$\mathcal{MQ}$Crypto Samples

Eliver Pérez Villegas
Edgar González Fernández
Departamento de Computación
Centro de Investigación y Estudios Avanzados del IPN

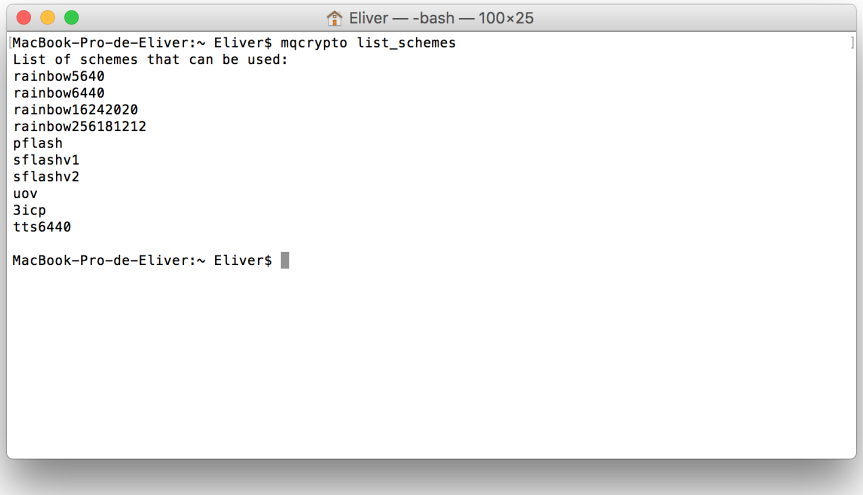
August 11, 2017

1 List of schemes

list_schemes can be used for printing the list of schemes in $\mathcal{MQ}$Crypto:

```
mqcrypto list_schemes
```

which would display in screen the following contents:



```
MacBook-Pro-de-Eliver:~ Eliver$ mqcrypto list_schemes
List of schemes that can be used:
rainbow5640
rainbow6440
rainbow16242020
rainbow256181212
pflash
sflashv1
sflashv2
uov
3icp
tts6440

MacBook-Pro-de-Eliver:~ Eliver$
```

2 Rainbow5640

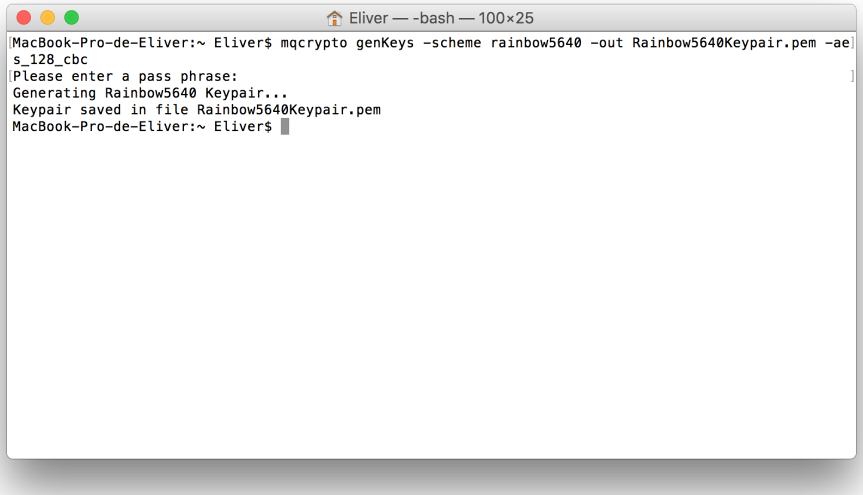
2.1 Key generation

The following instruction:

```
mqcrypto genKeys -scheme rainbow5640 -out Rainbow5640Keypair.pem
     -aes_128_cbc -passout pass:password
```

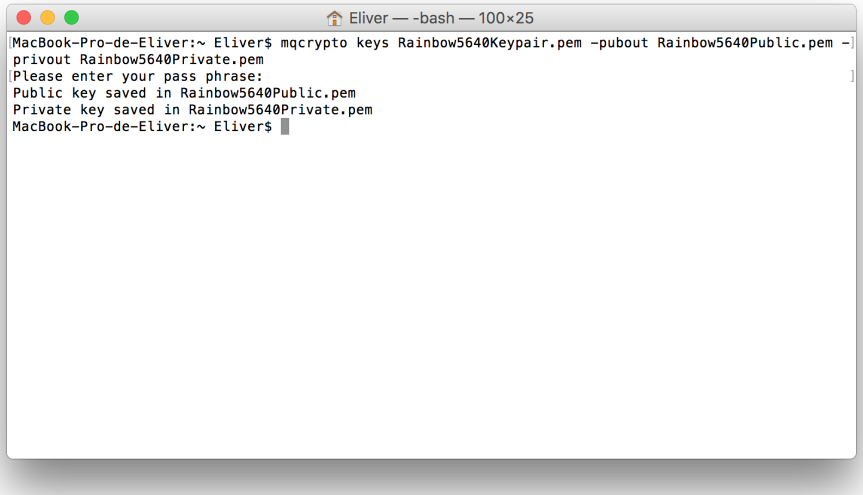
can be used to create a new set of keys of the `rainbow5640` schemes. Once executed the `genKeys` instruction, a message will be displayed describing the execution status. The `-passout` option is optional, the password can be asked for input once executed the keys generation instruction. For the symmetric encryption algorithm, the following can be used:

- -aes_128_cbc
- -aes_128_ecb
- -aes_192_cbc
- -aes_192_ecb
- -aes_256_cbc
- -aes_256_ecb



```
MacBook-Pro-de-Eliver:~ Eliver$ mqcrypto genKeys -scheme rainbow5640 -out Rainbow5640Keypair.pem -ae
s_128_cbc
Please enter a pass phrase:
Generating Rainbow5640 Keypair...
Keypair saved in file Rainbow5640Keypair.pem
MacBook-Pro-de-Eliver:~ Eliver$
```

The key generation can also output a zip file using the `-zip` option, the compression algorithm used is `bzip2`.



```
MacBook-Pro-de-Eliver:~ Eliver$ mqcrypto keys Rainbow5640Keypair.pem -pubout Rainbow5640Public.pem -
privout Rainbow5640Private.pem
Please enter your pass phrase:
Public key saved in Rainbow5640Public.pem
Private key saved in Rainbow5640Private.pem
MacBook-Pro-de-Eliver:~ Eliver$
```

3 Extract keys

The `keys` instruction can be used for extracting the public and private key from the keypair generated.

```
mqcrypto keys Rainbow5640Keypair.pem -pubout Rainbow5640Public.pem
-privout Rainbow5640Private.pem -passin pass:password
```

using the keypair stored in `Rainbow5640Keypair.pem`, extracts the public key in the `Rainbow5640Public.pem` file and the private key in `Rainbow5640Private.pem`. The password can be used in the `keys` line, otherwise, it will be asked for input once the extraction is executed. The keys can also be compressed using `bzip2`, with the `-zip` option.

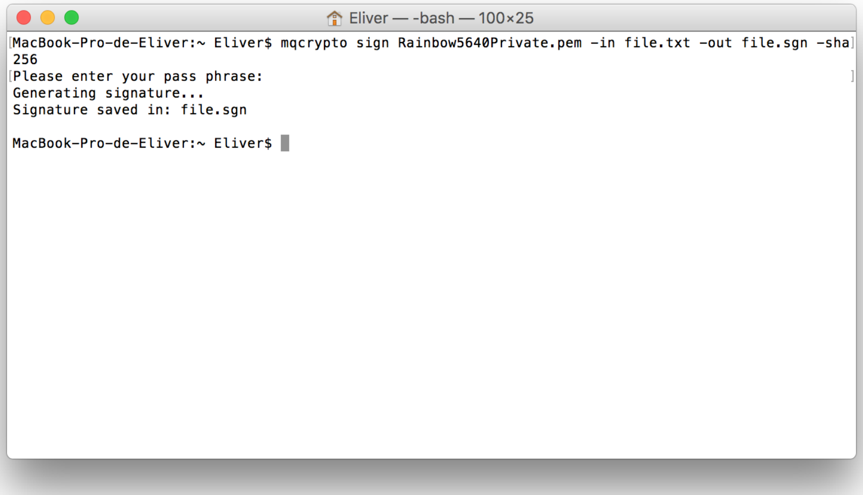
4 Signature

Signing a document can be done with the `sign` function, either using the Keypair or the private key after extracting it:

```
mqcrypto sign Rainbow5640Private.pem -in file.txt -out file.sgn
-sha256 -passin pass:password
```

the input `file.txt` will be signed and the signature will be stored in the `file.sgn`.

The following digest algorithms can be used in $\mathcal{MQ}$`Crypto`:



```
MacBook-Pro-de-Eliver:~ Eliver$ mqcrypto sign Rainbow5640Private.pem -in file.txt -out file.sgn -sha
256
Please enter your pass phrase:
Generating signature...
Signature saved in: file.sgn

MacBook-Pro-de-Eliver:~ Eliver$
```

- sha256
- sha512

5 Verification

For verifying a signature, the `verify` function is used:

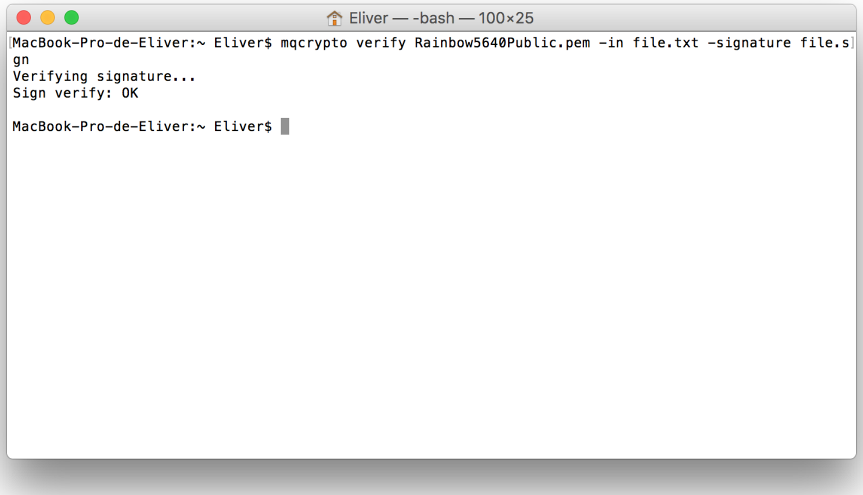
```
mqcrypto verify Rainbow5640Public.pem -in file.txt -signature file.sgn
```

which would use the public key in the `Rainbow5640Public.pem` file for verifying the signature of the `file.txt` stored in `file.sgn`.

A help menu can be shown for each function by using the `help` flag.

6 Instruction list

```
---------------------------------------------------------------------
RAINBOW5640
---------------------------------------------------------------------
```



```
MacBook-Pro-de-Eliver:~ Eliver$ mqcrypto verify Rainbow5640Public.pem -in file.txt -signature file.s
gn
Verifying signature...
Sign verify: OK

MacBook-Pro-de-Eliver:~ Eliver$
```

```
mqcrypto genKeys -scheme rainbow5640 -out Rainbow5640Keypair.pem
-passout pass:password

mqcrypto keys Rainbow5640Keypair.pem -pubout rainbow5640-public-key.pem
-privout rainbow5640-private-key.pem -passin pass:password

mqcrypto sign Rainbow5640Keypair.pem -in file.txt -out Rainbow5640Signed.txt
-sha512 -passin pass:password

mqcrypto sign rainbow5640-private-key.pem -in file.txt
-out Rainbow5640SignedPrivate.txt -sha512 -passin pass:password

mqcrypto verify Rainbow5640Keypair.pem -in file.txt
-signature Rainbow5640Signed.txt -passin pass:password

mqcrypto verify Rainbow5640Keypair.pem -in file.txt
-signature Rainbow5640SignedPrivate.txt -passin pass:password

mqcrypto verify rainbow5640-public-key.pem -in file.txt
-signature Rainbow5640Signed.txt

mqcrypto verify rainbow5640-public-key.pem -in file.txt
-signature Rainbow5640SignedPrivate.txt
```

```
------------------------------------------------------------------------
RAINBOW6440
------------------------------------------------------------------------

mqcrypto genKeys -scheme rainbow6440 -out Rainbow6440Keypair.pem
-passout pass:password

mqcrypto keys Rainbow6440Keypair.pem -pubout rainbow6440-public-key.pem
-privout rainbow6440-private-key.pem -passin pass:password

mqcrypto sign Rainbow6440Keypair.pem -in file.txt -out Rainbow6440Signed.txt
-sha512 -passin pass:password

mqcrypto sign rainbow6440-private-key.pem -in file.txt
-out Rainbow6440SignedPrivate.txt -sha512 -passin pass:password

mqcrypto verify Rainbow6440Keypair.pem -in file.txt
-signature Rainbow6440Signed.txt -passin pass:password

mqcrypto verify Rainbow6440Keypair.pem -in file.txt
-signature Rainbow6440SignedPrivate.txt -passin pass:password

mqcrypto verify rainbow6440-public-key.pem -in file.txt
-signature Rainbow6440Signed.txt

mqcrypto verify rainbow6440-public-key.pem -in file.txt
-signature Rainbow6440SignedPrivate.txt


------------------------------------------------------------------------
RAINBOW16242020
------------------------------------------------------------------------

mqcrypto genKeys -scheme rainbow16242020 -out Rainbow16242020Keypair.pem
-passout pass:password

mqcrypto keys Rainbow16242020Keypair.pem -pubout rainbow16242020-public-key.pem
-privout rainbow16242020-private-key.pem -passin pass:password

mqcrypto sign Rainbow16242020Keypair.pem -in file.txt
-out Rainbow16242020Signed.txt -sha512 -passin pass:password

mqcrypto sign rainbow16242020-private-key.pem -in file.txt
-out Rainbow16242020SignedPrivate.txt -sha512 -passin pass:password

mqcrypto verify Rainbow16242020Keypair.pem -in file.txt
```

```
-signature Rainbow16242020Signed.txt -passin pass:password

mqcrypto verify Rainbow16242020Keypair.pem -in file.txt
-signature Rainbow16242020SignedPrivate.txt -passin pass:password

mqcrypto verify rainbow16242020-public-key.pem -in file.txt
-signature Rainbow16242020Signed.txt

mqcrypto verify rainbow16242020-public-key.pem -in file.txt
-signature Rainbow16242020SignedPrivate.txt


------------------------------------------------------------------------
RAINBOW256181212
------------------------------------------------------------------------

mqcrypto genKeys -scheme rainbow256181212 -out Rainbow256181212Keypair.pem
-passout pass:password

mqcrypto keys Rainbow256181212Keypair.pem -pubout rainbow256181212-public-key.pem
-privout rainbow256181212-private-key.pem -passin pass:password

mqcrypto sign Rainbow256181212Keypair.pem -in file.txt
-out Rainbow256181212Signed.txt -sha512 -passin pass:password

mqcrypto sign rainbow256181212-private-key.pem -in file.txt
-out Rainbow256181212SignedPrivate.txt -sha512 -passin pass:password

mqcrypto verify Rainbow256181212Keypair.pem -in file.txt
-signature Rainbow256181212Signed.txt -passin pass:password

mqcrypto verify Rainbow256181212Keypair.pem -in file.txt
-signature Rainbow256181212SignedPrivate.txt -passin pass:password

mqcrypto verify rainbow256181212-public-key.pem -in file.txt
-signature Rainbow256181212Signed.txt

mqcrypto verify rainbow256181212-public-key.pem -in file.txt
-signature Rainbow256181212SignedPrivate.txt


------------------------------------------------------------------------
PFLASH
------------------------------------------------------------------------

mqcrypto genKeys -scheme pflash -out pflashKeypair.pem -passout pass:password
mqcrypto keys pflashKeypair.pem -pubout pflash-public-key.pem
-privout pflash-private-key.pem -passin pass:password

mqcrypto sign pflashKeypair.pem -in file.txt -out pflashSigned.txt -sha512
-passin pass:password

mqcrypto sign pflash-private-key.pem -in file.txt -out pflashSignedPrivate.txt
-sha512 -passin pass:password

mqcrypto verify pflashKeypair.pem -in file.txt -signature pflashSigned.txt
-passin pass:password

mqcrypto verify pflashKeypair.pem -in file.txt -signature pflashSignedPrivate.txt
-passin pass:password

mqcrypto verify pflash-public-key.pem -in file.txt -signature pflashSigned.txt

mqcrypto verify pflash-public-key.pem -in file.txt -signature pflashSignedPrivate.txt

------------------------------------------------------------------------
TTS6440
------------------------------------------------------------------------

mqcrypto genKeys -scheme tts6440 -out tts6440Keypair.pem -passout pass:password

mqcrypto keys tts6440Keypair.pem -pubout tts6440-public-key.pem
-privout tts6440-private-key.pem -passin pass:password

mqcrypto sign tts6440Keypair.pem -in file.txt -out tts6440Signed.txt -sha512
-passin pass:password

mqcrypto sign tts6440-private-key.pem -in file.txt -out tts6440SignedPrivate.txt
-sha512 -passin pass:password

mqcrypto verify tts6440Keypair.pem -in file.txt -signature tts6440Signed.txt
-passin pass:password

mqcrypto verify tts6440Keypair.pem -in file.txt -signature tts6440SignedPrivate.txt
-passin pass:password

mqcrypto verify tts6440-public-key.pem -in file.txt -signature tts6440Signed.txt

mqcrypto verify tts6440-public-key.pem -in file.txt -signature tts6440SignedPrivate.txt
```

```
------------------------------------------------------------------------
3ICP
------------------------------------------------------------------------

mqcrypto genKeys -scheme 3icp -out 3icpKeypair.pem -passout pass:password

mqcrypto keys 3icpKeypair.pem -pubout 3icp-public-key.pem -privout 3icp-private-key.pem
-passin pass:password

mqcrypto sign 3icpKeypair.pem -in file.txt -out 3icpSigned.txt -sha512
-passin pass:password

mqcrypto sign 3icp-private-key.pem -in file.txt -out 3icpSignedPrivate.txt
-sha512 -passin pass:password

mqcrypto verify 3icpKeypair.pem -in file.txt -signature 3icpSigned.txt
-passin pass:password

mqcrypto verify 3icpKeypair.pem -in file.txt -signature 3icpSignedPrivate.txt
-passin pass:password

mqcrypto verify 3icp-public-key.pem -in file.txt -signature 3icpSigned.txt

mqcrypto verify 3icp-public-key.pem -in file.txt -signature 3icpSignedPrivate.txt


------------------------------------------------------------------------
SFLASHV1
------------------------------------------------------------------------

mqcrypto genKeys -scheme sflashv1 -out sflashv1Keypair.pem -passout pass:password

mqcrypto keys sflashv1Keypair.pem -pubout sflashv1-public-key.pem
-privout sflashv1-private-key.pem -passin pass:password

mqcrypto sign sflashv1Keypair.pem -in file.txt -out sflashv1Signed.txt
-sha512 -passin pass:password

mqcrypto sign sflashv1-private-key.pem -in file.txt -out sflashv1SignedPrivate.txt
-sha512 -passin pass:password

mqcrypto verify sflashv1Keypair.pem -in file.txt
-signature sflashv1Signed.txt -passin pass:password

mqcrypto verify sflashv1Keypair.pem -in file.txt
-signature sflashv1SignedPrivate.txt -passin pass:password
```

```
mqcrypto verify sflashv1-public-key.pem -in file.txt
-signature sflashv1Signed.txt

mqcrypto verify sflashv1-public-key.pem -in file.txt
-signature sflashv1SignedPrivate.txt


------------------------------------------------------------------------
SFLASHV2
------------------------------------------------------------------------

mqcrypto genKeys -scheme sflashv2 -out sflashv2Keypair.pem -passout pass:password

mqcrypto keys sflashv2Keypair.pem -pubout sflashv2-public-key.pem
-privout sflashv2-private-key.pem -passin pass:password

mqcrypto sign sflashv2Keypair.pem -in file.txt -out sflashv2Signed.txt -sha512
-passin pass:password

mqcrypto sign sflashv2-private-key.pem -in file.txt -out sflashv2SignedPrivate.txt
-sha512 -passin pass:password

mqcrypto verify sflashv2Keypair.pem -in file.txt
-signature sflashv2Signed.txt -passin pass:password

mqcrypto verify sflashv2Keypair.pem -in file.txt
-signature sflashv2SignedPrivate.txt -passin pass:password

mqcrypto verify sflashv2-public-key.pem -in file.txt
-signature sflashv2Signed.txt

mqcrypto verify sflashv2-public-key.pem -in file.txt
-signature sflashv2SignedPrivate.txt


------------------------------------------------------------------------
UOV
------------------------------------------------------------------------

mqcrypto genKeys -scheme uov -out uovKeypair.pem -passout pass:password

mqcrypto keys uovKeypair.pem -pubout uov-public-key.pem -privout uov-private-key.pem
-passin pass:password

mqcrypto sign uovKeypair.pem -in file.txt -out uovSigned.txt -sha512
```

```
-passin pass:password

mqcrypto sign uov-private-key.pem -in file.txt -out uovSignedPrivate.txt -sha512
-passin pass:password

mqcrypto verify uovKeypair.pem -in file.txt
-signature uovSigned.txt -passin pass:password

mqcrypto verify uovKeypair.pem -in file.txt
-signature uovSignedPrivate.txt -passin pass:password

mqcrypto verify uov-public-key.pem -in file.txt
-signature uovSigned.txt

mqcrypto verify uov-public-key.pem -in file.txt
-signature uovSignedPrivate.txt
```