Komplexitätsabschätzung von hardwareakzelerierten Attacken auf ECC-Kryptoverfahren

Markus Böttger

Übersicht

1. Kryptographie
2. Mathematische Grundlagen der elliptischen Kurven
3. Kryptosysteme mittels elliptischer Kurven
4. Angriffsstrategien auf ein ECC
5. Implementierungen der gewählten Strategie
6. Ergebnisse

Übersicht

1. Kryptographie
2. Mathematische Grundlagen der elliptischen Kurven
3. Kryptosysteme mittels elliptischer Kurven
4. Angriffsstrategien auf ein ECC
5. Implementierungen der gewählten Strategie
6. Ergebnisse

1. Kryptographie

Verschlüsselung von Nachrichten (E-Mail)

Verschlüsselung von Datenbeständen (HDD-Partition)

Verschlüsselung von Wertinformationen (Telefonkarte)

Identifikation von Gegenständen (Preisschild im Einzelhandel)

Authentifikation (Wegfahrsperre)

Die Enigma

Das RSA-Verfahren (Rivest Shamir Adleman)

Falltürfunktion: Integer Faktorisierungsproblem (IFP)

„Es ist schwer, zwei große Primzahlen p und q aus der Kenntnis des Produktes $n = p \cdot q$ zurückzugewinnnen.“

Wähle Primzahlen p und q. $n = p \cdot q$. $\varphi(n) = (p\text{-}1)\cdot(q\text{-}1)$.

Wähle c mit $ggT(c, \varphi(n)) = 1$, $1 < c < n$.

Bestimme $d \in \mathbb{N}$, so daß $c \cdot d = 1 \bmod \varphi(n)$.

Verschlüsselung: $E(w) = w^c \bmod n$

Entschlüsselung: $D(w) = w^d \bmod n$

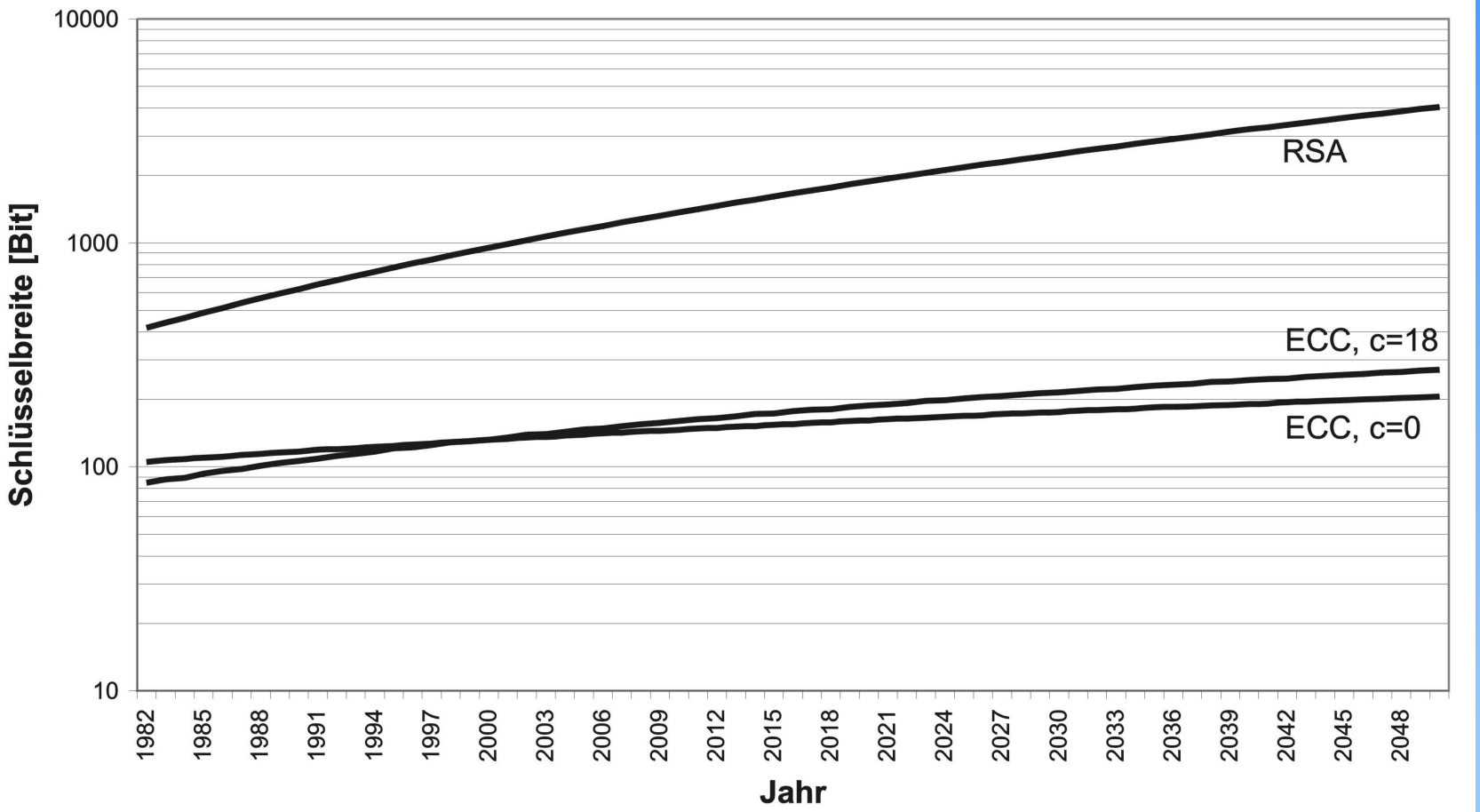
Das ECC-Verfahren (Elliptic Curve Cryptosystem):

Falltürfunktion: Problem des diskreten Logarithmus (DLP)

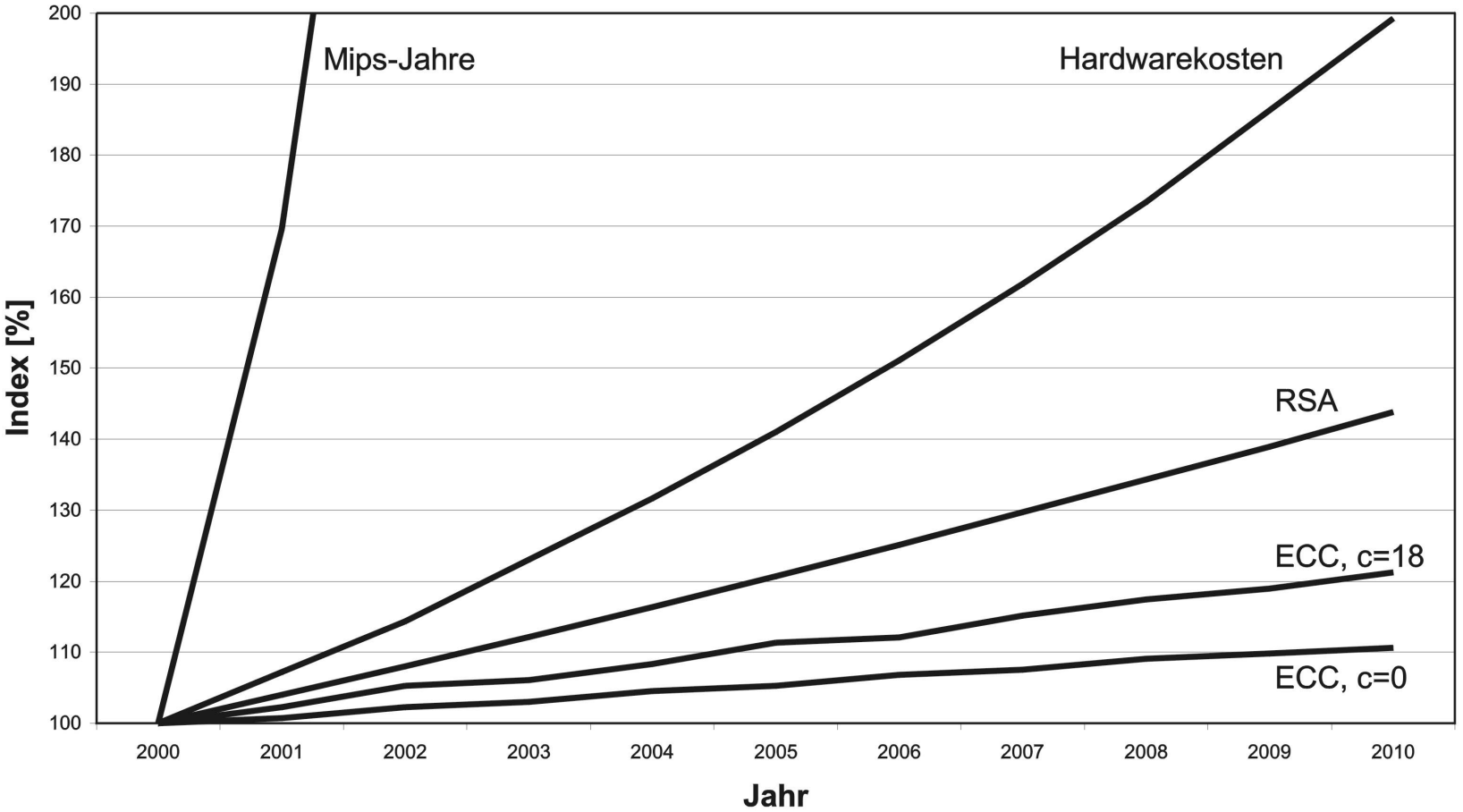
„Gegeben p, g und y, bestimme k so, daß

$y = g^k \bmod p$ gilt.“

Schlüssellängenvergleich zwischen RSA und ECC



Entwicklung der Schlüssellängen bis 2010



Übersicht

1. Kryptographie
2. Mathematische Grundlagen der elliptischen Kurven
3. Kryptosysteme mittels elliptischer Kurven
4. Angriffsstrategien auf ein ECC
5. Implementierungen der gewählten Strategie
6. Ergebnisse

2. Mathematische Grundlagen der ECC

Betrachtung findet über einem endlichen Körper GF(p^q) statt, mit *p*: Charakteristik und *q*: Erweiterungsgrad.

Beispiel:
Körper GF(13) mit a = 5 und b = 9:

Addition	5 + 9 = 14, 14 mod 13 = 1
Subtraktion	5 – 9 = - 4, - 4 mod 13 = 9
Multiplikation	5 · 9 = 45, 45 mod 13 = 6
Division	$5 / 9 = 5 \cdot 9^{-1} = 5 \cdot 3 = 15$, 15 mod 13 = 2

Die Berechnung des Inversen

Division: $5 / 9 = 5 \cdot 9^{-1} = 5 \cdot 3 = 15,\ 15 \bmod 13 = 2$

Berechnung von 9^{-1}:

$$y \cdot y^{-1} = 1 \bmod p \quad \Rightarrow \quad 9 \cdot 9^{-1} = 1 \bmod 13$$
$$\Leftrightarrow \quad 9 \cdot 3 = 1 \bmod 13$$

Der Aufwand zur Berechnung der Inversion ist $O(p)$!

Gleichungen von Elliptischen Kurven

allgemeine Weierstraß-Gleichung:

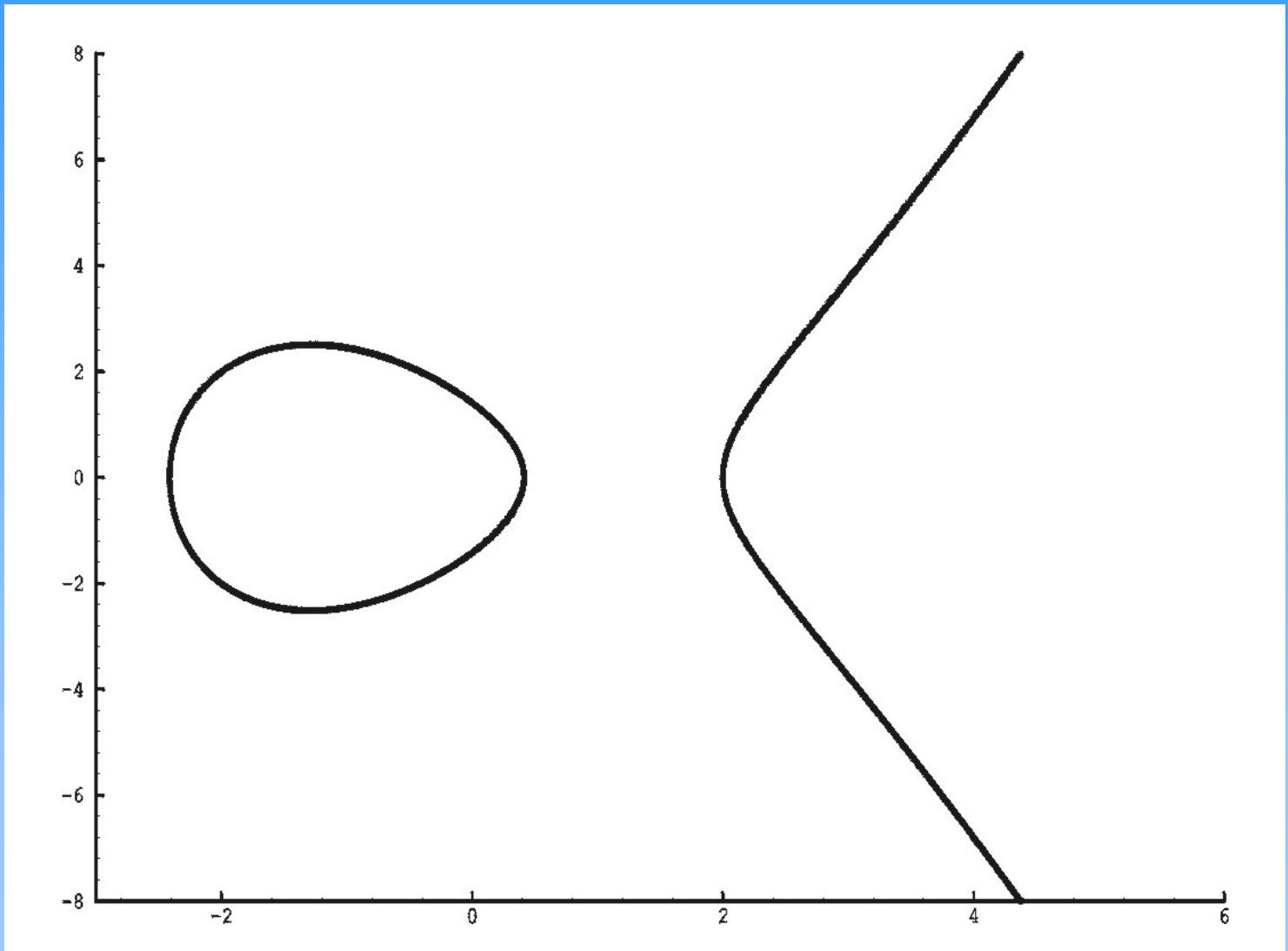
$$y^2 + a_1xy + a_2y = x^3 + a_3x^2 + a_4x + a_5 \text{ ,mit } x, y, a_i \in K$$

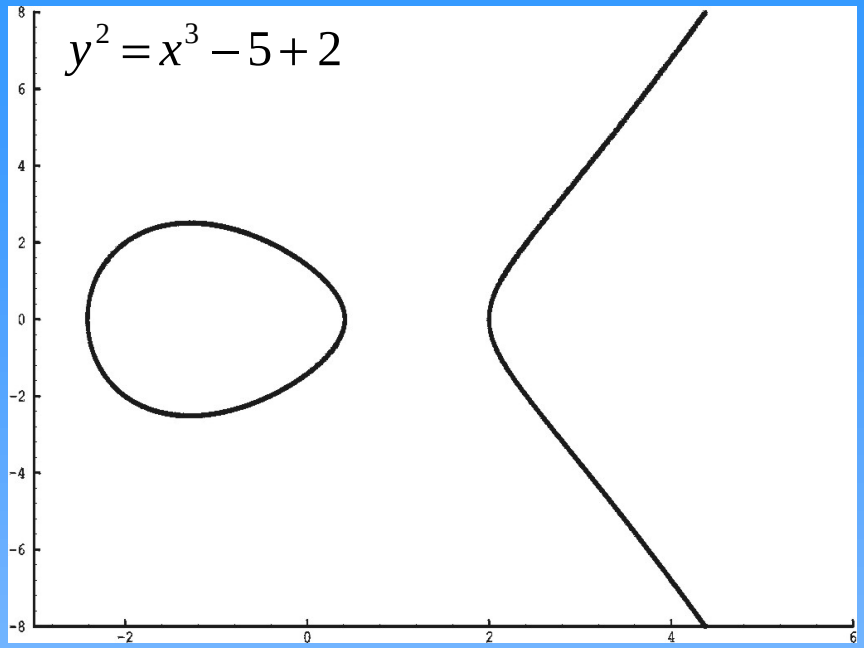
Vereinfachung für EC über R:

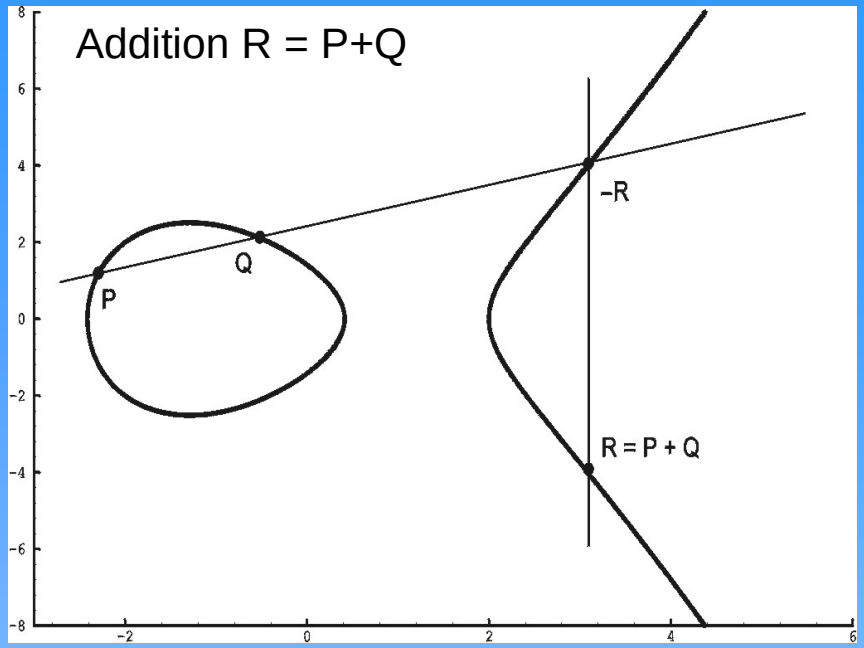
$$y^2 = x^3 + ax + b \text{,mit } x, y, a, b \in R$$

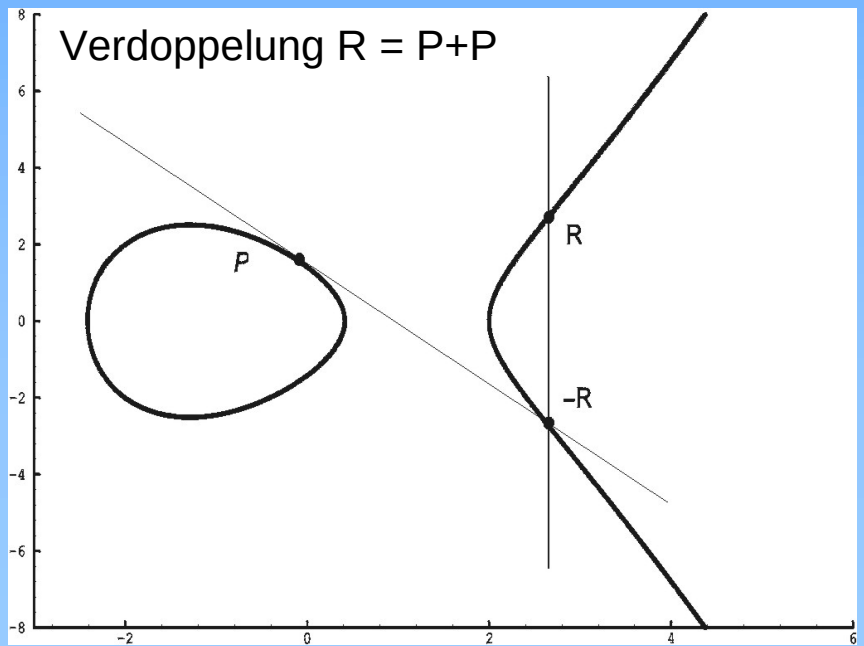
Beispiel über R:

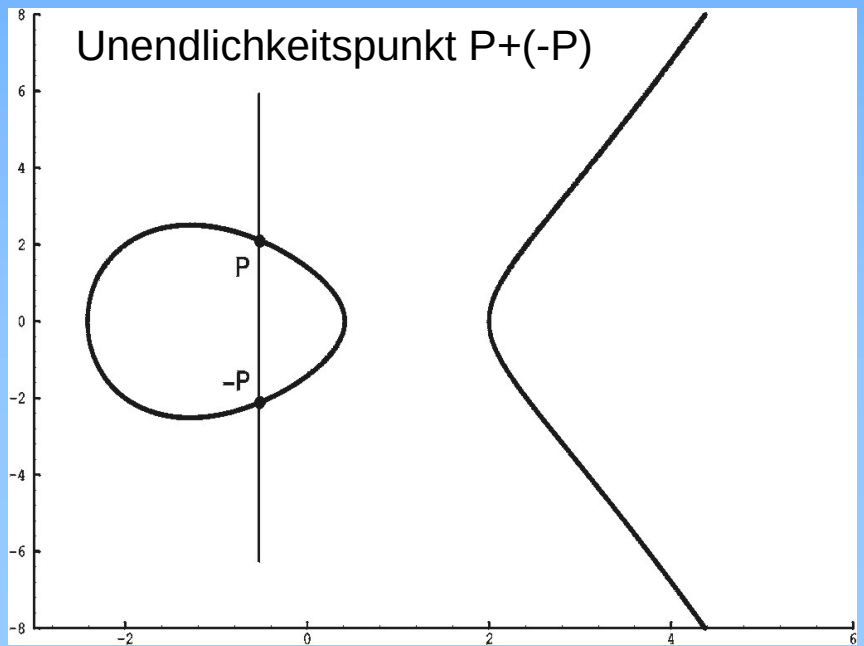
$y^2 = x^3 + ax + b$ mit $a = -5,\ b = 2$




$y^2 = x^3 - 5 + 2$


Addition R = P+Q
P
Q
-R
R = P + Q


Verdoppelung R = P+P
P
R
-R


Unendlichkeitspunkt P+(-P)
P
-P

Gleichungen von Elliptischen Kurven

allgemeine Weierstraß-Gleichung:

$$y^2 + a_1xy + a_2y = x^3 + a_3x^2 + a_4x + a_5 \text{ ,mit } x, y, a_i \in K$$

Vereinfachung für EC über R:

$$y^2 = x^3 + ax + b \text{,mit } x, y, a, b \in R$$

Vereinfachung für EC über GF(2^m):

$$y^2 + xy = x^3 + ax^2 + b \text{, mit } b \neq 0,\ a, b, x, y \in K$$

Beispiel: Körperelemente des GF(2^3):

Interpretation als Polynom	Interpretation als Dualzahl
0	0
1	1
x	1 0
$x + 1$	1 1
x^2	1 0 0
$x^2 + 1$	1 0 1
$x^2 + x$	1 1 0
$x^2 + x + 1$	1 1 1

Beispiel:

Verknüpfungen im Körper GF(2^3) mit Primpolynom (x^3+x+1)

Addition	$(x^2+x)+(x^2+1)=x+1$
Subtraktion	identisch zur Addition
Multiplikation	$(x^2+x)\cdot(x^2+1)=$ $(x^4+x^3+x^2+x)\bmod(x^3+x+1)=(x+1)$
Division	...

Die Kurvenordnung

nach dem Theorem von Hasse hat eine Kurve über GF(2^m) näherungsweise 2^m Kurvenpunkte.

Die Anzahl der Kurvenpunkte zzgl. des Unendlichkeitspunktes wird Kurvenordnung genannt und mit #E bezeichnet.

Die projektive Punktdarstellung

bisher: affine Darstellung: $P = (x,y)$

jetzt: projektive Darstellung: $P = (X,Y,Z)$

mit $(X,Y,Z) = (\lambda^2 X, \lambda^3 Y, \lambda Z)$, $\forall \lambda \neq 0$, $\lambda \in K$

Umrechnung:

projektiv $\rightarrow$ affin: $(x,y,1)$, mit $x = \frac{X}{Z^2}, y = \frac{Y}{Z^3}$

affin $\rightarrow$ projektiv: $X \leftarrow x$, $Y \leftarrow y$, $Z \leftarrow 1$

Verdoppelung eines Punktes:

Affin	Projektiv
$2(x_1, y_1) = (x_2, y_2)$, mit	$2(X_1, Y_1, Z_1) = (X_2, Y_2, Z_2)$, mit
$\theta = x_1 + \frac{y_1}{x_1}$	$Z_2 = X_1 Z_1^2$
	$X_2 = (X_1 + cZ_1^2)^4$
$x_2 = \theta^2 + \theta + a$	$U = Z_2 + X_1^2 + Y_1 Z_1$
$y_2 = x_1^2 + (\theta + 1)x_2$	$Y_2 = X_1^4 Z_2 + UX_2$

dargelegte Vorteile:

- Betrachtung von Kurven über GF(2^m):

  schnelle, hardwarenahe Implementierung möglich

- Verwendung der projektiven Punktdarstellung:

  keine Berechnung des Inversen nötig

Übersicht

1. Kryptographie
2. Mathematische Grundlagen der elliptischen Kurven
3. Kryptosysteme mittels elliptischer Kurven
4. Angriffsstrategien auf ein ECC
5. Implementierungen der gewählten Strategie
6. Ergebnisse

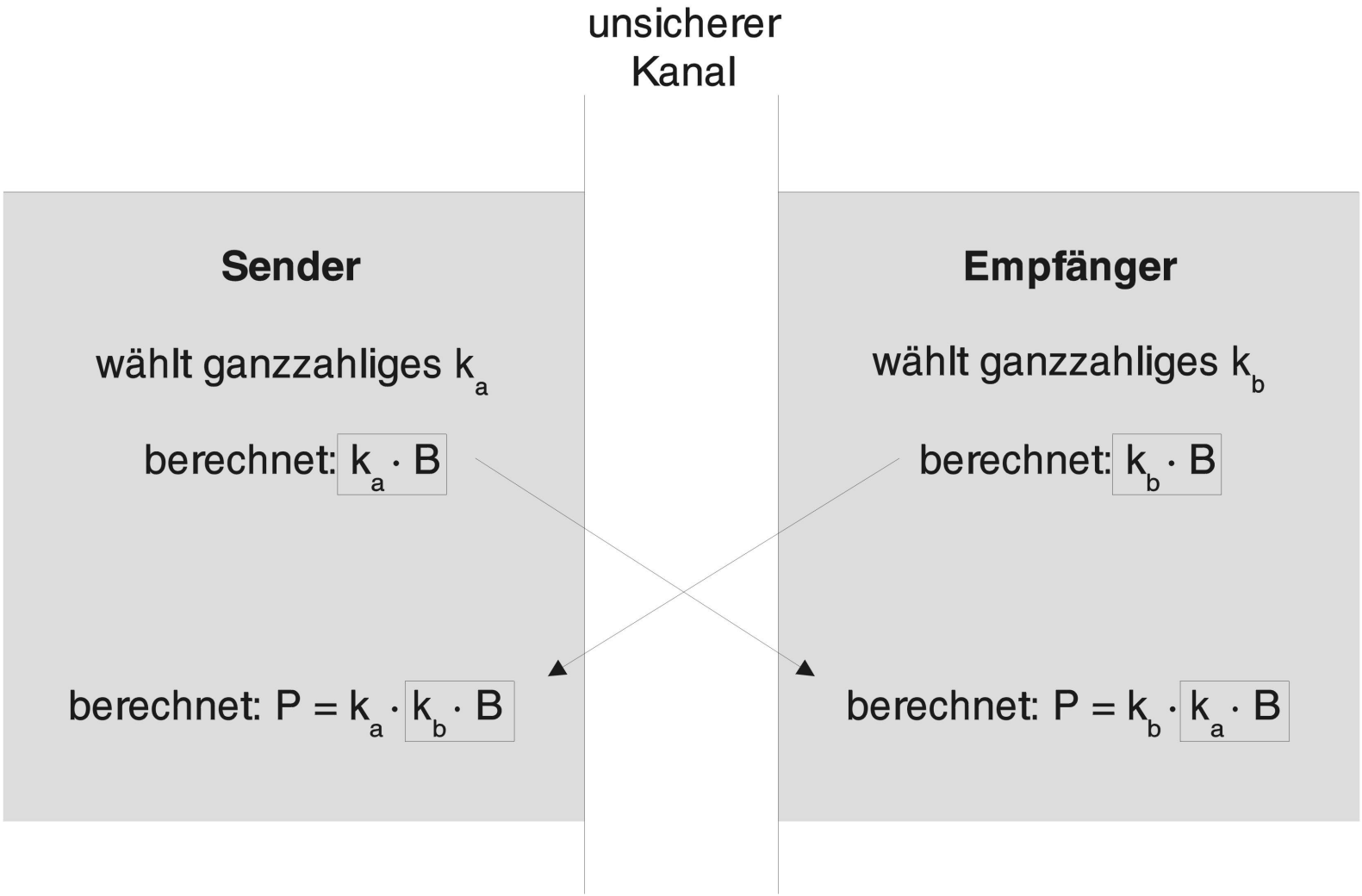
3. Kryptosysteme mittels elliptischer Kurven

- Die Diffie-Hellmann-Schlüsselvereinbarung
- Das ElGamal-Verfahren

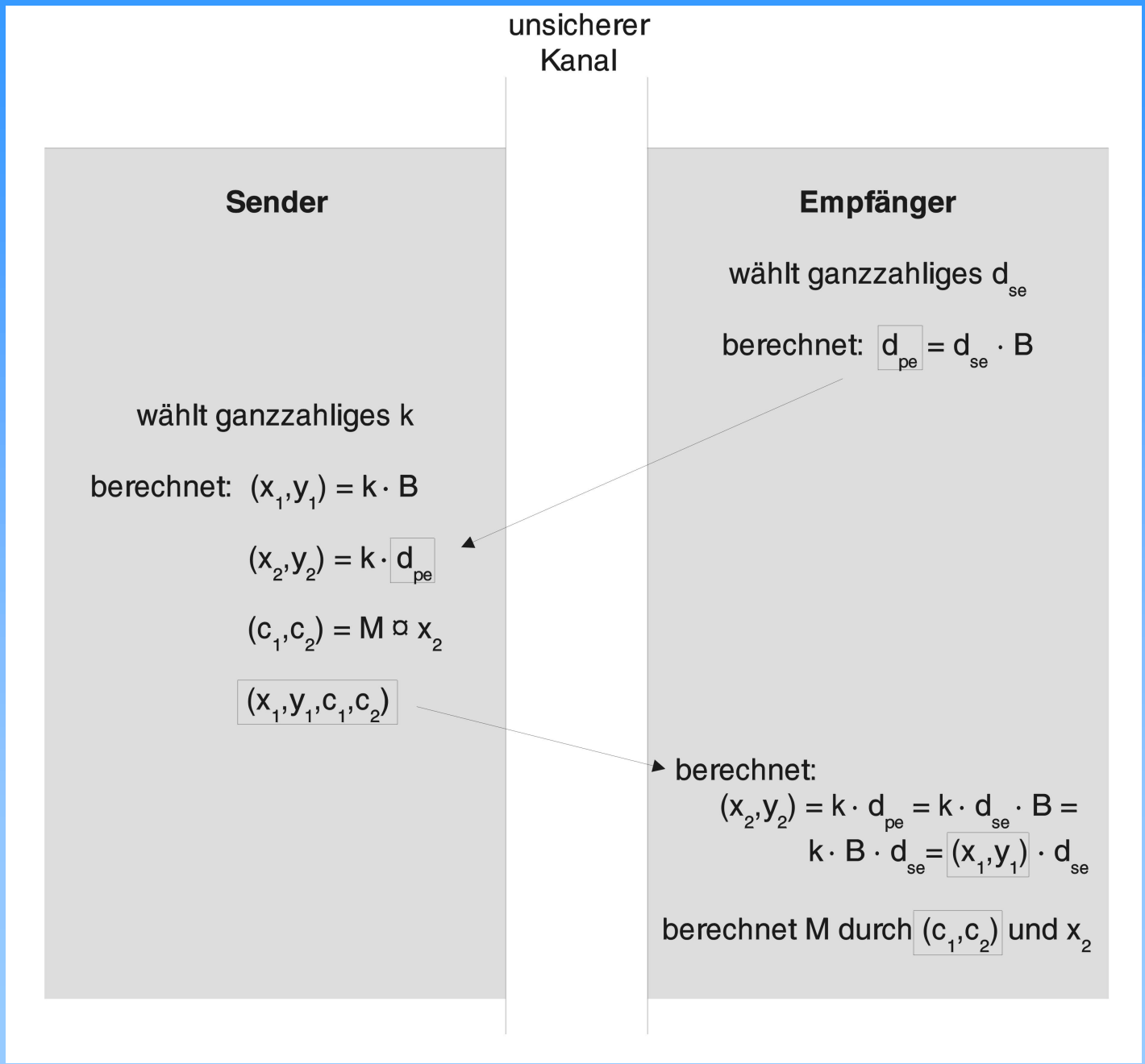
Öffentliche Parameter:

- Kurvenparameter *a* und *b* der Gleichung $y^2 + xy = x^3 + ax^2 + b$
- Primpolynom
- Basispunkt B

Die Diffie-Hellmann-Schlüsselvereinbarung:



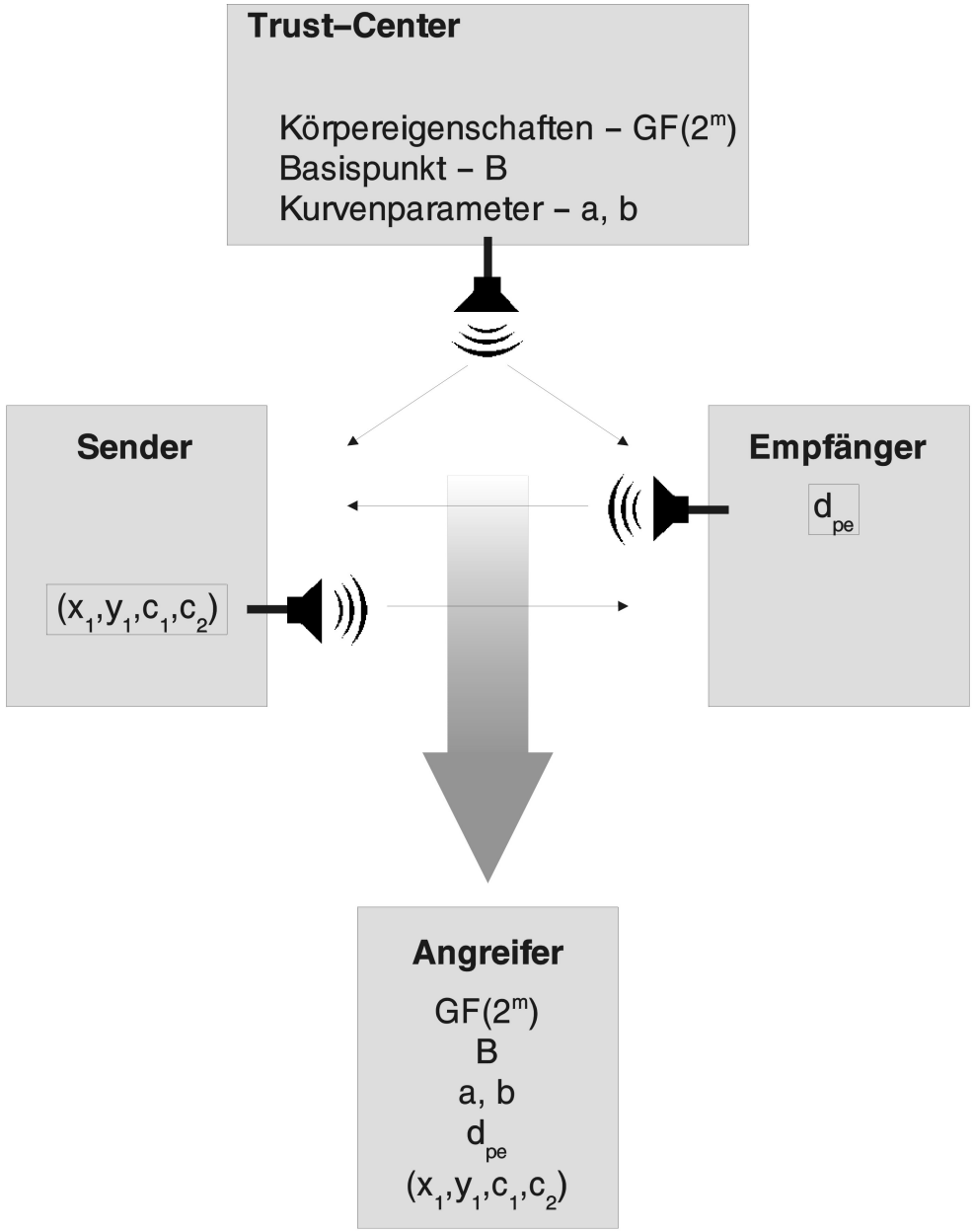
Das ElGamal-Verfahren:



Übersicht

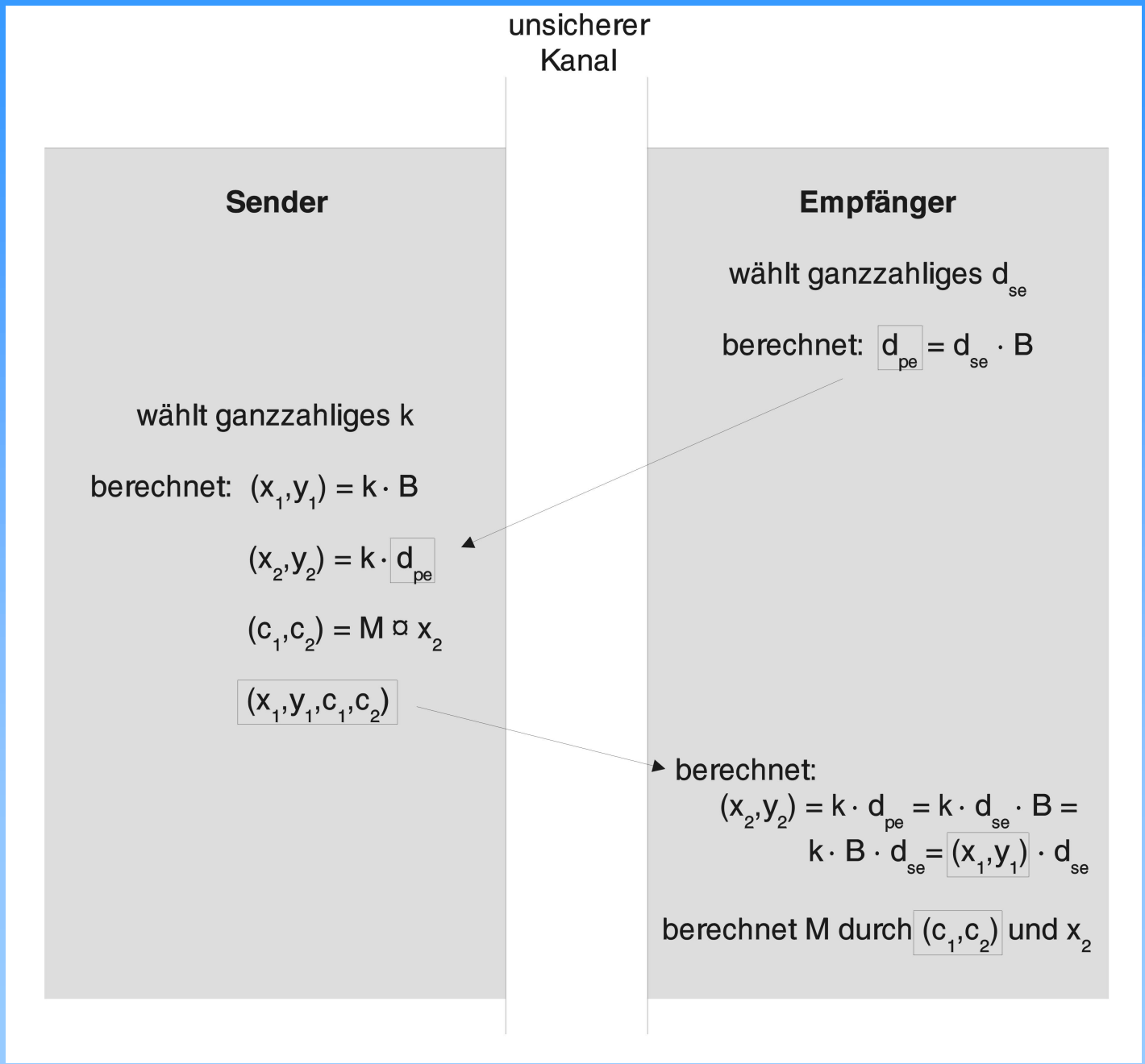
1. Kryptographie
2. Mathematische Grundlagen der elliptischen Kurven
3. Kryptosysteme mittels elliptischer Kurven
4. Angriffsstrategien auf ein ECC
5. Implementierungen der gewählten Strategie
6. Ergebnisse

Die Informationen eines Angreifers:



Das

ElGamal-Verfahren:



Strategien zur Lösung von $P = k \cdot B$

- Pollard-Rho
- Pollard-Lambda
- sukzessive Addition
- sukzessive Verdoppelung

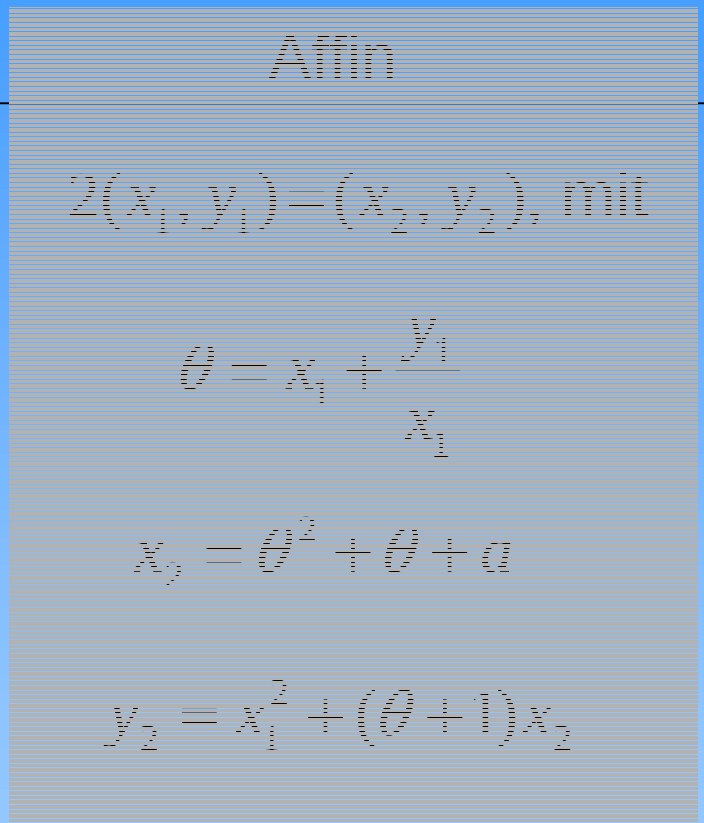
Übersicht

1. Kryptographie
2. Mathematische Grundlagen der elliptischen Kurven
3. Kryptosysteme mittels elliptischer Kurven
4. Angriffsstrategien auf ein ECC
5. Implementierungen der gewählten Strategie
6. Ergebnisse

5. Implementierungen der gewählten Strategie

- Verhaltensbeschreibung in C++
- Hardwarebeschreibung in VHDL

Verdoppelung eines Punktes:



Projektiv

$2(X_1, Y_1, Z_1) = (X_2, Y_2, Z_2)$, mit

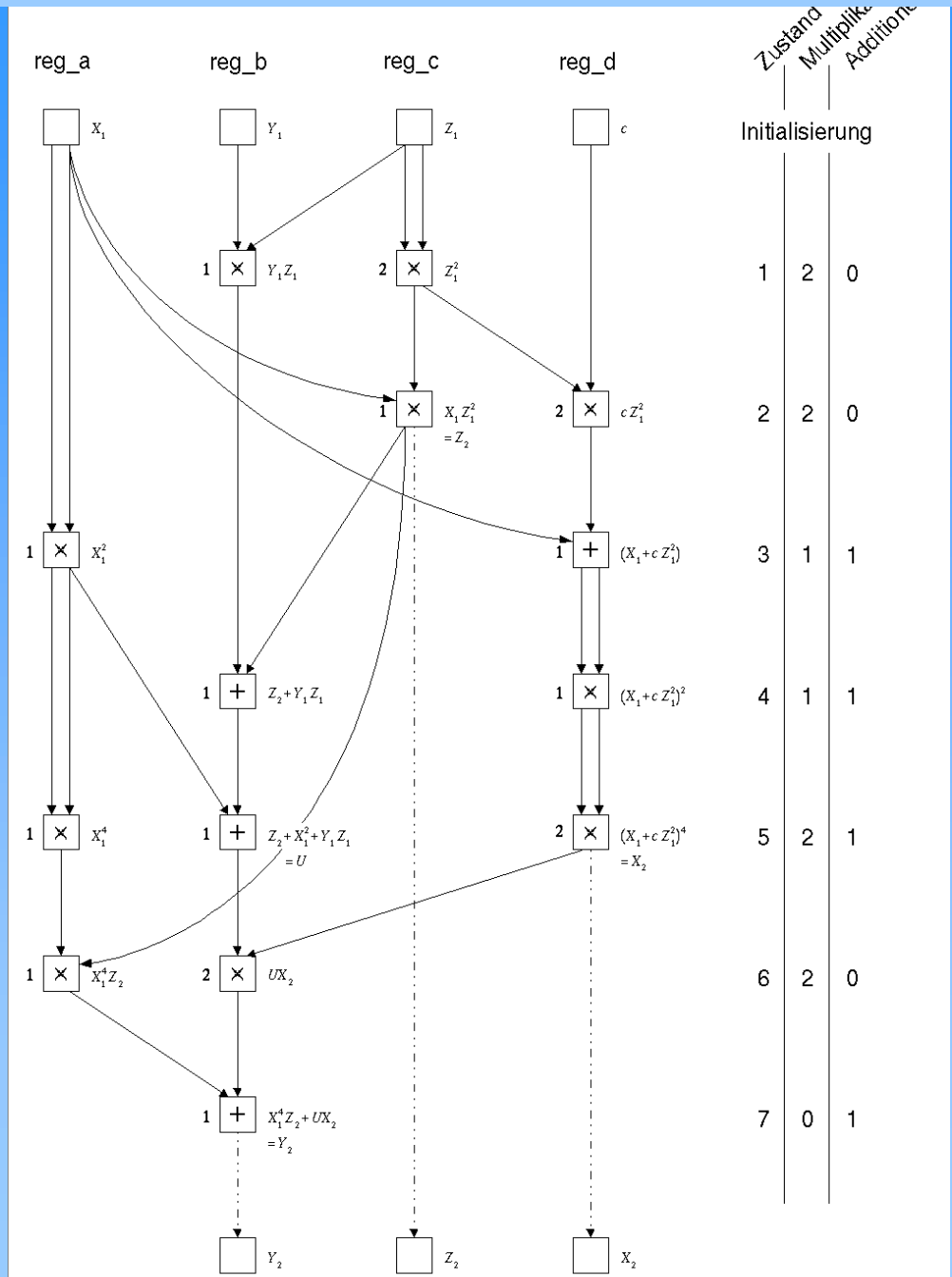
$$Z_2 = X_1 Z_1^2$$

$$X_2 = (X_1 + cZ_1^2)^4$$

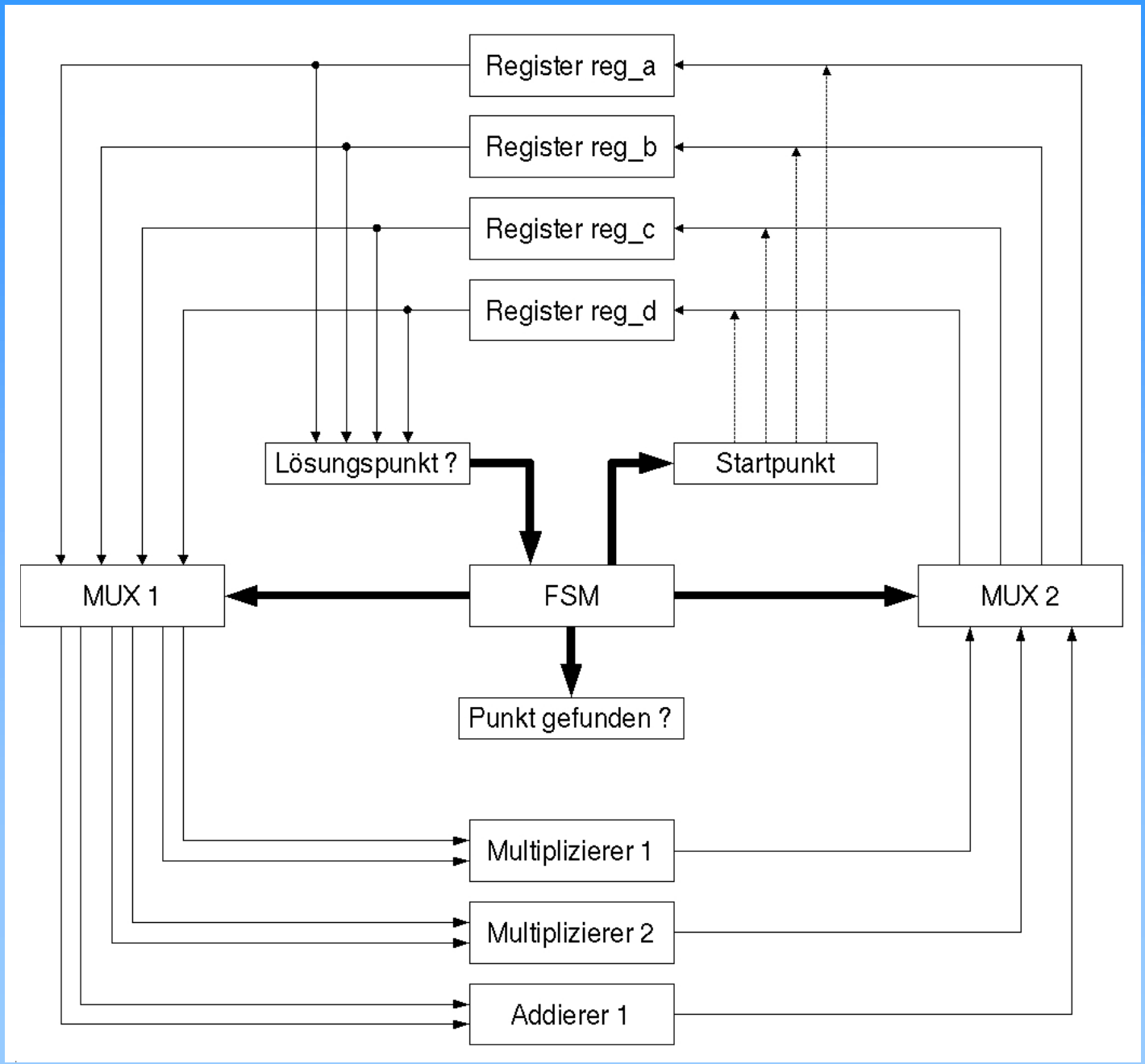
$$U = Z_2 + X_1^2 + Y_1 Z_1$$

$$Y_2 = X_1^4 Z_2 + U X_2$$

Der Datenfluß der Punktverdoppelung



Ablaufschema der FSM



Welchen Aufwand erfordert der Punktvergleich?

$$P = k \cdot B$$

affin ← k , B → projektiv

$$(x, y) = (X, Y, Z)$$

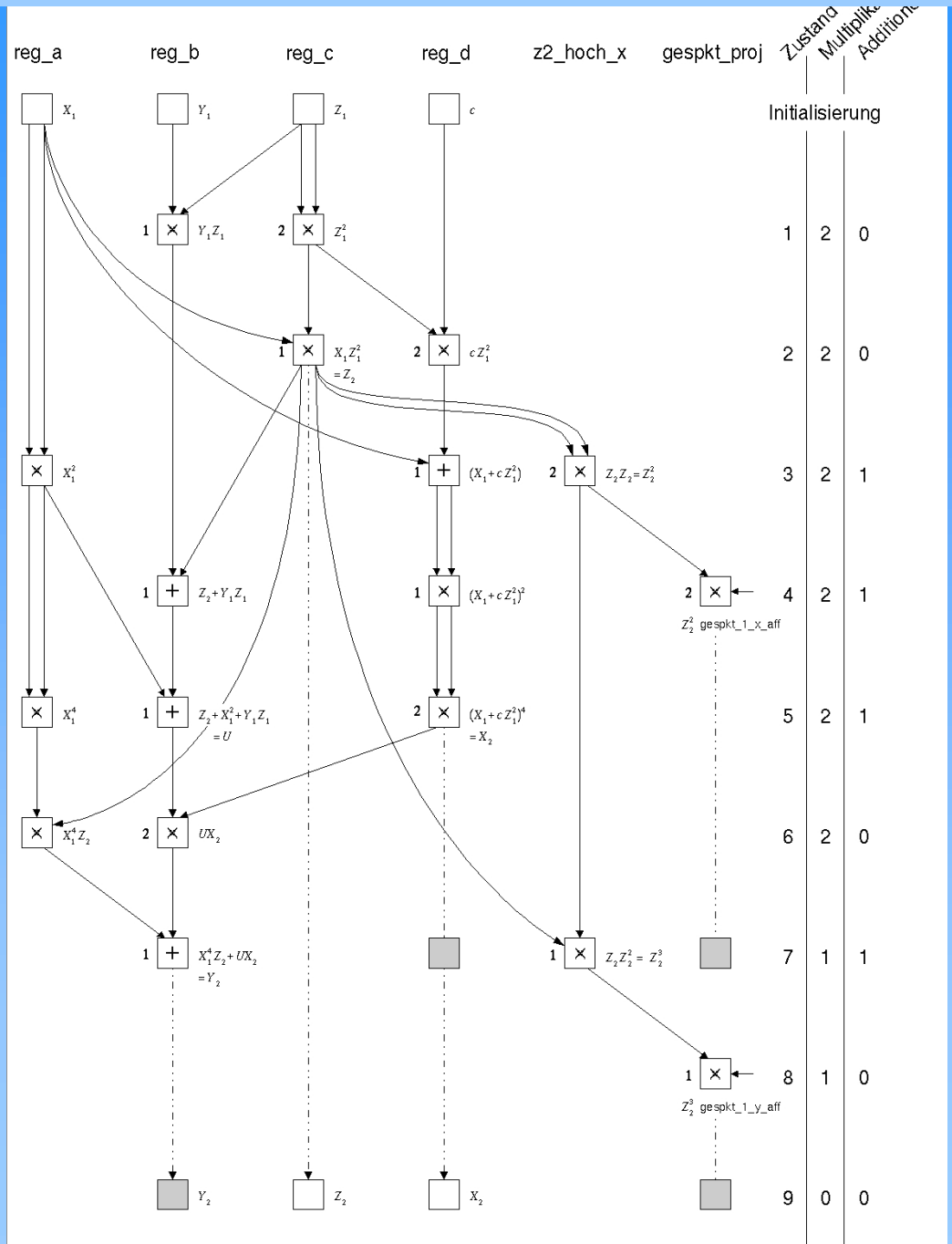
$$\Leftrightarrow (x, y, 1) = (X, Y, Z)$$

mit $(X,Y,Z) = (\lambda^2 X, \lambda^3 Y, \lambda Z)$ folgt

$$(Z^2 x, Z^3 y, Z) = (X, Y, Z)$$

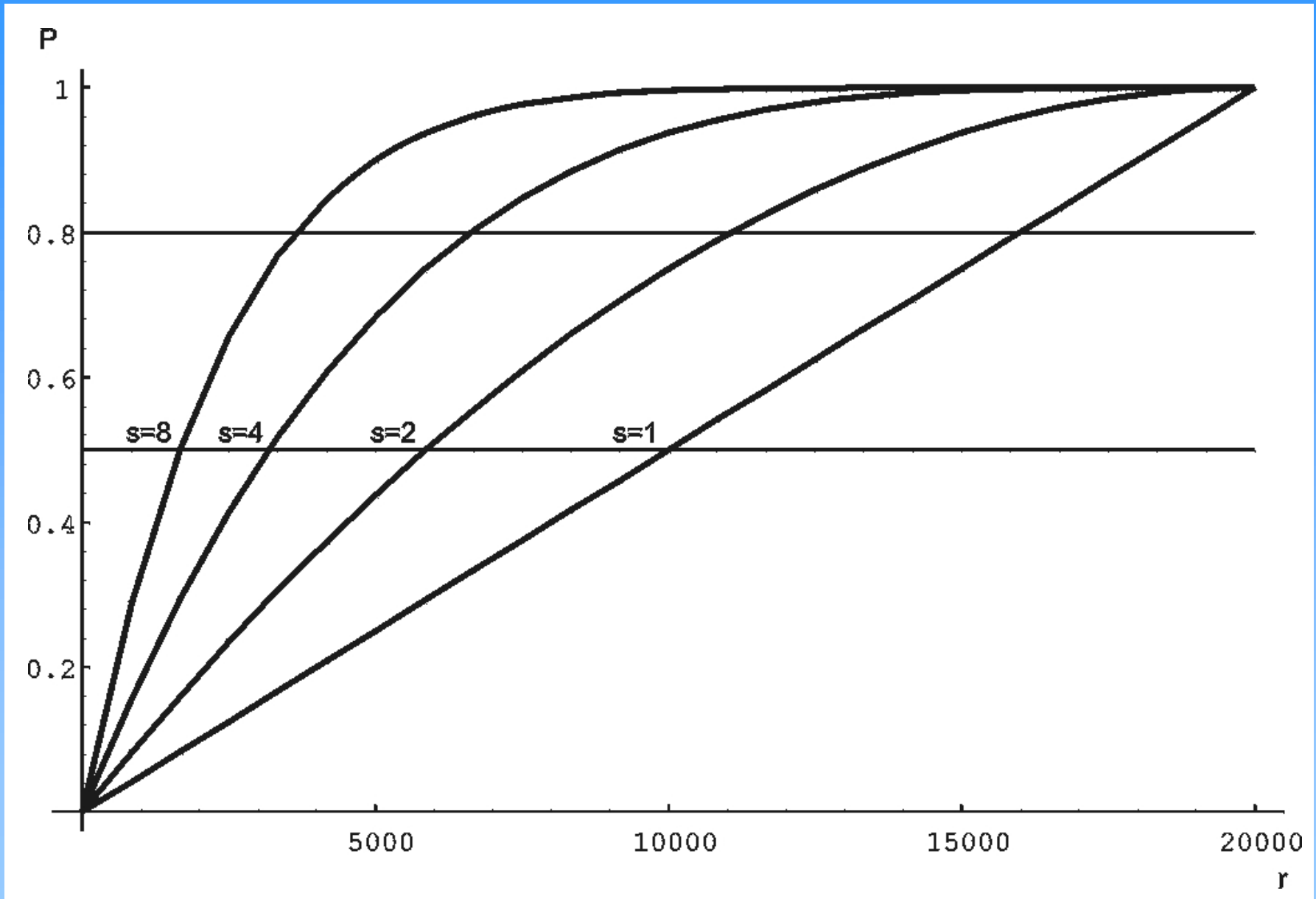
Der Datenfluß der Punktverdoppelung

zzgl. Punktvergleich



Verwendung mehrerer Suchpunkte

- jede Nachricht übermittelt einen Suchpunkt (x_1, y_1)
- Schlüssel bleiben bei vielen Implementierungen über lange Zeit gültig
- Beschleunigung der Attacke relativ zum höheren Aufwand der Punktvergleiche


P
1
0.8
0.6
0.4
0.2
s=8
s=4
s=2
s=1
5000
10000
15000
20000
r

Zustand		gesuchte Punkte 1	2	3	4	5	6	7	8	...		s
1	herkömmliche Strategie											
2												
3												
4		×										
5												
6												
7		=	×									1
8			=	×	×							2
9				=	=	×	×					4
10						=	=	×	×			6
11								=	=			8
⋮										⋱		⋮
n											=	2·(n−7)
n+1			u.U. Multiplikation mit Z_2^3									
n+2			u.U. Vergleich mit Y_2									

× Multiplikation mit Z_2^2

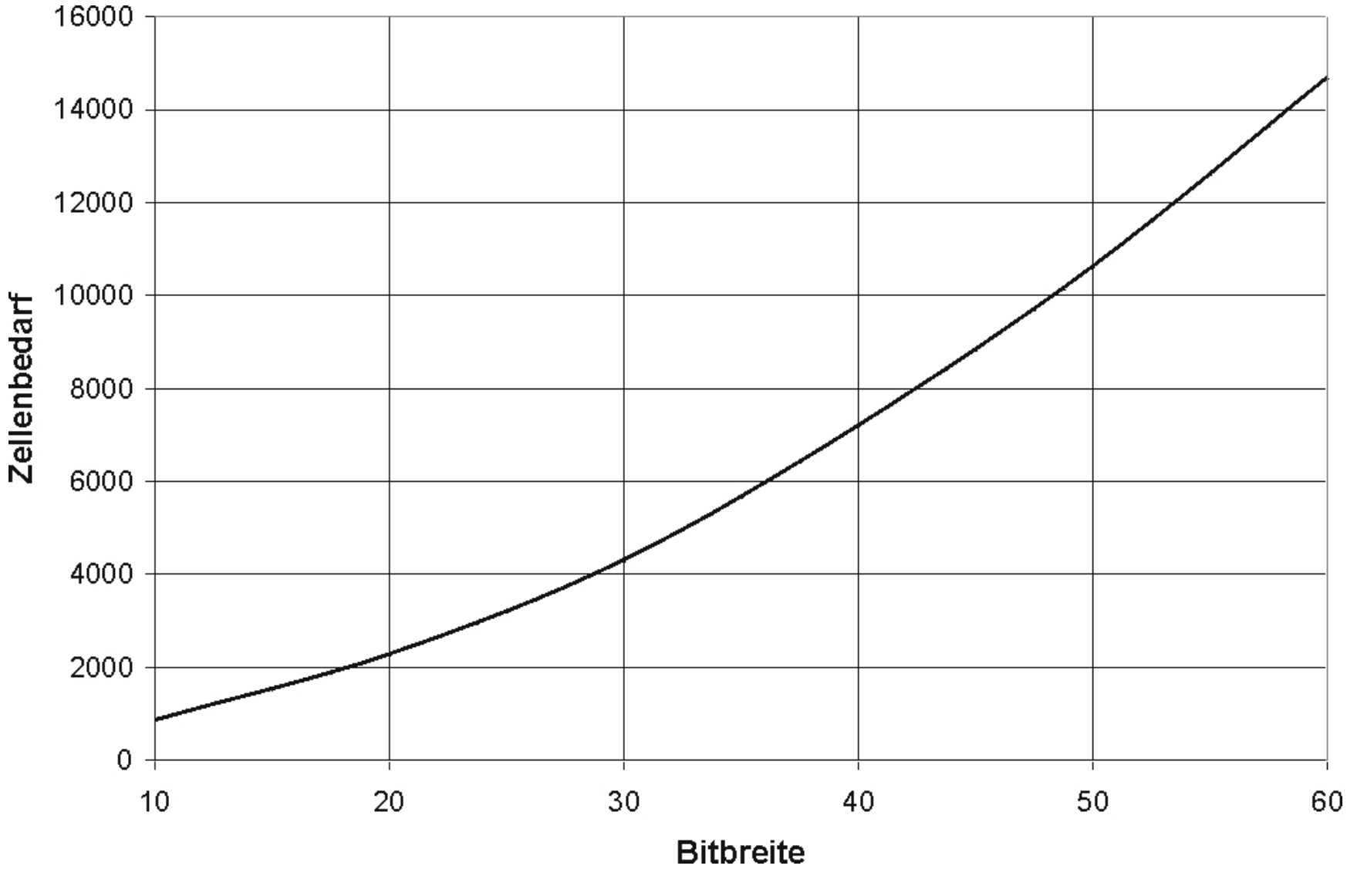
= Vergleich mit X_2

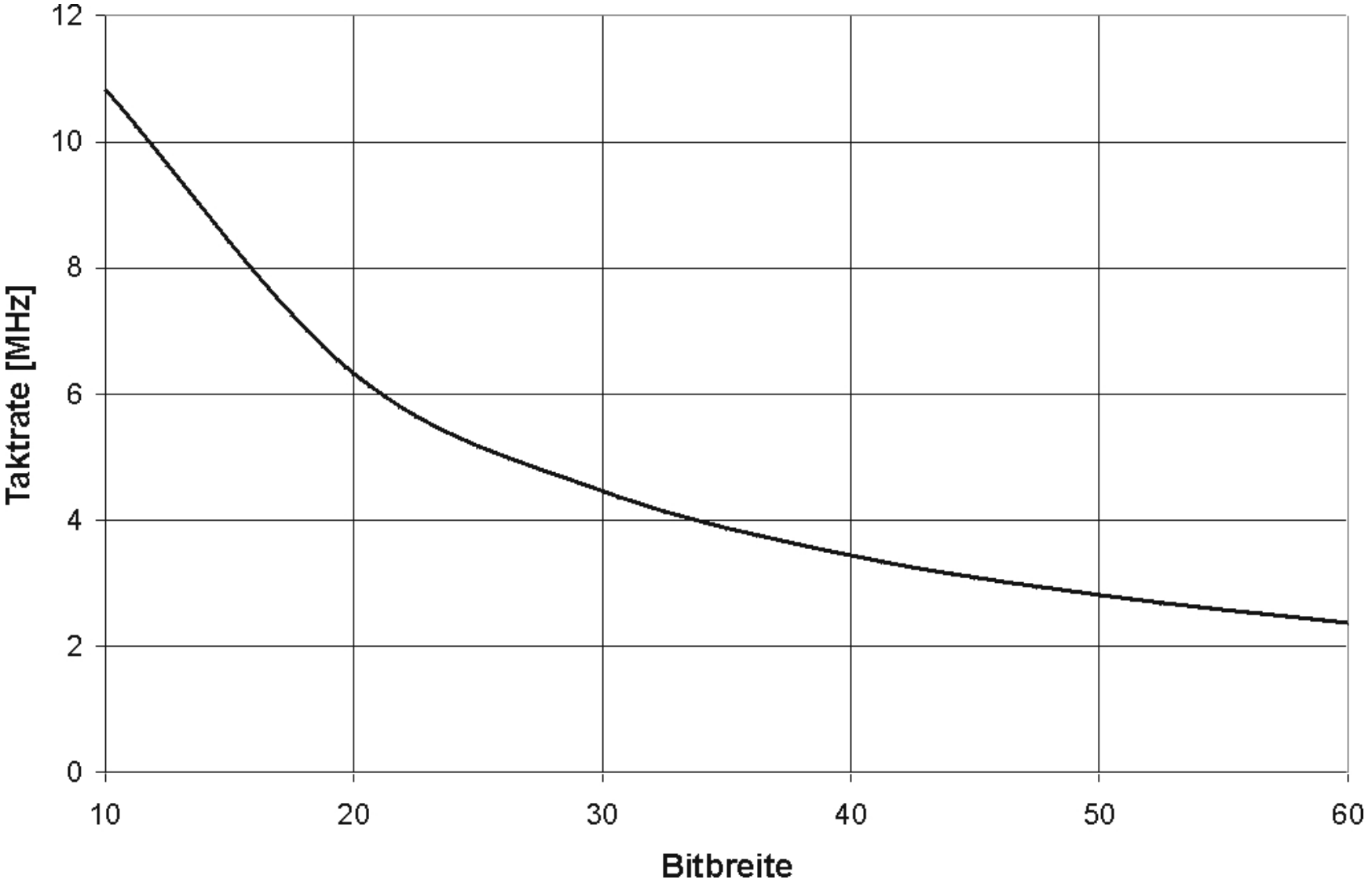
Übersicht

1. Kryptographie
2. Mathematische Grundlagen der elliptischen Kurven
3. Kryptosysteme mittels elliptischer Kurven
4. Angriffsstrategien auf ein ECC
5. Implementierungen der gewählten Strategie
6. Ergebnisse

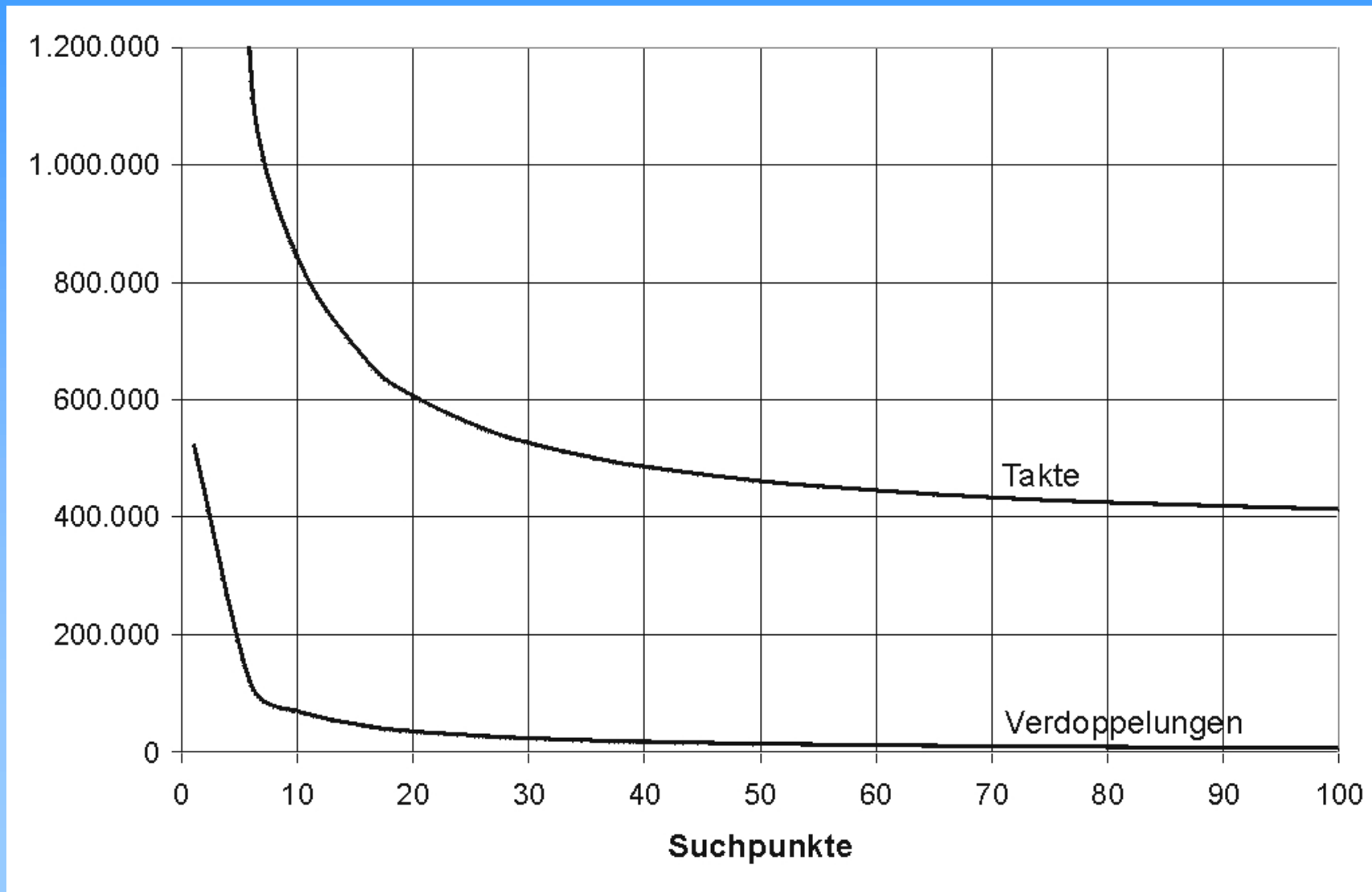
6. Ergebnisse

Ergebnisse des Synthesevorgangs

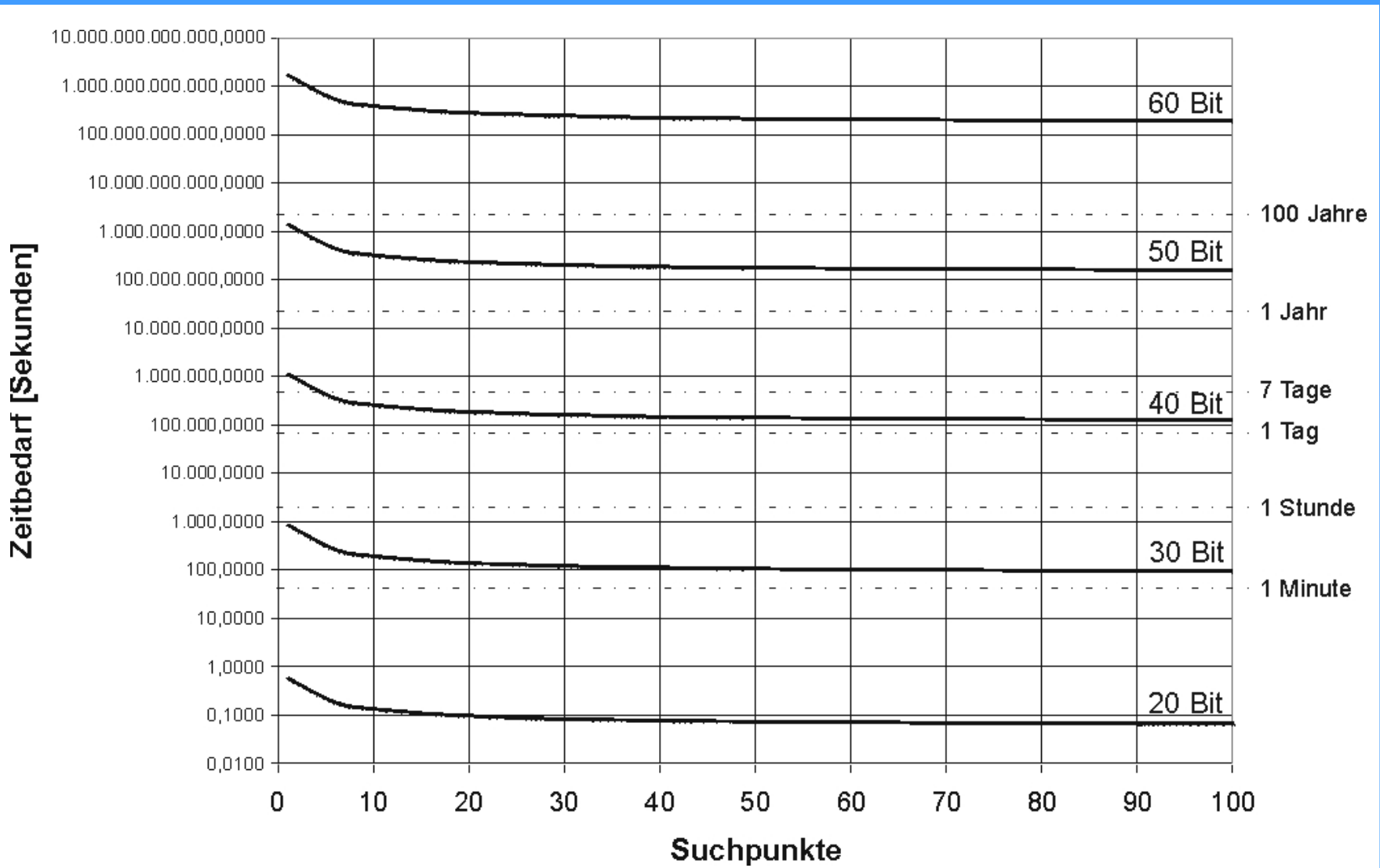

16000
14000
12000
10000
8000
6000
4000
2000
0
Zellenbedarf
10
20
30
40
50
60
Bitbreite


12
10
8
6
4
2
0
Taktrate [MHz]
10
20
30
40
50
60
Bitbreite

Anzahl der nötigen Verdoppelungen und Takte für eine Kurve über GF(2^{20}) bei Erfolgswahrscheinlichkeit von 50%:



Zeitaufwand für Erfolgswahrscheinlichkeit von 50%:



Vielen Dank für Ihre Aufmerksamkeit !