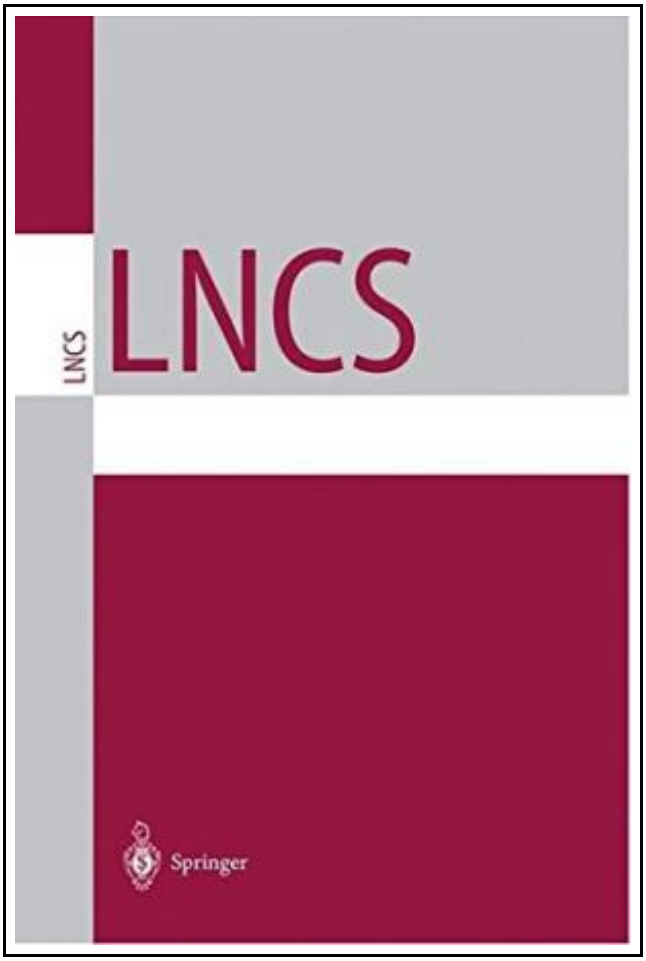
Advances in Cryptology: Proceedings of Crypto 84



Filesize: 4.9 MB

Reviews

A whole new e book with a new point of view. This is certainly for all those who statte there had not been a well worth looking at. I am just very easily could get a delight of looking at a created pdf.
(Hyman Goyette)

ADVANCES IN CRYPTOLOGY: PROCEEDINGS OF CRYPTO 84

Springer. Paperback. Book Condition: New. Paperback. 496 pages. Dimensions: 11.0in. x 8.5in. x 1.1in.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 and 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. This item ships from multiple locations. Your book may arrive from Roseburg,OR, La Vergne,TN. Paperback.

Other PDFs

Marm Lisa

Echo Library. Paperback. Book Condition: New. Paperback. 80 pages. Dimensions: 9.0in. x 6.0in. x 0.2in.Kate Douglas Wiggin, nee Smith (1856-1923) was an American childrens author and educator. She was born in Philadelphia, and was of...

Download Document »

DK Readers Invaders From Outer Space Level 3 Reading Alone

DK CHILDREN. Paperback. Book Condition: New. Paperback. 48 pages. Dimensions: 8.9in. x 5.9in. x 0.1in.Are aliens from other planets visiting Earth Read these amazing stories of alien encounters -- and make up your own mind!...

Download Document »

Dont Line Their Pockets With Gold Line Your Own A Small How To Book on Living Large

Madelyn D R Books. Paperback. Book Condition: New. Paperback. 106 pages. Dimensions: 9.0in. x 6.0in. x 0.3in.This book is about my cousin, Billy a guy who taught me a lot over the years and who...

Download Document »

Molly on the Shore, BFMS 1 Study score

Petrucci Library Press. Paperback. Book Condition: New. Paperback. 26 pages. Dimensions: 9.7in. x 6.9in. x 0.3in.Percy Grainger, like his contemporary Bela Bartok, was intensely interested in folk music and became a member of the English...

Download Document »

Shepherds Hey, Bfms 16: Study Score

Petrucci Library Press. Paperback. Book Condition: New. Paperback. 22 pages. Dimensions: 9.4in. x 7.1in. x 0.0in.Percy Grainger, like his contemporary Bela Bartok, was intensely interested in folk music and became a member of the English...

Download Document »