TB001

Technical Brief
Secure Learning RKE Systems Using KEELOQ® Encoders

Author: Chris R. Burger
Secure Data Products

INTRODUCTION

Learning capability in remote keyless entry (RKE) and remote-controlled security systems is regarded as essential by most manufacturers. The logistical problems associated with the supply of replacement and additional transmitters for personalized decoders quickly become overwhelming if any dealer intervention is required.

In the case of a learning system, the user can purchase a pre-programmed transmitter off the shelf and then add that transmitter to the decoder system without assistance. Dealer intervention is completely unnecessary, and only one type of transmitter needs to be stocked for a particular product line. Each transmitter is pre-programmed with a unique serial number and key.

However, learning systems need to be properly managed to ensure that they maintain an adequate level of security. A badly implemented learning system could provide an outsider with access to the system. On the other hand, a well-designed learning system should not reduce the security level of the basic code-hopping system at all.

SINGLE-ALGORITHM SYSTEMS

Code hopping systems often use a single encoding and decoding algorithm for all transmitters in a particular product line. Most of the systems on the market fall into this category.

Learning is really simple—the decoder simply decodes the incoming transmission during learning and stores the resultant parameters for later use. For their security, these systems rely on the assumption that the algorithm will remain secret. In this era of Internet and instant worldwide communications, the probability that a widely-used algorithm will permanently remain secret is low and the assumption naive.

THE KEELOQ KEY-BASED SYSTEM

The KEELOQ system uses a separate 64-bit key for each transmitter. Such a key is simply a very large random number, unique to that transmitter. Effectively, this arrangement provides a unique encoding and decoding algorithm for each transmitter. An outsider that does not know the key, cannot decode the variable code portion of a transmission and consequently cannot determine the identity parameters of the originating transmitter.

This uniqueness of each transmitter's encoding algorithm complicates learning. The key cannot be determined from the variable code transmission, and no information can be derived from the transmission without the key.

Obviously, some other piece of information must be transmitted during learning to enable the decoder to calculate the correct key. Two approaches are suggested. Each approach has pros and cons, which will be the subject of a comparative discussion in a later section.

KEELOQ Normal (Serial Number-derived) System

Each KEELOQ transmitter contains a unique serial number, programmed into the transmitter on the production line. This serial number is transmitted as part of the fixed code portion of every transmission.

When a transmission has been received, decoders typically use this serial number to determine the identity of the originating transmitter. The serial number is compared with those stored in memory. If a match is found, the decoder knows the identity of the transmitter, and therefore also knows which key and counter to use to process that transmission.

Each transmitter is also programmed with a key, calculated from the serial number using a secret learning algorithm. The relationship between the serial number and the key is very complex. This ensures that the relationship is not evident to outsiders.

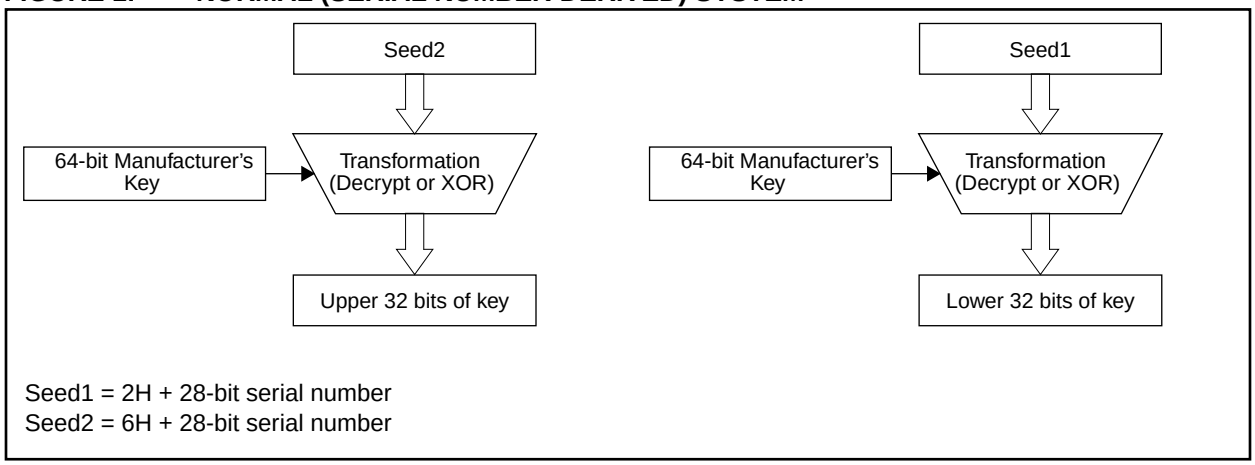
During learning, the decoder calculates the key for that transmitter, using the same secret learning algorithm used for programming the transmitter. Once the key has been determined, the decoder can decode the transmission and store the parameters associated with that transmitter, including the key.

This learning procedure offers simplicity and high security—provided that the learning algorithm remains secret. To reduce the possibility of the learning algorithm being jeopardized, the KEELOQ system uses a learning algorithm that is only implemented in custom ICs. The first decoder to use this algorithm is slated to become available during 1996. As an interim solution, customers with a requirement for unusually robust learning security can enquire about coprocessor-based solutions.

In addition, the system relies on a manufacturer's key to determine the learning relationship. The manufacturer's key is protected by a smart card-based system and is stored in EEPROM inside the custom IC. Even if the learning algorithm itself becomes known, each manufacturer has a second line of defence in the manufacturer's key. Should a single manufacturer allow their key to become public knowledge, other manufacturers are not endangered.

One final comment—the envelope encryption capability on some of the KEELOQ encoders does not materially alter the nature of the learning algorithm. All devices in a particular product line share a single envelope encryption key, and any decoder in that product line can readily decode an incoming serial number. Once the serial number has been determined, the learning algorithm proceeds exactly as detailed.

FIGURE 1: NORMAL (SERIAL NUMBER-DERIVED) SYSTEM



KEELOQ Secure (Seed-derived) System

The ultimate in secure learning is a system where no reliance is placed on the secrecy of any of the algorithms, or a single manufacturer's key.

The KEELOQ code hopping system was designed under this assumption. Even if an outsider has the code hopping algorithm, a particular transmitter's transmissions are still incomprehensible if that transmitter's secret key is not known.

Determining the key by analyzing a number of transmissions is also not feasible. In 1995, it was estimated that an attacker with access to the algorithm requires a custom-designed $1,000,000 computer (designed exclusively to analyze KEELOQ transmitters) and 37 days of computer time per transmitter to find the secret key. Also, if a particular transmitter is jeopardized, no harm has been done to the security of other transmitters, even from the same product line.

To extend the security advantages of open algorithms to learning systems, the KEELOQ developers have applied for patents covering a novel learning technique. The learning technique does not rely on the secrecy of the learning algorithm at all.

On the production line, each transmitter is programmed with a serial number, a learning seed, and a key. There should not be any deterministic or mathematical relationship between the serial number and the key. Instead, a fixed (but complex) relationship exists between the learning seed and the key. The learning seed is only transmitted during learning. A special action is required from the user to activate transmission of the learning seed.

The learning seed is never transmitted during normal operation.

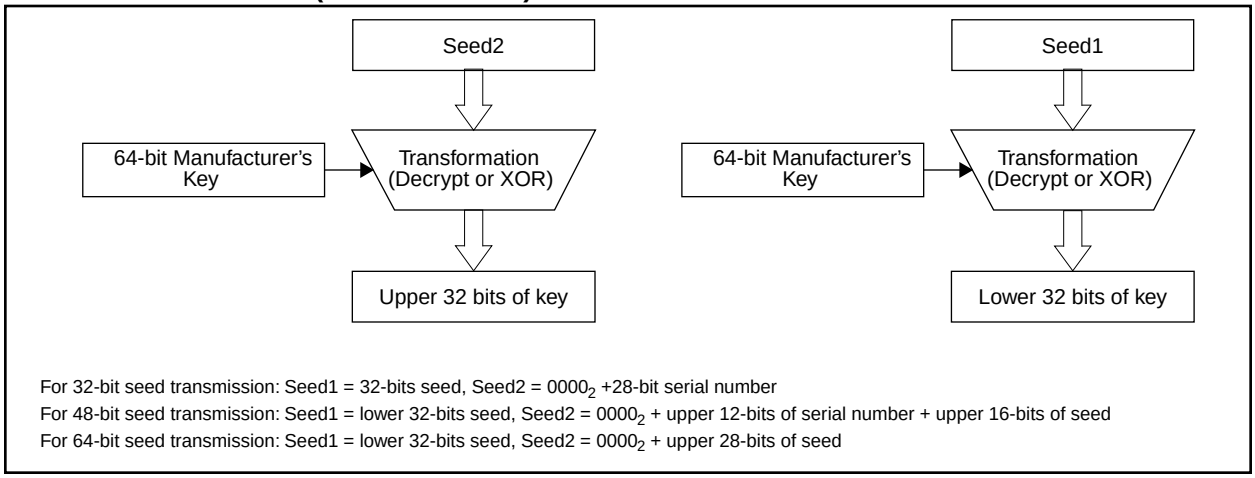
The HCS300 encoder can transmit a learning seed when all the function inputs are activated simultaneously. The 32-bit variable code is then replaced by a 32-bit learning seed, retrieved from the encoder's EEPROM memory. The decoder can derive the key from the learning seed alone, or from both the learning seed and the serial number.

Seed transmission in the HCS360 can be activated in two ways, details of which can be found in the following section and in the device specifications. During seed transmission, the HCS360 replaces both the 32-bit variable code and 16 bits of the serial number with fixed information retrieved from EEPROM, in essence transmitting a 48-bit seed. Also, additional protection against attack is provided. If desired, the transmitter can be configured to completely lose its ability to transmit the learning seed once the learning process has been completed. The mechanism works by permanently disabling seed transmission capability when the synchronization counter reaches 128. The user does not need to take any conscious action, as seed transmission is automatically inhibited after a few normal code hopping transmissions and cannot be activated again unless the encoder is reconfigured in total.

Because the learning seed and the key are both stored in read-protected EEPROM, there is no way to obtain the learning seed or the key from the transmitter, once the seed transmission capability has been inhibited.

A major advantage of seed based learning systems is that the security is not reliant upon a single key (or algorithm) that must be present in every decoder. However, a secret manufacturer's key that determines the relationship between the seed and the key still ensures protection against situations where access to the transmitter is possible (i.e. servicing, valet, etc.) and against the manufacturing of pirate transmitters.

FIGURE 2: SECURE (SEED-DERIVED) SYSTEM



For 32-bit seed transmission: Seed1 = 32-bits seed, Seed2 = 0000_2 +28-bit serial number
For 48-bit seed transmission: Seed1 = lower 32-bits seed, Seed2 = 0000_2 + upper 12-bits of serial number + upper 16-bits of seed
For 64-bit seed transmission: Seed1 = lower 32-bits seed, Seed2 = 0000_2 + upper 28-bits of seed

USING LEARNING SEED TRANSMISSION (HCS300, HCS301, HCS200, HCS360, AND HCS361)

HCS300/301

The HCS300 transmits a fixed code (stored in EEPROM) when all four control inputs are activated (i.e. $S_3S_2S_1S_0$ = 1111).

HCS200

The HCS200 transmits a fixed code (stored in EEPROM) when all three control inputs are activated (i.e. $S_2S_1S_0$ = 1).

HCS360/361

In the HCS360, the seed transmission capability is optional. If this option is selected during programming, transmission can be initiated in two ways: either $S_3S_2S_1S_0$ = 0011 and delayed mode is active (i.e. after about 3 seconds of variable code transmission), or $S_3S_2S_1S_0$ = 1000.

The fixed code capability can be permanent or temporary, depending on the setting of another EEPROM configuration bit. If the temporary mode has been selected, fixed code capability is disabled when either of the hopping code counters reaches a value of 128. The user can transmit the learning seed as many times as required to complete learning, and then originate up to 128 code hopping transmissions. The HCS360 will then protect the learning seed against readback and transmission for the remainder of its lifetime. If a number of transmissions less than 128 is required, the initial counter value can be increased accordingly.

Transmission Format

Normal HCSxxx encoder transmissions consist of a 32-bit hopping code, a 28-bit serial number, a 4-bit function code, and a flag field. These bits include a low voltage warning flag, a transmission repetition flag, and CRC bits for error checking. The flag field differs for the two encoders, and is not germane to this discussion. More information appears in the specification documents for each of the encoders.

H_0	Hopping	H_{31}	N_0	Serial	N_{27}	$S_2S_1S_0S_3$	Flags

The HCS200's and HCS300's seed transmission mode is identical, except that the 32 bit variable code is replaced by a 32-bit seed value, retrieved from EEPROM.

K_0	Seed	K_{31}	N_0	Serial	N_{27}	$S_2S_1S_0S_3$	Flags

In the HCS360's seed transmission mode, the fixed code is composed of a 48-bit learning seed, bits 16 to 27 of the serial number (the first 16 bits are replaced by seed bits), the 4 function bits, and the flag field.

K_0	Learning seed	K_{47}	N_{16}	Serial	N_{27}	$S_2S_1S_0S_3$	Flags

If compatibility between HCS300/301 and HCS360/361 transmitters is required, the HCS360 can simply be programmed so that the upper portion of the seed (bits K_{32} to K_{47}) corresponds to the lower portion of the serial number (bits N_0 to N_{15}). The resulting transmissions are then identical, except for possible differences in the flag field.

DECIDING ON A LEARNING SOLUTION

Factors to be Considered

Any security system is a compromise between convenience to the user, cost and security. The KEELOQ system has made very high security available at low prices, all but eliminating cost as a consideration. The designer must therefore decide on the relative importance of security and user-friendliness in the system.

If security is of paramount importance, a seed-based system with automatic seed inhibition is preferred. However, this system has the disadvantage that the user must place both the transmitter and the receiver in learning mode, and that the transmitter can only be learned by a decoder once during its lifetime.

If user-friendliness is more important, a seed-based system without seed inhibition or a serial number-based system can be used. In the case of a serial number-based system, the user does not have to memories any special button combinations for use exclusively during learning. In the case of a seed-based system, the user needs to know the special button combination, but the transmitter retains its learning capability indefinitely.

TABLE 1: PROS AND CONS OF THE DIFFERENT LEARNING SYSTEMS

Learning Mode	How Used	Advantages	Disadvantages
Serial Number-based Learning	During learning, the key is derived from a serial number, included as part of every transmission from the transmitter.	The user does not need to activate a special encoder mode to conduct learning. Normal transmissions are used during learning, and the key is derived from the included serial number information. Also, a transmitter can be re-learned at any time if required.	The security of the system is dependent on the secrecy of the learning algorithm and/or manufacturer's key. This disadvantage can be overcome by using a learning algorithm implemented in a custom IC. However, for the largest OEM product lines, syndicates may still find it worth their while to reverse-engineer the custom IC.
Seed-based Learning With Seed Inhibition	During learning, a special learning seed is transmitted. The decoder derives the key from this learning seed. During normal operation, the transmitter loses its ability to transmit the learning seed. The seed is also stored in read-protected EEPROM, fully protected against outside access.	The security of the system is independent of the secrecy of the learning algorithm. The learning algorithm can thus be implemented on any platform, including generic microprocessors, without fear of jeopardizing the security of the system.	The user must operate a special button or combination of buttons on the transmitter to transmit the learning seed. Also, the transmitter cannot be re-learned once seed transmission has been disabled.
Seed-based Learning Without Seed Inhibition	During learning, a special learning seed is transmitted. The decoder derives the key from this learning seed. During normal operation, the transmitter does not transmit the learning seed. The system is therefore not susceptible to outside attack, even from someone that knows the learning algorithm and manufacturer's key. However, the transmitter permanently retains its ability to transmit the learning seed, and can be re-learned at any time.	The security of the system is independent of the secrecy of the learning algorithm, as the learning seed is not transmitted during normal operation. The learning algorithm can be implemented on any platform, including generic microprocessors, without fear of jeopardizing the security of the system. The transmitter can be re-learned at any time, as required.	The user must operate a special button or combination of buttons on the transmitter to transmit the learning seed. Also, there is some risk of the learning seed being revealed, as an outsider with temporary access to the transmitter can cause the transmitter to transmit the learning seed.

IMPLEMENTATION ISSUES

This section presents hardware and software issues surrounding various implementations and should be read as a guide to implementation once a solution has been chosen.

Serial Number-based Systems

Proceed to implement a decoder as indicated in the relevant KEELOQ documents. Pay attention to the platform being used. ROM-based microprocessors should only be used as a last resort. If possible, use a KEELOQ decoder or coprocessor to ensure that the learning algorithm remains secret.

Three stages can be identified in the learning process. These three stages involve two different transmissions. The user presses the button, causing a normal code hopping transmission from the transmitter. During the first stage, the serial number is stored in EEPROM, and the corresponding key is calculated. During the second stage, the decoder decodes the incoming transmission using that key and stores the decoded parameters (function, integrity testing information and synchronization counter) in EEPROM. Some form of user feedback is then provided, prompting the user to press the transmitter button again. The third stage consists of decoding the resulting transmission, comparing the integrity testing information to the stored version, and ensuring that the two counter values are successive.

If code space is at a premium, or the simplicity of the user interface is paramount, the second transmission (and hence the third stage) can be omitted. Some integrity is sacrificed, as the second transmission is used to ensure that the transmitter's key has been correctly calculated and that the transmitter actually belongs to the same product line as the decoder. If the second transmission is forfeited, the system designer should ensure that the integrity testing information bits are subject to some convention, failing which any incoming transmission would be accepted as valid during learning. A possible programming convention is to use the lower 12 bits of the serial number as integrity testing information.

Learning Seed-based Systems

a) Decide on the user interface during learning. Would it make more sense to press a separate secret button, which normally requires disassembly of the transmitter, or to press a combination of two buttons?

   For two button transmitters based on the HCS360, no additional hardware is required to implement a secure learning system. If the two transmitter buttons are pressed together, the transmitter transmits a normal hopping code, and then reverts to fixed code mode after approximately 3 seconds. The decoder can determine the 28-bit serial number from the initial transmission and then calculate the key from the learning seed when the transmitter reverts to fixed code encoder mode.

   During a further transmission, the decoder can decode the incoming transmission to determine and store the counters and integrity testing information. The designer may elect to include a third transmission to verify the correctness of the decoding operation. Similar considerations to those mentioned in Section 6.1 apply.

   After the predetermined number (up to 128) of code hopping transmissions has been made, the transmitter loses the ability to transmit the learning seed. From this point, pressing the two buttons together for more than 3 seconds results in a delayed function transmission with a function code of 0011.

   For other HCS360-based transmitters, activation of S3 results in transmission of the learning seed. S3 may be activated by installing a temporary link on the board, or even by a separate push button.

   After the predetermined number (up to 128) of code hopping transmissions has been made, the transmitter loses the ability to transmit the learning seed. From this point, activating S3 results in a normal hopping code transmission with a function code of 1000. For multi-button transmitters, this option opens up the possibility of using a normal button (i.e. fully accessible from outside) for learning, as the button regains full functionality after the fixed code transmission mode is disabled.

   For HCS300/301-based systems, all control inputs (S_0 to S3) must be high to activate seed transmission. The designer should include special provisions for forcing all these inputs high, especially in the case of a transmitter with less than four buttons.

b) Modify the decoder algorithm to calculate the key from the learning seed rather than from the serial number.

c) Choose the number of hopping code transmissions allowed before the encoder loses the ability to transmit the learning seed.

   Remember that the transmitter cannot be re-learned once the fixed code transmission has been disabled. If permanent re-learning capability is required, fixed code transmission should be left active permanently, or a serial number-based learning technique should be implemented. In most consumer products, the security level offered by the normal learning technique is perfectly adequate and sacrificing the convenience of re-learning is not justified.

NOTES:

WORLDWIDE SALES & SERVICE

AMERICAS

Corporate Office
Microchip Technology Inc.
2355 West Chandler Blvd.
Chandler, AZ 85224-6199
Tel: 602 786-7200 Fax: 602 786-7277
Technical Support: 602 786-7627
Web: http://www.microchip.com/

Atlanta
Microchip Technology Inc.
500 Sugar Mill Road, Suite 200B
Atlanta, GA 30350
Tel: 770 640-0034 Fax: 770 640-0307

Boston
Microchip Technology Inc.
5 Mount Royal Avenue
Marlborough, MA 01752
Tel: 508 480-9990 Fax: 508 480-8575

Chicago
Microchip Technology Inc.
333 Pierce Road, Suite 180
Itasca, IL 60143
Tel: 708 285-0071 Fax: 708 285-0075

Dallas
Microchip Technology Inc.
14651 Dallas Parkway, Suite 816
Dallas, TX 75240-8809
Tel: 214 991-7177 Fax: 214 991-8588

Dayton
Microchip Technology Inc.
Suite 150
Two Prestige Place
Miamisburg, OH 45342
Tel: 513 291-1654 Fax: 513 291-9175

Los Angeles
Microchip Technology Inc.
18201 Von Karman, Suite 1090
Irvine, CA 92715
Tel: 714 263-1888 Fax: 714 263-1338

AMERICAS *(continued)*

New York
Microchip Technology Inc.
150 Motor Parkway, Suite 416
Hauppauge, NY 11788
Tel: 516 273-5305 Fax: 516 273-5335

San Jose
Microchip Technology Inc.
2107 North First Street, Suite 590
San Jose, CA 95131
Tel: 408 436-7950 Fax: 408 436-7955

Toronto
Microchip Technology Inc.
5925 Airport Road, Suite 200
Mississauga, Ontario L4V 1W1, Canada
Tel: 905 405-6279 Fax: 905 405-6253

ASIA/PACIFIC

Hong Kong
Microchip Technology
Rm 3801B, Tower Two
Metroplaza,
223 Hing Fong Road,
Kwai Fong, N.T., Hong Kong
Tel: 852 2 401 1200 Fax: 852 2 401 3431

Korea
Microchip Technology
168-1, Youngbo Bldg. 3 Floor
Samsung-Dong, Kangnam-Ku,
Seoul, Korea
Tel: 82 2 554 7200 Fax: 82 2 558 5934

Singapore
Microchip Technology
200 Middle Road
#10-03 Prime Centre
Singapore 188980
Tel: 65 334 8870 Fax: 65 334 8850

Taiwan
Microchip Technology
10F-1C 207
Tung Hua North Road
Taipei, Taiwan, ROC
Tel: 886 2 717 7175 Fax: 886 2 545 0139

EUROPE

United Kingdom
Arizona Microchip Technology Ltd.
Unit 6, The Courtyard
Meadow Bank, Furlong Road
Bourne End, Buckinghamshire SL8 5AJ
Tel: 44 1 628 850303 Fax: 44 1 628 850178

France
Arizona Microchip Technology SARL
Zone Industrielle de la Bonde
2 Rue du Buisson aux Fraises
91300 Massy - France
Tel: 33 1 69 53 63 20 Fax: 33 1 69 30 90 79

Germany
Arizona Microchip Technology GmbH
Gustav-Heinemann-Ring 125
D-81739 Muenchen, Germany
Tel: 49 89 627 144 0 Fax: 498962714444

Italy
Arizona Microchip Technology SRL
Centro Direzionale Colleoni
Palazzo Taurus 1 V. Le Colleoni 1
20041, Agrate Brianza, Milan Italy
Tel: 39 39 689 9939 Fax: 39396899883

JAPAN

Microchip Technology Intl. Inc.
Benex S-1 6F
3-18-20, Shin Yokohama
Kohoku-Ku, Yokohama
Kanagawa 222 Japan
Tel: 81 45 471 6166 Fax: 81454716122

5/10/96

MICROCHIP