UNIVERSITY OF CALIFORNIA,
IRVINE

Sharing Sensitive Information with Privacy

DISSERTATION

submitted in partial satisfaction of the requirements
for the degree of

DOCTOR OF PHILOSOPHY

in Networked Systems

by

Emiliano De Cristofaro

Dissertation Committee:
Professor Gene Tsudik, Chair
Professor Claude Castelluccia
Professor Athina Markopoulou

2011

To Eve — without you, none of this would be possible

Contents

List of Figures vi

List of Tables viii

Acknowledgments ix

Curriculum Vitae xi

Abstract of the Dissertation xv

1 Introduction 1
- 1.1 Sharing Sensitive Information with Privacy . . . 1
- 1.2 Cryptographic Protocols and Open Problems . . . 3
  - 1.2.1 Protocols for Implicit Authentication and Oblivious Information Transfer . 3
  - 1.2.2 Some Open Problems . . . 5
- 1.3 Practical Aspects of Privacy-Preserving Sharing of Sensitive Information . . . 7
- 1.4 Summary of Contributions . . . 8
- 1.5 Organization . . . 8
- 1.6 Collaboration . . . 9

2 Preliminaries 11
- 2.1 Notation . . . 11
- 2.2 Cryptosystems . . . 12
- 2.3 Assumptions . . . 13
- 2.4 Tools . . . 14
- 2.5 Adversarial Models . . . 15

3 Related Work 17
- 3.1 Cryptographic Protocols for Implicit Authentication . . . 17
- 3.2 Protocols for Oblivious Information Transfer . . . 18
- 3.3 Private Set Intersection . . . 19
  - 3.3.1 Available PSI Protocols . . . 19
  - 3.3.2 Authorized Private Set Intersection . . . 23
  - 3.3.3 Size-Hiding Protocols . . . 24

3.3.4 Additional Constructs . . . 24

4 Transferring Confidential Information based on Implicit Signature Verification 26

4.1 Introduction & Motivation . . . 26

4.2 Preliminaries . . . 27

4.2.1 Players . . . 28

4.2.2 PPIT Algorithms . . . 28

4.2.3 Security & Privacy Requirements . . . 28

4.3 RSA-PPIT . . . 30

4.4 Schnorr-PPIT . . . 32

4.5 IBE-PPIT . . . 34

4.6 Discussion . . . 36

4.6.1 Unlinkability and Forward Security . . . 36

4.6.2 Batched PPIT for Multiple Client Authorizations . . . 38

4.6.3 Performance Analysis . . . 39

4.7 Proofs . . . 40

4.7.1 RSA-PPIT Proofs . . . 40

4.7.2 Schnorr-PPIT Proofs . . . 43

4.7.3 IBE-PPIT . . . 44

5 Linear-Complexity Private Set Intersection Protocols 45

5.1 From PPIT to PSI, via APSI . . . 45

5.2 Definitions . . . 46

5.3 Designing Efficient Private Set Intersection Protocols . . . 47

5.3.1 Baseline: APSI from PPIT . . . 47

5.3.2 APSI with Linear Costs . . . 49

5.3.3 Deriving Efficient PSI . . . 50

5.4 Efficient PSI based on RSA Blind-Signatures . . . 52

5.5 Realizing PSI-DT and APSI-DT . . . 55

5.6 Performance Evaluation . . . 56

6 Private Set Intersection with Linear Complexities Secure in the Malicious Model 58

6.1 Security in the Malicious Model for Private Set Intersection . . . 58

6.2 Linear-Complexity APSI Secure in the Malicious Model . . . 60

6.3 Deriving Linear-Complexity PSI Secure in the Malicious Model . . . 66

6.4 Efficiency . . . 71

7 Size-Hiding Private Set Intersection 72

7.1 Why Size Matters? . . . 72

7.2 SHI-PSI Definitions . . . 74

7.3 SHI-PSI Construction . . . 75

7.3.1 Protocol Description . . . 76

7.3.2 Protocol Complexity . . . 79

7.4 Extensions . . . 81

7.4.1 Linear-Complexity SHI-PSI . . . 81

7.4.2 SHI-PSI with Data Transfer 82

8 Building a Toolkit for Privacy-preserving Sharing of Sensitive Information 84

8.1 Introduction 84
8.2 Preliminaries 85
8.2.1 Syntax & Notation 85
8.2.2 Privacy Requirements 85
8.2.3 Pre-Distribution in PSI 87
8.2.4 Related Primitives 87
8.3 A Strawman Approach 88
8.4 PPSSI Toolkit 89
8.4.1 The `Token` Function 89
8.4.2 Database Encryption with counters 91
8.4.3 Lookup with counters 93
8.4.4 Discussion 94
8.4.5 Performance Evaluation 95

9 Private Interest Sharing and Activity Scheduling for Smartphones 97

9.1 Introduction 97
9.1.1 Motivation 98
9.1.2 Roadmap 99
9.2 Preliminaries 99
9.2.1 Players 100
9.2.2 Server-Assisted Privacy-preserving Computation 100
9.2.3 Trust Assumptions 101
9.3 Sharing Interests with Privacy 101
9.3.1 PIS Protocol Specification 103
9.3.2 Privacy of PIS 105
9.4 Private Scheduling 105
9.5 PrivSched-v1 106
9.5.1 PrivSched-v1 Protocol Specification 107
9.5.2 Privacy of PrivSched-v1 111
9.6 PrivSched-v2 111
9.6.1 PrivSched-v2 Protocol Specification 112
9.6.2 Complexity of PrivSched-v2 116
9.6.3 Privacy of PrivSched-v2 116
9.7 Symmetric-Key Private Scheduling: S-PrivSched 116
9.7.1 S-PrivSched Protocol Specification 117
9.7.2 Privacy of S-PrivSched 119
9.8 Performance Analysis 119
9.9 Related Primitives 121

10 Conclusion and Open Problems 124

Bibliography 126

A Performance Evaluation of Private Set Intersection Protocols 138

List of Figures

3.1 High-level view of Private Set Intersection protocols based on Oblivious Pseudo-Random Functions. 21

4.1 Our RSA-PPIT instantiation. 31
4.2 Our Schnorr-PPIT instantiation. 33
4.3 Our IBE-PPIT instantiation. 35

5.1 APSI protocol derived from RSA-PPIT. 48
5.2 New APSI protocol with linear complexities. 49
5.3 PSI protocol with linear complexities. 51
5.4 Efficient PSI protocol based on RSA Blind Signatures. 53

6.1 APSI protocol with linear complexities secure in the malicious model, in ROM, under the RSA and DDH assumptions. 61
6.2 PSI protocol with linear complexities secure in the malicious model, in ROM, under the DDH assumption. 67

7.1 Proposed SHI-PSI protocol. 77
7.2 Tree-based strategy to reduce client computation. 80
7.3 New (linear-complexity) SHI-PSI protocol. 81

8.1 Outline of our PPSSI construction. 90
8.2 Oblivious computation of `Token` using DT10-1. 91
8.3 Oblivious computation of `Token` using DT10-APSI. 91
8.4 `Token` Oblivious Computation. 96
8.5 Lookup-Table Encryption (line 8-15 of Algorithm 1). 96
8.6 Record-level Encryption (line 1-6 of Algorithm 1). 96
8.7 Comparison between our PPSSI construction and GR-PIR [73]. 96

9.1 Our Private Interest Sharing (PIS) Protocol. 103
9.2 Our PrivSched-v1 Protocol. 109
9.3 Our PrivSched-v2 Protocol. 113
9.4 Our S-PrivSched Protocol. 118
9.5 Initiator 121
9.6 Each participant 121

9.7 Server 121

A.1 Symmetric key en-/de-cryption performance. 141
A.2 Server pre-computation overhead. 141
A.3 Client online computation w.r.t. client set size. 142
A.4 Client online computation w.r.t. server set size. 142
A.5 Server online computation w.r.t. client set size. 142
A.6 Server online computation w.r.t. server set size. 142
A.7 Bandwidth consumption w.r.t. client set size. 142
A.8 Bandwidth consumption w.r.t. server set size. 142

List of Tables

4.1 Performance Comparison of PPIT Instantiations. 40

5.1 Performance Comparison of PSI and APSI protocols secure in semi-honest model. 56

6.1 Performance Comparison of PSI and APSI protocols in the malicious model. . . . 71

8.1 Notation used in Chapter 8. 86
8.2 `Token` definition for DT10-1 and DT10-APSI. 90

A.1 Implemented PSI-DT and APSI-DT protocols. 139

Acknowledgments

I would like to express my sincere appreciation to all the people who helped me during my doctoral work.

I am extremely grateful to Gene Tsudik – not only for the time, patience, and commitment dedicated to advising me, but also for sparkling my curiosity and serving as a precious source of inspiration. He has pushed me to improve myself both as a researcher and as a (relatively) young man (not to mention as a tentative runner, cigar smoker, and food enthusiast).

I would also like to express my gratitude to my doctoral committee for their encouragement and precious comments.

I am indebted to a number of exceptional people and researchers, whose teaching and feedback have tremendously contributed to my research education: Carlo Blundo, Jihye Kim, Stanislaw Jarecki, Claude Castelluccia, Giuseppe Ateniese – just to mention a few. It is not easy to explain how much I learned from them.

I am very thankful to my internship supervisors and co-workers, in particular, Dirk Westhoff, Jens-Matthias Bohli, Claude Castelluccia, Imad Aad, Valtteri Niemi.

I have also been very lucky to work with other great folks: Mishari Al Mishari, Enzo Auletta, Pierre Baldi, Roberta Baronio, Aniello Del Sorbo, Xuhua Ding, Roberto Di Pietro, Anthony Durussel, Karim El Defrawy, Aurelien Francillon, Julien Freudiger, Clemente Galdi, Paolo Gasti, Dali Kaafar, Yanbin Lu, Mark Manulis, Daniele Perito, Pino Persiano, Bertram Poettering, Rino Raimato, Andrei Serjantov, Claudio Soriente, Ivan Visconti.

I extend many thanks also to all the researchers that have invited me for talks, seminars, and research visits: Filipe Beato, Claudia Diaz, and Markulf Kohlweiss from KU Leuven, Julien Freudiger and Jean-Pierre Hubaux from EPFL, Srdjan Čapkun from ETH, Cynthia Kuo from NRC Palo Alto, Rafi Ostrovski and Ivan Visconti from UCLA, Xuhua Ding from SMU, Bryan Parno and David Molnar from MSR Redmond, Tomas Toft and Carmit Hazay from Aarhus University, Mark Manulis from TU Darmstadt: the fun of traveling as well as the feedback from different environments and communities have intensely motivated me.

Last, but not least, thanks to all the friends of the SPROUT lab not mentioned above (Di Ma, Ivan Martinovic, Einar Mykletun, Rishab Nithyanand, Gabriele Oligeri, Kasper Bonne Rasmussen, John Solis, Ersin Uzun), to the "Italian community" at UCI, to my surfing buddies Julius, JoJo, and Juris, to my roommates Adam, Charline, Clara, Claudio, Fabio, Joshua, Leo, Paco, Roby, Samia, Sandra, and to all the great people that I have met along the way: you have a great "responsibility" in making these past four years a lot of fun for me.

Curriculum Vitae

EMILIANO DE CRISTOFARO

EDUCATION

2007 – Present *University of California, Irvine*, Ph.D. Candidate, Networked Systems, GPA 3.99

2000 – 2005 *Università di Salerno, Italy*, Laurea (5-year undergraduate program) in Computer Science, Summa Cum Laude

RESEARCH EXPERIENCE

6/2010 - 10/2010 *Nokia Research Center, Lausanne, Switzerland*, PhD Intern

9/2009 - 12/2009 *INRIA Rhône Alpes, France*, Research Visitor

1/2009 - 2/2009 *Singapore Management University*, Research Visitor

6/2008 - 9/2008 *NEC Europe Labs, Heidelberg, Germany*, PhD Intern

TEACHING EXPERIENCE

3/2011 - 6/2011 *University of California, Irvine*, Teaching Assistant: Network Security

2/2006 - 7/2006 *Università di Salerno*, Teaching Assistant: Network Programming.

REFEREED CONFERENCE PUBLICATIONS

1. P. Baldi, R. Baronio, E. De Cristofaro, P. Gasti, G. Tsudik. *Countering GATTACA: Efficient and Secure Testing of Fully-Sequenced Human Genomes.* 18th ACM Conference on Computer and Communications Security (CCS'11), Chicago, Illinois, October 2011.
2. C. Castelluccia, E. De Cristofaro, A. Francillon, M.A. Kafaar. *EphPub: Toward Robust Ephemeral Publishing.* 19th IEEE International Conference on Network Protocols, Vancouver, Canada, October 2011.

3. E. De Cristofaro, Y. Lu, G. Tsudik. *Efficient Techniques for Privacy-Preserving Sharing of Sensitive Information.* 4th International Conference on Trust and Trustworthy Computing (TRUST'11), Pittsburgh, Pennsylvania, June 2011.
4. E. De Cristofaro, C. Soriente. *PEPSI: Privacy Enhancing Participatory Sensing Infrastructure.* 4th ACM Conference on Wireless Security (WiSec'11), Hamburg, Germany, June 2011.
5. E. De Cristofaro, M. Manulis, B. Poettering. *Private Discovery of Common Social Contacts.* 9th International Conference on Applied Cryptography and Network Security (ACNS'11), Nerja, Spain, June 2011.
6. E. De Cristofaro, A. Durussel, I. Aad. *Reclaiming Privacy for Smartphone Applications.* 9th IEEE International Conference on Pervasive Computing and Communications (PerCom'11), Seattle, Washington, March 2011.
7. G. Ateniese, E. De Cristofaro, G. Tsudik. *(If) Size Matters: Size-Hiding Private Set Intersection.* 14th IACR International Conference on Practice and Theory of Public Key Cryptography (PKC'11), Taormina, Italy, March 2011.
8. E. De Cristofaro, J. Kim, G. Tsudik. *Linear-Complexity Private Set Intersection Protocols Secure in Malicious Model.* 17th IACR International Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt'10), Singapore, December 2010.
9. C. Castelluccia, E. De Cristofaro, D. Perito. *Private Information Disclosure from Web Searches.* 10th Privacy Enhancing Technologies Symposium (PETS'10), Berlin, Germany, July 2010.
10. E. De Cristofaro and G. Tsudik. *Practical Private Set Intersection Protocols with Linear Complexity.* 14th International Conference on Financial Cryptography and Data Security (FC'10), Tenerife, Spain, January 2010.
11. V. Auletta, C. Blundo, A. De Caro, E. De Cristofaro, G. Persiano, I. Visconti. *Increasing Privacy Threats in the Cyberspace: the Case of Italian e-Passports.* 1st Workshop on Lightweight Cryptography for Resource-Constrained Devices (WLC'10), Tenerife, Spain, January 2010.
12. E. De Cristofaro, S. Jarecki, J. Kim, G. Tsudik. *Privacy-preserving Policy-based Information Transfer.* 9th Privacy Enhancing Technologies Symposium (PETS'09), Seattle, Washington, August 2009.

13. E. De Cristofaro, X. Ding, G. Tsudik. *Privacy-preserving Querying in Sensor Networks.* 18th IEEE International Conference on Computer Communications and Networks (ICCCN’09), San Francisco, California, August 2009.

14. E. De Cristofaro, J.M. Bohli, D. Westhoff. *FAIR: Fuzzy-based Aggregation providing In-network Resilience for real-time WSNs.* 2nd ACM Conference on Wireless Network Security (WiSec’09), Zurich, Switzerland, March 2009.

15. C. Blundo, E. De Cristofaro, A. Del Sorbo, C. Galdi, G. Persiano. *A Distributed Implementation of the Certified Information Access Service.* 13th European Symposium on Research in Computer Security (ESORICS’08), Malaga, Spain, October 2008.

16. C. Blundo, E. De Cristofaro, C. Galdi, G. Persiano. *Validating Orchestration of Web Services with BPEL and Aggregate Signatures.* 6th IEEE European Conference on Web Services (ECOWS’08), Dublin, Ireland, November 2008.

17. E. De Cristofaro. *A Secure and Privacy-Protecting Aggregation Scheme for Sensor Networks.* 8th IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM’07), Helsinki, Finland, June 2007.

18. V. Auletta, C. Blundo, E. De Cristofaro. *HTTP over Bluetooth: a J2ME experience.* IARIA International Journal On Advances in Telecommunications. Vol. 1, 2007.

19. V. Auletta, C. Blundo, E. De Cristofaro, S. Cimato, G. Raimato. *Authenticated Web Services: A WS-Security Based Implementation.* 2nd IFIP International Conference on New Technologies, Mobility, and Security (NTMS’07), Paris, France, May 2007.

20. C. Blundo and E. De Cristofaro. *A Bluetooth-based JXME infrastructure.* 9th International Symposium on Distributed Objects, Middleware, and Applications (DOA’07), Vilamoura, Portugal, November 2007.

21. V. Auletta, C. Blundo, E. De Cristofaro. *A J2ME transparent middleware to support HTTP connections over Bluetooth.* 2nd IARIA International Conference on Systems and Network Communications (ICSNC’07), Cap Esterel, France, August 2007.

22. V. Auletta, C. Blundo, E. De Cristofaro, G. Raimato. *Performance Evaluation for Web Services invocation over Bluetooth.* 9th ACM Conference on Modeling, Analysis, and Simulation of Wireless and Mobile Systems (MSWiM’06), Torremolinos, Spain, October 2006.

23. V. Auletta, C. Blundo, E. De Cristofaro, G. Raimato. *A lightweight framework for Web Services invocation over Bluetooth.* 4th IEEE International Conference on Web Services (ICWS'06), Chicago, Illinois, September 2006.

INTERNATIONAL JOURNAL PUBLICATIONS

1. E. De Cristofaro and J. Kim. *Some like it private: Sharing Confidential Information based on Oblivious Authorization.* IEEE Security and Privacy, July-August, 2010.

HONORS AND AWARDS

Fall 2010	*Dissertation Fellowship – UC Irvine*
2007 - 2011	*Dean's Fellowship – Donald Bren School of Information and Computer Science, UC Irvine*