Public Key Cryptography: Introduction

Liljana Babinkostova
The RSA scheme (1977)

Choose a finite group \((G, \circ)\)

Choose an \(n\) with \(\gcd(n, |G|) = 1\)

Compute \(m\) which solves \(1 = x \ast n \mod |G|\)
The RSA scheme (1977)

- Choose a finite group \((G, \circ)\)
The RSA scheme (1977)

- Choose a finite group \((G, \circ)\)
- Choose an \(n\) with \(\gcd(n, |G|) = 1\)
The RSA scheme (1977)

- Choose a finite group \((G, \circ)\)
- Choose an \(n\) with \(\gcd(n, |G|) = 1\)
- Compute \(m\) which solves \(1 = x \ast n \mod |G|\)
Public key cryptosystems based on groups

The RSA scheme
The El Gamal scheme
Elliptic Curve Cryptography

Specify a one-to-one function $E: \text{Set of messages} \rightarrow G$

Publish $n$ and the definition of the group $G$

Keep $m$ SECRET

Private key: $m$

Public key: $E, (G, \circ)$ and $n$
Specify a one-to-one function $E$: Set of messages $\rightarrow G$
• Specify a one-to-one function $E$: Set of messages $\rightarrow G$
• Publish $n$ and the definition of the group $G$
Specify a one-to-one function $E$: Set of messages $\rightarrow G$
Publish $n$ and the definition of the group $G$
Keep $m$ SECRET
Private key: \( m \)
Public key: \( E, (G, \circ) \) and \( n \)

- Specify a one-to-one function \( E: \text{Set of messages} \rightarrow G \)
- Publish \( n \) and the definition of the group \( G \)
- Keep \( m \) SECRET
RSA encryption

Fix a message to be encrypted $M$.

Represent the message as a group element in $(G, \circ)$.

Compute $e = f(M) = M^n$ in the group $(G, \circ)$.

$e$ is the encrypted version of the message (ciphertext).
RSA encryption

- Fix a message to be encrypted
RSA encryption

- Fix a message to be encrypted
- $M = E(message)$ represents the message as a group element in $(G, \circ)$
Fix a message to be encrypted

\[ M = E(message) \] represents the message as a group element in \((G, \circ)\)

Compute \( e = f(M) = M^n \) in the group \((G, \circ)\)
RSA encryption

- Fix a message to be encrypted
- $M = E(message)$ represents the message as a group element in $(G, \circ)$
- Compute $e = f(M) = M^n$ in the group $(G, \circ)$

*e is the encrypted version of the message (ciphertext)*
RSA decryption

Compute $d = h(e) \equiv e^m \pmod{|G|}$

Compute $b = E^{-1}(d)$

$b$ is the decrypted version of the message (plaintext)

d = e^m = (M^n)^m = M^{nm} \equiv M \pmod{|G|}$
Compute $d = h(e) = e^m$ in the group $(G, \circ)$.
RSA decryption

- Compute $d = h(e) = e^m$ in the group $(G, \circ)$
- Compute $b = E^{-1}(d)$
RSA decryption

- Compute $d = h(e) = e^m$ in the group $(G, \circ)$
- Compute $b = E^{-1}(d)$

$b$ is the decrypted version of the message (plaintext)
RSA decryption

- Compute \( d = h(e) = e^m \) in the group \((G, \circ)\)
- Compute \( b = E^{-1}(d) \)

\( b \) is the decrypted version of the message (plaintext)

\[
d = e^m = (M^n)^m = M^{nm} = M^{nm \mod |G|} = M
\]
The Diffie Hellman key negotiation (1976)

- Alice and Bob agree on a finite group \((G, \circ)\)

Alice and Bob agree on a point \(g \in (G, \circ)\)

Alice secretly chooses a positive integer \(m\), and computes

\[ b_A = g^m \text{ in } (G, \circ) \]

Bob secretly chooses a positive integer \(n\), and computes

\[ b_B = g^n \text{ in } (G, \circ) \]

Alice communicates \(b_A\) to Bob, and Bob communicates \(b_B\) to Alice

Alice secretly computes

\[ d_A = b_B^m \text{ in } (G, \circ) \]

Bob secretly computes

\[ d_B = b_A^n \text{ in } (G, \circ) \]

KEY:

\[ d_A = d_B \]

Liljana Babinkostova

Public Key Cryptography: Introduction
The Diffie Hellman key negotiation (1976)

- Alice and Bob agree on a finite group \((G, \circ)\)
- Alice and Bob agree on a point \(g \in (G, \circ)\)
The Diffie Hellman key negotiation (1976)

- Alice and Bob agree on a finite group \((G, \circ)\)
- Alice and Bob agree on a point \(g \in (G, \circ)\)
- Alice secretly chooses a positive integer \(m\), and computes \(b_A = g^m\) in the group \((G, \circ)\)
The Diffie Hellman key negotiation (1976)

- Alice and Bob agree on a finite group \((G, \circ)\)
- Alice and Bob agree on a point \(g \in (G, \circ)\)
- Alice secretly chooses a positive integer \(m\), and computes \(b_A = g^m\) in the group \((G, \circ)\)
- Bob secretly chooses a positive integer \(n\), and computes \(b_B = g^n\) in the group \((G, \circ)\)
The Diffie Hellman key negotiation (1976)

- Alice and Bob agree on a finite group \((G, \circ)\)
- Alice and Bob agree on a point \(g \in (G, \circ)\)
- Alice secretly chooses a positive integer \(m\), and computes \(b_A = g^m\) in the group \((G, \circ)\)
- Bob secretly chooses a positive integer \(n\), and computes \(b_B = g^n\) in the group \((G, \circ)\)
- Alice communicates \(b_A\) to Bob, and Bob communicates \(b_B\) to Alice
The Diffie Hellman key negotiation (1976)

- Alice and Bob agree on a finite group $(G, \circ)$
- Alice and Bob agree on a point $g \in (G, \circ)$
- Alice secretly chooses a positive integer $m$, and computes $b_A = g^m$ in the group $(G, \circ)$
- Bob secretly chooses a positive integer $n$, and computes $b_B = g^n$ in the group $(G, \circ)$
- Alice communicates $b_A$ to Bob, and Bob communicates $b_B$ to Alice
- Alice secretly computes $d_A = b_B^m$ in $(G, \circ)$, and Bob secretly computes $d_B = b_A^n$ in $(G, \circ)$
The Diffie Hellman key negotiation (1976)

- Alice and Bob agree on a finite group \((G, \circ)\)
- Alice and Bob agree on a point \(g \in (G, \circ)\)
- Alice secretly chooses a positive integer \(m\), and computes \(b_A = g^m\) in the group \((G, \circ)\)
- Bob secretly chooses a positive integer \(n\), and computes \(b_B = g^n\) in the group \((G, \circ)\)
- Alice communicates \(b_A\) to Bob, and Bob communicates \(b_B\) to Alice
- Alice secretly computes \(d_A = b_B^m\) in \((G, \circ)\), and Bob secretly computes \(d_B = b_A^n\) in \((G, \circ)\)

KEY : \(d_A = d_B\)
Alice encrypts the message

Fixes a message to be encrypted $M = E(message)$ represents the message as a group element in $(G, \circ)$

Computes $e = M \circ d_A$ in $(G, \circ)$

CIPHERTEXT : $e$
Alice encrypts the message

- Fixes a message to be encrypted
Alice encrypts the message

- Fixes a message to be encrypted
- $M = E(message)$ represents the message as a group element in $(G, \circ)$. 
Alice encrypts the message

- Fixes a message to be encrypted
- $M = E(message)$ represents the message as a group element in $(G, \circ)$
- Computes $e = M \circ d_A$ in $(G, \circ)$
Alice encrypts the message

- Fixes a message to be encrypted
- $M = E(\text{message})$ represents the message as a group element in $(G, \circ)$
- Computes $e = M \circ d_A$ in $(G, \circ)$

**CIPHERTEXT :** $e$
Bob decrypts the message

$v = e \circ d - 1 \in (G, \circ)$

$h = E^{-1}(v)$
Bob decrypts the message

\[ v = e \circ d - 1 \in (G, \circ) \]

\[ h = E^{-1}(v) \]

\[ \text{PLAINTEXT:} \]

Liljana Babinkostova

Public Key Cryptography: Introduction
Bob decrypts the message

- Computes $v = e \circ d_B^{-1}$ in $(G, \circ)$
Bob decrypts the message

- Computes $v = e \circ d_B^{-1}$ in $(G, \circ)$
- Computes $h = E^{-1}(v)$
Bob decrypts the message

- Computes $v = e \circ d_B^{-1}$ in $(G, \circ)$
- Computes $h = E^{-1}(v)$

PLAINTEXT: $h$
The El Gamal scheme (1985)

Choose a finite group \((G, \circ)\)

Choose an element \(g \in (G, \circ)\)

Choose a random number \(x\)

Compute \(b = f(x) = g^x\) in the group \((G, \circ)\)
The El Gamal scheme (1985)

- Choose a finite group \((G, \circ)\)
The El Gamal scheme (1985)

- Choose a finite group \((G, \circ)\)
- Choose an element \(g \in (G, \circ)\)
The El Gamal scheme (1985)

- Choose a finite group \((G, \circ)\)
- Choose an element \(g \in (G, \circ)\)
- Choose a random number \(x\)
The El Gamal scheme (1985)

- Choose a finite group \((G, \circ)\)
- Choose an element \(g \in (G, \circ)\)
- Choose a random number \(x\)
- Compute \(b = f(x) = g^x\) in the group \((G, \circ)\)
Public key cryptosystems based on groups

The RSA scheme
The El Gamal scheme
Elliptic Curve Cryptography

Specify a one-to-one function

\[ E : \text{Set of messages} \rightarrow (G, \cdot) \]

Publish the function \( E, g, b \) and the definition of the group \( (G, \cdot) \)

Keep \( x \) SECRET

Private key: \( x \)
Public key: \( E, (G, \cdot), g, b \)
Specify a one-to-one function $E$: Set of messages $\rightarrow (G, \circ)$
• Specify a one-to-one function $E$: Set of messages $\rightarrow (G, \circ)$
• Publish the function $E, g, b$ and the definition of the group $(G, \circ)$
Specify a one-to-one function $E$: Set of messages $\longrightarrow (G, \circ)$

- Publish the function $E$, $g$, $b$ and the definition of the group $(G, \circ)$
- Keep $x$ SECRET
Specify a one-to-one function $E$: Set of messages $\rightarrow (G, \circ)$

Publish the function $E$, $g$, $b$ and the definition of the group $(G, \circ)$

Keep $x$ SECRET

Private key: $x$
Public key: $E$, $(G, \circ)$, $g$ and $b$
El Gamal encryption

Fix a message to be encrypted $M = E(message)$ represents the message as a group element in $(G, \circ)$.

Choose a random number $r$.

Compute $s = b^r$ in the group $(G, \circ)$.

Compute $y = f(r) = g^r$ in the group $(G, \circ)$.

Compute $e = s \circ M$ in the group $(G, \circ)$.

Keep $r$ SECRET.

The pair $(e, y)$ is the encrypted version of the message (ciphertext).
El Gamal encryption

- Fix a message to be encrypted
El Gamal encryption

- Fix a message to be encrypted
- $M = E(message)$ represents the message as a group element in $(G, \circ)$
El Gamal encryption

- Fix a message to be encrypted
- $M = E(message)$ represents the message as a group element in $(G, \circ)$
- Choose a random number $r$. 
El Gamal encryption

- Fix a message to be encrypted
- $M = E(message)$ represents the message as a group element in $(G, \circ)$
- Choose a random number $r$.
- Compute $s = b^r$ in the group $(G, \circ)$
El Gamal encryption

- Fix a message to be encrypted
- \( M = E(message) \) represents the message as a group element in \((G, \circ)\)
- Choose a random number \( r \).
- Compute \( s = b^r \) in the group \((G, \circ)\)
- Compute \( y = f(r) = g^r \) in the group \((G, \circ)\)
El Gamal encryption

- Fix a message to be encrypted
- $M = E(message)$ represents the message as a group element in $(G, \circ)$
- Choose a random number $r$.
- Compute $s = b^r$ in the group $(G, \circ)$
- Compute $y = f(r) = g^r$ in the group $(G, \circ)$
- Compute $e = s \circ M$ in the group $(G, \circ)$
El Gamal encryption

- Fix a message to be encrypted
- \( M = E(\text{message}) \) represents the message as a group element in \((G, \circ)\)
- Choose a random number \( r \).
- Compute \( s = b^r \) in the group \((G, \circ)\)
- Compute \( y = f(r) = g^r \) in the group \((G, \circ)\)
- Compute \( e = s \circ M \) in the group \((G, \circ)\)
- Keep \( r \) SECRET

The pair \((e, y)\) is the encrypted version of the message (ciphertext)
El Gamal decryption

- Compute $d = y^x$ in the group $(G, \circ)$
- Compute $m = d^{-1} \circ e$ in the group $(G, \circ)$
- Compute $h = E^{-1}(m)$

$h$ is the decrypted version of the message (plaintext)
El Gamal decryption

Compute $d = y^x$ in the group $(G, \circ)$
El Gamal decryption

- Compute $d = y^x$ in the group $(G, \circ)$
- Compute $m = d^{-1} \circ e$ in the group $(G, \circ)$
El Gamal decryption

- Compute $d = y^x$ in the group $(G, \circ)$
- Compute $m = d^{-1} \circ e$ in the group $(G, \circ)$
- Compute $h = E^{-1}(m)$
El Gamal decryption

- Compute $d = y^x$ in the group $(G, \circ)$
- Compute $m = d^{-1} \circ e$ in the group $(G, \circ)$
- Compute $h = E^{-1}(m)$

$h$ is the decrypted version of the message (plaintext)
Fix a group $G$ and an element $g \in G$. The Discrete Logarithm Problem (DLP) for $G$ is

Given an element $b \in <g>$ find an integer $x$ such that $b = g^x$. 
Proposed groups for real-world cryptosystems

- \( \mathbb{F}_p^* \), multiplicative group of prime field (field with prime order).
- \( \mathbb{F}_q^* \), multiplicative group of any finite field.
- \( E(\mathbb{F}_q) \) elliptic curve group

How hard is to solve DLP?
Proposed groups for real-world cryptosystems

- \( \mathbb{F}_p^* \), multiplicative group of prime field (field with prime order).
- \( \mathbb{F}_q^* \), multiplicative group of any finite field.
- \( E(\mathbb{F}_q) \) elliptic curve group

How hard is to solve DLP?

- DLP in \( \mathbb{F}_p^* \) and \( \mathbb{F}_q^* \) can be solved in subexponential time (NFS)
Proposed groups for real-world cryptosystems

- $\mathbb{F}_p^*$, multiplicative group of prime field (field with prime order).
- $\mathbb{F}_q^*$, multiplicative group of any finite field.
- $E(\mathbb{F}_q)$ elliptic curve group

How hard is to solve DLP?

- DLP in $\mathbb{F}_p^*$ and $\mathbb{F}_q^*$ can be solved in subexponential time (NFS)
- The best known attack on DLP in $E(\mathbb{F}_q)$ is exponential (Pollard’s $\rho$)
Proposed groups for real-world cryptosystems

- $\mathbb{F}_p^*$, multiplicative group of prime field (field with prime order).
- $\mathbb{F}_q^*$, multiplicative group of any finite field.
- $E(\mathbb{F}_q)$ elliptic curve group

How hard is to solve DLP?

- DLP in $\mathbb{F}_p^*$ and $\mathbb{F}_q^*$ can be solved in subexponential time (NFS)
- The best known attack on DLP in $E(\mathbb{F}_q)$ is exponential (Pollard’s $\rho$) for now
Public key cryptosystems based on groups

The RSA scheme
The El Gamal scheme
Elliptic Curve Cryptography

Proposed groups for real-world cryptosystems

- $\mathbb{F}_p^*$, multiplicative group of prime field (field with prime order).
- $\mathbb{F}_q^*$, multiplicative group of any finite field.
- $E(\mathbb{F}_q)$ elliptic curve group

How hard is to solve DLP?

- DLP in $\mathbb{F}_p^*$ and $\mathbb{F}_q^*$ can be solved in subexponential time (NFS)
- The best known attack on DLP in $E(\mathbb{F}_q)$ is exponential (Pollard’s $\rho$) for now

Quantum algorithm for solving DLP: Shor’s algorithm (polynomial time algorithm)
The construction of an elliptic curve cryptosystem requires:

1. Selecting a finite field $F_q$.
2. Selecting a representation for the elements of $F_q$.
3. Efficient implementation of the arithmetic in $F_q$.
4. Selecting an appropriate elliptic curve $E$ over $F_q$.
5. Efficient implementation of the elliptic curve operations in $E$.
7. Efficient encryption/decryption algorithms.
The construction of an elliptic curve cryptosystem requires:

1. Selecting a finite field $F_q$. 

Liljana Babinkostova
Public Key Cryptography: Introduction
Construction of Elliptic Curve cryptosystem

The construction of an elliptic curve cryptosystem requires:

1. Selecting a finite field \( F_q \).
2. Selecting a representation for the elements of \( F_q \).
The construction of an elliptic curve cryptosystem requires:

1. Selecting a finite field $F_q$.
2. Selecting a representation for the elements of $F_q$.
3. Efficient implementation of the arithmetic in $F_q$.
Construction of Elliptic Curve cryptosystem

The construction of an elliptic curve cryptosystem requires:

1. Selecting a finite field $F_q$.
2. Selecting a representation for the elements of $F_q$.
3. Efficient implementation of the arithmetic in $F_q$.
4. Selecting an appropriate elliptic curve $E$ over $F_q$. 
Construction of Elliptic Curve cryptosystem

The construction of an elliptic curve cryptosystem requires:

1. Selecting a finite field $F_q$.
2. Selecting a representation for the elements of $F_q$.
3. Efficient implementation of the arithmetic in $F_q$.
4. Selecting an appropriate elliptic curve $E$ over $F_q$.
5. Efficient implementation of the elliptic curve operations in $E$. 
The construction of an elliptic curve cryptosystem requires:

1. Selecting a finite field $F_q$.
2. Selecting a representation for the elements of $F_q$.
3. Efficient implementation of the arithmetic in $F_q$.
4. Selecting an appropriate elliptic curve $E$ over $F_q$.
5. Efficient implementation of the elliptic curve operations in $E$.
The construction of an elliptic curve cryptosystem requires:

1. Selecting a finite field $F_q$.
2. Selecting a representation for the elements of $F_q$.
3. Efficient implementation of the arithmetic in $F_q$.
4. Selecting an appropriate elliptic curve $E$ over $F_q$.
5. Efficient implementation of the elliptic curve operations in $E$.
7. Efficient encryption/decryption algorithms.
The story of ECC

H. W. Lenstra's elliptic curve factoring algorithm (1987)

N. Koblitz and V. Miller independently proposed using the group of points on an elliptic curve defined over a finite field in DL cryptosystems (1985). They never applied for a patent.

Certicom Inc.

Implementation issues

Supersingular elliptic curves (for example $y^2 = x^3 - x$ over $\mathbb{F}_p$ with $4 | (p + 1)$)

MOV attack (1993)

Xedni calculus (1998)

Anomalous curves (1999)

NIST accepted ECC as a standard

ECC nowadays is used in the BlackBerry, Windows Media Player, U.S. Federal Aviation Administration collision avoidance systems, Sony Playstation, ....
The story of ECC

The story of ECC

- N. Koblitz and V. Miller independently proposed using the group of points on an elliptic curve defined over a finite field in DL cryptosystems (1985). They never applied for a patent.
The story of ECC

- N. Koblitz and V. Miller independently proposed using the group of points on an elliptic curve defined over a finite field in DL cryptosystems (1985). They never applied for a patent.
- Certicom Inc.
The story of ECC

- N. Koblitz and V. Miller independently proposed using the group of points on an elliptic curve defined over a finite field in DL cryptosystems (1985). They never applied for a patent.
- Certicom Inc.
- Implementation issues
The story of ECC

- N. Koblitz and V. Miller independently proposed using the group of points on an elliptic curve defined over a finite field in DL cryptosystems (1985). They never applied for a patent.
- Certicom Inc.
- Implementation issues
- Supersingular elliptic curves (for example $y^2 = x^3 - x$ over $\mathbb{F}_p$ with $4| (p + 1)$)
The story of ECC

- N. Koblitz and V. Miller independently proposed using the group of points on an elliptic curve defined over a finite field in DL cryptosystems (1985). They never applied for a patent.
- Certicom Inc.
- Implementation issues
- Supersingular elliptic curves (for example $y^2 = x^3 - x$ over $\mathbb{F}_p$ with $4| (p + 1)$)
- MOV attack (1993)
The story of ECC

- N. Koblitz and V. Miller independently proposed using the group of points on an elliptic curve defined over a finite field in DL cryptosystems (1985). They never applied for a patent.
- Certicom Inc.
- Implementation issues
- Supersingular elliptic curves (for example $y^2 = x^3 - x$ over $\mathbb{F}_p$ with $4 | (p + 1)$)
- MOV attack (1993)
- Xedni calculus (1998)
H. W. Lenstra’s elliptic curve factoring algorithm (1987)
N. Koblitz and V. Miller independently proposed using the group of points on an elliptic curve defined over a finite field in DL cryptosystems (1985). They never applied for a patent.

Certicom Inc.

Implementation issues

Supersingular elliptic curves (for example $y^2 = x^3 - x$ over $\mathbb{F}_p$ with $4|(p + 1)$)

MOV attack (1993)

Xedni calculus (1998)

Anomalous curves (1999)
The story of ECC

- N. Koblitz and V. Miller independently proposed using the group of points on an elliptic curve defined over a finite field in DL cryptosystems (1985). They never applied for a patent.
- Certicom Inc.
- Implementation issues
- Supersingular elliptic curves (for example $y^2 = x^3 - x$ over $\mathbb{F}_p$ with $4 | (p + 1)$)
- MOV attack (1993)
- Xedni calculus (1998)
- Anomalous curves (1999)
- NIST accepted ECC as a standard
The story of ECC

- N. Koblitz and V. Miller independently proposed using the group of points on an elliptic curve defined over a finite field in DL cryptosystems (1985). They never applied for a patent.
- Certicom Inc.
- Implementation issues
- Supersingular elliptic curves (for example $y^2 = x^3 - x$ over $\mathbb{F}_p$ with $4|(p+1)$)
- MOV attack (1993)
- Xedni calculus (1998)
- Anomalous curves (1999)
- NIST accepted ECC as a standard
- ECC nowadays is used in the blackberry, Windows Media Player, U. S. Federal Aviation Administration collision avoidance systems, Sony Playstation, .....
NIST recommended keys

<table>
<thead>
<tr>
<th>Symmetric Key Size (bits)</th>
<th>RSA and Diffie-Hellman Key Size (bits)</th>
<th>Elliptic Curve Key Size (bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>1024</td>
<td>160</td>
</tr>
<tr>
<td>112</td>
<td>2048</td>
<td>224</td>
</tr>
<tr>
<td>128</td>
<td>3072</td>
<td>256</td>
</tr>
<tr>
<td>192</td>
<td>7680</td>
<td>384</td>
</tr>
<tr>
<td>256</td>
<td>15360</td>
<td>521</td>
</tr>
</tbody>
</table>

National Security Agency: “Elliptic Curve Cryptography provides greater security....vendors should seriously consider the elliptic curve alternative.....1024-bit systems are sufficient for use until 2010”
Beyond ECC

Remember the quantum algorithm!
Remember the quantum algorithm!

Academic research for new hard problems for Cryptography

- Lattice based cryptography (∼ 1995)
- Braid group cryptography (∼ 1999)
- Pairing based cryptography (∼ 2000)
Generalized Weierstrass equation

An elliptic curve $E$ over a field $K$ is defined by the equation

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$  \[1\]

where $a_1, a_2, a_3, a_4, a_6 \in K$ and

$$d_2 = a_1^2 + 4a_2$$
$$d_4 = 2a_4 + a_1 a_3$$
$$d_6 = a_2^3 + 4a_6$$
$$d_8 = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2$$
$$\Delta = -d_2^2 d_8 - 8d_4^3 - 27d_6^2 + 9d_2 d_4 d_6 \neq 0$$

Equation [1] is called a Weierstrass equation.

Graph Examples: $y^2 = x^3 - j \ast x + 5, j=1,2,3,...,200$
**Question:** To what extent is the Weierstrass equation for an elliptic curve unique?

Any two Weierstrass equations for $E$ are related by a linear change of variables of the form

$$X = u^2 x + r \text{ and } Y = u^3 y + u^2 sx + t$$  \[2\]

with $u, r, s, t \in K, u \neq 0$.

The transformation \[2\] is called *admissible change of variables*.
Elliptic curve over field $K$ with $\text{char}(K) \neq 2, 3$

The admissible change of variables

$$(x, y) \rightarrow \left( \frac{x - 3a_1^2 - 12a_2}{36}, \frac{y - 3a_1x}{216} - \frac{a_1^3 + 4a_1a_2 - 12a_3}{24} \right)$$

transforms $E$ to the curve $y^2 = x^3 + Ax + B$ where $A, B \in K$.

The discriminant $\Delta = -16(4A^3 + 27B^2)$. 
Elliptic curve over field $K$ with $\text{char}(K) = 2, 3$

- For a field $K$ with $\text{char}(K) = 2$ there is an admissible change of variables that transforms $E$ to

$$y^2 + Cy = x^3 + Ax^2 + B,$$

where $A, B, C \in K$.

- For a field $K$ with $\text{char}(K) = 3$ there is an admissible change of variables that transforms $E$ to

$$y^2 = x^3 + Ax^2 + Bx + C,$$

where $A, B, C \in K$. 

Liljana Babinkostova
Public Key Cryptography: Introduction
For a field $K$ with $\text{char}(K) = 2$ there is an admissible change of variables that transforms $E$ to

$$y^2 + xy = x^3 + Ax^2 + B$$ where $A, B \in K$ when $a_1 \neq 0$. 

For a field $K$ with $\text{char}(K) = 3$ there is an admissible change of variables that transforms $E$ to

$$y^2 = x^3 + Ax^2 + Bx + C$$ where $A, B, C \in K$. 

Elliptic curve over field $K$ with $\text{char}(K) = 2, 3$
For a field $K$ with $\text{char}(K) = 2$ there is an admissible change of variables that transforms $E$ to

- $y^2 + xy = x^3 + Ax^2 + B$ where $A, B \in K$ when $a_1 \neq 0$.
- $y^2 + Cy = x^3 + Ax^2 + B$ where $A, B, C \in K$. 

For a field $K$ with $\text{char}(K) = 3$ there is an admissible change of variables that transforms $E$ to

$y^2 = x^3 + Ax^2 + Bx + C$ where $A, B, C \in K$. 

Elliptic curve over field $K$ with $\text{char}(K) = 2, 3$

For a field $K$ with $\text{char}(K) = 2$ there is a admissible change of variables that transforms $E$ to
- $y^2 + xy = x^3 + Ax^2 + B$ where $A, B \in K$ when $a_1 \neq 0$.
- $y^2 + Cy = x^3 + Ax^2 + B$ where $A, B, C \in K$.

For a field $K$ with $\text{char}(K) = 3$ there is a admissible change of variables that transforms $E$ to
$y^2 = x^3 + Ax^2 + Bx + C$ where $A, B, C \in K$. 
Public key cryptosystems based on groups

The RSA scheme
The El Gamal scheme
Elliptic Curve Cryptography

Alternative representations of elliptic curves over a field $K$

1. Edwards curves: $x^2 + y^2 = 1 + dx^2y^2, \ d \in K \setminus \{0, 1\}$.
2. Hessian curves: $x^3 + y^3 + 1 = 3dxy$
3. Twisted Edwards curves: $ax^2 + y^2 = 1 + dx^2y^2$
4. Twisted Hessian curves: $ax^3 + y^3 + 1 = dxy$
5. Montgomery curves: $by^2 = x^3 + ax^2 + x$
6. Koblitz curves: $y^2 + xy = x^3 + ax^2 + 1, \ a = 0 \text{ or } 1$

D. Bernstein1, T. Lange, Faster addition and doubling on elliptic curves, ECRYPT (2007)
Adding points on an elliptic curve

(a) Addition: \( P + Q = R \)  
(b) Doubling: \( P + P = R \)
Elliptic curve $E(K) : y^2 = x^3 + Ax + B$ where $\text{char}(K) \neq 2, 3$ and
$\Delta = 4A^3 + 27B^2 \neq 0$: 
Group Law Algorithm

Elliptic curve $E(K) : y^2 = x^3 + Ax + B$ where $\text{char}(K) \neq 2, 3$ and $\Delta = 4A^3 + 27B^2 \neq 0$:

- $P + \infty = \infty + P = P$ for all $P \in E(K)$
Elliptic curve $E(K) : y^2 = x^3 + Ax + B$ where $\text{char}(K) \neq 2, 3$ and $\Delta = 4A^3 + 27B^2 \neq 0$:

- $P + \infty = \infty + P = P$ for all $P \in E(K)$

- Let $P(x, y) \in E(K)$. Then $P + (\neg P) = (\neg P) + P = \infty$ for all $P \in E(K)$ where $\neg P = (x, -y)$. 
Elliptic curve $E(K) : y^2 = x^3 + Ax + B$ where $\text{char}(K) \neq 2, 3$ and $\Delta = 4A^3 + 27B^2 \neq 0$:

- $P + \infty = \infty + P = P$ for all $P \in E(K)$

- Let $P(x, y) \in E(K)$. Then $P + (\neg P) = (\neg P) + P = \infty$ for all $P \in E(K)$ where $\neg P = (x, -y)$.

- Let $P(x_1, y_1) \in E(K)$ and $Q(x_2, y_2) \in E(K)$ where $P \neq \pm Q$. Then $P + Q = (x_3, y_3)$ where

  $$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \text{ and } y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1$$
Elliptic curve $E(K): y^2 = x^3 + Ax + B$ where $\text{char}(K) \neq 2, 3$ and $\Delta = 4A^3 + 27B^2 \neq 0$:

- $P + \infty = \infty + P = P$ for all $P \in E(K)$

- Let $P(x, y) \in E(K)$. Then $P + (-P) = (-P) + P = \infty$ for all $P \in E(K)$ where $-P = (x, -y)$.

- Let $P(x_1, y_1) \in E(K)$ and $Q(x_2, y_2) \in E(K)$ where $P \neq \pm Q$. Then $P + Q = (x_3, y_3)$ where
  
  $x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$ and $y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1$

- Let $P(x_1, y_1) \in E(K)$ and $P \neq -P$. Then $2P = (x_3, y_3)$ where
  
  $x_3 = \left(\frac{3x_1^2 + A}{2y_1}\right)^2 - 2x_1$ and $y_3 = \left(\frac{3x_1^2 + A}{2y_1}\right)(x_1 - x_3) - y_1$
Theorem

Let $E$ be an elliptic curve over $\mathbb{F}_q$. Then $E(\mathbb{F}_q)$ is isomorphic to $\mathbb{Z}_n$ for some $n \geq 1$ or $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ where $n_1, n_2 \geq 1$ with $n_1 | n_2$. 
Supersingular curves

Theorem (Hasse, 1922)

Let $E$ be an elliptic curve over the finite field $\mathbb{F}_q$. Then the order of $\#E(\mathbb{F}_q) = q + 1 - t$ where $|t| \leq 2\sqrt{q}$.
Supersingular curves

Theorem (Hasse, 1922)

Let $E$ be an elliptic curve over the finite field $\mathbb{F}_q$. Then the order of $\#E(\mathbb{F}_q) = q + 1 - t$ where $|t| \leq 2\sqrt{q}$.

Definition

An elliptic curve $E$ defined over a field $\mathbb{F}_q$ of characteristic $p$ is called a **supersingular** if $p | t$. If $p$ does not divide $t$, then $E$ is called (ordinary) non-supersingular.
Supersingular curves

Theorem (Hasse, 1922)

Let $E$ be an elliptic curve over the finite field $\mathbb{F}_q$. Then the order of $\#E(\mathbb{F}_q) = q + 1 - t$ where $|t| \leq 2\sqrt{q}$.

Definition

An elliptic curve $E$ defined over a field $\mathbb{F}_q$ of characteristic $p$ is called a **supersingular** if $p | t$. If $p$ does not divide $t$, then $E$ is called (ordinary) non-supersingular.

The ECDLP in a supersingular elliptic curve over $\mathbb{F}_q$ can be reduced to the DLP in $\mathbb{F}_q^*$. (MOV attack, 1993)
Anomalous curves

An elliptic curve $E$ over $\mathbb{F}_q$ is called an anomalous if $\#E(\mathbb{F}_q) = q$.

The ECDLP in an anomalous elliptic curve over $\mathbb{F}_q$ can be solved in polynomial time. (Smart, 1999)