1. Record Nr. UNISA996465804403316

Titolo	Advances in cryptology--CRYPTO '91 : proceedings of CRYPTO 82 / / Edited by G. Goos and J. Hartmanis
Pubbl/distr/stampa	Berlin, Germany ; ; New York, New York : , : Springer-Verlag, , [1985] ©1985
ISBN	3-540-39568-7
Edizione	[1st ed. 1985.]
Descrizione fisica	1 online resource (XII, 496 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 196
Disciplina	001.64
Soggetti	Computers - Access control Chemistry, Physical and theoretical
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references at the end of each chapters and index.
Nota di contenuto	Public Key Cryptosystems and Signatures -- A Prototype Encryption System Using Public Key -- A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms -- A Public-Key Cryptosystem Based on the Word Problem -- Efficient Signature Schemes Based on Polynomial Equations (preliminary version) -- Identity-Based Cryptosystems and Signature Schemes -- A Knapsack Type Public Key Cryptosystem Based On Arithmetic in Finite Fields (preliminary draft) -- Some Public-Key Crypto-Functions as Intractable as Factorization -- Cryptosystems and Other Hard Problems -- Computing Logarithms in GF (2n) -- Wyner's Analog Encryption Scheme: Results of a Simulation -- On Rotation Group and Encryption of Analog Signals -- The History of Book Ciphers -- An Update on Factorization at Sandia National Laboratories -- An LSI Digital Encryption Processor (DEP) -- Efficient hardware and software implementations for the DES -- Efficient hardware implementation of the DES -- A Self-Synchronizing Cascaded Cipher System with Dynamic Control of Error Propagation -- Randomness and Its Concomitants -- Efficient and Secure Pseudo-Random Number Generation (Extended Abstract) -- An LSI Random Number Generator (RNG) -- Generalized Linear Threshold Scheme -- Security of Ramp Schemes -- A Fast Pseudo Random Permutation Generator With Applications to Cryptology -- On the Cryptographic

Applications of Random Functions (Extended Abstract) -- An Efficient Probabilistic Public-Key Encryption Scheme Which Hides All Partial Information -- Analysis and Cryptanalysis -- RSA/Rabin least significant bits are secure (Extended Abstract) -- Information Theory without the Finiteness Assumption, I: Cryptosystems as Group-Theoretic Objects -- Cryptanalysis of Adfgvx Encipherment Systems -- Breaking Iterated Knapsacks -- Dependence of output on input in DES: Small avalanche characteristics -- Des has no Per Round Linear Factors -- Protocols and Authentication -- A Message Authenticator Algorithm Suitable for a Mainframe Computer -- Key Management for Secure Electronic Funds Transfer in a Retail Environment -- Authentication Theory/Coding Theory -- New Secret Codes Can Prevent a Computerized Big Brother -- Fair Exchange of Secrets (extended abstract) -- Cryptoprotocols: Subscription to a Public Key, The Secret Blocking and The Multi-Player Mental Poker Game (extended abstract) -- Poker Protocols -- Impromptu Talks -- A “Paradoxical” Solution to The Signature Problem -- Sequence Complexity as a Test for Cryptographic Systems -- An Update on Quantum Cryptography -- How to Keep a Secret Alive.

Sommario/riassunto

Recently, there has been a lot of interest in provably "good" pseudo-random number generators [lo, 4, 14, 31. These cryptographically secure generators are "good" in the sense that they pass all probabilistic polynomial time statistical tests. However, despite these nice properties, the secure generators known so far suffer from the han- cap of being inefiicient; the most efiicient of these take n2 steps (one modular multip- cation, n being the length of the seed) to generate one bit. Pseudc-random number g- erators that are currently used in practice output n bits per multiplication (n2 steps). An important open problem was to output even two bits on each multiplication in a cryptographically secure way. This problem was stated by Blum, Blum & Shub [3] in the context of their z2 mod N generator. They further ask: how many bits can be o- put per multiplication, maintaining cryptographic security? In this paper we state a simple condition, the XOR-Condition and show that any generator satisfying this condition can output logn bits on each multiplication. We show that the XOR-Condition is satisfied by the lop least significant bits of the z2-mod N generator. The security of the z2 mod N generator was based on Quadratic Residu- ity [3]. This generator is an example of a Trapdoor Generator [13], and its trapdoor properties have been used in protocol design. We strengthen the security of this gene- tor by proving it as hard as factoring.