UNC CHARLOTTE

The Application of Elliptic Curves Cryptography in Embedded Systems

Wang Qingxian
School of Computer Science and Engineering
University of Electronic Science and Technology
China

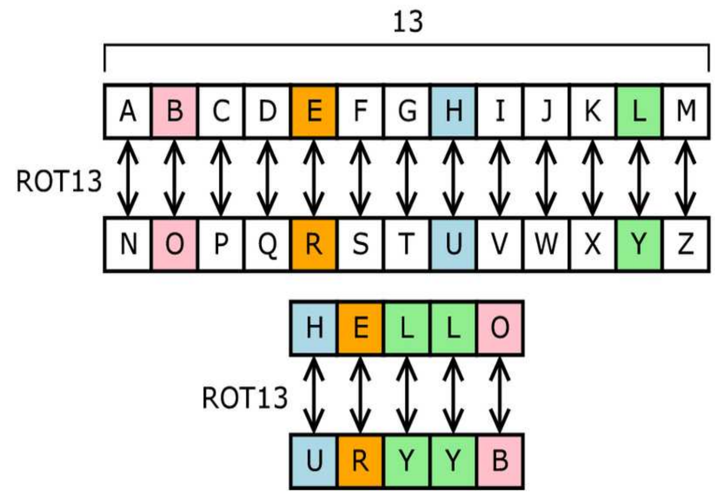
Introduction to Cryptography

Components of a Cryptosystem:

a. Plain text
b. Cipher
c. Code
d. Key

Popular Schemes used:

a. Public-key cryptography
   - Message is encrypted using a public key.
   - It is decrypted using a private key.
   - Private key is related to public key.
b. Three pass protocol
   - Message is encrypted by sender.
   - Message is super encrypted by receiver.
   - Sender decrypts message using private key.
   - Key exchange is not required.



Source:
http://upload.wikimedia.org/wikipedia/commons/2/2a/ROT13.png

Strategies for Public key Infrastructure

- RSA (Ron Rivest, Adi Shamir and Len Adleman)
  - Product of two large prime numbers is used to create a public key and private key.
  - With suitably large prime numbers, the problem of factorization increases.
  - Key sizes increase as the need of security level increase.

- DSA (Digital Signal Algorithm)
  - Based on the problem of discrete log over finite field.
  - For a problem a^b = c, ‘a’ and ‘c’ are known, b is required.
  - Can be solved easily using logarithms.
  - For larger number the complexity increases and desired level of security is achieved.

- DSA and RSA are computationally intensive in terms of memory requirement and time.

Elliptical Curves

Basic Properties:

- Equation of an elliptic curve:
  $y^2 = x^3 + ax + b$

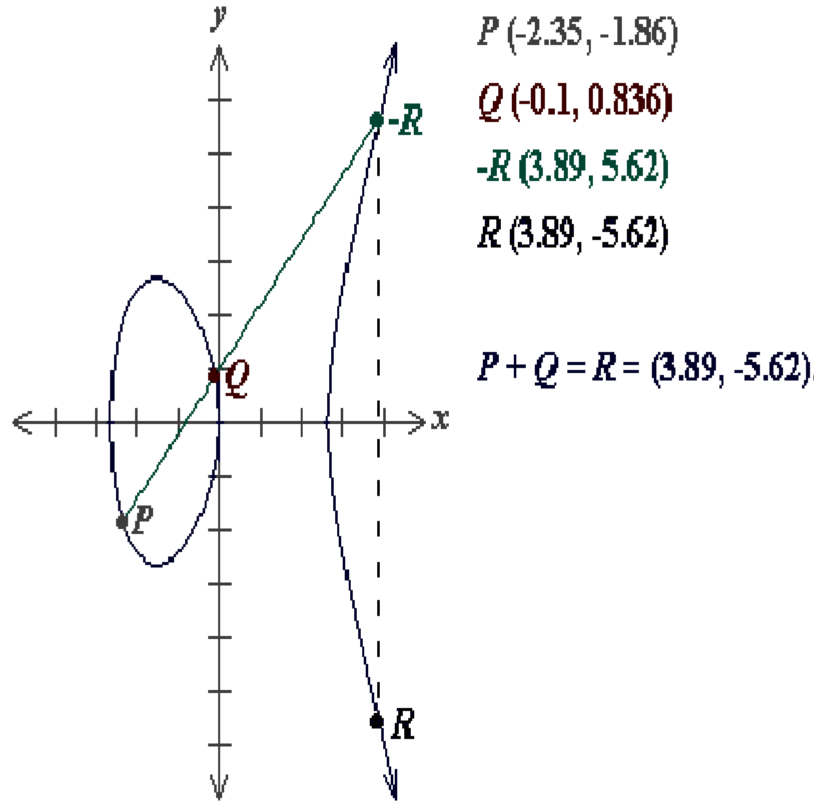
- The equation is defined for no repeated factors.

- Elliptic curve groups are additive groups.

- The addition of any two points on curve is defined geometrically.

- Law of addition:
  P+Q = R.

- The point –R on the curve is reflected on x-axis to point R.

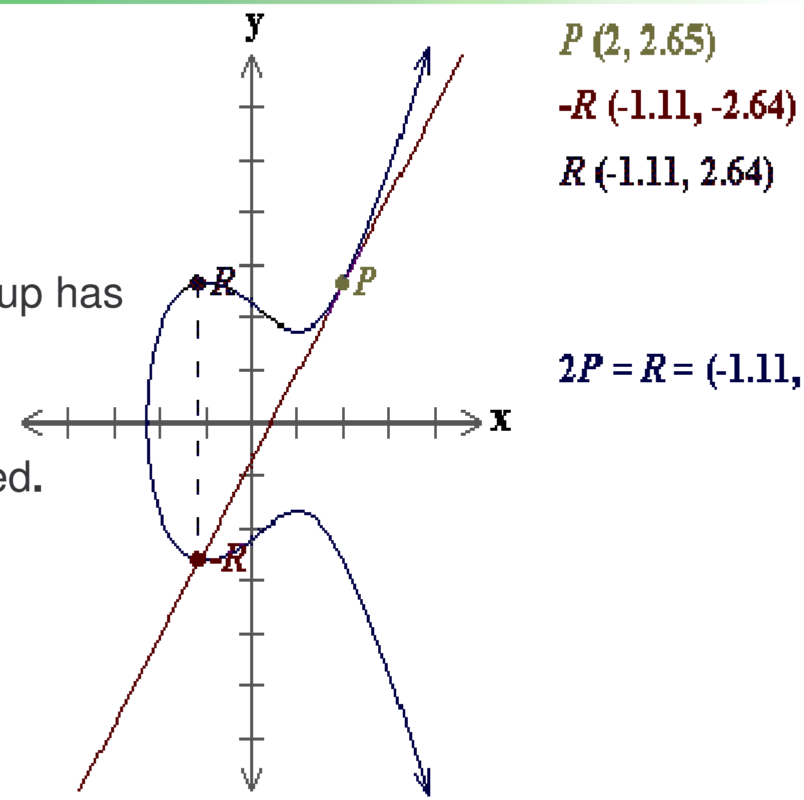


$y^2 = x^3 - 7x$

Source: http://www.certicom.com/index.php?action=ecc_tutorial,ecc_tut_2_1

Elliptical Curves for Cryptography

- Law for doubling a point on elliptic curve
  P+P = 2P = R.
- An essential property for cryptography is that a group has a finite number of points.
- An elliptic curve of underlying field Fp or F_2m is used.
- The modified equation for each underlying field is:
  $y^2 \bmod p = x^3 + ax + b \bmod p$
  $y^2 + xy = x^3 + ax^2 + b$
- Elliptic Curve cryptography is based upon the complexity of discrete log problem.



$y^2 = x^3 - 3x + 5$

Data security and Embedded systems

- Need of data security in Embedded Systems

  - Increase in number of wireless applications
  - Realization of these application on embedded systems platform.

- Current Security Algorithms and Embedded System
  - Time consuming signature generation and authentication.
  - Large key sizes
  - RSA and DSA provide a high level of security, but are expensive in terms of memory.
  - By reducing key size for RSA and DSA, security level is compromised.

- Elliptical Curve DSA (ECDSA)
  - Smaller key sizes without compromising level of security.
  - Quick signature generation and authentication.

ECDSA Implementation

- The elliptic curve discrete log problem:

  Given points P and Q in the group, find a number n such that Pn = Q.

- The private key used is Q.

- Signature generation:

  $r = x\_coord(K = kG) \bmod p$ (For any random number k, with G)
  $s = k$^(-1) ($m + nr$)

- Signature verification:

  - For a user knowing private key Q and verifying signature for message 'm':

    K' = (s^(-1) m) G + (s^(-1) r) Q.
    r' = $x\_coord(K')$

- Accept if r == r'

- Why we obtain smaller key sizes using ECDSA?
  - RSA and DSA complexity increases as the numbers involved increases.
  - The use of finite field and modification in the equation of the curve.

Elliptic-Curve Digital Signature Algorithm (ECDSA)

NIST Guidelines for Public Key Sizes for AES			
ECC key size (bits)	RSA key size (bits)	Key size ratio	AES key size (bits)
163	1,024	1:6	
256	3,072	1:12	128
384	7,680	1:20	192
512	15,360	1:30	256

Supplied by NIST to ANSIX9F1

Table 1

- Advantages of using ECDSA on Embedded systems
  - Signature can be calculated before hand.
  - Smaller key size.
  - Less intensive modular operations.
  - Quick generation of signatures

- Implementation of ECDSA on TI MSP430x33x
  - Acceptable performance at lower cost.
  - Modified underlying field for faster arithmetic operations.
  - Signature generation time is 3.4 sec

- ECDSA on Palm PDAs
  - Signature generation time – 0.9 sec
  - Signature verification time – 2.4 sec
  - 163 bit ECDSA key provides same level of security as 1024 RSA key.

- Conclusion

Performance advantages of ECDSA

- Computationally less intensive than RSA and DSA.
- High security levels in constrained environments.
- Reduction in key size without compromising the data integrity.
- By having smaller key sizes and efficient signature generation ECDSA is extremely suitable for embedded applications.