Anna Lisa Ferrara

July 2022

3395902018 • annalisa.ferrara@unimol.it

Dipartimento di Bioscienze e Territorio
Università degli Studi del Molise
Contrada Fonte Lappone – 86090 Pesche (IS), ITALY

Citizenship: Italian, British

Languages: Italian (Native), English (Fluent)

Education

PhD in Computer Science

April 2006

Degree awarded by the University of Salerno, Italy
Thesis Title: On Access Control Policies and Key Assignment Schemes
Supervisor: Alfredo De Santis

Laurea Degree in Computer Science

July 2002

Degree awarded by the University of Salerno
Thesis Title: Assegnamento di Chiavi Crittografiche in una Gerarchia
Supervisor: Alfredo De Santis

Employment

Universitá degli Studi del Molise, Campobasso, IT
Associate Professor *March 2019–present*

University of Southampton, UK
Lecturer B in Cyber Security
Department of Electronics and Computer Science *January 2017– February 2019*

University of Surrey, Guildford, UK
Lecturer B in Cyber Security
Department of Computing *October 2013–December 2016*

University of Bristol, Bristol, UK
Associate Researcher
Bristol Cryptography Group *November 2011–September 2013*

Southampton University, Southampton, UK
Post-doc Researcher
School of Electronics and Computer Science *May 2011–October 2011*

Universitá degli Studi di Salerno, IT
Post-doc Researcher
Dipartimento di Informatica ed Applicazioni — *June 2010–April 2011*

University of Illinois, Urbana-Champaign, USA
Post-doc Researcher
Department of Computer Science — *February 2008–April 2009*

Johns Hopkins University, Baltimore, USA
Post-doc Researcher
Security and Privacy Applied Reasearch (SPAR) Lab
Department of Computer Science — *February 2007–January 2008*

Universitá degli Studi di Salerno, Salerno, IT
Research Assistant
Dipartimento di Informatica ed Applicazioni — *December 2005–January 2007*

Visiting Positions

University of Illinois at Urbana-Champaign, USA
Visiting Researcher
Department of Computer Science — *July 2011*

Universitá degli Studi di Trento, Italy
Invited Researcher
Department of Information Sciences and Engineeering — *May 2009*

University of Waterloo, Ontario, Canada
Visiting Scholar
Centre for Applied Cryptographic Research
Department of Computer Science — *September 2004–May 2005*

Research Interests

- Computer Security
- Applied Cryptography
- Formal Methods for Computer Security

Professional Activities and Service

Conference Program Committee Member

- The 18th ACM ASIA Conference on Computer and Communications Security - ACM ASIACCS 2023
- The 27th European Symposium on Research in Computer Security - ESORICS 2022
- The 19th International Conference on Security and Cryptography - SECRYPT 2022
- The 15th International Colloquium on Theoretical Aspects of Computing - ICTAC 2018
- The 14th EAI International Conference on Collaborative Computing - CollaborateCom 2018
- The 5th EAI International Conference on Smart Cities - Mobility IoT 2018
- The 13th EAI International Conference on Collaborative Computing - CollaborateCom 2017
- The 29th IEEE Computer Security Foundations Symposium - CSF 2016
- The 12th International Conference on Mobile Web and Intelligent Information Systems - MobiWis 2015
- The 10th InternationalConferenceonElectronicCommerceandWebTechnologies - EC-Web2009
- The 11th InternationalConferenceonElectronicCommerceandWebTechnologies - EC-Web2010

Journal Referee

- ACM Transactions on Information and System Security (TISSEC)
- Theoretical Computer Science (TCS)
- Design, Codes and Cryptography (DCC)
- IEEE Transaction on Computers
- Information Processing Letters (IPL)
- IEEE Transaction on Knowledge and Data Engineering
- IEEE Transaction on Information Forensic and Security
- IEEE Transaction on Dependable and Secure Computing (TDSC)
- Information Sciences

Conference Referee

- Int'l ACM Conference on Computer and Communications Security (CCS)
- Int'l Conference on Practice and Theory of Public-Key Cryptography (PKC)
- Int'l Symposium on Logic in Computer Science (LICS)
- Int'l Colloquium on Automata, Languages, and Programming (ICALP)
- Int'l Theory of Cryptography Conference (TCC)
- Int'l ACM ASIA Conference on Computer and Communications Security (ASIACCS)
- Int'l European Symposium on Research in Computer Security (ESORICS)
- Int'l Conference on Security and Cryptography (SECRYPT)

PhD Examiner

- **Anastasios Bikos**
First year viva, University of Surrey (UK) *July 2013*

• **Emanuela Flores**
Third year viva, University of Salerno (IT) *February 2019*

PostDoc Supervision

• Dott.Truc Nguyen Lam (August 2017-December 2017)
• Dott. Ivo Timev (June 2018-September 2018)
• Dott. Enrico Steffinlongo (May 2018-August 2018)

Invited seminar Speaker

• Corporate Security and Corporate Intelligence, Cyber Security Centre, University of Southampton, July 2018.
• Corporate Security and Corporate Intelligence, Cyber Security Centre, University of Southampton, July 2017.
• Security Analysis of Access Control Policies, University of Kent, UK, October 2014.
• Securing the CyberSpace: Managing with Access Control Issues, U. Southampton, UK, October 2014.
• Securing the CyberSpace: Managing with Access Control Issues, U. Surrey, UK, July 2014.
• Design and Analysis of Security Systems, King's College London, UK, November 2012.
• Design and Analysis of Security Systems, Bristol University, UK, September 2012.
• Design and Analysis of Cryptographic Protocols, King's College London, UK, July 2011.
• Cryptographic Enforcment of Access Control Policies, University of Southampton, UK, February 2011.
• Batch Verification of Short Signatures, Universita' di Trento, Italy, December 2007.
• On Hierarchical Key Assignment Schemes, University of Illinois, USA, December 2006.

Organizing Committees

• Local Arrangement Chair of 14th International Conference on Applied Cryptography and Network Security (ACNS 2016).
• Workshops Chair of Human Factors in Cyber Security Workshop, Surrey Centre for Cyber-Security (SCCS), (March 2016), University of Surrey (UK).

University Activities

Teaching

• **Networking Security and Software Security**
Laurea Magistrale in Sicurezza dei Sistemi Software, Universitá del Molise, IT. *A.A. 2021/2022*

• **Cryptography**
Laurea Magistrale in Sicurezza dei Sistemi Software, Universitá del Molise, IT. *A.A. 2021/2022*

• **Computer Networking**
Corso di Laurea in Informatica, Universitá del Molise, IT. *A.A. 2021/2022*

• **Networking Security and Software Security**
Laurea Magistrale in Sicurezza dei Sistemi Software, Universitá del Molise, IT. *A.A. 2019/2020*

• **Cryptography**
Laurea Magistrale in Sicurezza dei Sistemi Software, Universitá del Molise, IT. *A.A. 2019/2020*

• **Computer Networking**
Corso di Laurea in Informatica, Universitá del Molise, IT. *A.A. 2019/2020*

• **Networking Security and Software Security**
Corso di Laurea in Informatica, Universitá del Molise, IT. *A.A. 2018/2019*

• **Cryptography**
Laurea Magistrale in Sicurezza dei Sistemi Software, Universitá del Molise, IT. *A.A. 2018/2019*

• **Computer Networking**
Corso di Laurea in Informatica, Universitá del Molise, IT. *A.A. 2018/2019*

• **Cryptography**
Laurea Magistrale in Sicurezza dei Sistemi Software, Universitá del Molise, IT. *A.A. 2017/2018*

• **Networking Security and Software Security**
Corso di Laurea in Informatica, Universitá del Molise, IT. *A.A. 2017/2018*

• **Computer Networking**
Corso di Laurea in Informatica, Universitá del Molise, IT. *A.A. 2016/2017*

• **Foundation of Computing**
UG program in Computer Science, University of Surrey, UK. *A.A. 2015/2016*

• **Information and Network Security**
Master in Information Security, University of Surrey, UK. *A.A. 2015/2016*

• **Foundation of Computing**
UG program in Computer Science, University of Surrey, UK. *A.A. 2014/2015*

• **Information and Network Security**
Master in Information Security, University of Surrey, UK. *A.A. 2014/2015*

• **Secure Systems and Applications**
Master in Information Security, University of Surrey, UK. *A.A. 2013/2014*

• **Information and Network Security**
Master in Information Security, University of Surrey, UK. *A.A. 2013/2014*

• **Sicurezza su Reti**
Corso di Laurea in Informatica, Universitá di Salerno, IT. *A.A. 2011/2012*

• **An Information Theoretic Approach and Provable Secure Solutions**
Advanced Topics in Network Security,
International Doctorate School, Trento, IT. *May 2009*

Administration/Other

• **MSc Coordinator**
Master in Information Security, University of Surrey, UK. *October 2014 - October 2016*

• **MSc Admissions Tutor**
Master in Information Security, University of Surrey, UK. *October 2014 - October 2016*

• **Academic Integrity Officer**
Master in Information Security, University of Surrey, UK. *October 2015 - October 2016*

• **Athena Swan co-leader Self Assessment Team**
University of Surrey, UK. *2015 - 2016*

Awards

Abilitazione Scientifica Nazionale a Professore di seconda fascia
settore concorsuale 01/B1 - INF/01. *2019*

Abilitazione Scientifica Nazionale a Professore di seconda fascia
settore concorsuale 01/B1 - INF/01. *2014*

Fellow of the Higher Education Academy (FHEA) (UK)
2015

Maitre de Conferences in Informatique (France)
2011

Partecipation in funded Research Projects

• Advanced Grant European Research Council: ERC-2010-Adg-267188-CRIPTO.
• European Network of Excellence in Cryptology - ECRYPT II - MAYA.
• European Network of Excellence in Cryptology - ECRYPT I.
• NSF Grant: Formal Security Analysis of Access Control Models and Extensions. NSF Pro- gram: Trustworthy Computing. Principal Investigators: V. Atluri (Rutgers University, (USA)), P. Madhusudan (University of Illinois at Urbana-Champaign (USA)), Jaideep Vaidya (Rutgers University (USA)).
• Italian Projects FARB (ex 60 • Italian Project PRIN 2006: Analisys and Design of Cryptographic Protocols for Distributed Access Control Systems.

Research Grants

Engineering and Physical Sciences Research Council (EPSRC)
VAC+: Verifier of Access Control.
120.000 GBP. *August 2017–May 2019*

Microsoft Azure for Research Award
Automated Analysis of Role-based Access Control in Azure-like Platforms.
$20.000 in cloud resources. *January 2017–January 2018*

Leaves

Maternity Leave
February 2013–July 2013

Maternity Leave
August 2017–January 2017

Publications

[1] Fuzzy-based Approach to Assess and Prioritize Privacy Risks. *Soft Computing, Springer*, Doi: 10.1007/s00500-019-03986-5 (2019)
(with S. Hart, and F. Paci).

[2] Security Analysis for Temporal Role Based Access Control. *Journal of Computer Security*, 22(6): 961-996, (2014)
(with E. Uzun, V. Atluri, S. Sural, J. Vaidya, G. Parlato, and P. Madhusudan).

[3] A Note on Time-Bound Hierarchical Key Assignment Schemes. *Information Processing Letters*, Inf. 113(5-6): 151-155, (2013)
(with G. Ateniese, A. De Santis and B. Masucci).

[4] Provably-Secure Time-Bound Hierarchical Key Assignment Schemes. *Journal of Cryptology*, vol. 25(2), pp. 243-270, (2012)
(with G. Ateniese, A. De Santis, and B. Masucci).

[5] Efficient Provably-Secure Hierarchical Key Assignment Schemes. *Theorethical Computer Science*, vol. 412(41), pp. 5684-5699, (2011)
(with A. De Santis and B. Masucci).

[6] Variations on a Theme by Akl and Taylor: Security and Tradeoffs. *Theorethical Computer Science*, vol. 411, pp. 213-227, (2010)
(with P. D'Arco, A. De Santis, and B. Masucci).

[7] An Attack on a Payment Scheme. *Information Sciences*, Vol. 178, No. 5, pp. 1418-1421, (2008)
(with A. De Santis, and B. Masucci).

[8] New Constructions for Provably-Secure Time-Bound Hierarchical Key Assignment Schemes. *Theoretical Computer Science*, Vol. 407, pp. 213-230, (2008)
(with A. De Santis, and B. Masucci).

[9] Enforcing the Security of a Time-bound Hierarchical Key Assignment Scheme. *Information Sciences*, Vol. 176, No. 12, pp. 1684–1694, (2006)
(with A. De Santis, and B. Masucci).

[10] Unconditionally Secure Key Assignment Schemes. *Discrete Applied Mathematics*, Vol. 154, No. 2, pp. 234–252, (2006)
(with A. De Santis, and B. Masucci).

[11] Ideal Contrast Visual Cryptography Schemes with Reversing. *Information Processing Letters*, Vol. 93, n. 4, pp. 199-206, (2005)
(with S. Cimato, A. De Santis, and B. Masucci).

[12] Cryptographic Key Assignment Schemes for any Access Control Policy. *Information Processing Letters*, Vol. 92, n. 4, pp. 199-205, (2004)
(with A. De Santis, and B. Masucci).

[13] A Simple Algorithm for the Constrained Sequence Problems. *Information Processing Letters*, Vol. 92, n. 4, pp. 199-205, (2004)
(with A. De Santis, Francis Y. L. Chin, N. L. Ho, and S. K. Kim).

[14] Modeling A Certified Email Protocol using I/O Automata. *Electronic Notes in Theoretical Computer Science*, vol. 99, pp. 339-359, (2004)
(with C. Blundo, S. Cimato and R. De Prisco).

---

[15] Verifiable Hierarchical Key Assignment Schemes. *In 35st Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy*, (DBSec 2021)
(with F. Paci and C. Ricciardi).

[16] Preventing unauthorized data flows. *In 31st Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy*, (DBSec 2017)
(with E. Uzun, G. Parlato, V. Atluri, J. Vaidya, S. Sural, and D. Lorenzi).

[17] Toward group-based user-attribute policies in azure-like access control systems. *In 31st Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy*, (DBSec 2017)
(with A. Squicciarini, C. Liao, T. Nguyen).

[18] Policy Privacy in Cryptographic Access Control. *In Proc. IEEE 28th Computer Security Foundations Symposium*, (CSF 2015)
(with G. Fuchsbauer, Bin Liu, and B. Warinschi).

[19] VAC: Verifier of Administrative Role-based Access Control Policies. *In Proc. 26th International Conference on Computer Aided Verification (CAV 2014)*
(with P. Madhusudan, T. L. Nguyen, and G. Parlato).

[20] Cryptographically Enforced RBAC. *In Proc. IEEE 26th Computer Security Foundations Symposium* (CSF 2013)
(with G. Fuchsbauer, and B. Warinschi).

[21] Policy Analysis for Self-Administrated Role-Based Access Control. *In Proc. 19th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2013)*
(with P. Madhusudan, and G. Parlato.).

[22] Security Analysis of Access Control Policies through Program Verification. *In Proc. 25th IEEE Computer Security Foundations Symposium (CSF 2012)*
(with P. Madhusudan, and G. Parlato).

[23] Analyzing Temporal Role Based Access Control Models. *In Proc. 17th ACM Symposium on Access Control Models and Technologies (SACMAT 2012)*
(with V. Atluri, P. Madhusudan, G. Parlato, S. Sural, E. Uzun, and J. Vaidya).

[24] Security and Tradeoffs of the Akl-Taylor Scheme and its Variants. *In Proc. 34th International Symposium on Mathematical Foundations of Computer Science (MFCS 2009)*
(with P. D'Arco, A. De Santis, and B. Masucci).

[25] Practical Short Signature Batch Verification. *In Proc. Topics in Cryptology. The Cryptographers' Track at the RSA Conference 2009 (CT-RSA 2009)*
(with M. Green, S. Hohenberger, and M. O. Pedersen).

[26] Efficient Provably-Secure Hierarchical Key Assignment Schemes. *In Proc. 32nd International Symposium on Mathematical Foundations of Computer Science (MFCS 2007)*
(with A. De Santis, and B. Masucci).

[27] New Constructions for Provably-Secure Time-Bound Hierarchical Key Assignment Schemes. *In Proc. 12th ACM Symposium on Access Control Models and Technologies (SACMAT 2007)*
(with A. De Santis, and B. Masucci).

[28] Provably-Secure Time-Bound Hierarchical Key Assignment Schemes. *In Proc. 14th ACM Conference on Computer and Communications Security (CCS 2006)*
(with G. Ateniese, A. De Santis, and B. Masucci).

[29] A New Key Assignment Scheme for Access Control in a Complete Tree Hierarchy. *In Proc.International Workshop on Coding and Cryptography (WCC 2005)*
(with A. De Santis, and B. Masucci).

[30] Unconditionally Secure Hierarchical Key Assignment Schemes. *In Proc. International Workshop on Coding and Cryptography (WCC 2003)*
(with A. De Santis, and B. Masucci).

[31] An Information-Theoretic Approach to the Access Control Problem. *In Proc. of The Eighth Italian Conference on Theoretical Computer Science (ICTCS 2003)*
(with B. Masucci).

---

[32] On Access Control Policies and Key Assignment Schemes. Tesi di dottorato, Università degli Studi di Salerno, Aprile 2006.

[33] Assegnamento di Chiavi in una Gerarchia. Tesi di Laurea, Università degli Studi di Salerno, Luglio 2002.

---

[34] Visual Cryptography Schemes with Reversing. In *Visual Cryptography and Secret Image Sharing*, CRC Press, Boca Raton, USA, August 2011.
(with A. De Santis, and B. Masucci).
