$RSA$
$RSA$
$?$
$p$
$\ell_A^{e_A} \ell_B^{e_B} . f \pm$
$1$
$E_0$
$F_{p^2}$
$?$
$\{P_A, Q_A\}$
$\{P_B, Q_B\}$
$E_0[\ell_A^{e_A}]$
$E_0[\ell_B^{e_B}]$
$p$
$E_0$
$E_0[\ell_A^{e_A}]$
$E_0[\ell_B^{e_B}]$
$\vdots$
$\phi_A :$
$E_0 \rightarrow$
$E_A$
$\langle [m_A]P_A +$
$[n_A]Q_A \rangle$
$m_A$
$n_A$
$(Z/\ell_A^{e_A} Z)$
$\ell_A$
$E_A$
$\phi_A(P_B)$
$\phi_A(Q_B)$
$\langle R_A \rangle =$
$\langle [m_A]P_A +$
$[n_A]Q_A \rangle$
$E_0$
$E_A$
$\phi_A$
$\phi_A(P_B)$
$\phi_A(Q_B)$
$CSSI$
$R_A (=$
$[m_A]P_A +$
$[n_A]Q_A)$
$P_A$
$Q_A$
$m_A$
$n_A$
$E_0$
$?$
$\phi_A(P_B)$
$\phi_A(Q_B)$

:
$_0[r, "\phi"][d]E_3[d]$
$_1[r, "\phi'"]E_2$
$\phi$ :
$E_0 \to$
$E_3$
$\ell_A^{e_A}$
$(E_1, E_2, \phi')$
$1/2$
$R$
$\ell_B^{e_B}$
$E_1 =$
$E_0/\langle R \rangle$
$E_2 =$
$E_3/\langle \phi_R \rangle$
$\phi'$ :
$E_1 \to$
$E_2$
$\ell_A^{e_A}$
$E_1$
$E_0$
$\phi'$ :
$E_1 \to$
$E_2$
$\ell_A^{e_A}$
$DSSP$
?

?
?
[4]
??
(com, 0, resp_0)
(com, 1, resp_1)
com =
(E_1, E_2)
resp_0 =
(R, φ(R))
ψ :
E →
E/⟨R⟩
resp_1 =
ψ(S)
φ′
ψ
ψ′ :
E/⟨R⟩ →
E
ψ′(resp_1)
⟨S⟩
φ"[d, thick, "ψ"]E/⟨S⟩[d, thick, "ψ′"]
⟨R⟩[r, thick, "φ′"]E/⟨R, S⟩
φ′
ψ
⟨S⟩
(S)
S
b =
0
S
R ∈
E
E[ℓ_B^{e_B}]
φ(R)
φ
E[ℓ_B^{e_B}]
ψ :
E →
E/⟨R⟩
ψ′ :
E/⟨S⟩ →
E/⟨S, R⟩
ψ"]E/⟨S⟩[d, "ψ′"]
⟨R⟩[r, "φ′"]E/⟨R, S⟩
E_1 =
E/⟨R⟩
E_2 =
E/⟨S, R⟩
b =
1
E′
E
R ∈
E′
E[ℓ_A^{e_A}]
φ′ :
E′ →
E′/⟨R⟩
φ"]E/⟨S⟩
⟨R⟩[r, "φ′"]E/⟨R, S⟩
E_1 =
E′
E_2 =
E′/⟨R⟩
(E_1, E_2, b, R)
m
S
S
b
S
1−
b
1/2
DSSP
b =
0
S
D
φ′ :
E_1 →
E_2
S
D
DSSP