RSA
RSA
p
q
$N =$
$p\cdot$
q
v
N
s

$$sv \equiv 1 \pmod{(p-1)(q-1)}$$

s
v
RSA
v
s
D
$1 <$
$D <$
N
$S \equiv D^s \pmod{N}$

S
D
$S^v \pmod{N}$

D
$S^v \equiv D^{sv} \equiv D \pmod{N}$

$1/2$
n
$1/2^n$
$p =$
$\ell_A^{e_A}\ell_B^{e_B}\cdot$
$f\pm$
1
ℓ_A
ℓ_B
$\ell_A^{e_A}$
$\ell_B^{e_B}$
f
p
?
E
F_{p^2}
$(\ell_A^{e_A}\ell_B^{e_B})^2$
$E[\ell_A^{e_A}]$
$E[\ell_B^{e_B}]$
$\langle P_A, Q_A\rangle$
$\langle P_B, Q_B\rangle$
E
??
S
$\phi :$
$E \to$
$E/\langle S\rangle$
:
ϕ
S
:
$E/\langle S\rangle$
P_B
Q_B
$\phi(P_B)$
$\phi(Q_B)$
$\phi"][d,"\psi"]E/\langle S\rangle[d,"\psi'"]$
$\langle R\rangle[r,"\phi'"]E/\langle R,S\rangle$

$\langle S\rangle$
R
$\ell_B^{e_B}$
$\psi :$
$E \to$
$E/\langle R\rangle$
$\phi' :$
$E/\langle R\rangle \to$
$E/\langle R,S\rangle$
$\langle\psi(S)\rangle$
$\psi' :$
$E/\langle S\rangle \to$
$E/\langle R,S\rangle$
$\langle\phi(R)\rangle$
$com \equiv$
(E_1, E_2)
$E_1 =$
$E/\langle R\rangle$
$E_2 =$
$E/\langle R,S\rangle$

$\phi"][d, dashrightarrow, "\psi"]E/\langle S\rangle[d, dashrightarrow, "\psi'"]$
$\langle R\rangle[r, "\phi'"]E/\langle R, S\rangle$
ϕ
λ
p
6λ
λ
λ
S
R
??
$E/\langle S\rangle$
??
ψ
ψ'
ϕ'
S
S
$ch =$
0
ψ
ϕ'
$ch =$
1
ϕ'
?
?
$\mathcal{P}$
x
$\mathcal{V}$
x
w
R
x
w
$(x, w) \in$
R
v
S
s
$(v, s) \in R; R : \{sv \equiv 1((p-1)(q-1))\}$

m
$\Sigma =$
$((P^1, P^2), V)$
$com =$
$P^1(x, w)$
x
w
ch
N_{ch}
$resp =$
$P^2(x, w, com, ch)$
ch
$V(x, com, ch, resp)$
$\Sigma =$
(P, V)
$P =$
(P^1, P^2)
$\mathcal{P}$
w
x
$\mathcal{V}$
E_Σ
$(com, ch, resp)$
$(com, ch', resp')$
$ch \neq$
ch'
w
$(x, w) \in$
R
com
ch
ch'
$resp$
$resp'$
com
S_Σ
$(com, ch, resp)$
??
$P(x, w)$
π
w
$V(x, \pi)$
π
x
(P, V)
w
x
V
$\pi =$
$P(x, w)$
S
$\mathcal{P}$
E
w
x
(Σ)
(P_{OE}, V_{OE})
(Σ)
$\Sigma =$
(P_Σ, V_Σ)
$P_\Sigma =$
(P^1_Σ, P^2_Σ)

```
$H$
$A$
$G$
$V_{\Sigma}$
$\pi$
$J_i$
$resp_{i,J_i}$
$ch_{i,j}$
$ch_{i,J_i}$
$resp_{i,J_i}$
$V_{OE}$
$(x, \pi)$
$\pi =$
$((com_i)_i, (ch_{i,j})_{i,j}, (h_{i,j})_{i,j}, (resp_{i,J_i})_i)$
$i =$
$1$**to**$t$
**check**$ch_{i,1}, \cdots ch_{i,m} pairwisedistinct$
**check**$h_{i,J_i} =$
$G(resp_i)$
**check**$V_{\Sigma}(x, com_i, ch_{i,J_i}, resp_i) =$
$1$
**re-**
**turn**
```

$KeyGen(\lambda)$
λ
(pk, sk)
$Sign(sk, m)$
m
sk
σ
$Verify(pk, m, \sigma)$
pk
σ
m
$\mathcal{A}$
$sig :$
$m \mapsto$
$Sign(sk, m)$
$KeyGen$
(sk, pk)
pk
sk
$x =$
pk
$w =$
sk
$(x, w) \in$
R
(x, w)
$KeyGen$
x
$x =$
(pk, m)
R
$((pk, m), w) \in$
R
(pk, m)
(P, V)
$\mathcal{DS}$
$\mathcal{DS} = (KeyGen, Sign, Verify)$

$Sign(sk, m) = P((pk, m), sk)$

$Verify(pk, m, \sigma = V((pk, m, \sigma)))$

(P, V)
$NIZK$
$\mathcal{DS}$

$p =$
$\ell_A^{e_A}\ell_B^{e_B}.$
$f \pm$
1
E
$(\ell_A^{e_A}\ell_B^{e_B})^2$
F_{p^2}
(P_B, Q_B)
$E[\ell_B^{e_B}]$
S
$\ell_A^{e_A}$
$\phi :$
$E \to$
$E/\langle S\rangle$
(pk, sk)
$pk =$
$\Big(E/\langle S\rangle, \phi(P_B), \phi(Q_B)\Big)$
$sk =$
S
m
$Sign(sk, m) = P_{OE}((pk, m), sk)$

σ
m
$Verify(pk, m, \sigma) = V_{OE}((pk, m), \sigma)$

S
$\ell_A^{e_A}$
$\phi :$
$E \to$
$E/\langle S\rangle$
$\langle S\rangle$
$E/\langle S\rangle$
ϕP_B
ϕQ_B
pk
S
(pk, sk)
m
sk
2λ
R
$\ell_B^{e_B}$
ψ
$\langle R\rangle$
$\psi :$
$E \to$
$E/\langle R\rangle$
ϕ'
ψ'
$\phi' : E/\langle R\rangle \to E/\langle R, S\rangle$

$\psi' : E/\langle S\rangle \to E/\langle R, S\rangle$

ϕ'
ψ'
$(E_1, E_2) \leftarrow (E/\langle R\rangle, E/\langle R, S\rangle)$

$com_i \leftarrow (E_1, E_2)$

$ch_{i,0} \leftarrow_R \{0, 1\}$

$(resp_{i,0}, resp_{i,1}) \leftarrow ((R, \phi(R)), \psi(S))$

G
$h_{i,j} \leftarrow G(resp_{i,j})$

2λ
$J_1 \parallel \cdots \parallel J_{2\lambda} \leftarrow H(pk, m, (com_i)_i, (ch_{i,j})_{i,j}, (h_{i,j})_{i,j})$

H

$\sigma \leftarrow ((com_i)_i, (ch_{i,j})_{i,j}, (h_{i,j})_{i,j}, (resp_{i,J_i})_i)$

$resp$
J_i
pk
m
σ

$J_1 \parallel \cdots \parallel J_{2\lambda} \leftarrow H(pk, m, (com_i)_i, (ch_{i,j})_{i,j}, (h_{i,j})_{i,j})$

π
2λ

¨o

J. Comb. Number Theory

Conference on the Theory and Application of Cryptographic Techniques

Journal of Symbolic Computation

Annual International Conference on the Theory and Applications of Cryptographic Techniques