From: pqc-forum@list.nist.gov on behalf of Violetta Weger <wegerviolетta@gmail.com>
Sent: Friday, December 1, 2023 9:40 AM
To: pqc-forum
Subject: [pqc-forum] Round 1(Additional Signatures) OFFICIAL COMMENT: CROSS

Dear all,

We are happy to announce a new release for CROSS.
The new documentation and the new implementation can be found on the website https://cross-crypto.com

In particular, we present an optimized implementation for the Intel AVX2 and new parameter sets (signing and verification is as fast as 1.28 and 0.78 Mcycles for R-SDP, and 0.94 and 0.55 for R-SDP(G)).

In more details, this new version contains the following modifications:

- We have an **optimized implementation** for the Intel AVX2 instruction set. With this new implementation, each one between signing and verifying takes less than a millisecond on our benchmarking platform (AMD Ryzen 5 Pro 3500U @ 2.1 GHz), and verification is as fast as (about) 250 micro-seconds.

- We have improved the C implementation. We report the results of a stack-size optimized version which can be fit into a Cortex-M4 **microcontroller.**
In particular, all Category 1 memory requirements are below 29 kiB.

- We present an **improved generic decoder** for R-SDP(G) and update the parameters accordingly. The signatures have increased by only 3.5% for the "small signature size" version.

- We propose parameters for a **new optimization corner**: we now consider "fast", "balanced" and "signature size" optimization criteria. The "fast" choice for the number of rounds and weight of the constant weight challenge is the newly introduced choice, and it is aimed at obtaining even lower latency than the previous "fast" choice (now renamed "balanced").

- We now employ a **single auxiliary cryptographic primitive** for both hashing and pseudorandom bit generation: SHAKE. This allows both the software and hardware implementations to use less code/area resources.

We also highlight the performance of CROSS for NIST category I in the attached table.

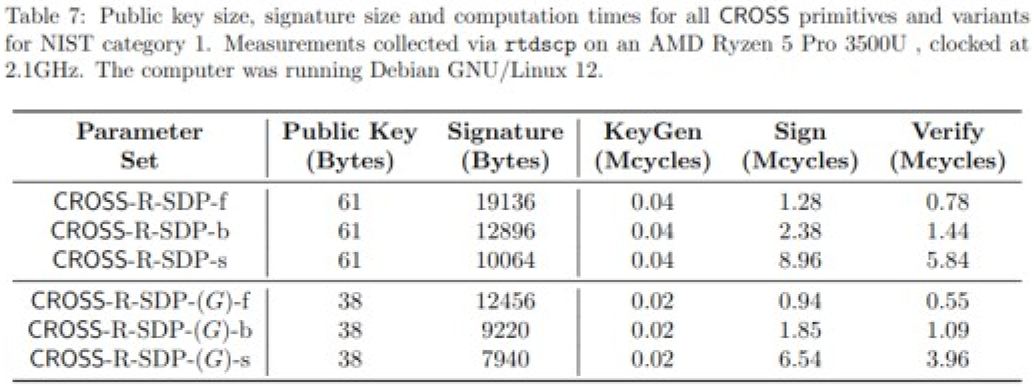

Table 7: Public key size, signature size and computation times for all CROSS primitives and variants for NIST category 1. Measurements collected via `rtdscp` on an AMD Ryzen 5 Pro 3500U , clocked at 2.1GHz. The computer was running Debian GNU/Linux 12.

Parameter Set	Public Key (Bytes)	Signature (Bytes)	KeyGen (Mcycles)	Sign (Mcycles)	Verify (Mcycles)
CROSS-R-SDP-f	61	19136	0.04	1.28	0.78
CROSS-R-SDP-b	61	12896	0.04	2.38	1.44
CROSS-R-SDP-s	61	10064	0.04	8.96	5.84
CROSS-R-SDP-(G)-f	38	12456	0.02	0.94	0.55
CROSS-R-SDP-(G)-b	38	9220	0.02	1.85	1.09
CROSS-R-SDP-(G)-s	38	7940	0.02	6.54	3.96

Best regards,

the CROSS team

--