From: 'Greg Zaverucha' via pqc-forum <pqc-forum@list.nist.gov>
Sent: Wednesday, December 05, 2018 6:16 PM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: [pqc-forum] OFFICIAL COMMENT: Picnic

Dear pqc-forum
I'm writing to announce that the Picnic team has published an updated specification and reference implementation for the algorithm.

The largest change is the addition of additional parameter sets having shorter signatures. The overall design remains the same, but the MPC protocol used to implement the zero-knowledge proof system is different in the new parameter sets. The new MPC protocol is based on the work of Jonathan Katz, Vladimir Kolesnikov and Xiao Wang [KKW18], who have joined the Picnic team.

The new parameter sets reduce signature size by a factor of 2.7 on average. For example, at L1, signatures were 32.8KB and are now 12.3KB. While we do not have an optimized implementation of these parameter sets yet, based on our experience with the implementation described in [KKW18] we expect CPU performance to be comparable to the existing parameter sets.

Another change to the spec addresses a multi-target attack reported to us by Itai Dinur and Niv Nadler. (Their attack should be made public soon.) At a high level, their attack involves an attacker who guesses a secret value used by a signer, derives data from that secret as the signer would, and then compares that data to data from multiple signatures (possibly by multiple signers) to check for a match. If the secret is k bits long and T signatures have been issued, this reduces the expected time for an attack to be successful from 2^k to about 2^(k-7)/T. The change to our spec to address this attack involves having the signer use a random salt value per signature.

I would also like to mention some changes to our optimized implementation, detailed in [KPPRR17] and [D18] that improve signing and verification times by a factor between 1.7 and 3.7. No spec changes were required here.
Links to the updated spec and code can be found on the Picnic website: https://microsoft.github.io/Picnic/

Greg Zaverucha, on behalf of the Picnic team

[KKW18] Jonathan Katz and Vladimir Kolesnikov and Xiao Wang.
Improved Non-Interactive Zero Knowledge with Applications to Post-Quantum Signatures.
Cryptology ePrint Archive: Report 2018/475. https://eprint.iacr.org/2018/475

[KPPRR17] Daniel Kales and Léo Perrin and Angela Promitzer and Sebastian Ramacher and Christian Rechberger.
Improvements to the Linear Operations of LowMC: A Faster Picnic.
Cryptology ePrint Archive: Report 2017/1148. https://eprint.iacr.org/2017/1148

[D18] Itai Dinur. Linear Equivalence of Block Ciphers with Partial Non-Linear Layers: Application to LowMC .
Cryptology ePrint Archive: Report 2018/772. https://eprint.iacr.org/2018/772
--