Pairing の計算法とその実装

筑波大学　岡本栄司

謝辞　松田誠一、金山直樹、Jean-Luc Beuchat
白勢政明、高木　剛、土井　洋、側高幸治

発表内容

- Pairingとは
- Pairing計算法
  - 曲線について→2.
- ソフトウェア実装
- ハードウェア実装
- 応用→3., 4.

Pairing

$$e : G_1 \times G_2 \rightarrow G_3$$

$$G_1, G_2, G_3 : \text{群}$$

- 双線形性

$$e(P_1 + P_2, Q) = e(P_1, Q) \cdot e(P_2, Q)$$

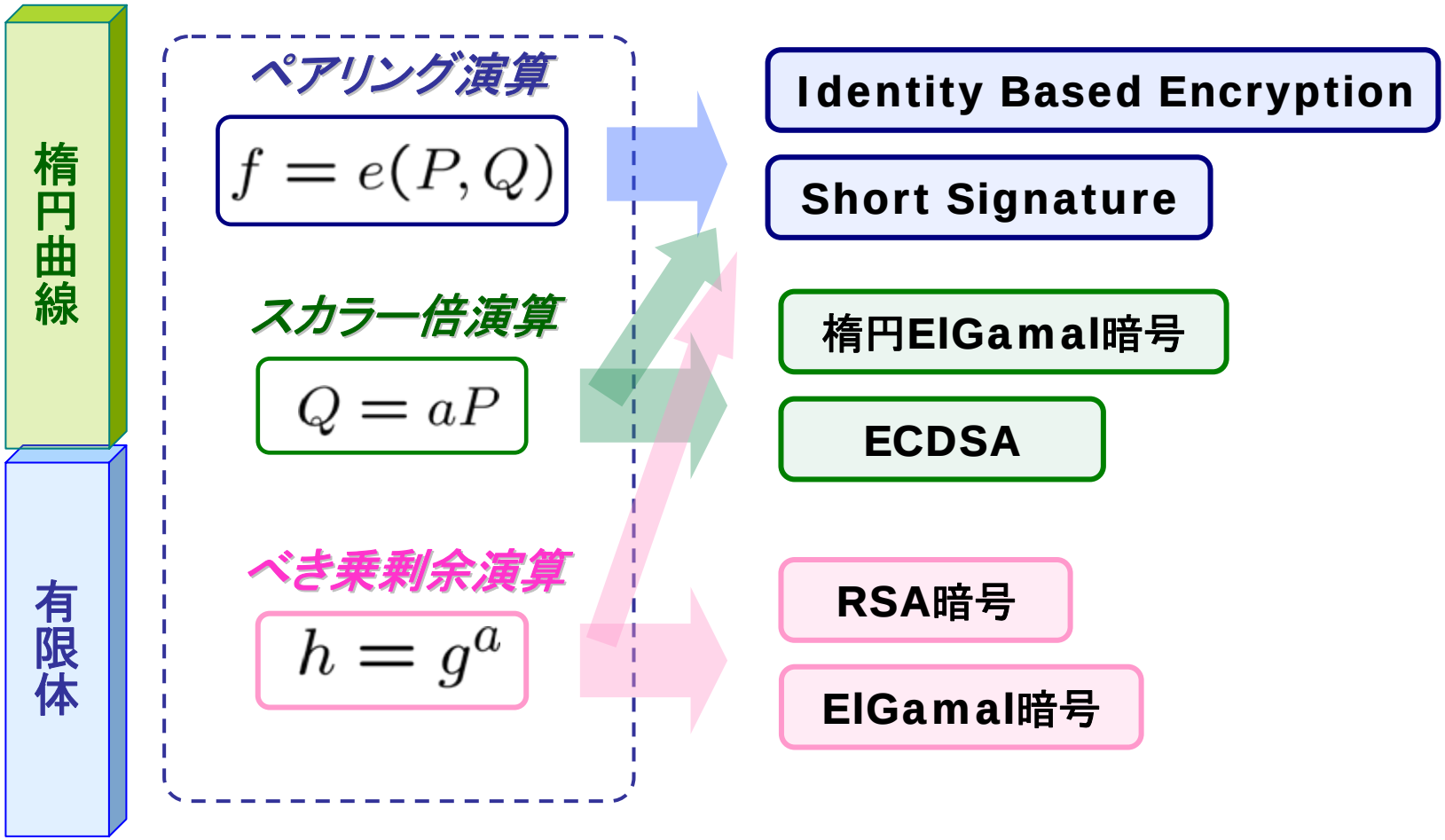
$$e(P, Q_1 + Q_2) = e(P, Q_1) \cdot e(P, Q_2)$$

- 非縮退性

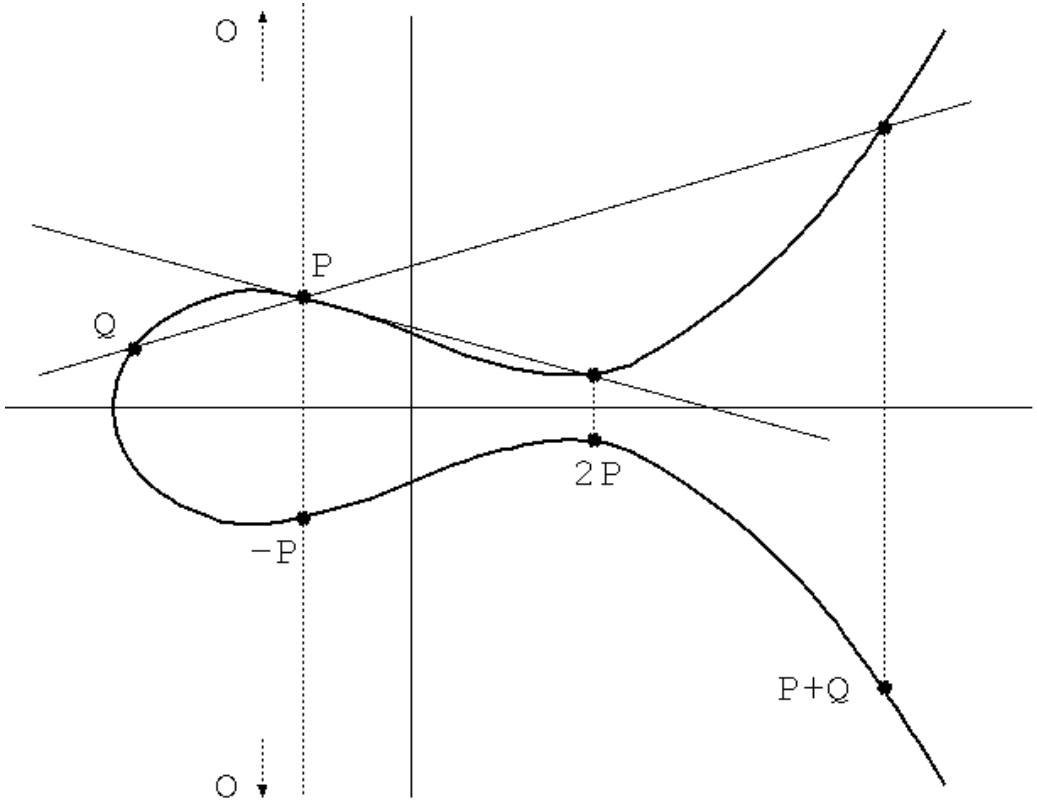
$$\forall P, e(P, Q) = 1 \Rightarrow Q = \mathrm{O}$$

$$\forall Q, e(P, Q) = 1 \Rightarrow P = \mathrm{O}$$

暗号におけるPairingの位置づけ



楕円曲線



$$P=(x_1,y_1),\ Q=(x_2,y_2)$$

$$P+Q=(x_3,y_3)$$

$$x_3=\lambda^2-x_1-x_2$$

$$y_3=\lambda(x_1-x_3)-y_1$$

$$\lambda=\begin{cases}\frac{y_2-y_1}{x_2-x_1} & if\ \ P\neq\pm Q\\ \frac{3{x_1}^2+a}{2y_1} & if\ \ P=Q\end{cases}$$

$$P+(-P)=O,\ P+O=P$$

$$aP=\underbrace{P+\cdots+P}_{a}$$

$$E(F_q)=\{(x,y)\in {F_q}^2 : y^2=x^3+ax+b\}\cup\{O\}$$

Pairing (Tate)

- 楕円曲線
  - Ordinary curve $E/F_q : y^2 = x^3 + ax + b, q = p^m$
  - 素数 $:r$ $\sharp E(F_q) = hr = q + 1 - t$ を満たす
  - 埋め込み次数 $k : r | q^k - 1$ を満足する最小の整数
- Tate Pairing

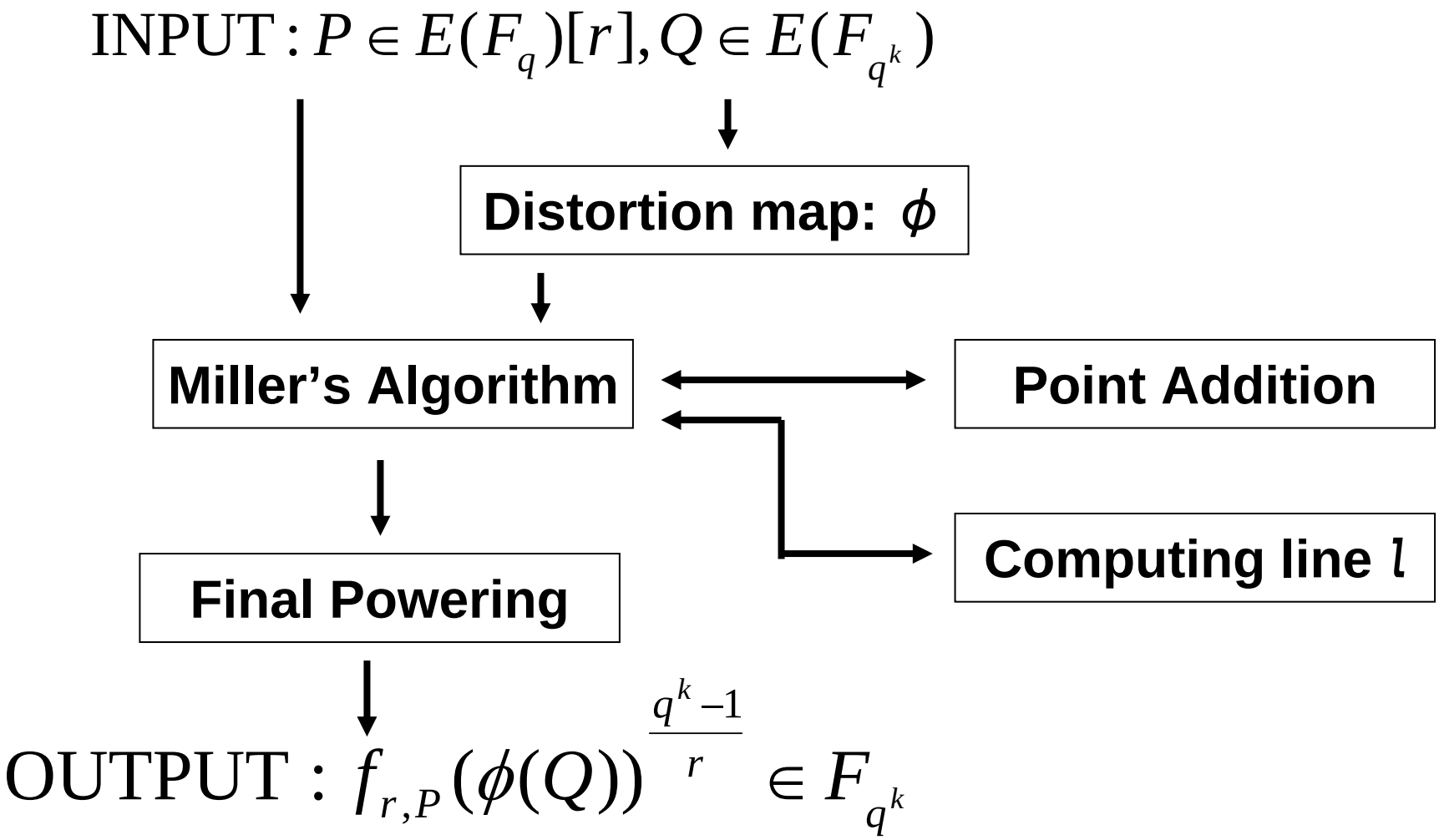
$$\langle \cdot, \cdot \rangle_r : \begin{cases} E(\mathbb{F}_q)[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) & \to \mathbb{F}^*_{q^k}/(\mathbb{F}^*_{q^k})^r \\ (P, Q) & \mapsto \langle P, Q \rangle_r = f_{r,P}(Q) \end{cases}$$

Reduced

Tate Pairing $e(P, Q) = \langle P, Q \rangle_r^{(q^k-1)/r}$

双線形性、非縮退性

Tate Pairing 計算のフロー



Divisor

$$D = \sum_i a_i (A_i), \quad A_i \in E$$

$$\deg(D) = \sum_i a_i \in Z$$

$$sum(D) = \sum_i a_i A_i \in E$$

$$\text{Principal Divisor}: \ div(f) = \sum_{A \in E} ord_A(f)(A) \ \in Div(E)$$

$$ord_A(f) = \quad \text{Multiplicity of } \ f \ \text{ at } A \text{ over } E$$

補題　$Div_0(E)$において、$sum(D) = \mathrm{O} \Leftrightarrow div(\exists f) = D$

Principal Divisorの例

$$div(l_{R,S}) = (R) + (S) + (-(R+S)) - 3(O)$$

$$div(v_P) = (P) + (-P) - 2(O)$$

$l_{R,S}$はRとS[と$-(R+S)$とO]を通る直線

v_PはP[と$-P$とO]を通る垂線

$f_{r,P}$の定義

$$div(f_j) = j(P) - (jP) - (j-1)(\mathrm{O})$$

$$\deg(j(P) - (jP) - (j-1)(\mathrm{O})) = 0$$

$$sum(j(P) - (jP) - (j-1)(\mathrm{O})) = \mathrm{O}$$

$$f_{r,P} \overset{def}{=} f_r$$

Pairingの計算法

- 再帰的公式

$$f_{i+j} = f_i f_j \frac{l_{iP,jP}}{v_{(i+j)P}}$$

$\because$)

$$div(f_{i+j}) - div(f_i) - div(f_j)$$

$$= \{(i+j)(P) - ((i+j)P) - (i+j-1)(O)\} - \{i(P) - (iP) - (i-1)(O)\} - \{j(P) - (jP) - (j-1)(O)\}$$

$$= (iP) + (jP) - ((i+j)P) - (O)$$

$$= \{(iP) + (jP) + (-(i+j)P) - 3(O)\} - \{((i+j)P) + (-(i+j)P) - 2(O)\}$$

$$= div(l_{iP,jP}) - div(v_{(i+j)P})$$

$$= div\left(\frac{l_{iP,jP}}{v_{(i+j)P}}\right)$$

Millerのアルゴリズム

$e(P,Q)$の計算

$r=(r_{t-1},\cdots,r_0)_2,\ f=1,V=P$

for $i=t-1$ to 0 do

$$f=f^2\frac{l_{V,V}(Q)}{v_{2V}(Q)} \text{ and } V=2V$$

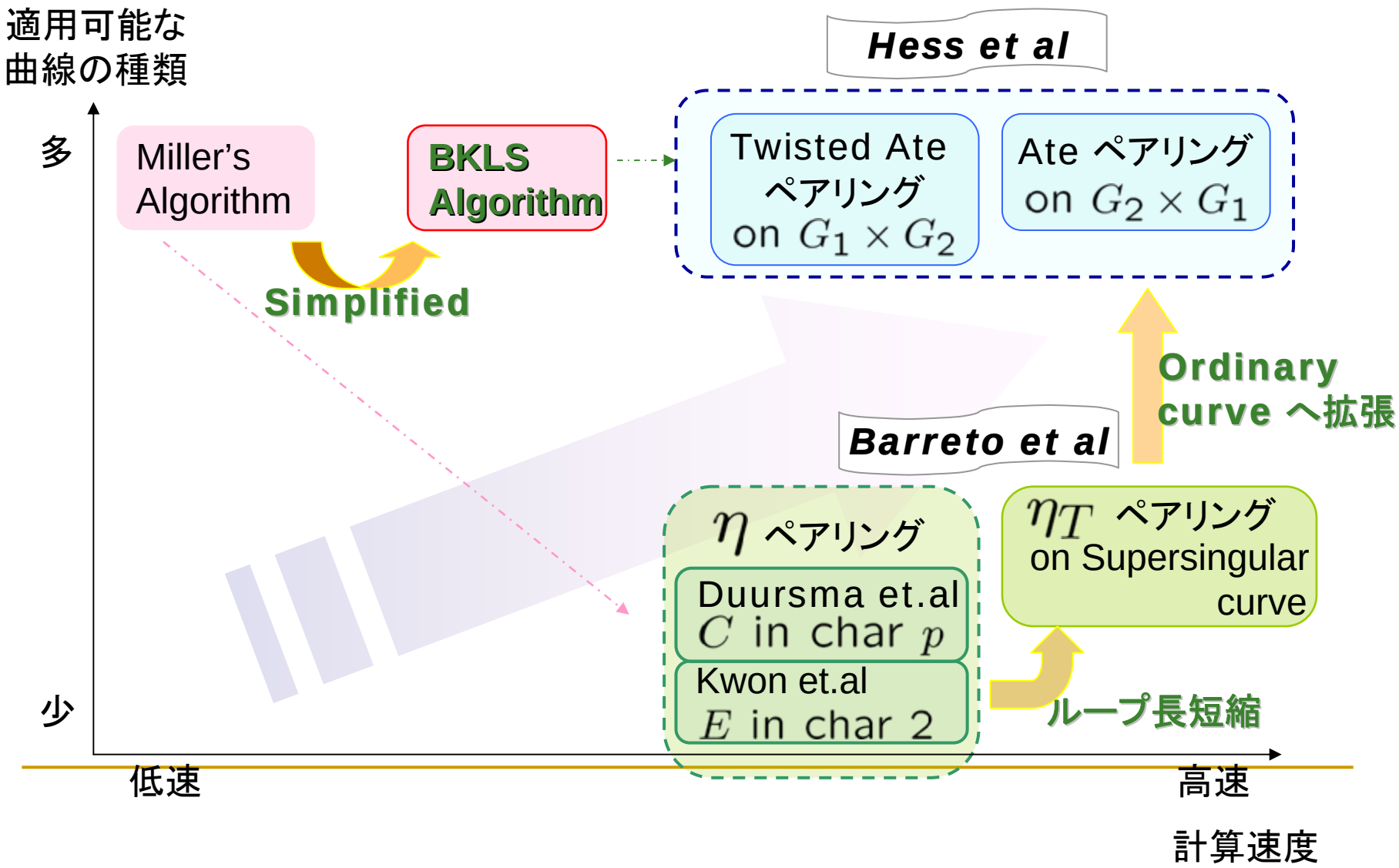
if $r_i=1$ then $f=f\frac{l_{V,P}(Q)}{v_{V+P}(Q)}$ and $V=V+P$

end for

return $f^{\frac{q^k-1}{r}}$

アルゴリズムの研究動向

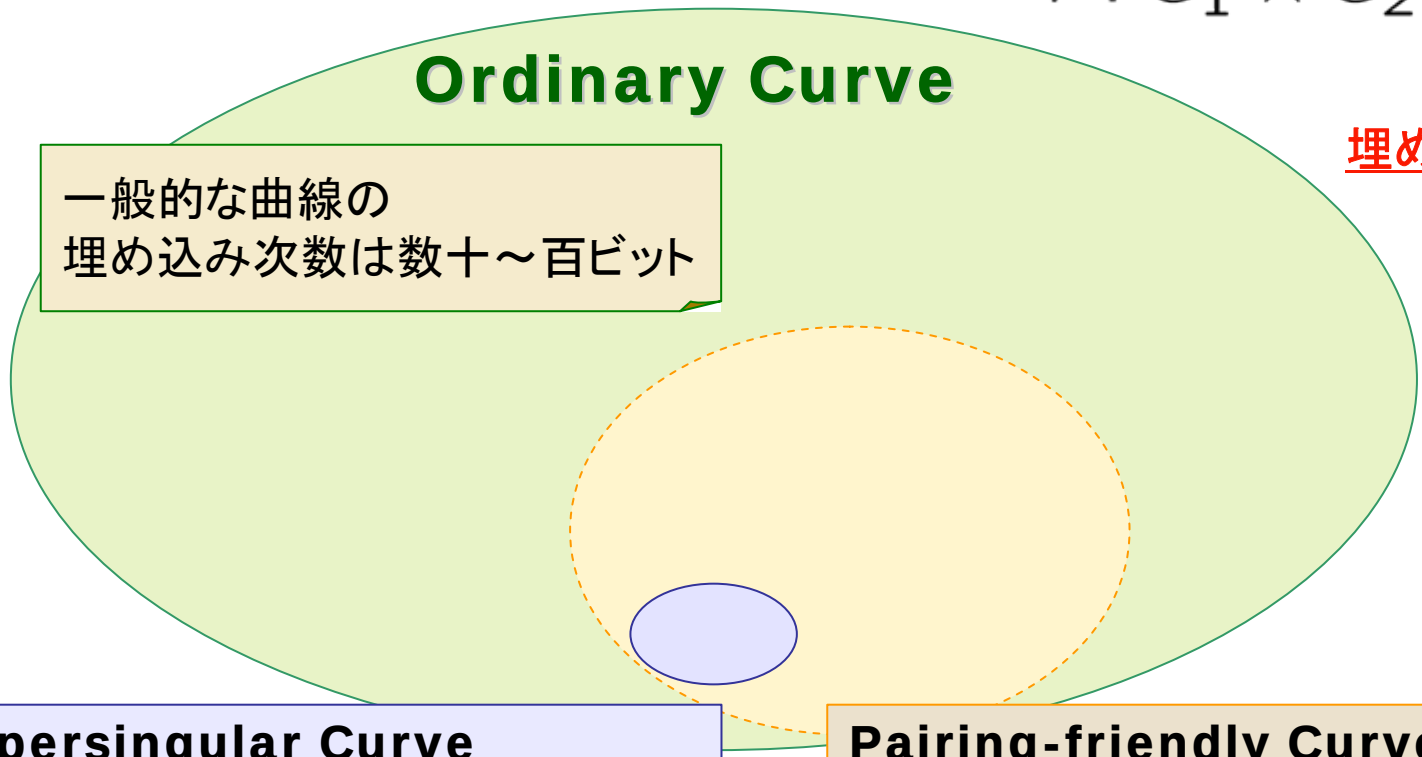
$G_1 : E(F_q)[r]$
$G_2 : E(F_{q^k})[r]$



Pairing-friendly Curve

$$\tau : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{F}_{q^k}^*$$

埋め込み次数



Duursma and Lee (2003)
Eta ペアリング(2004)

Twisted Ate ペアリング(2006)
Ate ペアリング(2006)

Pairing-friendly Curve

- Supersingular Curve

$E[p] = \{R \in E(\overline{F_p}) \mid pR = \mathrm{O}\} = \{\mathrm{O}\}$

位数がわかっているという特徴がある。

$q = p$なら$y^2 = x^3 + 1 (p \equiv 2 \bmod 3), y^2 = x^3 + x (p \equiv 3 \bmod 4)$で、$\#E(F_q) = p + 1$

$q = 2^m$なら$y^2 + y = x^3 + x$や$y^2 + y = x^3 + x + 1$で、$\#E(F_q) = 2^m + 1 \pm 2^{\frac{m+1}{2}}$

$q = 3^m$なら$y^2 = x^3 - x \pm 1$で、$\#E(F_q) = 3^m + 1 \pm 3^{\frac{m+1}{2}}$

- MNT Curve→2.
- Ordinary Curve

・Twisted Ate、Ate[HSV06]→Optimization [MKHO07]

留意点

- 点P,Qの求め方

$$(P,Q)\in E(F_q)[r]\times E(F_{q^k})\Big/ rE(F_q)$$

$$P=\frac{\#E(F_r)}{r}R,\ \forall R\in E(F_r)$$

$Q\in E(F_{q^k})-E(F_q)$でないと最終冪で$e(P,Q)=1$となってしまう。

- Distortion Map利用 ← Supersingular

$$\phi: E(F_q)\to E(F_{q^k})-E(F_q)$$

例　$\phi(x,y)=(-x,iy)$　$q=p$のとき、$i^2+1=0$

$\phi(x,y)=(\rho-x,\sigma y)$　$q=3^m$のとき、$\sigma^2+1=0,\rho^3-\rho-1=0$

ただし$y^2=x^3-x+1$

簡単化Millerアルゴリズム($q=p$のとき)

$e(P,Q)$の計算

$r=(r_{t-1},\cdots,r_0)_2,\ f=1, V=P$

for $i=t-1$ to 0 do

$f=f^2\cdot l_{V,V}(\varphi(Q))$ and $V=2V$

if $r_i=1$ then $f=f\cdot l_{V,P}(\varphi(Q))$ and $V=V+P$

end for

return $f^{\frac{q^k-1}{r}}$

標数$p=3$のときの高速化とη_TPairing

- 3倍算が容易

  $3(x,y)=(x^9-1,-y^9)$

- rの3進表現

  $r=(r_{t-1},\cdots,r_0)_3,\ r_i=0,\pm1$とすると、$-P$の計算の容易性を使える。

- 2次曲線利用

  再帰式 $f_{3j}=f_j^{\,3}\dfrac{l_{jP,2jP}}{v_{3jP}}\cdot\dfrac{l_{jP,jP}}{v_{2jP}}$において

  直線4式の代わりに$h_V=\beta^3y-(\alpha^3-x+b)^2$が使える。

- η_TPairing

  rより小さいあるTに対して、 $\eta_T(P,Q)=f_{T,P}(\phi(\mathrm{Q}))$は双線形性を持ち、

  $(\eta_T(P,Q)^M)^{3T^2}=e(P,\phi(Q))^L$

η_T Pairingアルゴリズム

$\eta_T(P,Q)$の計算

$P=(x_p,y_p), Q=(x_q,y_q)$

$y_p \leftarrow -y_P$

$f \leftarrow \sigma y_q + y_p(\rho - x_p - x_q - 1)$

for $j \leftarrow 0$ to $(m-1)/2$ do

$u \leftarrow x_p + x_q + b$

$g \leftarrow \sigma y_p y_q - u^2 - \rho u - \rho^2$

$f \leftarrow fg$

$x_p \leftarrow x_p^{1/3}, y_p \leftarrow y_p^{1/3}$

$x_q \leftarrow x_q^{3}, y_q \leftarrow y_q^{3}$

end for

return f

改良 η_T Pairingアルゴリズム[STO06]

$\eta_T(P,Q)^{3^{(m+1)/2}}$ の計算

$y_p \leftarrow -y_p$

$u \leftarrow x_p + x_q + b$

$d \leftarrow b$

$f \leftarrow \sigma y_q - u y_p + \rho y_p$

for $j \leftarrow 0$ to $(m-1)/2$ do

$u \leftarrow x_p + x_q + d$

$g \leftarrow \sigma y_p y_q - u^2 - \rho u - \rho^2$

$f \leftarrow (fg)^3$

$y_p \leftarrow -y_p$

$x_q \leftarrow x_q^{\,9}, y_q \leftarrow y_q^{\,9}$

$d \leftarrow d - b \bmod 3$

end for

return f

η_T Pairingの実装例：ソフトウェア

環境

- OS：Red Hat Linux 9
- CPU：Pem4 3.4GHzz
- メモリ：1GB

処理時間

- $\eta_T : E(F_{3^{97}}) \times E(F_{3^{6\cdot 97}}) \to F_{3^{6\cdot 97}}$　4.32msec

同環境で

- 1024ビットRSA型べき乗剰余演算　8.69msec

η_T Pairingの実装例：ハードウェア

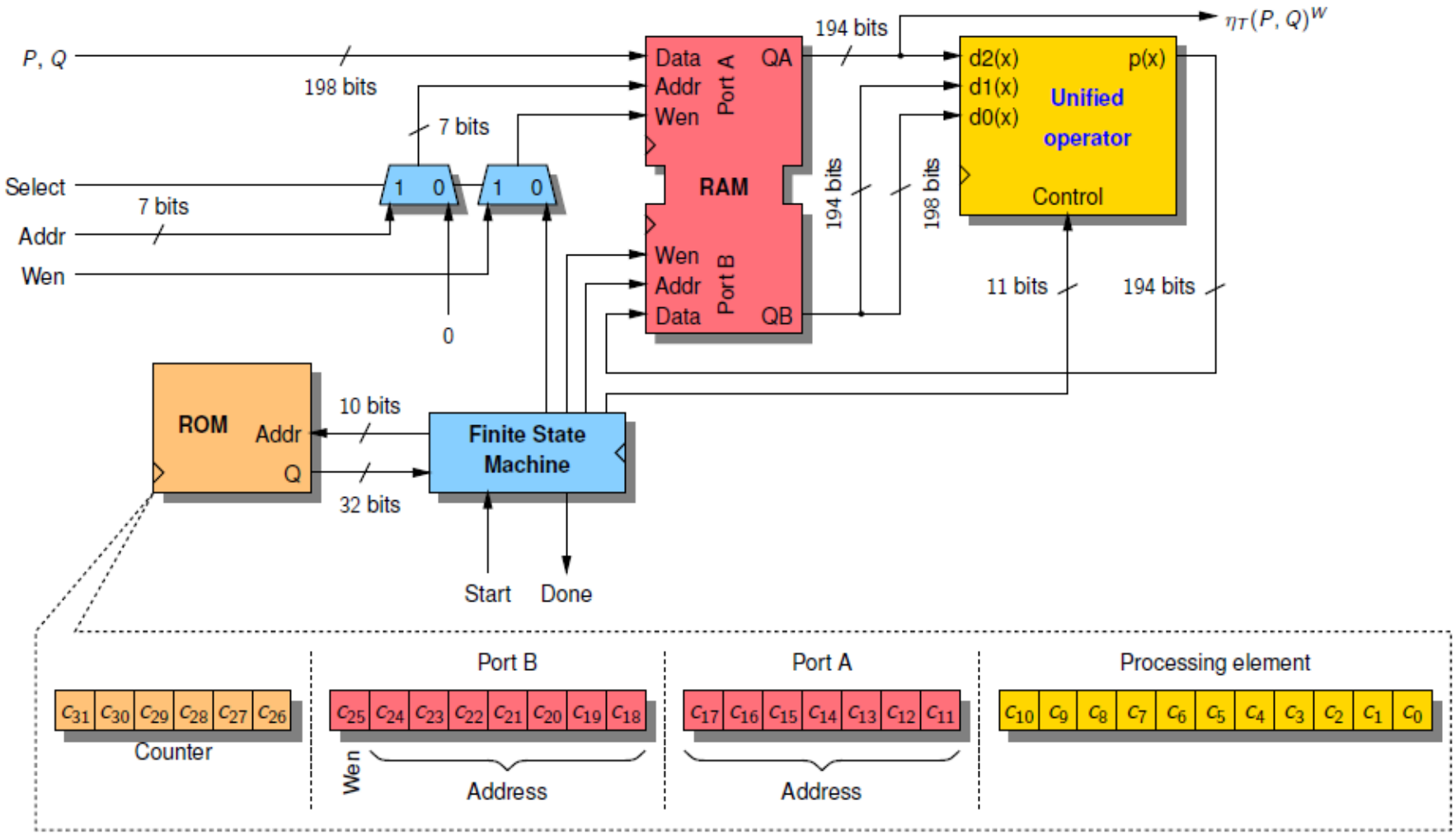
- FPGA　マルチプロセッサタイプ

・Cyclone Ⅱ EP2C35
・9プロセッサ
・18000スライス
・クロック周波数　149MHz
・計算時間　27 μ sec

- FPGA　シングルプロセッサタイプ

・Vertex-4 LX15
・1プロセッサ
・1857スライス
・クロック周波数　200MHz
・計算時間　141 μ sec

Hardware Architecture



まとめ

- Pairingの定義を与えた。
- Pairing計算のアルゴリズムを与え、その改良例を紹介した。
- ソフトウェア実装例を示した。
- ハードウェア実装例を示した。