ROBERTO CIVINO

Curriculum Vitae

Personal information

iD	0000-0003-3672-8485

Research profile

SSD	MAT-02
Research interests	Cryptography; algebraic cryptanalysis of symmetric primitives; permutation groups; combinatorial aspects of integer partitions
Other interests	Digital forensics, mobile forensics

Current position

2022- **Researcher**, *Department of Information Engineering, Computer Science, and Mathematics of the University of L'Aquila*.
art. 24, comma 3, letter A of Law 30/12/2010 n. 240 - d.r. rep. 1242-22, prot. 113952, 30.09.2022; from 02.11.2022

Past academic positions

2020-2022 **Postdoctoral researcher**, *Department of Information Engineering, Computer Science, and Mathematics of the University of L'Aquila*, research project: Tecniche algebriche di crittanalisi per la sicurezza, funded by UnivAq and by the Centre of excellence ExEMERGE at UnivAq.
art. 22 of Law 240/2010 - rep. 46, prot. 2041, 25.05.2022; from 01.06.2022 to 31.10.2022
art. 22 of Law 240/2010 - rep. 53, prot. 1762, 26.05.2021; from 01.06.2021 to 31.05.2022
art. 22 of Law 240/2010 - rep. 40, prot. 1570, 28.05.2020; from 01.06.2020 to 31.05.2021

2019-2020 **Postdoctoral researcher**, *Department of Information Engineering, Computer Science, and Mathematics of the University of L'Aquila*, research project: Tecniche algebriche di crittanalisi per la sicurezza, funded by UnivAq and by GT50 srl.
art. 22 of Law 240/2010 - rep. 155, prot. 1976, 24.05.2019, from 01.06.2019 to 31.05.2020

2018-2019 **Postdoctoral researcher**, *Department of Mathematics of the University of Trento*, research project: Applicazioni della Teoria dei Gruppi alla crittografia simmetrica.
art. 22 of Law 240/2010 - d.d. n. 20, 23.04.2018; from 01.05.2018 to 30.04.2019

Education

2014–2018 **PhD in Mathematics**, *University of Trento, Department of Mathematics*, supervised by Massimiliano Sala (UniTn) and Céline Blondeau (Aalto University).
Certification of Doctor Europaeus
Mark: excellent cum laude (obtained 06/03/2018)

2010–2014 **Master's Degree in Mathematics (LM-40)**, *University of Salento, Department of Mathematics and Physics 'E. De Giorgi'*, supervised by Massimo Cafaro (UniSalento) and Barbara Masucci (UniSa).
Mark: 110/110 cum laude (obtained 29/04/2014)

2007–2010 **Bachelor's Degree in Mathematics (L-35)**, *University of Salento, Department of Mathematics and Physics 'E. De Giorgi'*, supervised by Giorgio Metafune.
Mark: 110/110 cum laude (obtained 10/12/2010)

Abroad

2017 **Visiting PhD student**, *Aalto University*, Helsinki, Finland, September 11-17.
supervised by Céline Blondeau

2016 **Visiting PhD student**, *Aalto University*, Helsinki, Finland, August-December.
supervised by Kaisa Nyberg and Céline Blondeau

Publications / Research Outputs

Doctoral Thesis

Title *Differential attacks using alternative operations and block cipher design*

Supervisors Massimiliano Sala (University of Trento) and Céline Blondeau (Aalto University)

Journals

[J14] R. Aragona, R. Civino, and F. Dalla Volta. On the primitivity of the AES-128 key-schedule. To appear on *Journal of algebra and its applications*
click to see on the publisher's website

[J13] R. Aragona, L. Campioni, R. Civino, and M. Lauria. On the maximal part in unrefinable partitions of triangular numbers. *Aequationes Mathematicae*, 2022
click to see on the publisher's website

[J12] R. Aragona, R. Civino, N. Gavioli, and C.M. Scoppola. Unrefinable partitions into distinct parts in a normalizer chain. *Discrete Mathematics Letters*, 8:72-77, 2022
click to see on the publisher's website

[J11] R. Aragona, R. Civino, N. Gavioli, and C.M. Scoppola. A chain of normalizers in the Sylow 2-subgroups of the symmetric group on 2^n letters. *Indian Journal of Pure and Applied Mathematics*, 52(3):735-746, 2021
click to see on the publisher's website

[J10] R. Aragona and R. Civino. On invariant subspaces in the Lai-Massey scheme and a primitivity reduction. *Mediterranean Journal of Mathematics*, 18(4):Paper No. 165, 14, 2021
click to see on the publisher's website

[J9] R. Aragona, R. Civino, N. Gavioli, and M. Pugliese. An authenticated key scheme over elliptic curves for topological networks. *Journal of Discrete Mathematical Sciences and Cryptography*, pages 1-20, 2021
click to see on the publisher's website

[J8] R. Civino, and R. Longo. Formal security proof for a scheme on a topological network. *Advances in Mathematics of Communications*, `https://www.aimsciences.org/article/doi/10.3934/amc.2021009`, 2021

[J7] R. Aragona, R. Civino, N. Gavioli, and C.M. Scoppola. Rigid commutators and a normalizer chain. *Monatshefte für Mathematik*, 196(3):431-455, 2021
click to see on the publisher's website

[J6] M. Calderini, R. Civino, and M. Sala. On properties of translation groups in the affine general linear group with applications to cryptography. *Journal of Algebra*, 569:658-680, 2021
click to see on the publisher's website

[J5] R. Aragona, M. Calderini, and R. Civino. Some group-theoretical results on Feistel Networks in a long-key scenario. *Advances in Mathematics of Communications*, 14(4):727, 2020
click to see on the publisher's website

[J4] R. Aragona, R. Civino, N. Gavioli, and C.M. Scoppola. Regular subgroups with large intersection. *Annali di matematica pura e applicata (1923-)*, 198(6):2043-2057, 2019
click to see on the publisher's website

[J3] R. Aragona, M. Calderini, R. Civino, M. Sala, and I. Zappatore. Wave-Shaped Round Functions and Primitive Groups. *Advances in Mathematics of Communications*, 13(1):67, 2019
click to see on the publisher's website

[J2] R. Civino, C. Blondeau, and M. Sala. Differential Attacks: Using Alternative Operations. *Designs, codes and cryptography* 87(2):225-247, 2019
click to see on the publisher's website

[J1] M. Cafaro, R. Civino, and B. Masucci. On the Equivalence of Two Security Notions for Hierarchical Key Assignment Schemes in the Unconditional Setting. *IEEE Transactions on Dependable and Secure Computing*, 12(4):485-490, 2014
click to see on the publisher's website

Preprints

[P2] R. Aragona, L. Campioni, and R. Civino. The number of maximal unrefinable partitions. Under review. Available at `https://arxiv.org/abs/2206.04261`

[P1] R. Aragona, L. Campioni, R. Civino, and M. Lauria. Verification and generation of unrefinable partitions. Under review. Available at `https://arxiv.org/abs/2112.15096`

Conferences

[C3] R. Aragona, R. Civino, N. Gavioli, and C. M. Scoppola. *On the groups of alternative operations for differential cryptanalysis*. Paper accepted for a talk at *The Eleventh International Workshop on Coding and Cryptography 2019*

[C2] C. Blondeau, R. Civino, and M. Sala. *Differential Attacks: Using Alternative Operations*. Paper accepted for a talk at *The Tenth International Workshop on Coding and Cryptography 2017*

[C1] R. Aragona, M. Calderini, R. Civino, M. Sala, and I. Zappatore. *Generalised Round Functions for Block Ciphers*. Paper accepted for a talk at *The 13th International Conference on Finite Fields and their Applications*

Teaching

Courses for PhD students

2021 **Group-theoretical cryptanalysis of block ciphers and alternative actions**, *DISIM, University of L'Aquila*, February.
full course, 10/10 hrs.

2020 **Group theoretical approach for symmetric encryption methods**, *DISIM, University of L'Aquila*, January - February.
teaching assistant, 2/10 hrs.

2019 **Permutation Groups and Applications to Cryptography**, *DISIM, University of L'Aquila*, January.
teaching assistant, 2/10 hrs.

Courses for Bachelor-Master students

2021-2022 **Algebra for Cryptography**, *DISIM, University of L'Aquila*, 2^{nd} term.
teaching assistant, 13/60 hrs.

2020-2021 **Combinatorics and Cryptography**, *DISIM, University of L'Aquila*, 2^{nd} term.
teaching assistant, 10/60 hrs.

2019-2020 **Combinatorics and Cryptography**, *DISIM, University of L'Aquila*, 2^{nd} term.
teaching assistant, 11/60 hrs.

2018-2019 **Combinatorics and Cryptography**, *DISIM, University of L'Aquila*, 2^{nd} term.
teaching assistant, 6/60 hrs.

2017-2018 **Analisi Matematica 1**, *Ingegneria Industriale, University of Trento*, September - January.
teaching assistant, 40/120 hrs.

Courses for IT security specialists

2022 **Smartphone encryption**, *offered by University of Trento*, October.
full course, 8/8 hrs.

2021 **Introduction to modern cryptography**, *offered by Telsy s.p.a.*, March.
full course, 40/40 hrs.

2020 **Cifrari a blocchi e identificazione relative vulnerabilità**, *offered by University of Trento*, November - December.
full course, 40/40 hrs.

Other courses

2022 **Decifris Trends in Modern Cryptography**, *online course organized by the University of Trento*, May.
lecturer

Tutoring

2021- **Co-advisor**, *Ph.D. thesis of the Ph.D. candidate Valerio Fedele*, advisor Norberto Gavioli.
Research topic: automorphisms of binary bi-braces

2020- **Co-advisor**, *Ph.D. thesis of the Ph.D. candidate Lorenzo Campioni*, advisor Riccardo Aragona.
Research topic: unrefinable partitions of integers

Contributed and invited talks

2022 *Maximal unrefinable partitions*, given at Combinatorics, Computing, Group Theory and Applications in South Florida, Deerfield Beach, Florida, August 17 (online)

2022 *The use of elementary abelian regular subgroups in cryptography*, given at The Algebra of the Yang-Baxter Equation, Bedlewo, Poland, July 12

2021 *On invariant subspaces in the Lai-Massey scheme and a primitivity reduction*, Associazione De Componendis Cifris, Italy, June 18 (online)

2020 *Differential cryptanalysis using alternative operations*, Invited by prof. M. Pedicini, Roma 3 University, Italy, February 26

2020 *Crittografia e identità digitali*, I.I.S. G.Leopardi - E.Majorana, Pordenone, Italy, January 18

2019 *On the groups of alternative operations for differential cryptanalysis*, given at the Eleventh International Workshop on Coding and Cryptography 2017, Saint-Jacut-de-la-Mer, France, April 2

2018 *Differential cryptanalysis using alternative operations and block cipher design*, Invited by prof. C. M. Scoppola, University of L'Aquila, Italy, February 12

2017 *Differential Attacks: Using Alternative Operations*, given at the Tenth International Workshop on Coding and Cryptography 2017, St. Petersburg, Russia, September 18-22

2017 *Generalised Round Functions for Block Ciphers*, given at the 13th International Conference on Finite Fields and their Applications, Gaeta, Italy, June 5

2017 *Differential Cryptanalysis with respect to Alternative Operations*, Invited by prof. F. Catino, University of Salento, Italy, April 18

2017 *Cryptography after RSA*, ITT Buonarroti, Trento, Italy, April 8

2016 *Differential Cryptanalysis with respect to Different Actions*, Aalto University, School of Science, Helsinki, Finland, September 5

2015 *Zero-Knowledge Proof in Multi-Party Computation*, University of Verona, Italy, June 8

2014 *Unconditional Security of Hierarchical Key Assignment Schemes*, University of Trento, Italy, December 22

2014 *Provable Security of Akl-Taylor Scheme*, University of Trento, Italy, December 15

Partecipation to national and international research projects

2017-2020 **Participant to PRIN 2015**, *Group theory and applications*, Scientific manager Prof. Andrea Lucchini, (Prot. 2015TW9LSR).
Research outputs include 4 publications [J2, J3, J4, J6]

Commissioned activities

2020- Consulente tecnico del Pubblico Ministero

2018-2019 Security assessment for a mobile encryption application, for GT50 s.r.l.

Reviewing activities

2021- Reviewer for zbMath (author ID civino.roberto - 19562)

2021- Reviewer for MathSciNet (MR author ID: 1308184)

2019 Referee for the volume "Algebra for Cryptography" in the series Collectio Ciphrarum

2018- Referee for Applicable Algebra in Engineering, Cryptologia, Communication and Computing, Discrete Mathematics, Mathematics, The Computer Journal, Journal of Computer Security, Journal of High Speed Networks

Organizing tasks

2022 *Street Science Pop-Up - Node e forme pazze in matematica*, University of L'Aquila, Italy, September 30

2022 *Topics in Algebra*, University of Trento, Italy, September 1-2

2020 *Cryptowars 2020*, University of Milan & Decifris, Italy, October 25-31

2019 *First Workshop in Algebra for Cryptography*, L'Aquila, Italy, October 10-11

Representative tasks

2014-2016 Representative of PhD students at the Department of Mathematics of the University of Trento

Attended conferences

2022 *Combinatorics, Computing, Group Theory and Applications in South Florida*, Deerfield Beach, Florida, August 14 - 21 (attending online)

2022 *The Algebra of the Yang-Baxter Equation*, Bedlewo, Poland, July 10 - 16

2022 *Ischia Group Theory 2022*, Ischia, Italy, June 20 - 25

2022 *The Twelfth International Workshop on Coding and Cryptography 2022*, Rostock, Germany, March 7 - 11 (online event)

2019 *First Workshop in Algebra for Cryptography*, L'Aquila, Italy, October 10-11

2019 *The Eleventh International Workshop on Coding and Cryptography 2019*, Saint-Jacut-de-la-Mer, France, March 31 - April 5

2018 *BFA-2018 – The workshop on Boolean Functions and their Applications*, Loen, Norway, June 17-22

2017 *The Tenth International Workshop on Coding and Cryptography 2017*, St. Petersburg, Russia, September 18-22

2017 *The 13th International Conference on Finite Fields and their Applications*, Gaeta, Italy, June 4-10

2016 *Security and Trust of Next Generation Enterprise Information Systems*, Trento, Italy, February 8-12

2015 *School on Design and Security of Cryptographic Algorithms and Devices*, Chia, Italy, October 18-23

2015 *Summer School on Mathematical and Practical Aspects of Fully Homomorphic Encryption and Multi-Linear Maps*, Paris, France, October 12-16 (*I have been awarded a stipend from the COST Action IC1306 for this school*)

2015 *Effective Methods in Algebraic Geometry - MEGA 2015*, Trento, Italy, June 15 - 19

2015 *The Ninth International Workshop on Coding and Cryptography - WCC 2015*, Paris, France, April 13-17

2014 *The 17th International Conference on Network-Based Information System - NBIS 2014 and The 6th International Conference on Intelligent Networking and Collaborative Systems - INCOS 2014*, Salerno, Italy, September 10-12

Membership

- Member of the INDAM group "GNSAGA - Gruppo Nazionale per le Strutture Algebriche, Geometriche e le loro Applicazioni"
- Member of "Iniziativa nazionale De Componendis Cifris"

Others

2021-2022 Cultore della materia "Algebra for Cryptography"

2020-2021 Cultore della materia "Combinatorics and Cryptography"

2019-2020 Cultore della materia "Combinatorics and Cryptography"

Computer skills

OS's	Microsoft Windows, Mac OS, Linux (Ubuntu, Deft, Caine), Android, iOs
Comp. Algebra	Magma, Matlab, Mathematica
Programming	C
Typesetting	LaTeX, Office
Forensics	Cellebrite UFED, Oxygen Forensic Detective, Axiom Examiner, Forensic Explorer

Languages

Italian	Mothertongue
English	Advanced (C1*)
Spanish	Intermediate (B1*)

**Common European Framework of Reference for Languages (CEFR)*

In compliance with the Italian Legislative Decree no. 196 dated 30/06/2003, I hereby authorize the recipient of this document to use and process my personal details for the purpose of recruiting and selecting staff and I confirm to be informed of my rights in accordance to art. 7 of the above mentioned decree. Everything stated in this document corresponds to the truth pursuant to art. 46 and 47 of the Presidential Decree 28 December 2000, n. 445 and subsequent amendments and additions.

Autorizzo il trattamento dei miei dati personali ai sensi ai sensi del Decreto Legislativo 101/2018 e dell'art. 13 GDPR (Regolamento UE 2016/679) ai fini della ricerca e selezione del personale. Quanto dichiarato corrisponde a verità ai sensi degli artt. 46 e 47 del D.P.R. 28 dicembre 2000, n. 445.

This CV consists of eight (8) pages — December 1, 2022.

Roberto Civino