

Proceedings of the

The First International Symposium on Data, Privacy, and E-Commerce

November 1-3, 2007, Chengdu, China



Los Alamitos, California

Washington • Tokyo



Table of Contents

First International Symposium on Data, Privacy and E-Commerce (ISDPE 2007)

Preface	xv
Organizing Committee	xvi
Program Committee	xvii

Track A

Session A1-1

A New Spatial Diversity Equalizer for Wireless Communication.....	3
<i>Rao Wei, Wang Le-ping, and Guo Ye-cai</i>	
Mining Process Models from Event Logs in Distributed Bioinformatics Workflows.....	8
<i>Jianchuan Xing, Zhishu Li, Yanhong Cheng, Feng Yin, Baolin Li, and Li Chen</i>	
A New Blind Equalization Algorithm Based on Combination Error Function	13
<i>Rao Wei, Dai Guo-xing, and Guo Ye-cai</i>	

Session A1-2

Boundary Extract and Reduction of Mass Data in Reverse Engineering	18
<i>Cheng Xiaomin, Cheng Hong, Yang Wei, and Zhang Jianjian</i>	
Processing Multi-Attribute Queries in Peer-to-Peer Systems.....	22
<i>Min Yu, Zhanhuai Li, and Longbo Zhang</i>	
Research of Pension Fund Market Risk Model Based on Data Mining	28
<i>Xianlin Zhuo, Zhisheng You, and Taowei Zhang</i>	

Session A1-3

Semantics-Based Complex Event Processing for RFID Data Streams.....	32
<i>Tao Ku, YunLong Zhu, and KunYuan Hu</i>	
Dynamic Incremental SVM learning Algorithm for Mining Data Streams.....	35
<i>Zhong-Wei Li, Jing Yang, and Jian-Pei Zhang</i>	
A Novel Document Analysis Method Using Compressibility Vector	38
<i>Nuo Zhang, Toshinori Watanabe, Daisuke Matsuzaki, and Hisashi Koga</i>	
A Method of Using Personal Habits for Path Prediction in Network Games.....	41
<i>Shaolong Li, Changjia Chen, and Lei Li</i>	

Session A1-4

An Improved Heuristic Algorithm Used in Attribute Reduction of Rough Set.....	44
<i>Zhang Li, Lu Xiuying, Wu Huayu, Liu Song, and Hao Shengzhi</i>	
Using Group Interaction of Players to Prevent In-game Cheat in Network Games.....	47
<i>Shaolong Li, Changjia Chen, and Lei Li</i>	
A New Approach of Data Clustering by Improved ACA with Fuzzy Similarity	50
<i>Wen-Yan Wu, Kun Cheng, and Hong-Wei Zhang</i>	
Random Sampling over Streaming Window Joins	53
<i>Jiadong Ren, Wanchang Jiang, and Cong Huo</i>	

Session A2-1

Development of WWW Business Applications Based on the Cellular Data System	56
<i>Toshio Kodama, Toshiyasu L. Kunii, and Yoichi Seki</i>	
Language Feature Mining for Document Subjectivity Analysis.....	62
<i>Bo Chen, Hui He, and Jun Guo</i>	
DM Integration: A Framework for Iterative Large Volume Data Integration	68
<i>Junkui Li, Yuanzhen Wang, and Zhuan Li</i>	

Session A2-2

Automated Large-Scale Simulation Test-Data Generation for Object-Oriented Software Systems.....	74
<i>Yujun Zheng, Yan Ma, and Jinyun Xue</i>	
The Outliers Mining Algorithm Based on Constrained Concept Lattice.....	80
<i>Jiang Yiyong, Zhang Jifu, Cai Jianghui, Zhang Sulan, and Hu Lihua</i>	
Fast Algorithm for Mining Maximal Frequent Itemsets.....	86
<i>Lisheng Ma and Huiwen Deng</i>	

Session A2-3

EM: An Improved Schema Matching Algorithm in the Update of XML Views.....	92
<i>Zhang Dongming, Chen Wei, and Liu Guohua</i>	
Evaluation of Three Discrete Methods on Customer Churn Model Based on Neural Network and Decision Tree in PHSS.....	95
<i>Luo Bin, Shao Peiji, and Liu Duyu</i>	
A Quick Algorithm for Reduction of Attribute in Information Systems	98
<i>Yue-jin Lv and Jin-hai Li</i>	
An Efficiency apriori Algorithm: P_Matrix Algorithm.....	101
<i>Sixue Bai and Xinxi Dai</i>	
A Grid-Based Clustering Algorithm for Network Anomaly Detection.....	104
<i>Xiaotao Wei, Houkuan Huang, and Shengfeng Tian</i>	

Session A2-4

Exploration of a Category Theory-Based Object-Oriented Database for Surface Texture Information Management.....	107
<i>Yuanping Xu, Zhijie Xu, and Xiangqian Jiang</i>	
Ontology-driven Conceptual Modeling for Spatiotemporal Database Applications	110
<i>Peiquan Jin, Shouhong Wan, and Lihua Yue</i>	
Motion Retrieval Based on Multiple Instance Learning by Isomap and RBF	113
<i>Jian Xiang</i>	
An Incremental Rule Extract Algorithm Based on Rough Set and SearchTree.....	116
<i>Yinghong Ma and Zhaolei Qiu</i>	
Access Control Based on RBAC in Distributed Cooperation Environment.....	119
<i>Yin Shao-hong and Wang Wei</i>	

Session A3-1

MANET Loss Tomography Based on Circle-Movement Mobile Model	122
<i>Wang Bei-Zhan, Wang Ya-Ping, Wang Wei, and Lou Run-Yu</i>	
Quantum Authentication Protocol Using Bell State	128
<i>Xiaoyu Li and Liju Chen</i>	

Session A3-2

Efficient Identity Based Signature/Signcryption Scheme in the Standard Model	133
<i>Ren Yanli and Gu Dawu</i>	
Privacy-Preserving Authentication Based on Short Group Signature in Vehicular Networks	138
<i>Jingliang Zhang, Lizhen Ma, Wanli Su, and Yumin Wang</i>	

Session A3-3

A Survey Study on XML Functional Dependencies.....	143
<i>Teng Lv and Ping Yan</i>	
An Efficient Bulk Updating Method for Finite Automaton Based XML Filtering Systems	146
<i>Yongrui Qin, Weiwei Sun, Ping Yu, and Zhuoyao Zhang</i>	
G-HITS: A Link Analysis Algorithm Based on Gravitation Model.....	149
<i>Xianchao Zhang, Xinyue Liu, Liguozhang, and Hong Yu</i>	
Self-Adaptive Spatial Information Multi-grid Database.....	152
<i>Cheng Zhong, Deren Li, and Ming Li</i>	
Meta-information Mechanism and Variable Precision Rough Set Model	155
<i>Jian Su and Wenyong Weng</i>	

Session A3-4

A New Index Method for Large Motion Capture Data.....	158
<i>HongLi Zhu and Jian Xiang</i>	
A Structural Complexity Metric for Software Components	161
<i>Fangjun Wu and Tong Yi</i>	
An Improvement of BAM in Storage Capacity and Error-Correction Capability	164
<i>Min Wang and Songcan Chen</i>	
Genetic Algorithms Designed for Solving Support Vector Classifier	167
<i>Ma MinShu</i>	
Distributed Video Coding with Dynamic Virtual Channel Model Estimation	170
<i>Linbo Qing, Xiaohai He, and Rui Lv</i>	

Track B

Session B1-1

An Improved Method of Differential Fault Analysis on the SMS4 Cryptosystem.....	175
<i>Wei Li and Dawu Gu</i>	
An Efficient and Unconditionally-Secure Oblivious Polynomial Evaluation Protocol.....	181
<i>Yang Bo, Wang Qinglong, and Cao Yunfei</i>	
A New Authorization Protocol for Trusted Computing.....	185
<i>Zhang Xing, Zhang Xiaofei, and Shen Changxiang</i>	

Session B1-2

Greedy Clustering with Sample-Based Heuristics for K-Anonymisation	191
<i>Grigorios Loukides and Jianhua Shao</i>	
A Quantitative Prediction Method of Network Security Situation Based on Wavelet Neural Network.....	197
<i>Lai Jibao, Wang Huiqiang, Liu Xiaowu, and Liang Ying</i>	
Firewall Rules Sorting Based on Markov Model	203
<i>Weiping Wang, Rong Ji, Wenhui Chen, Bo Chen, and Zhepeng Li</i>	

Session B1-3

Research of DoS Intrusion Real-time Detection Based on Danger Theory.....	209
<i>Chun Xu, Xing-shu Chen, Hui Zhao, Yu-ming Jiang, Nian Liu, and Tie-fang Wang</i>	
Secure Media Distribution in P2P Networks.....	212
<i>Chen Xi</i>	
A Window-Based Feature Extraction Method in Document Copy Detection.....	215
<i>Xu Li, Guo-Hua Liu, and Hui-Dong Ma</i>	
A Scheme Based on Trusted Computing for Terminal Security.....	218
<i>Jun Zhang, Zheng Zhou, Wei-peng Liu, and Jian Li</i>	

Side-Channel Attack on Biometric Cryptosystem Based on Keystroke Dynamics	221
<i>Zhang Tao, Fan Ming-Yu, and Fu Bo</i>	

Session B1-4

Authentication and Key Establishment Scheme Based on Token for Mobile Commerce.....	224
<i>Li Chen, Jun Liu, and Huibin Wang</i>	
Statistical Decision Modeling for IDS Alert Analysis.....	227
<i>Li Zhi-tang, Li Dong, Lei Jie, and Zhang Aifang</i>	
An Improved Identity-Based KCDSA Signcryption Scheme.....	230
<i>Fagen Li and Chunxiang Xu</i>	
An Identity-Based Threshold Ring Signature Scheme Based on the Bilinear Pairings	233
<i>Jiu-Qing Shang, Qiu-Liang Xu, and Xin Liu</i>	
An Efficient Certificateless Signature from Pairings.....	236
<i>Changji Wang, Hui Huang, and Yong Tang</i>	
Text Information Hiding Method Based on Chaotic Map and BCH Code in DWT Domain of a Carrier Image.....	239
<i>Shu-Guo Yang, Chun-Xia Li, and Sheng-He Sun</i>	

Session B2-1

<i>ThTrust</i> : Transaction History Based Peer-to-Peer Trust Model	242
<i>Shaojie Qiao, Xingshu Chen, and Changjie Tang</i>	
A Practical Certificateless Signature Scheme.....	248
<i>Lifeng Guo, Lei Hu, and Yong Li</i>	
On the Undecidability of Quasi-Private-Key-Encryption Statistical Indistinguishability	254
<i>Ning Ding and Dawu Gu</i>	

Session B2-2

Efficient ID-Based Blind Signature Schemes.....	260
<i>Yang Ming and Yumin Wang</i>	
An Information-Sharing Based Anti-Phishing System.....	265
<i>Yueqing Cheng, Zhen Yuan, Lei Ma, and Robert Deng</i>	

Session B2-3

Security Analysis of DVB Common Scrambling Algorithm.....	271
<i>Wei Li and Dawu Gu</i>	
On Karatsuba Multiplication Algorithm.....	274
<i>Xianjin Fang and Longshu Li</i>	
A Composite Image Encryption Scheme Using AES and Chaotic Series	277
<i>Xiao Huijuan, Qiu Shuisheng, and Deng Chengliang</i>	

A Secure and Efficient Three-Party Password-Based Authenticated Key Exchange Protocol..... 280
He Yong-Zhong and Cai Ying

Application of Oblivious Transfer Protocol in Distributed Data Mining with Privacy-preserving 283
Weiping Wang, Bing Deng, and Zhepeng Li

Session B2-4

Another Efficient Identity-Based Ring Signature Scheme and Its Extension..... 286
Jianhong Zhang and Ji Cheng

An Approach to the Sensitive Information Protection for Mobile Code 289
Liu Weiwei, Han Zhen, and Wang Qinglong

The Improvement of a Task Scheduling Algorithm in Grid Computing 292
Yu Liang and Zhou Jiliu

An Improved Nonrepudiable Threshold Proxy Signature Scheme with Known Signers 298
Xin Liu, Qiu-Liang Xu, and Jiu-Qing Shang

Least-Privilege-Based Access Control Model for Job Execution in Grid 301
Ke Xue, Shaohua Tang, and Lina Ge

SEDBRS: A Secure and Efficient Desktop Backup and Recovery System..... 304
Dejun Wang, Lina Wang, and Jingbo Song

Session B3-1

An Information Flow Security Model to Trusted Computing System..... 310
Hu Jun and Shen Changxiang

Advanced DES Algorithm against Differential Power Analysis and its Hardware Implementation 316
Jiang Huiping, Xu Rui, and Bao Sheng

Key Management Using Biometrics..... 321
Haiyong Chen, Hongwei Sun, and Kwok-Yan Lam

Session B3-2

Further Cryptanalysis of a Provably Secure CRT-RSA Algorithm 327
Baodong Qin, Ming Li, and Fanyu Kong

A New Construction of Zero-Knowledge Sets Secure in Random Oracle Model..... 332
Rui Xue, Ninghui Li, and Jiangtao Li

Session B3-3

An Efficient Designated Verifier Signature Scheme without Random Oracles 338
Jianhong Zhang and Cheng Ji

Several Algorithms to find Annihilators of Boolean Function 341
Cao Hao, Wei Shimin, and Zhuo Zepeng

Terminal Data Protection Based on DBLP Model 344
Wang Fei and Liu Yi

Object Oriented Fine-Granularity Access Control for XML Document..... 347
Tao Peng, Minghua Jiang, and Ming Hu

Session B3-4

Secure Spread-Spectrum Watermark Detection Based on Extended TPM..... 350
Hao Yanjun, Zhang Huanguo, and Wang Lina

Research on the 4th S-Box Collision in Differential Power Analysis of the DES..... 353
Qian SiJin, He DeQuan, Zhang KaiZe, and Wang YanBo

A SAML/XACML Based Access Control between Portal and Web Services 356
Hao Yin, Jiliu Zhou, Huilin Wu, and Liang Yu

Track C

Session C1-1

PRN: A Novel Trust Model..... 361
Biao Cai, Zhishu Li, and Xun Lin

On Two Special Cases of Online Device Replacement Problem 367
Chunlin Xin, Weimin Ma, and Lei Yang

Using Third-party Subsidy Program to Improve Trading Efficiency for Online Marketplaces 373
Ngai Lung, Liu Lian-chen, Wu Cheng, Mak Phil, and He Ling-juan

Session C1-2

A Reputation-Based Market Model in Grid Environment..... 379
Weina Lu, Shoubao Yang , Liangmin Guo, Dong Wei, and Wen Ji

Analysis of Trust-Based E-Commerce Recommender Systems Under Recommendation Attacks..... 385
Zhang Fug-uo and Xu Sheng-hua

QoS Consistency as Basis of Reputation Measurement of Web Service..... 391
Xiaodong Fu, Ping Zou, Ying Jiang, and Zhenhong Shang

Session C1-3

A First-order Logic Semantics for SPKI/SDSI..... 397
Xiuhua Geng, Zhen Han, and Li Jin

Preventing DoS Attack on Hidden Credentials 400
Guoming Cai, Yadi Wang, Miao Wang, and Haiying Gao

Multi-Period Optimal Design of Online Auctions..... 403
Chen Sheng-li, Yang Xiao-hua, and Luo Yun-feng

Analysis of Current E-Payment Solution in China-Third Party Payment Platform..... 406
Nie Jin

A Service Recommender System Based on the Co-evolutionary Contract Net for Migrating Workflows 409
Rui Wang and Guangzhou Zeng

Session C1-4

An Approach to Dynamic Grid Service Selection Based on Improved Reinforcement Q-learning 412
*Chen Liangyin, Li Zhishu, Li Qing, Zhang Jingyu,
Cheng Yanhong, and Chen Liangwei*

Research on Risk Evaluation for Venture Capital Based on Intuitionistic Fuzzy Set and TOPSIS..... 415
Peide Liu

Dynamic Fair Electronic Cash System without Trustees..... 418
Lizhen Ma, Jingliang Zhang, Shichong Tan, and Yumin Wang

A New Secure Network Upgrade System..... 421
Jun Tan, Xingshu Chen, and Shaojie Qiao

Session C2-1

Inverse Problem in DSMT and Its Applications in Trust Management 424
Jin Wang and Huaijiang Sun

Culture's Role in E-Commerce Success: A Conceptual Model..... 429
Shifeng Liu and Mincong Tang

A Security Enhancement Architecture for COTS Operating System 434
Chen Zemao, Liu Yi, Shen Changxiang, Liu Jingchao, and Zhou Libing

Session C2-2

Constant-Round Restricted-Verifier Zero-Knowledge with Polynomial Precision..... 439
Ning Ding and Dawu Gu

A Time-Bound Key Management Scheme for Hierarchical Tree 445
Jiqiang Liu and Sheng Zhong

A Multi-Level Security Model Based on Trusted Computing..... 448
Zhao Jia, Liu Ji-qiang, and Chen Jing

Session C2-3

Improved Algorithm of the Tate Pairing in Characteristic Three 453
Ting Wu, Huan-Qiang Du, Min Zhang, and Rong-Bo Wang

A New Computer Self-immune Model against Malicious Codes..... 456
Zhou Zheng, Liu Yi, Li Jian, and Shen Chang-xiang

RFID Authentication Protocol Using Synchronized Secret Information..... 459
Yoon-Su Jeong, Yoon-Cheol Hwang, Ning Sun, Ki-Su Kim, and Sang-Ho Lee

The FPGA Implementation of 128-bits AES Algorithm Based on Four 32-bits Parallel Operation 462
Chi-Wu Huang, Chi-Jeng Chang, Mao-Yuan Lin, and Hung-Yun Tai

Session C2-4

An Operating System Trusted Security Model for Important Sensitive Information System	465
<i>Zhao Yong, Liu Ji Qiang, Han Zhen, and Shen Chang Xiang</i>	
Distributed Intrusion Alert Fusion Based on Multi Keyword.....	469
<i>Ming Xu and Wei Han</i>	
Improvement of One Type Xorshift Random Number Generators	472
<i>Guang Zeng, Wenbao Han, and Wei Sun</i>	
An Efficient Ring Signature Scheme for Privacy and Anonymous Communication	475
<i>Lingling Wang, Guoyin Zhang, and Chunguang Ma</i>	

Session C3-1

A Delegation-Based Workflow Access Control Model.....	478
<i>Yonghe Wei and Qilin Shu</i>	
A Novel Network Security Evaluation System Based on Immune Principle	484
<i>J. Yang, T. Li, S.J. Liu, and G. Liang</i>	
Provably Secure Password-Based Tripartite Key Exchange Protocol from Weil Pairing	490
<i>Guomin Li, Dake He, and Xianhui Lu</i>	

Session C3-2

Quantum Message Signature Scheme without an Arbitrator.....	496
<i>Xiaojun Wen and Yun Liu</i>	
A Novel Key Assignment Algorithms for Secure Multicast	501
<i>Gao Zhi Min and Yao Qi</i>	

Session C3-3

8-bit AES Implementation in FPGA by Multiplexing 32-bit AES Operation	505
<i>Chi-Jeng Chang, Chi-Wu Huang, Hung-Yun Tai, and Mao-Yuan Lin</i>	
RFID Protocol Enabling Ownership Transfer to Protect against Traceability and DoS Attacks.....	508
<i>Hong Lei and Tianjie Cao</i>	
An Artificial Immune Clustering Approach to Unsupervised Network Intrusion Detection.....	511
<i>Wang Sifei and Xu Jiayi</i>	
A Novel Scheme for Robust Video Watermark in the 3D-DWT Domain.....	514
<i>Lv Anqiang and Li Jing</i>	

Session C3-4

A Network Intrusion Detection System Based Soft Computing 517
Niandong Liao, Shengfeng Tian, Houkuan Huang, and Tinghua Wang

A Novel Anti-spam Scheme for Image-Based Email 520
Jianshe Dong, Zhanting Yuan, Qiuyu Zhang, and Yufeng Zheng

Author Index **523**