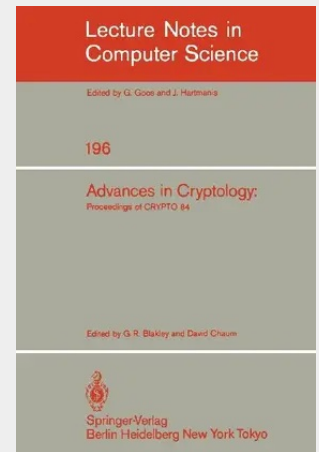


Advances in Cryptology

Proceedings of CRYPTO '84

Recently, there has been a lot of interest in provably "good" pseudo-random number generators [10, 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 handicap of being inefficient; the most efficient of these take n^2 steps (one modular multiplication, n being the length of the seed) to generate one bit. Pseudo-random number generators that are currently used in practice output n bits per multiplication (n^2 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 $z^2 \bmod N$ generator. They further ask: how many bits can be output 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 $\log n$ bits on each multiplication. We show that the XOR-Condition is satisfied by the $\log$ least significant bits of the $z^2 \bmod N$ generator. The security of the $z^2 \bmod N$ generator was based on Quadratic Residuosity [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 generator by proving it as hard as factoring.

Recently, there has been a lot of interest in provably "good" pseudo-random number generators [10, 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 handicap of being inefficient; the most efficient of these take n^2 steps (one modular multiplication, n being the length of the seed) to generate one bit. Pseudo-random number generators that are currently used in practice output n bits per multiplication (n^2 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 $z^2 \bmod N$ generator. They further ask: how many bits can be output 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 $\log n$ bits on each multiplication. We show that the XOR-Condition is satisfied by the $\log$ least significant bits of the $z^2 \bmod N$ generator. The security of the $z^2 \bmod N$ generator was based on Quadratic Residuosity [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 generator by proving it as hard as factoring.



53,49 €

49,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783540156581
Medium: Buch
ISBN: 978-3-540-15658-1
Verlag: Springer
Erscheinungstermin: 01.07.1985
Sprache(n): Englisch
Auflage: 1. Auflage 1985
Serie: Lecture Notes in Computer Science
Produktform: Kartoniert
Gewicht: 1560 g
Seiten: 496
Format (B x H): 155 x 235 mm

