Bundesamt
für Sicherheit in der
Informationstechnik

Ein neuer Standard für elliptische Kurven

Dr. Manfred Lochter
BSI

Bundesamt
für Sicherheit in der
Informationstechnik

Dr. Johannes Merkle
secunet Security Networks

secunet
secunet Security Networks AG

11. Deutscher IT-Sicherheitskongress

Bundesamt
für Sicherheit in der
Informationstechnik

Einführung

- Problemstellung
- Zielsetzung
- Inhalt des neuen Standards
- Standardisierungsprozess
- Einsatz in Praxis
- Kritik
- Andere Standards
- Quellen

Problemstellung

- Elliptische Kurve: E: $y^2=x^3+Ax+B$ über GF(p).
- Elliptic Curve Kryptographie findet immer weitere Anwendung
  - Signaturgesetz
  - Personaldokumente
  - Gesundheitskarte
  - Diverse Projekte des BSI
  - Behördenbereich
  - Produkte (VPN, E-Mail, etc.)
  - ...

Bundesamt
für Sicherheit in der
Informationstechnik

Problemstellung

- Bedarf an standardisierten Elliptischen Kurven
  - Interoperabilität
  - Verifizierte und nachprüfbare Sicherheit
- NIST-Kurven
  - Spezielle Körper (Pseudo-Mersenne-Primzahlen)
    - Schnelle Arithmetik auf NIST-Kurven ist patentbehaftet
  - Schutz gegen Seitenkanalangriffe schwierig
    - Durch Experimente belegt
  - Konstruktion der Seeds nicht nachvollziehbar
- Für Bitlängen > 160 keine alternativen Kurven standardisiert
  - Was wenn eine Kurve gebrochen wird?

Bundesamt
für Sicherheit in der
Informationstechnik

Zielsetzung des neuen Standards

- Standardisierte elliptische Kurven, die
  - höchsten Sicherheitsansprüchen genügen
  - vollständig nachvollziehbar pseudo-zufällig erzeugt sind
  - Implementierungsprobleme vermeiden helfen
    - Patentkonflikte
    - typische Implementierungsfehler (Überlauf)
    - Anfälligkeit gegen Seitenkanalangriffe
  - über OIDs referenzierbar sind
- Verfahren zur Erzeugung „guter“ elliptischer Kurven
- Out-of-Scope: Kurven für paarungsbasierte Kryptographie

Bundesamt
für Sicherheit in der
Informationstechnik

Inhalt des neuen Standards

- Anforderungen an „gute Kurven“
- Methode zur Kurvenerzeugung
  - Vollständig pseudo-zufällig
  - Nachvollziehbare Seeds auf Basis der Naturkonstanten π und e
- Kurven für 160, 192, 224, 256, 384, 512 Bit
  - Nur Primkörper
  - Zusätzlich jeweils isomorphe Kurve mit A=-3
    - Ermöglicht effiziente Implementierung
- Zusätzlich wird beschrieben, wie die Forderungen des Signaturgesetzes nachgerechnet werden können.
- OIDs und Vorgaben zur Nutzung in X.509-Zertifikaten

Der Standardisierungsprozess

- Initiiert durch ECC-Brainpool
  - Arbeitsgruppe von Wissenschaft, Industrie und Behörden
  - Förderung des sicheren Einsatzes von elliptischen Kurven

ECC Brainpool
Elliptic Curve Cryptography

- Erzeugung und Prüfung der Kurven durch BSI
- Internationale Anerkennung
  - Informational RFC der IETF
  - Prozess fast abgeschlossen
    - Veröffentlichung in ca. einem Monat
    - draft-lochter-pkix-brainpool-ecc-03

Bundesamt
für Sicherheit in der
Informationstechnik

Einsatz in Praxis

- Deutsche Personaldokumente
  - Country Signing Authority: 256 Bit Brainpool-Kurve
  - Document-Signer: 224 Bit Brainpool-Kurve.
- SINA
- Prüfverfahren bei SmartCard-Zertifizierung
- BSI-Produkte im Behördeneinsatz
- NATO-Anwendungen
- Implementierung in freier Crypto++ Bibliothek
- Interesse von PGP Corporation

Bundesamt
für Sicherheit in der
Informationstechnik

Kritik und Probleme

- Kurvenerzeugung mit SHA-1 sicher?
  - Irrelevant, da Seeds vollständig nachvollziehbar
- Abweichung der Methode zur Kurvenerzeugung von X9.62
  - Keine Kennzeichnung in X.509 Zertifikaten als pseudo-zufällig
  - Aber: Kennzeichnung durch neuen RFC 5480 der PKIX obsolet
- Kritik von Koblitz-Koblitz-Menezes (2008)
  - „Übertriebene Anforderungen“
    - Bedingungen werden von fast allen Kurven erfüllt
    - Klassenzahlbedingung sinnvoll
  - „Paarungsbasierte Kryptographie ausgeschlossen“
    - Fehlinterpretation des Anwendungsbereiches

Bundesamt
für Sicherheit in der
Informationstechnik

Quellen

- OIDs der Kurven sind über TeleTrust registriert
  - Quellenangabe hat sich geändert
- Auch über die Webseite des ECC-Brainpools abrufbar
  - http://www.ecc-brainpool.org

Bundesamt
für Sicherheit in der
Informationstechnik

Kontakt

Dr. Manfred Lochter
Bundesamt für Sicherheit in der
Informationstechnik (BSI)

Postfach 200363
53175 Bonn
Tel: +49 (0)22899-9582-5643
Fax: +49 (0)22899-10-9582-5643

manfred.lochter@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de

Dr. Johannes Merkle
secunet Security Networks AG

Mergenthaler Allee 77
65760 Eschborn
Tel: +49 (0)201-5454-2021
Fax: +49 (0)201-5454-1325

johannes.merkle@secunet.com
www.secunet.com