Asymmetric Key Cryptography

Elliptic Curve Cryptography (ECC) over
Binary Galois Extension Field $\mathbb{F}_{2^k}$

THE UNIVERSITY OF UTAH

Priyank Kalla
Professor
Electrical & Computer Engineering

ECC in $\mathbb{F}_{2^k}$

- Over $\mathbb{F}_{2^k} \equiv \mathbb{F}_2[x] \pmod{P(x)}, P(x) =$ primitive polynomial of degree k
- Cannot use the same curve as in $\mathbb{R}$ i.e. $E_{\mathbb{R}} : y^2 = x^3 + ax + b;$
- Curve equation used in $\mathbb{F}_{2^k}$: $E: \; y^2 + xy = x^3 + ax^2 + b, a, b \in \mathbb{F}_{2^k}, b \neq 0$
  - Such a curve is called "nonsupersingular", and the discriminant $\Delta = b \neq 0$
    - The rules for point addition and doubling in $\mathbb{F}_{2^k}$ are different than those for $\mathbb{R}$ or $\mathbb{F}_p$, because $\mathbb{F}_{2^k}$ has characteristic 2
    - P+Q = R:

$$\lambda = (y_2 + y_1) / (x_2 + x_1)$$
$$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a \qquad y_3 = \lambda\,(x_1 + x_3) + x_3 + y_1$$

    - P+P = 2P = R:

$$\lambda = x_1 + y_1 / x_1$$
$$x_3 = \lambda^2 + \lambda + a \qquad y_3 = {x_1}^2 + (\lambda + 1)\,x_3$$

Deriving Point Doubling Computation in $\mathbb{F}_{2^k}$

- Let $E: \ y^2 + xy = x^3 + ax^2 + b, a, b \in \mathbb{F}_{2^k}, b \neq 0$, and $P(x_1, y_1)$ be a point

- Write $E: \ y^2 + xy + x^3 + ax^2 + b = 0$; as $-1 = +1 \pmod 2$

- Implicit differentiation of E (keep in mind, coeff. Reduced mod (2)):

$$2y\frac{dy}{dx} + (x\frac{dy}{dx} + y \cdot 1) + 3x^2 + 2ax = 0$$

$$x\frac{dy}{dx} + y + x^2 = 0$$

- $$\frac{dy}{dx} = \frac{y + x^2}{x} = x + y/x$$

- Therefore, slope at $P(x_1, y_1) = \lambda = x_1 + y_1/x_1$

Inverse points in $\mathbb{F}_{2^k}$

- Another issue to resolve in $\mathbb{F}_{2^k}$ is inverse points
- Over $\mathbb{R}, P(x_1, y_1)$, then $-P = (x_1, -y_1)$
- But over $\mathbb{F}_{2^k}, -1 = +1$, so $-P = (x_1, -y_1) = (x_1, y_1)$
  - So P = -P for all points P? This gives -P + P = 2P, but we want P - P = O, the zero point!
- For out curve $E: \ y^2 + xy = x^3 + ax^2 + b, a, b \in \mathbb{F}_{2^k}, b \neq 0$
- Inverse point $= P(x_1, y_1)$, then $-P = (x_1, x_1 + y_1)$
- Proof: In E, y appears in LHS only. Replace y with x+y:
- $$\begin{aligned} E(x, x+y):\ & (x+y)^2 + x(x+y) = x^3 + ax^2 + b \\ & x^2 + y^2 + 2xy + x^2 + xy = x^3 + ax^2 + b \\ E(x, y):\ & y^2 + xy = x^3 + ax^2 + b \end{aligned}$$

ECC Curve Example

- Let $\mathbb{F}_8 = \mathbb{F}_2[x] \pmod{P(x) = x^3 + x + 1}$
- Let $P(\alpha) = 0 : \alpha^3 + \alpha + 1 = 0$, or $\alpha^3 = \alpha + 1$
- $\mathbb{F}_8 = \{0, 1 = \alpha^7, \alpha, \alpha^2, \alpha^3 = \alpha + 1, \alpha^4 = \alpha^2 + \alpha, \alpha^5 = \alpha^2 + \alpha + 1, \alpha^6 = \alpha^2 + 1\}$
- Let the ECC curve be $E : y^2 + xy = x^3 + \alpha^3 x^2 + 1$
- Find all the valid points on the curve E
    - For all $x \in \mathbb{F}_8$, compute corresponding values of y
    - E.g. x=0, $y^2 = 1, y = 1, 1$ (two equal roots): two points (0,1),(0,1)
    - $x = \alpha : y^2 + \alpha y = \alpha^3 + \alpha^5 + 1 = \alpha^2 + 1$
    - $x = \alpha : y^2 + \alpha y + \alpha^2 + 1 = 0$. Quadratic equation of the form: $ay^2 + by + c$
    - Find roots using factorization (subst() and factorize() functions in Singular)

ECC Points Generation

- $E : y^2 + xy = x^3 + \alpha^3 x^2 + 1$, with $\alpha^3 + \alpha + 1 = 0$

- Points over the curve:

- $$\begin{array}{rl} (0,1) & (0,1) \\ (\alpha, \alpha^2) & (\alpha, \alpha^2 + \alpha = \alpha^4) \\ (\alpha^2, 1) & (\alpha^2, \alpha^2 + 1 = \alpha^6) \\ (\alpha^3, \alpha^2) & (\alpha^3, \alpha^2 + \alpha + 1 = \alpha^5) \\ (\alpha^4, 0) & (\alpha^4, \alpha^2 + \alpha = \alpha^4) \\ (\alpha^5, 1) & (\alpha^5, \alpha^2 + \alpha = \alpha^4) \\ (\alpha^6, \alpha) & (\alpha^6, \alpha^2 + \alpha + 1 = \alpha^5) \end{array}$$

- But we cannot ignore the point at infinity, as that's the identity element of the group. So, include the point O.

- This gives us 13 distinct points above, 1 duplicate point (0,1), and O: giving us 14 distinct points: $E = \{O, (0,1), (\alpha, \alpha^2), \ldots, (\alpha^6, \alpha^5)\}$

ECC Points Generation

- $E: y^2 + xy = x^3 + \alpha^3 x^2 + 1$, with $\alpha^3 + \alpha + 1 = 0$

- We know now that $E = \{O, (0,1), (\alpha, \alpha^2), \ldots, (\alpha^6, \alpha^5)\}$ and that $\langle E, + \rangle$ forms an additive group.

- Does there exist a point in E that generates the group? Yes: (α, α^2) generates the whole group. But (0,1) does not.

- $$\begin{array}{lll} P = (\alpha, \alpha^2) & 2P = (\alpha^3, \alpha^5) & 3P = 2P + P = (\alpha^2, 1) \\ 4P = (\alpha^5, 1) & 5P = (\alpha^4, \alpha^4) & 6P = (\alpha^6, \alpha^5) \\ 7P = (0, 1) & 8P = (\alpha^6, \alpha) & 9P = (\alpha^4, 0) \\ 10P = (\alpha^5, \alpha^4) & 11P = (\alpha^2, \alpha^6) & 12P = (\alpha^3, \alpha^2) \\ 13P = (\alpha, \alpha^4) & 14P = O & 15P = O + P = P \end{array}$$

- If P = (0,1), 2P = O: when x=0, slope = infy, so 2P = O

$$\lambda = x_1 + y_1 / x_1$$

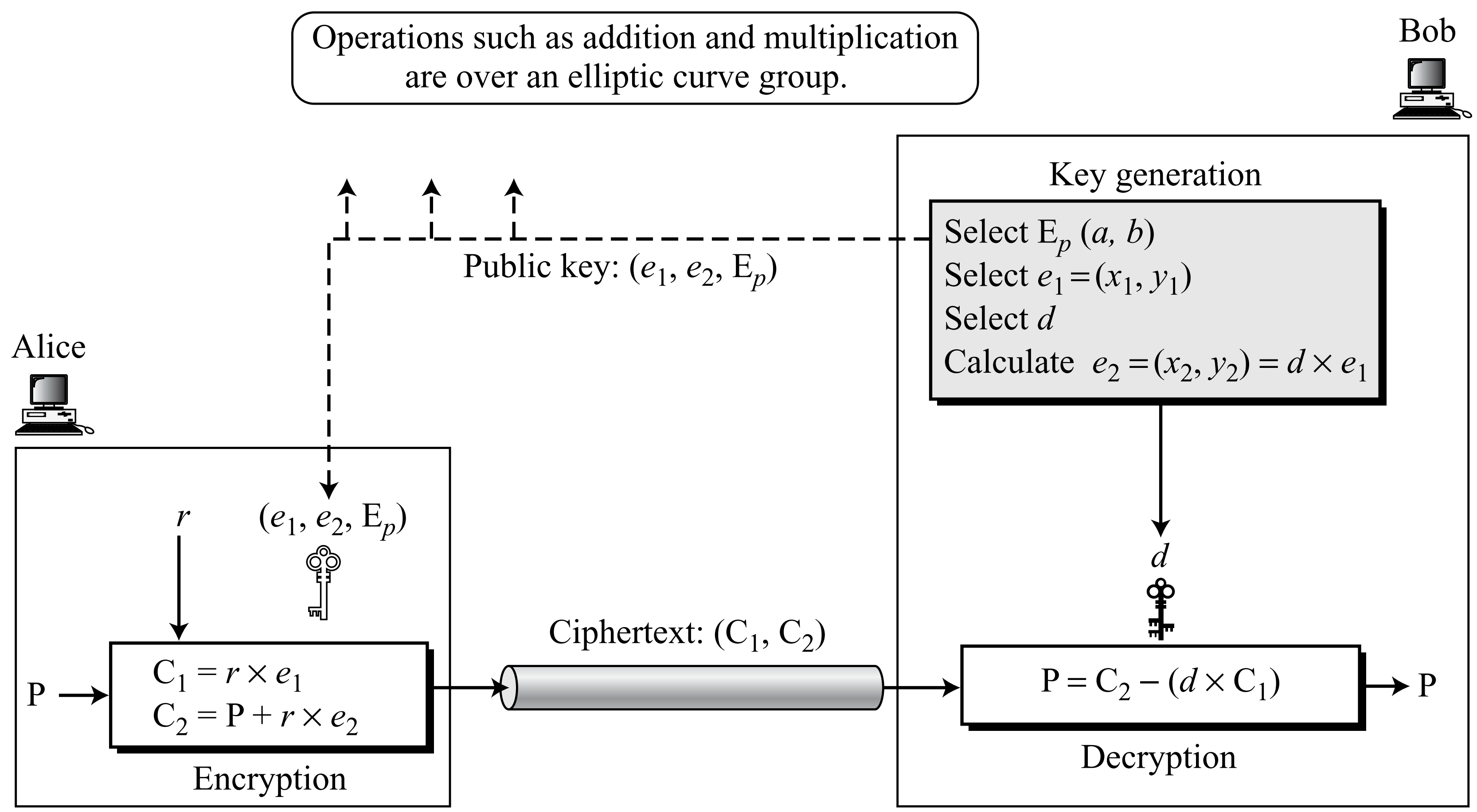
$$x_3 = \lambda^2 + \lambda + a \qquad y_3 = x_1{}^2 + (\lambda + 1)\, x_3$$

- R(x3,y3) = 2P(x1,y1)

How many points over E?

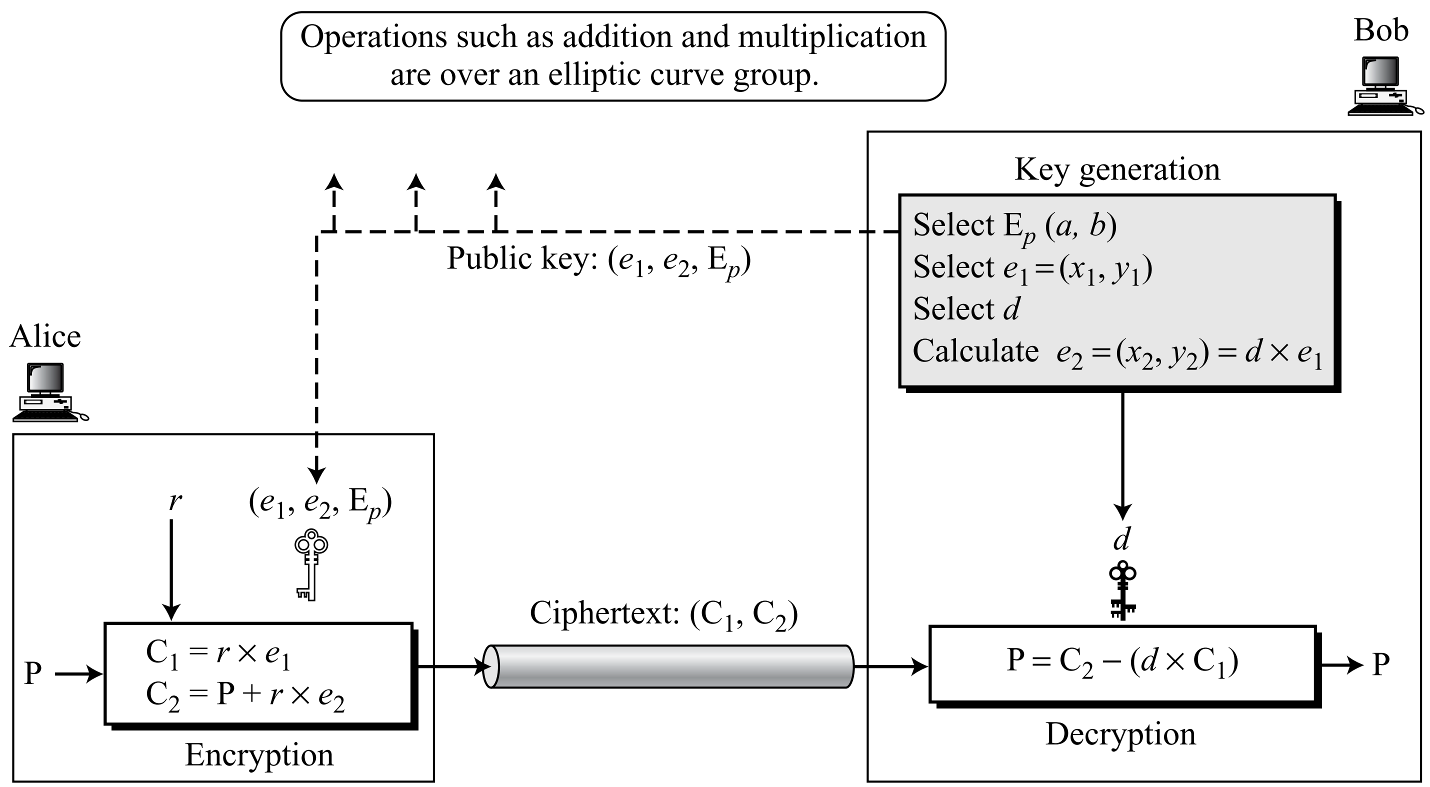
- The number of points on an elliptic curve over $\mathbb{F}_q$is given by a bound:
- $q + 1 - 2\sqrt{q} \leq \#E(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q}$
- This is called Hesse-Weil formula

El Gamal over ECC in $\mathbb{F}_{2^k}$



- Choose curve $E(\alpha^3, 1)$: and let $e_1 = (\alpha^2, 1)$, and $d = 2$
- Calculate $e_2 = 2e_1 : \lambda = \alpha + 1, x_3 = \alpha^6, y_3 = \alpha^5$
- $e_2 = (\alpha^6, \alpha^5)$

El Gamal over ECC in $\mathbb{F}_{2^k}$: Encipherment



- Choose $E(\alpha^3,1)$: $e_1 = (0,1), d = 2$. Compute $e_2 = 2e_1 = O$
- Alice chooses $r = 3$: $C_1 = 3e_1 = 2e_1 + e_1 = O + e_1 = e_1$
- $C_2 = P + 3e_2 = P + 3O = P + O = P$ (encrypted = plaintext)
- Decryption: $C_2 - (dC_1) = P - 2e_1 = P - O = P$ (we get plaintext back)

Projective Coordinates and Hardware Design

- For point addition and doubling operation, need to compute slope λ, which requires division
- Division = multiplicative inverse = extended Euclidean algorithm — which is non-trivial to implement in a modulo arithmetic ALU
- To avoid computation of inverses, many hardware crypto systems use Projective Coordinates:
- $E: \ y^2 + xy = x^3 + ax^2 + b, a, b \in \mathbb{F}_{2^k}, b \neq 0$
- Put $x = X/Z, y = Y/Z$, $E: \ Y^2/Z^2 + (X/Z)(Y/Z) = X^3/Z^3 + aX^2/Z^2 + b$
- Homogenize E, i.e. multiply by Z^3, we get $E: \ Y^2Z + XYZ = X^3 + aX^2Z + bZ^3$
- Affine Point $(x_1, y_1) \equiv (X_1 : Y_1 : Z_1)$ becomes the projective point, if $Z_1 \neq 0$, and inverse point $(x_1, x_1 + y_1) \equiv (X_1 : X_1 + Y_1 : Z_1)$.
- When $Z_1 = 0$, then point at infinity is represented as (0:1:0), or (1:m:0)

Projective Coordinates and Hardware Design

- $E: \quad Y^2Z + XYZ = X^3 + aX^2Z + bZ^3$
- Affine Point $(x_1, y_1) \equiv (X_1 : Y_1 : Z_1)$ becomes the projective point, if $Z_1 \neq 0$, and inverse point $(x_1, x_1 + y_1) \equiv (X_1 : X_1 + Y_1 : Z_1)$.
- When $Z_1 = 0$, then point at infinity is represented as (0:1:0), or (1:m:0)
- (rX : rY : rZ) = r(X : Y : Z) = (X : Y : Z) = Equivalence class of points
- Two parallel lines of slope *m* intersect at (1 : m : 0), two vertical lines at (0:1:0). Point (0:0:0) is disallowed.
- Using Projective coordinates, point addition and doubling don't require inverses
- Given affine point (x_i, y_i), how to select z_i for (x_i, y_i, z_i)?
- Any $z_i \neq 0$ will do, so just select $z_i = 1$

Point addition in projective coordinates

$$Y^2Z + XYZ = X^3 + a_2X^2Z + a_6Z^3.$$

Addition

Let $P = (X_1 : Y_1 : Z_1)$, $Q = (X_2 : Y_2 : Z_2)$ such that $P \neq \pm Q$ then $P \oplus Q = (X_3 : Y_3 : Z_3)$ is given by

$$A = Y_1Z_2 + Z_1Y_2, \quad B = X_1Z_2 + Z_1X_2, \quad C = B^2,$$
$$D = Z_1Z_2, \quad E = (A^2 + AB + a_2C)D + BC,$$
$$X_3 = BE, \quad Y_3 = C(AX_1 + Y_1B)Z_2 + (A + B)E, \quad Z_3 = B^3D.$$

Doubling

If $P = (X_1 : Y_1 : Z_1)$ then $[2]P = (X_3 : Y_3 : Z_3)$ is given by

$$A = X_1^2, \quad B = A + Y_1Z_1, \quad C = X_1Z_1,$$
$$D = C^2, \quad E = (B^2 + BC + a_2D),$$
$$X_3 = CE, \quad Y_3 = (B + C)E + A^2C, \quad Z_3 = CD.$$

Errors/Typos in this derivation From the "Handbook of ECC"

Correct formula on the next slides

No inverses needed, only GF addition, multiplication and squaring

Point addition: 16M + 2S;

Point Doubling: 8M + 2S

Point Addition in Projective Coordinates

$$E: \quad Y^2Z + XYZ = X^3 + aX^2Z + bZ^3$$

$$\begin{aligned}
A &= x_2 z_1 + x_1 \\
B &= y_2 z_1 + y_1 \\
C &= A + B \\
D &= A^2(A + a z_1) + z_1 BC
\end{aligned}$$

$$\begin{aligned}
x_3 &= AD \\
y_3 &= CD + A^2(B x_1 + A y_1) \\
z_3 &= A^3 z_1
\end{aligned}$$

- In our example, $a = \alpha^3, b = 1, \mathbb{F}_8$
- Where $P(\alpha) = \alpha^3 + \alpha + 1$

- $(x_3, y_3, z_3) = (x_1, y_1, z_1) + (x_2, y_2, z_2)$;
- When affine (x_i, y_i) is given, choose $z_i = 1$ (simple!!)
- $P = (\alpha, \alpha^2), Q = 2P = (\alpha^3, \alpha^5), R = P + Q = (\alpha^2, 1)$
- $13P = (\alpha, \alpha^4), P = (\alpha, \alpha^2), R = 13P + P = 14P = (0 : \alpha + 1 : 0) = O$
- See the Singular file on Canvas: “ecc-projective.sing”;

Point Doubling in Projective Coordinates

$$E: \; Y^2Z + XYZ = X^3 + aX^2Z + bZ^3$$

$$\begin{aligned} A &= x_1 z_1 \\ B &= b z_1^4 + x_1^4 \end{aligned}$$

$$\begin{aligned} x_3 &= AB \\ y_3 &= x_1^4 A + B(x_1^2 + y_1 z_1 + A) \\ z_3 &= A^3 \end{aligned}$$

- $(x_3, y_3, z_3) = 2(x_1, y_1, z_1)$;
- P = (0,1), 2P = O: $x_3 = 0, y_3 = 1, z_3 = 0$

Final Remark on ECC Security

- Choose e_1 preferably as a generator of the group $\langle E, + \rangle$
- $e_2 = d \times e_1$
- Both e_1, e_2 are public. Can Eve find d?
- This is the elliptic curve discrete logarithm problem (ECDLP)
- Known methods for ECDLP is based on the Pollard Rho algorithm, and the “baby-step giant-step” algorithm
- Overall complexity is $O(\sqrt{r})$, where r is the number of elements in the group = order of the group = # of points on the curve
- $r \leq q + 1 + 2\sqrt{q}, q = 2^n, n =$ # of bits: If n = 163 (NIST spec)
- But ECC over $\mathbb{F}_{2^n}$ is becoming vulnerable to side-channel attacks, so shielding is an important issue