Поправка к Р 1323565.1.003-2017 Информационная технология. Криптографическая защита информации. Криптографические алгоритмы выработки ключей шифрования информации и аутентификационных векторов, предназначенные для реализации в аппаратных модулях доверия для использования в подвижной радиотелефонной связи

В каком месте	Напечатано	Должно быть
Пункт 5.1	$F_{OP} = K\|\|algoname\|\|OP\|\|inf_1 \in V_{287}$	$F_{OP} = K\|\|OP\|\|inf_1\|\|algoname \in V_{287}$
Пункт 5.3	Из шести строк $K \in V_{128}$, $RAND \in V_{128}$, $OP_C \in V_{128}$, $inf_2 \in V_7$, $algoname \in V_{24}$, $add \in V_{32}$ формируется строка	Из шести строк $K \in V_{128}$, $RAND \in V_{128}$, $OP_C \in V_{128}$, $inf_3 \in V_7$, $algoname \in V_{24}$, $add \in V_{32}$ формируется строка
Пункт 5.3	$f_2 = f_2[63]\|\|...\|\|f_2[0] = HF_1[511]\|\|...\|\|HF_1[448] \in V_{64}$, $f_3 = f_3[127]\|\|...\|\|f_3[0] = HF_1[447]\|\|...HF_1[320] \in V_{128}$, $f_4 = f_4[127]\|\|...\|\|f_4[0] = HF_1[319]\|\|...\|\|HF_1[192] \in V_{128}$, $f_5 = f_5[47]\|\|...\|\|f_5[0] = HF_1[191]\|\|...\|\|HF_1[144] \in V_{48}$, $f_5^* = f_5^*[47]\|\|...\|\|f_5^*[0] = HF_1[143]\|\|...\|\|HF_1[96] \in V_{48}$.	$f_2 = f_2[63]\|\|...\|\|f_2[0] = HF_2[511]\|\|...\|\|HF_2[448] \in V_{64}$, $f_3 = f_3[127]\|\|...\|\|f_3[0] = HF_2[447]\|\|...\|\|HF_2[320] \in V_{128}$, $f_4 = f_4[127]\|\|...\|\|f_4[0] = HF_2[319]\|\|...\|\|HF_2[192] \in V_{128}$, $f_5 = f_5[47]\|\|...\|\|f_5[0] = HF_2[191]\|\|...\|\|HF_2[144] \in V_{48}$, $f_5^* = f_5^*[47]\|\|...\|\|f_5^*[0] = HF_2[143]\|\|...\|\|HF_2[96] \in V_{48}$.
Пункт 6.2	Из девяти строк $KV \in V_{256}$, $RAND \in V_{128}$, $SQN \in V_{48}$, $AMF \in V_{128}$, $TOP_C \in V_{128}$, $instance \in V_8$, $add \in V_{32}$, $inf_2 \in V_8$, $algoname \in V_{72}$ формируется строка	Из девяти строк $KV \in V_{256}$, $RAND \in V_{128}$, $SQN \in V_{48}$, $AMF \in V_{128}$, $TOP_C \in V_{256}$, $instance \in V_8$, $add \in V_{32}$, $inf_2 \in V_8$, $algoname \in V_{72}$ формируется строка
Пункт 6.3	Из семи строк $RV \in V_{256}$, $RAND \in V_{128}$, $TOP_C \in V_{128}$, $instance \in V_8$, $add \in V_{32}$, $inf_3 \in V_8$, $algoname \in V_{72}$ формируется строка	Из семи строк $KV \in V_{256}$, $RAND \in V_{128}$, $TOP_C \in V_{256}$, $instance \in V_8$, $add \in V_{32}$, $inf_3 \in V_8$, $algoname \in V_{72}$ формируется строка
Пункт 6.4	Из семи строк $KV \in V_{256}$, $RAND \in V_{128}$, $TOP_C \in V_{128}$, $instance \in V_8$, $add \in V_{32}$, $inf_4 \in V_8$, $algoname \in V_{72}$ формируется строка $F_{3,4} = KV\|\|RAND\|\|TOP_C\|\|instance\|\|add\|\|inf_4\|\|algonsme \in V_{760}$, где $instance[0] = instance[1] = 1$,	Из семи строк $KV \in V_{256}$, $RAND \in V_{128}$, $TOP_C \in V_{256}$, $instance \in V_8$, $add \in V_{32}$, $inf_4 \in V_8$, $algoname \in V_{72}$ формируется строка $F_{3,4} = KV\|\|RAND\|\|TOP_C\|\|instance\|\|add\|\|inf_4\|\|algoname \in V_{760}$, где $instance[0] = 0, instance[1] = 1$,
Пункт А.2.1	Двоичное представление строки $inf_1 = (0\|\|0\|\|0\|\|0\|\|0\|\|0\|\|0)$,	Двоичное представление строки $inf_1 = (0\|\|0\|\|0\|\|0\|\|0\|\|0\|\|0\|\|0)$,
Пункт А.2.2	Двоичное представление строки $inf_2 = (0\|\|0\|\|0\|\|0\|\|0\|\|0\|\|1)$,	Двоичное представление строки $inf_2 = (0\|\|0\|\|0\|\|0\|\|0\|\|0\|\|0\|\|1)$,
Пункт А.2.3	Двоичное представление строки $inf_3 = (0\|\|0\|\|0\|\|0\|\|0\|\|1\|\|0)$,	Двоичное представление строки $inf_3 = (0\|\|0\|\|0\|\|0\|\|0\|\|0\|\|1\|\|0)$,
Пункт А.2.4	Будем считать, что $\|RES\| = 64$ и $\|CK\| = \|IK\| = 128$, тогда строка $instance = 13$. Двоичное представление строки $inf_4 = (0\|\|0\|\|0\|\|0\|\|0\|\|1\|\|1)$,	Будем считать, что $\|RES\| = 64$ и $\|CK\| = \|IK\| = 128$, тогда строка $instance = 12$. Двоичное представление строки $inf_4 = (0\|\|0\|\|0\|\|0\|\|0\|\|0\|\|1\|\|1)$,