

Contents

1	Introduction	1
1.1	Reconfigurable Computing	2
1.2	Trustworthy Reconfiguration	4
1.3	Summary of Contributions	6
1.4	Limitations	6
1.5	Remainder of this Thesis	7
2	Trustworthy Computing	9
2.1	The Meaning of Trustworthiness	11
2.2	Trusted Computing Group	13
2.2.1	Trusted Computing Limitations	13
2.2.2	Trusted Platform Module Specification	14
2.2.3	Platform Integrity Measurements	19
2.2.4	Measured Boot	21
2.2.5	Secure Boot	22
2.2.6	Authentication Protocols	22
2.2.7	System Integrity Reporting	23
2.3	Supporting Multiple Stakeholders	25
2.3.1	Reference Integrity Metric Certificates	26
2.4	Beyond TCG Specifications and Related Products	27
2.4.1	Intel Trusted Execution Technology	29
2.4.2	ARM TrustZone	30
2.4.3	Texas Instruments M-Shield	31
2.5	Trustworthy Systems using FPGAs	31
2.5.1	Software-based Attestation	32
2.5.2	Hardware-based Attestation	33
3	Requirements for Trustworthiness	35
3.1	Key Storage and Certificate Management	36
3.1.1	Cryptographic Memories	38
3.1.2	Storing Cryptographic Secrets	40
3.1.3	Certificate Management	44

3.2	Identification and Authentication	47
3.2.1	Requirements for Cryptographic Keys	48
3.2.2	Device Identifiers	49
3.2.3	Physically Unclonable Functions	49
3.3	A Notion of Time	52
3.4	Measurements for Security	53
3.4.1	The Orange Book	54
3.4.2	Common Criteria for IT Security Evaluation	55
3.4.3	NIST-FIPS 140-2	58
4	Design Security and Cyber-Physical Threats	61
4.1	Design Security Goals	63
4.2	Vendor Specific Design Security	66
4.2.1	Tamper Protection	71
4.3	Generic IP-Protection	71
4.4	Cyber-Physical Threats	72
4.4.1	Cloning, Overbuilding and Counterfeiting	74
4.4.2	Physical Attacks	75
4.5	Common Security Scenarios	82
4.5.1	Trusted Computing Group	82
4.5.2	FPGA Vendor	82
4.6	TPM Specific Attacks	83
5	Towards Trustworthy Cyber-Physical Systems	85
5.1	Reconfigurable System Challenges	87
5.1.1	Storage of Security-Sensitive Data	87
5.2	Trustworthy Reconfigurable Systems	88
5.2.1	The Use of Partial Reconfiguration	90
5.2.2	System State Reporting	91
5.2.3	Freshness of Configuration Data	92
5.2.4	TinyTPM Architecture	93
5.2.5	Life-Cycle	96
5.2.6	Bootstrapping	97
5.2.7	Update Protocol	99
5.2.8	Proof-Of-Concept Implementation	102
5.2.9	Evaluation	103
5.3	TinyTPM Optimizations	110
5.3.1	Authenticated Encryption	110
5.3.2	Partial Reconfiguration Performance	118

5.4	Physical Attack Resistance	120
5.4.1	Side-Channel Aware TinyTPM Architecture	120
5.4.2	Evaluation	121
5.4.3	Tamper Protection	121
5.5	Supporting Multiple Stakeholders	123
5.5.1	Dynamic Context Management Concept	124
5.5.2	dcTPM Proof-of-Concept	129
5.5.3	Context Authorization Protocol	133
5.5.4	dcTPM-Commands	134
5.5.5	Multi-Context Trust/Live Migration	135
6	Application Scenarios	137
6.1	IP-Protection for Partial Reconfiguration	137
6.1.1	Trustworthy Reconfiguration enforcing IP-Protection	138
6.1.2	Configuration Management	141
6.2	Hard Disk Encryption	141
6.2.1	Proof-of-Concept Implementation	142
6.2.2	Multi-User Environments	145
6.3	Pay TV Content Protection	146
6.3.1	Reconfigurable Security	147
6.3.2	Proof-of-Concept Implementation	149
7	Summary	151
A	Cryptographic Primitives	155
A.1	Selection of Algorithms	155
A.1.1	Providing Integrity	157
A.1.2	Providing Authenticity	157
A.1.3	Providing Confidentiality	158
A.1.4	Providing Non-Repudiation	158
A.1.5	Providing Long-Term Security	158
A.2	Secure Hash Algorithm	159
A.3	Advanced Encryption Standard	160
A.3.1	Low Latency AES Implementation	160
A.3.2	Sub-Bytes Implementations	161
A.4	Message Authentication Codes (MAC)	163
A.4.1	Hash-based Message Authentication Codes (HMACs)	164
A.5	Authenticated Encryption	164
A.5.1	AES Counter Mode with CBC-MAC – AES-CCM	165
A.5.2	Hardware Implementation	166

A.6 Random Number Generators	168
B FPGA Technology	171
B.1 Configuration Technologies	171
B.2 Partial Reconfiguration	172
B.2.1 Workflow	173
List of Publications	175
List of Supervised Theses	177