From: Bo-Yin Yang <moscito@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] UOV parameters
Date: Sunday, June 19, 2022 04:02:09 AM ET

Dear PQC-list:

In view of the recent Beullens attack on Rainbow and the new NIST upcoming call stressing longstanding digital signature schemes, it is surely important to select some parameter sets for Unbalanced Oil and Vinegar, the most venerable non-lattice extant PQ digital signature scheme.

Our team has examined the design space and come up with the following parameter sets and will implement them for the public good. The numbers are (where q is the field size, n is #oil+#vinegar, and m=#oil) for NIST security levels 1, 3, and 5.

q: 16, n: 160, m: 64, (SL1)
q: 256, n: 112, m: 44, (SL1)
q: 256, n: 184, m: 72, (SL3)
q: 256, n: 244, m: 96, (SL5)

best wishes,
Ward Beullens, Ming-Shing Chen, Jintai Ding, Matthias J. Kannwischer, Jacques Patarin, Albrecht Petzoldt, Dieter Schmidt, Chengdong Tao, and Bo-Yin Yang
--

From: Daniel Apon <dapon.crypto@gmail.com> via pqc-forum@list.nist.gov
To: Bo-Yin Yang <moscito@gmail.com>
CC: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] UOV parameters
Date: Sunday, June 19, 2022 05:41:04 PM ET

Thanks, guys.

Have you benchmarked these new parameter sets for clock cycles of KG/Sign/Verify?

--Daniel

On Sun, Jun 19, 2022 at 4:01 AM Bo-Yin Yang <moscito@gmail.com> wrote:

> Dear PQC-list:
>
> In view of the recent Beullens attack on Rainbow and the new NIST upcoming call stressing longstanding digital signature schemes, it is surely important to select some parameter sets for Unbalanced Oil and Vinegar, the most venerable non-lattice extant PQ digital signature scheme.
>
> Our team has examined the design space and come up with the following parameter sets and will implement them for the public good. The numbers are (where q is the field size, n is #oil+#vinegar, and m=#oil) for NIST security levels 1, 3, and 5.
>
> q: 16, n: 160, m: 64, (SL1)
> q: 256, n: 112, m: 44, (SL1)
> q: 256, n: 184, m: 72, (SL3)
> q: 256, n: 244, m: 96, (SL5)
>
> best wishes,
> Ward Beullens, Ming-Shing Chen, Jintai Ding, Matthias J. Kannwischer, Jacques Patarin, Albrecht Petzoldt, Dieter Schmidt, Chengdong Tao, and Bo-Yin Yang
> --
> 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/16e85f78-a37a-4213-81cb-f2dd48d85e02n%40list.nist.gov.

--

From: Bo Lin <bolinsco@gmail.com> via pqc-forum@list.nist.gov
To: Bo-Yin Yang <moscito@gmail.com>
CC: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] UOV parameters
Date: Monday, June 20, 2022 02:39:24 AM ET

Hi,
Thanks for the update.

Does this mean that the key size of UOV is as follows?

q	n	m	key size (bits) (q*m*n^2)/2	key size (bytes) (key size (bits)) / 8
16	160	64	5,242,880	655,360
256	122	44	30,232,576	3,779,072
256	184	72	122,093,568	15,261,696
256	244	96	287,834,112	35,979,264

Regards,

Bo

On Sun, 19 Jun 2022 at 09:01, Bo-Yin Yang <moscito@gmail.com> wrote:

> Dear PQC-list:
>
> In view of the recent Beullens attack on Rainbow and the new NIST upcoming call stressing longstanding digital signature schemes, it is surely important to select some parameter sets for Unbalanced Oil and Vinegar, the most venerable non-lattice extant PQ digital signature scheme.
>
> Our team has examined the design space and come up with the following parameter sets and will implement them for the public good. The numbers are (where q is the field size, n is #oil+#vinegar, and m=#oil) for NIST security levels 1, 3, and 5.
>
> q: 16, n: 160, m: 64, (SL1)
> q: 256, n: 112, m: 44, (SL1)
> q: 256, n: 184, m: 72, (SL3)

> q: 256, n: 244, m: 96, (SL5)
>
> best wishes,
> Ward Beullens, Ming-Shing Chen, Jintai Ding, Matthias J. Kannwischer, Jacques Patarin, Albrecht Petzoldt, Dieter Schmidt, Chengdong Tao, and Bo-Yin Yang --
> 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/16e85f78-a37a-4213-81cb-f2dd48d85e02n%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/CAL3OXVzDkhG%2BW3Lo4yXJ1v-T4iL9rwVma8cOEQ0of_jJOGZZBA%40mail.gmail.com.

From: Matthias Kannwischer <m.kannwischer@gmail.com> via pqc-forum@list.nist.gov
To: Bo Lin <bolinsco@gmail.com>
CC: Bo-Yin Yang <moscito@gmail.com>, pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] UOV parameters
Date: Monday, June 20, 2022 03:07:35 AM ET

Dear Bo,
No, the public-key size of plain UOV is log_256(q)*m*n*(n+1)/2 bytes.

So, you have public keys of

412160 bytes
278432 bytes
1225440 bytes
2869440 bytes

Cheers,

Matthias

On Mon, 20 Jun 2022 at 14:39, Bo Lin <bolinsco@gmail.com> wrote:

> Hi,
> Thanks for the update.
>
> Does this mean that the key size of UOV is as follows?
>
> | q | n | m | key size (bits) (q*m*n^2)/2 | key size (bytes) (key size (bits)) / 8 |
> |---|---|---|---|---|
> | 16 | 160 | 64 | 5,242,880 | 655,360 |
> | 256 | 122 | 44 | 30,232,576 | 3,779,072 |
> | 256 | 184 | 72 | 122,093,568 | 15,261,696 |
> | 256 | 244 | 96 | 287,834,112 | 35,979,264 |
>
> Regards,
>
> Bo
>
> On Sun, 19 Jun 2022 at 09:01, Bo-Yin Yang <moscito@gmail.com> wrote:

> Dear PQC-list:
>
> In view of the recent Beullens attack on Rainbow and the new NIST upcoming call stressing longstanding digital signature schemes, it is surely important to select some parameter sets for Unbalanced Oil and Vinegar, the most venerable non-lattice extant PQ digital signature scheme.
>
> Our team has examined the design space and come up with the following parameter sets and will implement them for the public good. The numbers are (where q is the field size, n is #oil+#vinegar, and m=#oil) for NIST security levels 1, 3, and 5.
>
> q: 16, n: 160, m: 64, (SL1)
> q: 256, n: 112, m: 44, (SL1)
> q: 256, n: 184, m: 72, (SL3)
> q: 256, n: 244, m: 96, (SL5)
>
> best wishes,
> Ward Beullens, Ming-Shing Chen, Jintai Ding, Matthias J. Kannwischer, Jacques Patarin, Albrecht Petzoldt, Dieter Schmidt, Chengdong Tao, and Bo-Yin Yang --
>

--

--

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/CAKaNK-7yN_6oKi%2BM7D6RM7Rhp6RXKHJP1D%3DLFVt3wBd3vuZrcw%40mail.gmail.com.

From: Bo Lin <bolinsco@gmail.com> via pqc-forum@list.nist.gov
To: Matthias Kannwischer <m.kannwischer@gmail.com>
CC: Bo-Yin Yang <moscito@gmail.com>, pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] UOV parameters
Date: Monday, June 20, 2022 04:25:09 AM ET

Thanks Matthias.
Yes, indeed, I missed the log operation and misplaced the m and n in the Spreadsheet. The (n+1) item was not known to me though. The following table is a re-calculation according to your correction:

parameters				key size (bits)	key size (bytes)
q	**log(q)**	**n**	**m**	**(log(q)*m*n*(n+1))/2**	**(key size (bits)) / 8**
16	4	160	64	3,297,280	412,160
256	8	122	44	2,641,056	330,132
256	8	184	72	9,803,520	1,225,440
256	8	244	96	22,955,520	2,869,440

On Mon, 20 Jun 2022 at 08:07, Matthias Kannwischer <m.kannwischer@gmail.com> wrote:

> Dear Bo,
> No, the public-key size of plain UOV is log_256(q)*m*n*(n+1)/2 bytes.
>
> So, you have public keys of
>
> 412160 bytes
> 278432 bytes
> 1225440 bytes
> 2869440 bytes
>
> Cheers,
>
> Matthias

On Mon, 20 Jun 2022 at 14:39, Bo Lin <bolinsco@gmail.com> wrote:

> Hi,
> Thanks for the update.

Does this mean that the key size of UOV is as follows?

q	n	m	key size (bits) (q*m*n^2)/2	key size (bytes) (key size (bits)) / 8
16	160	64	5,242,880	655,360
256	122	44	30,232,576	3,779,072
256	184	72	122,093,568	15,261,696
256	244	96	287,834,112	35,979,264

Regards,

Bo

On Sun, 19 Jun 2022 at 09:01, Bo-Yin Yang <moscito@gmail.com> wrote:

> Dear PQC-list:
>
> In view of the recent Beullens attack on Rainbow and the new NIST upcoming call stressing longstanding digital signature schemes, it is surely important to select some parameter sets for Unbalanced Oil and Vinegar, the most venerable non-lattice extant PQ digital signature scheme.
>
> Our team has examined the design space and come up with the following parameter sets and will implement them for the public good. The numbers are (where q is the field size, n is #oil+#vinegar, and m=#oil) for NIST security levels 1, 3, and 5.
>
> q: 16, n: 160, m: 64, (SL1)
> q: 256, n: 112, m: 44, (SL1)
> q: 256, n: 184, m: 72, (SL3)
> q: 256, n: 244, m: 96, (SL5)
>
> best wishes,
> Ward Beullens, Ming-Shing Chen, Jintai Ding, Matthias J. Kannwischer, Jacques Patarin, Albrecht Petzoldt, Dieter Schmidt, Chengdong Tao, and Bo-Yin Yang --
>

> > To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/16e85f78-a37a-4213-81cb-f2dd48d85e02n%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/CAL3OXVzDkhG%2BW3Lo4yXJ1v-T4iL9rwVma8cOEQ0of_jJOGZZBA%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/CAL3OXVzWhNJ3mP6w449FPDnXFKvyvAVUjwDHP3nU2GYRsqY0JA%40mail.gmail.com.

From: Matthias Kannwischer <m.kannwischer@gmail.com> via pqc-forum@list.nist.gov
To: Bo Lin <bolinsco@gmail.com>
CC: Bo-Yin Yang <moscito@gmail.com>, pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] UOV parameters
Date: Monday, June 20, 2022 04:38:19 AM ET

Dear Bo,

n should be 112 for the second parameter set.

Cheers,

Matthias

On Mon, 20 Jun 2022 at 16:24, Bo Lin <bolinsco@gmail.com> wrote:

> Thanks Matthias.
> Yes, indeed, I missed the log operation and misplaced the m and n in the Spreadsheet. The (n+1) item was not known to me though. The following table is a re-calculation according to your correction:

parameters				key size (bits)	key size (bytes)
q	**log(q)**	**n**	**m**	**(log(q)*m*n*(n+1))/2**	**(key size (bits)) / 8**
16	4	160	64	3,297,280	412,160
256	8	122	44	2,641,056	330,132
256	8	184	72	9,803,520	1,225,440
256	8	244	96	22,955,520	2,869,440

> On Mon, 20 Jun 2022 at 08:07, Matthias Kannwischer <m.kannwischer@gmail.com> wrote:
>
> > Dear Bo,
> > No, the public-key size of plain UOV is log_256(q)*m*n*(n+1)/2 bytes.
> >
> > So, you have public keys of
> >
> > 412160 bytes
> > 278432 bytes

1225440 bytes
2869440 bytes

Cheers,

Matthias

On Mon, 20 Jun 2022 at 14:39, Bo Lin <bolinsco@gmail.com> wrote:

> Hi,
> Thanks for the update.
>
> Does this mean that the key size of UOV is as follows?

q	n	m	key size (bits) (q*m*n^2)/2	key size (bytes) (key size (bits)) / 8
16	160	64	5,242,880	655,360
256	122	44	30,232,576	3,779,072
256	184	72	122,093,568	15,261,696
256	244	96	287,834,112	35,979,264

> Regards,
>
> Bo
>
> On Sun, 19 Jun 2022 at 09:01, Bo-Yin Yang <moscito@gmail.com> wrote:
>
> > Dear PQC-list:
> >
> > In view of the recent Beullens attack on Rainbow and the new NIST upcoming call stressing longstanding digital signature schemes, it is surely important to select some parameter sets for Unbalanced Oil and Vinegar, the most venerable non-lattice extant PQ digital signature scheme.
> >
> > Our team has examined the design space and come up with the following parameter sets and will implement them for the public good. The numbers are (where q is the field size, n is #oil+#vinegar, and m=#oil) for NIST security levels 1, 3, and 5.
> >
> > q: 16, n: 160, m: 64, (SL1)

> > > q: 256, n: 112, m: 44, (SL1)
> > > q: 256, n: 184, m: 72, (SL3)
> > > q: 256, n: 244, m: 96, (SL5)
> > >
> > > best wishes,
> > > Ward Beullens, Ming-Shing Chen, Jintai Ding, Matthias J. Kannwischer, Jacques Patarin, Albrecht Petzoldt, Dieter Schmidt, Chengdong Tao, and Bo-Yin Yang --
> > > 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/16e85f78-a37a-4213-81cb-f2dd48d85e02n%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/CAL3OXVzDkhG%2BW3Lo4yXJ1v-T4iL9rwVma8cOEQ0of_jJOGZZBA%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/CAKaNK-4LwM6NmfpzPwXU0LPHznJVP6n0nJbUknBdg9VLHKSpQw%40mail.gmail.com.

From: ward@beullens.com via pqc-forum@list.nist.gov
To: Matthias Kannwischer <m.kannwischer@gmail.com>, Bo Lin <bolinsco@gmail.com>
CC: Bo-Yin Yang <moscito@gmail.com>, pqc-forum <pqc-forum@list.nist.gov>
Subject: RE: [pqc-forum] UOV parameters
Date: Monday, June 20, 2022 05:01:57 AM ET

Dear all,

Note that a large part of a UOV public key is uniformly random and can be expanded from a short seed. (see https://eprint.iacr.org/2010/424 for the details)

So, the public key size is really only log(q)m^2(m+1)/2 bits + a short seed.

This reduces the public key size from 412.2KB to 66.6 KB for the first parameter set.

All the best,
Ward

> **From:** pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> **On Behalf Of** Matthias Kannwischer
> **Sent:** Monday, 20 June 2022 10:38
> **To:** Bo Lin <bolinsco@gmail.com>
> **Cc:** Bo-Yin Yang <moscito@gmail.com>; pqc-forum <pqc-forum@list.nist.gov>
> **Subject:** Re: [pqc-forum] UOV parameters
>
> Dear Bo,
>
> n should be 112 for the second parameter set.
>
> Cheers,
>
> Matthias
>
> On Mon, 20 Jun 2022 at 16:24, Bo Lin <bolinsco@gmail.com> wrote:
>
> > Thanks Matthias.

Yes, indeed, I missed the log operation and misplaced the m and n in the Spreadsheet. The (n+1) item was not known to me though. The following table is a re-calculation according to your correction:

parameters				key size (bits)	key size (bytes)
q	**log(q)**	**n**	**m**	**(log(q)*m*n*(n+1))/2**	**(key size (bits)) / 8**
16	4	160	64	3,297,280	412,160
256	8	122	44	2,641,056	330,132
256	8	184	72	9,803,520	1,225,440
256	8	244	96	22,955,520	2,869,440

On Mon, 20 Jun 2022 at 08:07, Matthias Kannwischer <m.kannwischer@gmail.com> wrote:

> Dear Bo,
>
> No, the public-key size of plain UOV is log_256(q)*m*n*(n+1)/2 bytes.
>
> So, you have public keys of
>
> 412160 bytes
> 278432 bytes
> 1225440 bytes
> 2869440 bytes
>
> Cheers,
>
> Matthias
>
> On Mon, 20 Jun 2022 at 14:39, Bo Lin <bolinsco@gmail.com> wrote:
>
> > Hi,
> >
> > Thanks for the update.
> >
> > Does this mean that the key size of UOV is as follows?
> >
> > | | | | key size (bits) | key size (bytes) |
> > |---|---|---|---|---|
> > | **q** | **n** | **m** | | |

			(q*m*n^2)/2	(key size (bits)) / 8
16	160	64	5,242,880	655,360
256	122	44	30,232,576	3,779,072
256	184	72	122,093,568	15,261,696
256	244	96	287,834,112	35,979,264

Regards,

Bo

On Sun, 19 Jun 2022 at 09:01, Bo-Yin Yang <moscito@gmail.com> wrote:

> Dear PQC-list:
>
> In view of the recent Beullens attack on Rainbow and the new NIST upcoming call stressing longstanding digital signature schemes, it is surely important to select some parameter sets for Unbalanced Oil and Vinegar, the most venerable non-lattice extant PQ digital signature scheme.
>
> Our team has examined the design space and come up with the following parameter sets and will implement them for the public good. The numbers are (where q is the field size, n is #oil+#vinegar, and m=#oil) for NIST security levels 1, 3, and 5.
>
> q: 16, n: 160, m: 64, (SL1)
> q: 256, n: 112, m: 44, (SL1)
> q: 256, n: 184, m: 72, (SL3)
> q: 256, n: 244, m: 96, (SL5)
>
> best wishes,
> Ward Beullens, Ming-Shing Chen, Jintai Ding, Matthias J. Kannwischer, Jacques Patarin, Albrecht Petzoldt, Dieter Schmidt, Chengdong Tao, and Bo-Yin Yang
>
> --
> 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/16e85f78-a37a-4213-81cb-f2dd48d85e02n%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/CAL3OXVzDkhG%2BW3Lo4yXJ1v-T4iL9rwVma8cOEQ0of_jJOGZZBA%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/CAKaNK-4LwM6NmfpzPwXU0LPHznJVP6n0nJbUknBdg9VLHKSpQw%40mail.gmail.com.

From: Bo Lin <bolinsco@gmail.com> via pqc-forum@list.nist.gov
To: Matthias Kannwischer <m.kannwischer@gmail.com>
CC: Bo-Yin Yang <moscito@gmail.com>, pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] UOV parameters
Date: Monday, June 20, 2022 06:08:19 AM ET

Hi, Matthias,
Thanks for the correction. It is ratified as

parameters				key size (bits)	key size (bytes)
q	**log(q)**	**n**	**m**	**(log(q)*m*n*(n+1))/2**	**(key size (bits)) / 8**
16	4	160	64	3,297,280	412,160
256	8	112	44	2,227,456	278,432
256	8	184	72	9,803,520	1,225,440
256	8	244	96	22,955,520	2,869,440

On Mon, 20 Jun 2022 at 09:37, Matthias Kannwischer <m.kannwischer@gmail.com> wrote:

> Dear Bo,
>
> n should be 112 for the second parameter set.
>
> Cheers,
>
> Matthias
>
> On Mon, 20 Jun 2022 at 16:24, Bo Lin <bolinsco@gmail.com> wrote:
>
> > Thanks Matthias.
> > Yes, indeed, I missed the log operation and misplaced the m and n in the Spreadsheet. The (n+1) item was not known to me though. The following table is a re-calculation according to your correction:
> >
> > | parameters | | | | key size (bits) | key size (bytes) |
> > |---|---|---|---|---|---|
> > | **q** | **log(q)** | **n** | **m** | **(log(q)*m*n*(n+1))/2** | **(key size (bits)) / 8** |
> > | 16 | 4 | 160 | 64 | 3,297,280 | 412,160 |
> > | 256 | 8 | 122 | 44 | 2,641,056 | 330,132 |
> > | 256 | 8 | 184 | 72 | 9,803,520 | 1,225,440 |

256	8	244	96	22,955,520	2,869,440

On Mon, 20 Jun 2022 at 08:07, Matthias Kannwischer <m.kannwischer@gmail.com> wrote:

> Dear Bo,
> No, the public-key size of plain UOV is log_256(q)*m*n*(n+1)/2 bytes.
>
> So, you have public keys of
>
> 412160 bytes
> 278432 bytes
> 1225440 bytes
> 2869440 bytes
>
> Cheers,
>
> Matthias
>
> On Mon, 20 Jun 2022 at 14:39, Bo Lin <bolinsco@gmail.com> wrote:
>
> > Hi,
> > Thanks for the update.
> >
> > Does this mean that the key size of UOV is as follows?
> >
> > | q | n | m | key size (bits) (q*m*n^2)/2 | key size (bytes) (key size (bits)) / 8 |
> > |---|---|---|---|---|
> > | 16 | 160 | 64 | 5,242,880 | 655,360 |
> > | 256 | 122 | 44 | 30,232,576 | 3,779,072 |
> > | 256 | 184 | 72 | 122,093,568 | 15,261,696 |
> > | 256 | 244 | 96 | 287,834,112 | 35,979,264 |
> >
> > Regards,
> >
> > Bo
> >
> > On Sun, 19 Jun 2022 at 09:01, Bo-Yin Yang <moscito@gmail.com> wrote:

> > > Dear PQC-list:
> > >
> > > In view of the recent Beullens attack on Rainbow and the new NIST upcoming call stressing longstanding digital signature schemes, it is surely important to select some parameter sets for Unbalanced Oil and Vinegar, the most venerable non-lattice extant PQ digital signature scheme.
> > >
> > > Our team has examined the design space and come up with the following parameter sets and will implement them for the public good. The numbers are (where q is the field size, n is #oil+#vinegar, and m=#oil) for NIST security levels 1, 3, and 5.
> > >
> > > q: 16, n: 160, m: 64, (SL1)
> > > q: 256, n: 112, m: 44, (SL1)
> > > q: 256, n: 184, m: 72, (SL3)
> > > q: 256, n: 244, m: 96, (SL5)
> > >
> > > best wishes,
> > > Ward Beullens, Ming-Shing Chen, Jintai Ding, Matthias J. Kannwischer, Jacques Patarin, Albrecht Petzoldt, Dieter Schmidt, Chengdong Tao, and Bo-Yin Yang --
> > > 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/16e85f78-a37a-4213-81cb-f2dd48d85e02n%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/CAL3OXVzDkhG%2BW3Lo4yXJ1v-T4iL9rwVma8cOEQ0of_jJOGZZBA%40mail.gmail.com.

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

From: Matthias Kannwischer <m.kannwischer@gmail.com> via pqc-forum@list.nist.gov
To: Daniel Apon <dapon.crypto@gmail.com>
CC: Bo-Yin Yang <moscito@gmail.com>, pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] UOV parameters
Date: Tuesday, June 21, 2022 04:26:28 AM ET

Dear Daniel,

thanks for your question about performance benchmarks.

We are currently finalizing AVX2, SSSE3, Arm Neon, and Arm Cortex-M4 implementations of the proposed UOV parameter sets and we will be posting the benchmarking results on the forum soon.

Best regards,
The Team

On Mon, 20 Jun 2022 at 05:40, Daniel Apon <dapon.crypto@gmail.com> wrote:

> Thanks, guys.
>
> Have you benchmarked these new parameter sets for clock cycles of KG/Sign/Verify?
>
> --Daniel
>
> On Sun, Jun 19, 2022 at 4:01 AM Bo-Yin Yang <moscito@gmail.com> wrote:
>
> > Dear PQC-list:
> >
> > In view of the recent Beullens attack on Rainbow and the new NIST upcoming call stressing longstanding digital signature schemes, it is surely important to select some parameter sets for Unbalanced Oil and Vinegar, the most venerable non-lattice extant PQ digital signature scheme.
> >
> > Our team has examined the design space and come up with the following parameter sets and will implement them for the public good. The numbers are (where q is the field size, n is #oil+#vinegar, and m=#oil) for NIST security levels 1, 3, and 5.

> > q: 16, n: 160, m: 64, (SL1)
> > q: 256, n: 112, m: 44, (SL1)
> > q: 256, n: 184, m: 72, (SL3)
> > q: 256, n: 244, m: 96, (SL5)
> >
> > best wishes,
> > Ward Beullens, Ming-Shing Chen, Jintai Ding, Matthias J. Kannwischer, Jacques Patarin, Albrecht Petzoldt, Dieter Schmidt, Chengdong Tao, and Bo-Yin Yang
> > --
> > 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/16e85f78-a37a-4213-81cb-f2dd48d85e02n%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/CAPxHsSJkzqNrPth_qHxHgYDPgXAMM5ipOPFBVnPVsXhXkhzP0A%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/CAKaNK-6tVceyWnSn_%3DG7wNtMgqCGa405c-EnOPXznMR6dt6G0g%40mail.gmail.com.

From: andy yi <hy8196695@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
CC: Matthias Kannwischer <m.kannwischer@gmail.com>, mos...@gmail.com <moscito@gmail.com>, pqc-forum <pqc-forum@list.nist.gov>, Daniel Apon <dapon.crypto@gmail.com>
Subject: Re: [pqc-forum] UOV parameters
Date: Wednesday, June 22, 2022 08:45:32 PM ET

Does anyone know what the Rainbow algorithm is about submitting the updated parameters?

在2022年6月21日星期二 UTC+8 16:26:16<Matthias Kannwischer> 写道：

> Dear Daniel,
>
> thanks for your question about performance benchmarks.
>
> We are currently finalizing AVX2, SSSE3, Arm Neon, and Arm Cortex-M4 implementations of the proposed UOV parameter sets and we will be posting the benchmarking results on the forum soon.
>
> Best regards,
> The Team
>
> On Mon, 20 Jun 2022 at 05:40, Daniel Apon <dapon....@gmail.com> wrote:
>
> > Thanks, guys.
> >
> > Have you benchmarked these new parameter sets for clock cycles of KG/Sign/Verify?
> >
> > --Daniel
> >
> > On Sun, Jun 19, 2022 at 4:01 AM Bo-Yin Yang <mos...@gmail.com> wrote:
> >
> > > Dear PQC-list:
> > >
> > > In view of the recent Beullens attack on Rainbow and the new NIST upcoming call stressing longstanding digital signature schemes, it is surely important to select some parameter sets for Unbalanced Oil and Vinegar, the most venerable non-lattice extant

> > PQ digital signature scheme.
> >
> > Our team has examined the design space and come up with the following parameter sets and will implement them for the public good. The numbers are (where q is the field size, n is #oil+#vinegar, and m=#oil) for NIST security levels 1, 3, and 5.
> >
> > q: 16, n: 160, m: 64, (SL1)
> > q: 256, n: 112, m: 44, (SL1)
> > q: 256, n: 184, m: 72, (SL3)
> > q: 256, n: 244, m: 96, (SL5)
> >
> > best wishes,
> > Ward Beullens, Ming-Shing Chen, Jintai Ding, Matthias J. Kannwischer, Jacques Patarin, Albrecht Petzoldt, Dieter Schmidt, Chengdong Tao, and Bo-Yin Yang --
> > 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/16e85f78-a37a-4213-81cb-f2dd48d85e02n%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+...@list.nist.gov.
> To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/CAPxHsSJkzqNrPth_qHxHgYDPgXAMM5ipOPFBVnPVsXhXkhzP0A%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/7a13f798-e89f-4596-85ac-97dba686dc18n%40list.nist.gov.

From: Jintai Ding <jintai.ding@gmail.com> via pqc-forum@list.nist.gov
To: andy yi <hy8196695@gmail.com>
CC: Daniel Apon <dapon.crypto@gmail.com>, Matthias Kannwischer <m.kannwischer@gmail.com>, mos...@gmail.com <moscito@gmail.com>, pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] UOV parameters
Date: Wednesday, June 22, 2022 08:50:47 PM ET

Yes. Soon, we are doing final check our numbers.

On Thu, Jun 23, 2022 at 8:45 AM andy yi <hy8196695@gmail.com> wrote:

> Does anyone know what the Rainbow algorithm is about submitting the updated parameters?
>
> 在2022年6月21日星期二 UTC+8 16:26:16<Matthias Kannwischer> 写道：
>
> > Dear Daniel,
> >
> > thanks for your question about performance benchmarks.
> >
> > We are currently finalizing AVX2, SSSE3, Arm Neon, and Arm Cortex-M4 implementations of the proposed UOV parameter sets and we will be posting the benchmarking results on the forum soon.
> >
> > Best regards,
> > The Team
> >
> > On Mon, 20 Jun 2022 at 05:40, Daniel Apon <dapon....@gmail.com> wrote:
> >
> > > Thanks, guys.
> > >
> > > Have you benchmarked these new parameter sets for clock cycles of KG/Sign/Verify?
> > >
> > > --Daniel
> > >
> > > On Sun, Jun 19, 2022 at 4:01 AM Bo-Yin Yang <mos...@gmail.com> wrote:

> > Dear PQC-list:
> >
> > In view of the recent Beullens attack on Rainbow and the new NIST upcoming call stressing longstanding digital signature schemes, it is surely important to select some parameter sets for Unbalanced Oil and Vinegar, the most venerable non-lattice extant PQ digital signature scheme.
> >
> > Our team has examined the design space and come up with the following parameter sets and will implement them for the public good. The numbers are (where q is the field size, n is #oil+#vinegar, and m=#oil) for NIST security levels 1, 3, and 5.
> >
> > q: 16, n: 160, m: 64, (SL1)
> > q: 256, n: 112, m: 44, (SL1)
> > q: 256, n: 184, m: 72, (SL3)
> > q: 256, n: 244, m: 96, (SL5)
> >
> > best wishes,
> > Ward Beullens, Ming-Shing Chen, Jintai Ding, Matthias J. Kannwischer, Jacques Patarin, Albrecht Petzoldt, Dieter Schmidt, Chengdong Tao, and Bo-Yin Yang --
> > 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/16e85f78-a37a-4213-81cb-f2dd48d85e02n%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+...@list.nist.gov.
> To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/CAPxHsSJkzqNrPth_qHxHgYDPgXAMM5ipOPFBVnPVsXhXkhzP0A%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/7a13f798-e89f-4596-85ac-97dba686dc18n%40list.nist.gov.

--
Jintai Ding, PhD
Professor of Mathematics
Tsinghua University

--
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/CAB7J41Sk%2BCQJoCs1y165VcqkBp8m5TynTV1vUdD6ahfpe8Du-Q%40mail.gmail.com.