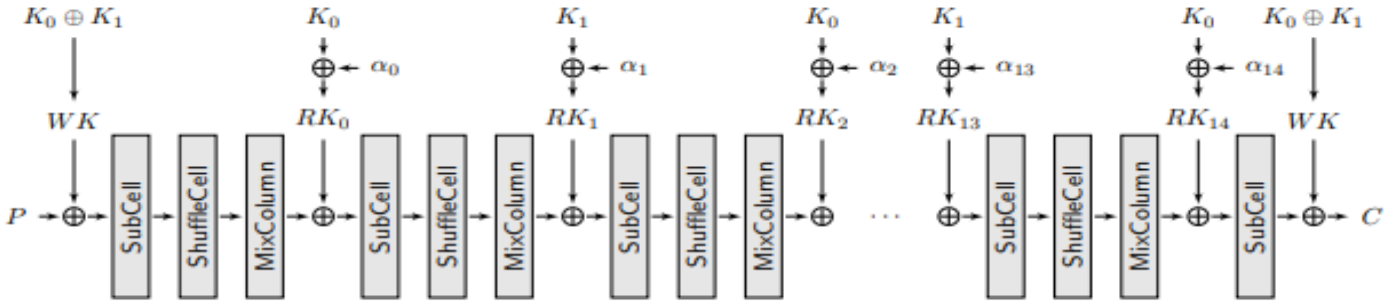
Invariant Subspace Attack Against Full Midori64

Algoritmul Midori64

Foloseste un state S, o matrice de 4x4, pe care se aplica mai multe operatii, intr-un anumit numar de runde.

Plaintext-ul si ciphertext-ul sunt 2 structuri bytes de cate 64 de bits fiecare, iar cheia este formata din 2 subchei, de cate 64 de bits fiecare, cu care se va lucra.



Midori64 encryption algorithm.

Acesta este algoritmul de criptare. Se introduce P(plaintext-ul) in starea S pe care se vor face 4 operatii pe parcursul a R=14 runde. K0 si K1 sunt cele 2 subchei, si in functie de paritatea rundei se face XOR cu una din cele 2. Mai intai de aplica operatia de KeyAdd, unde se face XOR intre plaintext si WK(whitening key) care este rezultatul XOR-ului dintre cele 2 subchei. Mai departe, de R runde ori, se fac, in ordine, operatiile de SubCell, ce aplica un S-box de 4 biti peste matrice, ShuffleCell, ce, cum reiese si din nume, amesteca celulele matricei, MixColumn, ce XOR-uieste celule de pe fiecare coloana si KeyAdd, din nou, dar cu un RK(round key) ce reprezinta rezultatul unui XOR intre subcheie si o alta matrice A ce difera la fiecare runda. A-urile sunt tot o matrici de 4x4, constante, prezinta doar biti de 0 si 1 pe diferite pozitii, si sunt derivate de la forma hexadecimala de criptare a partii fractionale a lui PI. Dupa toate aceste R runde, se realizeaza un SubCell separat si un XOR cu WK. Apoi C(ciphertext-ul) este preluat din state-ul S.

Atacul asupra Midori64 cu subspatii

Atacul presupune un atac pe o cheie slaba apartinand unei clase de dimensiune 2 la puterea 32(numarul maxim de cautari pentru a o descoperi) .

Atacul presupune 2 subspatii:

K = {0, 1} si S = {8, 9}

Acesta aplica teorema subspatiului invariant care spune ca daca cheia contine doar biti din K iar plaintext-ul doar biti din S, atunci sunt sanse 100% ca ciphertext-ul sa contina doar biti din S. Teorema este demonstrata pentru toate cele 4 operatii aplicate starii S, KeyAdd, MixColumn, ShuffleCell si SubCell.

$$\begin{aligned}
\mathbb{S} &\leftarrow \mathsf{SubCell}(\mathbb{S}),\\
\mathbb{S} &\leftarrow \mathsf{ShuffleCell}(\mathbb{S}),\\
\mathbb{S} &\leftarrow \mathsf{MixColumn}(\mathbb{S}),\\
\mathbb{S} &\leftarrow \mathsf{KeyAdd}(\mathbb{S}, RK_i \in \mathbb{K}).
\end{aligned}$$

Evident, aceasta nu este o varianta prea realista intrucat subspatiile sunt de o dimensiunea extrem de mica si pentru cazuri mai mari ar trebui aplicat un brute-force enorm. Totusi, pentru a afla cheia, se poate scrie un sistem de ecuatii liniare astfel:

- vom nota fiecare element din cheie(subchei) cu k -> K, de la 0 la 31;
- vom nota fiecare element din plaintext cu p-> S, de la 0 la 15;
- vom nota fiecare element din ciphertext cu c -> S, de la 0 la 15.

$$K_0 = \begin{bmatrix} k_0 & k_4 & k_8 & k_{12} \\ k_1 & k_5 & k_9 & k_{13} \\ k_2 & k_6 & k_{10} & k_{14} \\ k_3 & k_7 & k_{11} & k_{15} \end{bmatrix} \in \mathbb{K}, \qquad K_1 = \begin{bmatrix} k_{16} & k_{20} & k_{24} & k_{28} \\ k_{17} & k_{21} & k_{25} & k_{29} \\ k_{18} & k_{22} & k_{26} & k_{30} \\ k_{19} & k_{23} & k_{27} & k_{31} \end{bmatrix} \in \mathbb{K},$$

$$P = \begin{bmatrix} p_0 & p_4 & p_8 & p_{12} \\ p_1 & p_5 & p_9 & p_{13} \\ p_2 & p_6 & p_{10} & p_{14} \\ p_3 & p_7 & p_{11} & p_{15} \end{bmatrix} \in \mathbb{S}, \qquad C = \begin{bmatrix} c_0 & c_4 & c_8 & c_{12} \\ c_1 & c_5 & c_9 & c_{13} \\ c_2 & c_6 & c_{10} & c_{14} \\ c_3 & c_7 & c_{11} & c_{15} \end{bmatrix} \in \mathbb{S}.$$

Vom obtine urmatorul sistem de ecuatii:

$$
\begin{aligned}
k_0 \oplus k_{11} \oplus k_{14} \oplus k_{15} \oplus k_{21} \oplus k_{22} \oplus k_{23} \oplus k_{26} \oplus k_{28} \oplus k_{29} \oplus k_{30} \oplus k_{31} &= p_0 \oplus p_5 \oplus p_6 \oplus p_7 \oplus p_{10} \oplus p_{11} \oplus p_{12} \oplus p_{13} \\
&\oplus c_5 \oplus c_6 \oplus c_7 \oplus c_{10} \oplus c_{12} \oplus c_{13} \oplus c_{14} \oplus c_{15} \\
k_1 \oplus k_{11} \oplus k_{19} \oplus k_{24} \oplus k_{26} \oplus k_{29} \oplus k_{31} &= p_1 \oplus p_3 \oplus p_8 \oplus p_{10} \oplus p_{11} \oplus p_{13} \oplus p_{15} \\
&\oplus c_3 \oplus c_8 \oplus c_{10} \oplus c_{13} \oplus c_{15} \oplus 1 \\
k_2 \oplus k_{14} \oplus k_{19} \oplus k_{21} \oplus k_{22} \oplus k_{23} \oplus k_{24} \oplus k_{28} \oplus k_{30} \oplus k_{31} &= p_2 \oplus p_3 \oplus p_5 \oplus p_6 \oplus p_7 \oplus p_8 \oplus p_{12} \oplus p_{15} \\
&\oplus c_3 \oplus c_5 \oplus c_6 \oplus c_7 \oplus c_8 \oplus c_{12} \oplus c_{14} \oplus c_{15} \\
k_3 \oplus k_{15} \oplus k_{19} \oplus k_{24} \oplus k_{25} \oplus k_{29} &= p_8 \oplus p_9 \oplus p_{13} \oplus p_{15} \oplus c_3 \oplus c_8 \oplus c_9 \oplus c_{13} \oplus 1 \\
k_4 \oplus k_{11} \oplus k_{13} \oplus k_{15} \oplus k_{22} \oplus k_{25} \oplus k_{27} \oplus k_{28} \oplus k_{29} \oplus k_{30} &= p_4 \oplus p_6 \oplus p_9 \oplus p_{12} \oplus p_{14} \oplus p_{15} \\
&\oplus c_6 \oplus c_9 \oplus c_{11} \oplus c_{12} \oplus c_{13} \oplus c_{14} \oplus 1 \\
k_5 \oplus k_{14} \oplus k_{22} \oplus k_{23} \oplus k_{25} \oplus k_{28} \oplus k_{29} \oplus k_{30} &= p_5 \oplus p_6 \oplus p_7 \oplus p_9 \oplus p_{12} \oplus p_{13} \\
&\oplus c_6 \oplus c_7 \oplus c_9 \oplus c_{12} \oplus c_{13} \oplus c_{14} \oplus 1 \\
k_6 \oplus k_{13} \oplus k_{14} \oplus k_{15} \oplus k_{22} \oplus k_{25} \oplus k_{28} \oplus k_{29} &= p_9 \oplus p_{12} \oplus p_{14} \oplus p_{15} \oplus c_6 \oplus c_9 \oplus c_{12} \oplus c_{13} \\
k_7 \oplus k_{13} \oplus k_{14} \oplus k_{15} \oplus k_{23} &= p_{13} \oplus p_{14} \oplus p_{15} \oplus c_7 \\
k_8 \oplus k_{15} \oplus k_{24} \oplus k_{29} &= p_{13} \oplus p_{15} \oplus c_8 \oplus c_{13} \\
k_9 \oplus k_{11} \oplus k_{13} \oplus k_{14} \oplus k_{24} \oplus k_{28} &= p_8 \oplus p_9 \oplus p_{11} \oplus p_{12} \oplus p_{13} \oplus p_{14} \oplus c_8 \oplus c_{12} \\
k_{10} \oplus k_{11} \oplus k_{25} &= p_9 \oplus p_{10} \oplus p_{11} \oplus c_9 \oplus 1 \\
k_{12} \oplus k_{13} \oplus k_{14} \oplus k_{15} \oplus k_{29} &= p_{12} \oplus p_{14} \oplus p_{15} \oplus c_{13} \\
k_{16} \oplus k_{19} \oplus k_{24} \oplus k_{25} \oplus k_{29} \oplus k_{31} &= p_0 \oplus p_3 \oplus p_8 \oplus p_9 \oplus p_{13} \oplus p_{15} \\
&\oplus c_0 \oplus c_3 \oplus c_8 \oplus c_9 \oplus c_{13} \oplus c_{15} \oplus 1 \\
k_{17} \oplus k_{19} \oplus k_{22} \oplus k_{23} \oplus k_{24} \oplus k_{25} \oplus k_{26} \oplus k_{27} \oplus k_{28} \oplus k_{31} &= p_1 \oplus p_3 \oplus p_6 \oplus p_7 \oplus p_8 \oplus p_9 \oplus p_{10} \oplus p_{11} \oplus p_{12} \oplus p_{15} \\
&\oplus c_1 \oplus c_3 \oplus c_6 \oplus c_7 \oplus c_8 \oplus c_9 \oplus c_{10} \oplus c_{11} \oplus c_{12} \oplus c_{15} \\
k_{18} \oplus k_{19} \oplus k_{21} \oplus k_{22} \oplus k_{23} \oplus k_{24} \oplus k_{28} \oplus k_{29} \oplus k_{30} \oplus k_{31} &= p_2 \oplus p_3 \oplus p_5 \oplus p_6 \oplus p_7 \oplus p_8 \oplus p_{12} \oplus p_{13} \oplus p_{14} \oplus p_{15} \\
&\oplus c_2 \oplus c_3 \oplus c_5 \oplus c_6 \oplus c_7 \oplus c_8 \oplus c_{12} \oplus c_{13} \oplus c_{14} \oplus c_{15} \oplus 1 \\
k_{20} \oplus k_{22} \oplus k_{23} \oplus k_{25} \oplus k_{28} \oplus k_{29} &= p_4 \oplus p_6 \oplus p_7 \oplus p_9 \oplus p_{12} \oplus p_{13} \\
&\oplus c_4 \oplus c_6 \oplus c_7 \oplus c_9 \oplus c_{12} \oplus c_{13},
\end{aligned}
$$

unde avem 32 de necunoscute, si fiind un sistem nedeterminat, clasa solutiilor este de dimensiune 2 la puterea 16 si contine 2 la puterea 16 de chei diferite. Prin rezolvarea sistemului de mai sus, avand un plaintext si un ciphertext cunoscut, se gasesc 16 valori ale k -> K din cheie, iar apoi, urmatorii 16 biti vor fi gasiti mult mai eficient.

Ca si evaluare a performantei si a costului de atac, metoda sistemului nedeterminat, care este si cea mai eficienta, prezinta un cost destul de mare, aproximativ 2 la puterea 16 doar pentru jumatate din valorile cheii + aflarea celorlalti biti. De asemenea, acest lucru este determinat si de dimensiunea subspatiilor ce, in cazul de fata sunt doar de dimensiune 2.