# List of Important Financial Cryptography Papers

| LastName | First Name | Title | Year | File/location | Publisheed |
|---|---|---|---|---|---|
| Ateniese | Guiseppe | Authenticated Group Key Agreement and Friends | 1998 | AtStTs98.ps | ACM Computer & Communicat |
| | | Some Open Issues and new directions in group signatures | 1999 | 16480196 | FC '99 |
| Abad Piero | J.L. | Designing a generic payment service, in IBM Systems Journal, Vol 37, No.1 - Internet Computing | 1998 | Designing a generic paym | IBM Corporation |
| Abadi | Martin | A logic of Authentication | 1989 | printed | |
| Abdall | Michel | Towards Making Broadcast Encryption Practical | 1999 | 16480140 | FC '99 |
| Asokan | N. | Optimistic Protocols for Fair Exchange | 1997 | assw_97.ps | |
| | | The State Of The Art in Electronic Payment Systems | 1997 | AJSW_97PayOver.IEEE. | IBM Zurich Research Lab |
| | | Designing a generic payment service, in IBM Systems Journal, Vol 37, No.1 - Internet Computing | 1998 | Designing a generic paym | IBM Corporation |
| | | Towards A Framework for Handling Disputes in Payment Systems | 1998 | AvHS98.ps | IBM Zurich Research Lab |
| | | Fairness in Electronic Commerce | 1998 | asokan98b.ps | IBM Zurich Research Lab |
| Anderson | Ross | Liability and Computer Security: Nine Principles | 1994 | printed | ESORICS '94 |
| | | Robustness principles for public key protocols | 1996 | robustness.ps | Cambridge University Computer |
| Aiello | William | Fast Digital Identity Revocation | 1998 | 14620137.pdf | CRYPTO '98 |
| Buldas | Ahto | Time-stamping with binary linking schemes | 1998 | 14620486 | CRYPTO '98 |
| Bosselaers | Antoon | The ESPRIT Project CAFÉ: High Security Digital Payment Systems | 1994 | BBCM1_94CafeEsorics.p | ESORICS '94 |
| Butler | Brian | Intermediaries & Cybermediaries: A Continuing Role for Mediating Players in the Electronic Marketplace | 1996 | sarkar.htm | JCMC |
| Bennet | Charles H. | Generalized Privacy Amplification | 1995 | Generalized_Privacy_Am | |
| Bortenlaenger | Christine | The Automation of Capital Markets | 1996 | picot.htm | Univ. Munchen |
| Boyd | Colin | A Payment Scheme Using Vouchers | 1998 | printed | FC '98 |
| | | Off-Line Fair Payment Protocols Using Convertible Signatures | 1998 | printed | ASIACRYPT '98 |
| Bleichenbacher | Daniel | On the Efficiency of One-time Digital Signatures | 1997 | a96pro.ps | |
| Birch | David G.W. | Electronic Cash - Technology Will Denationalise Money | 1997 | printed | FC '97 |
| Brickell | Ernie | Trustee-based Tracing Extensions to Anonymous Cash and the Making of Anonymous Change | 1994 | f11.ps | |

| LastName | First Name | Title | Year | File/location | Publisheed |
|---|---|---|---|---|---|
| Brisbane | Gareth | Region-Based Watermarking for Images | 1999 | 17290154.pdf | ISW '99 |
| Bleumer | Gerrit | Biometric Yet Privacy Protetcting Person Authentication | 1998 | 98.1.1.ps | AT&T Labs-Research, NJ |
| Boly | Jean-Paul | The ESPRIT Project CAFÉ: High Security Digital Payment Systems | 1994 | BBCM1_94CafeEsorics.p | ESORICS '94 |
| Brainard | John | An X.509-Compatible Syntax for Compact Certificates | 1999 | 17400076.pdf | CQRE '99 |
| Borcherding | Malte | Mobile Security - An Overview of GSM, SAT and WAP | 1999 | 17400133 | CQRE '99 |
| Breitbach | Markus | On Channel Capacity and Modulation of Watermarks in Digital Still Images | 1999 | 16480125.pdf | FC '99 |
| Blaze | Matt | KeyNote: Trust Management for Public-Key Infrastructures | 1998 | 98.11.1.body.ps | |
| Burrows | Michael | A logic of Authentication | 1989 | printed | |
| Bellare | Mihir | A forward-secure digital signature scheme | 1999 | 16660431 | CRYPTO '99 |
| | | Design, Implementation and Deployment of a Secure Account-Based Electronic Payment System | 1999 | BGHHKSTHW | |
| | | Translucent Cryptography - An Alternative to Key Escrow, and Its Implementation via Fractional Oblivious Transver | 1999 | 12n2p177.pdf | Cryptology 99 |
| Baric | Nico | Collision-Free Accumulators and Fail-Stop Signature Schemes Without Trees | 1997 | bapf97.ps | EUROCRYPT '97 |
| Brands | Stefan A. | Untraceable Off-line Cash in Wallets with Observers | 1993 | brands93.ps | Centrum voor Wiskunde en Inf |
| | | Distance-Bounding Protocol | 1993 | eurocrypt93.ps | Centrum voor Wiskunde en Inf |
| | | An Efficient Off-line Electronic Cash System Based On The Representation Problem | 1993 | cs-r9323.ps | Centrum voor Wiskunde en Inf |
| | | Off-Line Cash Transfer by Smart Cards | 1994 | cs-r9455 | Centrum voor Wiskunde en Inf |
| | | Electronic Cash on the Internet | 1994 | e-cash.ps | Centrum voor Wiskunde en Inf |
| | | Secret-key certificates | 1995 | cs-r9510.ps | Centrum voor Wiskunde en Inf |
| | | Off-line electronic cash based on secret key certificates | 1995 | cs-r9506.ps | Centrum voor Wiskunde en Inf |
| | | Secret-key certificates (continued) | 1995 | cs-r9555.ps | Centrum voor Wiskunde en Inf |
| | | Restrictive blind issuing of secret-key certificates in parallel mode | 1995 | cs-r9523.ps | Centrum voor Wiskunde en Inf |
| | | Erratum to CS-R9534 | 1995 | CS-R9534_erratum.htm | IBM Zurich Research Lab |
| | | Restrictive blinding of secret-key certificates | 1995 | cs-9505.ps | Centrum voor Wiskunde en Inf |
| | | Rapid Demonstration of Linear Relations Connected by Boolean Operators | 1997 | 97proofs.ps | EUROCRYPT '97 |
| | | Hard-Core Bits for Proofs of Knowledge | 1997 | witness.ps | |

| LastName | First Name | Title | Year | File/location | Publisheed |
|---|---|---|---|---|---|
| Boyko | Victor | On the Security Properties of OAEP as an all-or-nothing transform | 1999 | 16660503 | CRYPTO '99 |
| Choudhury | A.K. | Copyright Protection for Electronic Publishing over Computer Networks | 1994 | copyright.epub.ps | IEEE Network, June 1994 |
| Chan | Agnes | Mis-representation of Identities in E-cash Schemes and how to Prevent it | 1997 | misr.ps | |
| | | Easy come - easy go divisable cash | 1998 | ec98.ps | |
| Crede | Andreas | Electronic Commerce and the Banking Industry: The Requirement and Opportunities | 1999 | crede.htm | Univ. Sussex |
| Clark | Andrew J. | Key Recovery: Why, How, Who? | 1997 | keyrec01.pdf | Sapher Servers Ltd. |
| Carrol | Chris | Effcient key distribution for slow computing devices: Achieving fast over the air activation for wireless systems | 1998 | otasp.pdf | |
| Crepeau | Claude | Generalized Privacy Amplification | 1995 | Generalized_Privacy_Am | |
| Chaum | David | Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms | 1981 | chaum-acm-1981.html | Communications of the ACM |
| | | Security Without Identification: Transaction Systems to Make Big Brother Obsolete | 1985 | p1030-chaum.pdf | Communications of the ACM |
| | | Wallet databases with observers | 1992 | printed | CRYPTO '92 |
| | | Achieving Electronic Privacy | 1992 | Achieving Electronic Priv | Scientific American, Inc. |
| | | Distance-Bounding Protocol | 1993 | eurocrypt93.ps | Centrum voor Wiskunde en Inf |
| Curry | Ian | Trusted Public-Key Infrastructures | 1997 | pki.pdf | Entrust Technologies |
| Camenish | Jan L. | Blind Signatures Based on the Discrete Logarithm Problem | 1994 | blindsig.ps | |
| | | An Efficient Electronic Payment System Protecting Piracy | 1994 | eepspp.ps | |
| | | Security in Payment Systems | 1994 | piv94b.pfg | ETH Zurich |
| | | Fair Blind Signatures | 1995 | FairBlindSignatures.ps | |
| | | Digital Payment Systems with Passive Anonymity-Revoking Trustees | 1996 | Dig_Pay_Trustees.ps (ea) | |
| | | An Efficient Fair Payment System | 1996 | acm.ps | |
| | | Efficient and Generalized Group Signatures | 1997 | eggs.ps | EUROCRYPT '97 |
| | | A Group signature scheme based on an RSA-variant | 1998 | BRICS-RS-98-27.pdf | BRICS Report |
| | | Separability and Efficiency for Generic Group Signature Schemes | 1999 | 16660413 | CRYPTO '99 |
| Callas | Jon | Fair Use, Intellectual Property, and the Information Economy | 1999 | 16480173 | FC '99 |
| Cramer | Ronald | Improved Privacy in Wallets with Observers | 1993 | printed | EUROCRYPT '93 |

| LastName | First Name | Title | Year | File/location | Publisheed |
|---|---|---|---|---|---|
| Cramer | Ronald | The ESPRIT Project CAFÉ: High Security Digital Payment Systems | 1994 | BBCM1_94CafeEsorics.p | ESORICS '94 |
| de Solages | Aymeric | An Efficient Fair Off-Line Electronic Cash System with Extensions to Checks and Wallets with Observers | 1998 | printed | FC '98 |
| Davida | George | Anonymity Control in E-Cash Systems | 1997 | WI.ps | FC '97 |
| Domingo-Ferrer | Josep | Spending Programs: A Tool for Flexible Micropayments | 1999 | 17290001.pdf | ISW '99 |
| Deng | Robert H. | A New Type of Magic Ink Signatures - Towards Transcrupt-Irrelevant Anonymity Revocation | 1999 | 15600001 | PKC '99 |
| Ellison | Carl | Ten Risks of PKI | 2000 | pki-risks.pdf | Computer Security Journal |
| Ergun | Funda | A Note on the Limits of Collusion-Resistant Watermarks | 1999 | 15920140.pdf | EUROCRYPT '99 |
| Ezawa | Kazuo J. | Assesment of Threats for Smart Card based Electronic Cash | 1998 | printed | FC '98 |
|  |  | Assessment of Effectiveness of Counterfeit Transaction Detection Systems for Smart Card Based E-cash | 1999 | 16480072.pdf | FC '99 |
| Even | Shimon | A Randomized Protocol for Signing Contracts | 1985 | p637-even.pdf | Communications of the ACM |
|  |  | On-Line/Off-Line Digital Signatures | 1994 | egm.ps |  |
| Ebringer | Tim | Engineering an eCash System | 1999 | 172900032 | ISW '99 |
| Eng | Tony | Single-Term Divisible Electronic Coins | 1994 | printed | EUROCRYPT '94 |
| Fiat | Amos | Dynamic Traitor Tracing | 1999 | 16660354 | CRYPTO '99 |
| Feng | Bao | A New Type of Magic Ink Signatures - Towards Transcrupt-Irrelevant Anonymity Revocation | 1999 | 15600001 | PKC '99 |
| Fujisaki | Eiichiro | Practical Escrow Cash Schemes | 1998 | printed | IEICE Trans Fund, vol.E81-A |
| Franz | Elke | Comparison of commitment schemes used in mix-mediated anonymous comm for preventing pool-mode attacks | 1998 | 14380111.pdf | ACISP '98 |
|  |  | A Mix-Mediated Anonymity Service and Its Payment | 1998 | printed | ESORICS '98 |
| Foo | Ernest | A Payment Scheme Using Vouchers | 1998 | printed | FC '98 |
|  |  | Off-Line Fair Payment Protocols Using Convertible Signatures | 1998 | printed | ASIACRYPT '98 |
| Feigenbaum | Joan | Fair Use, Intellectual Property, and the Information Economy | 1999 | 16480173 | FC '99 |
| Ferguson | Niels | Single Term Off-Line Coins | 1993 | printed | EUROCRYPT '93 |
| Fumy | Walter | Principles of Key Management | 1993 | printed | IEEE J. Seelcted Areas in Com |
| Frankel | Yair | Anonymity Control in E-Cash Systems | 1997 | WI.ps | FC '97 |
|  |  | Mis-representation of Identities in E-cash Schemes and how to Prevent it | 1997 | misr.ps |  |

| LastName | First Name | Title | Year | File/location | Publisheed |
|---|---|---|---|---|---|
| Frankel | Yair | Indirect Discourse Proofs: Achieving Efficient Fair Off-Line E-Cash | 1997 | folc.ps | |
| | | Easy come - easy go divisable cash | 1998 | ec98.ps | |
| | | Beyond Identity: Warranty-Based Digital Signature Transactions | 1998 | printed | FC '98 |
| | | Effcient key distribution for slow computing devices: Achieving fast over the air activation for wireless systems | 1998 | otasp.pdf | |
| | | Fair Off-line E-Cash Made Easy | 1998 | folc-es.ps | |
| | | Cryptosystems Robust Against 'Dynamic Faults' Meet Enterprise Needs for Organizational "Change Control" | 1999 | 16480241.pdf | FC '99 |
| Goldschlag | David M. | Unlinkable Serial Transaction | 1997 | printed | FC '97 |
| | | Publicly Verifyable Lotteries: Applications of Delaying Functions | 1998 | printed | FC '98 |
| | | Conditional Access Concepts and Principles | 1999 | 16480158 | FC '99 |
| | | Fair Use, Intellectual Property, and the Information Economy | 1999 | 16480173 | FC '99 |
| Godhosi | Hossein | Secret sharing in multilevel and compartemented groups | 1998 | 14380367 | ACISP '98 |
| Garay | Juan A. | Design, Implementation and Deployment of a Secure Account-Based Electronic Payment System | 1999 | BGHHKSTHW | |
| | | Abuse-Free Optimistic Contract Signing | 1999 | 16660449 | CRYPTO '99 |
| Guillou | Louis Claude | Some Critical Remarks on "Dynamic Data Authentication" as Specified in EMV '96 | 1997 | printed | FC '97 |
| Goldreich | Oded | A Randomized Protocol for Signing Contracts | 1985 | p637-even.pdf | Communications of the ACM |
| | | On-Line/Off-Line Digital Signatures | 1994 | egm.ps | |
| | | Self-Delegation with Controlled Propagation - or - What If You Lose Your Laptop | 1998 | 14620153 | CRYPTO '98 |
| Gemmell | Peter | Trustee-based Tracing Extensions to Anonymous Cash and the Making of Anonymous Change | 1994 | f11.ps | |
| Govaerts | Rene | Efficient Electronic Cash with Restricted Privacy | 1997 | printed | FC '97 |
| Gennaro | Rosario | Secure Distributed Key Generation for Discrete-Log Based Cryptosystems | 1999 | 15920295.pdf | EUROCRYPT '99 |
| Hartemink | Alexander | Anonymous Authentication of Membership in Dynamic Groups | 1999 | 16480184.pdf | FC '99 |
| Huehnlein | Detlef | Secure and Cost Efficient Electronic Stamps | 1999 | 17400094.pdf | CQRE '99 |
| Hanaoka | Goichiro | LITESET: A Light-Weight Secure Electronic Transaction Protocol | 1998 | 14380215.pdf | ACISP '98 |

| LastName | First Name | Title | Year | File/location | Publisheed |
|---|---|---|---|---|---|
| Horn | Guenter | Authentication and Payment in Future Mobile Systems | 1998 | printed | ESORICS '98 |
| Hughes | John | The Realities of PKI Inter-operability | 1999 | 17400127 | CQRE '99 |
| Herrera-Joancomar | Jordi | Spending Programs: A Tool for Flexible Micropayments | 1999 | 17290001.pdf | ISW '99 |
| Haruma | Nobuaki | Unlinkable Electronic Coupon Protocol with Anonymity Control | 1999 | 17290037.pdf | ISW '99 |
| He | Qi | A Solution to Open Standard of PKI | 1998 | 14380099.pdf | ACISP '98 |
| Hirschfeld | Rafael | Making Electronic Refunds Safer | 1992 | printed | CRYPTO '92 |
| Hauser | Ralf | Design, Implementation and Deployment of a Secure Account-Based Electronic Payment System | 1999 | BGHHKSTHW | |
| Hwang | Seong Oun | An Electronic Exchange Check with Prevention of Double-Spending | 1998 | printed | Elec & Telecom Resc. Inst., Ta |
| | Tzonelih | On Zhang's Nonrepudiable Proxy Signature Schemes | 1998 | 14380415 | ACISP '98 |
| | | On the Security of the Lee-Chang Group Signature Scheme and Its Derivatives | 1999 | | ISW '99 |
| Imai | Hideki | LITESET: A Light-Weight Secure Electronic Transaction Protocol | 1998 | 14380215.pdf | ACISP '98 |
| | | On Channel Capacity and Modulation of Watermarks in Digital Still Images | 1999 | 16480125.pdf | FC '99 |
| Jerichow | Anja | Comparison of commitment schemes used in mix-mediated anonymous comm for preventing pool-mode attacks | 1998 | 14380111.pdf | ACISP '98 |
| | | A Mix-Mediated Anonymity Service and Its Payment | 1998 | printed | ESORICS '98 |
| Juels | Ari | Security of Blind Digital Signatures | 1997 | crypto97-blind.ps | CRYPTO '97 |
| | | X-Cash: Executable Digital Cash | 1998 | xcash.ps | |
| | | Trustee Tokens: Simple and Practical Anonymous Digital Coin Tracing | 1999 | 16480029.pdf | FC '99 |
| Joye | Marc | On the Security of the Lee-Chang Group Signature Scheme and Its Derivatives | 1999 | | ISW '99 |
| Jakobsson | Markus | Ripping Coins for Fair Exchange | 1995 | rip.ps | Univ. California, SD |
| | | Blackmailing Using Undeniable Signatures | 1995 | blackmail.ps | Univ. California, SD |
| | | Revokeable and Versatile Electronic Money | 1996 | revoke.ps | |
| | | Applying Anti-Trust Policies to Increase Trust in a Versatile E-Money System | 1997 | revoke2.ps | FC '97 |
| | | Privacy vs. Authenticity | 1997 | thesis.jakobsson.ps | Univ. California, SD |

| LastName | First Name | Title | Year | File/location | Publisheed |
|---|---|---|---|---|---|
| Jakobsson | Markus | Round-Optimal Zero-Knowledge Arguments Based on any One-Way Function | 1997 | zkargs.ps | EUROCRYPT '97 |
| | | Distributed "Magic Ink" Signatures | 1998 | magic.ps | |
| | | X-Cash: Executable Digital Cash | 1998 | xcash.ps | |
| | | Mix-based Electronic Payments | 1999 | mixpay.ps | |
| | | Mini-Cash: A Minimalistic Approach to E-Commerce | 1999 | minicash.ps | Bell Labs, NJ |
| | | Abuse-Free Optimistic Contract Signing | 1999 | 16660449 | CRYPTO '99 |
| | | Improved Magic Ink Signatures Using Hints | 1999 | 16480253 | FC '99 |
| | | Electronic Payment: where do we go from here? | 1999 | 17400043.pdf | CQRE '99 |
| | | On Quorum controlled asymetric proxy re-encryption | 1999 | 15600112 | PKC '99 |
| Janson | Phillipe A. | The State Of The Art in Electronic Payment Systems | 1997 | AJSW_97PayOver.IEEE. | IBM Zurich Research Lab |
| Jansen | R. | Towards Multiple-Payment Schemes for Digital Money | 1997 | printed | FC '97 |
| Jareki | Stanislaw | An efficient micropayment system based on probabilistic polling | 1997 | polling.pdf | FC '97 |
| | | Secure Distributed Key Generation for Discrete-Log Based Cryptosystems | 1999 | 15920295.pdf | EUROCRYPT '99 |
| Keromytis | Angelos D. | KeyNote: Trust Management for Public-Key Infrastructures | 1998 | 98.11.1.body.ps | |
| Kravitz | David | Trustee-based Tracing Extensions to Anonymous Cash and the Making of Anonymous Change | 1994 | f11.ps | |
| | | Highly Scalable On-line Payments Via Task Decoupling | 1997 | printed | FC '97 |
| | | Beyond Identity: Warranty-Based Digital Signature Transactions | 1998 | printed | FC '98 |
| | | Conditional Access Concepts and Principles | 1999 | 16480158 | FC '99 |
| Kristol | David M. | Anonymous Internet Mercantile Protocol | 1994 | accinet.ps | Bell Labs, NJ |
| Krawczyk | Hugo | Secure Distributed Key Generation for Discrete-Log Based Cryptosystems | 1999 | 15920295.pdf | EUROCRYPT '99 |
| Killian | Joe | Identity Escrow | 1998 | printed / 14620169.pdf | CRYPTO '98 |
| | | A Note on the Limits of Collusion-Resistant Watermarks | 1999 | 15920140.pdf | EUROCRYPT '99 |
| Knudsen | Lars R. | On the Difficulty of Software Key Escrow | 1996 | escrow.ps | |
| Kossarski | Mariusz | Assessment of Effectiveness of Counterfeit Transaction Detection Systems for Smart Card Based E-cash | 1999 | 16480072.pdf | FC '99 |
| Kudo | Michiharu | Secure Electronic Sealed-Bid Auction Protocol with Public Key Cryptography | 1998 | printed | IEICE Trans Fund, vol.E81-A |

| LastName | First Name | Title | Year | File/location | Publisheed |
|---|---|---|---|---|---|
| Kumar | Ravi | A Note on the Limits of Collusion-Resistant Watermarks | 1999 | 15920140.pdf | EUROCRYPT '99 |
| Kohlas | Reto | Reasoning about Publik-Key Certification: On Binding between Entities and Public Keys | 1999 | 16480086.pdf | FC '99 |
| Kim | Seungjoo | On the Difficulty of Key Recovery Systems | 1999 | 17290207.pdf | ISW '99 |
| Lempel | Abraham | A Randomized Protocol for Signing Contracts | 1985 | p637-even.pdf | Communications of the ACM |
| Lysyanskaya | Anna | Group Blind Digital Signatures: A Scalable Solution to Electronic Cash | 1998 | printed | FC '98 |
| Lu | Chun-Shien | Highly Robust Image Watermarking Using Complementary Modulations | 1999 | 17290136.pdf | ISW '99 |
| Lee | Dan Hyung | An Electronic Exchange Check with Prevention of Double-Spending | 1998 | printed | Elec & Telecom Resc. Inst., Ta |
| Lacoste | Gerard | SEMPER: A Security Framework for the Global Electronic Marketplace | 1998 | LacSte99.ps | IBM Corporation |
| Lee | Insoo | On the Difficulty of Key Recovery Systems | 1999 | 17290207.pdf | ISW '99 |
| Li | Jian Bao | Electronic Cash Scheme for Home Shopping | 1998 | printed | NUS |
| Lamond | Keith | Credit Card Transactions: Real World and Online | 1996 | Paying By Credit Card.ht | |
| Lam | Kwok Yan | Electronic Cash Scheme for Home Shopping | 1998 | printed | NUS |
| | | A Secure Pay-per-View Scheme for Web-Based Video Service | 1999 | 15600315 | PKC '99 |
| Liao | Mark | Highly Robust Image Watermarking Using Complementary Modulations | 1999 | 17290136.pdf | ISW '99 |
| Luby | Michael | Security of Blind Digital Signatures | 1997 | crypto97-blind.ps | CRYPTO '97 |
| Lee | Narn-Yih | On Zhang's Nonrepudiable Proxy Signature Schemes | 1998 | 14380415 | ACISP '98 |
| | | On the Security of the Lee-Chang Group Signature Scheme and Its Derivatives | 1999 | | ISW '99 |
| Laud | Peeter | Time-stamping with binary linking schemes | 1998 | 14620486 | CRYPTO '98 |
| Lipton | Richard J. | Micropayments via Efficient Coin-Flipping | 1998 | printed | FC '98 |
| Lodha | Sachin | Fast Digital Identity Revocation | 1998 | 14620137.pdf | CRYPTO '98 |
| Lelieveldt | Simon L. | Evaluating the Security of Electronic Money | 1997 | printed | FC '97 |
| Low | Steven H. | Anonymous Credit Cards | 1994 | anoncc.ps | Bell Labs, NJ |
| | | Anonymous Credit Cards and its Collusion Analysis | 1994 | collude.ps | Bell Labs, NJ |
| | | Anonymous Internet Mercantile Protocol | 1994 | accinet.ps | Bell Labs, NJ |
| | | The Use of Communication Networks to Increase Personal Privacy In a Health Insurance Architecture | 1996 | privacy.health.ps | Bell Labs, NJ |

| LastName | First Name | Title | Year | File/location | Publisheed |
|---|---|---|---|---|---|
| Mazzeo | A. | SECURE: A Simulation Tool for PKI Design | 1999 | 17400017.pdf | CQRE '99 |
| M'Raihi | David | Distributed Trustees and Revokeability: A Framework for Internet Payment | 1998 | printed | FC '98 |
| | | Mix-based Electronic Payments | 1999 | mixpay.ps | |
| | | Electronic Payment: where do we go from here? | 1999 | 17400043.pdf | CQRE '99 |
| Maher | David P. | A Platform of Privately Defined Currencies, Loyalty Credits, and Play Money | 1998 | printed | FC '98 |
| Miyano | Hiroshi | One Time Digital Signature and Pseudo k-time Digital Signature | 1998 | printed | IEICE Trans Fund, vol.E81-A |
| Merkle | Johannes | Secure and Cost Efficient Electronic Stamps | 1999 | 17400094.pdf | CQRE '99 |
| Mueller | Joy | Improved Magic Ink Signatures Using Hints | 1999 | 16480253 | FC '99 |
| Matheson | Lesley R. | Robustness and Security of Digital Watermarks | 1998 | printed | FC '98 |
| Michels | Markus | A Group signature scheme based on an RSA-variant | 1998 | BRICS-RS-98-27.pdf | BRICS Report |
| | | Separability and Efficiency for Generic Group Signature Schemes | 1999 | 16660413 | CRYPTO '99 |
| Manninger | Martin | Adapting an electronic purse for internet payments | 1998 | 14380205 | ACISP '98 |
| Mambo | Masahiro | Anonymous Public Key Certificates and their Applications | 1998 | printed | IEICE Trans Fund, vol.E81-A |
| | | On the Difficulty of Key Recovery Systems | 1999 | 17290207.pdf | ISW '99 |
| McEvoy | Neil A. | Electronic Cash - Technology Will Denationalise Money | 1997 | printed | FC '97 |
| Maxemchuk | Nicholas F. | Anonymous Credit Cards | 1994 | anoncc.ps | Bell Labs, NJ |
| | | Anonymous Internet Mercantile Protocol | 1994 | accinet.ps | Bell Labs, NJ |
| | | Copyright Protection for Electronic Publishing over Computer Networks | 1994 | copyright.epub.ps | IEEE Network, June 1994 |
| | | Anonymous Credit Cards and its Collusion Analysis | 1994 | collude.ps | Bell Labs, NJ |
| | | The Use of Communication Networks to Increase Personal Privacy In a Health Insurance Architecture | 1996 | privacy.health.ps | Bell Labs, NJ |
| MacKenzie | Phillip | Anonymous Investing: Hiding the Identities of Stockholders | 1999 | 16480212.pdf | FC '99 |
| | | Abuse-Free Optimistic Contract Signing | 1999 | 16660449 | CRYPTO '99 |
| Miner | Sarah K. | A forward-secure digital signature scheme | 1999 | 16660431 | CRYPTO '99 |
| Miyazaki | Shingo | Vulnerability of Anonymous E-cash System to Insider-Attacks from Untrusted Authorities | 1998 | printed | Kyushu Univ |
| | | A More Efficient Untraceable E-Cash System with Partially Blind Signatures Based on the Discrete Logarithm Problem | 1998 | printed | FC '98 |
| | | Toward Fair International Key Escrow | 1999 | 15600171 | PKC '99 |
| Micali | Silvio | On-Line/Off-Line Digital Signatures | 1994 | egm.ps | |

| LastName | First Name | Title | Year | File/location | Publisheed |
|---|---|---|---|---|---|
| Maurer | Ueli | Privacy Amplification Secure Against Active Adversaries | 1989 | paf.ps | |
| | | Generalized Privacy Amplification | 1995 | Generalized_Privacy_Am | |
| | | On the Security of a Practical Identification Scheme rev98 | 1996 | 12n4p247.pdf | Cryptology 99 |
| | | Digital Payment Systems with Passive Anonymity-Revoking Trustees | 1996 | Dig_Pay_Trustees.ps (ea) | |
| | | A Non-interactive Public-Key Distribution System, in Designs, Codes and Cryptography | 1996 | dcc.ps | |
| | | The Intrinsic Conditional Mutual Information and Perfect Secrecy | 1996 | Intrinsic_Info.ps | ETH Zurich |
| | | On the Efficiency of One-time Digital Signatures | 1997 | a96pro.ps | |
| | | Reasoning about Publik-Key Certification: On Binding between Entities and Public Keys | 1999 | 16480086.pdf | FC '99 |
| Mu | Yi | Secure and Efficient Digital Coins | 1997 | printed | IEEE |
| | | Micro-Digital Money for Electronic Commerce | 1997 | printed | IEEE |
| | | Undeniable Confirmer Signature | 1999 | 17290235.pdf | ISW '99 |
| | | Delegated Decryption | 1999 | 17460258 | Cryptography & Coding '99 |
| Napiorkowski | Gregory | Assessment of Effectiveness of Counterfeit Transaction Detection Systems for Smart Card Based E-cash | 1999 | 16480072.pdf | FC '99 |
| Nguyen | Khanh Quoc | Secure and Efficient Digital Coins | 1997 | printed | IEEE |
| | | Micro-Digital Money for Electronic Commerce | 1997 | printed | IEEE |
| | | Undeniable Confirmer Signature | 1999 | 17290235.pdf | ISW '99 |
| | | Delegated Decryption | 1999 | 17460258 | Cryptography & Coding '99 |
| Nystrom | Magnus | An X.509-Compatible Syntax for Compact Certificates | 1999 | 17400076.pdf | CQRE '99 |
| Naor | Moni | Threshold Traitor Tracing | 1998 | 14620502 | CRYPTO '98 |
| Needham | Roger | A logic of Authentication | 1989 | printed | |
| | | Robustness principles for public key protocols | 1996 | robustness.ps | Cambridge University Computer |
| Nakanishi | Toru | Unlinkable Electronic Coupon Protocol with Anonymity Control | 1999 | 17290037.pdf | ISW '99 |
| Odlyzko | Andrew | An efficient micropayment system based on probabilistic polling | 1997 | polling.pdf | FC '97 |
| Okamoto | Eiji | Anonymous Public Key Certificates and their Applications | 1998 | printed | IEICE Trans Fund, vol.E81-A |
| Ohta | Kazuo | Universal electronic cash | 1991 | printed | CRYPTO '91 |

| LastName | First Name | Title | Year | File/location | Publisheed |
|---|---|---|---|---|---|
| Ohta | Kazuo | One Time Zero-Knowledge Authentications and Their Application to Untraceable Electronic Cash | 1998 | printed | IEICE Trans Fund, vol.E81-A |
| Oishi | Kazuomi | Anonymous Public Key Certificates and their Applications | 1998 | printed | IEICE Trans Fund, vol.E81-A |
| Ostrovsky | Rafail | Security of Blind Digital Signatures | 1997 | crypto97-blind.ps | CRYPTO '97 |
| | | Fast Digital Identity Revocation | 1998 | 14620137.pdf | CRYPTO '98 |
| | | Micropayments via Efficient Coin-Flipping | 1998 | printed | FC '98 |
| Okamoto | Tatsuaki | Universal electronic cash | 1991 | printed | CRYPTO '91 |
| | | Single-Term Divisible Electronic Coins | 1994 | printed | EUROCRYPT '94 |
| | | An Efficient Divisible Electronic Cash Scheme | 1995 | printed | CRYPTO '95 |
| | | One Time Zero-Knowledge Authentications and Their Application to Untraceable Electronic Cash | 1998 | printed | IEICE Trans Fund, vol.E81-A |
| | | Practical Escrow Cash Schemes | 1998 | printed | IEICE Trans Fund, vol.E81-A |
| Pfizmann | Andreas | Networks Without User Observability | 1986 | NETWORKS WITHOUT | Univ. Karsruhe, Institute fur Inf |
| | | ISDN-Mixes: Untraceable Communication with Very Small Bandwidth Overhead | 1991 | PfPW_91TelMixGI_NT | Univ. Karsruhe, Institute fur Inf |
| | | Comparison of commitment schemes used in mix-mediated anonymous comm for preventing pool-mode attacks | 1998 | 14380111.pdf | ACISP '98 |
| Picot | Arnold | The Automation of Capital Markets | 1996 | picot.htm | Univ. Munchen |
| Preneel | Bart | Authentication and Payment in Future Mobile Systems | 1998 | printed | ESORICS '98 |
| Pinkas | Benny | Threshold Traitor Tracing | 1998 | 14620502 | CRYPTO '98 |
| Pfitzmann | Birgit | ISDN-Mixes: Untraceable Communication with Very Small Bandwidth Overhead | 1991 | PfPW_91TelMixGI_NT | Univ. Karsruhe, Institute fur Inf |
| | | How to Break and Repair a "Provably Secure" Untraceable Payment System | 1992 | PfWa2_92DamgZsysCr9 | |
| | | The ESPRIT Project CAFÉ: High Security Digital Payment Systems | 1994 | BBCM1_94CafeEsorics.p | ESORICS '94 |
| | | News on CAFÉ, April 1995 | 1995 | PfWe_95CAFE.Oakland. | |
| | | How to Break Another "Provably Secure" Payment System | 1995 | PfSW_95adAmCr.ps | |
| | | Strong Loss Tolerance of Electronic Coin Systems | 1997 | p194-pfitzman.pdf | ACM Transactions on Compute |
| | | Asymetric Fingerprinting for Larger Collusions | 1997 | p151-pfitzmann.pdf | ACM |
| | | Anonymous Fingerprinting | 1997 | PfWa1_97AnoFing.ps | EUROCRYPT '97 |
| | | Collision-Free Accumulators and Fail-Stop Signature Schemes Without Trees | 1997 | bapf97.ps | EUROCRYPT '97 |

| LastName | First Name | Title | Year | File/location | Publisheed |
|---|---|---|---|---|---|
| Pfitzmann | Birgit | Self-Delegation with Controlled Propagation - or - What If You Lose Your Laptop | 1998 | 14620153 | CRYPTO '98 |
| | | Optimal Efficiency of Optimistic Contract Signing | 1998 | p113-pfitzmann.pdf | ACM |
| | | Coin-Based Anonymous Fingerprinting | 1999 | 15920150.pdf | EUROCRYPT '99 |
| Park | Chang Soon | An Electronic Exchange Check with Prevention of Double-Spending | 1998 | printed | Elec & Telecom Resc. Inst., Ta |
| Pointcheval | David | Strengthened Security for Blind Signatures | 1998 | printed | EUROCRYPT '98 |
| Petrank | Erez | Identity Escrow | 1998 | printed / 14620169.pdf | CRYPTO '98 |
| Poupard | Guillaume | Efficient Scalable Fair Cash with Off-line Extortion Prevention | 1997 | CashSystem.ps | Ecole Normaler Superieure, Tec |
| Pagina | H. | Towards Multiple-Payment Schemes for Digital Money | 1997 | printed | FC '97 |
| Petersen | Holger | Efficient Scalable Fair Cash with Off-line Extortion Prevention | 1997 | CashSystem.ps | Ecole Normaler Superieure, Tec |
| Piveteau | Jean-Marc | Blind Signatures Based on the Discrete Logarithm Problem | 1994 | blindsig.ps | |
| | | An Efficient Electronic Payment System Protecting Piracy | 1994 | eepspp.ps | |
| | | Security in Payment Systems | 1994 | piv94b.pfg | ETH Zurich |
| | | Fair Blind Signatures | 1995 | FairBlindSignatures.ps | |
| | | An Efficient Fair Payment System | 1996 | acm.ps | |
| Pieprzyk | Josef | Secret sharing in multilevel and compartemented groups | 1998 | 14380367 | ACISP '98 |
| Paul | Sanjoy | Anonymous Credit Cards and its Collusion Analysis | 1994 | collude.ps | Bell Labs, NJ |
| | | Anonymous Credit Cards | 1994 | anoncc.ps | Bell Labs, NJ |
| | | Copyright Protection for Electronic Publishing over Computer Networks | 1994 | copyright.epub.ps | IEEE Network, June 1994 |
| Parnell | Todd | Anonymous Authentication of Membership in Dynamic Groups | 1999 | 16480184.pdf | FC '99 |
| Pedersen | Torben P. | Wallet databases with observers | 1992 | printed | CRYPTO '92 |
| | | Improved Privacy in Wallets with Observers | 1993 | printed | EUROCRYPT '93 |
| | | The ESPRIT Project CAFÉ: High Security Digital Payment Systems | 1994 | BBCM1_94CafeEsorics.p | ESORICS '94 |
| | | On the Difficulty of Software Key Escrow | 1996 | escrow.ps | |
| Rubin | Avi | Session Key Distribution Using Smart Cards | 1996 | keydist.ps | Bell Labs, NJ |
| Radu | Cristian | Efficient Electronic Cash with Restricted Privacy | 1997 | printed | FC '97 |
| Roberts | David W. | Security Management - The Process | 1998 | printed | COSIC '97 |
| Roehrl | Heiner | The Automation of Capital Markets | 1996 | picot.htm | Univ. Munchen |
| Romano | L. | SECURE: A Simulation Tool for PKI Design | 1999 | 17400017.pdf | CQRE '99 |

| LastName | First Name | Title | Year | File/location | Publisheed |
|---|---|---|---|---|---|
| Rivest | Ronald L. | Perspectives on Financial Cryptography | 1997 | fc97-paper.ps | |
| | | Electronic Lottery Tickets as Micropayments | 1997 | lottery.ps | MIT Lab |
| | | Self-Delegation with Controlled Propagation - or - What If You Lose Your Laptop | 1998 | 14620153 | CRYPTO '98 |
| | | Translucent Cryptography - An Alternative to Key Escrow, and Its Implementation via Fractional Oblivious Transver | 1999 | 12n2p177.pdf | Cryptology 99 |
| Rabin | Tal | Secure Distributed Key Generation for Discrete-Log Based Cryptosystems | 1999 | 15920295.pdf | EUROCRYPT '99 |
| Ramzan | Zulfikar | Group Blind Digital Signatures: A Scalable Solution to Electronic Cash | 1998 | printed | FC '98 |
| Shostack | Adam | Breaking Up Is Hard To Do: Modeling Security Threats for Smart Cards | 1998 | smart-card-threats.pdf | Counterpane |
| Sadeghi | Ahmad-Reza | Coin-Based Anonymous Fingerprinting | 1999 | 15920150.pdf | EUROCRYPT '99 |
| Schoenmakers | Berry | A simple publicly verifiable secret sharing scheme and its application to electronic voting | 1999 | 16660148 | CRYPTO '99 |
| Schneier | Bruce | Breaking Up Is Hard To Do: Modeling Security Threats for Smart Cards | 1998 | smart-card-threats.pdf | Counterpane |
| | | Ten Risks of PKI | 2000 | pki-risks.pdf | Computer Security Journal |
| Steinfield | Charles | Intermediaries & Cybermediaries: A Continuing Role for Mediating Players in the Electronic Marketplace | 1996 | sarkar.htm | JCMC |
| Sawyer | Erin | Fair Use, Intellectual Property, and the Information Economy | 1999 | 16480173 | FC '99 |
| Simmons | Gustaf J. | Cryptoanalysis and Protocol Failures | 1994 | printed | Communications of the ACM |
| Schulzrinne | H.G. | Copyright Protection for Electronic Publishing over Computer Networks | 1994 | copyright.epub.ps | IEEE Network, June 1994 |
| Stern | Jacques | SVP: A Flexible Micropayment Scheme | 1997 | printed | FC '97 |
| Sorensen | Jeffery | Anonymous Investing: Hiding the Identities of Stockholders | 1999 | 16480212.pdf | FC '99 |
| Sycara | Katia | A Solution to Open Standard of PKI | 1998 | 14380099.pdf | ACISP '98 |
| Sako | Kazuo | Implementation of a Digital Lottery Server on WWW | 1999 | 17400101 | CQRE '99 |
| Schmeh | Klaus | A Method of Defeloping PKI Models | 1999 | 17400119 | CQRE '99 |
| Sakurai | Kouichi | A More Efficient Untraceable E-Cash System with Partially Blind Signatures Based on the Discrete Logarithm Problem | 1998 | printed | FC '98 |
| | | Vulnerability of Anonymous E-cash System to Insider-Attacks from Untrusted Authorities | 1998 | printed | Kyushu Univ |
| | | Toward Fair International Key Escrow | 1999 | 15600171 | PKC '99 |

| LastName | First Name | Title | Year | File/location | Publisheed |
|---|---|---|---|---|---|
| Stadler | Markus A. | Blind Signatures Based on the Discrete Logarithm Problem | 1994 | blindsig.ps | |
| | | An Efficient Electronic Payment System Protecting Piracy | 1994 | eepspp.ps | |
| | | Security in Payment Systems | 1994 | piv94b.pfg | ETH Zurich |
| | | Fair Blind Signatures | 1995 | FairBlindSignatures.ps | |
| | | An Efficient Fair Payment System | 1996 | acm.ps | |
| | | Digital Payment Systems with Passive Anonymity-Revoking Trustees | 1996 | Dig_Pay_Trustees.ps (ea) | |
| Schunter | Matthias | The ESPRIT Project CAFÉ: High Security Digital Payment Systems | 1994 | BBCM1_94CafeEsorics.p | ESORICS '94 |
| | | How to Break Another "Provably Secure" Payment System | 1995 | PfSW_95adAmCr.ps | |
| | | News from CAFÉ, June 1995 | 1995 | ScWe_95.ps | |
| | | Privacy Oriented Clearing for the German Health-Care System | 1996 | blsc1_96.ps | Univ. Hildesheim, Institute fur I |
| | | Architecture and Design of a Secure Electronic Marketplace | 1997 | 431UD012.JENC8.ps | |
| | | Optimistic Protocols for Fair Exchange | 1997 | assw_97.ps | |
| | | Optimal Efficiency of Optimistic Contract Signing | 1998 | p113-pfitzmann.pdf | ACM |
| Steiner | Michael | The State Of The Art in Electronic Payment Systems | 1997 | AJSW_97PayOver.IEEE. | IBM Zurich Research Lab |
| | | Authenticated Group Key Agreement and Friends | 1998 | AtStTs98.ps | ACM Computer & Communicat |
| | | Designing a generic payment service, in IBM Systems Journal, Vol 37, No.1 - Internet Computing | 1998 | Designing a generic paym | IBM Corporation |
| | | Towards A Framework for Handling Disputes in Payment Systems | 1998 | AvHS98.ps | IBM Zurich Research Lab |
| | | SEMPER: A Security Framework for the Global Electronic Marketplace | 1998 | LacSte99.ps | IBM Corporation |
| | | Design, Implementation and Deployment of a Secure Account-Based Electronic Payment System | 1999 | BGHHKSTHW | |
| Sarkar | Mitra Barun | Intermediaries & Cybermediaries: A Continuing Role for Mediating Players in the Electronic Marketplace | 1996 | sarkar.htm | JCMC |
| Syverson | Paul F. | Unlinkable Serial Transaction | 1997 | printed | FC '97 |
| Safavi-Naini | Rei | Secret sharing in multilevel and compartemented groups | 1998 | 14380367 | ACISP '98 |
| | | Region-Based Watermarking for Images | 1999 | 17290154.pdf | ISW '99 |
| Schischka | Robert | Adapting an electronic purse for internet payments | 1998 | 14380205 | ACISP '98 |
| Schechter | Stuart | Anonymous Authentication of Membership in Dynamic Groups | 1999 | 16480184.pdf | FC '99 |
| Stubblebine | Stuart G. | Unlinkable Serial Transaction | 1997 | printed | FC '97 |

| LastName | First Name | Title | Year | File/location | Publisheed |
|---|---|---|---|---|---|
| Stubblebine | Stuart G. | Publicly Verifyable Lotteries: Applications of Delaying Functions | 1998 | printed | FC '98 |
| Sander | Tomas | On Anonymous Electronic Cash and Crime | 1999 | 17290202.pdf | ISW '99 |
| | | Flow Control: A New Approach for Anonymity Control in Electronic Cash Systems | 1999 | 16480046.pdf | FC '99 |
| | | Auditable, Anonymous Electronic Cash | 1999 | printed 16660555 | CRYPTO '99 |
| Shoup | Victor | Session Key Distribution Using Smart Cards | 1996 | keydist.ps | Bell Labs, NJ |
| | | On the Security of a Practical Identification Scheme rev98 | 1996 | 12n4p247.pdf | Cryptology 99 |
| | | On Formal Models for Secure Key Exchange | 1999 | shoup99.ps | IBM Zurich Research Lab |
| Sugiyama | Yuji | Unlinkable Electronic Coupon Protocol with Anonymity Control | 1999 | 17290037.pdf | ISW '99 |
| Shavitt | Yuval | Towards Making Broadcast Encryption Practical | 1999 | 16480140 | FC '99 |
| Su | Zhongmin | A Solution to Open Standard of PKI | 1998 | 14380099.pdf | ACISP '98 |
| Ta-Shma | Amnon | On Anonymous Electronic Cash and Crime | 1999 | 17290202.pdf | ISW '99 |
| | | Flow Control: A New Approach for Anonymity Control in Electronic Cash Systems | 1999 | 16480046.pdf | FC '99 |
| | | Auditable, Anonymous Electronic Cash | 1999 | printed 16660555 | CRYPTO '99 |
| Tsudik | Gene | Authenticated Group Key Agreement and Friends | 1998 | AtStTs98.ps | ACM Computer & Communicat |
| | | Some Open Issues and new directions in group signatures | 1999 | 16480196 | FC '99 |
| | | Design, Implementation and Deployment of a Secure Account-Based Electronic Payment System | 1999 | BGHHKSTHW | |
| Traore | Jacques | An Efficient Fair Off-Line Electronic Cash System with Extensions to Checks and Wallets with Observers | 1998 | printed | FC '98 |
| Thorne | Peter | Engineering an eCash System | 1999 | 172900032 | ISW '99 |
| Tassa | Tamir | Dynamic Traitor Tracing | 1999 | 16660354 | CRYPTO '99 |
| Tsiounis | Yiannis | Anonymity Control in E-Cash Systems | 1997 | WI.ps | FC '97 |
| | | Indirect Discourse Proofs: Achieving Efficient Fair Off-Line E-Cash | 1997 | folc.ps | |
| | | Efficient Electronic Cash: New Notions and Techniques | 1997 | thesis.ps | Northeastern Univ. |
| | | Mis-representation of Identities in E-cash Schemes and how to Prevent it | 1997 | misr.ps | |
| | | Easy come - easy go divisable cash | 1998 | ec98.ps | |
| | | Effcient key distribution for slow computing devices: Achieving fast over the air activation for wireless systems | 1998 | otasp.pdf | |

| LastName | First Name | Title | Year | File/location | Publisheed |
|---|---|---|---|---|---|
| Tsiounis | Yiannis | Fair Off-line E-Cash Made Easy | 1998 | folc-es.ps | |
| | | Electronic Payment: where do we go from here? | 1999 | 17400043.pdf | CQRE '99 |
| | | Micropayments and Anonymous E-Cash (ppt) | 1999 | micro-ecash.ppt | Northeastern University/ GTE |
| Van Herreweghen | Els | Risk and Potentials of Using EMV for Internet Payments | 1998 | VHW98.ps | IBM Zurich Research Lab |
| Vandlewalle | Joos | Efficient Electronic Cash with Restricted Privacy | 1997 | printed | FC '97 |
| Vedder | Klaus | GSM: Security, Services and the SIM | 1998 | printed | COSIC '97 |
| | | Smart Cards - Requirements, Properties, and Applications | 1998 | printed | COSIC '97 |
| Varadharajan | Vijay | Micro-Digital Money for Electronic Commerce | 1997 | printed | IEEE |
| | | Secure and Efficient Digital Coins | 1997 | printed | IEEE |
| | | Undeniable Confirmer Signature | 1999 | 17290235.pdf | ISW '99 |
| | | Delegated Decryption | 1999 | 17460258 | Cryptography & Coding '99 |
| Wool | Avishai | Towards Making Broadcast Encryption Practical | 1999 | 16480140 | FC '99 |
| Wang | Chih hung | On Zhang's Nonrepudiable Proxy Signature Schemes | 1998 | 14380415 | ACISP '98 |
| Weikmann | Franz | Smart Cards - Requirements, Properties, and Applications | 1998 | printed | COSIC '97 |
| Waidner | Michael | Networks Without User Observability | 1986 | NETWORKS WITHOUT | Univ. Karsruhe, Institute fur Inf |
| | | ISDN-Mixes: Untraceable Communication with Very Small Bandwidth Overhead | 1991 | PfPW_91TelMixGI_NT | Univ. Karsruhe, Institute fur Inf |
| | | How to Break and Repair a "Provably Secure" Untraceable Payment System | 1992 | PfWa2_92DamgZsysCr9 | |
| | | The ESPRIT Project CAFÉ: High Security Digital Payment Systems | 1994 | BBCM1_94CafeEsorics.p | ESORICS '94 |
| | | How to Break Another "Provably Secure" Payment System | 1995 | PfSW_95adAmCr.ps | |
| | | Strong Loss Tolerance of Electronic Coin Systems | 1997 | p194-pfitzman.pdf | ACM Transactions on Compute |
| | | Architecture and Design of a Secure Electronic Marketplace | 1997 | 431UD012.JENC8.ps | |
| | | Asymetric Fingerprinting for Larger Collusions | 1997 | p151-pfitzmann.pdf | ACM |
| | | Anonymous Fingerprinting | 1997 | PfWa1_97AnoFing.ps | EUROCRYPT '97 |
| | | The State Of The Art in Electronic Payment Systems | 1997 | AJSW_97PayOver.IEEE. | IBM Zurich Research Lab |
| | | Optimistic Protocols for Fair Exchange | 1997 | assw_97.ps | |
| | | Open Issues in Secure Electronic Commerce | 1998 | Waidner98.ps | IBM Zurich Research Lab |
| | | Optimal Efficiency of Optimistic Contract Signing | 1998 | p113-pfitzmann.pdf | ACM |
| | | Designing a generic payment service, in IBM Systems Journal, Vol 37, No.1 - Internet Computing | 1998 | Designing a generic paym | IBM Corporation |

| LastName | First Name | Title | Year | File/location | Publisheed |
|---|---|---|---|---|---|
| Waidner | Michael | Design, Implementation and Deployment of a Secure Account-Based Electronic Payment System | 1999 | BGHHKSTHW | |
| Wolf | Stefan | Privacy Amplification Secure Against Active Adversaries | 1989 | paf.ps | |
| | | The Intrinsic Conditional Mutual Information and Perfect Secrecy | 1996 | Intrinsic_Info.ps | ETH Zurich |
| Wille | Uta | Risk and Potentials of Using EMV for Internet Payments | 1998 | VHW98.ps | IBM Zurich Research Lab |
| Xu | Shouhuai | Money Conservation via Atomicity in Fair Off-Line E-Cash | 1999 | 17290014.pdf | ISW '99 |
| Young | Adam | Auto-Recoverable Cryptosystems with Faster Initalization and the Escrow Hierarchy | 1999 | 15600306 | PKC '99 |
| | | Auto-recoverable auto-certifiable cryptosystems (a survey) | 1999 | 17400204 | CQRE '99 |
| Yung | Moti | Revokeable and Versatile Electronic Money | 1996 | revoke.ps | |
| | | Indirect Discourse Proofs: Achieving Efficient Fair Off-Line E-Cash | 1997 | folc.ps | |
| | | Round-Optimal Zero-Knowledge Arguments Based on any One-Way Function | 1997 | zkargs.ps | EUROCRYPT '97 |
| | | Anonymity Control in E-Cash Systems | 1997 | WI.ps | FC '97 |
| | | Applying Anti-Trust Policies to Increase Trust in a Versatile E-Money System | 1997 | revoke2.ps | FC '97 |
| | | Beyond Identity: Warranty-Based Digital Signature Transactions | 1998 | printed | FC '98 |
| | | Distributed "Magic Ink" Signatures | 1998 | magic.ps | |
| | | Fair Off-line E-Cash Made Easy | 1998 | folc-es.ps | |
| | | Electronic Payment: where do we go from here? | 1999 | 17400043.pdf | CQRE '99 |
| | | Money Conservation via Atomicity in Fair Off-Line E-Cash | 1999 | 17290014.pdf | ISW '99 |
| | | Cryptosystems Robust Against 'Dynamic Faults' Meet Enterprise Needs for Organizational "Change Control" | 1999 | 16480241.pdf | FC '99 |
| | | Auto-Recoverable Cryptosystems with Faster Initalization and the Escrow Hierarchy | 1999 | 15600306 | PKC '99 |
| | | Auto-recoverable auto-certifiable cryptosystems (a survey) | 1999 | 17400204 | CQRE '99 |
| Yacobi | Yacov | Efficient Electronic Money | 1994 | printed | AsiaCRYPT '94 |
| | | A Non-interactive Public-Key Distribution System, in Designs, Codes and Cryptography | 1996 | dcc.ps | |
| | | On the Continum Between On-line and Off-line E-cash Systems - I | 1997 | printed | FC '97 |

| LastName | First Name | Title | Year | File/location | Publisheed |
|---|---|---|---|---|---|
| Yacobi | Yacov | Risk Management for E-cash Systems with Partial Real-Time Audit | 1999 | 16480062 | FC '99 |
| Zhang | Gendu | Money Conservation via Atomicity in Fair Off-Line E-Cash | 1999 | 17290014.pdf | ISW '99 |
| Zimmerman | Hans-Dieter | An Integrated Electronic Payment System As A Generic Market Service For Electronic Commerce Platforms | 1998 | Cotim97.pdf | Univ. St. Gallen, MCM |
| Zhou | Jianying | A Secure Pay-per-View Scheme for Web-Based Video Service | 1999 | 15600315 | PKC '99 |
| Zheng | Yuliang | Digital Signcryption or How to Achieve Cost(Signature & Encryption) << Cost(Signature) + Cost(Encryption) | 1997 | c97-fnl-rvs.ps | CRYPTO '97 |
| | | LITESET: A Light-Weight Secure Electronic Transaction Protocol | 1998 | 14380215.pdf | ACISP '98 |