advanced cryptographic technology

Kryptographie im Bereich Embedded Systems

Thomas Zeggel

cv cryptovision GmbH

thomas.zeggel@cryptovision.com

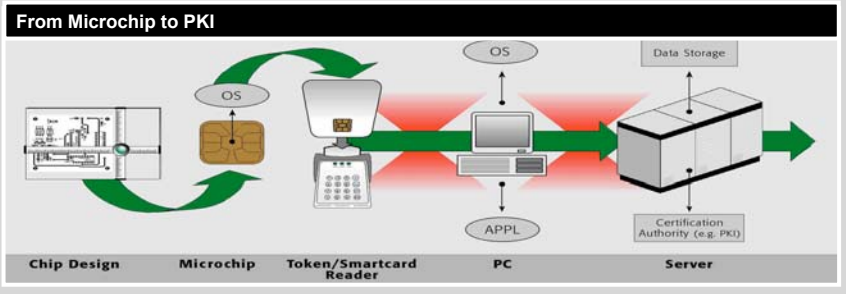
2. SELMA-Workshop, Berlin, 15./16.10.2003

Überblick

- cv cryptovision GmbH: Schwerpunkte
- Kryptographie auf Basis elliptischer Kurven
- Embedded Systems: Beispielprojekte
  - Auto-Navigationssystem
  - Verkehrs-Überwachungssystem
  - Automobil-Controller (Motorsteuerung)
- Zusammenfassung und Ausblick

Die cv cryptovision GmbH

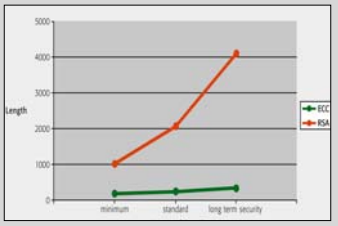
- Gegründet 1999 mit 4 Mitarbeitern
- Spin-Off des Instituts für experimentelle Mathematik
- Fokus auf kryptographischen Anwendungen
- Technologie-Schwerpunkt: Elliptic Curve Cryptography (ECC)
- Heute: 50 Mitarbeiter (hauptsächlich R&D)
- Anbieter von IT-Sicherheitslösungen



Kryptographie auf Basis elliptischer Kurven

Im Vergleich zu gängigen Verfahren (RSA, DSA):

- Deutlich kürzere Parameter bei gleicher Sicherheit
- Schnellere Ausführung der relevanten Operationen
- Kürzere Signaturen



→ Geringeres Datenaufkommen, weniger Kommunikationsbandbreite

ECC	**0xb23ec135a3a16be766d6a**
RSA	**0x4e2675be91501430ad310d46a3c499e1905ddadafd3c514eccb5a57d319e8945a64b318e74**

- Sehr geringe Ressourcenanforderungen

→ Realisierbarkeit in beschränkten Umgebungen

Embedded Systems und Kryptographie

Zusätzliches Token oder Smartcard:

+ Sehr hohes Sicherheitsniveau der Hardware (Schlüsselspeicherung)
+ Verfügbare zertifizierte Implementierungen (Token oder Smartcard)
+ Vorgegebene Performance
- Erhöhter Integrationsaufwand (Schnittstelle, Ansteuerung)

Direkte Nutzung von Embedded-System-Prozessoren:

+ Nutzung vorhandener Hardware
+ Geringer Integrationsaufwand
o Erreichbare Performance sehr unterschiedlich
- Erstinvestition für Implementierung
- Zusätzliche Kosten bei Sicherheitsevaluierung

Beispiel 1: Auto-Navigationssystem

Aufgabe: **Entwicklung eines Conditional-Access-Systems**
- Sämtliche Kartendaten auf Datenträger
- Selektive Freischaltung gewünschter Leistungen
- Update-Möglichkeit für Altgeräte

Ansatz:
- ECC-Signaturen zur Absicherung von Updates und Daten
- Symmetrische Verschlüsselung der Access Keys
- ECC-Schlüsselaustausch
- Interne Schlüsselgenerierung
- Übertragung von Freischaltcodes und Rückkanal mit Base32-Kodierung

Empfohlene Schlüssellängen (Lenstra and Verheul)

Year	Symmetric key size	RSA key size	ECC key size	ECC key size (assumption of higher increase of knowledge)
2000	70	952	132	132
2002	72	1028	135	139
2004	73	1108	138	143
2006	75	1191	141	148
2008	76	1279	144	155
2010	78	1369	146	160
2012	80	1464	149	165
2014	81	1562	152	172
2016	83	1664	155	177
2018	84	1771	158	181
2020	86	1881	161	188
2022	87	1995	164	193
2024	89	2113	167	198

Empfohlene Schlüssellängen (Lenstra and Verheul)

Year	Symmetric key size	RSA key size	ECC key size	ECC key size (assumption of higher increase of knowledge)
2000	70	952	132	132
2002	72	1028	135	139
2004	73	1108	138	143
2006	75	1191	141	148
2008	76	1279	144	155
2010	78	1369	146	160
2012	**80**	1464	149	**160** 165
2014	81	1562	152	172
2016	83	1664	155	177
2018	84	1771	158	181
2020	86	1881	161	188
2022	87	1995	164	193
2024	89	2113	167	198

Konzept (1)

Hardware: Toshiba ASIC mit 32-Bit-RISC-Prozessor, MIPS-Kern,
~ 108 MHz (54 MHz), 32 Mbyte NVRAM (16 MByte)

Performance:

ECC-Verifikation	~ 100ms
symm. Operationen	< 50ms
Hash (SHA-1)	~ 1,4 MByte/s

Mit älterer Hardware: etwa 110-150% mehr Rechenzeit

Insgesamt: Rechenzeiten unkritisch

-> Warum nicht RSA?

Vorteile von ECC: - *Kleinere Schlüssel*
- *Kleinere Signaturen*
- *Kompakter Datenstrom bei Schlüsselaustausch*

Konzept (2)

Access Keys: **80 Bit -> 16 Base-32-Zeichen**

A2G6 – Z7MB – D5HP – 17FS

Schlüsselübertragung: **161 Bit -> 33 Base-32-Zeichen**

G - 65HP – FCK9 – W3DX – YSML – 6GHK2 – KG76 – V3BY – PF4E

Übertragung von Schlüsseln ist verschieden möglich...

- Telefonisch
- SMS
- Internet (manuelle Eingabe)

Ergebnis (1)

Ergebnis (2)

Conditional Access für Navigationssysteme

Zusammengefasst:

- Individuelle (symmetrische) Schlüssel für jedes Gerät
- Interne Schlüsselgenerierung und ECC-Schlüsselaustausch
- Interne Verschlüsselung und sichere Speicherung der Schlüssel
- Sicherung von Updates und Daten durch Signaturprüfung
- Access Keys symmetrisch verschlüsselt (80 Bit)
- „Manuelles“ Handling der Schlüssel mit Base-32-Kodierung

Realisierung nur mit ECC möglich!

Beispiel 2: Verkehrs-Überwachungsanlagen

Aufgabe: Schutz der Datenintegrität bei digital aufgenommenen Beweisbildern

Lösung: ECC-Signatur in der Kamera vor der Weitervermittlung

Konzept (1)

Anforderung: Digitale Signatur der Beweisbilder direkt in der Kamera

Hardware:
- Embedded PC mit ~ 500 MHz
- USB-Token mit Infineon SLE 66P (Eutron) und cryptovision CardOS-ECC-Package

Performance:

ECC-Signatur (Token)	~ 70ms (160 Bit)
	~ 130ms (224 Bit)
Hash (PC)	~ 18 MByte/s

Protokoll: + etwa 100ms

Insgesamt: Rechenzeiten (knapp) ausreichend

Konzept (2)

Zusammengefasst:

- Digitale Signatur der Beweisbilder
- Kamera: Embedded PC
- Einsatz eines USB-Tokens mit CardOS-ECC-Package
- Geschützte Umgebung (Gehäuse)

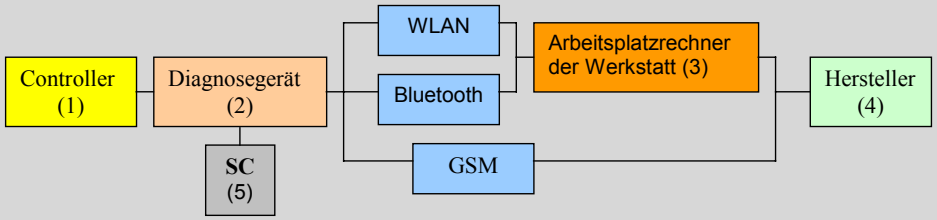
Beispiel 3: Automobil-Controller

Aufgabe: Absicherung der Prozesse bei
- Wartung
- Reparatur
- Daten-Update
- Programm-Update

Ansatz: Abgestuftes Sicherheitskonzept mit kryptographischen Komponenten im Controller

Szenario:
- Bei Wartungs- und Reparaturarbeiten wird mobiles Diagnosegerät mit Controller verbunden
- Wesentliche Eingriffe müssen vom Hersteller authorisiert sein
- Identifikation des Anfragenden (Person, Werkstatt)

Konzept (1)



Konzept (2)

Hardware: Beispiel Motorola HC12, 16 Bit, 8 MHz

Performance:

ECC-Verifikation	~ 6,5s (160 Bit)
ECC-Signatur	~ 3s (160 Bit)
Symm. Operation (MAC)	< 100ms

Insgesamt: Rechenzeiten ausreichend

-> Warum nicht RSA?

Nachteil von ECC: *- Dauer der Verifikation*

Aber: bei höheren Sicherheitsniveaus Unterschied geringer

Vorteil von ECC:
- Kleinere Schlüssel
- Kleinere Signaturen
- Kompakter Datenstrom bei Schlüsselaustausch

Konzept (3)

Verschiedene Sicherheitsstufen:

- Jede Anfrage muss vom Hersteller signiert sein
- Der Controller muss mit einer Hersteller-signierten Anfrage in den Wartungsmodus versetzt werden
- Einfache Anfragen benötigen Authentifizierung des Wartungsdienstes

Zusammenfassung

Einsatz von ECC im Bereich Embedded Systems nimmt zu

- Low-Cost-Controller (8 oder 16 Bit)
  -> Rechenzeiten ~ mehrere Sekunden

- Ab dem mittleren Bereich (32 Bit)
  -> Rechenzeiten (deutlich) unter einer Sekunde

Vorteile von ECC:

- Rechenzeiten (Signatur, Schlüsselgenerierung)
- Kompakte Signaturen und Zertifikate
- Kompakter Schlüsselaustausch

cryptoVision

Vielen Dank für Ihre Aufmerksamkeit!

advanced cryptographic technology