Микросхемы KeeLoq
с технологией "прыгающего кода"

Статья основывается на технической документации TB003
компании Microchip Technology Incorporated, USA.

Москва - 2001

тел. (095) 737-7545
www.microchip.ru

Микросхемы KeeLoq с технологией "прыгающего кода"

Статья основывается на технической документации TB003
компании Microchip Technology Incorporated, USA.

Введение

Системы дистанционного управления нашли широкое применение в современных радиоэлектронных устройствах – охранные системы для автомобилей, системы ограничения доступа в помещения, идентификационные системы, управление технологическими процессами и т.д. В качестве среды передачи данных (команд) чаше всего используют – радиоканал, проводной канал связи или ИК лучи.

Относительно простые и недорогие системы дистанционного управления используют однонаправленный канал связи, что приводит к снижению безопасности системы в целом. В таких устройствах, обычно, кодовая комбинация не изменяется или их число ограничено. Системы с обратным каналом связи имеют высокую степень защиты, но из-за своей сложности и высокой стоимости не нашли широкого коммерческого применения.

«Взлом» систем с однонаправленным каналом связи и ограниченным числом кодовых комбинаций возможен за короткий промежуток времени, простым перебором всех возможных вариантов. По такому принципу работают устройства называемые – сканер кода. Например, в устройствах содержащих восемь конфигурационных перемычек (256 комбинаций) отвечающих за выбор кода защиты, код может быть подобран за 32 секунды (пробуя 8 комбинаций в секунду). Даже в системах использующих 16-битный код (более 65 000 комбинаций) время на полный перебор всех вариантов составит около 2 часов. Среднее время подбора кода составляет половину от максимально возможного времени. Методом защиты от сканирования может быть увеличение разрядности кода. Так 66-битный код содержит 7.3x10^19 возможных комбинаций и на его полный перебор уйдет время, равное 2.3x10^11 годам.

Другой способ получения несанкционированного доступа к системе – это использование устройства перехватчика кода. После нажатия кнопки на пульте дистанционного управления кодер передает в эфир кодовую последовательность. Устройство перехвата кода принимает и запоминает данные. Затем при необходимости записанная кодовая комбинация повторяется, что приводит к несанкционированному доступу в систему. Устройства перехвата кода имеют выигрыш по времени по сравнению со сканерами кода.

Следуя из выше сказанного можно сформулировать два правила, которые позволят системе дистанционного управления с однонаправленным каналом связи называться безопасной.

- Число возможных кодовых комбинаций должно быть большим.
  66-битная кодовая посылка делает сканирование кода невозможным.
  32-битная кодовая посылка дает результат в 4 миллиарда кодовых комбинаций. При этом на сканирование кода уйдет порядка 17 лет.
  Сканирование 34-битного кода займет 5600 миллиардов лет.
- Кодер не должен формировать один и тот же код дважды.

Всякий раз, когда нажимается кнопка на пульте дистанционного управления, кодер формирует не повторяющуюся комбинацию. Для посторонней системы, такая кодовая посылка будет казаться абсолютно случайной. Каждая кодовая комбинация будет уникальна, и между посылками не будет прослеживаться взаимосвязи.

В технологии KeeLoq, кодовая последовательность повториться более чем через 65 000 команд. Если пульт дистанционного управления использовать 8 раз в сутки, то пройдет 22 года, прежде чем та же самая кодовая комбинация повторится снова. При этом повторная передача кода (например при помощи устройства перехвата кода) не вызовет срабатывание системы.

Алгоритм KeeLoq использует особенную систему синхронизации. Принятая посылка декодируется и сохраняется в памяти. Последующие посылки считаются истинными, если они лежат в зоне 16 возможных следующих кодовых комбинаций. Это сделано для того, что бы не восстанавливать синхронизацию каждый раз после нажатия кнопки на пульте управления в не досягаемости для приемника. В случае выхода кодовой комбинации из зоны 16 вариантов, необходимо дважды нажать кнопку на пульте управления, и синхронизация будет восстановлена. Операция синхронизации полностью прозрачна – пользователь даже не будет знать о том, что синхронизация была потеряна и восстановлена.

Очевидны преимущества использования технологии KeeLoq, стоимость которой сопоставима с ценой систем на основе фиксированного кода. Применение заказных микросхем KeeLoq , с минимальным количеством внешних компонентов, позволяют строить конкурентно способные системы с высоким уровнем безопасности.

Описание алгоритма Keeloq

KeeLoq является блочным алгоритмом шифрования, использующий 32-битный блок и 64-битный ключ. При простой аппаратной реализации он имеет высокий уровень защиты сопоставимый с алгоритмом DES. Такой уровень защиты является подходящим для систем дистанционного управления с защитой от перехвата кода. Для кодирования и декодирования передаваемой информации используется 64-битный ключ. Подобрать ключ исходя из перехваченной информации невозможно. Существуют испытания систем, которые могут быть использованы для проверки характеристик безопасности алгоритма кодирования и также для предсказания следующего передаваемого кода. На данном алгоритме были проверены такие виды атаки как: “Эффект Лавины” (Avalanche Effect) и его подмножества. Результат проверки дал хороший показатель эффективности системы безопасности:

Эффект Лавины (**AE**). Блочный шифр удовлетворяет критериям AE, если при замене одного информационного бита, в среднем меняется половина передаваемых битов. Применительно к алгоритму *KeeLoq*, это подразумевает, что изменение одного бита в функции и/или информации синхронизации заставит в среднем измениться 16 из 32 битов в переданном коде.

Строгий Лавинный Критерий (**SAC**). Чтобы удовлетворять данному критерию необходимо, чтобы на один измененный бит зашифрованной информации изменялось половина выходных информационных битов. Следовательно, возможность угадывания любого бита информации равна 0.5, а вероятность правильного угадывания всей 32-разрядной информационной посылки равна одна к 4,300,000,000! На вход алгоритма, при проведении тестов, подавалось случайное значение 64-битного ключа, а также содержимое счетчика Грэя, который считал начиная с нуля. В каждом случае значение, появляющееся на выходе алгоритма сравнивалось с входной величиной (SAC тест) или с предыдущим кодом (AE тест). Оба случая дали следующие результаты: При AE тесте средняя величина изменяемых битов оказалась равной 16.0 (50%) со стандартным разбросом значений 2.83 (8.8%). При SAC тесте изменение одного входного бита дает изменение выходного значения в среднем на 50%, с средним разбросом значение в 8.8%.

Основные определения технологии KeeLoq

Серийный номер – в каждый передатчик, при изготовлении, программируется 28 или 32 битный уникальный серийный номер.

Секретный ключ – это 64-битный код формируемый функцией генератора ключей из 28/32-битного серийного номера или 32/48-битного «кодового зерна» и 64-битного заводского номера. Секретный ключ не может быть считан, он никогда не передается.

«Кодовое зерно» - это 32/ 48-битное значение программируется в кодер передатчика. При этом половина кодового значения используется при генерации ключа. Значение “кодового зерна” передается передатчиком только после нажатия на нем определенной комбинации клавиш и может выключаться по окончании процесса обучения.

Генерация секретного ключа – используется для формирования уникального номера передатчика. При генерации используется серийный номер и «кодовое зерно». Генерация кода производиться по нелинейному закону производится программатором при программировании кодера.

Заводской ключ – программируется в декодер при изготовлении устройства, и используется для генерации секретного ключа.

Нормальный режим обучения - приемник использует информацию, полученную из обычной кодовой посылки для получения секретного ключа передатчика, определение величины различия и счетчика синхронизации. Вся информация, полученная от передатчика, сохраняется.

Безопасное обучение – передатчик активизируется через определенную комбинацию кнопок, после чего он передает 32- или 48-битную кодовую посылку (“кодовое зерно”), которая может использоваться при генерации ключа как его часть.

Величина дискриминации – величина дискриминации представляет собой 12-битную фиксированную часть зашифрованного слова. Данная величина используется приемником при расшифровке.

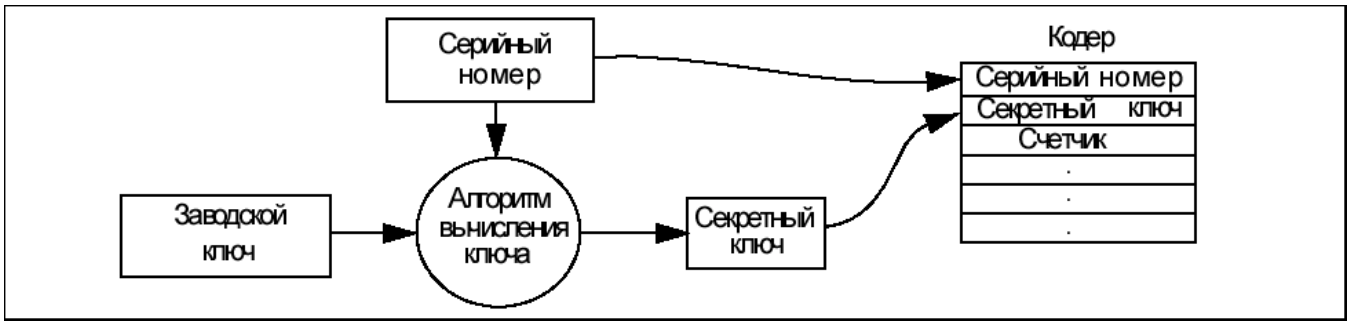
Счетчик синхронизации – 16-битный счетчик, который увеличивает свое значение на единицу всякий раз, когда происходит активизация передатчика. Приемник запоминает значение счетчика во внутренней памяти и сравнивает его со значением, полученным из предыдущей посылки. Если значение попадает в рабочее окно, то код принимается.

Основные технические характеристики и возможности элементов, для систем дистанционного управления, выполненных по технологии KeeLoq.

Кодеры

Формирователи «прыгающего» кода KeeLoq предназначены для однонаправленных систем дистанционного управления. В функции кодера входит только формирование кодовой посылки, разработчику системы дистанционного управления необходимо позаботиться об организации канала связи. Инициализация кодера, на передачу кода, происходит по нажатию на кнопку пульта дистанционного управления. Для радиомаяка, на основе технологии KeeLoq, инициализация передачи кода может происходить и под воздействием внешнего электромагнитного поля.

В технологии KeeLoq используется своеобразная система реверсивной идентификации по принципу «свой - чужой». На основе серийного номера передатчика и заводского ключа приемника формируется 64-битный секретный ключ, по специальному алгоритму, записываемый в кодер на этапе его программирования. Секретный ключ не может быть считан из кодера, и он никогда не передается по каналу связи.



При каждой инициализации кодера (нажатие на кнопку пульта дистанционного управления) формируется кодовая последовательность, в которую входит 32-битный «прыгающий код» полученный из 64-битного секретного ключа. «Прыгающий код» уникален для каждой новой кодовой последовательности. Счетчик

В KeeLoq кодерах используется 66/67 битный формат передачи данных.

66-разрядное кодовая последовательность состоит из:

- 32-битного «прыгающего кода»
- 28-битного серийного номера
- 4-битного функционального кода (нажатие кнопок)
- 1-битный флаг разряда батареи питания
- 1-битный флаг повторения

«Прыгающий код»	Серийный номер	Функцио н. код	Флаг разр. батареи	Флаг повтор.
32 бита	28 бит	4 бита	1 бит	1 бит

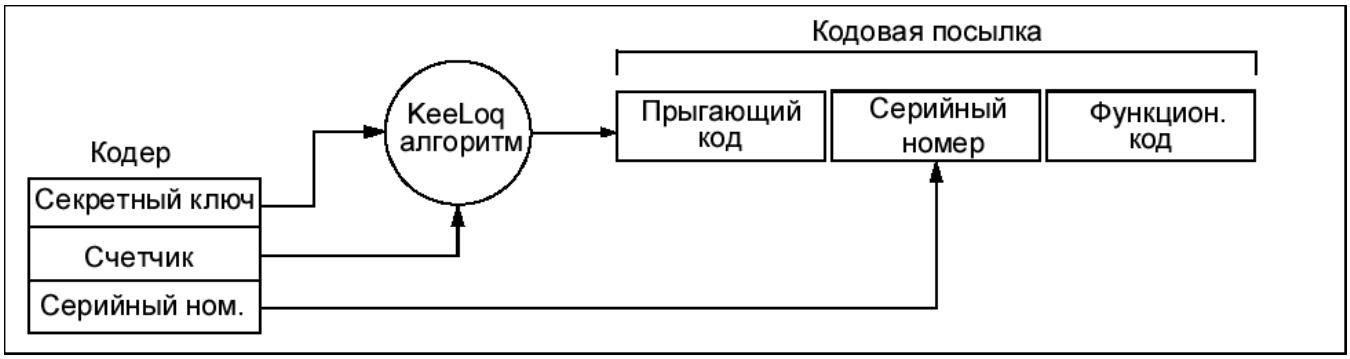
67-разрядное кодовая последовательность состоит из:

- 32-битного «прыгающего кода»
- 28/32-битного серийного номера
- 4/0-битного функционального кода (нажатие кнопок)
- 1-битный флаг разряда батареи питания
- 2-битный CRC

«Прыгающий код»	Серийный номер	Функцио н. код	Флаг разр. батареи	CRC
32 бита	28 бит	4 бита	1 бит	2 бит
32 бита	32 бита	0 бит	1 бит	2 бит

67-битная кодовая последовательность применяется в системах дистанционного управления с повышенными требованиями к помехозащищенности.

Алгоритм формирования кодовой посылки



В целях энергосбережения, в схему кодера включен коммутатор питания формирователя кодовой последовательности. Если ни одна из кнопок не нажата формирователь обесточен. В случае длительного удержания клавиши в нажатом состоянии произойдет автоматическое отключение формирователя кодовой последовательности. Для повторной инициализации передачи кода необходимо отпустить и вновь нажать кнопку на пульте.

Кодер поддерживает три скорости передачи кодовой последовательности:
- 833 бит/с (100мс)
- 1667 бит/с (50 мс)
- 3333 бит/с (25 мс)

Все кодеры KeeLoq повторяют передачу кодовой последовательности до тех пор, пока остается нажатой кнопка или не сработала защита разряда батареи.

Кодовая последовательность всегда передается полностью, даже если кнопка будет отпущена, а передача еще не закончена. Кодер автоматически передаст всю сформированную кодовую последовательность и перейдет в режим ожидания. Также в кодере предусмотрена функция защиты от дребезга контактов кнопок или кратковременных, ошибочных нажатий на клавишу. Защиту от дребезга контактов можно включить/выключить на этапе программирования кодера.

Государственным Комитетом по Распределению Частот РФ определена максимальная средняя мощность радиоизлучения в 10мВт, для устройств не подлежащих регистрации в органах ГСН РФ (Правила по ввозу и эксплуатации на территории РФ радиоэлектронных средств и устройств). Для повышения надежности работы системы может быть выгодно увеличить скорость передачи кодовой посылки, увеличив при этом мощность передатчика. Другой способ снижения средней мощности передачи – это запрещение непрерывных повторов кодовой последовательности при удержании клавиши на пульте дистанционного управления. Например повторять передачу кодовой последовательности раз в секунду или каждое четвертое кодовое слово.

Параметры кодеров KeeLoq:

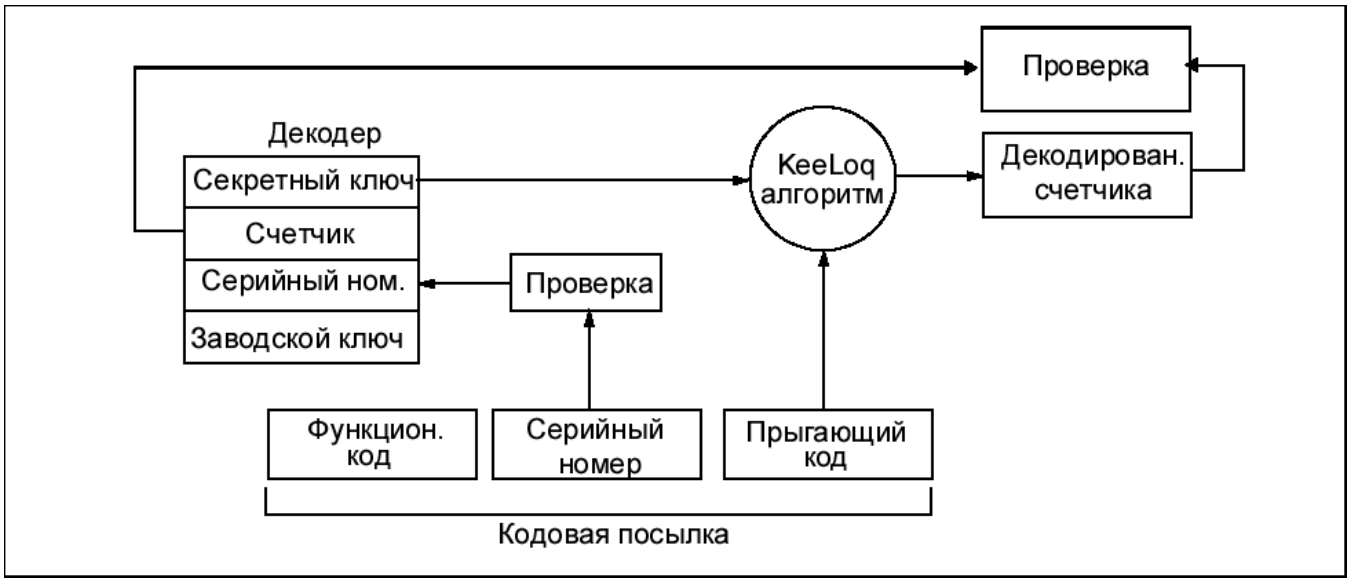
Секретность
- 28/32-битный серийный номер
- Программируемый 64-битный секретный ключ
- Длина кодовой последовательности 66/67 бит
- 32-битный «прыгающий код»
- 34/35-битный фиксированный код
- Защита от чтения секретного ключа

Параметры
- Питание от 3.0В до 12.0В
- Низкое энергопотребление
- 3/4 кнопки, 7/15 функций
- Выбор скорости передачи
- Автоматическое завершение передачи кодовой посылки
- Сигнал о разряде батарей
- Энергонезависимая синхронизация
- Поддержка модуляция для ИК систем

Состав
- Внутренняя память EEPROM
- Интегрированный тактовый генератор и таймеры
- Схема сброса
- Подтягивающие резисторы на входах кнопок
- Токовый выход для светодиода

Декодеры

Декодеры KeeLoq предназначены для дешифрации команд поступающие от кодера по каналу связи. После проверки принятого в кодовой последовательности серийного номера и «прыгающего кода», декодер на основании функционального кода активизирует выходы, соответствующие входам кнопок в кодере. Выходы будут удерживаться в активном состоянии до тех пор, пока нажата кнопка на кодере. Время удерживания выходов в активном состоянии после последней принятой кодовой последовательности 500 мс.



Для исполнения команд декодером, ему необходимо указать 28/32-битный серийный номер и 64-битный секретный ключ кодера. Также одним из условий выполнения команд декодером, является его синхронизация с кодером.

Технология KeeLoq позволяет использовать один секретный ключ для нескольких кодеров, работающих с данным декодером. Одно-ключевая система менее безопасна, но уменьшается сложность программы и объем необходимой памяти. В одно-ключевой системе поддерживается синхронизация с каждым из кодеров, вне зависимости от частоты использования.

В декодерах KeeLoq используется независимая ключевая система. Для каждого из передатчиков хранится свой серийный номер, секретный ключ и текущая синхронизация.

В технологии KeeLoq существуют два режима обучения декодера.

Нормальный режим.

В этом режиме, при нажатии на кнопку пульта дистанционного управления кодер формирует стандартную кодовую последовательность.

«Прыгающий код»	Серийный номер	Функцион. код	Статус/ CRC
32 бита	28 бит	4 бита	2/3 бит

«Прыгающий код»	Серийный номер	Статус/ CRC
32 бита	32 бита	2/3 бит

Декодер, получив первую кодовую последовательность, вычисляет на основании серийного номера 64-битный секретный ключ, который был запрограммирован в кодер. Декодер ожидает второй кодовой последовательности, для проверки результата вычислений. Перед записью данных декодер проверяет в полученных кодовых последовательностях – серийные номера, последовательность кода, правильность вычисления «прыгающего кода». После этого кодер считается зарегистрированным в декодере.

Безопасный режим.

После перевода кодера в режим безопасного обучения, на кодере нажимается комбинация кнопок для передачи 32/48-битного кодового зерна.

Кодовое зерно	Серийный номер	Функцио н. код	Статус/ CRC
32/48 бит	28/12 бит	4 бита	2/3 бит

Кодовое зерно	Серийный номер	Статус/ CRC
32/48 бит	32/24 бит	2/3 бит

В кодовой последовательности «прыгающий код» будет заменен 32/48-битным кодовым зерном. На основе кодового зерна декодер вычислит 64-битный секретный ключ. После нажатия на любую клавишу пульта дистанционного управления, кодер сформирует нормальную кодовую последовательность. Декодер проверит правильность вычисления «прыгающего кода», установит синхронизацию с кодером и сохранит результат в энергонезависимой памяти.

Кодовое зерно формируется передатчиком только в процессе обучения. Как мера защиты, от вскрытия секретного ключа, на этапе обучения декодера, предусматривается запрещение передачи кодового зерна в период от 1 до 128 инициализаций кодера.

Для хранения регистрационной информации о передатчиках, в декодерах KeeLoq. предусмотрена внутренняя энергонезависимая память. Для каждого зарегистрированного передатчика используется 16 байт памяти.

Все декодеры KeeLoq позволяют менять регистрационную информацию о передатчиках. Для удаления информации о всех передатчиках, необходимо удерживать активный уровень сигнала на обучающем входе декодера в течении 10 сек. Допускается циклическая запись данных о новом передатчике. При этом передатчик, который был зарегистрирован раньше всех, будет удален.

Параметры декодеров KeeLoq.

Секретность
- Защищенное хранение заводского ключа
- Защищенное хранение секретного ключа
- Нормальный и безопасный режим обучения
- Поддержка 4 и более передатчиков

Параметры
- Напряжение питания от 2.0В до 6.0В
- Внутренний 4МГц RC генератор
- Автоматическое определение скорости передачи
- Внутренняя энергонезависимая память
- До 15 функций
- Одно или двух проводной интерфейс
- Индикатор разряда батареи

Типовые применения технологии KeeLoq
- Автомобильные охранные системы
- Автомобильные иммобилайзеры
- Системы ограничения доступа
- Электронные замки
- Идентификационные системы
- Устройства дистанционного управления

Кодеры Microchip выполненные по технологии KeeLoq

Устройство	Кодовая посылка бит	«Прыгающий код» бит	Кодовое зерно бит	Функций	Напряжение питания В	Примечание
HCS101	66	-	-	7	3,5 – 13,3	Фиксированный код
HCS200	66	32	32	7	3,5 – 13,0	Поддержка фиксированного кода
HCS201	66	32	32	7	3,5 – 13,0	Шаговый регулятор
HCS300	66	32	32	15	2,0 – 6,3	Драйвер светодиода
HCS301	66	32	32	15	3,5 – 13,0	Драйвер светодиода
HCS320	66	32	32	16	3,5 – 13,0	Кнопка Shift
HCS360	67	32	48	15	2,0 – 6,6	Манчестерская, ШИМ, ИК модуляция; 2-бит CRC
HCS361	67	32	48	15	2,0 – 6,6	ШИМ, ИК модуляция; 2-бит CRC
HCS362	69	32	48	15	2,0 – 6,3	Манчестерская, ШИМ модуляция; 2-бит CRC; Shift
HCS365	67/69	32	60	15	2,0 – 5,5	Манчестерская, ШИМ модуляция; 2-бит CRC; Shift
HCS370	67/69	32	60	15	2,0 – 5,5	6 кнопок + Shift
HCS410	69	32	60/64	7	2,0 – 6,6	Режим радиомаяка
HCS412	69	32	60	7	2,0 – 6,3	Режим радиомаяка
HCS473	69	32	60	15	2,0 – 5,5	Режим радиомаяка, 3 колебательных контура

Декодеры Microchip выполненные по технологии KeeLoq

Устройство	Кодовая посылка бит	Кол-во поддержив. передатчиков	Интерфейс связи	Функций	Напряжение питания В	Типы поддерживаемых кодеров HCSXXX
HCS500	67	7	SPI	15	4,5 – 5,5	200, 300, 301, 360, 410
HCS512	67	4	-	15	3,0 – 6,0	200, 300, 301, 360, 361
HCS515	67	7	SPI	15	4,5 – 5,5	200, 201, 300, 301, 320, 360, 361, 362, 365, 370, 410, 412, 473

Статья основывается на технической документации TB003
компании Microchip Technology Incorporated, USA.