From: Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu> via pqc-forum@list.nist.gov
To: 赵运磊 <ylzhao@fudan.edu.cn>
CC: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] More clarifications about patents
Date: Wednesday, May 18, 2022 10:38:53 PM ET
Attachments: smime.p7m

On 5/18/22, 22:05, "'赵运磊' via pqc-forum" <pqc-forum@list.nist.gov> wrote:
> Dear Uri:
> Thanks for your interest in our CTRU and OSKR works.

Thank you for publishing it!

> (1)For OSKR, we have implementations in C, AVX2, ARM Cortex-M4.
> For CTRU, we currently only have reference implementations in C,
> but we are optimizing the implementations in C and AVX, which
> should be given in the near future.

Excellent! Are those implementations Open Source? Freely available?
If so, could you please point me at them? If it isn't Open Source at
this point - may I suggest considering open-sourcing at least some of them?

> If needed, we can send the implementation codes in a private mail.

That would be very nice, thank you!

> (2)For patents, yes, all our proposals are under patent protection now.
> As mentioned, we hold patents mainly for protection to be against
> discredits.

Yes, I understand. There are two concerns here. One is the IPR that you hold - and the following is addressing it. The other one is about alleged patent claims against algorithms like Kyber - and whether those same claims could be alleged against OSKR or CTRU.

> If needed, I will do my best to coordinate towards a positive
> outputs for freely using our proposal.

I cannot speak for NIST, but I think it would benefit the process and increase the chances for success, if there were an official statement – and a NIST lawyer could probably describe what it should say to alleviate any concerns. I think in the past, big companies that held patents made statements like "if our invention is included in the standard, we allow anybody using it free use of our intellectual property, on condition that holders of other patents involved in this standard will allow free use of theirs". Maybe something like this – unfortunately, it is something

Thank you!

> ———原始邮件———
> 发件人: "Blumenthal, Uri - 0553 - MITLL" <uri@ll.mit.edu>
> 发送时间: 2022-05-19 01:53:21 (星期四)
> 收件人: "赵运磊" <ylzhao@fudan.edu.cn>
> 抄送: "pqc-forum@list.nist.gov" <pqc-forum@list.nist.gov>
> 主题: Re: [pqc-forum] More clarifications about patents
>
> Dear Yunlei,
>
> Thank you for your proposals – they are very interesting. I have a few questions.
>
> 1. Are there reference implementations of CTRU, OSKR, and others? Optimized implementations?
>
> 2. Would your proposed algorithms, such as OSKR, still be potential subjects to the same patent claims that, e.g., Kyber is dealing with?
>
> 3. You (University, Company, etc.) have some patents covering CTRU, OSKR, and other algorithms that you proposed. It is nice that your email stated: "we would like to give up all the patents for using our proposals. We hold the patents only for protection." Not being a lawyer, I cannot evaluate whether that statement is sufficient from legal point of view. Would the patent(s) holders be willing to make a more "official" statement to that extent?
>
> Please feel free to answer on this mailing list, or privately – as you prefer.
>

> Thank you!
> --
> V/R,
> Uri
>
>
> On 5/12/22, 12:03, "'赵运磊' via pqc-forum" <pqc-forum@list.nist.gov> wrote:
>
> Dear Prof. Bernstein and dear all in PQC community:
>
> Here, we would like to make the patent issues clearer.
>
> For all the KEM schemes based on LWE/MLWE/LWR/MLWR, they actually have the same scheme structures. The key differences can be well interpreted w.r.t what are referred to as the Con/Rec mechanism in
> https://arxiv.org/abs/1611.06150 (as well as in our KCL proposal). Every KEM based on LWE/MLWE/LWR/MLWR implies a Con/Rec mechanism. The difference between LWE\MLWE-based KEM and LWR\MLWR-based KEM is that Con/Rec in LWE\MLWE-based is w.r.t. the modulus q, but Con/Rec in LWR\MLWR-based is w.r.t the compression parameter p. The Con/Rec implied by Frodo is just one previously proposed, but it is not optimal (as a consequence Frodo does not violate our patents). To the best of our knowledge, AKCN in https://arxiv.org/abs/1611.06150 (as well as in our KCL proposal) is the first one that is proved to be optimal. The Con/Rec mechanisms in Kyber and Saber are also optimal in correcting errors, but Rec in Kyber involves an unnecessary rounding operation which makes it less efficient and more error-prone (the Con of AKCN and that of Kyber are the same). Con/Rec of AKCN-MLWE and Saber are essentially the same, but w.r.t. the compression parameter p in Saber. These differences can be clearly noted from the mentioned two arXiv reports:
>
> https://arxiv.org/abs/2109.02893
>
> https://arxiv.org/abs/1611.06150
>
> Finally, we would like to stress again we hold all the patents only for protection against credit (not for economic reasons). We hope the above clarifications could make the situation clearer.
>
> All my best

> Yunlei
>
>
>
> > ———原始邮件———
> > 发件人: "D. J. Bernstein" <djb@cr.yp.to>
> > 发送时间: 2022-05-12 20:55:14 (星期四)
> > 收件人: pqc-forum@list.nist.gov
> > 抄送:
> > 主题: Re: On the possibility of achieving NIST security goals with the recent advances of dual attacksRe: Re: [pqc-forum] Improved Dual Lattice Attack
> >
> > '赵运磊' via pqc-forum writes:
> > > The recent advances of dual attacks might bring the worry the
> > > possibility of achieving the security goals set by NIST for
> > > lattice-based KEM schemes, particularly on dimension of 512. Our
> > > recent work shows it may still be possible, but with optimized
> > > constructions.
> >
> > Can you please comment on what's covered by your patents related to this
> > work? I noticed that your patents
> >
> >   https://patents.google.com/patent/CN107566121A/en
> >   https://patents.google.com/patent/CN108173643B/en
> >
> > were reported in the KCL/OKCN/AKCN/CNKE submission, which is very
> > similar to "NewHope without reconciliation". The patents were filed a
> > month before "NewHope without reconciliation" was published, and I
> > haven't seen any analysis of the patent coverage.
> >
> > It would be useful to see public assurances as to your company's
> > position regarding usage of "NewHope without reconciliation" and its
> > variants, such as Kyber, SABER, and your latest proposals.
> >
> > ——D. J. Bernstein
> >
> > --

> > 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/20220512125514.219585.qmail%40cr.yp.to.
>
>
>
>
>
> --
> 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/5a91d094.8ba5.180b902887e.Coremail.ylzhao%40fudan.edu.cn.
>
> --
> 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/740E846A-A9A9-4CC3-BD7E-8C5FF3DD4F3E%40ll.mit.edu.

--
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/2d0f4351.70e6.180da0f8e96.Coremail.ylzhao%40fudan.edu.cn.

--

From: 赵运磊 <ylzhao@fudan.edu.cn> via pqc-forum <pqc-forum@list.nist.gov>
To: Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>
CC: pqc-forum@list.nist.gov
Subject: Re: Re: [pqc-forum] More clarifications about patents
Date: Thursday, May 19, 2022 12:03:11 AM ET

> ———原始邮件———
> 发件人: "Blumenthal, Uri - 0553 - MITLL" <uri@ll.mit.edu>
> 发送时间: 2022-05-19 10:38:14 (星期四)
> 收件人: "赵运磊" <ylzhao@fudan.edu.cn>
> 抄送: "pqc-forum@list.nist.gov" <pqc-forum@list.nist.gov>
> 主题: Re: [pqc-forum] More clarifications about patents
>
> On 5/18/22, 22:05, "'赵运磊' via pqc-forum" <pqc-forum@list.nist.gov> wrote:
> > Dear Uri:
> > Thanks for your interest in our CTRU and OSKR works.
>
> Thank you for publishing it!
>
> > (1)For OSKR, we have implementations in C, AVX2, ARM Cortex-M4.
> > For CTRU, we currently only have reference implementations in C,
> > but we are optimizing the implementations in C and AVX, which
> > should be given in the near future.
>
> Excellent! Are those implementations Open Source? Freely available?
> If so, could you please point me at them? If it isn't Open Source at
> this point - may I suggest considering open-sourcing at least some of them?
>
The implementation codes are currently not open source? The reason is that CTRU and OSKR are not related to any standard processes, so we would like not to open source. If NIST or some other standard organization are interested, we can make the implementations codes open.

> > If needed, we can send the implementation codes in a private mail.
>
> That would be very nice, thank you!

I will send the implementation in a separate private mail to you.

>
> > (2)For patents, yes, all our proposals are under patent protection now.
> > As mentioned, we hold patents mainly for protection to be against
> > discredits.
>
> Yes, I understand. There are two concerns here. One is the IPR that you hold - and the following is addressing it. The other one is about alleged patent claims against algorithms like Kyber - and whether those same claims could be alleged against OSKR or CTRU.
>
> > If needed, I will do my best to coordinate towards a positive
> > outputs for freely using our proposal.
>
> I cannot speak for NIST, but I think it would benefit the process and increase the chances for success, if there were an official statement - and a NIST lawyer could probably describe what it should say to alleviate any concerns. I think in the past, big companies that held patents made statements like "if our invention is included in the standard, we allow anybody using it free use of our intellectual property, on condition that holders of other patents involved in this standard will allow free use of theirs". Maybe something like this - unfortunately, it is something
>
Yes, certainly we can make such an official claims about patents as you suggest. It may formally start the work after NIST or other standard organizations show the applicability interest. Indeed, in our KCL proposal in the first round of NIST-PQC, we have already made similar claims. To be frank, we suggest CTRU has another benefit or advantage, as it can be used to improve the state-of-the-art of lattice-based IBE (which is inconvenient to do so based on LWE-based KEMs, besides patent threats to LWE-based KEMS).

Best regards
Yunlei

> Thank you!

>
>
> > ———原始邮件———
> > 发件人: "Blumenthal, Uri - 0553 - MITLL" <uri@ll.mit.edu>
> > 发送时间: 2022-05-19 01:53:21 (星期四)
> > 收件人: "赵运磊" <ylzhao@fudan.edu.cn>
> > 抄送: "pqc-forum@list.nist.gov" <pqc-forum@list.nist.gov>
> > 主题: Re: [pqc-forum] More clarifications about patents
> >
> > Dear Yunlei,
> >
> > Thank you for your proposals - they are very interesting. I have a few questions.
> >
> > 1. Are there reference implementations of CTRU, OSKR, and others? Optimized implementations?
> >
> > 2. Would your proposed algorithms, such as OSKR, still be potential subjects to the same patent claims that, e.g., Kyber is dealing with?
> >
> > 3. You (University, Company, etc.) have some patents covering CTRU, OSKR, and other algorithms that you proposed. It is nice that your email stated: "we would like to give up all the patents for using our proposals. We hold the patents only for protection." Not being a lawyer, I cannot evaluate whether that statement is sufficient from legal point of view. Would the patent(s) holders be willing to make a more "official" statement to that extent?
> >
> > Please feel free to answer on this mailing list, or privately - as you prefer.
> >
> > Thank you!
> > --
> > V/R,
> > Uri
> >
> >
> > On 5/12/22, 12:03, "'赵运磊' via pqc-forum" <pqc-forum@list.nist.gov> wrote:
> >

> > Dear Prof. Bernstein and dear all in PQC community:
> >
> > Here, we would like to make the patent issues clearer.
> >
> > For all the KEM schemes based on LWE/MLWE/LWR/MLWR, they actually have the same scheme structures. The key differences can be well interpreted w.r.t what are referred to as the Con/Rec mechanism in
> > https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Farxiv.org%2Fabs%2F1611.06150&data=05%7C01%7Candrew.regenscheid%40nist.gov%7Cdc6d8aa2e07f4b34d68008da394c7b36%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637885297915615122%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=DDNNCw8ZOPpQUFdiXVm9gL62DGVSd%2BR3Sy%2FyVCsJOaI%3D&reserved=0 (as well as in our KCL proposal). Every KEM based on LWE/MLWE/LWR/MLWR implies a Con/Rec mechanism. The difference between LWE\MLWE-based KEM and LWR\MLWR-based KEM is that Con/Rec in LWE\MLWE-based is w.r.t. the modulus q, but Con/Rec in LWR\MLWR-based is w.r.t the compression parameter p. The Con/Rec implied by Frodo is just one previously proposed, but it is not optimal (as a consequence Frodo does not violate our patents). To the best of our knowledge, AKCN in https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Farxiv.org%2Fabs%2F1611.06150&data=05%7C01%7Candrew.regenscheid%40nist.gov%7Cdc6d8aa2e07f4b34d68008da394c7b36%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637885297915771346%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=WJCYmHJbOx6HZMCBaYwOdFHWWSph7lqu7tVLHr1z698%3D&reserved=0 (as well as in our KCL proposal) is the first one that is proved to be optimal. The Con/Rec mechanisms in Kyber and Saber are also optimal in correcting errors, but Rec in Kyber involves an unnecessary rounding operation which makes it less efficient and more error-prone (the Con of AKCN and that of Kyber are the same). Con/Rec of AKCN-MLWE and Saber are essentially the same, but w.r.t. the compression parameter p in Saber. These differences can be clearly noted from the mentioned two arXiv reports:
> >
> > https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Farxiv.org%2Fabs%2F2109.02893&data=05%7C01%7Candrew.regenscheid%40nist.gov%7Cdc6d8aa2e07f4b34d68008da394c7b36%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637885297915771346%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=qCd6qQz2VODMcXK0dZgyNDYiSDmOoP55aP9Rm8j6QTo%3D&reserved=0
> >

> > https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Farxiv.org%2Fabs%2F1611.06150&data=05%7C01%7Candrew.regenscheid%40nist.gov%7Cdc6d8aa2e07f4b34d68008da394c7b36%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637885297915771346%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=WJCYmHJbOx6HZMCBaYwOdFHWWSph7lqu7tVLHr1z698%3D&reserved=0
> >
> > Finally, we would like to stress again we hold all the patents only for protection against credit (not for economic reasons). We hope the above clarifications could make the situation clearer.
> >
> > All my best
> > Yunlei
> >
> >
> >
> > > ———原始邮件———
> > > 发件人: "D. J. Bernstein" <djb@cr.yp.to>
> > > 发送时间: 2022-05-12 20:55:14（星期四）
> > > 收件人: pqc-forum@list.nist.gov
> > > 抄送:
> > > 主题: Re: On the possibility of achieving NIST security goals with the recent advances of dual attacksRe: Re: [pqc-forum] Improved Dual Lattice Attack
> > >
> > > '赵运磊' via pqc-forum writes:
> > > > The recent advances of dual attacks might bring the worry the
> > > > possibility of achieving the security goals set by NIST for
> > > > lattice-based KEM schemes, particularly on dimension of 512. Our
> > > > recent work shows it may still be possible, but with optimized
> > > > constructions.
> > >
> > > Can you please comment on what's covered by your patents related to this
> > > work? I noticed that your patents
> > >

> > > https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fpatents.google.com%2Fpatent%2FCN107566121A%2Fen&data=05%7C01%7Candrew.regenscheid%40nist.gov%7Cdc6d8aa2e07f4b34d68008da394c7b36%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637885297915771346%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=vrmk%2F0SKFIZ%2FgZQqnqk%2BmlbedUG4r%2FrjFPWjgVFC3nI%3D&reserved=0
> > > https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fpatents.google.com%2Fpatent%2FCN108173643B%2Fen&data=05%7C01%7Candrew.regenscheid%40nist.gov%7Cdc6d8aa2e07f4b34d68008da394c7b36%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637885297915771346%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=%2F8qlOKEt4FZvYawp0UbwiWSmLiwwE%2BlFMEXiTZjdMt4%3D&reserved=0
> > >
> > > were reported in the KCL/OKCN/AKCN/CNKE submission, which is very
> > > similar to "NewHope without reconciliation". The patents were filed a
> > > month before "NewHope without reconciliation" was published, and I
> > > haven't seen any analysis of the patent coverage.
> > >
> > > It would be useful to see public assurances as to your company's
> > > position regarding usage of "NewHope without reconciliation" and its
> > > variants, such as Kyber, SABER, and your latest proposals.
> > >
> > > ——D. J. Bernstein
> > >
> > > --
> > > 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/20220512125514.219585.qmail%40cr.yp.to.
> >
> >
> >
> >
> >
> >
> > --

> > 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/5a91d094.8ba5.180b902887e.Coremail.ylzhao%40fudan.edu.cn.
> >
> > --
> > 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/740E846A-A9A9-4CC3-BD7E-8C5FF3DD4F3E%40ll.mit.edu.
>
>
>
>
>
> --
> 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/2d0f4351.70e6.180da0f8e96.Coremail.ylzhao%40fudan.edu.cn.
>
> --
> 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/7361538F-4FD1-4B3C-A4C0-EAF003D331A6%40ll.mit.edu.

--