





# Modes of Operation for Compressed Sensing based Encryption

DISSERTATION  
zur Erlangung des Grades eines Doktors  
der Naturwissenschaften  
**Dr. rer. nat.**

vorgelegt von  
Robin Fay, M. Sc.

eingereicht bei der Naturwissenschaftlich-Technischen Fakultät  
der Universität Siegen  
Siegen 2017

1. Gutachter: Prof. Dr. rer. nat. Christoph Ruland
  2. Gutachter: Prof. Dr.-Ing. Robert Fischer
- Tag der mündlichen Prüfung: 14.06.2017

**Institut für  
Digitale Kommunikationssysteme**

**Forschungsberichte**

Herausgeber: Univ.-Prof. Dr. Christoph Ruland

Band 34

**Robin Fay**

---

**Modes of Operation for  
Compressed Sensing based  
Encryption**

---

**SHAKER  
VERLAG**

Aachen 2017

**Bibliographic information published by the Deutsche Nationalbibliothek**  
The Deutsche Nationalbibliothek lists this publication in the Deutsche  
Nationalbibliografie; detailed bibliographic data are available in the Internet at  
<http://dnb.d-nb.de>.

Zugl.: Siegen, Univ., Diss., 2017

Copyright Shaker Verlag 2017

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the publishers.

Printed in Germany.

ISBN 978-3-8440-5445-3  
ISSN 1614-0508

Shaker Verlag GmbH • P.O. BOX 101818 • D-52018 Aachen  
Phone: 0049/2407/9596-0 • Telefax: 0049/2407/9596-9  
Internet: [www.shaker.de](http://www.shaker.de) • e-mail: [info@shaker.de](mailto:info@shaker.de)

TO VERENA . . .

s7+OZThMeDz6/wjzq29ACJxERLMATbFdP2jZ7I6tpyLJDYa/yjCz6OYmBOK548fer  
76zoelzF8dNf/0k8H1KgTuMdPQg4ukQNmadG8vSnHGOVpxXNEPWx7sBOTpn3CJzei  
d3hbFD/cOgYP4N5wFs8auDaUaycgricPAWGAw18aYhTkbjnfswk4zPvRIF++EGH  
UbdBMdOWWQp4G44ZbzMiMTlzlzm6La5gRQ65esUgnOoZLy73dEy+DIZW5+NsBCaj  
GBttsJta6XheB7mIOphMZUTj51jM0CDMNvJl39bq/TQLocvV/4inFUNhfa8ZM  
7kazoz5tqjxCZocBi153PSsFae0BksynaA9ZlVpZM9N4++oAkBiFeZxRrdGLUQ6H  
e5A6HFyxMSel8sWN65SCDpQNd2FwdkzuiT2Z4RkDCiJ1D19vXICuZVx5StDmYrx  
S6mWzcg1aAsEm2k+Skhayux4a+qt19sD5j5cDLECo8ac+RL7/ovnzuExZ3trm+o  
6GN9c7mJBgCFEDkeror5AF4VHUtz2bDlyqCr42u4yxVjsj5FWIC9k4aJy6XzQ  
cRKGnsNrVOZcGokRO+IacuWBpI4o3n3Amst8MayayKU+b94VgnrJAo02Fp0873wa  
hyJ1qVF9YyRX+cou151wD/W/e151qy/x/Pd9hdTyd755mCmpoLo7c9yHCVuKWyOgw  
ZLu1zPKX1YNegeAP8iyeaJLnPln1L-z4447lsobnVzMs3ktWO6k071OH7zTy9  
w+0UzbxDd/qdJ1rENryiAO9864j4bUi9+yS/2/kLL7nPy5Kxg3Et0F1319/+c/  
IY0wNyAcotWp+hPtHw46dcDO1Jz0rMQf1XCdn0kTQ61nHe5MG7Tz2uNtR3by+7U  
CLgNPkv17hFPW/IX3Y1kVwh04p6AZJTyktsSPubqrE9PG00L5np1V3B/x+Cce2p  
nijoR32u01TK17/T1p0enFvD8C351BnjC86Z201badnB9DnQSP3XH4JdQfbtN8  
BXhOglfbobj5T9SHVZBpbhZdeXAFlmdoZQ8JhdZ03EHDhjyzsXD1KUA6Xey03wU  
unwrpTPz94cdQM7vwCbdJn1Pyta2f79NwAHICXdlp0pV5yNH20biAADH6Q94Vc  
DhgjzjaFnVbhuHvsxKOOQ61GDeW/F+xGb9P9OpwDgAxRa/40IBaRDt2nhN4k9c0  
1whVbfft2T1Vb1rJUsjCAZFKR/3P8siZ5ggVd7zNMCNmLwQDGKNQanOxPscVWuJ3  
A4ETETcvRouPdLOGE0DioyCavA5ljNltqTjNkuje3NkDjv/PZ6x013rCLZKMi4o  
KGJAS8Eyj0UjzXXY7Yq5s9nAzk0yW5uQRIsseGG6f1o7j0IN2OAjTcegmFl  
PK8G1rCJch8Y2VvnuLVPQsPTAghOyQrHeR/+jSSFrHGmufDMo348Vs2MPA  
ynFnvSA6oZs79hsQZoXyHi5CcvgE5sRHTM1GrHhbvgpoO+7VegL6s195J3-n  
RCuQbf3iHk5yQ44p/r1zds1k1a8q0r1v+viKJ188uwzSr7PmOrR3UPSYotJroH  
WUVgZr+CaljaLhWCwpZxhJwKwCv69CnCtBg0skD1Auds4v8aOKbzgkZkj7  
Ji1fVHo+Vpj1hHs1lSvgyKQS7AAIIWhbZJWqEEmgYALB9BQj5rloukBHJ08cFXt  
6jYSjhR4gWIVY+MneoTNUM57mvq20j5zcW/CXKhqdGBIGVnXoqBGX5zrlqTqVIK06  
wdM1dXpQwbmltEshf+XmGGMJF5qKy219OcupvYialmge0PkwCqpcQxxqAFH  
C0qnjggF0v2PQV8Ungq13fh0fBtuR7y0bULBAShDntduTwD87BVgixLobiUKw  
eN9s8itDfsu1EduUM12AB2h5/rphW28ULofSP51Qh0H8NsFuXTA8is1Pr3GQe2+  
LrGEHEJzJoz6QBNfkmhWlja1VjuFybzQ5R5v07x/4K1f7bwF5XubS195pPlci+fGB  
/yeZYjs9NjKo1r3ch8DA1Y10w4J1mpfnb9q/EzVsSW51Wi3dgoCWw5g25TAyRf  
AkzBvaPGSGDdin/Pseq59dQ4GKSA1XQZriX5ounNjBysRvckirAv7ADzB9kL9X6Q  
XoLdacRYYBw4gWYH918h1u1zOc6ZgE4O2u+z/wuUKHian4CBTiasRuHprCz91PnK0L  
GEcuJp8YPgXtyfKR49nwPBKjwf6EFRfd71XRXWE9vMgfF+mNflcgivVGZOKQGQus  
Ayjs5bD8sz8w2ck1bcwQ7Up948P2dTfmeoSt7ip1VYRvbfXh6yEA2cKtD  
IWk7aAvEsDob4wAypgjue/ajrwd1/X9vpHB6Zjx358AmvOufyICLT495NC3xq  
RhndJ1vGclCs8vBvepSaMJDG2cG7V8tOGYERuH2GDCDJZsMtPSHM7vKzRjC  
ootOT5H6GPjY8KEFVVR0REFib2Wg/X9zSQTdPkgQnweZ9gg5pu+VR8GamaisQfb  
iT6s2muh26h6c7aqw120Jep54vrvuiwdj94AiavarxKLFVgcvHCAy2vBhJa  
BTM1uUOBLKWD1Z51/yRPLco8+fm3ap2Yno16YwOl6sboiFyYSxtmtrUm8sdqaP  
DsBsOeCVEU71gZdgVAieDheNk0AdASwUxGrFgI9UNzTVKbxRydwtlXIj6pNSJtrb  
b8gz/QLKwbaAdgo5Wsj3X0hox97ft47UgT2H543zBzApP3cVwMpwL73GbmVRG  
zcc0/LbaLdtXxm+v+M8x5F6HdpKnoEc1P50f9WWR0PFGDN10qCfj08tw3r1A  
A6idjrYQd5krP+eXZUUXMKxVxXerX1OxTpex/5sjeOXiZYpXW5AGAs  
z/190d+UCKDHE7YmQ4WKnN+RgSDWAi7x2IM17F53qgloXLw5HTzaipnUNRhpRg  
WEZ+YbwUnQOYN-hSiOxYAUSC3z+G8SkT2HhE+9A5pHxTgNQEDjO/RfQ0h1rbxtF  
SEvDzX6LF2rKe8YAEFitTrbPMyx8EmYG+ZvKaaD1Zz/ub5xG1xvFQ+tQo6WpsT  
051wKbLu7E5117x7FTRfou686PfwHtv1t05JVdLzj7t3coZvgxek+hxqaGj0PHdHnK  
e0etBo28n0NTdx3c+jfp7nJAyW824P4b0q3Y+y/+2s8225uipHC7Ob1CCD05ph  
1uy/hPV8GH4eWaQnjgJnsc/OaciInmrFC9CPyOCTwRuvWuRXLu7K7OxyhgAksz  
blCtdzXN4A8r7JwdFobs7U61NxMdh0+twW8keES10GsbAvOzwgcOrndNivNM0Dj  
1+8HRK01CS5fzVdJWQ6Wc9H1xq7yyBwICIN8HjBmshon2qDtegAdtF+n+RvQ8Cbc  
VIXv8hbdofcTxEQLPyDn9V19s6AcNLTmdWCsheZlw38FQR+8TO2W174s5v3aTLG1  
geXAlaJCZzk+u9h12DqNkfKeFGJyVWk8wCz+RXNbEx3VymGDLY9ZJeP7FytIDOV  
7kXU1w1ToW4dSZTSzBo8r1t7OB9xQvT4mdQEpY4N4FR0xkliGJ4XrgPkoA45JkH  
lbwXc+PK9Sx+gDiLTDfKCMzT

## Acknowledgement

This research was funded by the German Research Foundation (DFG) under project number RU 600-11/1.



# Abstract

Compressed Sensing offers the possibility to jointly compress and encrypt sparse or compressible signals during the sampling process, i.e. directly at the sensor level. For the purpose of encryption, only the sampling matrix, which is also needed for the signal recovery, must be kept secret. However, this type of encryption scheme is no longer secure if multiple signals are encrypted, since the same plaintext will always yield the same ciphertext. This thesis proposes modes of operations for Compressed Sensing that allow the secure encryption of multiple signals.

First, different attacks and threat models are analyzed in order to develop security definitions for Compressed Sensing based encryption and Compressed Sensing modes of operations. The results from this analysis are used to design a general model for Compressed Sensing modes, which ensure confidentiality and additionally reduce the information leakage of Compressed Sensing encryption. The security and performance of cryptographic constructions that are suitable for implementing the general model are evaluated and three dedicated modes with different quality of service properties are derived from the general design. These modes of operation and their corresponding security analysis are the first main result of this thesis.

In addition to confidentiality, which is achieved through encryption, another important security service is data integrity. This work also examines so-called authenticated-encryption modes for Compressed Sensing, which ensure confidentiality and data integrity simultaneously. A general model for Compressed Sensing with authenticated-encryption is developed and dedicated schemes are derived from this model. The security of these schemes is reduced to the security of the underlying cryptographic constructions and primitives. Compressed Sensing with authenticated encryption provides security even in the case where an adversary has the ability to tamper with the ciphertext.

The final contribution of this thesis is the integration of the proposed Compressed Sensing modes into a distributed application. A software architecture for Industry 4.0 applications is developed and implemented. The designed system includes all necessary components for the usage of Compressed Sensing modes, like key-establishment and parameter exchange. Next to security, a main design goal of this system is usability. The user just determines the security service for his application and all security relevant operations are handled by the software, transparent for the user. This approach prevents security problems that are caused by inappropriate usage of cryptographic schemes.

The Compressed Sensing modes developed in this thesis are suitable for a wide range of real world applications due their joint sampling, compression and end-to-end security that starts at the sensor level. The proposed software-system completes the contribution of this work, since it realizes all necessary components for the usage of the designed modes.

# Zusammenfassung

Compressed Sensing bietet die Möglichkeit spärlich besetzte oder komprimierbare Signale bereits bei der Abtastung - also im Sensor - zu komprimieren und gleichzeitig zu verschlüsseln. Dabei muss zur Verschlüsselung lediglich die Abtastmatrix, welche auch für die Signalrekonstruktion notwendig ist, geheim gehalten werden. Allerdings ist diese Verschlüsselungstechnik nicht mehr sicher, wenn mehrere Signale verschlüsselt werden, da derselbe Klartext immer denselben Schlüsseltext ergibt. Deshalb befasst sich diese Dissertation mit Betriebsarten für Compressed Sensing, die eine sichere Verschlüsselung von mehreren Signalen ermöglichen.

Zunächst werden verschiedene Angriffe und Angreifermodelle untersucht, um Sicherheitsdefinitionen für Compressed Sensing basierte Verschlüsselung und Compressed Sensing-Betriebsarten zu entwickeln. Basierend auf den Ergebnissen dieser Analyse wird ein generelles Modell für Compressed Sensing-Betriebsarten entworfen, welche Vertraulichkeit gewährleisten und darüber hinaus den Informationsverlust der Compressed Sensing-Verschlüsselung reduzieren. Nach einer Sicherheits- und Performancebewertung der für die Implementierung geeigneten kryptographischen Verfahren werden drei dedizierte Betriebsarten aus dem generellen Design abgeleitet, die verschiedene Dienstgütekriterien wie Parallelisierbarkeit oder Selbstsynchronisation aufweisen. Diese Betriebsarten und die damit verbundenen Sicherheitsanalysen sind das erste Hauptergebnis dieser Dissertation.

Zusätzlich zur Vertraulichkeit, die durch Verschlüsselung erreicht wird, ist Datenunversehrtheit ein weiterer wichtiger Sicherheitsdienst. Deshalb werden in dieser Arbeit auch sogenannte Authenticated-Encryption-Betriebsarten für Compressed Sensing entworfen, die Vertraulichkeit und zeitgleich den Schutz der Datenunversehrtheit gewährleisten. Auch hier wird zunächst ein generelles Modell für diese Betriebsarten entwickelt, aus dem dann konkrete Implementie-

rungen abgeleitet werden, deren Sicherheit auf die zugrundeliegenden kryptographischen Verfahren zurückgeführt wird. Compressed Sensing mit Authenticated-Encryption bietet auch dann Sicherheit, wenn ein Angreifer gezielt Schlüsseltexte manipulieren kann.

Ein letzter Aspekt, der in dieser Arbeit betrachtet wird, ist die Integration der entwickelten Betriebsarten in eine verteilte Anwendung. Dazu wird eine Softwarearchitektur für Industrie 4.0-Anwendungen entworfen und implementiert, welche die nötigen Komponenten für den Einsatz der Compressed Sensing-Betriebsarten, wie Schlüsselvereinbarung und Parameteraustausch, beinhaltet. Neben der Sicherheit ist ein Hauptziel des entworfenen Systems die Benutzerfreundlichkeit. Alle sicherheitsrelevanten Operationen werden für den Anwender transparent von der Software durchgeführt, sodass der Anwender lediglich festlegen muss, wie die Daten seiner Anwendung geschützt werden sollen. Auf diese Weise werden Sicherheitsprobleme vermieden, die durch unsachgemäße Verwendung von kryptographischen Verfahren entstehen.

Die in dieser Arbeit entwickelten Betriebsarten für Compressed Sensing sind durch die gleichzeitige Abtastung und Komprimierung für viele reale Anwendungsfälle interessant und ermöglichen echte Ende-zu-Ende-Sicherheit, die bereits im Sensor beginnt. Das vorgestellte Softwaresystem vervollständigt den Beitrag dieser Arbeit, da es die nötigen Komponenten für die Verwendung der entwickelten Betriebsarten realisiert.

# Contents

<b>1. Introduction</b>	<b>1</b>
1.1. Motivation . . . . .	1
1.2. Outline . . . . .	2
1.3. Remarks . . . . .	5
<b>2. Related Work</b>	<b>7</b>
2.1. Security of Compressed Sensing Based Encryption . . . . .	7
2.2. Related Encryption Schemes . . . . .	8
2.3. Open Problems . . . . .	9
<b>3. Fundamentals</b>	<b>11</b>
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
<b>4. Compressive Sensing Based Encryption</b>	<b>33</b>
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
<b>5.</b>	<b>Compressive Sensing Encryption Modes</b>	<b>49</b>
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
<b>6.</b>	<b>Compressive Sensing with Authenticated-Encryption</b>	<b>99</b>
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
<b>7.</b>	<b>Fog Computing Security by Compressive Sensing Modes</b>	<b>113</b>
7.1.	System Design . . . . .	113
7.2.	Implementation . . . . .	118
7.2.1.	Software architecture . . . . .	118
7.2.2.	The service framework . . . . .	118
<b>8.</b>	<b>Conclusion</b>	<b>125</b>
8.1.	Contributions . . . . .	125
8.2.	Future Work . . . . .	127
<b>Appendix A. Alternative Confidentiality Mode Designs</b>		<b>129</b>
<b>Bibliography</b>		<b>133</b>