Beaver, Cheryl L.; **Gemmell, Peter S.**; **Johnston, Anna M.**; **Neumann, William**
On the cryptographic value of the q^{th} root problem. (English) Zbl 1014.94553
Varadharajan, Vijay (ed.) et al., Information and communication security. 2nd international conference, ICICS '99, Sydney, Australia, November 9-11, 1999. Proceedings. Berlin: Springer. Lect. Notes Comput. Sci. 1726, 135-142 (1999).

Summary: The authors show that, for a prime q and a group G, if $\mathrm{ord}(G) = q^k r$, $k > 1$, and r is smooth, then finding a qth root in G is equivalent to the discrete logarithm problem over G (note that the discrete logarithm problem over the group G reduces to the discrete logarithm problem over a subgroup of order q – see *S. Pohlig* and *M. Hellman* [IEEE Trans. Inf. Theory 24, 106-110 (1978; Zbl 0375.68023)]. Several publications describe techniques for computing qth roots. All have the stated or implied requirement of computing discrete logarithms in a subgroup of order q.

The emphasis here will be on demonstrating that with a fairly general qth root oracle, discrete logarithms in a subgroup of order q may be found, describing the cryptographic significance of this problem, and in introducing two new public key signature schemes based on it.

For the entire collection see [Zbl 0931.00051].

MSC:

94A60 Cryptography
11Y16 Number-theoretic algorithms; complexity

Keywords:

discrete logarithms; subgroup of order q; cryptographic significance; public key signature schemes