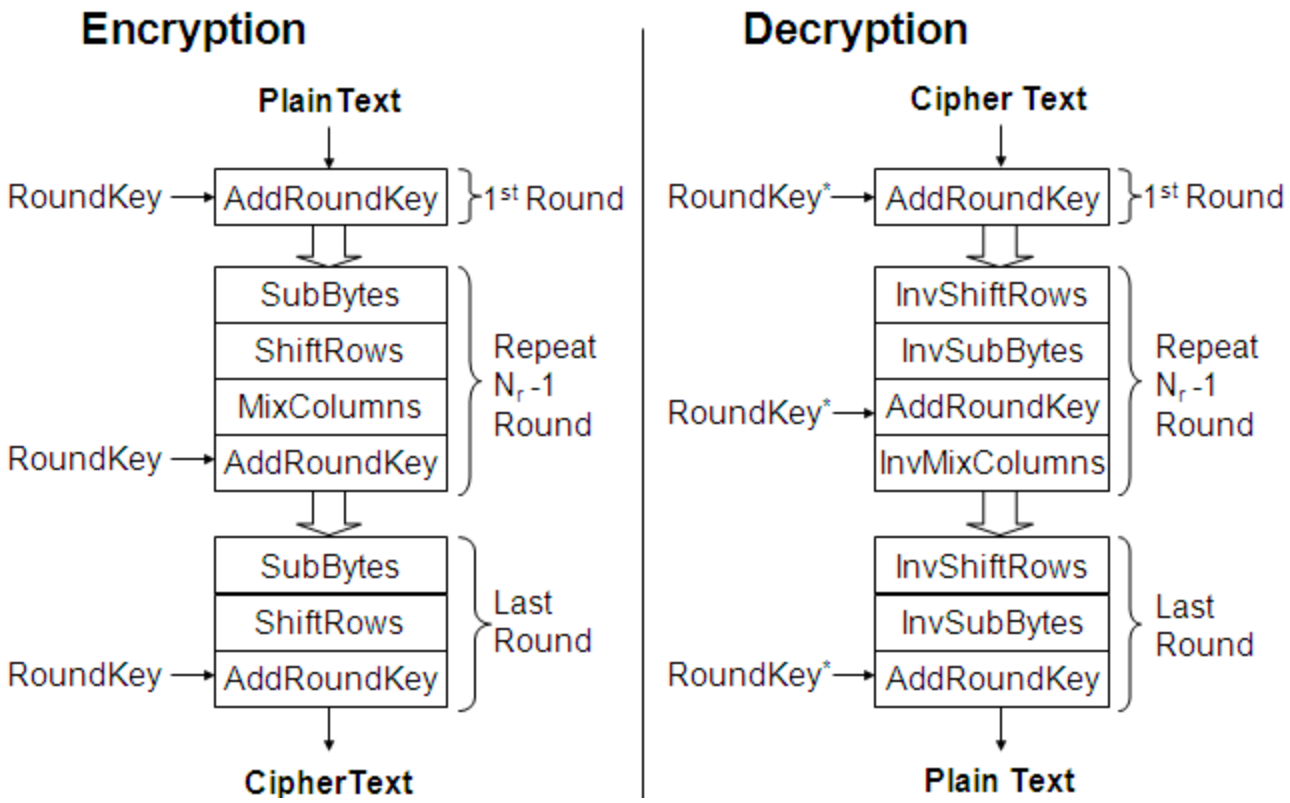
4ROUNDのAESに対するintegral攻撃の実装

セキュリティキャンプ全国大会2022
L1受講者 hirafish

AESの全体アルゴリズム



https://www.seleqt.net/programming/what-is-aes-encryption-working-performance-security/

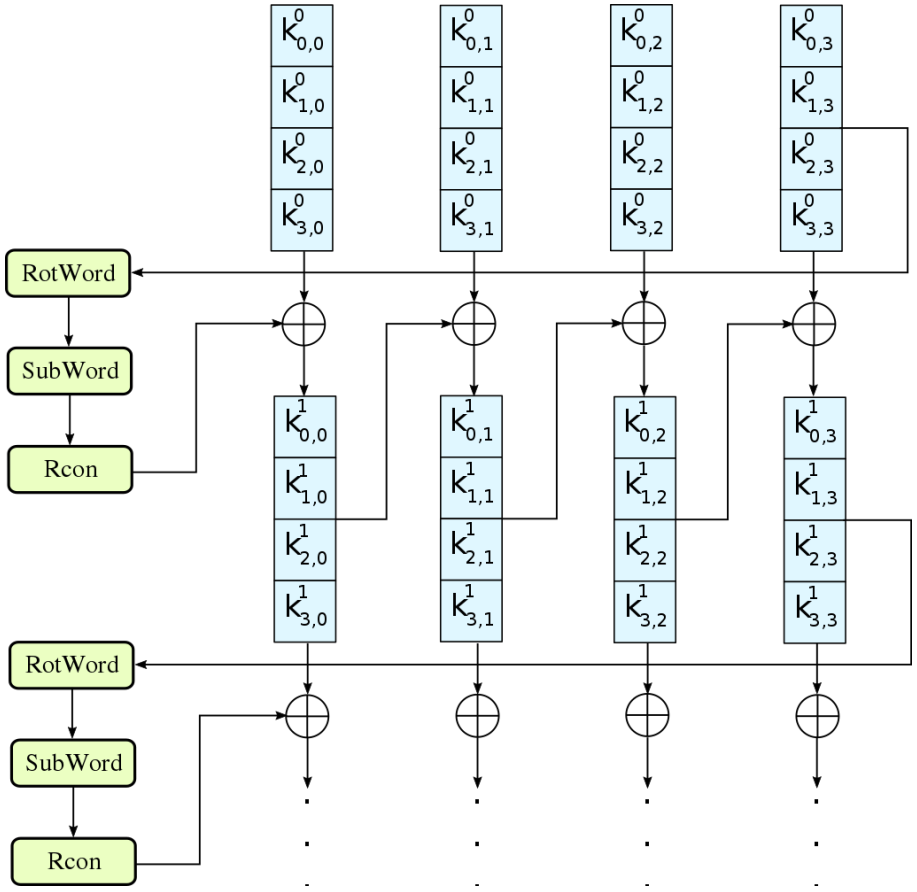
KeyScheduleにより各ラウンドで用いる鍵を生成後、各アルゴリズムを繰り返す

	Key Length (Nk words)	Block Size (Nb words)	Number of Rounds (Nr)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

3種類のAES

AESのKey Schedule部

AES128の場合のkey Schedule



ざっくりアルゴリズム

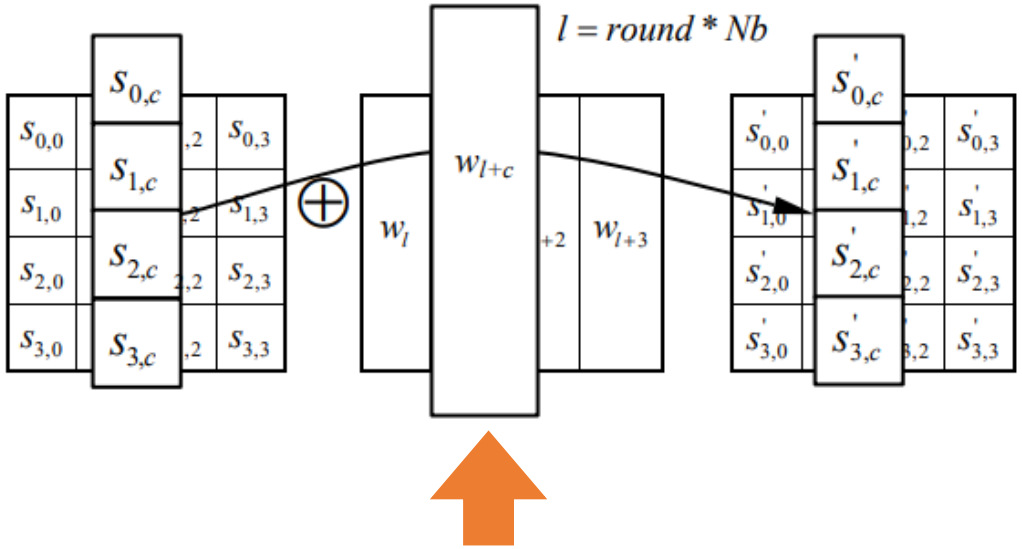
① 鍵を4分割する

② そのうち一つに対してRotWord, SubWord, Rcon などの処理(黄緑のbox)を行う

③ ②で得られたものと4分割した最初の鍵との差分を取得し、それと他の分割した鍵との差分を取得することを繰り返す

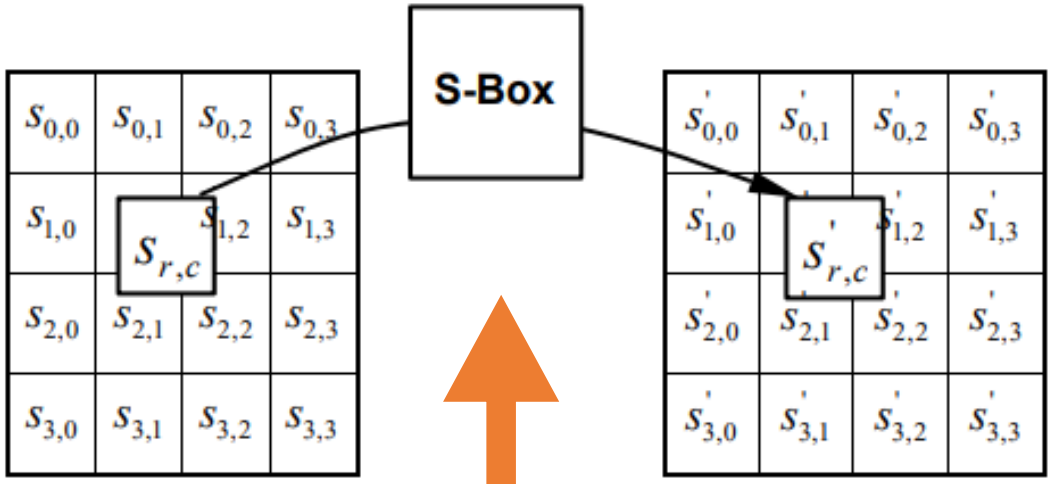
AESの暗号化部

AddRoundKey



Key Scheduleを用いて生成した
ラウンドごとの鍵

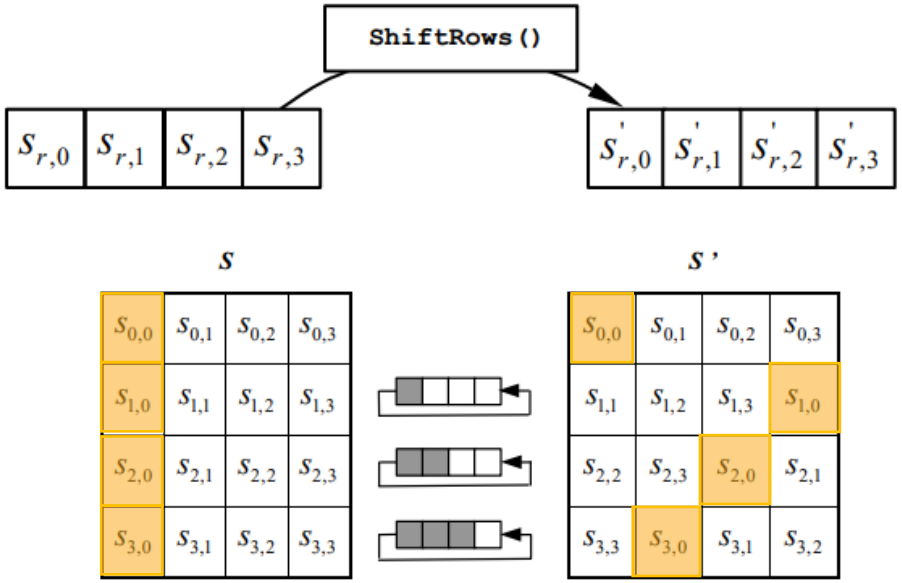
SubBytes



0～256までの全単射

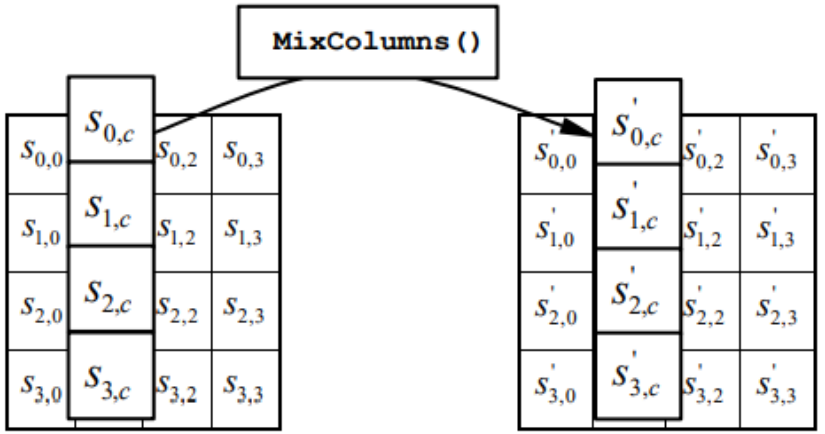
AESの暗号化部

ShiftRows



1行目から4行目を
0, 1, 2, 3バイト分左巡回シフト

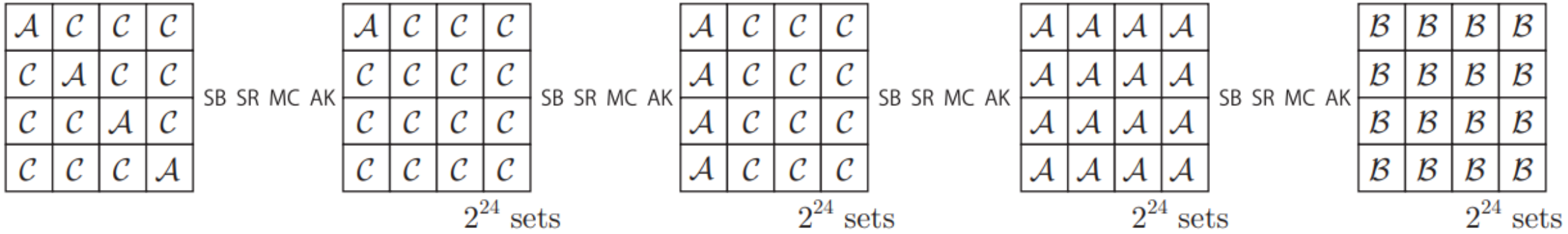
MixColumns



$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix}$$

Integral攻撃とは？

AESの場合



積分特性(Integral property)

1 ALL(A) : 集合の取りうるすべての値が複数回出現する

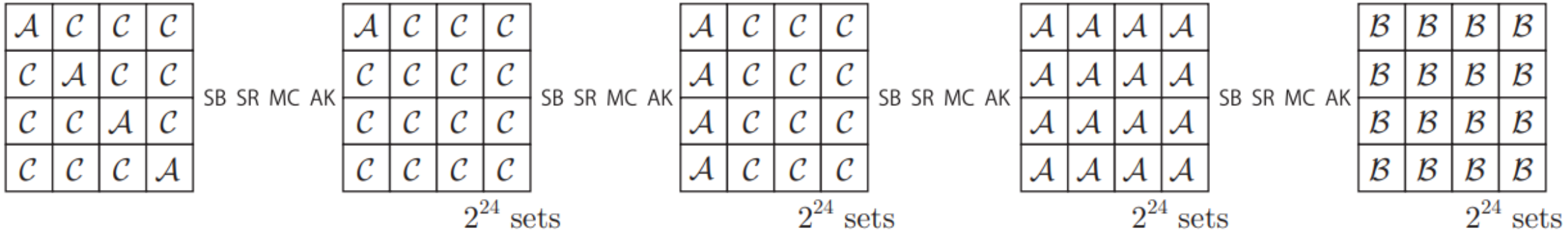
2 BALANCE(B) : 集合のすべての値の排他的論理和が 0 になる

3 CONSTANT(C) : 集合のすべての値が一定である

4 UNKNOWN(U) : すべての値がランダムに出現する(ランダムであることの区別がつかない)

Integral攻撃とは？

AESの場合



積分特性(Integral property)

1 ALL(A) : 集合の取りうるすべての値が複数回出現する

2 BALANCE(B) : 集合のすべての値の排他的論理和が 0 になる

3 CONSTANT(C) : 集合のすべての値が一定である

4 UNKNOWN(U) : すべての値がランダムに出現する(ランダムであることの区別がつかない)

１バイトずつ鍵候補(0～256)を探索して
XORが0になれば正しい鍵の候補になる

AES(4ROUND)に対する実装

GitHubにおいたコード
(https://github.com/hirafish/seccamp2022-L1/blob/main/integral.py)参照

```
1バイト目の鍵候補は: [161, 227]
2バイト目の鍵候補は: [18, 110]
3バイト目の鍵候補は: [2]
4バイト目の鍵候補は: [201, 217]
5バイト目の鍵候補は: [180]
6バイト目の鍵候補は: [104]
7バイト目の鍵候補は: [190]
8バイト目の鍵候補は: [160, 161, 215]
9バイト目の鍵候補は: [215]
10バイト目の鍵候補は: [81, 135, 163]
11バイト目の鍵候補は: [31, 87]
12バイト目の鍵候補は: [64, 150, 160]
13バイト目の鍵候補は: [20, 74, 163]
14バイト目の鍵候補は: [56, 82]
15バイト目の鍵候補は: [47, 73]
16バイト目の鍵候補は: [91, 104, 143]
```

4ROUND目で用いる鍵候補

①候補の直積を全探索
②KeyScheduleから最初の鍵まで逆算

！！解読成功！！

```
正解の鍵:
[84, 104, 97, 116, 115, 32, 109, 121,
32, 75, 117, 110, 103, 32, 70, 117]
得られた鍵:
[84, 104, 97, 116, 115, 32, 109, 121,
32, 75, 117, 110, 103, 32, 70, 117]
```

0ROUND目(最初に与える鍵)の鍵

今回のまとめと今後について

- 4ROUNDのAESに対して純粋なIntegral攻撃が成立する
- 現行では無条件の5ROUND以上であれば、
  純粋なIntegral攻撃に対する攻撃報告は
  見当たらなかった
- 純粋なIntegral攻撃の発展として
  Division Propertyの伝搬特性を用いたものがある
- 研究している差分解読法とIntegral攻撃を
  組み合わせた手法に取り組んでいきたい