國立屏東大學資訊工程學系碩士提審論文
An encryption algorithm By using replacement and displacement block

Advisor:Lung-Jen Wang,Ph. D

Speaker:Meng-Xian Du

Date:01/16/2024

Location:VAR Center 2f conference room

摘要

本研究預計將提出一種以AES、SHA的加密演算法，並試圖改善AES的雪崩效應。在原始版本的AES中，明文的長度越長並且更動越小，其雪崩效應越不明顯。

在雪崩效應不明顯為前提之下，可從已知密文中統計出特定的明文內容，甚至還有可能找出其統計上的規律

本研究將致力於提升演算法的雪崩效應，並且最大程度的壓低演算法的時間複雜度。

相關研究

在此領域中有需多相關的研究，其著手方向大致上可簡化成三個方向：

- 輕量化
- 安全性
- 速度

而本研究預計將以安全性為著手方向進行研究，在最小的時間複雜度增加為前提，最大程度提升演算發之雪崩效應。

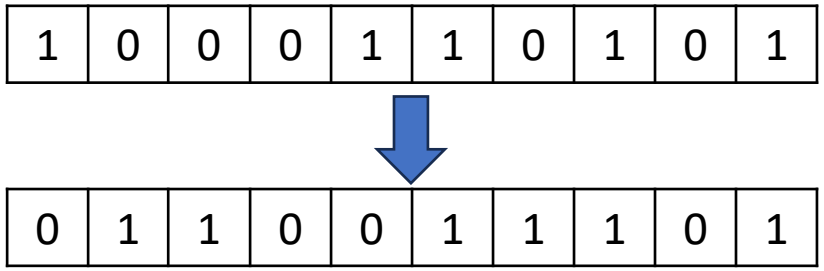
安全性

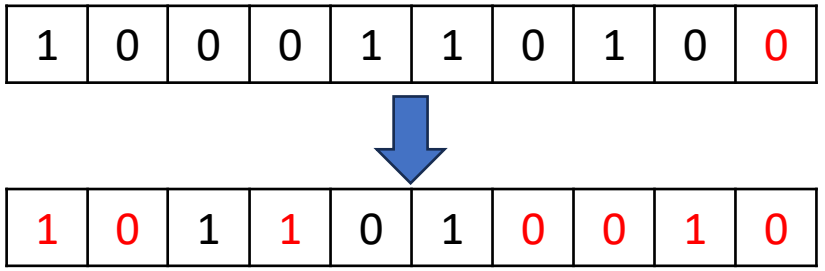
在其他的研究中可以看到，其評估演算法安全性的方式就是使用雪崩效應，而造成雪崩效應的原因有以下：

- 資料的位移
- 資料的旋轉
- 資料的置換

雪崩效應

雪崩效應根據維基百科的定義為，微小的輸入變化(例：反轉一個位元)會造成輸出不可區分性的改變。





位元獨立準則(Bit Independence Criterion)

BIC指出對於任意輸入位i與輸出位k、j，當輸入位被反轉時，輸出位j和k應當互不影響地獨立變化。

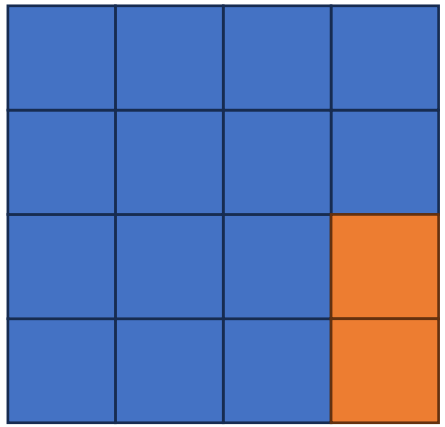
也就是說j跟k之間不會因為i的變化而同時變化，換言之就是j與k之間的變化，會根據除了i之外的輸入位的變化而有所改變。

AdvancedEncryptionStandaard介紹

AES是一種對稱式加密演算法，其操作原理如下所示

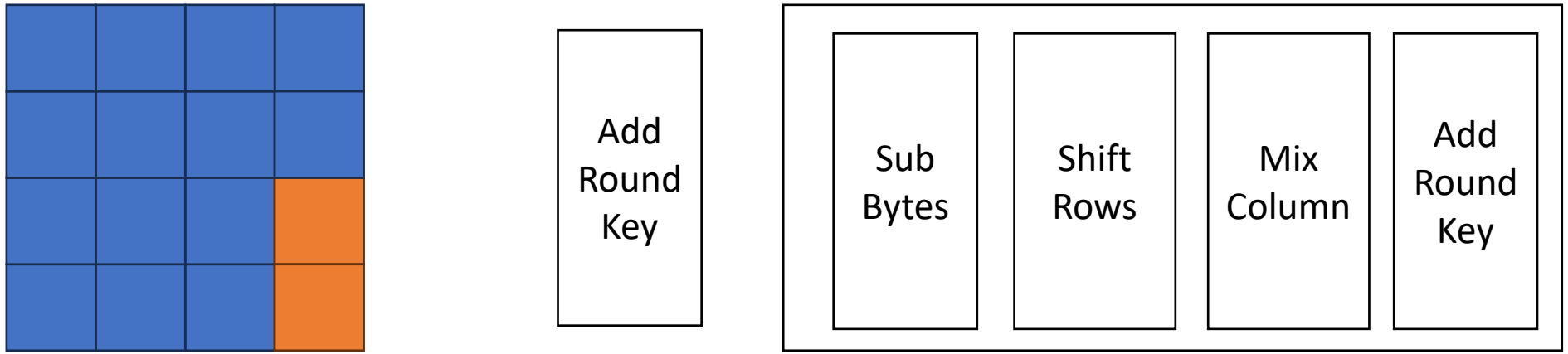
AdvancedEncryptionStandaard介紹

AES是一種對稱式加密演算法，其操作原理如下所示



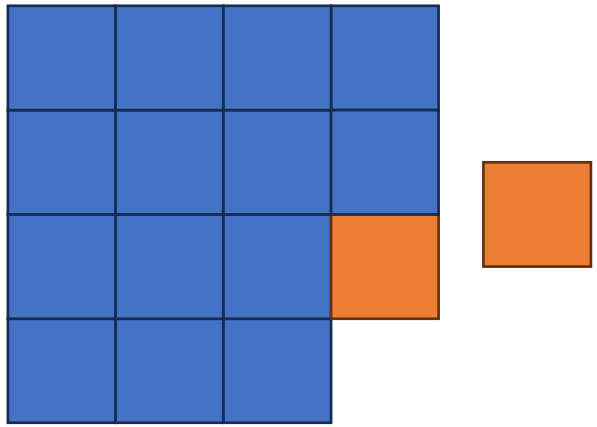
AdvancedEncryptionStandaard介紹

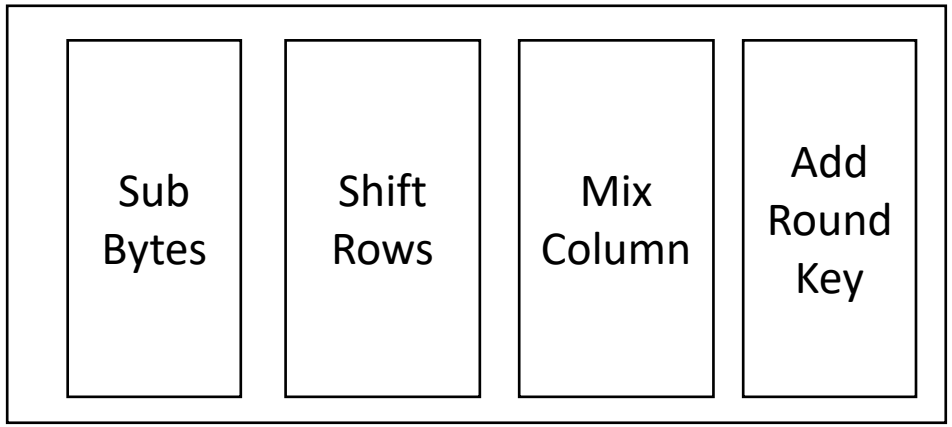
AES是一種對稱式加密演算法，其操作原理如下所示



AdvancedEncryptionStandaard介紹

AES是一種對稱式加密演算法，其操作原理如下所示





加密回合數

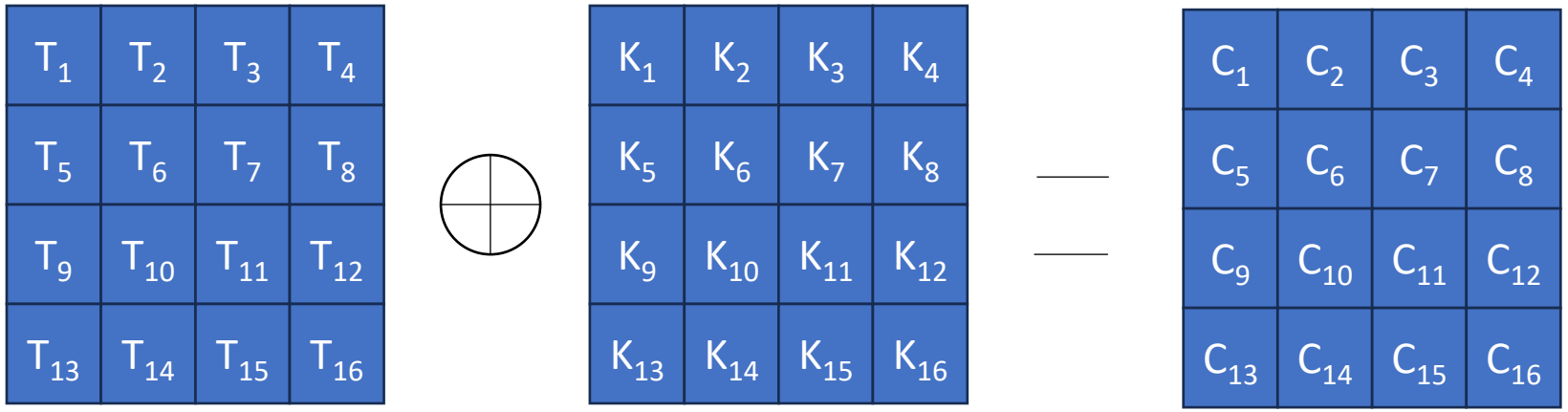
- 表1為”The Design of Rijndael”表3.2的內容，對AES而言N_b被固定為4這個值，對128位元的密鑰 ($N_k = 4$) 而言回合數是10 ($N_r = 10$)，而192位元的密鑰 ($N_k = 6$) 的回合數則是12，由此可知256 ($N_k = 8$) 位元長的密鑰其回合數 (Nr = 14) 為14。

表1. N_b($N_b = \frac{Block\ length}{32}$)與N_k($N_k = \frac{key\ length}{32}$)是N_r回合數(Number of Round)的函數。

N_k	N_b				
	4	5	6	7	8
4	10	11	12	13	14
5	11	11	12	13	14
6	12	12	12	13	14
7	13	13	13	13	14
8	14	14	14	14	14

AddRoundKey

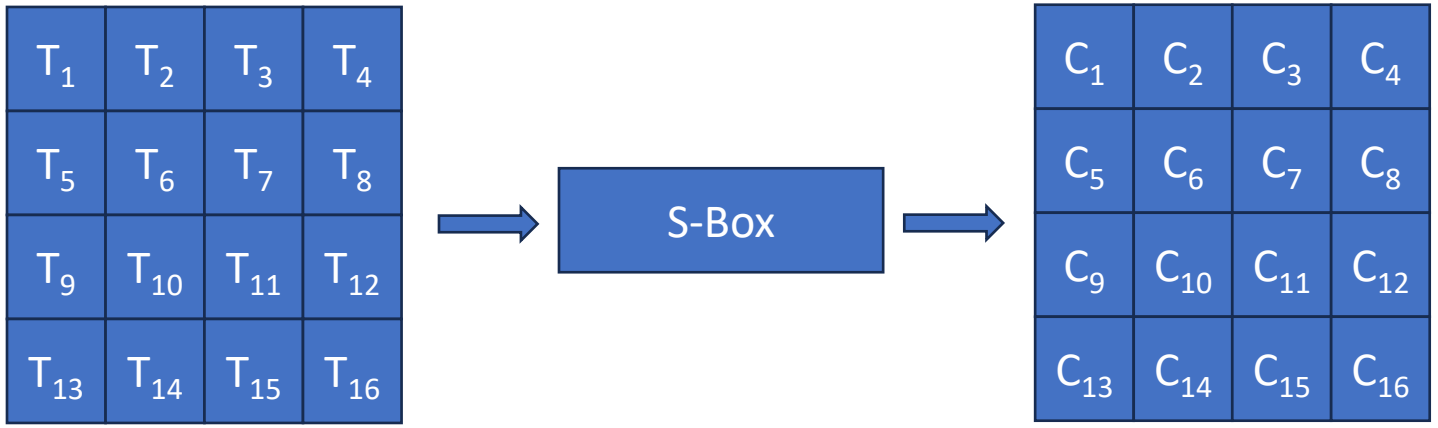
- 在這個步驟中需要讓明文陣列跟Round-Key做XOR的運算。而RoundKey的生成則是將Key的4x4陣列旋轉產生，也就是將每一行根據每一輪往左位移，而最左邊的字元則移到最右方。
- 此操作給予了密文非線性的混淆，並且藉由這樣不斷位移的方式產生新的Round-Key不僅兼顧了效率，也節省了記憶體空間。



SubBytes

SubBytes或稱Substitute Bytes在AES中扮演著混淆的角色。

其運作的方式是將資料的高位元中的4位當作行數，低位元的4位當成列數，取代成S-Box中相對應的字元。



S-Box

假設明文經過AddRoundKey後的密文如下表

93	21	45	e5
55	f2	35	ad
8a	c5	53	5e
76	84	5f	76

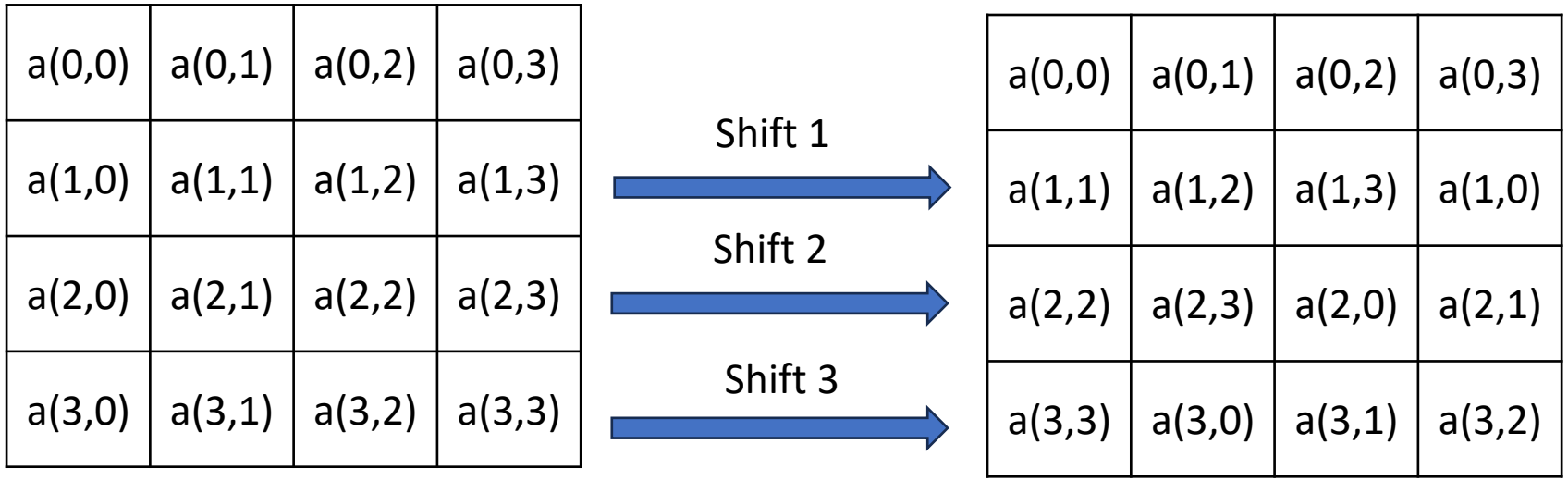
經過S-box的替換後內容將會如下表所示

dc	fd	6e	d9
fc	89	96	95
7e	a6	ed	58
38	5f	cf	38

	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

ShiftRows

在AES的第二個步驟ShiftRows中，會將4x4的陣列裡的每一欄按照行數向左位移行數減一位，並將溢位的字元移到該行的最末端。



MixColumns

這一步需要將明文所分切成的陣列，依列透過線性變換互相結合。在MixColumns的過程中會用到Bricklayer Function，如果Bricklayer Function 是使用非線性的方式轉換，在傳統上會稱為S-Box。如果是線性的轉換，AES的研發者稱之為D-Box（D為Diffusion之意）。

2	3	1	1
1	2	3	1
1	1	2	3
3	1	1	2

Padding

在加密的過程中如有字元數量不足的情況，通常會進行填充以確保加密的過程順利，以下是目前常見的填充方式：

	明文		填充
ANSI X.923	DD DD DD DD DD	DD DD DD DD DD	00 00 00 00 00 06
ISO 10126	DD DD DD DD DD	DD DD DD DD DD	4A 5E 66 72 45 06
PKCS7	DD DD DD DD DD	DD DD DD DD DD	06 06 06 06 06 06
ISO/IEC 7846-4	DD DD DD DD DD	DD DD DD DD DD	80 00 00 00 00 00
Zero Padding	DD DD DD DD DD	DD DD DD DD DD	00 00 00 00 00 00

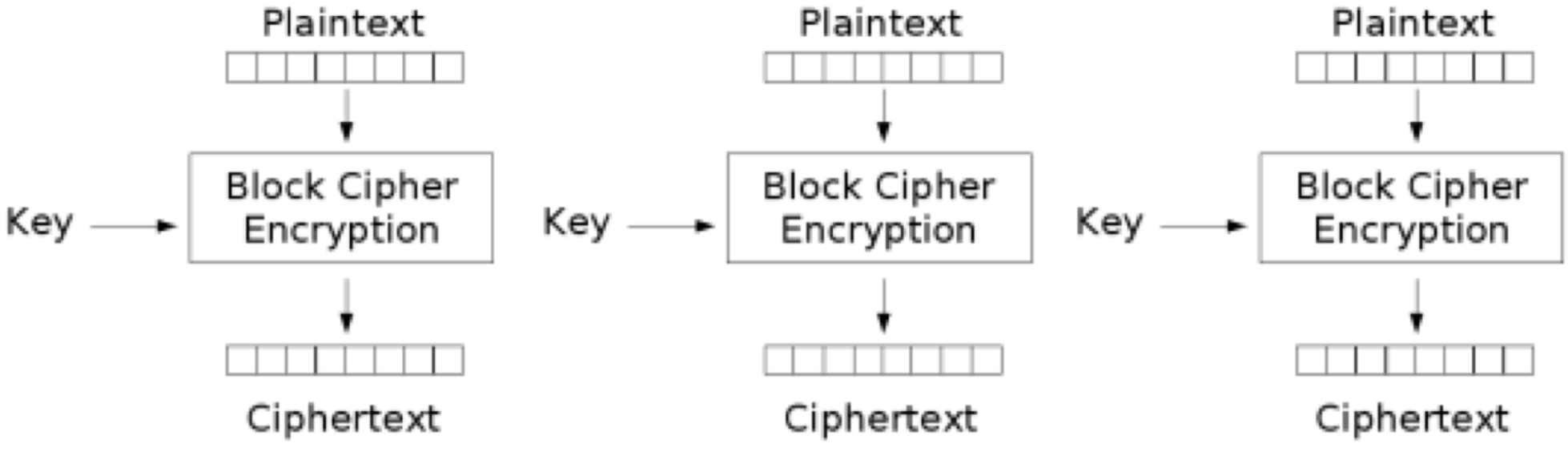
加密模式

在AES中有數種加密模式，大致可分為區塊加密模式、訊息保護模式，以及密碼流生成模式。以下為四種常見的加密模式

- ECB
- CBC
- CFB
- OFB

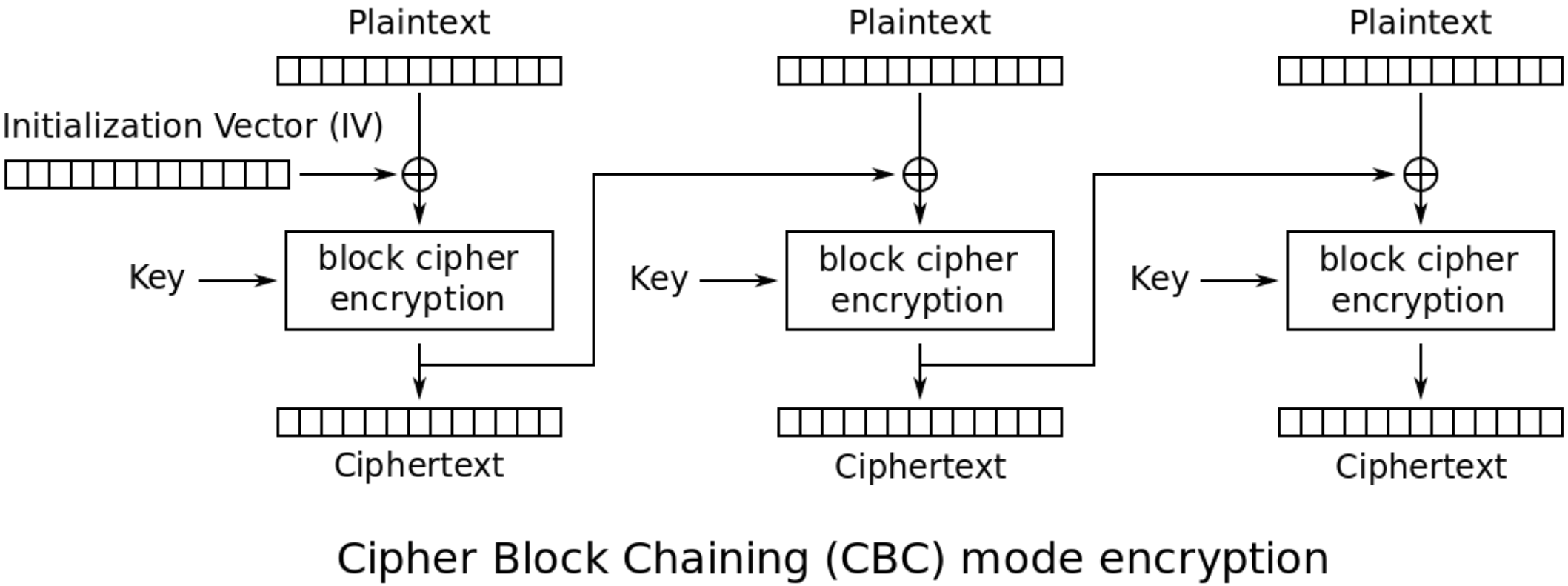
區塊加密模式
Block Cipher Mode

ECB



Electronic Codebook (ECB) mode encryption

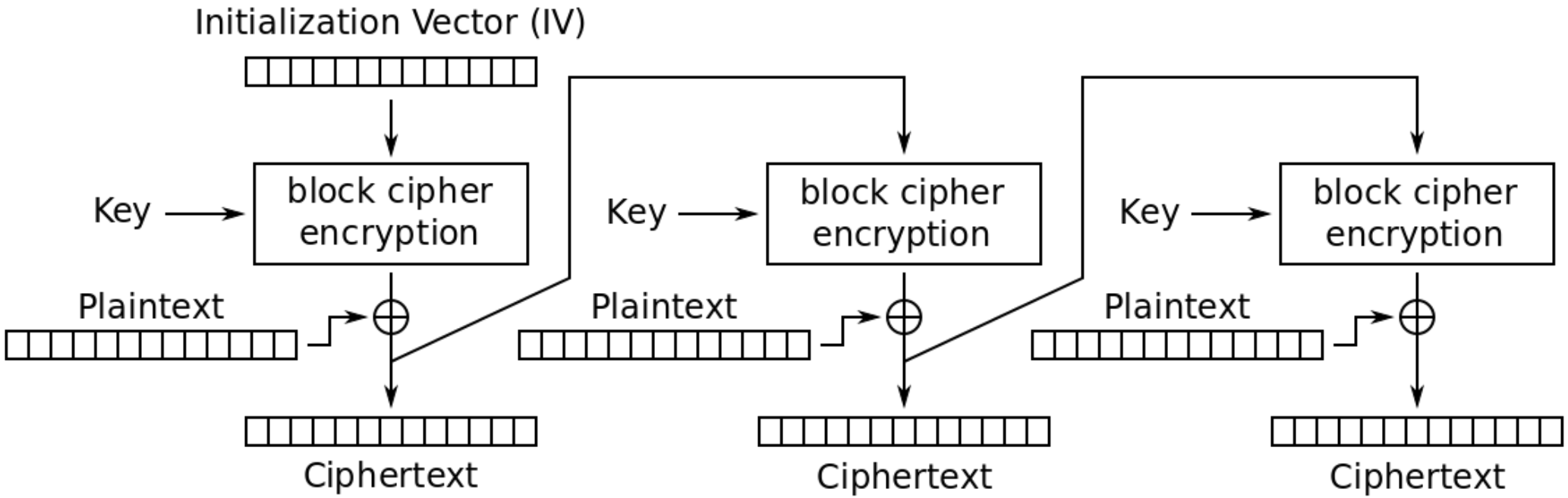
CBC



Cipher Block Chaining (CBC) mode encryption

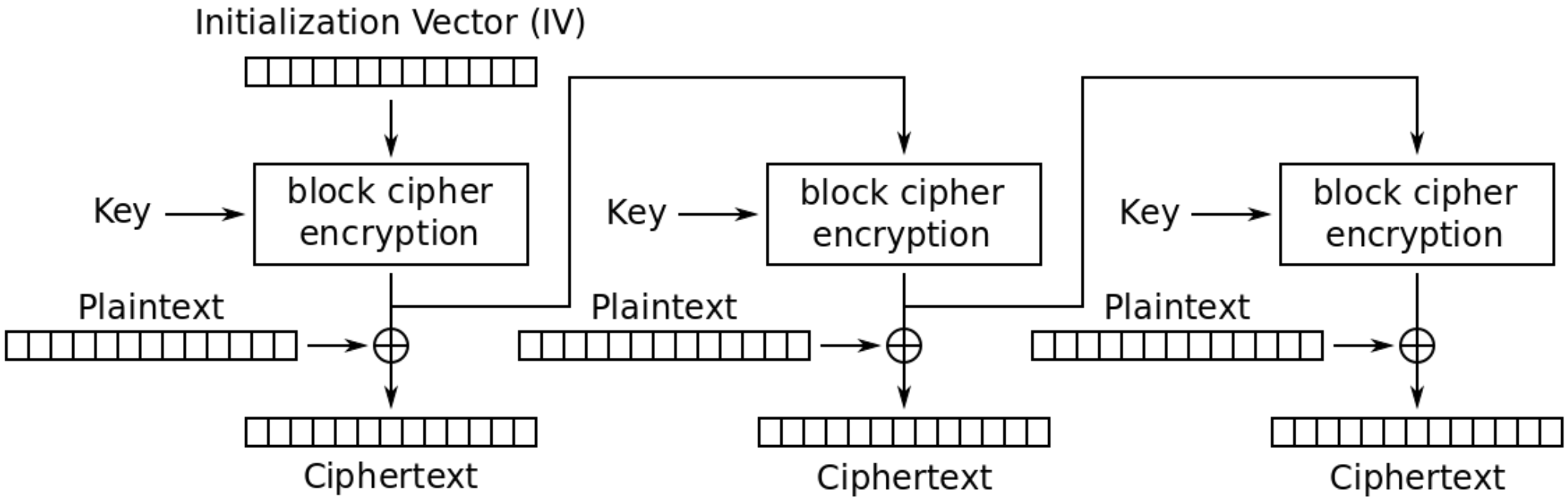
密碼流生成模式
(Key-Stream Generation Modes)

CFB



Cipher Feedback (CFB) mode encryption

OFB



Output Feedback (OFB) mode encryption

雜湊演算法

雜湊演算法是一種將不定長度的資料輸入進去後產出特定長度，並且輸出結果不可逆轉的演算法。目前常用的雜湊演算法為Keccak。被NIST選為NIST雜湊函數競賽的勝利者後，改名為SHA-3。

另外在使用雜湊函數時也會使用基於Merkle–Damgård construction的SHA-2。

本實驗將評估SHA-2與SHA-3所使用的時間成本、記憶體空間成本來決定使用何種雜湊函數。

實驗方法

本研究預計改良AES的ECB加密模式，並預計使用SHA-3對明文進行雜湊運算後輔助產生IV及Round-Key，藉由SHA-3的低碰撞率，及良好的雪崩效應與加密效率，來達到快速產生金鑰的目的。藉此來提升AES的雪崩效應。

預期結果

本研究預計將改良現有的AES演算法，並且結合SHA-3雜湊演算法以及Merkle tree，使修改過的演算法雪崩效應更加劇烈。以達到更高的安全性。並希望藉由Merkle Tree來達到資料準確性的驗證。