

# CURRICULUM VITAE ET STUDIORUM

MATTEO MAFFEI

April 2017

## General Information

Family Name, First Name: Maffei, Matteo  
Date of birth: 16.11.1978  
Citizenship: Italian and German  
Email address: matteo.maffei@tuwien.ac.at  
Telephone: +43-664-88537132  
Address: TU Wien  
Security and Privacy Group, E184/6  
1. Stock, Steige 2  
Wien, A-1040

## Academic Background

### Ca' Foscari University of Venice

Ph.D. in Computer Science, March 2006. 2002-2006  
*Dissertation:* Dynamic Typing for Cryptographic Protocols  
*Supervisors:* Riccardo Focardi and Michele Bugliesi

Laurea in Computer Science, July 2002. (110/110 cum laude) 1997-2002  
*Dissertation:* A Type System for Authentication Protocols  
*Supervisor:* Riccardo Focardi

## Current and Previous Positions

### TU Wien

Full Professor (tenured), Chair of Security and Privacy 2017 - present

### Saarland University

Associate Professor (W2, tenured), Chair of Secure and Privacy-preserving Systems 2013-2017

Independent Research Group Leader, Chair of Language-based Security 2008-2013  
Postdoc assistant 2006-2008

### Declined Offers

|                               |                                   |      |
|-------------------------------|-----------------------------------|------|
| Leibniz University of Hanover | Full Professorship (W3, tenured)  | 2016 |
| University of Lübeck          | Full Professorship (W3, tenured)  | 2016 |
| Saarland University           | Full Professorship (W3, tenured)  | 2016 |
| ITU University (Denmark)      | Associate Professorship (tenured) | 2013 |

## Awards and Recognitions (Selected)

|   |       |           |
|---|-------|-----------|
| Emmy Noether Fellowship                       | DFG   | 2009-2017 |
| Best Paper Award at ETAPS                     | EATCS | 2013      |
| Ph.D. Scholarship (1st ranked at Ca' Foscari) | MIUR  | 2002-2005 |

## Research Responsibilities

### Services for the Academic Community (Selected)

Regular Columnist (Security and Privacy column) of the Newsletter of the ACM SigLog.  
Member of IFIP WG 1.7 (Theoretical Foundations of Security Analysis and Design)  
Member of the ETAPS Steering Committee.  
Publicity Chair for the IEEE Computer Security Foundations Symposium

### PC Chair

|              |  |
|--------------|--|
| POST 2017    | 6th International Conference on Principles of Security and Trust                             |
| UEOP 2016    | 1st Workshop on Understanding and Enhancing Online Privacy                                   |
| FCS-FCC 2014 | Joint Workshop on Foundations of Computer Security and Formal and Computational Cryptography |
| TGC 2014     | 8th International Symposium on Trustworthy Global  |

**PC Member**

|                         |  |
|-------------------------|--|
| IEEE S&P 2016,2017      | IEEE Symposium on Security and Privacy   |
| POPL 2015,2016          | ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages  |
| CSF 2010,2012,2013,2016 | IEEE Symposium on Computer Security Foundations  |
| POST 2015,2016          | Conference on Principles of Security and Trust   |
| CCS 2015,2016,2017      | ACM Conference on Computer and Communications Security   |
| PLAS 2015               | ACM SIGPLAN Tenth Workshop on Programming Languages and Analysis for Security  |
| TPDP 2015               | Workshop on Theory and Practice of Differential Privacy  |
| Hot-Spot 2013,2014,2015 | Workshop on Hot Issues in Security Principles and Trust  |
| SAC 2014,2015           | ACM Symposium on Applied Computing, Security Track   |
| TGC 2011,2013,2015      | International Symposium on Trustworthy Global Computing  |
| ACNS 2014               | International Conference on Applied Cryptography and Network Security  |
| IEEE BigData 2013,2014  | IEEE International Conference on Big Data  |
| BigData 2014            | IEEE International Congress on Big Data  |
| ESEC/FSE 2013           | European Software Engineering Conference and ACM SIGSOFT Symposium on the Foundations of Software Engineering, New Ideas Track |
| FORTE/FMOODS 2013       | IFIP Joint International Conference on Formal Techniques for Distributed Systems   |
| GRSRD 2011,2012         | Grande Region Security and Reliability Day   |
| TACAS 2012              | International Conference on tools and algorithms for the construction and analysis of systems                                  |
| FCS 2011                | Workshop on Foundations of Computer Security   |
| ESOP 2010               | European Symposium on Programming  |
| ESORICS 2009            | European Symposium on Research in Computer Security  |
| SecCo 2008              | International Workshop on Security Issues in Concurrency   |

**Invited Speaker**

|                  |   |
|------------------|---|
| LogiCS/RiSE 2017 | LogiCS/RiSE Summer School                               |
| SCOS 2017        | Spring School on Security and Correctness in the IoT    |
| EWSCS 2016       | 21th Estonian Winter Schools in Computer Science        |
| POPL 2016        | 42th Symposium on Principles of Programming Languages   |
| GAFOE 2015       | 16th German-American Frontiers of Engineering Symposium |
| EFC 2014         | Joint EasyCrypt-F*-CryptoVerif School 2014              |
| ASA 2011         | 5th International Workshop on Analysis of Security APIs |

Other invited talks at various universities and research institutes, including KU Leuven, Johannes Kepler University, University of Graz, Loria, University of Venice, Institute for Advanced Studies Lucca, Leibniz-Zentrum für Informatik, TU München, Chalmers University, Purdue University.

## Project Experience

### Funded Projects (Selected)

**Collaborative Research Center** (PI) *Methods and Tools for Understanding and Controlling Privacy*. Funded by DFG. Years 2016-2019. ~8.4M€ for the first 4 years, out of which ~ **1M€** personal funding for the 3 (out of 13) projects:

**Emmy Noether Program** (Coordinator) *Formal Methods for the Verification and Design of Modern Cryptographic Applications*. Funded by DFG. Years 2009-2017. ~**1.2M€**. (Coordinator)

**Competence Center** (PI) *CISPA*. Funded by BMBF. Years 2011-2015, ~4M€; 2015-2019, 16M€; out of which ~ **1.1M€** personal funding.

**Individual Project:** (Coordinator) *Client-side Security Enforcement for Mobile and Web Applications*, PPP Italy-Germany Mobility Program, Funded by DAAD. Years 2016-2017. ~40K€ out of which ~20K€ personal funding for travels.

### Projects under Evaluation

**Doctoral Programm** (PI) *Logical Methods for Computer Science*. Years 2018-2021. FWF (Austria).

**ERC Consolidator Grant** (Coordinator) *Foundations and Tools for Client-Side Web Security*. Years 2018-2022. ERC.

## Academic Activities

### Teaching

**Computer Security** Core Lecture at Saarland University, WS 2010/2011, WS 2012/2013, WS 2014/2015, SS 2016.

**Privacy-Enhancing Cryptography** Advanced Lecture at Saarland University, WS 2016/2017.

**Privacy-Enhancing Technologies** Advanced Lecture at Saarland University, SS 2013, SS 2014, SS 2015, SS 2016.

**Crypto Currencies** Advanced Lecture at Saarland University, WS 2015/2016.

**Type Systems for Security Verification** Advanced Lecture, WS 2014/2015

**Web Security** Doctoral Privatissima at Saarland University, WS 2013/2014.

**Language-based Security** Advanced Lecture at Saarland University, WS 2006/2007, WS 2008/2009, WS 2013/2014.

**A Beginner's Guide to Security and Privacy** Proseminar at Saarland University, WS 2013/2014, WS 2014/2015, WS 2014/2015, WS 2015/2016.

**Hot Topics in Security and Privacy** Seminar at Saarland University, SS 2012.

**Electronic Voting Systems** Seminar at Saarland University, SS 2010, SS 2014, WS 2015/2016.

**System Security** Seminar at Saarland University, WS 2014/2015.

**Selected Topics in Information Security and Cryptography** Seminar at Saarland University, WS 2008/2009.

## **Ph.D. Students under Current Supervision**

- Clara Schneidwind
- Niklas Grinn
- Ilya Grischenko
- Manuel Reinert

## **Former Ph.D. Students and Post-Doc Assistants**

- Fabienne Eigner, Ph.D. in 2010-2016. Thesis: “A Theory of Types for Security and Privacy”, Summa cum Laude. Currently, post-doc assistant at Saarland University.
- Kim Pecina, Ph.D. in 2009-2015. Thesis: “Trustworthy and Privacy-Preserving Processing of Personal Information - Cryptographic Protocols, Constructions, and Tools”, Summa cum Laude. Currently, leader of the Peloba spin-off in IT security.
- Stefano Calzavara, post-doc in 2015. Currently, researcher at University of Venice.
- Catalin Hritcu, Ph.D. in 2007-2011. Thesis: “Union, Intersection, and Refinement Types and Reasoning about Type Disjointness for Security Protocol Analysis”, Summa cum Laude. Currently, Chargé de Recherche de 2ème classe (CR2) at INRIA.

## **Number of Supervised Theses**

PhD: 3, Master: 12, Bachelor: 3.

### **Invited Ph.D. Jury Member**

- Miriam Paiola (Inria, 2014)
- Robert Kunnemann (Inria, 2014)
- Pieter Agten (KU Leuven, 2015)
- Marco Stronati (Inria, 2015)
- Daniel Schoepe (Chalmers University, 2016)

## Publication List

### Refereed Publications

- [1] *SilentWhispers: Enforcing Security and Privacy in Decentralized Credit Networks*. Giulio Malavolta, Pedro Moreno-Sanchez, Aniket Kate, and Matteo Maffei. In Proceedings of 2017 Network and Distributed System Security Symposium (NDSS 2017)
- [2] *Maliciously Secure Multi-Client ORAM* Matteo Maffei, Giulio Malavolta, Manuel Reinert, and Dominique Schroeder. In Proceedings of the 15th International Conference on Applied Cryptography and Network Security (ACNS 2017).
- [3] *Micro-Policies for Web Session Security* Stefano Calzavara, Riccardo Focardi, Niklas Grimm, Matteo Maffei In Proceedings of 29th IEEE Computer Security Foundations Symposium (CSF 2016)
- [4] *HornDroid: Practical and Sound Security Static Analysis of Android Applications by SMT Solving*. Stefano Calzavara, Ilya Grishchenko, and Matteo Maffei. In Proceedings of 1st IEEE European Symposium on Security and Privacy (EuroS&P 2016)
- [5] *Privacy-preserving Data Aggregation with Optimal Utility Using Arithmetic SMC*. Fabienne Eigner, Aniket Kate, Matteo Maffei, Francesca Pampaloni, and Ivan Pryvalov. Book Chapter in Usable and Efficient Secure Multiparty Computation, LNCS, 2015
- [6] *Symbolic Malleable Zero-Knowledge Proofs*. Michael Backes, Fabian Bendun, Matteo Maffei, Esfandiar Mohammadi, Kim Pecina. In Proceedings of 28th IEEE Computer Security Foundations Symposium (CSF 2015)
- [7] *Privacy and Access Control for Outsourced Personal Records*. Matteo Maffei, Giulio Malavolta, Manuel Reinert, and Dominique Schröder In Proceedings of 36th IEEE Symposium on Security and Privacy (S&P 2015)
- [8] *Type-Based Verification of Electronic Voting Protocols*. Veronique Cortier, Fabienne Eigner, Steve Kremer, Matteo Maffei and Cyrille Wiedling. In Proceedings of 4th Conference on Principles of Security and Trust (POST 2015)
- [9] *Privacy Preserving Payments in Credit Networks: Enabling Trust with Privacy in Online Marketplaces*. Pedro Moreno-Sanchez, Aniket Kate, Matteo Maffei, Kim Pecina. In Proceedings of 2015 Network and Distributed System Security Symposium (NDSS 2015)
- [10] *Affine Refinement Types for Secure Distributed Programming*. Michele Bugliesi, Stefano Calzavara, Fabienne Eigner, and Matteo Maffei In ACM Transactions on Programming Languages and Systems (TOPLAS), ACM, 2015.

- [11] *Differentially Private Data Aggregation with Optimal Utility* Fabienne Eigner, Aniket Kate, Matteo Maffei, Francesca Pampaloni, and Ivan Pryvalov In Proceedings of 30th Annual Computer Security Applications Conference (ACSAC 2014), ACM, 2014.
- [12] *Brief Announcement: Towards Security and Privacy for Outsourced Data in the Multi-Party Setting.* M. Maffei, G. Malavolta, M. Reinert, D. Schroeder. In Proceedings of 33th Annual ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing (PODC 2014), ACM, pages 144-146, 2014.
- [13] *Union and Intersection Types for Secure Protocol Implementations.* M. Backes, C. Hritcu, and M. Maffei. In Journal of Computer Security, IOS Press, pages 301-353, 2014.
- [14] *AppGuard - Fine-grained Policy Enforcement for Untrusted Android Applications.* M. Backes, S. Gerling, C. Hammer, M. Maffei, and P. von Styp-Rekowsky. In Proceedings of 8th International Workshop on Data Privacy Management (DPM 2013), LNCS, pages 213-231, 2013.
- [15] *Differential Privacy by Typing in Security Protocols.* F. Eigner and M. Maffei. In Proceedings of 26th Computer Security Foundations Symposium (CSF 2013), IEEE, pages 272-286, 2013.
- [16] *Security and Privacy by Declarative Design.* M. Maffei, K. Pecina, and M. Reinert. In Proceedings of 26th Computer Security Foundations Symposium (CSF 2013), IEEE, pages 81-96, 2013.
- [17] *AppGuard - Enforcing User Requirements on Android Apps.* M. Backes, S. Gerling, C. Hammer, M. Maffei, and P. von Styp-Rekowsky. In Proceedings of 19th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2013), pages 543-548, LNCS, 2013.
- [18] *Logical Foundations of Secure Resource Management.* M. Bugliesi, S. Calzavara, F. Eigner, M. Maffei. In Proceedings of 2nd Conference on Principles of Security and Trust (POST 2013), LNCS, pages 105-125, 2013. **EATCS Best Paper Award in Theoretical Computer Science at ETAPS'13.**
- [19] *Affine Refinement Types for Authentication and Authorization.* M. Bugliesi, S. Calzavara, F. Eigner, M. Maffei. In Proceedings of 5th International Symposium on Trustworthy Global Computing (TGC 2011), LNCS, 2012.
- [20] *ObliviAd: Provably Secure and Practical Online Behavioral Advertising* M. Backes, A. Kate, M. Maffei, and K. Pecina. In Proceedings of 33rd IEEE Symposium on Security and Privacy (S&P 2012), IEEE, pages 257-271, 2012.



- [21] *Automated Synthesis of Privacy-Preserving Distributed Applications.* M. Backes, M. Maffei, and K. Pecina. In Proceedings of the 19th Annual Network and Distributed System Security Symposium (NDSS 2012), Internet Society, 2012.
- [22] *Types for Security Protocols.* R. Focardi and M. Maffei. Book Chapter in Formal Verification of Security Protocols, V. Cortier and S. Kremer editors, IOS Press, pages 143-181, 2011.
- [23] *Privacy-aware Proof-Carrying Authorization.* M. Maffei, K. Pecina. In Proceedings of 5th Workshop on Programming Languages and Analysis for Security (PLAS 2011), ACM, 2011.
- [24] *Resource-aware Authorization Policies for Statically Typed Cryptographic Protocols.* M. Bugliesi, S. Calzavara, F. Eigner, M. Maffei. In Proceedings of 24th IEEE Symposium on Computer Security Foundations (CSF 2011), IEEE, pages 83-98, 2011.
- [25] *Brief Announcement: Securing Social Networks.* M. Backes, M. Maffei, and K. Pecina. In Proceedings of the 30th Annual ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing (PODC 2011), ACM, pages 341-342, 2011.
- [26] *Union and Intersection Types for Secure Protocol Implementations.* M. Backes, C. Hritcu, and M. Maffei. In Proceedings of Theory of Security and Applications (TOSCA'11), Lecture Notes in Computer Science, pages 1-28, 2011.
- [27] *G2C: Cryptographic Protocols From Goal-Driven Specifications.* M. Backes, M. Maffei, K. Pecina, and R. Reischuk. In Proceedings of Theory of Security and Applications (TOSCA'11), Lecture Notes in Computer Science, pages 55-77, 2011.
- [28] *A Security API for Distributed Social Networks.* M. Backes, M. Maffei, and K. Pecina. In Proceedings of the 18th Annual Network and Distributed System Security Symposium (NDSS 2011), Internet Society, pages 35-52, 2011.
- [29] *Design and Verification of Anonymous Trust Protocols.* M. Backes and M. Maffei. In Proceedings of 17th International Workshop on Security Protocols, Lecture Notes in Computer Science, 2012.
- [30] *Computationally Sound Abstraction and Verification of Secure Multi-party Computations.* M. Backes, M. Maffei, and E. Mohammadi. In Proceedings of the 30th Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2010), Leibniz International Proceedings in Informatics (LIPIcs), pages 352-363, volume 8, 2010.

- [31] *Computationally Sound Verification of Source Code*. M.Backes, M. Maffei, and D. Unruh. In Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS 2010), ACM Press, pages 387-398, 2010.
- [32] *Ubiquitous Verification of Ubiquitous Systems (invited paper)*. R. Wilhelm and M. Maffei. In Proceedings of the 8th IFIP Workshop on Software Technologies for Future Embedded and Ubiquitous Systems (SEUS 2010), pages 47-58, Lecture Notes in Computer Science, 2010.
- [33] *Brief Announcement: Anonymity and Trust in Distributed Systems*. M. Backes, S. Lorenz, M. Maffei, and K. Pecina. In Proceedings of the 29th Annual ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing (PODC 2010), ACM Press, pages 237-238, 2010.
- [34] *Anonymous Webs of Trust*. M. Backes, S. Lorenz, M. Maffei, and K. Pecina. In Proceedings of the 10th Privacy Enhancing Technologies Symposium (PETS 2010), Lecture Notes in Computer Science, Springer-Verlag, pages 130-148, 2010.
- [35] *Types for Security Protocols*. R.Focardi and M. Maffei. In Electronic Notes in Theoretical Computer Science, 2009, volume 7. Abstract of invited talk at 7th International Workshop on Security Issues in Concurrency (SecCo).
- [36] *Anonymity and Censorship-Resistance in Unstructured Overlay Networks*. M. Backes, M. Hamerlik, A. Linari, M. Maffei, C. Tryfonopoulos, and G. Weikum. In Proceedings of the 16th Conference on Cooperative Information Systems (CoopIS 2009), Lecture Notes in Computer Science, Springer-Verlag, 2009.
- [37] *Achieving Security Despite Compromise Using Zero-Knowledge*. M. Backes, M. Grochulla, C. Hritcu, and M. Maffei. In Proceedings of 22nd IEEE Symposium on Computer Security Foundations (CSF 2009), pages 308-323, IEEE, 2009.
- [38] *Type-checking Zero-knowledge*. M. Backes, C. Hritcu, and M. Maffei. In Proceedings of the 15th ACM Conference on Computer and Communications Security (CCS 2008), pages 357-370, ACM Press, 2008.
- [39] *Anonymous and censorship resistant content sharing in unstructured overlays*. M. Backes, M. Hamerlik, A. Linari, M. Maffei, C. Tryfonopoulos, and G. Weikum. In Proceedings of the 27th ACM symposium on Principles of distributed computing (PODC 2008), page 429, ACM Press, 2008.
- [40] *CASPA: Causality-based Abstraction for Security Protocol Analysis*. M. Backes, S. Lorenz, M. Maffei, and K. Pecina. In Proceedings of the 20th International Conference on Computer Aided Verification (CAV 2008), pages 419-422, Volume 5123/2008 of Lecture Notes in Computer Science, Springer-Verlag, 2008.

- [41] *Automated Verification of Remote Electronic Voting Protocols*. M. Backes, C. Hritcu, and M. Maffei. In Proceedings of the 21st IEEE Symposium on Computer Security Foundations (CSF 2008), pages 195-209, IEEE, 2008.
- [42] *Zero-Knowledge in the Applied Pi-calculus and Automated Verification of the Direct Anonymous Attestation Protocol*. M. Backes, M. Maffei, and D. Unruh. In Proceedings of IEEE Symposium on Security and Privacy (S&P'08), pages 202-215. IEEE, 2008.
- [43] *Dynamic Types for Authentication*. M. Bugliesi, R. Focardi, and M. Maffei. In Journal of Computer Security, volume 15, number 6, pages 563-617, IOS Press, 2007.
- [44] *A Calculus of Challenges and Responses*. M. Backes, A. Cortesi, R. Focardi and M. Maffei. In FMSE' 07: Proceedings of the 2007 ACM workshop on Formal Methods in Security Engineering, pages 51-60, ACM Press, 2007.
- [45] *Causality-based Abstraction of Multiplicity in Security Protocols*. M. Backes, A. Cortesi, and M. Maffei. In Proceedings of the 20th IEEE Symposium on Computer Security Foundations (CSF 2007), pages 355-369, IEEE, 2007.
- [46] *Inferring authentication tags*. R. Focardi, M. Maffei, and F. Placella. In WITS '05: Proceedings of the 2005 Workshop on Issues in the Theory of Security, pages 41-49, ACM Press, 2005.
- [47] *Analysis of typed-based analyses of authentication protocols*. M. Bugliesi, R. Focardi, and M. Maffei. In Proceedings of the 18th IEEE Computer Security Foundations Workshop (CSFW 2005), pages 112-125, IEEE, 2005.
- [48] *Tags for multi-protocol authentication*. M. Maffei. In Electronic Notes in Theoretical Computer Science, volume 5, pages 55-63, 2005.
- [49]  *$\rho$ -spi calculus at work: Authentication case studies*. R. Focardi and M. Maffei. In Electronic Notes in Theoretical Computer Science, volume 99, pages 267-293, 2004.
- [50] *Authenticity by tagging and typing*. M. Bugliesi, R. Focardi, and M. Maffei. In FMSE '04: Proceedings of the 2004 ACM workshop on Formal methods in security engineering, pages 1-12, ACM Press, 2004.
- [51] *Compositional analysis of authentication protocols*. M. Bugliesi, R. Focardi, and M. Maffei. In Proceedings of European Symposium on Programming (ESOP 2004), volume 2986 of Lecture Notes in Computer Science, pages 140-154, Springer-Verlag, 2004.
- [52] *Principles for entity authentication*. M. Bugliesi, R. Focardi, and M. Maffei. In Proceedings of the 5th International Conference Perspectives of System Informatics (PSI 2003), volume 2890 of Lecture Notes in Computer Science, pages 294-307, Springer-Verlag, 2003.

## Edited Publications

- [53] *Proceedings of the 9th International Symposium on Trustworthy Global Computing (TGC 2014)*. M. Maffei and E. Tuosto. Volume 8902 of Lecture Notes in Computer Science, Springer-Verlag, 2014.
- [54] *Security & privacy column*. Preface (M. Maffei). Volume 1, Issue 1, ACM SIGLOG News, ACM, 2014.
- [55] *Security & privacy column*. Preface (M. Maffei), Formal verification of E-voting: solutions and challenges (V. Cortier), The Joint EasyCrypt-F\*-CryptoVerif School 2014 (C. Hritcu) Volume 2, Issue 1, ACM SIGLOG News, ACM, 2015.
- [56] *Security & privacy column*. Preface (M. Maffei), Location privacy via geoindistinguishability (K. Chatzikokolakis, C. Palamidessi, and M. Stronati) Volume 2, Issue 3, ACM SIGLOG News, ACM, 2015.
- [57] *Security & privacy column*. Preface (M. Maffei), Type Systems for Information Flow Control: The Question of Granularity (Vineet Rajani, Iulia Bastys, Willard Rafnsson, and Deepak Garg) Volume 4, Issue 1, ACM SIGLOG News, ACM, 2017.

## Refereed Informal Publications

- [58] *Whispers: A Distributed Architecture for Enforcing Privacy in Credit Networks* Aniket Kate, Matteo Maffei, Giulio Malavolta, Pedro Moreno-Sanchez. In Proceedings of 9th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs 2016).
- [59] *Privacy-preserving Data Aggregation with Optimal Utility Using Arithmetic SMC*. Fabienne Eigner, Aniket Kate, Matteo Maffei, Francesca Pampaloni, and Ivan Pryvalov. In Proceedings of Workshop on Usable and Efficient Secure Multiparty Computation, 2015.
- [60] *Differential Privacy by Typing in Security Protocols*. F. Eigner and M. Maffei In Proceedings of 1st Workshop on Hot Issues in Security Principles and Trust (HotSpot 2013)
- [61] *Security and Privacy by Declarative Design*. M. Maffei, K. Pecina, and M. Reinert. In Proceedings of 1st Workshop on Hot Issues in Security Principles and Trust (HotSpot 2013)
- [62] *ObliviAd: Provably Secure and Practical Online Behavioral Advertising*. M. Backes, A. Kate, M. Maffei, and K. Pecina. In Proceedings of the Provable Privacy Workshop, 2012.

- [63] *A Security API for Distributed Social Networks*. M. Backes, M. Maffei, and K.Pecina. In Proceedings of the 5th Workshop on Analysis of Security APIs (ASA-5), 2011.
- [64] *Computationally Sound Abstraction and Verification of Secure Multi-party Computations*. M. Backes, M. Maffei, and E. Mohammadi. In Proceedings of the Seventh Workshop on Formal and Computational Cryptography FCC 2011, 2011.
- [65] *Type-checking Implementations of Protocols Based on Zero-knowledge Proofs*. M. Backes, C. Hritcu, M. Maffei. In Proceedings of the Workshop on Foundations of Computer Security (FCS'09).
- [66] *Computational soundness of RCF*. M. Backes and M. Maffei and D. Unruh. In Proceedings of the Workshop on Formal and Computational Cryptography (FCC'09).
- [67] *Achieving Security Despite Compromise Using Zero-Knowledge*. M. Backes, M. Grochulla, C. Hritcu, and M. Maffei. In Proceedings of 9th International Workshop on Issues in the Theory of Security (WITS 2009).
- [68] *Zero-Knowledge in the Applied Pi-calculus*. M. Backes, M. Maffei, and D. Unruh. In Proceedings of Dagstuhl Seminar: Formal Protocol Verification Applied, 2008.
- [69] *Type-checking Zero-knowledge*. M. Backes, S. Lorenz, and M. Maffei. In Proceedings of 8th International Workshop on Issues in the Theory of Security (WITS 2008).
- [70] *Abstracting Multiplicity in Cryptographic Protocols*. M. Backes, A. Cortesi and M. Maffei. In Proceedings of 7th International Workshop on Issues in the Theory of Security (WITS 2007), pages 132-147, 2007.
- [71] *A Calculus of Challenges and Responses*. M. Backes, A. Cortesi, R. Focardi and M. Maffei. In Proceedings of the 7th International Workshop on Issues in the Theory of Security (WITS 2007), pages 101-116, 2007.

## Ph.D. Thesis

- [72] *Dynamic Typing for Cryptographic Protocols*. M. Maffei Computer Science Department, University of Venice, March 2006.