RSA

RSA

?

p

$\ell_A^{e_A}\ell_B^{e_B}.f\pm$

1

E_0

F_{p^2}

?

$\{P_A, Q_A\}$

$\{P_B, Q_B\}$

$E_0[\ell_A^{e_A}]$

$E_0[\ell_B^{e_B}]$

p

E_0

$E_0[\ell_A^{e_A}]$

$E_0[\ell_B^{e_B}]$

:

$\phi_A :$

$E_0 \rightarrow$

E_A

$\langle[m_A]P_A+$

$[n_A]Q_A\rangle$

m_A

n_A

$(Z/\ell_A^{e_A}Z)$

ℓ_A

E_A

$\phi_A(P_B)$

$\phi_A(Q_B)$

$\langle R_A\rangle =$

$\langle[m_A]P_A+$

$[n_A]Q_A\rangle$

E_0

E_A

ϕ_A

$\phi_A(P_B)$

$\phi_A(Q_B)$

$CSSI$

.

$R_A(=$

$[m_A]P_A+$

$[n_A]Q_A)$

P_A

Q_A

m_A

n_A

E_0

?

$\phi_A(P_B)$

$\phi_A(Q_B)$

:

$_0[r,”\phi”][d]E_3[d]$

$_1[r,”\phi'”]E_2$

$\phi:$

$E_0 \to$

E_3

$\ell_A^{e_A}$

(E_1, E_2, ϕ')

$1/2$

R

$\ell_B^{e_B}$

$E_1 =$

$E_0/\langle R\rangle$

$E_2 =$

$E_3/\langle \phi_R\rangle$

$\phi':$

$E_1 \to$

E_2

$\ell_A^{e_A}$

E_1

E_0

$\phi':$

$E_1 \to$

E_2

$\ell_A^{e_A}$

$DSSI$

?