Vladimir Kolesnikov

Bell Laboratories
600 Mountain Ave.
Murray Hill, NJ, 07974, USA

kolesnikov@research.bell-labs.com
www.cs.utoronto.ca/~vlad
Citizenship: Canada

Education:

Ph.D. **University of Toronto**, Canada, July 2006
Supervised by Ian F. Blake and Charles Rackoff
Research: Secure Two-Party Communication and Computation

M.Sc. **Rochester Institute of Technology**, Rochester, NY, USA, Aug 1997
Supervised by Stanislaw Radziszowski
Research: Subset Sum Problem (optimizations of heuristic methods of solving the Subset Sum problem using lattice reduction).

B. Sc. **Rochester Institute of Technology**, Highest honors, Aug 1996

Interests: **Cryptography, communication and network security.**

I am interested in research in secure computation among mistrusting parties (problems such as evaluation of private functions, secure database outsourcing, searchable encryption, computing on encrypted data, etc.) I am also interested in key exchange (method of establishing secure channels over insecure networks), especially based on password or biometric authentication. I worked on security and privacy of key exchange in several practical settings (including standards work – WiMAX), biometric authentication, digital rights management, secure financial transactions (e.g. auctions), and a variety of other subjects.

Other interests include various aspects of network security, distributed computing, general secure multiparty computation, complexity theory and lattice basis reduction algorithms and applications.

Software Eng. Skills: 3 yrs industrial experience. Java, C, C++, Matlab, JDBC.

Service:

- Program Committee Member of INSCRYPT 2007, CANS 2009
- Reviewer for ISIT 2005, Financial Crypto 2006, Eurocrypt 2006, Crypto 2006, BLTJ, PKC 2007, ISC 2007, Eurocrypt 2008, Int'l J. of Applied Cryptography, ISC 2008, CCS 2008, SCN 2008, PKC 2009, TCC 2009, Trans. Inf. Theory, Trans. Networking, Trans. Inf. Sys. Security
- Editor of WiMAX "Server Certificate Profile" and "Device Certificate Profile" standards documents.

Refereed Publications:

- Ian F. Blake and Vladimir Kolesnikov, Strong Conditional Oblivious Transfer and Computing on Intervals. In *Advances of Cryptology – ASIACRYPT 2004*. Springer-Verlag LNCS Vol. 3329. (Acceptance rate 17.3%.)
- Vladimir Kolesnikov, Gate Evaluation Secret Sharing and Secure One-Round Two-Party Computation. In *Advances of Cryptology – ASIACRYPT 2005*. Springer-Verlag LNCS Vol. 3788. (Acceptance rate 15.8%.)
- Vladimir Kolesnikov and Charles Rackoff, Key Exchange Using Passwords and Long Keys. In *Theory of Cryptography Conference 2006*. Springer-Verlag LNCS Vol. 3876.
- Ian F. Blake and Vladimir Kolesnikov, Conditional Encrypted Mapping and Comparing Encrypted Numbers. In *Financial Cryptography and Data Security Conference (FC) 2006*. (Acceptance rate 19.8% for technical papers.)
- Vladimir Kolesnikov and Thomas Schneider, A Practical Universal Circuit Construction and Secure Evaluation of Private Functions. In *Financial Cryptography and Data Security Conference (FC) 2008*. (Acceptance rate 19.1% for technical papers.)
- Vladimir Kolesnikov and Charles Rackoff, Password Mistyping in Two-Factor-Authenticated Key Exchange. In *International Colloquium on Automata, Languages and Programming (ICALP) 2008*.
- Vladimir Kolesnikov and Thomas Schneider, Improved Garbled Circuit: Free XOR Gates and Applications. In *International Colloquium on Automata, Languages and Programming (ICALP) 2008*.
- Ian F. Blake and Vladimir Kolesnikov, One-round secure comparison of integers. In *Journal of Applied Cryptography*, Volume 3, Issue 1 (May 2009).
- Vladimir Kolesnikov, Advances and Impact of Secure Function Evaluation, In *Bell Labs Technical Journal (BLTJ)*, Fall 2009
- Juan Garay, Vladimir Kolesnikov and Rae McLellan, MAC Precomputation with Applications to Secure Memory, In *Information Security Conference (ISC) 2009*.
- Mauro Barni, Pierluigi Failla, Vladimir Kolesnikov, Riccardo Lazzeretti, Ahmad-Reza Sadeghi and Thomas Schneider, Secure Evaluation of Private Linear Branching Programs with Medical Applications. In *European Symposium on Research in Computer Security (ESORICS) 2009*.
- Vladimir Kolesnikov, Ahmad-Reza Sadeghi and Thomas Schneider, Improved Garbled Circuit Building Blocks and Applications to Auctions and Computing Minima. In *Computer and Network Security (CANS) 2009*.
- Shlomi Dolev, Juan Garay, Niv Gilboa and Vladimir Kolesnikov, Swarming Secrets. *In 47th Annual Allerton Conference*, 2009
- Mauro Barni, Pierluigi Failla, Vladimir Kolesnikov, Riccardo Lazzeretti, Annika Paus, Ahmad-Reza Sadeghi, and Thomas Schneider. Efficient privacy-preserving classification of ECG signals. In *1st IEEE International Workshop on Information Forensics and Security (IEEE WIFS)*, 2009.

Workshop Contributions:

- Juan Garay, Vladimir Kolesnikov and Rae McLellan, Efficient Techniques for Securing Off-Chip Memory. In *Computer & Electronics Security Applications Rendez-vous (C&ESAR)*, 2008.
- Vladimir Kolesnikov, Ahmad-Reza Sadeghi and Thomas Schneider, How to Combine Homomorphic Encryption and Garbled Circuits: Improved Circuits and Computing the Minimum Distance Efficiently. In *The International Workshop on Signal Processing in the Encrypted Domain (SPEED 2009)*
- Mauro Barni, Pierluigi Failla, Vladimir Kolesnikov, Riccardo Lazzeretti, Ahmad-Reza Sadeghi, and Thomas Schneider, Combining Signal Processing and Cryptographic Protocol Design for Efficient ECG Classification. In *The International Workshop on Signal Processing in the Encrypted Domain (SPEED 2009)*

Work in Submission:

-

Work in Progress:

- Vladimir Kolesnikov and Thomas Schneider, Practical SFE.

Patents:

- A Method for Delegation of Authentication State in SSL/TLS, Patent application with Peter Bosch and Sape Mullender, Alcatel-Lucent Bell Labs, 2009
- A Method of Efficient Secure Function Evaluation Using Resettable Tamper-Resistant Hardware Tokens, Patent application, Alcatel-Lucent Bell Labs, 2009
- A Method To Implement Secure Virtual Machines, Patent application with Peter Bosch, Sape Mullender, Jim Mckie, Philippe Dobbelaere, Rae McLellan, Patent application, Alcatel-Lucent Bell Labs, 2009
- Efficient Techniques For Achieving Security Against Cheating Tamper-Resistant Tokens, Patent application, Alcatel-Lucent Bell Labs, 2009
- Improved Computation Of Garbled Tables In Garbled Circuit. Patent application, Alcatel-Lucent Bell Labs, 2009
- Efficient Key Management System and Method. Patent application with Vijay Gurbani, Alcatel-Lucent Bell Labs, 2009
- Password Mistyping in Two-Factor-Authenticated Key Exchange. Patent application, Alcatel-Lucent Bell Labs, 2007
- Message Authentication Code Pre-computation With Applications to Secure Memory. Patent application, with Juan Garay and Rae McLellan, Alcatel-Lucent Bell Labs, 2008
- Improved Garbled Circuit. Patent application, with Thomas Schneider, Alcatel-Lucent Bell Labs, 2008

- A Practical Universal Circuit Construction and Secure Evaluation of Private Functions. Patent application, with Thomas Schneider, Alcatel-Lucent Bell Labs, 2007
- Storage Area Network (SAN) Security Appliance. Patent, with Dr. Kumar Murty and Daniel Thanos, Kasten Chase, Inc., 2001

Technical Reports:

- A number of reports in support of WiMAX effort in Sprint Nextel and in Alcatel-Lucent Wireless Business Unit, 2007
- Biometric Key Binding. Technical report sponsored by Bioscrypt, Inc. and Canadian National Research Council's Industrial Research Assistance Program (NRC-IRAP). With Omid Jahromi, Rene McIver, Colin Soutar and Alex Stoianov, 2005
- Binding Strong Keys to Fingerprints Securely and Privately. Technical Report, Bioscrypt, Inc., 2005
- Efficient Storage Security. Technical Report, Kasten Chase, Inc., 2001
- Efficient Broadcast Encryption. Technical Report, Kasten Chase, Inc., 2001

Student Supervision:

- Thomas Schneider. Supervised his diploma thesis, a finalist in German computer science thesis competition (*Informatiktage*). Joint work accepted to Financial Cryptography 2008, and ICALP 2008.
  - Continuing collaboration while he works on Ph.D. at Ruhr-Universität Bochum.

Standards Work:

- *WiMAX security and authentication.* One of three or four WiMAX Forum's PKI security experts. Actively participated in WiMAX Forum's effort in standardizing use of certificates in authentication devices and subscribers. Lead meetings, edited standards documents. Responsible for technical aspects of WiMAX authentication solutions of Alcatel-Lucent and Sprint Nextel. Represented Alcatel-Lucent and Sprint Nextel in standards meetings. Wrote a number of technical reports influencing and supporting standards decisions. June 2007-present.

Industrial Research Experience:

Jul 2006-present	**Member of Technical Staff**. Bell Labs, Murray Hill, NJ, USA Performing research on secure multiparty computation and key exchange and supervising student research. Consulting for business units and external customers with BU and external funding. Participating in standards work (WiMAX).
Aug 2004-Mar 2005	**Researcher**. Bioscrypt Inc., Toronto, ON, Canada Researched security requirements and techniques for systems that use fingerprints as cryptographic keys. Worked on extracting uniform

(strong) randomness from weakly-random strings (fingerprint images). Analyzed the trade off between resulting key length and the unpredictability of its individual bits.

Apr 2001-Oct 2001 **Researcher**. Karthika, Inc./Kasten Chase, Toronto, Canada
Researched security of data storage and access control in Storage Area Networks (SAN). Solutions built on secret sharing techniques. My work became a basis for a patent and a large part of the company's product offering (Assurency: SecureData).

Industry Experience:

Oct 1999-Sept 2000 **Software Engineer**. Algorithmics Inc., Toronto, ON, Canada
Worked on data warehousing for financial risk management tools. Developed in-house JDBC-compliant database, with data strucutres designed for efficiency of application-specific queries. Java, JDBC.

May 1997-Sept 1999 **Software Engineer**. The MathWorks Inc., Natick, MA
Worked on Stateflow, a state machine visual programming tool for MATLAB. Developed automated report generator of (arbitrarily large) machines, which produces cross-linked PS, PDF, XML documents suitable for printing in Letter, A4 formats. C, C++, MATLAB.

Teaching Experience:

Sept 1995-May 1997, Sept 2000-May 2006 **Teaching assistant** for graduate and undergraduate courses at University of Toronto and Rochester Institute of Technology. (Cryptography, algorithms, data structures, software engineering, operating systems, algebra, calculus, etc.)

Invited Talks

- *Strong Conditional Oblivious Transfer and Computing on Intervals*, Theory Canal: The Rochester Theory Seminar Series, University of Rochester, March 2005
- *How to tell which of the encrypted numbers is greater*, Workshop on Cryptography: Underlying Mathematics, Provability and Foundations, Fields Institute, Toronto, Canada, November 27-December 1, 2006
- *Password Mistyping in Two-Factor-Authenticated Key Exchange*, iCIS Seminar, University of Calgary, Canada, August 2007

Conference Presentations and Seminar Talks:

- *MAC with Precomputation and Applications to Secure Memory*,
presented at C&ESAR Workshop 2008 (Rennes, France) and HGI Institute, Ruhr-Universität Bochum, Germany, 2008

- *Password Mistyping in Two-Factor-Authenticated Key Exchange*,
  presented at ICALP 2008 and IBM seminar and NYU seminar, 2007
- *Key Exchange Using Passwords and Long Keys*
  presented at the third Theory of Cryptography Conference (TCC), Concordia Univeristy, Bell Labs, Mar-Apr 2006
- *Conditional Encrypted Mapping and Comparing Encrypted Numbers*
  presented at the Financial Cryptography Conference (FC), Rochester Institute of Technology, HP Labs, NYU 2006-2007
- *Gate Evaluation Secret Sharing and Secure One-Round Two-Party Computation*
  presented at ASIACRYPT 2005, University of Waterloo, Ecole Normale Superieure (Paris), Nov-Dec 2005
- *Strong Conditional Oblivious Transfer and Computing on Intervals*
  presented at ASIACRYPT 2004, Simon Fraser University and Rochester Institute of Technology. Dec 2004-Mar 2005
- *Electronic Cash Systems*. Presented at Rochester Institute of Technology, Dec 2001
- *Secure Multiparty Computation and Applications*
  series of talks at Grodno University on subjects such as general secure two- and multiparty computation, electronic cash and biometric authentication, May 2003, 2004, 2005

Selected Awards:

- *Ontario Graduate Scholarship (OGS).* Canadian provincial award, CAD 15,000/yr. 2001-2002 (declined), 2004-2005
- *Medal for Service to the Faculty of Mathematics*, Grodno State University, 2003
- *NSERC (Natural Sciences and Engineering Research Council of Canada) Postgraduate Scholarship PGS B.* Canadian national award, CAD 21,000/yr, 2001-2003
- *Boston University Presidential University Graduate Fellowship.* (Only two awarded for the department of computer science). USD 35,000. 1998-99
- *RIT Graduate teaching assistantship.* (Only two awarded for department of computer science). USD 25,000. 1996-97
- *United States Information Agency (USIA) scholarship for one year of undergraduate study in the USA.* (One of only eight recipients from Belarus.) USD 30,000. 1995-96
- *George Soros' Academic Scholarship.* International award for excellence in studies. USD 1000. 1995-96 (declined)
- A variety of national, regional and institutional awards for olympiads in computer science and math and excellence in studies, Belarus, 1989-94

Languages: English, Russian, Belorussian, Polish, Ukrainian, basic Romanian

References are available upon request.