

**Beaver, Donald**

**Correlated pseudorandomness and the complexity of private computations.** (English)

Zbl 0917.94012

Proceedings of the 28th annual ACM symposium on the theory of computing (STOC). Philadelphia, PA, USA, May 22–24, 1996. New York, NY: ACM, 479-488 (1996).

**MSC:**

94A60 Cryptography

68Q25 Analysis of algorithms and problem complexity

68P25 Data encryption (aspects in computer science)

Cited in **2** Reviews  
Cited in **22** Documents

**Keywords:**

cryptographic primitives; obvious transfer; random number generation; one-way function; complexity; complete Boolean function