

# Cryptology ePrint Archive: Report 2011/268

## Birthday Forgery Attack on 128-EIA3 Version 1.5

*Raja Zeshan Haider*

**Abstract:** 128-EIA3 is an integrity algorithm considered for adoption as a third integrity algorithm by European Telecommunication Standard Institute (ETSI) for 4th generation of GSM networks. 128-EIA3 is vulnerable to birthday forgery attack. Birthday forgery attack requires minimum  $2^{16}$  known message-MAC pairs for finding collision in 128-EIA3. 128-EIA3 is susceptible to internal collision of its universal hash function and external collision of its XORing transformation. Birthday forgery attack on 128-EIA3 allows message forgery with success probability greater than  $1/2^{32}$ .

**Category / Keywords:** secret-key cryptography / Message Authentication Code

**Date:** received 26 May 2011

**Contact author:** zeshanjalip at hotmail com

**Available formats:** [PDF](#) | [BibTeX Citation](#)

**Version:** 20110528:180846 ([All versions of this report](#))

**Discussion forum:** [Show discussion](#) | [Start new discussion](#)

---

[ [Cryptology ePrint archive](#) ]