Технический комитет по стандартизации
«Криптографическая защита информации»
(ТК 26)

ПРОЕКТ МЕТОДИЧЕСКИХ РЕКОМЕНДАЦИЙ

КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ ВЫРАБОТКИ КЛЮЧЕЙ ШИФРОВАНИЯ ИНФОРМАЦИИ И АУТЕНТИФИКАЦИОННЫХ ВЕКТОРОВ, ПРЕДНАЗНАЧЕННЫЕ ДЛЯ РЕАЛИЗАЦИИ В АППАРАТНЫХ МОДУЛЯХ ДОВЕРИЯ ДЛЯ ИСПОЛЬЗОВАНИЯ В ПОДВИЖНОЙ РАДИОТЕЛЕФОННОЙ СВЯЗИ

Москва
2016

Содержание

Введение

В настоящее время широкое распространение в мире получили средства коммуникации, основанные на технологии мобильной связи третьего поколения (далее – 3G). 3G объединяет в себе высокоскоростной мобильный доступ к услугам радиосвязи и сети Интернет. При подключении пользователя к сети мобильной связи производится его аутентификация и выработка сеансовых ключей, формируемых из основного ключа, располагающегося на SIM-карте и в центре аутентификации. Рабочей группой по безопасности (TSG SA WG3) консорциума 3rd Generation Partnership Project (3GPP, www.3gpp.org) были разработаны конструкции MILENAGE [1, 2] и TUAK [3, 5, 4] (последняя обладает более высокими эксплуатационными и криптографическим характеристиками), которые содержат наборы примеров базовых функций алгоритма аутентификации и выработки сеансовых ключей. Конструкции MILENAGE и TUAK в качестве базовых криптографических алгоритмов используют алгоритм блочного шифрования AES и хэш-функцию Keccak [7, 8] соответственно. Замена иностранных криптографических алгоритмов в конструкциях MILENAGE и TUAK на отечественные криптографические алгоритмы является актуальной задачей и обеспечит повышение уровня защиты тайны переговоров и персональных данных граждан.

Ниже приводится описание наборов базовых функций криптографических алгоритмов выработки ключей шифрования информации и аутентификационных векторов, предназначенных для реализации в аппаратных модулях доверия для использования в подвижной радиотелефонной связи, и использующих в качестве базового криптографического преобразования отечественный алгоритм хэширования – ГОСТ Р 34.11-2012 [6] с длиной хэш-кода 512 бит, получившие названия S3G-128 и S3G-256 (S3G – Secure 3G).

1 Описание криптографических задач, решаемых с помощью предлагаемого решения

Конструкции S3G-128 и S3G-256 представляют собой криптографические алгоритмы аутентификации и выработки ключей шифрования информации, предназначенные для реализации в аппаратных модулях доверия для использования в подвижной радиотелефонной связи. При это они могут использоваться как в рамках сети 3G, так и, ввиду универсальности используемых механизмов, в сетях более низкого поколения. В частности, данные конструкции предназначены для аутентификации сторон в процессе информационного взаимодействия, а именно абонента (мобильный терминал) и базовой приемно-передающей станцией. В случае корректного завершения процедуры аутентификации между абонентом и базовой приемно-передающей

станцией, конструкции S3G-128 и S3G-256 используются для генерации центром аутентификации и пользователем (мобильный терминал) общих ключей шифрования и контроля целостности передаваемой информации.

2 Описание предлагаемого решения

При описании конструкций S3G-128 и S3G-256 будут использоваться терминология и обозначения введенные в документации 3GPP (см., например [1, 2, 3, 5, 4]). В рамках настоящего описания криптографические алгоритмы выработки ключей шифрования информации и аутентификационных векторов рассматриваются в виде набора некоторых базовых функций, построенных на основе отечественной криптографической хэш-функции ГОСТ Р 34.11-2012 [6] с длиной хэш-кода 512 бит, обозначаемой далее H.

2.1 Обозначения и сокращения

AMF	Authentication Management Field	управляющее поле аутентификации;
AK	Anonymity Key	ключ анонимизации;
CK	Cipher Key	ключ шифрования;
IK	Integrity Key	ключ контроля целостности;
K	Subscriber Key	ключ пользователя (основной ключ);
MAC	Message Authentication Code	код аутентификации;
MAC-A	Network Authentication Code	код аутентификации сети;
MAC-S	Resynchronisation Authentication Code	код аутентификации ресинхронизации;
OP	Operator Variant Algorithm Configuration Field	секретное значение, используемое в конструкции MILENAGE для персонификации оператора связи;
$\mathtt{OP}_\mathtt{C}$		вектор, получаемый из OP и K по правилу $\mathtt{OP}_\mathtt{C} = \mathtt{OP} \oplus \mathtt{E}_\mathtt{K}(\mathtt{OP})$;
RAND	Random Number	случайный вектор;
RES	Response to Challenge	идентификационный отзыв;
XRES	Expected User Response	предполагаемое значение идентификационного отзыва;

SQN	Sequence Number	номер попытки идентификации;
TOP	Operator Variant Algorithm Configuration Field	секретное значение, используемое в наборе функций TUAK для персонификации оператора связи;
$\mathtt{TOP}_C$		вектор, вырабатываемый из TOP и K;

2.2 S3G-128

Результатом функционирования конструкции MILENAGE [1, 2] являются семь значений, получаемых в результате вычисления семи базовых функций $f_1, f_1^*, f_2, f_3, f_4, f_5, f_5^*$. Значения, получаемые в результате вычисления каждой из упомянутых функций, будем ассоциировать с самой функцией, то есть в результате вычисления функции f_1 получается значение f_1, и т.д. В результате вычисления базовых функций конструкции S3G-128 получается семь значений $f_1, f_1^*, f_2, f_3, f_4, f_5, f_5^*$, где

$$
\begin{aligned}
f_1 &= f_1[63]||\ldots||f_1[0] \quad (\mathtt{MAC\text{-}A});\\
f_1^* &= f_1^*[63]||\ldots||f_1^*[0] \quad (\mathtt{MAC\text{-}S});\\
f_2 &= f_2[63]||\ldots||f_2[0] \quad (\mathtt{RES});\\
f_3 &= f_3[127]||\ldots||f_3[0] \quad (\mathtt{CK});\\
f_4 &= f_4[127]||\ldots||f_4[0] \quad (\mathtt{IK});\\
f_5 &= f_5[47]||\ldots||f_5[0] \quad (\mathtt{AK});\\
f_5^* &= f_5^*[47]||\ldots||f_5^*[0] \quad (\mathtt{AK}).
\end{aligned}
$$

2.2.1 Вычисление значения $\mathtt{OP}_C$

Для вычисления значения $\mathtt{OP}_C$ на вход конструкции S3G-128 поступают четыре вектора:

$$
\begin{aligned}
&\mathtt{K} \in V_{128} \quad &&\mathtt{algoname} \in V_{24}\\
&\mathtt{OP} \in V_{128} \quad &&\mathtt{inf}_1 \in V_7
\end{aligned}
$$

Вектор algoname содержит краткое название алгоритма в ASCII-кодировке, а именно «AUT» (без кавычек). Вектор $\mathtt{inf}_1$ равен (0||0||0||0||0||0||0).

Из четырех векторов формируется общий вектор

$$\mathtt{F}_{\mathtt{OP}} = \mathtt{K}||\mathtt{OP}||\mathtt{inf}_1||\mathtt{algoname} \in V_{287}.$$

Затем вычисляется

$$H(\mathtt{F}_{\mathtt{OP}}) = \mathtt{HO}[511]||\ldots||\mathtt{HO}[0] \in V_{512}.$$

Тогда

$$\mathtt{OP}_C = \mathtt{OP}_C[127]||\ldots||\mathtt{OP}_C[0] = \mathtt{HO}[511]||\ldots||\mathtt{HO}[384].$$

Замечание 1. *В соответствии с рекомендациями 3GPP значение* $\mathtt{OP}_C$ *вычисляется на предварительном этапе и хранится на USIM.*

2.2.2 Вычисление значений f_1, f_1^*

Для вычисления значений f_1 и f_1^* на вход конструкции S3G-128 поступают восемь векторов:

$$\begin{array}{llll} \mathtt{K} \in V_{128} & \mathtt{RAND} \in V_{128} & \mathtt{SQN} \in V_{48} & \mathtt{AMF} \in V_{16} \\ \mathtt{OP}_C \in V_{128} & \mathtt{inf}_2 \in V_7 & \mathtt{algoname} \in V_{24} & \mathtt{add} \in V_{32} \end{array}$$

При вычислении значений f_1, f_1^* вектор $\mathtt{inf}_2$ полагается равным $(0||0||0||0||0||0||1)$. Вектор $\mathtt{add}$ полагается равным нулевому вектору длины 32, вместе с тем, при необходимости, значение данного вектора может выбираться оператором связи.

Из восьми векторов формируется общий вектор

$$\mathtt{F}_1 = \mathtt{K}||\mathtt{RAND}||\mathtt{SQN}||\mathtt{AMF}||\mathtt{OP}_C||\mathtt{add}||\mathtt{inf}_2||\mathtt{algoname} \in V_{511}.$$

Затем вычисляется

$$H(\mathtt{F}_1) = \mathtt{HF}_1[511]||\ldots||\mathtt{HF}_1[0] \in V_{512}.$$

Тогда

$$\begin{aligned} f_1 &= f_1[63]||\ldots||f_1[0] = \mathtt{HF}_1[511]||\ldots||\mathtt{HF}_1[448]; \\ f_1^* &= f_1^*[63]||\ldots||f_1^*[0] = \mathtt{HF}_1[447]||\ldots||\mathtt{HF}_1[384]. \end{aligned}$$

Общая схема вычисления значений f_1, f_1^* изображена на рисунке 1.

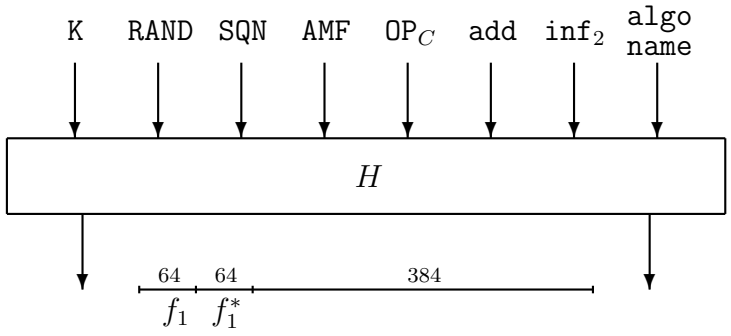

Рис. 1: Вычисление значений f_1, f_1^*

2.2.3 Вычисление значений f_2, f_3, f_4, f_5 и f_5^*

Для вычисления значений f_2, f_3, f_4, f_5 и f_5^* на вход конструкции S3G-128 поступают шесть векторов:

$$\begin{array}{lll} \mathtt{K} \in V_{128} & \mathtt{RAND} \in V_{128} & \mathtt{OP}_C \in V_{128} \\ \mathtt{inf}_3 \in V_7 & \mathtt{algoname} \in V_{24} & \mathtt{add} \in V_{32} \end{array}$$

При вычислении значений f_2, f_3, f_4, f_5 и f_5^* вектор $\mathtt{inf}_3$ полагается равным $(0||0||0||0||0||1||0)$.

Из шести векторов формируется общий вектор

$$\mathtt{F}_2 = \mathtt{K}||\mathtt{RAND}||\mathtt{OP}_C||\mathtt{add}||\mathtt{inf}_3||\mathtt{algoname} \in V_{447}.$$

Затем вычисляется

$$H(\mathtt{F}_2) = \mathtt{HF}_2[511]|| \ldots ||\mathtt{HF}_2[0] \in V_{512}.$$

Тогда

$$\begin{array}{l} f_2 = f_2[63]|| \ldots ||f_2[0] = \mathtt{HF}_2[511]|| \ldots ||\mathtt{HF}_2[448]; \\ f_3 = f_3[127]|| \ldots ||f_3[0] = \mathtt{HF}_2[447]|| \ldots ||\mathtt{HF}_2[320]; \\ f_4 = f_4[127]|| \ldots ||f_4[0] = \mathtt{HF}_2[319]|| \ldots ||\mathtt{HF}_2[192]; \\ f_5 = f_5[47]|| \ldots ||f_5[0] = \mathtt{HF}_2[191]|| \ldots ||\mathtt{HF}_2[144]; \\ f_5^* = f_5^*[47]|| \ldots ||f_5^*[0] = \mathtt{HF}_2[143]|| \ldots ||\mathtt{HF}_2[96]. \end{array}$$

Общая схема вычисления значений f_2, f_3, f_4, f_5 и f_5^* изображена на рисунке 2.

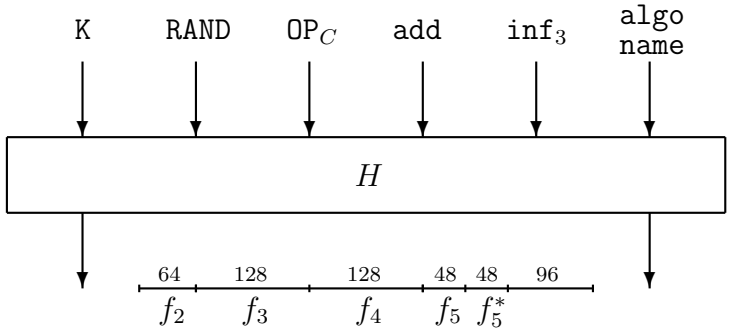

Рис. 2: Вычисление значений f_2, f_3, f_4, f_5 и f_5^*

2.3 S3G-256

Приводится описание базовых функций, предназначенных для замены базовых функций в конструкции TUAK (см., например [3, 5, 4]). При вычислении значений функций из конструкции TUAK используются параметры:

- $\texttt{algoname}$ – строка $\texttt{TUAK1.0}$ в ASCII-кодировке, её размер 56 бит;
- $\texttt{instance}$ – 8-битный вектор, задающий вычисляемую функцию, где
  - $\texttt{instance}[0], \texttt{instance}[1]$ – указывают, какая функция реализуется;
  - $\texttt{instance}[2], \texttt{instance}[3], \texttt{instance}[4]$ – определяют длину $\texttt{MAC-A}$, $\texttt{MAC-S}$, $\texttt{RES}$, либо заполняется нулями в случае вычисления значения функции f_5^* или параметра $\texttt{TOP}_C$;
  - $\texttt{instance}[5], \texttt{instance}[6], \texttt{instance}[7]$ – указывают, равны ли 256 битам длины $\texttt{CK}$, $\texttt{IK}$, $\texttt{K}$.

В конструкции S3G-256 также используются указанные выше параметры. Вектор $\texttt{instance} \in V_8$ совпадает с тем, что используется в TUAK. При этом в качестве $\texttt{algoname}$ выступает 72-битный вектор ($\texttt{algoname} \in V_{72}$), являющийся представлением строки «$\texttt{GOSTR3411}$» в ASCII-кодировке (без кавычек). В рамках конструкции S3G-256 вектор $\texttt{add}$ полагается равным нулевому вектору длины 32, вместе с тем, при необходимости, значение данного вектора может выбираться оператором связи.

2.3.1 Вычисление значения $\texttt{TOP}_C$

Для использования конструкции S3G-256 необходимо вычислить значение параметра $\texttt{TOP}_C$, на вход конструкции S3G-256 поступают пять векторов

$$\begin{array}{llll} \texttt{KV} \in V_{256} & \texttt{instance} \in V_8 & \texttt{algoname} \in V_{72} \\ \texttt{TOP} \in V_{256} & \texttt{inf}_1 \in V_8 \end{array}$$

из которых формируется общий вектор

$$\texttt{T} = \texttt{KV}||\texttt{TOP}||\texttt{instance}||\texttt{inf}_1||\texttt{algoname} \in V_{600},$$

в котором:

- $\texttt{instance} = \texttt{instance}[7]|| \ldots ||\texttt{instance}[0]$, где

$$\texttt{instance}[0] = \cdots = \texttt{instance}[6] = 0,$$
$$\texttt{instance}[7] = \begin{cases} 0, \text{если } |\texttt{K}| = 128; \\ 1, \text{если } |\texttt{K}| = 256, \end{cases}$$

- $\texttt{KV} \in V_{256}$ такой, что

$$\texttt{KV} = \begin{cases} \texttt{K}, & \texttt{K} \in V_{256}; \\ \texttt{K}||\texttt{O}, & \texttt{K} \in V_{128}, \end{cases} \tag{1}$$

  $\texttt{O}$ – нулевой вектор длины 128;

- $\texttt{inf}_1 = (0||0||0||0||0||0||0||0)$.

С использованием хэш-функции и сформированного вектора $\texttt{T}$ вычисляется

$$H(\texttt{T}) = \texttt{HT}[511]|| \ldots ||\texttt{HT}[0] \in V_{512}.$$

Тогда

$$\texttt{TOP}_C = \texttt{TOP}_C[255]|| \ldots ||\texttt{TOP}_C[0] = \texttt{HT}[511]|| \ldots ||\texttt{HT}[256].$$

Замечание 2. *Значение* $\texttt{TOP}_C$ *вычисляется на предварительном этапе и хранится на USIM.*

Общая схема вычисления значения $\texttt{TOP}_C$ изображена на рисунке 3.

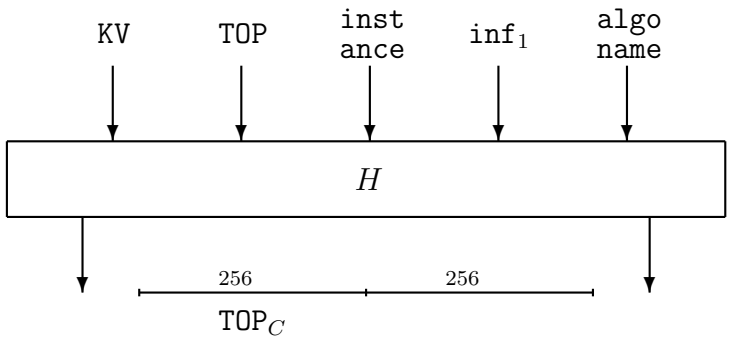

Рис. 3: Вычисление значения $\texttt{TOP}_C$

2.3.2 Вычисление значений f_1 и f_1^*

Для вычисления значений f_1 и f_1^* на вход конструкции S3G-256 поступают девять векторов

$\texttt{KV} \in V_{256}$ $\texttt{SQN} \in V_{48}$ $\texttt{TOP}_C \in V_{256}$ $\texttt{add} \in V_{32}$ $\texttt{algoname} \in V_{72}$
$\texttt{RAND} \in V_{128}$ $\texttt{AMF} \in V_{128}$ $\texttt{instance} \in V_8$ $\texttt{inf}_2 \in V_8$

из которых формируется общий вектор

$$\texttt{F}_1 = \texttt{KV}||\texttt{RAND}||\texttt{SQN}||\texttt{AMF}||\texttt{TOP}_C||\texttt{instance}||\texttt{add}||\texttt{inf}_2||\texttt{algoname} \in V_{936},$$

в котором

- $\texttt{instance} = \texttt{instance}[7]||\ldots||\texttt{instance}[0]$, где

  $\texttt{instance}[0] = \texttt{instance}[1] = 0,$

  $$\texttt{instance}[2]||\texttt{instance}[3]||\texttt{instance}[4] = \begin{cases} 0||0||1, \text{если } |\texttt{MAC}_\texttt{A}| = 64; \\ 0||1||0, \text{если } |\texttt{MAC}_\texttt{A}| = 128; \\ 1||0||0, \text{если } |\texttt{MAC}_\texttt{A}| = 256, \end{cases}$$

  $\texttt{instance}[5] = \texttt{instance}[6] = 0,$

  $$\texttt{instance}[7] = \begin{cases} 0, \text{если } |\texttt{K}| = 128; \\ 1, \text{если } |\texttt{K}| = 256, \end{cases}$$

- $\texttt{KV}$ вычисляется в соответствии с равенством (1);
- $\texttt{inf}_2 = (0||0||0||0||0||0||0||1)$.

С использованием хэш-функции и сформированного вектора $\texttt{F}_1$ вычисляется

$$H(\texttt{F}_1) = \texttt{HF}_1[511]||\ldots||\texttt{HF}_1[0].$$

Тогда значением f_1 будет

- если $|\texttt{MAC}_\texttt{A}| = 64$, то $f_1 = f_1[63]||\ldots||f_1[0] = \texttt{HF}_1[511]||\ldots||\texttt{HF}_1[448]$;
- если $|\texttt{MAC}_\texttt{A}| = 128$, то $f_1 = f_1[127]||\ldots||f_1[0] = \texttt{HF}_1[511]||\ldots||\texttt{HF}_1[384]$;
- если $|\texttt{MAC}_\texttt{A}| = 256$, то $f_1 = f_1[255]||\ldots||f_1[0] = \texttt{HF}_1[511]||\ldots||\texttt{HF}_1[256]$.

Значением f_1^* будет

- если $|\texttt{MAC}_\texttt{S}| = 64$, то $f_1^* = f_1^*[63]||\ldots||f_1^*[0] = \texttt{HF}_1[255]||\ldots||\texttt{HF}_1[192]$;
- если $|\texttt{MAC}_\texttt{S}| = 128$, то $f_1^* = f_1^*[127]||\ldots||f_1^*[0] = \texttt{HF}_1[255]||\ldots||\texttt{HF}_1[128]$;
- если $|\texttt{MAC}_\texttt{S}| = 256$, то $f_1^* = f_1^*[255]||\ldots||f_1^*[0] = \texttt{HF}_1[255]||\ldots||\texttt{HF}_1[0]$.

2.3.3 Вычисление значений f_2, f_5 и f_5^*

Для вычисления значения f_2, f_5 и f_5^* на вход конструкции S3G-256 поступают семь векторов

$$\begin{array}{llll} \texttt{KV} \in V_{256} & \texttt{TOP}_C \in V_{256} & \texttt{add} \in V_{32} & \texttt{algoname} \in V_{72} \\ \texttt{RAND} \in V_{128} & \texttt{instance} \in V_8 & \texttt{inf}_3 \in V_8 & \end{array}$$

из которых формируется общий вектор

$$\texttt{F}_{2,5} = \texttt{KV}||\texttt{RAND}||\texttt{TOP}_C||\texttt{instance}||\texttt{add}||\texttt{inf}_3||\texttt{algoname} \in V_{760},$$

в котором

- $\texttt{instance} = \texttt{instance}[7]||\ldots||\texttt{instance}[0]$, где

  $\texttt{instance}[0] = \texttt{instance}[1] = 1,$

  $$\texttt{instance}[2]||\texttt{instance}[3]||\texttt{instance}[4] = \begin{cases} 0||0||0, \text{если } |\texttt{RES}| = 32; \\ 0||0||1, \text{если } |\texttt{RES}| = 64; \\ 0||1||0, \text{если } |\texttt{RES}| = 128; \\ 1||0||0, \text{если } |\texttt{RES}| = 256, \end{cases}$$

  $$\texttt{instance}[5] = \begin{cases} 0, \text{если } |\texttt{CK}| = 128; \\ 1, \text{если } |\texttt{CK}| = 256, \end{cases}$$

  $$\texttt{instance}[6] = \begin{cases} 0, \text{если } |\texttt{IK}| = 128; \\ 1, \text{если } |\texttt{IK}| = 256, \end{cases}$$

  $$\texttt{instance}[7] = \begin{cases} 0, \text{если } |\texttt{K}| = 128; \\ 1, \text{если } |\texttt{K}| = 256, \end{cases}$$

- $\texttt{KV}$ вычисляется в соответствии с равенством (1);
- $\texttt{inf}_3 = (0||0||0||0||0||0||1||0)$.

С использованием хэш-функции и сформированного вектора $\texttt{F}_{2,5}$ вычисляется

$$H(\texttt{F}_{2,5}) = \texttt{HF}_{2,5}[511]||\ldots||\texttt{HF}_{2,5}[0].$$

Тогда значением f_2 будет

- если $|\texttt{RES}| = 32$, то $f_2 = f_2[31]||\ldots||f_2[0] = \texttt{HF}_{2,5}[511]||\ldots||\texttt{HF}_{2,5}[480]$;
- если $|\texttt{RES}| = 64$, то $f_2 = f_2[63]||\ldots||f_2[0] = \texttt{HF}_{2,5}[511]||\ldots||\texttt{HF}_{2,5}[448]$;
- если $|\texttt{RES}| = 128$, то $f_2 = f_2[127]||\ldots||f_2[0] = \texttt{HF}_{2,5}[511]||\ldots||\texttt{HF}_{2,5}[384]$;
- если $|\texttt{RES}| = 256$, то $f_2 = f_2[255]||\ldots||f_2[0] = \texttt{HF}_{2,5}[511]||\ldots||\texttt{HF}_{2,5}[256]$.

Значением f_5 будет

$$f_5 = f_5[47]||\ldots||f_5[0] = \texttt{HF}_{2,5}[255]||\ldots||\texttt{HF}_{2,5}[208].$$

Значением f_5^* будет

$$f_5^* = f_5^*[47]||\ldots||f_5^*[0] = \texttt{HF}_{2,5}[207]||\ldots||\texttt{HF}_{2,5}[160].$$

2.3.4 Вычисление значений f_3, f_4

Для вычисления значений f_3, f_4 на вход конструкции S3G-256 поступают семь векторов

$$\begin{array}{llll} \mathtt{KV} \in V_{256} & \mathtt{TOP}_C \in V_{256} & \mathtt{add} \in V_{32} & \mathtt{algoname} \in V_{72} \\ \mathtt{RAND} \in V_{128} & \mathtt{instance} \in V_8 & \mathtt{inf}_4 \in V_8 & \end{array}$$

из которых формируется общий вектор

$$\mathtt{F}_{3,4} = \mathtt{KV}||\mathtt{RAND}||\mathtt{TOP}_C||\mathtt{instance}||\mathtt{add}||\mathtt{inf}_4||\mathtt{algoname} \in V_{760},$$

в котором

- $\mathtt{instance} = \mathtt{instance}[7]||\ldots||\mathtt{instance}[0]$, где

  $\mathtt{instance}[0] = 0,\ \mathtt{instance}[1] = 1,$

  $$\mathtt{instance}[2]||\mathtt{instance}[3]||\mathtt{instance}[4] = \begin{cases} 0||0||0, \text{если } |\mathtt{RES}| = 32; \\ 0||0||1, \text{если } |\mathtt{RES}| = 64; \\ 0||1||0, \text{если } |\mathtt{RES}| = 128; \\ 1||0||0, \text{если } |\mathtt{RES}| = 256, \end{cases}$$

  $$\mathtt{instance}[5] = \begin{cases} 0, \text{если } |\mathtt{CK}| = 128; \\ 1, \text{если } |\mathtt{CK}| = 256, \end{cases}$$

  $$\mathtt{instance}[6] = \begin{cases} 0, \text{если } |\mathtt{IK}| = 128; \\ 1, \text{если } |\mathtt{IK}| = 256, \end{cases}$$

  $$\mathtt{instance}[7] = \begin{cases} 0, \text{если } |\mathtt{K}| = 128; \\ 1, \text{если } |\mathtt{K}| = 256, \end{cases}$$

- $\mathtt{KV}$ вычисляется в соответствии с равенством (1),
- $\mathtt{inf}_4 = (0||0||0||0||0||0||1||1)$.

С использованием хэш-функции и сформированного вектора $\mathtt{F}_{3,4}$ вычисляется

$$H(\mathtt{F}_{3,4}) = \mathtt{HF}_{3,4}[511]||\ldots||\mathtt{HF}_{3,4}[0].$$

Тогда значением f_3 будет

- если $|\mathtt{CK}| = 128$, то $f_3 = f_3[127]||\ldots||f_3[0] = \mathtt{HF}_{3,4}[511]||\ldots||\mathtt{HF}_{3,4}[384]$;
- если $|\mathtt{CK}| = 256$, то $f_3 = f_3[255]||\ldots||f_3[0] = \mathtt{HF}_{3,4}[511]||\ldots||\mathtt{HF}_{3,4}[256]$.

Значением f_4 будет

- если $|\mathtt{IK}| = 128$, то $f_4 = f_4[127]||\ldots||f_4[0] = \mathtt{HF}_{3,4}[255]||\ldots||\mathtt{HF}_{3,4}[128]$;
- если $|\mathtt{IK}| = 256$, то $f_4 = f_4[255]||\ldots||f_4[0] = \mathtt{HF}_{3,4}[255]||\ldots||\mathtt{HF}_{3,4}[0]$.

Список литературы

[1] 3GPP TS 35.205 V13.0.0 (2016-01). 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: General (Release 13).

[2] 3GPP TS 35.206 V13.0.0 (2016-01). 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 2: Algorithm Specification (Release 13).

[3] 3GPP TS 35.231 V13.0.0 (2016-01). 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the Tuak algorithm set: A second example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: Algorithm specification (Release 13).

[4] 3GPP TS 35.233 V13.0.0 (2016-01). 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the Tuak algorithm set: A second example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 3: Design conformance test data (Release 13).

[5] ETSI TS 135 232 V13.0.0 (2016-01). Universal Mobile Telelecommunications System (UMTS); LTE; Specification of the TUAK algorithm set: A second example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 2: Implementers' test data (3GPP TS 35.232 version 13.0.0 Release 13).

[6] Национальный стандарт Российской Федерации. ГОСТ 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования.

[7] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche. Cryptographic sponge functions. `http://noekeon.org`.

[8] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche. The keccak reference. `http://noekeon.org`.