Justin Ciocoi

Nov. 27, 2023

CSCI 360 Textbook Notes

Chapter 9: Elliptic Curve Cryptosystems

9.1: How to Compute with Elliptic Curves

- Elliptic curve cryptosystems, like other public-key cryptosystems, is based on the generalized discrete logarithm problem
- Thus, we must first find a cyclic group on which we can build our cryptosystem
- The mere existence of such a cyclic group is not enough though, as the group must be computationally hard to prevent against brute-force attacks
- **9.1.1: Definition of Elliptic Curves**
    - The *elliptic curve* over $\mathbb{Z}_p,\ p > 3$, is the set of all pairs $(x, y) \in \mathbb{Z}_p$ which fulfill

      $$y^2 \equiv x^3 + a \cdot x + b \bmod p$$

      together with an imaginary point of infinity, ∞, where

      $$a, b \in \mathbb{Z}_p$$

      and the condition $4 \cdot a^3 + 27 \cdot b^2 \neq 0 \bmod p$

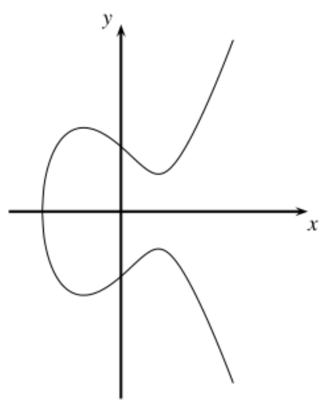
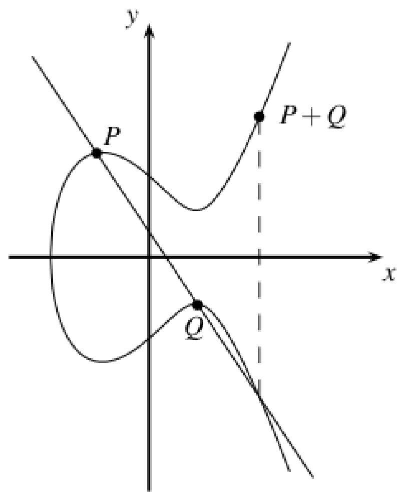
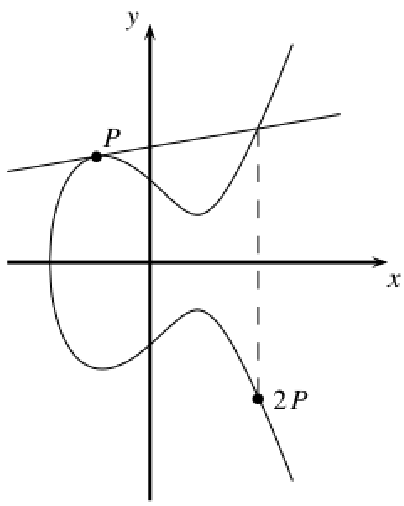


Fig. 9.3 $y^2 = x^3 - 3x + 3$ over $\mathbb{R}$

- **9.2.2: Group Operations on Elliptic Curves**

- Point addition, $P+Q$ and point doubling, $P+P$ can be achieved using the following methods respectively





- In addition, we can find the inverse of a point on an elliptic curve by finding its reflection over the x-axis

9.2: Building a Discrete Logarithm Problem with Elliptic Curves

- **Theorem 9.2.1**

  The points on an elliptic curve together with ∞ have cyclic subgroups, and under certain conditions all points on an elliptic curve form a cyclic group

9.3: Diffie-Hellman Key Exchange with Elliptic Curves

- **Elliptic Curve Diffie-Hellman Domain Parameters**

  1. Choose a prime p and the elliptic curve

$$E : y^2 \equiv x^3 + a \cdot x + b \bmod p$$

2. Choose a primitive element $P = (x_p, y_p)$

The prime p, the curve given by its coefficients a, b, and the primitive element P are the domain parameters

- Key exchange here is done in essentially the same way as conventional Diffie-Hellman key exchange

Elliptic Curve Diffie–Hellman Key Exchange (ECDH)

Alice		**Bob**
choose $k_{prA} = a \in \{2, 3, \ldots, \#E - 1\}$		choose $k_{prB} = b \in \{2, 3, \ldots, \#E - 1\}$
compute $k_{pubA} = aP = A = (x_A, y_A)$		compute $k_{pubB} = bP = B = (x_B, y_B)$
	$\xrightarrow{A}$	
	$\xleftarrow{B}$	
compute $aB = T_{AB}$		compute $bA = T_{AB}$

Joint secret between Alice and Bob: $T_{AB} = (x_{AB}, y_{AB})$.

9.4: Security

- The reason why elliptic curves are used in modern cryptography is the fact that they have very good one way properties
- As opposed to the simpler discrete logarithm problems based in $\mathbb{Z}_p^*$, discrete logarithm problems in elliptic curve groups are not vulnerable to index calculus attacks
- Thus, the best remaining algorithms when attacking an elliptic curve discrete logarithm problem are Shanks' baby-step giant-step methos and Pollard's rho method
- With these attacks, the number of computations needed is the square root of the cardinality of the group
  - Therefore, a prime p should be chosen to be 256 bits in order to provide 128 bits of security, since $\sqrt{2^{256}} = 2^{128}$

9.5: Implementation in Software and Hardware

- In practice, a core requirement for using ECC in cryptography is that the cyclic group formed by the curve points has prime order
- When implementing elliptic curve cryptography, it is useful to view an ECC scheme as a structure with four layers

- On the bottom layer, modular arithmetic is performed
- On the next layer, the two group operations, point addition and point doubling, are realized
- On the third layer, scalar multiplication is realized, which uses the group operations of the previous layer
- The top layer implements the protocol, such as ECDH (Elliptic Curve Diffie-Hellman) or ECDSA (Elliptic Curve Digital Signature Algorithm)