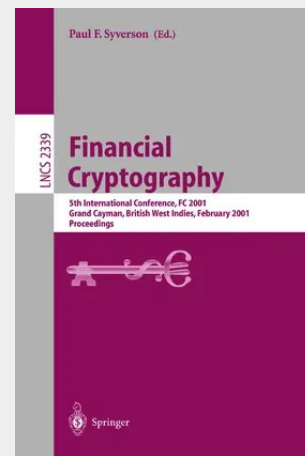


Financial Cryptography

5th International Conference, FC 2001, Grand Cayman, British West Indies, February 19-22, 2001. Proceedings

ThankstogeneralchairStuartHaberfordoingmanythingsthatnoneofthe attendeesnoticedbecausehedidthemsonicely. HewasablyassistedbyHinde tenBerge. ThankstoHarrisMcCoyforhandlinglocalarrangementsandJason CronkformaintainingtheWebsite. ThankstotheIFCAdirectorsforkeeping FCthriving,toAdamShostackforvenuearrangements,andtoBarbFox,the sponsorshipchair. Thankstoour?nancialsponsors,whoarelistedonthenext page. SpecialthankstoRayHirschfeldwhoseadvicetomeandtotheothersm- tionedherehasbeeninvaluable. Thanks?nallytoattendeeswithoutwhomthere wouldbenoconference. March2001 PaulSyverson VI Preface ProgramCommittee MattBlaze,AT&TLabs-Research YairFrankel,Ecash MattFranklin,UCDavis DavidKravitz,WaveSystemsCorp. ArjenLenstra,Citicorp PhilipMacKenzie,LucentBellLabs AviRubin,AT&TLabs-Research JacquesStern,EcoleNormaleSup´erieure KazueSako,NEC StuartStubblebine,CertCo PaulSyverson(Chair),NavalResearchLab WinTreese,OpenMarket,Inc. DougTygar,UCBerkeley MichaelWaidner,IBMZurichResearchLab MotiYung,CertCo GeneralChair StuartHaber,Intertrust SponsorshipChair BarbFox,Microsoft FinancialCryptography2001wasorganizedbytheInternationalFinancialCr- tographyAssociation(IFCA),andwassponsoredbyBibitInternetPayments, CertCo,Certicom,HushCommunications,IBM,InterTrustSTARLab,- crosoft,nCipher,RSASecurity,andZero-KnowledgeSystems. TableofContents ManagingPaymentTransactionCosts AmortizedE-Cash. 1 MosesLiskov,SilvioMicali O? ineMicropaymentswithoutTrustedHardware. 21 MattBlaze,JohnIoannidis,AngelosD. Keromytis Panel(I) ThePracticalProblemsofImplementingMicroMint. 41 NickovanSomeren ProtectingDigitalRights. 51 YairFrankel AspectsofDigitalRightsManagementandtheUseofHardwareSecurity Devices. 54 DavidW. Kravitz ASolutiontotheNapsterPhenomenon:WhyValueCannotBeCreated AbsenttheTransferofSubjectiveData. 59 ScottMoskowitz GoldenTimesforDigitalRightsManagement?. 64 TomasSander ApplicabilityofPublicKeyCryptosystemstoDigitalRightsManagement Applications. 75 JeremyWyant TrustandRiskManagement OntheGlobalContentPMI:ImprovedCopy- ProtectedInternetContent Distribution. 79 TadayoshiKohno,MarkMcGovern Trust:ACollisionofParadigms. 91 L. JeanCamp,HelenNissenbaum,CathleenMcGrath GroupsandAnonymity OntheSecurityofHomageGroupAuthenticationProtocol. 106 ElianeJaulmes,GuillaumePoupard VIII Table of Contents Anonymitywithout'Cryptography'. 117 DahliaMalkhiandElanPavlov FairTracingwithoutTrustees. 136 DennisKügler,HolgerVogt InvitedTalk WhytheWaronMoneyLaunderingShouldBeAborted. 149 RichardW. Rahn Certi?catesandAuthentication ProvablySecureImplicitCerti? cateSchemes. 156 DanielR. L. Brown,RobertGallant,ScottA. Vanstone Nonmonotonicity,UserInterfaces,andRiskAssessmentinCerti?cate Revocation. 166 NinghuiLi,JoanFeigenbaum MutualAuthenticationforLow-PowerMobileDevices. 178 MarkusJakobsson,DavidPointcheval CreditCardSecurity O?-LineGenerationofLimited- UseCreditCardNumbers. 196 AviD. Rubin,RebeccaN. Wright ASecurityFrameworkforCard-BasedSystems. 210 YiannisTsionis SecureClick:AWebPaymentSystemwithDisposableCreditCard Numbers. 232 AdiShamir Panel(II) TheBusinessofElectronicVoting. 243 EdGerck,C. AndrewNe?,RonaldL. Rivest,AviD. Rubin, MotiYung MarketsandMultipartyComputation PrivacyfortheStockMarket. 269 GiovanniDiCrescenzo SecureDistributedComputinginaCommercialEnvironment. 289 PhilippeGolle,StuartStubblebine Table of Contents IX SignaturesinFinancialCryptography MonotoneSignatures. 305 DavidNaccache,DavidPointcheval,ChristopheTymen ThePowerofRSAInversionOraclesandtheSecurityofChaum's RSA-



53,49 €

49,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783540440796

Medium: Buch

ISBN: 978-3-540-44079-6

Verlag: Springer Berlin Heidelberg

Erscheinungstermin: 14.08.2002

Sprache(n): Englisch

Auflage: 2002

Serie: Lecture Notes in Computer Science

Produktform: Kartoniert

Gewicht: 1220 g

Seiten: 379

Format (B x H): 155 x 235 mm

