From: buyo buyo <cdnefa@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] PQCrypto: Integrating Post Quantum Cryptography into Golang
Date: Wednesday, March 23, 2022 04:07:41 AM ET

PQCrypto is a cryptography project, which considers crypto agility and integrates go 1.17.6 crypto(a fork of it), Open Quantum Safe (OQS) liboqs/liboqs-go 0.7.12 and tjfoc gmsm-1.4.13. This project aims to study the migration and application adaptation of post quantum cryptography (PQC) algorithms and Chinese national commercial cryptography algorithms (sm-series).

If anyone interests our work, please visit https://github.com/buyobuyo404/PQCrypto

--
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/b881bdff-5a02-4082-a7cd-26f707084069n%40list.nist.gov.

From: Kris Kwiatkowski <kris@amongbytes.com> via pqc-forum@list.nist.gov
To: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] PQCrypto: Integrating Post Quantum Cryptography into Golang
Date: Wednesday, March 23, 2022 04:43:24 AM ET

Hello,

Thanks for information. Just FYI CIRCL library already has number
of PQ implementations in Go:
https://github.com/cloudflare/circl

FWIW, SM3 in Go can be found here:
https://github.com/kriskwiatkowski/nobs/tree/master/hash/sm3

Cheers,
Kris

On 23/03/2022 08:06, buyo buyo wrote:

> **PQCrypto** is a cryptography project, which considers crypto agility and integrates go 1.17.6 crypto(a fork of it), Open Quantum Safe (OQS) liboqs/liboqs-go 0.7.12 and tjfoc gmsm-1.4.13. This project aims to study the migration and application adaptation of post quantum cryptography (PQC) algorithms and Chinese national commercial cryptography algorithms (sm-series).
>
> If anyone interests our work, please visit https://github.com/buyobuyo404/PQCrypto
>
> --
> 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/b881bdff-5a02-4082-a7cd-26f707084069n%40list.nist.gov.