Attacks on the KeeLoq Block Cipher and Authentication Systems

Andrey Bogdanov

Chair for Communication Security
Ruhr-University Bochum, Germany
abogdanov@crypto.rub.de

3rd Conference on RFID Security, Malaga, 2007
# Table of Contents

1. **KeeLoq Access Control System**
   - Suppliers
   - Use Cases

2. **KeeLoq Algorithm**
   - Specification
   - Analysis

3. **KeeLoq Protocols**
   - Rolling Codes
   - IFF

4. **KeeLoq Key Generation**
   - Specification
   - Analysis
<table>
<thead>
<tr>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>- KeeLoq was developed by Nanoteq in mid 80s</td>
</tr>
<tr>
<td>- KeeLoq is supplied by Microchip Technology Inc.</td>
</tr>
<tr>
<td>- KeeLoq is a complex automotive access control system including</td>
</tr>
<tr>
<td>- encryption algorithm,</td>
</tr>
<tr>
<td>- authentication protocols and</td>
</tr>
<tr>
<td>- multiple key management schemes</td>
</tr>
</tbody>
</table>
KeeLoq is used by Chrysler, Daewoo, Fiat, GM, Honda, Toyota, Volvo, VW, Jaguar for car access

Other use cases:
- garage door openers (HomeLink),
- property authentication,
- product identification, etc.
KeeLoq Block Cipher

**Definition**

- KeeLoq is a block cipher
- 32-bit blocks $Y = (y_{31}, y_{30}, \ldots, y_1, y_0)$
- 64-bit key $K = (k_{63}, k_{62}, \ldots, k_1, k_0)$
- NLFSR-based = extremely unbalanced Feistel network
- One encryption = 528 encryption cycles
- Hardware footprint - about 700 GE
KeeLoq Block Cipher

One encryption cycle and \( NLF \)

Nonlinear update function

\[
NLF(x_4, x_3, x_2, x_1, x_0) = x_0 \oplus x_1 \oplus x_0x_1 \\
\oplus x_1x_2 \oplus x_2x_3 \oplus x_0x_4 \oplus x_0x_3 \oplus x_2x_4 \\
\oplus x_0x_1x_4 \oplus x_0x_2x_4 \oplus x_1x_3x_4 \oplus x_2x_3x_4
\]

Feedback computation

\[
\varphi = NLF(y_0^{(i)}, y_1^{(i)}, y_2^{(i)}, y_3^{(i)}_9, y_1^{(i)}) \\
\oplus y_0^{(i)} \oplus y_1^{(i)} \oplus k_0^{(i)}
\]

Data and key update

\[
Y^{(i+1)} = (\varphi, y_{31}^{(i)}, \ldots, y_1^{(i)}) \\
K^{(i+1)} = (k_0^{(i)}, k_{63}^{(i)}, \ldots, k_1^{(i)})
\]
KeeLoq Block Cipher
Round Structure

Notation

\[ F(K) : \mathbb{F}_2^{32} \rightarrow \mathbb{F}_2^{32} = \text{one round} = 64 \text{ encryption cycles} \]

\[ F'(K') : \mathbb{F}_2^{32} \rightarrow \mathbb{F}_2^{32} = \frac{1}{4} \text{ round} = 16 \text{ encryption cycles} \]
Basic Properties and Attack Principles

Key Schedule

- 8 full rounds $K = (k_{63}, \ldots, k_0)$ and 1/4 round $K' = (k_{15}, \ldots, k_0)$:
- The KeeLoq key schedule is very self-similar
  $\Rightarrow$ slide attacks

Resilience of NLF

NLF is 1-resilient, but not 2-resilient $\Rightarrow$ linear approximations
$\Rightarrow$ linear analysis
Pseudo-slide group

If 16-bit subkey $K'$ and a slide pair $(I_0, O_0), (I_1, O_1)$ are guessed, a pseudo-slide group can be generated if the whole code book is known:

$$\{I_i, O_i\}_{i=0}^{2^8-1},$$

where $O_i = F_K(I_i)$. 
Lemma

For uniformly distributed $x_4, x_3, x_2 \in GF(2)$ the following holds:

- $\text{Pr} \{ NLF(x_4, x_3, x_2, x_1, x_0) = 0 \mid x_0 \oplus x_1 = 0 \} = \frac{5}{8},$
- $\text{Pr} \{ NLF(x_4, x_3, x_2, x_1, x_0) = 1 \mid x_0 \oplus x_1 = 1 \} = \frac{5}{8}.$

Corollary

NLF can be efficiently approximated by $x_0 \oplus x_1.$
**Attack Outline**

**Correlation Step**  $\Rightarrow  k_{16} \oplus k_{32}$

---

**Relations**

\[
\begin{align*}
y^{(32)}_{16} & = c_0 \oplus k_{16} \\
y^{(64)}_{0} & = NLF(y^{(32)}_{31}, y^{(32)}_{26}, y^{(32)}_{20}, y^{(32)}_{9}, y^{(32)}_{1}) \\
& \oplus y^{(32)}_{0} \oplus (c_0 \oplus k_{16}) \oplus k_{32}
\end{align*}
\]

**Obtaining $k_{16} \oplus k_{32}$**

- Recover $k_{16} \oplus k_{32}$ statistically using the pseudo-slide group
- $k_{16} \oplus k_{32} = y^{(64)}_{0} \oplus y^{(32)}_{9} \oplus c_0 \oplus \epsilon(l_i, K')$
- $Pr\{\epsilon(l_i, K') = y^{(32)}_{9} \oplus y^{(32)}_{1}\} = 1/2 + 1/8$

---

**Legend**

- $\square = \text{unknown}$
- $\square = \text{known}$
- $\square = \text{updated}$

---

**Andrey Bogdanov**  
Attacks on KeeLoq
**Attack Outline**

**Correlation Step**  \( k_{16} \oplus k_{32} \Rightarrow k_{16}, k_{32} \)

---

**Obtaining \( k_{16} \) and \( k_{32} \)**

- Recover \( k_{16} \oplus k_{32} \) statistically using the pseudo-slide group
- Recover \( k_{17} \oplus k_{33} \) and \( k_{16} \oplus k_{17} \oplus k_{33} \) in a similar way using the pseudo-slide group

\[
\begin{align*}
\alpha &= k_{16} \oplus k_{32} \\
\beta &= k_{17} \oplus k_{33} \\
\gamma &= k_{16} \oplus k_{17} \oplus k_{33} \\
\Rightarrow k_{16} &= \beta \oplus \gamma \\
k_{32} &= k_{16} \oplus \alpha
\end{align*}
\]

- Recover \((k_{47}, \ldots, k_{16})\) using this technique

---

**Legend**

- **未知** = unknown
- **已知** = known
- **已更新** = updated
Now 48 key bits are known: \((k_{47}, \ldots, k_0) \Rightarrow \text{compute } Y^{(48)}\)

\[
k_{48} = y_{16}^{(64)} \oplus NLF(y_{31}^{(48)}, y_{26}^{(48)}, y_{20}^{(48)}, y_9^{(48)}, y_1^{(48)}) \oplus y_{16}^{(48)} \oplus y_0^{(48)}
\]

Now 49 key bits are known: \((k_{48}, \ldots, k_0) \Rightarrow \text{compute } Y^{(49)}\)

\[
k_{49} = y_{17}^{(64)} \oplus NLF(y_{31}^{(49)}, y_{26}^{(49)}, y_{20}^{(49)}, y_9^{(49)}, y_1^{(49)}) \oplus y_{16}^{(49)} \oplus y_0^{(49)}
\]

Now 50 key bits are known: \((k_{49}, \ldots, k_0) \Rightarrow \text{compute } Y^{(50)}\)

\[
k_{50} = y_{18}^{(64)} \oplus NLF(y_{31}^{(50)}, y_{26}^{(50)}, y_{20}^{(50)}, y_9^{(50)}, y_1^{(50)}) \oplus y_{16}^{(50)} \oplus y_0^{(50)}
\]

\[
\ldots
\]
Attack Outline

Guess 16 key bits: \( K' = (k_{15}, \ldots, k_0) \)

Guess the output \( O_0 \) of the first round for some input \( I_0 \):

\[
O_0 = F(I_0)
\]

For each guess:

- Generate a pseudo-slide group of size \( 2^8 \)
- Determine \( (k_{47}, \ldots, k_{16}) \) statistically (correlation step)
- Compute \( (k_{63}, \ldots, k_{48}) \) deterministically (linear step)

**Overall complexity:** \( 2^{50.6} \) encryptions and \( 2^{32} \) PTs
Permutation Structure Analysis [CB07]

- For a random $n$-bit permutation: $\ln 2^n$ cycles
- About 22 cycles and about 11 even cycles for $F_K$
- Permutation $F^8_K(\cdot)$ has about $22/2^{\log 8} \approx 2.75$ even cycles
- To determine $K'$:
  - Guess $K'$
  - Count the number of even cycles for $F^8_K(\cdot)$
    - If $> 6$ even cycles $\Rightarrow$ incorrect hypothesis (random)
    - If $\leq 6$ even cycles $\Rightarrow$ correct (8 iterations)
- **Complexity ($K'$):** $2^{37}$ encryptions and $2^{32}$ PTs
Combined Attack
Linear Sliding Attack + Permutation Structure Analysis

- Recover $K' = (k_{15}, \ldots, k_0)$ using permutation structure analysis $\Rightarrow 2^{37}$
- Guess $(I_0, O_0)$
- For each guess perform the linear sliding attack (correlation and linear steps) $\Rightarrow 2^{33}$
- **Overall complexity:** $2^{37}$ encryptions and $2^{32}$ PTs
### Rolling Codes

\[
T \rightarrow V : \text{KEELOQ}(C_{15,0}|D_{11,0}|F), N_{27,0}|F|A
\]

<table>
<thead>
<tr>
<th>KeeLoq-encrypted</th>
<th>Plaintext</th>
</tr>
</thead>
<tbody>
<tr>
<td>( C_{15,0} )</td>
<td>( N_{27,0} )</td>
</tr>
<tr>
<td>( D_{11,0} )</td>
<td>( F )</td>
</tr>
<tr>
<td>( F )</td>
<td>( A )</td>
</tr>
</tbody>
</table>

- \( C_{15,0} \) = synchronized counter
- \( D_{11,0} \) = discrimination value
- \( F = F_{3,0} \) = functional bits
- \( N_{27,0} \) = transponder’s identifier
- \( A \) = several auxiliary bits
Identify Friend or Foe (IFF)

\[ V \rightarrow T : R \quad \text{(32)} \]
\[ T \rightarrow V : K_{\text{EELOQ}}(R) \quad \text{(32)} \]

- \( R = 32\)-bit random challenge
- Simple challenge-response protocol
**XOR-Based Secure Key Generation**

**Notation**

\[
\begin{align*}
S &= \text{seed (32, 48 or 60 bit)} \\
MK &= \text{64-bit \textbf{global} manufacturer key} \\
K &= \text{64-bit individual key}
\end{align*}
\]
Attacks on Key Generation

Scenario 1: Seed unknown

- $K$ known and 32-bit seed $\Rightarrow$ 32 bits of $MK$ known $\Rightarrow 2^{32}$
- $K$ known and 48-bit seed $\Rightarrow$ 16 bits of $MK$ known $\Rightarrow 2^{48}$
- $K$ known and 60-bit seed $\Rightarrow$ 4 bits of $MK$ known $\Rightarrow 2^{60}$

Scenario 2: Seed known

- $K$ completely defines $MK$
- Obtaining $MK$ instantly from $K$
KeeLoq block cipher cryptanalyzed:
- Basic Attack: $2^{50.6}$ KeeLoq encryptions and $2^{32}$ PTs
- Enhanced Attack: $2^{37}$ KeeLoq encryptions and $2^{32}$ PTs $\Rightarrow$ best known attack working for the whole key space

KeeLoq key management analyzed:
- 3 vulnerable key generation schemes found
- Breaking one key leads to the recovery of master key bits