Seitenkanalattacken gegen Kryptographie auf Elliptischen Kurven

Peter Schwabe <schwabe@ti.rwth-aachen.de>

Lehrstuhl für Theoretische Informationstechnik, RWTH Aachen

15.07.2005

Überblick

1. Einleitung und Motivation
2. Mathematischer Hintergrund
3. Implementation von Elliptischen Kurven
4. Seitenkanalattacken
5. Zusammenfassung

Geschichte der elliptischen Kurven

- Theorie der elliptischen Kurven ist recht alt (Gauß)
- Entscheidende Fortschritte Anfang 19. Jahrhundert (Abel, Jacobi, Eisenstein, Dirichlet)
- Kryptosysteme erstmals 1985 (Miller, Koblitz)

Motivation

Geschichte der elliptischen Kurven

- Theorie der elliptischen Kurven ist recht alt (Gauß)
- Entscheidende Fortschritte Anfang 19. Jahrhundert (Abel, Jacobi, Eisenstein, Dirichlet)
- Kryptosysteme erstmals 1985 (Miller, Koblitz)

Elliptische Kurven heute


heise online

news 07.03.2005 15:51

<< Vorige | Nächste >>

Suche ...

7-Tage-News
News-Archiv
News unterwegs
Newsletter

NSA setzt auf Verschlüsselung mit Elliptischen Kurven

Die National Security Agency (NSA) will auf Elliptic Curve Cryptography (ECC) in kommenden Kryptosystemen zum Schutz der Kommunikation zwischen

Die Gruppenaxiome

Definition

Sei M eine Menge, $+ : M \times M \to M$ eine Verknüpfung. Dann heißt $(M, +)$ Gruppe, wenn:

- $a + (b + c) = (a + b) + c \quad \forall\, a, b, c \in M$ (Assoziativität)

Die Gruppenaxiome

Definition

Sei M eine Menge, $+ : M \times M \to M$ eine Verknüpfung. Dann heißt $(M, +)$ Gruppe, wenn:

- $a + (b + c) = (a + b) + c \quad \forall\, a, b, c \in M$ (Assoziativität)
- $\exists\, e \in M : a + e = a \quad \forall\, a \in M$ (Neutrales Element)

Die Gruppenaxiome

Definition

Sei M eine Menge, $+ : M \times M \to M$ eine Verknüpfung. Dann heißt $(M, +)$ Gruppe, wenn:

- $a + (b + c) = (a + b) + c \quad \forall\, a, b, c \in M$ (Assoziativität)
- $\exists\, e \in M : a + e = a \quad \forall\, a \in M$ (Neutrales Element)
- $\forall\, a \in M\, \exists\, (-a) \in M : (-a) + a = e$ (Inverses Element)

Die Gruppenaxiome

Definition

Sei M eine Menge, $+ : M \times M \rightarrow M$ eine Verknüpfung. Dann heißt $(M, +)$ Gruppe, wenn:

- $a + (b + c) = (a + b) + c \quad \forall\, a, b, c \in M$ (Assoziativität)
- $\exists\, e \in M : a + e = a \quad \forall\, a \in M$ (Neutrales Element)
- $\forall\, a \in M\, \exists\, (-a) \in M : (-a) + a = e$ (Inverses Element)

Definition

Gilt zusätzlich, dass:

- $a + b = b + a \quad \forall\, a, b \in M$,

so nennt man die Gruppe kommutativ oder abelsch.

Endliche Körper

- Für jede Primzahl p ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper mit p Elementen

Endliche Körper

- Für jede Primzahl p ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper mit p Elementen
- Bezeichung: $\mathbb{F}_p$, oder $GF(p)$

Endliche Körper

- Für jede Primzahl p ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper mit p Elementen
- Bezeichung: $\mathbb{F}_p$, oder $GF(p)$
- p prim, f irreduzibles Polynom vom Grad k über $\mathbb{F}_p$
  $\Rightarrow \mathbb{F}_p[X]/f \cdot \mathbb{F}_p[X]$ ist Körper mit p^k Elementen

Endliche Körper

- Für jede Primzahl p ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper mit p Elementen
- Bezeichung: $\mathbb{F}_p$, oder $GF(p)$
- p prim, f irreduzibles Polynom vom Grad k über $\mathbb{F}_p$
  $\Rightarrow \mathbb{F}_p[X]/f \cdot \mathbb{F}_p[X]$ ist Körper mit p^k Elementen
- Bezeichnung $\mathbb{F}_{p^k}$ oder $GF(p^k)$

Endliche Körper

- Für jede Primzahl p ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper mit p Elementen
- Bezeichung: $\mathbb{F}_p$, oder $GF(p)$
- p prim, f irreduzibles Polynom vom Grad k über $\mathbb{F}_p$
  $\Rightarrow \mathbb{F}_p[X]/f \cdot \mathbb{F}_p[X]$ ist Körper mit p^k Elementen
- Bezeichnung $\mathbb{F}_{p^k}$ oder $GF(p^k)$
- p ist die Charakteristik eines endlichen Körpers

Elliptische Kurven

Definition

Sei K Körper und seien $a_1, a_2, a_3, a_4, a_6 \in K$. Dann definiert die folgende Gleichung die elliptische Kurve E:

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

wenn die Diskriminante Δ von E ungleich 0 ist.

Elliptische Kurven

Definition

Sei K Körper und seien $a_1, a_2, a_3, a_4, a_6 \in K$. Dann definiert die folgende Gleichung die elliptische Kurve E:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

wenn die Diskriminante Δ von E ungleich 0 ist.

Bemerkung

Ist die Charakteristik von K ungleich 2 und 3, so erhält man die vereinfachte Form:

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

Definition

Sei L Erweiterungskörper von K. Dann heißt:

$$E(L) = \{(x, y) \in L \times L : y^2 + a_1 xy + a_3 y - x^3 - a_2 x^2 - a_4 x - a_6 = 0\} \cup \{\infty\}$$

die Menge L-rationaler Punkte auf E.

Elliptische Kurven und Gruppen

Definition

Sei L Erweiterungskörper von K. Dann heißt:

$$E(L) = \{(x, y) \in L \times L : y^2 + a_1 xy + a_3 y - x^3 - a_2 x^2 - a_4 x - a_6 = 0\} \cup \{\infty\}$$

die Menge L-rationaler Punkte auf E.

- Verknüpfung $+$ auf die Elemente von $E(L)$

Elliptische Kurven und Gruppen

Definition

Sei L Erweiterungskörper von K. Dann heißt:

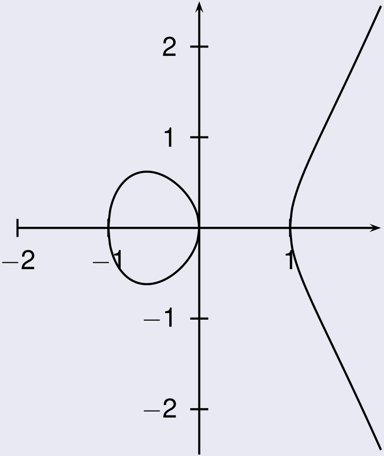
$$E(L) = \{(x, y) \in L \times L : y^2 + a_1 xy + a_3 y - x^3 - a_2 x^2 - a_4 x - a_6 = 0\} \cup \{\infty\}$$

die Menge L-rationaler Punkte auf E.

- Verknüpfung $+$ auf die Elemente von $E(L)$
- Gruppenstruktur mit Einheitselement ∞

Punktaddition: Beispiel: $y^2 = x^3 - x$ über $\mathbb{R}$

Graphische Darstellung über $\mathbb{R}$

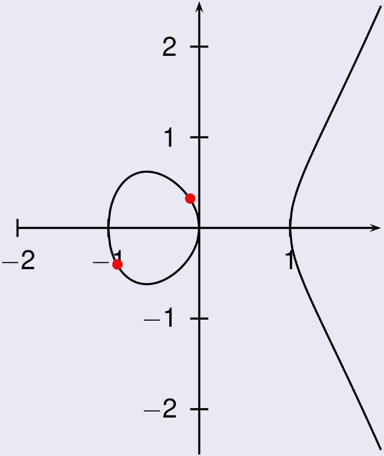


Punktaddition: Beispiel: $y^2 = x^3 - x$ über $\mathbb{R}$

Addition von Punkten

- Addiere die Punkte $P = (-0,9; -0,4135)$ und $Q = (-0,1; 0,3146)$

Graphische Darstellung über $\mathbb{R}$

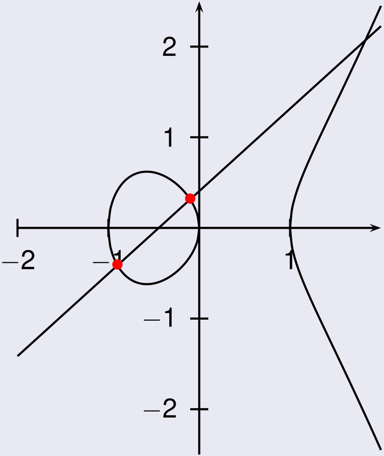


Punktaddition: Beispiel: $y^2 = x^3 - x$ über $\mathbb{R}$

Addition von Punkten

- Addiere die Punkte $P = (-0,9; -0,4135)$ und $Q = (-0,1; 0,3146)$
- Berechne Gerade durch die beiden Punkte

Graphische Darstellung über $\mathbb{R}$

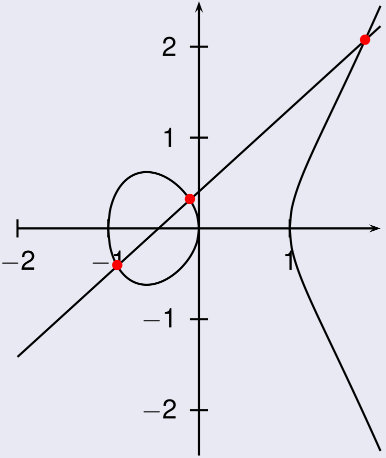


Punktaddition: Beispiel: $y^2 = x^3 - x$ über $\mathbb{R}$

Addition von Punkten

- Addiere die Punkte $P = (-0,9; -0,4135)$ und $Q = (-0,1; 0,3146)$
- Berechne Gerade durch die beiden Punkte
- Bestimme dritten Schnittpunkt $R = (x_R, y_R)$ mit der elliptischen Kurve

Graphische Darstellung über $\mathbb{R}$

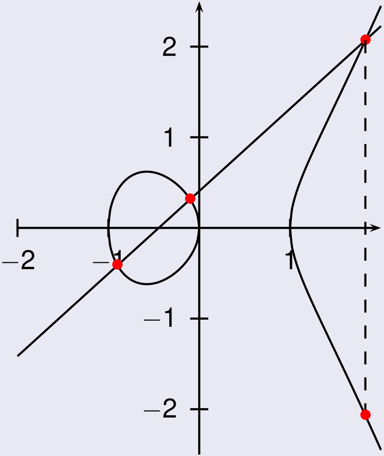


Punktaddition: Beispiel: $y^2 = x^3 - x$ über $\mathbb{R}$

Addition von Punkten

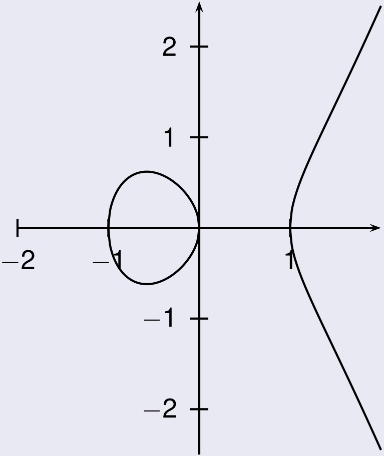
- Addiere die Punkte $P = (-0,9; -0,4135)$ und $Q = (-0,1; 0,3146)$
- Berechne Gerade durch die beiden Punkte
- Bestimme dritten Schnittpunkt $R = (x_R, y_R)$ mit der elliptischen Kurve
- Ergebnis der Addition: $P + Q = (x_R, -y_R)$

Graphische Darstellung über $\mathbb{R}$



Punktverdopplung: Beispiel: $y^2 = x^3 - x$ über $\mathbb{R}$

Graphische Darstellung über $\mathbb{R}$

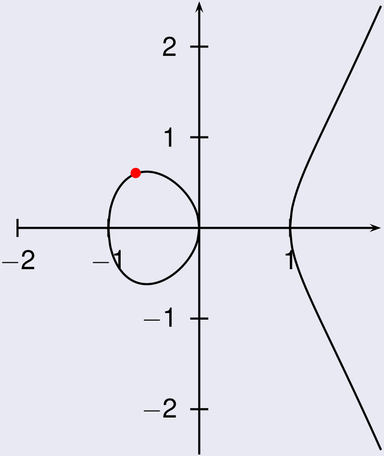


Punktverdopplung: Beispiel: $y^2 = x^3 - x$ über $\mathbb{R}$

Verdopplung von Punkten

- Verdopple den Punkt $P = (-0.7, 0.5975)$

Graphische Darstellung über $\mathbb{R}$

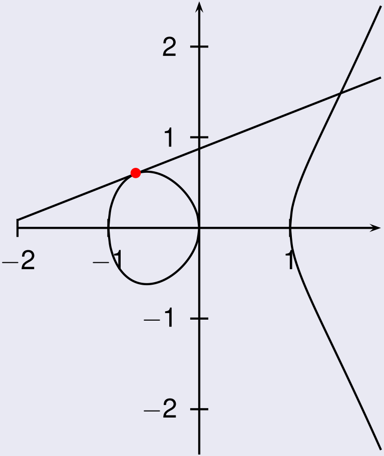


Punktverdopplung: Beispiel: $y^2 = x^3 - x$ über $\mathbb{R}$

Verdopplung von Punkten

- Verdopple den Punkt $P = (-0.7, 0.5975)$
- Berechne Tangente an den Punkt

Graphische Darstellung über $\mathbb{R}$

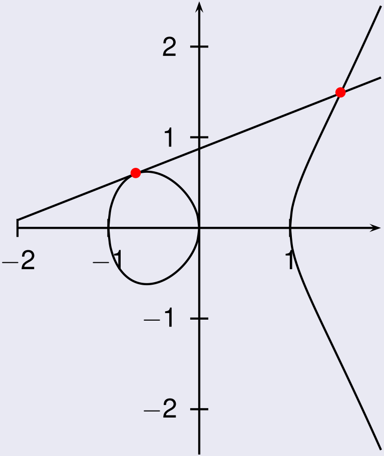


Punktverdopplung: Beispiel: $y^2 = x^3 - x$ über $\mathbb{R}$

Verdopplung von Punkten

- Verdopple den Punkt $P = (-0.7, 0.5975)$
- Berechne Tangente an den Punkt
- Bestimme weiteren Schnittpunkt $R = (x_R, y_R)$ mit der Kurve

Graphische Darstellung über $\mathbb{R}$

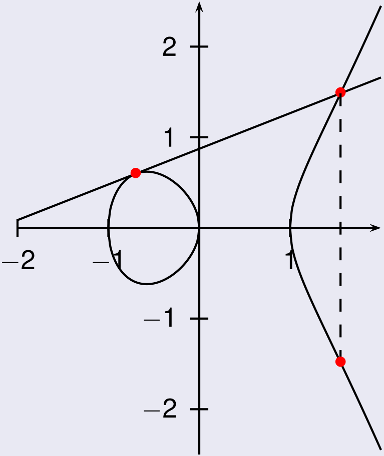


Punktverdopplung: Beispiel: $y^2 = x^3 - x$ über $\mathbb{R}$

Verdopplung von Punkten

- Verdopple den Punkt $P = (-0.7, 0.5975)$
- Berechne Tangente an den Punkt
- Bestimme weiteren Schnittpunkt $R = (x_R, y_R)$ mit der Kurve
- Ergebnis der Verdopplung: $2P = (x_R, -y_R)$

Graphische Darstellung über $\mathbb{R}$



Punktaddition in Formeln

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

Punktaddition in Formeln

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

Punktaddition

- $P = (x_P, y_P), Q = (x_Q, y_Q) \rightarrow P + Q = R = (x_R, y_R)$ mit

Punktaddition in Formeln

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

Punktaddition

- $P = (x_P, y_P), Q = (x_Q, y_Q) \rightarrow P + Q = R = (x_R, y_R)$ mit
- $x_R = \left(\frac{y_Q - y_P}{x_Q - x_P}\right)^2 - x_P - x_Q$
- $y_R = \left(\frac{y_Q - y_P}{x_Q - x_P}\right)(x_P - x_R) - y_P$

Punktaddition in Formeln

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

Punktaddition

- $P = (x_P, y_P), Q = (x_Q, y_Q) \rightarrow P + Q = R = (x_R, y_R)$ mit
- $x_R = \left(\frac{y_Q - y_P}{x_Q - x_P}\right)^2 - x_P - x_Q$
- $y_R = \left(\frac{y_Q - y_P}{x_Q - x_P}\right)(x_P - x_R) - y_P$

Punktverdopplung

- $P = (x_P, y_P), 2P = (x_R, y_R)$ mit

Punktaddition in Formeln

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

Punktaddition

- $P = (x_P, y_P), Q = (x_Q, y_Q) \rightarrow P + Q = R = (x_R, y_R)$ mit
- $x_R = \left(\frac{y_Q - y_P}{x_Q - x_P}\right)^2 - x_P - x_Q$
- $y_R = \left(\frac{y_Q - y_P}{x_Q - x_P}\right)(x_P - x_R) - y_P$

Punktverdopplung

- $P = (x_P, y_P), 2P = (x_R, y_R)$ mit
- $x_R = \left(\frac{3x_P^2 + a}{2y_P}\right)^2 - 2x_P$
- $y_R = \left(\frac{3x_P^2 + a}{2y_P}\right)(x_P - x_R) - y_P$

Jacobische Projektive Koordinaten

- Kurvengleichung: $y^2 = x^3 + ax + b$

Jacobische Projektive Koordinaten

- Kurvengleichung: $y^2 = x^3 + ax + b$
- Ersetze x durch X/Z^2 und y durch Y/Z^3:

$$\frac{Y^2}{Z^6} = \frac{X^3}{Z^6} + a\frac{X}{Z^2} + b$$

Jacobische Projektive Koordinaten

- Kurvengleichung: $y^2 = x^3 + ax + b$
- Ersetze x durch X/Z^2 und y durch Y/Z^3:

$$\frac{Y^2}{Z^6} = \frac{X^3}{Z^6} + a\frac{X}{Z^2} + b$$

- Multipliziere beide Seiten mit Z^6:

$$Y^2 = X^3 + aXZ^4 + bZ^6$$

Jacobische Projektive Koordinaten

- Kurvengleichung: $y^2 = x^3 + ax + b$
- Ersetze x durch X/Z^2 und y durch Y/Z^3:

$$\frac{Y^2}{Z^6} = \frac{X^3}{Z^6} + a\frac{X}{Z^2} + b$$

- Multipliziere beide Seiten mit Z^6:

$$Y^2 = X^3 + aXZ^4 + bZ^6$$

- Darstellung von Punkten durch $(X : Y : Z)$

Jacobische Projektive Koordinaten

- Kurvengleichung: $y^2 = x^3 + ax + b$
- Ersetze x durch X/Z^2 und y durch Y/Z^3:

$$\frac{Y^2}{Z^6} = \frac{X^3}{Z^6} + a\frac{X}{Z^2} + b$$

- Multipliziere beide Seiten mit Z^6:

$$Y^2 = X^3 + aXZ^4 + bZ^6$$

- Darstellung von Punkten durch $(X : Y : Z)$
- Umrechnung: $(X : Y : Z) \longrightarrow (X/Z^2, Y/Z^3)$

Darstellung in Jacobi-Koordinaten II

Addition

$(X_P : Y_P : Z_P) + (X_Q : Y_Q : 1) = (X_R : Y_R : Z_R)$ mit

Darstellung in Jacobi-Koordinaten II

Addition

$(X_P : Y_P : Z_P) + (X_Q : Y_Q : 1) = (X_R : Y_R : Z_R)$ mit

- $X_R = (Y_Q Z_P^3 - Y_P)^2 - (X_Q Z_P^2 - X_P)^2 (X_P + X_Q Z_P^2)$
- $Y_R = (Y_Q Z_P^3 - Y_Q)(X_P (X_Q Z_P^2 - X_P)^2) - X_R) - Y_P (X_Q Z_P^2 - X_P)^3$
- $Z_R = (X_Q Z_P^2 - X_P) Z_P$

Darstellung in Jacobi-Koordinaten II

Addition

$(X_P : Y_P : Z_P) + (X_Q : Y_Q : 1) = (X_R : Y_R : Z_R)$ mit

- $X_R = (Y_Q Z_P^3 - Y_P)^2 - (X_Q Z_P^2 - X_P)^2 (X_P + X_Q Z_P^2)$
- $Y_R = (Y_Q Z_P^3 - Y_Q)(X_P (X_Q Z_P^2 - X_P)^2) - X_R) - Y_P (X_Q Z_P^2 - X_P)^3$
- $Z_R = (X_Q Z_P^2 - X_P) Z_P$

Berechenbar mit 3 Quadrierungen und 8 Multiplikationen

Darstellung in Jacobi-Koordinaten II

Addition

$(X_P : Y_P : Z_P) + (X_Q : Y_Q : 1) = (X_R : Y_R : Z_R)$ mit

- $X_R = (Y_Q Z_P^3 - Y_P)^2 - (X_Q Z_P^2 - X_P)^2 (X_P + X_Q Z_P^2)$
- $Y_R = (Y_Q Z_P^3 - Y_Q)(X_P (X_Q Z_P^2 - X_P)^2) - X_R) - Y_P (X_Q Z_P^2 - X_P)^3$
- $Z_R = (X_Q Z_P^2 - X_P) Z_P$

Berechenbar mit 3 Quadrierungen und 8 Multiplikationen

Verdopplung

$2 \cdot (X_P : Y_P : Z_P) = (X_R : Y_R : Z_R)$ mit

Darstellung in Jacobi-Koordinaten II

Addition

$(X_P : Y_P : Z_P) + (X_Q : Y_Q : 1) = (X_R : Y_R : Z_R)$ mit

- $X_R = (Y_Q Z_P^3 - Y_P)^2 - (X_Q Z_P^2 - X_P)^2 (X_P + X_Q Z_P^2)$
- $Y_R = (Y_Q Z_P^3 - Y_Q)(X_P (X_Q Z_P^2 - X_P)^2) - X_R) - Y_P (X_Q Z_P^2 - X_P)^3$
- $Z_R = (X_Q Z_P^2 - X_P) Z_P$

Berechenbar mit 3 Quadrierungen und 8 Multiplikationen

Verdopplung

$2 \cdot (X_P : Y_P : Z_P) = (X_R : Y_R : Z_R)$ mit

- $X_R = (3X_P^2 + aZ_1^4)^2 - 8X_P Y_P^2$
- $Y_R = (3X_P^2 + aZ_1^4)(4X_P Y_P^2 - X_R) - 8Y_1^4$
- $Z_R = 2Y_P Z_P$

Darstellung in Jacobi-Koordinaten II

Addition

$(X_P : Y_P : Z_P) + (X_Q : Y_Q : 1) = (X_R : Y_R : Z_R)$ mit

- $X_R = (Y_Q Z_P^3 - Y_P)^2 - (X_Q Z_P^2 - X_P)^2 (X_P + X_Q Z_P^2)$
- $Y_R = (Y_Q Z_P^3 - Y_Q)(X_P (X_Q Z_P^2 - X_P)^2) - X_R) - Y_P (X_Q Z_P^2 - X_P)^3$
- $Z_R = (X_Q Z_P^2 - X_P) Z_P$

Berechenbar mit 3 Quadrierungen und 8 Multiplikationen

Verdopplung

$2 \cdot (X_P : Y_P : Z_P) = (X_R : Y_R : Z_R)$ mit

- $X_R = (3X_P^2 + aZ_1^4)^2 - 8X_P Y_P^2$
- $Y_R = (3X_P^2 + aZ_1^4)(4X_P Y_P^2 - X_R) - 8Y_1^4$
- $Z_R = 2Y_P Z_P$

Berechenbar mit 6 Quadrierungen und 4 Multiplikationen

DLP auf Elliptischen Kurven

Das Diskrete Logarithmus Problem (DLP)

Gegeben:

- $n \in \mathbb{N}$
- $a \in \mathbb{Z}_n^*, a \neq 1$
- $b = a^x \mod n$

Gesucht: x

DLP auf Elliptischen Kurven

Das Diskrete Logarithmus Problem (DLP)

Gegeben:
- $n \in \mathbb{N}$
- $a \in \mathbb{Z}_n^*, a \neq 1$
- $b = a^x \mod n$

Gesucht: x

Das DLP für elliptische Kurven

Gegeben:
- Elliptische Kurve E über endlichem Körper K
- Endlicher Erweiterungskörper L von K
- $P \in E(L), P \neq \infty$
- $Q = k \cdot P$

Gesucht: k

Implementation der Skalaren Multiplikation

- Berechne $k \cdot P$

Implementation der Skalaren Multiplikation

- Berechne $k \cdot P$
- Sei $(k_{n-1} \dots k_0)$ die Binärdarstellung von k

Implementation der Skalaren Multiplikation

- Berechne $k \cdot P$
- Sei $(k_{n-1} \dots k_0)$ die Binärdarstellung von k

Double and Add

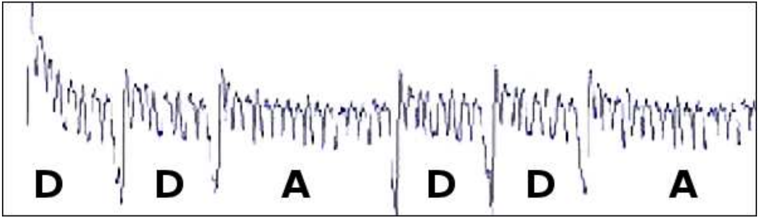
```
Q = P
for(i = n − 2; i ≤ 0; i − −)
{
  Q = 2Q;
  if(k_i = 1) then Q+ = P;
}
return Q
```

Simple Power Analysis Attack (SPA)

- Addition ist aufwendiger als Verdopplung

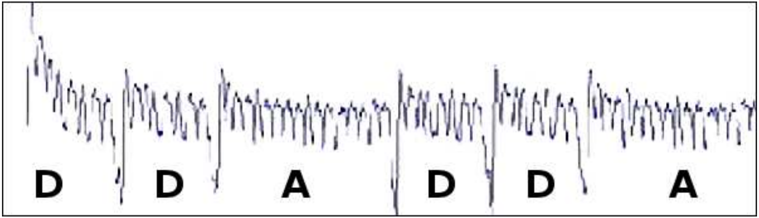
Simple Power Analysis Attack (SPA)

- Addition ist aufwendiger als Verdopplung



Simple Power Analysis Attack (SPA)

- Addition ist aufwendiger als Verdopplung



- Geheimer Schlüssel kann abgelesen werden

SPA-Gegenmaßnahmen

- Identische mathematische Formeln für Addition und Verdopplung (Eric Brier und Marc Joyce, 2002)

SPA-Gegenmaßnahmen

- Identische mathematische Formeln für Addition und Verdopplung (Eric Brier und Marc Joyce, 2002)
- Veränderung des „Double and Add“-Algorithmus

SPA-Gegenmaßnahmen

- Identische mathematische Formeln für Addition und Verdopplung (Eric Brier und Marc Joyce, 2002)
- Veränderung des „Double and Add“-Algorithmus
- Einfügen von Dummy-Operationen in Addition und Verdopplung

Veränderung des „Double and Add"-Algorithmus

- Berechne $k \cdot P$
- Sei $(k_{n-1} \ldots k_0)$ die Binärdarstellung von k

Veränderung des „Double and Add"-Algorithmus

- Berechne $k \cdot P$
- Sei $(k_{n-1} \dots k_0)$ die Binärdarstellung von k

Double and Add always

$\mathtt{Q}_0 = \mathtt{P}$
$\mathtt{for}(\mathtt{i} = \mathtt{n} - 2; \mathtt{i} \leq 0; \mathtt{i} - -)$
$\{$
$\quad \mathtt{Q}_0 = 2\mathtt{Q}_0;$
$\quad \mathtt{Q}_1 = \mathtt{Q}_0 + \mathtt{P};$
$\quad \mathtt{Q}_0 = \mathtt{Q}_{\mathtt{k}_\mathtt{i}}$
$\}$
$\mathtt{return}\ \mathtt{Q}$

Veränderung des „Double and Add“-Algorithmus

- Berechne $k \cdot P$
- Sei $(k_{n-1} \dots k_0)$ die Binärdarstellung von k

Double and Add always

$$
\begin{array}{l}
\mathtt{Q}_0 = \mathtt{P} \\
\mathtt{for}(\mathtt{i} = \mathtt{n} - 2; \mathtt{i} \leq 0; \mathtt{i} - -) \\
\{ \\
\quad \mathtt{Q}_0 = 2\mathtt{Q}_0; \\
\quad \mathtt{Q}_1 = \mathtt{Q}_0 + \mathtt{P}; \\
\quad \mathtt{Q}_0 = \mathtt{Q}_{\mathtt{k}_\mathtt{i}} \\
\} \\
\mathtt{return}\ \mathtt{Q}
\end{array}
$$

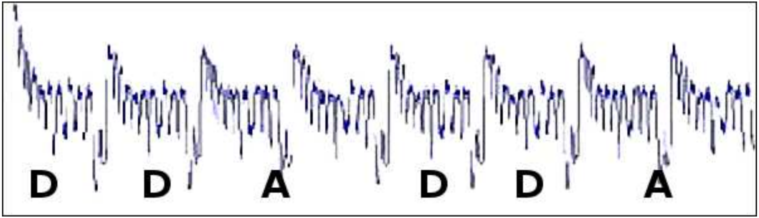
Achtung: Compileroptimierung

Einfügen von Dummy Operationen

- Addition sieht aus wie 2 Verdopplungen

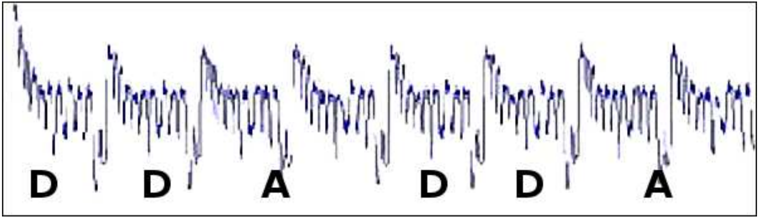
Einfügen von Dummy Operationen

- Addition sieht aus wie 2 Verdopplungen



Einfügen von Dummy Operationen

- Addition sieht aus wie 2 Verdopplungen



- Schlüssel kann nicht mehr abgelesen werden

Differential Power Analysis (DPA)

- Berechnung von $kP_1, \ldots, kP_n$

Differential Power Analysis (DPA)

- Berechnung von $kP_1, \ldots, kP_n$
- Attacke gegen Bit $k_{n-2} \rightarrow$ Wir raten: $k_{n-2} = 0$

Differential Power Analysis (DPA)

- Berechnung von $kP_1, \dots, kP_n$
- Attacke gegen Bit $k_{n-2} \rightarrow$ Wir raten: $k_{n-2} = 0$
- Richtig geraten: Im 2. Iterationsschritt wird $4P_i$ berechnet

Differential Power Analysis (DPA)

- Berechnung von $kP_1, \ldots, kP_n$
- Attacke gegen Bit $k_{n-2} \rightarrow$ Wir raten: $k_{n-2} = 0$
- Richtig geraten: Im 2. Iterationsschritt wird $4P_i$ berechnet
- Sortiere die Powertraces nach einem Bit von $4P_i, i = 1 \ldots n$

Differential Power Analysis (DPA)

- Berechnung von $kP_1, \ldots, kP_n$
- Attacke gegen Bit $k_{n-2} \rightarrow$ Wir raten: $k_{n-2} = 0$
- Richtig geraten: Im 2. Iterationsschritt wird $4P_i$ berechnet
- Sortiere die Powertraces nach einem Bit von $4P_i, i = 1 \ldots n$
- Bilde differentielle Powertrace, überprüfe, ob k_{n-2} korrekt geraten war

Differential Power Analysis (DPA)

- Berechnung von $kP_1, \ldots, kP_n$
- Attacke gegen Bit $k_{n-2} \rightarrow$ Wir raten: $k_{n-2} = 0$
- Richtig geraten: Im 2. Iterationsschritt wird $4P_i$ berechnet
- Sortiere die Powertraces nach einem Bit von $4P_i, i = 1 \ldots n$
- Bilde differentielle Powertrace, überprüfe, ob k_{n-2} korrekt geraten war
- Voraussetzung: Angreifer kennt Darstellung von $4P_i,\ i = 1, \ldots, n$

Zufällige Projektive Koordinaten

- Sei $P = (x, y)$

Zufällige Projektive Koordinaten

- Sei $P = (x, y)$
- Wähle $\theta \in L^*$ zufällig und bilde die Jacobische Projektive Form $(\theta^2 x : \theta^3 y : \theta)$

Zufällige Projektive Koordinaten

- Sei $P = (x, y)$
- Wähle $\theta \in L^*$ zufällig und bilde die Jacobische Projektive Form $(\theta^2 x : \theta^3 y : \theta)$
- Berechne $(X_R : Y_R : Z_R) = kP$ mit diesen zufälligen Projektiven Koordinaten

Zufällige Projektive Koordinaten

- Sei $P = (x, y)$
- Wähle $\theta \in L^*$ zufällig und bilde die Jacobische Projektive Form $(\theta^2 x : \theta^3 y : \theta)$
- Berechne $(X_R : Y_R : Z_R) = kP$ mit diesen zufälligen Projektiven Koordinaten
- Transformiere in affine Koordinaten: $kP = (X_R/Z_R^2, Y_R/Z_R^3)$

Zufällige Kurven Isomorphismen

- Kurvengleichung: $E : y^2 = x^3 + ax + b$

Zufällige Kurven Isomorphismen

- Kurvengleichung: $E : y^2 = x^3 + ax + b$
- Wähle $\theta \in L^*$ zufällig, berechne: $a' = \theta^{-4}a$ und $b' = \theta^{-6}b$

Zufällige Kurven Isomorphismen

- Kurvengleichung: $E : y^2 = x^3 + ax + b$
- Wähle $\theta \in L^*$ zufällig, berechne: $a' = \theta^{-4} a$ und $b' = \theta^{-6} b$
- Kurve $E' : y^2 = x^3 + a'x + b'$

Zufällige Kurven Isomorphismen

- Kurvengleichung: $E : y^2 = x^3 + ax + b$
- Wähle $\theta \in L^*$ zufällig, berechne: $a' = \theta^{-4}a$ und $b' = \theta^{-6}b$
- Kurve $E' : y^2 = x^3 + a'x + b'$
- Bilde Isomorphismus $\varphi : E(L) \to E'(L), \begin{cases} \infty \mapsto \infty \\ (x, y) \mapsto (\theta^{-2}x, \theta^{-3}y) \end{cases}$

Zufällige Kurven Isomorphismen

- Kurvengleichung: $E : y^2 = x^3 + ax + b$
- Wähle $\theta \in L^*$ zufällig, berechne: $a' = \theta^{-4}a$ und $b' = \theta^{-6}b$
- Kurve $E' : y^2 = x^3 + a'x + b'$
- Bilde Isomorphismus $\varphi : E(L) \to E'(L), \begin{cases} \infty \mapsto \infty \\ (x, y) \mapsto (\theta^{-2}x, \theta^{-3}y) \end{cases}$
- Berechne $R' = k * \varphi(P)$ in $E'(L)$.

Zufällige Kurven Isomorphismen

- Kurvengleichung: $E : y^2 = x^3 + ax + b$
- Wähle $\theta \in L^*$ zufällig, berechne: $a' = \theta^{-4}a$ und $b' = \theta^{-6}b$
- Kurve $E' : y^2 = x^3 + a'x + b'$
- Bilde Isomorphismus $\varphi : E(L) \to E'(L), \begin{cases} \infty \mapsto \infty \\ (x, y) \mapsto (\theta^{-2}x, \theta^{-3}y) \end{cases}$
- Berechne $R' = k * \varphi(P)$ in $E'(L)$.
- Berechne $R = \varphi^{-1}(R')$

Zufällige Kurven Isomorphismen

- Kurvengleichung: $E : y^2 = x^3 + ax + b$
- Wähle $\theta \in L^*$ zufällig, berechne: $a' = \theta^{-4}a$ und $b' = \theta^{-6}b$
- Kurve $E' : y^2 = x^3 + a'x + b'$
- Bilde Isomorphismus $\varphi : E(L) \to E'(L), \begin{cases} \infty \mapsto \infty \\ (x, y) \mapsto (\theta^{-2}x, \theta^{-3}y) \end{cases}$
- Berechne $R' = k * \varphi(P)$ in $E'(L)$.
- Berechne $R = \varphi^{-1}(R')$

Achtung: Für K mit Charakteristik 2 nicht ausreichend

Zufällige Körper Isomorphismen

- Körper L mit p^m Elementen wird generiert von irreduziblem Polynom f über $\mathbb{F}_p$

Zufällige Körper Isomorphismen

- Körper L mit p^m Elementen wird generiert von irreduziblem Polynom f über $\mathbb{F}_p$
- Finde anderes irreduzibles Polynom f' über $\mathbb{F}_p \rightarrow L'$

Zufällige Körper Isomorphismen

- Körper L mit p^m Elementen wird generiert von irreduziblem Polynom f über $\mathbb{F}_p$
- Finde anderes irreduzibles Polynom f' über $\mathbb{F}_p \ \rightarrow L'$
- Körperisomorphismus $\varphi : L \rightarrow L'$

Zufällige Körper Isomorphismen

- Körper L mit p^m Elementen wird generiert von irreduziblem Polynom f über $\mathbb{F}_p$
- Finde anderes irreduzibles Polynom f' über $\mathbb{F}_p \rightarrow L'$
- Körperisomorphismus $\varphi : L \rightarrow L'$
- Berechne E' über K' mit Parametern $\varphi(a)$ und $\varphi(b)$

Zufällige Körper Isomorphismen

- Körper L mit p^m Elementen wird generiert von irreduziblem Polynom f über $\mathbb{F}_p$
- Finde anderes irreduzibles Polynom f' über $\mathbb{F}_p \ \rightarrow L'$
- Körperisomorphismus $\varphi : L \rightarrow L'$
- Berechne E' über K' mit Parametern $\varphi(a)$ und $\varphi(b)$
- Berechne $P' = (\varphi(x), \varphi(y))$ und $k \cdot P' = (x_{R'}, y_{R'})$ in $E'(L')$

Zufällige Körper Isomorphismen

- Körper L mit p^m Elementen wird generiert von irreduziblem Polynom f über $\mathbb{F}_p$
- Finde anderes irreduzibles Polynom f' über $\mathbb{F}_p \rightarrow L'$
- Körperisomorphismus $\varphi : L \rightarrow L'$
- Berechne E' über K' mit Parametern $\varphi(a)$ und $\varphi(b)$
- Berechne $P' = (\varphi(x), \varphi(y))$ und $k \cdot P' = (x_{R'}, y_{R'})$ in $E'(L')$
- Berechne $R = (\varphi^{-1}(x_{R'}), \varphi^{-1}(y_{R'}))$

Goubins Attacke

- Idee: Finde „spezielle“ Punkte $(x, 0)$ bzw. $(0, y) \rightarrow P_0$

Goubins Attacke

- Idee: Finde „spezielle“ Punkte $(x, 0)$ bzw. $(0, y) \rightarrow P_0$
- Attacke gegen das Bit k_i
- Berechnetes Q_0 im Schritt mit Laufvariablenwert i:

$$\left(\sum_{j=i+1}^{n-1} k_j 2^{j-i} \quad + k_i \right) \cdot P$$

Goubins Attacke

- Idee: Finde „spezielle“ Punkte $(x, 0)$ bzw. $(0, y) \rightarrow P_0$
- Attacke gegen das Bit k_i
- Berechnetes Q_0 im Schritt mit Laufvariablenwert i:

$$\left(\sum_{j=i+1}^{n-1} k_j 2^{j-i} \quad + k_i \right) \cdot P$$

- Im nächsten Schritt:

$$k_i = 0 : Q_1 = \left(\sum_{j=i+1}^{n-1} k_j 2^{j-i+1} \quad + 1 \right) \cdot P$$

$$k_i = 1 : Q_1 = \left(\sum_{j=i+1}^{n-1} k_j 2^{j-i+1} \quad + 3 \right) \cdot P$$

Goubins Attacke

- Annahme: Wir raten $k_i = 0$

Goubins Attacke

- Annahme: Wir raten $k_i = 0$
- Berechne nun:

$$P_1 = \left[\left(\sum_{j=i+1}^{n-1} k_j 2^{j-i+1} \quad + 1 \right)^{-1} \mod |E(L)| \right] \cdot P_0$$

Goubins Attacke

- Annahme: Wir raten $k_i = 0$
- Berechne nun:

$$P_1 = \left[\left(\sum_{j=i+1}^{n-1} k_j 2^{j-i+1} \quad + 1 \right)^{-1} \quad \mod |E(L)| \right] \cdot P_0$$

- Verschlüssele sehr häufig P_1 (*chosen-ciphertext*)

Goubins Attacke

- Annahme: Wir raten $k_i = 0$
- Berechne nun:

$$P_1 = \left[\left(\sum_{j=i+1}^{n-1} k_j 2^{j-i+1} + 1 \right)^{-1} \mod |E(L)| \right] \cdot P_0$$

- Verschlüssele sehr häufig P_1 (*chosen-ciphertext*)
- Richtig geraten: 0-Koordinate führt zu einem Peak in der Mittelung der Powertraces

Goubins Attacke

Bemerkungen

- Betrachte von FIPS, ANSI, ISO/IEC und WTLS standardisierte Kurven

Goubins Attacke

Bemerkungen

- Betrachte von FIPS, ANSI, ISO/IEC und WTLS standardisierte Kurven
- Die meisten Kurven haben Punkte $(0, y)$

Goubins Attacke

Bemerkungen

- Betrachte von FIPS, ANSI, ISO/IEC und WTLS standardisierte Kurven
- Die meisten Kurven haben Punkte $(0, y)$
- Kurvenordung: $q, 2q, 4q, 6q$ (q prim)

Goubins Attacke

Bemerkungen

- Betrachte von FIPS, ANSI, ISO/IEC und WTLS standardisierte Kurven
- Die meisten Kurven haben Punkte $(0, y)$
- Kurvenordung: $q, 2q, 4q, 6q$ (q prim)
- Attacke auch auf andere SPA-Gegenmaßnahmen anwendbar (Montgomery-Addition)

Andere Seitenkanalattacken

Timing-Attacken

- Gegen Signaturverfahren (z.B. ECDSA) nicht einsetzbar
- Keine erfolgreichen Attacken bekannt

Andere Seitenkanalattacken

Timing-Attacken

- Gegen Signaturverfahren (z.B. ECDSA) nicht einsetzbar
- Keine erfolgreichen Attacken bekannt

Analyse von elektromagnetischer Abstrahlung

- SEMA: Gegenmaßnahme „Double and add always“
- DEMA: ähnlich wie DPA

Andere Seitenkanalattacken

Fault Analysis Attacken

- Induzierung von Fehlern → Berechnung auf anderer Kurve
- Idee: Falsche Kurve ist kryptographisch unsicher

Andere Seitenkanalattacken

Fault Analysis Attacken

- Induzierung von Fehlern → Berechnung auf anderer Kurve
- Idee: Falsche Kurve ist kryptographisch unsicher
- Gegenmaßnahme: Ergebnis überprüfen

Andere Seitenkanalattacken

Fault Analysis Attacken

- Induzierung von Fehlern → Berechnung auf anderer Kurve
- Idee: Falsche Kurve ist kryptographisch unsicher
- Gegenmaßnahme: Ergebnis überprüfen
- Andere Idee: Vorzeichen der y-Koordinate ändern (Blömer, Otto, Seifert (2004))

Andere Seitenkanalattacken

Fault Analysis Attacken

- Induzierung von Fehlern → Berechnung auf anderer Kurve
- Idee: Falsche Kurve ist kryptographisch unsicher
- Gegenmaßnahme: Ergebnis überprüfen
- Andere Idee: Vorzeichen der y-Koordinate ändern (Blömer, Otto, Seifert (2004))
- Gegenmaßnahme: z.B. Montgomery-Addition

Zusammenfassung

- Kryptographie auf elliptischen Kurven ist mit Seitenkanalattacken angreifbar

Zusammenfassung

- Kryptographie auf elliptischen Kurven ist mit Seitenkanalattacken angreifbar
- Zahlreiche algorithmische Gegenmaßnahmen

Zusammenfassung

- Kryptographie auf elliptischen Kurven ist mit Seitenkanalattacken angreifbar
- Zahlreiche algorithmische Gegenmaßnahmen
- Gegenmaßnahmen kosten Effizienz

Zusammenfassung

- Kryptographie auf elliptischen Kurven ist mit Seitenkanalattacken angreifbar
- Zahlreiche algorithmische Gegenmaßnahmen
- Gegenmaßnahmen kosten Effizienz
- Nicht in jedem Fall Sicherheit gegen Seitenkanalattacken erreichbar

Zusammenfassung

- Kryptographie auf elliptischen Kurven ist mit Seitenkanalattacken angreifbar
- Zahlreiche algorithmische Gegenmaßnahmen
- Gegenmaßnahmen kosten Effizienz
- Nicht in jedem Fall Sicherheit gegen Seitenkanalattacken erreichbar

$\Longrightarrow$ Implementierungen für bestimmte Anwendungsbereiche entwickeln