From: (b) (6)
To: Moody, Dustin (Fed)
Subject: Re: CT-RSA paper on attacks on SIDH
Date: Tuesday, October 26, 2021 8:45:50 AM

Ok, sounds good, thanks again!

On Tue, Oct 26, 2021 at 8:45 AM Moody, Dustin (Fed) <dustin.moody@nist.gov> wrote:

> Thanks.
>
> Yeah - I agree with them - it's fine for it to not be accepted. It'll get accepted somewhere else at some point.
>
> **From:** Gorjan Alagic (b) (6)
> **Sent:** Tuesday, October 26, 2021 8:42 AM
> **To:** Moody, Dustin (Fed) <dustin.moody@nist.gov>
> **Subject:** Re: CT-RSA paper on attacks on SIDH
>
> Sure, here they are.
>
> Review #1
> ---
> 0: (borderline paper)
> In this paper, the authors propose a variant of the adaptive attack on SIDH by Galbraith et al. (GPST). This is no better than any existing attack, and this is acknowledged by the authors. The approach, still playing with the torsion points, is a bit different from the previous ones, though, and gives some insight on the difficult problem underlying supersingular isogeny cryptosystems.
>
> The scenario of the attack is when Alice uses a static key, and Bob runs many key exchanges with her, hence has access to some oracle related to Alice secret. As in GPST, the main idea is that the Weil pairing test is not enough to guarantee that the torsion points were honestly generated by Bob.
>
> The technique also borrows ideas from Petit and others.
>
> An important ingredient in the paper is that Bob does not directly get the images of the points he wants by Alice's isogeny, but only get them up to a multiplicative factor. In other words, he gets images of cyclic subgroups. This is shown to be sufficient to mount an attack.
>
> Due to the fact that this does not bring any new attack scenario,
> I consider that this is a borderline case.
>
> There are also quite a few math typos that make it difficult to read in the present state (but this should be easy to fix).

Minor remarks and typos:
- page 6: replace P_A by Q_A (after "He generates...")
- page 7: "of degree N_A" (instead of A)
- page 7: missing hat over \psi_2 in Eq 2
- page 7: replace \phi_1 by \psi_1 (3 lines after Eq 2)
- page 8: replace A by N_A
- page 9: "bey solving" -> "by solving"
- page 9: e_{N_N} -> e_N
- page 11: "Let G_1, G_2, G_3 are cyclic subgroups of E_0[N_BN] order"
-> "Let G_1, G_2, G_3 BE cyclic subgroups of E_0[N_BN] OF order"
(2 typos, here)
- page 11: replace r by n (twice)
- page 11: the last paragraph speaks about \mu, which is not yet defined.
- page 12: replace "the" by "then in Lemma 2.
- page 12: remove "since" in "a random supersingular curve since"
- page 13, in Algorithm 1:
- in "Require", replace P_M and Q_M by B_P and Q_B
- missing _{G_i} for the phi's in lines 6 and 15
- missing _{G_i} for E in lines 9 and 18
- page 16: the statement of Theorem 2 is not standalone: the complexity
talks about u_j, v_i and l_i, but these are internal to Algorithm 4.
The complexity should be expressed in terms of log p, in order to show
that this is a polynomial-time attack.
- in the References, bibtex has killed the capitals in some titles, e.g.
Sidh, sike, ...

Review #2

This paper presents an active attack on SIDH, during which malicious Bob manages to compute Alice's (static) secret isogeny in polynomial time, by repeatedly sending her manipulated public keys. More precisely, the manipulation happens at the level of the "auxiliary torsion points" that form part of the key. Such an active attack was already presented by Galbraith, Petit, Shani and Ti at Asiacrypt 2016. The current attack is quite different in nature: using manipulated torsion points it tricks Alice into revealing the action of her secret isogeny on a much larger subgroup than intended. As such, the scheme becomes vulnerable to a passive attack due to Petit (or its updated version due to de Quehen et al.), which breaks all instances of SIDH in which Alice and Bob's torsion subgroups are highly unbalanced.

The idea is certainly neat, and I also liked the generalization of Petit's attack to the setting where one reveals the action on subgroups, rather than individual points, as described in Section 3. But overall I think that the paper is a little lightweight, and since it does not improve upon the state-of-the-art (the attack is slower and more far-fetched than that of Galbraith et al.) I would be inclined towards rejection. The authors' main selling point is that this is "a new cryptanalytic tool for isogeny-based cryptography". I partly buy this, and the idea deserves to be communicated, but I'm not sure it is convincing enough for CT-RSA.

While the general structure and flow is good, the paper contains many typos and would benefit from several round of proofreading (including the bibliography, e.g. capitalization of prf, sidh, ...). I will restrict to the mathematical/symbolic issues that I've spotted:

> * p3 "three cyclic disjoint groups G1, G2, G3 \in E_0[N_B] of order N_B*N" --> E_0[N_B] does not contain any cyclic subgroups of said order
> * p5 "In SIDH, given (E_B, R, S) returned by Bob" --> did you want to write R_a, S_a?
> * p6 "He generates (E_B, phi_B(P_A), phi_B(P_A)) ..." --> second P_A should be Q_A
> * p6 alpha --> \alpha
> * p6 the K_i in the formula for d should be left out
> * p7 {P,Q} --> <P,Q>
> * p7 "isogeny of degree A" --> N_A
> * p7 in formula (2) you should swap \psi_1 and \psi_2, and similarly in the two occurrences of that right-hand side about 6-7 lines below
> * p7 "the kernels of the isogenies \phi_1 : E -> E_1 and ..." --> that should be \psi_1
> * p8 in item 3 on quantum claw-finding, there is an A that should be N_A
> * p9 "we can evaluate [\lambda] \circ \psi" --> should be \phi
> * p9 "the equation x^2 \equiv a^2 \mod N_B has more than two solutions" --> may have more than two solutions (e.g. if N_B is twice a prime power it will still have two)
> * p9 "and N is coprime to d" --> "and N_A is coprime to N_B" (also, you already use this a few lines before, when saying that {Q_1, Q_2} is a basis of E[N_B], so maybe that would have been a more natural place to refer to this coprimality
> * p9 in the Weil pairings, all lower indices N (and there is also an occurrence of N_N) should be N_B
> * p11 "\mathcal{N}-smooth" --> you did not define \mathcal{N}, and never come back to this, so I would just write "smooth"
> * p11 at two occasions you write G_1 \cap G_2 \cap G_3 = {0} as an assumption, but I don't think that this is strong enough, you really want G_1 \cap G_2 = G_1 \cap G_3 = G_2 \cap G_3 = {0}
> * p11 say what mu is when you first use it
> * p11 "Then if H is the image of the group G through \phi" --> \phi_A
> * p12 In the proof of Lemma 2, say that you assume E_H = E_G / phi_G(ker phi_A), as this is not clear from the start. The first sentence of the second paragraph (ending in "since.") is incomplete.
> * p13 in the pseudocode of Algorithm 1, P_M and Q_M should be P_B and Q_B
> * p14 in the proof of Lemma 5 there is an \epsilon^t that should be \epsilon^k
> * p15 I did not understand what you mean with "let N = \prod \ell_i^2 = p^{1 + \epsilon}" (well, I have an idea, but the sentence is not clear)
> * p16 in the pseudocode of Algorithm 4, one should return ker(\phi_A) rather than ker(\psi_A)
> * p16 the discussion below Algorithm 4 contains two occurrences of ell that should be ell_i
>
> On Tue, Oct 26, 2021 at 8:30 AM Moody, Dustin (Fed) <dustin.moody@nist.gov> wrote:
>
>> Gorjan,
>>
>> I'd say not to fight for it. To me the idea is theoretically interesting, but it will have no practical impact.
>>
>> I would be curious to see the other reviews, if that's possible. If not - that's fine of course.
>>
>> Dustin

From: Gorjan Alagic (b) (6) [redacted]
Sent: Tuesday, October 26, 2021 7:42 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: CT-RSA paper on attacks on SIDH

Hi Dustin,

Thanks again for that review. The other reviews have come in now. While I think you all agree on the facts of the paper, the other reviewers seem to think the attack is just not that interesting, and gave it a borderline score.

So, if you think the paper is worth fighting for, let me know and I'm happy to do that. Otherwise it will probably not get in.

Best,
Gorjan

On Fri, Oct 15, 2021 at 7:48 AM Gorjan Alagic (b) (6) [redacted] wrote:

> Great, thanks Dustin! I will let you know if I have any questions, or if any issues come up during discussion. Thanks again for your help! -Gorjan
>
> On Thu, Oct 14, 2021 at 3:46 PM Moody, Dustin (Fed) <dustin.moody@nist.gov> wrote:
>
> > Gorjan,
> >
> > I submitted my review via EasyChair. I recommended to accept it. Let me know if you have any questions or anything.
> >
> > Dustin
> >
> > ---
> >
> > **From:** Gorjan Alagic (b) (6) [redacted]
> > **Sent:** Monday, September 27, 2021 3:21 PM
> > **To:** Moody, Dustin (Fed) <dustin.moody@nist.gov>
> > **Subject:** Re: CT-RSA paper on attacks on SIDH
> >
> > Great, thanks! Below are the review guidelines, and I will send you the official invite from EasyChair shortly. Thanks again! -Gorjan
> >
> > \---
> >
> > Review Guidelines for CT-RSA 2022
> >
> > Please provide a detailed review, including a justification for your scores. Both the score and the review text are required.
> >
> > Writing a Report
> > Each reviewer assigns a grade to each reviewed paper to reflect the recommendation on acceptance/rejection for the paper, as well as a weight to reflect the confidence of

the reviewer in the recommendation.

Overall grades:
3: strong accept
2: accept
1: weak accept
0: borderline paper
-1: weak reject
-2: reject
-3: strong reject

Reviewer's confidence:
5: (expert)
4: (high)
3: (medium)
2: (low)
1: (none)

Report Style
Your report should be critical but constructive. Explain the goal of the paper and its strengths. Of course you should mention problems or weaknesses, but please refrain from using aggressive language or making personalised comments in your reviews. Try to be as precise as possible in the parts of your reviews that are related to technical and editorial issues.

In short: Try to write the sort of reviews that you would like to receive as an author.

Report contents
Reports will consist of grades, a weight, and comments. The comments should help the authors as well as other committee members understand your opinions. Please don't write one-line reviews and don't over-use the "Confidential remarks for the program committe" field. (It is ok for the "Confidential remarks for the program committe" field to be empty.) Authors of rejected papers deserve to know why their papers were rejected, and we want accepted papers to be improved based on our comments. There is no additional structure to the reports that you have to follow. However, here are a few points that you may want to refer to when organising and writing your report:

- Summary of the problem and paper contribution.
- What is best about the paper: new ideas, proofs, simplifications, formalisations, implementation, performance improvement, new insight, etc.
- What are the paper's weaknesses: lack of originality, small increment over previous work, unsubstantiated claims, bad presentation, insufficient discussion of relation with prior work etc.
- Target audience: who will be interested in the results, who will be benefited from its publication in the proceedings, who will want to hear the talk at the conference.
- Summary of recommendation: Accept/Reject, main reason.
- Further, detailed technical comments.

On Mon, Sep 27, 2021 at 8:46 AM Moody, Dustin (Fed) <dustin.moody@nist.gov>

>>>> wrote:
>>>>
>>>>> Sure, Gorjan.
>>>>>
>>>>> Happy to do it.
>>>>>
>>>>> ---
>>>>>
>>>>> **From:** Gorjan Alagic (b) (6)
>>>>> **Sent:** Sunday, September 26, 2021 9:17 AM
>>>>> **To:** Moody, Dustin (Fed) <dustin.moody@nist.gov>
>>>>> **Subject:** CT-RSA paper on attacks on SIDH
>>>>>
>>>>> Hi Dustin,
>>>>>
>>>>> I'm on the PC for CT-RSA and one of the papers in my pile is about an apparently new adaptive attack on SIDH. The paper is attached below. Would you like to review it? I would need the review by October 26th.
>>>>>
>>>>> If you're interested, let me know and I will send the official invite + review guidelines.
>>>>>
>>>>> Thanks!
>>>>> Gorjan