europass Curriculum vitae

PERSONAL INFORMATION

Alessandro De Piccoli

alessandro.depiccoli@unimi.it

https://homes.di.unimi.it/depiccoli

https://github.com/ale-depi

https://gitlab.di.unimi.it/alessandro.depiccoli

ORCID 0000-0002-6399-3164

WORK EXPERIENCE

2021 – 2022 Mathematics tutor

Tutoring for students having mathematical Additional Training Obligations resulting from the entry test of *Università degli Studi di Milano*. – 80 hours

2008 – 2022 Science Teacher

Private lessons of mathematics to students of bachelor degree in biology and chemistry. Private lessons of mathematics and physics to students of high school.

2012 – 2016 Music Teacher

Private lessons of classical guitar for the music school *Esacordo*, Cabiate (CO).

2009 – 2012 Music Teacher

Private lessons of classical guitar for the music school *La Consonanza*, Varedo (MB).

EDUCATION AND TRAINING

2018 – 2021 PhD in Computer Science

Università degli Studi di Milano, Italia

Thesis: Optimized representations in cryptographic primitives

2011 – 2018 Master of Science in Mathematics

Università degli Studi di Milano, Italia

Thesis Title: *High-speed cryptography: new results*

2009 – 2011 General Musical Culture

Conservatorio *Luca Marenzio* di Darfo Boario Terme (BS)

2007 – 2011 Bachelor of Science in Mathematics

Università degli Studi di Milano, Italia

Thesis Title: *Algebraic plane curves of order 3*

2009 Lower diploma in Guitar

Conservatorio *Luca Marenzio* di Darfo Boario Terme (BS)

2002 – 2007 Scientific High School Diploma

Liceo Scientifico *Ettore Majorana*, Desio (MB)

2006 **License of Music Theory and Solfeggio**

Conservatorio *Lucio Campiani* di Mantova (MN)

PERSONAL SKILLS

Mother tongue: Italian, Spanish

Other languages

	UNDERSTANDING		SPEAKING		WRITING
	Listening	Reading	Spoken interaction	Spoken production	
English	B2	B2	B2	B2	B2
	Cambridge FCE (First Certificate in English)				

Levels: A1 and A2: Basic user – B1 and B2: Independent user – C1 and C2: Proficient user
Common European Framework of Reference for Languages

Computer skills: Languages and working periods.

- C: 2007 programming course 1 (bachelor of science in mathematics), 2010 algorithms course (bachelor of science in mathematics), 2018 – today
- HTML: 2019 – today (self-taught)
- Java: 2013 programming course 2 (master of science in mathematics), 2015 programming course 3 (master of science in mathematics)
- LaTeX: 2009 – today (self-taught)
- Lilypond: 2015 – today (self-taught for personal interest)
- Python: 2019 – today (self-taught)

Driving licence: B

PUBLICATIONS

[1] **Alessandro De Piccoli**, Andrea Visconti, and Ottavio Giulio Rizzo. “Polynomial multiplication over binary finite fields: new upper bounds”. In: *Journal of Cryptographic Engineering* 10.3 (Sept. 2020), pp. 197–210. ISSN: 2190-8516. DOI: 10.1007/s13389-019-00210-w.

[2] Emanuele Bellini, **Alessandro De Piccoli**, Rusydi Makarim, Sergio Polese, Lorenzo Riva, and Andrea Visconti. “New Records of Pre-image Search of Reduced SHA-1 Using SAT Solvers”. In: *Proceedings of the Seventh International Conference on Mathematics and Computing*. Ed. by Debasis Giri, Kim-Kwang Raymond Choo, Saminathan Ponnusamy, Weizhi Meng, Sedat Akleylek, and Santi Prasad Maity. Singapore: Springer Singapore, 2022, pp. 141–151. ISBN: 978-981-16-6890-6. DOI: 10.1007/978-981-16-6890-6_11.

[3] Michela Ceria, **Alessandro De Piccoli**, Martino Tiziani, and Andrea Visconti. “Optimizing the Key-Pair Generation Phase of McEliece Cryptosystem”. In: *4th International Conference on Wireless, Intelligent and Distributed Environment for Communication*. Ed. by Isaac Woungang and Sanjay Kumar Dhurandher. Cham: Springer International Publishing, 2022, pp. 111–122. ISBN: 978-3-030-89776-5. DOI: 10.1007/978-3-030-89776-5_8.

[4] Rohon Kundu, **Alessandro De Piccoli**, and Andrea Visconti. “Public Key Compression and Fast Polynomial Multiplication for NTRU using the Corrected Hybridized NTT-Karatsuba Method”. In: *Proceedings of the 8th International Conference on Information Systems Security and Privacy - ICISSP*, INSTICC. SciTePress, 2022, pp. 145–153. ISBN: 978-989-758-553-1. DOI: 10.5220/0010881300003120.