Cryptology pointers

Starting points

Newsgroups Blogs FAQs Introductions to Crypto Collections of links

Conferences, Workshops, Seminars

2009 2010 Seminars, Courses... Style files & help for authors

Literature

Bibliographies Books JournalsLecture Notes

Basic Symmetric Primitives

Block ciphers (AES) Stream ciphers Hash functions Hand Ciphers

Groups and individuals working on crypto

Universities Industr. Research Groups CryptographersOrganizations Companies Research and Education

Advanced Symmetric Primitives & Cryptosystems

Block Cipher Modes MACsPseudorandom Functions Boolean functions

Public-Key Cryptography

Public-Key Encryption Theory of PKCThreshold Encryption

PKC Based on Some Special Mathematical Structures

Braid Groups Elliptic Curves PairingsMultilinear Maps Class GroupsLattice Based Crypto & Lattice Reduction

Signature schemes

Undeniable Signatures Group SignaturesTrapdoor Signatures

Other public-key primitives

Commitment Pseudorandom Generators

Authentication, Identification and Key Exchange protocols

Identification Schemes Password-Authenticated Key Exchange Zero-Knowledge Proofs of knowledge Mixnets/Shuffles

Cryptographic Protocols

E-Cash E-Auctions Traitor Tracing/Broacast Encryption Electronic Voting Fair Exchange

Protocols on large data-sets

Oblivious Transfer and Private Information Retrieval Private SearchPrivacy-Preserving Data mining

Infrastructure Protocols

Time-Stamping Public Key InfrastructureCountermeasures to DoS

Practical Aspects

Implementations SoftwareHardware Mobile DevicesSmartcards Internet CryptographyStandards Law Patents

Secure Computation & Foundations

Two-Party Computations Multi-Party Computations Secret Sharing Security in Malicious Model

Formal Methods, Various Security Models

Information-Theoretic CryptographyRandom Oracle Model Generic Group Model Authentication LogicUniversal Composability LeakageImpossibility Results

Related Areas in Security

Steganography/Watermarking/ObfuscationBiometrics

Related Areas in General

Data Compression Coding TheoryCommunication ComplexityBranching Programs Data StructuresNumber Theory (Primality tests)Quantum Computation and Cryptography Game Theory

Miscellaneous Information

History Regional Sites EntertainmentUnsorted links (Everything else)

About this page

More than *6000* links on cryptology (i.e., cryptography and cryptanalysis) and chosen areas of data security plus links to information on more than 800cryptographers; total number of links thus exceeds *7000*! Maintained by Helger Lipmaa, <helger.lipmaa>@gmail.com. Any comments and additions are welcome. for