

Table of Contents

Abstract	V
1 Introduction	1
2 Fundamentals	5
2.1 Components of a Transmission System	5
2.2 Message Authentication Codes	8
2.2.1 General	8
2.2.2 Generation using a symmetric Block Cipher	11
2.2.3 Generation using a Dedicated Hash Function	12
2.2.4 Security Aspects of Message Authentication Codes	13
2.2.5 Message Authentication Codes and Digital Signatures	15
2.3 Channel Coding	16
2.3.1 Reed-Solomon Codes	16
2.3.2 Convolutional and Turbo Codes	19
2.3.3 Soft Input Soft Output Decoding	21
2.3.4 Concatenated Codes	22
2.4 Joint Source and Channel Coding	24
3 Related Work	27
3.1 Channel Coding with Bit Inversion	27
3.2 Error tolerant Cryptographic Checksums	29
3.3 Authentication over Noisy Channels	32
4 Soft Input Hard Verification	33
4.1 Correction by Iterative Bit Inversion	33
4.2 Security Aspects of Soft Input Hard Verification	37
4.3 Correction Improvement by Interleaving and Feedback	39
4.4 Correction by Insertion of Known Bits	44
5 Applications of Soft Input Bit Inversion	47
5.1 Correction of Reed-Solomon Decoding Errors	47
5.2 HARQ IBF Algorithm	51
5.3 N-Channel STOP and WAIT Protocol of WiMAX	53

5.4	Enhanced Packet Combining over HYBRID-ARQ	56
5.5	Error Correcting and Weighted Noise Tolerant Message Authentication Codes	58
6	Soft Verification of the Message Authentication Codes	61
6.1	Soft Verification versus Hard Verification	61
6.2	Soft Input Soft Verification.....	61
6.3	Calculation of the Threshold.....	65
6.3.1	Probability Distribution Function of the Hamming Distance	65
6.3.2	Analysis of the Hamming Distance and the Threshold.....	71
6.3.3	Simulative Specification of the Threshold.....	81
6.4	Verification Gain.....	84
7	Security Aspects of Soft Input Soft Verification	89
7.1	Forgery Attacks.....	89
7.1.1	Birthday Paradox for Near Collisions.....	89
7.1.2	Compensation of the Reduced Complexity of a Forgery Attack	92
7.2	Wrong Decisions	94
7.2.1	Probability of a Wrong Decision	94
7.2.2	Compensation of the Increased Probability of Wrong Decision	98
7.3	Total Compensation	100
7.4	Selection of the Algorithmic Parameters	105
8	Soft Output of Soft Input Soft Verification	109
9	Applications of Soft Input Soft Verification	113
10	Summary and Future Work	115
	Epilogue	117
	Works Cited	119
	List of Abbreviations	125