A Forgery Attack on the Candidate LTE Integrity Algorithm 128-EIA3

http://www.firstlight.cn 2010-12-02

In this note we show that the message authentication code 128-EIA3 considered for adoption as one of the integrity algorithms of th e emerging mobile standard LTE is vulnerable to a simple existential forgery attack. This attack allows, given any message and the associate d MAC value under an unknown integrity key and an initial vector, to predict the MAC value of a related message under the same key and th e same initial vector with a success probability 1/2.

存档文本