

1107-11-342

R. Wm. Gosper, **Hilarie Orman** (hilarie@purplestreak.com) and **Rich Schroepel***
(rcs@xmission.com). *Cryptographic Applications for Somos Sequences*.

We present a Diffie-Hellman key exchange and an ElGamal style signature scheme based on Somos Sequences over finite fields. The sequences have novel formulas for computing "giant steps" without relying on cyclic group structures. Our schemes use index addition instead of multiplication. (Received January 19, 2015)