

# Inhaltsverzeichnis

<b>1. Einleitung</b>	<b>1</b>
1.1. Einführung und Motivation . . . . .	1
1.2. Fragestellung und Zielsetzung . . . . .	5
1.3. Aufbau der Arbeit . . . . .	6
<b>2. Grundlagen</b>	<b>7</b>
2.1. Mathematische Grundlagen . . . . .	7
2.1.1. Endliche Körper und ihre Arithmetik . . . . .	7
2.1.2. Reduktionsverfahren bei general. Mersenne-Primzahlen . . . . .	10
2.1.3. Elliptische Kurven und ihre Arithmetik . . . . .	12
2.1.4. Darstellung in projektiven Koordinaten . . . . .	15
2.2. Kryptographische Verfahren . . . . .	16
2.2.1. Zufallszahlenerzeugung . . . . .	16
2.2.2. Kryptographisches Hashen . . . . .	18
2.2.3. Chiffrierung . . . . .	20
2.2.4. Digitale Signaturen . . . . .	23
2.2.5. Public Key Infrastruktur . . . . .	29
2.2.6. Sicherheitslevel und Schlüssellängen . . . . .	30
2.3. Trusted Computing . . . . .	31
2.3.1. Trusted Platform . . . . .	32
2.3.2. Vertrauensanker und transitives Vertrauen . . . . .	34
2.3.3. Technischer Aufbau – Das Trusted Platform Module . . . . .	37
2.3.4. Zertifizierung einer Trusted Platform . . . . .	41
2.3.5. Aussage über die Sicherheit einer Trusted Platform . . . . .	42
2.4. Fahrzeug-zu-Fahrzeug Kommunikation . . . . .	43
2.4.1. Hauptanwendungen und Klassifikation . . . . .	43
2.4.2. Nachrichtenaustausch und Kommunikationssystem . . . . .	44
2.4.3. Standardisierung und regionale Unterschiede . . . . .	46
2.4.4. Eigenschaften und Herausforderungen . . . . .	48
2.5. Field-Programmable Gate Arrays . . . . .	50
2.5.1. Basisarchitektur . . . . .	50
2.5.2. Spezielle Funktionsblöcke . . . . .	52
2.5.3. FPGA Entwicklungsmethodik . . . . .	53
2.5.4. Bitstromaufbau . . . . .	54
2.5.5. Konfiguration des FPGA . . . . .	55
2.5.6. Verwendete Hardwareplattformen . . . . .	57

<b>3. Stand der Technik</b>	<b>59</b>
3.1. Security-Architekturen für C2X-Kommunikation	59
3.1.1. Die Sicherheitsarchitektur des SEVECOM-Projekts	60
3.1.2. EVITA	62
3.1.3. sim <sup>TD</sup>	62
3.1.4. COMeSafety	63
3.1.5. C2X-Hardwareplattformen	64
3.2. Realisierungen für ECDSA	66
3.2.1. Softwareimplementierungen	66
3.2.2. Hardwarerealisierungen	67
3.2.3. Performanzvergleich	68
3.3. Trusted Computing für rekonfigurierbare Systeme	69
<b>4. Angreifermodell</b>	<b>73</b>
4.1. Angreifermodellierung	73
4.2. Angriffsarten	75
4.3. Safety-Einfluss von Security-Angriffen	76
<b>5. Sichere C2X Kommunikation</b>	<b>79</b>
5.1. Motivation	79
5.2. Absicherung der C2X-Kommunikation	79
5.2.1. Verarbeitungskette der C2X-Nachrichten	79
5.2.2. Sicherheitsmechanismen	81
5.2.3. Herausforderungen für das Sicherheitssystem	81
5.3. C2X-Kommunikationssystem	83
5.3.1. Architektur des Kommunikationssystems	84
5.3.2. Komponenten des Systems	86
5.3.3. Nachrichtenverarbeitung im C2X-System	90
5.3.4. Das Signaturmodul im Überblick	91
5.3.5. Komponenteninteraktion und Nachrichtenformate	93
5.4. Das Signaturmodul im Detail	96
5.4.1. Aufbau des Signaturmoduls	96
5.4.2. Hashwert-Berechnung	97
5.4.3. Zufallszahlenerzeugung	98
5.4.4. Schlüsselmanagement	99
5.4.5. Zertifikate-Cache	100
5.5. ECDSA-Hardware: Referenzimplementierung	100
5.5.1. Modulararithmetik - Implementierung der Basisoperationen	101
5.5.2. Zentrale GF(p)-ALU	104
5.5.3. Gesamtaufbau und Steuerung	108
5.5.4. Performanz und Ressourcenverbrauch	111
5.6. ECDSA-Hardware: Optimierte Implementierung	113
5.6.1. Darstellung im projektiven Raum	114
5.6.2. Modulararithmetik auf DSP-Hardware	115

5.6.3.	$GF(p)$ -ALU auf DSP-Hardware . . . . .	122
5.6.4.	Skalare Multiplikation mit Fensterung . . . . .	125
5.6.5.	Performanz und Ressourcenverbrauch . . . . .	130
5.7.	Demonstrator für das Gesamtsystem . . . . .	133
5.8.	Beurteilung . . . . .	134
<b>6.</b>	<b>Trusted Platforms auf rekonfigurierbarer Hardware</b>	<b>137</b>
6.1.	Problemstellung und Anforderungen . . . . .	137
6.2.	Ansatz und Ziele für die Trusted Platform . . . . .	138
6.3.	Analyse der FPGA-Eigenschaften bzgl. Trusted Computing . . . . .	139
6.4.	Konzept: Trusted Computing auf FPGAs . . . . .	140
6.4.1.	Ansatz zur Integritätsmessung und -Speicherung . . . . .	140
6.4.2.	Funktion und Betrieb der Trusted Platform . . . . .	147
6.4.3.	Realisierungsalternativen . . . . .	149
6.5.	Sicherheitsbetrachtung . . . . .	150
6.5.1.	Vollständige Integritätsmessung . . . . .	150
6.5.2.	Systemstart und Initialisierung . . . . .	151
6.5.3.	Korrekte Aktualisierung . . . . .	152
6.5.4.	Erkennen von Manipulationsversuchen . . . . .	153
6.6.	Realisierung mit Standard-TPM . . . . .	155
6.6.1.	Systemarchitektur . . . . .	156
6.6.2.	Zustandsmodellierung . . . . .	159
6.6.3.	Implementierung . . . . .	162
6.6.4.	Bewertung des Standard-TPM Ansatzes . . . . .	169
6.7.	Realisierung mit funktionserweitertem Active-TPM . . . . .	170
6.7.1.	Systemaufbau . . . . .	170
6.7.2.	Einbettung in die JTAG-Chain . . . . .	173
6.7.3.	Betrieb der Trusted Platform mit ActiveTPM . . . . .	175
6.7.4.	Implementierung . . . . .	175
6.7.5.	Beurteilung und Test . . . . .	181
6.8.	Anwendung auf die C2X-Kommunikation . . . . .	183
6.8.1.	Angriffsdefinition für C2X-Kommunikation . . . . .	183
6.8.2.	Zertifizierungssystem und Protokolle . . . . .	185
6.8.3.	Umsetzung auf Fahrzeugebene . . . . .	188
6.8.4.	Sicherheitsbetrachtung der Trusted Platform für C2X . . . . .	189
<b>7.</b>	<b>Zusammenfassung und Ausblick</b>	<b>191</b>
7.1.	Zusammenfassung . . . . .	191
7.2.	Kritische Einordnung und Diskussion . . . . .	193
7.3.	Fazit und Ausblick . . . . .	194
<b>A.</b>	<b>Schreibweisen, Parameter und Beweise</b>	<b>197</b>
A.1.	Verwendete Schreibweisen und Formelzeichen . . . . .	197

A.2. Kryptographische Parameter . . . . .	198
A.2.1. NIST P-224 ECDSA-Parameter . . . . .	198
A.2.2. NIST P-256 ECDSA-Parameter . . . . .	198
A.3. Beweis von Lemma 5.2 . . . . .	199
<b>B. Leistungsbetrachtungen und Implementierung</b>	<b>203</b>
B.1. ECDSA-Tracing auf affinen Koordinaten . . . . .	203
B.2. SHA-1 Benchmark . . . . .	204
B.3. Implementierungsdetails . . . . .	207
B.3.1. Nachrichtenformat für das On-Chip-BusNoC . . . . .	207
B.3.2. LPC-Bus . . . . .	208
<b>C. Sicheres Update für eingebettete Systeme</b>	<b>211</b>
<b>Verzeichnisse</b>	<b>213</b>
Abbildungsverzeichnis . . . . .	213
Tabellenverzeichnis . . . . .	215
Algorithmenverzeichnis . . . . .	217
Abkürzungsverzeichnis . . . . .	219
<b>Literatur- und Quellennachweise</b>	<b>225</b>
<b>Betreute studentische Arbeiten</b>	<b>247</b>
<b>Eigene Veröffentlichungen</b>	<b>249</b>