Errata

Dung H. Duong, Le Van Luyen, Ha T.N. Tran

July 16, 2020

In [1, Section 5], the “optimal" subfield is chosen to be $L = \mathbb{F}_{2^5}$. However, it is not correct since L is not a subfield of $K = \mathbb{F}_{2^8}$. We thank Vishakha VISHAKHA for pointing out this mistake to us.

Hence, we provide here the correction by choosing $L = \mathbb{F}_{2^4}$ together with the choice of new parameters. The Table 3 in [1] can be replaced by the following table. The LRainbow still has an advantage of smaller public key size, with the price of slighly increased signature.

Table 1: Parameters and key sizes of LRainbow and CyclicRainbow

Sec. Level	Scheme(v_1, o_1, o_2)	Public Key (kB)	Signature (B)
100 bits	CyclicRainbow$(26, 16, 17)$	21.7	59
	LRainbow$(26, 18, 22)$	**17.6**	**66**
128 bits	CyclicRainbow(36.21.22)	47.3	79
	LRainbow$(34, 25, 28)$	**39.5**	**87**
192 bits	CyclicRainbow$(63, 33, 33)$	172.3	129
	LRainbow$(55, 40, 44)$	**151.8**	**139**
256 bits	CyclicRainbow$(85, 47, 46)$	459.4	178
	LRainbow$(73, 52, 60)$	**351.4**	**185**

References

[1] Dung Hoang Duong, Le Van Luyen, Ha Thanh Nguyen Tran: Choosing subfields for LUOV and lifting fields for rainbow. IET Information Security 14(2): 196-201 (2020)