The Application of Elliptic Curves Cryptography in Embedded Systems

Wang Qingxian
School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, 610054, P. R. China
msshang@uestc.edu.cn

Abstract

It is widely recognized that data security will play a central role in the design of future IT systems. Many of those IT applications will be realized as embedded systems which rely heavily on security mechanisms. This paper focuses on basic concepts, properties and performance of Elliptic Curves Croptosystems (ECC), the relevance between ECC and embedded systems applications, and the performance advantages to be obtained in the embedded systems
Keywords: *ECC; Embedded system; Security*

1. Introduction

It is widely recognized that data security will play a central role in the design of future IT systems. Forecasters predict more than a billion wireless users by 2005[1]. With the wireless industry exploding, it faces a growing need for security. Many of those applications rely heavily on security mechanisms, such as security for wireless phones, faxes, wireless computing, pay-TV, and copy protection schemes for audio/video consumer products and digital cinemas. Note that a large share of those embedded applications will be wireless, which makes the communication channel especially vulnerable and the need for security even more obvious.

In addition to embedded devices, the explosive growth of digital communications also brings additional security challenges. Millions of electronic transactions are completed each day, and the rapid growth of eCommerce has made security a vital issue for many consumers. In the future, valuable business opportunities will be realized over the Internet and megabytes of sensitive data will be transferred and moved over insecure communication.

Therefore, both for secure (authenticated, private) Web transactions and for secure (signed, encrypted) messaging, a full and efficient public key infrastructure is needed.

Three basic choices for public key systems are available for these applications:

• RSA

The RSA cryptosystem, invented by Ron Rivest, Adi Shamir, and Len Adleman [7]. The cryptosystem is most commonly used for providing privacy and ensuring authenticity of digital data.

• DH or DSA

Diffie and Hellman invented an entirely new type of cryptography, called public key [8]; Digital Signature Algorithm (DSA) are based on the discrete log problem in a prime field F_p. In 1991， the U.S. govern-ment's National Institute of Standards and Technology proposed a digital signature standard using the DSA.

• ECDH or ECDSA

RSA is a system that was published in 1978 by Rivest, Shamir, and Adleman, based on the difficulty of factoring large integers. Whitfield Diffie and Martin Hellman proposed the public key system now called Diffie-Hellman Key Exchange in 1976. DH is key agreement and DSA is signature, and they are not directly interchangeable, although they can be combined to authenticate key agreement. Both the key exchange and digital signature algorithm are based on the difficulty of solving the discrete logarithm problem in the multiplicative group of integers modulo a prime p. Elliptic curve groups were proposed in 1985 as a substitute for the multiplicative groups modulo p in either the DH or DSA protocols.

For the same level of security per best currently known attacks, elliptic curve-based systems can be implemented with much smaller parameters, leading to significant performance advantages. Such performance improvements are particularly important in the wireless arena where computing power, memory, and battery life of devices are more constrained.

This paper focuses on basic concepts, properties and performance of Elliptic Curves Croptosystems(ECC), the relevance between ECC and embedded systems applications, and the performance advantages to be obtained in the embedded systems.

2. Background on elliptic curves

Assume first that F is a field of characteristic not equal to 2 or 3. An elliptic curve E over F is an equation

$$y^2=x^3+ax+b \qquad (1)$$

where $a,b\in F$,and $4a^3+27b^2\neq 0$ （mod p）(the latter condition ensures that the cubic on the right does not have multiple roots). If K is a field containing F, then the set of K-points of *E*, denoted *E(K)*, consists of all solutions (x, y) $\in$ $K\times K$ of equation (1) together with a special point ∞ called the point at infinity.

It is well known that *E(K)* is an (additively written) abelian group with the point ∞ serving as its identity element. The rules for group addition are summarized below.

2.1 Addition formulas

The following are Addition Formulas for the Curve (1):

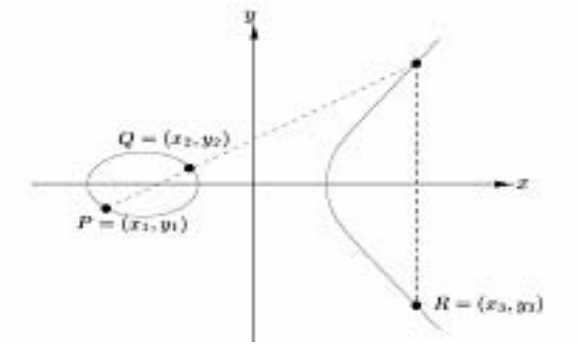
If $P=(x_1,y_1)\in E$ ， then $-P=(x_1,-y_1)$. If $Q=(x_2,y_2)\in E$, $Q\neq -P$,then P+Q= (x_3, y_3), where

$$\begin{cases} x_3=k^2-x_1-x_2 \\ y_3=k(x_1-x_3)-y_1 \end{cases} \qquad (2)$$

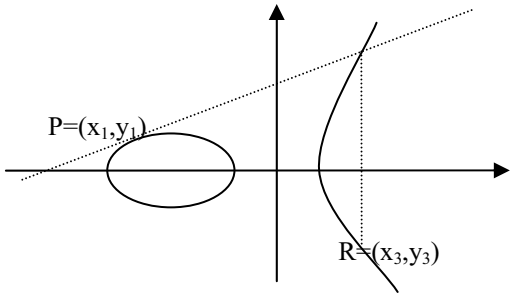
and

$$k=\begin{cases} \dfrac{y_2-y_1}{x_2-x_1}, & (P\neq Q) \\ \dfrac{3x_1^{\,2}+a}{2y_1}, & (P=Q) \end{cases} \qquad (3)$$

There is a nice classical way | called the chord and tangent construction— to visualize the group law on an elliptic curve defined over the real numbers. We illustrate with the elliptic curve $y^2 = x^3 - x$, pictured in Figure 1.



(a) Addition: P+Q=R



(b) Doubling: P+P=R

Fig. 1. Geometric addition and doubling of elliptic curve points.

To add two points *P* and *Q*, we draw a chord between them and find its third point of intersection with the curve. The point R symmetric to this point with respect to the x-axis is the sum *P* + *Q*. If *Q* = *P*, then instead of a chord we take the tangent line to the curve at *P*.

For *k* a positive integer and *P* a point we use the notation *kP* to denote *P* added to itself k times.

If F is a field of characteristic 3, then we have an equation similar to (1) but with an x_2-term which cannot be eliminated by a linear change of variables. The formulas for point addition are similar to the ones above.

Elliptic curves defined over a finite field are of two types. Most are what are called ordinary or non-supersingular curves, but a small number are supersingular. If *F* is a field of characteristic 2, then a supersingular elliptic curve *E* is an equation

$$y^2 + cy = x^3 + ax + b \qquad (4)$$

where *a, b, c* $\in F$, $c \neq 0$, together with the point at infinity ∞; and a non-supersingular elliptic curve E is an equation

$$y^2 + xy = x^3 + ax^2 + b \quad (5)$$

where *a, b* $\in F$, $b \neq 0$, together with the point at infinity ∞. In both cases, *E(K)* for any $K \supset F$ is an abelian group with the point ∞ serving as the identity. The addition formulas for the two types of curves in characteristic 2 are similar to the ones given above for equation (1).

2.2 Properties of elliptic eurve rational Points group

If E is defined over a finite field Fq, then E(Fq) is a finite abelian group of rank 1 or 2; in other words, either it is cyclic or else a product of two cyclic groups. We have E(Fq) $\cong C_{n_1} \oplus C_{n_2}$, , where Cn denotes a cyclic group of order n, n_2 divides n_1, and furthermore $n_2|(q-1)$. A well-known theorem of Hasse (see[2], p. 131) states that the cardinality #E(Fq) = q + 1- t, where $|t| \leq 2\sqrt{q}$ .We call [q +1- $2\sqrt{q}$, q +1+ $2\sqrt{q}$] the Hasse interval. The curve E is said to be supersingular if t^2 = 0,q, 2q, 3q, or 4q; otherwise the curve is non-supersingular.

When q is a power of 2, this agrees with the definition given earlier. In that case #E(Fq) is odd if E is supersingular and even if E is non-supersingular.

A result of Waterhouse states that if q is a prime, then for each t satisfying $|t| \leq 2\sqrt{q}$, there exists at least one elliptic curve E defined over Fq with #E(Fq) =q+1-t. If q is a power of 2, then for each even t satisfying $|t| \leq 2\sqrt{q}$ there exists at least one (non-supersingular) elliptic curve E defined over Fq with #E(Fq) = q+1- t. Schoof derived a formula for the number of isomorphism classes of elliptic curves defined over Fq with #E(Fq) = q+1-t for each t satisfying $|t| \leq 2\sqrt{q}$.

The above properties also can see the reference [3].

3 Security levels analysis

The primary advantage that elliptic curve systems have over systems based on the multiplicative group of a finite field (and also over systems based on the intractability of integer factorization) is the absence of a sub-exponential-time algorithm (such as those of "index-calculus" type) that could find discrete logarithms in these groups. Consequently, one can use an elliptic curve group that is smaller in size while maintaining the same level of security. The result is smaller key sizes, bandwidth savings, and faster implementations—features which are especially attractive for security applications where computational power and integrated circuit space is limited, such as smart cards, personal digital assistants, and wireless devices.

Therefore, they have the potential to provide faster public-key cryptosystems with smaller key sizes in comparison with RSA systems. Many public-key algorithms, like Diffie-Hellman, ElGamal, and Schnorr, can be easily implemented in elliptic curves over finite fields.

We can found such as table 1 in a number of the standards documents (e.g., [4]).

Table 1. Key sizes for equivalent security levels (in bits)

ECC-p	ECC-2^m	DH/DSA/RSA-n	Symmetric
192	163	1024	Skipjack: 80
224	233	2048	3-DES: 112
256	283	3072	AES-Small: 128
384	409	7680	AES-Medium:192
521	571	15360	AES-Large:256

For the same level of resistance against the best known attacks, the system parameters for an elliptic-curve-based system can be chosen to be much smaller than the parameters for RSA or mod p systems. For example, in table 1, an elliptic curve over a 163-bit field currently gives the same level of security as a 1024-bit RSA modulus or Diffie-Hellman prime. The difference becomes even more dramatic as the desired security level increases. For example, 571-bit ECC is currently equivalent in security to 15,360-bit RSA/DH/DSA. Public key protocols are used in combination with symmetric key algorithms. The overall strength of the system is the strength of the weakest link. Recently the new federal Advanced Encryption Standard (AES) was introduced, providing greater security than its symmetric key predecessor. At key lengths of 128, 192, and 256, AES has made ECC systems even more attractive as a key agreement alternative.

This growing difference in key bit length for equivalent security levels accounts for the performance advantages to be obtained from substituting ECC for RSA/DH/DSA in public key cryptographic protocols.

4 ECC on embedded systems

In this section, we summarize the contributions in [5] and [6].

In [5], an ECC implementation over prime fields on the 16-bit TI MSP430x33x family of low-cost microcontrollers is described. The authors in [5] show that it is possible to implement EC cryptosystems in highly constrained embedded systems and still obtain acceptable performance at low cost. They modified the EC point addition and doubling formulae to reduce the number of intermediate variables while at the same time allowing for flexibility. In addition, [5] use Generalized-Mersenne primes to implement the arithmetic in the underlying field, taking advantage of the special form of the moduli to minimize the number of precomputations needed to implement the underlying arithmetic. These ideas are combined to achieve an EC scalar point multiplication in 3.4 seconds without any stored/precomputed values and the processor clocked at 1 MHz.

The authors in [6] implemented EC over binary fields on a Motorola Dragonball CPU which is used on the popular Palm Personal Digital Assistants (PDAs). The Dragonball offers 16-bit and 32-bit operations and runs at 16 MHz. Using Koblitz curves over GF(2^{163}), [6] shows that it is possible to perform an ECDSA signature generation operation in less than 0.9 sec. while a verification operation requires less than 2.4 sec. The authors point out that Koblitz curves over fields GF(2^{163}) provide about the same level of security as RSA with a 1024-bit length, while at the same time providing acceptable performance which is not possible to achieve by using RSA-based systems since the integer multiplier in the Dragonball processor is very slow.

This paper focuses on the relevance between Elliptic Curves Croptosystems(ECC) and embedded systems applications, and the performance advantages to be obtained in the embedded systems.

5 Conclusion

We have introduced the basic concepts, properties and performance of Elliptic Curves Croptosystems (ECC), the performance advantages to be obtained in the embedded systems. And by using the [5,6] , illustrate the application of ECC in embedded system.

References

[1]. Kristin Lauter, The Advantages of Elliptic Curve Cryptography for Wireless Security, IEEE Wireless Communications February 2004

[2]. J. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag, 1986.

[3]. Neal Koblitz, A Survey of Public-Key Cryptosystems, August 7, 2004, Available at http://www.cacr.math.uwaterloo.ca/

[4]. Additional ECC Groups for IKE, Mar. 2001, http://www. ietf.org/proceedings/01dec/I-D/draft-ietf-ipsec-ike-eccgroups-03.txt

[5]. J. Guajardo, R. Bluemel, U. Krieger, and C. Paar. Efficient Implementation of Elliptic Curve Cryptosystems on the TI MSP430x33x Family of Microcontrollers. In K. Kim, editor, Fourth International Workshop on Practice and Theory in Public Key Cryptography - PKC 2001, volume LNCS 1992, pages 365{382, Berlin, February 13-15 2001. Springer-Verlag.

[6]. A. Weimerskirch, C. Paar, and S. Chang Shantz. Elliptic Curve Cryptography on a Palm OS Device. In V. Varadharajan and Y. Mu, editors, The 6th Australasian Conference on Information Security and Privacy | ACISP 2001, volume LNCS 2119, pages 502{513, Berlin, 2001. Springer-Verlag.

[7]. R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures andpublic key cryptosystems. Commun. of the ACM, 21:120{126, 1978.

[8]. W.Diffie and M.Hellman, New directions in cryptography, IEEE Transactions on Information Theory, 22 (1976), pp. 644-654.