现代密码学

第十六讲 A5流密码算法

信息与软件工程学院

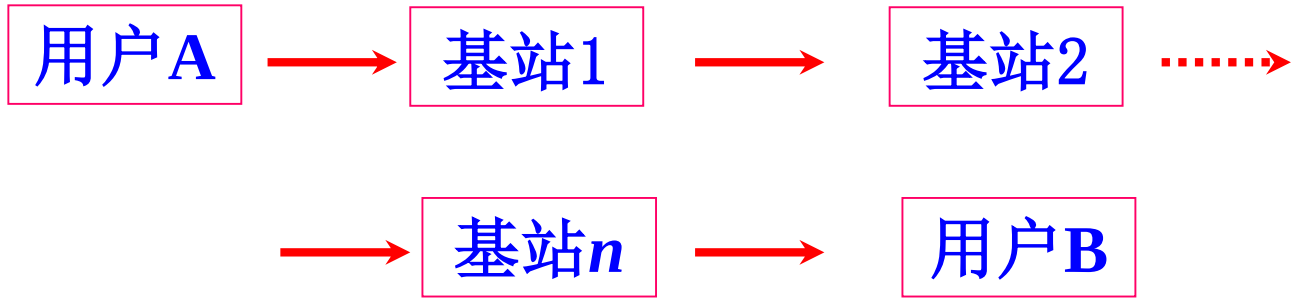
第十六讲 A5流密码算法

- A5流密码算法的基本用法
- A5流密码算法的基本原理

A5/1流密码算法的基本用法

- 用于蜂窝式移动电话系统语音和数字加密。
- A5/1算法用于用户的手机到基站之间的通信加密，通信内容到基站后先解密变成明文，然后再进行基站到基站之间、以及基站到用户手机之间的信息加密，完成通信内容在通信过程的加密保护

通信模式



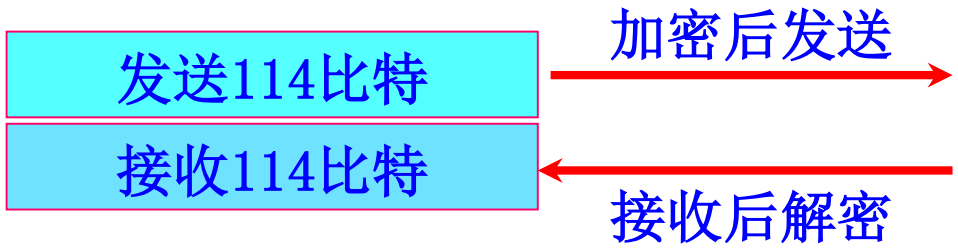
A5/1流密码算法的基本用法（续）

- 应用环节
  - 只需考察用户A到基站1之间通信内容的加解密，中间消息的传送由基站到基站之间的加密完成，而接收方用户B对消息的加解密与用户A到基站1之间的通信完全类似，只不过是用户B先解密消息。
- 基本密钥K_{A1}
  - 基本密钥K_{A1}：预置在SIM卡中，与基站1共享。
  - 生存期：一旦植入SIM卡将不再改变。
  - 用途：用来分配用户和基站之间的会话密钥。

A5/1流密码算法的基本用法（续）

- 会话密钥k
  - 产生方式：在每次会话时，基站产生一个64比特的随机数k。
  - 分配方式：利用基本密钥K_{A1}，使用其它密码算法将k加密传给用户手机。
  - 生存期：仅用于一次通话时间。
- 明文处理
  - 按每帧228比特分为若干帧后逐帧加密，每帧处理方式相同。

$$M = M_1 \| M_2 \| \cdots \| M_i \| \cdots \qquad |M_i| = 228$$



A5/1流密码算法的基本用法（续）

- 加密方式
  - 加密： $E_k(M)=E_{k1}(M_1)E_{k2}(M_2)E_{k3}(M_3)\cdots$
  - 一次通话使用一个会话密钥，对每帧使用不同的帧密钥
  - 帧会话密钥：帧序号，长度为22比特
  - 帧会话密钥共产生228比特密钥流，实现对本帧228比特通信数据的加解密
  - 明密结合方式：逐位异或
  - 一次通话量：至多2^{22}帧数据，约0.89×2^{30}比特

A5/1序列密码算法中的线性反馈移位寄存器

- 算法使用3个级数为19、22和23的本原移存器。

LFSR-1 → $f_1(x) = x^{19} \oplus x^{18} \oplus x^{17} \oplus x^{14} \oplus 1$

LFSR-2 → $f_2(x) = x^{22} \oplus x^{21} \oplus x^{17} \oplus x^{13} \oplus 1$

LFSR-3 → $f_3(x) = x^{23} \oplus x^{22} \oplus x^{19} \oplus x^{18} \oplus 1$

注：A5/1算法中，LFSR的移位方式是左移方式。 各寄存器的编号从第0级编号到第*n*-1级。

算法初始化

- 初始化是利用一次通话的会话密钥***k***和帧序号设定三个移存器的起点，即初始状态。
- **Step 1：**将三个**LFSR**的初态都设置为全零向量；
- **Step 2：(**密钥参与**)** 三个**LFSR**都规则动作**64**次，每次动作**1**步。
- 在第***i***步动作时，三个**LFSR**的反馈内容都首先与密钥的第***i***比特异或，并将异或结果作为**LFSR**反馈的内容。

密钥参与过程举例

以移存器1为例的密钥参与过程：

$k = k_{64}k_{63}\cdots k_1$　　$f_1(x) = x^{19} \oplus x^{18} \oplus x^{17} \oplus x^{14} \oplus 1$

初始状态：　$S_0 = (x_{18}, x_{17}, \cdots, x_0) = (0,0,\cdots,0)$

动作1步后状态：　$S_1 = (x_{18}, x_{17}, \cdots, x_0) = (0,0,\cdots,k_1)$

动作2步后状态：　$S_2 = (x_{18}, x_{17}, \cdots, x_0) = (0,0,\cdots,k_1,k_2)$

动作14步后状态：　$S_{14} = (x_{18}, x_{17}, \cdots, x_0) = (0,0,\cdots,k_1,k_2,\cdots,k_{13},k_{14})$

动作15步后状态：　$S_{15} = (x_{18}, x_{17}, \cdots, x_0) = (0,0,\cdots,k_1,k_2,\cdots,k_{14},k_1 \oplus k_{15})$

动作64步完成密钥参与过程。

帧序号参与

- **Step 3**：（帧序号参与）三个LFSR都规则动作22次，每次动作1步。在第*i*步动作时，三个LFSR的反馈内容都首先与帧序号的第*i*比特异或，并将异或的结果作为LFSR反馈的内容；帧序号比特的序号是从最低位编到最高位。
- 帧序号参与方式：与密钥参与方式相同，不同的明文数据帧按顺序编号，每个编号为22比特。
- 记帧序号为

$$T_0 = t_{22}t_{21}\cdots t_1 = 00\cdots 00 \quad T_1 = t_{22}t_{21}\cdots t_1 = 00\cdots 01 \quad \cdots\cdots$$

- 帧密钥参与的目的：对不同的帧设置不同的帧会话密钥，保证对每帧以不同的起点生成密钥流，尽可能避免密钥重用。

第十六讲 A5流密码算法

- A5流密码算法的基本用法
- A5流密码算法的基本原理

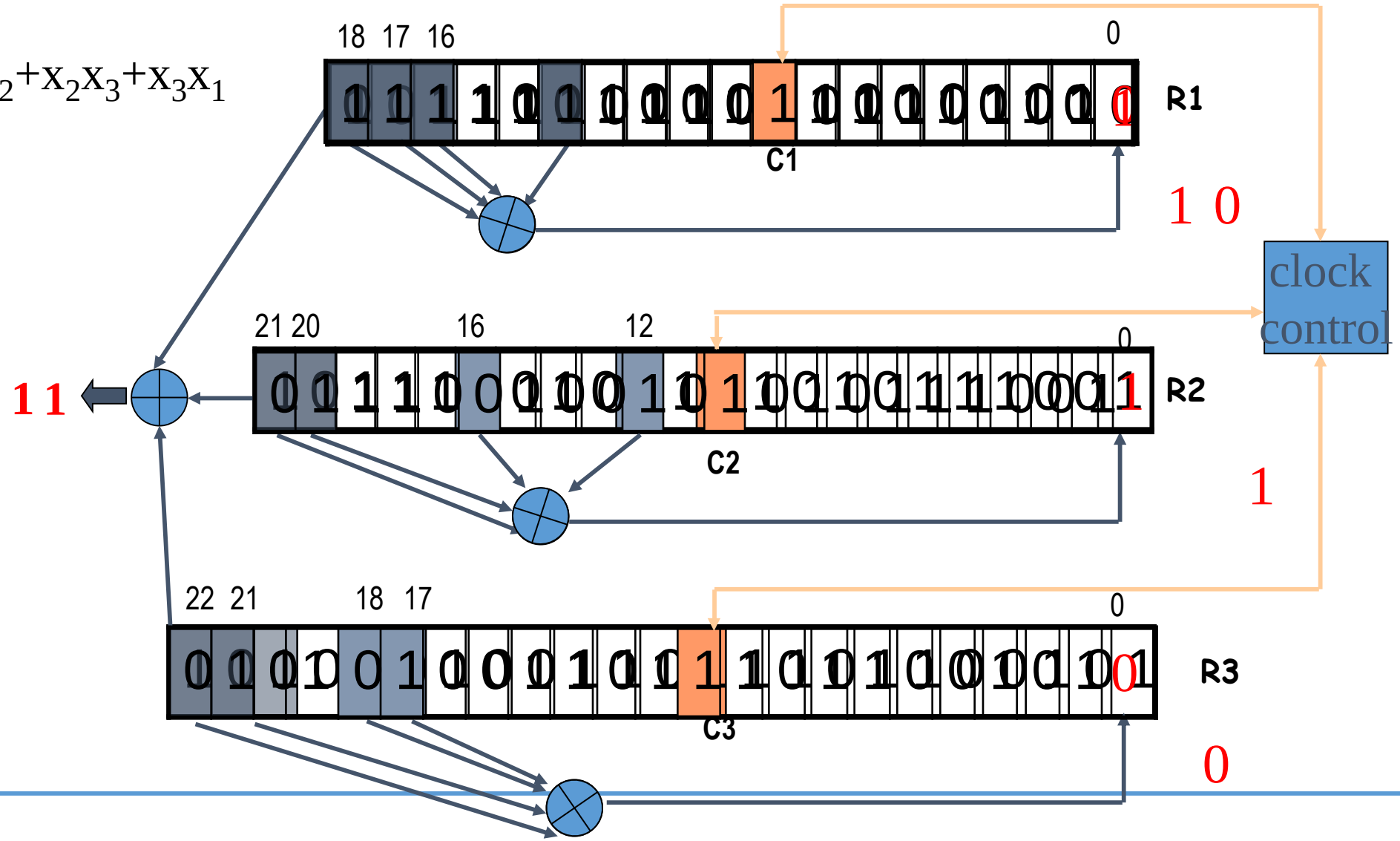
密钥流生成与加解密

- A5算法中，采用钟控方式控制3个LFSR来产生密钥流。
- 钟控信号x_1 x_2 x_3的采取：x_1取自LFSR-1第9级； x_2取自LFSR-2第11级； x_3取自LFSR-3第11级 。
- 控制方式：采用多项式$g(x)=x_1x_2+x_2x_3+x_3x_1$来确定，取钟控信号和多项式值相同的进行移位，不同的就不动。

(X_1,X_2,X_2)	000	001	010	011	100	101	110	111
LFSR-1	动	动	动	不动	不动	动	动	动
LFSR-2	动	动	不动	动	动	不动	动	动
LFSR-3	动	不动	动	动	动	动	不动	动

钟控方式

$g(x)=x_1x_2+x_2x_3+x_3x_1$



关于加密

- **Step 4**：三个LFSR以钟控方式连续动作100次，但不输出密钥流；
- **Step 5**：三个LFSR以钟控方式连续动作114次，在每次动作后，三个LFSR都将最高位寄存器中的值输出，这三个比特的异或就是当前时刻输出的1比特密钥。
- 连续动作114步，共输出114比特密钥流，用于对用户手机到基站传送的114比特数据的加密；

加密方式： $c_i = m_i \oplus d_i; i = 1,2,\cdots,114$

关于解密

- **Step 6**：三个LFSR以钟控方式连续动作100次，但不输出密钥流；
- **Step 7**：三个LFSR以钟控方式连续动作114次，在每次动作后，三个LFSR都将最高级寄存器中的值输出，这三个比特的模2和就是当前时刻输出的1比特密钥流。
- 连续动作114步，共输出114比特密钥流，这114比特用于对基站到用户手机传送的114比特数据的解密。

解密方式：$m_i' = c_i' \oplus d_i; i = 115,116,\cdots,228$

A5/1算法的弱点

- 移位寄存器太短容易遭受穷举攻击
  - A5/1算法把主密钥作为算法中三个寄存器的初始值，长度为64比特。如果利用已知明文攻击，只需要知道其中两个寄存器的初始值，就可以计算出另一个寄存器的初始值，这只需要2^{40}步就可以得出寄存器LFSR-1和LFSR-2的结构。
- 事实上，A5/1加密算法中存在严重的安全问题
  - 利用了GSM通信加密中的两个安全漏洞，可以通过离线迭代计算生成一个彩虹表，它包含有密钥和其相对应的输出密码。这个彩虹表的大小为984GB。得到了彩虹表之后，安全专家就可以在短短的九秒内确定用于加密通信数据的密钥。

密钥流生成器的基本原则

- 设计一个性能良好的序列密码是一项十分困难的任务。最基本的设计原则是“密钥流生成器的不可预测性”，它可分解为下述基本原则：
  ① 长周期。
  ② 高线性复杂度(用最少的移位寄存器来实现)。
  ③ 统计性能良好。
  ④ 足够的“混乱”。
  ⑤ 足够的“扩散”。
  ⑥ 抵抗不同形式的攻击。

感 谢 聆 听!

xynie@uestc.edu.cn