A New Improved Key-Scheduling for Khudra

Secure Embedded Architecture Laboratory,

Indian Institute of Technology, Kharagpur, India

Rajat Sadhukhan, Souvik Kolay, Shashank Srivastava, Sikhar Patranabis, Santosh Ghosh, Debdeep Mukhopadhyay

Topics

- Lightweight Block Cipher
- Khudra – A case study for lightweight block cipher
- Architecture of Khudra
- Attacks on Khudra
- Resistance against Attacks
- Conclusion

- Motivation: Emerging growth of wearable technologies, pervasive devices, lightweight communication protocols

- Aim: To provide adequate security with minimal hardware requirements constrained by area, power, and cost

- Target application areas: Internet-of-Things (IoTs), battery powered wireless sensor networks (WSNs)

Topics

- Lightweight Block Cipher
- Khudra – A case study of lightweight block cipher
- Architecture of Khudra
- Attacks on Khudra
- Resistance against Attacks
- Conclusion

Khudra - Features

- Lightweight Block Cipher targeting both ASIC and low cost FPGAs
- Simple Key Scheduling algorithm
- Unique balanced LUTs and Flip-Flops as lightweight strategy

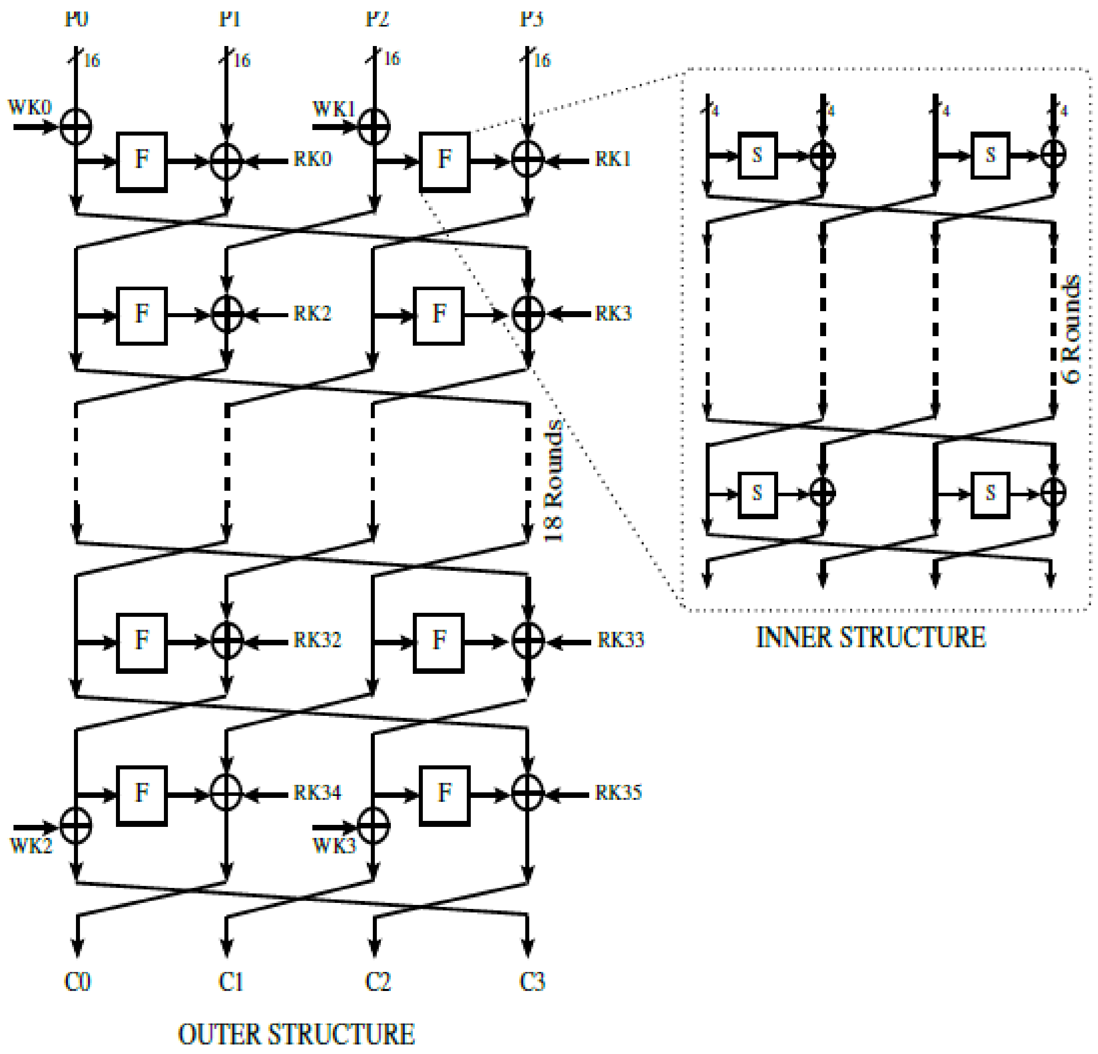
Topics

- Lightweight Block Cipher
- Khudra – A case study for lightweight block cipher
- Architecture of Khudra
- Attacks on Khudra
- Resistance against Attacks
- Conclusion

Khudra – Architecture (Data Processing)

- 64-bit data block, 80-bit master key, 32-bit round key, 18-rounds
- Generalized Type-2 Fiestel structure based Block Cipher implementation
- Data Processing part consist of recursive Fiestel structure in each rounds
- The Fiestel structure consist of two parts: Fiestel permutation and F function. F function in turn again consist of 6 rounds of recursive Fiestel function

Khudra – Architecture (Data Processing)



Khudra – Architecture (Key Scheduling)

- Generates two 16-bit round keys (RKi)
- Uses two round keys in each round, so total 36 round keys generated
- Four whitening keys (WKi) of 16-bit each

Algorithm 1: Key Scheduling $(k_0, k_1, k_2, k_3, k_4)$

$WK0 \leftarrow k_0, WK1 \leftarrow k_1, WK3 \leftarrow k_3, WK4 \leftarrow k_4$

for $i \leftarrow 0$ *to* 35 **do**

  $RCi \leftarrow \{0||i_{(6)}||00||i_{(6)}||0\}$

  $RKi \leftarrow k_{i \bmod 5} \oplus RCi$

end

Topics

- Lightweight Block Cipher
- Khudra – A case study for lightweight block cipher
- Architecture of Khudra
- Attacks on Khudra
- Resistance against Attacks
- Conclusion

Attack : Reduction in round key size from 32-bit to 16-bit

- Why ??
  - Every round second and fourth branch intermediate data and the round key gets XORed with output of F-function from first and third branch

- Result
  - The same key is getting XORed with data at ith round in branch 2 and then at (i+2)th round in branch 4
  - Only 16-bits key gets used in every round with a reduced equivalent structure

when i = 1, where i is ith round

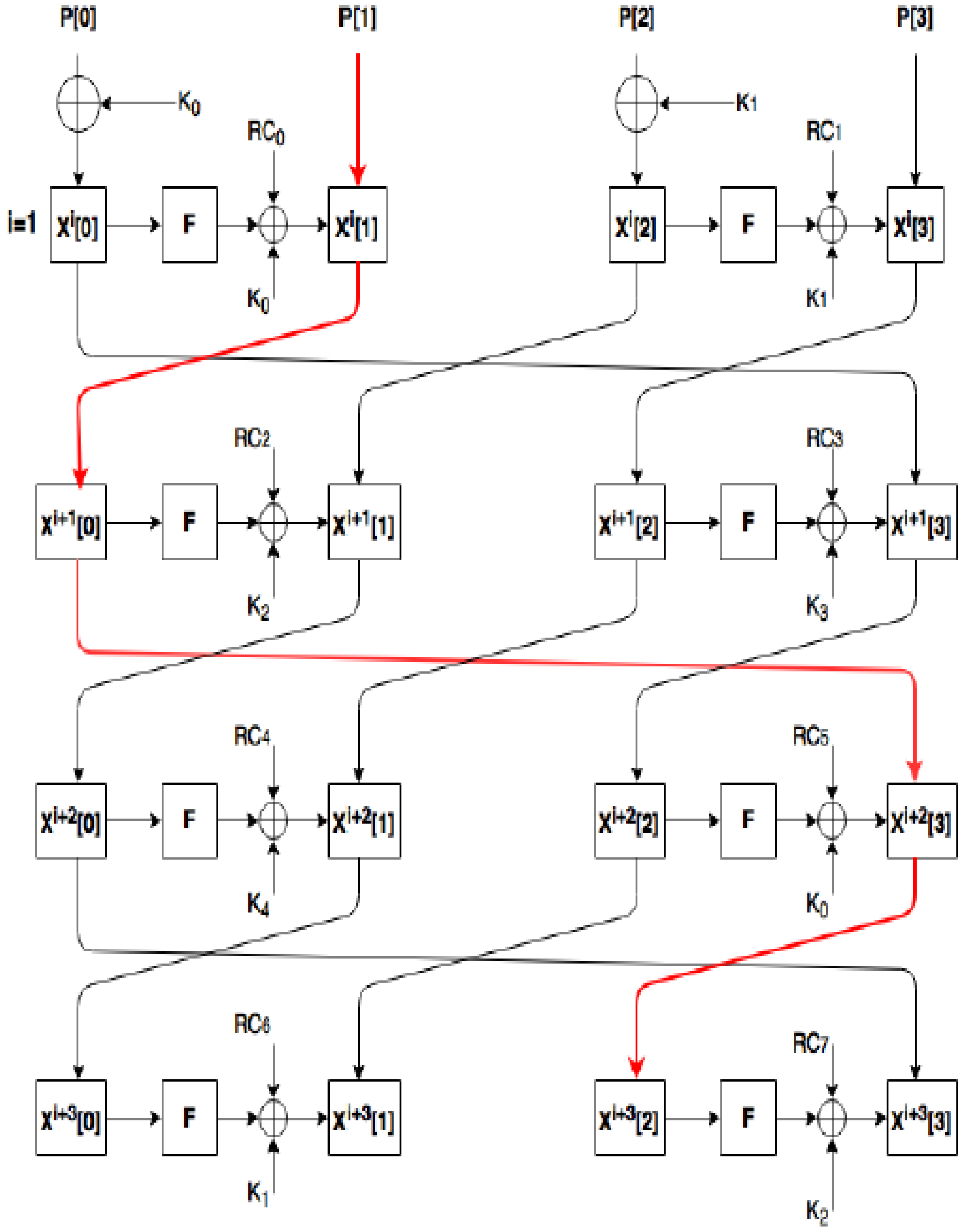
$X^4[2] = K_0 \oplus RC_5 \oplus X^3[3] \oplus F(X^3[2])$

$X^4[2] = K_0 \oplus RC_5 \oplus X^2[0] \oplus F(X^3[2])$ (as $X^3[3] = X^2[0]$)

$X^4[2] = K_0 \oplus RC_5 \oplus F(P[0] \oplus K_0) \oplus RC_0 \oplus K_0 \oplus P[1] \oplus F(X^3[2])$ .... (i)

Ignoring the round constants RC_5 and RC_0 equation (i) can be written as,

$X^4[2] = F(P[0] \oplus K_0) \oplus P[1] \oplus F(X^3[2])$ .... (ii)

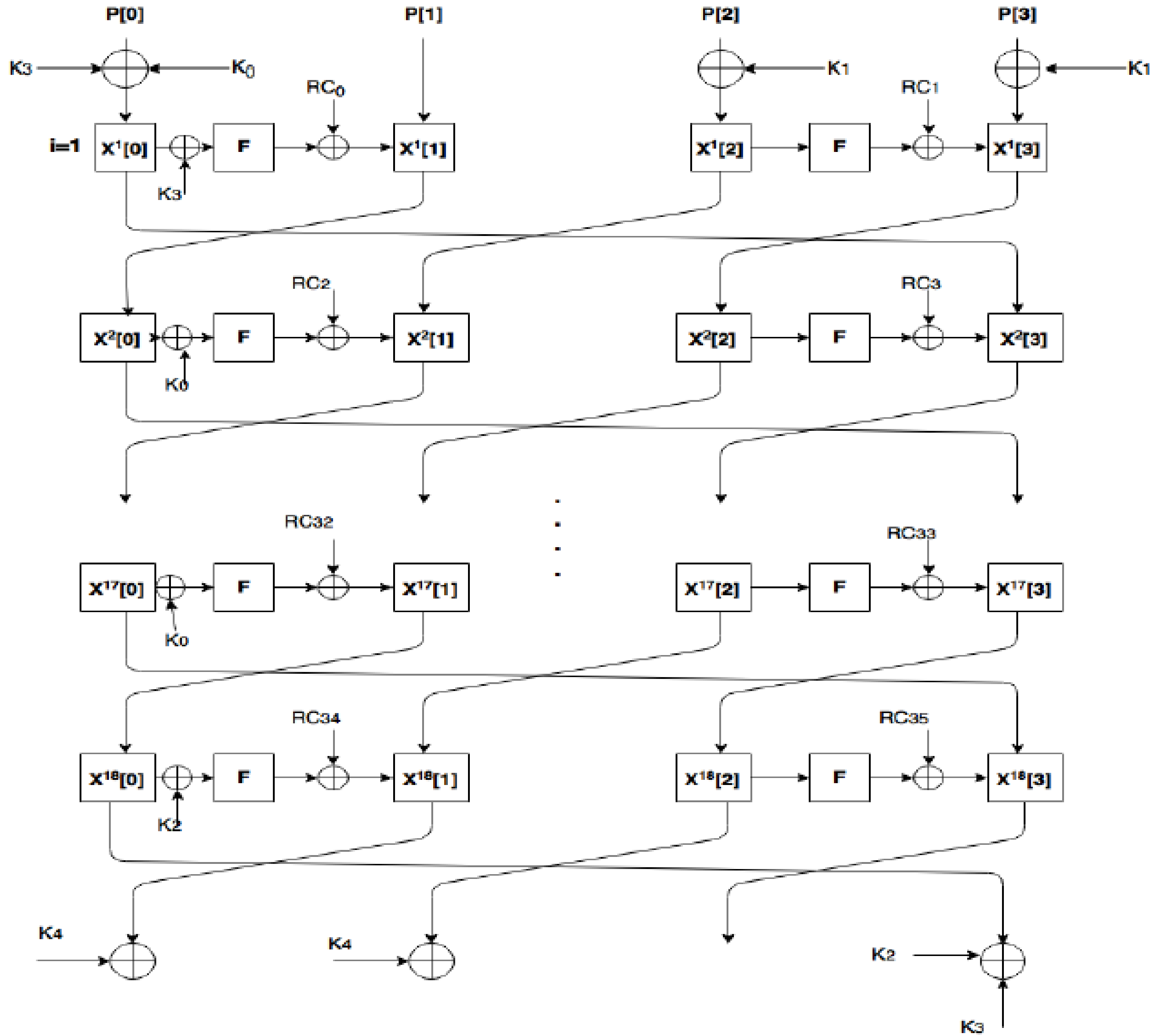


So from equation (ii) it is clear that all right hand side keys can be ignored. Rewriting equation (ii) as follows:

$X^4[2] = F(P[0] \oplus K_0 \oplus K_3 \oplus K_3) \oplus P[1] \oplus F(X^3[2])$ .... (iii)

where, $K_0 \oplus K_3$ is the whitening key. Since in round 2 K_3 is used, so to remove K_3 from the branch it can be added as whitening key with K_0 in the same branch. So whitenening key is now $K_3 \oplus K_0$ instead K_0 for P[0]. Similarly K_1 from right side branch of round 1 by adding it to the P[3] as whitening key. In similar fashion last round whitening keys can be adjusted as shown in the figure 3

- Whitening Keys gets changed in equivalent structure
- K3,K0,K2,K4,K1 are the keys to be used cyclically in the clockwise direction in the reduced architecture



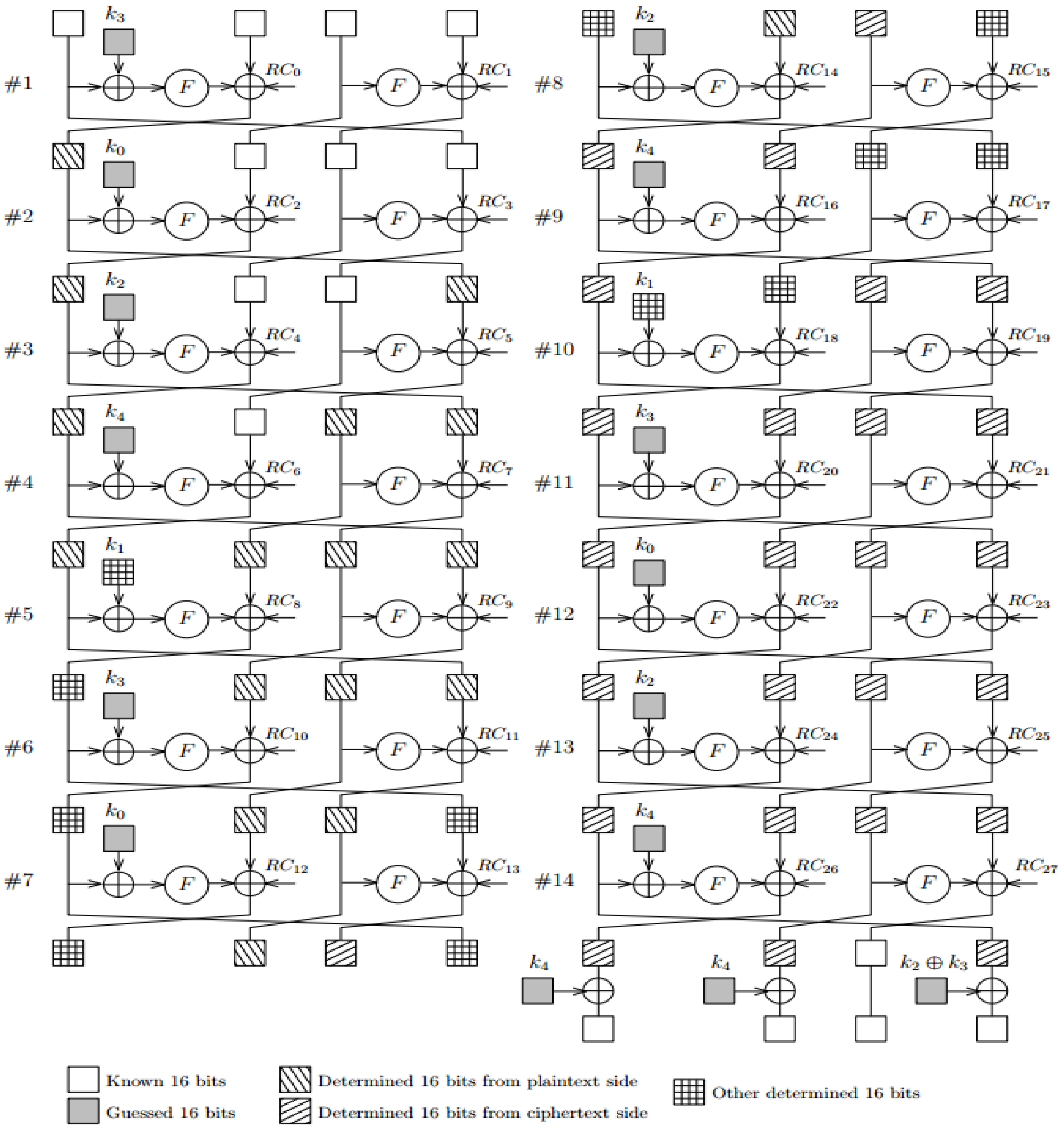
Attack : Guess-and-Determine Attack

- Why ??
  - Reduction in effective length of 32-bit key to 16-bit in each round with keys getting used only on the left side and right side is keyless

- Result
  - Launched on 14-rounds Khudra
  - Requires only two pairs of plaintext-ciphertext
  - Memory complexity: 2, data complexity: 2^{64}

Input: 2 plaintext-ciphertext pairs (P_1, C_1) and (P_2, C_2)
Output: 80-bit key $(K = (k_0 \| k_1 \| k_2 \| k_3 \| k_4))$
for all possible values of (k_0, k_2, k_3, k_4) **do**
    Compute $X_1, X_2, X_3, X_4, X_5[1,2,3], X_6[1,2], X_7[1]$ using P_1.
    Compute $X_{14}, X_{13}, X_{12}, X_{11}, X_{10}, X_9[0,2,3], X_8[0,1], X_7[2]$ using C_1.
    $X_5[0] = X_6[3] \leftarrow F(X_6[2]) \oplus X_7[2] \oplus RC_{13}$
    $k_1 \leftarrow F^{-1}(X_5[0] \oplus X_4[1] \oplus RC_8) \oplus X_4[0]$
    $X_7[3] = X_6[0] \leftarrow F(X_5[0] \oplus k_3) \oplus X_5[1] \oplus RC_{10}$
    $X_8[3] = X_7[0] \leftarrow F(X_6[0] \oplus k_0) \oplus X_6[1] \oplus RC_{12}$
    if $X_8[0] = F(X_7[0] \oplus k_2) \oplus X_7[1] \oplus RC_{14}$ **then**
        $X_9[1] = X_8[2] \leftarrow F(X_7[2]) \oplus X_7[3] \oplus RC_{15}$
        if $(X_9[2] = F(X_8[2]) \oplus X_8[3] \oplus RC_{17})$ and $(X_{10}[0] = F(X_9[0] \oplus k_1) \oplus X_9[1] \oplus RC_{18})$ **then**
            if 80-bit key $(k_0, k_1, k_2, k_3, k_4)$ satisfies the (P_2, C_2) pair **then**
                Output the key
            end if
        end if
    end if
end for

$$k_1 = F^{-1}(X_5[0] \oplus X_4[1] \oplus RC_8) \oplus X_4[0]$$



Large Weak Key Space

- Why ??
  - Symmetric round constant 0||i6||00||i6|0

- Result
  - Plaintext, ciphertext and the masterkey will follow closed property under xor operation if they are also symmetric as round constant
  - As masterkey has five 16-bit blocks and in each block 2^8 symmetric patterns possible, so there are about 2^{40} weak keys present

Differential Probability observation

- Why ??
  - All 16-bits of data enters a single F-function, without any keys getting used inside F-function, so considered as one 16x16 S-box

- Result
  - By exhaustive search it has been found that differential probability is $2^{-9.48}$ for an F-function and as Khudra has minimum six active F-function the differential probability is $2^{-56.88} < 2^{-64}$

Topics

- Lightweight Block Cipher
- Khudra – A case study for lightweight block cipher
- Architecture of Khudra
- Attacks on Khudra
- Resistance against Attacks
- Conclusion

Increase number of rounds in F-function

- Result
  - By exhaustive search it has been found that differential probability will change from $2^{-9.48}$ for an F-function with six rounds to $2^{-10.83}$ with eight rounds
  - As a result as Khudra has minimum six active F-function the differential probability is $2^{-64.98} > 2^{-64}$
  - No hardware changes needed to intercept the above modification

Change in Key Scheduling Algorithm

$WK0 \leftarrow k_0, WK1 \leftarrow k_1, WK3 \leftarrow k_3, WK4 \leftarrow k_4$
$j \leftarrow 0$
for $i \leftarrow 0$ *to* 35 **do**
$\quad j \leftarrow j + (i \bmod 2)$
$\quad RC_i \leftarrow \{00||i_{(6)}||0||i_{(6)}||0\}$
$\quad RK_i \leftarrow k_{j \bmod 5} \oplus RC_i$
end

- Result
  - Change eliminates the earlier equivalent definition of a round of Khudra
  - Overcomes the guess and determine attack
  - stops the chances of memory optimization to Meet-in-the-middle attack

Change in Round Constant

- Result
  - The round constant is changed from symmetric 0||i6||00||i6||0 to asymmetric 00||i6||0||i6||0
  - even symmetric 16-bit blocks of a key will not lead to a symmetric round key, and thus eliminate the issue of weak keys

Topics

- Lightweight Block Cipher
- Khudra – A case study for lightweight block cipher
- Architecture of Khudra
- Attacks on Khudra
- Resistance against Attacks
- Conclusion

- With minimal modifications we are able to mitigate the attacks proposed by authors
- The modified key scheduling algorithm is also as lightweight as the older design
- Also proposed addition of two more rounds over present six rounds inside F-function to improve the differential probability at no cost over the hardware
- Opens door for future research towards exploring the performance and security issues by expanding the key length from 64-bits to 128-bits

References

- Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J., Seurin, Y., Vikkelsoe, C.: Present: An ultra-lightweight block cipher. In: Proceedings of the 9th International Workshop on Cryptographic Hardware and Embedded Systems. pp. 450–466. CHES ’07, Springer-Verlag, Berlin, Heidelberg (2007), http://dx.doi.org/10.1007/978-3-540-74735-2_31
- Kolay, S., Mukhopadhyay, D.: Khudra: A New Lightweight Block Cipher for FPGAs, pp.126–145. Springer International Publishing, Cham (2014), http://dx.doi.org/10.1007/978-3-319-12060-7_9
- O¨ zen, M., C¸ oban, M., Karakoc¸, F.: A guess-and-determine attack on reduced-round khudra and weak keys of full cipher. IACR Cryptology ePrint Archive 2015, 1163 (2015), http://eprint.iacr.org/2015/1163