Valerio Pastro

Postdoctoral Researcher · Yale University

(646) 932-8727
valerio.pastro@yale.edu
www.cs.yale.edu/homes/pastro-valerio

AKW 402
51 Prospect Street
New Haven, CT 06511-8937

Areas of expertise

- **Cryptography**, encompassing: computing on encrypted data, verifiable cloud computation, statistical applications, secure distributed storage, secure protocols.
- **Mathematics**, including: applied probability, statistical estimation, elliptic curves, numerical analysis.

Employment

- **Postdoctoral researcher** 2016–Now
  Yale University, Connecticut
  Computer Science Department, Cryptography group
  Mentor: Prof. Mariana Raykova
  - (Ongoing) *Construction of witness encryption from minimal assumptions*
  - (Ongoing) *Implementation of a practical multiparty computation protocol with minimal computation costs*
  - (Ongoing) *Implementation of distributed linear regression over vertically partitioned databases*
  - *Designed and implemented a system for private data aggregation on a distributed database (join work with snips.ai) [1]*
- **Postdoctoral researcher** 2014–2016
  Columbia University, New York
  Computer Science Department, Cryptography group
  Mentor: Prof. Allison Bishop
  - *Designed a robust and privacy-preserving distributed storage scheme, secure against local attacks [4]*
  - *Constructed a provably optimal secret-sharing scheme supporting maximal corruptions [3]*
  - *Constructed a simplified framework for garbling schemes (a specific type of program obfuscation) [2]*
- **Postdoctoral researcher** 2013–2014
  The City University of New York
  Computer Science Department, Cryptography group
  Mentor: Prof. Rosario Gennaro
  - *Designed a framework for general secure cloud computation on encrypted data*
  - *Constructed a secure cloud computation service for statistical functions over encrypted data.*
  - *Prototype implementation of the above, coded in C [5]*

Education

- **PhD in Computer Science** 2010–2013
  Aarhus University, Denmark
  Advisor: Prof. Ivan Damgård (Co-advisor: Prof. Ronald Cramer)
  Thesis: **Zero Knowledge Protocols and Multiparty Computation**
  - *A series of fast distributed protocols to compute any function, guaranteeing privacy of inputs, even where all but one players are corrupted [7, 6]*

– *A provably optimal zero-knowledge protocol for multiplicative relations [8]*

- **Master's in Mathematics** (full marks) 2008–2010
  Leiden University, The Netherlands
  Advisor: Dr. Cecilia Salgado
  Thesis: **Construction of Rational Elliptic Surfaces of Mordell-Weil Rank Four**

- **Bachelor's in Mathematics** (full marks) 2005–2008
  Padova University, Italy
  Advisor: Dr. Maurizio Cailotto
  Thesis: **On the Projective Classification of Complex Plane Quartics**

Papers

1. Morten Dahl, Valerio Pastro, Mathieu Poumeyrol. Private Data Aggregation on a Budget. *PMPML NIPS Workshop*, 2016.

2. Tal Malkin, Valerio Pastro, Abhi Shelat. An Algebraic Approach to Garbling. *Manuscript*.

3. Allison Bishop, Valerio Pastro, Rajmohan Rajaraman, Daniel Wichs. Essentially Optimal Robust Secret Sharing with Maximal Corruptions. *Advances in Cryptology - EUROCRYPT*, 2016.

4. Allison Bishop, Valerio Pastro. Robust Secret Sharing Schemes Against Local Adversaries. *Public-Key Cryptography - PKC*, 2016.

5. Dario Fiore, Rosario Gennaro, and Valerio Pastro. Efficiently Verifiable Computation on Encrypted Data. *ACM SIGSAC Conference on Computer and Communications Security*, 2014.

6. Ivan Damgård, Marcel Keller, Enrique Larraia, Valerio Pastro, Peter Scholl, and Nigel P. Smart. Practical Covertly Secure MPC for Dishonest Majority – or: Breaking the SPDZ Limits. *Computer Security - ESORICS*, 2013 (**Best paper award**).

7. Ivan Damgård, Nigel P. Smart, Valerio Pastro, and Sarah Zakarias. Multiparty Computation from Somewhat Homomorphic Encryption. *Advances in Cryptology - CRYPTO*, 2012.

8. Ronald Cramer, Ivan Damgård, and Valerio Pastro. On the Amortized Complexity of Zero Knowledge Protocols for Multiplicative Relations. *Information Theoretic Security - ICITS*, 2012.

9. Valerio Pastro. Construction of Rational Elliptic Surfaces of Mordell-Weil Rank Four. *Commentarii Mathematici Univerisitatis Sancti Pauli*, vol. 61, no. 1, 2012.

Selected Talks

- Essentially Optimal Robust Secret Sharing with Maximal Corruptions [3]
  Theory of Computation seminar, MIT, Massachusetts [link] 2016
  Theory seminar, John Hopkins University, Maryland [link] 2016
  NYC Cryptoday, Columbia University, New York [link] 2016

- An Algebraic Approach to Garbling [2]
  Cryptography Summer Program at the Simons Institute for the Theory of Computing,
  UC Berkeley, California [link] 2015

- Robust Secret Sharing Schemes Against Local Adversaries [4]
  DIMACS Workshop on Coding-Theoretic Methods for Network Security,
  Rutgers University, New Jersey [link] 2015

- Efficiently Verifiable Computation on Encrypted Data [5]
  Cryptography seminar, New York University, New York 2013

- On Multiparty Computation [6, 7]
  Cryptography seminar, New York University, New York 2013
- Multiparty Computation from Somewhat Homomorphic Encryption [7]
  Crypto seminar, IBM Research, New York 2013
  BUSec Security seminar, Boston University, Massachusetts 2013
- Construction of Rational Elliptic Surfaces of Mordell-Weil Rank Four [9]
  Arithmetic aspects of elliptic surfaces at the Hausdorff Institute for Mathematics, University of Bonn, Germany [link] 2010

Professional Service

- **Program Committee Member**: *Theory of Cryptography - TCC* 2016
- **Referee**:
  - *Journal of Cryptology - JoC* 2016, 2015, 2014
  - *Symposium on Theory of Computing - STOC* 2016
  - *Advances in Cryptology - EUROCRYPT* 2016
  - *Theory of Cryptography - TCC* 2016
  - *Advances in Cryptology - CRYPTO* 2014, 2013, 2011
  - *Automata, Languages, and Programming - ICALP* 2014
  - *Innovations in Theoretical Computer Science - ITCS* 2013
  - *Provable Security - PROVSEC* 2011
  - *Public-Key Cryptography - PKC* 2011

Awards

- **Computer Security - ESORICS Best Paper Award** 2013
  Best paper award for "Practical Covertly Secure MPC for Dishonest Majority – or: Breaking the SPDZ Limits" [6]
- **AlGaNT-Erasmus Fellowship** 2008–2010
  Qualified to an honors master's program for distinguished students (25 worldwide) run by Padova and Leiden University
- **INdAM Scholarship (Italian Institute for High Mathematics)** 2005–2007
  Won the scholarship for outstanding performance on a series of nationwide tests

Computer Skills

- **Programming** (best language first): C, C++, Python, R
- **Applications**: SQL, Mathematica, Matlab, Latex, Microsoft Office
- **Operating systems**: Linux, OS X, Windows

Teaching

- **Optimization** (teaching assistant) 2012
- **Regularity and Automata** (teaching assistant) 2012, 2011
- **Elliptic Curves Seminar Series** (instructor) 2011
- **Computability and Logic** (teaching assistant) 2011

Language Skills

English (fluent), Italian (native), Danish (intermediate), French (basic), Portuguese (basic)