CURRICULUM VITAE

Personal Information

- NAME: Alexandre V. Evfimievski
- DATE OF BIRTH: February 1977
- E-MAIL: (given by request) HOMEPAGE: `http://www.cs.cornell.edu/aevf/`
- PHONE: (607) 255-9730, FAX: (607) 255-4428
- ADDRESS: 5136 Upson Hall, Department of Computer Science, Cornell University, Ithaca, NY 14853-7501, USA.

Education

- Expected Degree of Ph. D. in Computer Science — Aug 2004
- Degree of Master of Science in Computer Science, Cornell University, USA — 2003
- Ph. D. Graduate student in Computer Science, Cornell University, USA — 1998–2004
  Scientific advisor: Prof. Johannes Gehrke
- Graduate Student in Mathematics (not completed) — 1997–98
  Faculty of Mathematics and Mechanics, Moscow State University, Russia
- Graduation in Mathematics, with excellence — 1992–97
  Faculty of Mathematics and Mechanics, Moscow State University, Russia
  Scientific advisor: Prof. Nikolai K. Vereshchagin

Awards

Graduation with excellence in mathematics (1997), Petrovsky fellowship (fall 1995 – spring 1997), George Soros fellowship ("Soros student") (fall 1994 – spring 1995)

Work Experience

Summer internships at IBM Almaden Research Center in Summer 2001 and Summer 2002, under the supervision of Dr. Ramakrishnan Srikant (mentor) and Dr. Rakesh Agrawal (manager). Conducted research in privacy preserving mining of association rules (Summer 2001) and sovereign information integration (Summer 2002).

Publications

[1] Alexandre Evfimievski, Ramakrishnan Srikant, Rakesh Agrawal, and Johannes Gehrke. Privacy preserving mining of association rules. In *Proceedings of the 8th ACM SIGKDD International Conference on Knowledge Discovery in Databases and Data Mining*, pages 217–228, Edmonton, Alberta, Canada, July 23–26 2002.

[2] Alexandre Evfimievski, Ramakrishnan Srikant, Rakesh Agrawal, and Johannes Gehrke. Privacy preserving mining of association rules (invited journal version). *Information Systems*, 29(4):343–364, June 2004.

[3] Alexandre Evfimievski. Randomization in privacy-preserving data mining. *SIGKDD Explorations: Newsletter of the ACM Special Interest Group on Knowledge Discovery and Data Mining*, 4(2):43–48, December 2002.

[4] Rakesh Agrawal, Alexandre Evfimievski, and Ramakrishnan Srikant. Information sharing across private databases. In *Proceedings of the ACM SIGMOD International Conference on Management of Data*, pages 86–97, San Diego, California, USA, June 9–12 2003.

[5] Alexandre Evfimievski, Johannes Gehrke, and Ramakrishnan Srikant. Limiting privacy breaches in privacy preserving data mining. In *Proceedings of the 22-nd ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems*, pages 211–222, San Diego, California, USA, June 9–11 2003.

[6] Alexandre Evfimievski. A probabilistic algorithm for updating files over a communication link. In *Proceedings of the 9-th Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 300–305, San Francisco, California, USA, January 25–27 1998.

Paper in Preparation

[7] Alexandre Evfimievski, Johannes Gehrke, Ramakrishnan Srikant, and Rakesh Agrawal. Privacy preserving join sizes using sketches.

U.S. Patent Applications

- Rakesh Agrawal, Alexandre Evfimievski, and Ramakrishnan Srikant. Method for Privacy Preserving Mining of Association Rules. Filed July 2003
- Rakesh Agrawal, Alexandre Evfimievski, and Ramakrishnan Srikant. Method for Information Sharing Across Private Databases. Filed June 2003

Research

Most of my research so far has been in the field of privacy preserving information sharing, in the following three directions:

Privacy Preserving Mining of Association Rules: We gave a framework for preserving privacy of individual transactions residing at numerous clients while permitting the central server to find association rules. We defined a class of randomization operators that are effective at limiting privacy breaches. Formulae were derived to estimate support and confidence of associations from randomized data, together with their uncertainty. Performance and privacy were tested on real-life data [1, 2].

Sovereign Information Integration: We used secure multiparty computation techniques such as commutative encryption to efficiently evaluate intersections and joins over relational tables residing at two different servers, without compromising the privacy of data records [4]. Our protocols were shown to be significantly more efficient than the generic approach. In an ongoing work, we combined cryptography, sketches, and randomization into a join size privacy preserving protocol with sublinear communication and encryption cost [7].

A Statistical Approach To Privacy: We developed a statistical methodology for preserving privacy, and applied it in situations where traditional "computation hardness" approach is not efficient. The new methodology is intended to limit privacy breaches while performing multiparty computation; a privacy breach occurs when an adversary's belief (in statistical sense) for a certain privacy-sensitive question is significantly affected by the information disclosed during computation. We used it to evaluate privacy in algorithms based on pseudorandom generators [5] and sketches [7].

This work has been joint with and under the supervision of Prof. Johannes Gehrke, Dr. Ramakrishnan Srikant, and Dr. Rakesh Agrawal. Besides it, I also worked on an algorithm for learning hidden variables over Boolean-vector data streams, and on an algorithm for updating files over a communication link with logarithmic communication complexity [6].

Teaching

Teaching Assistant for the following courses at Cornell University:

- CS 632 "Advanced Database Systems" — Spring 2002
- CS 632 "Advanced Database Systems" — Spring 2001
- CS 280 "Discrete Structures" — Spring 2000
- CS 381 "Introduction to Theory of Computing" — Fall 1999
- CS 482 "Introduction to Analysis of Algorithms" — Spring 1999
- CS 280 "Discrete Structures" — Fall 1998

References

Prof. Johannes Gehrke
4105B Upson Hall, Dept. of Computer Science,
Cornell University, Ithaca, NY 14853, USA
Phone: (607) 255-1045, Fax: (607) 255-4428
E-mail: (given by request)
http://www.cs.cornell.edu/johannes/

Prof. Jayavel Shanmugasundaram
4105A Upson Hall, Dept. of Computer Science,
Cornell University, Ithaca, NY 14853, USA
Phone: (607) 255-4117, Fax: (607) 255-4428
E-mail: (given by request)
http://www.cs.cornell.edu/People/jai/

Dr. Ramakrishnan Srikant
IBM Almaden Research Center, K55/B1,
650 Harry Road, San Jose, CA 95120, USA
Phone: (408) 927-1774, Fax: (408) 927-3215
E-mail: (given by request)
http://www.almaden.ibm.com/cs/people/srikant/