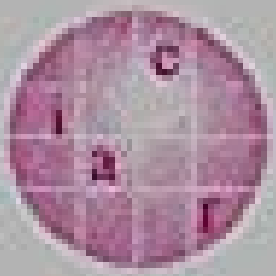
Lecture Notes in Computer Science 1880

Mihir Bellare (Ed.)

Advances in Cryptology – CRYPTO 2000

20th Annual International Cryptology Conference
Santa Barbara, California, USA, August 2000
Proceedings



Springer

Mihir Bellare

Advances in Cryptology - CRYPTO 2000: 20th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2000. Proceedings (Lecture Notes in Computer Science)

Crypto2000wasthe20thAnnualCryptoconference. Itwassponsoredbythe InternationalAssociationforCryptologicResearch(IACR)incooperationwith theIEEEComputerSocietyTechnicalCommitteeonSecurityandPrivacyand theComputerScienceDepartmentoftheUniversityofCaliforniaatSantaB- bara. Theconferencereceived120submissions, andtheprogramcommittee- lected32oftheseforpresentation. Extendedabstractsofrevisedversionsof thesepapersareintheseproceedings. Theauthorsbearfullresponsibilityfor thecontentsoftheirpapers. VI Preface Theweb-reviewsoftwareweusedwaswrittenforEurocrypt2000byWim MoreauandJorisClaessensunderthedirectionofEurocrypt2000programchair BartPreneel, andIthankthemforallowingustodeploytheirusefulandcolorful device.nalabstractsintotheproceedings youseehere.? Mart? ShetypesfasterthanIspeak.cultcases.?n'stalkisincludedintheseproceedings. Inthesecondphase, committeemembersusedthe softwaretobrowseeachother'sreports, discuss, andupdatetheirownreports. Meaw)whoprovided systems, logistical, andmoralsupportfortheentireCrypto2000process.ectedintheseproceedings. She wrotethesoftwarefortheweb-basedsubmissions, adaptedandranthew- reviewsoftwareatUCSD, andcompiledthe?rsttimeusedawebinterfaceratherthanemail. (Perhapsasaresult, therewere nohardcopysubmissions.)Thesubmissionreviewprocesshadthreephases. In the? FinallythankstoMattFranklinwhoasgeneralchairwasinchargeofthelocal organizationand? Theconferenceprogramalsoincludeditstraditional"rumpsession"ofshort, informalorimpromptupresentations, chairedthistimebyStuartHaber. LastlytherewasaprogramcommitteemeetingtodiscussthedI? Anabstract correspondingtoMart? Iamextremelygratefultotheprogramcommitteemembersfortheiren- mousinvestmentoftime, e?ort, andadrenalineinthedi?cultanddelicate processofreviewandselection. (Alistofprogramcommitteemembersand-refereestheyinvokedcanbefoundonsucceedingpagesofthisvolume.)Ialso thanktheauthorsofsubmittedpapers-inequalmeasureregardlessofwhether theirpaperswereacceptedornot-fortheirsubmissions. Itistheworkofthis bodyofresearchersthatmakesthisconferencepossible. IthankRebeccaWrightforhostingtheprogramcommitteemeetingatthe AT&TbuildinginNewYorkCityandmanagingthelocalarrangements, and RanCanettifororganizingthepost-PC-meetingdinnerwithhischaracteristic gastronomicandoenophilic?surroundings. Theconferenceprogramincludedtwoinvitedlectures. IammostgratefultoChanathipNamprempre(aka. These presentationsarenotre? Anelectronicsubmissionprocesswasavailableandrecommended, butforthe ? DonCoppersmith's presentation"ThedevelopmentofDES"recordedhisinvolvementwithoneof themostimportantcryptographicdevelopmentsever, namelytheDataEncr- tionStandard, andwasparticularlyaptgiventheimminentselectionofthe AdvancedEncryptionStandard.nAbadi'spresentation"Tamingthe-versary"wasaboutbridgingthegapbetweenusefulbutperhapssimplisticthreat abstractionsandrigorousadversarialmodels, orperhaps, evenmoregenerally, betweenviewpointsofthesecurityandcryptographycommunities. IamgratefultoHugoKrawczykforhisinsightandadvice, providedovera

longperiodoftimewithhisusualcombinationofhonestyandcharm, andto himandotherpastprogramcommitteechairs, mostnotablyMichaelWiener andBartPreneel, forrepliestothehostofquestionsIposedduringthep- cess. InadditionIreceivedusefuladvicefrommanymembersofourcommunity includingSilvioMicali, TalRabin, RonRivest, PhilRogaway, andAdiShamir.rstphase, programcommitteememberscompiledreports(assistedattheir discretionbysub-refereesoftheirchoice, butwithoutinteractionwithother programcommitteemembers)andenteredthem, viawebforms, intoweb- review softwarerunningatUCSD.nances

Conference, Santa Barbara, California, USA, August 20-24, 2000. Proceedings (Lecture Notes in Computer Science) djvu