A note on RYDE performances

RYDE Team

Abstract

In this short note, we report improvements on the performances of RYDE up to a factor 2 with respect to RYDE v2.1.0 (without impacting sizes). Should the scheme be selected to advance in the next round of the NIST PQC Standardization Process of Additional Digital Signature Schemes, a new package including these improvements would be released.

Overview. Hereafter, we present speed-ups for RYDE signing and verification algorithms ranging between 1.1 to 2.0 depending on parameter sets. These improvements are due to various optimizations on arithmetic operations and symmetric primitive usage. We made conservative choices regarding symmetric primitive use by considering the recent suggestions from [KX25, KX26] which should provide a clear path towards a security proof in the quantum random oracle model. We recall keys and signature sizes of RYDE in Table 1 and report our recent improvements on its performances in Table 2.

Benchmark platform. New numbers were computed on a machine running Ubuntu Server 22.04.5 LTS, equipped with a 13th-generation Intel(R) Core(TM) i9-13900K CPU running at 3GHz (with efficient core base frequency at 2.2GHz) and 64GB of RAM. All the experiments were performed with Hyper-Threading, Turbo Boost, and SpeedStep features disabled. The results of each parameter set were obtained by computing the average from 25 random instances. To minimize biases from background tasks running on the benchmark platform, each instance has been repeated 25 times and averaged. The scheme has been compiled with Clang (version 22).

Numbers from RYDE v2.1.0 are taken from its specifications. Although the benchmarks have been computed using the same machine, one should note that numbers for RYDE v2.1.0 have been computed using GCC (version 11.4.0), we defer the interested reader to [ABB+25] for additional details.

Instance	sk	pk	σ
RYDE-1-Short	32 B	69 B	3 115 B
RYDE-1-Fast	32 B	69 B	3 597 B
RYDE-1-Faster	32 B	69 B	4 976 B
RYDE-3-Short	48 B	101 B	7 064 B
RYDE-3-Fast	48 B	101 B	8 264 B
RYDE-3-Faster	48 B	101 B	11 672 B
RYDE-5-Short	64 B	132 B	12 607 B
RYDE-5-Fast	64 B	132 B	14 779 B
RYDE-5-Faster	64 B	132 B	20 850 B

Table 1: Keys and signature sizes of RYDE (in Bytes).

Instance		**Performance**			**Comparison**		
Name	Version	Keygen	Sign	Verify	Keygen	Sign	Verify
RYDE-1-Short		34 K	18 M	15 M	-	-	-
RYDE-1-Fast	v2.1.0	34 K	7.0 M	2.8 M	-	-	-
RYDE-1-Faster		34 K	1.7 M	0.9 M	-	-	-
RYDE-1-Short		37 K	14 M	13 M	0.9	**1.3**	**1.2**
RYDE-1-Fast	This Work	37 K	4.1 M	2.3 M	0.9	**1.7**	**1.2**
RYDE-1-Faster		37 K	1.4 M	0.8 M	0.9	**1.2**	**1.1**
RYDE-3-Short		64 K	106 M	94 M	-	-	-
RYDE-3-Fast	v2.1.0	61 K	21 M	17 M	-	-	-
RYDE-3-Faster		61 K	4.8 M	4.3 M	-	-	-
RYDE-3-Short		60 K	55 M	48 M	1.1	**1.9**	**2.0**
RYDE-3-Fast	This Work	60 K	12 M	8.8 M	1.0	**1.8**	**1.9**
RYDE-3-Faster		60 K	2.8 M	2.6 M	1.0	**1.7**	**1.7**
RYDE-5-Short		67 K	141 M	131 M	-	-	-
RYDE-5-Fast	v2.1.0	67 K	29 M	24 M	-	-	-
RYDE-5-Faster		67 K	7.3 M	6.6 M	-	-	-
RYDE-5-Short		67 K	84 M	77 M	1.0	**1.7**	**1.7**
RYDE-5-Fast	This Work	66 K	18 M	14 M	1.0	**1.6**	**1.7**
RYDE-5-Faster		67 K	4.8 M	4.6 M	1.0	**1.5**	**1.4**

Table 2: Performances of RYDE (in CPU cycles). The comparison presents the performance speed-ups with respect to RYDE v2.1.0.

References

[ABB+25] Nicolas Aragon, Magali Bardet, Loïc Bidoux, Jesús-Javier Chi-Domínguez, Victor Dyseryn, Thibauld Feneuil, Philippe Gaborit, Antoine Joux, Romaric Neveu, Matthieu Rivain, Jean-Pierre Tillich, and Adrien Vincotte. RYDE Version 2.1.0. NIST's Post-Quantum Cryptography Standardization of Additional Digital Signature Schemes Project, https://pqc-ryde.org/, 2025.

[KX25] Haruhisa Kosuge and Keita Xagawa. New security proofs of MPC-in-the-head signatures in the quantum random oracle model. Cryptology ePrint Archive, Report 2025/1999, 2025.

[KX26] Haruhisa Kosuge and Keita Xagawa. Towards Formal Security Proofs of MQOM. Cryptology ePrint Archive, Report 2026/629, 2026.