Agence nationale de la sécurité
des systèmes d'information

Linear Biases in AEGIS Keystream

Brice Minaud

ANSSI, France

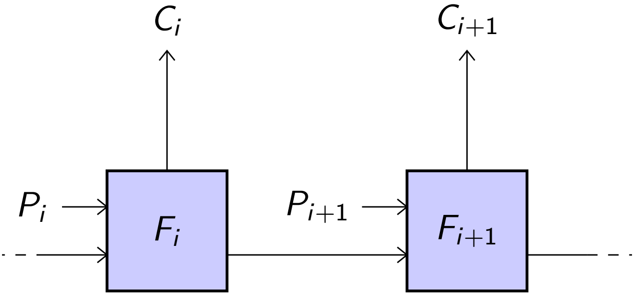
SAC – August 15, 2014

Plan

1. Blockwise Stream Ciphers
2. Presentation of AEGIS
3. Linear Biases in AEGIS

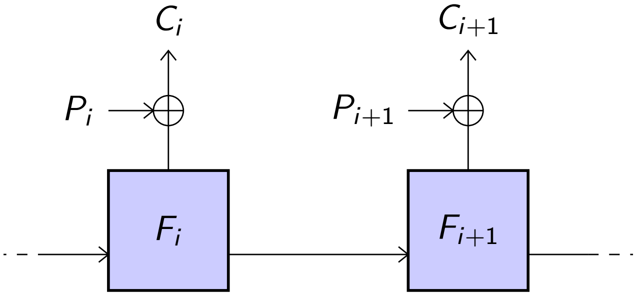
Blockwise Stream Ciphers

Authenticated Encryption Schemes



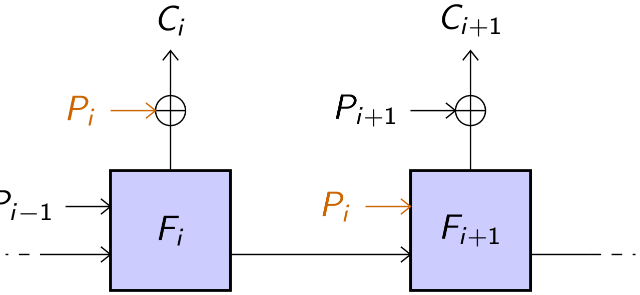
This requires F_i^{-1} for decryption.

Authenticated Encryption Schemes



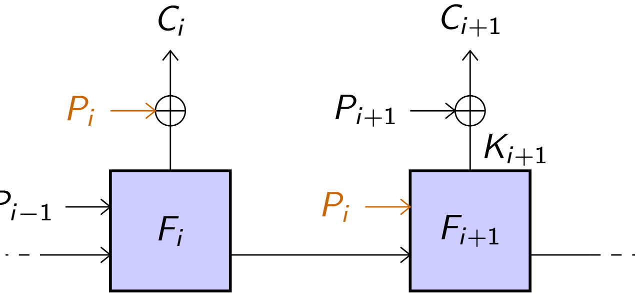
This is malleable.

Authenticated Encryption Schemes



P_i is inserted into the state after C_i is output.

Blockwise Stream Cipher



A single round behaves like a stream cipher.

K_{i+1} depends on $P_i, P_{i-1}, \ldots$ but not P_{i+1}.

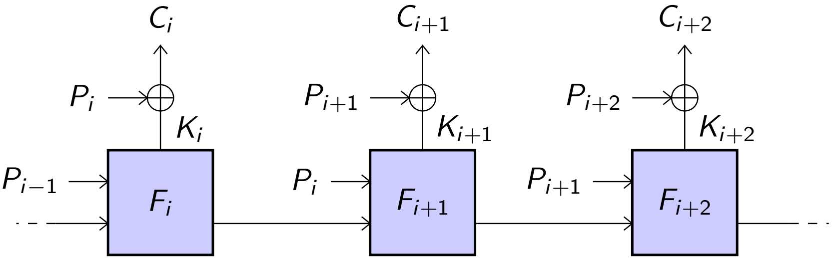
Blockwise Stream Ciphers in CAESAR

Duplex constructions behave in this way.

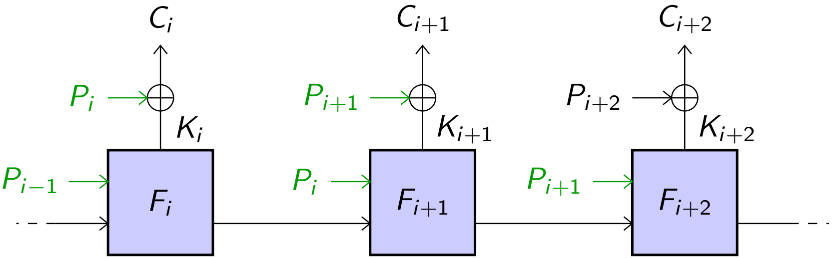
So do many CAESAR candidates.

AEGIS, Artemia, Ascon, CBEAM, ICEPOLE, Keyak, Ketje, MORUS, PAES, PANDA, π-Cipher, 2/3 PRIMATEs, STRIBOB, Tiaoxin...

Keystream Biases



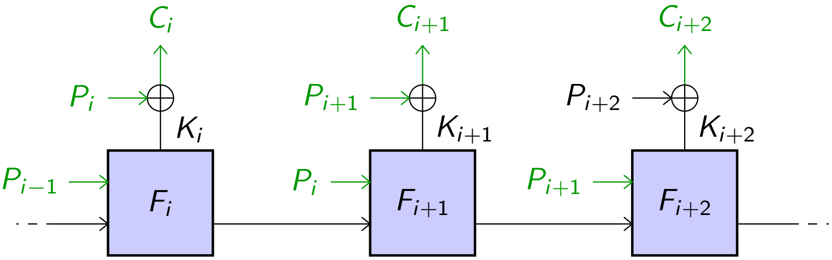
Keystream Biases



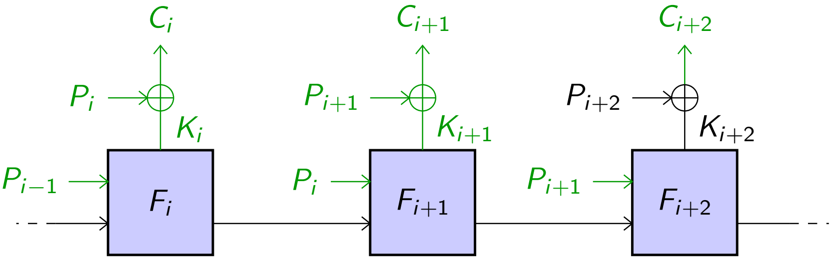
Assume we know, say, P_{i-1}, P_i, P_{i+1}, (e.g. headers).

We are interested in P_{i+2}.

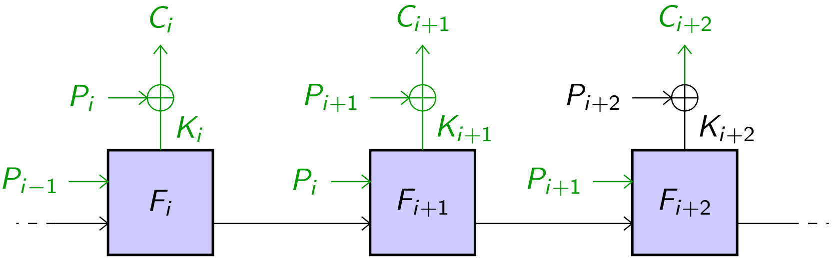
Keystream Biases



Keystream Biases



Keystream Biases

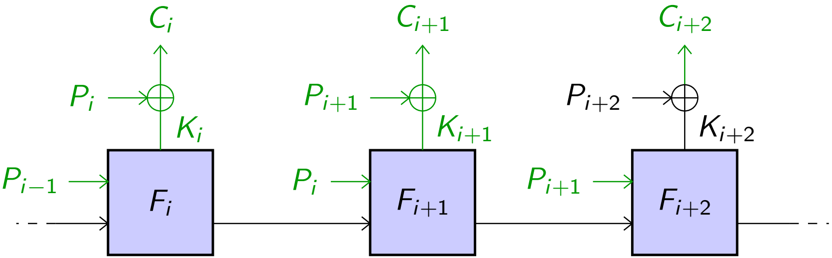


Assume knowing P_{i-1}, P_i, P_{i+1}, there exists a bias on :

$$\alpha_i \cdot K_i \oplus \alpha_{i+1} \cdot K_{i+1} \oplus \alpha_{i+2} \cdot K_{i+2}$$

Then $\alpha_i \cdot C_i \oplus \alpha_{i+1} \cdot C_{i+1} \oplus \alpha_{i+2} \cdot C_{i+2}$ gives us information on $\alpha_{i+2} \cdot P_{i+2}$.

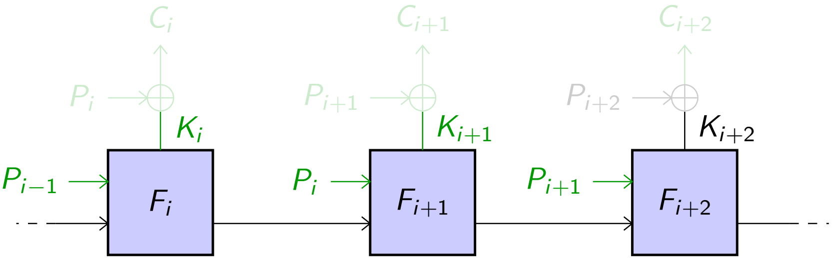
Keystream Biases



Thus, if $P_{i-1}, \ldots, P_{i+2}$ is encrypted enough times for the bias on $\alpha_i \cdot K_i \oplus \alpha_{i+1} \cdot K_{i+1} \oplus \alpha_{i+2} \cdot K_{i+2}$ to be significant, we recover information on P_{i+2}.

- This type of attack is independent of the key or nonce.
- It is not considered in most security analyses.

Keystream Biases



In summary, knowing P_{i-1}, P_i, P_{i+1}, we want to find a bias on :

$$\alpha_i \cdot K_i \oplus \alpha_{i+1} \cdot K_{i+1} \oplus \alpha_{i+2} \cdot K_{i+2}$$

We call this a “keystream” bias.

Our Results on AEGIS

Cipher	(Single) Keystream Bias	Data
AEGIS-128	2^{-77}	2^{154} (est. 2^{140})
AEGIS-256	2^{-89}	2^{178}

- The data requirements are far below a generic attack. However they are also far above any realistic threat. Above security parameters for AEGIS-128.
- The biases involve only 3 consecutive rounds, while the size of the inner state is 5 (resp. 6) times the size of the output per round.

Presentation of AEGIS

AEGIS

AEGIS : authenticated cipher introduced at SAC 2013 by Hongjun Wu and Bart Preneel. CAESAR candidate.

- AES-NI pipeline $\Rightarrow$ outstanding speed in software.
- Simple structure.
- Already inspired other designs : Tiaoxin, PAES.

AEGIS

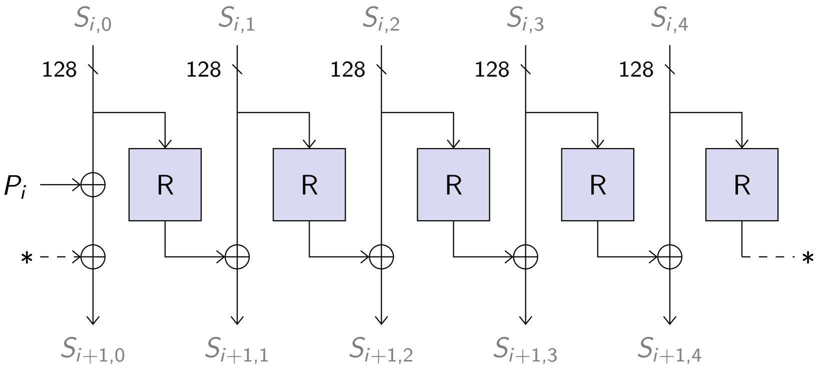
Three variants : AEGIS-128, AEGIS-128L, AEGIS-256.

- AEGIS-128 : 128-bit blocks, 128-bit nonce, 128-bit tag, 128-bit key.
- AEGIS-256 : 128-bit blocks, 128-bit nonce, 128-bit tag, 256-bit key.

Process of AEGIS

1. Initialization.
2. Processing of associated data.
3. Encryption.
4. Finalization and tag generation.

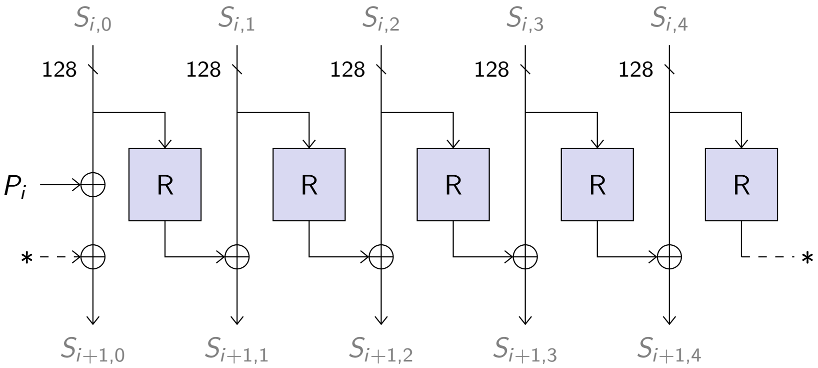
Round function of AEGIS-128



Inner state : 5 $\times$ 128 bits in registers $S_{i,0}, \ldots, S_{i,4}$.

R : one round of AES, no key addition.
P_i : plaintext block number i.

Round function of AEGIS-128

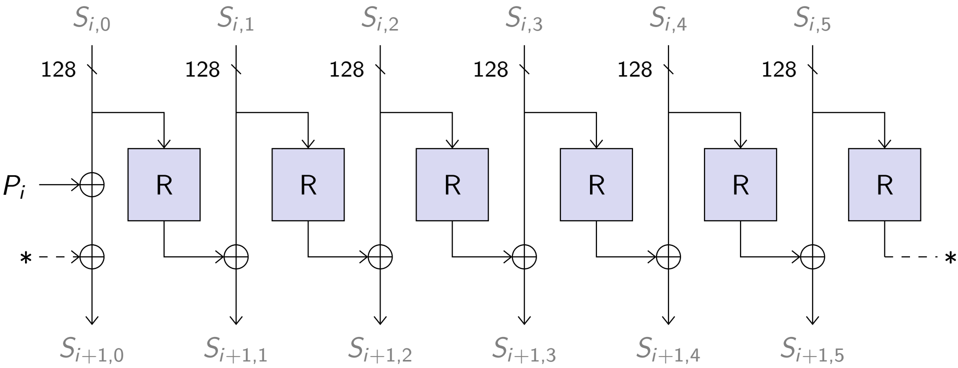


Output :

$$C_i = S_{i,1} \oplus (S_{i,2} \,\&\, S_{i,3}) \oplus S_{i,4} \oplus P_i$$

where & denotes bitwise `AND`.

Round function of AEGIS-256



Output :

$$C_i = S_{i,1} \oplus (S_{i,2} \,\&\, S_{i,3}) \oplus S_{i,4} \oplus S_{i,5} \oplus P_i$$

Linear Biases in AEGIS

Output at round i

$$K_i = S_{i,1} \;\oplus\; (S_{i,2}\,\&\,S_{i,3}) \;\oplus\; S_{i,4}$$

$$\alpha\cdot K_i = \alpha\cdot S_{i,1} \;\oplus\; \alpha\cdot(S_{i,2}\,\&\,S_{i,3}) \;\oplus\; \alpha\cdot S_{i,4}$$

Output at round i

$$K_i = S_{i,1} \oplus (S_{i,2} \,\&\, S_{i,3}) \oplus S_{i,4}$$

$$\alpha \cdot K_i = \alpha \cdot S_{i,1} \oplus \alpha \cdot (S_{i,2} \,\&\, S_{i,3}) \oplus \alpha \cdot S_{i,4}$$

Lemma

If X, Y are n-bit uniformly random variables, the events :

$$\alpha \cdot (X \& Y) = 0$$
$$\alpha \cdot (X \& Y) = \alpha \cdot X$$
$$\alpha \cdot (X \& Y) = \alpha \cdot Y$$
$$\alpha \cdot (X \& Y) = \alpha \cdot (X \oplus Y) \oplus 1$$

all have probability $1/2 + 2^{-\mathrm{hw}(\alpha)-1}$.

Linear approximation of &

Hence, with the same probability :

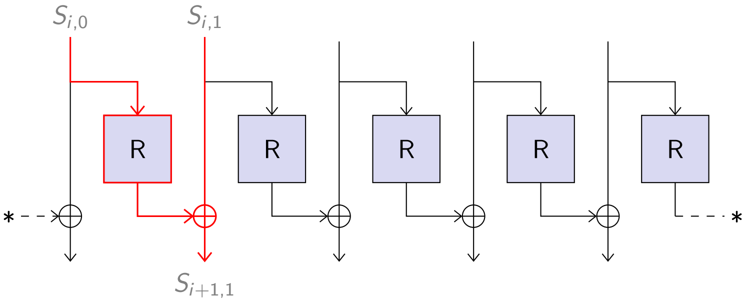
$$
\begin{aligned}
\alpha\cdot K_i &= \alpha\cdot(S_{i,1} \oplus S_{i,4}) \\
\alpha\cdot K_i &= \alpha\cdot(S_{i,1} \oplus S_{i,2} \oplus S_{i,4}) \\
\alpha\cdot K_i &= \alpha\cdot(S_{i,1} \oplus S_{i,3} \oplus S_{i,4}) \\
\alpha\cdot K_i &= \alpha\cdot(S_{i,1} \oplus S_{i,2} \oplus S_{i,3} \oplus S_{i,4}) \oplus 1
\end{aligned}
$$

We write :

$$\boxed{K_i \approx S_{i,1} \oplus [S_{i,2}] \oplus [S_{i,3}] \oplus S_{i,4}}$$

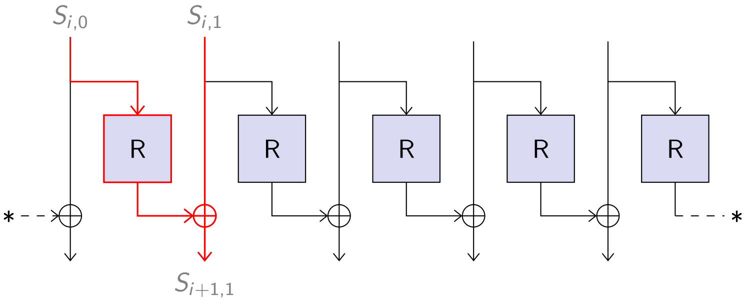
This is our output at round i.

Output at round $i + 1$



$$S_{i+1,1} \oplus S_{i,1} = \mathrm{R}(S_{i,0})$$

Output at round $i+1$

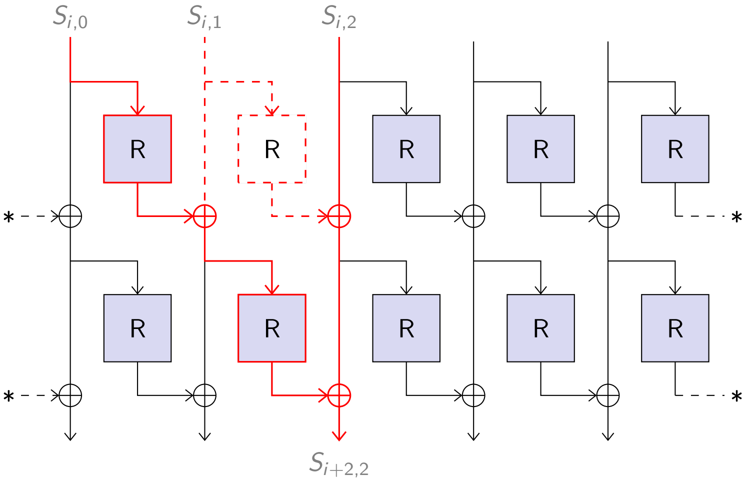


$$S_{i+1,1} \oplus S_{i,1} = \mathrm{R}(S_{i,0})$$

$$K_i \approx S_{i,1} \;\oplus\; [S_{i,2}] \;\oplus\; [S_{i,3}] \;\oplus\; S_{i,4}$$

$$\boxed{K_{i+1} \oplus K_i \;\approx\; \mathrm{R}(S_{i,0}) \;\oplus\; [\mathrm{R}(S_{i,1})] \;\oplus\; [\mathrm{R}(S_{i,2})] \;\oplus\; \mathrm{R}(S_{i,3})}$$

Output at round $i + 2$



$$S_{i+2,2} \oplus S_{i,2} \;=\; \mathrm{R}(S_{i+1,1}) \;\oplus\; \mathrm{R}(S_{i+1,1} \oplus \mathrm{R}(S_{i,0}))$$

Output at round $i+2$

If we approximate (with a probability cost) :

$$\beta\cdot \mathrm{R}(X) = \alpha\cdot X$$

Then :

$$\begin{aligned} & \beta\cdot(\mathrm{R}(S_{i+1,1}) \;\oplus\; \mathrm{R}(S_{i+1,1} \oplus \mathrm{R}(S_{i,0}))) \\ = \; & \alpha\cdot S_{i+1,1} \oplus \alpha\cdot S_{i+1,1} \oplus \alpha\cdot \mathrm{R}(S_{i,0}) \\ = \; & \alpha\cdot \mathrm{R}(S_{i,0}) \end{aligned}$$

Hence we approximate :

$$\begin{aligned} S_{i+2,2} \oplus S_{i,2} \; &= \; \mathrm{R}(S_{i+1,1}) \;\oplus\; \mathrm{R}(S_{i+1,1} \oplus \mathrm{R}(S_{i,0})) \\ &\approx \; \mathrm{D}(\mathrm{R}(S_{i,0})) \end{aligned}$$

where $\mathrm{D}(X) = \mathrm{R}(U) \oplus \mathrm{R}(U \oplus X)$, U uniformly random.

$$\boxed{K_{i+2} \oplus K_i \;\approx\; \mathrm{D}(\mathrm{R}(S_{i,4})) \;\oplus\; [\mathrm{D}(\mathrm{R}(S_{i,0}))] \;\oplus\; [\mathrm{D}(\mathrm{R}(S_{i,1}))] \;\oplus\; \mathrm{D}(\mathrm{R}(S_{i,2}))}$$

Final bias

$$
\begin{aligned}
K_i &\approx & & & S_1 &\oplus & [S_2] &\oplus & [S_3] &\oplus & S_4 \\
K_{i+1} \oplus K_i &\approx & \mathrm{R}(S_0) &\oplus & [\mathrm{R}(S_1)] &\oplus & [\mathrm{R}(S_2)] &\oplus & \mathrm{R}(S_3) & & \\
K_{i+2} \oplus K_i &\approx & [\mathrm{D}(\mathrm{R}(S_0))] &\oplus & [\mathrm{D}(\mathrm{R}(S_1))] &\oplus & \mathrm{D}(\mathrm{R}(S_2)) &\oplus & & & \mathrm{D}(\mathrm{R}(S_4))
\end{aligned}
$$

Final bias

$$
\begin{array}{rccccc}
K_i \approx & & S_1 \oplus & [S_2] \oplus & [S_3] \oplus & S_4 \\
K_{i+1} \oplus K_i \approx & \mathrm{R}(S_0) \oplus & [\mathrm{R}(S_1)] \oplus & [\mathrm{R}(S_2)] \oplus & \mathrm{R}(S_3) & \\
K_{i+2} \oplus K_i \approx & [\mathrm{D}(\mathrm{R}(S_0))] \oplus & [\mathrm{D}(\mathrm{R}(S_1))] \oplus & \mathrm{D}(\mathrm{R}(S_2)) \oplus & & \mathrm{D}(\mathrm{R}(S_4))
\end{array}
$$

Choose masks α, β, γ such that with good probability :

$$\alpha \cdot X = \beta \cdot \mathrm{R}(X) \qquad \text{and} \qquad \beta \cdot Y = \gamma \cdot \mathrm{D}(Y)$$

We consider :

$$\alpha \cdot K_i \ \oplus\ \beta \cdot (K_{i+1} \oplus K_i) \ \oplus\ \gamma \cdot (K_{i+2} \oplus K_i)$$

Any two terms in the same column will cancel out.

Final bias

$$
\begin{aligned}
K_i &\approx S_1 \oplus [S_2] \oplus [S_3] \oplus S_4 \\
\cancel{K_{i+1} \oplus K_i} &\cancel{\approx \mathrm{R}(S_0) \oplus [\mathrm{R}(S_1)] \oplus [\mathrm{R}(S_2)] \oplus \mathrm{R}(S_3)} \\
K_{i+2} \oplus K_i &\approx [\mathrm{D}(\mathrm{R}(S_0))] \oplus [\mathrm{D}(\mathrm{R}(S_1))] \oplus \mathrm{D}(\mathrm{R}(S_2)) \oplus \mathrm{D}(\mathrm{R}(S_4))
\end{aligned}
$$

Final bias

$$K_i \approx S_1 \oplus [S_2] \oplus [S_3] \oplus S_4$$

$$K_{i+2} \oplus K_i \approx [\mathrm{D}(\mathrm{R}(S_0))] \oplus [\mathrm{D}(\mathrm{R}(S_1))] \oplus \mathrm{D}(\mathrm{R}(S_2)) \oplus \mathrm{D}(\mathrm{R}(S_4))$$

Final bias

$$K_i \approx S_1 \oplus S_2 \oplus S_4$$

$$K_{i+2} \oplus K_i \approx \mathrm{D}(\mathrm{R}(S_1)) \oplus \mathrm{D}(\mathrm{R}(S_2)) \oplus \mathrm{D}(\mathrm{R}(S_4))$$

Final bias

$$K_i \approx \quad S_1 \oplus \quad S_2 \oplus \quad S_4$$

$$K_{i+2} \oplus K_i \approx \quad \mathrm{D}(\mathrm{R}(S_1)) \oplus \mathrm{D}(\mathrm{R}(S_2)) \oplus \quad \mathrm{D}(\mathrm{R}(S_4))$$

Thus $\alpha \cdot K_i \oplus \gamma \cdot (K_i \oplus K_{i+2})$ is biased.

Final bias

$$K_i \approx \quad S_1 \oplus \quad S_2 \oplus \quad S_4$$

$$K_{i+2} \oplus K_i \approx \quad \mathrm{D}(\mathrm{R}(S_1)) \oplus \mathrm{D}(\mathrm{R}(S_2)) \oplus \quad \mathrm{D}(\mathrm{R}(S_4))$$

Thus $\alpha \cdot K_i \oplus \gamma \cdot (K_i \oplus K_{i+2})$ is biased.

Probability cost : essentially 3 $\times$ the cost of :

$$\alpha \cdot X = \beta \cdot \mathrm{R}(X) \qquad \text{and} \qquad \beta \cdot Y = \gamma \cdot \mathrm{D}(Y)$$

Plus the cost of linearizing & in the K_i's.

Total : $3 \cdot (12 + 6) + 5 + 2 \cdot 9 = 77 \Rightarrow$ bias 2^{-77}.
AEGIS-256 : bias 2^{-89}.

Conclusion

- Attack model rarely taken into account in security analyses.
- Theoretical cryptanalysis of AEGIS-256 (high data requirements).
- Further work to be carried out on other authenticated ciphers with similar stream cipher-like behavior.

Questions

Thank you for your attention.