

Curriculum Vitae



Stanislav V. Bulygin, 28.01.1982

Secure Data, Center for Advanced Security Research
(CASED)

Morneuegstrasse, 32
64293 Darmstadt, Germany

Room: 4.3.09

Phone (office): +49 6151 16 70484

Mobile phone (private): +49 176 21321299

Email: Stanislav.Bulygin@cased.de, s_bulygin@hotmail.com

URL: <http://www.mathematik.uni-kl.de/~bulygin/>

CURRENT POSITION:

Researcher, post doctoral fellow

Working group Cryptographic Primitives

Department Secure Data

CASED

Supervisor: Prof. Dr. J. Buchmann

Research concentration: coding-based and multivariate cryptography, algebraic cryptanalysis

ACADEMIC PREPARATION:

Ph.D. candidate in Mathematics, University of Kaiserslautern (Germany), since March, 2006

Date of defence: 12.06.2009

Supervisor: Prof. Dr. Greuel G.-M.

Topic of the dissertation: "Polynomial system solving for decoding linear codes and algebraic cryptanalysis"

Grade: magna cum laude (very good)

M.Sc. in Mathematics, University of Kaiserslautern (Germany), February, 2006

Concentrations: Computer Algebra, Algebraic Geometry, and Computer Science

Thesis: "Some Problems of Coding Theory and Cryptography" (grade: 1.0)

Supervisor: Prof. Dr. Greuel G.-M.

GPA: 1.0 (1.0 is the best possible, 5.0 is the lowest, 0.3 is the step)

Diploma in Mathematics, Kyiv National Shevchenko University (Kyiv, Ukraine), June, 2005

Concentrations: Applied Mathematics, Teaching of Mathematics

Thesis: "Asymptotically good algebraic-geometric codes. Questions of algorithmic realization", (grade: 5), in Ukrainian

Advisor: Prof. Dr. Ovsienko S.A.

GPA: 4.9 (5.0 max)

Bachelor of Mathematics, Kyiv National Shevchenko University (Kyiv, Ukraine), June, 2004

Diploma with honors

Concentrations: Mathematics, Applied Mathematics

Thesis: "On some applications of Algebraic Function Fields to the Problems of Coding Theory", (grade: 5)

Advisor: Prof. Dr. Ovsienko S.A.

GPA: 4.9 (5.0 max)

Freedom Support Act Undergraduate Program, University of Southern Indiana (Evansville, IN, USA), 2001-2002
Concentrations: Economics, Statistical Data Analysis
GPA: 4.0 (4.0 max)

PROJECTS INVOLVEMENT:

KryFoVe: Computeralgebra (Dependable Adaptive Systems and Mathematical Modeling: Cluster of Excellence in Rhineland-Palatinate), March 2006 - May 2008

- Applications of advanced algebraic-symbolic methods of computer algebra to cryptanalysis, to coding theory and to formal verification of microelectronic systems

Book project: A book on methods from algebra, geometry, and combinatorics in coding theory and cryptography to be published by the Cambridge University Press, March 2008 - present

Development, implementation, and application of mathematical-algebraic algorithms to the formal verification of digital systems with arithmetic blocks (Deutsche Forschungsgemeinschaft (German Research Foundation) research project), March 2009 - June 2009

PRACTICAL SKILLS:

Programming languages: C/C++, Python

Computer algebra systems: SINGULAR, GAP (Groups, Algorithms, and Programming), Magma

Member of the SINGULAR-Team: development and maintenance for the coding theory related functionality, benchmarking, general support

Member of the GBABL-Team: working on the implementation of symbolic techniques for formal verification of digital circuits

CURRENT RESEARCH INTERESTS:

- *Symbolic methods in cryptology.* In particular, Gröbner bases-based cryptanalysis of block ciphers
- *Symbolic methods in the theory of error-correcting codes.* In particular, Gröbner bases in decoding of linear codes, determination of their minimum distance
- Algebraic coding theory
- Combinatorics

LANGUAGES:

- Russian native
- Ukrainian second native
- English fluent
- German good
- Spanish basics

PROFESSIONAL EXPERIENCE:

Research experience:

Research Visit, April 2009

University of Aalborg, Aalborg, Denmark

- Research activity on linear network error-correction and security

Research Assistant (HiWi), March 2006 – December 2008

Department of Mathematics, University of Kaiserslautern, Germany

- Working in the group that develops SINGULAR computer algebra system, developing libraries in C-like SINGULAR language and also C/C++ programming

Research Visit, March 2008

University of Valladolid, Soria, Spain

- Research activity on the generalizations of cyclic error-correcting codes

Research Visit, March 2008

Universitat Rovira i Virgili, Tarragona, Spain

- Research activity on the numerical semigroups: combinatorial methods, computer simulations

Research Visit, April-May 2006

Johann Radon Institute for Computational and Applied Mathematics (RICAM), Linz, Austria

- Research activity connected with the Special Semester on Groebner Bases 2006. Concentration on algebraic cryptanalysis

Teaching experience:**Invited Lecturer**, July 2008

University of Valladolid, Soria, Spain

- Lectures on computer algebra methods in coding theory for the "Soria Summer School on Computational Mathematics: Algebraic Coding Theory"

Instructor, May 2008

University of Kaiserslautern, Kaiserslautern, Germany

- Lectures on verification codes for the high school students within the "Techno Tag" (Day of Technology) organized by the University to promote technical education among high school students

Teaching Assistant (HiWi), November 2007 – February 2008

Department of Mathematics, University of Kaiserslautern, Germany

- Giving example classes and substituting the lecturer for the course "Kryptographie und Codierungstheorie" (Cryptography and Coding theory) in German

Teaching Assistant (HiWi), November 2006 – February 2007

Department of Mathematics, University of Kaiserslautern, Germany

- Administration and assistance for the seminar "Elliptic curve cryptography" (in English and German)

Teaching Assistant (HiWi), November 2005 – February 2006

Department of Mathematics, University of Kaiserslautern, Germany

- Giving example classes and substituting the lecturer for the course "Kryptographie und Codierungstheorie" (Cryptography and Coding theory) in German

Mathematics Tutor, winter 2002 - spring 2002

Academic Skills Department, University of Southern Indiana, Evansville, IN, USA

- Tutoring students who have problems with high school/college mathematics.

Practical experience:**Research Assistant (HiWi)**, March 2009 -June 2009

System Analysis, Prognosis and Control Department, Fraunhofer Institut Techno- and Wirtschaftsmathematik (ITWM) (Institute for Industrial and Financial Mathematics), Kaiserslautern, Germany

- Implementation of algorithms needed for formal verification of digital circuits in C++ using STL

Student assistance supervision, May – June 2007

University of Kaiserslautern, Kaiserslautern, Germany

- Supervising the student assistance in organizing a series of conferences at the Department of Mathematics: Computeralgebra, Algebraic Geometry and Computer Algebra, Summer School on SINGULAR and Applications

Intern, November 2004 - February 2005

Image Processing and Modeling Department, Fraunhofer ITWM, Kaiserslautern, Germany

- Working in a group, which was responsible for MAVI software package (Modular Algorithms for Volume Images), programming in C++

Intern, summer 2003

Document Printing Solutions, Kiev, Ukraine

- Participation in electronic signatures distribution project. Working with technical and legal documentation

Translator, summer 2002 - spring 2004

„Ukrainian Translator“, Kyiv, Ukraine

- Translation of different texts/documentation from English into Russian/Ukrainian and vice versa, with a special emphasis on technical documentation.

Intern, Winter 2002 - Spring 2002

Department of Institutional Research and Assessment, University of Southern Indiana, Evansville, IN, USA

- Statistical analysis of different data with an emphasis on financial data.

PAPERS:

1.) *Bounded distance decoding of linear error-correcting codes with Gröbner bases*. To appear in **Journal of Symbolic Computation**, Special Issue **Gröbner Bases Techniques in Cryptography and Coding Theory**, joint with Ruud Pellikaan, 2010. DOI: 10.1016/j.jsc.2007.12.003

2.) *Attacking AES via Solving Systems in the Key Variables Only*. Proceedings of the **First International Conference on Symbolic Computation and Cryptography**, Beijing, China, April 28-30, pp.118-123, joint with Michael Brickenstein, 2009.

3.) *Decoding linear error-correcting codes up to half the minimum distance with Gröbner bases*. In Sala, M.; Mora, T.; Perret, L.; Sakata, S.; Traverso, C. (Eds.) **Gröbner Bases, Coding, and Cryptography (RISC Book Series, Springer)**, pp.361-365 (2009), joint with Ruud Pellikaan, 2009.

4.) *Decoding and finding the minimum distance with Gröbner bases: history and new insights*. A chapter to appear in the **Selected Topics in Information and Coding Theory**, World Scientific, joint with Ruud Pellikaan, 2009.

5.) *Towards a Better Understanding of the Semigroup Tree*. Accepted to **Semigroup Forum**, joint with Maria Bras-Amoros, 2009.

6.) *Decoding error-correcting codes with Groebner bases*. Proceedings of the **28-th Symposium on Information Theory in the Benelux**, Enschede, The Netherlands, May 24-25, pp.3-10, joint with Ruud Pellikaan, 2007.

7.) *Generalized Hermitian Codes over $GF(2^r)$* , **IEEE Transactions on Information Theory**, vol.52, no.10, pp.4664-4669, 2006.

8.) *Some problems of coding theory and cryptography*, **Master Thesis**, University of Kaiserslautern, 2006.

9.) *On some applications of algebraic function fields to the problems of coding theory*, **Bachelor Thesis**, Kyiv National Shevchenko University, 2004.

10.) *On estimation of one cryptographic function using algebraic geometric codes technique*, **Bulletin of the University of Kiev**, Series: Physics&Mathematics, no.2, pp. 24-28, 2003.

CONFERENCE TALKS, LECTURES, AND PRESENTATIONS

INVITED:

1.) *Complexity issues in decoding linear codes via polynomial systems solving*. **Applications of Computer Algebra**, Hagenberg, Austria, 2008.

2.) *Decoding and finding the minimum distance of codes with Gröbner bases*. A lecture at **Soria School on Computational Mathematics**, Soria, Spain, 2008.

3.) *Algebraic-geometry codes in SINGULAR*. A lecture at **Soria School on Computational Mathematics**, Soria, Spain, 2008.

4.) *Decoding linear codes via systems solving: complexity issues and generalized Newton identities*. **Algebraic seminar of SINGACOM group**, Valladolid, Spain, 2008.

5.) *Decoding Linear Error-correcting Codes with Groebner Bases*. **Seminar on Coding Theory and Cryptography, ENSTA**, Paris, 2006.

6.) *Non-commutative Polly Cracker: Chosen-ciphertext attacks*. **Oberseminar, Ruhr University Bochum**, 2006.

7.) *Generalized Hermitian Codes over $GF(2^r)$* . **Combinatorial Theory Seminar, Eindhoven University of Technology**, Netherlands, 2005.

CONTRIBUTED:

1.) *Symbolic methods in cryptanalysis and coding theory (short overview)*. **Oberseminar Computer Security, Bonn-Aachen International Center for Information Technology**, Bonn, Germany, 2008.

2.) *Obtaining and solving systems of equations in key variables only for the small variants of AES*. **Applications of Computer Algebra**, Hagenberg, Austria, 2008.

4.) *Decoding linear codes via polynomial systems solving. Generalized Newton identities for linear codes*. **Soria School on Computational Mathematics**, Soria, Spain, 2008.

5.) *Attacking AES via Solving Systems in the Key Variables Only*. **The First International Conference on Symbolic Computation and Cryptography**, Beijing, China, 2008.

6.) *Decoding linear codes with Groebner bases. Part II: Experimental results and comparison of methods*. **Workshop on Algebraic Geometry and Coding Theory**, Segovia, Spain, 2007.

7.) *On decoding up to error correcting capacity of linear error-correcting codes with Gröbner bases*. **MEGA Conference "Effective Methods in Algebraic Geometry"**, Strobl, Austria, 2007.

8.) *Decoding linear codes via solving systems of polynomial equations*. **IMA Workshop "Complexity, Coding, and Communications"**, poster session, Minneapolis, MN, USA, 2007.

9.) *Some Problems from Coding Theory and Cryptography*. **Student Conference of the German Mathematical Union (DMV)**, Berlin, Germany, 2007.

10.) *New developments in the theory of Gröbner bases to formal verification, cryptography, and coding theory*. **DASMOD cluster Workshop**, joint presentation with Oliver Wienand, 2007.

11.) *Decoding and finding the minimum distance of error-correcting codes with Groebner bases*. **DIAMANT/EIDMA cluster Symposium**, Vught, Netherlands, 2006.

12.) *Finding Minimum Distance and Decoding Linear Error-correcting Codes with Groebner Bases*. **Special Semester on Groebner Bases**, poster session, Linz, Austria, 2006.

13.) *Non-commutative Polly Cracker: Chosen-ciphertext attacks*. **Special Semester on Groebner Bases**, Linz, Austria, 2006.

14.) *On estimation of one cryptographic function using algebraic geometric codes technique (in Russian)*. **Seminar on Information Security**, Kyiv, Ukraine, 2002.

RESEARCH SUBMITTED AND IN PREPARATION:

1.) *Codes and Cryptography on Algebraic Curves*. A book in progress, to be published by **Cambridge University Press**, joint work with Ruud Pellikaan and Xinwen Wu, 2011.

2.) *Obtaining and solving systems of equations in key variables only for the small variants of AES.*
Submitted to **Mathematics in Computer Science**, special Issue "**Symbolic Computation and Cryptography**", joint with Michael Brickenstein, 2008.

PEER REVIEW ACTIVITY:

- International Workshop on Coding and Cryptography organized by the French National Institute for Research in Computer Science and Control (INRIA), 2007,
- Journal of Symbolic Computation, 2008-2009,
- Institute of Electrical and Electronics Engineers (IEEE) Transactions on Information Theory, 2009.

HONORS, AWARDS, AND CERTIFICATES:

- DASMODO Cluster of Excellence in Rheinland-Palatinate, Research Fellowship, Kaiserslautern, Germany, 2006-2008.
- Best Master thesis, Department of Mathematics, University of Kaiserslautern, Germany, 2006.
- Included in the 25th Annual National Dean's List (USA) for 2001-2002 academic year.
- CRLA (College Reading & Learning Association) Regular Tutoring Certificate, 2002, USA.
- US Department of State Certificate for the successful completion with high honors of the FREEDOM Support Act Undergraduate Program.

REFERENCES:

The following persons can be referenced to for a recommendation on my behalf:

- Prof. Dr. Gert-Martin Greuel, University of Kaiserslautern and Mathematisches Forschungsinstitut Oberwolfach (Mathematical Research Institute at Oberwolfach - Director). Phone (office): +49-631-205-2850, +49-7834-979-52. E-mail: greuel@mathematik.uni-kl.de.
- Prof. Dr. Gerhard Pfister, University of Kaiserslautern. Phone (office): +49-631-205-2336. E-mail: pfister@mathematik.uni-kl.de.
- Dr. Ruud Pellikaan, Eindhoven University of Technology. Phone (office): +31-40-247-42-22. E-mail: g.r.pellikaan@tue.nl.
- Dr. Edgar Martinez-Moro, University of Valladolid. Phone (office): +34 975 129420. E-mail: edgar@maf.uva.es.
- Prof. Dr. Sergiy Ovsienko, Kyiv National Shevchenko University. Email: ovsienko.sergiy@gmail.com