现代密码学

第二十讲 DES算法简介

信息与软件工程学院

第二十讲 DES算法简介

- 美国制定数据加密标准简况
- DES的框架和主要参数

美国制定数据加密标准简况

- 目的

通信与计算机相结合是人类步入信息社会的一个阶梯，它始于六十年代末，完成于90年代初。计算机通信网的形成与发展，要求信息作业标准化，安全保密亦不例外。只有标准化，才能真正实现网的安全，才能推广使用加密手段，以便于训练、生产和降低成本。

美国制定数据加密标准简况

- 美国NBS在1973年5月15公布了征求建议。1974年8月27日NBS再次出公告征求建议，对建议方案提出如下要求：

(1)算法必须提供高度的安全性

(2)算法必须有详细的说明,并易于理解

(3)算法的安全性取决于密钥,不依赖于算法

(4)算法适用于所有用户

(5)算法适用于不同应用场合

(6)算法必须高效、经济

(7)算法必须能被证实有效

(8)算法必须是可出口的

美国制定数据加密标准简况

- IBM公司在1971年完成的LUCIFER密码 (64 bit分组，代换-置换，128 bit密钥)的基础上，改进成为建议的DES体制
- 1975年3月17日NBS公布了这个算法，并说明要以它作为联邦信息处理标准，征求各方意见。
- 1977年1月15日建议被批准为联邦标准[FIPS PUB 46]，并设计推出DES芯片。
- 1981年美国ANSI 将其作为标准，称之为DEA[ANSI X3.92]
- 1983年国际标准化组织(ISO)采用它作为标准，称作DEA-1

美国制定数据加密标准简况

- NSA宣布每隔5年重新审议DES是否继续作为联邦标准，1988年（FIPS46-1）、1993年（FIPS46-2），1998年不再重新批准DES为联邦标准。
- 虽然DES已有替代的数据加密标准算法，但它仍是迄今为止得到最广泛应用的一种算法，也是一种最有代表性的分组加密体制。
- 1993年4月，Clinton政府公布了一项建议的加密技术标准，称作密钥托管加密技术标准EES(Escrowed Encryption Standard)。算法属美国政府SECRET密级。

美国制定数据加密标准简况

- DES发展史确定了发展公用标准算法模式，而EES的制定路线与DES的背道而驰。人们怀疑有陷门和政府部门肆意侵犯公民权利。此举遭到广为反对。
- 1995年5月AT&T Bell Lab的M. Blaze博士在PC机上用45分钟时间使SKIPJACK的 LEAF协议失败，伪造ID码获得成功。1995年7月美国政府宣布放弃用EES来加密数据，只将它用于语音通信。
- 1997年1月美国NIST着手进行AES（Advanced Encryption Standard）的研究，成立了标准工作室。2001年Rijndael被批准为AES标准。

美国制定数据加密标准简况

- **DES（Data Encryption Standard）**算法于1977年得到美国政府的正式许可，是一种用56位密钥来加密64位数据的方法。这是IBM的研究成果。
- DES是第一代公开的、完全说明细节的商业级现代算法，并被世界公认。

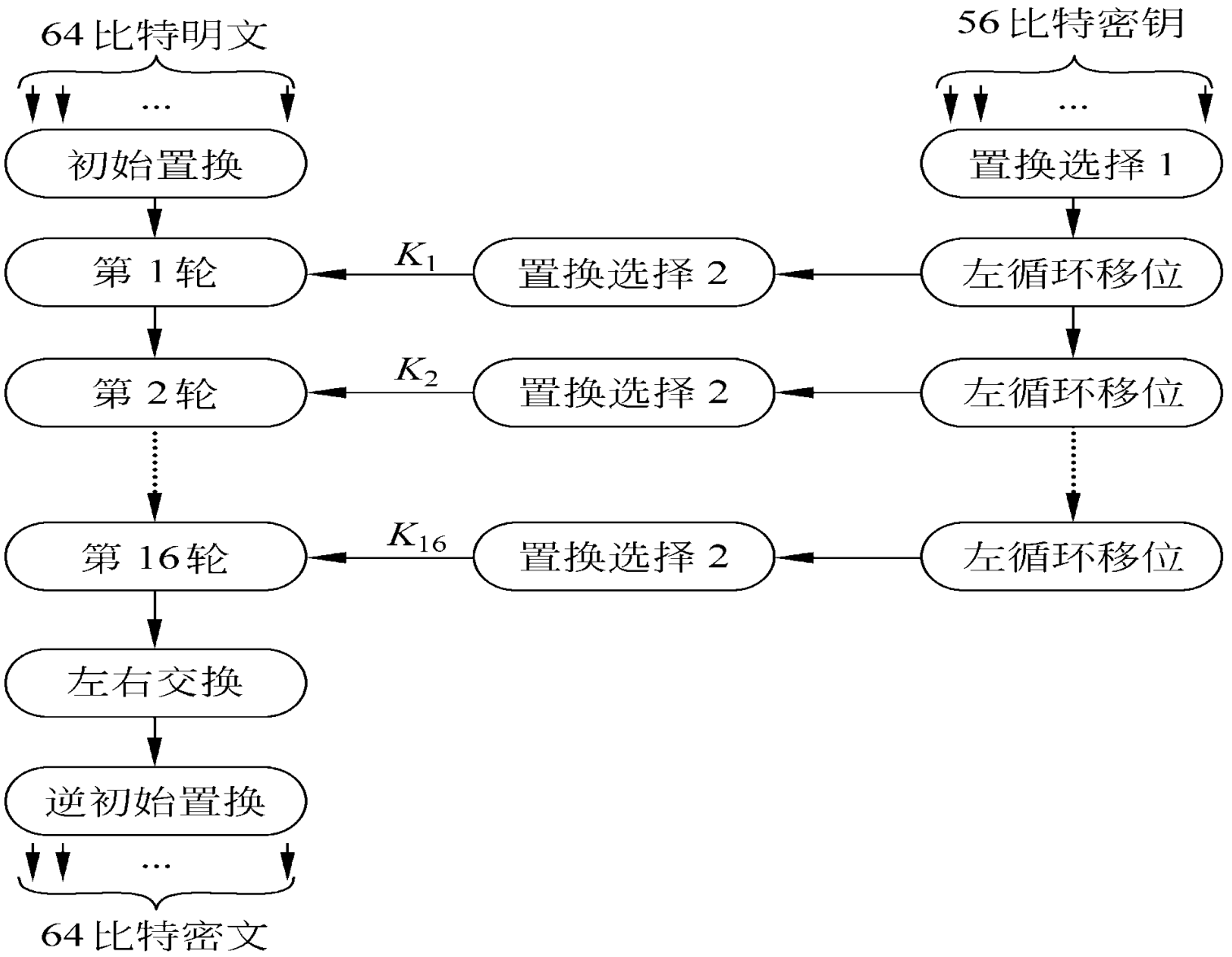
第二十讲 DES算法简介

- 美国制定数据加密标准简况
- DES的框架和主要参数

DES 算法

- 分组长度为**64 bits (8 bytes)**
- 密文分组长度也是**64 bits**。
- 密钥长度为**64 bits**，有**8 bits**奇偶校验，有效密钥长度为**56 bits**。
- 算法主要包括：初始置换***IP***、**16**轮迭代的乘积变换、逆初始置换IP^{-1}以及**16**个子密钥产生器。

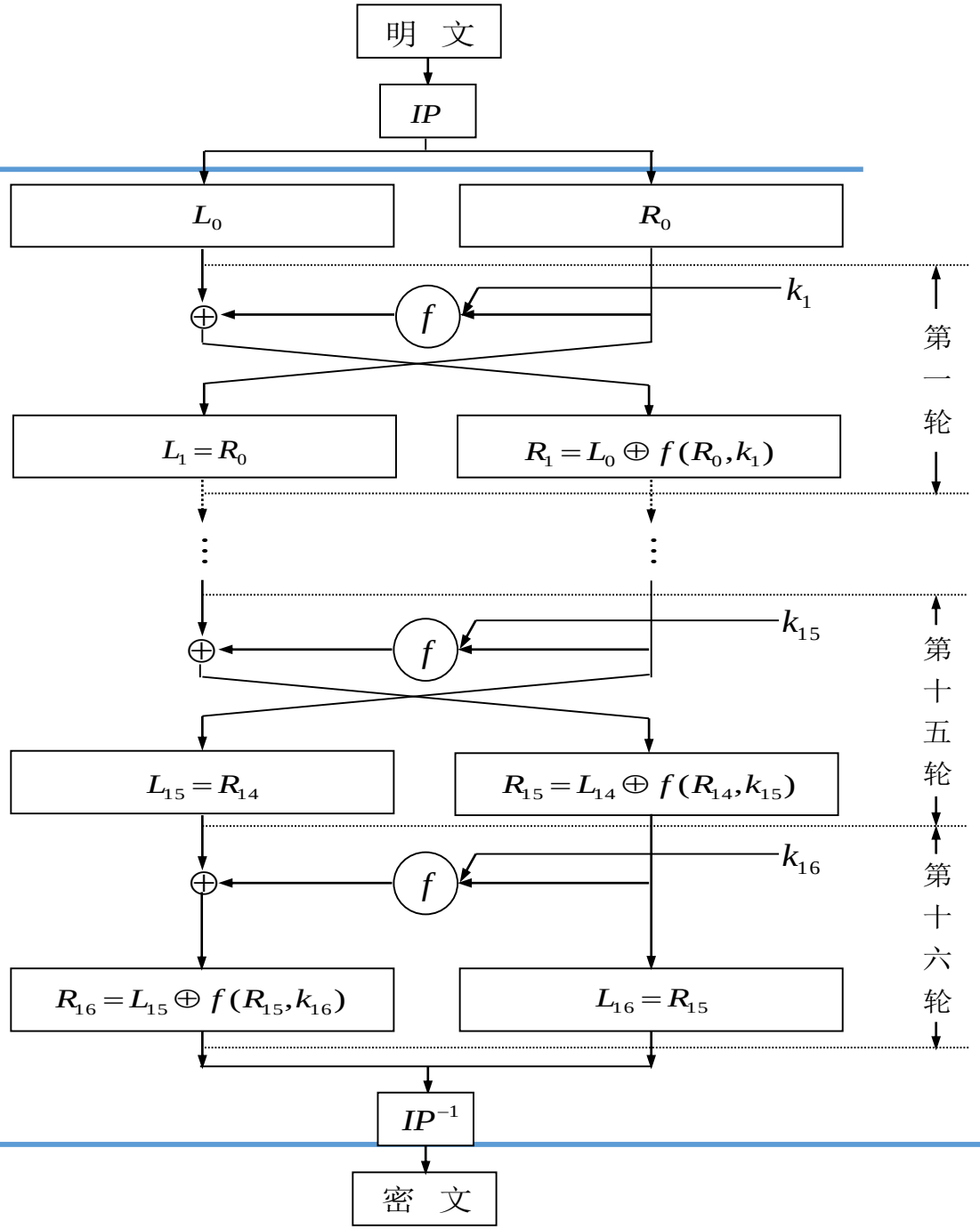
DES算法框图


64 比特明文
56 比特密钥
初始置换
置换选择 1
第 1 轮
K_1
置换选择 2
左循环移位
第 2 轮
K_2
置换选择 2
左循环移位
第 16 轮
K_{16}
置换选择 2
左循环移位
左右交换
逆初始置换
64 比特密文

DES算法流程

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus F\left(R_{i-1},\ K_i\right)$$



初始置换*IP*与逆初始置换

- 初始置换是将**64 bit**明文的位置进行置换，得到一个乱序的**64 bit**明文组。
- 逆初始置换IP^{-1}。将**16**轮迭代后给出的**64 bit**组进行置换，得到输出的密文组。输出为阵中元素按行读得的结果。
- ***IP***和IP^{-1}在密码意义上作用不大，它们的作用在于打乱原来输入***x***的**ASCII**码字划分的关系。

初值置换IP

(a) 初始置换 IP

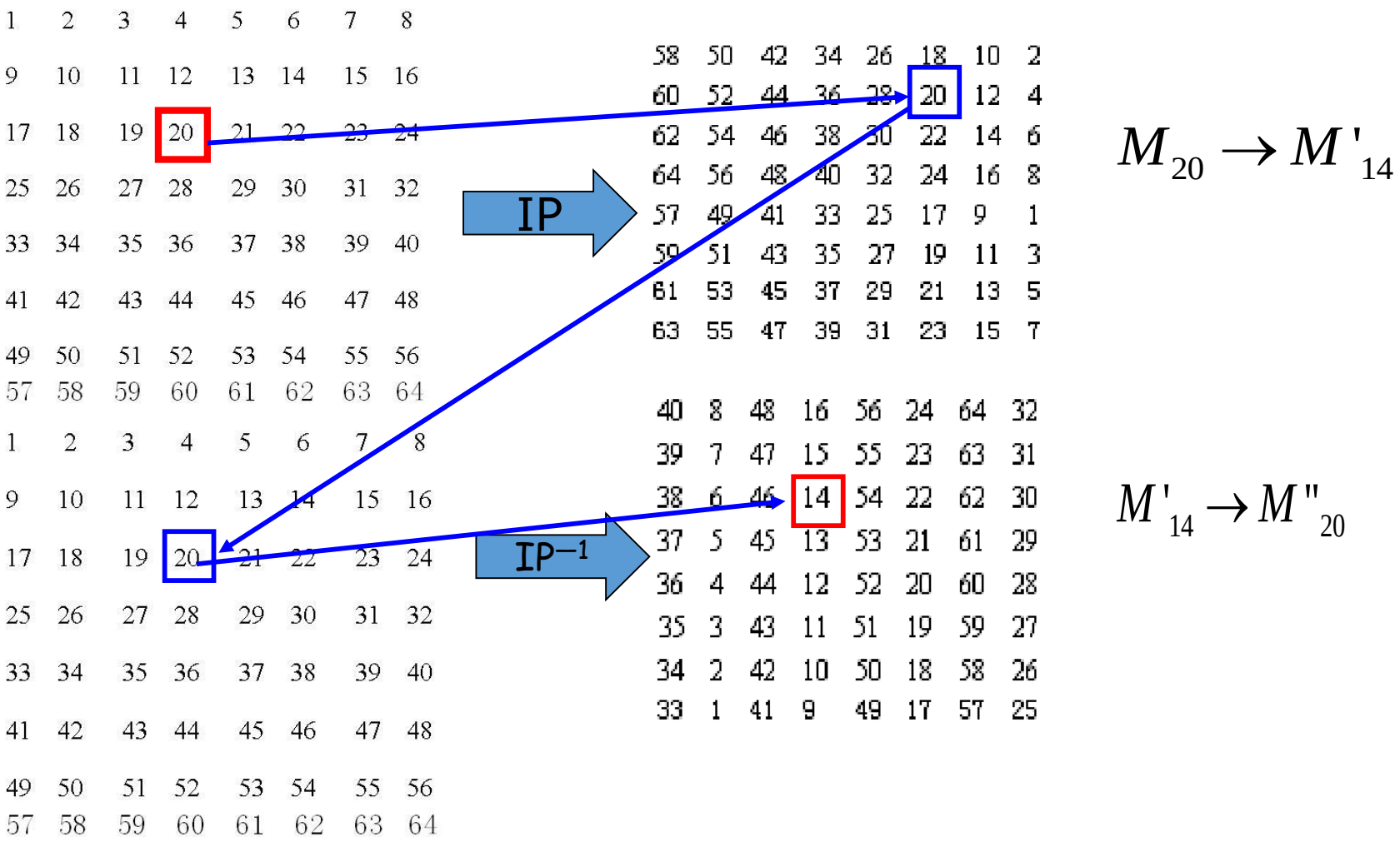
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

逆初值置换IP^{-1}

（b） 逆初始置换 IP^{-1}

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

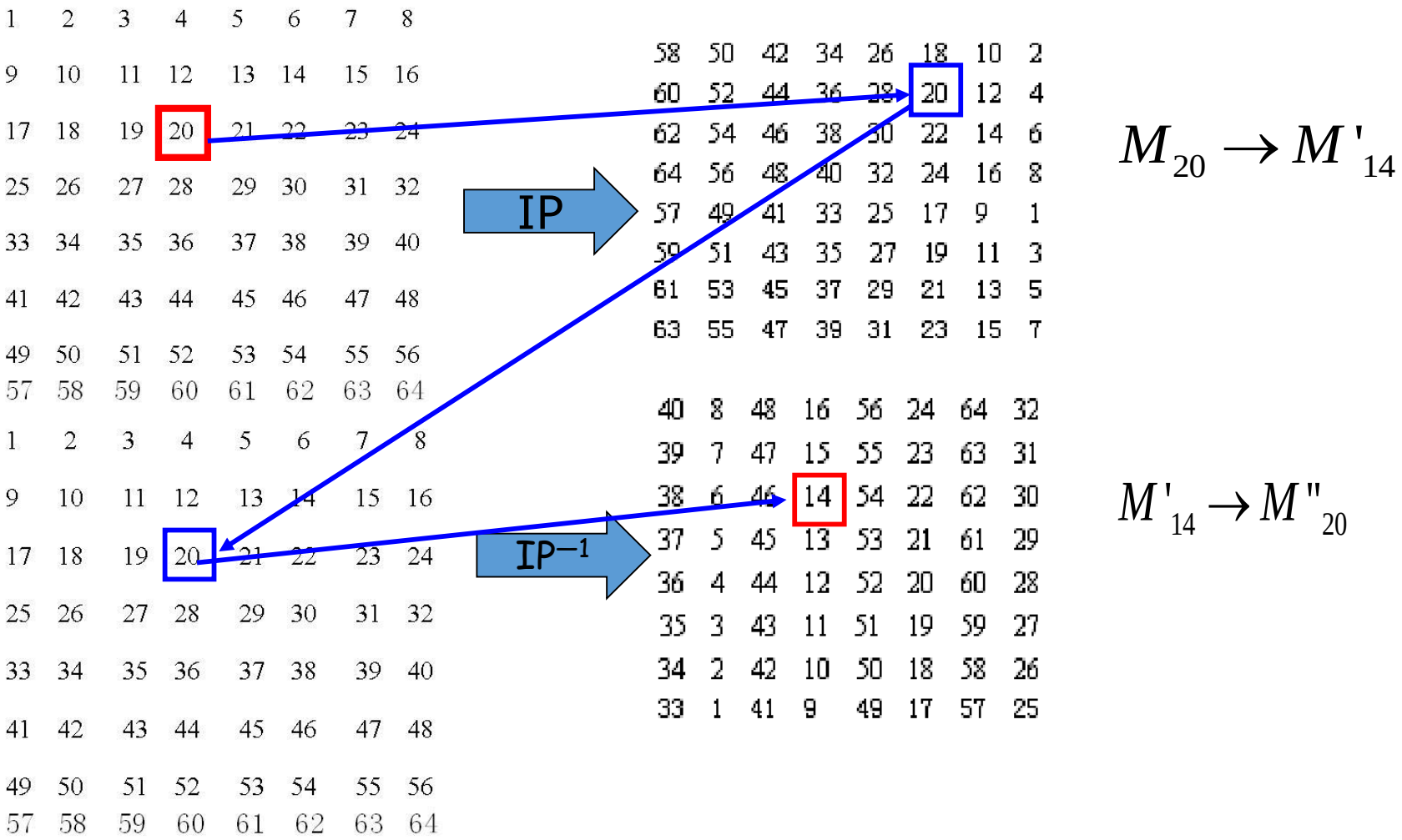
IP与IP^{-1}



$$M_{20} \rightarrow M'_{14}$$

$$M'_{14} \rightarrow M''_{20}$$

IP和IP^{-1}


1 2 3 4 5 6 7 8
9 10 11 12 13 14 15 16
17 18 19 20 21 22 23 24
25 26 27 28 29 30 31 32
33 34 35 36 37 38 39 40
41 42 43 44 45 46 47 48
49 50 51 52 53 54 55 56
57 58 59 60 61 62 63 64
IP
58 50 42 34 26 18 10 2
60 52 44 36 28 20 12 4
62 54 46 38 30 22 14 6
64 56 48 40 32 24 16 8
57 49 41 33 25 17 9 1
59 51 43 35 27 19 11 3
61 53 45 37 29 21 13 5
63 55 47 39 31 23 15 7
$M_{20} \rightarrow M'_{14}$
1 2 3 4 5 6 7 8
9 10 11 12 13 14 15 16
17 18 19 20 21 22 23 24
25 26 27 28 29 30 31 32
33 34 35 36 37 38 39 40
41 42 43 44 45 46 47 48
49 50 51 52 53 54 55 56
57 58 59 60 61 62 63 64
IP^{-1}
40 8 48 16 56 24 64 32
39 7 47 15 55 23 63 31
38 6 46 14 54 22 62 30
37 5 45 13 53 21 61 29
36 4 44 12 52 20 60 28
35 3 43 11 51 19 59 27
34 2 42 10 50 18 58 26
33 1 41 9 49 17 57 25
$M'_{14} \rightarrow M''_{20}$

感 谢 聆 听!

xynie@uestc.edu.cn