



ФЕДЕРАЛЬНАЯ СЛУЖБА
 ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
 ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) **ЗАЯВКА НА ИЗОБРЕТЕНИЕ**

(21), (22) Заявка: **2004129581/09, 05.03.2003**

(30) Приоритет: **05.03.2002 AT A 338/2002**

(43) Дата публикации заявки: **10.06.2005 Бюл. № 16**

(85) Дата перевода заявки РСТ на национальную фазу: **05.10.2004**

(86) Заявка РСТ:
AT 03/00063 (05.03.2003)

(87) Публикация РСТ:
WO 03/075507 (12.09.2003)

Адрес для переписки:
**103735, Москва, ул. Ильинка, 5/2, ООО
 "Союзпатент", пат.пов. С.Б.Фелицыной**

(71) Заявитель(и):
КОРДЕС Рене-Майкл (АТ)

(72) Автор(ы):
ХАФФНЕР Томас М. (АТ)

(74) Патентный поверенный:
Фелицына Светлана Борисовна

(54) **ГЕНЕРАТОР КОДА И УСТРОЙСТВО ДЛЯ СИНХРОННОЙ И АСИНХРОННОЙ, А ТАКЖЕ ПОСТОЯННОЙ ИДЕНТИФИКАЦИИ ИЛИ ШИФРОВАНИЯ И РАСШИФРОВЫВАНИЯ ДАННЫХ ПРОИЗВОЛЬНОЙ ДЛИНЫ**

Формула изобретения

1. Генератор кода с несколькими включенными в генерирующий код ряд (R) элементами (FF_{1,2,...,n}) памяти, например триггерами, причем выход последнего в ряду (R) элемента (FF₅) памяти соединен с входом первого в ряду (R) элемента (FF₁) памяти в окружность, а выходы и входы элементов памяти рекурсивно соединены через промежуточно включенные логические элементы "исключающее ИЛИ", отличающийся тем, что предусмотрен, по меньшей мере, один логический элемент "исключающее ИЛИ" (EXOR_{p1}), первый вход (1) которого соединен с выходом одного находящегося в генерирующем код ряду (R) элемента (FF₁) памяти, второй вход которого (2) соединен с выходом другого находящегося в генерирующем код ряду (R) элемента (FF₃) памяти, а его выход (3) соединен со входом элемента (FF₂) памяти, следующего в генерирующем код ряду (R) за соединенным с первым входом (1) логического элемента "исключающее ИЛИ" (EXOR_{p1}) элементом (FF₂) памяти, при этом выход одного находящегося в генерирующем код ряду (R) элемента (FF₅) памяти соединен с входом инвертора (INV), а выход инвертора (INV) соединен с входом другого находящегося в генерирующем код ряду (R) элемента (FF₁) памяти.

2. Генератор по п.1, отличающийся тем, что в линию, соединяющую второй вход (2), по меньшей мере, одного логического элемента "исключающее ИЛИ" (EXOR_{p1}) и выход другого находящегося в генерирующем код ряду (R) элемента (FF₃) памяти, включен логический элемент "И" (UND_{p1}) таким образом, что выход (4) логического элемента "И" (UND_{p1}) соединен с вторым входом (2) логического элемента "исключающее ИЛИ" (EXOR_{p1}), первый вход (6) логического элемента "И" (UND_{p1}) соединен с выходом другого

находящегося в генерирующем код ряду (R) элемента (FF_3) памяти, а второй вход (5) логического элемента “И” (UND_{p1}) соединен с выходом программирующего код элемента (FF_{p1}) памяти.

3. Генератор по п.1 или 2, отличающийся тем, что предусмотрено несколько логических элементов “исключающее ИЛИ” ($EXOR_{p1,p2,p3,p4}$), первый вход каждого из которых запитывается от выхода одного находящегося в генерирующем код ряду (R) элемента ($FF_{1,2,3,4}$) памяти, а второй вход - от выхода другого находящегося в генерирующем код ряду (R) элемента ($FF_{8,15,20,23}$) памяти, который удален в направлении течения ряда (R) от соответственно соединенного с первым входом элемента ($FF_{1,2,3,4}$) памяти на количество элементов памяти, соответствующее отличному простому числу, которое больше единицы и не является частичной суммой общего числа включенных в ряд (R) элементов ($FF_{1,2,...n}$) памяти.

4. Генератор по п.2, отличающийся тем, что предусмотрено несколько программирующих код соответствующих одному логическому элементу “И” (UND_{p1}) и одному логическому элементу “исключающее ИЛИ” ($EXOR_{p1,p2,p3,p4}$) элементов ($FF_{p1,p2,p3,p4,...pn}$) памяти, которые включены в замкнутый в окружность, программирующий код ряд (RR), и расположен, по меньшей мере, один логический элемент “исключающее ИЛИ” ($EXOR_{pp1}$), первый вход которого соединен с выходом находящегося в программирующем код ряду (RR) элемента (FF_5) памяти, второй вход которого соединен с выходом другого находящегося в программирующем код ряду (RR) элемента (FF_{p5}) памяти, а выход соединен со входом элемента (FF_{p1}) памяти, следующего в программирующем код ряду (RR) за соединенным с первым входом логического элемента “исключающее ИЛИ” ($EXOR_{pp1}$) элементом (FF_{p6}) памяти.

5. Генератор по п.4, отличающийся тем, что в линию, соединяющую второй вход, по меньшей мере, одного логического элемента “исключающее ИЛИ” ($EXOR_{pp1}$) и выход другого находящегося в программирующем код ряду (RR) элемента (FF_{p3}) памяти, включен логический элемент “И” (UND_{pp1}) таким образом, что выход логического элемента “И” (UND_{pp1}) соединен со вторым входом логического элемента “исключающее ИЛИ” ($EXOR_{pp1}$), первый вход логического элемента “И” (UND_{pp1}) соединен с выходом другого находящегося в программирующем код ряду (RR) элемента (FF_{p3}) памяти, а второй вход логического элемента “И” (UND_{pp1}) соединен с выходом элемента (FF_{pp5}) памяти, служащего для программирования программирующего код ряда (RR).

6. Генератор по п.5, отличающийся тем, что предусмотрено несколько, служащих для программирования программирующего код ряда (RR), соответствующих одному логическому элементу “И” (UND_{pp1}) и одному логическому элементу “исключающее ИЛИ” ($EXOR_{pp1}$) элементов ($FF_{pp1,pp2,pp3,pp4,...ppn}$) памяти, которые включены в замкнутый в окружность ряд (RRR), и расположен, по меньшей мере, один логический элемент “исключающее ИЛИ” ($EXOR_{ppp1}$), первый вход которого соединен с выходом находящегося в ряду (RRR) элемента (FF_{pp1}) памяти, второй вход которого соединен с выходом другого находящегося в ряду (RRR) элемента (FF_{pp3}) памяти, а выход соединен с входом элемента (FF_{pp2}) памяти, следующего в ряду (RRR) за соединенным с первым входом логического элемента “исключающее ИЛИ” ($EXOR_{ppp1}$) элементом (FF_{pp2}) памяти.

7. Генератор по любому из пп.1, 2, 4, 5 или 6, отличающийся тем, что он содержит, по меньшей мере, один вывод, по меньшей мере, для одного второго, выполненного идентичным генератора кодов, так что оба генератора кодов могут быть снабжены одновременно одним и тем же программным тактом.

8. Генератор по п.3, отличающийся тем, что он содержит, по меньшей мере, один вывод, по меньшей мере, для одного второго, выполненного идентичным генератора кодов, так что оба генератора кодов могут быть снабжены одновременно одним и тем же программным тактом.

9. Устройство для передачи и приема зашифрованной информации, содержащее, по меньшей мере, два генератора кодов по любому из пп.1-8, отличающееся тем, что каждый генератор кодов имеет, по меньшей мере, один вывод для одновременного снабжения программирующих коды элементов ($FF_{p1,p2,p3,p4}$) памяти всех объединенных генераторов кодов одним и тем же программным тактом, так что программирующие коды элементы

($FF_{p1,p2,p3,...pn}$) памяти всех объединенных генераторов кодов одновременно проходят все возможные комбинации состояний и при одновременном отделении генераторов кодов от программного такта запрограммированы одинаково.

10. Устройство по п.9, отличающееся тем, что каждый генератор кодов имеет два вывода для одновременного снабжения программирующих коды элементов ($FF_{p1,p2,p3,...pn}$) памяти и служащих для программирования программирующих коды элементов ($FF_{p1,p2,p3,...pn}$) памяти элементов ($FF_{pp1,pp2,pp3,pp4,...ppn}$) памяти всех объединенных генераторов кодов двумя протекающими независимо друг от друга программными тактами, причем элементы ($FF_{pp1,pp2,pp3,pp4,...ppn}$) памяти, служащие для программирования программирующих коды элементов ($FF_{p1,p2,p3,...pn}$) памяти, проходят, по меньшей мере, один раз все возможные комбинации состояний, а программирующие код элементы ($FF_{p1,p2,p3,...pn}$) памяти всех объединенных генераторов кодов проходят определенное количество всех возможных комбинаций состояний, а после одновременного отделения генераторов кодов от программных тактов все объединенные генераторы кодов запрограммированы одинаково.

RU 2004129581 A

RU 2004129581 A