?

??

Generación de llaves

Encapsulado

Decapsulado

?

Keccak-p

?

Funciones de hash

224

256

384

512

$SHA3-$ 256

Funciones de salida extendida

$SHAKE-$ 128

$SHAKE-$ 256

Keccak-p

Keccak-p

El ancho de la permuta

$b \in \{25, 50, 100, 200, 400, 800, 1600\}$

El número de rondas

$n_r \in Z$

b
$w =$
$b/25$
$l =$
$\log_2(b/25)$
$||$
0^j
j
$\texttt{len}(P)$
P
$Z(j)$
j
Z
$Z =$
10010
$Z(4) =$
1
$\texttt{trunc}_d(Z)$
d
Z
Keccak-p
b
S
$A(x, y, z)$
$x, y \in$
$\{0, 1, 2, 3, 4\}$
z
w
??
??

S
A

$$A(x, y, z) = S(w\cdot(5y+x)+z) \tag{1}$$

A
S
S

$$\begin{aligned} Linea(i, j) &== A(i, j, 0) \,||\, A(i, j, 1) \,||||\, A(i, j, w-1) \\ Plano(j) &= Linea(0, j) \,||\, Linea(1, j) \,||||\, Linea(4, j) \\ S &= Plano(0) \,||\, Plano(1) \,||||\, Plano(4) \end{aligned} \tag{2}$$

θ
ρ
π
χ
ι
$A(x, y, z)$
$A'(x, y, z)$
ι
i_r
Transformada
θ
$\oplus$
$A(x, y, z)$
$C(x-$
$1 mod 5, z)$
$C(x+$
$1 mod 5, z-$
$1 mod w)$
θ
Entrada: A
Salida: A'
C

$$C(x, z) := A(x, 0, z) \oplus A(x, 1, z) \oplus A(x, 2, z) \oplus A(x, 3, z) \oplus A(x, 4, z) \tag{3}$$

D

$$D(x, z) := C(x-1 \bmod 5, z) \oplus C(x+1 \bmod 5, z-1 \bmod w) \tag{4}$$

$$A'(x, y, z) := A(x, y, z) \oplus D(x, z) \tag{5}$$

A'
Transformada
ρ
??
$x = 3 x = 4 x = 0 x = 1 x = 2$
$y = 2$
$y = 1$
$y = 0$
$y = 4$
$y = 3$
ρ
ρ
Entrada: A
Salida: A'
$(x, y, z) :=$
$(0, 0, z)$

$$A'(0, 0, z) := A(0, 0, z) \tag{6}$$

Transformada
π
(x, y)
?? $x = 3x = 4x = 0x = 1x = 2$
$y = 2$
$y = 1$
$y = 0$
$y = 4$
$y = 3$
π
$A'(x, y)$
(x', y')
A
π
Entrada: A
Salida: A'
$A'(x, y, z) := A(x+3ymod5, x, z)$

(8)

A'
Transformada
X
??
X
?
$A(x, y, z)$
$A'(x, y, z)$

χ

Entrada: A

Salida: A'

$$A'(x,y,z) := A(x,y,z) \oplus \{[A(x+1 mod 5, y, z) \oplus 1] \& A(x+2 mod 5, y, z)\} \quad (9)$$

A'

Transformada

ι

$(0,0)$

i_r

ι

Entrada: $A i_r$

Salida: A'

$$A'(x,y,z) := A(x,y,z) \quad (10)$$

RC

w

$l =$

$\log_2(b/25)$

$$RC(2^j - 1) := \texttt{rc}(j + 7 i_r) \quad (11)$$

$$A'(0,0,z) := A'(0,0,z) \oplus RC(z) \quad (12)$$

A'

$\texttt{rc}(t)$

t

Entrada: t

Salida: $rc(t)$

$t mod 255 =$

0

255

$R :=$

$R||R$

$R[0] :=$

$R[0] \oplus$

$R[8]$

$R[4] :=$

$R[4] \oplus$

$R[8]$

$R[5] :=$

$R[5] \oplus$

$R[8]$

$R[6] :=$

$R[6] \oplus$

$R[8]$

$R :=$

$\texttt{Trunc}_8[R]$

$R[0]$

$\texttt{Rnd}(A, i_r)$

$\texttt{Rnd}(A, i_r) = \iota(\chi(\pi(\rho(\theta(A)))), i_r)$

(13)

$\texttt{Keccak-p}(b, n_r)$

n_r

$\texttt{Rnd}$

b

Entrada: Sn_r

Salida: S'

S

A

i_rn_r

$\texttt{Rnd}(A, i_r)$

A

S'

b

S'

$\texttt{sponge}[f, pad, r](N, d)$

N

Z

d

f

pad

r

b

f

$\texttt{sponge}$

??

r

b

f

$\texttt{keccak-p}$

$c = b{-}r$

(14)

r

d

sponge
?
sponge
Entrada: Nd
Salida:
$P = N||\texttt{pad}(r, \texttt{len}(N))$
(15)
$n = len(P)r$
(16)
$c = b - r$
$S = 0^b$
$P_0, , P_{n-1}$
r
$P = P_0||||P_{n-1}$
$S = f(S \oplus (P_i||0^c))$
(17)
Z
$Z = Z||\texttt{Trunc}_r(S)$
(18)
$d \leq len(Z)$
$\texttt{Trunc}_d(S)$
$S = f(S)$
(19)
sponge
pad10*1
x
m
P
$m + \texttt{len}(P) = \lambda x$
(20)
pad10*1
Entrada: xm
Salida:
$j = -m - 2 mod x$
(21)
$P = 1||0^j||1$
(22)
P
$b = 1600$
$\texttt{Keccak}[c](N, d)$
$\texttt{Keccak}[c](N, d) = \texttt{sponge}[\texttt{Keccak-p}(1600, 24), \texttt{pad10*1}, 1600 - c](N, d)$
(23)
$\texttt{SHA3-224}(M)\texttt{Keccak}(M||01, 224)$
$\texttt{SHA3-256}(M)\texttt{Keccak}(M||01, 256)$
$\texttt{SHA3-384}(M)\texttt{Keccak}(M||01, 384)$
$\texttt{SHA3-512}(M)\texttt{Keccak}(M||01, 512)$
$\texttt{SHAKE128}(M, d)\texttt{Keccak}(M||1111, d)$
$\texttt{SHAKE256}(M, d)\texttt{Keccak}(M||1111, d)$
?
Resistencia a la colisión
Resistencia a preimagen
h
x
$\texttt{hash}(x) = h$
Resistencia a preimagen secundaria
x_1
x_2
$\texttt{hash}(x_1) = \texttt{hash}(x_2)$

?

?

?

$\mathcal{B} =$

$\{0, \ldots, 255\}$

k

$\mathcal{B}^k$

$\mathcal{B}^*$

$||$

$+k$

k

a

l

b

$$c = a||b \tag{24}$$

$$b = c+l \tag{25}$$

$v[i]$

v

i

$A[i][j]$

i

j

A

A^T

$\lfloor x \rceil$

x

$\lfloor 2{,}3 \rceil =$

2

$\lfloor 2{,}5 \rceil =$

3

$\lfloor 2{,}8 \rceil =$

3

$\|x\|$

α

$$r' = r mod^{\pm} \alpha \Longrightarrow -\alpha 2 < r' \leq \alpha 2 \tag{26}$$

$$r' = r mod^{+} \alpha \Longrightarrow 0 \leq r' < \alpha \tag{27}$$

$s \leftarrow$

S

s

S

S

s

$\mathcal{O}(n^2)$
$\mathcal{O}(n\log(n))$
?
R_q

$R_q Z_q[X] X^n + 1$
(28)
?
$q =$
3329
$n =$
256
$n|(q-1)$
n
$(q-1)$
n
Z_q
0
n
$q > 1$
Z_q
$n|(q-1)$
ω
Z_q

$$\Omega = \left\{1, \omega, \omega^2, \dots, \omega^{n-1}\right\}$$
(29)

H
G_{q-1}
H
G_{q-1}
$n \mid (q-1)$
G_{q-1}
α

$$\alpha^{q-1} = 1$$
(30)

G_{q-1}

$$G_{q-1} = \left\{1, \alpha, \alpha^2, \dots, \alpha^{q-2}\right\}$$
(31)

ω

$$\omega = \alpha^{\frac{q-1}{n}},$$
(32)

$$\omega^n = \alpha^{q-1} = 1,$$
(33)

$0 <$
$k <$
n

$$k \cdot \frac{q-1}{n} < q-1 \Rightarrow \omega^k \neq 1.$$
(34)

ω
Z_q

$X^{256}+$
1
Z_q
Z_q
n

$$\hat{a}_j = \sum_{i=0}^{n-1} \phi^{i(2j+1)} a_j mod q$$
(35)

$$a_i = n^{-1} \sum_{j=0}^{n-1} \phi^{-i(2j+1)} \hat{a}_j mod q$$
(36)

ϕ
$\phi^2 =$
ω
ω
Z_q
n^{-1}
n
Z_q
?
$G(x) =$
$5+$
$6x+$
$7x^2+$
$8x^3$
$g =$
$[5, 6, 7, 8]$
Z_{7681}
$\phi =$
1925
$\hat{g}$
g

$$\hat{g} = \phi^0\phi^1\phi^2\phi^3\phi^0\phi^3\phi^6\phi^1\phi^0\phi^5\phi^2\phi^7\phi^0\phi^7\phi^6\phi^5 \cdot 5678 = 11925338364681646842981925157563383121311213429857 56 \cdot 5678 = 24$$
(37)

$\phi =$
1925
Z_{7681}
$\phi^{-1} =$
1213
$n =$
4
$n^{-1} =$
5761

$$g = n^{-1}\phi^0\phi^0\phi^0\phi^0\phi^{-1}\phi^{-3}\phi^{-5}\phi^{-7}\phi^{-2}\phi^{-6}\phi^{-2}\phi^{-6}\phi^{-3}\phi^{-1}\phi^{-7}\phi^{-5} \cdot \hat{g} = 576111111213575664681925429833834298338357561$$
(38)

$R_q Z_q[X] X^n + 1$
g
h

$$g \cdot h = NTT^{-1}(NTT(g) \circ NTT(h))$$
(39)

$\circ$
$Z_q[X]$

$\mathcal{O}(n\log(n))$

$\phi^{k+2n}=\phi^{k}$

(40)

$\phi^{k+n}=\phi^{-k}$

(41)

?

$$\hat{a}_j=\sum_{i=0}^{n-1}\phi^{i(2j+1)}a_j modq=\sum_{i=0}^{n/2-1}\phi^{4ij+2i}a_{2i}+\phi^{2j+1}\sum_{i=0}^{n/2-1}\phi^{4ij+2i}a_{2i+1}modq$$

(42)

$A_j=$
$\sum_{i=0}^{n/2-1}\phi^{4ij+2i}a_{2i}$
$B_j=$
$\sum_{i=0}^{n/2-1}\phi^{4ij+2i}a_{2i+1}$
ϕ

$\hat{a}_j=A_j+\phi^{4ij+2i}B_j modq$

(43)

$\hat{a}_{j+n/2}=A_j-\phi^{4ij+2i}B_j modq$

(44)

A_j
B_j
$\frac{n}{2}$
$\mathcal{O}(n\log(n))$
?
R_q
$\left\{\xi,\xi^3,\ldots,\xi^{255}\right\}$
$\xi=$
17

$$X^{256}+1=\prod_{i=0}^{127}\left(X^2-\xi^{2i+1}\right)$$

(45)

?
$f\in$
R_q

$$NTT(f)=\hat{f}=\left(\hat{f}_0+\hat{f}_1X,\hat{f}_2+\hat{f}_3X,...,\hat{f}_{254}+\hat{f}_{255}X\right)$$

(46)

$$\hat{f}_{2i}=\sum_{j=0}^{127}f_{2j}\xi^{(2i+1)j}$$

$$\hat{f}_{2i+1}=\sum_{j=0}^{127}f_{2j+1}\xi^{(2i+1)j}$$

(47)

$^{-1}$
$fg\in$
R_q

$$h=f\cdot g=NTT^{-1}\left[NTT(f)\circ NTT(g)\right]$$

(48)

$\hat{h}=$
$\hat{f}\circ$
$\hat{g}=$
$NTT(f)\circ$
$NTT(g)$

$$\hat{h}_{2i}+\hat{h}_{2i+1}X=(\hat{f}_{2i}+\hat{f}_{2i+1})\left(\hat{g}_{2i}+\hat{g}_{2i+1}\right)mod\left(X^2-\xi^{2i+1}\right)$$

(49)

??
$\mathcal{O}(n^2)$
$^{-1}$
$\mathcal{O}(n\log(n))$
$\hat{f}$
$\circ$
$\hat{g}$
$\hat{h}$
?
n
$B=$
$\{b_1,...,b_n\}$

$$\mathcal{A}=\mathcal{L}(B)=\left\{\sum_{i\in n}z_ib_i:z\in Z^n\right\}$$

(50)

??
q
n
sk
pk
$Z_q[x]/(X^n+$
$1)$
0

Entrada: qn
Salida: $skpk$
$a \in$
R_q
$sk, e \in$
R_q

$$b := a \cdot sk + e \tag{51}$$

$(sk, pk :=$
$a||b)$
pk
$z \in$
$\{0,1\}^n$
u
v
0

Entrada: $pkzqn$
Salida: uv
$r, e_1, e_2 \in$
R_q
u

$$u := a \cdot r + e_1 mod^+ q \tag{52}$$

v

$$v := b \cdot r + e_2 + \lfloor q2 \rceil \cdot z mod^+ q \tag{53}$$

(u, v)
u
v
z
$\varepsilon =$
$r \cdot$
$e -$
$s \cdot$
$e_1 +$
e_2
$\|\varepsilon\| <$
$q/4$
2^{-174}
?

0

Entrada: $skuvqn$

Salida: z

z'

$$z' := v - u \cdot s = (r \cdot e - s \cdot e_1 + e_2) + \lfloor q2 \rceil \cdot z mod^{+} q \tag{54}$$

(z'_i)

z'

1.1:

0

$$d_i(0) := \left\| z'_i mod^{\pm} \lfloor q2 \rceil \right\| \tag{55}$$

1.2:

$\lfloor q2 \rceil$

$$d_i\left(q2\right) := \left\| \lfloor q2 \rceil - d_i(0) \right\| \tag{56}$$

$d_i(0) <$

$d_i\left(q2\right)$

i

z

0

i

z

1

z

??

?

R_q

d

$s \in R_q^d (elvectorsecreto) A \in R_q^{d \times d} (lamatrizpblica, muestreada R_q^{d \times d}$

ρ

$\in$

$R_q^d (elvectordeerror, concoeficientespequeos)$

$b \in$

$R_q^d (laparejaresultante)$

$b =$

$A \cdot$

$s +$

$e \in$

R_q^d

(A, b)

$R_q^{d \times d} \times$

R_q^d

d

A

n	k	q	η_1	η_2	d_u	d_v	δ	$pk(bytes)$	$sk(bytes)$	$c(bytes)$
256	4	3329	2	2	11	5	2^{-174}	3168(32)	1568	1568

$n =$

256

$k =$

4

$q =$

3329

$n | (q -$

$1)$

η_1

η_2

d_u

d_v

δ

(32)

?

(pk)

(sk)

??

$Parse(x)$

a_i

$\log_2(q) \approx$

11.7

$a_i <$

q

$CBD_\eta(x)$

$B \in$

$\mathcal{B}^{64\eta}$

$f \in$

R_q

$Encode_k(x)$

$B \in$

$\mathcal{B}^{32l}$

$f \in$

R_q

Salida: $pk \in \mathcal{B}^{12\cdot k\cdot n/8+32} sk \in \mathcal{B}^{24\cdot k\cdot n/8+96}$

$d, z \in$
$\mathcal{B}^{32}$
ρ, σ
d

$(\rho, \sigma) := SHA3 - 512(d)$
(57)
$\hat{A}[i][j] :=$
$Parse[SHAKE - 128(\rho, j, i)]$
$N :=$
0
$s[i] :=$
$CBD_{\eta_1}[SHAKE - 256(\sigma, N)]$
$N :=$
$N+$
1
$e[i] :=$
$CBD_{\eta_1}[SHAKE - 256(\sigma, N)]$
$N :=$
$N+$
1
$\hat{s} := NTT(s)$
$\hat{e} := NTT(e)$
$\hat{t} := \hat{A} \circ \hat{s} + \hat{e}$
(58)
$pk := Encode_{12}(\hat{t} mod^{+} q)||\rho$
(59)
$\hat{b}$
ρ
$\hat{A}$
$sk := Encode_{12}(\hat{s} mod^{+} q)||pk||SHA3 - 256(pk)||z$
(60)
(pk, sk)
c
pk
m
γ
$Compress_q(x, y)$
$Decompress_q(x, y)$
$Decode_k(x)$
$f \in$
R_q
$B \in$
$\mathcal{B}^{32l}$

```
    **Entrada:** $pk \in \mathcal{B}^{12\cdot k\cdot n/8+32} m \in \mathcal{B}^{32} \gamma \in \mathcal{B}^{32}$
    **Salida:** $c \in \mathcal{B}^{d_u\cdot k\cdot n/8+d_v\cdot n/8}$
    $N :=$
    $0$
    $r[i] :=$
    $CBD_{\eta_1}[SHAKE-256(\gamma, N)]$
    $r$
    $N :=$
    $N+$
    $1$
    $e_1[i] :=$
    $CBD_{\eta_2}[SHAKE-256(\gamma, N)]$
    $N :=$
    $N+$
    $1$
    $e_2[i] :=$
    $CBD_{\eta_2}[SHAKE-256(\gamma, N)]$
    $\hat{r} := NTT(r)$
    $u := NTT^{-1}(\hat{A}^T \circ \hat{r}) + e_1$
    $v := NTT^{-1}(\hat{t}^T \circ \hat{r}) + e_2 + Decompress_q[Decode_1(m), 1]$
    $c_1 := Encode_{d_u}[Compress_q(u, d_u)]$
    $c_2 := Encode_{d_v}[Compress_q(v, d_v)]$
(61)
    $c :=$
    $c1||c2$
    $pk$
    $c$
    $k$
    **Entrada:** $pk \in \mathcal{B}^{12\cdot k\cdot n/8+32}$
    **Salida:** $c \in \mathcal{B}^{d_u\cdot k\cdot n/8+d_v\cdot n/8} k \in \mathcal{B}^*$
    $\hat{t} := Decode_{12}(pk)$
    $p := pk + 12 \cdot k \cdot n/8$
(62)
    $\hat{A}^T$
    $\rho$
    $m'$
    $m, \kappa, \gamma$
    $m'$
    $m := SHA3-256(m')$
    $(\kappa, \gamma) := SHA3-512[m||SHA3-256(pk)]$
(63)
    $c \leftarrow CifradoKyber(pk, m, \gamma)$
(64)
    $k := SHAKE-256[\kappa||SHA3-256(c)]$
(65)
    $c, k$
    $c$
    $sk$
    $k$
    **Entrada:** $c \in \mathcal{B}^{d_u\cdot k\cdot n/8+d_v\cdot n/8} sk \in \mathcal{B}^{24\cdot k\cdot n/8+96}$
    **Salida:** $k \in \mathcal{B}^*$
    $u$
    $v$
    $s$
    $u := Decompress_q[Decode_{d_u}(c, d_u)]$
    $v := Decompress_q[Decode_{d_v}(c + d_u \cdot k \cdot n/8, d_v)]$
    $\hat{s} := Decode_{12}(sk)$
(66)
    $m'$
    $m' := Encode_1[Compress_q\left(v - NTT^{-1}(\hat{s}^T \circ NTT(u)), 1\right)]$
(67)
    $m'$
    $pk$
    $\gamma$
    $c'$

    $pk := sk + 12 \cdot k \cdot n/8$
    $h := sk + 24 \cdot k \cdot n/8 + 32$
    $(\kappa, \gamma) := SHA3-512[m'||h]$
    $c' \leftarrow CifradoKyber(pk, m', \gamma)$
(68)
    $z$
    $z := sk+24\cdot k\cdot n/8+64$
(69)
    $c ==$
    $c'$
    $K :=$
    $SHAKE-256[\kappa||SHA3-256(c)]$
    $K :=$
    $SHAKE-256[z||SHA3-256(c)]$
    **?**
    $R_q = Z_q X^n + 1$
(70)
    $n =$
    $256$
    $q =$
    $2^{13}$
    $2$
    $2$
    **?**
    $2$
```

?
(a, u)
(a, b)
$a \leftarrow \mathcal{U}(R_q^{l\times l})$
$s \leftarrow \beta_\mu(R_q^{l\times 1}))$
$b \in R_p^{l\times 1}$
$b = \lfloor pq(A \cdot s) \rceil$
(82)
$\mathcal{U}$
β_μ
μ
$\sigma =$
$\sqrt{\mu/2}$
l
$\texttt{bits}(x, i, j)$

$$\texttt{bits}(x, i, j) = [x >> (i-j)] \& (2^j - 1) = \begin{cases} x2^{i-j} mod^{+j} \\ \neq & sij = i \\ ixmod^{+j} \end{cases}$$

(83)
Entrada: $qpnl\mu$
Salida: $skbA$
$A \in$
$R_q^{l\times l}$
$sk \in$
$R_q^{l\times 1}$
β_μ
$b \in$
$R_p^{l\times 1}$

$b := \texttt{bits}(A \cdot s + h, \varepsilon_q, \varepsilon_p)$
(84)
(sk, b, A)
ε_i
$\varepsilon_i =$
$\log_2(i)$
$h \in$
R_q
$2^{\varepsilon_q - \varepsilon_p - 1}$
Entrada: $pkAqptnl\mu$
Salida: $ss'b'c$
$s' \in$
$R_q^{l\times 1}$
β_μ
$b' \in$
$R_p^{l\times 1}$
$v' \in$
R_p
A
b

$b' := \texttt{bits}(A^T \cdot s' + h, \varepsilon_q, \varepsilon_p)$
$v' := b \cdot \texttt{bits}(s', \varepsilon_p, \varepsilon_p) + h_1$
(85)
$c \in$
R_t
v'

$c := \texttt{bits}(v', \varepsilon_p - 1, \varepsilon_t)$
(86)
ss

$ss' := \texttt{bits}(v', \varepsilon_p, 1)$
(87)
(ss', b', c)
$h_1 \in$
R_q
$2^{\varepsilon_q - \varepsilon_p - 1}$
Entrada: $skb'cpt$
Salida: ss
$v \in$
R_p

$v := b'^T \cdot \texttt{bits}(s, \varepsilon_p, \varepsilon_p) + h_1$
(88)
ss

$ss := \texttt{bits}(v - 2^{\varepsilon_p - \varepsilon_t - 1} \cdot c + h_2), \varepsilon_p, 1$
(89)
ss
$h_2 \in$

```
**Salida:** $pk \in \mathcal{B}^{n\cdot l\cdot\varepsilon_p/8+32} sk \in \mathcal{B}^{n\cdot l\cdot\varepsilon_q/8+n\cdot l\cdot\varepsilon_p/8+96}$
$A$
$z$
$seed_A$
$seed_s$
$z \in$
$B^{32}$
$seed_A$
$seed_A := \texttt{SHAKE-128}(seed_A, 32)$
(105)
$A$
$buf := \texttt{SHAKE-128}(seed_A, l^2{\cdot}n{\cdot}\varepsilon_q/8)$
(106)
$buf$
$l^2\cdot$
$n$
$\varepsilon_q$
$k :=$
$0$
$A[i,j][k] :=$
$buf[k]$
$k :=$
$k+$
$1$
$s$
$buf := \texttt{SHAKE-128}(seed_s, l{\cdot}n{\cdot}\mu/8)$
(107)
$buf$
$2\cdot$
$l\cdot$
$n$
$\mu/2$
$k :=$
$0$
$s[i,j] :=$
$\texttt{HammingWeight}(buf[k])-$
$\texttt{HammingWeight}(buf[k+$
$1])mod^+q$
$k :=$
$k+$
$2$
$b$

$b := \left(A^T \circ s + h mod^+ q\right)/2^{\varepsilon_q-\varepsilon_p}$
(108)
$pk := seed_A||\texttt{POLVEC}_q\texttt{2BS}(b)$
(109)
$sk := z||\texttt{SHA3-256}(pk)||pk||\texttt{POLVEC}_q\texttt{2BS}(s)$
(110)
$(pk, sk)$
```

c
pk
m
γ
$\texttt{BS2POLVEC}_x(y)$
y
$l\cdot$
$k\cdot$
$256/8$
$R_x^{l\times 1}$
$\texttt{POL}_x\texttt{2BS}(y)$
$y \in$
R_x
$k\cdot$
$256/8$

Entrada: $pk \in \mathcal{B}^{n\cdot l\cdot \varepsilon_p/8+32} m \in \mathcal{B}^{32} \gamma \in \mathcal{B}^{32}$

Salida: $c \in \mathcal{B}^{n\cdot l\cdot \varepsilon_p/8+n\cdot \varepsilon_t/8}$

A
pk'
pk
s'
b'

$$b' := \left(A \circ s' + hmod^{+}q\right)/2^{\varepsilon_q-\varepsilon_p} \tag{111}$$

b

$$b := \texttt{BS2POLVEC}_p(pk') \tag{112}$$

v'

$$v' := b^T \circ (s' mod^{+} p) mod^{+} p \tag{113}$$

c

$$c := (v' - m\cdot 2^{\varepsilon_p - 1} + h_1 mod^{+} p)/2^{\varepsilon_p-\varepsilon_t} \tag{114}$$

$c :=$
$\texttt{POL}_T\texttt{2BS}(c)||\texttt{POLVEC}_p\texttt{2BS}(b')$
pk
c
k

Entrada: $pk \in \mathcal{B}^{n\cdot l\cdot \varepsilon_p/8+32}$

Salida: $c \in \mathcal{B}^{n\cdot l\cdot \varepsilon_p/8+n\cdot \varepsilon_t/8} k \in \mathcal{B}^{*}$

$m \in$
$\mathcal{B}^{32}$
m
pk
buf

$$m := \texttt{SHA3-256}(m)$$
$$hash_{pk} := \texttt{SHA3-256}(pk)$$
$$buf := hash_{pk}||m \tag{115}$$

γ

$$(\gamma||r) := \texttt{SHA3-512}(buf) \tag{116}$$

c

$$c := \texttt{Cifrado Saber}(pk, m, \gamma) \tag{117}$$

k

$$k := \texttt{SHA3-256}(r||\texttt{SHA3-256}(c)) \tag{118}$$

c, k

c
sk
k
Entrada: $c \in \mathcal{B}^{n\cdot l\cdot \varepsilon_p/8+n\cdot \varepsilon_t/8} sk \in \mathcal{B}^{n\cdot l\cdot \varepsilon_q/8+n\cdot l\cdot \varepsilon_p/8+96}$
Salida: $k \in \mathcal{B}^*$
sk'
z
sk
s

$s := \texttt{BS2POLVEC}_q(sk')$
(119)
$(c_m||ct) := c$
(120)
m'

$c_m := c_m \cdot 2^{\varepsilon_p-\varepsilon_t}$
$b' := \texttt{BS2POLVEC}_p(ct)$
$m' := (b'^T \circ (smod^+p) - c_m + h_2mod^+p)/2^{\varepsilon_p-1}$
(121)
m
$m := \texttt{POL}_2\texttt{2BS}(m')$
(122)
γ
r

$(\gamma||r) := \texttt{SHA3-512}(buf)$
(123)
c'
c
$c' := \texttt{Cifrado Saber}(pk, m, \gamma)$
(124)
k

$k := \texttt{SHA3-256}(r||\texttt{SHA3-256}(c'))$
(125)
k

$k := \texttt{SHA3-256}(z||\texttt{SHA3-256}(c'))$
(126)

?
?
$\mathcal{V}$
n
F_2
F_2^n
$\mathcal{V}$
$\mathcal{R} =$
$F_2[x]/(C^n -$
$1)$
?
$\omega(x)$
x
n
$(X^n -$
$1)/(X -$
$1)$
$\mathcal{R}$
$u, v \in$
$\mathcal{V}$
$\mathcal{R}$
$w =$
$u \cdot$
v

$$w_k = \sum_{i+j=kmod^+n} u_i \cdot v_j \forall k \in 0, , n-1 \tag{127}$$

$\texttt{rot}(h)$
$h \in$
$\mathcal{V}$
i
h_i
x^i

$v = (v_0, , v_{n-1}) \in F_2^n$
$\texttt{rot}(v) = (\ v\ )_0$
v_{n-1}
v_1
v_1
v_0
v_2

v_{n-1}
v_{n-2}
v_0

(128)

$u, v \in$
$\mathcal{V}$

$$u \cdot v = u \cdot \texttt{rot}(v)^T = (\texttt{rot}(u) \cdot v^T)^T = v \cdot u \tag{129}$$

C
n
k
$[n, k]$
R
k
$G \in$
$F_2^{k \times n}$

$$C = \{m \cdot G, m \in F_2^k\} \tag{130}$$

$H \in$
$F_2^{(n-k) \times n}$
$C^{\perp}$
C

$$C = \{v \in F_2^n | H \cdot v^T = 0\}$$
$$C^T = \{u \cdot H, u \in F_2^k\} \tag{131}$$

$v \in$
F_2^n

$$H \cdot v^T \rightarrow siv \in C \rightarrow H \cdot v^T = 0 \tag{132}$$

$C[n, k] \in$
$\mathcal{R}$
d

$$d = \min_{u,v \in C u \neq v} \omega(u - v) \tag{133}$$

δ
$r =$
$u +$
e
u
e