Additional ECC Resources

Code and Cipher

ECC Challenge

ECC Challenge details (PDF)

ECC FAQ

ECC Tutorial

Certicom's SHA-3 Submission

Certicom was founded in 1985 by Dr. Scott A. Vanstone and Dr. Ron Mullin, to further the research started at the University of Waterloo on Public-Key Cryptography. Dr. Vanstone is one of the leading experts in the field of Elliptic Curve Cryptography (ECC) research, having authored or co-authored over 250 publications on the topic.

The research team is very focused on ECC technology, including studying efficient implementations, methods to enhance the security and developing new protocols.

Today, Certicom holds over 300 patents pending and filed relating to ECC. The patents cover all areas of security optimizations and security implementations, including general concept hardware, protocol, curve selection, efficiencies, certificates and VPN.

Our flagship product, Security Builder Crypto, initially released in 1997, was the first commercial product based on ECC.

The Certicom ECC Challenge was introduced in 1997 to increase industry understanding and appreciation for the difficulty of the elliptic curve discrete logarithm problem, and to encourage and stimulate further research in the security analysis of elliptic curve cryptosystems.

We also continue to maintain a co-operative relationship with the university through corporate sponsorship of the Centre for Applied Cryptographic Research . Since 1999, we have sponsored their annual Workshop on Elliptic Curve Cryptography.

Research Members	Research Associates
Dr. Scott A. Vanstone	Dr. Darrel Hankerson
Dr. Adrian Antipa	Dr. Alfred J. Menezes
Dr. Daniel R.L. Brown	Dr. Ron C. Mullin
Dr. Robert P. Gallant	Dr. Taher Elgamal
Dr. John O. Goyo	
Dr. Robert J. Lambert	
Dr. Matthew Campagna	

Dr. David Kravitz
Dr. Nevine Ebeid
Dr. Greg Zaverucha