Dengguo Feng
Dongdai Lin
Moti Yung (Eds.)

LNCS 3822

Information Security and Cryptology

First SKLOIS Conference, CISC 2005
Beijing, China, December 2005
Proceedings

Springer

Dengguo Feng   Dongdai Lin
Moti Yung (Eds.)

Information Security and Cryptology

First SKLOIS Conference, CISC 2005
Beijing, China, December 15-17, 2005
Proceedings

Springer

Volume Editors

Dengguo Feng
Dongdai Lin
Chinese Academy of Sciences, Institute of Software
State Key Laboratory of Information Security
Beijing, 100080, P. R. China
E-mail: {feng,ddlin}@is.iscas.ac.cn

Moti Yung
RSA Laboratories and Columbia University
Computer science Department
Room 464, S.W. Mudd Building, New York, NY 10027, USA
E-mail: moti@cs.columbia.edu

Library of Congress Control Number: 2005937143

CR Subject Classification (1998): E.3, D.4.6, F.2.1, C.2, J.1, C.3, K.4.4, K.6.5

ISSN 0302-9743
ISBN-10 3-540-30855-5 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-30855-3 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springeronline.com

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11599548 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 3822

Preface

The first SKLOIS Conference on Information Security and Cryptography (CISC 2005) was organized by the State Key Laboratory of Information Security of the Chinese Academy of Sciences. It was held in Beijing, China, December 15-17, 2005 and was sponsored by the Institute of Software, the Chinese Academy of Sciences, the Graduate School of the Chinese Academy of Sciences and the National Science Foundation of China. The conference proceedings, representing invited and contributed papers, are published in this volume of Springer's Lecture Notes in Computer Science (LNCS) series.

The area of research covered by CISC has been gaining importance in recent years, and a lot of fundamental, experimental and applied work has been done, advancing the state of the art. The program of CISC 2005 covered numerous fields of research within the general scope of the conference.

The International Program Committee of the conference received a total of 196 submissions (from 21 countries). Thirty-three submissions were selected for presentation as regular papers and are part of this volume. In addition to this track, the conference also hosted a short-paper track of 32 presentations that were carefully selected as well. All submissions were reviewed by experts in the relevant areas and based on their ranking and strict selection criteria the papers were selected for the various tracks. We note that stricter criteria were applied to papers co-authored by program committee members. We further note that, obviously, no member took part in influencing the ranking of his or her own submissions. In addition to the contributed regular papers, this volume contains the two invited papers by Serge Vaudenay and Giovanni Di Crescenzo.

Many people and organizations helped in making the conference a reality. We would like to take this opportunity to thank the Program Committee members and the external experts for their invaluable help in producing the conference program. We would like to thank the Organizing Committee members, the Co-chairs Dongdai Lin and Chunkun Wu, and the members Jiwu Jing and Wenling Wu. Dongdai Lin also served as a "Super Program Chair", organizing the electronic program discussions and coordinating the decision making process. We thank the various sponsors and, last but not least, we wish to thank all the authors who submitted papers to the conference, the invited speakers, the session chairs and all the conference attendees.

December 2005 Dengguo Feng and Moti Yung

CISC 2005

First SKLOIS Conference on Information Security and Cryptology

Beijing, China December 15-17, 2005

Sponsored and organized by
State Key Laboratory of Information Security
(Chinese Academy of Sciences)

Program Chairs

Dengguo Feng	SKLOIS, Chinese Academy of Sciences, China
Moti Yung	RSA Labs and Columbia University, USA

Program Committee

Dan Bailey	RSA Laboratory, USA
Feng Bao	Institute for Infocomm Research, Singapore
Carlo Blundo	University of Salerno, Italy
Felix Brandt	Stanford University, USA
Ahto Buldas	Tallin Technical University, Estonia
YoungJu Choie	POSTECH, Korea
Zongduo Dai	GSCAS, Chinese Academy of Sciences, China
George Davida	UWM, USA
Ed Dawson	QUT, Australia
Cunsheng Ding	HKUST, Hong Kong, China
Keqin Feng	Tsinghua University, China
Keith Frikken	Purdue University, USA
Jun Furukawa	NEC, Japan
Guang Gong	University of Waterloo, Canada
Jiwu Huang	Zhongshan University, China
Kwangjo Kim	ICU, Korea
Xuejia Lai	Shanghai Jiaotong University, China
Dongdai Lin	SKLOIS, Chinese Academy of Sciences, China
Mulan Liu	AMSS, CAS, China
Wenbo Mao	Hewlett-Packard Labs, UK
Tsutomu Matsumoto	Yokohama National University, Japan
Sjouke Mauw	EUT, Netherlands
Bodo Moller	Calgary, Canada
Svetla Nikova	K.U. Leuven, Belgium
Thomas Pornin	Cryptolog, France

Michel Riguidel	ENST, France
Eiji Okamato	Tsukuba University, Japan
Duong Hieu Phan	ENS, France
Bimal Roy	Indian Statistical Institute, India
Ahmad-Reza Sadeghi	Bochum, Germany
Kouichi Sakurai	Kyushu University, Japan
Tom Shrimpton	Portland State University, USA
Willy Susilo	University of Wollongong, Australia
Vijay Varadharajan	Macquarie, Australia
Xiaoyun Wang	Shandong University, China
Chuan-kun Wu	SKLOIS, Chinese Academy of Science, China
Yixian Yang	BUPT, China
Huanguo Zhang	Wuhan University, China
Yuliang Zheng	UNCC, USA
Hong Zhu	Fudan University, China
Yuefei Zhu	Information Engineering University, China

Organizing Committee

Dongdai LIN (Co-chair)	SKLOIS, Chinese Academy of Sciences, China
Chuankun Wu (Co-chair)	SKLOIS, Chinese Academy of Sciences, China
Jiwu JING	SKLOIS, Chinese Academy of Sciences, China
Wenling WU	SKLOIS, Chinese Academy of Sciences, China

Lecture Notes in Computer Science

For information about Vols. 1–3722

please contact your bookseller or Springer

Vol. 3837: K. Cho, P. Jacquet (Eds.), Technologies for Advanced Heterogeneous Networks. IX, 307 pages. 2005.

Vol. 3835: G. Sutcliffe, A. Voronkov (Eds.), Logic for Programming, Artificial Intelligence, and Reasoning. XIV, 744 pages. 2005. (Subseries LNAI).

Vol. 3833: K.-J. Li, C. Vangenot (Eds.), Web and Wireless Geographical Information Systems. XI, 309 pages. 2005.

Vol. 3826: B. Benatallah, F. Casati, P. Traverso (Eds.), Service-Oriented Computing - ICSOC 2005. XVIII, 597 pages. 2005.

Vol. 3824: L.T. Yang, M. Amamiya, Z. Liu, M. Guo, F.J. Rammig (Eds.), Embedded and Ubiquitous Computing. XXIII, 1204 pages. 2005.

Vol. 3823: T. Enokido, L. Yan, B. Xiao, D. Kim, Y. Dai, L.T. Yang (Eds.), Embedded and Ubiquitous Computing. XXXII, 1317 pages. 2005.

Vol. 3822: D. Feng, D. Lin, M. Yung (Eds.), Information Security and Cryptology. XII, 420 pages. 2005.

Vol. 3821: R. Ramanujam, S. Sen (Eds.), FSTTCS 2005: Foundations of Software Technology and Theoretical Computer Science. XIV, 566 pages. 2005.

Vol. 3818: S. Grumbach, L. Sui, V. Vianu (Eds.), Advances in Computer Science – ASIAN 2005. XIII, 294 pages. 2005.

Vol. 3814: M. Maybury, O. Stock, W. Wahlster (Eds.), Intelligent Technologies for Interactive Entertainment. XV, 342 pages. 2005. (Subseries LNAI).

Vol. 3810: Y.G. Desmedt, H. Wang, Y. Mu, Y. Li (Eds.), Cryptology and Network Security. XI, 349 pages. 2005.

Vol. 3809: S. Zhang, R. Jarvis (Eds.), AI 2005: Advances in Artificial Intelligence. XXVII, 1344 pages. 2005. (Subseries LNAI).

Vol. 3808: C. Bento, A. Cardoso, G. Dias (Eds.), Progress in Artificial Intelligence. XVIII, 704 pages. 2005. (Subseries LNAI).

Vol. 3807: M. Dean, Y. Guo, W. Jun, R. Kaschek, S. Krishnaswamy, Z. Pan, Q.Z. Sheng (Eds.), Web Information Systems Engineering – WISE 2005 Workshops. XV, 275 pages. 2005.

Vol. 3806: A.H. H. Ngu, M. Kitsuregawa, E.J. Neuhold, J.-Y. Chung, Q.Z. Sheng (Eds.), Web Information Systems Engineering – WISE 2005. XXI, 771 pages. 2005.

Vol. 3805: G. Subsol (Ed.), Virtual Storytelling. XII, 289 pages. 2005.

Vol. 3804: G. Bebis, R. Boyle, D. Koracin, B. Parvin (Eds.), Advances in Visual Computing. XX, 755 pages. 2005.

Vol. 3803: S. Jajodia, C. Mazumdar (Eds.), Information Systems Security. XI, 342 pages. 2005.

Vol. 3799: M. A. Rodríguez, I.F. Cruz, S. Levashkin, M.J. Egenhofer (Eds.), GeoSpatial Semantics. X, 259 pages. 2005.

Vol. 3798: A. Dearle, S. Eisenbach (Eds.), Component Deployment. X, 197 pages. 2005.

Vol. 3797: S. Maitra, C. E. V. Madhavan, R. Venkatesan (Eds.), Progress in Cryptology - INDOCRYPT 2005. XIV, 417 pages. 2005.

Vol. 3796: N.P. Smart (Ed.), Cryptography and Coding. XI, 461 pages. 2005.

Vol. 3795: H. Zhuge, G.C. Fox (Eds.), Grid and Cooperative Computing - GCC 2005. XXI, 1203 pages. 2005.

Vol. 3794: X. Jia, J. Wu, Y. He (Eds.), Mobile Ad-hoc and Sensor Networks. XX, 1136 pages. 2005.

Vol. 3793: T. Conte, N. Navarro, W.-m.W. Hwu, M. Valero, T. Ungerer (Eds.), High Performance Embedded Architectures and Compilers. XIII, 317 pages. 2005.

Vol. 3792: I. Richardson, P. Abrahamsson, R. Messnarz (Eds.), Software Process Improvement. VIII, 215 pages. 2005.

Vol. 3791: A. Adi, S. Stoutenburg, S. Tabet (Eds.), Rules and Rule Markup Languages for the Semantic Web. X, 225 pages. 2005.

Vol. 3790: G. Alonso (Ed.), Middleware 2005. XIII, 443 pages. 2005.

Vol. 3789: A. Gelbukh, Á. de Albornoz, H. Terashima-Marín (Eds.), MICAI 2005: Advances in Artificial Intelligence. XXVI, 1198 pages. 2005. (Subseries LNAI).

Vol. 3788: B. Roy (Ed.), Advances in Cryptology - ASIACRYPT 2005. XIV, 703 pages. 2005.

Vol. 3785: K.-K. Lau, R. Banach (Eds.), Formal Methods and Software Engineering. XIV, 496 pages. 2005.

Vol. 3784: J. Tao, T. Tan, R.W. Picard (Eds.), Affective Computing and Intelligent Interaction. XIX, 1008 pages. 2005.

Vol. 3781: S.Z. Li, Z. Sun, T. Tan, S. Pankanti, G. Chollet, D. Zhang (Eds.), Advances in Biometric Person Authentication. XI, 250 pages. 2005.

Vol. 3780: K. Yi (Ed.), Programming Languages and Systems. XI, 435 pages. 2005.

Vol. 3779: H. Jin, D. Reed, W. Jiang (Eds.), Network and Parallel Computing. XV, 513 pages. 2005.

Vol. 3778: C. Atkinson, C. Bunse, H.-G. Gross, C. Peper (Eds.), Component-Based Software Development for Embedded Systems. VIII, 345 pages. 2005.

Vol. 3777: O.B. Lupanov, O.M. Kasim-Zade, A.V. Chaskin, K. Steinhöfel (Eds.), Stochastic Algorithms: Foundations and Applications. VIII, 239 pages. 2005.

Vol. 3775: J. Schönwälder, J. Serrat (Eds.), Ambient Networks. XIII, 281 pages. 2005.

Vol. 3773: A. Sanfeliu, M.L. Cortés (Eds.), Progress in Pattern Recognition, Image Analysis and Applications. XX, 1094 pages. 2005.

Vol. 3772: M. Consens, G. Navarro (Eds.), String Processing and Information Retrieval. XIV, 406 pages. 2005.

Vol. 3771: J.M.T. Romijn, G.P. Smith, J. van de Pol (Eds.), Integrated Formal Methods. XI, 407 pages. 2005.

Vol. 3770: J. Akoka, S.W. Liddle, I.-Y. Song, M. Bertolotto, I. Comyn-Wattiau, W.-J. van den Heuvel, M. Kolp, J. Trujillo, C. Kop, H.C. Mayr (Eds.), Perspectives in Conceptual Modeling. XXII, 476 pages. 2005.

Vol. 3768: Y.-S. Ho, H.J. Kim (Eds.), Advances in Multimedia Information Processing - PCM 2005, Part II. XXVIII, 1088 pages. 2005.

Vol. 3767: Y.-S. Ho, H.J. Kim (Eds.), Advances in Multimedia Information Processing - PCM 2005, Part I. XXVIII, 1022 pages. 2005.

Vol. 3766: N. Sebe, M.S. Lew, T.S. Huang (Eds.), Computer Vision in Human-Computer Interaction. X, 231 pages. 2005.

Vol. 3765: Y. Liu, T. Jiang, C. Zhang (Eds.), Computer Vision for Biomedical Image Applications. X, 563 pages. 2005.

Vol. 3764: S. Tixeuil, T. Herman (Eds.), Self-Stabilizing Systems. VIII, 229 pages. 2005.

Vol. 3762: R. Meersman, Z. Tari, P. Herrero (Eds.), On the Move to Meaningful Internet Systems 2005: OTM 2005 Workshops. XXXI, 1228 pages. 2005.

Vol. 3761: R. Meersman, Z. Tari (Eds.), On the Move to Meaningful Internet Systems 2005: CoopIS, DOA, and ODBASE, Part II. XXVII, 653 pages. 2005.

Vol. 3760: R. Meersman, Z. Tari (Eds.), On the Move to Meaningful Internet Systems 2005: CoopIS, DOA, and ODBASE, Part I. XXVII, 921 pages. 2005.

Vol. 3759: G. Chen, Y. Pan, M. Guo, J. Lu (Eds.), Parallel and Distributed Processing and Applications - ISPA 2005 Workshops. XIII, 669 pages. 2005.

Vol. 3758: Y. Pan, D.-x. Chen, M. Guo, J. Cao, J.J. Dongarra (Eds.), Parallel and Distributed Processing and Applications. XXIII, 1162 pages. 2005.

Vol. 3757: A. Rangarajan, B. Vemuri, A.L. Yuille (Eds.), Energy Minimization Methods in Computer Vision and Pattern Recognition. XII, 666 pages. 2005.

Vol. 3756: J. Cao, W. Nejdl, M. Xu (Eds.), Advanced Parallel Processing Technologies. XIV, 526 pages. 2005.

Vol. 3754: J. Dalmau Royo, G. Hasegawa (Eds.), Management of Multimedia Networks and Services. XII, 384 pages. 2005.

Vol. 3753: O.F. Olsen, L.M.J. Florack, A. Kuijper (Eds.), Deep Structure, Singularities, and Computer Vision. X, 259 pages. 2005.

Vol. 3752: N. Paragios, O. Faugeras, T. Chan, C. Schnörr (Eds.), Variational, Geometric, and Level Set Methods in Computer Vision. XI, 369 pages. 2005.

Vol. 3751: T. Magedanz, E.R. M. Madeira, P. Dini (Eds.), Operations and Management in IP-Based Networks. X, 213 pages. 2005.

Vol. 3750: J.S. Duncan, G. Gerig (Eds.), Medical Image Computing and Computer-Assisted Intervention – MICCAI 2005, Part II. XL, 1018 pages. 2005.

Vol. 3749: J.S. Duncan, G. Gerig (Eds.), Medical Image Computing and Computer-Assisted Intervention – MICCAI 2005, Part I. XXXIX, 942 pages. 2005.

Vol. 3748: A. Hartman, D. Kreische (Eds.), Model Driven Architecture – Foundations and Applications. IX, 349 pages. 2005.

Vol. 3747: C.A. Maziero, J.G. Silva, A.M.S. Andrade, F.M.d. Assis Silva (Eds.), Dependable Computing. XV, 267 pages. 2005.

Vol. 3746: P. Bozanis, E.N. Houstis (Eds.), Advances in Informatics. XIX, 879 pages. 2005.

Vol. 3745: J.L. Oliveira, V. Maojo, F. Martín-Sánchez, A.S. Pereira (Eds.), Biological and Medical Data Analysis. XII, 422 pages. 2005. (Subseries LNBI).

Vol. 3744: T. Magedanz, A. Karmouch, S. Pierre, I. Venieris (Eds.), Mobility Aware Technologies and Applications. XIV, 418 pages. 2005.

Vol. 3742: J. Akiyama, M. Kano, X. Tan (Eds.), Discrete and Computational Geometry. VIII, 213 pages. 2005.

Vol. 3740: T. Srikanthan, J. Xue, C.-H. Chang (Eds.), Advances in Computer Systems Architecture. XVII, 833 pages. 2005.

Vol. 3739: W. Fan, Z.-h. Wu, J. Yang (Eds.), Advances in Web-Age Information Management. XXIV, 930 pages. 2005.

Vol. 3738: V.R. Syrotiuk, E. Chávez (Eds.), Ad-Hoc, Mobile, and Wireless Networks. XI, 360 pages. 2005.

Vol. 3735: A. Hoffmann, H. Motoda, T. Scheffer (Eds.), Discovery Science. XVI, 400 pages. 2005. (Subseries LNAI).

Vol. 3734: S. Jain, H.U. Simon, E. Tomita (Eds.), Algorithmic Learning Theory. XII, 490 pages. 2005. (Subseries LNAI).

Vol. 3733: P. Yolum, T. Güngör, F. Gürgen, C. Özturan (Eds.), Computer and Information Sciences - ISCIS 2005. XXI, 973 pages. 2005.

Vol. 3731: F. Wang (Ed.), Formal Techniques for Networked and Distributed Systems - FORTE 2005. XII, 558 pages. 2005.

Vol. 3729: Y. Gil, E. Motta, V. R. Benjamins, M.A. Musen (Eds.), The Semantic Web – ISWC 2005. XXIII, 1073 pages. 2005.

Vol. 3728: V. Paliouras, J. Vounckx, D. Verkest (Eds.), Integrated Circuit and System Design. XV, 753 pages. 2005.

Vol. 3727: M. Barni, J. Herrera Joancomartí, S. Katzenbeisser, F. Pérez-González (Eds.), Information Hiding. XII, 414 pages. 2005.

Vol. 3726: L.T. Yang, O.F. Rana, B. Di Martino, J.J. Dongarra (Eds.), High Performance Computing and Communications. XXVI, 1116 pages. 2005.

Vol. 3725: D. Borrione, W. Paul (Eds.), Correct Hardware Design and Verification Methods. XII, 412 pages. 2005.

Vol. 3724: P. Fraigniaud (Ed.), Distributed Computing. XIV, 520 pages. 2005.

Vol. 3723: W. Zhao, S. Gong, X. Tang (Eds.), Analysis and Modelling of Faces and Gestures. XI, 4234 pages. 2005.

Table of Contents

Signature Schemes

Symmetric Key Mechanisms

Zero-Knowledge and Secure Computations

Threshold Cryptography

Intrusion Detection Systems

Protocol Cryptanalysis

ECC Algorithms

Applications

Secret Sharing

Denial of Service Attacks

On Bluetooth Repairing: Key Agreement Based on Symmetric-Key Cryptography

Serge Vaudenay

EPFL,
CH-1015 Lausanne, Switzerland
http://lasecwww.epfl.ch

Abstract. Despite many good (secure) key agreement protocols based on public-key cryptography exist, secure associations between two wireless devices are often established using symmetric-key cryptography for cost reasons. The consequence is that common daily used security protocols such as Bluetooth pairing are insecure in the sense that an adversary can easily extract the main private key from the protocol communications. Nevertheless, we show that a feature in the Bluetooth standard provides a pragmatic and costless protocol that can eventually repair privateless associations, thanks to mobility. This proves (in the random oracle model) the pragmatic security of the Bluetooth pairing protocol when repairing is used.

1 Setting Up Secure Communications

Digital communications are often secured by means of symmetric encryption and message authentication codes. This provided high throughput and security. However, setting up this channel requires agreeing on a private key with large entropy. Private key agreement between remote peers through insecure channel is a big challenge. A first (impractical) solution was proposed in 1975 by Merkle [19]. A solution was proposed by Diffie and Hellman in 1976 [12]. It works, provided that the two peers can communicate over an authenticated channel which protects the integrity of messages and that a standard computational problem (namely, the Diffie-Hellman problem) is hard.

To authenticate messages of the Diffie-Hellman protocol is still expensive since those messages are pretty long (typically, a thousand bits, each) and that authentication is often manually done by human beings. Folklore solutions consist of shrinking this amount of information by means of a collision-resistant hash function and of authenticating only the *digest* of the protocol transcript. The amount of information to authenticate typically reduces to 160 bits. However, collision-resistant hash functions are threatened species these days due to collapses of MD5, RIPEMD, SHA, SHA-1, etc. [9,23,24,25,26]. Furthermore, 160 bits is still pretty large for human beings to authenticate. Another solution using shorter messages have been proposed by Pasini and Vaudenay [20] using a hash function which resists second preimage attacks (like MD5 [21]; namely: collision resistance is no longer required) and a commitment scheme. Other solutions such as MANA protocols [13, 14] have been proposed. They can reduce the amount of information to be authenticated down to 20 bits, but they work assuming a stronger hypothesis on the authenticated channel, namely that the authentication occurs without any latency for the delivery. Some protocols based on the Diffie-Hellman one were

D. Feng, D. Lin, and M. Yung (Eds.): CISC 2005, LNCS 3822, pp. 1–9, 2005.

proposed [11, 15] with an incomplete security analysis. A provably secure solution was finally proposed by Vaudenay [22]. This protocol can work with only 20 bits to authenticate and is based on a commitment scheme. Those authentication protocols *can* be pretty cheap (namely: without public-key cryptography) and provably secure (at least in the random oracle model). So, the remaining overwhelming cost is still the Diffie-Hellman protocol. Since key agreement is the foundation to public-key cryptography, it seems that setting up secure communications with an authenticated channel only cannot be solved at a lower expense than regular public-key algorithms.

The Bluetooth standard starts from a slightly different assumption, namely that there is a private channel between the two devices involving the human user. Of course, this channel should be used to transmit as few bits as possible. This would, in principle, be possible by using password-based authenticated key agreement. A first protocol family was proposed (without security proof) in 1992 by Bellovin and Merritt [8]. SRP [27, 28] is another famous protocol, available as the RFC 2945, proposed in 1998 by Wu. The security analysis followed a long research program initiated by Bellare and Rogaway [5, 6]. Specific instances of the Bellovin-Merritt protocols with security based on the random oracle model were provided in [3, 4, 7, 10, 18] starting in 2000. Finally, another protocol without random oracles were proposed in 2001 by Katz, Ostrovsky, and Yung [16]. All those protocols are however at least as expensive as the Diffie-Hellman protocol.

Despite all this nice and extensive piece of theory, standards such as Bluetooth [1, 2] stick to symmetric-key techniques (for cost reasons) and continue to use insecure protocols.

In this paper, we review the Bluetooth pairing protocol and its insecurity. The Bluetooth version 1.2 [1] mentioned (in a single sentence) the possibility to refresh keys. More details (namely, how to do so) were provided in Bluetooth version 2.0 in 2004 [2]. We finally show that this feature (that we call *repairing*) substantially increases the security and may be considered as a pragmatic costless solution. Security is based on the assumption that the radio channel (considered to be insecure by default) *sometimes* provides privacy in an unpredictable way, i.e. that the adversary Eve can in principle easily listen to the channel from time to time, but it is unlikely that she can do it *all the time* throughout the history of the devices association. This assumption is quite reasonable due to the mobility context of Bluetooth applications.

2 Bluetooth-Like Pre-pairing and the Security Issue

We assume a set of N possible participants with identifier strings ID_i. (Note that the notion of identity is rather weak since authentication will be based on a human user manipulating physical devices: it can just be a mnemonic identifier like "laser printer", maybe extended by a MAC address.) We assume that they all manage a local database of (K_j, ID_j) pairs, meaning that the current private key to be used with participant ID_j is K_j. The goal of a pairing protocol between Alice of identity ID_A and Bob of identity ID_B is to create (or replace) an entry (K, ID_B) in the database of ID_A and an entry (K, ID_A) in the database of ID_B so that the key K is the same and private to both participants.

Alice		Bob
input: $\widehat{\mathsf{ID}}_B$		**input**: $\widehat{\mathsf{ID}}_A$
private input: π_A		**private input**: π_B
pick $R^i \in_U \{0,1\}^\rho$	$\xrightarrow{R^i}$	
$K_A^i \leftarrow G(\mathsf{ID}_A, \widehat{\mathsf{ID}}_B, R^i, \pi_A)$		$K_B^i \leftarrow G(\widehat{\mathsf{ID}}_A, \mathsf{ID}_B, \hat{R}^i, \pi_B)$
final key for $\widehat{\mathsf{ID}}_B$: K_A^i		**final key for** $\widehat{\mathsf{ID}}_A$: K_B^i

Fig. 1. A One-Move Preparing Protocol

For cost reasons, nowadays wireless devices (e.g. Bluetooth devices) only use symmetric-key cryptographic protocols for establishing secure communications over insecure channels. When they connect to each other for the first time, they establish some initial private key materials K^i. Both devices, Alice and Bob, start with their identities ID_A and ID_B, pick some random numbers R_A^i and R_B^i. Additionally, a user types some random one-time private code π on both devices and both devices run a π-based authenticated key agreement protocol. When they prompt the user to type π, they may display a piece of the identifier strings (a mnemonic) for user-friendliness reasons. Due to the state of the art on symmetric-key primitives, the protocol must leak R_A^i and R_B^i so that we have

$$K^i = G(\mathsf{ID}_A, \mathsf{ID}_B, R_A^i, R_B^i, \pi)$$

for some function G. In a one-move variant, R_B^i is void so that only R_A^i (which is rather denoted R^i) needs to be sent. (See Fig. 1.)[1]

Following our setting model, π has low entropy. Indeed, the private code is typed by a human user and is typically pretty small. Eventually, exhaustive search leads to guessing π. Hence, an adversary can typically compute K^i from R^i by guessing π. The adversary only needs some information about K^i to check whether π is correct or not to run an *offline* dictionary attack. Peer authentication protocols based on K^i are based on symmetric-key cryptography. They eventually leak such an information by releasing some S and $F(S, K^i)$ for some function F from the protocol. In the Bluetooth case, this attack was described by Jakobsson and Wetzel [17].

This attack can be completed by a man-in-the-middle attack. Namely, an adversary can claim to have identity ID_B to Alice of identity ID_A and to have identity ID_A to Bob of identity ID_B. Even though the adversary does not get π from the user who wants to pair the real Alice and Bob, the adversary can easily infer it from the previous attack. The consequence is that Alice and Bob would be independently paired with the adversary even though they think they are paired together.

Those protocols can nevertheless be secure *in principle* provided that

- either enumerating all possible values for the code π is infeasible
- or the transmission of R^i is confidential.

In Section 6 we prove it in the random oracle model.

[1] By convention, notations without a hat are sent values and notations with a hat are received values. If no attack occurs, the value should not be changed by putting a hat.

3 The Two-Round Bluetooth Pairing

The Bluetooth standard [1, 2] is quite interesting in the sense that it uses a 2-round pairing protocol that we call *preparing* and *repairing*. Fig. 1 and Fig. 2 illustrate the two rounds, respectively. In a first round, a 128-bit (ephemeral) initialization key K^i is established from some random numbers R^i and π. In a second round, the final key is established from new random numbers R_A and R_B, the identities of Alice and Bob, and K^i. More precisely, the second round works as follows.

1. Bob picks a random R_B and sends $C_B = R_B \oplus K^i$ to Alice.
2. Alice picks a random R_A and sends $C_A = R_A \oplus K^i$ to Bob[2].
3. Both compute $K = H(\mathsf{ID}_A, \mathsf{ID}_B, R_A, R_B) = H(\mathsf{ID}_A, \mathsf{ID}_B, C_A \oplus K^i, C_B \oplus K^i)$.

We assume that (K, ID_B) (resp. (K, ID_A)) replaces (K^i, ID_B) (resp. (K^i, ID_A)) in the database of ID_A (resp. ID_B) so that K^i is discarded.

Alice		Bob
input: $\widehat{\mathsf{ID}}_B$		**input**: $\widehat{\mathsf{ID}}_A$
initial key for $\widehat{\mathsf{ID}}_B$: K_A^i		**initial key for** $\widehat{\mathsf{ID}}_A$: K_B^i
pick $R_A \in_U \{0,1\}^\rho$		pick $R_B \in_U \{0,1\}^\rho$
$C_A \leftarrow R_A \oplus K_A^i$	$\xrightarrow{C_A}$	$\hat{R}_A \leftarrow \hat{C}_A \oplus K_B^i$
$\hat{R}_B \leftarrow \hat{C}_B \oplus K_A^i$	$\xleftarrow{C_B}$	$C_B \leftarrow R_B \oplus K_B^i$
$K_A \leftarrow H(\mathsf{ID}_A, \widehat{\mathsf{ID}}_B, R_A, \hat{R}_B)$		$K_B \leftarrow H(\widehat{\mathsf{ID}}_A, \mathsf{ID}_B, \hat{R}_A, R_B)$
final key for $\widehat{\mathsf{ID}}_B$: K_A		**final key for** $\widehat{\mathsf{ID}}_A$: K_B

Fig. 2. The Bluetooth Repairing Protocol

Note that the internal structure of H in Bluetooth is of the form

$$H(\mathsf{ID}_A, \mathsf{ID}_B, R_A, R_B) = H'(\mathsf{ID}_A, R_A) \oplus H'(\mathsf{ID}_B, R_B).$$

Obviously, this does *not* instantiate a random oracle since we have unexpected relations such as

$$H(\mathsf{ID}_A, \mathsf{ID}_B, R_A, R_B) \oplus H(\mathsf{ID}_B, \mathsf{ID}_C, R_B, R_C) = H(\mathsf{ID}_A, \mathsf{ID}_C, R_A, R_C).$$

We further note that if Alice and Bob were already the victims of a man-in-the-middle attack, they can remain in the same attacked state if the adversary can continue an active attack. When the adversary becomes out of reach, the repairing protocol fails and Alice and Bob end in a state so that they can no longer communicate.

In Section 6 we prove that the repairing protocol alone is secure if either the initialization key is private or the communication of either C_A or C_B is private. We deduce that the preparing and repairing together achieve a secure pairing protocol provided that either π is large or the communication is private: repairing does not decrease the security. The incremental role of the repairing protocol will be made clear in the following section.

[2] It is worth noticing that Alice and Bob actually exchange R_A and R_B by using a (safe) two-time pad.