

Table of Contents

1	Introduction	1
1.1	Motivation	1
1.2	Summary of research contributions and outline	3
1.2.1	Lightweight block ciphers	3
1.2.2	Lightweight hash functions	4
1.2.3	Lightweight public key cryptography	4
2	Fundamentals	7
2.1	Design strategies for lightweight cryptography	7
2.2	Notations	8
2.3	Introduction to ASIC design	9
2.3.1	Semi-custom standard cell design flow	9
2.3.2	Power consumption	10
2.3.3	Metrics	10
2.3.4	Architecture strategies	11
2.4	Hardware properties of cryptographic building blocks	12
2.4.1	Internal state storage	12
2.4.2	Combinatorial elements	13
2.4.3	Confusion and diffusion	14
3	New Lightweight DES Variants	17
3.1	DESL and DESXL: design ideas and security consideration	17
3.2	Related work	18
3.3	Design criteria of DESL	19
3.3.1	Improved resistance against differential cryptanalysis and Davies Murphy attack	20
3.3.2	Improved resistance against linear cryptanalysis	21
3.3.3	4R iterative linear approximation	23
3.3.4	5R iterative linear approximation	24
3.3.5	nR iterative linear approximation	26
3.3.6	Resistance against algebraic attacks	26
3.3.7	Improved S-box	26
3.4	Implementation results	27
3.4.1	Lightweight hardware implementation of DES and DESX	27
3.4.2	Lightweight hardware implementation of DESL and DESXL	29
3.4.3	Lightweight software implementation results	29
3.5	Conclusions	31
4	PRESENT - An Ultra-Lightweight Block Cipher	33
4.1	Related work	33

Table of Contents

4.2	Design decisions	34
4.3	Algorithmic description of the PRESENT encryption routine	35
4.3.1	addRoundKey	36
4.3.2	sBoxlayer	36
4.3.3	pLayer	37
4.4	Algorithmic description of the PRESENT decryption routine	39
4.4.1	addRoundKey	39
4.4.2	invSBoxlayer	39
4.4.3	invPLayer	40
4.5	The key schedule	40
4.5.1	The key schedule for PRESENT-80	40
4.5.2	The key schedule for PRESENT-128	40
4.6	Cryptanalytic Aspects	42
4.6.1	Differential and linear cryptanalysis	42
4.6.2	Structural attacks	46
4.6.3	Algebraic attacks	46
4.6.4	Key schedule attacks	47
4.6.5	Statistical saturation attacks	47
4.6.6	Algebraic differential attacks	48
4.7	Further observations	48
5	Implementation Results of PRESENT	51
5.1	ASIC Implementations	51
5.1.1	Serialized ASIC implementation	51
5.1.2	Round-based ASIC implementation	53
5.1.3	Parallelized ASIC implementation	54
5.1.4	Discussion of the implementation results	55
5.2	FPGA implementation results	57
5.2.1	Target platform and designflow	57
5.2.2	Architecture of the round-based FPGA implementation	57
5.2.3	Implementation results	59
5.3	Hardware/Software co-design implementation results	60
5.3.1	ASIC based co-processor implementation results	60
5.3.2	FPGA-based co-processor implementation results	61
5.3.3	Instruction set extensions for bit-sliced implementation	63
5.4	Software Implementations	64
5.4.1	Implemented variants	64
5.4.2	Software implementation on a 4 bit microcontroller	65
5.4.3	Software implementations on an 8-Bit microcontroller	71
5.4.4	Software implementations on a 16-Bit microcontroller	75
5.4.5	Software implementations on a 32-Bit CPU	78
5.4.6	Other software implementations of PRESENT	80
5.5	Conclusions	82
6	Lightweight Hash Functions	83
6.1	Motivation	83
6.2	Related Work	84
6.3	Design decisions	85

6.4	Background on hash function constructions	86
6.4.1	Dedicated hash function constructions	86
6.4.2	Block cipher constructions	86
6.5	Compact hash functions with a digest size of 64 bits	87
6.5.1	Description of DM-PRESENT-80 and DM-PRESENT-128	87
6.5.2	Implementation results of DM-PRESENT-80	88
6.5.3	Implementation results of DM-PRESENT-128	92
6.6	Compact hash functions with a digest size of 128 bits	95
6.6.1	Description of H-PRESENT-128	96
6.6.2	Implementation results of H-PRESENT-128	96
6.7	Compact hash functions with a digest size of ≥ 160 bits	100
6.7.1	Description of C-PRESENT-192	100
6.7.2	Implementation results and estimations of C-PRESENT-192	102
6.7.3	Dedicated design elements inspired by PRESENT	103
6.7.4	Estimations of PROP-1 and PROP-2	105
6.8	Conclusion	106
7	Lightweight Public-Key Cryptography	109
7.1	Motivation	109
7.2	Related Work	109
7.3	The GPS identification scheme	110
7.3.1	History	110
7.3.2	Parameters and optimizations	110
7.3.3	Design decisions	113
7.4	The crypto-GPS proof-of-concept prototype board	114
7.4.1	The input and output pins of the ASIC	114
7.4.2	The handshake protocol for communication between microcontroller and crypto-GPS ASIC	115
7.4.3	Different architectures of the ASIC	116
7.5	Hardware implementations of round-based crypto-GPS	117
7.5.1	Implementation of the Controller component	119
7.5.2	Implementation of the Addwc component	119
7.5.3	Implementation of the S_Storage component with a fixed secret s	119
7.5.4	Implementation of the S_Storage component with a variable secret s	120
7.6	Hardware implementation of serialized crypto-GPS	120
7.6.1	Implementation of the Controller component	120
7.6.2	Implementation of the S_Storage component with a fixed secret s	122
7.7	Discussion of implementation results	122
8	Physical Security Aspects	125
8.1	Motivation	125
8.2	A pervasive attacker model	125
8.2.1	Classification of attackers	125
8.2.2	Classification of attacks	126
8.2.3	Classification of attack costs	127
8.3	Classification of pervasive devices	127
8.3.1	Unprotected pervasive devices	128
8.3.2	Partly protected pervasive devices	128

Table of Contents

8.3.3	Tamper resistant pervasive devices	130
8.4	Evaluation of pervasive devices with respect to physical security aspects	131
8.4.1	Evaluation of unprotected pervasive devices	131
8.4.2	Evaluation of partly protected pervasive devices	131
8.4.3	Evaluation of tamper resistant pervasive devices	132
8.5	Introduction to side channel attacks and their countermeasures	132
8.5.1	Countermeasures at the algorithmic level	133
8.5.2	Countermeasures at the cell level	135
8.6	Cost overhead estimations of side channel countermeasures	137
8.6.1	Cost overhead estimations for a masked serialized hardware implementations of PRESENT	137
8.6.2	Cost overhead estimations for a masked 4 bit software implementations of PRESENT	140
8.7	Conclusions	140
9	Conclusion	143
	Bibliography	147
	List of Figures	165
	List of Tables	167
	Appendix	169
	Curriculum Vitae	175