“TD-SCDMA标准与测试”技术培训

—USIM-ME接口技术

信息产业部电信研究院通信标准研究所
无线与移动研究室 杨红梅
yanghongmei@mail.ritt.com.cn

内容

- 概述
- UICC/USIM简介
- PLMN选择
- 电话簿
- USIM中的鉴权过程
- SIM/USIM互操作
- USAT简介

SIM、USIM和UICC

- **SIM （Subscriber Identity Module）**

  GSM定义的智能卡（ICC），它最初被定义为一种物理和逻辑实体，不区分平台和应用，SIM只能接受2G命令。

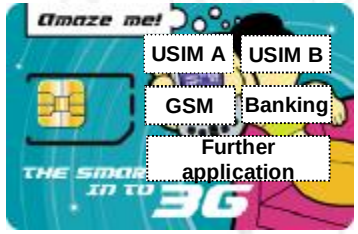
- **USIM （Universal Subscriber Identity Module）**

  一种驻留在UICC上的纯逻辑应用，以便接入到UMTS网络中。USIM可以提供2G鉴权和密钥协商机制以便3G终端接入2G网络。

- **UICC （Universal Integrated Circuit Card）**

  可移动的硬件模块， 可以认为是一个可移动的多应用IC卡。USIM的物理和逻辑平台。至少包含一个USIM应用，也可以包含SIM应用，另外，还可以包含其他应用

  （如移动银行和移动商务）。



SIM和USIM的异同

项目	USIM	SIM
多应用	多应用UICC	单GSM应用
鉴权算法	f1,f1*,f2,f3,f4,f5等	A3,A8
电话本	2个名字(EFADN, EFSNE）;多个号码（EFANR）;多个email地址（EF EMAIL）	1个名字，一个号码
加密算法	WIM, CryptoAPI, RSA1024	DES、3DES

USIM

- 3G关注移动多媒体
- 3G卡关注安全
- USIM关注“安全的移动多媒体”

主要国际标准

- **TS 21.111 "USIM and IC card requirements“**
- **TS 31.101 “UICC - Terminal Interface; Physical and Logical Characteristics”**

TS 31.101的移动通信IC卡的底层和终端相关的内容已经转移到 ETSI EP SCP (TS 102 221)

- **TS 31.102 “Characteristics of the USIM Application”**

介绍USIM 特定的命令、参数、文件结构、应用协议和安全功能等

- **TS 31.111 "USIM Application Toolkit“**

SIM 应用工具箱 (GSM 11.14)的UMTS版本。

GSM 11.11 等同于31.101 和31.102 的合并版本

3G终端与2G终端

- **3G终端**

3G单模终端　——仅支持3G无线接入网

2G/3G双模终端——即支持**3G**无线接入网也支持**2G**无线接入网

单模和双模的**3G**终端都可以处理 **3G AKA** 和 **2G AKA**，可以与**UICC**上的 **USIM**应用互操作。

- **2G终端**

仅支持**2G**无线接入网络（**GSM**），只能处理**2G AKA**，可以与**UICC**上的**SIM**应用以及**SIM**卡互操作。

内容

- 概述
- UICC/USIM简介
- PLMN选择
- 电话簿
- USIM中的鉴权过程
- SIM/USIM互操作
- USAT简介

UICC/USIM简介

- 物理和电气特性
- 传输协议
- UICC文件系统
- UICC安全特性

物理特性

- **卡的尺寸**

与SIM卡相同(ID-1 & Plug-In)

- **卡的工作温度范围**

正常操作温度范围-25℃～+70℃，偶然的峰值温度可以到+85℃。

- **触点的规定**

ME： C4和C8不用，应为高阻；对于嵌入式卡，**C6**不使用。

UICC：不需提供C4和C8，如提供则内部不应与UICC连接；

C6除了提供**Vpp**外，不与卡中其它部分连线。

电气特性

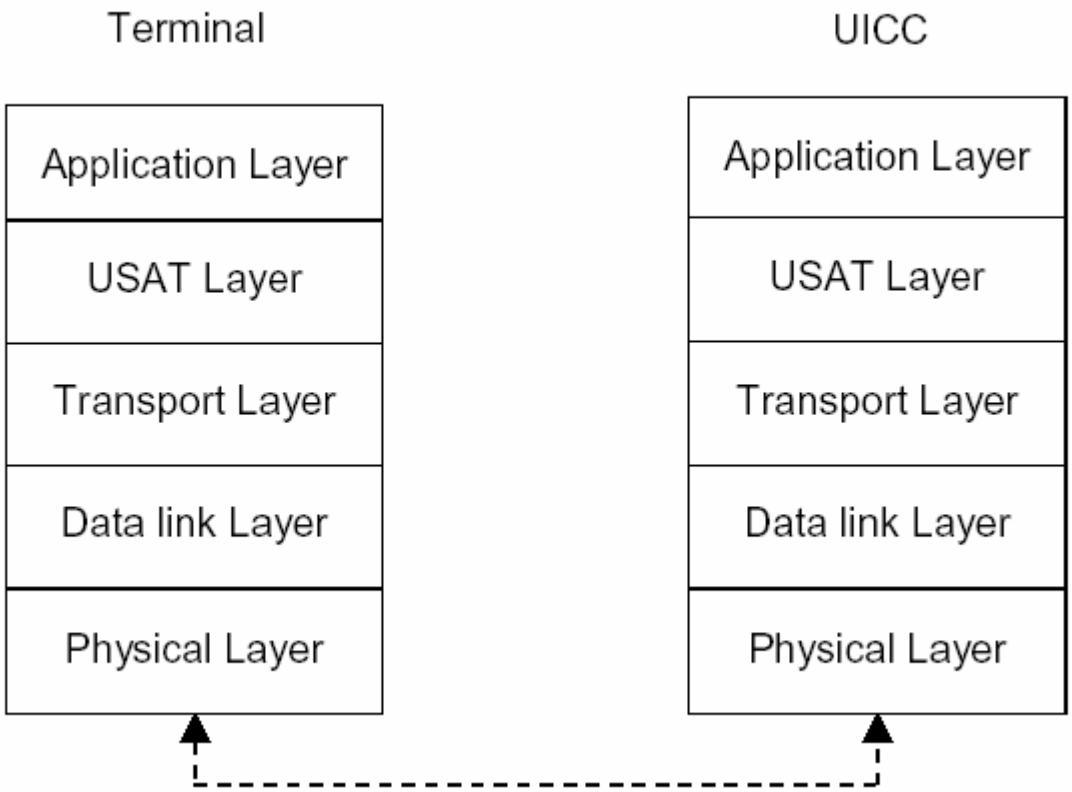
- 电气特性：**3**种类别 (A, B, C)
  - B是必选项
  - 至少支持两个类别

类别	电压 (V)	最小电流 (会话期间)	最大电流 * (会话期间)	
A	4.5 - 5.5	10mA	60mA	
B	**2.7 – 3.3**	**7,5mA**	**50mA**	**必选**
C	1.62 – 1.98	5mA	30mA	

*** 应用可以在对SELECT命令的响应中指定自己最大功率消耗值**

传输协议（1）

- 传输协议用于在UICC和ME之间交换数据。
- 终端和UICC中的协议栈结构如下图所示。



传输协议（2）

ØT=0协议

一种基于半双工异步字符的传输协议。

所有使用T=0协议的命令均由ME发起,通知UICC如何做。

ME总是‘主’，UICC总是‘从’。

ØT=1协议

一种基于半双工异步块的传输协议。

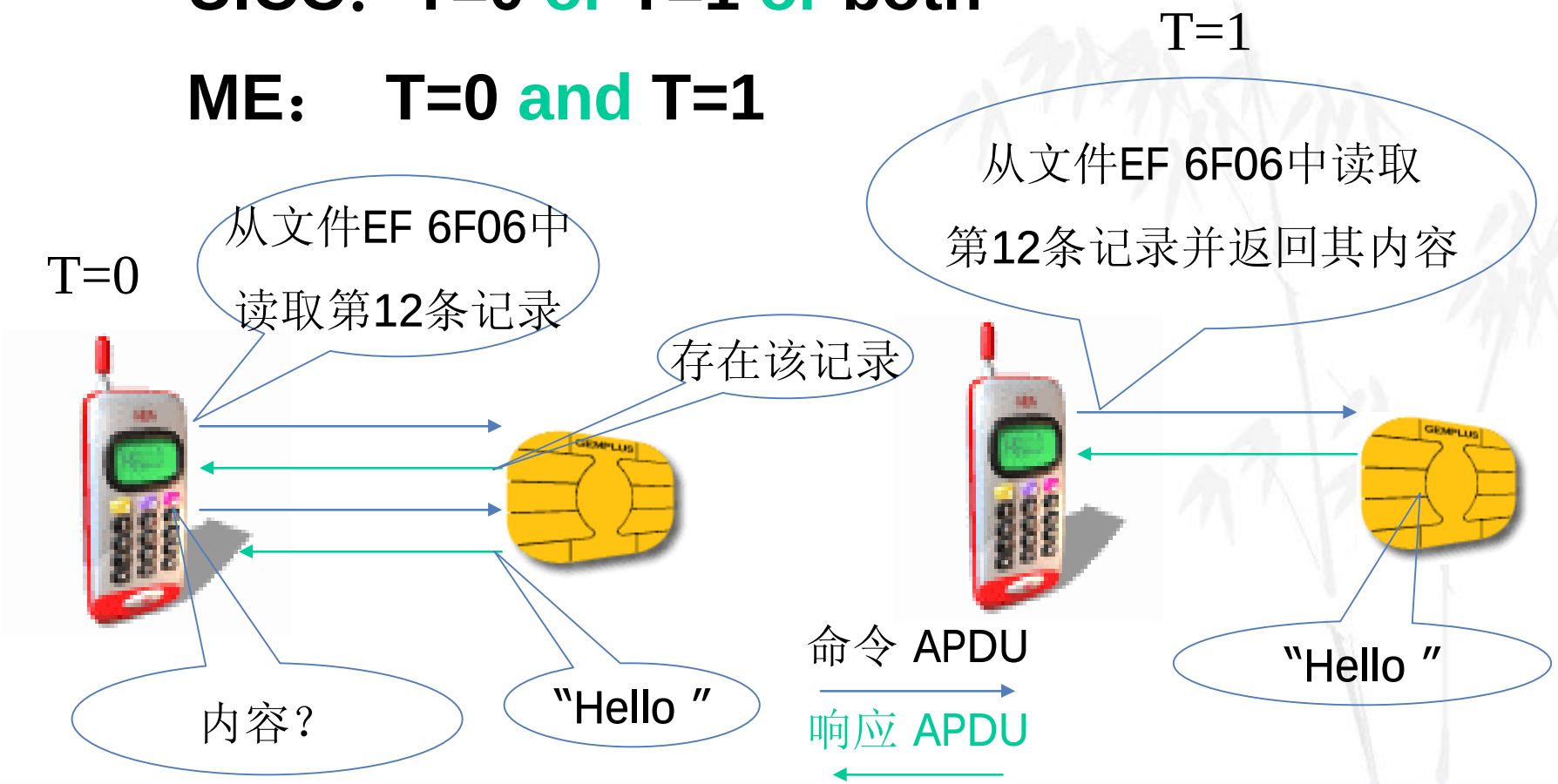
通信由ME向UICC发送一个块开始。

发送块的权利在ME和UICC间交替。

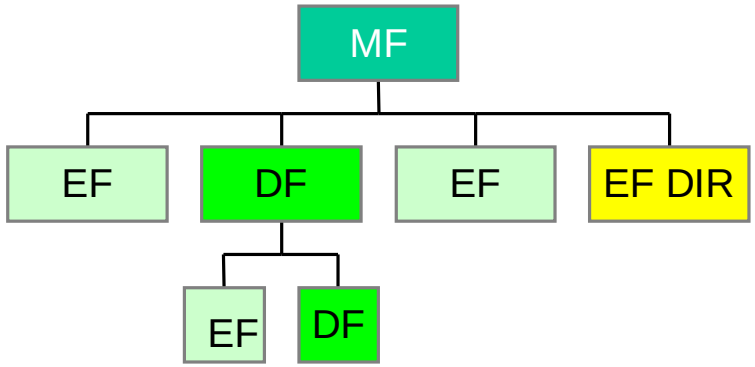
传输协议（3）

UICC：T=0 or T=1 or both

ME： T=0 and T=1



UICC 文件系统（1）

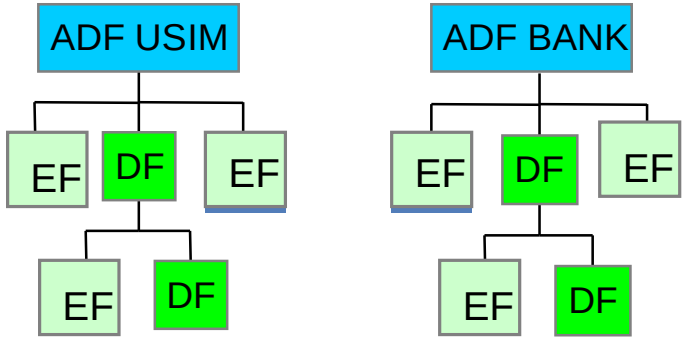


保留的GSM文件

主要文件 (MF)

基本文件 (EF)

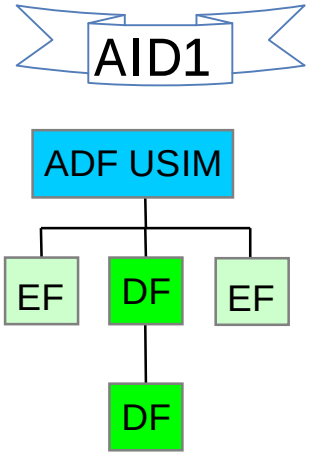
专用文件 (DF)

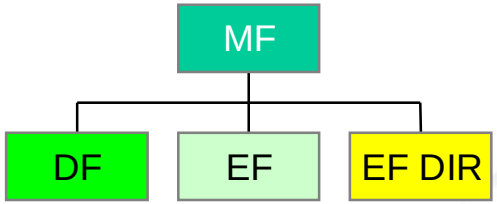


新增文件类型

专用应用文件 (ADF)

UICC 文件系统（2）





- **AID1**
- **AID2**
- **AID3**
- **AID4**

ADF：

ü专用于某个应用

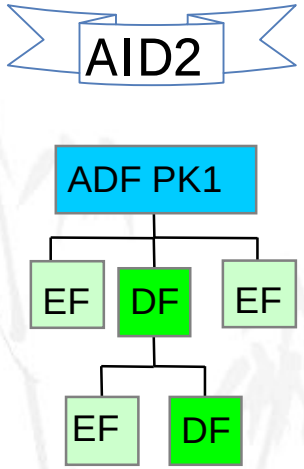
ü包含 appli.文件系统

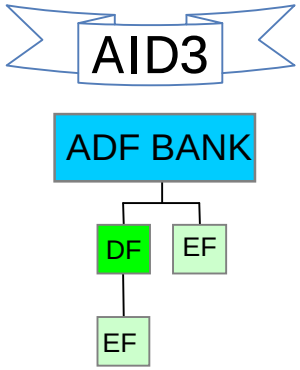
ü从MF文件系统中分离而来

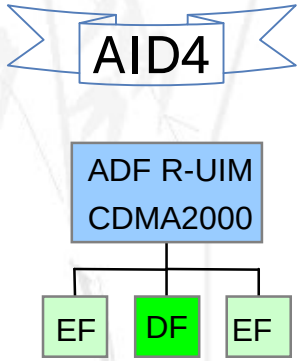
ü通过标识符AID选择

EF DIR：

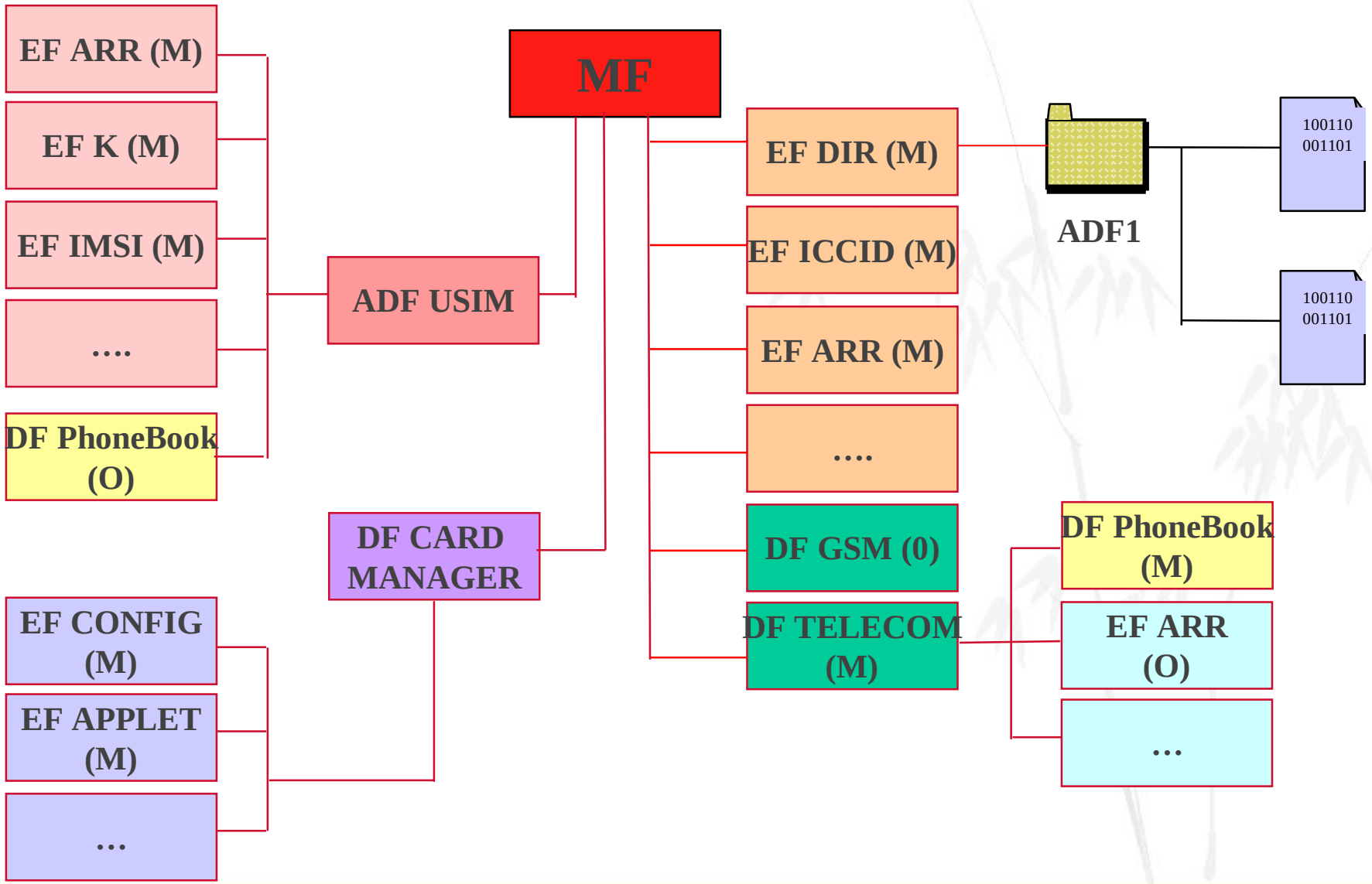
ü包含AID列表







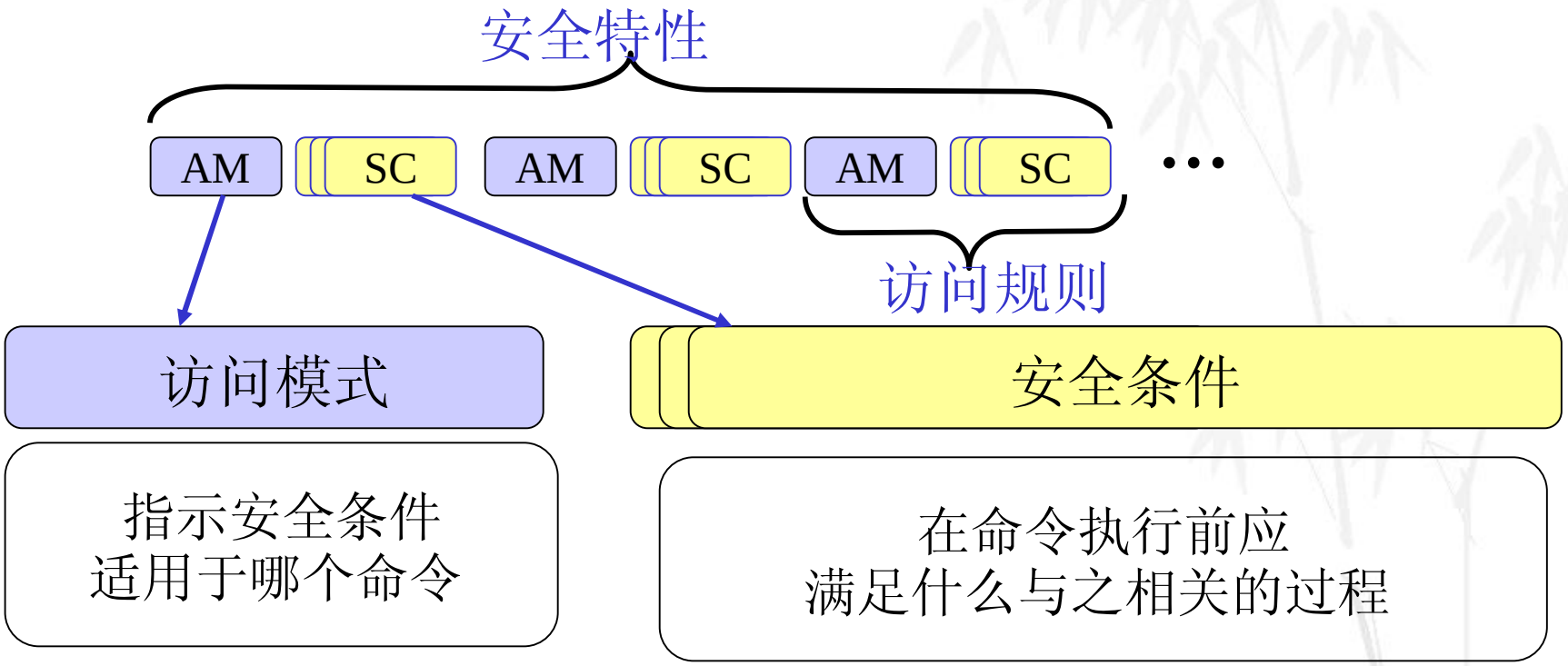
UICC 文件系统（3）



UICC安全特性

- 访问条件主要基于安全特性实现

每个EF，DF都有其相应的安全特性



UICC PIN 系统

Ø通用PIN：专门用于多应用卡，允许几个应用共享一个公共的PIN。

Ø应用PIN：允许访问UICC上的任何文件。

Ø本地PIN：使用本地密钥查询的PIN。可以用来保护当前DF之下的文件或当前ADF下的所有文件。

内容

- 概述
- UICC/USIM简介
- PLMN选择
- 电话簿
- USIM中的鉴权过程
- SIM/USIM互操作
- USAT简介

PLMN选择的原则

- 终端在PLMN自动选择模式下，开机或从无覆盖区恢复时，搜索PLMN；
- 规定终端按照一定的优先级选择**PLMN**（**RPLMN**、HPLMN列表、UPLMN列表、OPLMN列表中的PLMN+RAT的次序）
- 终端在漫游状态时，要周期性地搜索优先级更高的PLMN +RAT（优先级列表中与VPLMN的MNC相同的PLMN）；
- 无线接入技术包括UTRAN（WCDMA/TD-SCDMA)、GSM、GSM COMPACT等

PLMN＋ACT优先级

- 运营商在HPLMN和OPLMN列表中写入本网PLMN号＋ACT，以及漫游网络的PLMN号**+ACT**；
- 用户在UPLMN列表中对不同的网络和无线接入技术进行优先级排序。
- 终端按照PLMN列表中规定的**PLMN**和＋**ACT**的优先级，进行**PLMN**选择。

内容

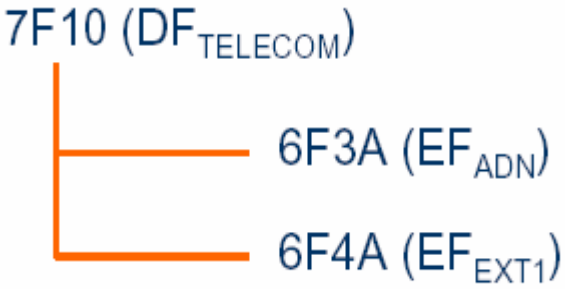
- 概述
- UICC/USIM简介
- PLMN选择
- 电话簿
- USIM中的鉴权过程
- SIM/USIM互操作
- USAT简介

电话簿

- 目前GSM中的电话簿功能
- 3G中的电话簿
- 应用专用和公共电话簿
- 电话簿同步

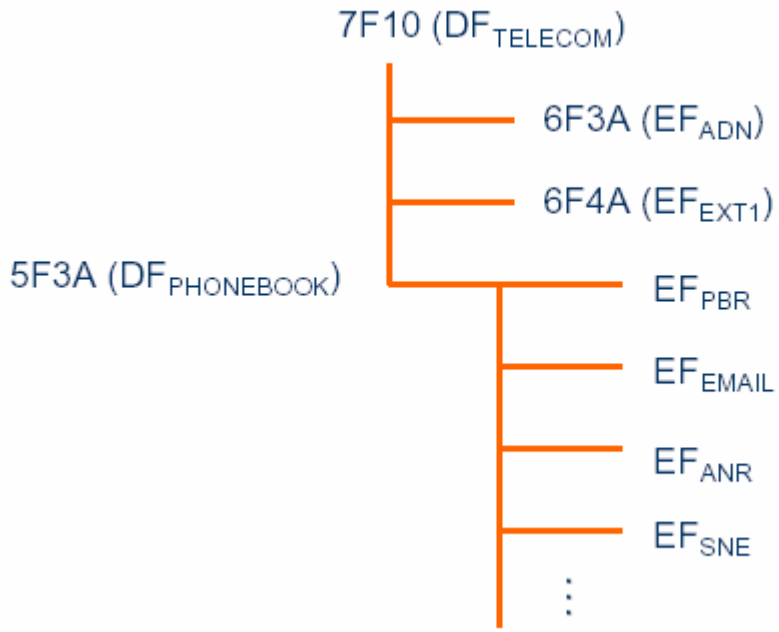
GSM中的电话簿

- 最多有AND、EXT1两个文件



3G中的电话簿

- 采用更加复杂的电话簿结构，从而可以存储更多内容。
- 分为应用专用电话簿和公共电话簿



应用专用和公共电话簿

- 把应用专用电话簿定义在ADF USIM（7FF0）中

（只有3G终端才可以调用）

- 把公共电话簿定义在DF TELECOM（7F10）中，可用于2G和3G终端

电话簿同步

- 当一个电话簿记录被GSM手机修改或删除时，在EF PBC中加入标记。
- 在UICC卡插入3G手机中时，记录被更新。

内容

- 概述
- UICC/USIM简介
- 电话簿
- USIM中的鉴权过程
- SIM/USIM互操作
- USAT简介

鉴权密钥协商（AKA)

- **2G AKA**

  服务网络对ICC鉴权并生成密钥Kc

  适用网络：

  除了BSS之外，其他网元（ICC,ME,VLR/SGSN,HLR/AUC)中必须至少有一个是2G的。

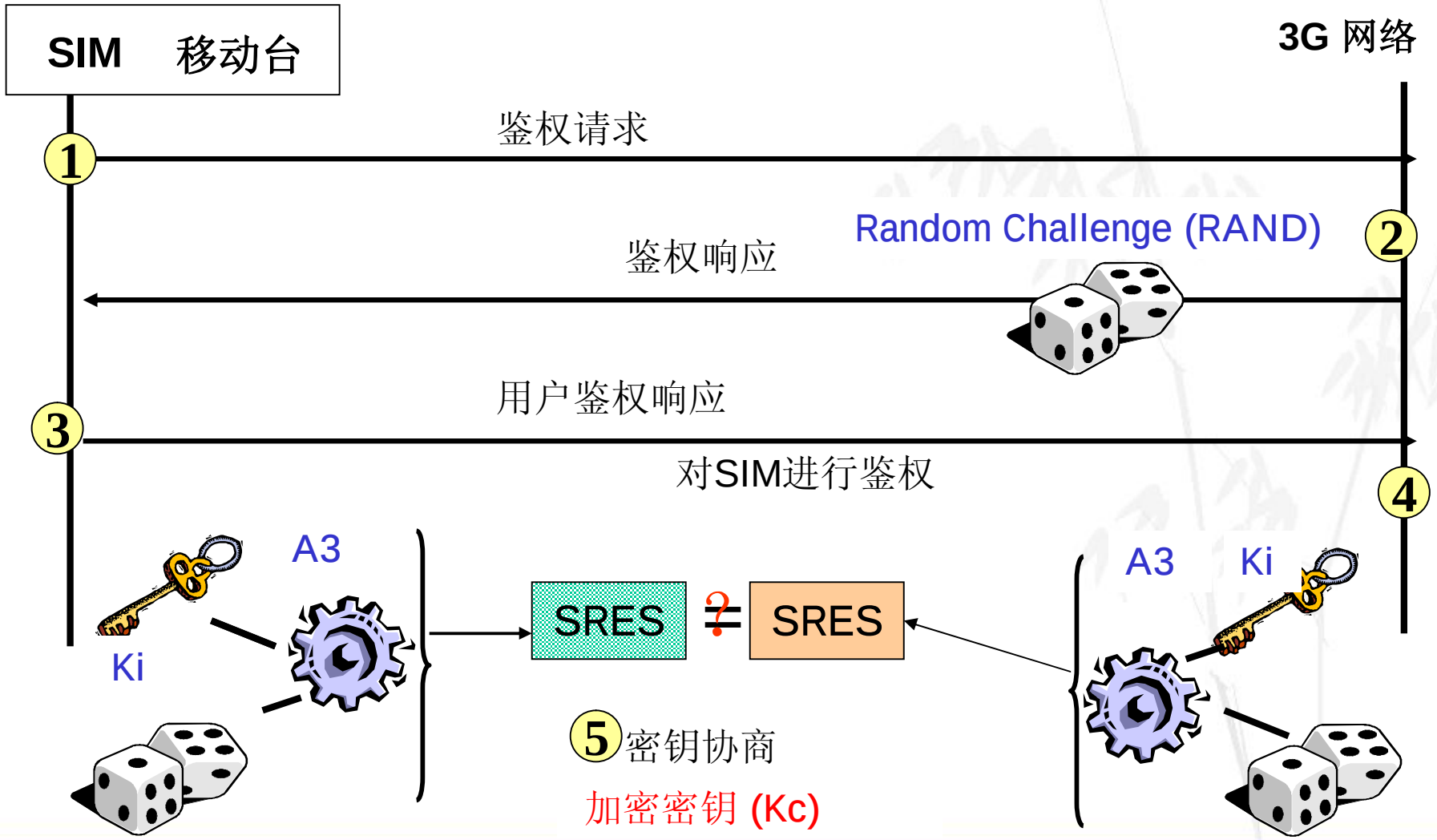
- **3G AKA**

  服务网络和ICC之间的互相鉴权并生成加密密钥（CK）和完整性保护密钥（IK）。

  适用网络：

  除了BSS之外，其他网元都必须是3G的。

2G鉴权和密钥协商



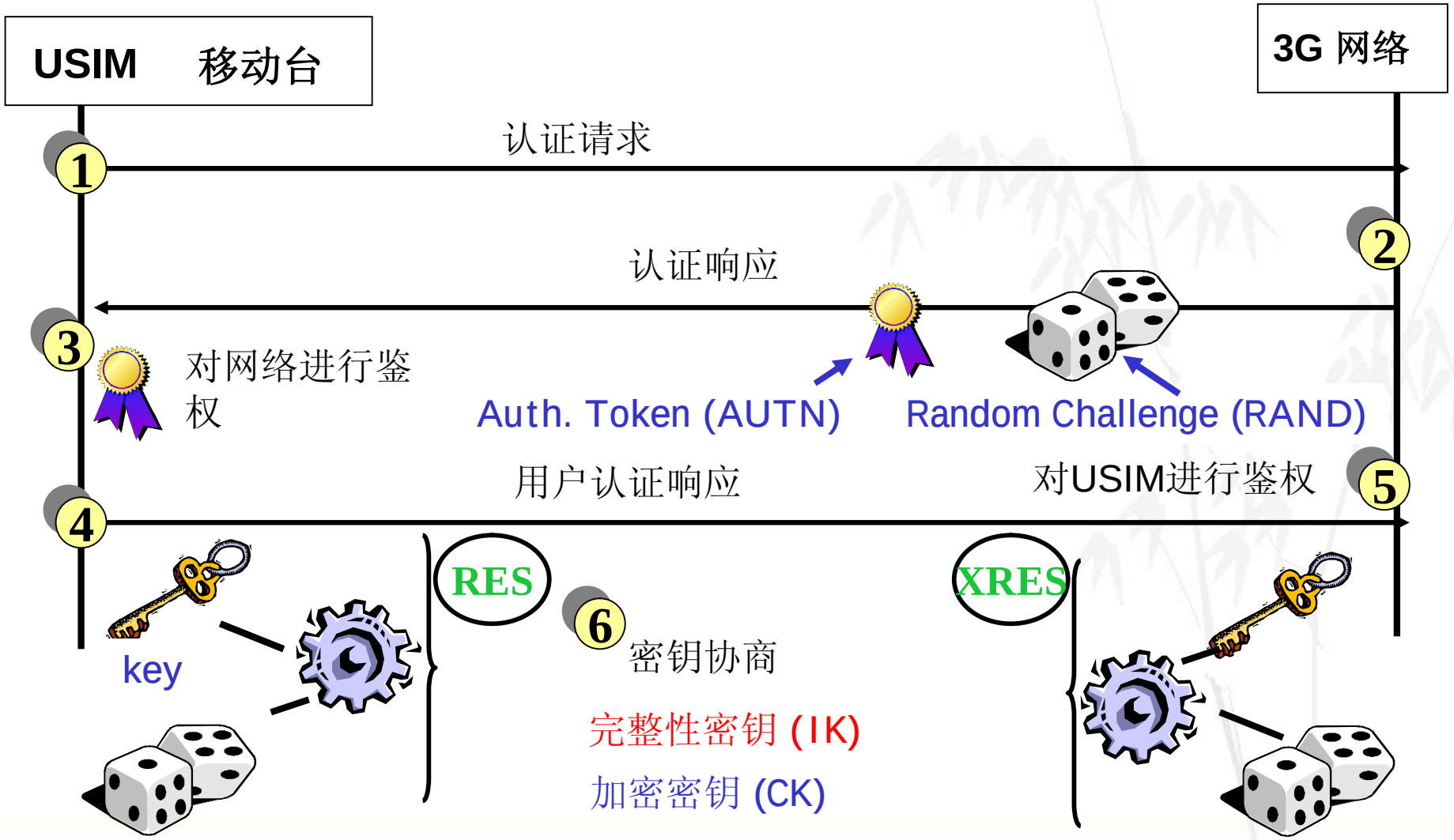
3G 安全特性

- 鉴权
  - 网络对用户的鉴权
  - 用户对网络的鉴权
- 加密
  - 用户标识 (IMSI，位置，业务)
  - 用户语音和数据
- 完整性保护
  - 信令数据

3G安全机制

- 相互认证
- 计算完整性密钥 IK
- 计算加密密钥CK

3G鉴权和密钥协商



3G鉴权参数

- **3G鉴权使用3个参数：**

鉴权标记 (AUTN)　16B

USIM使用其对网络进行鉴权

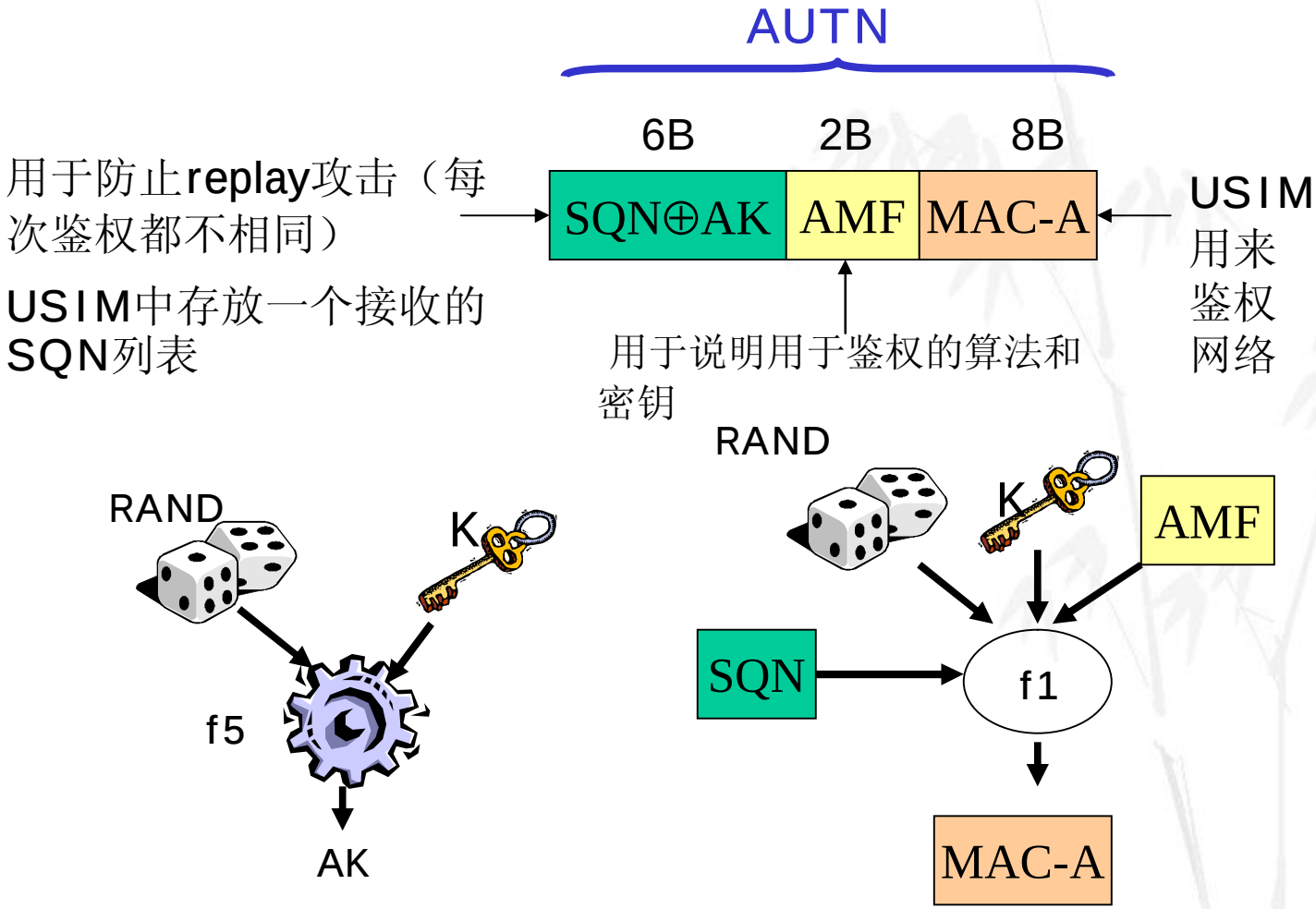
随机数 (RAND)　16B

网络发送该随机数用于对USIM进行鉴权

Secret key (K)　16B

卡和网络侧共享的密钥

鉴权标记（AUTN）



USIM认证网络（1）

USIM 从网络侧收到:

RAND

AUTN

USIM完成两次不同的检查:

MAC-A

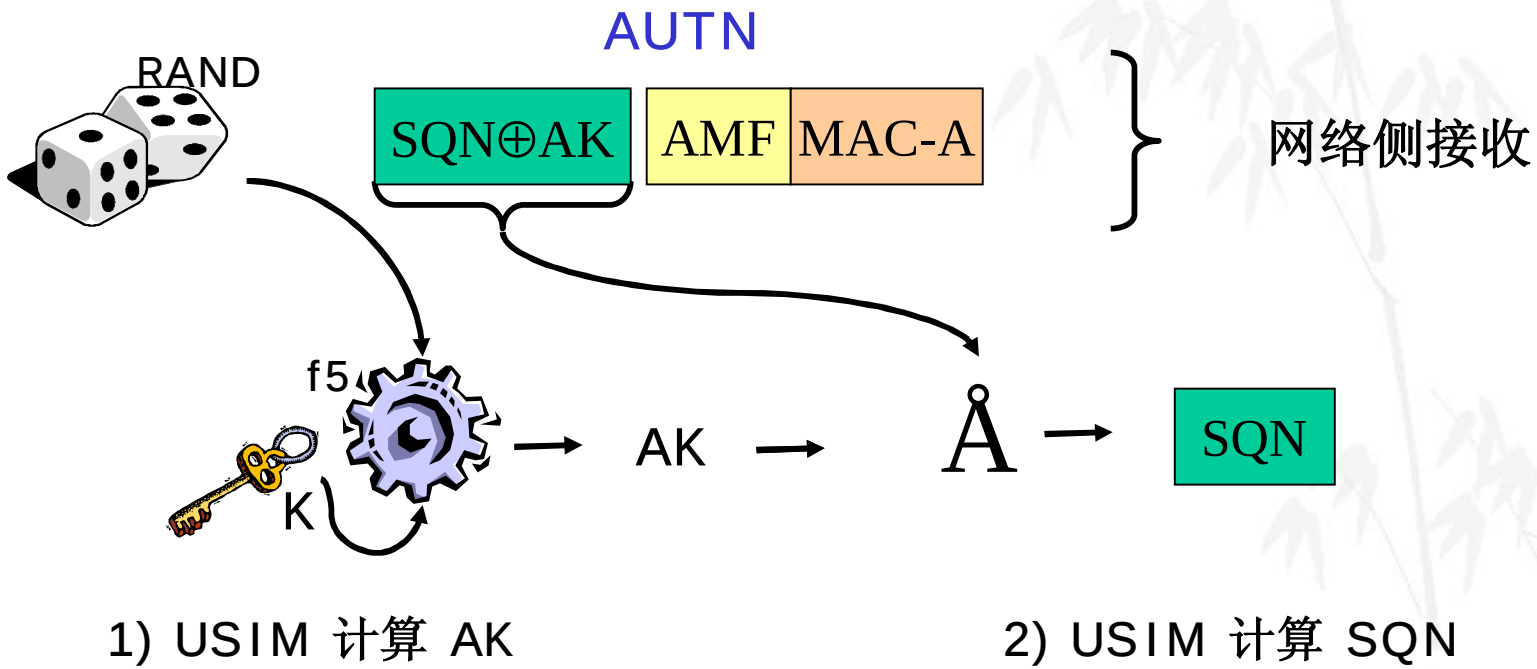
- 鉴权检查
  - 用以认证网络

- 同步检查

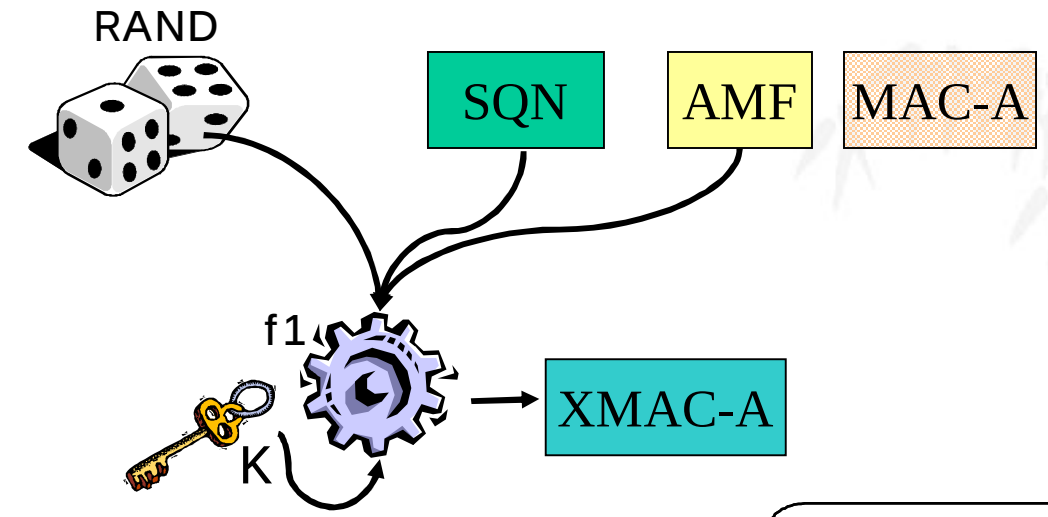
SQN⊕AK

- 用以验证AUTN是"新鲜的"
- 用以预防replay攻击

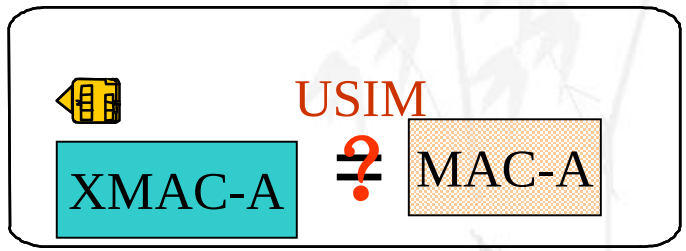
USIM认证网络（2）



USIM认证网络（3）



3) USIM 计算 XMAC-A

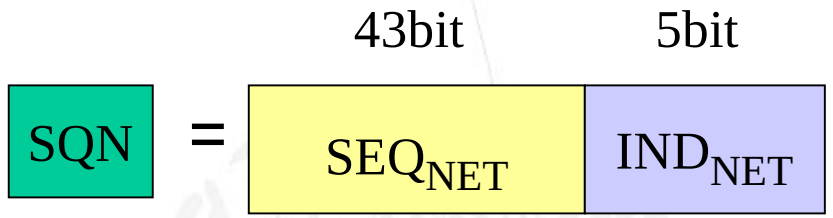


4) USIM 验证 MAC-A

USIM侧的同步检测（1）

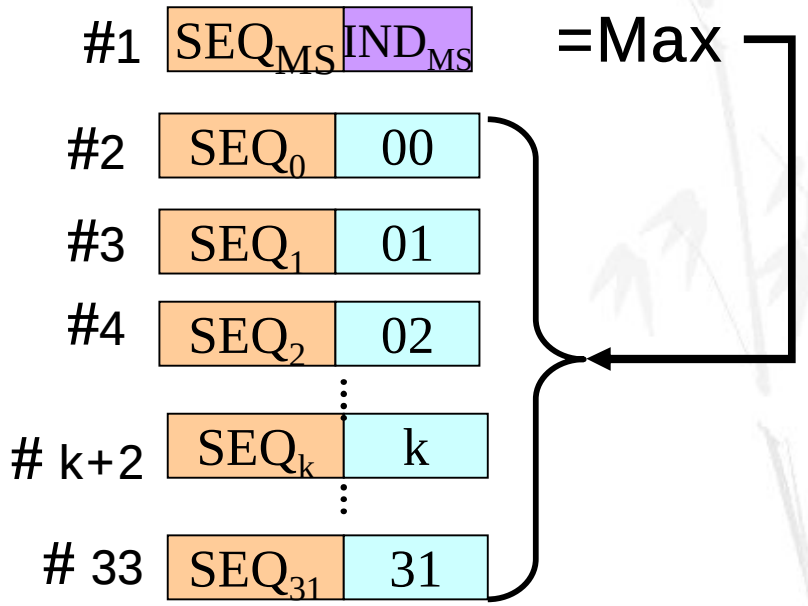
AUC中：

- 存储为指定用户生成的最近的**SQN**
- 分配一个新的索引***IND***用来生成下一个 ***SQN***



USIM中：

在EF SQN文件中存储最近收到的32个(认可的) SQN

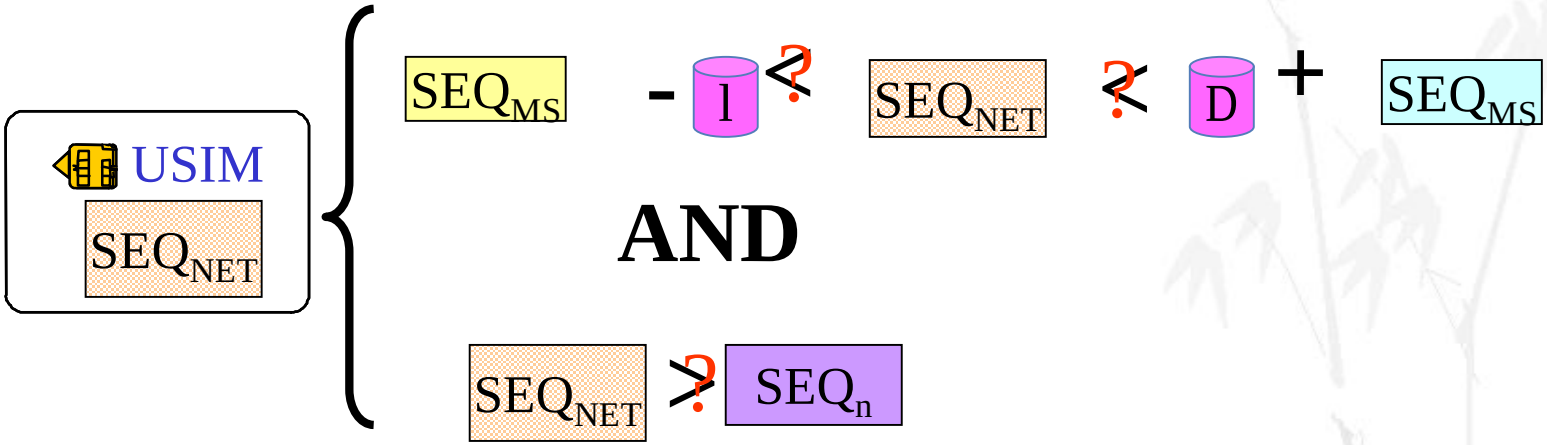


USIM侧的同步检测（2）

1) USIM 从网络侧接收 SQN

2) USIM 用"n"选择相应的SQN

3) USIM 执行同步检测



注：$\Delta=2^{\alpha}$ $\lambda=2^{\beta}$ α, β 在 文件EF AUTHPARAM 中定义

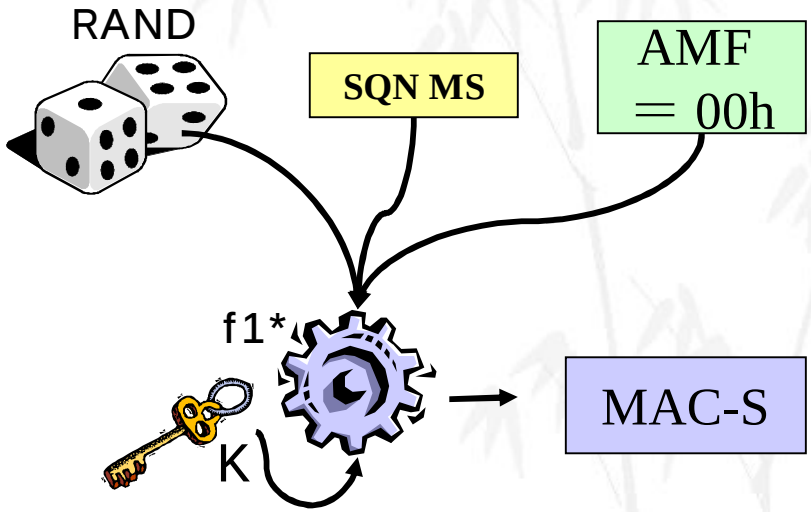
USIM侧的同步检测（3）

若同步检测失败，USIM把当前的SQN_{MS}值发送给网络以便重新进行同步。

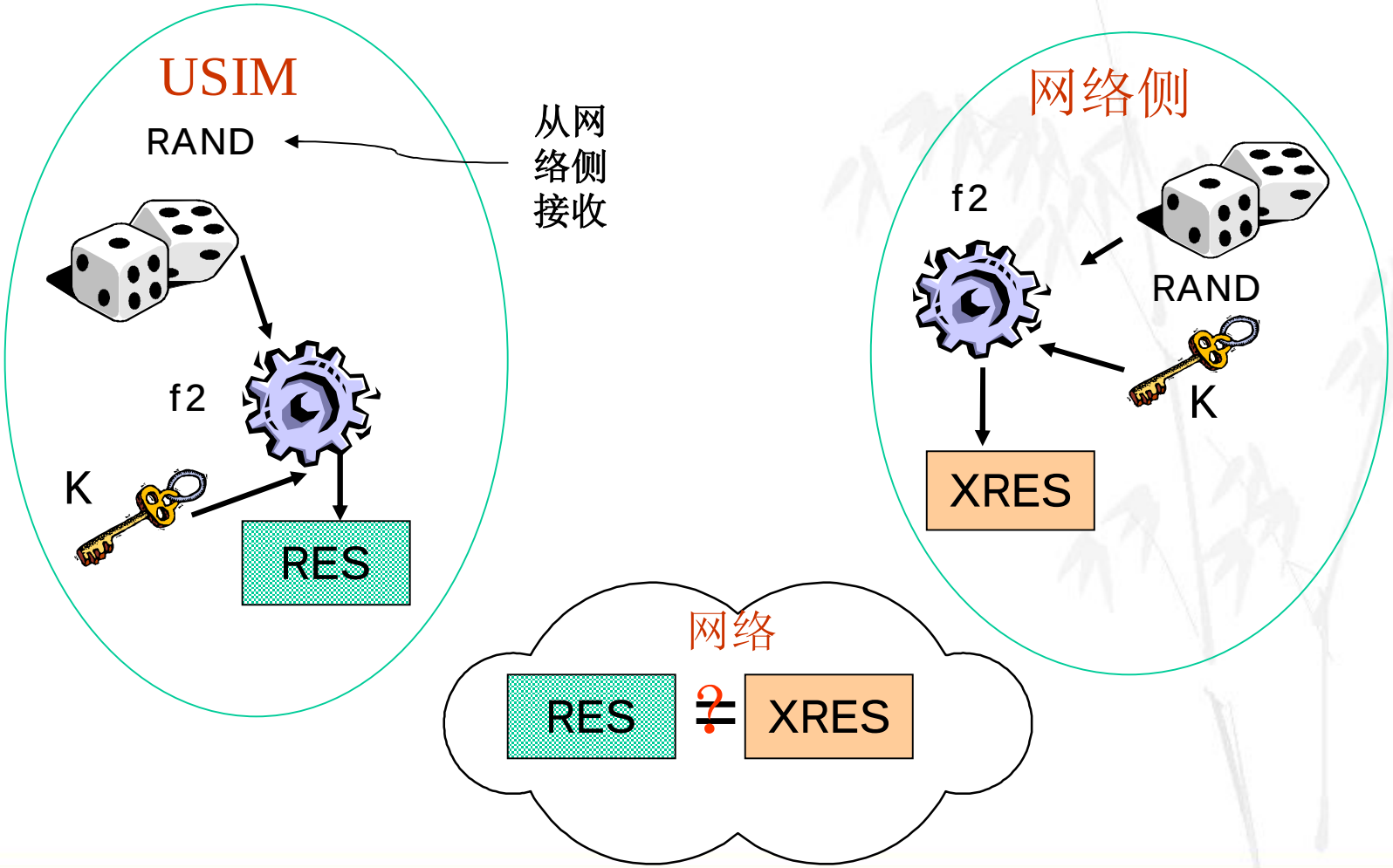
AUTS

SQN_{MS} ⊕AK	MAC-S

存储在USIM中的SQN_{MS}和AK异或

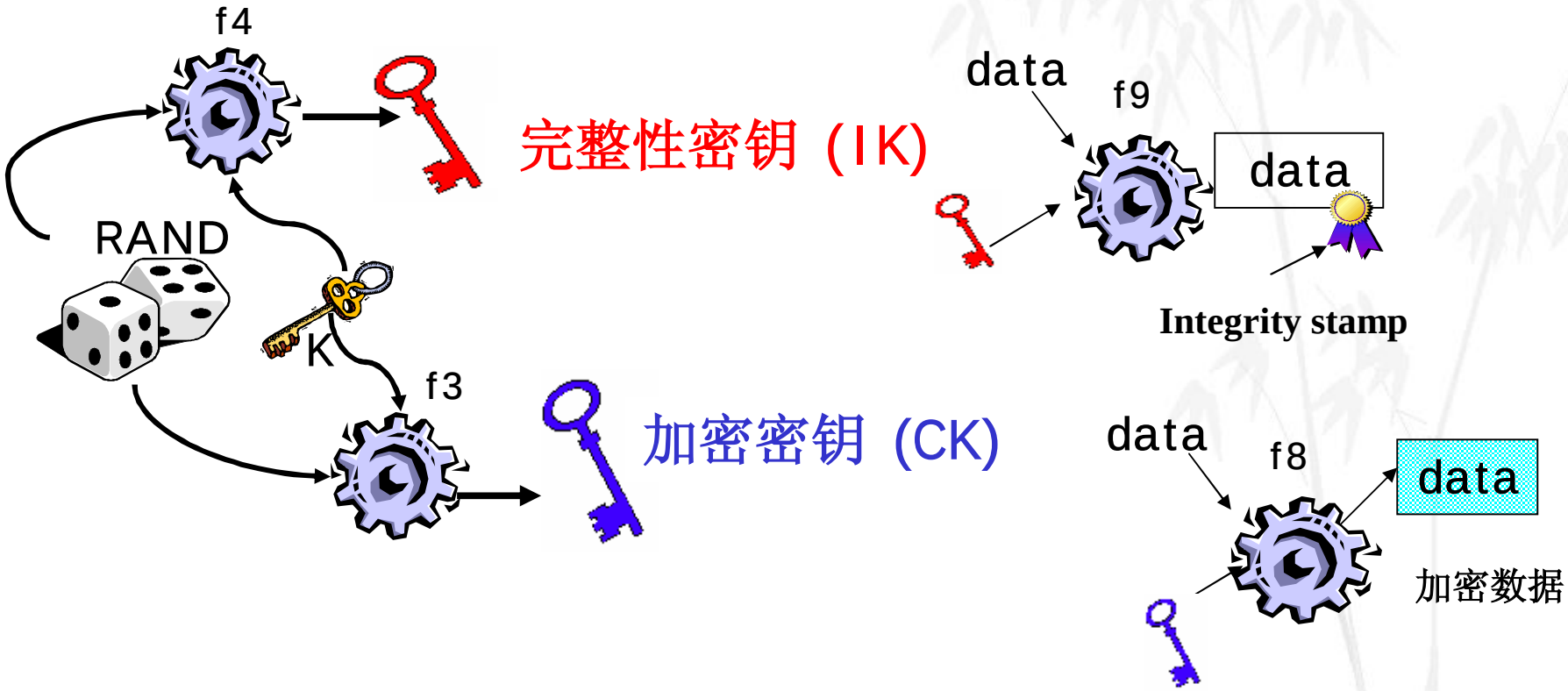


网络对USIM的鉴权



密钥协商

成功鉴权后，USIM和网络共享一组计算出的密钥



3G 安全函数

- **AKA 安全函数**
  - 不是标准的，但可以满足一系列需求
  - 3G 标准算法(f1,f2,f3,f4,f5)
    - § 基于AES (Advanced Encryption Standard)
    - § 可被运营商个性化
- **用于完整性和加密保护的算法(f8,f9)**
  - 标准的
  - 基于 “Kasumi” 算法

内容

- 概述
- UICC/USIM简介
- PLMN选择
- 电话簿
- USIM中的鉴权过程
- SIM/USIM互操作
- USAT简介

SIM/USIM互操作

- 同一UICC上的SIM/USIM应用互操作
- 2G/3G 终端 与SIM/USIM
- 混合网络中的鉴权过程

同一UICC上的SIM/USIM应用互操作

- 不能同时激活也不能互相切换，不存在直接的互操作。
- 一些文件对SIM和USIM应用是相同的，可以共享。
- 可以共享参数以便于激活双模用户或节约资源损耗，有以下几种选择：

——$IMSI_{GSM}$!= $IMSI_{USIM}$, Ki != K

——$IMSI_{GSM}$!= $IMSI_{USIM}$, Ki = K

——$IMSI_{GSM}$ = $IMSI_{USIM}$, Ki = K

2G/3G终端与SIM/USIM（1）

- **2G网络**
  - ——2G终端＋SIM
  - ——2G终端＋UICC(SIM）
  - ——3G双模终端＋UICC(SIM）
  - ——3G双模终端＋SIM

- **3G网络**
  - ——3G终端＋USIM
  - ——3G终端＋SIM
  - ——3G终端＋UICC(USIM)

2G/3G 终端 与SIM/USIM（2）

- 典型的混合网络

1. **2G BSS+2G VLR/SGSN+3G HLR/AUC**

（在不同阶段引入3G技术时最常见的一种网络）

——3G双模终端＋3G UICC(SIM)

——3G双模终端＋SIM

——2G终端＋ 3G UICC(SIM)

——2G终端＋ SIM

2. **2G BSS+3G VLR/SGSN+3G HLR/AUC**

（3G网络发展初期，现存的2G BSS还没有完全被3G技术取代）

——3G双模终端+ 3G UICC(SIM)

——3G双模终端+ SIM

——2G终端＋ 3G UICC(SIM)

——2G终端＋ SIM

混合网络中的鉴权过程举例

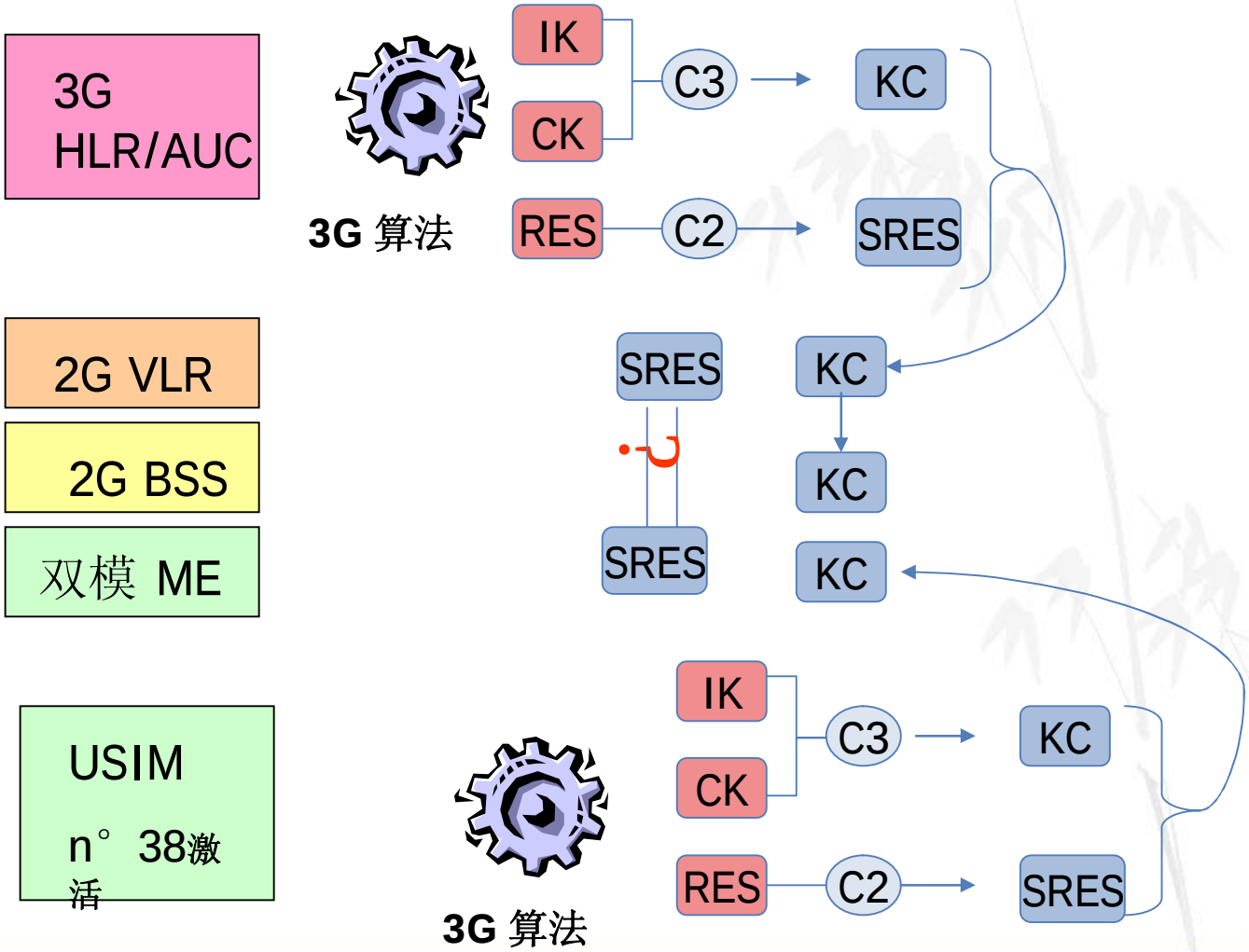
- 2G BSS+2G VLR/SGSN+3G HLR/AUC中的鉴权过程

  3G用户漫游到2G网络中

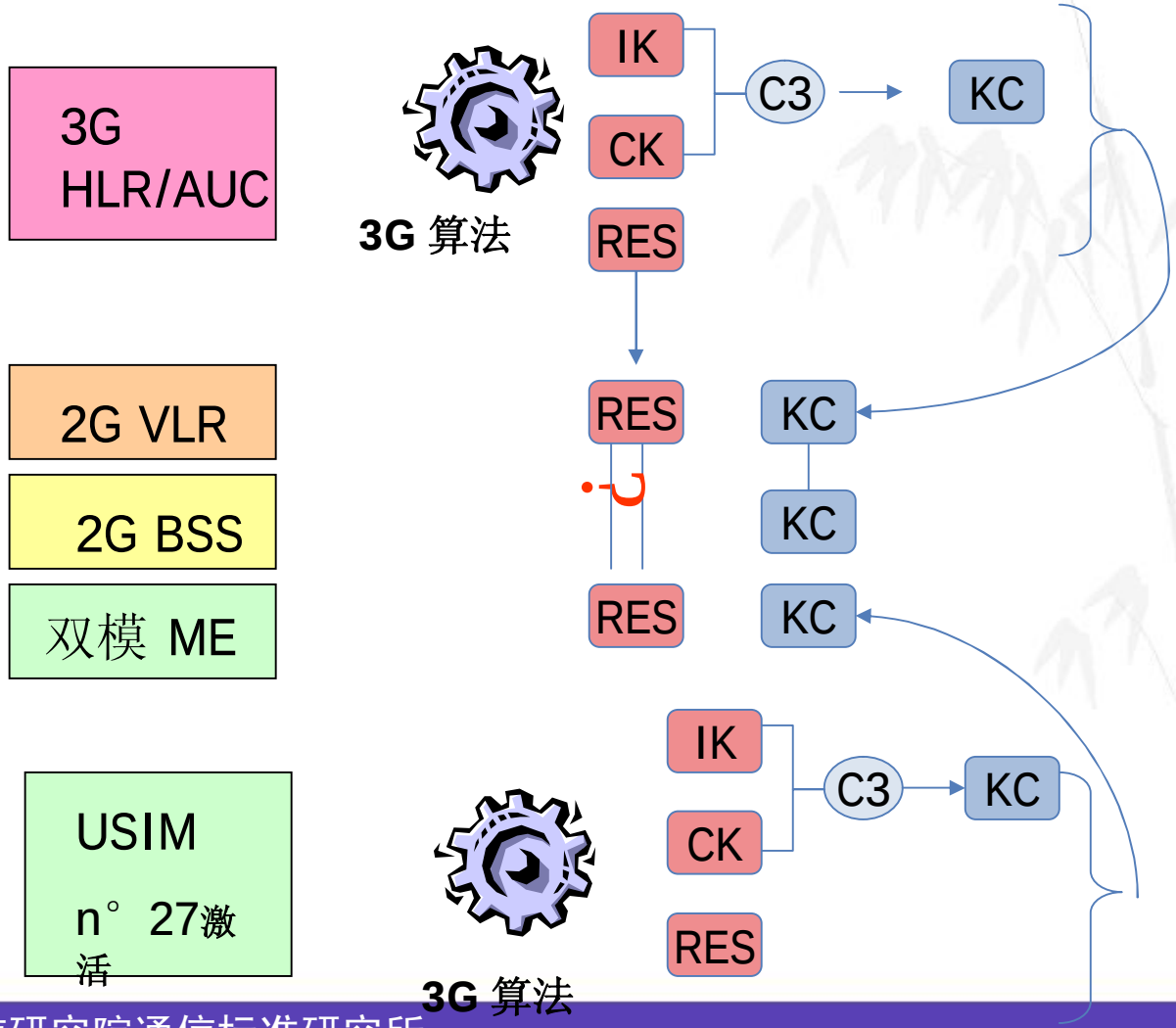
- 2G BSS+3GVLR/SGSN+3G HLR/AUC中的鉴权过程

  3G用户漫游到2G RAN

3G用户漫游到2G网络中



3G用户漫游到2G RAN中

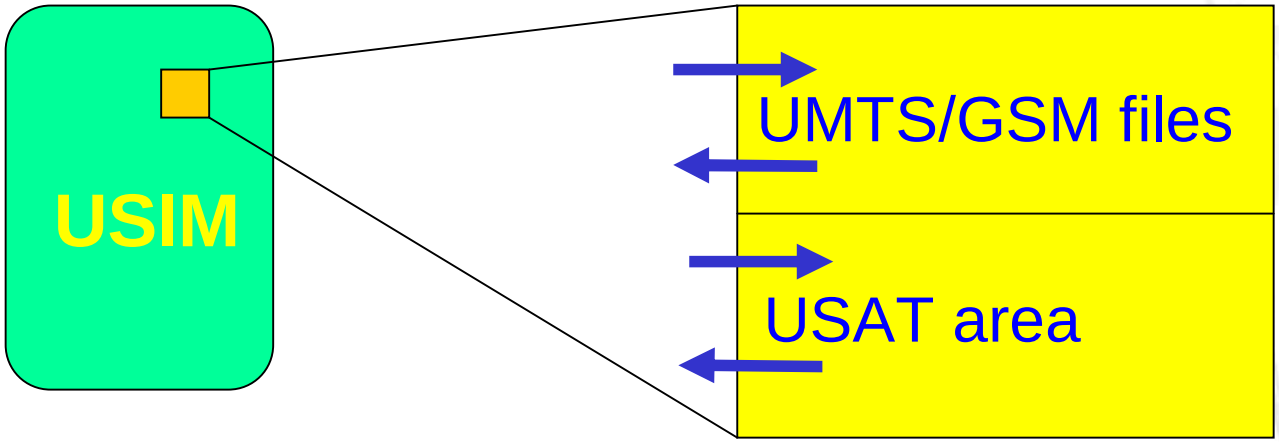


内容

- 概述
- UICC/USIM简介
- PLMN选择
- 电话簿
- USIM中的鉴权过程
- SIM/USIM互操作
- USAT简介

USAT 概述

- 物理实现位于**USIM**
- 逻辑上是独立的功能
  - 并不是UMTS/GSM文件结构的一部分
- 在**USIM-ME**接口定义了特定的工具箱命令



USAT与ME之间的接口

USAT与ME之间主要定义了“主动激活” (proactive) 的功能－由USIM卡要求ME进行特定的动作，以便与用户建立和保持交互的对话，或与网络进行通信。而ME应通知SIM卡是否执行了该命令。

－在ME上显示USIM提供的文本；
－根据USIM卡的指示，建立与特定号码间的数据呼叫，采用特定的承载能力和优先级
－提供对于呼叫的控制能力；
－发起MO SMS，其内容由USIM发送；
－向ME提供位置信息；
－在移动设备中建立新的菜单；
－SIM控制采用音频设施播送信号音

USAT功能的主要过程

- 终端的PROFILE下载过程
- 主动式UICC会话过程
- Envelope命令过程

终端的PROFILE下载过程

通过Profile 下载机制，终端可以告诉UICC它的能力。

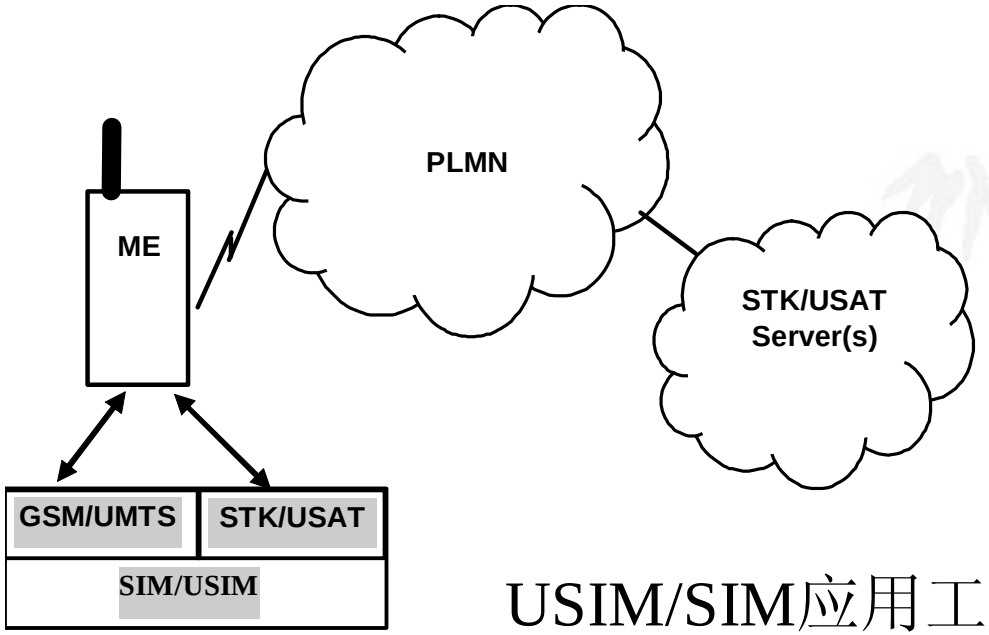
主动式UICC会话过程

- 通过主动式UICC会话机制，使得UICC能够主动发送指令给终端，要求终端执行某些操作。常见的指令如：
  - DISPLAY TEXT
  - GET INKEY/ INPUT
  - PLAY TONE
  - SET UP MENU
  - SELECT ITEM
  - SEND SHORT MESSAGE/SS/USSD
  - SET UP CALL
  - PROVIDE LOCAL INFORMATION
  - SET UP EVENT LIST
  - SET UP IDLE MODE TEXT
  - OPEN /CLOSE CHANNEL
  - …….

Envelope命令过程

- 数据下载
  - ENVELOPE(SMS-PP DOWNLOAD)
  - ENVELOPE (CELL BROADCAST DOWNLOAD)
- 菜单选择
  - ENVELOPE（Menu Selection）
- **USIM控制的呼叫**
  - ENVELOPE (CALL CONTROL)
- **USIM控制的终端发送短消息**
  - ENVELOPE (MO SHORT MESSAGE CONTROL)
- 计时器超时
  - ENVELOPE(Timer Expiration)
- 事件下载
  - ENVELOPE(Event download)

USAT的业务实现方式



USIM/SIM应用工具箱(USAT/STK)

－手机终端

－(U)SIM卡

（SIM厂商与运营者合作）

－STK服务器

－STK与SIM、STK与网络间接口

USAT应用举例

- 数据备份 (电话本, SMS,…)
- 应用(Java) & 菜单下载
- 产品升级
- …

USAT与网络的接口协议

- **BIP允许USIM与终端以及远端的网络服务器（OTA）之间建立透明的数据通道。**

- 主要指令：

Open channel 、Close channel、 Send data 、 Receive data、 Channel status 、Service Search 、 Get service information 、 Declare service等

- 主要事件：

Data available 、 Get status、Local connection 等

谢谢大家！