Le NIST (National Institute of Standards and Technology) vient de mettre à jour le FIPS (Federal Information Processing Standards) 180-3 de Juin 2007 sur les fonctions de hachage. Il convient désormais de se référer au FIPS 180-4 (Secure Hash Standard) de Mars 2012. Les changements concernent la suppression d'une contrainte sur la façon dont est réalisé le padding, ainsi que l'introduction de variantes permettant d'obtenir avec SHA512 des empreintes plus courtes (SHA512/224, SHA512/256 ou plus généralement SHA512/t). Le lecteur intéressé peut se référer au texte .