


copyright reserved

基于喷泉码的对称加密算法

陈博 胡鸣

2016. 5. 20



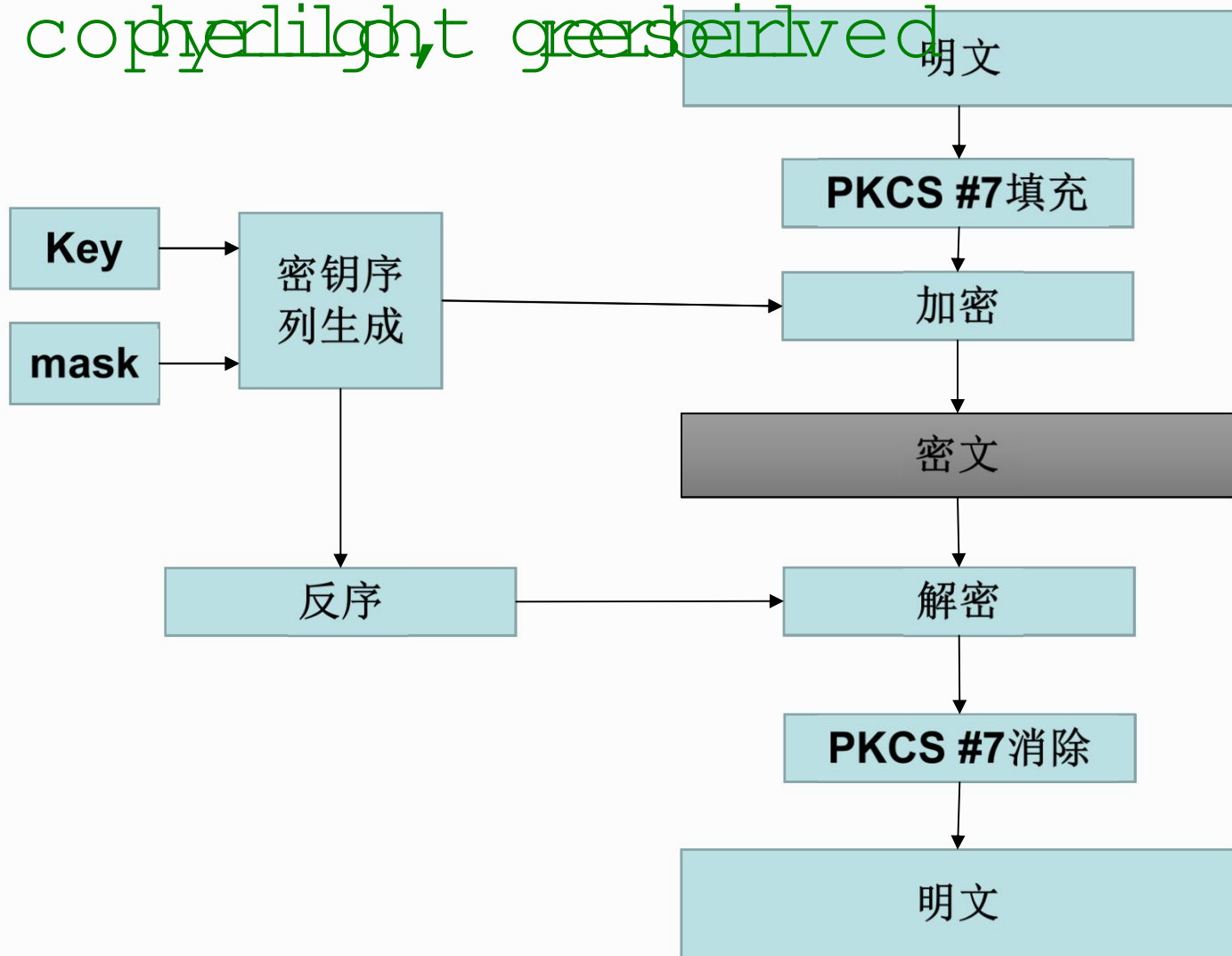
背景

copyright reserved

- 云服务大量出现，云存储，云播放，云查看等。非对称加密没法满足快速，大量文件加密要求。
- 常见的对称加密算法不够灵活：
 - 密钥长度局限，可选的种类少
 - 数据需要手动填充

基于喷泉码的对称加密算法

copyright reserved





算法特性

copyright reserved

- 密钥多样化

- 密钥长度为8的倍数 $8n$ (1, 2, 3, 4 ...)
- 最短8位, 没有上限
- 16进制字符串

- PKCS #7块自动填充

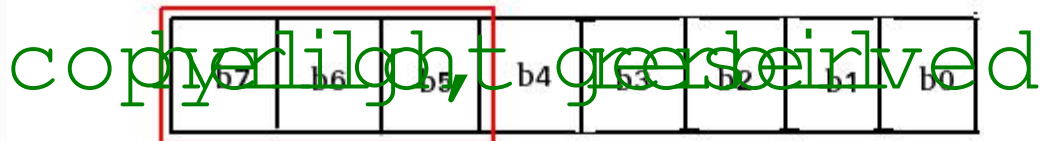
- 喷泉码混淆与扩散

- XOR, 链式压缩, 混乱信息熵
- 块内行换位, 扩散明文信息

加密

copyright reserved

b7	b6	b5	b4	b3	b2	b1	b0
----	----	----	----	----	----	----	----



message = B7B6B5B4B3B2B1B0

key = b7b6b5 \wedge mask

$B'[0] = B[key++]$

$B'[1] = B[key++ \% bsize] \wedge B'[0]$

$B'[2] = B[key++ \% bsize] \wedge B'[1]$

$B'[3] = B[key++ \% bsize] \wedge B'[2]$

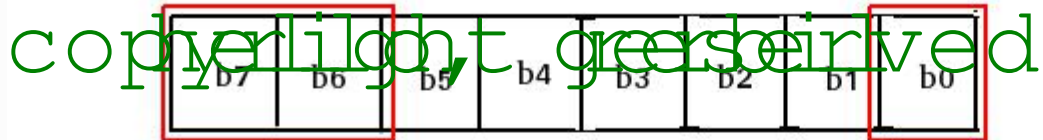
...

$B'[7] = B[key++ \% bsize] \wedge B'[6]$

解密

copyright reserved

b7	b6	b5	b4	b3	b2	b1	b0
----	----	----	----	----	----	----	----



cliper = B7B6B5B4B3B2B1B0

key = b0b7b6 \wedge mask

B'[key++] = B[0]

B'[key++ % bsize] = B[1] \wedge B[0]

B'[key++ % bsize] = B[2] \wedge B[1]

...

B'[key++ % bsize] = B[7] \wedge B[6]



算法测试

copyright reserved

- 1、密钥长度测试
- 2、明文长度测试
- 3、二进制文件测试
- 4、压缩测试
- 5、明文与密文相似度测试
- 6、雪崩效应测试

DEMO

copyright reserved

表 5-9 测试结果

算法	测试结果	压缩比率
SEF	success	99.9445832361
DES	success	100.019329338
DES3	success	100.023680687
AES	success	100.022062417

表 5-10 密钥雪崩效应测试

密钥（原密钥）	密钥（改变后）	密文变化比率
6477710ee4154d39	6477710ae4154d39	9.884 %
d5a47bef2844be4b	d5a47baf2844be4b	9.855 %
abf096587a897b4c	abf096187a897b4c	9.893 %

密文压缩测试

雪崩效应测试

时间复杂度与密钥长度关系

