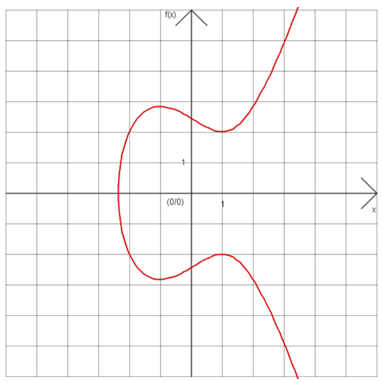
ECC:
Elliptic Curve Cryptography

Teil 2: Elliptische Kurven - Kryptographie

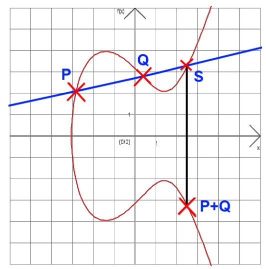
Universität Bremen

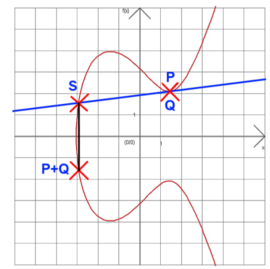
Albert Diner
Kilian Krys

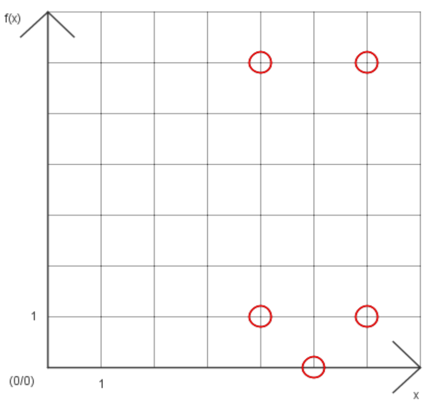
kurze Wiederholung von Teil 1



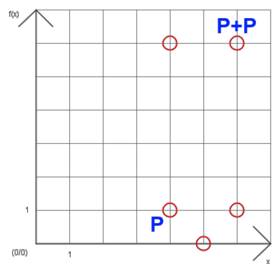
Elliptische Kurven in Z_R

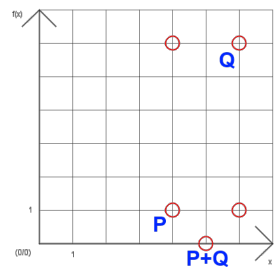






Elliptische Kurven auf endl. Körpern Z_P



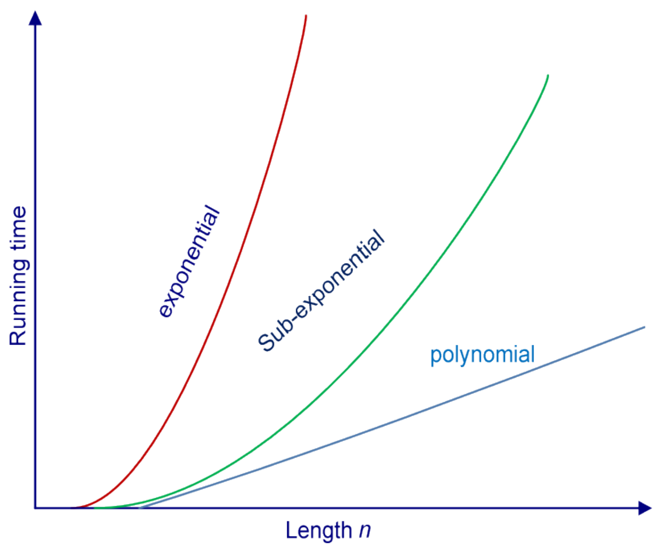


Operationen der Gruppe: Addition, skalare Multiplikation

Sicherheit der Krypto-Algorithmen

- RSA: Faktorisierungsproblem
  - der zeitlicher Aufwand ist subexponentiell

- Diffie-Hellman: Problem des Diskreten Logarithmus
  - auch hier subexponentielle Laufzeit



Quellen:
• Wikipedia. *Komplexitätstheorie*, 2013-04-27, URL: de.wikipedia.org/wiki/Komplexitätstheorie (Aufruf 2013-05-24).
• LIU, Fuwen. *A tutorial of elliptic curve cryptography (ECC)*, 2010, URL: www-rnks.informatik.tu-cottbus.de/de/node/1131 (Aufruf 2013-05-24).

ECC - Geschichte und Hintergrund

- 1985 unabhängig voneinander von Neal Koblitz und Victor Miller vorgeschlagen
- Verfahren, die auf DLP in endlichen Körpern basieren lassen sich einfach auf elliptische Kurven übertragen
- Anwendung hat immer höhere Bedeutung
- Erweiterung bei RSA: Verdopplung der Bits, ECC: ein paar Bits mehr

- Vorteile:
  - Schnellere Verschlüsselung und größere Flexibilität
  - Durch Effizienz besser in Situationen, wo Speicher und Rechenleistung begrenzt sind

Quellen:
- Wikipedia. *Elliptic curve cryptography*, 2013-05-02, URL: en.wikipedia.org/wiki/Elliptic_curve_cryptography (Aufruf 2013-05-25).
- NILLIES, Frank. *Kryptographie auf elliptischen Kurven am Beispiel von ElGamal und Menezes-Vanstone*, Proseminar Public-Key Kryptographie, 2006, URL: www2.cs.uni-paderborn.de/cs/ag-bloemer/lehre/proseminar_WS2005/material/Nillies_Ausarbeitung.pdf (Aufruf 2013-05-25).
- KOBLITZ, Ann Hibner; KOBLITZ, Neal; MENEZES, Alfred. Elliptic curve cryptography: The serpentine course of a paradigm shift. *Journal of Number Theory*, 2011, 131. Jg., Nr. 5, S. 781-814, URL: http://eprint.iacr.org/2008/390.pdf (Aufruf 2013-05-27).

Diffie-Hellman mit elliptischen Kurven (1)

Alice

Wählt zufällige Zahl A zwischen 1 und n-1

Berechnet α:=A·P

Berechnet K_{AB}:= A·β

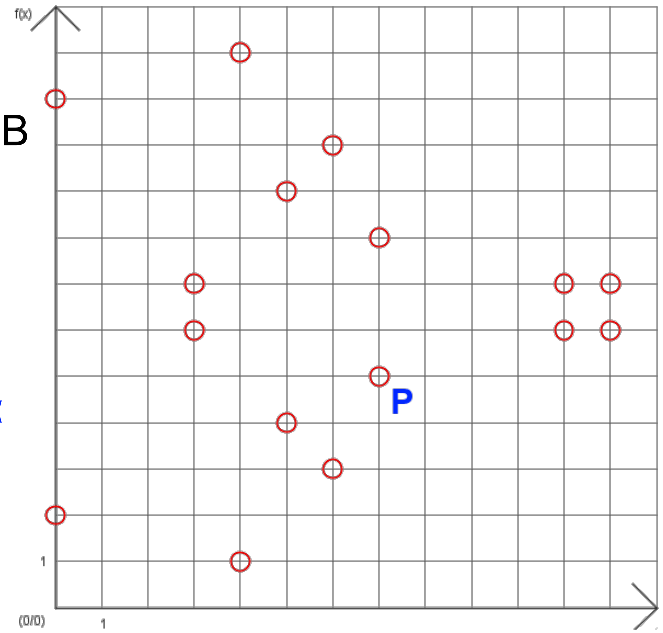
Bob

Wählt zufällige Zahl B zwischen 1 und n-1

Berechnet β:=B·P

Berechnet K_{BA}:= B·α

$A \cdot \beta = A \cdot (B \cdot P) = B \cdot (A \cdot P) = B \cdot \alpha$



Beide Kommunikationspartner einigen sich zur Beginn auf eine gemeinsame Kurve mit den gleichen Parametern (hier Primzahl p=13, Koeffizient a=6 und Koeffizient a=4) und wählen dort einen gemeinsamen Punkt P mit der Ordnung n aus.

Quelle:

- MCGREW, D. A.; IGOE, K. M.; SALTER, M. *Fundamental Elliptic Curve Cryptography Algorithms*, RFC 6090, February, 2011, Seite 10, URL: http://tools.ietf.org/html/rfc6090#page-10 (Abruf 2013-05-26).

Diffie-Hellman mit elliptischen Kurven (2)

Alice

Wählt zufällige Zahl A zwischen 1 und n-1

Berechnet $\alpha := A \cdot P$

Berechnet $K_{AB} := A \cdot \beta$

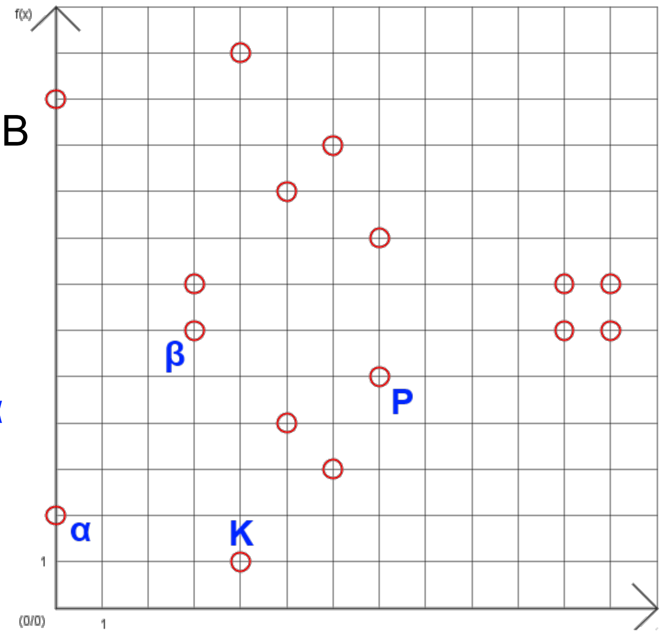
Bob

Wählt zufällige Zahl B zwischen 1 und n-1

Berechnet $\beta := B \cdot P$

Berechnet $K_{BA} := B \cdot \alpha$

$A \cdot \beta = A \cdot (B \cdot P) = B \cdot (A \cdot P) = B \cdot \alpha$



für A = 2, $P = (7,5)$

$\alpha := A \cdot P = 2 \cdot (7,5) = (0,2)$

$K_{AB} := A \cdot \beta = 2 \cdot (3,6) = \mathbf{(4,1)}$

für B = 3, $P = (7,5)$

$\beta := B \cdot P = (3,6)$

$K_{BA} := B \cdot \alpha = 3 \cdot (0,2) = \mathbf{(4,1)}$

Quelle:

• MCGREW, D. A.; IGOE, K. M.; SALTER, M. *Fundamental Elliptic Curve Cryptography Algorithms*, RFC 6090, February, 2011, Seite 10, URL: http://tools.ietf.org/html/rfc6090#page-10 (Abruf 2013-05-26).

ECDLP: Elliptic Curve Discrete Logarithm Problem (1)

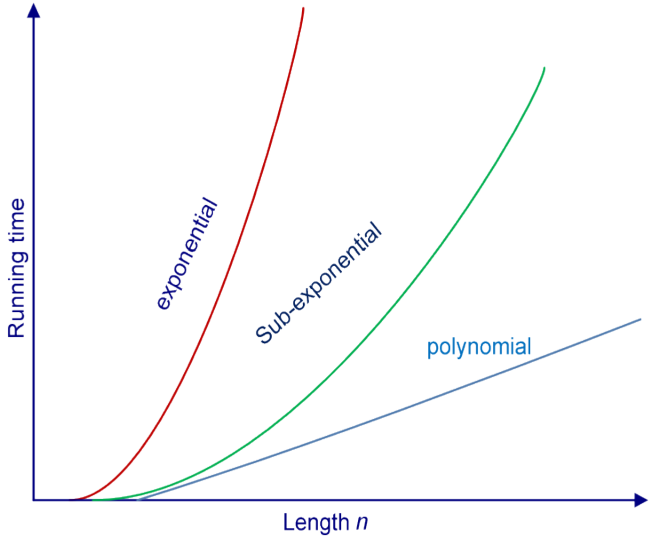
- E ist eine elliptische Kurve in Z_P
- E: $y^2 = x^3 + a \cdot x + b$
- mit a, b $\in Z_P$ und den Punkten P und K in $E(Z_P)$
- Aufgabe: finde eine Zahl m, sodass $K = m \cdot P$
- Naive Lösung: mit c als Zufallszahl, $c \cdot P$ berechnen, bis das Produkt das gleiche ist wie $K = m \cdot P$
- Erwartete Laufzeit hier ist O(p), da $\#E(Z_P) = O(p)$

Universität Bremen

Quellen:
- Wikipedia. *Elliptic Curve Cryptography*, 2013-05-05, URL: de.wikipedia.org/wiki/Elliptic_Curve_Cryptography (Aufruf 2013-05-25).
- Wikipedia. *Komplexitätstheorie*, 2013-04-27, URL: de.wikipedia.org/wiki/Komplexitätstheorie (Aufruf 2013-05-24).
- LIU, Fuwen. *A tutorial of elliptic curve cryptography (ECC)*, 2010, URL: www-rnks.informatik.tu-cottbus.de/de/node/1131 (Aufruf 2013-05-24).

ECDLP: Elliptic Curve Discrete Logarithm Problem (2)

- Die schnellsten bekannten Algorithmen die das Problem lösen sind:
  - Babystep-Giantstep-Algorithmus
  - Pollard-Rho-Methode
- Laufzeit* $O(2^{n/2})$
- exponentielle Laufzeit:
  $O(d^n)$ für $d > 1$



Quellen: * Wikipedia. *Elliptic Curve Cryptography*, 2013-05-05, URL: de.wikipedia.org/wiki/Elliptic_Curve_Cryptography (Aufruf 2013-05-25).
• Wikipedia. *Komplexitätstheorie*, 2013-04-27, URL: de.wikipedia.org/wiki/Komplexitätstheorie (Aufruf 2013-05-24).
• LIU, Fuwen. *A tutorial of elliptic curve cryptography (ECC)*, 2010, URL: www-rnks.informatik.tu-cottbus.de/de/node/1131 (Aufruf 2013-05-24).

Vergleich der Herausforderungen

- Die 232-stellige Zahl RSA-768 wurde 2009 in Primfaktoren zerlegt.
  - Aufwand: ca. 2,5 Jahre mit mehreren hundert Rechnern.
- Die Herausforderung mit ECC-p-109 wurde 2002 gelöst und ECC-2^m-109 wurde 2004 gelöst.
  - An der Herausforderung mit ECC-2^m-109 rechneten 2.600 Computer 17 Monate lang.

Quellen:
- Wikipedia. *RSA Factoring Challenge*, 2013-04-04, URL: de.wikipedia.org/wiki/RSA_Factoring_Challenge (Aufruf 2013-05-25)
- KLEINJUNG, Thorsten, et al. Factorization of a 768-bit RSA modulus. In: *Advances in Cryptology–CRYPTO 2010*. Springer Berlin Heidelberg, 2010. S. 333-350.
- MEIER, Willi; STAFFELBACH, Othmar. Kryptographie und elliptische Kurven. *Elemente der Mathematik*, 1997, 52. Jg., Nr. 4, S. 137-151.
- <kes> online. *109-Bit-ECC-Challenge gelöst*, 2004-04-29, URL: www.kes.info/archiv/online/040429-ecc109.htm (Aufruf 2013-05-25).
- Certicom Research. *Certicom ECC Challenge*, 2009-09-10, URL: www.certicom.com/images/pdfs/challenge-2009.pdf (Aufruf 2013-05-25).

Ungeeignete Kurven

- Kurven geringer Ordnung
- singuläre Kurven
- anomale Kurven
  - $\#E(Z_P) = p$
- Allgemein: Jede Kurve, die auf irgendeine Art "speziell" ist

Quellen:
- HAINZ, Christian. *Kryptographie und elliptische Kurven*, Ausarbeitung zum Vortrag, 2001, URL: http://homepages.thm.de/~hg10013/Lehre/MMS/SS01_WS0102/Elyps/ (Abruf 2013-05-26).
- GREBE, Ingo. *Elliptische Kurven in der Kryptographie*, Seminar Kryptographie und Datensicherheit, Präsentation, Universität Potsdam, 2005-07-07, URL: www.cs.uni-potsdam.de/ti/lehre/05-Kryptographie/slides/Elliptische_Kurven.pdf (Abruf 2013-05-26).
- KOBLITZ, Ann Hibner; KOBLITZ, Neal; MENEZES, Alfred. Elliptic curve cryptography: The serpentine course of a paradigm shift. *Journal of Number Theory*, 2011, 131. Jg., Nr. 5, S. 781-814, URL: http://eprint.iacr.org/2008/390.pdf (Aufruf 2013-05-27).

Kurvenbeispiele

- Zufallskurven
  - zuerst die Parameter zufällig wählen
  - danach Punkteanzahl bestimmen
  - Kurven miteinander vergleichen und die beste wählen
- Methode der Komplexen Multiplikation (CM)*
- Koblitz-Kurven*

* momentan noch geeignet, könnte sich aber in Zukunft ändern

Quellen:
• HAINZ, Christian. *Kryptographie und elliptische Kurven*, Ausarbeitung zum Vortrag, 2001, URL: http://homepages.thm.de/~hg10013/Lehre/MMS/SS01_WS0102/Elyps/ (Abruf 2013-05-26).
• KOBLITZ, Ann Hibner; KOBLITZ, Neal; MENEZES, Alfred. Elliptic curve cryptography: The serpentine course of a paradigm shift. *Journal of Number Theory*, 2011, 131. Jg., Nr. 5, S. 781-814, URL: http://eprint.iacr.org/2008/390.pdf (Aufruf 2013-05-27).

Geeignete Kurven (1)

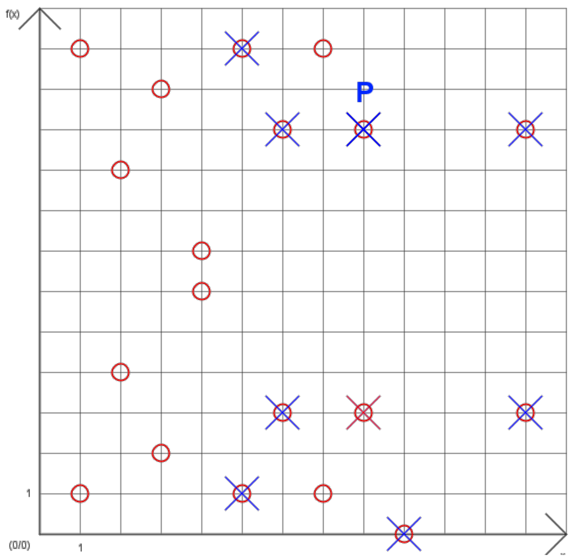
- Anzahl der Punkte auf der Kurve
  - (am besten mehr als 2^{160})
- p sollte eine Primzahl sein oder einen großen Primteiler enthalten

- Passende Werte für folgende Parameter finden:
  - Primzahl p, Parameter a und b
  - Startpunkt P = (x_P, y_P)
  - Ordnung **n** der von P erzeugten Untergruppe

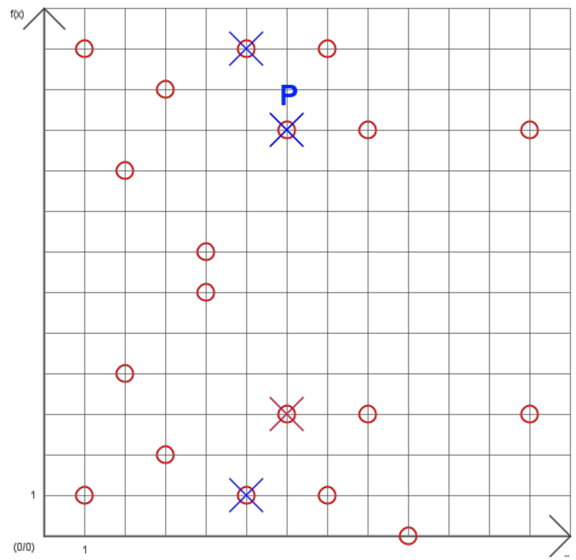
Quellen:
• NILLIES, Frank. *Kryptographie auf elliptischen Kurven am Beispiel von ElGamal und Menezes-Vanstone*, Proseminar Public-Key Kryptographie, 2006, URL: www2.cs.uni-paderborn.de/cs/ag-bloemer/lehre/proseminar_WS2005/material/Nillies_Ausarbeitung.pdf (Aufruf 2013-05-25).
• GRÜßIEN, Berit. *Einführung: Elliptische Kurven in der Kryptologie*, Seminar "Moderne Kryptosysteme", 2006-10-15, URL: www.ki.informatik.hu-berlin.de/algorithmenII/Lehre/ss06/modern_krypt/EllipstischeKurven.pdf (Aufruf 2013-05-25).
• HAINZ, Christian. *Kryptographie und elliptische Kurven*, Ausarbeitung zum Vortrag, 2001, URL: http://homepages.thm.de/~hg10013/Lehre/MMS/SS01_WS0102/Elyps/ (Abruf 2013-05-26).

Bsp: von P erzeugte Untergruppen

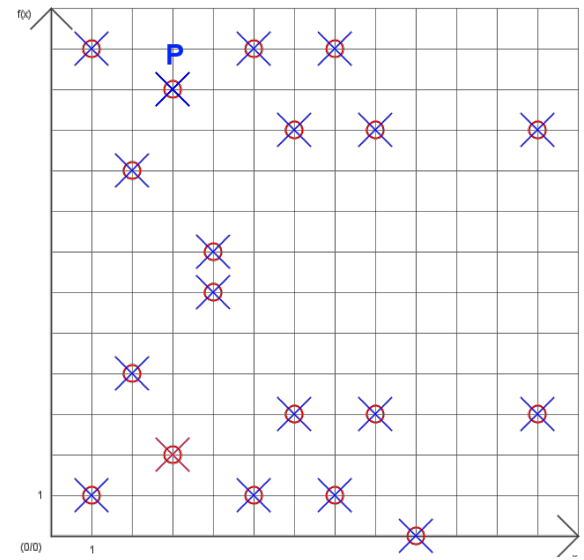
p = 13, a = 8, b = 5



P = (8,10)
Ordn. UG(P) = 10



P = (6,10)
Ordn. UG(P) = 5



P = (3,11)
Ordn. UG(P) = 20

Quelle:
- cv cryptovision GmbH. *ECC – Kryptographie auf Basis elliptischer Kurven*, Eine kurze Einführung, 2009, URL: www.cryptovision.com/fileadmin/media/documents/Whitepaper_Produkte/02-Whitepaper-Technical-ECC_EN.pdf (Abruf 2013-05-26).

Geeignete Kurven (2) - Standards

- Normierungsstellen schlagen optimale Werte für die einzelnen Parameter p, a, b, n, x_P, y_P vor
- Vorschläge in Standards / Dokumenten:
  - RFC 6090
  - NIST - "Recommended Elliptic Curves for Federal Government use" (1999)
  - SECG - "SEC 2: Recommended Elliptic Curve Domain Parameters" (2000)
  - ECC Brainpool - "ECC Brainpool Standard Curves and Curve Generation" (2005)

Quelle:
• GREBE, Ingo. *Elliptische Kurven in der Kryptographie*, Seminar Kryptographie und Datensicherheit, Präsentation, Universität Potsdam, 2005-07-07, URL: www.cs.uni-potsdam.de/ti/lehre/05-Kryptographie/slides/Elliptische_Kurven.pdf (Abruf 2013-05-26).

Geeignete Kurven (3) - Standards

- **SECG** empfiehlt in SEC 2 folgende Parameter:
  - für **256-bit ECC (secp256r1)**:
    - **p** = FFFFFFFF 00000001 00000000 00000000 00000000 FFFFFFFF FFFFFFFF FFFFFFFF
    - **a** = FFFFFFFF 00000001 00000000 00000000 00000000 FFFFFFFF FFFFFFFF FFFFFFFC
    - **b** = 5AC635D8 AA3A93E7 B3EBBD55 769886BC 651D06B0 CC53B0F6 3BCE3C3E 27D2604B
    - **n** = FFFFFFFF 00000000 FFFFFFFF FFFFFFFF BCE6FAAD A7179E84 F3B9CAC2 FC632551
    - **P** = 04 6B17D1F2 E12C4247 F8BCE6E5 63A440F2 77037D81 2DEB33A0 F4A13945 D898C296 4FE342E2 FE1A7F9B 8EE7EB4A 7C0F9E16 2BCE3357 6B315ECE CBB64068 37BF51F5

Quelle:
• Certicom Research. *SEC 2: Recommended Elliptic Curve Domain Parameters*, Standards for Efficient Cryptography, Version 1.0, 2000-09-20, URL: www.secg.org/collateral/sec2_final.pdf (Aufruf 2013-05-26).

Geeignete Kurven (4) - Standards

- **RFC 6090** nennt folgende Parameter
  - **für 156-bit ECC**
    - **p** = FFFFFFFF 00000001 00000000 00000000 00000000 FFFFFFFF FFFFFFFF FFFFFFFF
    - **a** = -3
    - **b** = 5AC635D8 AA3A93E7 B3EBBD55 769886BC 651D06B0 CC53B0F6 3BCE3C3E 27D2604B
    - **n** = FFFFFFFF 00000000 FFFFFFFF FFFFFFFF BCE6FAAD A7179E84 F3B9CAC2 FC632551
    - $\mathbf{x_P}$ = 6B17D1F2 E12C4247 F8BCE6E5 63A440F2 77037D81 2DEB33A0 F4A13945 D898C296
    - $\mathbf{y_P}$ = 4FE342E2 FE1A7F9B 8EE7EB4A 7C0F9E16 2BCE3357 6B315ECE CBB64068 37BF51F5

Quelle:
• MCGREW, D. A.; IGOE, K. M.; SALTER, M. *Fundamental Elliptic Curve Cryptography Algorithms*, RFC 6090, February, 2011, Seite 31, URL: http://tools.ietf.org/html/rfc6090#page-31 (Abruf 2013-05-26).

Digitale Signaturen mit elliptischen Kurven nach RFC 6090 (1)

Signatur erstellen:

P: gemeinsamer Punkt P auf der elliptischen Kurve Z_P mit Ordnung n

h(m): Hashwert der Nachricht m, berechnet mit einer zuvor vereinbarten Hashfunktion

wähle Privaten Schlüssel a zwischen 1.. n-1

Öffentlicher Schlüssel $\alpha := a \cdot P$

1. wähle k zwischen 1.. n-1 $\Rightarrow$ $R = (x_R, y_R) = P \cdot k$
2. $s_1 = x_R \bmod n \neq 0$ (Wenn doch $\Rightarrow$ zurück zu Punkt 1)
3. $s_2 = (h(m) + a \cdot s_1) \cdot k^{-1} \bmod n \neq 0$ (Wenn doch $\Rightarrow$ zurück zu Punkt 1)
4. Signatur $S = (s_1, s_2)$

Quellen:
• MCGREW, D. A.; IGOE, K. M.; SALTER, M. *Fundamental Elliptic Curve Cryptography Algorithms*, RFC 6090, February, 2011, Seite 12, URL: http://tools.ietf.org/html/rfc6090#page-12 (Abruf 2013-05-26).
• SPITZ, Stephan; PRAMATEFTAKIS, Michael; SWOBODA, Joachim. *Kryptographie und IT-Sicherheit: Grundlagen und Anwendungen*. Vieweg+ Teubner Verlag, 2011, S. 146-147.

Digitale Signaturen mit elliptischen Kurven nach RFC 6090 (2)

Signatur verifizieren:

1. if $(0 < s_1 < n)$and$(0 < s_2 < n)$ $\Rightarrow$ weiter, sonst nicht verifizierbar
2. $s_2^{-1} = 1 / s_2 \bmod n$
3. $u_1 = h(m) \cdot s_2^{-1} \bmod n$ $u_2 = s_1 \cdot s_2^{-1} \bmod n$
4. $R' = (x_{R'}, y_{R'}) = u_1 \cdot P + u_2 \cdot \alpha$
5. if $(x_{R'} \bmod q) == s_1$ $\Rightarrow$ verifiziert

Nachweis der Verifikationsbedingung:

$$R' = u_1 \cdot P + u_2 \cdot \alpha = u_1 \cdot P + u_2 \cdot a \cdot P = (u_1 + u_2 \cdot a) \cdot P = (h(m) \cdot s_2^{-1} + s_1 \cdot s_2^{-1} \cdot a) \cdot P$$

$$= (h(m) + s_1 \cdot a) \cdot s_2^{-1} \cdot P = (h(m) + s_1 \cdot a) \cdot (h(m) + s_1 \cdot a)^{-1} \cdot (k^{-1})^{-1} \cdot P = k \cdot P = R$$

Quellen:
• MCGREW, D. A.; IGOE, K. M.; SALTER, M. *Fundamental Elliptic Curve Cryptography Algorithms*, RFC 6090, February, 2011, Seite 12, URL: http://tools.ietf.org/html/rfc6090#page-12 (Abruf 2013-05-26).
• Wikipedia. *Elliptic Curve DSA*, 2013-03-08, URL: en.wikipedia.org/wiki/Elliptic_Curve_DSA#Correctness_of_the_Algorithm (Aufruf 2013-05-27).

Certicom

- Spezialisiert auf Kryptographie
- Gegründet: 1985 von G. Agnew, R. Mullin, S. Vanstone
- 2009 von RIM (BlackBerry) für ca. 105 Mio USD aufgekauft
- Parallel gab es auch ein Angebot von VeriSign

- Seit Übernahme: ECC ist Hauptbestandteil der BlackBerry Sicherheitsarchitektur

- Mehr als 350 Patente Weltweit
  - Davon laut NSA über 130 für ECC

Quellen:
- ARGHIRE, Ionut. *Certicom Accepts RIM's Acquisition Offer*. 2009-02-11, URL: http://news.softpedia.com/news/Certicom-Accepts-RIM-039-s-Acquisition-Offer-104273.shtml (Aufruf 2013-05-27).
- Wikipedia. *BlackBerry (company)*. 2013-05-23, URL: http://en.wikipedia.org/wiki/BlackBerry_(company)#Certicom (Aufruf 2013-05-27).
- KOBLITZ, Ann Hibner; KOBLITZ, Neal; MENEZES, Alfred. Elliptic curve cryptography: The serpentine course of a paradigm shift. *Journal of Number Theory*, 2011, 131. Jg., Nr. 5, S. 781-814, URL: http://eprint.iacr.org/2008/390.pdf (Aufruf 2013-05-27).

Patente (1)

- insgesamt über 130 Patente für ECC
  - davon wurden 26 von der NSA lizenziert

- Patentierte Verfahren:
  - Schlüsselaustausch
  - Komprimierung von Punkten
  - Verwendung einer bestimmten Anzahl von Bits
  - ...

Quellen:
- KJÆRSGAARD, Jan Ulrich; Landrock, Peter. *Patents on Elliptic Curves*, 2011-09-09, URL: www.cryptomathic.com/news-events/blog/patents-on-elliptic-curves (Aufruf 2013-05-25).
- RSA Laboratories. *6.3 Patents on Cryptography*, URL: www.rsa.com/rsalabs/node.asp?id=2321 (Aufruf 2013-05-25)
- D. J. Bernstein. *Irrelevant patents on elliptic-curve cryptography* URL: http://cr.yp.to/ecdh/patents.html (Aufruf 2013-05-25)
- Wikipedia. *ECC patents*, 2013-04-11, URL: https://en.wikipedia.org/wiki/ECC_patents (Aufruf 2013-05-25)

Patente (2) - MQV

- Benannt nach Menezes, Qu und Vanstone
- Protokoll für authentifizierten Schlüsselaustausch

- ECMQV: MQV mit elliptischen Kurven
- Sicherheitsprobleme!
  - Nachfolger: HMQV, FHMQV

- MQV 2005 von NSA für 25 mio USD lizensiert
  - Verwendet für NSA Suite B Algorithmus

Quellen:
• KRAWCZYK, Hugo. *HMQV: A High-Performance Secure Diffie-Hellman Protocol,* Cryptology ePrint Archive, Report 2005/176, 2005, URL: http://eprint.iacr.org/2005/176.pdf (Abruf 2013-05-26).
• BARKER, Elaine; CHEN, Lily; SMID, Miles; Allen ROGINSKY, Allen. *Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography (Draft Revision)*, NIST Special Publication 800-56A, 2012, Seite 51ff.
• LIU, Fuwen. *A tutorial of elliptic curve cryptography (ECC)*, 2010, Seite 49ff, URL: www-rnks.informatik.tu-cottbus.de/de/node/1131 (Aufruf 2013-05-24).
• Certicom Research. *SEC 1: Elliptic Curve Cryptography*, Standards for Efficient Cryptography, Version 2.0, 2009-03-21, Seite 58-60, Seite 76f, URL: http://www.secg.org/download/aid-780/sec1-v2.pdf (Aufruf 2013-05-26).

Patente (3) - ECMQV Protokoll

P: gem. Punkt auf der elliptischen Kurve Z_P mit Ordnung n h:= $\#E(Z_P) / n$

q_A, q_B: privater Schlüssel ($1 \le q \le n-1$) Q_A, Q_B: öffentlicher Schlüssel $Q_A = q_A \cdot P$ $Q_B = q_B \cdot P$

KDF: gemeinsam vereinbarte Schlüsselableitungsfunktion ID_A, ID_B: Identifizierungswert

Alice

1. wählt zufällige Zahl a ($1 \le a \le n-1$)
   Berechnet $\alpha := a \cdot P$, sendet α, ID_A an Bob

3. $S_A = (a + x_\alpha \cdot q_A) \bmod n$
   $Z = h \cdot S_A(\beta + x_\beta \cdot Q_B)$
   $(k_1, k_2) \Leftarrow KDF(x_Z)$
   $t = MAC_{k1}(2, ID_B, ID_A, \beta, \alpha)$
   Prüft ob $t = t_B$
   $t_A = MAC_{k1}(3, ID_A, ID_B, \alpha, \beta)$
   sendet t_A an Bob

Bob

2. wählt zufällige Zahl b ($1 \le b \le n-1$)
   Berechnet $\beta := b \cdot P$
   $S_B = (b + x_\beta \cdot q_B) \bmod n$
   $Z = h \cdot S_B (\alpha + x_\alpha \cdot Q_A)$
   $(k_1, k_2) \Leftarrow KDF(x_Z)$
   $t_B = MAC_{k1}(2, ID_B, ID_A, \beta, \alpha)$
   sendet ID_B, β, t_B an Alice

4. $t = MAC_{k1}(3, ID_A, ID_B, \alpha, \beta)$
   prüft ob $t = t_A$

Quellen:
• HANKERSON, Darrel; MENEZES, Alfred J.; VANSTONE, Scott. *Guide to elliptic curve cryptography*. Springer, 2004, Seite 195f.
• MENEZES, Alfred; USTAOGLU, Berkant. On the importance of public-key validation in the MQV and HMQV key agreement protocols. In: *Progress in Cryptology-INDOCRYPT 2006*. Springer Berlin Heidelberg, 2006. S. 135, URL: www.cryptolounge.net/pdf/MU06.pdf (Aufruf 2013-05-27).

Patente (4) - Point Compression

- Punkte werden komprimiert, um Bandbreite zu sparen
- die Y-Koordinate eines Punktes kann in Abhängigkeit von der X-Koordinate beschrieben werden
- funktioniert ähnlich wie bei einem Polynom zweiter Ordnung $y^2 = x^3 + ax + b$, um beide Nullstellen zu berechnen
  - $y_{1,2}=\pm\sqrt{(x^3 + ax + b)}$
- also ist nur wichtig zu wissen ob y_1 oder y_2 bei der Y-Koordinate rauskommen soll, also zur X-Koordinate wird noch ein zusätzlicher 1-bit-Wert benötigt

Quellen:
• KING, Brian. A point compression method for elliptic curves defined over GF (2 n). In: *Public Key Cryptography–PKC 2004*. Springer Berlin Heidelberg, 2004. S. 333-345.
• MAVROGIANNOPOULOS, Nikos. *Do we need elliptic curve point compression?*, 2012-01-01, URL: http://nmav.gnutls.org/2012/01/do-we-need-elliptic-curve-point.html (Aufruf 2013-05-25).
• NILLIES, Frank. *Kryptographie auf elliptischen Kurven am Beispiel von ElGamal und Menezes-Vanstone*, Proseminar Public-Key Kryptographie, 2006, URL: www2.cs.uni-paderborn.de/cs/ag-bloemer/lehre/proseminar_WS2005/material/Nillies_Ausarbeitung.pdf (Aufruf 2013-05-25).
• LOPEZ, Julio; DAHAB, Ricardo. *Point Compression Algorithms for Binary Curves*, Präsentation, 2005-04-14, URL: http://cs.ucsb.edu/~koc/ccs130h/projects/03-ecc-protocols/Julio_Slides.pdf (Aufruf 2013-05-26).

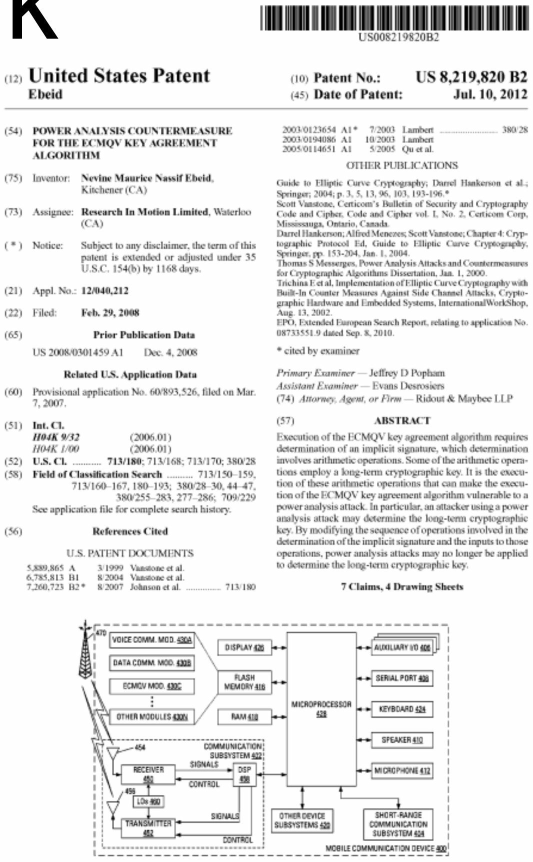
Patentsituation: vgl. ECC und RSA

- laut RSA-Security bei ECC (Z_P) nur Implementierung patentiert, nicht das Verfahren
- RSA: Verfahren patentiert, nicht die Implementierung

Quelle:
• LIU, Fuwen. *A tutorial of elliptic curve cryptography (ECC)*, 2010, Seite 51ff, URL: www-rnks.informatik.tu-cottbus.de/de/node/1131 (Aufruf 2013-05-24).

Alternative ECC Varianten ohne Patentproblematik

- Welche Patente laufen wann ab?
  - Point Compression: Patentiert von HP Aug. 1998 (US6252960)*
    - läuft ab im Juni 2018
  - Teil von ECMQV: patentiert von RIM im Feb. 2008 (US8219820)**
    - läuft ab im Feb. 2028
- alternative Varianten ohne Patente
  - ECC Bibliothek in Java und .NET, OpenSSL, ...



US008219820B2

(12) **United States Patent**
Ebeid

(10) **Patent No.:** **US 8,219,820 B2**
(45) **Date of Patent:** **Jul. 10, 2012**

(54) **POWER ANALYSIS COUNTERMEASURE FOR THE ECMQV KEY AGREEMENT ALGORITHM**

(75) Inventor: **Nevine Maurice Nassif Ebeid**, Kitchener (CA)

(73) Assignee: **Research In Motion Limited**, Waterloo (CA)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 1168 days.

(21) Appl. No.: **12/040,212**

(22) Filed: **Feb. 29, 2008**

(65) **Prior Publication Data**

US 2008/0301459 A1 Dec. 4, 2008

Related U.S. Application Data

(60) Provisional application No. 60/893,526, filed on Mar. 7, 2007.

(51) **Int. Cl.**
H04K 9/32 (2006.01)
H04K 1/00 (2006.01)

(52) **U.S. Cl.** **713/180**; 713/168; 713/170; 380/28

(58) **Field of Classification Search** 713/150–159, 713/160–167, 180–193; 380/28–30, 44–47, 380/255–283, 277–286; 709/229
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,889,865 A 3/1999 Vanstone et al.
6,785,813 B1 8/2004 Vanstone et al.
7,260,723 B2 * 8/2007 Johnson et al. 713/180
2003/0123654 A1 * 7/2003 Lambert 380/28
2003/0194086 A1 10/2003 Lambert
2005/0114651 A1 5/2005 Qu et al.

OTHER PUBLICATIONS

Guide to Elliptic Curve Cryptography; Darrel Hankerson et al.; Springer; 2004; p. 3, 5, 13, 96, 103, 193-196.*
Scott Vanstone, Certicom's Bulletin of Security and Cryptography Code and Cipher, Code and Cipher vol. I, No. 2, Certicom Corp, Mississauga, Ontario, Canada.
Darrel Hankerson; Alfred Menezes; Scott Vanstone; Chapter 4: Cryptographic Protocol Ed, Guide to Elliptic Curve Cryptography, Springer, pp. 153-204, Jan. 1, 2004.
Thomas S Messerges, Power Analysis Attacks and Countermeasures for Cryptographic Algorithms Dissertation, Jan. 1, 2000.
Trichina E et al, Implementation of Elliptic Curve Cryptography with Built-In Counter Measures Against Side Channel Attacks, Cryptographic Hardware and Embedded Systems, InternationalWorkShop, Aug. 13, 2002.
EPO, Extended European Search Report, relating to application No. 08733551.9 dated Sep. 8, 2010.

* cited by examiner

Primary Examiner — Jeffrey D Popham
Assistant Examiner — Evans Desrosiers
(74) *Attorney, Agent, or Firm* — Ridout & Maybee LLP

(57) **ABSTRACT**

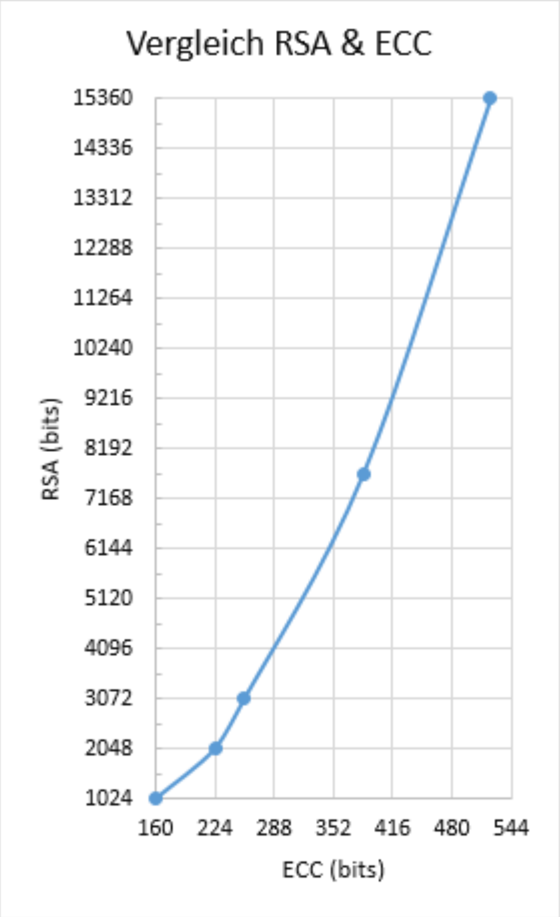
Execution of the ECMQV key agreement algorithm requires determination of an implicit signature, which determination involves arithmetic operations. Some of the arithmetic operations employ a long-term cryptographic key. It is the execution of these arithmetic operations that can make the execution of the ECMQV key agreement algorithm vulnerable to a power analysis attack. In particular, an attacker using a power analysis attack may determine the long-term cryptographic key. By modifying the sequence of operations involved in the determination of the implicit signature and the inputs to those operations, power analysis attacks may no longer be applied to determine the long-term cryptographic key.

7 Claims, 4 Drawing Sheets

Quellen: • NationMaster. *Elliptic curve cryptography*. URL: www.nationmaster.com/encyclopedia/Elliptic-curve-cryptography#Implementations (Aufruf 2013-05-28).
* SEROUSSI, Gadiel. *Compression and decompression of elliptic curve data points.* U.S. Patent Nr. 6,252,960, 2001, URL: www.google.com/patents/US6252960 (Aufruf 2013-05-24).
** EBEID, Nevine Maurice Nassif, et al. *Power analysis countermeasure for the ECMQV key agreement algorithm.* U.S. Patent Nr. 8,219,820, 2012, URL: www.google.com/patents/US8219820 (Aufruf 2013-05-24).

NIST empfiehlt

Symmetric Key Size (bits)	RSA and Diffie-Hellman Key Size (bits)	Elliptic Curve Key Size (bits)	Ratio of DH Cost : EC Cost
80	1024	160	3:1
112	2048	224	6:1
128	3072	256	10:1
192	7680	384	32:1
256	15360	521	64:1



Quelle:
• National Security Agency. *The Case for Elliptic Curve Cryptography*, 2009-01-15, URL: www.nsa.gov/business/programs/elliptic_curve.shtml (Aufruf 2013-05-24).

Schlüssellängen-Empfehlungen im Vergleich

empfohlen von	Zeitraum	Symmetrisch	Asymmetrisch	ECC
ECRYPT II	2011-2015	80	1248	160
	2016-2020	96	1776	192
NIST	2011-2030	112	2048	224
ANSSI	2010-2020	100	2048	200
BSI	2011-2015	-	1976	224
	> 2019	-	1976	250
Durchschnitt bis 2020		*103*	*1962*	*217*

Quelle:
• GIRY, Damien. *Cryptographic Key Length Recommendation*, URL: www.keylength.com/en/compare/ (Aufruf 2013-05-25).

SSL mit RSA vs SSL mit ECC

- Vordergrund der Studie war ein Vergleich der Leistung von Schlüsselaustausch in SSL mit RSA vs. ECC
- Schlüsselaustausch mit RSA (auf Servern) in SSL sehr rechenintensiv, Idee von Dienstleistern: dies evtl. sogar auf entsprechender Hardware auszulagern
- Alternative zur RSA - also ECC - sollte ohne zusätzliche Hardware eine Verbesserung bringen

Quelle:
• GUPTA, Vipul; et al. Speeding up secure Web transactions using elliptic curve cryptography. In: *11th Annual Network and Distributed System Security Symposium (NDSS 2004)*, 2004.

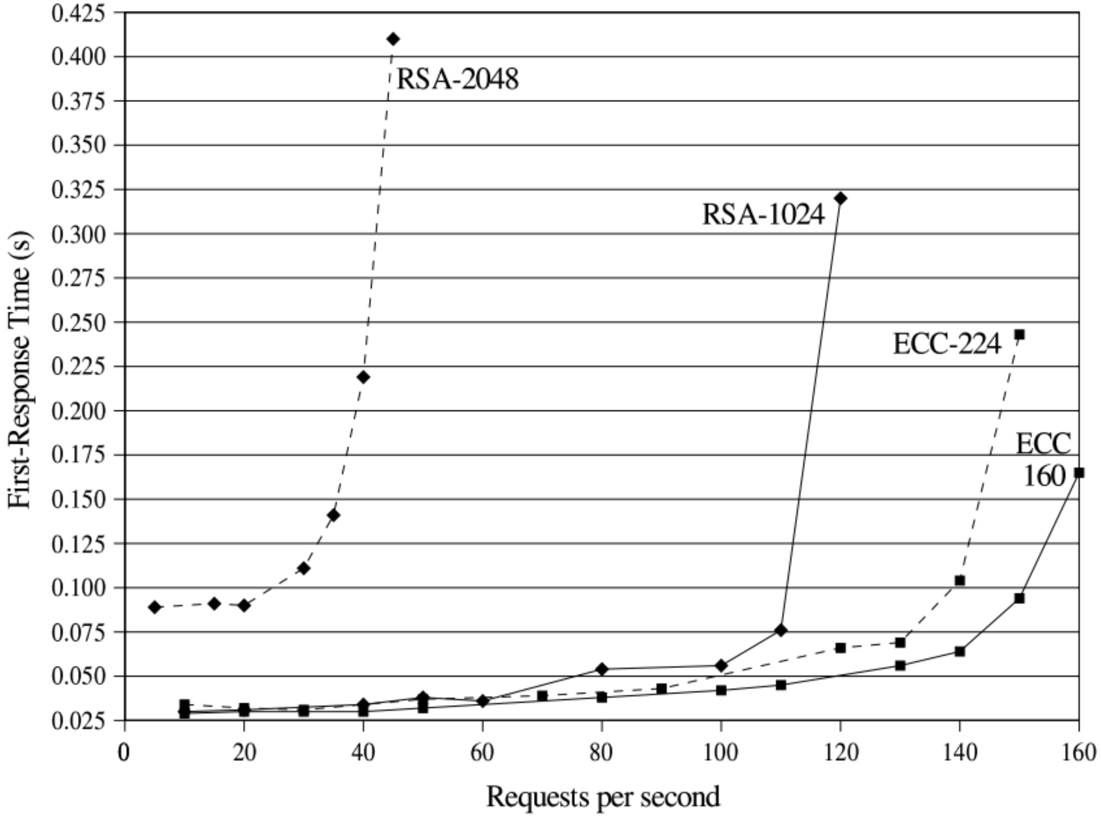
Ergebnisse der Studie (Benchmark)

	ECC-160	RSA-1024	ECC-192	RSA-1536	ECC-224	RSA-2048
Ops / sec	271,3	114,3	268,5	36,4	195,5	17,8
Performance ratio	2,4 : 1		7,4 : 1		21,4 : 1	
Key-size ratio	1 : 6,4		1 : 8		1 : 9,1	

- Ergebnis: Apache Web-Server mit OpenSSL erweitert mit ECC kann 11%-31% mehr HTTPS-Anfragen verarbeiten als mit RSA. Die Schlüssellänge von ECC-224 müsste mindestens bis zum Jahr 2020 als ausreichend sicher gelten.
- Hardware/Software: Sun Fire V480 mit 900 MHz UltraSPARC III Prozessor und 2GB RAM, Solaris 9, Apache 2.0.45 web server kompiliert mit OpenSSL

Quelle:
• GUPTA, Vipul; et al. Speeding up secure Web transactions using elliptic curve cryptography. In: *11th Annual Network and Distributed System Security Symposium (NDSS 2004)*, 2004.

Vergleich der Antwortzeiten



Universität Bremen

Quelle:
• GUPTA, Vipul; et al. Speeding up secure Web transactions using elliptic curve cryptography. In: *11th Annual Network and Distributed System Security Symposium (NDSS 2004)*, 2004.

Benchmarks von Intel (2012)

Domain	OpenSSL v1.0.0a Test	Unit	Vanilla	Patched	P/V
gf2	speed ecdhk233	[op/s]	1374.1	7036.9	5.2
	speed ecdsak233	[sign/s]	1099.8	3036.8	2.8
		[verify/s]	660.3	3256.7	5.0
	speed ecdhb233	[op/s]	1309.4	7407.8	5.7
	speed ecdsab233	[sign/s]	1095.8	3026.4	2.8
		[verify/s]	631.7	3402.4	5.4
gfp	speed ecdhp224	[op/s]	1925.5	---	---
	speed ecdsap224	[sign/s]	7278.8	---	---
		[verify/s]	1599.8	---	---
int	speed dsa2048	[sign/s]	1237.6	---	---
		[verify/s]	1061.4	---	---
	speed rsa2048	[sign/s]	361.5	---	---
		[verify/s]	12461.6	---	---

- Hardware/Software: Intel Prozessor mit 3,33 GHz basierend auf Intel-Mikroarchitektur "Westmere", 64-bit Linux, gcc v4.4.0

Quelle:
• JANKOWSKI, Krzysztof; LAURENT, Pierre; O'MAHONY, Aidan. Intel Polynomial Multiplication Instruction and its Usage for Elliptic Curve Cryptography, 2012, URL: www.intel.com/content/dam/www/public/us/en/documents/white-papers/polynomial-multiplication-instructions-paper.pdf (Aufruf 2013-05-25).

Wo ist ECC bereits im Einsatz

- Telefone von BlackBerry
- OpenSSH Ver. 5.7 (seit 2012)
- Produkte der Mozilla Foundation (min. 256-bit)
- Ausweise in Österreich seit 2004
- Zugriffskontrolle in deutschen Personalausweisen und Reisepässe der meisten EU-Staaten
- Sony verwendet ECDSA zur Signierung der Software für PS3

Quellen:
• NILLIES, Frank. *Kryptographie auf elliptischen Kurven am Beispiel von ElGamal und Menezes-Vanstone*, Proseminar Public-Key Kryptographie, 2006, URL: www2.cs.uni-paderborn.de/cs/ag-bloemer/lehre/proseminar_WS2005/material/Nillies_Ausarbeitung.pdf (Aufruf 2013-05-25).
• Wikipedia. *Elliptic Curve Cryptography*, 2013-05-05, URL: de.wikipedia.org/wiki/Elliptic_Curve_Cryptography (Aufruf 2013-05-25).
• HENDRIX, Joe. *Elliptic Curve Cryptography*, 2013-04-08, URL: www.linuxjournal.com/content/elliptic-curve-cryptography?page=0,2 (Abruf 2013-05-26).

Zusammenfassung und Ausblick

- Mit ECC ist effizienter als die momentan eingesetzten asymmetrischen Verfahren (RSA, DH)
  - kürzere Schlüssellängen bei gleicher Sicherheit
  - ressourcensparender als RSA

- Suche nach Angriffsverfahren und Verbesserung der Effizienz und Sicherheit
- Drei Jahre nach EC: Hyperelliptische Kurven
  - Polynom vom Grad 5 oder 7
  - Bis heute nicht verbreitet, da die Implementierung noch komplexer ist als bei den vorgestellten elliptischen Kurven

Quellen:

- NILLIES, Frank. *Kryptographie auf elliptischen Kurven am Beispiel von ElGamal und Menezes-Vanstone*, Proseminar Public-Key Kryptographie, 2006, URL: www2.cs.uni-paderborn.de/cs/ag-bloemer/lehre/proseminar_WS2005/material/Nillies_Ausarbeitung.pdf (Aufruf 2013-05-25).
- LIU, Fuwen. *A tutorial of elliptic curve cryptography (ECC)*, 2010, URL: www-rnks.informatik.tu-cottbus.de/de/node/1131 (Aufruf 2013-05-24).
- SCHWEIZER, Patrick. *Berechnung elliptischer und hyperelliptischer Kurven für paarungsbasierte Kryptografie*, Diplomarbeit, Institut für Mathematik, Technische Universität Berlin, 2008, URL: www.math.tu-berlin.de/~kant/publications/diplom/schweitzer.pdf (Aufruf 2013-05-27).

Literatur (1)

- NILLIES, Frank. *Kryptographie auf elliptischen Kurven am Beispiel von ElGamal und Menezes-Vanstone*, Proseminar Public-Key Kryptographie, 2006, URL: www2.cs.uni-paderborn.de/cs/ag-bloemer/lehre/proseminar_WS2005/material/Nillies_Ausarbeitung.pdf (Aufruf 2013-05-25).
- LIU, Fuwen. *A tutorial of elliptic curve cryptography (ECC)*, 2010, URL: www-rnks.informatik.tu-cottbus.de/de/node/1131 (Aufruf 2013-05-24).
- SCHWEIZER, Patrick. *Berechnung elliptischer und hyperelliptischer Kurven für paarungsbasierte Kryptografie*, Diplomarbeit, Institut für Mathematik, Technische Universität Berlin, 2008, URL: www.math.tu-berlin.de/~kant/publications/diplom/schweitzer.pdf (Aufruf 2013-05-27).
- Wikipedia. *Komplexitätstheorie*, 2013-04-27, URL: de.wikipedia.org/wiki/Komplexitätstheorie (Aufruf 2013-05-24).
- Wikipedia. *Elliptic curve cryptography*, 2013-05-02, URL: en.wikipedia.org/wiki/Elliptic_curve_cryptography (Aufruf 2013-05-25).
- GRÜßIEN, Berit. *Einführung: Elliptische Kurven in der Kryptologie*, Seminar "Moderne Kryptosysteme", 2006-10-15, URL: www.ki.informatik.hu-berlin.de/algorithmenII/Lehre/ss06/modern_krypt/ElliptischeKurven.pdf (Aufruf 2013-05-25).
- Wikipedia. *Elliptic Curve Cryptography*, 2013-05-05, URL: de.wikipedia.org/wiki/Elliptic_Curve_Cryptography (Aufruf 2013-05-25).
- Wikipedia. *Neal Koblitz*, 2013-04-15, URL: de.wikipedia.org/wiki/Neal_Koblitz (Aufruf 2013-05-25).
- Wikipedia. *Victor S. Miller*, 2013-03-31, URL: de.wikipedia.org/wiki/Victor_S._Miller (Aufruf 2013-05-25).

Literatur (2)

- KOBLITZ, Ann Hibner; KOBLITZ, Neal; MENEZES, Alfred. Elliptic curve cryptography: The serpentine course of a paradigm shift. *Journal of Number Theory*, 2011, 131. Jg., Nr. 5, S. 781-814, URL: http://eprint.iacr.org/2008/390.pdf (Aufruf 2013-05-27).
- MCGREW, D. A.; IGOE, K. M.; SALTER, M. *Fundamental Elliptic Curve Cryptography Algorithms*, RFC 6090, February, 2011, URL: http://tools.ietf.org/html/rfc6090 (Abruf 2013-05-26).
- SILVERMAN, Joseph H. *An Introduction to the Theory of Elliptic Curve*, 2006, URL: www.math.brown.edu/~jhs/Wyoming/WyomingEllipticCurveJune7LbyL.pdf (Aufruf 2013-05-25).
- MIYAJI, Atsuko. On ordinary elliptic curve cryptosystems. In: *Advances in Cryptology—ASIACRYPT'91*. Springer Berlin Heidelberg, 1993. S. 460-469.
- Stack Exchange. *ECC algorithm pollard's ρ complexity*, URL: http://crypto.stackexchange.com/questions/2262/ecc-algorithm-pollards-rho-complexity (Aufruf 2013-05-25).
- MEIER, Willi; STAFFELBACH, Othmar. Kryptographie und elliptische Kurven. *Elemente der Mathematik*, 1997, 52. Jg., Nr. 4, S. 137-151.
- Wikipedia. *RSA Factoring Challenge*, 2013-04-04, URL: de.wikipedia.org/wiki/RSA_Factoring_Challenge (Aufruf 2013-05-25)
- KLEINJUNG, Thorsten, et al. Factorization of a 768-bit RSA modulus. In: *Advances in Cryptology–CRYPTO 2010*. Springer Berlin Heidelberg, 2010. S. 333-350.
- <kes> online. *109-Bit-ECC-Challenge gelöst*, 2004-04-29, URL: www.kes.info/archiv/online/040429-ecc109.htm (Aufruf 2013-05-25).

Literatur (3)

- Certicom Research. *Certicom ECC Challenge*, 2009-09-10, URL: www.certicom.com/images/pdfs/challenge-2009.pdf (Aufruf 2013-05-25).
- certicom. *The Certicom ECC Challenge*, URL: www.certicom.com/index.php/the-certicom-ecc-challenge (Aufruf 2013-05-25).
- RSA Laboratories. *3.5.5 What is the Certicom ECC Challenge?*, URL: www.rsa.com/rsalabs/node.asp?id=2246 (Aufruf 2013-05-25).
- HAINZ, Christian. *Kryptographie und elliptische Kurven*, Ausarbeitung zum Vortrag, 2001, URL: http://homepages.thm.de/~hg10013/Lehre/MMS/SS01_WS0102/Elyps/ (Abruf 2013-05-26).
- GREBE, Ingo. *Elliptische Kurven in der Kryptographie*, Seminar Kryptographie und Datensicherheit, Präsentation, Universität Potsdam, 2005-07-07, URL: www.cs.uni-potsdam.de/ti/lehre/05-Kryptographie/slides/Elliptische_Kurven.pdf (Abruf 2013-05-26).
- cv cryptovision GmbH. *ECC – Kryptographie auf Basis elliptischer Kurven*, Eine kurze Einführung, 2009, URL: www.cryptovision.com/fileadmin/media/documents/Whitepaper_Produkte/02-Whitepaper-Technical-ECC_EN.pdf (Abruf 2013-05-26).
- Certicom Research. *SEC 2: Recommended Elliptic Curve Domain Parameters*, Standards for Efficient Cryptography, Version 1.0, 2000-09-20, URL: www.secg.org/collateral/sec2_final.pdf (Aufruf 2013-05-26).
- Certicom Research. *SEC 2: Recommended Elliptic Curve Domain Parameters*, Standards for Efficient Cryptography, Version 2.0, 2010-01-27, URL: www.secg.org/download/aid-784/sec2-v2.pdf (Aufruf 2013-05-26).
- SPITZ, Stephan; PRAMATEFTAKIS, Michael; SWOBODA, Joachim. *Kryptographie und IT-Sicherheit: Grundlagen und Anwendungen*. Vieweg+ Teubner Verlag, 2011, S. 146-147.

Literatur (4)

- Wikipedia. *Elliptic Curve DSA*, 2013-03-08, URL: en.wikipedia.org/wiki/Elliptic_Curve_DSA#Correctness_of_the_Algorithm (Aufruf 2013-05-27).
- ARGHIRE, Ionut. *Certicom Accepts RIM's Acquisition Offer*. 2009-02-11, URL: http://news.softpedia.com/news/Certicom-Accepts-RIM-039-s-Acquisition-Offer-104273.shtml (Aufruf 2013-05-27).
- Wikipedia. *BlackBerry (company)*. 2013-05-23, URL: http://en.wikipedia.org/wiki/BlackBerry_(company)#Certicom (Aufruf 2013-05-27).
- KJÆRSGAARD, Jan Ulrich; LANDROCK, Peter. *Patents on Elliptic Curves*, 2011-09-09, URL: www.cryptomathic.com/news-events/blog/patents-on-elliptic-curves (Aufruf 2013-05-25).
- RSA Laboratories. *6.3.1 Is RSA patented?* URL: www.rsa.com/rsalabs/node.asp?id=2322 (Aufruf 2013-05-25).
- RSA Laboratories. *6.3.4 Are elliptic curve cryptosystems patented?* URL: www.rsa.com/rsalabs/node.asp?id=2325 (Aufruf 2013-05-25).
- RSA Laboratories. *6.3.5 What are the important patents in cryptography?* URL: www.rsa.com/rsalabs/node.asp?id=2326 (Aufruf 2013-05-25).
- D. J. Bernstein. *Irrelevant patents on elliptic-curve cryptography* URL: http://cr.yp.to/ecdh/patents.html (Aufruf 2013-05-25).
- Wikipedia. *ECC patents*, 2013-04-11, URL: https://en.wikipedia.org/wiki/ECC_patents (Aufruf 2013-05-25).
- KRAWCZYK, Hugo. *HMQV: A High-Performance Secure Diffie-Hellman Protocol,* Cryptology ePrint Archive, Report 2005/176, 2005, URL: http://eprint.iacr.org/2005/176.pdf (Abruf 2013-05-26).

Literatur (5)

- BARKER, Elaine; CHEN, Lily; SMID, Miles; Allen ROGINSKY, Allen. *Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography (Draft Revision)*, NIST Special Publication 800-56A, 2012, Seite 51ff.
- Certicom Research. *SEC 1: Elliptic Curve Cryptography*, Standards for Efficient Cryptography, Version 2.0, 2009-03-21, Seite 58-60, Seite 76f, URL: http://www.secg.org/download/aid-780/sec1-v2.pdf (Aufruf 2013-05-26).
- HANKERSON, Darrel; MENEZES, Alfred J.; VANSTONE, Scott. *Guide to elliptic curve cryptography*. Springer, 2004, Seite 195f.
- MENEZES, Alfred; USTAOGLU, Berkant. On the importance of public-key validation in the MQV and HMQV key agreement protocols. In: *Progress in Cryptology-INDOCRYPT 2006*. Springer Berlin Heidelberg, 2006. S. 135, URL: www.cryptolounge.net/pdf/MU06.pdf (Aufruf 2013-05-27).
- KING, Brian. A point compression method for elliptic curves defined over GF (2 n). In: *Public Key Cryptography–PKC 2004*. Springer Berlin Heidelberg, 2004. S. 333-345.
- MAVROGIANNOPOULOS, Nikos. *Do we need elliptic curve point compression?*, 2012-01-01, URL: http://nmav.gnutls.org/2012/01/do-we-need-elliptic-curve-point.html (Aufruf 2013-05-25).
- LOPEZ, Julio; DAHAB, Ricardo. *Point Compression Algorithms for Binary Curves*, Präsentation, 2005-04-14, URL: http://cs.ucsb.edu/~koc/ccs130h/projects/03-ecc-protocols/Julio_Slides.pdf (Aufruf 2013-05-26).
- SEROUSSI, Gadiel. *Compression and decompression of elliptic curve data points*. U.S. Patent Nr. 6,252,960, 2001, URL: www.google.com/patents/US6252960 (Aufruf 2013-05-24).
- EBEID, Nevine Maurice Nassif, et al. *Power analysis countermeasure for the ECMQV key agreement algorithm*. U.S. Patent Nr. 8,219,820, 2012, URL: www.google.com/patents/US8219820 (Aufruf 2013-05-24).

Literatur (6)

- National Security Agency. *The Case for Elliptic Curve Cryptography*, 2009-01-15, URL: www.nsa.gov/business/programs/elliptic_curve.shtml (Aufruf 2013-05-24).
- GIRY, Damien. *Cryptographic Key Length Recommendation*, URL: www.keylength.com/en/compare/ (Aufruf 2013-05-25).
- GUPTA, Vipul; et al. Speeding up secure Web transactions using elliptic curve cryptography. In: *11th Annual Network and Distributed System Security Symposium (NDSS 2004)*. 2004.
- JANKOWSKI, Krzysztof; LAURENT, Pierre; O'MAHONY, Aidan. Intel Polynomial Multiplication Instruction and its Usage for Elliptic Curve Cryptography, 2012, URL: www.intel.com/content/dam/www/public/us/en/documents/white-papers/polynomial-multiplication-instructions-paper.pdf (Aufruf 2013-05-25).
- HENDRIX, Joe. *Elliptic Curve Cryptography*, 2013-04-08, URL: www.linuxjournal.com/content/elliptic-curve-cryptography?page=0,2 (Abruf 2013-05-26).
- NationMaster. *Elliptic curve cryptography*. URL: www.nationmaster.com/encyclopedia/Elliptic-curve-cryptography#Implementations (Aufruf 2013-05-28).