

Contents

1. Introduction	1
1.1. Motivation	1
1.2. Outline	2
1.3. Remarks	5
2. Related Work	7
2.1. Security of Compressed Sensing Based Encryption	7
2.2. Related Encryption Schemes	8
2.3. Open Problems	9
3. Fundamentals	11
3.1. Compressive Sensing	11
3.1.1. Signal representation	11
3.1.2. Requirements on the sampling system	14
3.1.3. Reconstruction	15
3.2. Symmetric Cryptography	17
3.2.1. General	17
3.2.2. Security for one-time key encryption	19
3.2.3. Modes of operation	21
3.2.3.1. Security in the many-time key scenario	21
3.2.3.2. Standardized block cipher modes	22
3.2.4. Data integrity and authentication-encryption	25
3.2.4.1. Message unforgeability	25
3.2.4.2. Authenticated-encryption	27
4. Compressive Sensing Based Encryption	33
4.1. General	33

4.2.	Secrecy for One-Time Encryption	34
4.2.1.	Establishing security definitions	34
4.2.2.	Impact of different sensing matrix designs	38
4.3.	Secrecy for Many-Time Encryption	43
5.	Compressive Sensing Encryption Modes	49
5.1.	Introduction	49
5.2.	The General Design	52
5.2.1.	Design goals	52
5.2.2.	Matrix generation	53
5.2.2.1.	Matrix generation algorithm	53
5.2.2.2.	Implementation details	54
5.2.2.3.	Security analysis	59
5.2.2.4.	Performance analysis	61
5.2.3.	Normalized encryption	62
5.2.4.	Decryption	65
5.3.	Compressive Sensing Counter Mode	66
5.3.1.	Design and concept	66
5.3.2.	Security analysis	68
5.3.3.	Properties	70
5.4.	Compressive Sensing with Cipher Block Chaining	72
5.4.1.	Design and concept	72
5.4.2.	Security analysis	74
5.4.3.	Properties	75
5.5.	Compressive Sensing with Cipher Feedback	77
5.5.1.	Design and concept	77
5.5.2.	Security analysis	79
5.5.3.	Properties	80
5.6.	Comparison of the Proposed Modes	83
5.7.	Experimental Results	86
5.7.1.	Proof of concept	86
5.7.2.	Measurement distribution	90
5.7.3.	Error sensibility	93
6.	Compressive Sensing with Authenticated-Encryption	99
6.1.	Introduction	99
6.2.	Generic Constructions	100
6.2.1.	General	100
6.2.2.	CS-encrypt-and-MAC	101
6.2.3.	MAC-then-CS-encrypt	102
6.2.4.	CS-encrypt-then-MAC	103

6.3. CS Authenticated-Encryption Modes	104
6.3.1. Design and concept	104
6.3.2. Implementation and security	108
6.3.2.1. Implementation details	108
6.3.2.2. Security analysis	111
6.3.2.3. Proof of concept	112
7. Fog Computing Security by Compressive Sensing Modes	113
7.1. System Design	113
7.2. Implementation	118
7.2.1. Software architecture	118
7.2.2. The service framework	118
8. Conclusion	125
8.1. Contributions	125
8.2. Future Work	127
Appendix A. Alternative Confidentiality Mode Designs	129
Bibliography	133