

1. Record Nr.	UNISA996199683803316
Titolo	Privacy in Statistical Databases [[electronic resource]] : UNESCO Chair in Data Privacy, International Conference, PSD 2014, Ibiza, Spain, September 17-19, 2014. Proceedings / / edited by Josep Domingo-Ferrer
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2014
ISBN	3-319-11257-0
Edizione	[1st ed. 2014.]
Descrizione fisica	1 online resource (XII, 367 p. 68 illus.)
Collana	Information Systems and Applications, incl. Internet/Web, and HCI ; ; 8744
Disciplina	005.8
Soggetti	Application software Database management Computer security Data encryption (Computer science) Computers and civilization Computer Appl. in Administrative Data Processing Database Management Systems and Data Security Cryptology Computers and Society
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Tabular Data Protection -- Enabling Statistical Analysis of Suppressed Tabular Data -- Assessing the Information Loss of Controlled Adjustment Methods in Two-Way Tables -- Further Developments with Perturbation Techniques to Protect Tabular Data -- Comparison of Different Sensitivity Rules for Tabular Data and Presenting a New Rule -- The Interval Rule -- Pre-tabular Perturbation with Controlled Tabular Adjustment: Some Considerations -- Measuring Disclosure Risk with Entropy in Population Based Frequency Tables -- A CTA Model Based on the Huber Function -- Microdata Masking Density Approximant Based on Noise Multiplied Data -- Reverse Mapping to Preserve the

Marginal Distributions of Attributes in Masked Microdata -- JPEG-Based Microdata Protection -- Protection Using Privacy Models -- Improving the Utility of Differential Privacy via Univariate Microaggregation -- Differentially Private Exponential Random Graphs -- km-Anonymity for Continuous Data Using Dynamic Hierarchies -- Differentially-Private Logistic Regression for Detecting Multiple-SNP Association in GWAS Databases -- Synthetic Data -- Disclosure Risk Evaluation for Fully Synthetic Categorical Data -- v-Dispersed Synthetic Data Based on a Mixture Model with Constraints -- Nonparametric Generation of Synthetic Data for Small Geographic Areas -- Using Partially Synthetic Data to Replace Suppression in the Business Dynamics Statistics: Early Results -- Synthetic Longitudinal Business Databases for International Comparisons -- Record Linkage -- A Comparison of Blocking Methods for Record Linkage -- Probabilistic Record Linkage for Disclosure Risk Assessment -- Hierarchical Linkage Clustering with Distributions of Distances for Large-Scale Record Linkage -- Remote Access -- Comparison of Two Remote Access Systems Recently Developed and Implemented in Australia -- Privacy-Preserving Protocols -- Towards Secure and Practical Location Privacy through Private Equality Testing -- Case Studies -- Controlled Shuffling, Statistical Confidentiality and Microdata Utility: A Successful Experiment with a 10% Household Sample of the 2011 Population Census of Ireland for the IPUMS-International Database -- Balancing Confidentiality and Usability: Protecting Sensitive Data in the Case of Inward Foreign Affiliates Statistics (FATS) -- Applicability of Confidentiality Methods to Personal and Business Data.

Sommario/riassunto

This book constitutes the refereed proceedings of the International Conference on Privacy in Statistical Databases, PSD 2014, held in Ibiza, Spain in September 2014 under the sponsorship of the UNESCO chair in Data Privacy. The 27 revised full papers presented were carefully reviewed and selected from 41 submissions. The scope of the conference is on following topics: tabular data protection, microdata masking, protection using privacy models, synthetic data, record linkage, remote access, privacy-preserving protocols, and case studies.

2. Record Nr.	UNINA9910828065603321
Autore	Delgrossi Luca
Titolo	Vehicle safety communications : protocols, security, and privacy / / Luca Delgrossi, Tao Zhang
Pubbl/distr/stampa	Hoboken, : Wiley, 2012
ISBN	9786613911438 9781118452196 1118452194 9781283598989 1283598981 9781118452189 1118452186 9781118452219 1118452216
Edizione	[1st ed.]
Descrizione fisica	1 online resource (400 p.)
Collana	Wiley series on information and communication technology
Classificazione	TEC009020
Altri autori (Persone)	ZhangTao <1962->
Disciplina	629.2/76
Soggetti	Vehicular ad hoc networks (Computer networks) - Safety measures Automobiles - Safety appliances Automobiles - Collision avoidance systems
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	-- Foreword xv / Ralf G. Herrtwich -- Foreword xvii / Flavio Bonomi -- Foreword xix / Adam Drobot -- Preface xxi -- Acknowledgments xxv -- 1 Traffic Safety 1 -- 1.1 Traffic Safety Facts 1 -- 1.1.1 Fatalities 2 -- 1.1.2 Leading Causes of Crashes 3 -- 1.1.3 Current Trends 5 -- 1.2 European Union 5 -- 1.3 Japan 7 -- 1.4 Developing Countries 7 -- References 8 -- 2 Automotive Safety Evolution 10 -- 2.1 Passive Safety 10 -- 2.1.1 Safety Cage and the Birth of Passive Safety 10 -- 2.1.2 Seat Belts 11 -- 2.1.3 Air Bags 11 -- 2.2 Active Safety 12 -- 2.2.1 Antilock Braking System 12 -- 2.2.2 Electronic Stability Control 13 -- 2.2.3 Brake Assist 13 -- 2.3 Advanced Driver Assistance Systems 14 -- 2.3.1 Adaptive Cruise Control 15 -- 2.3.2 Blind Spot Assist 16 -- 2.3.3 Attention Assist 16 -- 2.3.4 Precrash Systems 16 -- 2.4 Cooperative

Safety	17	--	References	18	--	3 Vehicle Architectures	20	--	3.1
Electronic Control Units	20	--	3.2 Vehicle Sensors	21	--	3.2.1 Radars			
	21	--	3.2.2 Cameras	21	--	3.3 Onboard Communication Networks	22		
		--	3.3.1 Controller Area Network	23	--	3.3.2 Local Interconnect Network	23	--	3.3.3 FlexRay
			24	--	3.3.4 Media Oriented Systems Transport	24	--	3.3.5 Onboard Diagnostics	24
				--	3.4 Vehicle Data	25			
				--	3.5 Vehicle Data Security	26	--	3.6 Vehicle Positioning	27
				--	3.6.1 Global Positioning System	27	--	3.6.2 Galileo	29
				--	3.6.3 Global Navigation Satellite System	29	--	3.6.4 Positioning Accuracy	30
				--	References	30	--	4 Connected Vehicles	32
				--	4.1 Connected Vehicle Applications	32	--	4.1.1 Hard Safety Applications	32
				--	4.1.2 Soft Safety Applications	33	--	4.1.3 Mobility and Convenience Applications	33
				--	4.2 Uniqueness in Consumer Vehicle Networks	34	--	4.3 Vehicle Communication Modes	36
				--	4.3.1 Vehicle-to-Vehicle Local Broadcast	36	--	4.3.2 V2V Multihop Message Dissemination	37
				--	4.3.3 Infrastructure-to-Vehicle Local Broadcast	38	--	4.3.4 Vehicle-to-Infrastructure Bidirectional Communications	39
				--	4.4 Wireless Communications Technology for Vehicles	39	--	References	42
				--	5 Dedicated Short-Range Communications	44	--	5.1 The 5.9 GHz Spectrum	44
				--	5.1.1 DSRC Frequency Band Usage	45	--	5.1.2 DSRC Channels	45
				--	5.1.3 DSRC Operations	46	--	5.2 DSRC in the European Union	46
				--	5.3 DSRC in Japan	47	--	5.4 DSRC Standards	48
				--	5.4.1 Wireless Access in Vehicular Environments	48	--	5.4.2 Wireless Access in Vehicular Environments Protocol Stack	48
				--	5.4.3 International Harmonization	50	--	References	50
				--	6 WAVE Physical Layer	52	--	6.1 Physical Layer Operations	52
				--	6.1.1 Orthogonal Frequency Division Multiplexing	52	--	6.1.2 Modulation and Coding Rates	53
				--	6.1.3 Frame Reception	54	--	6.2 PHY Amendments	55
				--	6.2.1 Channel Width	56	--	6.2.2 Spectrum Masks	56
				--	6.2.3 Improved Receiver Performance	57	--	6.3 PHY Layer Modeling	57
				--	6.3.1 Network Simulator Architecture	58	--	6.3.2 RF Model	59
				--	6.3.3 Wireless PHY	61	--	References	62
				--	7 WAVE Media Access Control Layer	64	--	7.1 Media Access Control Layer Operations	64
				--	7.1.1 Carrier Sensing Multiple Access with Collision Avoidance	64	--	7.1.2 Hidden Terminal Effects	65
				--	7.1.3 Basic Service Set	66	--	7.2 MAC Layer Amendments	66
				--	7.3 MAC Layer Modeling	67	--	7.3.1 Transmission	68
				--	7.3.2 Reception	68	--	7.3.3 Channel State Manager	68
				--	7.3.4 Back-Off Manager	69	--	7.3.5 Transmission Coordination	70
				--	7.3.6 Reception Coordination	71	--	7.4 Overhauled ns-2 Implementation	72
				--	References	74	--	8 DSRC Data Rates	75
				--	8.1 Introduction	75	--	8.2 Communication Density	76
				--	8.2.1 Simulation Study	77	--	8.2.2 Broadcast Reception Rates	78
				--	8.2.3 Channel Access Delay	81	--	8.2.4 Frames Reception Failures	83
				--	8.3 Optimal Data Rate	85	--	8.3.1 Modulation and Coding Rates	85
				--	8.3.2 Simulation Study	86	--	8.3.3 Simulation Matrix	87
				--	8.3.4 Simulation Results	88	--	References	91
				--	9 WAVE Upper Layers	93	--	9.1 Introduction	93
				--	9.2 DSRC Multichannel Operations	94	--	9.2.1 Time Synchronization	94
				--	9.2.2 Synchronization Intervals	95	--	9.2.3 Guard Intervals	96
				--	9.2.4 Channel Switching	96	--	9.2.5 Channel Switching State Machine	96
				--	9.3 Protocol Evaluation	97	--	9.3.1 Simulation Study	98
				--	9.3.2 Simulation Scenarios	99	--	9.3.3 Simulation Results	99
				--	9.3.4 Protocol Enhancements	102	--	9.4 WAVE Short Message Protocol	103
				--	References	104	--	10 Vehicle-to-Infrastructure Safety Applications	106
				--	10.1 Intersection Crashes	106	--	10.2 Cooperative Intersection Collision Avoidance System for Violations	107
				--	10.2.1 CICAS-V Design	107	--	10.2.2 CICAS-V Development	110
				--	10.2.3 CICAS-V Testing	116	--	10.3 Integrated Safety Demonstration	118
				--	10.3.1 Demonstration Concept	118	--		

10.3.2 Hardware Components	120
10.3.3 Demo Design	121
References	124
11 Vehicle-to-Vehicle Safety Applications	126
11.1 Cooperation among Vehicles	126
11.2 V2V Safety Applications	127
11.3 V2V Safety Applications Design	128
11.3.1 Basic Safety Messages	129
11.3.2 Minimum Performance Requirements	129
11.3.3 Target Classification	131
11.3.4 Vehicle Representation	132
11.3.5 Sample Applications	133
11.4 System Implementation	135
11.4.1 Onboard Unit Hardware Components	135
11.4.2 OBU Software Architecture	135
11.4.3 Driver / Vehicle Interface	137
11.5 System Testing	138
11.5.1 Communications Coverage and Antenna Considerations	138
11.5.2 Positioning	139
References	140
12 DSRC Scalability	141
12.1 Introduction	141
12.2 DSRC Data Traffic	142
12.2.1 DSRC Safety Messages	142
12.2.2 Transmission Parameters	143
12.2.3 Channel Load Assessment	144
12.3 Congestion Control Algorithms	145
12.3.1 Desired Properties	145
12.3.2 Transmission Power Adjustment	146
12.3.3 Message Rate Adjustment	147
12.3.4 Simulation Study	148
12.4 Conclusions	148
References	149
13 Security and Privacy Threats and Requirements	151
13.1 Introduction	151
13.2 Adversaries	151
13.3 Security Threats	152
13.3.1 Send False Safety Messages Using Valid Security Credentials	152
13.3.2 Falsely Accuse Innocent Vehicles	153
13.3.3 Impersonate Vehicles or Other Network Entities	153
13.3.4 Denial-of-Service Attacks Specific to Consumer Vehicle Networks	154
13.3.5 Compromise OBU Software or Firmware	155
13.4 Privacy Threats	155
13.4.1 Privacy in a Vehicle Network	155
13.4.2 Privacy Threats in Consumer Vehicle Networks	156
13.4.3 How Driver Privacy can be Breached Today	158
13.5 Basic Security Capabilities	159
13.5.1 Authentication	159
13.5.2 Misbehavior Detection and Revocation	160
13.5.3 Data Integrity	160
13.5.4 Data Confidentiality	160
13.6 Privacy Protections Capabilities	161
13.7 Design and Performance Considerations	161
13.7.1 Scalability	162
13.7.2 Balancing Competing Requirements	162
13.7.3 Minimal Side Effects	163
13.7.4 Quantifiable Levels of Security and Privacy	163
13.7.5 Adaptability	163
13.7.6 Security and Privacy Protection for V2V Broadcast	163
13.7.7 Security and Privacy Protection for Communications with Security Servers	164
References	165
14 Cryptographic Mechanisms	167
14.1 Introduction	167
14.2 Categories of Cryptographic Mechanisms	167
14.2.1 Cryptographic Hash Functions	168
14.2.2 Symmetric Key Algorithms	169
14.2.3 Public Key (Asymmetric Key) Algorithms	170
14.3 Digital Signature Algorithms	172
14.3.1 The RSA Algorithm	172
14.3.2 The DSA Algorithm	178
14.3.3 The ECDSA Algorithm	184
14.3.4 ECDSA for Vehicle Safety Communications	194
14.4 Message Authentication and Message Integrity Verification	196
14.4.1 Authentication and Integrity Verification Using Hash Functions	197
14.4.2 Authentication and Integrity Verification Using Digital Signatures	198
14.5 Diffie / Hellman Key Establishment Protocol	200
14.5.1 The Original Diffie / Hellman Key Establishment Protocol	200
14.5.2 Elliptic Curve Diffie / Hellman Key Establishment Protocol	201
14.6 Elliptic Curve Integrated Encryption Scheme (ECIES)	202
14.6.1 The Basic Idea	202
14.6.2 Scheme Setup	202
14.6.3 Encrypt a Message	202
14.6.4 Decrypt a Message	204
14.6.5 Performance	204
References	206
15 Public Key Infrastructure for Vehicle Networks	209
15.1 Introduction	209
15.2 Public Key Certificates	210
15.3 Message Authentication with Certificates	211
15.4 Certificate Revocation List	212
15.5 A Baseline Reference Vehicular PKI Model	213
15.6 Configure Initial	

Security Parameters and Assign Initial Certificates	215	--	15.6.1
Vehicles Create Their Private and Public Keys	216	--	15.6.2
Certificate Authority Creates Private and Public Keys for Vehicles	217	--	15.7
Acquire New Keys and Certificates	217	--	15.8
Distribute Certificates to Vehicles for Signature Verifications	220	--	15.9
Detect Misused Certificates and Misbehaving Vehicles	222	--	15.9.1
Local Misbehavior Detection	223	--	15.9.2
Global Misbehavior Detection	224	--	15.9.3
Misbehavior Reporting	224	--	15.10
Ways for Vehicles to Acquire CRLs	226	--	15.11
How Often CRLs should be Distributed to Vehicles?	228	--	15.12
PKI Hierarchy	230	--	15.12.1
Certificate Chaining to Enable Hierarchical CAs	231	--	15.12.2
Hierarchical CA Architecture Example	231	--	15.13
Privacy-Preserving Vehicular PKI	233	--	15.13.1
Quantitative Measurements of Vehicle Anonymity	234	--	15.13.2
Quantitative Measurement of Message Unlinkability	234	--	References
235	--	16	Privacy Protection with Shared Certificates
237	--	16.1	Shared Certificates
237	--	16.2	The Combinatorial Certificate Scheme
237	--	16.3	Certificate Revocation Collateral Damage
239	--	16.4	Certified Intervals
242	--	16.4.1	The Concept of Certified Interval
242	--	16.4.2	Certified Interval Produced by the Original Combinatorial Certificate Scheme
242	--	16.5	Reduce Collateral Damage and Improve Certified Interval
244	--	16.5.1	Reduce Collateral Damage Caused by a Single Misused Certificate
245	--	16.5.2	Vehicles Become Statistically Distinguishable When Misusing Multiple Certificates
248	--	16.5.3	The Dynamic Reward Algorithm
250	--	16.6	Privacy in Low Vehicle Density Areas
253	--	16.6.1	The Problem
253	--	16.6.2	The Blend-In Algorithm to Improve Privacy
256	--	References	259
17	--	Privacy Protection with Short-Lived Unique Certificates	260
17.1	--	Short-Lived Unique Certificates	260
17.2	--	The Basic Short-Lived Certificate Scheme	261
17.3	--	The Problem of Large CRL	263
17.4	--	Anonymously Linked Certificates to Reduce CRL Size	264
17.4.1	--	Certificate Tags	264
17.4.2	--	CRL Processing by Vehicles	265
17.4.3	--	Backward Unlinkability	267
17.5	--	Reduce CRL Search Time	268
17.6	--	Unlinked Short-Lived Certificates	269
17.7	--	Reduce the Volume of Certificate Request and Response Messages	270
17.8	--	Determine the Number of Certificates for Each Vehicle	270
References	--	273	18
Privacy Protection with Group Signatures	274	--	18.1
Group Signatures	274	--	18.2
Zero-Knowledge Proof of Knowledge	275	--	18.3
The ACJT Group Signature Scheme and its Extensions	277	--	18.3.1
The ACJT Group Signature Scheme	277	--	18.3.2
The Challenge of Group Membership Revocation	282	--	18.3.3
ACJT Extensions to Support Membership Revocation	283	--	18.4
The CG Group Signature Scheme with Revocation	286	--	18.5
The Short Group Signatures Scheme	288	--	18.5.1
The Short Group Signatures Scheme	288	--	18.5.2
Membership Revocation	291	--	18.6
Group Signature Schemes with Verifier-Local Revocation	292	--	References
293	--	19	Privacy Protection against Certificate Authorities
295	--	19.1	Introduction
295	--	19.2	Basic Idea
295	--	19.3	Baseline Split CA Architecture, Protocol, and Message Processing
297	--	19.4	Split CA Architecture for Shared Certificates
301	--	19.5	Split CA Architecture for Unlinked Short-Lived Certificates
302	--	19.5.1	Acquire One Unlinked Certificate at a Time
302	--	19.5.2	Assign Batches of Unlinked Short-Lived Certificates
304	--	19.5.3	Revoke Batches of Unlinked Certificates
306	--	19.5.4	Request for Decryption Keys for Certificate Batches
307	--	19.6	Split CA Architecture for Anonymously Linked Short-Lived Certificates
308	--	19.6.1	Assign One Anonymously Linked Short-Lived Certificate at a Time
308	--	19.6.2	Assign Batches of Anonymously Linked Short-Lived Certificates
311	--	19.6.3	Revoke Batches of Anonymously Linked Short-Lived

Certificates 312 -- 19.6.4 Request for Decryption Keys for Certificate Batches 313 -- References 314 -- 20 Comparison of Privacy-Preserving Certificate Management Schemes 315 -- 20.1 Introduction 315 -- 20.2 Comparison of Main Characteristics 316 -- 20.3 Misbehavior Detection 320 -- 20.4 Abilities to Prevent Privacy Abuse by CA and MDS Operators 321 -- 20.5 Summary 322 -- 21 IEEE 1609.2 Security Services 323 -- 21.1 Introduction 323 -- 21.2 The IEEE 1609.2 Standard 323 -- 21.3 Certificates and Certificate Authority Hierarchy 325 -- 21.4 Formats for Public Key, Signature, Certificate, and CRL 327 -- 21.4.1 Public Key Formats 327 -- 21.4.2 Signature Formats 328 -- 21.4.3 Certificate Format 329 -- 21.4.4 CRL Format 332 -- 21.5 Message Formats and Processing for Generating Encrypted Messages 333 -- 21.6 Sending Messages 335 -- 21.7 Request Certificates from the CA 336 -- 21.8 Request and Processing CRL 343 -- 21.9 What the Current IEEE 1609.2 Standard Does Not Cover 344 -- 21.9.1 No Support for Anonymous Message Authentication 344 -- 21.9.2 Separate Vehicle-CA Communication Protocols Are Required 344 -- 21.9.3 Interactions and Interfaces between CA Entities Not Addressed / 346 -- References 346 -- 22 4G for Vehicle Safety Communications 347 -- 22.1 Introduction 347 -- 22.2 Long-Term Revolution (LTE) 347 -- 22.3 LTE for Vehicle Safety Communications/ 353 -- 22.3.1 Issues to Be Addressed 353 -- 22.3.2 LTE for V2I Safety Communications 353 -- 22.3.3 LTE for V2V Safety Communications 356 -- 22.3.4 LTE Broadcast and Multicast Services 357 -- References 358 -- Glossary 360 -- Index 367.

Sommario/riassunto

"Owing to their safety applications, cooperative vehicle systems, which use sensors and wireless technologies to reduce traffic accidents, continue to be the focus of heavy research and development efforts around the world. Written by industry professionals, this book provides a systematic description of cooperative vehicle systems, discussing key technical issues in such systems, the latest advances in enabling technologies, and cutting-edge research trends. Coverage includes important technologies such as 5.9 GHz Dedicated Short Range Communications (DSRC), on-board equipment (OBE), and roadside equipment (RSE)"--

"Provides an up-to-date, in-depth look at current crucial issues in the research community, automotive industry, and government agencies around the world"--
