ECC/DLP and Factoring-Based Cryptography: A Tale of Two Families (Invited Lecture)

Burton S. Kaliski Jr.

RSA Laboratories, 20 Crosby Drive, Bedford, MA 01730, USA
E-mail: burt@rsa.com

Abstract. They came into prominence in the 1970's, though their roots extend back several centuries. In the 1980's, they survived substantial testing and many new members were added. The roles of their various members became better understood in the 1990's, as the families gained influence throughout the world.

These are, of course, the two families of public-key cryptography. One family consists of algorithms whose security is based on the discrete logarithm problem (DLP), including elliptic curve cryptography (ECC). The other bases its security on the difficulty of integer factorization. Today, both families have significant influence and applications. They have much in common, having emerged, survived and grown together.

Researchers have studied numerous aspects of these families, from underlying security, to algorithms and protocols, to generation of keys and parameters, to efficient implementation. Standards are being written with each family in mind, and it is clear that each family will play a part in the security infrastructure that is now being developed.

How the families came to be, how they are similar, how they differ, and how the strengths of each can be combined, are all questions of current interest in assessing what role each family is likely to have, as we move into the next century.

K. Ohta and D. Pei (Eds.): ASIACRYPT'98, LNCS 1514, p. 50–50, 1998.