

Alexander Iliev

Dartmouth College
6211 Sudikoff Lab
Hanover, NH 03755
USA

603-646-9179
sasho@cs.dartmouth.edu
www.cs.dartmouth.edu/~sasho/
USA

Objective	A position in the Information Security field, researching, designing and implementing solutions to challenging problems.		
Education	<i>2001–2006</i>	<i>Dartmouth College</i>	<i>Hanover, NH</i>
	<ul style="list-style-type: none">• PhD program in Computer Science, expected graduation in Fall 2006.• Adviser: Prof. Sean Smith.• Thesis: <i>Using Tiny Trusted Third Parties to Enhance Secure Two-Party Computations.</i> Examines how two adversarial participants can compute a function on their private data so that no information about each participant's data is revealed to the other (or anyone else). We are targeting larger functions on larger data (eg. graph search) than earlier works, and to this end employ a physically secure computer (like the IBM 4758 secure coprocessor) as a trusted device. The main challenge stems from the fact that such devices have very small protected memory, and thus need to use external (untrusted) resources, without leaking information.		
	<i>1997–2001</i>	<i>Dartmouth College</i>	<i>Hanover, NH</i>
	<ul style="list-style-type: none">• B.A., Computer Science major, Engineering Sciences minor.• Thesis: <i>An Armored Data Vault</i>, adviser Prof. Sean Smith.		
Research Interests	Network and systems security, hardware-based security and acceleration, secure multiparty computation, privacy and anonymity, secure virtualization, functional programming, domain-specific languages.		
Selected Work Experience	<i>Jun-Dec 2004</i>	<i>Intel Corp., Trusted Platforms group</i>	<i>Hillsboro, OR</i>
	Security Architecture and Implementation Intern <ul style="list-style-type: none">• Worked on the design of the security architecture for the LaGrande Technology (LT) platform, including the Trusted Platform Module (TPM) version 1.2.• Worked on an implementation of the Trusted Computing Group (TCG) stack.• Designed an application of the LT platform for secure co-processing.		
	<i>2002–present</i>	<i>Dartmouth PKI Lab</i>	<i>Hanover, NH</i>
	Research Assistant <ul style="list-style-type: none">• <i>Hardware-assisted Secure Computation:</i> Designed and implemented a compiler and runtime to perform execution of general programs on the 4758 secure coprocessor, using very little trusted RAM and without leaking information outside the secure coprocessor.• <i>Private Directory:</i> Developed an LDAP directory offering Private Information Retrieval (PIR) of X.509 certificates, using the IBM 4758 Secure Coprocessor.		
	<i>2001–2002</i>	<i>Dartmouth CS Department</i>	<i>Hanover, NH</i>
	Teaching Assistant <ul style="list-style-type: none">• Algorithms: CS 25, with Prof. Javed Aslam.• Computer Networks: CS 78, with Prof. David Kotz.• Concepts in Computing: CS 4, with Prof. Tom O'Connell.		

	<hr/> <p><i>Jun–Sep 2000</i> <i>Microsoft Corp., PocketPC group</i> <i>Redmond, WA</i></p> <p>Software Design Engineer in Test</p> <ul style="list-style-type: none"> • Investigated and implemented software complexity measurements. • Implemented an instrumentation system for the Pocket PC, in C++. <hr/>
	<p><i>Jun 1998–Oct 1999</i> <i>Mobile Agents Research Group</i> <i>Hanover, NH</i></p> <p>Programmer (part time)</p> <ul style="list-style-type: none"> • Designed and implemented a graphical tracking system for mobile agents, using Tcl/Tk. • Implemented a Persistent Query Service for mobile agents, using Java and interfacing to a document-clustering library written in C++. <hr/>
Publications	<ul style="list-style-type: none"> • Alexander Iliev and Sean Smith, “Protecting Client Privacy with Trusted Computing at the Server: Two Case Studies”, <i>IEEE Security and Privacy Magazine</i>, Vol. 3 No. 2, pages 20-28, March 2005. • Alexander Iliev and Sean Smith, “More Efficient Secure Function Evaluation Using Tiny Trusted Third Parties”, <i>Dartmouth College CS Technical Report 2005-551</i>, July 2005. • Alexander Iliev and Sean Smith, “Towards Tiny Trusted Third Parties”, <i>Dartmouth College CS Technical Report 2005-547</i>, July 2005. • Alexander Iliev and Sean Smith, “Private Information Storage with Logarithmic-space Secure Hardware”, <i>I-NetSec04: 3rd Working Conference on Privacy and Anonymity in Networked and Distributed Systems</i>, Aug 2004. • Alex Iliev and S.W. Smith, “Privacy-Enhanced Directory Services.” <i>PKI Research Workshop 2003</i>. April 2003. • Alex Iliev and S.W. Smith, “Prototyping an Armored Data Vault: Rights Management on Big Brother’s Computer.” <i>Privacy Enhancing Technologies 2002</i>. April 2002. Springer-Verlag LNCS 2482. <hr/>
Computer Experience	<ul style="list-style-type: none"> • Platforms: Linux/Unix, Windows NT/2000/XP. • Programming languages: C/C++, Haskell, Java, Perl, Tcl/Tk, HTML, Javascript, ML, some Lisp/Scheme. • Toolkits: NSS, OpenSSL. • Other: XML/XSLT, DOM, RPC/XDR. <hr/>
Languages	<p>English, native Bulgarian, good German, basic French and Polish.</p> <hr/>