

Warum sind elliptische Kurven für die Kryptographie so interessant?

Thomas Risse

Institut für Informatik & Automation, IIA
FB E&I, Hochschule Bremen, HSB

15. Januar im Jahr der Mathematik 2008

Einführung

Bausteine

Elliptische Kurven

Galois-Körper

$(E,+)$

Kryptographische
Anwendungen

Performance

Ausblick

Referenzen

Agenda

- 1 Einführung
- 2 Bausteine
- 3 Elliptische Kurven
- 4 Galois-Körper
- 5 Gruppenstruktur auf elliptischen Kurven
- 6 Kryptographische Anwendungen
- 7 Performance
- 8 Ausblick
- 9 Referenzen

Einführung

Bausteine

Elliptische Kurven

Galois-Körper

 $(E,+)$ Kryptographische
Anwendungen

Performance

Ausblick

Referenzen

Wir treiben Mathematik, um Anwendungsprobleme zu lösen.

Klassisches Beispiel für angewandte Mathematik:

Kryptographie

Evolution seit Caesar, Vigenère, DES, RSA, AES, ECC

vgl. z.B. www.weblearn.hs-bremen.de/risse/MAI/docs/puzzles.pdf

Angriff & Verteidigung

bei immer leistungsfähigeren 'Waffen' & 'Panzerungen'

statt auf multi core PC jetzt aber auch auf dem Handy

d.h. performance gap

the answer is: Elliptic Curve Cryptography, ECC!

definiere Abel'sche Gruppen auf elliptischen Kurven über Galois-Körpern; dort ist etwa das diskrete Logarithmus Problem extrem schwer zu lösen

Einführung

Bausteine

Elliptische Kurven

Galois-Körper

(E,+)

Kryptographische
Anwendungen

Performance

Ausblick

Referenzen

- Abel'sche/kommutative Gruppen wie $(\mathbb{Z}, +)$ oder $(\{e^{i\varphi} : \varphi \in \mathbb{R}\}, *)$ mit neutralem Element, inversen Elementen, Assoziativität und Kommutativität
- Körper, fields \mathbb{F} wie $(\mathbb{Q}, +, *)$ oder $(\mathbb{R}, +, *)$ d.h. $(\mathbb{F}, +)$ und $(\mathbb{F}^*, *)$ sind Abel'sche Gruppen, Distributivität
- endliche (!) Galois-Körper wie $(\{0, 1\}, +, *)$ oder allgemein \mathbb{GF}_p oder \mathbb{GF}_{p^m} , speziell \mathbb{GF}_{2^m}
- Elliptische Kurven E wie $y^2 = x^3 + ax + b$ über \mathbb{R} entsprechend auch über oder \mathbb{GF}_p oder \mathbb{GF}_{2^m}
- 'Addition' auf E , so daß $(E, +)$ Abel'sche Gruppe
- diskreter Logarithmus in endlichen Gruppen, etwa in $(\mathbb{Z}_p^*, *) = (\{1, 2, \dots, p-1\}, *)$ mit $*$ modulo p
z.B. $3^4 = 81 = 13 \in \mathbb{Z}_{17}$ und umgekehrt $\log_3 13 = 4$

seit 150 Jahren bekannt, schon Weierstraß¹ untersucht


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

Anwendung in der Kryptographie 1985 durch Miller und Koblitz

$$E = E_{a,b}(\mathbb{F}) = \{(x, y) \in \mathbb{F}^2 : y^2 = x^3 + ax + b\} \text{ für } a, b \in \mathbb{F}$$

definiert *elliptische Kurve über* \mathbb{F}

- zunächst $E = E_{a,b} = E_{a,b}(\mathbb{R}) \subset \mathbb{R}^2$
 Visualisierung per MATLABs
`ezplot('y^2=x^3+a*x+b')`
 für verschiedene Parameter a und b, $4a^3 + 27b^2 \neq 0$
- dann $E = E_{a,b} = E_{a,b}(\mathbb{F})$ für $\mathbb{F} = \mathbb{GF}_p$ oder $\mathbb{F} = \mathbb{GF}_{2^m}$

¹Karl Theodor Wilhelm Weierstrass (1815-1897) 

Galois²-Körper oder Galois-Felder sind *die* endlichen Körper.

\mathbb{GF}_p z.B. $\mathbb{GF}_2 = (\{0, 1\}, \vee, \wedge) = (\mathbb{Z}_2, +, *)$

allgemeiner $\mathbb{GF}_p = (\mathbb{Z}_p, +, *)$ für primes p

\mathbb{GF}_{p^m} nämlich $\mathbb{GF}_{p^m} = \{ \sum_{i=0}^{m-1} c_i x^i : c_i \in \mathbb{GF}_p \}$ mit

Polynom-Addition und -Multiplikation (modulo $\text{irp}(x)$)

Arithmetik in \mathbb{GF}_p bzw. in \mathbb{GF}_{p^m} ausprobieren!

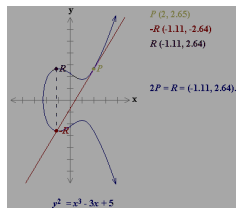
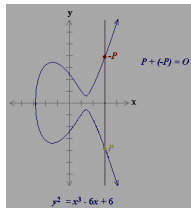
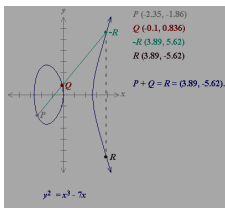
vgl. z.B. www.weblearn.hs-bremen.de/risse/MAI/docs/puzzles.pdf

Erwartungsgemäß ist \mathbb{GF}_{2^m} für Kryptographie besonders interessant . . .

Gruppenstruktur auf E

Jede nicht-senkrechte Gerade schneidet eine elliptische Kurve $E_{a,b}$ mit $4a^3 + 27b^2 \neq 0$ in genau drei Punkten³.

Unabhängig von \mathbb{F} kann man geometrisch und damit sehr anschaulich $E = E_{a,b}(\mathbb{F})$ als Gruppe auffassen, indem man eine 'Addition' und ein neutrales Element definiert:



Elliptische Kurven mit dieser 'Addition' sind Abel'sche Gruppen. Also gibt's (diskreten) Logarithmus & DLP!

³vgl. `elliptic_curves.m`

Kryptographische Anwendungen

Das Diskrete Logarithmus Problem, DLP, in Gruppe $(G, *)$

$$\text{zu } g, h \in G \text{ finde } n \text{ mit } g^n = \overbrace{g * g * \dots * g}^{n \text{ mal}} = h$$

lautet in $E = E_{a,b}(\mathbb{F})$ mit der oben eingeführten Addition +

$$\text{zu } P, Q \in E \text{ finde } n \in \mathbb{N} \text{ mit } nP = \overbrace{P + P + \dots + P}^{n \text{ mal}} = Q$$

„DLP ist für $1 \ll \text{card}(E)$ enorm schwer/aufwändig!“

z.B: Diffie-Hellman Schlüssel-Austausch: Alice & Bob
öffentlich sind $E(\mathbb{F})$ und public $P \in E$.

Alice bzw. Bob wählt zufälliges $a \in \mathbb{F}$ bzw. $b \in \mathbb{F}$.

Alice schickt aP an Bob; Bob schickt bP an Alice.

$b(aP) = G = a(bP) \in E$ ist dann gemeinsames Geheimnis!

Jahr	Schlüssellänge symmetrischer Verfahren	Asymmetrische Schlüssellänge (z.B. RSA)	Schlüssellängen von ECC	Erforderliche MIPS-Jahre	Erforderliche Jahre auf 450 Mhz PC
2000	70	952	132	$7.13 * 10^9$	$1.58 * 10^7$
2002	72	1028	137	$2.06 * 10^{10}$	$4.59 * 10^7$
2004	73	1108	141	$5.98 * 10^{10}$	$1.33 * 10^8$
2006	75	1191	145	$1.73 * 10^{11}$	$3.84 * 10^8$
2008	76	1279	149	$5.01 * 10^{11}$	$1.11 * 10^9$
2010	78	1369	153	$1.45 * 10^{12}$	$3.22 * 10^9$
2012	80	1464	157	$4.19 * 10^{12}$	$9.32 * 10^9$
2014	81	1562	162	$1.21 * 10^{13}$	$2.70 * 10^{10}$
2016	83	1664	166	$3.51 * 10^{13}$	$7.81 * 10^{10}$
2018	84	1771	170	$1.02 * 10^{14}$	$2.26 * 10^{11}$
2020	86	1881	175	$2.94 * 10^{14}$	$6.54 * 10^{11}$

S. www.cryptovision.com

Vergleich des Aufwands für Attacken (cracking)

RSA, DH, DSA subexponentiell

DLP über ECs exponentiell

S. <http://blogs.sun.com/jyrivirkki/resource/ECC-TLS-BOF-6958.pdf>

- schwache Kurven vermeiden, geeignete Kurven wählen
- Arithmetik in \mathbb{GF} beschleunigen: z.B. Normal-Basen
- Standardisierung (ANSI, FIPS, IEEE, ISO, NIST, SECG) berücksichtigen: ECIES, ECDH, ECDSA ...

jede Menge Software verfügbar: Certicom, MS, SUN, ...
schnelle Implementierungen auf SmartCard, handy, RFID, ...
auf FPGAs (s. z.B. DSI, <http://www.dsi-it.de>) finden!

Certicom: ECC is ideal in constrained environments; it is also ideal for use in high security environments.

NSA pushes elliptic-curve cryptography to secure small devices and lend support to interoperable communication networks.

SUN: Securing the Web with Elliptic Curve Cryptography

Virkki, SUN: Elliptic Curve Cryptography: The Future of SSL (TLS)

links

<http://cnscenter.future.co.kr/crypto/algorithm/ecc.htm>

Referenzen



Federal Information Processing Standards, FIPS:
Advanced Encryption Standard (AES); Publication 197

<http://csrc.nist.gov/>

[publications/fips/fips197/fips-197.pdf](http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf)

Advanced Encryption Standard Algorithm Validation List

<http://csrc.nist.gov/cryptval/aes/aesval.html>



cv cryptovision GmbH: ECC – Kryptographie auf Basis
elliptischer Kurven www.cryptovision.com



Daemen, Joan, Rijmen, Vincent: The Design of Rijndael –
AES, The Advanced Encryption Standard; Springer 2002



Federal Information Processing Standards, FIPS: Data
Encryption Standard (DES); Publication 46-3

<http://csrc.nist.gov/>

[publications/fips/fips46-3/fips46-3.pdf](http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf)

Referenzen



Federal Information Processing Standards, FIPS: Digital Signature Standard (DSS) – DSA, RSA, and ECDSA algorithms; Publication 186-2

<http://csrc.nist.gov/cryptval/dss.htm>



Hankerson, Darrel, Menezes, Alfred, Vanstone, Scott: Guide to Elliptic Curve Cryptography; Springer 2004



Lenstra, Arjen K., Verheul, Eric R.: Selecting Cryptographic Key Sizes; Journal of Cryptology, Springer 2001 vol 14, no 4, pp 255–293

s.a. <http://islab.oregonstate.edu/koc/ece575/papers/cryptosizes.pdf>



Oswald, Elisabeth: Introduction to Elliptic Curve Cryptography;

www.iaik.tugraz.at/aboutus/people/oswald/papers/Introduction_to_ECC.pdf

Referenzen



Risse, Thomas: Puzzles – Interaktive Mathematische Puzzles: Primzahlen, Divisionsreste, Galois Fields, Kryptographie, Kodierung, Pseudo-Zufallszahlen; Hochschule Bremen www.weblearn.hs-bremen.de/risse/MAI/docs/puzzles.pdf.



Risse, Thomas: ePuzzles – Interactive Mathematical Puzzles: Primes, Remainders, Galois Fields, Cryptography, Coding, Random Number Generation; Hochschule Bremen www.weblearn.hs-bremen.de/risse/MAI/docs/ePuzzles.pdf.



Standards for Efficient Cryptography Group, SECG: SEC1 – Elliptic Curve Cryptography; www.secg.org/collateral/sec1_final.pdf



Wagner, Neal R.: The Laws of Cryptography; www.cs.utsa.edu/~wagner/lawsbookcolor/laws.pdf