europass Currículum vitae

INFORMACIÓNES PERSONALES

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

EXPERIENCIA PROFESIONAL

2021 – 2022

Tutor de matemáticas

Actividad de tutoring para estudiantes que tienen Obligaciones Adicionales de Formación (OAF) de matemáticas surgidos por la prueba de ingreso. *Università degli Studi di Milano*. – 80 horas

2008 – 2022

Enseñanza de matemáticas e física

Clases particulares de matemáticas generales para estudiantes de la licenciatura en biología y química. Clases particulares de matemáticas y física para estudiantes de secundaria (primer y segundo grado).

2012 – 2016

Enseñanza de música

Clases particulares de guitarra clasica para la escuela de música *Esacordo*, Cabiate (CO).

2009 – 2012

Enseñanza de música

Clases particulares de guitarra clasica para la escuela de música *La Consonanza*, Varedo (MB).

EDUCACIÓN Y FORMACIÓN

2018 – 2021

Doctorado en Informatica

Università degli Studi di Milano, Italia

Tesis: Optimized representations in cryptographic primitives

2011 – 2018

Maestría de matemáticas

Università degli Studi di Milano, Italia

Tesis: *High-speed cryptography: nuevos resultados*

2009 – 2011

Cultura musical general (Armonía complementaria)

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

2007 – 2011

Licenciatura in matematica

Università degli Studi di Milano, Italia

Tesis: *Curvas algebraicas planas de orden 3*

2009

Diploma inferior de guitarra

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

2002–2007 **Diploma de bachillerato científico**

Liceo scientifico *Ettore Majorana*, Desio (MB)

2006 **Licencia de teoria y solfeo**

Conservatorio *Lucio Campiani*, Mantova (MN)

HABILIDADES PERSONALES

Lengua materna: Italiano, Español

Otros idiomas

	COMPRENDER		HABLAR		EXPRESIÓN ESCRITA
	Comprensión auditiva	Comprensión de lectura	Interacción oral	Expresión oral	
Inglés	B2	B2	B2	B2	B2
	Cambridge FCE (First Certificate in English)				

Niveles: A1/A2: Usuario básico – B1/B2: Usuario independiente – C1/C2: Usuario competente
Marco común Europeo de referencia para las lenguas

Habilidades digitales: Lenguajes y periodos de uso.

- C: 2007 curso de programacion 1 (licenciatura en matemáticas), 2010 curso de algoritmos (licenciatura en matemáticas), 2018 – presente
- HTML: 2019 – presente (autodidacta)
- Java: 2013 curso de programacion 2 (maestria en matemáticas), 2015 curso de programacion 3 (maestria en matemáticas)
- LaTeX: 2009 – presente (autodidacta)
- Lilypond: 2015 – presente (autodidacta por interés personal)
- Python: 2019 – presente (autodidacta)

Licencia de conducción: B

PUBLICACIONES

[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.