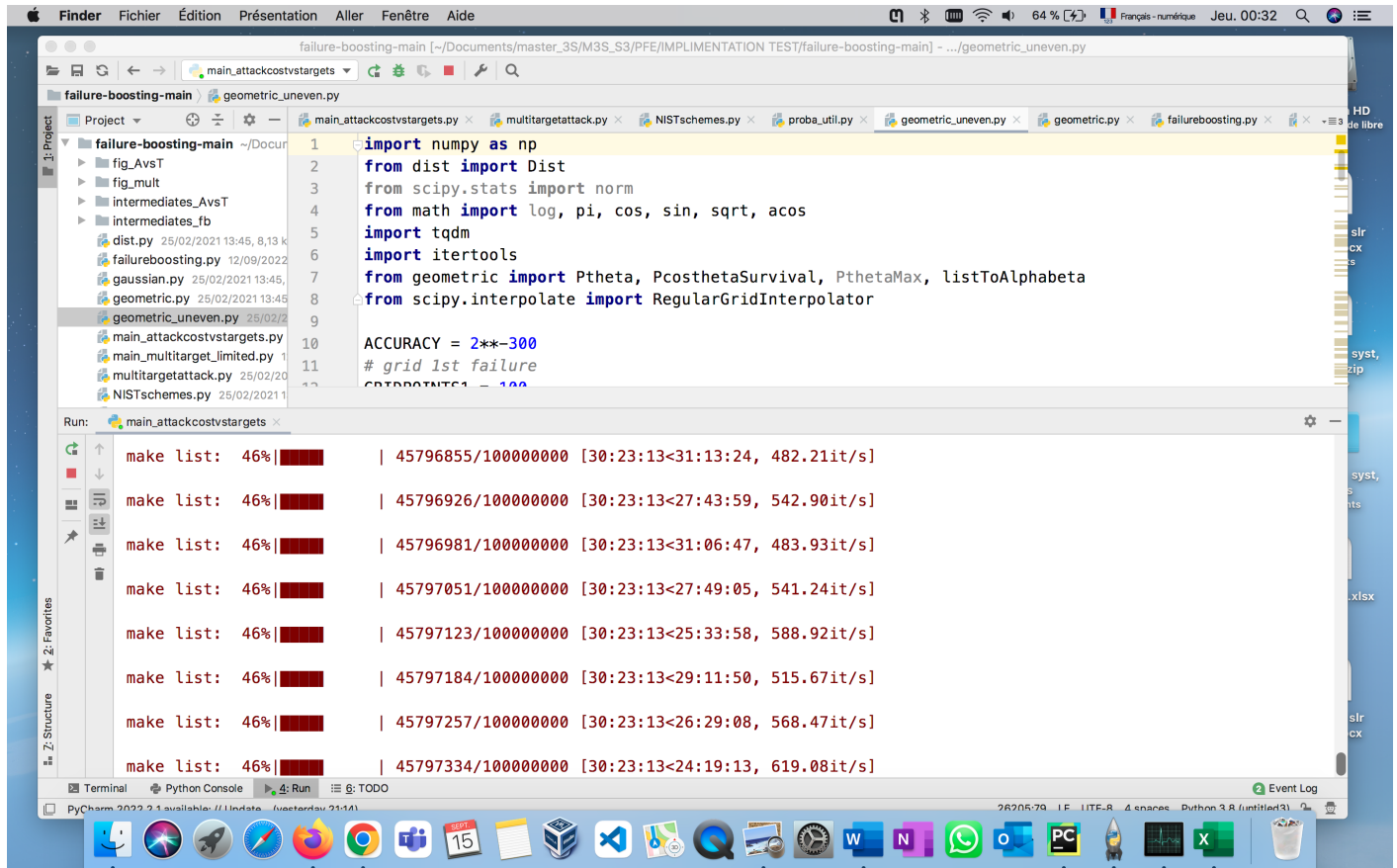


From: Fatima ASEBRIY <fatima.asebriy@gmail.com> via pqc-forum@list.nist.gov
To: [pqc-forum](mailto:pqc-forum@list.nist.gov) <pqc-forum@list.nist.gov>
Subject: [pqc-forum] Decryption Failure Attacks,(LWE/RLWE)
Date: Wednesday, September 14, 2022 07:35:41 PM ET
Attachments: [Capture decran 2022-09-15 a 00.32.47.png](#)



The screenshot shows a PyCharm IDE window with a project named 'failure-boosting-main'. The file explorer on the left shows a directory structure with files like 'fig_AvsT', 'fig_mult', 'intermediates_AvsT', 'intermediates_fb', 'dist.py', 'failureboosting.py', 'gaussian.py', 'geometric.py', 'geometric_uneven.py', 'main_attackcoststargets.py', 'main_multitarget_limited.py', 'multitargetattack.py', and 'NISTschemes.py'. The main editor displays the code in 'main_attackcoststargets.py', which includes imports for numpy, scipy, and math, and defines a function 'make_list' that iterates over a range of values and calculates a cost. The Run console at the bottom shows the output of the 'make_list' function, displaying progress bars and timing information for each iteration.

```
1 import numpy as np
2 from dist import Dist
3 from scipy.stats import norm
4 from math import log, pi, cos, sin, sqrt, acos
5 import tqdm
6 import itertools
7 from geometric import Ptheta, PcosthetaSurvival, PthetaMax, listToAlphabet
8 from scipy.interpolate import RegularGridInterpolator
9
10 ACCURACY = 2**-300
11 # grid 1st failure
12 COSTBOOSTING = 100
```

Run: main_attackcoststargets

Iteration	Progress	Value	Time
1	46%	45796855/100000000	[30:23:13<31:13:24, 482.21it/s]
2	46%	45796926/100000000	[30:23:13<27:43:59, 542.90it/s]
3	46%	45796981/100000000	[30:23:13<31:06:47, 483.93it/s]
4	46%	45797051/100000000	[30:23:13<27:49:05, 541.24it/s]
5	46%	45797123/100000000	[30:23:13<25:33:58, 588.92it/s]
6	46%	45797184/100000000	[30:23:13<29:11:50, 515.67it/s]
7	46%	45797257/100000000	[30:23:13<26:29:08, 568.47it/s]
8	46%	45797334/100000000	[30:23:13<24:19:13, 619.08it/s]

good evening my teacher

I hope you are well

Sir I found an implementation on decryption failure, I tried to execute it locally on my machine, I launched the execution and it is almost 3 days, it is still processing.

sir please, if it is possible to advise me if this implementation is good to test it?

Do you know of any other implementation regarding attack against LWE better.

You can explain to me why this implementation is very late except physical condition of my pc, are there problems at the level of calculation or something else

thank you in advance sir

<https://github.com/KULeuven-COSIC/failure-boosting>

--

You received this message because you are subscribed to the Google Groups "pqc-forum" group.

To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.

To view this discussion on the web visit <https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/3398b255-b3d9-41d9-9b2d-a1f8aacca21dn%40list.nist.gov>.

From: Jan-Pieter D'Anvers <janpieter.danvers@esat.kuleuven.be> via pgc-forum@list.nist.gov
To: pgc-forum@list.nist.gov
Subject: Re: [pgc-forum] Decryption Failure Attacks,(LWE/RLWE)
Date: Tuesday, September 20, 2022 07:33:04 AM ET

Hi Fatima,

I'm the author of this code.

As the README file states:

"Generation of failure boosting curves is costly, but should be done only once (intermediate results are saved). As such running the main functions for the first time will take approximately 1 day to 1 week of time per scheme and per set of constraints."

Depending on the scheme, the computations can indeed be very slow, 3 days is certainly not unexpected for some schemes. The results are stored and you should be able to re-use them later to speed up the computers.

If you have any further questions you can always direct them to me.

Best regards,

Jan-Pieter

On 15/09/2022 01:35, Fatima ASEBRIY wrote:

good evening my teacher

I hope you are well

Sir I found an implementation on decryption failure, I tried to execute it locally on my machine, I launched the execution and it is almost 3 days, it is still processing.

sir please, if it is possible to advise me if this implementation is good to test it?

Do you know of any other implementation regarding attack against LWE better.

You can explain to me why this implementation is very late except physical condition of my pc, are there problems at the level of calculation or something else
thank you in advance sir

<https://github.com/KULeuven-COSIC/failure-boosting>

--

You received this message because you are subscribed to the Google Groups "pqc-forum" group.

To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.

To view this discussion on the web visit <https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/3398b255-b3d9-41d9-9b2d-a1f8aacca21dn%40list.nist.gov>.

From: Fatima ASEBRIY <fatima.asebriy@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
CC: janpiete...@esat.kuleuven.be <janpieter.danvers@esat.kuleuven.be>
Subject: Re: [pqc-forum] Decryption Failure Attacks,(LWE/RLWE)
Date: Thursday, September 22, 2022 08:01:32 PM ET

Thank you Sir for the time you gave me to answer. Concerning the program, I left it for a week while reading the instructions, but I got no results, and as my computer suffers from working 24 hours a day, that's why I had to stop it...

If you have time Sir please help me Compare this type of attack to kyber and saber, and which we will consider most protective against decryption failure

Best regards,

ASE

Le mardi 20 septembre 2022 à 12:32:56 UTC+1, janpiete...@esat.kuleuven.be a écrit :

Hi Fatima,

I'm the author of this code.

As the README file states:

"Generation of failure boosting curves is costly, but should be done only once (intermediate results are saved). As such running the main functions for the first time will take approximately 1 day to 1 week of time per scheme and per set of constraints."

Depending on the scheme, the computations can indeed be very slow, 3 days is certainly not unexpected for some schemes. The results are stored and you should be able to re-use them later to speed up the computers.

If you have any further questions you can always direct them to me.

Best regards,

Jan-Pieter

On 15/09/2022 01:35, Fatima ASEBRIY wrote:

Capture d'écran 2022-09-15 à 00.32.47.png

good evening my teacher

I hope you are well

Sir I found an implementation on decryption failure, I tried to execute it locally on my machine, I launched the execution and it is almost 3 days, it is still processing.

sir please, if it is possible to advise me if this implementation is good to test it?

Do you know of any other implementation regarding attack against LWE better.

You can explain to me why this implementation is very late except physical condition of my pc, are there problems at the level of calculation or something else

thank you in advance sir

<https://github.com/KULeuven-COSIC/failure-boosting>

--

You received this message because you are subscribed to the Google Groups "pqc-forum" group.

To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+...@list.nist.gov.

To view this discussion on the web visit <https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/3398b255-b3d9-41d9-9b2d-a1f8aacca21dn%40list.nist.gov>.

--

You received this message because you are subscribed to the Google Groups "pqc-forum" group.

To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.

To view this discussion on the web visit <https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/79518a28-336a-4a48-b4f8-4c072d8dbf81n%40list.nist.gov>.

From: Fatima ASEBRIY <fatima.asebriy@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] Decryption Failure Attacks,(LWE/RLWE)
Date: Friday, September 23, 2022 12:09:54 PM ET

In Kyber round 3 specification, the table 4 gave the security estimates of Primal and Dual attack with respect to Kyber 512, 768 and 1024 (see the figure below). However, using the python script given in the paper (see the [github](#), run *Kyber.py*), it seems that I cannot reproduce the same result (however the numbers are very closed). I cannot figure out the reason, need help.

The result I get by this script is:

```
Kyber512 (light): ----- security: Primal attacks uses block-size 406 and
486 samples; dim d=999 Primal & 486 & 406 & 118 & 107 & 84 Dual attacks uses block-size
403 and 512 samples; dim d=1024 shortest vector used has length l=3294.02, q=3329,
`l<q`= 1 log2(epsilon) = -41.82, log2 nvector per run 83.63 Dual & 512 & 403 & 117 &
106 & 83 params: {'n': 256, 'm': 2, 'ks': 3, 'ke': 3, 'ke_ct': 2, 'q': 3329, 'rqk':
4096, 'rqc': 1024, 'rq2': 16} com costs: (800.0, 768.0) failure: 0.0 = 2^-139.1
Kyber768 (recommended): ----- security: Primal attacks uses block-size
626 and 650 samples; dim d=1419 Primal & 650 & 626 & 183 & 166 & 129 Dual attacks uses
block-size 620 and 650 samples; dim d=1418 shortest vector used has length l=5003.21,
q=3329, `l<q`= 0 log2(epsilon) = -64.32, log2 nvector per run 128.66 Dual & 650 & 620 &
181 & 164 & 128 params: {'n': 256, 'm': 3, 'ks': 2, 'ke': 2, 'ke_ct': 2, 'q': 3329,
'rqk': 4096, 'rqc': 1024, 'rq2': 16} com costs: (1184.0, 1088.0) failure: 0.0 =
2^-165.2
Kyber1024 (paranoid): ----- security: Primal attacks uses
block-size 878 and 860 samples; dim d=1885 Primal & 860 & 878 & 256 & 232 & 182 Dual
attacks uses block-size 868 and 838 samples; dim d=1862 shortest vector used has length
l=5920.11, q=3329, `l<q`= 0 log2(epsilon) = -90.06, log2 nvector per run 180.13 Dual &
838 & 868 & 253 & 230 & 180 params: {'n': 256, 'm': 4, 'ks': 2, 'ke': 2, 'ke_ct': 2,
'q': 3329, 'rqk': 4096, 'rqc': 2048, 'rq2': 32} com costs: (1568.0, 1568.0) failure:
0.0 = 2^-175.2
```

Le ven. 23 sept. 2022 à 01:01, Fatima ASEBRIY <fatima.asebriy@gmail.com> a écrit :

Thank you Sir for the time you gave me to answer. Concerning the program, I left it for a week while reading the instructions, but I got no results, and as my computer suffers from working 24 hours a day, that's why I had to stop it...

If you have time Sir please help me Compare this type of attack to kyber and saber, and which we will consider most protective against decryption failure

Best regards,

ASE

Le mardi 20 septembre 2022 à 12:32:56 UTC+1, janpiete...@esat.kuleuven.be a écrit :

Hi Fatima,

I'm the author of this code.

As the README file states:

"Generation of failure boosting curves is costly, but should be done only once (intermediate results are saved). As such running the main functions for the first time will take approximately 1 day to 1 week of time per scheme and per set of constraints."

Depending on the scheme, the computations can indeed be very slow, 3 days is certainly not unexpected for some schemes. The results are stored and you should be able to re-use them later to speed up the computers.

If you have any further questions you can always direct them to me.

Best regards,

Jan-Pieter

On 15/09/2022 01:35, Fatima ASEBRIY wrote:

Capture d'écran 2022-09-15 à 00.32.47.png

good evening my teacher

I hope you are well

Sir I found an implementation on decryption failure, I tried to execute it locally on my machine, I launched the execution and it is almost 3 days, it is still processing.

sir please, if it is possible to advise me if this implementation is good to test it? Do you know of any other implementation regarding attack against LWE better.

You can explain to me why this implementation is very late except physical condition of my pc, are there problems at the level of calculation or something

else

thank you in advance sir

<https://github.com/KULeuven-COSIC/failure-boosting>

--

You received this message because you are subscribed to the Google Groups "pqc-forum" group.

To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+...@list.nist.gov.

To view this discussion on the web visit <https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/3398b255-b3d9-41d9-9b2d-a1f8aacca21dn%40list.nist.gov>.

--

You received this message because you are subscribed to the Google Groups "pqc-forum" group.

To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.

To view this discussion on the web visit <https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/79518a28-336a-4a48-b4f8-4c072d8dbf81n%40list.nist.gov>.

--

Cordialement

ASEBRIY FATIMA

*Master de recherche **M3S_TA***

Master Sécurité Systèmes et Services

Université Mohammed V, ENSIAS

Rabat, Maroc

--

You received this message because you are subscribed to the Google Groups "pqc-forum" group.

To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.

To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/CAG_Shvw9p9TnOoTSc7hcq3BB3N9zh3EFegFa%2BUQokQwW%3D9UBMw%40mail.gmail.com.

From: Peter Schwabe <peter@cryptojedi.org> via pqc-forum@list.nist.gov
To: Fatima ASEBRIY <fatima.asebriy@gmail.com>
CC: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Decryption Failure Attacks,(LWE/RLWE)
Date: Saturday, September 24, 2022 02:35:47 AM ET

Fatima ASEBRIY <fatima.asebriy@gmail.com> wrote:

Dear Fatima,

> In Kyber round 3 specification, the table 4 gave the security estimates of
> Primal and Dual attack with respect to Kyber 512, 768 and 1024 (see the
> figure below). However, using the python script given in the paper (see the
> github <<https://github.com/pq-crystals/security-estimates>>, run *Kyber.py*),
> it seems that I cannot reproduce the same result (however the numbers are
> very closed). I cannot figure out the reason, need help.

What numbers do you think don't match? I'm looking at Table 4 on page 21
of <https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fpq-crystals.org%2Fkyber%2Fdata%2Fkyber-specification-round3-20210804.pdf&data=05%7C01%7Cyi-kai.liu%40nist.gov%7Cba20d1d20f53487536c508da9df70213%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637995981469469533%7CUnknown%7CTWFPbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Iik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=H0GOZEIjWhgNMzNrL0t7dgylWhGJXVjuyyXZ6nNMxaM%3D&reserved=0>
and compare those numbers with the "Primal" lines in the Kyber.py
output, but I don't see where they don't match.

All the best,

Peter

>
>
>
> The result I get by this script is:
>
> Kyber512 (light):

```
> _____
> security:
> Primal attacks uses block-size 406 and 486 samples; dim d=999
> Primal & 486 & 406 & 118 & 107 & 84
> Dual attacks uses block-size 403 and 512 samples; dim d=1024
> shortest vector used has length l=3294.02, q=3329, `l<q`= 1
> log2(epsilon) = -41.82, log2 nvector per run 83.63
> Dual & 512 & 403 & 117 & 106 & 83
> params: {'n': 256, 'm': 2, 'ks': 3, 'ke': 3, 'ke_ct': 2, 'q': 3329,
> 'rqk': 4096, 'rqc': 1024, 'rq2': 16}
> com costs: (800.0, 768.0)
> failure: 0.0 = 2^-139.1
>
> Kyber768 (recommended):
> _____
> security:
> Primal attacks uses block-size 626 and 650 samples; dim d=1419
> Primal & 650 & 626 & 183 & 166 & 129
> Dual attacks uses block-size 620 and 650 samples; dim d=1418
> shortest vector used has length l=5003.21, q=3329, `l<q`= 0
> log2(epsilon) = -64.32, log2 nvector per run 128.66
> Dual & 650 & 620 & 181 & 164 & 128
> params: {'n': 256, 'm': 3, 'ks': 2, 'ke': 2, 'ke_ct': 2, 'q': 3329,
> 'rqk': 4096, 'rqc': 1024, 'rq2': 16}
> com costs: (1184.0, 1088.0)
> failure: 0.0 = 2^-165.2
>
> Kyber1024 (paranoid):
> _____
> security:
> Primal attacks uses block-size 878 and 860 samples; dim d=1885
> Primal & 860 & 878 & 256 & 232 & 182
> Dual attacks uses block-size 868 and 838 samples; dim d=1862
> shortest vector used has length l=5920.11, q=3329, `l<q`= 0
> log2(epsilon) = -90.06, log2 nvector per run 180.13
> Dual & 838 & 868 & 253 & 230 & 180
> params: {'n': 256, 'm': 4, 'ks': 2, 'ke': 2, 'ke_ct': 2, 'q': 3329,
```

```
> 'rqk': 4096, 'rqc': 2048, 'rq2': 32}
> com costs: (1568.0, 1568.0)
> failure: 0.0 = 2^-175.2
>
>
>
> Le ven. 23 sept. 2022 à 01:01, Fatima ASEBRIY <fatima.asebriy@gmail.com> a
> écrit :
>
> > Thank you Sir for the time you gave me to answer. Concerning the program,
> > I left it for a week while reading the instructions, but I got no results,
> > and as my computer suffers from working 24 hours a day, that's why I had
> > to stop it...
> > If you have time Sir please help me Compare this type of attack to kyber
> > and saber, and which we will consider most protective against decryption
> > failure
> >
> > Best regards,
> >
> > ASE
> >
> > Le mardi 20 septembre 2022 à 12:32:56 UTC+1, janpiete...@esat.kuleuven.be
> > a écrit :
> >
> >> Hi Fatima,
> >>
> >> I'm the author of this code.
> >>
> >> As the README file states:
> >> "Generation of failure boosting curves is costly, but should be done only
> >> once (intermediate results are saved). As such running the main functions
> >> for the first time will take approximately 1 day to 1 week of time per
> >> scheme and per set of constraints."
> >>
> >> Depending on the scheme, the computations can indeed be very slow, 3 days
> >> is certainly not unexpected for some schemes. The results are stored and
> >> you should be able to re-use them later to speed up the computers.
```

> >>
> >> If you have any further questions you can always direct them to me.
> >>
> >> Best regards,
> >>
> >> Jan-Pieter
> >> On 15/09/2022 01:35, Fatima ASEBRIY wrote:
> >>
> >> [image: Capture d'écran 2022-09-15 à 00.32.47.png]
> >> good evening my teacher
> >> I hope you are well
> >> Sir I found an implementation on decryption failure, I tried to execute
> >> it locally on my machine, I launched the execution and it is almost 3 days,
> >> it is still processing.
> >> sir please, if it is possible to advise me if this implementation is good
> >> to test it?
> >> Do you know of any other implementation regarding attack against LWE
> >> better.
> >> You can explain to me why this implementation is very late except
> >> physical condition of my pc, are there problems at the level of calculation
> >> or something else
> >> thank you in advance sir
> >>
> >> <https://github.com/KULEuven-COSIC/failure-boosting>
> >>
> >> --
> >> You received this message because you are subscribed to the Google Groups
> >> "pqc-forum" group.
> >> To unsubscribe from this group and stop receiving emails from it, send an
> >> email to pqc-forum+...@list.nist.gov.
> >> To view this discussion on the web visit
> >> <https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/3398b255-b3d9-41d9-9b2d-a1f8aacca21dn%40list.nist.gov>
> >> <https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/3398b255-b3d9-41d9-9b2d-a1f8aacca21dn%40list.nist.gov?utm_medium=email&utm_source=footer>
> >> .
> >>

> >> --

> > You received this message because you are subscribed to the Google Groups
> > "pqc-forum" group.

> > To unsubscribe from this group and stop receiving emails from it, send an
> > email to pqc-forum+unsubscribe@list.nist.gov.

> > To view this discussion on the web visit

> > <https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/79518a28-336a-4a48-b4f8-4c072d8dbf81n%40list.nist.gov>

> > <https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/79518a28-336a-4a48-b4f8-4c072d8dbf81n%40list.nist.gov?utm_medium=email&utm_source=footer>

> > .

> >

>

>

> --

>

> Cordialement

>

> *ASEBRIY FATIMA *

>

> *Master de recherche M3S_TA*

>

> *Master Sécurité Systèmes et Services*

>

> *Université Mohammed V, ENSIAS*

>

> *Rabat, Maroc*

>

> --

> You received this message because you are subscribed to the Google Groups "pqc-forum" group.

> To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.

> To view this discussion on the web visit <https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/>

CAG_Shvv9p9Tn0oTSc7hcq3BB3N9zh3EFegFa%2BUQokQwW%3D9UBMw%40mail.gmail.com.

--

You received this message because you are subscribed to the Google Groups "pqc-forum" group.

To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.

To view this discussion on the web visit <https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/Yy6lANrka/6jS8zS%40disp3269>.