A note on Mirath performances

Mirath Team

Abstract

In this short note, we report improvements on the performances of Mirath up to a factor 2.5 with respect to Mirath v2.1.0. In addition, we also present numbers corresponding to an implementation of the VOLEitH variant of Mirath-b. 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 Mirath signing and verification algorithms ranging between 1.2 to 2.5 depending on parameter sets. These improvements are due to various optimizations on MPC parameters, 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. In addition, we also present numbers corresponding to the VOLEitH variant of Mirath-b featuring speed-ups ranging between 1.7 to 3.2 with respect to Mirath v2.1.0. Numbers for Mirath-a and Mirath-b are given in Tables 1 and 2 respectively.

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

1 Sizes and performances of Mirath-a

Instance		Size & Performance			Comparison		
Name	Version	Sign	Verify	Signature	Sign	Verify	Signature
Mirath-1a-Short	v2.1.0	16 M	14 M	3 182 B	-	-	-
Mirath-1a-Fast	(TCitH)	5.9 M	3.3 M	3 728 B	-	-	-
Mirath-1a-Short	This Work	13 M	11 M	3 182 B	**1.2**	**1.3**	1.00
Mirath-1a-Fast	(TCitH)	2.8 M	1.6 M	3 792 B	**2.1**	**2.1**	1.02
Mirath-3a-Short	v2.1.0	133 M	130 M	7 456 B	-	-	-
Mirath-3a-Fast	(TCitH)	27 M	20 M	8 548 B	-	-	-
Mirath-3a-Short	This Work	57 M	53 M	7 360 B	**2.3**	**2.5**	0.99
Mirath-3a-Fast	(TCitH)	13 M	11 M	8 692 B	**2.1**	**1.8**	1.02
Mirath-5a-Short	v2.1.0	132 M	119 M	13 091 B	-	-	-
Mirath-5a-Fast	(TCitH)	40 M	28 M	15 440 B	-	-	-
Mirath-5a-Short	This Work	78 M	73 M	13 219 B	**1.7**	**1.6**	1.01
Mirath-5a-Fast	(TCitH)	18 M	13 M	15 632 B	**2.2**	**2.2**	1.01

Table 1: Sizes (in Bytes) and Performances (in CPU cycles) of Mirath-a ($q = 16$). The comparison presents the size overhead and the performance speed-ups with respect to Mirath-a v2.1.0.

2 Sizes and performances of Mirath-b

Instance		Size & Performance			Comparison		
Name	Version	Sign	Verify	Signature	Sign	Verify	Signature
Mirath-1b-Short	v2.1.0	24 M	18 M	2 990 B	-	-	-
Mirath-1b-Fast	(TCitH)	9.8 M	5.5 M	3 456 B	-	-	-
Mirath-1b-Short	This Work	18 M	14 M	2 990 B	**1.3**	**1.3**	1.00
Mirath-1b-Fast	(TCitH)	6.2 M	3.9 M	3 584 B	**1.6**	**1.4**	1.04
Mirath-1b-Short	This Work	12 M	10 M	2 966 B	**2.0**	**1.8**	0.99
Mirath-1b-Fast	(VOLEitH)	4.2 M	3.2 M	3 496 B	**2.3**	**1.7**	1.01
Mirath-3b-Short	v2.1.0	112 M	96 M	6 825 B	-	-	-
Mirath-3b-Fast	(TCitH)	47 M	38 M	7 924 B	-	-	-
Mirath-3b-Short	This Work	56 M	47 M	6 969 B	**2.0**	**2.0**	1.02
Mirath-3b-Fast	(TCitH)	21 M	15 M	8 164 B	**2.2**	**2.5**	1.03
Mirath-3b-Short	This Work	47 M	42 M	6 668 B	**2.4**	**2.3**	0.98
Mirath-3b-Fast	(VOLEitH)	16 M	12 M	7 769 B	**2.9**	**3.2**	0.98
Mirath-5b-Short	v2.1.0	155 M	132 M	12 229 B	-	-	-
Mirath-5b-Fast	(TCitH)	70 M	52 M	14 198 B	-	-	-
Mirath-5b-Short	This Work	101 M	87 M	12 485 B	**1.5**	**1.5**	1.02
Mirath-5b-Fast	(TCitH)	37 M	25 M	14 390 B	**1.9**	**2.1**	1.01
Mirath-5b-Short	This Work	77 M	70 M	11 995 B	**2.0**	**1.9**	0.98
Mirath-5b-Fast	(VOLEitH)	25 M	20 M	13 752 B	**2.8**	**2.6**	0.97

Table 2: Sizes (in Bytes) and Performances (in CPU cycles) of Mirath-b ($q = 2$). The comparison presents the size overhead and the performance speed-ups with respect to Mirath-b v2.1.0.

References

[AAB+25] Gora Adj, Nicolas Aragon, Stefano Barbero, Magali Bardet, Emmanuele Bellini, Loïc Bidoux, Jesús-Javier Chi-Domínguez, Victor Dyseryn, Andre Esser, Thibauld Feneuil, Philippe Gaborit, Romaric Neveu, Matthieu Rivain, Luis Rivera-Zamarripa, Carlo Sanna, Jean-Pierre Tillich, Javier Verbel, and Floyd Zweydinger. Mirath version 2.1. NIST's Post-Quantum Cryptography Standardization of Additional Digital Signature Schemes Project, https://pqc-mirath.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.