中国标准出版社第四编辑室　编

信息安全标准汇编

密码技术卷

中国标准出版社

信息安全标准汇编

密码技术卷

中国标准出版社第四编辑室　编

中国标准出版社

北　京

图书在版编目（CIP）数据

信息安全标准汇编. 密码技术卷/中国标准出版社第四编辑室编. —北京：中国标准出版社，2009
ISBN 978-7-5066-5240-7

Ⅰ.信… Ⅱ.中… Ⅲ.①信息系统-安全管理-国家标准-汇编-中国②密码-安全技术-国家标准-汇编-中国 Ⅳ.TP309-65 TN918-65

中国版本图书馆 CIP 数据核字（2009）第 044291 号

中国标准出版社出版发行
北京复兴门外三里河北街 16 号
邮政编码：100045
网址 www.spc.net.cn
电话：68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 10.5 字数 310 千字
2009 年 4 月第一版 2009 年 4 月第一次印刷
*
定价 58.00 元

出 版 说 明

在信息化社会，信息技术飞速发展，随之而来的信息技术的安全问题日益突出，它关系到信息系统的正常运行和健康发展，影响到信息化社会的各个方面，不容忽视。国家标准化管理委员会已制定和发布了一系列信息安全国家标准，为我国信息系统的安全提供了技术支持，为信息安全的监督和管理提供了依据和指导。

为满足广大信息技术人员的需求，方便学习和查阅，我们将信息安全国家标准按照信息安全标准体系收集、分类、汇编成卷，共分为以下5卷：

——基础卷

——信息安全管理卷

——信息安全测评卷

——技术与机制卷

——密码技术卷

其中信息安全测评卷、技术与机制卷根据需要又分为若干分册。

随着信息安全标准体系的完善和标准制修订情况的变化，本套汇编将陆续分卷分册出版。

本卷为密码技术卷，共收入截至2009年2月发布的相关标准7项。

编　　者

2009年2月

目　　录

注：本汇编收集的国家标准的年号在目录中用四位数字表示，国家标准正文部分仍保持原样。

中华人民共和国国家标准

信息处理　数据加密　物理层互操作性要求

GB/T 15278—94

Information processing—Data encipherment—Physical layer interoperability requirements

本标准等效采用国际标准 ISO 9160—1988《信息处理——数据加密——物理层互操作性要求》。

本标准规定了在传送自动数据处理(ADP)信息的远程通信系统中,开放系统互连(OSI)参考模型的物理层采用加密的互操作性和安全性的有关要求。

本标准便于要求密码保护的数据通信设备和系统中使用的数据加密设备互操作的实现。

物理层加密的目的是对抗包括业务分析在内的所有形式的被动攻击。只有在同步操作中才能提供彻底对抗业务分析的保护,这是因为在同步操作中所有比特均可加密,而在异步操作中起始和停止比特不可加密。本标准不提供对物理连接建立的保护。

1　主题内容与适用范围

本标准适用于在数据通信物理层中加密 ADP 信息的系统。

无论数据加密设备(DEE)是作为物理上独立的设备实现,还是作为数据终端设备(DTE)或作为数据电路终接设备(DCE)的一部分实现,本标准均可同等适用。当加密部分集成到 DTE 或 DCE 中时,本标准适用于 DTE 或 DCE 设计中实现本标准要求的那些部分。本标准的互操作性要求是为下述物理接口定义规定的:GB 3454、GB 11592、GB 11593、GB 11599 和 GB 11600。

GB 9387 中描述了物理层。在物理层加密中,所有的 SDU(服务数据单元)通常都被加密。本标准所描述的互操作性要求对全双工方式和半双工方式中的同步操作和异步操作均适用。

本标准的正文规定了适用于使用各种加密算法的要求。附录 B(参考件)举例说明使用一个 64 bit 分组密码算法的附加要求。

本标准规定了同步操作的两种可选方式:延迟选项和立即选项。这两种方式互不兼容。

本标准还规定了对异步操作中断(BREAK)的两种可选动作:A 类和 B 类。这两种动作互不兼容。

2　引用标准

GB 5271.9　数据处理　词汇　09 部分　数据通信	
GB 9387　信息处理系统　开放系统互连　基本参考模型	
GB/T 15277　信息处理　64 bit 分组密码算法的工作方式	
GB 3454 CCITT 建议 V.24	数据终端设备(DTE)和数据电路终接设备(DCE)之间的接口电路定义表
GB 11592 CCITT 建议 X.20	公用数据网上起/止传输业务使用的数据终端设备(DTE)和数据电路终接设备(DCE)间的接口
GB 11593 CCITT 建议 X.21	公用数据网上同步工作的数据终端设备(DTE)和数据电路终接设备(DCE)间的接口

国家技术监督局 1994-12-07 批准　　1995-08-01 实施

GB 11599 CCITT 建议 X. 21bis	与同步 V 系列调制解调器接口的数据终端设备(DTE)在公用数据网上的用法
GB 11600 CCITT 建议 X. 20bis	与同步双工 V 系列调制解调器接口的数据终端设备(DTE)在公用数据网上的用法
GJB 389. 1 CCITT 建议 V. 54	在电话网上进行数据通信的调制解调器的维护和测试　调制解调器用的环路测试设备
ISO 7498—2	信息处理系统　开放系统互连基本参考模型　第 2 部分　安全体系结构

3　术语

3.1　本标准使用 GB 5271. 9 中定义的下列数据通信术语：

物理层　physical layer

数据通信　data communication

数据终端设备(DTE)　data terminal equipment

数据电路终接设备(DCE)　data circuit-terminating equipment

数据电路终接设备/数据终端设备接口　DCE/DTE interface

呼叫建立　call establishment

数据传送　data transfer

测试环路　test loops

串行传输　serial transmission

异步传输　asynchronous transmission

起止式传输　start/stop transmission

起始信号　start signal

停止信号　stop signal

同步传输　synchronous transmission

双工传输　duplex transmission

半双工传输　half duplex transmission

3.2　本标准使用有关标准中定义的下列术语：

服务数据单元(SDU)　service data unit(GB 9387)

物理连接　physical connection(GB 9387)

密文　ciphertext (ISO 7498-2)

明文　plaintext(ISO 7498-2)

初始化值(IV)　initializing valuc(GB/T 15277)

启动变量(SV)　starting variable(GB/T 15277)

4　适用的接口

在 DEE 与 DTE 之间、DEE 与 DCE 之间或 DEE 与 DTE 和 DCE 之间如果有接口，该接口可以是 GB 3454、GB 11592、GB 11593、GB 11599 和 GB 11600 中的一种。本标准涉及通过这些不同的接口以不同方式传送而实现的物理层连接的呼叫建立。既不影响 DEE 操作也不受 DEE 操作影响的控制信号应直接通过 DEE，或在 DEE 处重新驱动。

提供标准 DCE/DTE 接口的 DEE，当它向 DTE 转发如“发送准备好”、“数据设备准备好”或“数据准备好”等信号时，因要求完成其自身的操作，需要延迟这些控制信号。

由 DEE 引起的延迟加上由 DCE 引起的延迟应符合 DTE 所确定的超时要求。DTE 在收到上述相应的控制信号之前不应开始数据传输。

4.1 GB 3454 的接口

对于 GB 3454 的互换电路，DCE 使用时的从 DTE 到 DCE 的电路 108(“数据终端准备好”/“把数据设备接至线路”)、从 DCE 至 DTE 的电路 107(“数据设备准备好”)和从 DCE 到 DTE 的电路 109(“数据信道接收线路信号检测器”)都直接通过 DEE 或由 DEE 以最小延迟重新驱动。

建议 DEE 将电路 109 上的接通状态延迟传送给 DTE，直到 DEE 能在电路 104(“接收数据”)上将数据传送给 DTE 时为止。在电路 107 上的接通状态传送到 DTE 之前，DEE 不应将电路 109 上的接通状态传送给 DTE。

将 DEE 插入 DTE/DCE 接口就在控制信号中引进了固有的延迟，应当考虑现有设备的超时规定。超时规定主要取决于双工传输和半双工传输。具体须查询合适的调制解调器标准。

4.1.1 双工传输

物理连接的呼叫建立是由 DEE 接收到来自 DCE 的电路 107 上的接通状态来指示的。在租用线路的操作中，电路 107 永远处于接通。当电路 109 和电路 106 处于接通时，发送和接收数据信道均是激活的。

当下列条件全部满足时 DEE 才将电路 106 上的接通状态传送给 DTE：

a. 从 DCE 到 DEE 的电路 107 被接通，并经 DEE 通到 DTE。

b. 如果 DCE 要求的话，接通来自 DTE 的电路 105 并通到 DCE。

c. 来自 DCE 的电路 106 是接通的，并且 DEE 的初始化操作已完成。

物理连接能由下列设备清除：

a. DCE，这种清除由电路 107 跃变成断开状态来指示，它可作为一个任选项；或

b. DTE，它由电路 108 跃变成断开状态来指示；或

c. DEE，它由至 DCE 的电路 108 和至 DTE 的电路 107 跃变成断开状态来指示。当发生这种情况时，它指示 DEE 出现故障。

4.1.2 半双工传输

物理连接的呼叫建立是通过接收到来自 DCE 的电路 107 上的接通状态来指示的。在租用线路操作中，电路 107 永远处于接通。根据“请求发送”(电路 105)的状态，在一个时刻，或者是发送数据信道激活，或者是接收数据信道激活。

发送状态准备好(电路 106 接通)是在 DTE 和 DEE 将电路 105 接通后，由 DCE 指示的。接收状态准备好是由来自 DCE 的电路 109 接通来指示的。

电路 105 应这样使用：它用来使得接通状态跃变总是直接通过 DEE，或者由 DEE 以最小延迟重新驱动。至 DCE 的电路跃变成断开状态由 DEE 加以延迟，直到最后一个数据比特在“发送数据”(电路 103)上被发送为止。在 DEE 初始化操作完成之后，才指示 DEE 到 DTE 的电路 106 接通状态。

物理连接能由下列设备清除：

a. DCE，这种清除由电路 107 跃变成断开状态来指示，它可作为一个任选项；或

b. DTE，它由电路 108 跃变成断开状态来指示；或

c. DEE，它由至 DCE 的电路 108 和至 DTE 的电路 107 跃变成断开状态来指示。当发生这种情况时，它指示 DEE 出现故障。

注：在电路 105 上由接通到断开的跃变及随后的 DCE 电路 109 上由断开到接通的跃变之后不久，电路 104 上可能出现伪信号。为了避免伪信号引起 DEE 伪解密启动，DEE 应与下述 DCE 一起使用，该 DCE 使用 GB 3454 第 4.3 条箝位任选项；同时其电路 106 由断开到接通的较长响应时间应由有关 DCE 标准规定。

4.2 GB 11600 或 GB 11599 的接口

对于 GB 11600 和 GB 11599 的互换电路，查询上面所述适用的 GB 3454 双工传输操作。

4.3 GB 11592 的接口

对于 GB 11592 的互换电路，物理连接的呼叫建立提供了起止式传输和双工传输。它是在“接收”互

换电路 R 上接收到呼叫控制字符 ACK 来指示的。在租用电路业务中，可以在任何时候发送和接收数据。

在电路交换业务中，接收数据（接收状态准备好）可以在收到 ACK 之后立即进行。此状态称作“连接的”。发送数据（发送状态准备好）在 ACK 出现 20 ms 以后发生，它称作“数据准备好”。

从 DEE 到 DTE“连接的”状态是在 DEE 初始化操作完成之后由 ACK 来指示的。

清除物理连接在进行清除的 DTE 处由“DCE 清除证实”指示，或在被清除的 DTE 处由“DTE 清除证实”来指示。两者都是由在电路 R 上传输连续的二进制“0”（即 r=0）来指示的，它至少持续 210 ms。清除既可以由来自 DTE 的“DTE 清除请求”、来自 DCE 的“DCE 清除指示”来启动，也可以由 DEE 对 DCE 指示“DTE 清除请求”和对 DTE 指示“DCE 清除指示”来启动。DEE 启动的清除表明 DEE 出现故障。

4.4 GB 11593 的接口

对于 GB 11593 的互换电路，物理连接的呼叫建立提供同步和双工传输。它要求从 DTE 到 DCE 的“发送”互换电路 T 处于接通状态。呼叫建立是由“数据准备好”状态指示的，该状态由来自 DCE 的“指示”互换电路 I 跃变为接通指示。在租用电路业务中，电路 I 接通以作为对电路 T 被接通的响应。从 DTE 到 DCE 的电路 T 总是直接通过 DEE 或由 DEE 以最小延迟重新驱动。

发送和接收数据（发送状态准备好和接收状态准备好）要在电路 I 接通 16bit 时间之后发生。

从 DEE 到 DTE 的“数据准备好”状态（即电路 I 接通）是在 DEE 初始化操作完成之后指示的。

清除物理连接在进行清除的 DTE 处由“DCE 清除证实”指示，或在被清除的 DTE 处由“DTE 清除证实”来指示。两者都由来自 DCE 的电路 I 跃变为断开连同电路 R 上一串二进制“0”（即 r=0，电路 I“断开”）指示。清除既可以通过来自 DTE 的“DTE 清除请求”、来自 DCE 的“DCE 清除指示”来启动，也可以通过由 DEE 对 DCE 指示“DTE 清除指示”和对 DTE 指示“DCE 清除指示”来启动。DEE 启动的清除表明 DEE 出现故障。

4.5 发送和接收数据的互换电路

本标准中的“发送数据的互换电路”在 GB 3454、GB 11600 或 GB 11599 接口情况下指电路 103，而在 GB 11592 或 GB 11593 的接口情况下指电路 T。

本标准中的“接收数据的互换电路”在 GB 3454、GB 11600 或 GB 11599 接口情况下指电路 104，而在 GB 11592 或 GB 11593 的接口情况下指电路 R。

5 一般要求

当使用本标准使各 DEE 之间配合工作时，要求配合工作的组中的全部 DEE 满足下列条件：

a. 相同的密码算法。

b. 相同的密钥值。

c. 相同的 IV 长度、IV 结构和 IV 比特传输顺序。

本标准没有规定特定的密码算法，但要求所使用的任何算法每次以单个比特或单个字符为处理单元，适应于所提供的物理层服务。

注：① 使用 GB/T 15277 所规定的 1 bit 密文反馈（CFB-1）工作方式下的分组密码算法满足本标准的要求。

② 附录 B 举例说明使用一个 64 bit 分组密码算法进行加密时的 IV 要求。

如果 DEE 之间的同步丢失并且该状态被检测出来，那么可以先清除物理连接，然后采用适合于第 4 章中所规定接口类型的步骤重新建立物理连接，由 DEE 或 DTE 强行再同步。该 DEE 不应启动连接重新建立。

6 同步加密操作

6.1 IV

IV 的长度和结构可以按照应用来选择。对于配合工作的组，全部 DEE 的 IV 长度和 IV 结构应预先

商定。

6.2 发送

一旦呼叫建立物理连接并指示发送状态准备好，发送数据的互换电路就处于传号(MARK)状态。在此刻发送IV值，并且在IV的前面用单个二进制“0”bit为其定界。加密一直持续到物理连接清除或半双工传输中数据信道转换为止。

传输SDU的第一个已加密数据比特应按下列选择方式中的一种，紧跟在IV传输之后进行。

6.2.1 选择方式A：立即

第一个已加密的比特紧跟在IV传输之后。

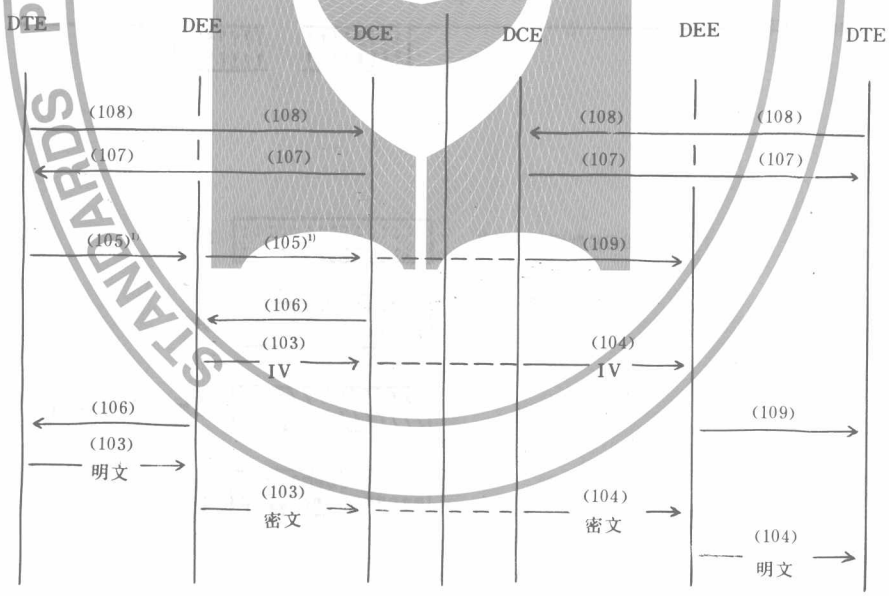
6.2.2 选择方式B：延迟

紧跟在IV之后可以发送数目不定的二进制“1”比特(传号状态)。但如果选用此方式，则该延迟状态至少应维持10 ms，最长不超过50 ms。在这些二进制“1”比特后紧跟单个二进制“0”比特来为数据定界，之后接第一个已加密的数据比特。

6.3 接收

一旦呼叫建立物理连接并指示接收状态准备好，接收数据的互换电路就处于传号状态。紧跟在第一个二进制“0”比特后面的IV被立即接收。在选择方式A中所有随后接收的比特都被解密。在选择方式B中，接收DEE在10 ms内应具有识别定界的二进制“0”比特的能力，并解密以后进来的数据。在选择方式A和选择方式B中，解密都持续到清除物理连接或半双工传输中数据信道转换为止。

图1表示双工传输GB 3454互换电路的操作。图2和图3分别说明同步加密选择方式A和选择方式B的GB 3454半双工传输的信号顺序。



注：1) 如果DCE要求。

图1 表示一个方向上数据加密的GB 3454互换电路的操作

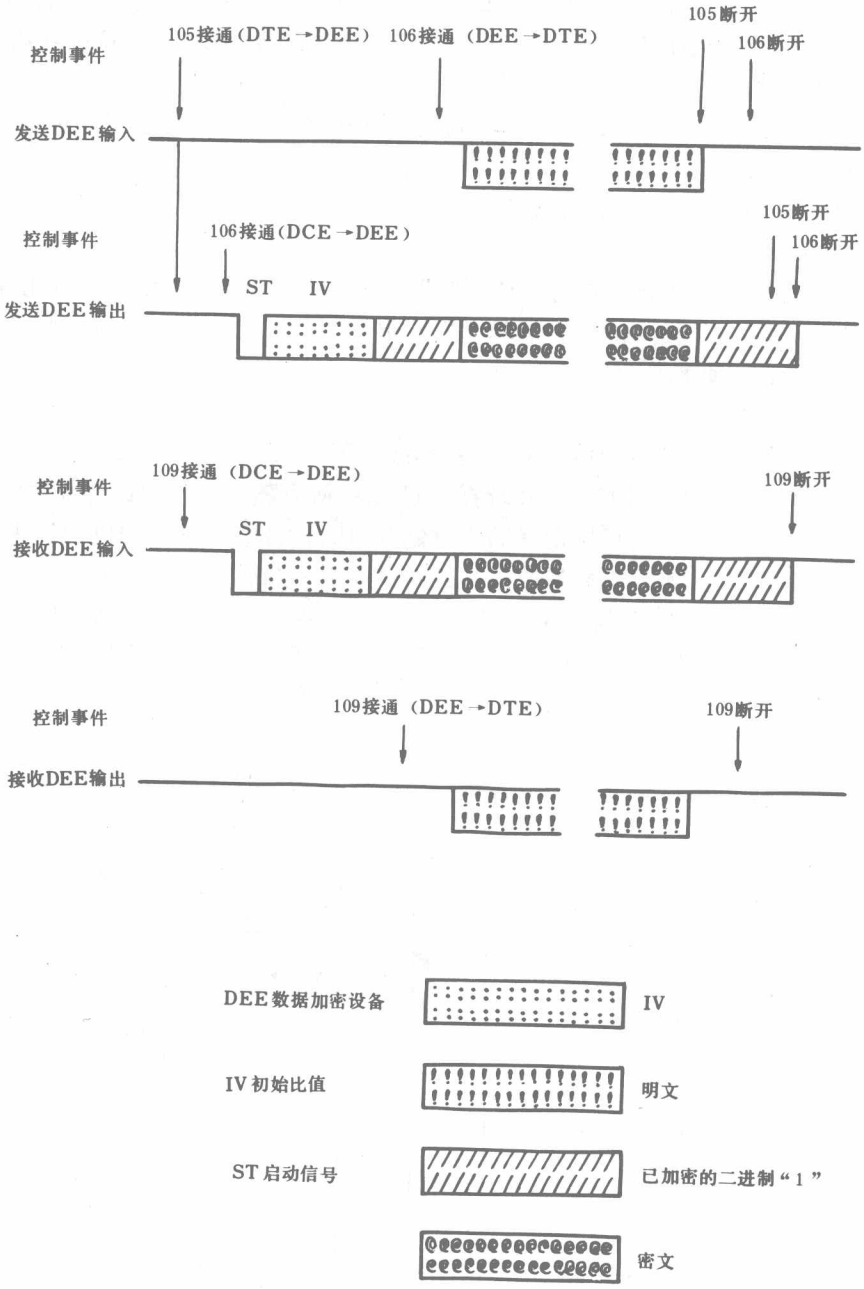


图 2　同步加密的 GB 3454 半双工传输信号顺序，选择方式 A

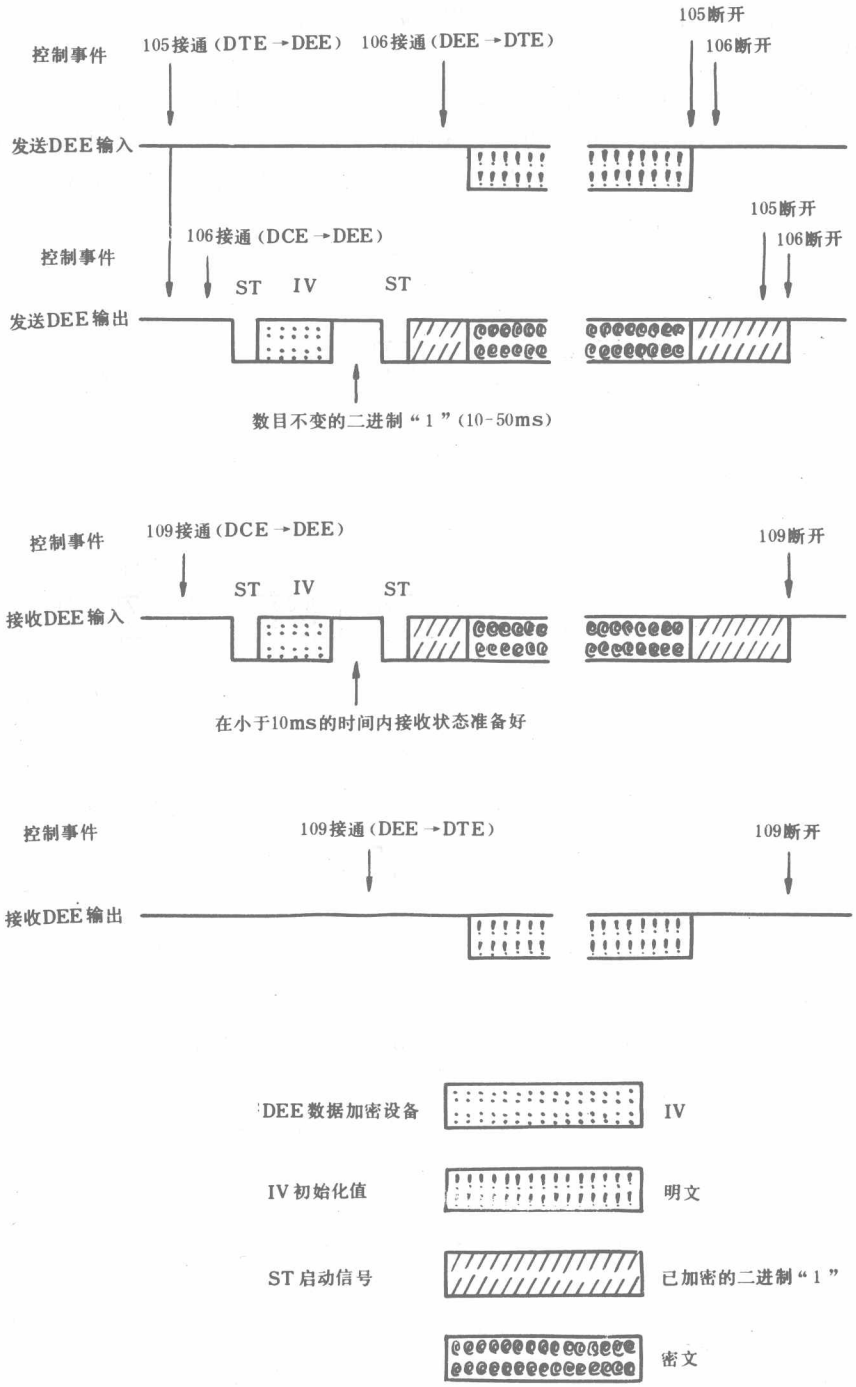


图 3　同步加密的 GB 3454 半双工传输信号顺序，选择方式 B

7　异步加密操作

注：为了提高操作的效率，建议使用能进行双工传输的物理连接。

7.1　发送

7.1.1　IV

一旦建立物理层连接并指示发送状态准备好，发送数据互换电路就处于传号状态。应将 IV 分解成

与待加密和待传送的字符长度相等的单元来发送。该IV的长度和结构可根据应用来选择。在发送和接收DEE之间，应预先商定IV长度、IV结构以及IV按发送字符的编帧。

7.1.2 启动加密

在起始信号和停止信号之间已编帧的SDU字符(对应于发送数据互换电路上的诸字符)紧跟在最后一个IV字符后面被加密发送。对起始和停止编帧信号不进行加密。除下面描述的中断(BREAK)以外，加密一直到要持续到清除物理连接或半双工传输中数据信道转换为止。图4说明了异步加密的启动及下面描述的A类中断操作。

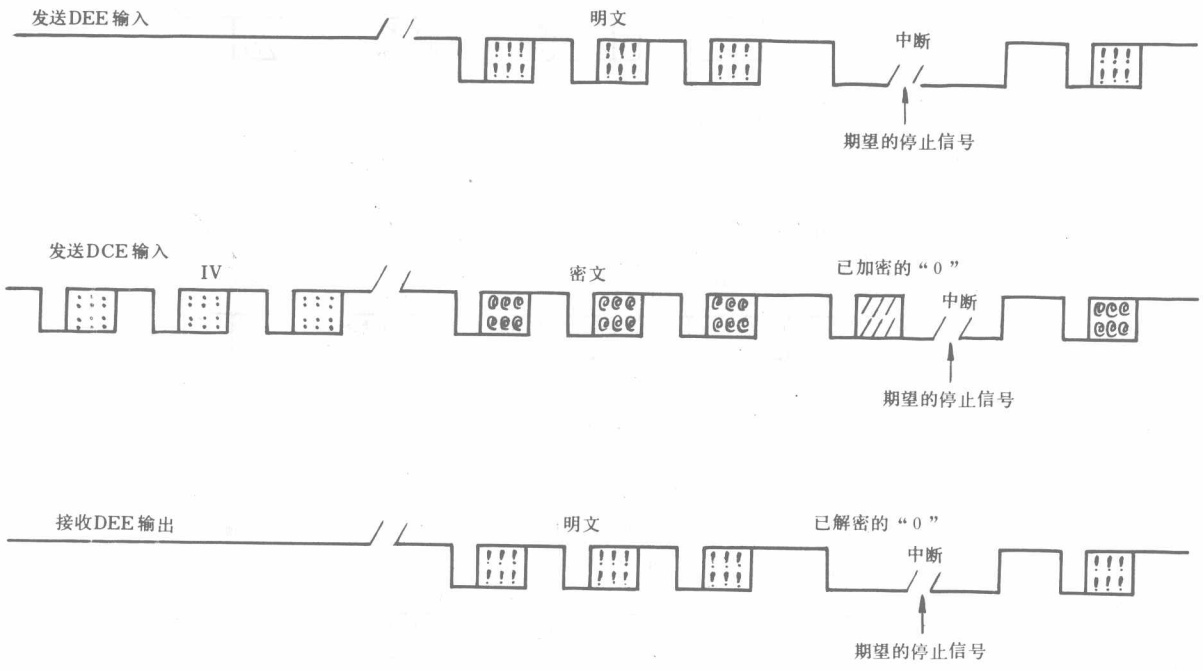


图4 异步加密的启动和A类中断操作

7.1.3 中断

中断是用一个字符时间(或更长)的空号(SPACE)状态来表示的。DEE对中断的动作选择下面两种动作中的一种。

7.1.3.1 A类

将中断的第一个二进制“0”比特当作起始信号。对以后的n个二进制“0”比特进行加密，其中n是不包含起始信号和停止信号的以比特数度量的通常字符长度。DEE不输出停止信号(传号状态)。对中断内的后续二进制“0”比特不进行加密，且DEE继续输出二进制“0”状态。图4的右侧描述了这一动作。DEE输入跃变为传号状态将引起DEE输出产生对应的跃变。随后，DEE恢复正常的操作。

7.1.3.2 B类

在收到停止信号之前，DEE通常不输出任何字符。中断是由于未出现期望的停止信号而被检测出的。一旦检测出中断，DEE就输出一个等同的中断并同时停止加密。在适当延迟之后，中断终止，紧接着就恢复正常的操作。图5说明了B类中断操作。

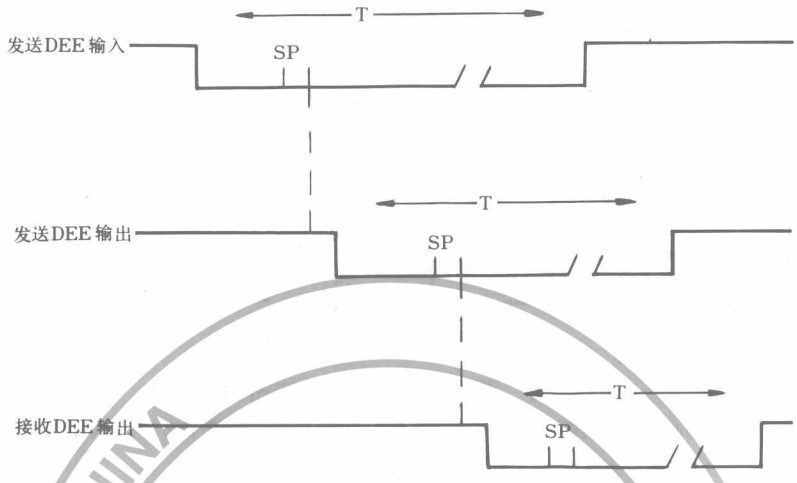


图 5　B 类中断操作

SP—期望的停止信号

7.2　接收

7.2.1　启动解密

一旦呼叫建立物理连接并指示接收状态准备好，接收数据的互换电路就处于传号状态。按照在发送和接收 DEE 之间关于 IV 长度、IV 结构及其按字符编帧的约定，除起始信号和停止信号外，首先接收的几个字符即为 IV。所有随后的字符(除起始信号和停止信号外)均被解密。除中断期间外，解密一直持续到清除物理连接或半双工传输数据信道转换为止。

7.2.2　中断的接收

下面描述 DEE 接收加密形式的中断的动作，它依赖于发送 DEE 的操作类型。

7.2.2.1　A 类

将由已加密的二进制“0”比特组成的字符解密。若无停止信号表示中断操作已经开始。直到在 DEE 输入端中断终止之前，该接收 DEE 的输出一直保持空号状态；此后，DEE 输出至传号状态的跃变并且 DEE 恢复正常操作。图 4 的右侧描述了这种操作。

7.2.2.2　B 类

中断是由未出现停止信号而被检测出来的。在接收到停止信号之前，DEE 不输出任何字符。一旦检测到中断，DEE 就输出一个相同的中断并暂停解密。在适当延迟之后，中断终止，随后就恢复正常操作。图 5 说明了这种操作。

8　旁路控制设施(任选)

作为一个附加的功能，物理层加密可以任选地提供加密过程旁路，以便在 GJB 389.1、GB 11599、GB 11600 中描述的互换电路控制下进行测试环路操作。尽管测试环路被定义为接口的用户设施，但在本标准中对 GB 11592 和 GB 11593 的接口未规定旁路控制设施。

在使用此任选项时，只要来自 DCE 的电路 142“测试指示器”处于接通且来自 DTE 的电路 141“本地环回”或电路 140“环回/维护测试”之一处于接通，就出现旁路。电路 140 和电路 141 同时处于接通被看作是一种差错状态，此时不能进入旁路方式。DEE 在接口上重新将任一个环回信号发送给 DCE，并重新将“测试方式”发送给 DTE。图 6 说明了这些带有本地或远程数据环回的电路的操作。

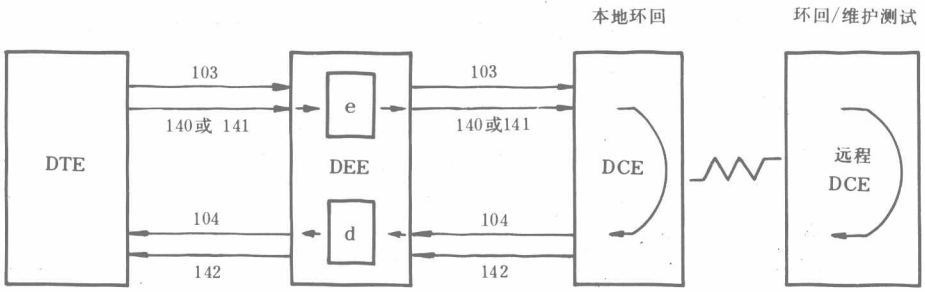


图 6　测试环路操作的加密旁路

电路 104—环回/维护测试；电路 141—本地环回；电路 142—测试指示器；
e—加密功能；d—解密功能

附 录 A
物理层加密的背景信息
（参考件）

A1 物理层加密的特性

物理层加密可简化 DEE 的设计。它通常不要求改变链路层或较高层的规程或协议。

假如实现加密操作是限制因素，使用 1bit 密文反馈(CFB—1)方式的分组加密可能会限制数据速率。然而，物理层加密常常在相对较低的数据速率下使用。

对于较高层，能察觉的链路性能变化是：

a. 延迟及业务量开销，它是在呼叫建立物理连接和指示发送及接收状态准备好后，数据传送之前，由发送 IV 而引起的。只有在具有短电文的半双工传输中数据信道快速转换的情况下，它才是重要的。在双工操作的情况下，它并不重要。

b. 传输差错扩展。密文中单个比特的差错通常会扩展到被接收明文的多个比特上。差错控制规程必须能够处理这种突发差错；或需加以变更以适应这一差错特性。物理层加密隐藏了线路上所有 SDU 信息的内容，包括较高层的所有标题和地址。这种业务信息的隐藏是十分有用的。

物理层加密对数据的插入、删除、更改或重用没有提供检测的规程。只能在较高层防止这种“主动攻击”的威胁。

A2 本标准中提供的选择方式

在异步操作中，对中断的动作提供了 A 类和 B 类选择方式。

A 类中断操作是以逐比特为基础进行的。它仅使通过 DEE 的数据延迟稍大于一个比特时间。但它产生一个没有正常停止信号的字符；这不是所有通信信道都能接受的，因为除中断外，它还可能导致一个数据差错指示。B 类中断操作要求数据延迟至少一个起始/停止信号传输时间。异步操作的 DEE 可提供一类或两类(A 类和 B 类)中断操作。

A3 旁路控制设施(任选)

通过本地和远程调制解调器的环回，旁路用来方便线路故障诊断。不必在连接的两端(或所有端)都提供旁路。DEE 的旁路设施不影响它与其他不包含这一任选项的 DEE 兼容。

在某些情况下，存在旁路设施可能会削弱安全性。用户在考虑便于自动线路测试的同时，也要考虑安全性这一要求。如果必要，DEE 可以备有旁路控制，使其只在需要时才起作用。

如果提供这种切换，建议采用锁的物理钥匙进行控制。它可提供以下三种操作方式的一种或几种作为可选的选择方式。

A3.1 旁路方式

当物理上实现旁路方式时，DEE 对数据传输通路实际上透明。DEE 中的加密和解密过程对所有数据旁路。在 DEE-DCE 接口处，所有 SDU 以明文出现。

A3.2 旁路/安全方式

当物理上实现旁路/安全方式时，旁路将由环回信号和测试指示器信号来控制。即仅在自动线路测试期间，该 DEE 才提供旁路功能。故选择这种方式时，只有当来自 DCE 的电路 142 及来自 DTE 的电路 141 或电路 140 均处于接通时(见图 6)，才会出现旁路。

A3.3 安全方式

提供通过 DEE-DCE 接口只传送密文用户数据的功能。

附 录 B
对 64bit 分组密码算法 IV 结构和传输的要求举例
（参考件）

B1 概述

可选的 IV 长度具有较高的安全性；但是对许多用户，强制性 IV 长度的安全性已足够。如果 IV 延迟和开销都不可忽视，则可使用强制性 IV 长度。如何选择应由用户来权衡。DEE 可以提供具有可切换选择的任选项。

B2 同步加密操作

DEE 支持一个 48bit 的 IV 长度。为了从该 IV 产生 64bit 的 SV，在其左边连续添加 16 个“0”。在这些“0”后面，SV 的下一个比特就是发送的 IV 的第一个比特。

DEE 可以任选地支持一个 64bit 的 IV 长度。该 SV 等于 IV，其左边是第一个发送的比特。

B3 异步加密操作

DEE 支持一个 IV 长度：它是不小于 48bit 的最小的字符长度整倍数（见表 B1）。为了从该 IV 产生 64bit 的 SV，在其左边连续添加若干个二进制“0”比特。图 B1 说明对 7bit 字符，从 49bitIV 进行的 SV 推导。

表 B1 IV 推导

每个字符的比特数	5	6	7	8
每个 IV 的字符数	10	8	7	6
IV 的长度	50	48	49	48

B3.1 IV 选项 1

DEE 可任选地支持一个 IV 长度：它是不小于 60bit 的最小的字符长度整倍数（见表 B2）。为了从 IV 产生 64bit 的 SV，在其左边连续添加若干个二进制“0”比特。图 B2 说明对 7bit 字符，从一个 63bitIV 进行的 SV 推导。

表 B2 IV 选项 1

每个字符的比特数	5	6	7	8
每个 IV 的字符数	12	10	9	8
IV 的长度	60	60	63	64

B3.2 IV 选项 2

DEE 可任选地支持一个 IV 长度：它是不小于 64bit 的最小的字符长度整倍数（见表 B3）。为了从该 IV 产生 64bit 的 SV，发送的超出 64bit 以外的部分都被丢弃；如果必要，也可以丢弃发送的前面几个比特。图 B3 说明了对 7bit 字符，从一个 70bitIV 进行的 SV 推导。