

Brendstrupgårdsvej 9C, st. 8  
8200 Aarhus N  
☎ +45 23695300  
✉ [robtrifiletti@gmail.com](mailto:robtrifiletti@gmail.com)  
🌐 [www.robtrifiletti.com](http://www.robtrifiletti.com)  
📄 [robtrifiletti](#)  
📍 [robtrifiletti](#)  
Nationality: Danish



# Roberto Trifiletti

Computer Scientist, PhD (Cryptography)

*Passionate about software, security and solutions – team player  
with ambition and the personal drive to back it up.*

## Resume

I'm a PhD student at Aarhus University working on cryptographic protocols, with emphasis on developing more efficient solutions for secure distributed computing. Dedication and determination drives my work forward, fueled by the interdisciplinary mix of my favorite computer science topics that constitute cryptography such as *network security, distributed systems and cloud, algorithm design/engineering*, and *mathematics*. Looking forward as I finish my PhD, I am eager to pursue new challenges in the industry applying my competencies to real-world problems.

### Areas of Expertise

- Cryptography and Protocols.
- High-Performance Computing.
- Distributed Systems.
- Rigorous Problem Solving.

### Technical Skills

- C++ and Java.
- Continuous Integration and TDD.
- Cloud Architecture.
- Strong Writing Skills.

## Work Experience

2013 – 2017 **Doctor of Philosophy (PhD)**, *Cryptography*, Aarhus University.

Experience in developing, verifying and implementing advanced cryptographic protocols for secure distributed computing. Throughout my research project I have had experience with

- Applying complex theoretical solutions to practice.
- Exploring practical trade-offs between computing resources: Compute vs Network vs Storage.
- Disseminating complex problems and solutions to uninitiated audiences.
- Successfully collaborating with international colleagues spread across timezones and cultures.
- Continuously managing and developing complex research projects with minimal supervision.
- Co-supervising a Master's thesis project on secure distributed poker.

2012 – 2013 **Student Programmer**, *Cryptography and Security Research Group*, Aarhus University.

Working on various projects with PhD students and Professors of the group. The project, FairplayCircuitTools (see below), was developed in this period.

## Software Projects

- 2017 **DUPLO**, *Continuation of the TinyLEGO project, 8-10x overall improvement (C++)*.
- 2017 **SplitCommit**, *XOR-homomorphic Commitment Scheme (C++)*.
- 2016 **TinyLEGO**, *Secure Computation Protocol based on Garbled Circuits (C++)*.
- 2013 **FairplayCircuitTools**, *Tools for Manipulating Boolean Circuits (Java)*.
- 2012 **Pairwise Alignment of DNA Sequences with CUDA**, *Course Project (CUDA C)*.

## Extracurricular Activity

- 2017 [Cloud Systems and Infrastructure](#)
- 2017 [Cloud Computing Concepts, Part 1](#)
- 2016 [Continuous Delivery Academy](#)
- 2012 [Cryptography I](#)
- 2017 [Big Data and Applications in the Cloud](#)
- 2017 [Cloud Computing Concepts, Part 2](#)
- 2016 [Learning from Data](#)

---

## Software Technologies

Development C/C++, Java, CUDA, Python.

Libraries ZMQ, Google Test, jUnit, OpenSSL, GMP.

Tools git, Docker, Jenkins, SVN, CMake, Eclipse.

Misc Amazon Web Services, L<sup>A</sup>T<sub>E</sub>X, SQL, HTTP, HTML/CSS/XML, JSON.

---

## Education

2013 – 2017 **Doctor of Philosophy (PhD)**, *Computer Science (Cryptography)*, Aarhus University.

2012 – 2015 **Master of Science (MSc)**, *Computer Science*, Aarhus University.

2009 – 2012 **Bachelor of Science (BSc)**, *Computer Science*, Aarhus University.

---

## Other Experience

2012 – 2017 **Teaching Assistant**, *Department of Computer Science, Aarhus University*.

Taught several installations of the following courses: Introduction to Programming, Security and Perspectives in Computer Science.

2011 – 2012 **Team Leader**, *Studentarhus Aarhus*.

In charge of social events such as concerts and stand-up comedy shows often attracting several hundred guests.

2010 – 2012 **Tutor**, *Mat/Fys Tutorforening*, Aarhus University.

Took part in organizing the arrival of and introducing new students to the Science and Technology faculty during my early years at university.

---

## Spoken Languages

**Danish** Native

**English** Professional

**Swedish** Professional

**Spanish** Intermediate

---

## Personal

I spend my free time with my family, enjoying everything the Aarhus area has to offer. I recharge with movies/series, board-games or exercise.

---

## Publications

- [RT17] Peter Rindal and Roberto Trifiletti. SplitCommit: Implementing and Analyzing Homomorphic UC Commitments. Cryptology ePrint Archive, Report 2017/407, 2017. <https://eprint.iacr.org/2017/407>.
- [KNR<sup>+</sup>17] Vladimir Kolesnikov, Jesper Buus Nielsen, Mike Rosulek, Ni Trieu, and Roberto Trifiletti. DUPLO: Unifying Cut-and-Choose for Garbled Circuits. Cryptology ePrint Archive, Report 2017/344, 2017. <https://eprint.iacr.org/2017/344.pdf>.
- [NST17] Jesper Buus Nielsen, Thomas Schneider, and Roberto Trifiletti. Constant Round Maliciously Secure 2PC with Function-independent Preprocessing using LEGO. In Ari Jules and Patrick Traynor, editors, *Network and Distributed System Security Symposium (NDSS)*, 2017. <https://eprint.iacr.org/2016/1069.pdf>.
- [FJNT16] Tore Kasper Frederiksen, Thomas P. Jakobsen, Jesper Buus Nielsen, and Roberto Trifiletti. On the Complexity of Additively Homomorphic UC Commitments. In Eyal Kushilevitz and Tal Malkin, editors, *Theory of Cryptography (TCC-A)*, 2016. <https://eprint.iacr.org/2015/694.pdf>.
- [FJNT15] Tore Kasper Frederiksen, Thomas P. Jakobsen, Jesper Buus Nielsen, and Roberto Trifiletti. TinyLEGO: An Interactive Garbling Scheme for Maliciously Secure Two-Party Computation. Cryptology ePrint Archive, Report 2015/309, 2015. <https://eprint.iacr.org/2015/309.pdf>.
- [CDD<sup>+</sup>15] Ignacio Cascudo, Ivan Damgård, Bernardo Machado David, Irene Giacomelli, Jesper Buus Nielsen, and Roberto Trifiletti. Additively Homomorphic UC Commitments with Optimal Amortized Overhead. In Jonathan Katz, editor, *Public-Key Cryptography (PKC)*, 2015. <https://eprint.iacr.org/2014/829.pdf>.