哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY
立足航天，服务国防，面向国民经济主战场

计算机网络之危机四伏

主讲人：李全龙

本讲主题

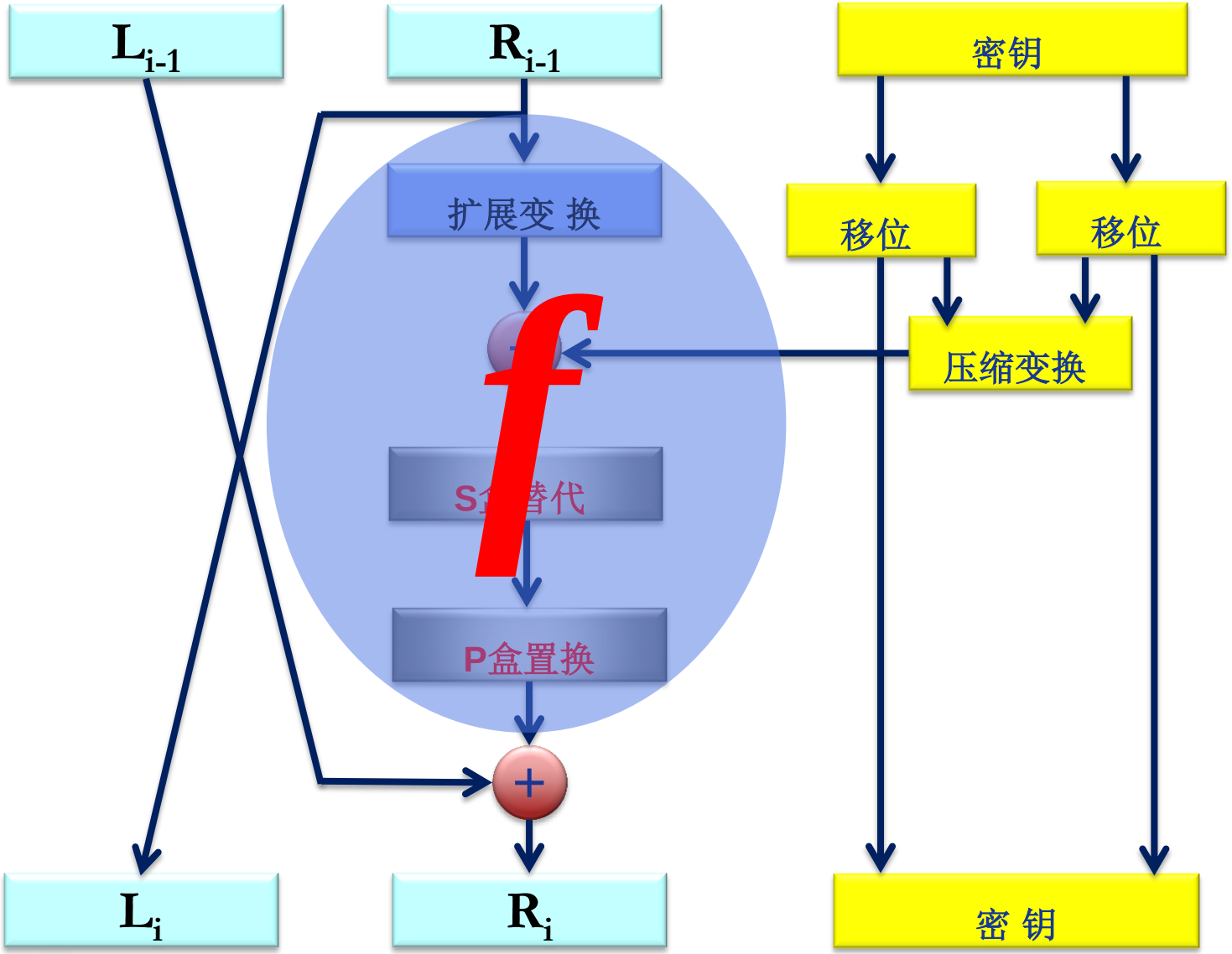
密码学基础（5）

初始置换IP(Initial Permutation)

- 把输入的64位数据的排列顺序打乱，每位数据按照下面规则重新组合

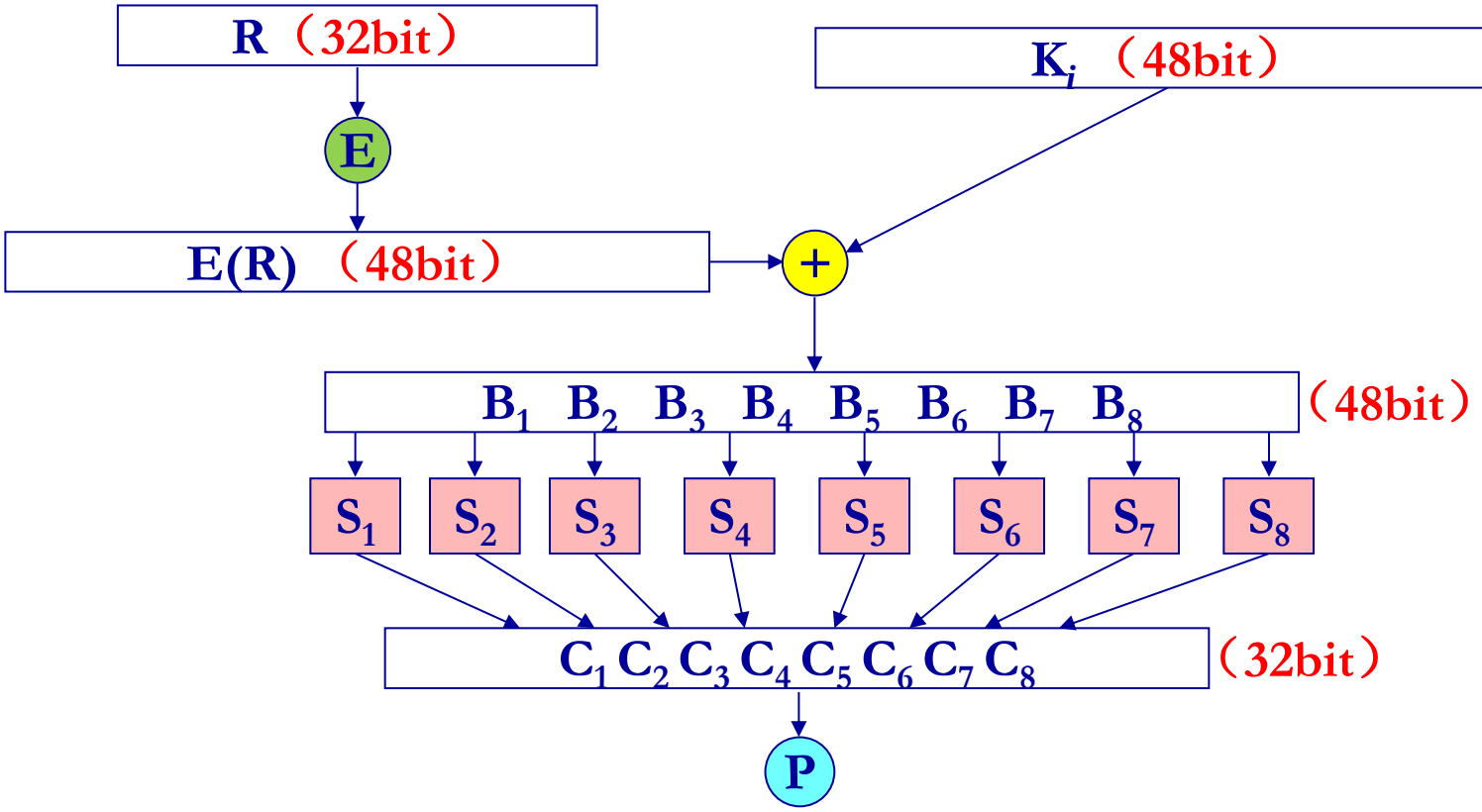
IP置换表							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

一轮DES加密过程



DES：f函数结构

- 黑盒变换
- 多个函数/操作(E、异或、S、P)的组合函数



f 函数的基本操作

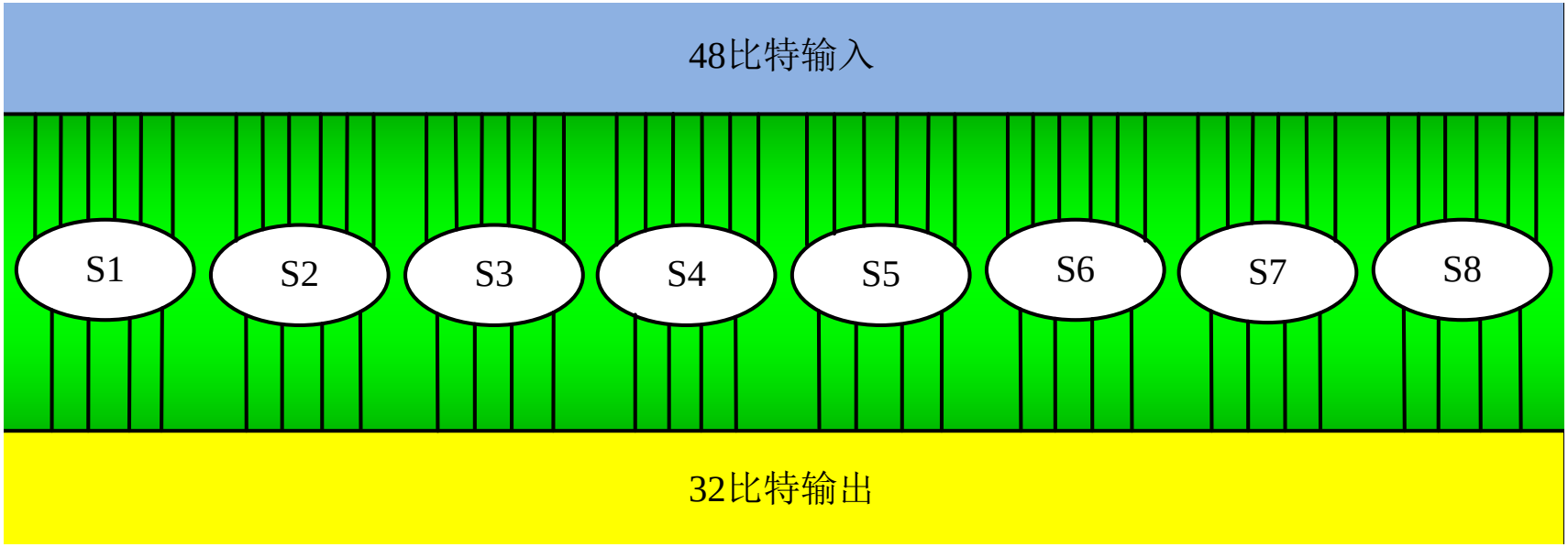
- **扩展变换：** 扩展变换（Expansion Permutation，也被称为E-盒）将64位输入序列的右半部分从32位扩展到48位。
  - 确保最终的密文与所有的明文位都有关

扩 展 变 换

32	1	2	3	4	5	4	5	6	7	8	9
8	9	10	11	12	13	12	13	14	15	16	17
16	17	18	19	20	21	20	21	22	23	24	25
24	25	26	27	28	29	28	29	30	31	32	1

f 函数的基本操作

- **S-盒替代**（S-boxes Substitution）



f 函数的基本操作

- **P-盒置换**（P-boxes Permutation）

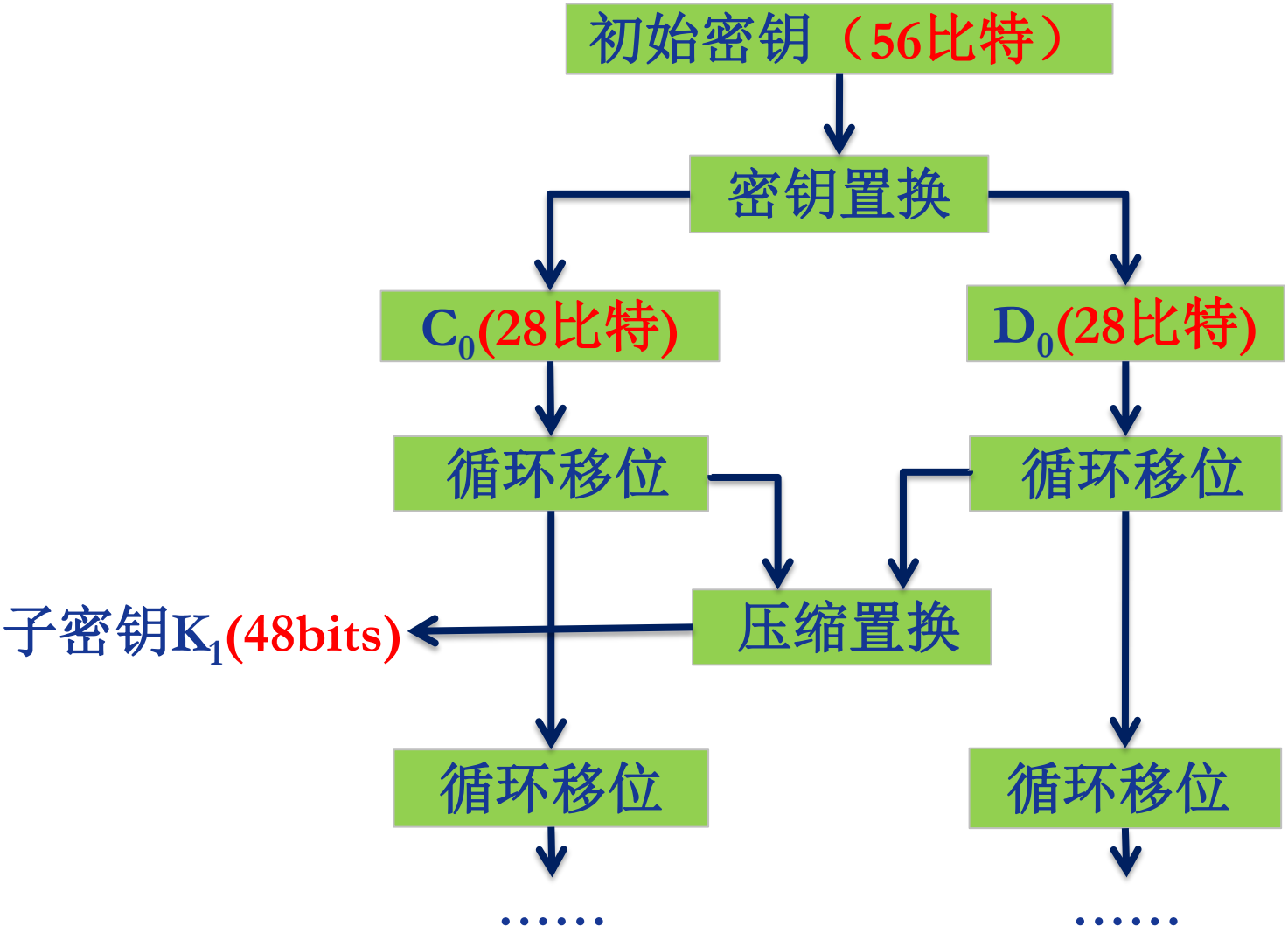
16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

逆初始置换(Inverse Initial Permutation)

- 初始置换和对应的逆初始置换操作并不会增强DES算法的安全性
- 主要目的是为了更容易地将明文和密文数据以字节大小放入DES芯片中

40	8	18	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

每轮子密钥的生成


初始密钥（56比特）
密钥置换
C_0(28比特)
D_0(28比特)
循环移位
循环移位
压缩置换
子密钥K_1(48bits)
循环移位
循环移位
……
……

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

立足航天，服务国防，面向国民经济主战场

谢 谢！