内部资料
请勿外传
不得复印

第二届

国外通信保密现状研讨会

会议录

四川省电子学会通信信息专业委员会

一九八七年十月

目　录

TeleTrusT——基于RSA公开密钥密码体制电子签名实例

龚奇敏　黄月江

（电子工业部第三十研究所）

Tele TrusT（可信电信）是Trustworthy Telematic Transactions的英文缩写。意为：可信的远程电信自动流交易（事务处理）。这是一个国际科研项目的名称，参与这项研究的有遍布欧洲的国有和私人的科研机构和组织。这个研究项目的目标是促成对如何应用及实施电子签名形成世界范围内的一致性意见。

今年4月可信电信西德工作组组长B·Sttuif先生访问了我国，给我们介绍了可信电信这个科研项目在西德进展的情况及他们今后的设想。这里我们向同行们简单介绍一下共同感兴趣的内容。

一、可信电信的应用模型

图1为可信电信的应用模型。这是一个倒金字塔型的结构。它以RSA体制作为基

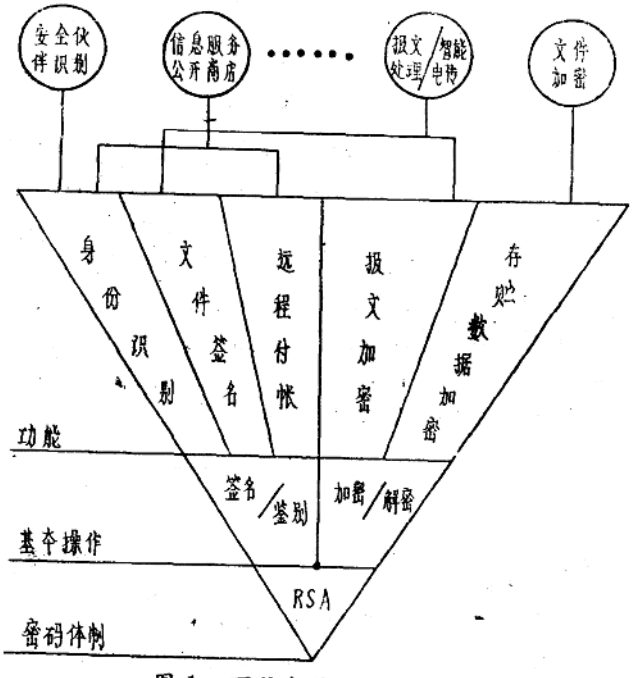


图1　可信电信应用模型

础，在此基础上，可有两种基本操作：签名／鉴别和加密／解密。在这两个基本操作的基础上，又可开发出多种功能，而这些功能的组合，便可构成各种具体的应用。

由于第二次世界大战遗留下来的某种历史原因，在西德发展民用保密事业可能会产生问题。故西德可信电信工作组的工作着重放在数字签名方面。他们认为公开密钥算法最为适宜于公开的环境以及数字签名。因此他们采用目前国际上公认的最可靠的公开密钥算法——RSA体制。在这次讲座中，Struif先生还提到了Fiat／和Shamir在CryPto 86国际密码学会议上提出的Fiat／Shamir公开密钥密码体制。这种算法的基础是在不知道模数n的因子分解条件下（n是两个大素数的乘积），求模平方根的困难性。其加解密用到的模乘法的数量只是RSA算法的4%。详情参见CryPto 86文献汇编。目前还未见到对这种体制的评价。在可信电信中还没有使用这种体制。

在公开密钥环境中，为了有效且安全地实现各种具体应用，需要一种称之为证书的东西，它是由提供各种服务的机构（签证当局）签发的。图2是可信电信的证书模型。

发放证书当局	邮电局	银　行	机构X	组织Y	？ Z
发放证书的目的	用户身份	信用保证	权限	成员关系	？
确认的信息	可区别的姓名	最大存款量	第 n 级	第m 组	？
其　它	公开密钥				
	失效期				

图 2　可信电信的证书模型

首先，它可以保证用户使用的密钥对的正确性。也就是说用户在最初使用密钥前，必须将其公开密钥向签证当局登记。签证当局用它的密钥对用户的密钥进行签名。这样才能保证用户密钥的合法性。发放证书的当局不同，确认的信息也不同。例如，邮电局发放证书的目的是鉴别用户的身份，则证书确认的是可资区别的姓名。而银行发放证书的目的是保证其用户的信用程度，则证书确认他的可能就是用户的存款量等等。

其次，可以保证用户所具有的某种特征，如权限、成员关系等。

在有的时候，可能需要几个证书。此时就可将发放证书的当局分级。这种方式称为“可信链”（Chain of trust）。图3是可信链的结构：

M	SIGu	PK^0	SIG_{CA1}	PK_{CA1}	SIG_{CA2}	PK_{CA2}	…
用户消息	用户签名	用户公开密钥	当局1签名	当局1公开密钥	当局2签名	当局2公开密钥	

图 3　可信链结构

这时候，须假定，分层结构中最高当局的公开密钥为接收者已知，或可采用查号服务的方式查到。

证书上，还可有些别的信息。如用户的公开密钥及失效日期等等。

二、数字签名方案中的散列函数

TeleTrusT中采用的数字签名方案如图4所示，它是以RSA公开密钥体制为基础的。

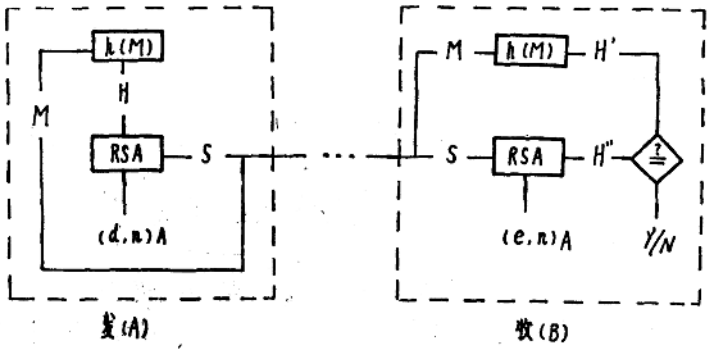


图 4　TeleTrusT签名方案

对于一个实用的RSA体制，必须考虑：模数n的大小；两个大素数P和q应满足的条件，例如本方案中确定P（q）有下列性质：$P = 2P' + 1$，$P' = 2P'' + 1$，其中P、P'、P''均是素数，q也有同样的性质；如何产生这样的P和q（包括如何检验一个随机产生的大数是素数，在多大程度上保证它是素数）；公开密钥和秘密密钥如何选择以及密钥管理等等一系列问题，对这些问题本文就不一一介绍了。本方案中，RSA的输入不是报文M，而是M的一个函域值h（M），h称为散列函数（hashing function）。我们将扼要介绍一下散列函数h的作用、构造和性质。

大家知道，RSA体制除了有许多优点因而被选作签名算法外，突出的缺点是它的运算速度慢。一旦要签名的报文较长时，直接对长报文运算是不足取的，所以引入散列函数h，以便通过它，将任意长报文压缩到长度等于模数n的长度$h_n = \log_2 n$（当然h的运算速度必须远远超过RSA的运算速度）。当需要将签名保存第三方时，为了不泄露明文内容，先将原报文经就使得由签名只能恢复报文经散列函数h后的结果，而不是报文本身。这样，散列函数过h变换后再由RSA签名，h应当是一个单向函数，即由H = h）M）计算M是极其困难的

TeleTrusT 中采用的散列函数是这样的

$$H = (\cdots(B_1^2 + B_2)^2 + \cdots + B_i)^2 \mod n$$

具体的运算过程如下：

设发送者要签名的报文为M，其长度为L。个字节，RSA公开密钥的模数为n，其长度为$L_n = \log_2 n$个比特，规定n是两个素数的乘积，且其长度是16的倍数，因此$L_n = 16m$，即$m = Ln/16$。

第 1 步：格式化

1.1　加报头——在M的前头加上L_1个字节的报文描述字，它包括报文标识符ID和L_0长度字段。

1.2　右填充——在报文M的后面加上L_2个字节的二进制数 0，以便得到总长度$L = m \cdot j$个字节的新的报文M_1。见图 5。

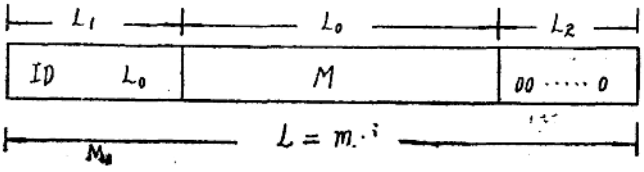


图 5　待签名报文的格式

第 2 步：字节扩充

将第 1 步得到的M_1分成j组X_1，…，X_j，每组含m个字节。

对每一组X_i，先划分成半字节串b_1，b_2，…b_{2m}，然后在每个半字节的左边加四个二进制数 1 即十六进制F，（B_i：1111，X_i：F），得到2m个字节Fb_1，Fb_2，…Fb_{2m}的新组B_i（i = 1，…j），见图 6。

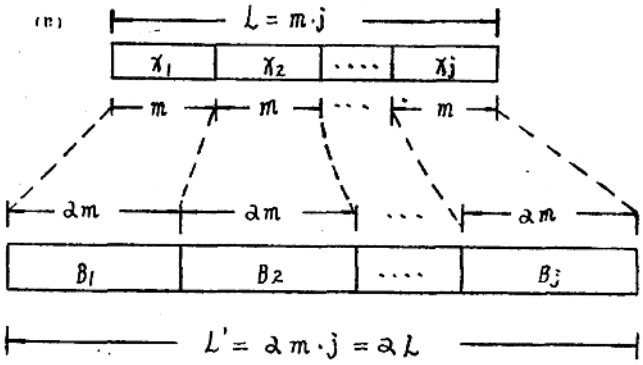


图 6　字节扩充

第 3 步：压缩

对这一字节串进行运算。

$$H_1 = B_1^2 \mod n$$

$$H_i = (H_{i-1} \oplus B_i)^2 \mod n \qquad i = 2, \cdots, j$$

这里每个B_i包含2m个字节，所以它的二进制长度为：$2m \times 8 = 16 \cdot m = n$。

第 4 步：规格化

若$H_j < [n/2]$，则$H = H_j + [n/2]$，否则$H = H_j$

H即是最后结果。

这个散列函数有着一些较好的性质（不加推导地列出几条）：

（1）.函数h是一个单向函数，由H=h(M)推出M是不可能的。

（2）.函数h不具有RSA体制的那种同态特性，对于RSA体制，乘积的签名等于签名的乘积，即D(x·y)=D(x)·D(y)，但h(x·y)≠h(x)·h(y)，所以D(h(x·y))≠D(h(x))·D(h(y))。

（3）.由已知M和H=h(M)，寻找一个新的报文M′，使得h(M′)=h(M)是计算上不可行的。

（4）.H是整个报文M的函数，而不是逐组计算的，因而也是不可分割的。

（5）.H对报文M的变化是十分敏感的，即H稍有变化，就会引起M的很大变化。

三、 可信电信应用1：安全伙伴识别

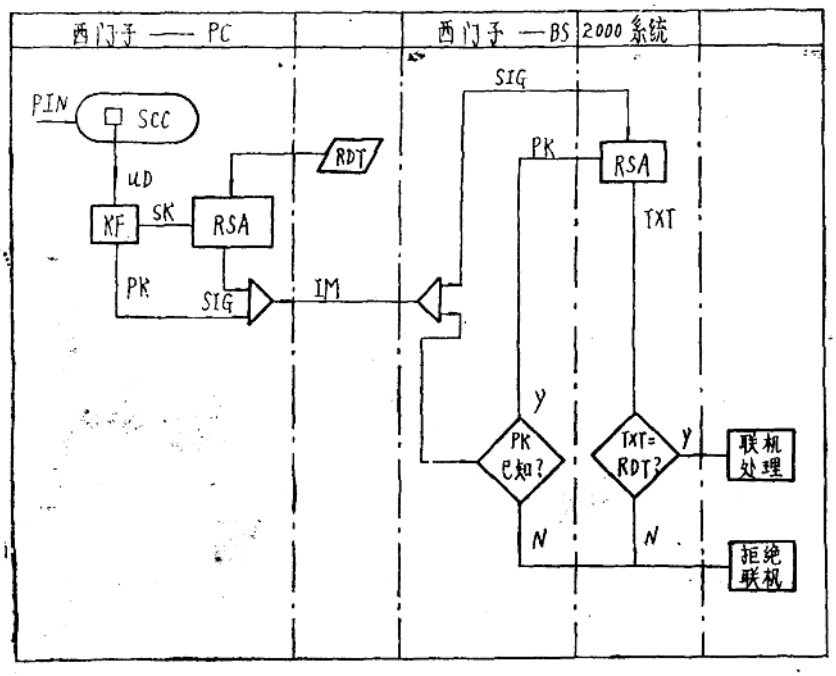
在西方，由于操作人员失误，雇用人员不诚实或发泄私愤，以及自然灾害，如火灾，水灾等给信息处理造成的损害仍然占据着相当大的比例。但由外部攻击及无事生非者骚扰而造成的损失也在逐年递增。

在西方世界中，尤其令人惊奇的是，居然有人专门出版有指导无事生非者对连接在网络上的信息系统进行攻击的书籍。也有的厂家销售供连续拨号攻击使用的连续拨号机。

因此，为了抵御外来威胁，严格鉴别进入信息系统的人员或终端在未来开放系统的应用中是十分必要的。图7是对进入西门子——BS2000巨型机系统的终端进行安全识别的例子。

在此例中，使用了芯片卡，芯片卡中存有用户的有关数据及秘密密钥和公开密钥。芯片卡是由计算中心发给用户的。因此，秘密密钥分发实际上是由系统管理者进行的。用户的终端是带有芯片卡读入设备的终端。用于产生鉴别信息的RSA算法是放在芯片卡，还是放在终端中，要视芯片卡的智能程度而定。算法当然最好是在芯片卡中，因为这样一来秘密密钥暴露的危险性就很小，但目前的水平还做不到这一步。

在进入系统前，用户将芯片卡插入读入设备，并输入个人身份PIN（是在芯片卡上，还是在读入设备中输入同样视芯片卡的智能程度而定），由个人身份号及用户数据导出秘密密钥和公开密钥。在接到联机请求后，主机产生一个随机数，并连同日期和时刻一起发送给终端。在终端中用RSA算法及秘密密钥对RDT进行签名。签名后的鉴别信息连同用户公开密钥一起发送到主机。主机收到鉴别信息后，首先判断此公开密钥是否已在主机中登记。若没有，则拒绝终端与主机联机。若已登记注册，则利用公开密钥对SIG信号解密。得到TXT，将TXT与RDT比较。相等则同意联机，进入联机处理过程。若不相等，则拒绝联机。实际当中，使用了散列函数，但框图中未列出。另外，主机对签名送回的RDT有一定的时间范围要求，若超过这个范围，同样拒绝联机，以防止重发攻击（即：非合法截取签名信息后用它来进入主机系统）。



PIN = 个人身份　KF = 密钥功能　SCC = 西门子计算机卡　SK = 秘密密钥
UD = 用户数据　PK = 公开密钥　RSA = RSA密码算法（未列入散列函数）
SIG = 数字签名　IM = 鉴别信息　TXT = 报文　RDT = 随机数、日期、时间

图 7　安全伙伴识别一例

四、信息服务公开商店（OSIS）

在西方国家中，国家及私人机构建立了形形色色的数据库，如象西德医药文件及信息研究所就提供有医药、文献、癌症等二十多种数据库，存有二千万个文件，这些数据库都连接到公共网络上。许多信息服务是需要付钱的。如何能使用户快速、方便地得到信息服务，并且使付钱的手续简化。是OSIS项目要解决的问题，OSIS实际上是将远程访问与电子记帐手段结合起来实现的。下面将OSIS的简要工作过程叙述如下：

在西德公共网中，邮电部提供了一个公共数据库。此数据库除提供许多免费的服务外。还将许多存贮页面租给提供各种各样收费数据库的机构，以存贮关于专门数据库的说明、内容等等。用户要访问某个专门的数据库，可以先访问公共数据库。从公共数据库可以知道专门数据库的信息，一但选择某个数据库后，公共数据库发送具体数据库的进入页面（Geteway Page）。进入页面是在视频终端上显示的一个彩色图案，上面有专门数据库的标志等等。当用户在终端确认这个进入页面后，就在终端与专门数据库的计算机间建立了一条连接。在可信电信模型中（仅是软件模型，还未用硬件实现），OSIS是这样工作的：当确认电信可信OSIS进入页面后，（带芯片卡读入设备的）终端便提醒用户

键入个人身份号。当个人身份号被接收后，终端屏幕上显示主菜单。所列的内容有：是否连接到公开信息商店的信息服务，是否显示已签发的电子支票等。当选择连接到公开信息商店信息服务后，则终端屏幕上显示出子菜单。可以在上面选择要访问的具体信息库，一旦选择一个具体的信息库，则此信息库送回欢迎信息。并发来一个电信可信的会话标识符，会话标识符由随机数、日期、访问时刻构成。提示用户对其签名。由于用户的秘密密钥是存贮在芯片卡上的，只要芯片卡已插入读入终端的设备，用户只须按一个功能键，便可由终端中的软件完成签名过程，并将签名发往信息服务的提供者。在发往信息服务提供者的签名中，除用户签名外（表示用户愿当为此服务付帐）。还有用户所在银行的证书（表明此用户能够付帐）。证书有下列部份：

a.要证明的信息（即用户的公开密钥。还可加上失效日期等）。b.银行的签名（保证银行是知道这个用户的，其用户的密钥对是合法的）。c.银行标识(银行的公开密钥，假定这个公开密钥是为信息服务提供者已知的)。当签名信息发往信息服务提供者并被认可后，就可以获取具体的信息了。当信息服务结束后，信息服务提供者便要求用户签署一张电子支票。电子支票的一部份要求用户填入，如象金额等。

电信可信的电子支票有下列部份：

a）.接收者、 b）.付款目的、 c）.付帐要求的期限、 d）.货币类型及数量、 e）.支票签发的日期、 f）.支票的序号、 g）.帐号、 h）.用户公开密钥、 i）.银行的公开密钥、 j）.用户的签名（对a、b、c、d、e、f进行的签名）、 k）.银行签名（对g、h部分进行的签名）。

从上面可以看到，银行只对固定部分签名，而用户则对可变部份签名。用户用电子支票付款不能超过银行确定的一个限度。另外，每当用户签署一个电子支票后，存贮在芯片卡（在电信可信项目中，称之为通行证）中存款量便会减少，当减少到一定值时，芯片卡必须由银行重新装入存贮内容才能使用。

当电子支票被信息服务提供者确认后，用户终端便会看到再见信息，及使用的计算机时间等。最后，用户与信息服务提供者间的连接便拆除了。

OSIS一个极粗略的软件结构如图 6 所示。

从用户的观点看，OSIS的益处有：

（ 1 ）可以避免获得用户的身份及通行证的合同过程。

（ 2 ）可及时且自然地访问数据库。

（ 3 ）可以象在商店里买商品一样购买信息。

（ 4 ）可实现不具名的访问。

（ 5 ）直接由电子支票付账可避免对手写签名付账的繁琐要求。

从信息服务提供者的观点来看，OSIS的益处有：

（ 1 ）不需要提供者与用户之间的合同过程。

（ 2 ）记账变得更为简便。

（ 3 ）账单可得到立即地支付。

（ 4 ）可争取到新的用户。

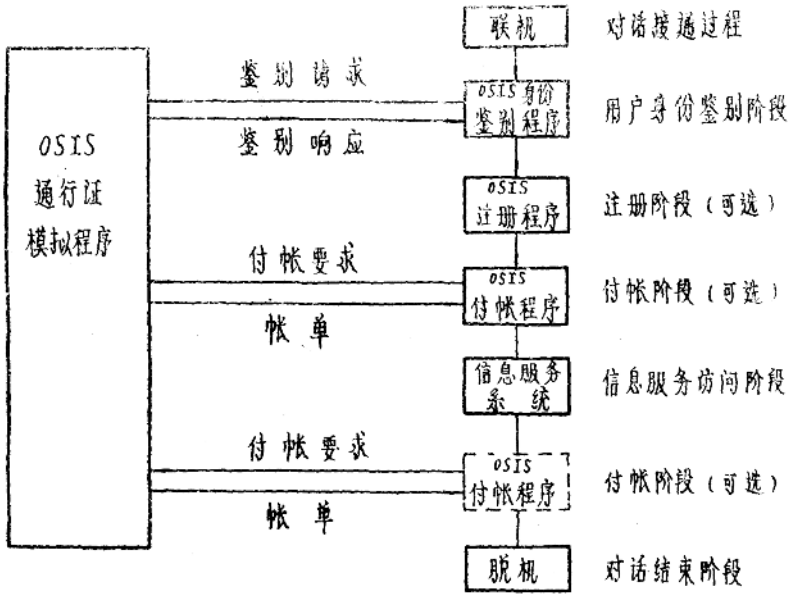


图 6　OSIS—软件结构略图

从银行的观点来看，OSIS的益处有：

（1）可为现代信息社会提供更先进的金融手段。

（2）电子支票可自动地进行处理。

（3）可满足安全上的新要求。

五、芯片卡技术

对于生活在西方世界的人来说，现在的世界是一个携带卡片的时代。越来越多的人要携带各式各样的卡片，用于购货、取款及其许许多多别的用途。但常规的卡片已有点过时了。因为我们现在正生活在一个电子时代，这些常规卡片正在被集成电路卡代替。在电信可信的研究项目中，有许多应用都是基于集成电路卡片的。如象OSIS及安全伙伴识别及许多我们在这里还未提到的应用。

根据智能程度分类，芯片卡可分为4类：

（1）简单存贮卡：只有一些存贮的功能。

（2）智能存贮卡：除存贮功能外，还有一些专门的安全逻辑。

（3）多功能处理器卡：卡中集成有处理器，ROM及RAM等，适用于各种不同的应用。

（4）超智能卡：在多功能处理器卡的基础上，还有键盘及显示器等。

决定芯片卡类型的还有多种因素：如芯片卡是单个还是多个芯片；处理器的比特长度，指令集、时钟频率、RAM及ROM大小；PROM的类型(是EEPROM还是EPROM)；

芯片在芯片卡上的位置，及芯片的接口（是有触点的，还是无触点的），这些都是选用芯片卡的因素。

从我们上面讲述的内容来看，高级的芯片卡实际上就是集成度更高的微机。因此，芯片卡有多大用途，是可以想象到的，它将在工厂自动化、家庭自动化、办公室自动化、医药卫生、交通、商业、金融、消闲、安全等领域中发挥越来越重要的作用。

随着我国集成电路工业以及通信事业的发展，芯片卡也应当自然地增入到我们的日常生活中来。

由于芯片卡的某些特性，如象便于携带、安全性好、有存贮及计算能力，它在安全领域中必将发挥越来越重要的作用。因此，我们应当注意芯片卡发展的动向，在可能的情况下，还可做一些开发应用的工作。

结束语

TeleTrusT是一项遍及西欧各先进国家的国际系统工程，也是利用公开密钥体制（RSA）来实现电子数字签名的一个大型实例，该系统已完成了部分应用功能的开发，证明方案是可行的，我们在这里只介绍了方案的基本思想及部分应用功能。

虽然由于我国目前具体条件的限制（例如还没有全国的X.25网），要研究和开发这样的系统工程还有很长一段路要走，但随着我国四化建设的进展，迟早要开展类似的研究和工程实现工作的。因此，利用各种渠道了解和吸收外国有益的东西，并在国内同行间交流，以促进我国的研究和开发工作，是会有益处的。

参考文献（略）

Fiat／Shamir密码体制简介

方关宝

（电子工业部第三十研究所）

现代世界是信息爆炸的时代。用手写签名词实信息的可信性已经远远不能满足实时、快速和信息量多的要求。1976年，赫尔曼提出了公开密钥体制，克服了大量分配密钥的困难。很快就有人提出把它用于数字签名来代替手写签名。这样的签名可以在信道上传送，适应了现代信息社会的要求。适用于公开密钥体制的各种方案，大都适用于数字签名。可惜至今公开提出的各种公开密钥体制只有RSA没被破译其它几乎都被破译了。许多国家都准备用RSA作为数字签名。但RSA模乘法量太大，速度太慢，针对这一情况，1986年Fiat和Shamir提出了一个新的体制，它甚至不要秘密密钥。1987年4月法国专家Stolif来华讲学，介绍了这一方案，并提供了显示演示软盘。现将此方案简述如下，以便大家研究。

此方案既不要秘密密钥，也不要公开密钥，代替密钥的是有关用户身份、名字、账号等一切信息的一个信息串I。

它还假设存在着一个可信赖的中心。这个中心验明了用户的实际身份以后，分发给用以签名的秘密密钥。而中心本身既不产生签名，也不验证签名。

中心在分发密钥以前它要选择一个模数n和一个随机函数f，f取值范围为[0，n]，而n为二个质数p、q之积。它和RSA不同的是p、q只有中心知道，所有的用户都不知道，且他们都用同一n。

这个密码体制使用的模数乘积只有RSA的4%，因而速度大大增快。

当合格的用户使用秘密密钥时，必须给中心一个含有用户所有信息的信息（I）。这时，中心执行下列步骤：

（1）对比较小的j，计算V（j）=f（I，j）

（2）选择K个，使得V（j）为平方剩余的j值，（对模n而言为平方剩余），并计算模n条件下，$1/v_{(j)}$的数最小平方根S（j）。

（3）秘密密钥就是K个S（j）的值。

现在，用户就可以用秘密密钥对消息签名了。

A对消息m的签名：

我们假设这个用户是A，它要对消息m签名，并发送给B：

（1）A选t个随机数r（1），r（2），…，r（t），且$0 \leqslant r(i) \leqslant n$，

计算$x(i)=[r(i)]^2 \pmod n$

（2）计算f（m，x（1），x（2），…，x（t）），并取其前K×t个比特，作为二进制矩阵e（i，j），$1 \leqslant i \leqslant t$，$1 \leqslant j \leqslant k$。

（3）计算t个，y（i）值　$1 \leqslant i \leqslant t$

$$y(i) = r(i) * s^*(j) \mod n$$

$s^*(j)$为矩阵e（i，j）中，元素e（i，j）= 1的所有的S（j）之积。

（4）A将I、K、矩阵e（i，j）以及t个y（i）值发送给B，以作验证签名的凭据。当然消息m也必发送，这里讲的是数字签名，只强调签名数据。

B对签名的验证：

（1）根据A给的K个j，计算v（j）

$$v(j) = f(i, j)$$

（2）计算t个z值

$$Z(i) = [y(i)]^2 \times V^*(j) \mod n$$

这儿$V^*(j)$是e矩阵中e（i，j）= 1的元素的所有V（j）之积。

（3）计算f（m，Z（1），Z（2），…，z（t）之值，并取其前t＊K个比特与A发来的e矩阵对照如完全吻合，则签名有效。

结束语

由上述方案可知，要破译这种密钥与破译RSA一样，需要分解n，所以二者保密程度是一样的，但本方案用了平方剩余，模数乘法大量减少，为RSA的4％，另外它又不必公开成秘密密钥，所以更为方便。它的缺点是有一个可信赖的中心，一但中心失去信誉，此方案也无法实施。

参考文献（略）

战术抗干扰(未加密)安全通信系统

洪福明

(成都电讯工程学院)

内容提要 现代战术通信要求抗干扰和不泄密。本文介绍一种不加特殊密码的通信系统，它能满足安全通信的种种要求：抗干扰、低截获、保密以及抑制干扰的能力，最适合于未来战术通信移动网的特点。

一、引言

现代通信技术及其对战争带来的影响是众所周知的。在第二次世界大战中，无线电通信、密码技术和情报侦察对战争结果起了相当大的作用，由于盟国的密码技术明显的占领优势以及德、日、法西斯的情报遭到破译，在很多战役中，例如诺曼底登陆战、中途岛之战等，美国将军们在战争取得胜利后的结论是："我们靠的就是它"，"它"指的是破译敌方电报和成功的密码。

从通信侦察发展到通信对抗是现代通信发展的必然趋势。扰敌和破坏敌方的通信联络，使敌方的指挥失灵，作战混乱，促使通信对抗对现代战争的胜败所起的影响越来越大，相反，由于密码技术的不断发展，破译越来越困难，即使得到破译，在现代闪电式战争中，也往往失去时效。因此，仍然沿袭情报侦察为主，通信干扰为辅的战术是行不通的，而且侦破也极端困难了。未来的通信对抗应该是以通信干扰为主体，通信的侦察和测向只是作为通信干扰的支援措施使用罢了。然而，这也确是密码技术的发展得到成功之处。

由此可知，在现代军事战术通信中，仅仅研究保密通信是不够的。通信的基本要求将是抗干扰和不泄密，这就是安全通信(Secure Communication)所要解决的问题。安全通信是通信反对抗的重要内容。由于通信对抗技术的发展，对通信安全的要求也将日益增长和迫切。对于无线电通信，由于电波辐射是发散的，易于被人截获。接收和干扰、安全措施更为重要，而以无线电通信为主的战术通信，其情况更是如此。

(1)在所传递的信号上有抗干扰措施；

(2)信号隐蔽，具有抗截获能力；

(3)信息具有保密措施；

（4）.对干扰信号具有抑制能力。

目前在美、苏两国以及其它先进国家出现并形成的指挥、控制、通信（C^3）系统，是一种包括多种通信手段和电子装备的系统。它在计算机的控制与管理下，将陆、海、空各军兵种等军事机构、部队和装备，通过各种通信手段组成的统一网络。这些通信装备中一些主要的移动设备都是扩频／跳频／天线零位自动调节能力的战术电台。由这些通信装备构成的系统将起到安全通信的目的。

本文将讨论一种跳频／直接序列扩频（FH／DS）通信系统，它在不采取密码系统的条件下，具有安全通信所要求的各种能力。预期它将是未来战争中极为重要的战术通信装备，这种装备即使未加保密装置，仍然具有一定的保密能力，要进行侦破其通信内容是极为困难的。它的系统方框图如图1所示。

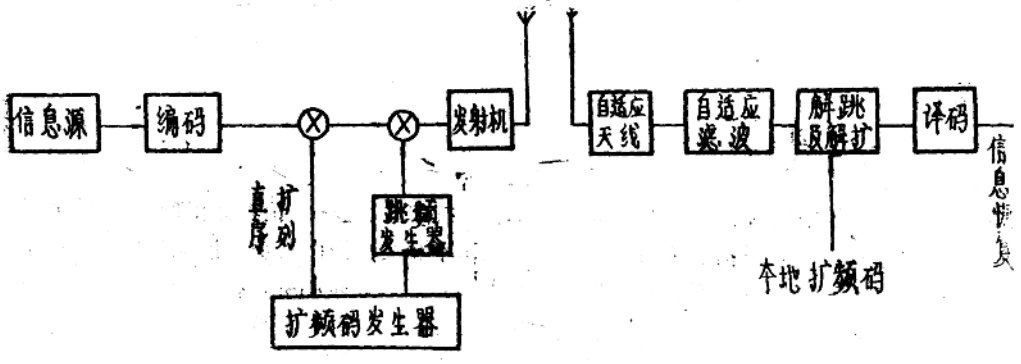


图1　FH／DS通信系统原理方框图

本系统将包括扩频通信系统，扩频编码设备，自适应天线和自适应滤波干扰抑制等部分。

二、扩频通信系统

如图1中所示，扩频通信发送部分具有跳频及直接序列扩频混合调制后的数字调制信号，设$S_i(t)$为发送的扩频信号：

$$S_i(t)=\sqrt{2P}\,m(i)\,C(t)\cos(\omega_i t+\Phi_i(t)) \qquad (1)$$

$$i=1,\ 2,\ \cdots\cdots N$$

式中：　P为发射功能；

$M(t)$为原始信息码；

$C(t)$为直接序列扩频码序列；

$\omega_i(t)$为N个跳频频率中在t_i时刻的某一频率，ω_i受跳频指令码控制；

$\Phi_i(t)$为频率ω_i的瞬时相位，$\Phi_i(t)=C(t)\pi$。

在接收端，只要用与发端相同的直扩序列码和跳频指令码进行解扩与解跳形成基带调制码后，再用一般数字解调方法恢复为原始信息信号m（t）。

这一信号在信道上有可能受到除信道白噪声以外的种种干扰，其中有敌方施放的人为干扰如单频等幅正弦干扰，以及通信网内其他扩频信号的干扰等。接收系统对这些干扰具有削弱的能力，即称为抗干扰能力。

由于本系统是跳频和直按序列扩频的混合调制，因此其抗干扰能力也由这两部分组成。衡量扩频系统抗干扰能力的参数是扩频系统处理增益G_P：

$$G_P = \frac{\text{输出信噪比}}{\text{输入信噪比}}$$

这一定义与一般的解调增益是一致的。这一信噪比的改善，在直接序列扩频系统中，是由于从射频带宽到信息带宽之间的交换而导致的，这是符合Shannon定理的基本规律的。一般假设射频带宽是$\left(\frac{\sin x}{x}\right)^2$型的直接序列扩频功率谱的主瓣宽度（PSK或FSK情况都是如此），它等于扩频码速率R_c值的两倍，若信息速率为R_b，则直接序列扩频处理增益G_{DS}为

$$G_{DS} = \frac{2R_c}{R_b} \qquad (2)$$

理论证明，不论对于广义平稳干扰或单频正弦干扰来说，这一结论都是正确的。定性的可以这样来说明，输入干扰信号由于同本地扩频码不相关，因而其功率谱受到扩频码功率谱的卷积而展宽了频谱。而由于有用信号与本地扩频码完全相关，在卷积过程中，将信号能量从扩频码带宽集中到基带信息带宽内，从而提高了输出信噪比。

跳频处理增益的定义和直扩处理增益是一样的，当跳频相邻频率间频谱是不交迭的或是正交而不影响检测时，则跳频处理增益可简单地用下式来计算：

$$G_{FH} = \text{可用的频率数} = N \qquad (3)$$

假设射频带宽为200MHZ，信息速率R_b为10kb／s，扩频码速率为1Mb／s，跳频频率数为200，跳频间隔1MHZ，则系统总处理增益为：

$$G_P = G_{D_s} + G_{FH} = 23 + 23 = 46\text{dB}$$

当系统在这一情况下工作时，若要求系统误频率为10^{-5}，则解调器输出信噪比应为10dB。这样，相关检测器输入端只需保证—36dB就行。一般的通信系统在这样恶劣条件下根本无法工作，这充分显示了扩频系统的优越性。由此可引入另一重要性能参数：干扰容限。用它来表示扩展频谱系统在干扰环境中的生产能力。

干扰容限考虑了一个可用系统输出信噪比的要求，而且涉及了系统内部信噪比损耗，接收机输入端能够承受的干扰比信号高出的分贝（dB）数。

$$M_j = G_P - \left[L_s + \left(\frac{S}{N}\right)_0\right] \quad (\text{dB}) \qquad (4)$$