europass Curriculum vitae

INFORMAZIONI PERSONALI

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

ESPERIENZA PROFESSIONALE

2021 – 2022 **Tutor di matematica**

Attività di tutoraggio per studenti con Obblighi Formativi Aggiuntivi (OFA) di matematica derivanti dal test d'ingresso per *Università degli Studi di Milano*. – 80 ore

2008 – 2022 **Insegnante di matematica e fisica**

Lezioni private di matematica generale a studenti del corso di laurea in biologia e chimica. Lezioni private di matematica e fisica per studenti di scuola secondaria (di primo e secondo grado).

2012 – 2016 **Insegnante di musica**

Lezioni private di chitarra classica per la scuola di musica *Esacordo*, Cabiate (CO).

2009 – 2012 **Insegnante di musica**

Lezioni private di chitarra classica per la scuola di musica *La Consonanza*, Varedo (MB).

ISTRUZIONE E FORMAZIONE

2018 – 2022 **Dottorato in Informatica**

Università degli Studi di Milano, Italia

Tesi: Optimized representations in cryptographic primitives

2011 – 2018 **Laurea magistrale in matematica**

Università degli Studi di Milano, Italia

Tesi: *High-speed cryptography: nuovi risultati*

2009 – 2011 **Cultura musicale generale (Armonia complementare)**

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

2007 – 2011 **Laurea triennale in matematica**

Università degli Studi di Milano, Italia

Tesi: *Curve algebriche piane di ordine 3*

2009 **Compimento inferiore di chitarra**

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

2002–2007 **Diploma di liceo scientifico**

Liceo scientifico *Ettore Majorana*, Desio (MB)

2006 **Licenza di teoria e solfeggio**

Conservatorio *Lucio Campiani* di Mantova (MN)

COMPETENZE PERSONALI

Lingua madre: Italiano, Spagnolo

Altre lingue

	COMPRENSIONE		PARLATO		PRODUZIONE SCRITTA
	Ascolto	Lettura	Interazione	Produzione orale	
Inglese	B2	B2	B2	B2	B2
	Cambridge FCE (First Certificate in English)				

Livelli: A1 e A2: Utente base – B1 e B2: Utente autonomo – C1 e C2: Utente avanzato
Quadro Comune Europeo di Riferimento delle Lingue

Competenze digitali: Linguaggi e relativi periodi d'uso.

- C: 2007 corso di programmazione 1 (laurea triennale in matematica), 2010 corso di algoritmi (laurea triennale in matematica), 2018 – presente
- HTML: 2019 – presente (autodidatta)
- Java: 2013 corso di programmazione 2 (laurea magistrale in matematica), 2015 corso di programmazione 3 (laurea magistrale in matematica)
- LaTeX: 2009 – presente (autodidatta)
- Lilypond: 2015 – presente (autodidatta per interesse personale)
- Python: 2019 – presente (autodidatta)

Patente di guida: B

PUBBLICAZIONI

[1] **Alessandro De Piccoli**, Andrea Visconti e Ottavio Giulio Rizzo. «Polynomial multiplication over binary finite fields: new upper bounds». In: *Journal of Cryptographic Engineering* 10.3 (set. 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 e 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*. A cura di Debasis Giri, Kim-Kwang Raymond Choo, Saminathan Ponnusamy, Weizhi Meng, Sedat Akleylek e 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 e Andrea Visconti. «Optimizing the Key-Pair Generation Phase of McEliece Cryptosystem». In: *4th International Conference on Wireless, Intelligent and Distributed Environment for Communication*. A cura di Isaac Woungang e 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** e 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.