



FORM NUM: 500.1.03

Academic Personnel Short Profile / Short CV

University:	University of Nicosia
Surname:	Mourouzis
Name:	Theodosis
Rank/Position:	Part Time Lecturer
Faculty:	School of Business
Department:	Digital Innovation
Scientific Domain: *	Cryptography

** Field of Specialization*

Academic qualifications (list by highest qualification)				
Qualification	Year	Awarding Institution	Department	Thesis title (Optional Entry)
BA/MA Mathematics	2009	University of Cambridge		
MSc Mathematics	2010	University of Cambridge		
MRes Security Science	2011	University College London		
PhD in Computer Science	2015	University College London		

Employment history in Academic Institutions/Research Centers – List by the three (3) most recent				
Period of employment		Employer	Location	Position
From	To			
09/2015	09/2019	CIIM	Cyprus	Lecturer
04/2017		UCL	Cyprus	Research Fellow



11/2018		Universtiy of Nicosia	Cyprus	Part Time Lecturer
---------	--	-----------------------	--------	--------------------

Key <u>refereed</u> journal papers, monographs, books, conference publications etc. List the five (5) more recent and other five (5) selected –(max total 10)						
Ref. Number	Year	Title	Other authors	Journal and Publisher / Conference	Vol.	Pages
1	2016	Hypothesis Testing and Advanced Distinguishers in Differential Cryptanalysis of Block Ciphers	Theodosios Mourouzis, Nicolas Courtois	Tatra Mountains, Mathematical Publications	64	1-14
2	2015	Advanced Truncated Differential Attacks Against GOST block cipher and its variants	Theodosios Mourouzis, Nicolas Courtois	Computation, Cryptography and Network Security	n/a	n/a
3	2014	Combined Truncated Differential-Algebraic Attacks against reduced-round SIMON	Nicolas Courtois, Theodosios Mourouzis, Guangyan Song, Pouyan Sepehrad, Petr Susi	SECRYPT 2014	n/a	399-404
4	2014	On Optimal Size in Truncated Differential Attacks	Nicolas Courtois, Theodosios Mourouzis, Anna GrochowskaCzurylo, JeanJacques Quisquater	CECC 2014	n/a	n/a
5	2014	Advanced Differential Cryptanalysis and GOST Cipher	Nicolas T. Courtois, Theodosios Mourouzis	IMA Conference on Mathematics in Defence	n/a	n/a
6	2015	Can GOST Be Made Secure Against Differential Cryptanalysis?	Nicolas Courtois, Theodosios Mourouzis, Michal Misztal, Jean-Jacques Quisquater and Guangyan Song	Cryptologia	39(2)	145-156



7	2015	Optimizations in algebraic and differential cryptanalysis	Theodosios Mourouzis	n/a		n/a
8	2013	Nicolas T. Courtois, Theodosios Mourouzis, Michal Misztal	n/a	n/a		411-418
9	2012	Extension of de Weger's Attack on RSA with Large Public Keys	Nicolas T. Courtois, TheoNicolas T. Courtois, Theodosios Mourouzis, Pho V. Le	SECRYPT 2013	n/a	411-418
10	2011	Black-box Collision Attacks on the Compression Function of the GOST Hash Function	Nicolas Courtois, Theodosios Mourouzis	SECRYPT 2011	n/a	325-332

**Academic Consulting Services and/or Participation in Councils / Boards/ Editorial Committees.
List the five (5) more recent (Optional Entry)**

Ref. Number	Period	Organization	Title of Position or Service	Key Activities
1	01/08/2018 - Present	Frontiers in Blockchain		
2	26/09/2018 - Present	Cyprus Mathematical Society		
3	TBA	Ad Hoc Blockchain Committee for the Government of Cyprus (Technology Track)		
4	01/09/2015 - 01/09/2016	LLoyds Banking Group		

**Awards / International Recognition (where applicable). List the five (5) more recent and other five (5) selected.
(max total 10) (Optional Entry)**

Ref. Number	Date	Title	Awarded by:
-------------	------	-------	-------------



1	2012	Nicolas Courtois, Daniel Hulme and Theodosios Mourouzis: Multiplicative Complexity and Solving Generalized Brent Equations With SAT Solvers. IARIA 2012: 22-27 (Best Paper Award)	
2	2002	Balkan Mathematical Olympiad (BMO Turkey 2002)	
3	2003	Balkan Mathematical Olympiad (BMO Turkey 2003)	
4	2001	Balkan Mathematical Olympiad (BMO Turkey 2001)	
5	2005	International Mathematical Olympiad (IMO – Mexico 2005)	
6	2013	Cyber Security Challenge 2013: Winner of the 1st University Challenge for cryptography/security announced by Cyber Security Challenge UK, 25 January 2013	