??

?

?
?
??
??
??
??
??
(ss)
FrodoKEM

	n	q	σ	χ	$B\bar{n}\bar{m}c$
FrodoKEM-640		2^{15}		$\{-12, \ldots, 12\}$	
FrodoKEM-976		2^{16}		$\{-10, \ldots, 10\}$	

1^{ℓ}
$\mathbf{s}||seed_{\mathbf{E}}||\mathbf{z} \leftarrow_{\$}$
$U(\{0,1\}^{128})$
$seed_{\mathbf{A}} \leftarrow$
$H(\mathbf{z})$
$\mathbf{A} \in$
$Z_q^{n \times n}$
$\mathbf{A} \leftarrow$
$Frodo.Gen(seed_{\mathbf{A}})$
$\mathbf{S} \leftarrow$
$Frodo.SampleMatrix(seed_{\mathbf{E}}, n, \bar{n}, T_\chi, 1)$
$\mathbf{E} \leftarrow$
$Frodo.SampleMatrix(seed_{\mathbf{E}}, n, \bar{n}, T_\chi, 2)$
$\mathbf{B} \leftarrow$
$\mathbf{AS}+$
$\mathbf{E}$
$pk \leftarrow$
$seed_{\mathbf{A}}||\mathbf{B}$
$sk' \leftarrow$
$(\mathbf{s}||seed_{\mathbf{A}}||\mathbf{B}, \mathbf{S})$
$pk =$
$seed_{\mathbf{A}}||\mathbf{b}$
$\mu \leftarrow$
$U(\{0,1\}^{len_\mu})$
$seed_{\mathbf{E}}||\mathbf{k}||\mathbf{d} \leftarrow$
$G(pk||\mu)$
$\mathbf{S}' \leftarrow$
$Frodo.SampleMatrix(seed_{\mathbf{E}}, \bar{m}, n, T_\chi, 4)$
$\mathbf{E}' \leftarrow$
$Frodo.SampleMatrix(seed_{\mathbf{E}}, \bar{m}, n, T_\chi, 5)$
$\mathbf{A} \in$
$Z_q^{n \times n}$
$\mathbf{A} \leftarrow$
$Frodo.Gen(seed_{\mathbf{A}})$
$\mathbf{B}' \leftarrow$
$\mathbf{S}'\mathbf{A}+$
$\mathbf{E}'$
$\mathbf{c}_1 \leftarrow$
$Frodo.Pack(\mathbf{B}')$
$\mathbf{E}'' \leftarrow$
$Frodo.SampleMatrix(seed_{\mathbf{E}}, \bar{m}, \bar{n}, T_\chi, 6)$
$\mathbf{B} \leftarrow$
$Frodo.Unpack(\mathbf{b}, n, \bar{n})$
$\mathbf{V} \leftarrow$
$\mathbf{S}'\mathbf{B}+$
$\mathbf{E}''$
$\mathbf{C} \leftarrow$
$\mathbf{V}+$
$Frodo.Encode(\mu)$
$\mathbf{c}_2 \leftarrow$
$Frodo.Pack(\mathbf{C})$
$\mathbf{ss} \leftarrow$
$F(\mathbf{c}_1||\mathbf{c}_2||\mathbf{k}||\mathbf{d})$
$\mathbf{c}_1||\mathbf{c}_2||\mathbf{d}$
ss
FrodoKEM
$sk =$
$(\mathbf{s}||seed_{\mathbf{A}}||\mathbf{b}, \mathbf{S}), \mathbf{c}_1||\mathbf{c}_2||\mathbf{d}$
$\mathbf{B}' \leftarrow$
$Frodo.Unpack(\mathbf{c}_1)$
$\mathbf{C} \leftarrow$
$Frodo.Unpack(\mathbf{c}_2)$
$\mathbf{M} \leftarrow$
$\mathbf{C}-$
$\mathbf{B}'\mathbf{S}$