$p =$
$\ell_A^{e_A}\ell_B^{e_B}\cdot$
$f \pm$
1
ℓ_A
ℓ_B
p
$\ell_A^{e_A} \approx$
$\ell_B^{e_B}$
$\ell_A^{e_A}$
$\ell_B^{e_B}$
$\ell_A^{e_A}\ell_B^{e_B}$
f
$p =$
$\ell_A^{e_A}\ell_B^{e_B}\cdot$
$f -$
$1 p =$
$\ell_A^{e_A}\ell_B^{e_B}\cdot$
$f +$
1
?
$p =$
$\ell_A^{e_A}\ell_B^{e_B}\cdot$
$f \pm$
1
E
F_{p^2}
$(p \mp 1)^2 =$
$(\ell_A^{e_A}\ell_B^{e_B}\cdot$
$f)^2$
E
F_p
F_p

$$E(F_p) = \{(x, y) \in F_p \times F_p | y^2 = x^3 + Ax + B\} \cup \{\infty\}$$

$$E(F_p) \subseteq (F_p \times F_p) \cup \{\infty\}$$

$p^2 +$
1
$E(F_p)$

$$\#E(F_p) \leq p^2 + 1$$

$$\#E(F_p) - 1 \leq p^2$$

$$p = \ell_A^{e_A}\ell_B^{e_B}\cdot f + 1 p = \ell_A^{e_A}\ell_B^{e_B}\cdot f - 1$$

$$p^2 = (\ell_A^{e_A}\ell_B^{e_B}\cdot f)^2 + 2(\ell_A^{e_A}\ell_B^{e_B}\cdot f) + 1 p^2 = (\ell_A^{e_A}\ell_B^{e_B}\cdot f)^2 - 2(\ell_A^{e_A}\ell_B^{e_B}\cdot f) - 1$$

$$(p^2 \pm 1)^2 = (\ell_A^{e_A}\ell_B^{e_B}\cdot f)^2 \pm 2\ell_A^{e_A}\ell_B^{e_B}\cdot f$$

$(\ell_A^{e_A}\ell_B^{e_B}\cdot$
$f) =$
p

$$p^2 \mp 2p \mp 1 = (\ell_A^{e_A}\ell_B^{e_B}\cdot f)^2$$

$$(p \mp 1)^2 = (\ell_A^{e_A}\ell_B^{e_B}\cdot f)^2$$

$E_0[\ell_A^{e_A}]$
$P \in_R E_0(F_{p^2})$
$(\ell_B^{e_B}\cdot f)^2$
P'
ℓ_A
p
$\ell_A^{e_A}$
$\ell_B^{e_B}$
P'
$\ell_A^{e_A}$
P'
ℓ_A
$P_A =$
P'
P
Q_A
ℓ_A
Q_A
P_A
$e(P_A, Q_A)$
$E[\ell_A]$
ℓ_A
Q_A
P_A
$P_A, Q_A \in$
$E[\ell_A]$
ℓ_A

$$e_n(P_A, Q_A) = 1 Q_A = k P_A$$