A Low Data Complexity Attack on the GMR-2 Cipher Used in the Satellite Phones

Ruilin Li, Heng Li, Chao Li, Bing Sun

National University of Defense Technology, Changsha, China

FSE 2013, Singapore

11th ~13th March, 2013

Outline

- Backgrounds and the GMR-2 Cipher
- Revisit the Component of the GMR-2 Cipher
- The Low Data Complexity Attack
- Experimental Result
- Conclusion

Outline

- Backgrounds and the GMR-2 Cipher
- Revisit each Component of the GMR-2 Cipher
- The Low Data Complexity Attack
- Experimental Result
- Conclusion

Backgrounds and the GMR-2 Cipher

- Mobile communication systems have revolutionized the way we interact with each other
  - GSM, UMTS, CDMA2000, 3GPP LTE
- When do we need satellite based mobile system?
  - In some special cases
    - researchers on a field trip in a desert
    - crew on ships on open sea
    - people living in remote areas or areas that are affected by a natural disaster

Backgrounds and the GMR-2 Cipher

- What is GMR?
  - GMR stands for GEO-Mobile Radio
  - GEO stands for Geostationary Earth Orbit
  - Design heavily inspired from GSM

Backgrounds and the GMR-2 Cipher

- Two major GMR Standards
  - GMR-1 (de-facto standard, Thuraya etc)
  - GMR-2 (Inmarsat and AcES)
- How to protect the security of the communication in GMR system?
  - Using symmetric cryptography
  - Both the authentication and encryption are similar as that of GSM A3/A5 algorithms.

Backgrounds and the GMR-2 Cipher

- Encryption Algorithms in GMR
  - Stream ciphers
  - Reconstructed by Driessen et al.
- GMR-1 Cipher
  - Based on A5/2 of GSM
  - Totally broken by ciphertext-only attack
- GMR-2 Cipher
  - New design strategy
  - Can be broken by known-plaintext attack
  - Read-collision based technique

Backgrounds and the GMR-2 Cipher

- In this talk, we focus on GMR-2 stream cipher
  - Revisit components of the GMR-2 cipher
  - Propose dynamic guess and determine strategy
  - Present a low data complexity attack

Method	Data	Time	Source
Read-Collision Based Technique	$15 \sim 20$ frames	2^{10}	[7]
Read-Collision Based Technique	$5 \sim 6$ frames ($50 \sim 65$ bytes)	2^{18}	[7]
Dynamic Guess-and-Determine	1 frames (15 bytes)	2^{28}	Sect. 5

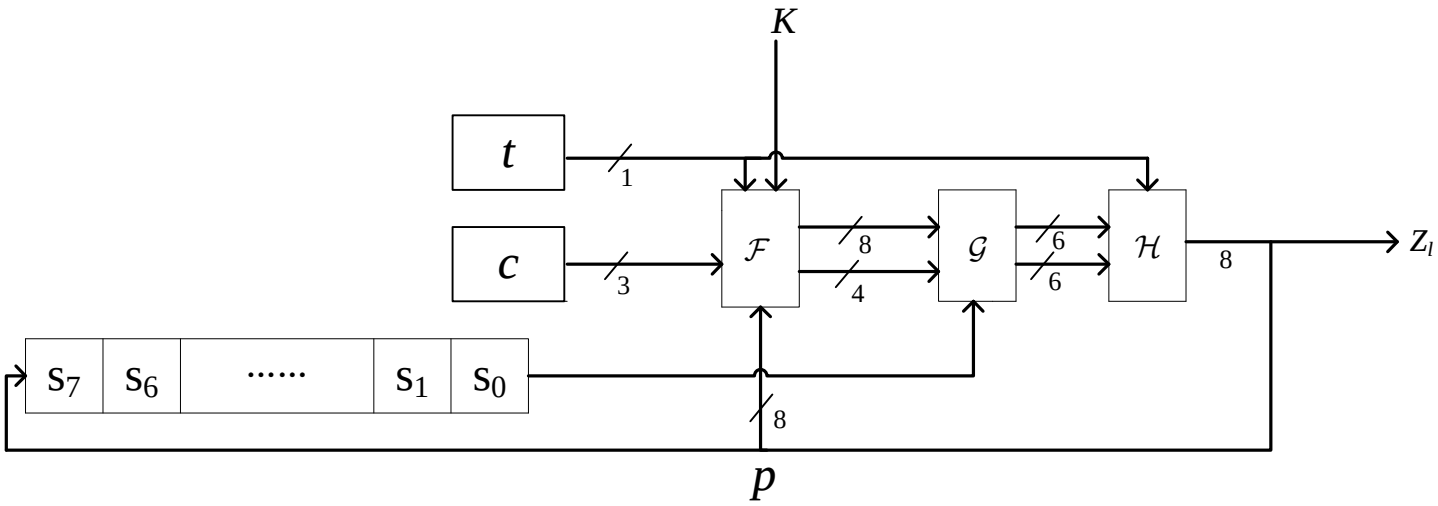
Outline

- Backgrounds and the GMR-2 Cipher
- Revisit each Component of the GMR-2 Cipher
- The Low Data Complexity Attack
- Experimental Result
- Conclusion

Revisit each Component of the GMR-2 Cipher

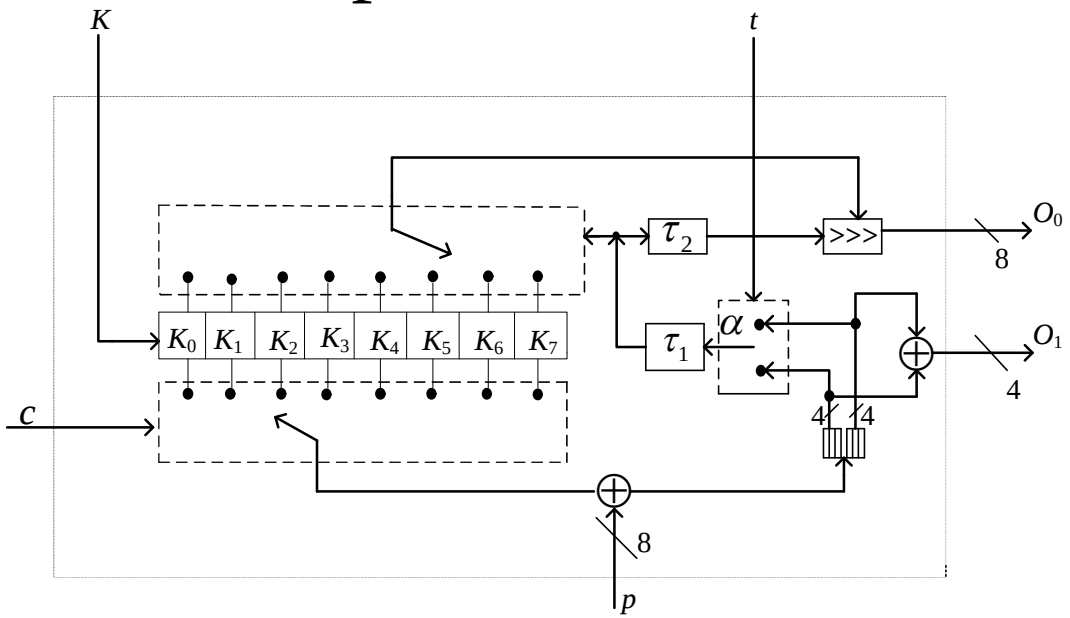
- Encryption mechanism of the GMR-2 cipher
  - Data are divided into frames identified by the frame number with 22-bits
  - New frame is re-initialized
  - Each frame contains 120-bit (15-byte)
- Parameters of the GMR-2 cipher
  - Key length: 64-bit (Session key)
  - IV length: 22-bit (Frame number)
  - Key stream bits length within a frame: 120-bit

Revisit each Component of the GMR-2 Cipher



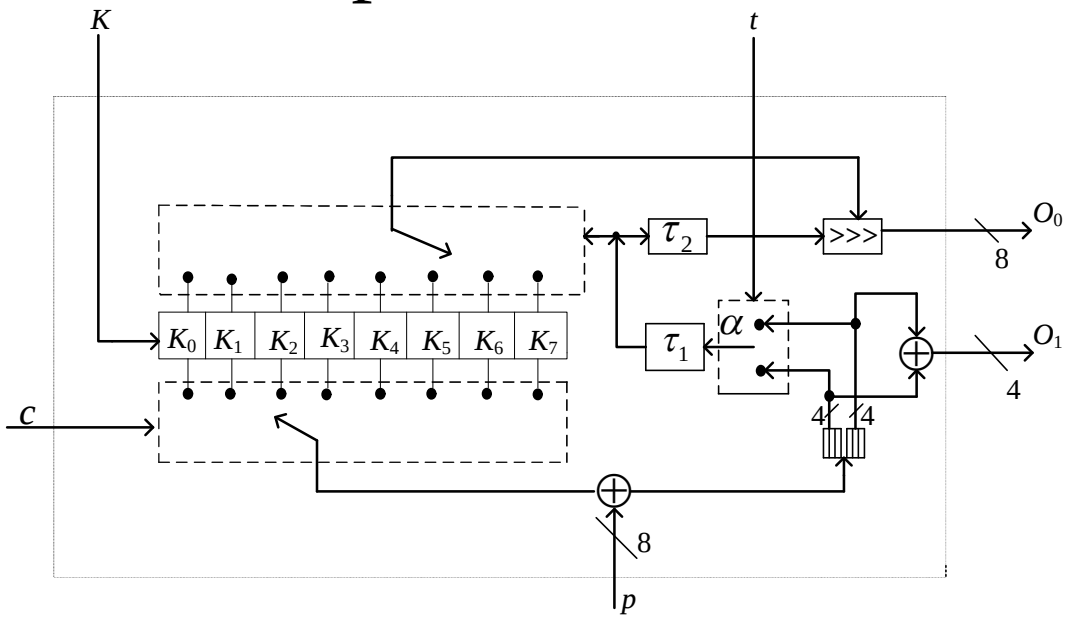
- An overview on the GMR-2 cipher
  - 8-byte shift register ***S***, a 3-bit counter ***c***, and a toggle bit ***t***
  - byte-oriented, three major components
  - $\mathcal{F}$ combines two bytes of session key with previous output
  - $\mathcal{G}$ is a linear function for mixing purpose
  - $\mathcal{H}$ consists two DES Sboxes as a nonlinear filter

Revisit each Component of the GMR-2 Cipher



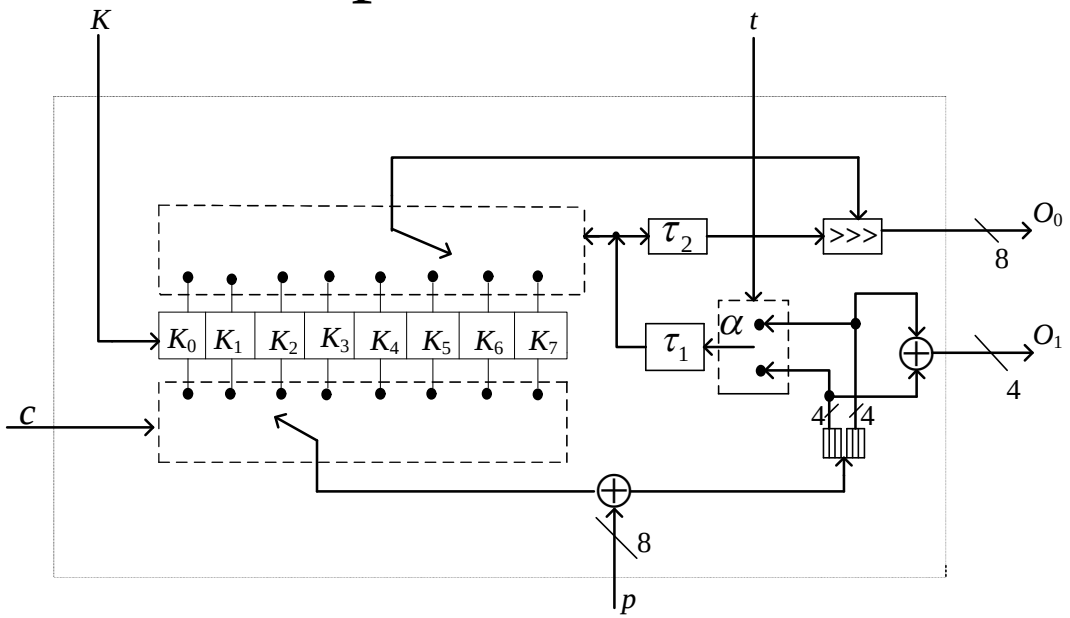
- The $\mathcal{F}$ component
  - At the l-th clock, the input
    - 8-byte array holding the session key $\boldsymbol{K}$, read from two sides.
    - a counter c ranging from 0 to 7 sequentially and repeatedly.
    - a toggle bit $t=c \bmod 2$.
    - the previous key stream byte $p=Z_{l-1}$

Revisit each Component of the GMR-2 Cipher



- The $\mathcal{F}$ component
  - The lower side outputs K_c with the help of the counter c.
  - The upper output depends on the lower output K_c, the previous key stream byte p and the toggle bit t.
  - τ_1 maps 4-bit to 3-bit which select the upper output.
  - τ_2 maps 3-bit to 3-bit which determine the rotation.

Revisit each Component of the GMR-2 Cipher

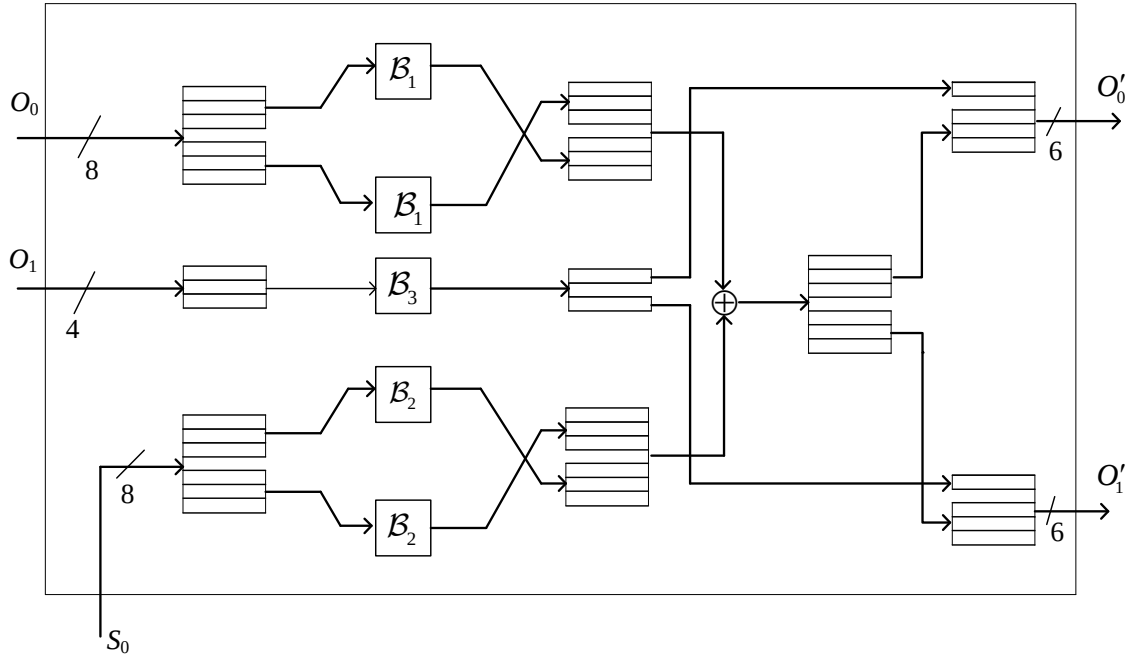


- The $\mathcal{F}$ component
  - The output is

$$\begin{cases} O_0 = K_{\tau_1(\alpha)} \ggg \tau_2(\tau_1(\alpha)) \\ O_1 = (((K_c \oplus p) \gg 4) \,\&\, 0\text{xF}) \oplus ((K_c \oplus p) \,\&\, 0\text{xF}) \end{cases}$$

$$\alpha = \begin{cases} (K_c \oplus p) \,\&\, 0\text{xF}, & \text{if } t = 0 \\ ((K_c \oplus p) \gg 4) \,\&\, 0\text{xF}, & \text{if } t = 1 \end{cases}$$

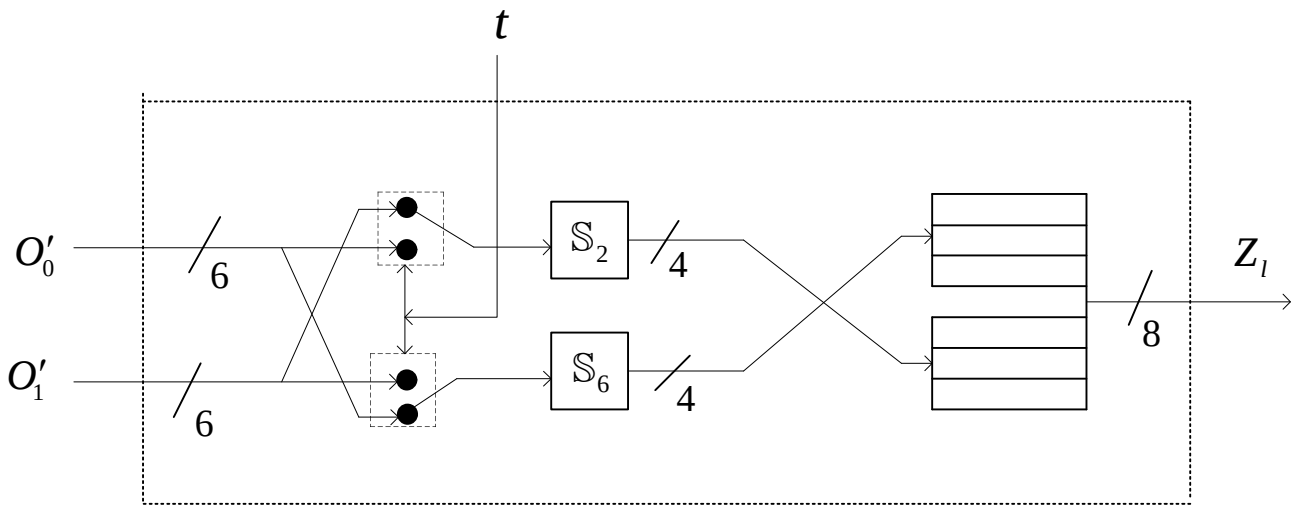
Revisit each Component of the GMR-2 Cipher



- The $\mathcal{G}$ component

$$\begin{cases} B_1 : (x_3, x_2, x_1, x_0) \mapsto (x_3 \oplus x_0,\ x_3 \oplus x_2 \oplus x_0,\ x_3,\ x_1); \\ B_2 : (x_3, x_2, x_1, x_0) \mapsto (x_1,\ x_3,\ x_0,\ x_2); \\ B_3 : (x_3, x_2, x_1, x_0) \mapsto (x_2,\ x_0,\ x_3 \oplus x_1 \oplus x_0, x_3 \oplus x_0). \end{cases}$$

Revisit each Component of the GMR-2 Cipher

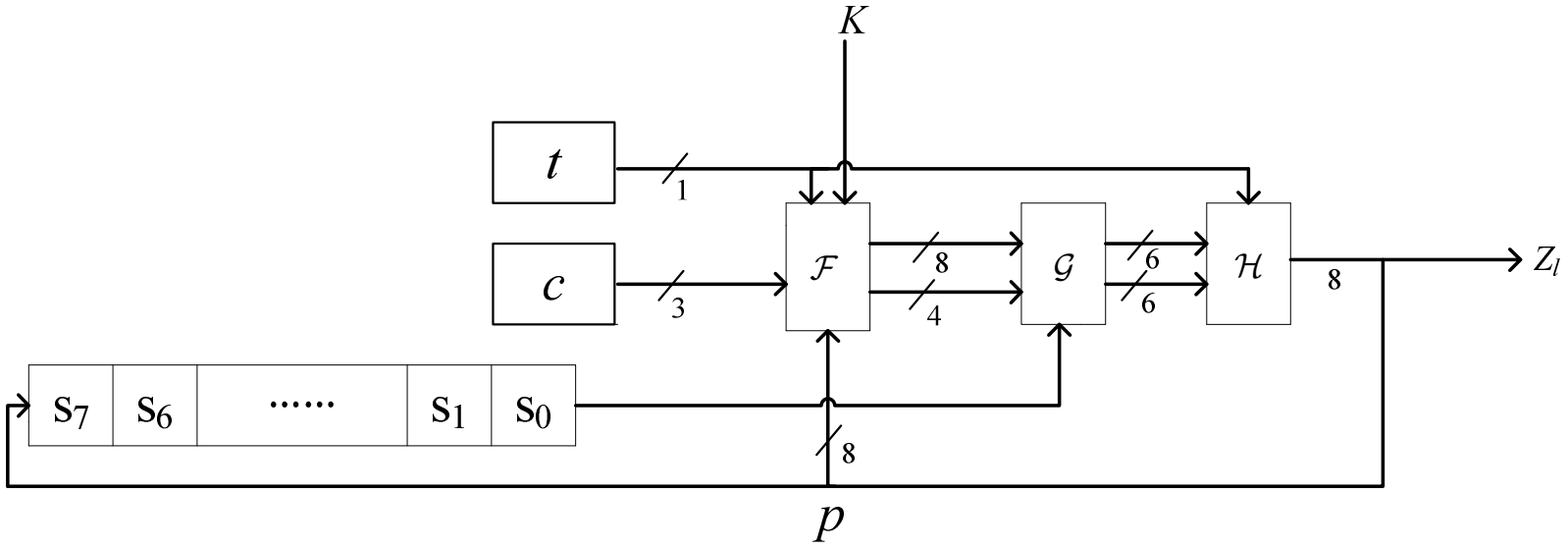


- The $\mathcal{H}$ component

$$Z_l = \begin{cases} (\mathbb{S}_2(O_1'), \mathbb{S}_6(O_0'))_8 & \text{if } t = 0 \\ (\mathbb{S}_2(O_0'), \mathbb{S}_6(O_1'))_8 & \text{if } t = 1 \end{cases}$$

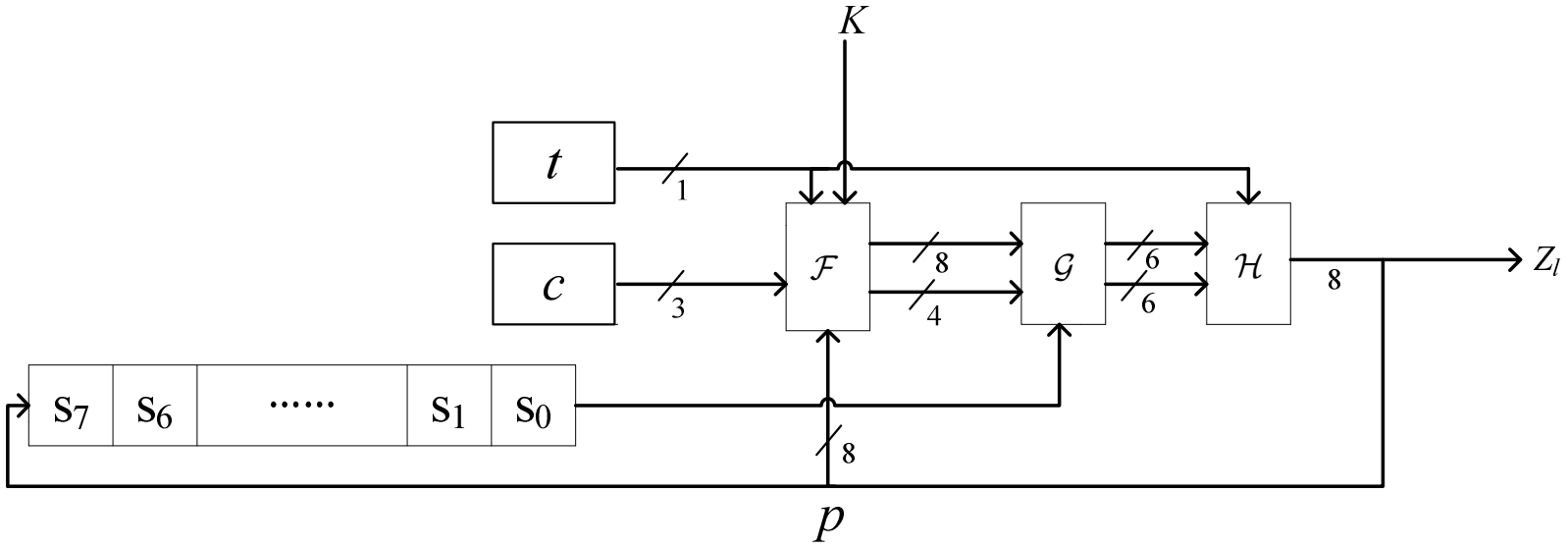
where $\mathbb{S}_2$ and $\mathbb{S}_6$ are the two sboxes of DES. Assume the input of $\mathbb{S}$ is $(x_5, x_4, x_3, x_2, x_1, x_0)$, then (x_1, x_0) selects the row index, and (x_5, x_4, x_3, x_2) selects the column index.

Revisit each Component of the GMR-2 Cipher



- Initialization Mode
  - Set c=0, t=0, and initialize S with frame number N
  - 8-byte key is written into the resister in $\mathcal{F}$
  - Clock the cipher 8 times and discard the output Z_l

Revisit each Component of the GMR-2 Cipher



- Generation Mode
  - For each frame number *N*, further clock the cipher 15 times, and the output keystream is

$$Z' = (Z_0^{(0)}, Z_1^{(0)}, \cdots, Z_{14}^{(0)}; Z_0^{(1)}, Z_1^{(1)}, \cdots Z_{14}^{(1)}; Z_0^{(2)}, \cdots)$$

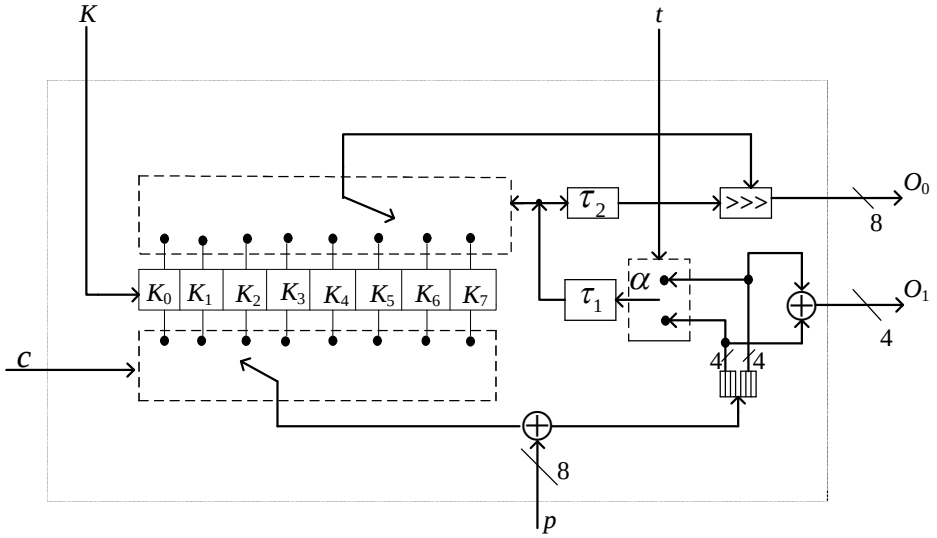
$Z_l^{(N)}$ denotes the *l*-th byte of keystream generated after initialization with *N*

Revisit each Component of the GMR-2 Cipher

- Property of $\mathcal{F}$

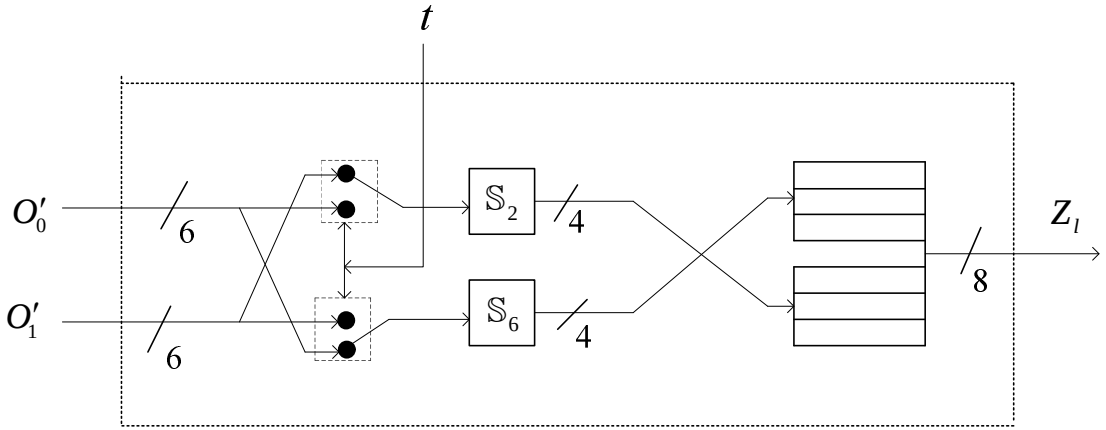
$$\alpha = \begin{cases} (K_c \oplus p)\,\&\,0\text{xF}, & \text{if } t = 0 \\ ((K_c \oplus p) \gg 4)\,\&\,0\text{xF}, & \text{if } t = 1 \end{cases}$$

  - If p is known, then we can get the value of α only by the most/least significant four bits of K_c



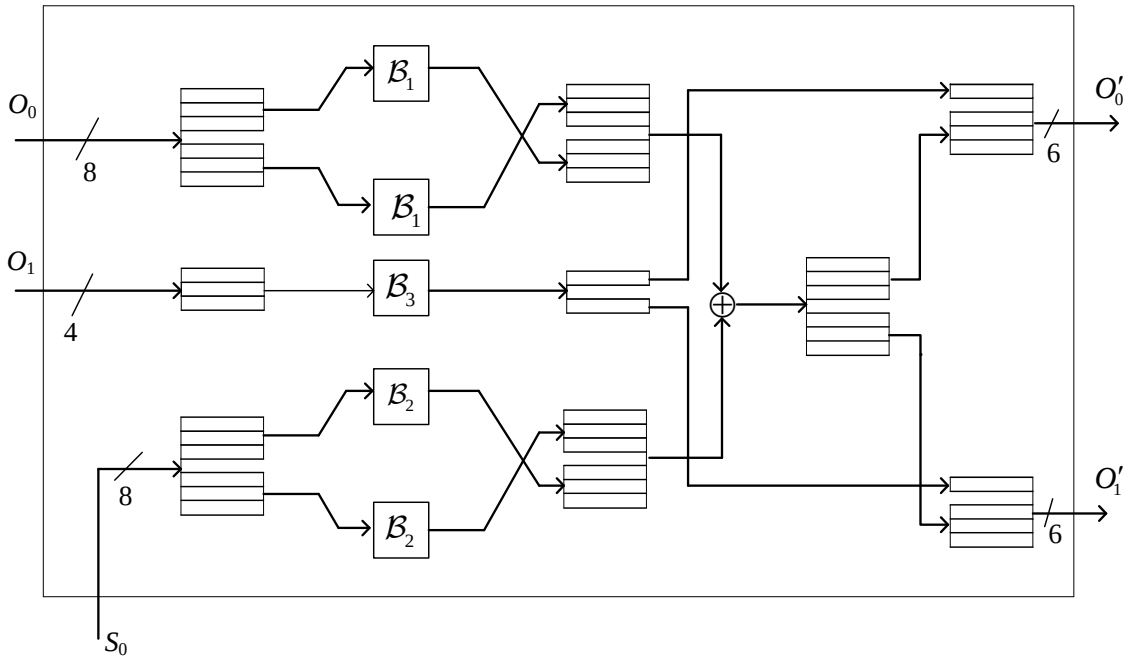
Revisit each Component of the GMR-2 Cipher

- Property of $\mathcal{H}$
  - We can "invert" $\mathbb{S}_2$ / $\mathbb{S}_6$
    - Given the row index and the output, the column index can be uniquely obtained.
    - Given the column index and the output, the row index can be uniquely obtained, except for $\mathbb{S}_6$ when the column index is 4 and the output is 9, the row index can be either 0 or 3.
    - Given the outputs of both S-boxes, there will be 16 possible inputs.

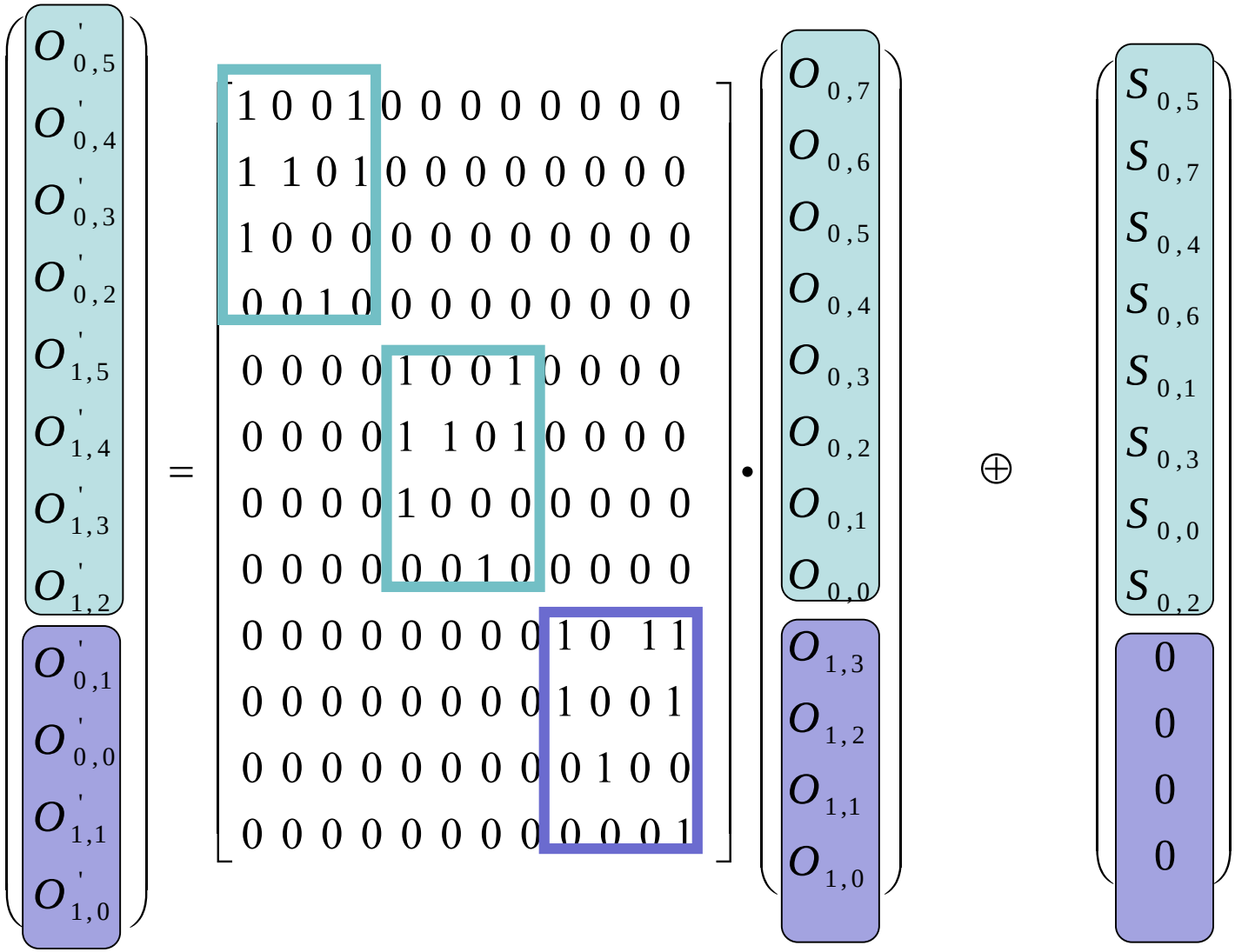


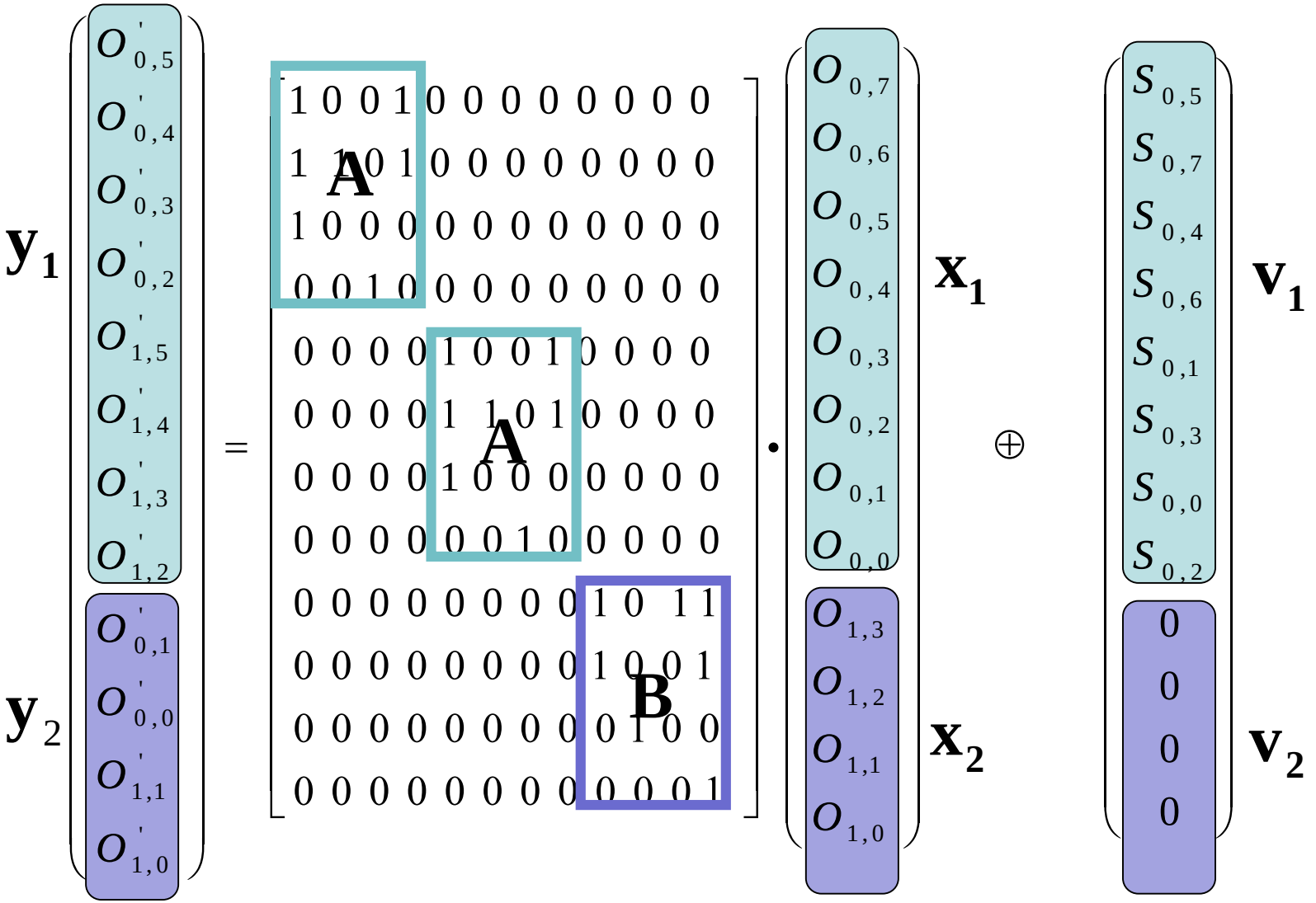
Revisit each Component of the GMR-2 Cipher

- Property of $\mathcal{G}$
  - The key point
  - The links between the input and output of the $\mathcal{G}$ component can be expressed by a well-structured matrix



$$
\begin{pmatrix} O'_{0,5} \\ O'_{0,4} \\ O'_{0,3} \\ O'_{0,2} \\ O'_{1,5} \\ O'_{1,4} \\ O'_{1,3} \\ O'_{1,2} \\ O'_{0,1} \\ O'_{0,0} \\ O'_{1,1} \\ O'_{1,0} \end{pmatrix} = \begin{bmatrix} 1&0&0&1&0&0&0&0&0&0&0&0 \\ 1&1&0&1&0&0&0&0&0&0&0&0 \\ 1&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&0&0&1&0&0&0&0 \\ 0&0&0&0&1&1&0&1&0&0&0&0 \\ 0&0&0&0&1&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&1&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&1&0&1&1 \\ 0&0&0&0&0&0&0&0&1&0&0&1 \\ 0&0&0&0&0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&1 \end{bmatrix} \bullet \begin{pmatrix} O_{0,7} \\ O_{0,6} \\ O_{0,5} \\ O_{0,4} \\ O_{0,3} \\ O_{0,2} \\ O_{0,1} \\ O_{0,0} \\ O_{1,3} \\ O_{1,2} \\ O_{1,1} \\ O_{1,0} \end{pmatrix} \oplus \begin{pmatrix} S_{0,5} \\ S_{0,7} \\ S_{0,4} \\ S_{0,6} \\ S_{0,1} \\ S_{0,3} \\ S_{0,0} \\ S_{0,2} \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}
$$


$O'_{0,5}$ $O'_{0,4}$ $O'_{0,3}$ $O'_{0,2}$ $O'_{1,5}$ $O'_{1,4}$ $O'_{1,3}$ $O'_{1,2}$
$O'_{0,1}$ $O'_{0,0}$ $O'_{1,1}$ $O'_{1,0}$
=
1 0 0 1 0 0 0 0 0 0 0 0
1 1 0 1 0 0 0 0 0 0 0 0
1 0 0 0 0 0 0 0 0 0 0 0
0 0 1 0 0 0 0 0 0 0 0 0
0 0 0 0 1 0 0 1 0 0 0 0
0 0 0 0 1 1 0 1 0 0 0 0
0 0 0 0 1 0 0 0 0 0 0 0
0 0 0 0 0 0 1 0 0 0 0 0
0 0 0 0 0 0 0 0 1 0 1 1
0 0 0 0 0 0 0 0 1 0 0 1
0 0 0 0 0 0 0 0 0 1 0 0
0 0 0 0 0 0 0 0 0 0 0 1
•
$O_{0,7}$ $O_{0,6}$ $O_{0,5}$ $O_{0,4}$ $O_{0,3}$ $O_{0,2}$ $O_{0,1}$ $O_{0,0}$
$O_{1,3}$ $O_{1,2}$ $O_{1,1}$ $O_{1,0}$
⊕
$S_{0,5}$ $S_{0,7}$ $S_{0,4}$ $S_{0,6}$ $S_{0,1}$ $S_{0,3}$ $S_{0,0}$ $S_{0,2}$
0 0 0 0


y1
y2
=
A
A
B
x1
x2
v1
v2

Revisit each Component of the GMR-2 Cipher

- Three linear systems

$$\mathbf{y} = \mathbf{W} \cdot \mathbf{x} \oplus \mathbf{v}$$
$$\mathbf{y_1} = \mathbf{W_1} \cdot \mathbf{x_1} \oplus \mathbf{v_1}$$
$$\mathbf{y_2} = \mathbf{W_2} \cdot \mathbf{x_2} \oplus \mathbf{v_2}$$

$$\mathbf{W} = \begin{pmatrix} \mathbf{A} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{A} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{B} \end{pmatrix}, \quad \mathbf{W_1} = \begin{pmatrix} \mathbf{A} & \mathbf{0} \\ \mathbf{0} & \mathbf{A} \end{pmatrix}, \quad \mathbf{W_2} = (\mathbf{B}),$$

$$\mathbf{y} = (\mathbf{y_1}, \mathbf{y_2}) \quad \mathbf{x} = (\mathbf{x_1}, \mathbf{x_2}) \quad \mathbf{v} = (\mathbf{v_1}, \mathbf{v_2})$$

Revisit each Component of the GMR-2 Cipher

- Another linear system
  - Let $\mathbf{k_h} = (K_{c,7}, K_{c,6}, K_{c,5}, K_{c,4})^T,$
    $\mathbf{k_l} = (K_{c,3}, K_{c,2}, K_{c,1}, K_{c,0})^T,$
    $\mathbf{u} = (p_7 \oplus p_3,\ p_6 \oplus p_2,\ p_5 \oplus p_1,\ p_4 \oplus p_0)^T,$

    then $\mathbf{x_2} = \mathbf{k_h} \oplus \mathbf{k_l} \oplus \mathbf{u}$

    thus from $\mathbf{y_2} = \mathbf{W_2} \cdot \mathbf{x_2} \oplus \mathbf{v_2}$

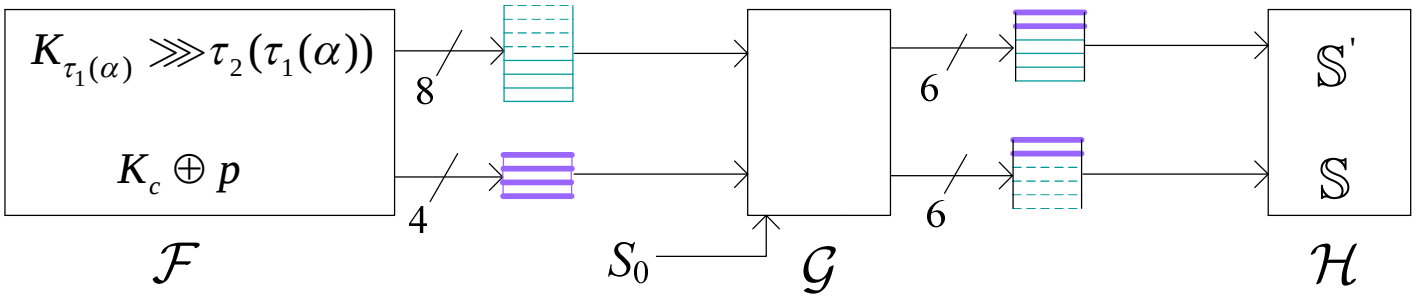
    we obtain $\mathbf{y_2} = \mathbf{W_2} \cdot \mathbf{k_h} \oplus \mathbf{W_2} \cdot \mathbf{k_l} \oplus \mathbf{W_2} \cdot \mathbf{u} \oplus \mathbf{v_2}$

Revisit each Component of the GMR-2 Cipher

$$\begin{cases} \mathbf{y} = \mathbf{W} \cdot \mathbf{x} \oplus \mathbf{v} \\ \mathbf{y}_1 = \mathbf{W}_1 \cdot \mathbf{x}_1 \oplus \mathbf{v}_1 \\ \mathbf{y}_2 = \mathbf{W}_2 \cdot \mathbf{x}_2 \oplus \mathbf{v}_2 \\ \mathbf{y}_2 = \mathbf{W}_2 \cdot \mathbf{k}_h \oplus \mathbf{W}_2 \cdot \mathbf{k}_l \oplus \mathbf{W}_2 \cdot \mathbf{u} \oplus \mathbf{v}_2 \\ \mathbf{x}_1 = K_{\tau_1(\alpha)} \ggg \tau_2(\tau_1(\alpha)) \end{cases}$$

- $\mathbf{W}, \mathbf{W}_1, \mathbf{W}_2, \mathbf{v}, \mathbf{v}_1, \mathbf{v}_2\ \mathbf{u}$ are known values.
- Given $\mathbf{x}\ (\mathbf{x}_i)$, we can obtain $\mathbf{y}(\mathbf{y}_i)$, and vice vera.
- Given $\mathbf{y}_1, \alpha$, we can get $\mathbf{x}_1, K_{\tau_1(\alpha)}$, and vice vera.
- $\mathbf{y}_1$ selects the column index of the S-box and $\mathbf{y}_2$ selects the row index.

Revisit each Component of the GMR-2 Cipher

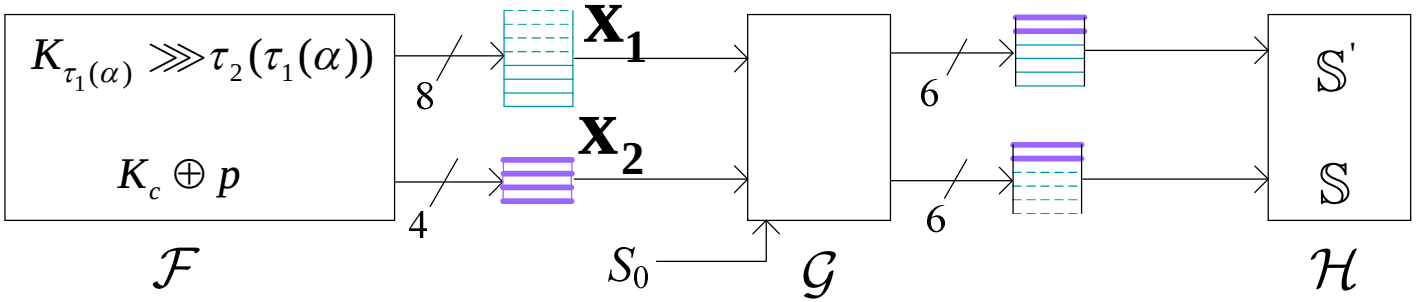


only related to the four most-significant bits of $K_{\tau_1(\alpha)} \ggg \tau_2(\tau_1(\alpha))$ and S_0

only related to the four least-significant bits of $K_{\tau_1(\alpha)} \ggg \tau_2(\tau_1(\alpha))$ and S_0

only related to $K_c \oplus p$

Revisit each Component of the GMR-2 Cipher

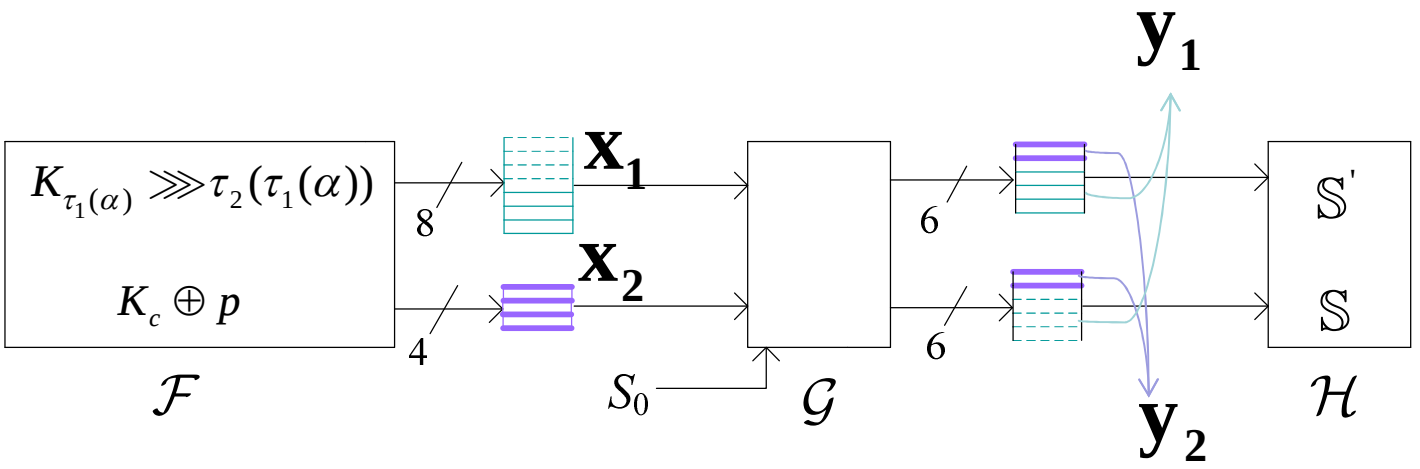


only related to the four most-significant bits of $K_{\tau_1(\alpha)} \ggg \tau_2(\tau_1(\alpha))$ and S_0

only related to the four least-significant bits of $K_{\tau_1(\alpha)} \ggg \tau_2(\tau_1(\alpha))$ and S_0

only related to $K_c \oplus p$

Revisit each Component of the GMR-2 Cipher



only related to the four most-significant bits of $K_{\tau_1(\alpha)} \ggg \tau_2(\tau_1(\alpha))$ and S_0

only related to the four least-significant bits of $K_{\tau_1(\alpha)} \ggg \tau_2(\tau_1(\alpha))$ and S_0

only related to $K_c \oplus p$

Outline

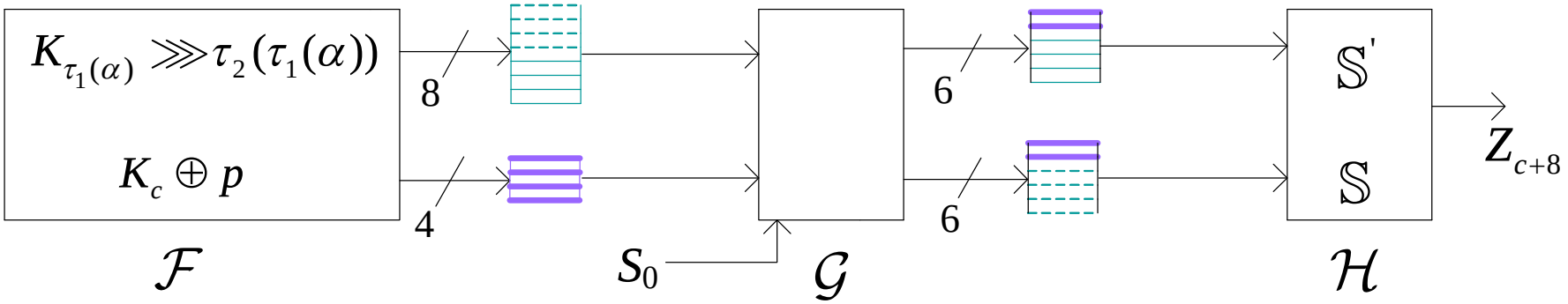
- Backgrounds and the GMR-2 Cipher
- Revisit each Component of the GMR-2 Cipher
- The Low Data Complexity Attack
- Experimental Result
- Conclusion

The Low Data Complexity Attack

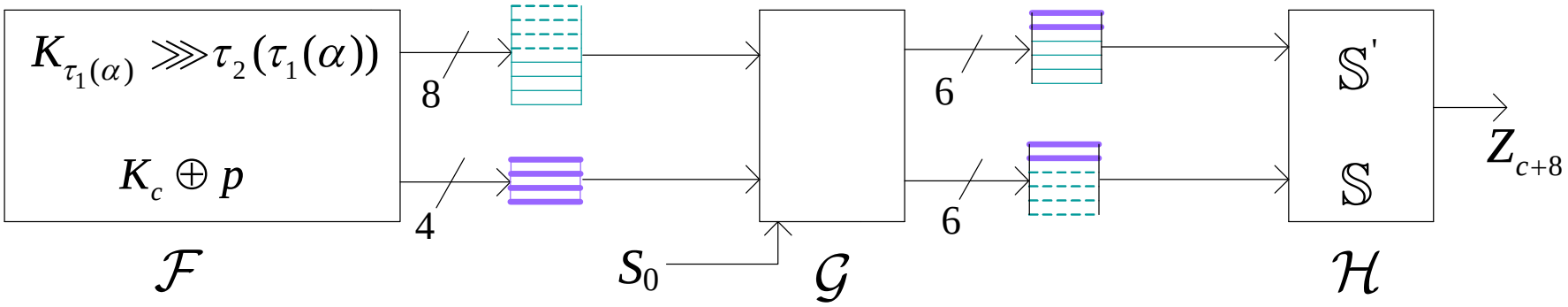
- Known-plaintext attack
  - From keystream bits to recover the session key
- Guess and Determine
  - **Guess -Determine -Verify**
  - **The Guessed and Determined Parts of the internal state are known in prior before applying the attack**
- Dynamic Guess and Determine
  - **Dynamically Guess and Determine**
  - **Dynamically Check the candidate by backtracking**

The Low Data Complexity Attack

- Basic Analysis
  - How these three components interact each other
    - The linear transformation $\mathcal{G}$ plays a central role
    - Since p and S_0 must be known to us, we should analyze the cipher at the $(c+8)$th-clock $(0 \le c \le 6)$ in the keystream generation phase.



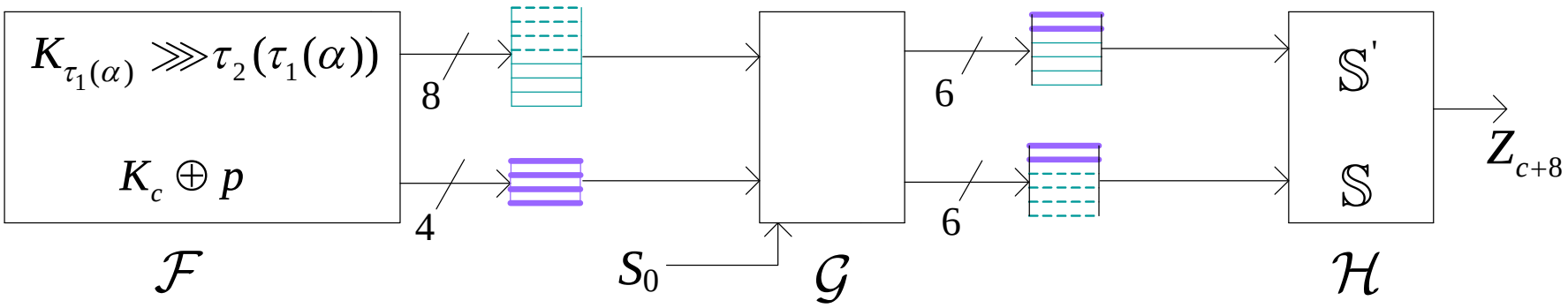
The Low Data Complexity Attack



- Rule 1
  - $\mathbf{y_2} = \mathbf{W_2} \cdot \mathbf{k_h} \oplus \mathbf{W_2} \cdot \mathbf{k_l} \oplus \mathbf{W_2} \cdot \mathbf{u} \oplus \mathbf{v_2}$

    Let $K_c = (\mathbf{k_h}, \mathbf{k_l})$, assume c is odd, and given a guessed value for $\mathbf{k_h}$, if $c = \tau_1(\alpha)$, then using the theory of *linear consistence test*, $\mathbf{k_l}$ has no solution or can be determined by $Z_{c+8}^{(N)}$; Similarly,assume c is even,and given a guessed value for $\mathbf{k_l}$, if $c = \tau_1(\alpha)$, then $\mathbf{k_h}$ has no solution or can be determined by $Z_{c+8}^{(N)}$.

The Low Data Complexity Attack

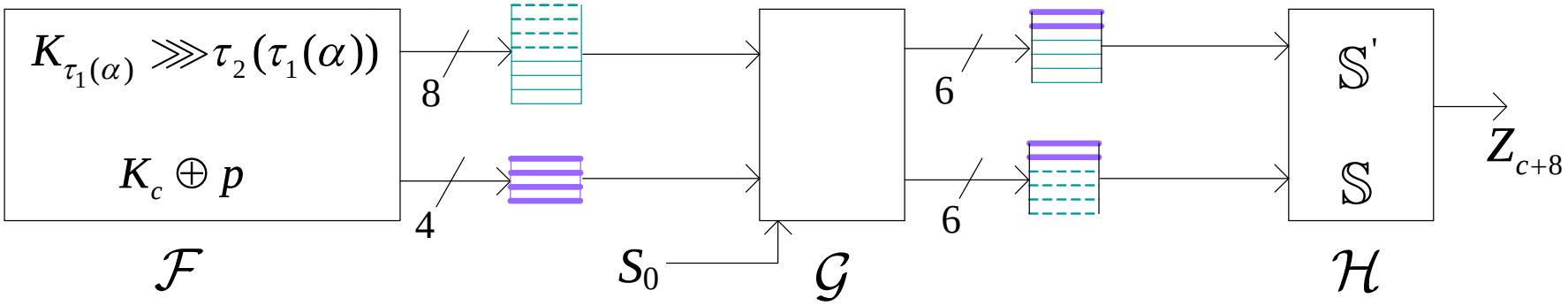


- Rule 2
  - $\mathbf{y_1} = \mathbf{W_1} \cdot \mathbf{x_1} \oplus \mathbf{v_1}$

    $\mathbf{y_2} = \mathbf{W_2} \cdot \mathbf{k_h} \oplus \mathbf{W_2} \cdot \mathbf{k_l} \oplus \mathbf{W_2} \cdot \mathbf{u} \oplus \mathbf{v_2}$

    Let $K_c = (\mathbf{k_h}, \mathbf{k_l})$, and given guessed values for $K_{\tau_1(\alpha)}$ and $\mathbf{k_h}$, then $\mathbf{k_l}$ can be determined by $Z_{c+8}^{(N)}$; Similarly, given guessed values for $K_{\tau_1(\alpha)}$ and $\mathbf{k_l}$, then $\mathbf{k_h}$ can be determined by $Z_{c+8}^{(N)}$.

The Low Data Complexity Attack

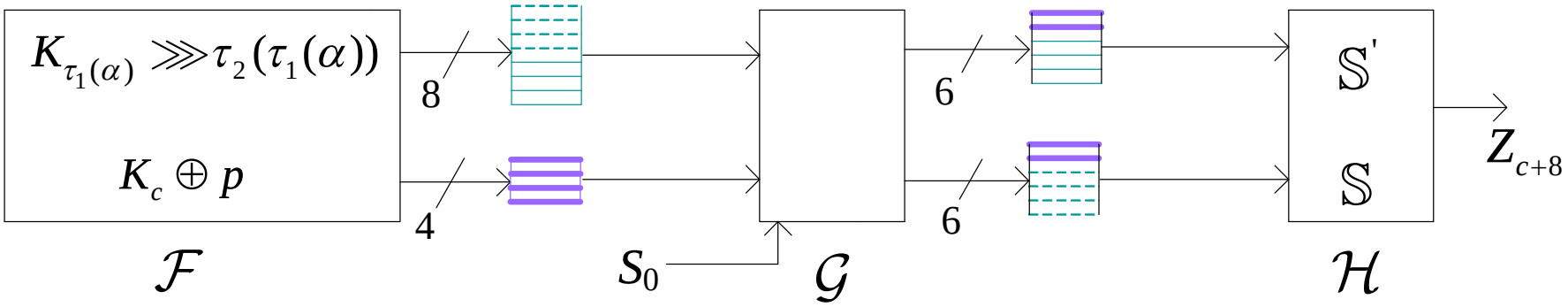


- Rule 3
  - $\mathbf{y_2} = \mathbf{W_2} \cdot \mathbf{x_2} \oplus \mathbf{v_2}$

    $\mathbf{y_1} = \mathbf{W_1} \cdot \mathbf{x_1} \oplus \mathbf{v_1}$

    Given a guessed value for K_c, if $\tau_1(\alpha) \neq c$, then $K_{\tau_1(\alpha)}$ can be determined by $Z_{c+8}^{(N)}$.

The Low Data Complexity Attack



- Rule 4
  - $\mathbf{y} = \mathbf{W} \cdot \mathbf{x} \oplus \mathbf{v}$

    Given guessed values for K_c and $K_{\tau_1(\alpha)}$, then we can determine whether those guessed values are wrong.

The Low Data Complexity Attack

- Attack Procedure
  - Capture a frame of keystream bits (15-byte)

$$\left(Z_0^{(0)}, Z_1^{(0)}, \ldots, Z_7^{(0)}, Z_8^{(0)}, \ldots, Z_{14}^{(0)}\right)$$

  - Apply Guess-and-Determine Attack on 8~14th clock
    - Define a index set Γ , and initialized with $\Gamma = \varnothing$
      - Γ saves the indices for the session key that has been known
    - Analyzing the cipher at the (c+8)-th clock sequentially
      - Calculate t, c, p, S_0, judge whether $c \in \Gamma$
      - Adopt Rule 1~ Rule 4 to perform the attack
      - A little boring, see the full version paper

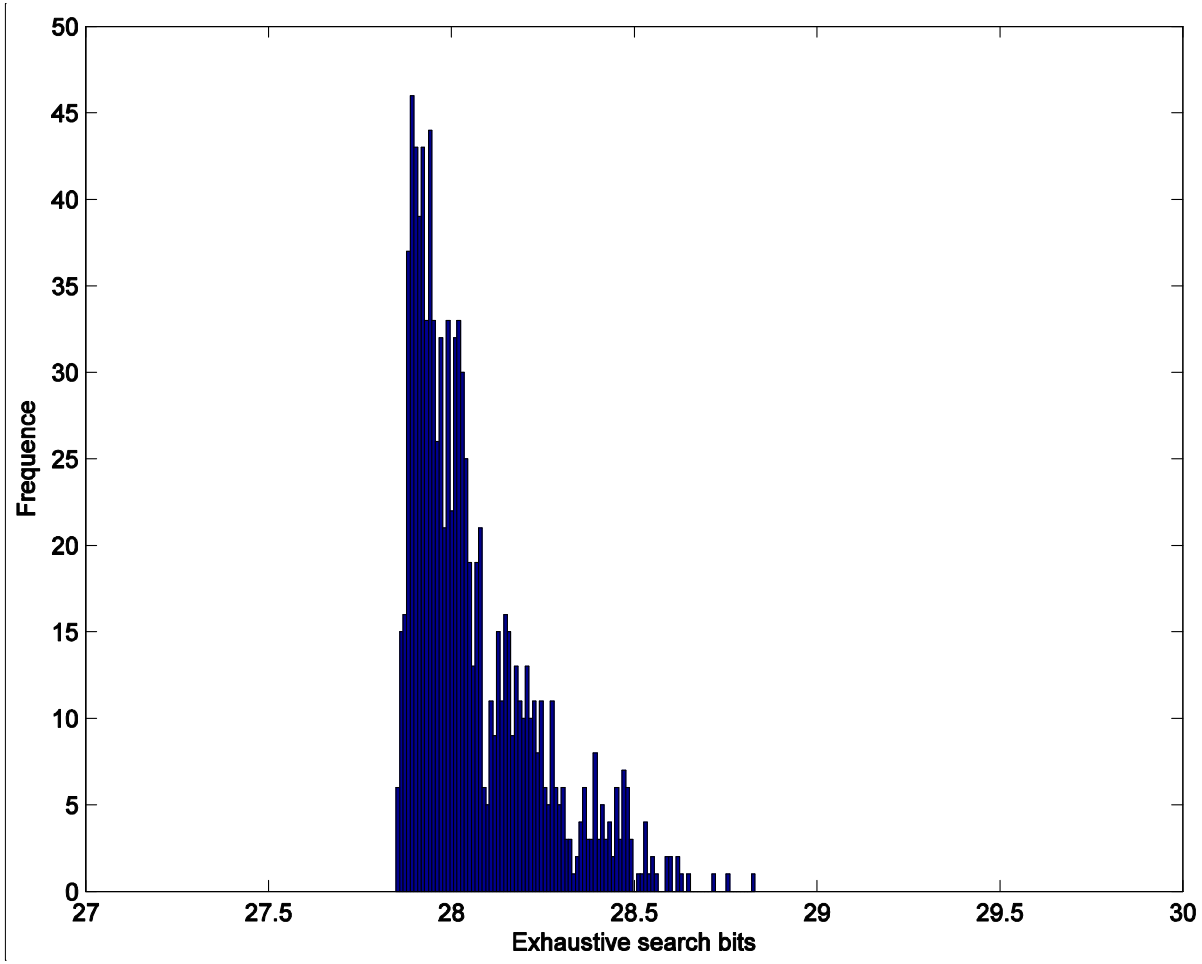
The Low Data Complexity Attack

- Complexity analysis
  - Data Comp.
    - A frame of Data (15-byte keystream)
    - The last 7 bytes used for guess-and-determine
    - The first 8 bytes used for verification
  - Time Comp.
    - When guessing 8/4-bit, we will determine 8/4-bit
    - The 64-bit session key can be obtained by guessing at most 32-bit
    - Rough estimation, seems hard to obtain exact analysis
    - Experimental results are a little better, about 2^{28} exhaustive search

Outline

- Backgrounds and the GMR-2 Cipher
- Revisit each Component of the GMR-2 Cipher
- The Low Data Complexity Attack
- Experimental Result
- Conclusion

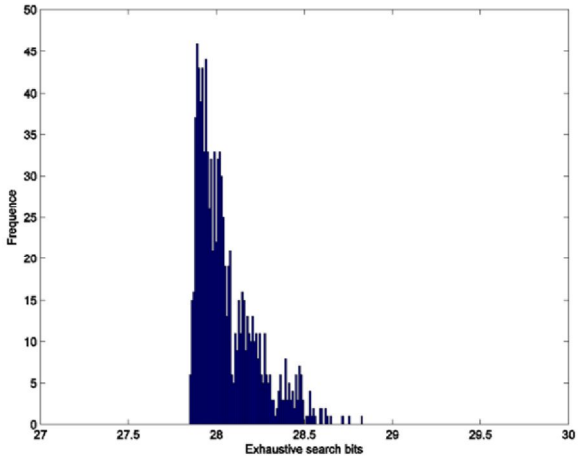
Experimental Result



1000 Experimental Results with Random IV and Session Key

Experimental Result

- Some explanations
  - Operated on a 3.2 GHz laptop
  - Non-optimized realization
  - 700 seconds on average
    - 580 seconds for deducing candidates
    - 120 seconds for exhaustive search



Outline

- Backgrounds and the GMR-2 Cipher
- Revisit each Component of the GMR-2 Cipher
- The Low Data Complexity Attack
- Experimental Result
- Conclusion

Conclusion

- We perform a security analysis of the GMR-2 cipher
  - Revisit the components of GMR-2 cipher
  - Propose “dynamic guess and determine strategy”
  - Present a low data complexity attack
- The design methodology of the GMR-2 cipher is far from what is “state of the art” in stream ciphers
- Be careful when using the Satellite phones

Thanks for your Attention!

Q & A