From: Yongge Wang <yongge.wang@gmail.com>
Sent: Sunday, December 24, 2017 4:22 PM
To: pqc-comments; pqc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: McNie

Dear Designers of McNie and all,
I am afraid the parameters in this proposal have at most 4 to 6-bits security under the Information Set Decoding (ISD) attack.

In the proposal, the public key is (G', F) where G' is an l x n matrix and F is an l x (n-k) matrix.

The encryption proceeds as: c1=mG'+e and c2=mF where e has weight at most r

The recommended parameter (l, n, n-k, r) is (I only include the ones useful for ISD attacks):
3Q_128_1: (62, 93, 31,5)
3Q_128_2: (70, 105, 35,5)
3Q_192_1: (74, 111, 37,7)
3Q_192_2: (82, 123, 41,7)
3Q_256_1: (74, 111, 37,7)
3Q_256_2: (94, 141, 47,9)
4Q_128_1: (45, 60, 30,5)
4Q_128_2: (54, 72, 36,5)
4Q_192_1: (57, 76, 38,7)
4Q_192_2: (63, 84, 42,7)
4Q_256_1: (57, 76, 38,7)
4Q_256_2: (66, 88, 44,8)

It is noted that the c2 contains no error. Thus for the basic ISD, one only needs to select l-(n-k) error free entries from c1. That is, the success probability is at least {n-r \choose l-(n-k)} / {n \choose l-(n-k)}

In other words, the security for these scheme are at most (instead of 128/192/256 bits):
3Q_128_1: 4 bits
3Q_128_2: 4 bits
3Q_192_1: 5 bits
3Q_192_2: 5 bits
3Q_256_1: 5 bits
3Q_256_2: 6 bits
4Q_128_1: 3 bits
4Q_128_2: 3 bits
4Q_192_1: 4 bits
4Q_192_2: 4 bits
4Q_256_1: 4 bits
4Q_256_2: 4 bits

Thanks!

From: Gaborit <gaborit@unilim.fr>
Sent: Sunday, December 24, 2017 5:21 PM
To: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] OFFICIAL COMMENT: McNie

Hi,

yes there is an attack on the system, which reduces the security by a factor 2 in the exponent

for their parameters, the authors know about it.

best,

philippe

Le 24/12/2017 à 22:22, Yongge Wang a écrit :

> Dear Designers of McNie and all,
> I am afraid the parameters in this proposal have at most 4 to 6-bits security under the Information Set Decoding (ISD) attack.
>
> In the proposal, the public key is (G', F) where G' is an l x n matrix and F is an l x (n-k) matrix.
>
> The encryption proceeds as: c1=mG'+e and c2=mF where e has weight at most r
>
> The recommended parameter (l, n, n-k, r) is (I only include the ones useful for ISD attacks):
> 3Q_128_1: (62, 93, 31,5)
> 3Q_128_2: (70, 105, 35,5)
> 3Q_192_1: (74, 111, 37,7)
> 3Q_192_2: (82, 123, 41,7)
> 3Q_256_1: (74, 111, 37,7)
> 3Q_256_2: (94, 141, 47,9)
> 4Q_128_1: (45, 60, 30,5)
> 4Q_128_2: (54, 72, 36,5)
> 4Q_192_1: (57, 76, 38,7)
> 4Q_192_2: (63, 84, 42,7)
> 4Q_256_1: (57, 76, 38,7)
> 4Q_256_2: (66, 88, 44,8)
>
> It is noted that the c2 contains no error. Thus for the basic ISD, one only needs

From: Yongge Wang <yongge.wang@gmail.com>
Sent: Sunday, December 24, 2017 5:32 PM
To: Gaborit
Cc: pqc-forum@list.nist.gov; pqc-comments
Subject: Re: [pqc-forum] OFFICIAL COMMENT: McNie

My analysis shows that given a cipher text and a public key, one needs at most 2^6 trials to recover the plaintext.. not a reduction of factor 2 in the exponent.
thanks!
Yongge

On Mon, Dec 25, 2017 at 1:20 AM, Gaborit <gaborit@unilim.fr> wrote:

> Hi,
>
> yes there is an attack on the system, which reduces the security by a factor 2 in the exponent
>
> for their parameters, the authors know about it.
>
> best,
>
> philippe
>
> Le 24/12/2017 à 22:22, Yongge Wang a écrit :
>
> > Dear Designers of McNie and all,
> > I am afraid the parameters in this proposal have at most 4 to 6-bits security under the Information Set Decoding (ISD) attack.
> >
> > In the proposal, the public key is (G', F) where G' is an l x n matrix and F is an l x (n-k) matrix.
> >
> > The encryption proceeds as: c1=mG'+e and c2=mF where e has weight at most r
> >
> > The recommended parameter (l, n, n-k, r) is (I only include the ones useful for ISD attacks):
> > 3Q_128_1: (62, 93, 31,5)
> > 3Q_128_2: (70, 105, 35,5)
> > 3Q_192_1: (74, 111, 37,7)
> > 3Q_192_2: (82, 123, 41,7)
> > 3Q_256_1: (74, 111, 37,7)

From: Paulo Barreto <pbarreto@gmail.com>
Sent: Sunday, December 24, 2017 5:38 PM
To: Yongge Wang
Cc: Philippe Gaborit; pqc-forum@list.nist.gov; pqc-comments
Subject: Re: [pqc-forum] OFFICIAL COMMENT: McNie

I understand that McNie is based on rank metric codes. How did you adapt ISD (typically used for the Hamming metric) to that setting? For the figures you report seem to be precisely what you get for the latter metric rather than the former one.

All the best,

Paulo Barreto.

On Dec 24, 2017 14:31, "Yongge Wang" <yongge.wang@gmail.com> wrote:

> My analysis shows that given a cipher text and a public key, one needs at most 2^6 trials to recover the plaintext..
> not a reduction of factor 2 in the exponent.
> thanks!
> Yongge
>
> On Mon, Dec 25, 2017 at 1:20 AM, Gaborit <gaborit@unilim.fr> wrote:
>
> > Hi,
> >
> > yes there is an attack on the system, which reduces the security by a factor 2 in the exponent
> >
> > for their parameters, the authors know about it.
> >
> > best,
> >
> > philippe
> >
> > Le 24/12/2017 à 22:22, Yongge Wang a écrit :
> >
> > > Dear Designers of McNie and all,
> > > I am afraid the parameters in this proposal have at most 4 to 6-bits security under the Information Set Decoding (ISD) attack.
> > >
> > > In the proposal, the public key is (G', F) where G' is an l x n matrix and F is
> > > an l x (n-k) matrix.

From: Gaborit <gaborit@unilim.fr>
Sent: Sunday, December 24, 2017 6:16 PM
To: Paulo Barreto; Yongge Wang
Cc: pqc-forum@list.nist.gov; pqc-comments
Subject: Re: [pqc-forum] OFFICIAL COMMENT: McNie

we adapted ISD for rank metric in 2016, rank metric is completely different from hamming, attacks have a greater complexity for given size of parameters than for hamming,the authors know about the attack on their system let them answer

best,

philippe

Le 24/12/2017 à 23:38, Paulo Barreto a écrit :

> I understand that McNie is based on rank metric codes. How did you adapt ISD (typically used for the Hamming metric) to that setting? For the figures you report seem to be precisely what you get for the latter metric rather than the former one.
>
> All the best,
>
> Paulo Barreto.
>
> On Dec 24, 2017 14:31, "Yongge Wang" <yongge.wang@gmail.com> wrote:
>
> > My analysis shows that given a cipher text and a public key, one needs at most 2^6 trials to recover the plaintext..
> > not a reduction of factor 2 in the exponent.
> > thanks!
> > Yongge
> >
> > On Mon, Dec 25, 2017 at 1:20 AM, Gaborit <gaborit@unilim.fr> wrote:
> >
> > > Hi,
> > >
> > > yes there is an attack on the system, which reduces the security by a factor 2 in the exponent
> > >
> > > for their parameters, the authors know about it.
> > >
> > > best,

From: Gaborit <gaborit@unilim.fr>
Sent: Sunday, December 24, 2017 6:22 PM
To: Yongge Wang
Cc: pqc-forum@list.nist.gov; pqc-comments
Subject: Re: [pqc-forum] OFFICIAL COMMENT: McNie

paulo is right your complexities for the attacks correspond to ISD in hamming which indeed makes no sense

for rank metric.

best,

philippe

Le 24/12/2017 à 23:31, Yongge Wang a écrit :

> My analysis shows that given a cipher text and a public key, one needs at most 2^6 trials to recover the plaintext..
> not a reduction of factor 2 in the exponent.
> thanks!
> Yongge
>
> On Mon, Dec 25, 2017 at 1:20 AM, Gaborit <gaborit@unilim.fr> wrote:
>
> > Hi,
> >
> > yes there is an attack on the system, which reduces the security by a factor 2 in the exponent
> >
> > for their parameters, the authors know about it.
> >
> > best,
> >
> > philippe
> >
> > Le 24/12/2017 à 22:22, Yongge Wang a écrit :
> >
> > Dear Designers of McNie and all,

From: Yongge Wang <yongge.wang@gmail.com>
Sent: Sunday, December 24, 2017 10:27 PM
To: Gaborit
Cc: pqc-forum@list.nist.gov; pqc-comments
Subject: Re: [pqc-forum] OFFICIAL COMMENT: McNie

OK.. Gaborit and Paulo,
I did not read your previous papers on rank-based McEliece schemes. This is the first time I read your scheme. I re-read your proposal.
It seems the term "rank" only shows up from Section 2.5... Before that you did not mention it is for rank-based McEliece scheme... So I took
it for granted that it is for regular McEliece scheme.

If it is for rank-based McEliece scheme, you are right.. my analysis does not work there.
thanks!
Yongge

On Mon, Dec 25, 2017 at 2:21 AM, Gaborit <gaborit@unilim.fr> wrote:

> paulo is right your complexities for the attacks correspond to ISD in hamming which indeed makes no sense
>
> for rank metric.
>
> best,
>
> philippe
>
> Le 24/12/2017 à 23:31, Yongge Wang a écrit :
>
> > My analysis shows that given a cipher text and a public key, one needs at most 2^6 trials to recover the plaintext..
> > not a reduction of factor 2 in the exponent.
> > thanks!
> > Yongge
> >
> > On Mon, Dec 25, 2017 at 1:20 AM, Gaborit <gaborit@unilim.fr> wrote:
> >
> > > Hi,
> > >
> > > yes there is an attack on the system, which reduces the security by a factor 2 in the exponent

From: Jon-Lark Kim <ctryggoggo1@gmail.com>
Sent: Tuesday, December 26, 2017 11:13 AM
To: pqc-forum
Cc: gaborit@unilim.fr; pqc-comments
Subject: Re: [pqc-forum] OFFICIAL COMMENT: McNie

Dear Yongge,

McNie can use any linear codes in Hamming metric or rank metric in general.

However, as mentioned in Page 3 of the introduction we focus on 3 or 4-quasi cyclic LRPC (low rank parity check) codes. So your analysis based on ISD attack using Hamming weight is incorrect.

Thanks.

Jon-Lark

On Monday, December 25, 2017 at 12:27:25 PM UTC+9, Yongge Wang wrote:

> OK.. Gaborit and Paulo,
> I did not read your previous papers on rank-based McEliece schemes. This is the first time I read your scheme. I re-read your proposal.
> It seems the term "rank" only shows up from Section 2.5... Before that you did not mention it is for rank-based McEliece scheme... So I took
> it for granted that it is for regular McEliece scheme.
>
> If it is for rank-based McEliece scheme, you are right.. my analysis does not work there.
> thanks!
> Yongge
>
> On Mon, Dec 25, 2017 at 2:21 AM, Gaborit <gab...@unilim.fr> wrote:
>
> > paulo is right your complexities for the attacks correspond to ISD in hamming which indeed makes no sense
> >
> > for rank metric.
> >
> > best,
> >
> > philippe
> >
> > Le 24/12/2017 à 23:31, Yongge Wang a écrit :
> >
> > > My analysis shows that given a cipher text and a public key, one needs at most 2^6 trials to recover the plaintext..
> > > not a reduction of factor 2 in the exponent.

From: Perlner, Ray (Fed) <ray.perlner@nist.gov>
Sent: Tuesday, December 26, 2017 11:43 AM
To: Gaborit; pqc-forum@list.nist.gov
Subject: RE: [pqc-forum] OFFICIAL COMMENT: McNie

Can you clarify the attack that reduces the security by a factor of 2? Is it mentioned in the submission or otherwise publicly available?

Thanks,
Ray

From: Gaborit [mailto:gaborit@unilim.fr]
Sent: Sunday, December 24, 2017 5:21 PM
To: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] OFFICIAL COMMENT: McNie

Hi,

yes there is an attack on the system, which reduces the security by a factor 2 in the exponent

for their parameters, the authors know about it.

best,

philippe

Le 24/12/2017 à 22:22, Yongge Wang a écrit :

> Dear Designers of McNie and all,
> I am afraid the parameters in this proposal have at most 4 to 6-bits security under the Information Set Decoding (ISD) attack.
>
> In the proposal, the public key is (G', F) where G' is an l x n matrix and F is an l x (n-k) matrix.
>
> The encryption proceeds as: c1=mG'+e and c2=mF where e has weight at most r
>
> The recommended parameter (l, n, n-k, r) is (I only include the ones useful for ISD attacks):
> 3Q_128_1: (62, 93, 31,5)

From: Jon-Lark Kim <ctryggoggo1@gmail.com>
Sent: Tuesday, December 26, 2017 12:09 PM
To: pqc-forum
Cc: gaborit@unilim.fr; Perlner, Ray (Fed)
Subject: Re: [pqc-forum] OFFICIAL COMMENT: McNie

Dear Ray,

Philippe Gaborit reported us that our security can be reduced by a factor of 2(called Attack 1) We have reviewed his argument and think that he is correct.

Below is his argument.

"when you compute c2=mF you got n-k linear relations between

the mi, it means that all the mi can be expressed

only from l-(n-k) fixed mi , hence you can put these relations in your other

equation c1=mG'+e, so that it becomes something

in c1=m'G''+e, where m' has size l-(n-k) and not l.

It means that the complexity of all the attacks have

to be taken with dimension l-(n-k) and not l.

I think it divides your security levels by almost 2 for 3-QC and 3 for 4-QC."

Furthermore Philippe mentioned his new algorithm for ISD attack for rank metric codes written in the paper
https://www.unilim.fr/pages_perso/philippe.gaborit/newGRS.pdf

Based on this new attack(called Attack 2), our security level decreases by about 30 bits more.

So our new parameters for McNie using 3-quasi cyclic LRPC codes at the security levels of 126, 192, 256 are given as follows.

n / l / k / d / r / m / q / failure 1 / failure 2 / Attack 1 /Attack 2/ key size(bits) /security level
120 / 80 / 80 / 3 / 8 / 53 / 2 / -17 / -42 / 162.9 / 128.0 / 6360 / 128
138 / 92 / 92 / 3 / 10 / 67 2 / -17 / -54 / 243.1 / 199.0 / 9246 / 192
156 / 104 / 104 / 3 / 12 / 71 / 2 / -17 / -46 / 303.9 / 257.0 / 11076 / 256

Using 4-quasi cyclic LRPC codes, we have the following new parameters.

n / l / k / d / r / m / q / failure 1 / failure 2 / Attack 1 /Attack 2/ key size(bits) /security level
92 / 46 / 69 / 3 / 10 / 59 / 2 / -17 / -38 / 174.5 / 130.9 / 6785 / 128
112 / 56 / 84 / 3 / 13 / 67 / 2 / -18 / -30 / 245.5 / 195.9 / 9380 / 192
128 / 64 / 96 / 3 / 16 / 73 / 2 / -17 / -18 / 320.6 / 266.4 / 11680 / 256

Thanks.

Jon-Lark Kim

On Wednesday, December 27, 2017 at 1:42:54 AM UTC+9, Perlner, Ray (Fed) wrote:

> Can you clarify the attack that reduces the security by a factor of 2? Is it mentioned in the submission or otherwise publicly available?
>
> Thanks,
>
> Ray
>
> ---
>
> **From:** Gaborit [mailto:gab...@unilim.fr]
> **Sent:** Sunday, December 24, 2017 5:21 PM
> **To:** pqc-...@list.nist.gov
> **Subject:** Re: [pqc-forum] OFFICIAL COMMENT: McNie
>
> Hi,
>
> yes there is an attack on the system, which reduces the security by a factor 2 in the exponent
>
> for their parameters, the authors know about it.
>
> best,
>
> philippe
>
> Le 24/12/2017 à 22:22, Yongge Wang a écrit :
>
> > Dear Designers of McNie and all,
> >
> > I am afraid the parameters in this proposal have at most 4 to 6-bits security under the Information Set Decoding (ISD) attack.
> >
> > In the proposal, the public key is (G', F) where G' is an l x n matrix and F is

From: Gaborit <gaborit@unilim.fr>
Sent: Tuesday, December 26, 2017 12:17 PM
To: Perlner, Ray (Fed); pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] OFFICIAL COMMENT: McNie

Hi Ray,

There is a simple message attack on the system.

For m(m_1,...,m_l) the message.

The ciphertext is (c1,c2) defined as c1=mG'+e and c2=mF with F a (l x (n-k)) matrix,

the security is based on decoding the random matrix G' (l x n) in the c1 part of the ciphertext.

Now since c2=mF you got n-k linear relations between

the m_i, it means that with a strong probability all the m_i can be expressed

only from l-(n-k) fixed m_i , hence you can put these relations in the other

equation c1=mG'+e, so that it becomes something

in c1=m'G''+e, where m' has size l-(n-k) and not l.

If one puts this into the parameters proposed, it divides the dimension

of the searched message m (now m') by a factor 2 or 3 depending

on the considered cases in the parameters. Since the general complexity of the attack

in the exponent is linear in the dimension of m (up to a polynomial factor), it divides almost directly

the complexity by the announced factor.

I informed the authors a few days ago, the system cannot be considered as

broken but the parameters have probably to be doubled or more

to reached the announced levels of complexity.

best,

philippe

Le 26/12/2017 à 17:42, Perlner, Ray (Fed) a écrit :

> Can you clarify the attack that reduces the security by a factor of 2? Is it mentioned in the submission or otherwise publicly available?
>
> Thanks,
>
> Ray
>
> **From:** Gaborit [mailto:gaborit@unilim.fr]
> **Sent:** Sunday, December 24, 2017 5:21 PM
> **To:** pqc-forum@list.nist.gov
> **Subject:** Re: [pqc-forum] OFFICIAL COMMENT: McNie
>
> Hi,
>
> yes there is an attack on the system, which reduces the security by a factor 2 in the exponent
>
> for their parameters, the authors know about it.
>
> best,
>
> philippe
>
> Le 24/12/2017 à 22:22, Yongge Wang a écrit :
>
> > Dear Designers of McNie and all,
> >
> > I am afraid the parameters in this proposal have at most 4 to 6-bits security under the Information Set Decoding (ISD) attack.

From: Yongge Wang <yongge.wang@gmail.com>
Sent: Tuesday, December 26, 2017 1:41 PM
To: Jon-Lark Kim
Cc: pqc-forum; pqc-comments
Subject: Re: [pqc-forum] OFFICIAL COMMENT: McNie

Dear Jon-Lark,
yes, you are right. Paul and Philippe have already mentioned this to me.
My badness, I overlooked that. My described attack only works if you the code using Hamming weight..
But your proposal uses rank metrics.
thanks!
Yongge

On Tue, Dec 26, 2017 at 7:12 PM, Jon-Lark Kim <ctryggoggo1@gmail.com> wrote:

> Dear Yongge,
>
> McNie can use any linear codes in Hamming metric or rank metric in general.
>
> However, as mentioned in Page 3 of the introduction we focus on 3 or 4-quasi cyclic LRPC (low rank parity check) codes.
> So your analysis based on ISD attack using Hamming weight is incorrect.
>
> Thanks.
>
> Jon-Lark
>
> On Monday, December 25, 2017 at 12:27:25 PM UTC+9, Yongge Wang wrote:
>
> > OK.. Gaborit and Paulo,
> > I did not read your previous papers on rank-based McEliece schemes. This is the first time I read your scheme. I re-read your proposal.
> > It seems the term "rank" only shows up from Section 2.5... Before that you did not mention it is for rank-based McEliece scheme... So I took
> > it for granted that it is for regular McEliece scheme.
> >
> > If it is for rank-based McEliece scheme, you are right.. my analysis does not work there.
> > thanks!
> > Yongge
> >
> > On Mon, Dec 25, 2017 at 2:21 AM, Gaborit <gab...@unilim.fr> wrote:
> >
> > > paulo is right your complexities for the attacks correspond to ISD in hamming which indeed makes no sense
> > >
> > > for rank metric.
> > >
> > > best,