# Erratum to BIG QUAKE's proposal

April 8, 2018

- Page 24, § 5.3, Line 9 : "$w_{\mathrm{msg}}$ work factor for message recovery errors." should be "$w_{\mathrm{msg}}$ denotes the logarithm of the work factor for message recovery attacks."
- Page 24, § 5.3, Line 10 : "Keys is a lower bound for the number of..." should be "Keys is a lower bound for the **logarithm** of the number of ..."
- §4.1.1 was unsufficient to understand how to estimate the number of keys. This issue is addressed in the corrected version. In addition, when evaluating the number of keys, we forgot the possible action of the affine group which entails a slight reduction of the number of keys. This is addressed in the corrected version where §5.3.1, 5.3.2 and 5.3.3 have been modified (see columns "Keys" in the three tables: their contents are now slightly smaller than those of the original version).
- In §6, we added a §6.3 providing details on the way extensions of $\mathbb{F}_2$ are represented in our implementation. See Page 25 of our corrected proposal.
- Page 32, Remark 8. The formula is wrong and should be:

$$s_r(2^m) = \begin{cases} m_r(2^m)\left(1-\frac{1}{\ell}\right) & \text{if} \quad \ell \nmid r \\ m_r(2^m)\left(1-\frac{1}{\ell}\right) + \frac{1}{\ell} s_{r/\ell}(2^m) & \end{cases}$$