Some work relevant to cryptos for 5G use

Jing Yang, Email:jing.yang@eit.lth.se

Department of Electrical and Information Technology, Lund University

May 19, 2020

3GPP has asked the SAGE group to select and evaluate possible cryptographic primitives for confidentiality and integrity protection in 5G. There are three suites of confidentiality and integrity protection algorithms in LTE, which are respectively AES-128 (in counter mode), SNOW 3G (with 128-bit) and ZUC (with 128-bit). The driving forces for new (or improved) confidentiality and integrity protection algorithms are from two aspects. Firstly, some upper-layer functions in the radio access networks in 5G could be cloudified and the confidentiality/integrity protection operations would likely be moved to the cloud and implemented there under the software environment without specialized hardware support. This makes it challenging for existing confidentiality/integrity algorithms to achieve the targeted speed of 20 Gbps downlink in 5G (with an exception of AES). The other driving force is that now 3GPP standardization organization is looking towards increasing the security level to 256-bit for 5G to resist against quantum computing.

We evaluated the security of SNOW 3G and ZUC to see if they can be directly adopted in 5G with the 256-bit security level. For SNOW 3G, we proposed a correlation attack resulting in key recovery with complexity 2^{177} and a distinguishing attack with compleixty 2^{172}, which indicates that if the key length in SNOW 3G would be increased to 256 bits, the 256-bit security level for long keystreams can not be achieved. For ZUC-256, we gave a distinguishing attack on ZUC-256 with complexity 2^{236}. While the attack is only 2^{20} times faster than exhaustive key search, it indicates that ZUC-256 does not provide a source with full 256-bit entropy in the generated keystream.

We also proposed a new stream cipher SNOW-V, to satisfy the requirements for 5G in terms of speed and security level. The general structure of SNOW-V inherits the design and security principles of SNOW 3G, with a linear LFSR and a non-linear FSM, but both are updated to better align with vectorized implementations to make it efficient under the software environment. The speed can be higher than 22 Gbps for encrypting plaintexts with sizes larger than 256 bytes. Both internal and external evaluations were made on SNOW-V and the results indicate it should be secure.