



Alexander May

Curriculum Vitae

Kontakt Daten

Anschrift Horst Görtz-Institut für IT-Sicherheit
Fakultät für Mathematik, 44801 Bochum
Telefon 0234 32-23261
Telefax 0234 32-14430
Email alex.may@rub.de
Homepage <http://www.cits.rub.de/index.html>
Geburtsdatum 22.03.1974
Geburtsort Friedberg (Hessen)
Familienstand verheiratet, 2 Söhne
Sprachen deutsch, englisch

Akademischer Werdegang

2007- **W3-Professor**, *Ruhr-Universität Bochum*, Kryptologie und IT-Sicherheit.
Horst-Görtz Institut für IT-Sicherheit, Fakultät Mathematik
2005-07 **Juniorprofessor**, *TU Darmstadt*, Kryptographische Protokolle.
Fachbereich Informatik
2004-05 **Post-Doc**, *Universität Paderborn*, DFG-Schwerpunkt Sicherheit in der IKT.
Fachbereich Informatik
2000-03 **Doktorand**, *Universität Paderborn*.
Fachbereich Informatik
2000 **Doktorand**, *ETH Zürich*.
Department Informatik
1993-99 **Informatik-Student**, *J.W. Goethe-Universität Frankfurt*.

Universitäre Funktionen

2014-16 **Sprecher**, *DFG-Graduiertenkolleg 1817 Ubiquitäre Kryptographie*.
2014- **Mitglied des Executive Boards**, *RUB Research School*, DFG-Exzellenzinitiative.
2012-14 **Instituts-Direktor**, *Horst-Görtz Institut für IT-Sicherheit*.

Drittmittel (letzte 5 Jahre)

DFG

- 2012-17 **Graduiertenkolleg 1817 Ubiquitäre Kryptographie'**, *Sprecherfunktion & Teilprojekt Homomorphic Encryption*, 1 Stelle.
- 2014-16 **Schwerpunktprogramm Big Data**, *Teilprojekt Security-Preserving Operations on Big Data*, 1 Stelle.
- 2011-13 **Schwerpunktprogramm 1307 Algorithm Engineering**, *Teilprojekt Representation Solving*, 1 Stelle.
- 2010-12 **RUB Research School (Exzellenz-Initiative)**, *Teilprojekt Coding-Based Cryptanalysis*, 1/2 Stelle.

EU

- 2015-17 **Koordinator Ruhr-Uni Bochum, Marie Skłodowska-Curie ITN**, *Teilprojekt Cryptanalysis in Cloud Computing*, 500 k€, 1 Stelle.
- 2012-17 **ERC Starting Grant 307952 Fast and Sound Cryptography**, *Koordinator: Alon Rosen(Israel)*, beteiligt als Partner mit eigenem Budget, 96k€.
- 2007-13 **Mitglied im Network of Excellence in Cryptology ECRYPT**, *Leiter der Arbeitsgruppe Cryptanalysis and Mathematical Foundations*.

Behörden

- 2011 **BSI-Projekt**, *Faktorisieren mit Schnorr-Gittern*, 36k€.

Industrie

- 2012-14 **Kooperation mit Secunet (Essen)**, *Post-Quantum Krypto*, 1/2 Stelle.

10 ausgewählte Publikationen (seit 2010)

Meine Zitierungsstatistik laut Google Scholar:

- **Zitate: 1686**
- **h-Index: 24**

Konferenzarbeiten (peer-reviewed)

- Parallel Implementation of BDD enumeration for LWE mit Elena Kirshanova, Friedrich Wiemer
In Applied Cryptography and Network Security (**ACNS 2016**), Lecture Notes in Computer Science, Springer-Verlag, 2016.
- On Computing Nearest Neighbors with Applications to Decoding of Binary Linear Codes mit Ilya Ozerov
In Advances in Cryptology (**Eurocrypt 2015**), Lecture Notes in Computer Science Volume 9056, Springer-Verlag, 2015.
- A Generic Algorithm for Small Weight Discrete Logarithms in Composite Groups mit Ilya Ozerov
In Selected Areas in Cryptography (**SAC 2014**), Lecture Notes in Computer Science Volume 8781, Springer-Verlag, 2014.

- Certifying RSA mit Saqib A. Kakvi, Eike Kiltz
In Advances in Cryptology (**Asiacrypt 2012**), Lecture Notes in Computer Science Volume 7658, 404-414, Springer-Verlag, 2012.
- Decoding Random Binary Linear Codes in $2^{n/20}$: How $1 + 1 = 0$ Improves Information Set Decoding mit Anja Becker, Antoine Joux, Alexander Meurer
In Advances in Cryptology (**Eurocrypt 2012**), Lecture Notes in Computer Science Volume 7237, Seiten 520-536, Springer-Verlag, 2012.
- Decoding Random Linear Codes in $\tilde{O}(2^{0.054n})$ mit Alexander Meurer, Enrico Thomae
In Advances in Cryptology (**Asiacrypt 2011**), Lecture Notes in Computer Science Volume 7118, Seiten 55-72, Springer-Verlag, 2011.
- On CCA-Secure Somewhat Homomorphic Encryption mit Jake Loftus, Nigel Smart, Frederik Vercauteren
In Selected Areas in Cryptography (**SAC 2011**), Lecture Notes in Computer Science Volume 7073, Seiten 197-124, Springer-Verlag, 2011.
- Correcting Errors in RSA Private Keys mit Wilko Henecka, Alexander Meurer
In Advances in Cryptology (**Crypto 2010**), Lecture Notes in Computer Science Volume 6223, Seiten 351-369, Springer-Verlag, 2010.
- Maximizing Small Root Bounds by Linearization and Applications to Small Secret Exponent RSA mit Mathias Herrmann
In Practice and Theory in Public Key Cryptography (**PKC 2010**), Lecture Notes in Computer Science Volume 6056, Springer-Verlag, 2010.

Buchkapitel

- Using LLL-Reduction for Solving RSA and Factorization Problems: A Survey
The LLL Algorithm: Survey and Applications, Springer, 2010.