Benchmark-basierter Ansatz zur Auswahl kryptographischer Verfahren für Automotive-Steuergeräte

Florian Sommer

Workshop SafeWare Engineering 2018

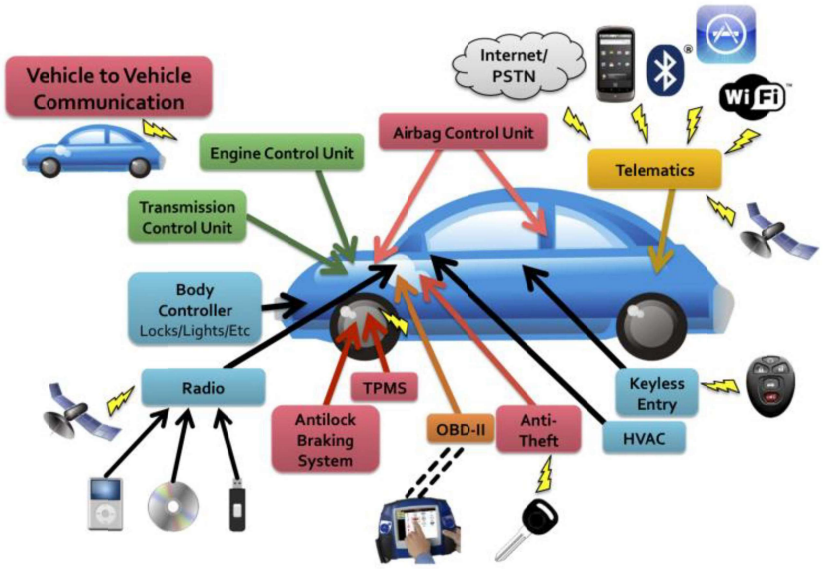
Motivation

0x10 0x02 0x11 0x01 0x00 0x00 0x00 0x00

Motivation

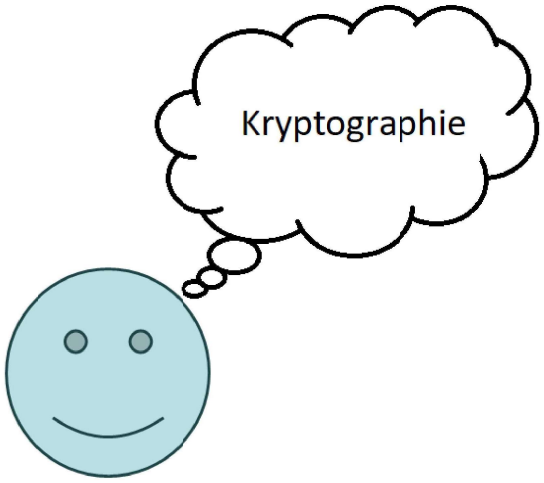
CAN-ID	DLC	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7	Byte 8
0x6F1	8	**0x10**	**0x02**	**0x11**	**0x01**	**0x00**	**0x00**	**0x00**	**0x00**

Das vernetzte Fahrzeug



Stephen Checkoway et. al., "*Comprehensive Experimental Analyses of Automotive Attack Surfaces*", IEEE Symposium on Security and Privacy, Oakland, CA, May 16–19, 2010.

Idee



Fahrzeugkommunikation

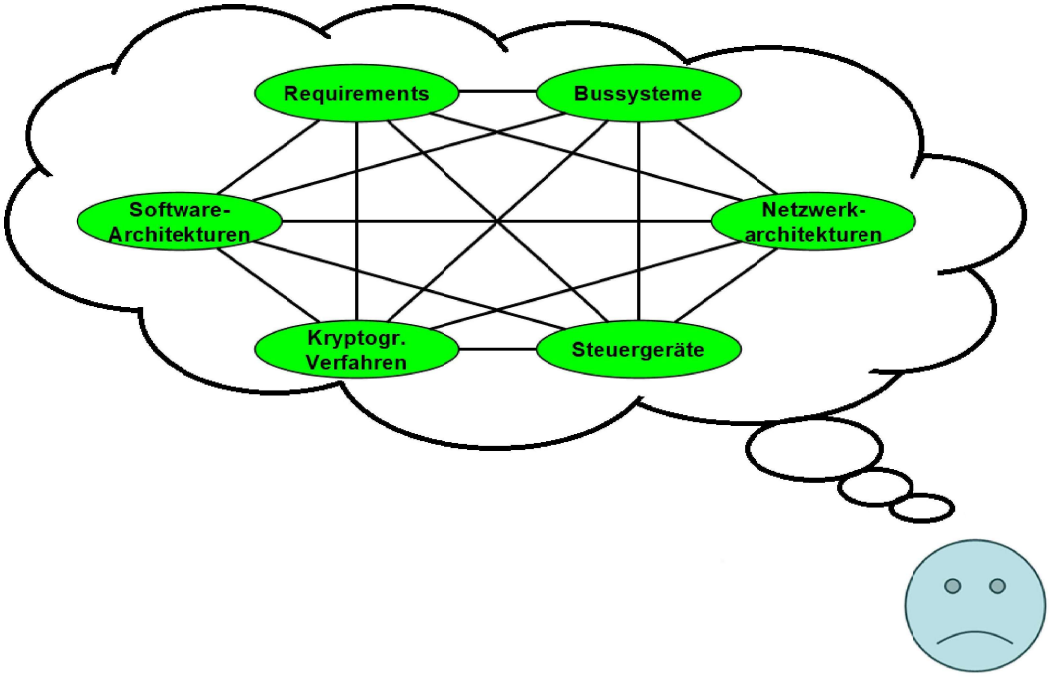
benötigt

Security-Maßnahmen

verwenden

Kryptographie

Idee



Idee

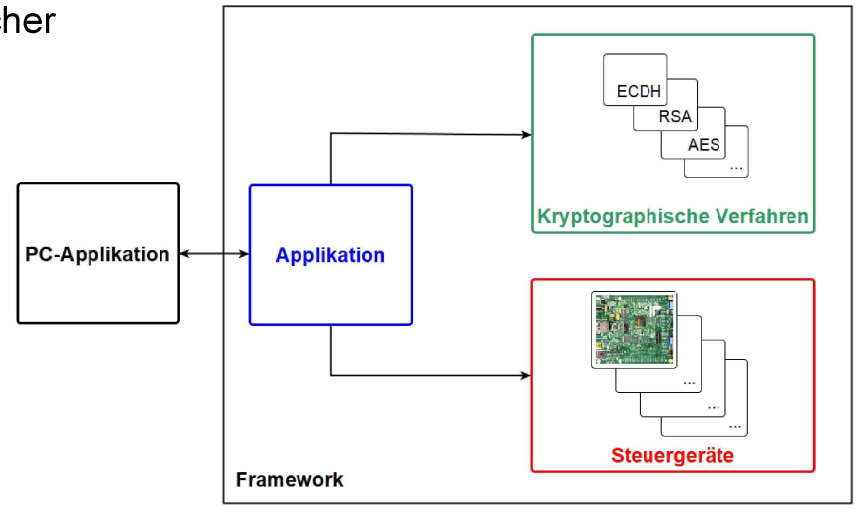
Auswahl kryptographischer Verfahren schwierig!

Fragestellung

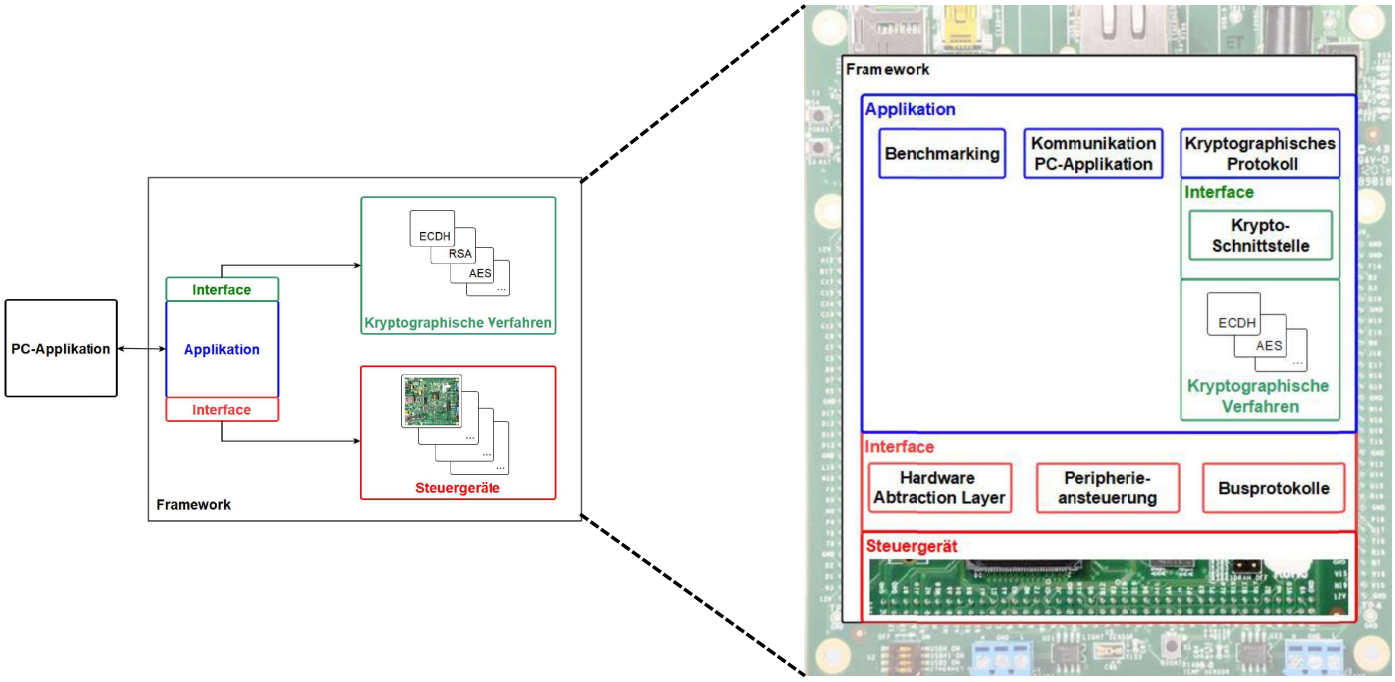
Wie kann die Einsatzfähigkeit von kryptographischen Verfahren für eingebettete Automotive-Systeme evaluiert werden?

Konzept: Framework zum Benchmarking kryptographischer Verfahren

- Integration kryptographischer Bibliotheken
- Verschiedene Steuergeräte
- Kryptographisches Protokoll
- Benchmarking
- Monitoring

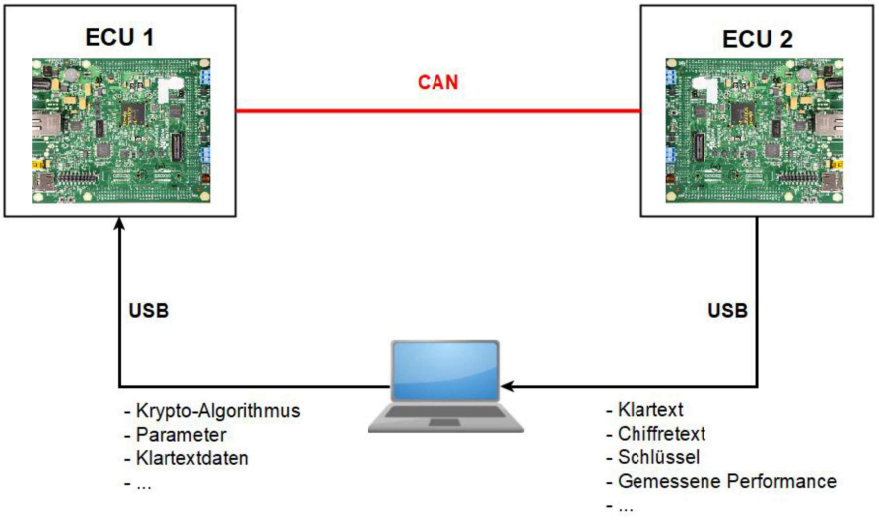


Implementierung



Testaufbau

- **CPU**: ARM Cortex-R4F 32-Bit
- **RAM**: 256 KB
- **Flash**: 3 MB
- **Taktfrequenz**: 180 MHz



Kryptographisches Protokoll

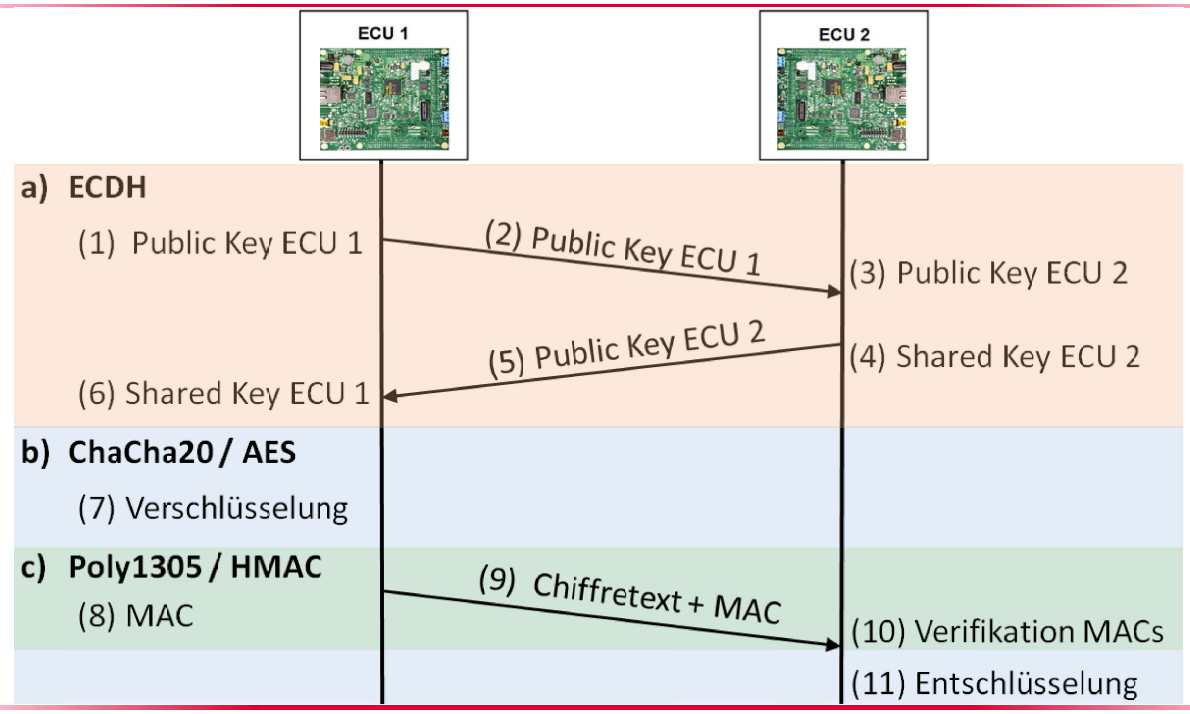
a) Asymmetrischer Schlüsselaustausch zur Berechnung eines geheimen Schlüssels.

b) Symmetrische Ver-/Entschlüsselung eines Klartexts mit Hilfe des geheimen Schlüssels zur Sicherstellung der Vertraulichkeit.

c) Bildung eines MACs (Message Authentication Codes) zur Sicherstellung der Authentizität einer Botschaft.

	Bibliothek 1: libsodium	**Bibliothek 2: mbed TLS**
a)	Elliptic-Curve-Diffie-Hellman-Schlüsselaustausch	Elliptic-Curve-Diffie-Hellman-Schlüsselaustausch
b)	ChaCha20	Advanced Encryption Standard (AES) im Cipher-Block-Chaining-Modus
c)	Poly1305	Keyed-Hashing for Message Authentication (HMAC)

Kryptographisches Protokoll



Messergebnisse

	Bibliothek 1: libsodium	Bibliothek 2: mbed TLS
a)	**93,590 ms** (ECDH-Schlüsselaustausch)	**1567,550 ms** (ECDH-Schlüsselaustausch)
b) + c)	**3,798 ms** (ChaCha20 + Poly1305)	**3,930 ms** (AES + HMAC)

Messergebnisse

	Bibliothek 1: libsodium	Bibliothek 2: mbed TLS
a)	**93,590 ms** (ECDH-Schlüsselaustausch)	**1567,550 ms** (ECDH-Schlüsselaustausch)
b) + c)	**3,798 ms** (ChaCha20 + Poly1305)	**3,930 ms** (AES + HMAC)

Messergebnisse

	Bibliothek 1: libsodium	Bibliothek 2: mbed TLS
a)	**93,590 ms** (ECDH-Schlüsselaustausch)	**1567,550 ms** (ECDH-Schlüsselaustausch)
b) + c)	**3,798 ms** (ChaCha20 + Poly1305)	**3,930 ms** (AES + HMAC)

Fazit

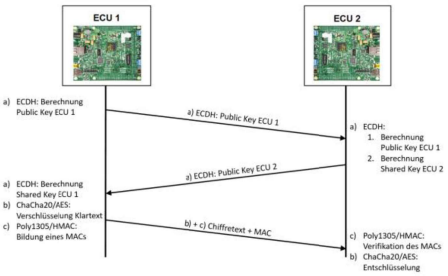
Framework kann zur Evaluierung der Einsatzfähigkeit einer kryptographischen Bibliothek auf eingebetteten Automotive-Systemen verwendet werden.

➔ Auswahl geeigneter kryptographischer Bibliotheken/Verfahren für den Einsatz auf Automotive-Steuergeräten möglich.

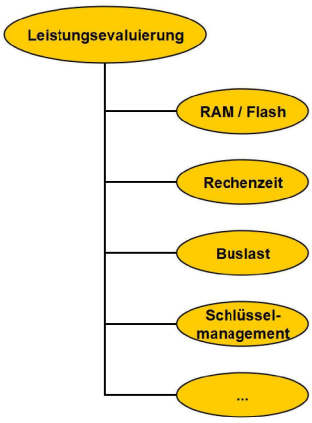
➔ Einsatz des Frameworks in frühen Entwicklungsphasen möglich.

Ausblick

Einbinden weiterer Steuergeräte



Realisierung weiterer kryptographischer Protokolle



Erweiterung des Benchmarkings

Erstellung einer Datenbank mit Messergebnissen

Vielen Dank für Ihre Aufmerksamkeit!

Fragen?

Florian Sommer, M. Sc.
Akademischer Mitarbeiter
Hochschule Karlsruhe - Technik und Wirtschaft
IEEM - Institut für Energieeffiziente Mobilität
Moltkestraße 30
76133 Karlsruhe