Roberto De Prisco
Moti Yung (Eds.)

Security and Cryptography for Networks

LNCS 4116

5th International Conference, SCN 2006
Maiori, Italy, September 2006
Proceedings

Springer

Roberto De Prisco Moti Yung (Eds.)

Security and Cryptography for Networks

5th International Conference, SCN 2006
Maiori, Italy, September 6-8, 2006
Proceedings

Springer

Volume Editors

Roberto De Prisco
Università di Salerno
Dipartimento di Informatica ed Applicazioni
via Ponte don Melillo, 84084 Fisciano (SA), Italy
E-mail: robdep@dia.unisa.it

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

Library of Congress Control Number: 2006931475

CR Subject Classification (1998): E.3, C.2, D.4.6, K.4.1, K.4.4, K.6.5, F.2

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-38080-9 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-38080-1 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11832072 06/3142 5 4 3 2 1 0

Preface

The Conference on Security and Cryptography for Networks 2006 (SCN 2006) was held in Maiori, Italy, on September 6-8, 2006. The conference was the fifth in the SCN series, and this year marked a change in its name (the former name was Security in Communication Networks). The name change meant to better describe the scope of the conference while preserving the SCN acronym. This year for the first time we had the proceedings volume ready at the conference. We feel that the SCN conference has matured and that it has become a tradition to hold it regularly in the beautiful setting of the Amalfitan coast as a biennial event.

The conference brought together researchers in the fields of cryptography and security in order to foster the extension of cooperation and exchange of ideas among them, aiming at assuring safety and trustworthiness of communication networks. The topics covered by the conference this year included: foundations of distributed systems security, signatures schemes, block ciphers, anonymity, e-commerce, public key encryption and key exchange, secret sharing, symmetric and public key cryptanalysis, randomness, authentication.

The international Program Committee consisted of 24 members who are top experts in the conference fields. We received 81 submissions amongst which 24 papers were selected for presentation at the conference. These proceedings include the extended abstract versions of the 24 accepted papers and the short abstract of the invited talk by Ivan Damgård.

The Program Committee selected papers on the basis of originality, quality and relevance to the conference scope. Due to the high number of submissions, paper selection was a difficult task and many good papers had to be rejected. Each paper was refereed by three or four reviewers. We thank the members of the Program Committee for their great efforts invested in the selection process. We also gratefully acknowledge the help of the external reviewers who evaluated submissions in their area of expertise. The names of these reviewers are listed on page VII, and we apologize for any inadvertent omissions or mistakes.

We also wish to thank the local organizing committee for their support in running the conference. Finally, we would like to thank the conference participants and the authors of all the submitted papers. It is the authors of all the submitted papers that allow the program committee to choose papers and to ultimately make this conference possible.

September 2006

R. De Prisco
M. Yung

SCN 2006
September 6-8, 2006, Maiori, Italy

Program Chair

Moti Yung	RSA Lab. and Columbia U., USA

General Chair

Roberto De Prisco	Università di Salerno, Italy

Program Committee

Giuseppe Ateniese	JHU, USA
Carlo Blundo	Università di Salerno, Italy
Dario Catalano	ENS, France
Alfredo De Santis	Università di Salerno, Italy
Rosario Gennaro	IBM, USA
Stuart Haber	HP, USA
Amir Herzberg	Bar-Ilan University, Israel
Nick Hopper	University of Minnesota, USA
Markus Jakobsson	Indiana University, USA
Stas Jarecki	UC Irvine, USA
Jonathan Katz	University of Maryland, USA
John Kelsey	NIST, USA
Aggelos Kiayias	University of Connecticut, USA
Eike Kiltz	CWI, Netherlands
Eyal Kushilevitz	Technion, Israel
Anna Lysyanskaya	Brown University, USA
Atsuko Miyaji	JAIST, Japan
David Naccache	ENS, France
Giuseppe Persiano	Università di Salerno, Italy
Carles Padro	Universitat Politècnica de Catalunya, Spain
Nigel Smart	University of Bristol, UK
Gene Tsudik	USC, USA
Shouhuai Xu	UTSA, USA
Moti Yung	RSA Lab. and Columbia U., USA (Chair)

Local Organization

Aniello Castiglione	Università di Salerno, Italy
Luigi Catuogno	Università di Salerno, Italy

External Referees

Michel Abdalla
Amos Beimel
Caroline Belrose
Ran Canetti
Rafi Chen
Liqun Chen
Reza Curtmola
Xuhua Ding
Orr Dunkelman
Karim Edefrawy
Jaume Martí-Farré
Serge Fehr
Amparo Fúster-Sabater
Clemente Galdi
Aline Gouget
Ignacio Gracia
Vanessa Gratzer
Tim Gneysu
Shai Halevi
Helena Handschuh
Javier Herranz
Shoichi Hirose
Dennis Hofheinz
Vishal Kher
Costas Kattirtzis
Hugo Krawczyk
Di Ma
Mitsuru Matsui
Takashi Matsunaka
Chris Mitchell
Anton Mityagin
Sean Murphy
Einar Mykletun
Svetla Nikova
Ivan Osipkov
Dan Page
Gilles Piret
Axel Poschmann
Jordi Pujolàs
S. Raj Rajagopalan
Prasad Rao
Leo Reyzin
Kouichi Sakurai
Nitesh Saxena
Taizo Shirai
Toshio Tokita
Jorge Luis Villar
Ivan Visconti
XiaoFeng Wang
Dai Watanabe
Hoeteck Wee
Stephen Weis
Christopher Wolf
Hong-Sheng Zhou

Sponsoring Institutions

Dipartimento di Informatica ed Applicazioni, Università di Salerno, Italy
Lanfredi Fund, France

Author Index

Lecture Notes in Computer Science 4116

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Lecture Notes in Computer Science

For information about Vols. 1–4037

please contact your bookseller or Springer

Vol. 4163: H. Bersini, J. Carneiro (Eds.), Artificial Immune Systems. XII, 460 pages. 2006.

Vol. 4162: R. Královič, P. Urzyczyn (Eds.), Mathematical Foundations of Computer Science 2006. XV, 814 pages. 2006.

Vol. 4153: N. Zheng, X. Jiang, X. Lan (Eds.), Advances in Machine Vision, Image Processing, and Pattern Analysis. XIII, 506 pages. 2006.

Vol. 4146: J.C. Rajapakse, L. Wong, R. Acharya (Eds.), Pattern Recognition in Bioinformatics. XIV, 186 pages. 2006. (Sublibrary LNBI).

Vol. 4144: T. Ball, R.B. Jones (Eds.), Computer Aided Verification. XV, 564 pages. 2006.

Vol. 4139: T. Salakoski, F. Ginter, S. Pyysalo, T. Pahikkala, Advances in Natural Language Processing. XVI, 771 pages. 2006. (Sublibrary LNAI).

Vol. 4138: X. Cheng, W. Li, T. Znati (Eds.), Wireless Algorithms, Systems, and Applications. XVI, 709 pages. 2006.

Vol. 4137: C. Baier, H. Hermanns (Eds.), CONCUR 2006 – Concurrency Theory. XIII, 525 pages. 2006.

Vol. 4134: K. Yi (Ed.), Static Analysis. XI, 443 pages. 2006.

Vol. 4133: J. Gratch, M. Young, R. Aylett, D. Ballin, P. Olivier (Eds.), Intelligent Virtual Agents. XIV, 472 pages. 2006. (Sublibrary LNAI).

Vol. 4130: U. Furbach, N. Shankar (Eds.), Automated Reasoning. XV, 680 pages. 2006. (Sublibrary LNAI).

Vol. 4129: D. McGookin, S. Brewster (Eds.), Haptic and Audio Interaction Design. XII, 167 pages. 2006.

Vol. 4128: W.E. Nagel, W.V. Walter, W. Lehner (Eds.), Euro-Par 2006 Parallel Processing. XXXIII, 1221 pages. 2006.

Vol. 4127: E. Damiani, P. Liu (Eds.), Data and Applications Security XX. X, 319 pages. 2006.

Vol. 4124: H. de Meer, J.P. G. Sterbenz (Eds.), Self-Organising Systems. XIV, 261 pages. 2006.

Vol. 4121: A. Biere, C.P. Gomes (Eds.), Theory and Applications of Satisfiability Testing - SAT 2006. XII, 438 pages. 2006.

Vol. 4119: C. Dony, J.L. Knudsen, A. Romanovsky, A. Tripathi (Eds.), Advanced Topics in Exception Handling Components. X, 302 pages. 2006.

Vol. 4117: C. Dwork (Ed.), Advances in Cryptology - Crypto 2006. XIII, 621 pages. 2006.

Vol. 4116: R. De Prisco, M. Yung (Eds.), Security and Cryptography for Networks. XI, 366 pages. 2006.

Vol. 4115: D.-S. Huang, K. Li, G.W. Irwin (Eds.), Computational Intelligence and Bioinformatics, Part III. XXI, 803 pages. 2006. (Sublibrary LNBI).

Vol. 4114: D.-S. Huang, K. Li, G.W. Irwin (Eds.), Computational Intelligence, Part II. XXVII, 1337 pages. 2006. (Sublibrary LNAI).

Vol. 4113: D.-S. Huang, K. Li, G.W. Irwin (Eds.), Intelligent Computing, Part I. XXVII, 1331 pages. 2006.

Vol. 4112: D.Z. Chen, D. T. Lee (Eds.), Computing and Combinatorics. XIV, 528 pages. 2006.

Vol. 4111: F.S. de Boer, M.M. Bonsangue, S. Graf, W.-P. de Roever (Eds.), Formal Methods for Components and Objects. VIII, 447 pages. 2006.

Vol. 4109: D.-Y. Yeung, J.T. Kwok, A. Fred, F. Roli, D. de Ridder (Eds.), Structural, Syntactic, and Statistical Pattern Recognition. XXI, 939 pages. 2006.

Vol. 4108: J.M. Borwein, W.M. Farmer (Eds.), Mathematical Knowledge Management. VIII, 295 pages. 2006. (Sublibrary LNAI).

Vol. 4106: T.R. Roth-Berghofer, M.H. Göker, H. A. Güvenir (Eds.), Advances in Case-Based Reasoning. XIV, 566 pages. 2006. (Sublibrary LNAI).

Vol. 4104: T. Kunz, S.S. Ravi (Eds.), Ad-Hoc, Mobile, and Wireless Networks. XII, 474 pages. 2006.

Vol. 4099: Q. Yang, G. Webb (Eds.), PRICAI 2006: Trends in Artificial Intelligence. XXVIII, 1263 pages. 2006. (Sublibrary LNAI).

Vol. 4098: F. Pfenning (Ed.), Term Rewriting and Applications. XIII, 415 pages. 2006.

Vol. 4097: X. Zhou, O. Sokolsky, L. Yan, E.-S. Jung, Z. Shao, Y. Mu, D.C. Lee, D. Kim, Y.-S. Jeong, C.-Z. Xu (Eds.), Emerging Directions in Embedded and Ubiquitous Computing. XXVII, 1034 pages. 2006.

Vol. 4096: E. Sha, S.-K. Han, C.-Z. Xu, M.H. Kim, L.T. Yang, B. Xiao (Eds.), Embedded and Ubiquitous Computing. XXIV, 1170 pages. 2006.

Vol. 4094: O. H. Ibarra, H.-C. Yen (Eds.), Implementation and Application of Automata. XIII, 291 pages. 2006.

Vol. 4093: X. Li, O.R. Zaïane, Z. Li (Eds.), Advanced Data Mining and Applications. XXI, 1110 pages. 2006. (Sublibrary LNAI).

Vol. 4092: J. Lang, F. Lin, J. Wang (Eds.), Knowledge Science, Engineering and Management. XV, 664 pages. 2006. (Sublibrary LNAI).

Vol. 4091: G.-Z. Yang, T. Jiang, D. Shen, L. Gu, J. Yang (Eds.), Medical Imaging and Augmented Reality. XIII, 399 pages. 2006.

Vol. 4090: S. Spaccapietra, K. Aberer, P. Cudré-Mauroux (Eds.), Journal on Data Semantics VI. XI, 211 pages. 2006.

Vol. 4089: W. Löwe, M. Südholt (Eds.), Software Composition. X, 339 pages. 2006.

Vol. 4088: Z.-Z. Shi, R. Sadananda (Eds.), Agent Computing and Multi-Agent Systems. XVII, 827 pages. 2006. (Sublibrary LNAI).

Vol. 4085: J. Misra, T. Nipkow, E. Sekerinski (Eds.), FM 2006: Formal Methods. XV, 620 pages. 2006.

Vol. 4082: K. Bauknecht, B. Pröll, H. Werthner (Eds.), E-Commerce and Web Technologies. XIII, 243 pages. 2006.

Vol. 4081: A M. Tjoa, J. Trujillo (Eds.), Data Warehousing and Knowledge Discovery. XVII, 578 pages. 2006.

Vol. 4079: S. Etalle, M. Truszczyński (Eds.), Logic Programming. XIV, 474 pages. 2006.

Vol. 4077: M.-S. Kim, K. Shimada (Eds.), Geometric Modeling and Processing - GMP 2006. XVI, 696 pages. 2006.

Vol. 4076: F. Hess, S. Pauli, M. Pohst (Eds.), Algorithmic Number Theory. X, 599 pages. 2006.

Vol. 4075: U. Leser, F. Naumann, B. Eckman (Eds.), Data Integration in the Life Sciences. XI, 298 pages. 2006. (Sublibrary LNBI).

Vol. 4074: M. Burmester, A. Yasinsac (Eds.), Secure Mobile Ad-hoc Networks and Sensors. X, 193 pages. 2006.

Vol. 4073: A. Butz, B. Fisher, A. Krüger, P. Olivier (Eds.), Smart Graphics. XI, 263 pages. 2006.

Vol. 4072: M. Harders, G. Székely (Eds.), Biomedical Simulation. XI, 216 pages. 2006.

Vol. 4071: H. Sundaram, M. Naphade, J.R. Smith, Y. Rui (Eds.), Image and Video Retrieval. XII, 547 pages. 2006.

Vol. 4070: C. Priami, X. Hu, Y. Pan, T.Y. Lin (Eds.), Transactions on Computational Systems Biology V. IX, 129 pages. 2006. (Sublibrary LNBI).

Vol. 4069: F.J. Perales, R.B. Fisher (Eds.), Articulated Motion and Deformable Objects. XV, 526 pages. 2006.

Vol. 4068: H. Schärfe, P. Hitzler, P. Øhrstrøm (Eds.), Conceptual Structures: Inspiration and Application. XI, 455 pages. 2006. (Sublibrary LNAI).

Vol. 4067: D. Thomas (Ed.), ECOOP 2006 – Object-Oriented Programming. XIV, 527 pages. 2006.

Vol. 4066: A. Rensink, J. Warmer (Eds.), Model Driven Architecture – Foundations and Applications. XII, 392 pages. 2006.

Vol. 4065: P. Perner (Ed.), Advances in Data Mining. XI, 592 pages. 2006. (Sublibrary LNAI).

Vol. 4064: R. Büschkes, P. Laskov (Eds.), Detection of Intrusions and Malware & Vulnerability Assessment. X, 195 pages. 2006.

Vol. 4063: I. Gorton, G.T. Heineman, I. Crnkovic, H.W. Schmidt, J.A. Stafford, C.A. Szyperski, K. Wallnau (Eds.), Component-Based Software Engineering. XI, 394 pages. 2006.

Vol. 4062: G. Wang, J.F. Peters, A. Skowron, Y. Yao (Eds.), Rough Sets and Knowledge Technology. XX, 810 pages. 2006. (Sublibrary LNAI).

Vol. 4061: K. Miesenberger, J. Klaus, W. Zagler, A. Karshmer (Eds.), Computers Helping People with Special Needs. XXIX, 1356 pages. 2006.

Vol. 4060: K. Futatsugi, J.-P. Jouannaud, J. Meseguer (Eds.), Algebra, Meaning, and Computation. XXXVIII, 643 pages. 2006.

Vol. 4059: L. Arge, R. Freivalds (Eds.), Algorithm Theory – SWAT 2006. XII, 436 pages. 2006.

Vol. 4058: L.M. Batten, R. Safavi-Naini (Eds.), Information Security and Privacy. XII, 446 pages. 2006.

Vol. 4057: J.P.W. Pluim, B. Likar, F.A. Gerritsen (Eds.), Biomedical Image Registration. XII, 324 pages. 2006.

Vol. 4056: P. Flocchini, L. Gąsieniec (Eds.), Structural Information and Communication Complexity. X, 357 pages. 2006.

Vol. 4055: J. Lee, J. Shim, S.-g. Lee, C. Bussler, S. Shim (Eds.), Data Engineering Issues in E-Commerce and Services. IX, 290 pages. 2006.

Vol. 4054: A. Horváth, M. Telek (Eds.), Formal Methods and Stochastic Models for Performance Evaluation. VIII, 239 pages. 2006.

Vol. 4053: M. Ikeda, K.D. Ashley, T.-W. Chan (Eds.), Intelligent Tutoring Systems. XXVI, 821 pages. 2006.

Vol. 4052: M. Bugliesi, B. Preneel, V. Sassone, I. Wegener (Eds.), Automata, Languages and Programming, Part II. XXIV, 603 pages. 2006.

Vol. 4051: M. Bugliesi, B. Preneel, V. Sassone, I. Wegener (Eds.), Automata, Languages and Programming, Part I. XXIII, 729 pages. 2006.

Vol. 4049: S. Parsons, N. Maudet, P. Moraitis, I. Rahwan (Eds.), Argumentation in Multi-Agent Systems. XIV, 313 pages. 2006. (Sublibrary LNAI).

Vol. 4048: L. Goble, J.-J.C.. Meyer (Eds.), Deontic Logic and Artificial Normative Systems. X, 273 pages. 2006. (Sublibrary LNAI).

Vol. 4047: M. Robshaw (Ed.), Fast Software Encryption. XI, 434 pages. 2006.

Vol. 4046: S.M. Astley, M. Brady, C. Rose, R. Zwiggelaar (Eds.), Digital Mammography. XVI, 654 pages. 2006.

Vol. 4045: D. Barker-Plummer, R. Cox, N. Swoboda (Eds.), Diagrammatic Representation and Inference. XII, 301 pages. 2006. (Sublibrary LNAI).

Vol. 4044: P. Abrahamsson, M. Marchesi, G. Succi (Eds.), Extreme Programming and Agile Processes in Software Engineering. XII, 230 pages. 2006.

Vol. 4043: A.S. Atzeni, A. Lioy (Eds.), Public Key Infrastructure. XI, 261 pages. 2006.

Vol. 4042: D. Bell, J. Hong (Eds.), Flexible and Efficient Information Handling. XVI, 296 pages. 2006.

Vol. 4041: S.-W. Cheng, C.K. Poon (Eds.), Algorithmic Aspects in Information and Management. XI, 395 pages. 2006.

Vol. 4040: R. Reulke, U. Eckardt, B. Flach, U. Knauer, K. Polthier (Eds.), Combinatorial Image Analysis. XII, 482 pages. 2006.

Vol. 4039: M. Morisio (Ed.), Reuse of Off-the-Shelf Components. XIII, 444 pages. 2006.

Vol. 4038: P. Ciancarini, H. Wiklicky (Eds.), Coordination Models and Languages. VIII, 299 pages. 2006.

Table of Contents

Public Key Encryption and Key Exchange

Secret Sharing

Symmetric Key Cryptanalysis and Randomness

Applied Authentication

Public Key Related Cryptanalysis

Invited Talk

Edge Eavesdropping Games

Amos Beimel[1,*] and Matthew Franklin[2,**]

[1] Department of Computer Science, Ben-Gurion University
[2] Department of Computer Science, University of California, Davis

Abstract. Motivated by the proactive security problem, we study the question of maintaining secrecy against a mobile eavesdropper that can eavesdrop to a bounded number of *communication channels* in each round of the protocol. We characterize the networks in which secrecy can be maintained against an adversary that can eavesdrop to t channels in each round. Using this characterization, we analyze the number of eavesdropped channels that complete graphs can withhold while maintaining secrecy.

Keywords: unconditional security, passive adversary, mobile adversary, graph search games.

1 Introduction

Many cryptographic protocols are secure if an unknown *fixed* set of processors of bounded size is dishonest. Proactive security [13,9] considers a more realistic scenario, where a mobile adversary can control a different set of processors of bounded size in each period. Protocols in the proactive model have to cope with a stronger adversary, which, for example, might have controlled every processor by some point during the protocol execution. In protocols secure in the proactive model, each processor has to "spread" the secret information it holds.

Franklin, Galil, and Yung [6] studied maintaining secrecy against a mobile eavesdropper which can eavesdrop to a bounded number of processors in each round of the protocol. Unfortunately, we discovered that the main characterization given in [6] of maintaining secrecy against a mobile eavesdropper is incorrect. We describe the flaw in their proof and the correct characterization, see Section 1.2. The main focus of this paper is a similar question, where a mobile eavesdropper can eavesdrop to a bounded number of *communication channels* in each round of the protocol. As eavesdropping to communication channels is easier than eavesdropping to processors, this is a natural question. Although the two problems are similar, there are differences between the two problems, for example in the number of rounds that an adversary can learn the secret information in a complete graph while eavesdropping to minimal number of vertices or edges respectively.

* On sabbatical at the University of California, Davis, partially supported by the Packard Foundation.

** Partially supported by NSF and the Packard Foundation.

R. De Prisco and M. Yung (Eds.): SCN 2006, LNCS 4116, pp. 1–17, 2006.

To model the question of maintaining the secrecy of a system against a mobile adversary that can eavesdrop to communication channels, we consider the following abstract game, similar to [6], called the distributed database maintenance game. There is a protocol trying to maintain the secrecy of one bit b in the system. The first stage in the game is an initialization stage in which each edge gets an initial value. (This abstracts an intermediate state of a more complex protocol.) In Round i, each vertex receives messages, and sends messages generated based on the messages it received in the previous round and a "fresh" random string. The secret bit b can be reconstructed in each round of the protocol from the messages sent in the system in that round. The mobile adversary eavesdrops to t channels of its choice in each round. We require that an unbounded adversary cannot learn the secret from the messages it heard. The adversary can only eavesdrop to channels; it cannot change, insert, or delete messages.

Following [6], because of the close connection with "graph search games [14,11]," we refer to the eavesdropping to a channel as placing a "guard" on this edge, and we say that a graph is "cleared" at the end of a "search" (finite sequence of subsets of edges the adversary eavesdrops) if the adversary has collected enough information to infer the secret bit b. A protocol maintaining privacy should prevent the adversary from clearing the graph.

We consider two variants of the edge eavesdropping game, depending on whether the underlying communication network is modeled as a directed or an undirected graph. When the network is modeled as an undirected graph, each edge is a full-duplex channel, and a single eavesdropper can monitor the message flow in both directions. When the network is modeled as a directed graph, each edge allows communication in one direction only, and a single eavesdropper can monitor the message flow in that direction only. Note that a full-duplex channel can be represented as a pair of directed edges, but then two eavesdroppers are required to monitor the message flow in both directions.

To see some of the subtleties of edge eavesdropping games, consider the three graphs described in Fig. 1. A single guard can clear these graphs, and thus the distributed database maintenance game on these networks is defeated by an adversary controlling a single mobile eavesdropper. An explanation of these examples can be found in Example 1 in Section 3.1 and in Section 4.3.

1.1 Our Results

Our first result (Theorem 1) is a characterization of when a search clears a graph. Given a directed or undirected graph G and given a search of length ℓ, we construct an undirected layered version of the graph where the number of layers is the length of the search. In the layered graph there are $\ell + 1$ copies of each vertex, and there is an edge between the ith copy of u to the $(i+1)$th copy of w iff there is an edge between u and v in G. We prove that a search clears a graph iff it cuts the first layer from the last layer in the layered graph. That is, we prove that:

- If there is a search that cuts the first layer from the last layer in the layered graph, then no protocol can maintain privacy against this search. This is proved by a reduction to the impossibility of unconditional key exchange.

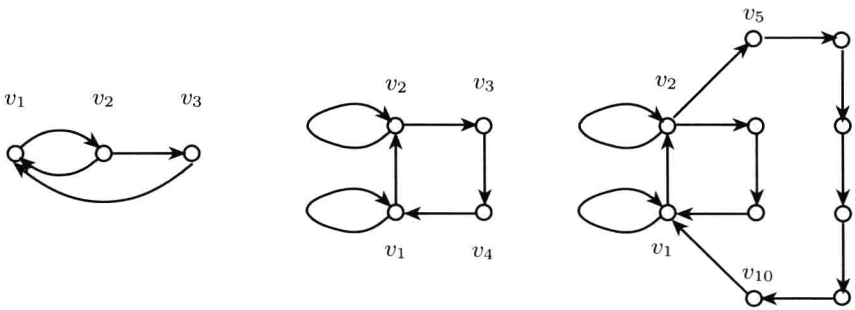

Fig. 1. Three graphs that can be cleared with one guard

– If there is no search with t guards that cuts the first layer from the last layer, then there is a simple protocol that can maintain privacy against any adversary that can eavesdrop to t channels in each round.

Inspired by this characterization, we say that an undirected path in the layered graph is contaminated if all edges in the path are unguarded; a vertex is contaminated after i rounds of the search if there is a contaminated path (through any layers) from the first layer to the copy of the vertex in layer i. That is, contamination "flows" both forwards and backwards in time.

We give a second characterization (Theorem 2) of when a search clears a graph based on the sets of contaminated vertices in each round of the protocol. This characterization is more useful for analyzing the possibility and impossibility of clearing graphs. Based on this second characterization, we prove an upper bound on the length of the search (Theorem 3): If an adversary can clear a graph while eavesdropping to at most t edges in each round, then it can clear the graph in at most 2^n rounds while eavesdropping to at most t edges in each round. We do not know if super-polynomial search length is sometimes necessary.

A search is "monotonic" if once a vertex is cleared, it will remain clear for the entire search. We explore the usefulness and limitations of a generic monotonic searches. On the positive side, we show that monotonic search is essentially optimal for directed and undirected complete graphs. A complete *directed* graph with n vertices can be cleared by $n^2/2$ guards in two rounds when n is even (by monotonic search). We prove that $n^2/2$ guards are required to clear this graph no matter how many rounds the adversary is allowed (by any search). For a complete *undirected* graph with n vertices, we show that it can be cleared by $n^2/4 + n/2$ guards in $O(\sqrt{n})$ rounds (by monotonic search). Furthermore, we prove that $n^2/4 + n/2$ guards are required to clear this graph no matter how many rounds the adversary is allowed (by any search), and $\Omega(\sqrt{n})$ rounds are required to clear the graph even if the adversary uses $n^2/4+O(n)$ guards (by any search). In contrast, with $3n^2/8 + n/4$ guards, the complete undirected graph can be cleared in two rounds (by monotonic search).

1.2 Comparison to the Vertex Eavesdropping Game

The problem we consider is similar to the vertex eavesdropping games considered in [6]. In the vertex eavesdropping game, a mobile adversary eavesdrops to processors – it monitors their internal state, the computations they perform, and the messages they send and receive. A search is a finite sequence of subsets of vertices; a search succeeds ("clears the graph") if the adversary learns enough information to infer the secret bit b in the distributed database maintenance game. Unfortunately, the main characterization given in [6] of successful searches is incorrect. The correct characterization is similar to the edge eavesdropping games: Given a directed or undirected graph, and given a search, construct the *undirected* layered version of the graph where the number of layers is the length of the search (and with all self-loops added, i.e., an edge from each node in each non-final layer to the same node in the next layer). A search clears a graph iff it cuts the first layer from the last layer in the *undirected* layered graph.

The mistake in [6] is that they considered the *directed* layered version of the graph instead of the undirected case. In particular, the flaw is in the proof of Lemma 4 of [6], i.e., Alice cannot simulate the behavior of every node in V_s by herself. A graph demonstrating this problem is described in Appendix A. The characterization of [6] is correct if we require that each vertex is *deterministic* during the execution of the protocol.

Although, the vertex eavesdropping game and the edge eavesdropping game seem similar, there are differences between them. For example, the search of complete graphs is simple in the vertex eavesdropping game: the complete graph with n vertices can be cleared with n guards in one round, and cannot be cleared by fewer guards in any number of rounds. By contrast, the search of undirected complete graphs in the edge eavesdropping game is more complicated as it requires $\Omega(\sqrt{n})$ rounds even if near optimal number of guards are used. See Sections 4 and 5 for a detailed treatment.

In [6] it was shown that for *directed* layered graphs, super-polynomial search length is sometimes necessary: There exists a family of graphs $\{G_n\}$ such that each G_n has $O(n^2)$ vertices, however, clearing the directed layered graph of G_n requires $\Omega(2^n)$ rounds using the optimal number of guards. This should be contrasted with classic search games, in which linear number of rounds are sufficient to clear a graph with optimal number of guards [12,2] (for background on search games on graphs [14,11]). However, due to the problem in the characterization of [6], the above sequence of graphs *does not* imply that in vertex eavesdropping games super-polynomial search length is sometimes necessary. It is not known if super-polynomial search length is ever necessary for the vertex eavesdropping game or for the edge eavesdropping game.

1.3 Historical Background

Ostrovsky and Yung [13] considered mobile faults under the control of a Byzantine adversary to achieve general secure distributed computation against virus-like waves of attack. Defense against mobile Byzantine faults was subsequently