From: Jannis Fengler <fenglerjannis@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] Questions regarding Falcon-512
Date: Wednesday, December 28, 2022 01:42:08 AM ET

I am thinking to use Falcon-512 in a blockchain setting. For ecdsa keys, it is common to take 12 or 24 random words from a wordlist (for example BIP 39). Usually 128 bits of entropy map to a 12-word seed phrase and 256 to a 24-word seed phrase. These words are concatenated and after a sha2 and a checksum, the result is the private ecdsa key. The derivation from the seed phrase to the private key is deterministic.
The construction of Falcon keys is very difficult. Is it possible to derive a private key deterministically?

Ecdsa signatures always have a fixed length. I was playing around with lib-oqs and it seems that the Falcon signatures have a variable length. I need a fixed length in my setting, so I was thinking about padding the signatures with zeros. But space is expensive in a blockchain. So my Questions are:

What is the maximum Falcon signature length?

Does it undermine security, if I generate multiple signatures for one message and choose the shortest one?

Best regards,

Jannis | www.eomii.org

From: Bas Westerbaan <bas@cloudflare.com> via pqc-forum <pqc-forum@list.nist.gov>
To: Jannis Fengler <fenglerjannis@gmail.com>
CC: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Questions regarding Falcon-512
Date: Wednesday, December 28, 2022 05:13:18 AM ET

> The construction of Falcon keys is very difficult. Is it possible to derive a private key deterministically?

For every scheme it's possible to make key generation deterministic by replacing "randombytes()" calls by calls to a XOF that has been seeded by the "private key seed". For some, like RSA, it's not practical because key generation is slow. For Falcon it should be fast enough for this application.

I think for applications like these (eg. FIDO), it'd be great if these private key seeds be part of the standard.

> Ecdsa signatures always have a fixed length. I was playing around with lib-oqs and it seems that the Falcon signatures have a variable length.

The latest version of Falcon has fixed signature size. This was a change from round 2 to 3 IIRC.

Best,

Bas

From: Jannis Fengler <fenglerjannis@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
CC: b...@cloudflare.com <bas@cloudflare.com>, pqc-forum <pqc-forum@list.nist.gov>, Jannis Fengler <fenglerjannis@gmail.com>
Subject: Re: [pqc-forum] Questions regarding Falcon-512
Date: Wednesday, December 28, 2022 05:26:02 PM ET

Oh, that's great. Thank you so much for your fast response!

b...@cloudflare.com schrieb am Mittwoch, 28. Dezember 2022 um 11:13:11 UTC+1:

> The construction of Falcon keys is very difficult. Is it possible to derive a private key deterministically?

For every scheme it's possible to make key generation deterministic by replacing "randombytes()" calls by calls to a XOF that has been seeded by the "private key seed". For some, like RSA, it's not practical because key generation is slow. For Falcon it should be fast enough for this application.

I think for applications like these (eg. FIDO), it'd be great if these private key seeds be part of the standard.

> Ecdsa signatures always have a fixed length. I was playing around with lib-oqs and it seems that the Falcon signatures have a variable length.

The latest version of Falcon has fixed signature size. This was a change from round 2 to 3 IIRC.

Best,

Bas

From: Fx FRT <talaverafructifera@gmail.com> via pqc-forum@list.nist.gov
To: Bas Westerbaan <bas@cloudflare.com>
CC: Jannis Fengler <fenglerjannis@gmail.com>, pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Questions regarding Falcon-512
Date: Thursday, December 29, 2022 12:47:17 PM ET

Bas, if You're are trying make Some ramdorizem words part of bytes un ASCII can make múltiple un if if else if else do do if else etc..well is common think un baremo to put schemes un the rate of random and derivations NOR NAND o OR AND NOT, etc by percent of variability with time and what is your case? What you want to move, I think is 66665 or 66666 high 66664 is in c like said considered low level to circunstance of 1,5 ×10 ^ 24 (G bytes)hz to be the normal processors and now with dynamic floats ssdd memories
can trap others concussion respond in the program automatically too to be confident I make the random of the ramdoms in 1997 when I appear with my 33×01tt 64 bits ramdoms of 32 in up and 32 in down and if you also make it possible you also can do a good conversor or data in your phone or include a good compressor but also if you know algorithms with sense like $(1-x)^n$=d(x)and you put =x^n-1 so only had to press if else x=((x*-x)-x*+x)=01×x so you can trust to be 1 and then if is 0 but not nominal so you also can change the algorithm or something or you can divide to make with key this others programs codification or multiplexer or de multiplexer if key is simple ramdorizem const are to be byte BITTER and then run

But instead I said this like compressor in ultimate think well is all right in C +

Others lenguages requires ramdoms of entry or back lines that I'd likes after req or resq etc well for more complex you also, well it like if you also make my 3301tt you also came to the back stars in our case psyquiatrism and problems that you don't like very well

El mié., 28 dic. 2022 11:13, 'Bas Westerbaan' via pqc-forum <pqc-forum@list.nist.gov> escribió:

> The construction of Falcon keys is very difficult. Is it possible to derive a private key deterministically?

For every scheme it's possible to make key generation deterministic by replacing "randombytes()" calls by calls to a XOF that has been seeded by the "private key seed". For some, like RSA, it's not practical because key generation is slow. For Falcon it should be fast enough for this application.

> I think for applications like these (eg. FIDO), it'd be great if these private key seeds be part of the standard.
>
> > Ecdsa signatures always have a fixed length. I was playing around with lib-oqs and it seems that the Falcon signatures have a variable length.
>
> The latest version of Falcon has fixed signature size. This was a change from round 2 to 3 IIRC.
>
> Best,
>
> Bas
>
> --
> 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/CAMjbhoUQ8YsGyJvv%3DhnCORxkp0ARhVvXxzGOrOMkW5O14MuQ4Q%40mail.gmail.com.

--
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/CAOP7cWb6Yea2E8E5UFmDcBTWEYLhh03vhOX8JnOeTzcp5aSmhw%40mail.gmail.com.