

# Curriculum Vitae

Markus Jakobsson  
markus@indiana.edu

April 25, 2006

## Milestones

- Associate Professor of Informatics, Indiana University Bloomington, 2004 –
- Associate Director, the Center of Applied Cybersecurity Research, 2004 –
- Co-founder, RavenWhite, 2005
- Visiting Research Fellow, Anti-Phishing Working Group, 2006 –
- Adjunct Associate Professor, New York University, 2002 – 2004
- Principal Research Scientist, RSA Laboratories, 2001 – 2004
- Member of Technical Staff, Bell Laboratories, 1997 – 2001
- PhD in Computer Science, University of California at San Diego (Advisor: Russell Impagliazzo), 1997
- M.Sc (Civilingenjör) in Computer Engineering, Lund Institute of Technology, 1993
- Researcher, San Diego Supercomputer Center and General Atomics 1996 – 1997
- Founder, Datopia, 1987
- Self-supporting multi-cell organism, 1968

A detailed list of consulting engagements is available upon request.

## Professional Activities

My current and recent professional involvement in the cryptographic community includes participation on the program committees of WOTE '06, ACISP '06, WWW '06, PET '06, ICC '06, PerSec '06, RSA-CT '06, Escar '05, VANET '05, CNIS '05, ESAS '05, TSPUC '05, MADNES '05, PET '05, ICISC '05, NordSec '05, VANET '04, PET '04, 2004 ACM International Conference on Information Security, ISC '04, WiSe '03, ACNS '03, ICISC '03, PET '03, FC '03, DRM '03, ICISC '02, Eurocrypt '02, RSA '02, PET '02, SPDRM '01, ICISC '01, DialM '01, Eurocrypt '00, PKC '00, Nordsec '00, Asiacypt '99, ACM Security '99, Financial Cryptography '99, Public Key Cryptography '99 and Eurocrypt '98.

I served as the program co-chair for ACNS '04, WiSe '05, WiSe '04 and a DIMACS workshop on voting. I am the general chair for Crypto '07. I have served as vice president of the International Financial Cryptography Association. I am an area editor of MC2R and on the board of IOS press. A list of PhD committees I have served on is available upon request.

## Publications

### Books

1. M. Jakobsson, S. Myers, “Phishing and Countermeasures”, 850 pages, Wiley, 2006.
2. W. Mao, M. Jakobsson, “Cryptographic Protocols”, 1025 pages, Addison-Wesley, 2006.
3. G. Jakobsson, M. Jakobsson, and M. Persson “NO till vardags” ISBN 91 88070 14 X, 2000.

### Academic Articles

1. P. Golle, X. Wang, M. Jakobsson, A. Tsow, “Deterring Voluntary Trace Disclosure in Re-encryption Mix Networks.” IEEE S&P '06
2. M. Jakobsson, A. Juels, T. Jagatic, “Cache Cookies for Browser Authentication,”? IEEE S&P '06
3. M. Jakobsson and J. Ratkiewicz, “Designing Ethical Phishing Experiments: A study of (ROT13) rOnl auction query features.”? WWW '06
4. M. Jakobsson and S. Stamm. “Invasive Browser Sniffing and Countermeasures.” WWW '06
5. J.Y. Choi, P. Golle and M. Jakobsson. “Auditable Privacy: On Tamper-Evident Mix Networks.” Financial Crypto '06
6. T. Jagatic, N. Johnson, M. Jakobsson, F. Menczer. “Social Phishing.” Communications of the ACM 2006
7. A. Juels, D. Catalano and M. Jakobsson. “Coercion-Resistant Electronic Elections.” WPES '05
8. N. Ben Salem, J.-P. Hubaux, M. Jakobsson. “Reputation-based Wi-Fi Deployment.” Mobile Computing and Communications Review, Volume 9, Number 3 ?(Best papers of WMASH 2004)
9. V. Griffith and M. Jakobsson. “Messin’ with Texas, Deriving Mother’s Maiden Names Using Public Records.” ACNS '05, 2005
10. M. Jakobsson and L. Yang. “Quantifying Security in Hybrid Cellular Networks.” ACNS '05, 2005
11. Y.-C. Hu, M. Jakobsson, and A. Perrig. “Efficient Constructions for One-way Hash Chains.” ACNS '05, 2005
12. N. Ben Salem, J. P. Hubaux, and M. Jakobsson. “Node Cooperation in Hybrid Ad hoc Networks.” IEEE Transactions on Mobile Computing, Vol. 5, No. 4, April 2006.
13. P. MacKenzie, T. Shrimpton, and M. Jakobsson. “Threshold Password-Authenticated Key Exchange.” Journal of Cryptology, 2005
14. M. Jakobsson. “Modeling and Preventing Phishing Attacks.” Phishing Panel in Financial Cryptography '05. 2005.
15. N. Ben Salem, J.-P. Hubaux, and M. Jakobsson. “Reputation-based Wi-Fi Deployment Protocols and Security Analysis.” In WMASH '04. ACM Press, 2004. pp. 29–40.
16. M. Jakobsson and S. Wetzel. “Efficient Attribute Authentication with Applications to Ad Hoc Networks.” In VANET '04. ACM Press, 2004. pp. 38–46.
17. M. Jakobsson, X. Wang, and S. Wetzel. “Stealth Attacks in Vehicular Technologies.” Invited paper. In Proceedings of IEEE Vehicular Technology Conference 2004 Fall (VTC-Fall 2004). IEEE, 2004.

18. M. Jakobsson, “Cryptographic Protocols.” Chapter from *The Handbook of Information Security*. Hossein Bidgoli, Editor-in-Chief. Copyright John Wiley & Sons, Inc., 2005, Hoboken, N.J.
19. M. Jakobsson, “Cryptographic Privacy Protection Techniques.” Chapter from *The Handbook of Information Security*. Hossein Bidgoli, Editor-in-Chief. Copyright John Wiley & Sons, Inc., 2005, Hoboken, N.J.
20. A. Ambainis, H. Lipmaa, and M. Jakobsson. “Cryptographic Randomized Response Technique.” In *PKC '04*. LNCS 2947. Springer-Verlag, 2004. pp. 425–438.
21. P. Golle, M. Jakobsson, A. Juels, and P. Syverson. “Universal Re-encryption for Mixnets.” In *CT-RSA '04*. LNCS 2964. Springer-Verlag, 2004. pp. 163–178.
22. P. Golle and M. Jakobsson. “Reusable Anonymous Return Channels.” In *WPES '03*. ACM Press, 2003. pp. 94–100.
23. M. Jakobsson, S. Wetzel, B. Yener. “Stealth Attacks on Ad-Hoc Wireless Networks.” In *IEEE VTC '03*, 2003.
24. M. Jakobsson and F. Menczer. “Untraceable Email Cluster Bombs: On Agent-Based Distributed Denial of Service.” CoRR preprint. 2003.
25. M. Jakobsson, J. Linn, and J. Algesheimer. “How to Protect Against a Militant Spammer.” ePrint archive. Report 2003/071. 2003.
26. N. Ben Salem, L. Buttyan, J.-P. Hubaux, and M. Jakobsson. “A Charging and Rewarding Scheme for Packet Forwarding in Multi-hop Cellular Networks.” In *ACM MobiHoc '03*. ACM Press, 2003. pp. 13–24.
27. M. Jakobsson, J.-P. Hubaux and L. Buttyan. “A Micro-Payment Scheme Encouraging Collaboration in Multi-Hop Cellular Networks.” In *FC '03*. LNCS 2742. Springer-Verlag, 2003. pp. 15–33.
28. M. Jakobsson, T. Leighton, S. Micali and M. Szydlo. “Fractal Merkle Tree Representation and Traversal.” In *RSA-CT '03* 2003.
29. A. Boldyreva and M. Jakobsson. “Theft protected proprietary certificates.” In *DRM '02*. LNCS 2696, 2002. pp. 208–220.
30. P. Golle, S. Zhong, M. Jakobsson, A. Juels, and D. Boneh. “Optimistic Mixing for Exit-Polls.” In *Asiacrypt '02*. LNCS 2501. Springer-Verlag, 2002. pp. 451–465.
31. P. MacKenzie, T. Shrimpton, and M. Jakobsson. “Threshold Password-Authenticated Key Exchange.” In *CRYPTO '02*. LNCS 2442. Springer-Verlag, 2002. pp. 385–400.
32. M. Jakobsson. “Fractal Hash Sequence Representation and Traversal.” One-page abstract. In *Proceedings of the 2002 IEEE International Symposium on Information Theory (ISIT '02)*. 2002. pp. 437–444.
33. M. Jakobsson, A. Juels, and R. Rivest. “Making Mix Nets Robust For Electronic Voting By Randomized Partial Checking.” In *Proceedings of the 11th USENIX Security Symposium*. USENIX Association, 2002. pp. 339–353.
34. D. Coppersmith and M. Jakobsson. “Almost Optimal Hash Sequence Traversal.” In *Financial Crypto '02*. 2002.
35. M. Jakobsson. “Financial Instruments in Recommendation Mechanisms.” In *Financial Crypto '02*. 2002.
36. J. Garay, and M. Jakobsson. “Timed Release of Standard Digital Signatures.” In *Financial Crypto '02*. 2002.

37. F. Menczer, N. Street, N. Vishwakarma, A. Monge, and M. Jakobsson. “Intellishopper: A Proactive, Personal, Private Shopping Assistant.” In AAMAS '02. ACM Press, 2002. pp. 1001–1008.
38. M. Jakobsson and M. Reiter. “Discouraging Software Piracy Using Software Aging.” In DRM '01. LNCS 2320. Springer-Verlag, 2002. pp. 1–12.
39. M. Jakobsson, A. Juels, and P. Nguyen. “Proprietary Certificates.” In CT-RSA '02. LNCS 2271. Springer-Verlag, 2002. pp. 164–181.
40. M. Jakobsson and A. Juels. “An Optimally Robust Hybrid Mix Network.” In PODC '01. ACM Press. 2001. pp. 284–292.
41. M. Jakobsson and S. Wetzel. “Security Weaknesses in Bluetooth.” In CT-RSA '01. LNCS 2020. Springer-Verlag, 2001. pp. 176–191.
42. M. Jakobsson and D. Pointcheval. “Mutual Authentication for Low-Power Mobile Devices.” In Financial Crypto '01. LNCS 2339. Springer-Verlag, 2001. pp. 178–195.
43. M. Jakobsson, D. Pointcheval, and A. Young. “Secure Mobile Gambling.” In CT-RSA '01. LNCS 2020. Springer-Verlag, 2001. pp. 110–125.
44. M. Jakobsson and S. Wetzel. “Secure Server-Aided Signature Generation.” In PKC '01. LNCS 1992. Springer-Verlag, 2001. pp. 383–401.
45. M. Jakobsson and A. Juels. “Addition of ElGamal Plaintexts.” In T. Okamoto, ed., ASIACRYPT '00. LNCS 1976. Springer-Verlag, 2000. pp. 346–358.
46. M. Jakobsson, and A. Juels. “Mix and Match: Secure Function Evaluation via Ciphertexts.” In ASIACRYPT '00. LNCS 1976. Springer-Verlag, 2000. pp. 162–177.
47. R. Arlein, B. Jai, M. Jakobsson, F. Monrose, and M. Reiter. “Privacy-Preserving Global Customization.” In ACM E-Commerce '00. ACM Press, 2000. pp. 176–184.
48. C.-P. Schnorr and M. Jakobsson. “Security of Signed ElGamal Encryption.” In ASIACRYPT '00. LNCS 1976. Springer-Verlag, 2000. pp. 73–89.
49. A. Juels, M. Jakobsson, E. Shriver, and B. Hillyer. “How To Turn Loaded Dice Into Fair Coins.” IEEE Transactions on Information Theory, vol. 46(3). May 2000. pp. 911–921.
50. P. Bohannon, M. Jakobsson, and S. Srikwan. “Cryptographic Approaches to Privacy in Forensic DNA Databases.” In Public Key Cryptography '00. LNCS 1751. Springer-Verlag, 2000. pp. 373–390.
51. J. Garay, M. Jakobsson, and P. MacKenzie. “Abuse-free Optimistic Contract Signing.” In CRYPTO '99. LNCS 1666. Springer-Verlag, 1999. pp. 449–466.
52. M. Jakobsson. “Flash Mixing.” In PODC '99. ACM Press, 1999. pp. 83–89.
53. G. Di Crescenzo, N. Ferguson, R. Impagliazzo, and M. Jakobsson. “How To Forget a Secret.” In STACS '99. LNCS 1563. Springer-Verlag, 1999. pp. 500–509.
54. M. Jakobsson, D. M'Raihi, Y. Tsiounis, and M. Yung. “Electronic Payments: Where Do We Go from Here?.” In CQRE (Secure) '99. LNCS 1740. Springer-Verlag, 1999. pp. 43–63.
55. C.P. Schnorr and M. Jakobsson. “Security Of Discrete Log Cryptosystems in the Random Oracle + Generic Model.” In Conference on The Mathematics of Public-Key Cryptography. 1999.
56. M. Jakobsson and A. Juels “Millimix: Mixing in Small Batches.” DIMACS Technical Report 99-33, 1999.
57. M. Jakobsson and A. Juels “Proofs of Work and Breadpudding Protocols.” In CMS '99. IFIP Conference Proceedings, Vol. 152. Kluwer, B.V., 1999. pp. 252272.

58. M. Jakobsson and C-P Schnorr. "Efficient Oblivious Proofs of Correct Exponentiation." In CMS '99. IFIP Conference Proceedings, Vol. 152. Kluwer, B.V., 1999. pp. 71–86.
59. M. Jakobsson, P. MacKenzie, and J.P. Stern. "Secure and Lightweight Advertising on the Web." In World Wide Web '99. Journal of Computer Networks, vol. 31, issue 11–16, Elsevier North-Holland, Inc., 1999. pp. 1101–1109.
60. M. Jakobsson, J.P. Stern, and M. Yung. "Scramble All, Encrypt Small." In Fast Software Encryption '99. LNCS 1636. Springer-Verlag, 1999. pp. 95–111.
61. M. Jakobsson and J. Mueller. "Improved Magic Ink Signatures Using Hints." In Financial Cryptography '99. LNCS 1648. Springer-Verlag, 1999. pp. 253–268.
62. M. Jakobsson. "Mini-Cash: A Minimalistic Approach to E-Commerce." In Public Key Cryptography '99. LNCS 1560. Springer-Verlag, 1999. pp. 122–135.
63. M. Jakobsson. "On Quorum Controlled Asymmetric Proxy Re-encryption." In Public Key Cryptography '99. LNCS 1560. Springer-Verlag, 1999. pp. 112–121.
64. M. Jakobsson and A. Juels. "X-Cash: Executable Digital Cash." In Financial Cryptography '98. LNCS 1465. Springer-Verlag, 1998. pp. 16–27.
65. M. Jakobsson and D. M'Raihi. "Mix-based Electronic Payments." In Proceedings of the Selected Areas in Cryptography. LNCS 1556. Springer-Verlag, 1998. pp. 157173.
66. M. Jakobsson, E. Shriver, B. Hillyer, and A. Juels. "A Practical Secure Physical Random Bit Generator." In CCS '98: Proceedings of the 5th ACM conference on Computer and communications security. ACM Press, 1998. pp. 103–111.
67. M. Jakobsson. "A Practical Mix." In Advances in Cryptology – EuroCrypt '98. LNCS 1403. Springer-Verlag, 1998. pp. 448–461.
68. M. Jakobsson and M. Yung. "On Assurance Structures for WWW Commerce." In Financial Cryptography '98. LNCS 1465. Springer-Verlag, 1998. pp. 141–157.
69. E. Gabber, M. Jakobsson, Y. Matias, and A. Mayer. "Curbing Junk E-Mail via Secure Classification." In Financial Cryptography '98. LNCS 1465. Springer-Verlag, 1998. pp. 198–213.
70. M. Jakobsson. "Privacy vs. Authenticity." Ph.D. Thesis, University of California at San Diego. 1997
71. M. Jakobsson and M. Yung. "Distributed "Magic Ink" Signatures." In Advances in Cryptology – EuroCrypt '97. LNCS 1233. Springer-Verlag, 1997. pp. 450–464.
72. M. Jakobsson and M. Yung. "Applying Anti-Trust Policies to Increase Trust in a Versatile E-Money System." In Financial Cryptography '97. LNCS 1318. Springer-Verlag, 1997. pp. 217–238.
73. A. Herzberg, M. Jakobsson, S. Jarecki, H. Krawczyk, and M. Yung. "Proactive public-key and signature schemes." In Proceedings of the 4th Annual Conference on Computer Communications Security. ACM Press, 1997. pp. 100–110.
74. M. Bellare, M. Jakobsson, and M. Yung. "Round-Optimal Zero-Knowledge Arguments Based on any One-Way Function." In Advances in Cryptology – EuroCrypt '97. LNCS 1233. Springer-Verlag, 1997. pp. 280–305.
75. M. Jakobsson and M. Yung. "Proving Without Knowing." In Crypto '96. LNCS 1109. Springer-Verlag, 1996. pp. 186–200.
76. M. Jakobsson, K. Sako, and R. Impagliazzo. "Designated Verifier Proofs and Their Applications." In Advances in Cryptology – EuroCrypt '96. LNCS 1070. Springer-Verlag, 1996. pp. 143–154.

77. M. Jakobsson and M. Yung. “Revokable and Versatile Electronic Money.” In CCS ’96: Proceedings of the 3rd ACM conference on Computer and communications security. ACM Press, 1996. pp. 76–87.
78. M. Jakobsson. “Ripping Coins for a Fair Exchange.” In Advances in Cryptology – EuroCrypt ’95. LNCS 921. Springer-Verlag, 1995. pp. 220–230.
79. M. Jakobsson. “Blackmailing using Undeniable Signatures.” In Advances in Cryptology – EuroCrypt ’94. LNCS 950. Springer-Verlag, 1994. pp. 425–427.
80. M. Jakobsson. “Reducing costs in identification protocols.” Rump Session, InCrypto ’92, 1992.
81. M. Jakobsson. “Machine-Generated Music with Themes.” In International Conference on Artificial Neural Networks ’92. Vol 2. Amsterdam: Elsevier, 1992. pp. 1645–1646

## Patent Publications

1. Software aging method and apparatus for discouraging software piracy
2. Method and apparatus for ensuring security of users of short range wireless enable devices
3. Verification of correct exponentiation or other operations in cryptographic applications
4. Method, apparatus, and article of manufacture for generating secure recommendations from market-based financial instrument prices
5. Secure distributed computation in cryptographic applications
6. Non malleable encryption method and apparatus using key-encryption keys and digital signature
7. Generation of repeatable cryptographic key based on varying parameters
8. System and method for incorporating advertising into printed images and printer having the same
9. Mixing in small batches
10. Mix and match: a new approach to secure multiparty computation
11. Method and system for providing translation certificates
12. Digital signatures having revokable anonymity and improved traceability
13. Flash mixing apparatus and method
14. Method and system for quorum controlled asymmetric proxy encryption
15. System and method for secure classification of electronic mail
16. Method and apparatus for ensuring security of users of bluetooth TM-enabled devices
17. Minimalistic electronic commerce system
18. Non malleable encryption apparatus and method
19. Probabilistic theft deterrence
20. Method and apparatus for extracting unbiased random bits from a potentially biased source of randomness
21. Practical mix-based election scheme
22. Storage device random bit generator
23. Executable digital cash for electronic commerce
24. Method and apparatus for encrypting, decrypting, and providing privacy for data values

## Awards and Grants

- Microsoft's Trusted Computing grant, 2005 (together with Fred Cate)
- E. Lundstroms Stiftelse, 1995
- von Beskows Stiftelse, The Royal Swedish Academy of Sciences, 1993
- G.S. Magnussons Stiftelse, The Royal Swedish Academy of Sciences, 1993
- Sweden-America Foundation, 1993
- Claes Adelskjolds Stiftelse, The Royal Swedish Academy of Sciences, 1992
- Helge Ax:son Johnsons Stiftelse, 1995
- Anna Whitlocks Minnesfond, 1993 – 95
- Paulson Award, 1993 – 95
- Lars Hiertas Minnesfond, 1993
- S-E Bankens Skanestipendium, 1992
- E. Lundstroms Stiftelse, 1991
- The California Grant, 1991
- Thomsens legat, 1989 – 91
- Michael Hansens stipendium, 1987
- Tranchells stipendium, 1987