ECCPERT
Elliptic Curve Cryptosystem Development and Design

Christina Miller
Department of Computer Science and Electrical Engineering
University of Queensland

October 15, 1999

Abstract

ECCpert is an implementation of an Elliptic Curve Cryptosystem which is based over a finite field from special class called Optimal Extension Fields (OEFs). OEFs utilise the fast integer arithmetic available on modern processors to produce very efficient results. Thus, they do not need to resort to multiprecision operations or arithmetic using polynomials of large degree. This paper discusses the theoretical and implementation issues associated with the development of this system. The performance results of ECCpert have shown that it has the potential to outperform the existing systems.

1 Introduction

With the development of the Internet and the current increasing demands for electronic business transactions, the need for secure communication via insecure channels is becoming of paramount importance. Public-key cryptosystems have made an enormous impact on secure communications and commerce by allowing nearly all the information, including keys, to be distributed over an insecure communications channel. Traditionally, systems such as RSA [8] and DSS [3] have been used for this purpose. However, Elliptic Curve Cryposystems (ECCs) have become a viable alternative since they provide greater security. ECCs utilise the group of points on an elliptic curve to provide secure communications.

This paper discusses the design and implementation of ECCpert: a fully functional ECC which provides commercial strength encryption. This system is based on a special type of finite field that have the potential to provide more efficient systems than the current fields in use. The initial results from ECCpert have been extremely promising and with further efficiences in place, and a more appropriate testing platform, ECCpert will outperform the existing commericial systems.

Within this paper, an introduction to cryptography and ECCs is presented and a brief background in the types of finite fields used is given. The ECCpert implementation is discussed and the initial results are stated.

2 Background

In 1976, Diffe and Hellman [2] developed an entirely new field of cryptography, called *public-key cryptography*, which made an enormous impact on the direction and applications of cryptography and shifted the focus of cryptography away from defence and government to secure commercial electronic business transactions.

Elliptic curves were first suggested as public-key cryptosystems independently by Koblitz [4] and Miller [7] in 1985. ECCs are based on the group of points on an elliptic curve over a finite field. They rely on the difficulty of finding the value of a scalar, given a point and that scalar multiple of that point. This corresponds to solving the *Discrete Logarithm Problem* [5]. However, it is more difficult to solve the elliptic curve discrete logarithm problem than its original counterpart. Thus, elliptic curve cryptosystems provide equivalent security as the existing public-key cryptosystems, but with much smaller key lengths. Therefore, they have smaller bandwidth and memory requirements which makes them extremely desirable for embedded systems such as smart cards, as well as use on personal computers and workstations.

Traditionally, ECCs are based on either prime fields $GF(p)$ or binary extension fields $GF(2^m)$. Although the prime fields can use integer arithmetic, to be secure, the size of the integers required far exceeds the size of an integer in a modern processor. Thus, inefficient multiprecision algorithms are necessary. Although binary extension fields use efficient binary subfield calculations, they require polynomials of large degree, which can be inefficient.

ECCpert is based on an ECC over a finite field with prime power order, that is $GF(p^m)$ where p is an odd prime and m is a positive integer. These give the practical benefits of both prime and binary extension fields without their limitations. The advantages are that all subfield arithmetic is integer arithmetic and does not require any multiprecision calculations. In addition,the polynomial degree n is very small for all secure fields so that the number of subfield calculations $(= n)$ is minimised.

For software solutions where the integer arithmetic operations are optimised, these fields $GF(p^m)$ are potentially faster, but have not previously been investigated fully since they require a more general approach that does not lead itself to specialised, tuned algorithms.

ECCpert uses a new class of finite fields in $GF(p^m)$ to achieve fast finite field arithmetic which are called OEFs [1]. The properties that are stipulated for the choice of p and m include choosing p to be less than but close to the word size of the processor so that all the subfield operations take advantage of the processor's fast integer arithmetic. Also, m should be chosen so that we have an irreducible binomial $x^m - \omega$ for efficient extension field modular reduction. The extension degree m can be small if the processor word size allows for large values of p.

As an example, when a modern PC with 32-bit architecture, such as the Intel Pentium family is the target platform, p would be chosen to be near 2^{32}. This approach has the advantage of fully exploiting the CPU's ability to perform 32-bit × 32-bit integer multiplication.

3 ECCpert Implementation

ECCpert [6] is a commerically secure ECC and thus provides the following functionality:

- initialisation of the cryptosystem, including the finite field $GF(p^m)$, elliptic curve E, and a random point G on E with order large enough so that the discrete logarithm problem is intractible;
- initialisation of keys for a user and public access to its public key;
- encryption of any plaintext messages to be sent to other users of the system;
- decryption of an encrypted message sent by any user to produce the original message.

ECCpert was designed and tested using Visual C++ version 6.0 under Windows 98. It was designed using a Win32 console application with the low level routines written in C for higher speeds and encapsulated in C++ classes for ease of use. For its demonstration, ECCpert was presented as an MFC GUI application under Windows 98.

4 Results

ECCpert's performance is very encouraging: it produced very fast results for all of the major arithmetic operations and acceptable times for the initialisation of OEF fields. With more computing power and time to improve the algorithms, ECCpert has the potential to be more efficient than all existing binary extension fields and prime field software implementations.

The major operations for both the OEF arithmetic and elliptic curve arithmetic over OEF fields were evaluated. Three representative fields were chosen with prime p ranging from 16 to 30 bits in length. Because commercially secure cryptosystems have a field bitlength of between 160- and 260-bits, all of the representative fields were chosen with orders within this range. Each of the two major operations were tested: OEF multiplication; OEF division. The results are given in Table 1 which were done on a Pentium II 350MHz machine with 64MB RAM.

5 Conclusions

ECCpert has successfully demonstrated the benefits of using elliptic curves as cryptosystems, in particular elliptic curves over $GF(p^m)$. Its performance was evaluated and the results are very encouraging, with OEF division only taking 61.1(μs) with a field of order 239. Thus, with further efficencies, and a more powerful testing platform, ECCpert will potentially outperform the existing systems over prime and binary extension fields.

References

[1] D. Bailey, C. Paar. Optimal Extension Fields for Fast Arithmetic in Public-Key Algorithms, *CRYPTO '98*, Springer-Verlag, Berlin, pp. 472-485, 1998.

[2] W. Diffe, M. E. Hellman. New Directions in Cryptography, *IEEE Transactions on Information Theory*, IT-22:644-654, 1976.

[3] FIPS 46. *Data encryption standard*, Federal Information Processing Standards Publication 46, U.S. Department of Commerce/National Bureau of Standards, National Technical Information Service, Springfield, Virginia, 1977.

[4] N. Koblitz. Elliptic Curve Cryptosystems, *Mathematics of Computation*, 48:203-209, 1987.

[5] A. Menezes, P. Oorschot, S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, USA, 1997.

[6] C. Miller, *ECCpert - Elliptic Curve Cryptosystem Development and Design*, Bachelor of Engineering Thesis, University of Queensland, 1999.

[7] V. Miller. Uses of Elliptic Curves in Cryptography, *CRYPTO '85*, Springer-Verlag, Berlin, pp. 417-426, 1976.

[8] R. L. Rivest, A. Shamir, L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, *Communications of the ACM*, 21(2):120-126.

Biography

Christina Miller was born in Brisbane, Australia in 1977, and is currently a final year combined Science and Computer System Engineering undergraduate.

She has significant experience in cryptography and software development. She worked extensively for CSIRO in the field of image processing. Her interests include cryptography, software development, and pure mathematics.

Field Bitlength	Base $p = 2^n - c$	Extension $x^m - \omega$	OEF Mult. (μs)	OEF Div. (μs)
239	$2^{16} - 165$	$x^{15} - 2$	233	61.1
215	$2^{24} - 243$	$x^9 - 2$	94.3	62.6
209	$2^{30} - 35$	$x^7 - 2$	64.2	73.0

Table 1: ECCpert Arithmetic Results on Pentium II 350MHz