Universal Mobile Telecommunications System (UMTS); LTE;
Specification of the TUAK algorithm set: A second example algorithm set for the 3GPP authentication and key generation functions $f_1$, $f_1^*$, $f_2$, $f_3$, $f_4$, $f_5$ and $f_5^*$;
Document 6: Security assessment (3GPP TR 35.936 version 13.0.0 Release 13)
Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for ETSI members and non-members, and can be found in ETSI SR 000 314: "Intellectual Property Rights (IPRs): Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards", which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "shall", "shall not", "should", "should not", "may", "need not", "will", "will not", "can" and "cannot" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"must" and "must not" are NOT allowed in ETSI deliverables except when used in direct citation.
Contents

Intellectual Property Rights ......................................................................................................................... 2
Foreword ....................................................................................................................................................... 2
Modal verbs terminology ............................................................................................................................. 2
Foreword ....................................................................................................................................................... 4

1 Scope ....................................................................................................................................................... 5
2 References ............................................................................................................................................... 5
3 Definitions, symbols and abbreviations ................................................................................................. 5
3.1 Definitions ............................................................................................................................................ 5
4 Security assessment of the Tuak algorithm set .................................................................................... 5

Annex A: Change history .............................................................................................................................. 6
History .......................................................................................................................................................... 7