**3GPP TSG-SA3 Meeting #104-e *S3-212686***

e-meeting, 16 - 27 August 2021

**Title: Response LS on 256-bit algorithms based on SNOW 3G or SNOW V**

**Response to: LS S3-211407 / SAGE (20) 14**

**Source: SA3 (Vodafone, Ericsson, BT)**

**To: ETSI SAGE**

**Cc:**

**Contact person: Tim Evans**

 **Tim.evans1@vodafone.com**

**Send any reply LS to: 3GPP Liaisons Coordinator,** **mailto:3GPPLiaison@etsi.org**

**Attachments:**

# 1 Overall description

SA3 thanks ETSI SAGE for their LS on 256-bit algorithms based on SNOW 3G or SNOW V, and the accompanying prototype algorithm specifications. SA3 has discussed the points raised.

SA3 has also been made aware of a recent research paper analysing SNOW V (<https://eprint.iacr.org/2021/1047>). This paper claims a bitwise linear approximation on SNOW V with correlation 2-49.54, allowing a distinguishing attack using 2240 bits of output, with space complexity
2248.81 and time complexity 2248.81. 2240 bits of output are far more than the SNOW V specification allows, and far more than would ever be used in a 3GPP application, so this does not constitute a direct threat; nevertheless, SA3 expects that SAGE will take this research into account.

 SA3 has come to the following conclusions:

* SA3 agrees that there is value in designing the integrity algorithm so that it can deliver at least a 64-bit MAC, even if that is not used straight away in 5G.
* SA3 expects that SAGE will take the above-mentioned research into account.
* Subject to the outcome of the previous point, SA3 kindly requests SAGE to go ahead and prepare 256-bit algorithms for confidentiality and integrity based on SNOW-V, as one of the proposed 256-bit algorithm sets for future consideration by SA3.

# 2 Actions

**To ETSI SAGE**

**ACTION:** SA3 kindly asks ETSI SAGE to assess the research paper mentioned above, and determine any implications on SNOW V.

**ACTION:** Subject to the outcome of the previous action, SA3 kindly asks ETSI SAGE to proceed with the development of 256-bit encryption and integrity algorithm specifications based on SNOW V.

# 3 Dates of next TSG SA WG 3 meetings

SA3#105 8 - 12 November 2021 Sophia Antipolis, FR

SA3#106 7 - 11 February 2022 TBC, EU