Estruturas Criptográficas

Trabalho Prático 4 - Exercício 3

José de Matos Moreira - PG53963

Pedro Freitas - PG52700

Enunciado do problema

Construir tabelas de comparações das suas implementações, para os vários níveis de segurança **NIST** e em termos dos seguintes parâmetros:

- Tempos: geração das chaves, produção da assinatura e verificação da assinatura
- Tamanhos: da chave pública, da chave privada e da assinatura

Resolução

Em primeiro lugar, mostram-se os *imports* que se revelaram bastante úteis no desenvolvimento do exercício:

In [1]:
```
import time
from prototypes.MLDSA import MLDSA
from prototypes.SLHDSA import SLHDSA
```

De seguida, apresentam-se as diversas variáveis criadas que constituem o corpo da tabela construída, ou seja, as diversas variáveis que contêm informação sobre tempos de geração de chaves, produção de assinaturas e verificação de assinaturas e tamanhos das chaves, pública e privada, e da assinatura.

ML-DSA

In [2]:
```
ml_dsa_44 = MLDSA(39, 128, 2 ** 17, 88, 4, 4, 2, 80)
kts44 = time.time()
pk44, sk44 = ml_dsa_44.ml_dsa_keygen()
kte44 = time.time()
ktime44 = "{:.2f}".format(kte44 - kts44)

ml_dsa_65 = MLDSA(49, 192, 2 ** 19, 32, 6, 5, 4, 55)
kts65 = time.time()
pk65, sk65 = ml_dsa_65.ml_dsa_keygen()
kte65 = time.time()
```

```
ktime65 = "{:.2f}".format(kte65 - kts65)

ml_dsa_87 = MLDSA(60, 256, 2 ** 19, 32, 8, 7, 2, 75)
kts87 = time.time()
pk87, sk87 = ml_dsa_87.ml_dsa_keygen()
kte87 = time.time()
ktime87 = "{:.2f}".format(kte87 - kts87)
```

SLH-DSA

In [3]:

```
sha2_128s = SLHDSA('SHA2', 's', 16, 63, 7, 9, 12, 14, 4, 30)
ktssha2_128s = time.time()
sksha2_128s, pksha2_128s = sha2_128s.slh_keygen()
ktesha2_128s = time.time()
ktimesha2_128s = "{:.2f}".format(ktesha2_128s - ktssha2_128s)
stssha2_128s = time.time()
ssha2_128s = sha2_128s.slh_sign(b"Messi, the GOAT!", sksha2_128s)
stesha2_128s = time.time()
stimesha2_128s = "{:.2f}".format(stesha2_128s - stssha2_128s)
vtssha2_128s = time.time()
sha2_128s.slh_verify(b"Messi, the GOAT!", ssha2_128s, pksha2_128s)
vtesha2_128s = time.time()
vtimesha2_128s = "{:.2f}".format(vtesha2_128s - vtssha2_128s)

shake_128s = SLHDSA('SHAKE', 's', 16, 63, 7, 9, 12, 14, 4, 30)
ktsshake_128s = time.time()
skshake_128s, pkshake_128s = shake_128s.slh_keygen()
kteshake_128s = time.time()
ktimeshake_128s = "{:.2f}".format(kteshake_128s - ktsshake_128s)
stsshake_128s = time.time()
sshake_128s = shake_128s.slh_sign(b"Messi, the GOAT!", skshake_128s)
steshake_128s = time.time()
stimeshake_128s = "{:.2f}".format(steshake_128s - stsshake_128s)
vtsshake_128s = time.time()
shake_128s.slh_verify(b"Messi, the GOAT!", sshake_128s, pkshake_128s)
vteshake_128s = time.time()
vtimeshake_128s = "{:.2f}".format(vteshake_128s - vtsshake_128s)

sha2_128f = SLHDSA('SHA2', 'f', 16, 66, 22, 3, 6, 33, 4, 34)
ktssha2_128f = time.time()
sksha2_128f, pksha2_128f = sha2_128f.slh_keygen()
ktesha2_128f = time.time()
ktimesha2_128f = "{:.2f}".format(ktesha2_128f - ktssha2_128f)
stssha2_128f = time.time()
ssha2_128f = sha2_128f.slh_sign(b"Messi, the GOAT!", sksha2_128f)
stesha2_128f = time.time()
stimesha2_128f = "{:.2f}".format(stesha2_128f - stssha2_128f)
vtssha2_128f = time.time()
sha2_128f.slh_verify(b"Messi, the GOAT!", ssha2_128f, pksha2_128f)
vtesha2_128f = time.time()
vtimesha2_128f = "{:.2f}".format(vtesha2_128f - vtssha2_128f)

shake_128f = SLHDSA('SHAKE', 'f', 16, 66, 22, 3, 6, 33, 4, 34)
ktsshake_128f = time.time()
skshake_128f, pkshake_128f = shake_128f.slh_keygen()
```

```
kteshake_128f = time.time()
ktimeshake_128f = "{:.2f}".format(kteshake_128f - ktsshake_128f)
stsshake_128f = time.time()
sshake_128f = shake_128f.slh_sign(b"Messi, the GOAT!", skshake_128f)
steshake_128f = time.time()
stimeshake_128f = "{:.2f}".format(steshake_128f - stsshake_128f)
vtsshake_128f = time.time()
shake_128f.slh_verify(b"Messi, the GOAT!", sshake_128f, pkshake_128f)
vteshake_128f = time.time()
vtimeshake_128f = "{:.2f}".format(vteshake_128f - vtsshake_128f)

sha2_192s = SLHDSA('SHA2', 's', 24, 63, 7, 9, 14, 17, 4, 39)
ktssha2_192s = time.time()
sksha2_192s, pksha2_192s = sha2_192s.slh_keygen()
ktesha2_192s = time.time()
ktimesha2_192s = "{:.2f}".format(ktesha2_192s - ktssha2_192s)
stssha2_192s = time.time()
ssha2_192s = sha2_192s.slh_sign(b"Messi, the GOAT!", sksha2_192s)
stesha2_192s = time.time()
stimesha2_192s = "{:.2f}".format(stesha2_192s - stssha2_192s)
vtssha2_192s = time.time()
sha2_192s.slh_verify(b"Messi, the GOAT!", ssha2_192s, pksha2_192s)
vtesha2_192s = time.time()
vtimesha2_192s = "{:.2f}".format(vtesha2_192s - vtssha2_192s)

shake_192s = SLHDSA('SHAKE', 's', 24, 63, 7, 9, 14, 17, 4, 39)
ktsshake_192s = time.time()
skshake_192s, pkshake_192s = shake_192s.slh_keygen()
kteshake_192s = time.time()
ktimeshake_192s = "{:.2f}".format(kteshake_192s - ktsshake_192s)
stsshake_192s = time.time()
sshake_192s = shake_192s.slh_sign(b"Messi, the GOAT!", skshake_192s)
steshake_192s = time.time()
stimeshake_192s = "{:.2f}".format(steshake_192s - stsshake_192s)
vtsshake_192s = time.time()
shake_192s.slh_verify(b"Messi, the GOAT!", sshake_192s, pkshake_192s)
vteshake_192s = time.time()
vtimeshake_192s = "{:.2f}".format(vteshake_192s - vtsshake_192s)

sha2_192f = SLHDSA('SHA2', 'f', 24, 66, 22, 3, 8, 33, 4, 42)
ktssha2_192f = time.time()
sksha2_192f, pksha2_192f = sha2_192f.slh_keygen()
ktesha2_192f = time.time()
ktimesha2_192f = "{:.2f}".format(ktesha2_192f - ktssha2_192f)
stssha2_192f = time.time()
ssha2_192f = sha2_192f.slh_sign(b"Messi, the GOAT!", sksha2_192f)
stesha2_192f = time.time()
stimesha2_192f = "{:.2f}".format(stesha2_192f - stssha2_192f)
vtssha2_192f = time.time()
sha2_192f.slh_verify(b"Messi, the GOAT!", ssha2_192f, pksha2_192f)
vtesha2_192f = time.time()
vtimesha2_192f = "{:.2f}".format(vtesha2_192f - vtssha2_192f)

shake_192f = SLHDSA('SHAKE', 'f', 24, 66, 22, 3, 8, 33, 4, 42)
ktsshake_192f = time.time()
skshake_192f, pkshake_192f = shake_192f.slh_keygen()
```

```
kteshake_192f = time.time()
ktimeshake_192f = "{:.2f}".format(kteshake_192f - ktsshake_192f)
stsshake_192f = time.time()
sshake_192f = shake_192f.slh_sign(b"Messi, the GOAT!", skshake_192f)
steshake_192f = time.time()
stimeshake_192f = "{:.2f}".format(steshake_192f - stsshake_192f)
vtsshake_192f = time.time()
shake_192f.slh_verify(b"Messi, the GOAT!", sshake_192f, pkshake_192f)
vteshake_192f = time.time()
vtimeshake_192f = "{:.2f}".format(vteshake_192f - vtsshake_192f)

sha2_256s = SLHDSA('SHA2', 's', 32, 64, 8, 8, 14, 22, 4, 47)
ktssha2_256s = time.time()
sksha2_256s, pksha2_256s = sha2_256s.slh_keygen()
ktesha2_256s = time.time()
ktimesha2_256s = "{:.2f}".format(ktesha2_256s - ktssha2_256s)
stssha2_256s = time.time()
ssha2_256s = sha2_256s.slh_sign(b"Messi, the GOAT!", sksha2_256s)
stesha2_256s = time.time()
stimesha2_256s = "{:.2f}".format(stesha2_256s - stssha2_256s)
vtssha2_256s = time.time()
sha2_256s.slh_verify(b"Messi, the GOAT!", ssha2_256s, pksha2_256s)
vtesha2_256s = time.time()
vtimesha2_256s = "{:.2f}".format(vtesha2_256s - vtssha2_256s)

shake_256s = SLHDSA('SHAKE', 's', 32, 64, 8, 8, 14, 22, 4, 47)
ktsshake_256s = time.time()
skshake_256s, pkshake_256s = shake_256s.slh_keygen()
kteshake_256s = time.time()
ktimeshake_256s = "{:.2f}".format(kteshake_256s - ktsshake_256s)
stsshake_256s = time.time()
sshake_256s = shake_256s.slh_sign(b"Messi, the GOAT!", skshake_256s)
steshake_256s = time.time()
stimeshake_256s = "{:.2f}".format(steshake_256s - stsshake_256s)
vtsshake_256s = time.time()
shake_256s.slh_verify(b"Messi, the GOAT!", sshake_256s, pkshake_256s)
vteshake_256s = time.time()
vtimeshake_256s = "{:.2f}".format(vteshake_256s - vtsshake_256s)

sha2_256f = SLHDSA('SHA2', 'f', 32, 68, 17, 4, 9, 35, 4, 49)
ktssha2_256f = time.time()
sksha2_256f, pksha2_256f = sha2_256f.slh_keygen()
ktesha2_256f = time.time()
ktimesha2_256f = "{:.2f}".format(ktesha2_256f - ktssha2_256f)
stssha2_256f = time.time()
ssha2_256f = sha2_256f.slh_sign(b"Messi, the GOAT!", sksha2_256f)
stesha2_256f = time.time()
stimesha2_256f = "{:.2f}".format(stesha2_256f - stssha2_256f)
vtssha2_256f = time.time()
sha2_256f.slh_verify(b"Messi, the GOAT!", ssha2_256f, pksha2_256f)
vtesha2_256f = time.time()
vtimesha2_256f = "{:.2f}".format(vtesha2_256f - vtssha2_256f)

shake_256f = SLHDSA('SHAKE', 'f', 32, 68, 17, 4, 9, 35, 4, 49)
ktsshake_256f = time.time()
skshake_256f, pkshake_256f = shake_256f.slh_keygen()
```

```
kteshake_256f = time.time()
ktimeshake_256f = "{:.2f}".format(kteshake_256f - ktsshake_256f)
stsshake_256f = time.time()
sshake_256f = shake_256f.slh_sign(b"Messi, the GOAT!", skshake_256f)
steshake_256f = time.time()
stimeshake_256f = "{:.2f}".format(steshake_256f - stsshake_256f)
vtsshake_256f = time.time()
shake_256f.slh_verify(b"Messi, the GOAT!", sshake_256f, pkshake_256f)
vteshake_256f = time.time()
vtimeshake_256f = "{:.2f}".format(vteshake_256f - vtsshake_256f)
```

Tabela de comparação de tempos (em segundos)

In [4]:

```
print('\n\n|----------------------|--------------------|-----------------------
print('|----------------------| Geração das chaves | Produção da assinatura
print('|----------------------|--------------------|-----------------------
print(f'|       ML-DSA-44      |     {ktime44: ^10}     |           ---
print(f'|       ML-DSA-65      |     {ktime65: ^10}     |           ---
print(f'|       ML-DSA-87      |     {ktime87: ^10}     |           ---
print(f'|   SLH-DSA-SHA2-128s  |     {ktimesha2_128s: ^10}     |       {stim
print(f'|  SLH-DSA-SHAKE-128s  |     {ktimeshake_128s: ^10}     |       {sti
print(f'|   SLH-DSA-SHA2-128f  |     {ktimesha2_128f: ^10}     |       {stim
print(f'|  SLH-DSA-SHAKE-128f  |     {ktimeshake_128f: ^10}     |       {sti
print(f'|   SLH-DSA-SHA2-192s  |     {ktimesha2_192s: ^10}     |       {stim
print(f'|  SLH-DSA-SHAKE-192s  |     {ktimeshake_192s: ^10}     |       {sti
print(f'|   SLH-DSA-SHA2-192f  |     {ktimesha2_192f: ^10}     |       {stim
print(f'|  SLH-DSA-SHAKE-192f  |     {ktimeshake_192f: ^10}     |       {sti
print(f'|   SLH-DSA-SHA2-256s  |     {ktimesha2_256s: ^10}     |       {stim
print(f'|  SLH-DSA-SHAKE-256s  |     {ktimeshake_256s: ^10}     |       {sti
print(f'|   SLH-DSA-SHA2-256f  |     {ktimesha2_256f: ^10}     |       {stim
print(f'|  SLH-DSA-SHAKE-256f  |     {ktimeshake_256f: ^10}     |       {sti
print('|----------------------|--------------------|-----------------------
```

```
|----------------------|--------------------|------------------------|------
--------------------|
|----------------------| Geração das chaves | Produção da assinatura | Verif
icação da assinatura |
|----------------------|--------------------|------------------------|------
--------------------|
|       ML-DSA-44      |       27.01        |           ---          |
---            |
|       ML-DSA-65      |       49.23        |           ---          |
---            |
|       ML-DSA-87      |       91.76        |           ---          |
---            |
|   SLH-DSA-SHA2-128s  |        1.69        |         12.71          |
0.01           |
|  SLH-DSA-SHAKE-128s  |        1.17        |          9.06          |
0.01           |
|   SLH-DSA-SHA2-128f  |        0.03        |          0.60          |
0.04           |
|  SLH-DSA-SHAKE-128f  |        0.02        |          0.43          |
0.03           |
|   SLH-DSA-SHA2-192s  |        2.34        |         21.71          |
0.02           |
|  SLH-DSA-SHAKE-192s  |        1.71        |         16.28          |
0.01           |
|   SLH-DSA-SHA2-192f  |        0.04        |          1.05          |
0.06           |
|  SLH-DSA-SHAKE-192f  |        0.03        |          0.74          |
0.04           |
|   SLH-DSA-SHA2-256s  |        1.56        |         19.68          |
0.03           |
|  SLH-DSA-SHAKE-256s  |        1.24        |         14.53          |
0.02           |
|   SLH-DSA-SHA2-256f  |        0.10        |          2.16          |
0.06           |
|  SLH-DSA-SHAKE-256f  |        0.08        |          1.52          |
0.04           |
|----------------------|--------------------|------------------------|------
--------------------|
```

Tabela de comparação de tamanhos (em bytes)

In [5]:
```
print('\n\n|----------------------|--------------------|--------------------
print('|----------------------|    Chave pública   |      Chave privada
print('|----------------------|--------------------|----------------------
print(f'|       ML-DSA-44      |     {len(pk44): ^10}     |       {len(sk44)
print(f'|       ML-DSA-65      |     {len(pk65): ^10}     |       {len(sk65)
print(f'|       ML-DSA-87      |     {len(pk87): ^10}     |       {len(sk87)
print(f'|   SLH-DSA-SHA2-128s  |     {len(pksha2_128s): ^10}     |       {le
print(f'|  SLH-DSA-SHAKE-128s  |     {len(pkshake_128s): ^10}     |       {l
print(f'|   SLH-DSA-SHA2-128f  |     {len(pksha2_128f): ^10}     |       {le
print(f'|  SLH-DSA-SHAKE-128f  |     {len(pkshake_128f): ^10}     |       {l
print(f'|   SLH-DSA-SHA2-192s  |     {len(pksha2_192s): ^10}     |       {le
print(f'|  SLH-DSA-SHAKE-192s  |     {len(pkshake_192s): ^10}     |       {l
print(f'|   SLH-DSA-SHA2-192f  |     {len(pksha2_192f): ^10}     |       {le
```

```
print(f'|  SLH-DSA-SHAKE-192f  |     {len(pkshake_192f): ^10}     |       {l
print(f'|   SLH-DSA-SHA2-256s  |     {len(pksha2_256s): ^10}     |       {le
print(f'|  SLH-DSA-SHAKE-256s  |     {len(pkshake_256s): ^10}     |       {l
print(f'|   SLH-DSA-SHA2-256f  |     {len(pksha2_256f): ^10}     |       {le
print(f'|  SLH-DSA-SHAKE-256f  |     {len(pkshake_256f): ^10}     |       {l
print('|----------------------|--------------------|-----------------------
```

```
|----------------------|--------------------|------------------------|------
----------------------|
|----------------------|    Chave pública   |      Chave privada     |
Assinatura        |
|----------------------|--------------------|------------------------|------
----------------------|
|       ML-DSA-44      |        1312        |          2560          |
---             |
|       ML-DSA-65      |        1952        |          4032          |
---             |
|       ML-DSA-87      |        2592        |          4896          |
---             |
|   SLH-DSA-SHA2-128s  |         32         |           64           |
7856            |
|  SLH-DSA-SHAKE-128s  |         32         |           64           |
7856            |
|   SLH-DSA-SHA2-128f  |         32         |           64           |
17088           |
|  SLH-DSA-SHAKE-128f  |         32         |           64           |
17088           |
|   SLH-DSA-SHA2-192s  |         48         |           96           |
16224           |
|  SLH-DSA-SHAKE-192s  |         48         |           96           |
16224           |
|   SLH-DSA-SHA2-192f  |         48         |           96           |
35664           |
|  SLH-DSA-SHAKE-192f  |         48         |           96           |
35664           |
|   SLH-DSA-SHA2-256s  |         64         |          128           |
29792           |
|  SLH-DSA-SHAKE-256s  |         64         |          128           |
29792           |
|   SLH-DSA-SHA2-256f  |         64         |          128           |
49856           |
|  SLH-DSA-SHAKE-256f  |         64         |          128           |
49856           |
|----------------------|--------------------|------------------------|------
----------------------|
```