

**Meeting:** 998, Houston, Texas, SS 17A, Special Session on Coding Theory and Cryptography

998-11-400            **Oliver A Schirokauer\*** ([oliver.schirokauer@oberlin.edu](mailto:oliver.schirokauer@oberlin.edu)), Department of Mathematics,  
Oberlin College, Oberlin, OH 44074. *Computing discrete logarithms in finite fields*. Preliminary  
report.

I will discuss some recent implementations of the number field sieve and function field sieve algorithms for computing discrete logarithms in a finite field  $F$ . I will pay particular attention to the methods used to overcome the obstruction caused by the need to construct  $l$ th powers in a global field for a prime divisor  $l$  of  $|F^*|$ .

(Received March 02, 2004)