



KeeLoq



— КЛЮЧИ И ЗАМКИ ОТ Microchip

История KeeLoq

KeeLoq изначально — это система алгоритмов, разработанная и запатентованная Южно-Африканской компанией Nanotek в середине 80-х. Nanotek была основана экспертами по кодированию и электронике из университета Претории и занималась вопросами информационной безопасности. Название KeeLoq созвучно английским словам «key» (ключ) и «lock» (замок).

В 1995 году фирма Microchip приобрела отделение KeeLoq у Nanotek вместе с лицензионными правами. Теоретические разработки Nanotek в сочетании с производственными мощностями и техническими возможностями Microchip (работа изделий при низких напряжениях и высокая надежность EEPROM) позволили реализовать великолепный новый ряд компактных микросхем контроля доступа серии HCSXXX, простых для пользователя, но изощренных для взломщика. Разработанные для систем контроля доступа, эти микросхемы завоевали признание исключительно высокой защищенностью и функциональной законченностью у таких серьезных производителей, как Chrysler, Daewoo, Fiat, GM, Honda, Toyota, Volvo, Clifford, Shurlok и многих других.

В настоящее время алгоритм KeeLoq принят во всем мире и положен в основу тестовых критериев для систем безопасности в Великобритании, адаптирован рядом европейских производителей и использован в собственных системах, разработанных «Форд» (для Escort) и «Ягуар» (для XJS).

Сканеры и грабберы

Необходимость разработки алгоритма KeeLoq была вызвана растущими возможностями техники сканеров и грабберов при вскрытии объектов типа автомобилей и гаражей, охраняемых системами с фиксированным кодом.

Грабберы способны перехватывать фиксированное сообщение, передаваемое брелоком по радио, записывать и воспроизводить на той же частоте. В отличие от них, сканеры передают последовательные или случайные коды со скоростью порядка десяти посылок в секунду. Один вариант защиты от сканера — отключение приемника на несколько минут после ряда попыток передачи ложных кодов, что значительно увеличивает время взлома. Другая мера — очень большое количество

кодовых комбинаций, требующая большого времени для перебора. Этот путь и использует KeeLoq, имеющий 4,6 миллиарда кодовых комбинаций и требующий для перебора около 15 лет.

Алгоритм KeeLoq

В основу алгоритма положен псевдослучайный «прыгающий» код, так что никто, кроме «своего» приемника, не может предсказать, какой код должен быть передан в следующий раз. «Прыгающий» код генерируется кодером по лицензированному алгоритму на основе 64-битного кода «ключа», 28-битного серийного номера и 16-битного счетчика синхронизации. Код «ключа» программируется пользователем в EEPROM кодера. Серийный номер уникален и задается в процессе производства. Приемники и передатчики KeeLoq работают в последовательном коде с посылкой длиной 66 или 69 бит, состоящей из кодированной «прыгающей» части в 32 бита, 28 бит серийного номера, 4 бит пользователя (состояние кнопок), 1 бита индикации разряда батареи и для ряда устройств — контрольной суммы CRC.

Рассинхронизация ключа и замка

Все системы дистанционного доступа, требующие синхронизации кодов приемника (декодера) и передатчика (кодера), имеют одно узкое место — часто возможна активация передатчика вне радиуса действия приемника. В этом случае синхронизация нарушается, так как все последующие принятые коды будут отличаться от ожидаемых декодером, и устройство не сработает. Большинство подобных систем требуют специальной процедуры синхронизации, часто неудобной для пользователя.

У KeeLoq эта проблема решена — процесс восстановления синхронизации автоматический и незаметен пользователю. Во-первых, декодер реагирует не только на первый ожидаемый код, но и на некоторое количество кодов, например 14, которые должны следовать далее. Таким образом, если передатчик 14 раз сработал вне зоны действия приемника, то на 15-й раз, оказавшись уже в зоне приема, он вызовет правильное срабатывание устройства. Действующие коды называются «окном валидности». При ширине окна 15 кодов и общем количестве возможных комбинаций более 4,5 миллиарда риск случайного несанкционированного доступа возрастает очень незначительно. Ширина «окна

валидности» — величина, программируемая пользователем выбирается оптимальной для конкретного канала связи и требований к безопасности.

Во-вторых, восстановление синхронизации в большом диапазоне кодов, достаточном для любых применений и без потери секретности, достигнуто следующим образом: декодер сравнивает два последовательно полученных кода, находящихся вне «окна валидности», с ожидаемыми, но в пределах большего окна — «окна рассинхронизации», и только если оба совпадут, устройство работает. На практике это может выглядеть так: владелец машины с помощью радиобрелока безуспешно пытается снять ее с сигнализации на большом расстоянии или из-за преграды, пока чувствительности приемника еще не хватает; когда же очередная посылка оказывается принятой декодером, то не вызывает его срабатывания из-за рассинхронизации, но уже следующая попытка владельца приводит к успеху, так как два последовательных кода оказались правильными. Восстановление синхронизации KeeLoq требует только одной дополнительной попытки. Ширина «окна рассинхронизации» — 32K кодов при 16-разрядном встроенном счетчике синхронизации. Все оставшиеся и уже «отработанные» коды автоматически относятся к третьему окну — «окну блокировки» и становятся запрещенными. Такие меры способны эффективно защитить систему от простых грабберов.

Защита от «умных» грабберов

«Умные» грабберы способны вынуждать пользователя охранной системы, работающей по радиоканалу, передавать несколько кодов подряд, записывать их, одновременно передавая предыдущий. Это «подвешивает» систему и оставляет «грабберу» последний валидный код доступа. KeeLoq защищен от такого воздействия с помощью механизма «отложенного инкремента». Декодер автоматически увеличивает счетчик синхронизации на 12 через 20 секунд после последней операции, что переводит все предыдущие коды в «окно блокировки», но следующие еще остаются в «окне валидности».

Обучение декодера

При утере ключа (кодера) возникает необходимость запрета старого кода ключа и введение нового. В семействе KeeLoq этот процесс, называемый обучением,

так же прост и надежен. Замыкание переключки на плате декодера активизирует встроенную программу обучения, которая обрабатывает специальную посылку от кодера, выделяя из нее серийный номер кодера и 64 бита кода ключа, и записывает их во встроенную энергонезависимую память декодера. Для повышения безопасности специальная посылка кодера, содержащая «обучающее зерно», генерируется при нажатии комбинации кнопок и может быть послана лишь однажды, после чего кодер может работать только в обычном режиме.

Технические особенности

Семейство KeeLoq выполнено по современной технологии, совмещающей аналоговые и цифровые компоненты с напряжением питания от 2 до 13 В. Большинство в 8-выводных корпусах. Все необходимые компоненты находятся на кристалле: это EEPROM повышенной надежности (более 200 К циклов записи), тактовый генератор, супервизор и стабилизатор питания, цепи защиты от дребезга контактов клавиатуры, токоограничивающие резисторы светодиодов. Надежность этих устройств подтверждена ежемесячными миллионными тиражами. Простота освоения заложена в полной функциональной законченности микросхем, совместимости и преемственности со всеми членами семейства. Также Microchip предлагает разработчикам ряд практических наборов для начала работы с KeeLoq, включающих литературу, программные средства, программатор KeeLoq, платы передатчика и приемника с интерфейсом RS232.

Состав семейства KeeLoq

Семейство KeeLoq состоит из ряда микросхем взаимно-совместимых кодеров (табл. 1) и декодеров (табл. 2), различающихся функциональными возможностями. Они разработаны для передачи защищенной информации по любому каналу связи: проводному, радиоканалу, ИК; с ШИМ или Манчестерской модуляцией.

Кроме однонаправленной передачи пароля кодером декодеру возможен и двусторонний обмен типа запрос—ответ IFF (Identification Friend or Foe). При таком типе обмена на каждый из нескольких последовательных запросов декодер должен получить отличные друг от друга, но правильные ответы кодера, что значительно повышает общую надежность системы безопасности. Двусторонний обмен реализован в микросхемах кодеров HCS410 и HCS412. Эти микросхемы также могут работать в режиме транспондера, то есть с питанием от энергии электромагнитного поля, наведенного генератором декодера (по принципу Proximity Card). Модуль HCS410-WM выпускается в безвыводном корпусе SOT385 и представляет собой упакованные в один корпус чип HCS410, конденсатор и катушку, являясь, таким образом, законченным транспондером. Этот модуль удобно использовать для создания бесконтактных систем доступа, иммобилайзеров и так далее.

Алгоритм декодирования можно реализовать не только с помощью специализированной микросхемы серии HCS5XX, но и программно на базе любого микроконтроллера PICmicro. Таким образом, задачу декодирования можно переложить на



основной управляющий микроконтроллер. Этот вариант удобно применять при проектировании миниатюрных систем, а также когда нужно до предела снизить себестоимость изделия.

Описание примеров построения программных декодеров, автомобильных систем сигнализации и многое другое вы можете найти на сайте www.microchip.com или компакт-диске в разделе Application Notes>KEELOQ® security.

Возможные применения

В первую очередь, это автосигнализации, системы контроля доступа в помещении и доступа к компьютерной информации. Но благодаря своей функциональной законченности и низкой цене микросхемы KeeLoq могут найти применение везде, где требуются малые габариты и низкое энергопотребление, при передаче небольшого количества информации, в одном направлении, по одному проводу от большого количества распределенных источников (или одного). Например: радиоуправляемые игрушки, любые виды пультов и приемников дистанционного управления, беспроводные датчики, датчики охранно-пожарной сигнализации или сети сбора данных. Впрочем, каждый может сам без труда найти вокруг себя ряд применений этим простым и надежным устройствам.

Таблица 1. Микросхемы кодеров семейства KeeLoq

Чип	Длина обучающей посылки, бит	Напряжение питания, В	Количество функций пользователя	Особенности	Тип корпуса
HCS101	-	3,5...13	7	Передатчик фиксированной кодовой последовательности, без кодирования	DIP8, SOIC8
HCS200	32	3,5...13	7	Базовая модель, поддержка фиксированного кода, индикатор разрядки батареи	DIP8, SOIC8
HCS201	32	3,5...13	7	Базовая модель, поддержка фиксированного кода, индикатор разрядки батареи, преобразователь питания	DIP8, SOIC8
HCS300	32	2,0...6,3	15	Управление светодиодом, биты переполнения, тайм-аут, индикатор разрядки батареи	DIP8, SOIC8
HCS301	32	3,5...13	15	Как у HCS300	DIP8, SOIC8
HCS320	32	3,5...13	16	Функция сдвига, управление светодиодом, биты переполнения, индикатор разрядки батареи	DIP8, SOIC8
HCS360	48	2,0...6,6	15	ИК-режим, ШИМ и Манчестерская модуляция, 2-бит CRC	DIP8, SOIC8
HCS361	48	2,0...6,6	15	ИК-режим, ШИМ и изменяемая ШИМ-модуляция, 2-бит CRC	DIP8, SOIC8
HCS365	60	2,0...5,5	4×15	2 независимых кодера, ШИМ и Манчестерская модуляция, 4 входа	DIP8, SOIC8
HCS370	60	2,0...5,5	4×15	2 независимых кодера, ШИМ и Манчестерская модуляция, 6 входов, преобразователь питания	DIP14, SOIC14
HCS410	60	2,0...6,6	7	2 режима работы: как кодер и как транспондер, также выпускается в специальном безвыводном корпусе	DIP8, SOIC8
HCS412	60	2,0...6,6	4×7	2 режима работы: как кодер и как транспондер	DIP8, SOIC8

Таблица 2. Микросхемы декодеров семейства KeeLoq

Чип	Напряжение питания, В	Функциональные выходы	Дополнительные особенности	Тип корпуса
HCS500	4,5...5,5	15 (последовательный канал)	Декодер с последовательным выходом	DIP8, SOIC8
HCS512	3,0...6,0	15 (последовательный + параллельный каналы)	Декодер с последовательным и параллельным выходом	DIP18, SOIC18
HCS515	4,5...5,5	15 по последовательному каналу, 3 — по параллельному	1К EEPROM пользователя	DIP14, SOIC14