From: pqc-forum@list.nist.gov on behalf of River Moreira Ferreira <river.moreira-ferreira@lip6.fr>
Sent: Tuesday, February 20, 2024 9:55 AM
To: pqc-forum
Cc: Ludovic Perret
Subject: [pqc-forum] Official comment: Attack on PROV v1.0 specification

Dear,

We would like to inform the community that we have found a vulnerability in the first specification of PROV (v1.0).
We observed that a small part of the secret-key is (indirectly) leaked during the signature generation process.
Indeed, the signature generation reveals a vinegar vector which is deterministically generated as v=Hash(3|| msg) (constant for a given message).
Given a signature s and the corresponding vinegar vector v, one can recover a vector o in the secret linear subspace (o = s - v, by definition of s).
This allows then to recover the entire secret-key in polynomial-time by slightly adapting to PROV a result from Pierre Pébereau “One vector to rule them all: Key recovery from one vector in UOV schemes” (available from https://eprint.iacr.org/2023/1131

We implemented the key-recovery attack, and it works well (few seconds for every security level).

The attack is not structural and can be avoided by generating the vinegar vector with the hash of the secret seed, for example v=Hash(3||seed_sk||msg).
The designer of PROV has been informed of this vulnerability and a new version of the specification (v1.1) is already available with the countermeasure (see https://prov-sign.github.io/).

We have detailed the results in a paper “Polynomial-Time Key-Recovery Attack on the NIST Specification of PROV” temporarily available from https://nuage.lip6.fr/s/zqSjSnYRndtewRR

[Sorry for multiple receptions, the duplicate will be remove from the archive]

Best regards,
Ludovic Perret, River Moreira Ferreira

From: pqc-forum@list.nist.gov on behalf of Louis Goubin <Louis.Goubin@uvsq.fr>
Sent: Thursday, April 4, 2024 5:50 AM
To: pqc-forum
Subject: Re: [pqc-forum] Official comment: Attack on PROV v1.0 specification

Dear Ludovic and River,

Thanks for pointing out this vulnerability, and for showing how it allows to break the scheme. Note that we were aware of this error, and had scheduled to correct it in the next version of PROV, but once again we would like to express our gratitude to you for communicating your findings to us transparently.

As mentioned in your message, we have already published PROV version 1.1 on our website (https://prov-sign.github.io/). This version corrects the error in the specification of the original 1.0 version, where the secret key seed was not included in the input to the hash function when generating the vinegar vector during signing.

Best wishes,

Louis Goubin, on behalf of the PROV team

Le 20/02/2024 à 15:55, River Moreira Ferreira a écrit :

> Dear,
>
> We would like to inform the community that we have found a
> vulnerability in the first specification of PROV (v1.0).
> We observed that a small part of the secret-key is (indirectly) leaked
> during the signature generation process.
> Indeed, the signature generation reveals a vinegar vector which is
> deterministically generated as v=Hash(3|| msg) (constant for a given
> message).
> Given a signature s and the corresponding vinegar vector v, one can
> recover a vector o in the secret linear subspace (o = s - v, by
> definition of s).
> This allows then to recover the entire secret-key in polynomial-time
> by slightly adapting to PROV a result from Pierre Pébereau “One vector
> to rule them all: Key recovery from one vector in UOV schemes”
> (available from
https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Feprint.iacr.org%2F2023%2F1131&data=05%7C02%7Csara.kerman%40nist.gov%7Ca23b4ee48e704b61707808dc548c98c4%7C2ab5d82fd8fa4797a93e054655c61dec%7C0%7C0%7C638478211240390256%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C80000%7C%7C%7C&sdata=h5pN9mxdp2yqk%2FcKkQ%2FT9izA4iZbWsgCM1KSumK0xs0%3D&reserved=0).
>
> We implemented the key-recovery attack, and it works well (few seconds