From: Ward Beullens <ward@beullens.com>
Sent: Monday, October 26, 2020 5:34 AM
To: pqc-comments
Cc: pqc-forum
Subject: ROUND 3 OFFICIAL COMMENT: Rainbow

Hi everyone,

I found 2 new attacks on the Rainbow signature scheme. The first attack uses the ideas from the Kipnis-Shamir attack [1] and reduces the security of Rainbow I, III and V by 7 bits, 4 bits and 19 bits respectively. This attack also applies to the UOV scheme.

The second attack is specific to Rainbow and is also more efficient. It reduces a key recovery to a new instance of the MinRank problem, which can then be solved with the methods of Bardet et al.[2] . This attack reduces the security level of Rainbow I, III and V by 20 bits, 40 bits and 55 bits respectively.

The paper is on ePrint: https://eprint.iacr.org/2020/1343

I would like to thank the Rainbow team for reviewing an earlier version of the paper and providing me with helpful feedback.

All the best,
Ward

[1] https://link.springer.com/chapter/10.1007/BFb0055733
[2] https://arxiv.org/abs/2002.08322

From: Bo-Yin Yang <moscito@gmail.com>
Sent: Monday, October 26, 2020 9:46 AM
To: pqc-forum
Cc: Ward Beullens; pqc-forum; pqc-comments
Subject: Re: ROUND 3 OFFICIAL COMMENT: Rainbow

Dear All,

The Rainbow team acknowledges that the new attacks by Ward Beullens are fundamentally correct and does cut down the security of Rainbow somewhat, in the same manner as most other schemes still in the NIST competition have lost a considerable number of security bits. We are actively studying the consequences and will formulate a comprehensive response including a new set of parameters soon.

Bo-Yin, for the Rainbow team members

On Monday, October 26, 2020 at 5:34:41 PM UTC+8 Ward Beullens wrote:

> Hi everyone,
>
> I found 2 new attacks on the Rainbow signature scheme. The first attack uses the ideas from the Kipnis-Shamir attack [1] and reduces the security of Rainbow I, III and V by 7 bits, 4 bits and 19 bits respectively. This attack also applies to the UOV scheme.
>
> The second attack is specific to Rainbow and is also more efficient. It reduces a key recovery to a new instance of the MinRank problem, which can then be solved with the methods of Bardet et al.[2] . This attack reduces the security level of Rainbow I, III and V by 20 bits, 40 bits and 55 bits respectively.
>
> The paper is on ePrint: https://eprint.iacr.org/2020/1343
>
> I would like to thank the Rainbow team for reviewing an earlier version of the paper and providing me with helpful feedback.
>
> All the best,
> Ward
>
> [1] https://link.springer.com/chapter/10.1007/BFb0055733
> [2] https://arxiv.org/abs/2002.08322