Luca Melis

Curriculum Vitae

Computer Science Dept,
University College London
Gower Street, London WC1E 6BT
✉ *luca.melis.14@ucl.ac.uk*
🖱 *http://lucamelis.github.io*

Personal Details

Residence	London	Country	United Kingdom

Education

July 2006 **High School's degree in accountability and computer programmer**, *Istituto tecnico commerciale "A. Maxia" Aritzo*, Italy, mark 100/100.

April 2010 **Bachelor's Degree in Computer Engineering**, *University of Florence*, mark 110/110 cum laude.

April 2013 **Master's Degree in Computer Engineering**, *University of Florence*, mark 110/110 cum laude and honorable mention.

April 2013 **Master's Degree in Computer Engineering**, *University of Florence*, mark 110/110 cum laude and honorable mention.

September 2014–Present **PhD in Applied Cryptography**, *University College of London*, London, United Kingdom.

Visits/Internships

August 2012–January 2013 **EU Erasmus**, Aarhus University, Aarhus, Denmark.
Master's thesis preparation under the supervision of Claudio Orlandi and Ivan Damgård; Research on post quantum cryptography.

September 2015–December 2015 **PhD Intern**, INRIA Rhone Alpes, Grenoble, France.
Working under the supervision of Dr. Claude Castelluccia; Research on Deep Learning and De-anonymization.

Schools/Workshops Attended

August 2011 **Computational Nanotechnology Summer School** *Gdansk University of Technology,Poland*

13-16 October 2014 **IACR/CryptoAction School on Cryptographic Attacks** *Porto,Portugal*

28-29 January 2015 **Privaski Workshop** *Correncon, France*

7-9 January 2015 **Real World Cryptography Workshop 2015** *London, United Kingdom*

31 August - 5 September 2015 **School on Foundations of Security Analysis and Design (FOSAD)** *Bertinoro, Italy*

Research interests

- Privacy and Applied Cryptography
- Systems and Network Security
- Machine learning applied to security problems

List of publications

Luca Melis, George Danezis, and Emiliano De Cristofaro. Efficient Private Statistics with Succinct Sketches. *23rd Network and Distributed System Security Symposium (NDSS 2016), to appear*, 2016.

Work experiences

May 2013–June 2013 **Application consultant**, Iconsulting S.p.A., Bologna, Italy.

July 2013–October 2013 **Computer Vision researcher**, T3LAB, Bologna, Italy.

November 2013–August 2014 **Software Test Engineer Level II**, Gaming Laboratories International (GLI), Bologna, Italy.

Language skills

Italian	**Mothertongue**	
English	**Fluent**	*Level C1, TOEFL internet based test with a score of 98 out of 120 (2014)*

Computer skills and competences

Operative Systems	**Unix/Linux, Windows**
Tools	**Oracle XE, Matlab/Octave, Windows Office, MySQL**
Languages	**C/C++, SQL, Java, PHP, Flex, JavaScript, Python, Visual Basic.Net, Bash, LaTeX**

Enclosures

Enclosure 1: Bachelor’s thesis abstract

Title	Implementation of a Buyer-Seller protocol based on group signatures
Supervisors	Prof. Alessandro Piva, Ing. Tiziano Bianchi
Date	19th April 2010

Abstract

In this thesis we propose the implementation of the Buyer- Seller protocol designed by Mina Deng, Tiziano Bianchi, Alessandro Piva, and Bart Preneel. In the article the authors propose a secure Buyer-Seller protocol based on homomorphic encryption techniques and the efficient watermark insertion in the encrypted domain, with the aim to combine the safety of fingerprinting protocols with the efficiency of Buyer-Seller protocols.

The protocol has been developed in C++ and C by modeling the four entities involved (Buyer, Seller, Judge Authority and Certificate Authority) as independent processes that exchange data through Sockets. In order to facilitate the use of the application we develope and create a graphical interface for the Buyer that can initiate the protocol for trading the images.

The system stores the data of all transactions performed along with the cryptographic keys necessary for the protocol security.

Enclosure 2: Bachelor's degree transcript of records

Database Systems	24/30
Industrial Computers	28/30
Multimedia design and production	29/30
Fundamentals of automatic	30/30
English	passed
Signal theory	27/30
Security of Multimedia contents	30/30
Telematics	28/30
Artificial intelligence	28/30
Cryptography	26/30
Discrete mathematics	30/30
Fundamentals of operations research	29/30
Electronics I	26/30
Fundamentals of computer II	29/30
Phisics II	30/30
Operating systems	24/30
Analysis and simulation of dynamic systems	30/30
Computer architectures	22/30
Phisics I	30/30
Mathematical methods	30/30 cum laude
Electrotechnical	29/30
Fundamentals of computer I	30/30 cum laude
Statistics and probability for the engineering	30/30
Numerical analysis	30/30
Software Engineering	30/30
Mathematical analysis II	28/30
Mathematical analysis I	28/30
Laboratory of telematics	28/30
Geometry and linear algebra	25/30

Enclosure 3: Master's thesis abstract

Title	On the Learning Parity with Noise Problem
Supervisors	Prof. Alessandro Piva, Prof. Fabrizio Argenti
Advisors	Ivan Damgård, Claudio Orlandi
Date	19th April 2013

Abstract

A new promising direction in cryptography is the field of the *Post Quantum Cryptography*. Despite classical cryptographic schemes, such as *RSA* and *El-Gamal*, post quantum cryptographic systems are believed to resist quantum computers attacks.

The purpose of this thesis is to investigate the *Learning Parity with Noise* Problem (LPN). The LPN problem is one of the most promising post quantum cryptographic systems as it combines quantum algorithm resistance with efficiency. For these reasons LPN is well suited for weak devices like *Radio Frequency identification* (*RFID*) tags or sensor nodes. We investigate and provide a *Threshold Public-Key Encryption* scheme and a *Commitment protocol* both based on LPN.

We present a *Threshold Public-Key Encryption* scheme that is secure in the *Semi-honest* model, where each party follows the protocol properly. Our scheme can also withstand to *replay attacks*. We also present a *Commitment protocol* that is statistically binding and computationally hiding. Furthermore, our Commitment protocol doesn't need a trusted third party for the public key generation..

Enclosure 4: Master's degree transcript of records

Software dependability elements	30/30
Verification and testing methods	30/30
Math analysis III	30/30 cum laude
Multimedia databases	30/30
Security and management of telecommunication networks	30/30
Machine learning	30/30 cum laude
Statistical physics and information theory	30/30 cum laude
Database technologies	30/30
Computer architectures	30/30
Numerical analysis	30/30
Real analysis	30/30 cum laude
Information theory and codes	30/30
Theoretical Computer Science	30/30 cum laude

Enclosure 5: Personal projects

Name: Distributed railway interlocking system

Dates: 1 month (2012)

Technical skills used: UMC, Bash, Unix

Description: We model a distributed railway interlocking system. We check the safety and stabilization properties of the system using UML Model Checker. The system is implemented as an automa system.

Name: Human actions recognition by means of Pyramid String Kernel

Dates: 1 month (2012)

Technical skills used: Matlab, C++, LibSVM, Unix

Description: We implement a system of human actions recognition using a brand new technique based on Support Vector Machine. We use the Levenshtein distance as kernel string and we represent the strings modeling the actions in a pyramidal way.

Name: Collaborative filtering and probabilistic matrix factorization

Dates: 1 month (2011)

Technical skills used: Python, Unix

Description: We implement a collaborative filtering, i.e. a technique used in recommender systems. In particular, the implemented system is based on a bayesian probabilistic matrix factorization using Markov Chain Monte Carlo.

Name: Design and development of a system for the plagiarism detection

Dates: 2 months (2012)

Technical skills used: javascript, node.js, sqlite, Unix

Description: We develope a software for the plagiarism detection. Our software takes a database of documents and for each document computes some signatures. These signatures represent a summary of the document and our aim is to find if a new document is a plagiarism of documents already in the database.

Name: A Buyer-Seller protocol based on group signatures

Dates: 6 months (2010)

Technical skills used: C++, C, Unix

Description: The protocol has been developed in C++ and C by modeling the four entities involved (Buyer, Seller, Judge Authority and Certificate Authority) as independent processes that exchange data through Socket. We develope and create a graphical interface for the Buyer using the GTK libraries.

Name: Implementation of a Red-Black tree

Dates: 1 month (2008)

Technical skills used: C++, Windows

Description: We develope a Red-Black tree in C++. We make use of C++ features like operator overloading, static and dynamic polymorphism, memory management and inheritance.

Name: A video annotation tool in Flex

Dates: 3 months (2009)

Technical skills used: Flex Builder, PHP, SQL, Windows

Description: Our video annotation tool permits to annotate events and objects. The application is also multi-user, defining multiple privilege levels for different accounts. The aim of this software is towards the automatic learning of visual events.

Name: Design and development of a library information system

Dates: 1 month (2009)

Technical skills used: Eclipse, StarUML, Java, Design Pattern, Windows

Description: We first design the UML model of the application domain with the case use and activity diagrams. Using the UML model we develope the application for the book reservation system.

London, October 24, 2015