Summary of Round 3 Changes for Picnic

The Picnic Design Team

September 30, 2020

1 Introduction

The Picnic specification and code were updated with the changes described here (find links to the latest at the Picnic website [Tea19]), as announced on the PQC list on April 15th, 2020. For the Round 3 submission in October we updated the official submission package with these changes. The design document was also be updated with the Picnic3 material in [KZ20].

2 Picnic3 – Revised Parameters

In the round two submission, we added the "Picnic2" parameter sets (`Picnic2-L1-FS`, `Picnic2-L3-FS`, `Picnic2-L5-FS`). These parameters used an alternative MPC protocol (from [KKW18]), and reduced signature sizes by a factor of roughly 2.7. The drawback of Picnic2 was a sharp increase in the CPU costs of the Sign and Verify operations.

By revisiting the parameter choices, and benchmarking many options with an optimized implementation, we found alternative parameters with significantly lower CPU costs. The new parameter sets are called Picnic3 (`Picnic3-L1`, `Picnic3-L3`, `Picnic3-L5`), and Picnic3 will replace Picnic2 in the specification (i.e., `Picnic2-L1-FS`, `Picnic2-L3-FS`, and `Picnic2-L5-FS` are removed). We summarize the differences compared to Picnic2 here, but a detailed description of the changes, rationale, and benchmarks can be found in [KZ20]. The result is that Picnic3 that signs messages 7.9 to 13.9 times faster, and verifies signatures 4.5 to 5.5 times faster than Picnic2, while having nearly the same signature sizes (about 2%, 1% and 5% larger, at security levels L1, L3, L5).

2.1 MPC Improvements

First we change the number of parties per MPC instance, from 64 to 16. This gives much better performance (since each MPC instance is cheaper), but slightly increases signature sizes (as we have to increase the number of instances to maintain security).

We then optimize the MPC computations, pushing more of the work to the preprocessing phase, where the signer has more opportunity for optimization. We also shorten proof size slightly, by recomputing a value rather than sending it (the shares of the output mask). These small changes to the MPC protocol specialize it to the LowMC circuit, and maintain existing security analyses. A side effect of these tweaks is that the specification and implementation of Picnic3 is simpler than Picnic2.

2.2 Full vs. Partial LowMC S-box Layer

We also re-visit the choice of the instance of the block cipher LowMC. Since LowMC is parameterizable, for κ-bit security we can have a LowMC instance with more S-boxes and fewer rounds, or vice versa. We find that using a full S-box layer (i.e., each bit in the state is input to an S-box in every round) performs better than the current instances. This option was missed in the original Picnic design since it requires the state to be a multiple of three, which is not the case when κ is 128 or 256. With a full S-box layer, the number of rounds decreases significantly (improving CPU performance), and the number of AND gates slightly lower than the existing Picnic parameters (giving a small reduction in signature size). Discussion of the security analysis of these alternate LowMC instances is in [KZ20, §4.2].

For L1, we chose to increase the LowMC key and block size to 129 bits, no change was required at L3 (since 192 is a multiple of three), and chose to use a 255 bit key and block size. This means that our choice might fall short of the L5 security by one bit. We made this choice since L5 has considerable security margin, and there is a greater negative impact on performance and implementation complexity when the state size exceeds the 256-bit AVX2 register size. That said, using 258 is also possible should NIST prefer.

3 Picnic-full

The LowMC instances with full S-box layer used by Picnic3 can also be used in parameter sets using the ZKB++ proof system (`Picnic-L1-FS`, `Picnic-L3-FS`, and `Picnic-L5-FS`). This reduces the cost of signing and verification by a factor of 1.3 to 1.8, and signatures are slightly shorter. We therefore defined parameter sets for this combination (`Picnic-L1-full`, `Picnic-L3-full`, and `Picnic-L5-full`). Benchmarks of these parameters are in the ePrint version of [KZ20].

4 Recommended Parameter Sets

Currently there are 12 parameter sets in the Picnic specification, and no guidance on which are recommended by the Picnic team. We will provide the following guidance:

- For applications where speed is more important than signature size: Use Picnic-full (`Picnic-L1-full`, `Picnic-L3-full`, and `Picnic-L5-full`).

- For applications where signature size is more important than speed: Use Picnic3 (`Picnic3-L1`, `Picnic3-L3`, and `Picnic3-L5`).

The other six parameter sets Picnic-*-FS and Picnic-*-UR are moved to historical status, and not recommeded for use or standardization.

Rationale. The UR parameter sets (using the Unruh transform) were originally defined for their QROM analysis. Since then our understanding of the Fiat-Shamir transform security in the QROM has progressed, and we now have a QROM security proof for Picnic3 and Picnic-full, which are much faster and shorter than the UR variant. Both proofs are non-tight, giving only asymptotic guarantees, but the analysis of the UR parameter sets was also non-tight.

The original Picnic-*-FS parameter sets are nearly the same as the Picnic-full parameters, except for the LowMC instance, but the latter is significantly faster with shorter signatures. Having a common set of LowMC instances across all six recommended parameter sets makes implementations simpler (since they need fewer constants), and helps to focus cryptanalysis.

References

[KKW18] Jonathan Katz, Vladimir Kolesnikov, and Xiao Wang. Improved non-interactive zero knowledge with applications to post-quantum signatures. In David Lie, Mohammad Mannan, Michael Backes, and XiaoFeng Wang, editors, *ACM CCS 2018*, pages 525–537. ACM Press, October 2018.

[KZ20] Daniel Kales and Greg Zaverucha. Improving the performance of the picnic signature scheme. To appear in IACR TCHES, Volume 2020, Issue 4., 2020. `https://eprint.iacr.org/2020/427`.

[Tea19] The Picnic Design Team. The Picnic website, March 2019. `https://microsoft.github.io/Picnic/`.