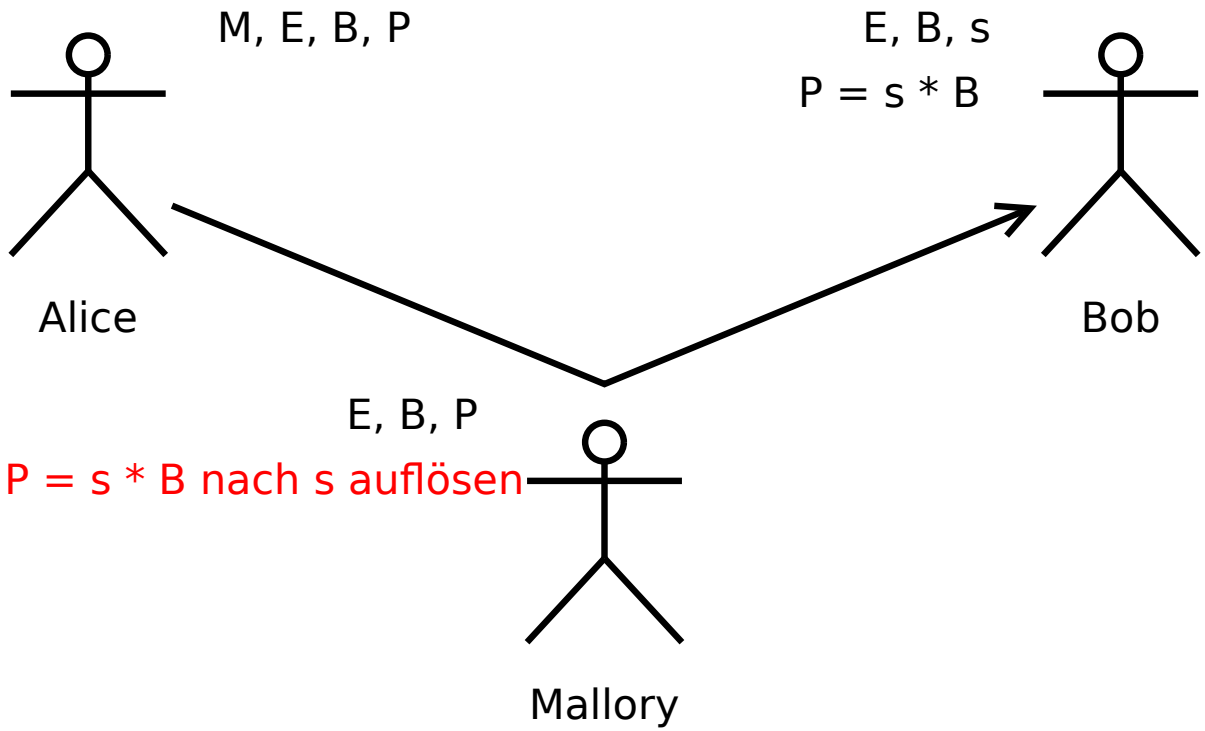
Beispiel einer ECC-verschlüsselten Kommunikation (5)



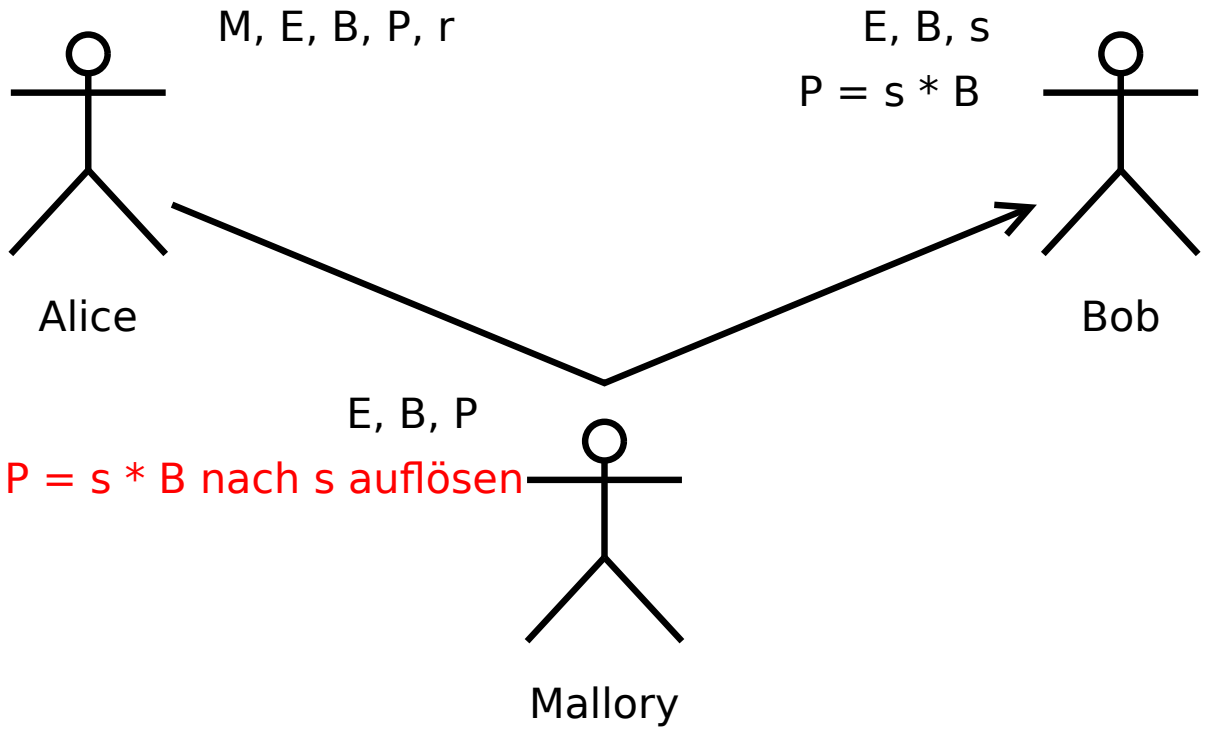
Beispiel einer ECC-verschlüsselten Kommunikation (6)



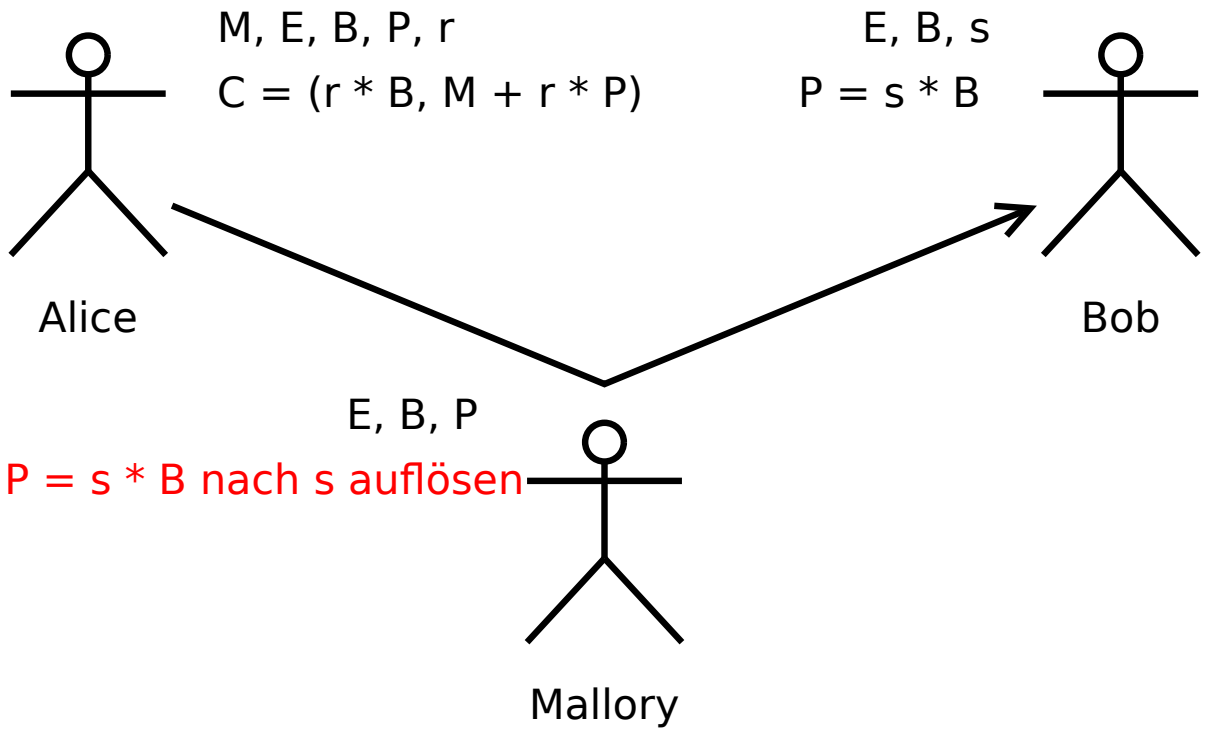
Beispiel einer ECC-verschlüsselten Kommunikation (7)



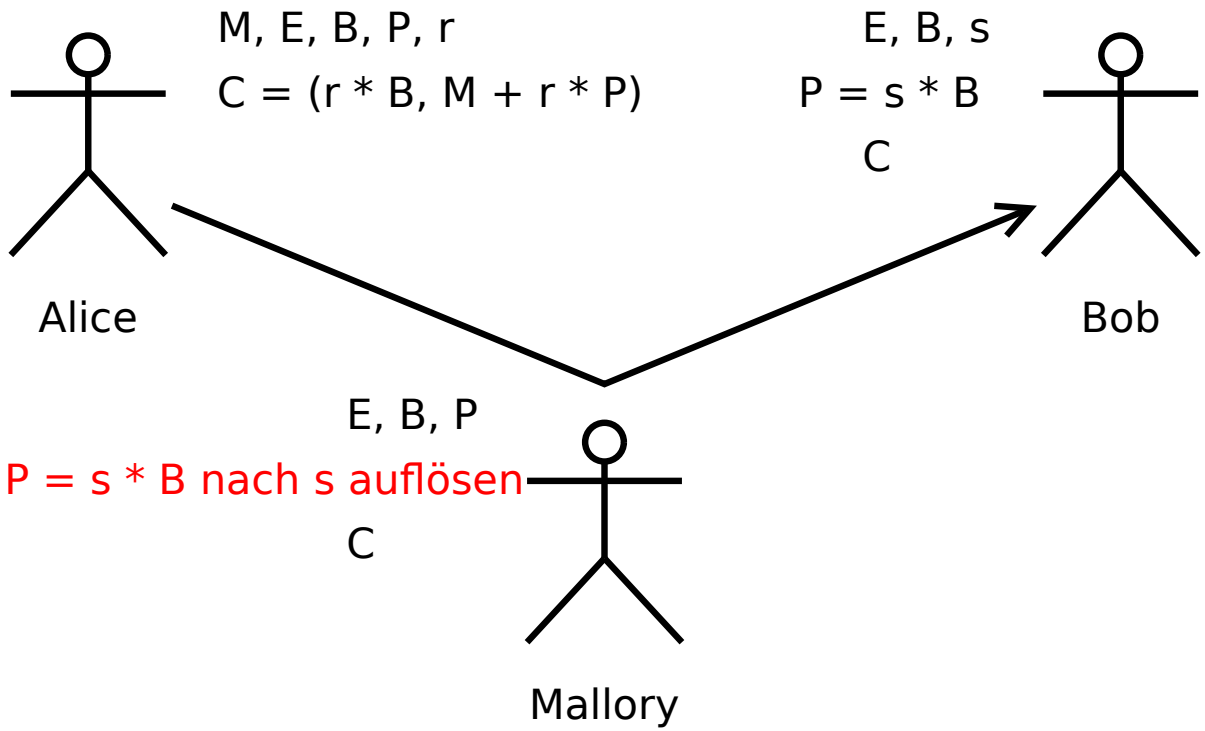
Beispiel einer ECC-verschlüsselten Kommunikation (8)



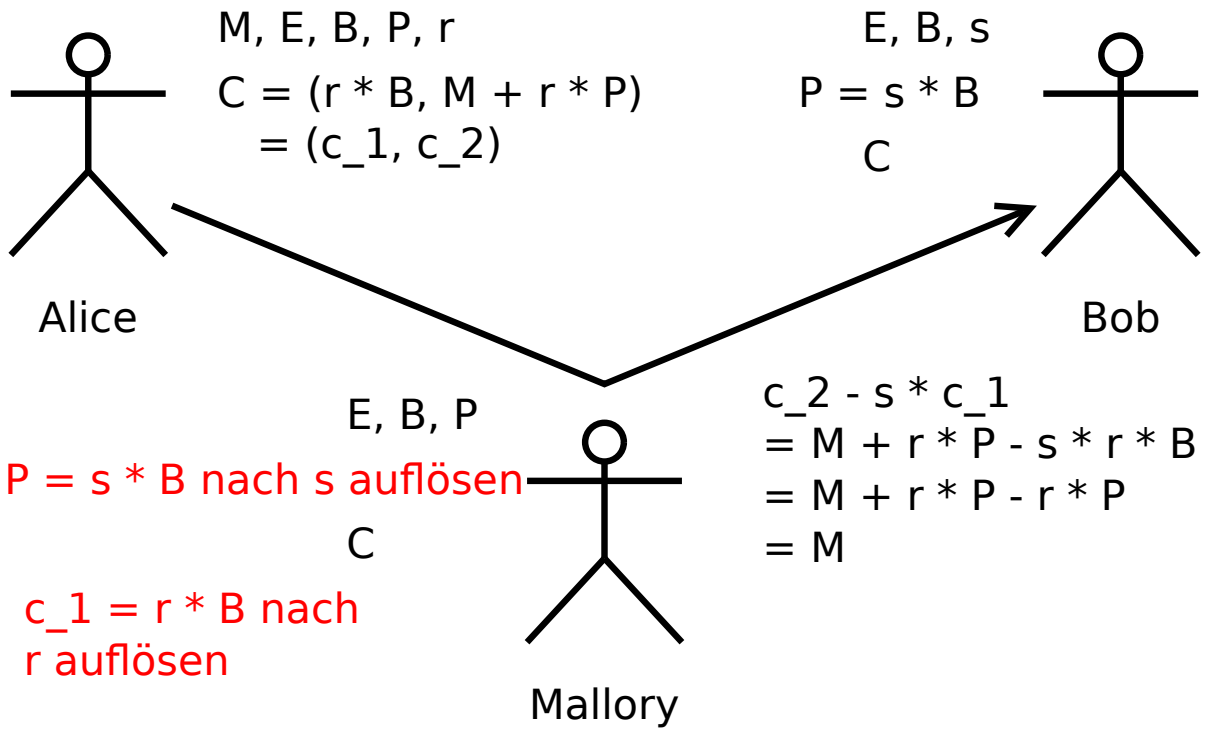
Beispiel einer ECC-verschlüsselten Kommunikation (9)



Beispiel einer ECC-verschlüsselten Kommunikation (10)



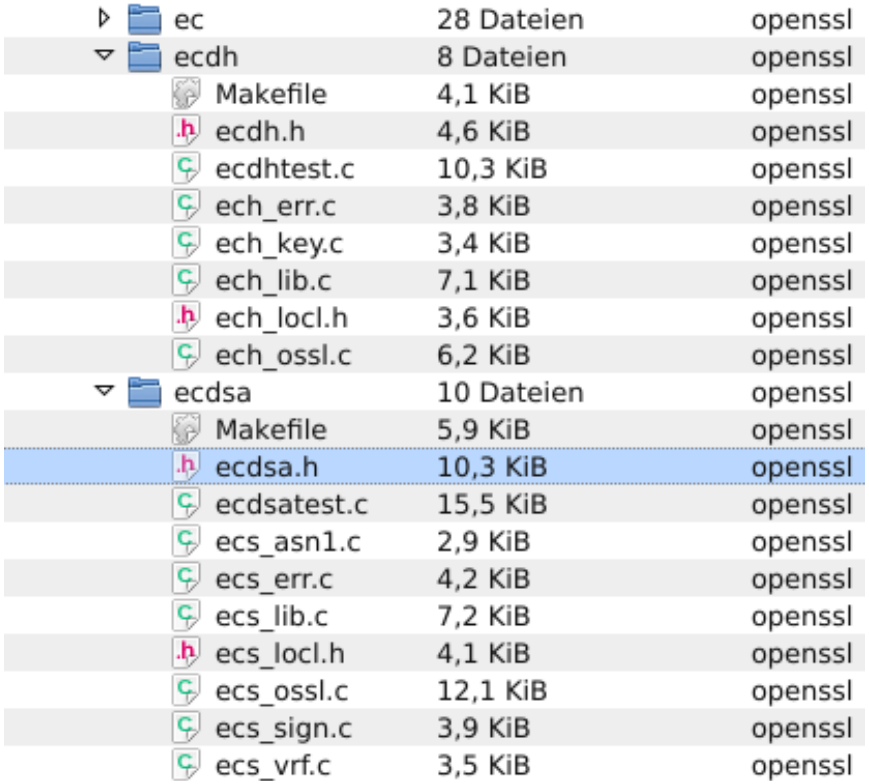
Beispiel einer ECC-verschlüsselten Kommunikation (11)



Anwendungen von ECC

- Elliptic-Curve-Diffie-Hellman (ECDH): Schlüsselaustauschprotokoll, dessen Sicherheit auf ECDLP basiert.
- Elliptic-Curve-Digital-Signature-Algorithm (ECDSA): Algorithmus zum Erstellen von digitalen Signaturen.

ECC in Krypto-Bibliotheken (1)



ec	28 Dateien	openssl
ecdh	8 Dateien	openssl
Makefile	4,1 KiB	openssl
ecdh.h	4,6 KiB	openssl
ecdhtest.c	10,3 KiB	openssl
ech_err.c	3,8 KiB	openssl
ech_key.c	3,4 KiB	openssl
ech_lib.c	7,1 KiB	openssl
ech_locl.h	3,6 KiB	openssl
ech_ossl.c	6,2 KiB	openssl
ecdsa	10 Dateien	openssl
Makefile	5,9 KiB	openssl
ecdsa.h	10,3 KiB	openssl
ecdsatest.c	15,5 KiB	openssl
ecs_asn1.c	2,9 KiB	openssl
ecs_err.c	4,2 KiB	openssl
ecs_lib.c	7,2 KiB	openssl
ecs_locl.h	4,1 KiB	openssl
ecs_ossl.c	12,1 KiB	openssl
ecs_sign.c	3,9 KiB	openssl
ecs_vrf.c	3,5 KiB	openssl

- OpenSSL: ECDSA z.B. seit 2005 implementiert. ECDH ist auch implementiert und kann genutzt werden.

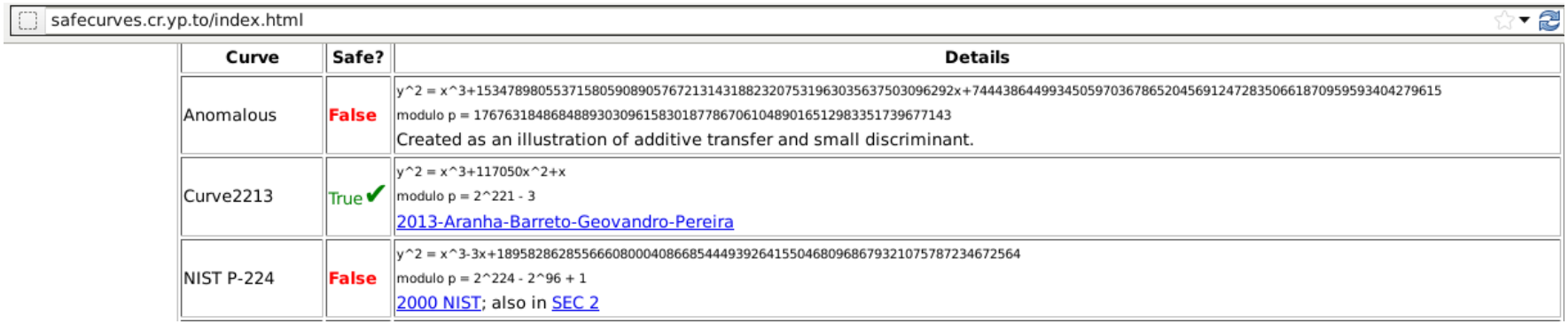
ECC in Krypto-Bibliotheken (2)

- OpenSSH: ECDSA und ECDH seit Januar 2011 implementiert.

Vorteil von ECC

Symmetric KL	Standard asymmetric KL	Elliptic Curve KL
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

Woher kommen die Kurven? (1)


safecurves.cr.yp.to/index.html

Curve	Safe?	Details
Anomalous	False	y^2 = x^3+153478980553715805908905767213143188232075319630356375030962 92x+744438644993450597036786520456912472835066187095959340427961 5 modulo p = 1767631848684889303096158301877867061048901651298335173967714 3 Created as an illustration of additive transfer and small discriminant.
Curve2213	True ✔	y^2 = x^3+117050x^2+x modulo p = 2^221 - 3 2013-Aranha-Barreto-Geovandro-Pereira
NIST P-224	False	y^2 = x^3-3x+18958286285566608000408668544493926415504680968679321075787234672564 modulo p = 2^224 - 2^96 + 1 2000 NIST; also in SEC 2

- Selber oder zufällig erstellte Kurven meist nicht sicher, daher ist es besser, Standards zu benutzen.

Woher kommen die Kurven? (2)

- Mit Hilfe bestimmter Kriterien kann beurteilt werden, wie sicher eine Kurve ist.
- Eine solche Liste von Kriterien gibt z.B. die BSI heraus.

Zusammenfassung

- Man kann asymmetrische Kryptographie mit Hilfe von elliptischen Kurven betreiben.
- Das Verfahren basiert auf Addition bzw. Multiplikation auf ECs.
- Multiplikation kP effizient berechenbar.
- Umkehrung der Multiplikation ist das ECDLP, nicht effizient berechenbar.
- ECC braucht deutlich kürzere Schlüssel im Vergleich zu RSA.
- ECC wird in ECDH und ECDSA verwendet.
- Beide Verfahren z.B. in OpenSSL implementiert, stehen zur Verwendung zur Verfügung.

Quellenangaben I

Bundesamt für Sicherheit in der Informationstechnik.
Technical guideline tr-03111: Elliptic curve cryptography.
Website, 2012.
Online verfügbar auf:
https://www.bsi.bund.de/cae/servlet/contentblob
/471398/publicationFile/30615/BSI-TR-03111_pdf.pdf.

Björn Mühlenfeld.
Einführung in elliptische kurven.
Website, Januar 2006.
Online verfügbar auf:
http://www2.cs.uni-paderborn.de/cs/ag-bloemer/lehre
/proseminar_WS2005/material/Muehlenfeld_Ausarbeitung.pdf.

Quellenangaben II

Douglas R. Stinson.
Cryptography: Theory and praxis, volume 3.
Chapman & Hall/CRC, 2006.

Annette Werner.
Elliptische Kurven in der Kryptographie.
Springer, 2002.