[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/08 (2006.01)
H04L 29/06 (2006.01)

[12] 发明专利说明书

专利号 ZL 02823862.1

[45] 授权公告日 2009 年 4 月 22 日

[11] 授权公告号 CN 100481762C

[22] 申请日 2002.10.8 [21] 申请号 02823862.1

[30] 优先权

[32] 2001.10.9 [33] US [31] 09/973,301

[86] 国际申请 PCT/US2002/032054 2002.10.8

[87] 国际公布 WO2003/032573 英 2003.4.17

[85] 进入国家阶段日期 2004.5.31

[73] 专利权人 高通股份有限公司

地址 美国加利福尼亚州

[72] 发明人 P·豪基斯 N·K·N·利恩

G·G·罗斯

[74] 专利代理机构 上海专利商标事务所有限公司

代理人 钱慰民

[56] 参考文献

CN1299497A 2001.6.13

US6055236A 2000.4.25

US5467398A 1995.11.4

审查员 庄 湧

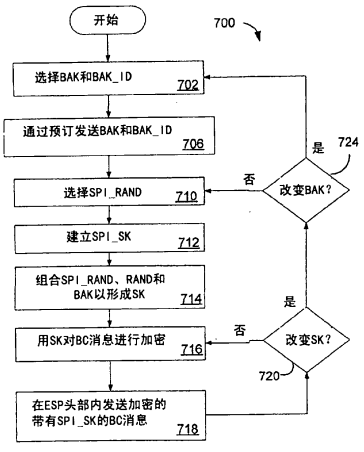
权利要求书 4 页 说明书 26 页 附图 22 页

[54] 发明名称

用于数据处理系统内安全性的方法和装置

[57] 摘要

一种用于安全传输的方法和装置。每个用户被提供了一个注册密钥。长时间更新的广播密钥使用注册密钥经加密并被周期性地提供给用户。短期更新的密钥使用广播密钥经加密。短期密钥在每个广播消息上都有，其中在广播内容前的因特网协议头部内提供了用于计算短期密钥的充分的信息。广播然后使用短期密钥经加密，其中用户使用短期密钥对广播消息进行解密。



1．一种用于安全传输的方法，其特征在于，包括：

为要传输的消息确定短期密钥，所述短期密钥具有短期密钥标识符；

确定所述消息的访问密钥，所述访问密钥具有访问密钥标识符；

用所述短期密钥对所述消息进行加密；

形成包括所述短期密钥标识符的分组头部；以及

发送具有所述分组头部的加密后的消息，

其中，所述短期密钥作为所述短期密钥标识符和所述访问密钥的函数被计算。

2．如权利要求 1 所述的方法，其特征在于，所述短期密钥标识符包括访问密钥标识符。

3．如权利要求 2 所述的方法，其特征在于，所述短期密钥标识符进一步包括安全性参数索引值。

4．如权利要求 3 所述的方法，其特征在于，所述安全性参数索引值是随机数。

5．如权利要求 1 所述的方法，其特征在于，所述短期密钥通过用所述访问密钥对所述短期密钥标识符进行加密而被计算。

6．如权利要求 1 所述的方法，其特征在于,所述分组头部是 ESP 头部的一部分。

7．如权利要求 6 所述的方法，其特征在于，所述分组头部还包括第二随机数，而第二随机数具有随机数标识符。

8．如权利要求 7 所述的方法，其特征在于，所述短期密钥标识符包括所述访问密钥标识符和所述随机数标识符。

9．如权利要求 8 所述的方法，其特征在于，所述短期密钥标识符进一步包括

安全性参数索引值。

10. 如权利要求 9 所述的方法，其特征在于，所述安全性参数索引值是随机数。

11. 如权利要求 7 所述的方法，其特征在于，所述短期密钥作为所述短期密钥标识符、所述第二随机数以及所述访问密钥的函数而被计算。

12. 如权利要求 11 所述的方法，其特征在于，所述短期密钥通过用所述访问密钥对所述短期密钥标识符和所述第二随机数进行加密而被计算。

13. 一种用于安全接收被发送消息的方法，其特征在于，该方法包括以下步骤：

接收对被发送消息特定的短期密钥标识符，所述短期密钥标识符对应于短期密钥；

根据所述短期密钥标识符，确定访问密钥；

用所述访问密钥对所述短期密钥标识符加密，以恢复所述短期密钥；以及

使用所述短期密钥对所述被发送消息进行解密。

14. 如权利要求 13 所述的方法，其特征在于，还包括：

将所述短期密钥标识符和所述短期密钥存储在内存存储单元内。

15. 如权利要求 13 所述的方法，其特征在于，所述短期密钥标识符包括随机数和与所述访问密钥相关的访问密钥标识符。

16. 如权利要求 13 所述的方法，其特征在于，用于对所述短期密钥标识符加密的所述步骤还包括：用所述访问密钥对所述短期密钥标识符和一随机数加密，以恢复所述短期密钥。

17. 一种在支持广播服务选项的无线通信系统内的基础设施元件，其特征在于，包括：

接收电路，用于接收对广播消息特定的短期密钥标识符，所述短期密钥标识符对应于短期密钥；

用户标识单元，用于恢复所述短期密钥，以对所述广播消息解密，所述用户标识单元包括：

处理单元，用于根据所述短期密钥标识符确定访问密钥，并且用所述访问密钥对所述短期密钥标识符加密，以恢复所述短期密钥；以及

移动设备单元，用于应用所述短期密钥以对所述广播消息进行解密，所述移动设备单元包括：

内存存储单元，用于存储多个短期密钥和短期密钥标识符。

18．如权利要求 17 所述的基础设施元件，其特征在于，所述用户标识单元还包括第二内存存储单元，用于存储多个访问密钥和访问密钥标识符。

19．如权利要求 17 所述的基础设施元件，其特征在于，所述内存存储单元是安全内存存储单元。

20．一种无线通信系统的基础设施元件，其特征在于，包括：

用于接收对被发送消息特定的短期密钥标识符的装置，所述短期密钥标识符对应于短期密钥；

用于根据短期密钥标识符确定访问密钥的装置；

用所述访问密钥对所述短期密钥标识符进行加密以恢复所述短期密钥的装置；以及

使用所述短期密钥对所述被发送消息解密的装置。

21．一种用于在与处理器耦合时控制所述处理器安全接收被发送消息的设备，其特征在于包括：

用于控制所述处理器接收对被发送消息特定的短期密钥标识符的装置，所述短期密钥标识符对应于短期密钥；

用于控制所述处理器根据所述短期密钥标识符确定访问密钥的装置；

用于控制所述处理器用所述访问密钥对所述短期密钥标识符加密以恢复所述短期密钥的装置；以及

用于控制所述处理器使用所述短期密钥对所述被发送消息进行解密的装置。

用于数据处理系统内安全性的方法和装置

背景

领域

本发明一般涉及数据处理系统，尤其涉及用于数据处理系统安全性的方法和装置。

背景

数据处理和信息系统（包括通信系统）内的安全性有益于责任性、公平性、准确性、保密性、可操作性以及多种其它期望的标准。加密或密码学一般领域在电子商务、无线通信、广播内都有使用，且其应用范围不受限。在电子商务中，加密被用于防止诈骗行为，以确认参与者的身份。加密以及各种其它安全性措施还被用于防黑客，保护 Web 网页并防止访问机密文档。

使用密码的系统，通常被称为密码系统，可以被分为对称密码系统和非对称密码系统。对称密码系统使用相同的密钥（即安全性密钥）以对消息加密和解密。而非对称加密系统使用第一密钥（即公共密钥）对消息加密，使用第二不同的密钥（即私钥）对其进行解码。非对称密码系统还被称为公共密钥密码系统。在对称密码系统内存在一个问题，即将密钥从发送者安全地提供给接收者。另外，还存在一个问题即当密钥或其它加密机制频繁经更新时。在数据处理系统内，安全地更新密钥的方法需要附加的处理时间、内存存储以及其它的处理开销。在无线通信系统内，更新密钥使用否则可用于传输的宝贵带宽。

现有技术不提供对大量移动站组更新密钥的方法，以使其能接入加密的广播。因此需要一种在数据处理系统内安全且有效地更新密钥的方法。另外，需要在无线通信系统内安全并有效地更新密钥的方法。

概述

在此揭示的实施例通过提供一种用于数据处理系统内的安全性的方法而满足了上述需要。在一方面，用于安全传输的方法包括为要传输的消息确定短期密钥，其中短期密钥有一短期密钥标识符，确定消息的访问密钥，其中访问

密钥有访问密钥标识符，用访问密钥对消息进行加密，形成包括短期密钥标识符的因特网协议头部，并发送带有因特网协议头部的加密消息。

在另一方面，在支持广播服务选项的无线通信系统内，基础设施元件包括接收电路、用户标识单元，用于恢复用于对广播消息解密的短期密钥，以及移动设备单元，用于应用短期密钥以对广播消息解密。用户标识单元包括处理单元，用于对密钥信息解密。移动设备单元包括内存存储单元，用于存储多个短期密钥和短期密钥标识符。

在另一方面，数字信号存储设备包括第一指令集合，用于接收传输特定的短期密钥标识符，短期密钥标识符对应短期密钥，第二指令集合用于根据短期密钥标识符确定访问密钥，第三指令集合用于用访问密钥加密短期密钥标识符以恢复短期密钥，以及第四指令集合用于使用短期密钥对传输进行解密。

附图的简要描述

图 1A 是加密系统图。

图 1B 是对称加密系统图。

图 1C 是非对称加密系统图。

图 1D 是 PGP 加密系统图。

图 1E 是 PGP 解密系统图。

图 2 是支持多个用户的扩频通信系统图。

图 3 是支持广播传输的通信系统框图。

图 4 是无线通信系统内的移动站框图。

图 5A 和 5B 说明在移动站内描述控制广播接入的密钥更新的模型。

图 6 是描述 UIM 内密码操作的模型。

图 7A－7D 说明在支持广播传输的无线通信系统内实现安全加密的方法。

图 7E 是支持广播传输的无线通信系统内安全性选项的密钥更新时段的时序图。

图 8A－8D 说明在支持广播传输的无线通信系统内安全性加密方法的应用。

图 9A 说明用于因特网协议传输的 IPSec 分组的格式。

图 9B 说明应用于 IPSec 分组的安全性关联标识符或 SPI。

图 9C 说明用于在移动站内存储 SPI 信息的内存存储设备。

图 9D 说明用于在移动站内存储广播访问密钥（BAK）的内存存储设备。

图 10 和 11 说明在无线通信系统内提供广播消息的安全性的方法。

图 12A 说明应用于 IPSec 分组的安全性关联标识符或 SPI。

图 12B 说明用于在移动站内存储 SPI 信息的内存存储设备。

图 13 和 14 说明在无线通信系统内提供广播消息的安全性的方法。

详细描述

“示例”一词在此仅用于指“用作示例、实例或说明”。任何在此作为“示例”描述的实施例不一定被认为是最优或优于其它实施例的。

无线通信系统广泛用于提供多种诸如语音、数据等类型的通信。这些系统可能基于码分多址（CDMA）、时分多址（TDMA）或一些其它的调制技术。CDMA 系统提供一些优于其它类型系统的优势，包括增加的系统容量。

CDMA 系统可能设计成支持一个或多个 CDMA 标准，诸如（1）“TIA/EIA-95-B Mobile Station-Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Cellular System”（IS-95 标准），由“3rd Generation Partnership Project”（3GPP）提供的标准，体现在一组文档内包括 Nos. 3G TS 25.211、3G TS 25.211、3G TS 25.212、3G TS 25.213 以及 3G TS 25.214（W－CDMA 标准），由“3rd Generation Partnership Project 2”（3GPP2）提供的标准，在此被称为 cdma2000 标准的 TR－45.5，先前被称为 IS－2000 MC。这些所述标准在此引入作为参考。

每个标准特别定义了从基站到移动的要传输的数据的处理，反之依然。作为示例实施例，以下的讨论考虑符合 cdma2000 的扩频通信系统。另外的实施例可能包括其它标准/系统。另外的实施例可能对任何类型的使用密码系统的数据处理系统应用在此揭示的安全性方法。

密码系统是一种伪装消息的方法，它使得特定的用户组能获取消息。图 1A 说明了基本的密码系统 10。密码学是建立和使用密码系统的技术。密码分析是破解密码系统的技术，即当你不在允许访问消息的特定用户组内时接收并理解消息。原消息被称为明文消息或明文。加密消息被称为密文，其中加密包括任何将明文转化为密文的方法。解密包括任何将密文转换为明文的方法，即恢复原消息。如图 1A 所说明的，明文消息经加密以形成密文。密文然后经接收并解密以恢复明文。密文然后经接收和解密以恢复明文。虽然术语明文和密文一

般指数据，但加密的概念可以应用到任何数字信息，包括数字形式的音频和视频数据。虽然在此提供的本发明的描述使用与密码学一致的明文和密文术语，但这些术语不排除数字通信的其它形式。

密码系统基于机密。如果在组外的实体不能在没有大量资源情况下获取机密，则称一组实体共享一个机密。

密码系统可能是算法的集合，其中每个算法经标记且这些标记被称为密钥。对称加密系统，经常被称为密码系统，使用相同密钥（即机密密钥）以对消息进行加密和解密。对称加密系统 20 在图 1B 内说明，其中加密和解密使用相同的私钥。

相比之下，对称加密系统使用第一密钥（即公共密钥）以对消息进行加密，并使用不同的密钥（例如私钥）对其进行解密。图 1C 说明非对称加密系统 30，其中为加密提供一个密钥，为解密提供第二密钥。非对称密码系统还被称为公共密钥密码系统。公共密钥经公布，且可用于对任何消息加密，然而，只有私钥可以用来对用公共密加密的消息进行解密。

在对称密码系统内存在将机密密钥安全地从发送者提供给接收者的问题。一个解决方案是可能使用信使以提供信息，或更有效并可靠的方法可能是使用公共密钥密码系统，诸如 Rivest、Shamir 和 Adleman（RSA）定义的公共密钥密码系统，以下将描述。RSA 系统在被称为相当好私密性（PGP）的流行安全性工具内被使用，这在以下将讨论。例如，原录制密码系统通过将每个字母在字母集内平移 n 个而改变明文内的字母，其中 n 是预定的常整数值。在该方案中，“A”用“D”来替换等，其中给定的加密方案可能包括几个不同的 n 的值。在该加密方案中“n”是密钥。预定的接收者在接收密文前被提供了加密方案。这样，只有知道密钥的任能对密文进行解密以恢复明文。然而，通过已知的加密知识来计算密钥，非意向的接收者可能能截获并对密文进行解密，从而导致了安全性的问题。

更复杂和成熟的密码系统使用策略密钥，它阻止了来自非意向方的截获和解密。经典的密码系统使用加密函数 E 和解密函数 D，诸如：

$$D_K(E_K(P)) = P, \text{ for any plaintext } P \qquad (1)$$

在公共密码系统内，E_K 可以很简单地从已知的“公共密钥”Y 中计算得到，该 Y 依次是从 K 计算而得得。公共密钥是公开的，故任何人都可加密消息。解密函数 D_K 从公共密钥 Y 计算而得，但只是在知道私钥 K 的情况下。在不知道私钥 K 的情况下，非意向的接收者可能不能对如此生成的密文解密。这样，只有生成 K 的接收者能对消息解密。

RSA 是 Rivest、Shamir 和 Adleman 定义的公共密钥密码系统，其中例如，明文考虑多达 2^{512} 的正整数。密钥是四元组（p，q，e，d），其中 p 作为 256 为质数给出，q 作为 258 位的质数给出，d 和 e 是（de－1）可被（p－1）（q－1）整除的大数。。另外，定义加密函数为：

$$E\_K(P) = P^e \bmod pq, D\_K(C) = C^d \bmod pq \qquad (2)$$

然而，E_K 很简单地能从对（pq，e）计算得到，没有已知的简单的方法可以从对（pq，e）计算 D_K。因此，生成 K 的接收者能公布（pq，e）。可能发送机密消息到接收者，因为他是能读消息的人。

PGP 组合了对称和非对称加密的特点。图 1D 和 1E 说明 PGP 系统 50，其中明文消息经加密并经恢复。在图 1D 内，明文消息经压缩以节省调制器传输时间和磁盘空间。压缩增强了加密安全性，因为这在加密和解密过程上加入了另一层转换。大多数密码分析技术使用在明文内发现的模式而破解密码。压缩减少了明文内的模式，从而增强了抗密码分析性。值得注意的是一个实施例不压缩：明文或其它太短而不能压缩的消息或是压缩不好的消息。

PGP 然后建立对话密钥，它是一次有效的机密密钥。该密钥是可能从任何随机事件生成的随机数，诸如在打字时计算机鼠标和键盘的随机移动。对话密钥与安全加密算法一起作用对明文进行加密，产生密文。一旦数据经加密，对话密钥然后被加密为接收者的公共密钥。公共密钥加密对话密钥连同密文一起发送给接收者。

为了解密，如图 1E 说明的，PGP 的接收者拷贝使用私钥恢复临时的对话密钥，PGP 然后使用该密钥对常规加密的密文进行解密。加密方法的组合利用了公共密钥加密的方便性和对称加密的速度。对称加密一般要比公共密钥加密快很多。公共密钥加密反过来提供了密钥发布和数据传输问题的解。组合起来，性能和密钥发布经改善而不牺牲安全性。

密钥是与密码算法一起使用的值以生成特定密文。密钥一般是很大的数字。密钥大小使用比特衡量的。在公共密钥加密内，安全性随着密钥大小增加而增加，然而，公共密钥大小和对称加密私钥大小一般不相关。虽然公共和私有密钥在数学上相关，在只有公共密钥的情况下，会有导出私钥的困难。在给出足够的时间和计算能力的情况下可能导出私钥，这使得密钥大小的选择是很重要的安全性问题。最优目标是为了最大化密钥的大小，考虑到安全性的考虑，而同时最小化密钥大小以方便快速处理。较大的密钥在较长时间上是密码安全的。附加的考虑是可能的截获者，特别是：1）对于第三方而言，什么是消息的重要性；以及 2）第三方有多少

资源用以对消息进行解密。

值得注意的是密钥以加密形式被存储。PGP 尤其将密钥存储在两个文件内：一个用于公共密钥，一个用于私钥。这些文件被称为密钥环。在应用中，PGP 加密系统将目标接收者的公共密钥加入到发送者的公共密钥环上。发送者的私钥被存储在发送者的私有密钥环上。

如在上述给出的示例中讨论的，发布用于加密和解密的密钥的方法可以很复杂。“密钥交换问题”涉及到首先保证密钥被交换，使得发送者和接收者可以实现相应的加密和解密，且对于双向通信而言，使得发送者和接收者可以同时对消息进行加密和解密。另外，希望密钥交换的实现使得能排除第三方和非意向方的截获。

最后，附加的考虑是验证，提供给接收机以保证，即消息是由预定发送方加密而不是第三方加密的。在私钥交换系统中，密钥经秘密交换，成功地密钥交换以及合法验证之后提供了改善的安全性。值得注意的是私钥加密方案隐式提供了验证。私钥密码系统内所基于的假设是只有预定的发送方有能对发送到预定接收方消息进行加密的密钥。而公共密钥加密方法解决了“密钥交换问题”很关键的一方面，尤其是在密钥交换时有被动偷听的抗分析性，然而，它们还是没有解决与密钥交换相关的所有问题。特别是，由于密钥被认为是“公共信息”（特别是 RSA 情况中），需要一些其它的机制提供验证。验证指示需要作为单独拥有密钥，而足以对消息加密，验证不是发送者的特定唯一身份，也不是自己拥有对应的解密密钥足以建立接收者的身份。

一个解决方案就是研发一种密钥发布机制，它保证了列出的密钥实际上是给定的实体的密钥，有时被称为可信任实体、证书实体或第三方签约代理。授权方一般实际上不生成密钥，但保证为发送方和接收方保存并用作参考的密钥列表与相关的身份标识是正确且未被受损害。另一方法依靠用户发布，且相互跟踪对方的密钥，是一种不正式、分发式的信托。在 RSA 中，如果用户希望除加密消息外还发送其身份信息，则用密钥对签名加密。接收者可以使用 RSA 算法反过来确定信息解密，使得只有发送方可以通过使用秘密密钥而对明文加密。一般加密的“签名”是“消息摘要”，它包括机密消息的唯一数学“概述”（如果签名在多个消息上是固定的，则一旦被知道则先前的接收者会非法地使用它）。这样，理论上，只有消息的发送方会生成为该消息的合法签名，从而为接收者验证它。

消息摘要常使用加密哈希函数而被计算。加密哈希函数从任何输入计算一值（带有固定的比特数），而不管输入的长度。加密哈希函数的一个特性如下：给定

输出值，计算上非常难确定导致该输出的输入。加密哈希函数的一个示例是在“Secure Hash Standard”内描述的SHA－1，FIPS PUB 180－1，由联邦信息处理标准公布颁布（FIP PUBS）并由国家标准和技术局发布。

图 2 作为支持多个用户并能实现至少本发明一些方面和实施例的通信系统100的示例。任何一种算法和方法可以被用于在系统100内进行调度安排。系统100提供多个小区102A到102G的通信，每个都由对应的基站104A和104G相应地提供服务。在示例实施例中，一些基站104有多个接收天线，其它只有一个接收天线。类似地，一些基站104有多个发射天线，而其它只有单个发射天线。在发射天线和接收天线的组合上没有任何限制。因此，对于基站而言，可能有多个发射天线，一个接收天线，或有多个接收天线和一个发射天线，或都只有单个或同时有多个发射和接收天线。

覆盖区域内的终端106可能是固定（即静止的）或移动的。如图2所示，个终端106散布在系统内。每个终端106与至少一个且可能多个基站104在下行链路和上行链路在任何给定时刻通信，这取决于是否使用软切换，或终端是否被设计成并被用于（迸发地或顺序地）接收来自多个基站的多个传输。CDMA 内的软切换在领域内是众知的，在美国专利号5101501内有详细描述，题为“Method and system for providing a Soft Handoff in a CDMA Cellular Telephone System”，它被转让给本发明的受让人。

下行链路是指从基站到终端的传输，上行链路是指从终端到基站的传输。在示例实施例中，一些终端 106 有多个接收天线，其它只有一个接收天线。在图 2 内，基站104A在下行链路上将数据发送到终端106A和106J，基站104B将数据发送到终端106B和106J，基站104C将数据发送到终端106C等。

对于无线数据传输增长的需要和通过无线通信技术可用的服务的扩展导致了特定数据服务的发展。一种该项服务被称为高数据率（HDR）。示例 HDR 服务在“EIA/TIA-IS856 cdma2000 High Rate Packet Data Air Interface Specification”内被提出，称为“HDR规范”。HDR服务一般覆盖预定通信系统，它提供了在无线通信系统内有效地发送数据分组的方法。由于发送的数据量增加，而且传输数目增加，可用于无线电传输的有限带宽成为关键资源。因此需要一种在通信系统内有效并公平地调度传输的方法，它能最优化可用带宽的使用。在示例实施例中，图 2 内说明的系统100符合带有HDR服务的CDMA类型系统。

根据一实施例，系统 100 支持高速多媒体广播服务，被称为高速广播服务

（HSBS）。HSBS 的一示例应用是电影、体育事件的视频流等。HSBS 服务是根据因特网协议（IP）的分组数据服务。根据示例实施例，服务提供商指明该种高速广播服务对用户的可用性。需要 HSBS 服务的用户预订接收服务并可能通过广告、短管理系统（SMS），无线应用协议（WAP）等发现广播服务安排。移动用户被称为移动站（MS）。基站（BS）在附加开销内发送 HSBS 相关的参数。当 MS 需要接收广播对话时，MS 读取附加开销并获悉合适的配置。MS 然后调谐到包含 HSBS 信道的频率，并接收广播服务的内容。

考虑的服务是高速多媒体广播服务。该服务在本文档内被称为高速广播服务（HSBS）。一种该示例是电影、体育事件等的视频流。该服务可能是基于因特网协议（IP）的分组数据服务。

服务提供商指明该种高速广播服务对用户的可用性。需要该项服务的移动站用户预订接收服务并可能通过广告、SMS，WAP 等发现广播服务安排。基站在附加开销内发送广播服务相关的参数。需要收听广播对话的移动会读取这些消息并确定合适的配置，调谐到包含高速广播信道的频率，并开始接收广播服务的内容。

有几种可能的 HSBS 服务的订户/收入模型，包括免费接入、控制接入和部分控制接入。对于免费接入，不需要预订以接收服务。BS 广播未经加密的内容，感兴趣的移动可以接收该内容。服务提供商的收入可以通过在广播信道上发送的广告获得。例如，到来的电影片段可以为付钱给服务提供商的电影摄制棚而发送。

对于控制的接入，MS 用户预订服务，且支付对应的费用以接收广播服务。未经预订的用户不能接收 HSBS 服务。控制的接入可以通过对 HSBS 传输/内容加密而实现，使得只有预订的用户能对内容解密。这可以使用空中密钥交换过程。该方案提供了很强的安全性并防止服务被偷窃。

混合接入方案，又被称为部分控制的接入，提供了作为加密的基于预订的 HSBS 服务，它断断续续地有不加密的广告传输。这些广告可能用于增加对加密 HSBS 服务的预订。这些未经加密的分段的调度可以通过外部装置为 MS 所知。

无线通信系统 200 在图 3 内被说明，其中视频和音频信息由内容服务器（CS）201 提供给分组化数据服务网络（PDSN）202。视频和音频信息可能来自电视节目或无线电传输。信息被提供为分组化数据，诸如在 IP 分组内。PDSN 202 处理 IP 分组用于在接入网络（AN）内发布。如说明的，AN 被定义为包括与多个 MS 206 通信的 BS 204 的系统部分。PDSN 202 耦合到 BS 204。对于 HSBS 服务，BS 204 接收

来自 PDSN 202 的信息流，并在指定信道上将信息提供给系统 200 内的订户。为了控制接入，内容由 CS 201 在提供给 PDSN 202 前经加密。订户用户被提供了解密密钥，使得能对 IP 分组进行解密。

图 4 详细说明了 MS 300，类似于图 3 的 MS 206。MS 300 有耦合到接收电路 304 的天线 302。MS 300 接收来自类似于图 3 的 BS 204 的 BS（未示出）的传输。MS 300 包括用户标识模块（UIM）308 和移动设备（ME）306。接收电路耦合到 UIM 308 和 ME 306。UIM 308 为 HSBS 传输的安全性提供确认过程，并提供各种密钥给 ME 306。ME 306 可能耦合到处理单元 312。ME 306 实现实质性的处理，包括但不限于 HSBS 内容流的解密。ME 306 包括内存存储单元 MEM 310。在示例实施例中，ME 306 处理单元内的数据（未示出）以及 ME 内存存储单元内的数据，MEM 310 可以简单地通过使用有限的资源由非订户访问，因此 ME 306 被称为是不安全的。任何传递到 ME 306 的信息或由 ME 306 处理的信息保持短时间的安全保密。因此需要经常改变与 ME 306 共享的任何机密信息，诸如密钥。

UIM 308 是可信任的，它存储并处理机密信息（诸如加密密钥），它可以保持机密较长时间。由于 UIM 308 是一个安全单元，在此存储的机密不一定需要系统经常改变机密信息。UIM 308 包括处理单元，被称为安全 UIM 处理单元（SUPU）316 和内存存储单元，被称为安全 UIM 存储单元（SUMU）314，它被信任是安全的。在 UIM 308 内，SUMU 314 存储机密信息的方式使得对信息未授权的访问很难实现。如果机密信息是从 UIM 308 被获得的，则访问会需要大量资源。而且在 UIM 308 内，SUPU 316 实现可能对 UIM 308 是外部和/或对 UIM 308 是内部的值上的计算。计算的结果可能被存储在 SUMU 314 内或传递到 ME 306。用 SUPU 316 实现的计算值可以从 UIM 308 由带有大量资源的实体获得。类似地，来自 SUPU 316 的输出被指定存储在 SUMU 314 内（但不输出到 ME 306），这些输出的设计使得需要大量资源才能进行未授权的截获。在一实施例中，UIM 308 是 MS 300 内的静止单元。值得注意的是除了 UIM 308 内的安全存储和处理外，UIM 308 还可能包括非安全存储器和处理（未示出）用于存储包括电话号码、电子邮件地址信息、Web 网页或 URL 地址信息和/或调度功能等的信息。

另外的实施例可能提供可移动和/或可重新编程 UIM。在示例实施例中，SUPU 316 对于在安全性和密钥处理之上的功能没有很大的处理功能，其中安全性和密钥过程一般可能被用于能对 HSBS 的广播内容进行加密。其它的实施例可能实现带有更强处理功能的 UIM。

UIM 308 与特定的用户相关，并首先被用于确认 MS 300 享有用户的特权，诸如接入移动电话网络。因此，用户与 UIM 308 相关而不是 MS 300。同一用户可能与多个 UIM 308 相关。

广播服务面临一个问题，即确定如何将密钥发布给订户。为了在特定时间对广播内容解密，ME 必须知道当前的解密密钥。为了避免偷窃服务，解密密钥应经常被改变，例如，一个服务每分钟改变密钥。这些解密密钥被称为短期密钥（SK）。SK 用于对广播内容在短时间内解密，所以 SK 被假设对于用户有一定量的固有费用值。例如，内在币值可能是注册费用的一部分。假设非订户从订户的内存存储单元 MEM 310 获得 SK 的费用超过 SK 的固有费用值。即非法获得 SK 的费用超过报酬，则导致没有净收益。结果是，减少了保护内存存储单元 MEM 310 内的 SK 的需要。然而，如果机密密钥的寿命长于 SK 的寿命，则非法获得该机密密钥的费用可能少于报酬。在该情况下，非法从内存存储单元 MEM 310 获得该密钥有净收益。因此，理想化情况下，内存存储单元 MEM 310 不会存储寿命长于 SK 的机密。

CS 用于将 SK 发布到各个订户单元的信道被假设为不安全的。换而言之，最优设计会假设信号是不安全的，并相应地设计 SK。因此，当发布给定的 SK 时，CS 希望使用一种技术，不让非订户用户知道 SK 的值。另外，CS 将 SK 发布到潜在的大量订户用于在相对较短的时间帧内在相应的 ME 内进行处理。密钥传输的已知安全方法一般较慢，且需要大量的密钥传输。密钥传输方法一般对于需要的安全性和有效性组合的准则不可行。示例实施例时可行的将解密密钥在短时间帧内发布到大订户集合的可行方法，使得非订户不能获得解密密钥。

示例实施例被描述为在因特网协议兼容的分组内发送信息，诸如以下描述的“IPSec”分组，因此，以下的描述提供了在与 IPSec 相关联的术语的简介。该术语在描述示例实施例时是有用的，但使用该术语不意味着将示例实施例限于使用 IPSec 的通信。

IPSec 的建立在 RFC 1825、RFC 1826 和 RFC 1827 内有规定，分别题为“Security Architecture for the Internet Protocol”，R. Atkinson, 1995 年 8 月；“IP Authentication Header”，R. Atkinson, 1995 年 8 月以及“IP Encapsulating Security Payload(ESP)”，R. Atkinson, 1995 年 8 月。验证头部是一种提供 IP 数据报完整性的机制，其中 IP 数据报一般是有用信息（被称为有效负荷）和网络控制信息和 IP 头部的组合。网络路由器使用 IP 头部以引导分组到合适的网络节点。在一些情况下，验证头部可能还提供对 IP 数据报的验证。ESP 是用于提供 IP 数据

报的机密性和完整性的机制，且可能与验证头部一起使用。IPSec 使用“安全相关”以描述参数，诸如加密密钥和加密算法，用于对实体组间的通信进行加密和/或验证。值得注意的是安全相关的概念应用在不基于 IPSec 的密码系统上是也是合适的。

IPSec 分组包括被称为安全参数索引（SPI）的 32 为参数，它与目的地地址一起用于标识用于对 IP 数据报内容加密和/或验证的安全相关联。实体可能在安全性关联数据库内存储安全性关联以及根据目的地地址和 SPI 对安全性关联进行索引。IPSec 分组的加密内容被称为有效负荷。

在示例实施例中，MS 300 支持无线通信系统内的 HSBS。为了获得到 HSBS 的接入，用户必须注册，然后预订服务。一旦启用了注册，根据需要更新各个密钥。在注册过程中，CS 和 UIM 308 协商安全性关联，并在注册密钥（RK）和其它为了用户和 CS 间的安全性关联需要的参数上取得一致。CS 然后可能将进一步的用 RK 加密的机密信息发送到 UIM 308。RK 在 UIM 308 内被保持为机密，而其它参数可能保存在 ME 306 内。RK 对于给定的 UIM 308 是唯一的，即每个用户被分配以不同的 RK。单独的注册过程不给予用户到 HSBS 的接入。

如上所述，在注册后，用户预订服务。在预订过程中，CS 将公共广播访问密钥（BAK）的值发送到 UIM 308。值得注意的是 RK 是对于 UIM 308 特定的，BAK 用于对到多个用户的广播消息加密。CS 将使用对 UIM 308 唯一的 RK 加密的 BAK 值发送到 MS 300，尤其是 UIM 308。UIM 308 能使用 RK 从加密的版本恢复原 BAK 的值。BAK 以及其它参数，形成了 CS 和订户用户组间的安全性关联。BAK 在 UIM 308 内被保留为机密，而其它的安全性关联参数可能被保留在 ME 306 内。CS 然后广播被称为 SK 信息（SKI）的数据，该信息在 UIM 308 内与 BAK 组合以导出 SK。UIM 308 然后将 SK 传递到 ME 306。这样，CS 可以有效地将 SK 的新值发布到订户用户的 ME。以下表示的是如果从 SKI 导出 SK 的示例，以及 SKI 采取的形式。注册和预订过程在描述 SKI 和 SK 之后详细讨论。

关于注册，当用户用给定的 CS 注册，UIM 308 和 CS（未示出）建立安全性关联。即 UIM 308 和 CS 在机密注册密钥 RK 上取得一致。RK 对于每个 UIM 308 是唯一的，虽然如果用户有多个 UIM，则这些 UIM 可能共享同一个取决于 CS 政策的 RK。该注册可发生在当用户预订由 CS 提供的广播信道时或可能发生在预订前。单个 CS 可能提供多个广播信道。CS 可能选择将用户与对所有信道相同的 RAK 相关联，或需要用户为每个信道注册，并将同一用户与不同信道上的不同 RK 相关联。多个 CS

可能选择使用相同的注册密钥或要求用户注册并为每个CS获得不同的RK。

三种为设立该安全性关联的情况包括:1)用于3GPP系统的验证密钥协定(AKA)方法；2）用于在IPSec内的因特网密钥交换（IKE）方法；以及3）Over-The-Air-Service-Provisioning(OTASP)。在两种情况下，UIM存储单元SUMU 314包含在此被称为A密钥的机密密钥。例如，使用AKA方法，A密钥是只有UIM和被信任第三方（TTP）知道的机密，其中TTP可能包括多于一个实体。TTP一般是用户与其进行注册的移动服务提供商。CS和TTP间的所有通信是安全的，CS相信TTP不会帮助对未经授权的广播服务的访问。当用户注册时，CS通知TTP，用户希望注册服务，且提供用户请求的确认。TTP使用一个类似于加密哈希函数的函数以计算来自A密钥的RK，以及被称为注册密钥信息（RKI）的附加数据。TTP将RK和/或RKI在安全信道上与其它数据一起传递到CS。CS将RKI发送到MS 300。接收机电路304将RKI传递到UIM 308并将RKI传递到ME 306。UIM 308从RKI计算RK,以及存储在UIM内存单元SUMU 314内的A密钥。RK被存储在UIM内存单元SUMU 314内，且不直接被提供给ME 306。另外的实施例可能使用IKE情况，或一些其它的方法以建立RK。CS和UIM 308间的安全性关联的其它参数必须也经协商。RK被在UIM 308内保持为机密，而安全性关联的其它参数可能被保留在ME 306内。在示例实施例中，其中BAK被作为使用RK加密的IPSec分组发送回UIM 308，CS和MS 300协商用于对安全性关联进行索引的SPI值，且该SPI被标记为SPI_RK。

在AKA方法中，RK是在CS、UIM和TTP间共享的机密。因此，如在此使用的，AKA方法暗示CS和UIM间的任何安全性相关隐含包括TTP。在任何安全性相关内包括TTP不被认为违反安全性，因为CS相信TTP不会帮助对广播信道未经授权的访问。如上所述，如果与ME 306一起共享密钥，需要经常改变密钥。这是因为有非订户访问存储在内存存储单元MEM 310内的信息的风险，这样会导致访问控制或部分控制的服务。ME 306在内存存储单元MEM 310内存储SK即用于对广播内容解密的密钥信息。CS发送预订的用户的充分的信息以计算SK。如果预订的用户的ME 306可以从该信息计算SK，则计算SK需要的附加信息就不是机密了。在该情况下，假设非预订用户的ME 306还能从该信息计算SK。因此，该SK值必须在SUPU 316内使用CS和SUMU 314共享的机密密钥而经计算。CS和SUMU 314共享RK值，然而每个用户有唯一的RK值。对于CS而言，没有充分的时间用每个RK值对SK加密，并将这些加密的值发送到每个预订的用户。

关于预订，为了保证安全性信息SK的有效发布，CS周期性地将公共广播访问

密钥（BAK）发送到每个订户 UIM 308。对于每个订户，CS 使用对应的 RK 对 BAK 加密以获得称为BAKI信息(BAKI)的值。CS将对应的BAKI发送到预订用户的MS 300。例如，BAK 可能作为使用对应每个 MS 的 RK 加密的 IP 分组而经发送。在示例实施例中，BAKI 是包含使用 RK 作为密钥而加密的 BAK 的 IPSec 分组。由于 RK 是每个用户的密钥，CS 必须单独将 BAK 发送到每个订户；因此 BAK 不在广播信道上被发送。MS 300 将 BAKI 传递到 UIM 308。SUPU 316 使用存储在 SUMU 314 内的 RK 值和 BAKI 值计算 BAK。BAK 值然后被存储在 SUMU 内。在示例实施例中，BAKI 包含被标为 SPI_SK 的 SPI 值，它对应包含 RK 的安全性关联。当 IPSec 分组是根据该安全性关联而经加密的时候，MS 300 知道 UIM 308 可以对有效负荷解密。结果是，当 MS 300 接收到根据该安全性关联加密的 IPSec 分组时，MS 300 将 BAKI 传递到 UIM 308，并指示 UIM 308 使用 RAK 以对有效负荷进行解密。

更新 BAK 的周期需要足够长，使得 CS 能单独地将 BAK 发送到每个订户而没有大量的附加开销。由于 ME 306 不被信任保持长时间的机密，UIM 308 不向 ME 306 提供 BAK。CS 和订户组间的安全性关联的其它参数也必须经协商。在一实施例中，这些参数是固定的，而在另一实施例中，这些参数可能作为 BAKI 的一部分被发送到 MS。在 BAKI 在 ME 306 内被保留机密的同时，安全性关联的其它参数也可能保留在 ME 306 内。在一实施例中，其中 SK 被作为使用 BAK 加密的 IPSec 分组被发送到 MS 300，CS 提供给订户用于对安全性关联建立索引的 SPI，该 SPI 被标明为 SPI_BAK。

以下讨论在成功预订过程后如何更新 SK。在用于更新 BAK 的每个时段内，在 SK 在广播信道上被发布期间提供了短期间隔。CS 使用加密函数以确定两个值 SK 和 SKI（SK 信息），使得 SK 可以从 BAK 和 SKI 而经确定。例如，SKI 可能是将 BAK 作为密钥的 SK 的加密。在一示例实施例中，SKI 是 IPSec 分组，其中有效负荷包含使用 BAK 作为密钥加密的 SK 值。或者，SK 可能是对模块 SKI 和 BAK 的串接应用加密哈希函数的结果。CS 理想地保证 SK 的值不会预先被预测。如果 SK 可以预先被预测，则攻击者即非法访问实体能向非预订用户发送预测的 SK 值。

作为一例，假设 N 个 SK 的值在 24 小时时段上被使用。如果 SK 被百分之百准确预测，则攻击者只需要要求 UIM 计算 N 个密钥。攻击者然后使得 N 个密钥对于非预订用户可用。非预订用户可以在每天开始时下载密钥，并不花钱且很方便地接入 HSBS 服务。如果攻击者只能以 50%的准确性预测 SK，则攻击者需要发送大致 2N 个密钥。随着预测的准确性减少，攻击者要生成的密钥数要增加。如果生成、存储和

发布预测的费用超过提供非法接入的好处，则攻击者会放弃发布对 SK 的预测。如果保证攻击者的预测准确性很小，则攻击者会有放弃的可能，从而增加密钥数目，攻击者会生成的密钥数是提供非法接入的费用超过好处的临界点。结果是任何生成 SK 的方案理想地保证了攻击者的最佳预测的准确性足够小。即，SK 的计算应包括一些只能预先以小准确性预测的一些随机值。

在示例实施例中，其中 SK 是以加密的形式，CS 可以使用随机或伪随机函数选择 SK。在另外实施例中，其中 SK 通过对 SKI 和 BAK 应用加密函数而导出，CS 在形成 SKI 时引入不可预测值。SKI 的一些部分是可预测的。例如，SKI 的部分可以在该 SKI 有效期间从系统时间导出。该部分被记为 SKI_PREDICT，作为广播服务的部分可能不被发送到 MS 300。SKI、SKI_RANDOM 的余数可能不可预测。即 SK_RANDOM 是以很小的准确性而被预测。SKI_RANDOM 作为广播服务的部分被发送到 MS 300。MS 300 从 SKI_PREDICT 和 SKI_RANDOM 重建 SKI，并将 SKI 提供给 UIM 308。SKI 可能在 UIM 308 内被重建。SKI 的值为每个新的 SK 而改变。因此，在计算新的 SK 时或是 SKI_PREDICT 和/或 SKI_RANDOM 改变。

CS 为广播传输将 SKI_RANDOM 发送到 BS。BS 广播 SKI_RANDOM，这由天线 302 检测到，并传递到接收电路 304。接收电路 304 将 SKI_RANDOM 提供给 MS 300，其中 MS 300 重建 SKI。MS 300 将 SKI 提供给 UIM 308，其中 UIM 308 使用存储在 SUMU 314 内的 BAK 获得 SK。SK 然后由 UIM 308 提供给 ME 306。ME 306 将 SK 存储在内存存储单元 MEM 310 中。ME 306 使用 SK 对从 CS 接收到的广播传输解密。

CS 和 BS 在对何时 SKI_RANDOM 要被发送的一些准则上达成一致。CS 可能需要通过经常改变 SK 而减少每个 SK 的固有费用。在该情况下，改变 SKI_RANDOM 数据的需要与最优化可用带宽间要进行平衡。在一些示例实施例中，SKI_RANDOM 与加密的内容一起被发送。这使得 MS 300 能生成 SK 并立即开始解密。在许多情况下，这会浪费带宽。一个例外是 SKI_RANDOM 作为通信参数被发送的方案。例如，IPSec 内的 SPI 值被允许改变，且可以被用于包括 SKI_RANDOM 值，如在以下将详述的。

在其它实施例中，SKI_RANDOM 与加密内容被分开发送。SKI_RANDOM 可能甚至在信道而不是广播信道上被发送。当用户“调谐到”广播信道上，接收电路 304 获得用于从“控制信道”定位广播信道的信息。当用户“调谐到”广播信道时可能需要快速接入。这需要 ME 306 在较短的时间内获得 SKI。ME 306 可能已经知道 SKI_PREDICT，然而，BS 将 SKI_RANDOM 在该短时间内提供给 ME 300。例如，BS 可能经常在控制信道上发送 SKI_RANDOM，以及用于定位广播信道的信息，或频繁地

在广播信道上发送SKI_RANDOM。BS“刷新”SKI_RANDOM的值频率越高，MS 300就可以越快地接入广播消息。刷新SKI_RANDOM数据的需要与最优化可用带宽间进行平衡，由于过于频繁地发送SKI_RANDOM数据可能使用在控制信道或广播信道内不可接受的带宽量。

在一些情况中，CS可能选择使用SKI_PREDICT和SKI_RANDOM的值，其中这两个对于每次生成的SK值而改变。在其它情况中，CS可能希望减少SKI_RANDOM改变的次数，使得MS 300不需要经常获得SKI_RANDOM。例如，如果用户在多个HSBS信道间经常改变，则如果SKI_RANDOM值在用户调到另一信道上时的五分钟内不改变会更好。如果SKI_RANDOM改变，则用户必须要等到新的SKI_RANDOM值被广播，说明如果SKI_RANDOM尽可能地保持恒定的方案会对用户更加友好。CS可能希望在SKI_RANDOM值的生存期间使用多个SK值，这是通过使用在任何CS希望改变SK的时候会改变的SKI_PREDICT的值。一个示例使用系统时间；然而，使用系统时间引入附加的涉及同步的问题。

关于广播内容的加密和传输，CS使用当前SK对广播内容进行加密。示例实施例使用加密算法，诸如高级加密标准（AES）密码算法。在示例实施例中，加密内容然后由IPSec分组根据封装安全性有效负荷（ESP）传输模式而进行传输，如下将讨论。IPSec分组还包含一SPI值，它指示ME 306使用当前SK以对接收到的广播内容进行解密。加密的内容通过广播信道被发送。

接收电路304将RKI和BAKI直接提供给UIM 308。另外，如果CS从SKI_RANDOM和SKI_PREDICT值计算得到SK，则接收电路304将SKI_RANDOM提供给MS 300合适的部分，在那儿它与SKI_PREDICT组合以获得SKI。在一实施例中，SKI被附加到加密的消息上，并为ME 306抽取。SKI由MS 300相关的部分被提供给UIM 308。UIM 308从RKI和A密钥计算RK，使用RK对BAKI解密以获得BAK，并使用SKI和BAK计算SK，以生成由ME 306使用的SK。ME 306使用SK对广播内容解密。示例实施例的UIM 308可能不足以强大以实时对广播内容进行解密，因此SK被传递到ME 306以对广播解密。

根据一示例实施例，图5B说明密钥的传输和处理，包括RK、BAK和SK。如说明的，在注册时，MS 300接收RK信息（RKI）并将其传递到UIM 308，其中SUPU 316使用RKI和A密钥计算RK，并将RK存储在UIM内存存储SUMU 314内。MS 300周期性地接收BAK信息（BAKI），它包括使用对UIM 308特定的RK值加密的BAK。加密的BAKI使用SUPU 316解密以恢复BAK，它被存储在UIM内存存储SUMU 314

内。MS 300 还周期性地获得 SKI。在示例实施例中，MS 300 接收 SKI_RANDOM，它与 SKI_PREDICT 一起组合形成 SKI。SUPU 316 从 SKI 和 BAK 计算 SK。SK 被提供给 ME 306，用于对广播内容解密。

在示例实施例中，CS 密钥不一定经加密并发送到 MS；CS 可能使用其它的方法。由 CS 生成的要传递到每个 MS 的密钥信息提供了足够的信息，使得 MS 能计算密钥。如图 6 的系统 350 内说明的，RK 由 CS 生成，但 RK 信息（RKI）被发送到 MS。CS 发送足以使 UIM 能导出 RK 的信息，其中预定的函数用于从来自 CS 的发送信息中导出 RAK。RKI 包含足够的信息用于使得 MS 确定来自 A 密钥和其它值（诸如系统时间）的原始 RK，使用预定的公共函数，被标为 d1，其中：

$$RK = d1(A\text{-}key, RKI) \quad (3)$$

在示例实施例中，函数 d1 定义了加密类型函数。根据一实施例，RK 被确定为：

$$RK = SHA'(A\text{-}key \,||\, RKI), \quad (4)$$

其中“||”表示包含 A 密钥和 RKI 的模块的串接，而 SHA'(X)表示给出输入 X，安全哈希算法 SHA－1 的输出的最后 128 位。在另一实施例中，RK 被确定为：

$$RK = AES(A\text{-}key, RKI) \quad (5)$$

其中 AES（X，Y）表示使用 128 位 A 密钥对 128 位模块 RKI 的加密。在根据 AKA 协议的进一步实施例中，RK 被确定位 3GPP 密钥生成函数 f3 的输出，其中 RKI 包括 RAND 的值以及标准定义的 AMF 和 SQN 的合适的值。

BAK 的处理方式不同，因为带有 RK 不同值的多个用户必须计算 BAK 的相同值。CS 可能使用任何技术以确定 BAK。然而，与特定 UIM 308 相关联的 BAKI 的值必须是 BAK 在与该 UIM 308 相关联的唯一 RK 下的加密。SUPU 316 使用存储在 SUMU 314 内的 RK 对 BAKI 进行解密，这是根据被标为 d2 的函数，根据：

$$BAK = d2(BAKI, RK) \quad (6)$$

在另一实施例中，CS 可能通过使用 RK 对 BAK 应用解密过程而计算 BAKI，且 SUPU 316 通过使用 RK 对 BAKI 应用加密过程而获得 BAK。这被认为是与 CS 加密 BAK 和 SUPU 316 对 BAKI 解密等价。其它的实施例可能在图 6 说明的位置或附加地实现多个密钥的组合。

SK 以与 RK 类似的方式进行处理。在一些实施例中，SKI 首先从 SKI_PREDICT 和 SKI_RANDOM 导出，其中 SKI_RANDOM 是从 CS 发送到 MS 的信息。然后被标为 d3 的预定函数被用于从 SKI 和 BAK（存储在 SUMU 314 内）导出 SK，根据：

$$SK = d3(BAK, SKI). \quad (7)$$

在一实施例中，函数 d3 定义加密类型函数。在示例实施例中，SK 被计算为：

$$SK = SHA(BAK \,||\, SKI), \quad (8)$$

其中在另一实施例中，SK 被计算为：

$$SK = AES(BAK, SKI) \quad (9)$$

为广播消息提供安全性的方法在图 7A－7D 内说明。图 7A 说明注册过程 400，其中订户与 CS 在步骤 402 处进行注册协商。在步骤 404 处的注册提供给 UIM 一个唯一的 RK。UIM 在步骤 406 处将 RK 存储在安全内存单元（SUMU）。图 7B 说明 CS 和 MS 间的预订过程。在步骤 422，CS 为 BAK 时间段 T1 生成 BAK。BAK 在整个 BAK 时间段 T1 期间是合法的，其中 BAK 经周期性更新。在步骤 424，CS 授权 UIM 在 BAK 计时器时段 T1 期间接入广播内容（BC）。在步骤 426 处，CS 使用每个订户的单个 RK 对 BAK 进行加密。加密的 BAK 被称为 BAKI。在步骤 428，CS 然后将 BAKI 发送到 UIM。在步骤 430，UIM 接收 BAKI 并使用 RAK 实现解密。解密后的 BAKI 导致原始生成的 BAK。UIM 在步骤 432 将 BAK 存储在 SUMU 内。

当用户在特定 BAK 更新时段内预订广播时，CS 发送合适的信息 BAKI，其中 BAKI 对应用 RK 加密的 BAK。这一般发生在该 BAK 更新时段开始前或当 MS 第一次在该 BAK 更新时段间调谐到广播信道上。这可能根据各种准则由 MS 或 CS 初始。多个 BAKI 可能被同时发送和解密。

值得注意的是当 BAK 更新时段快要过期时，MS 可能请求来自 CS 的更新的 BAK，如果 MS 已经预订了下一 BAK 更新时段。在另一实施例中，第一计时器 t1 为 CS 使用，其中在计时器超时时，即满足了 BAK 更新时段时，CS 发送 BAK。CS 可能在比预先计划好的时间前改变 BAK 的值。如果例如公开公布了当前的 BAK 值时这可能是需要的。

值得注意的是，对于用户而言，可能在 BAK 更新时段期间接收 BAK，其中例如当 BAK 更新是每个月进行一次，而订户在月中时加入服务。另外，BAK 和 SK 更新的时段可能被同步，使得所有的订户在给定时间被更新。

图 8A 说明根据示例实施例的无线通信系统 500 的注册过程。CS 502 与每个订户协商，即 MS 512，以生成对每个订户特定的 RK。RK 被提供给每个 MS 的 UIM 内的 SUMU 单元。如说明的，CS 502 生成存储在 UIM_1 的 $SUMU_1$ 510 内的 RK_1。类似地，CS 502 相应生成存储在 UIM_2 的 $SUMU_2$ 510 内和 UIM_N 的 $SUMU_N$ 510 内的 RK_2 的 RK_N。

图 8B 说明系统 500 内的订户过程。CS 502 进一步包括多个编码器 504。每个编码器 504 接收一个唯一的 RK 和在 CS 502 内生成的 BAK 值。每个编码器 504 的输出时为订户特别编码的 BAKI。BAKI 在每个 MS 的 UIM 处被接收到，诸如 UIM_1 512。每个 UIM 包括 SUPU 和 SUMU，诸如 UIM_1 的 $SUPU_1$ 514 和 $SUMU_1$ 510。SUPU 包括解码器，诸如解码器 516，它通过应用 UIM 的 RAK 而恢复 BAK。过程在每个订户处经重复。

图 8D 说明在注册和预订后的 BC 的处理。CS 502 包括使用当前 SK 对 BC 编码以生成 EBC 的编码器 560。EBC 然后被发送到订户。每个 MS 包括编码器，诸如编码器 544，它使用 SK 从 EBC 抽取 BC。

以下的描述考虑四个示例实施例，它可能被用于更新 SK 并广播内容。在第一示例实施例中，SK 从在包含广播内容的 IPSec 分组的头部内的 BAK 和 SPI 值导出。在第二示例实施例中，SK 从 BAK 表、在包含广播内容的 IPSec 分组的头部内被标为 RAND 和 SPI 值的广播随机值导出。在第三示例实施例中，SK 从 BAK、系统时间和标为 SK_RAND 的广播随机值导出。在第四示例实施例中，SK 作为 BAK 加密的 IPSec 分组被发送。其它的实施例可能提供 SK 作为上述的实施例的组合，或使用其它机制以经常提供 SK 给 MS，迫使放弃对广播服务的未授权接入。

由于短期密钥（SK）用于对广播内容进行加密和解密，且被存储在易被非法访问的存储器内，其中 SK 一般经常改变。存在如何经常改变 SK 而同时平衡以下四个目标的问题：1）对于刚调谐到广播的移动站最小化 SK 更新等待时间或中断时段；2）最小化用于更新 SK 值的带宽量；3）增加安全性等级；以及 4）增加 SK 与 IPSec 合并的容易性。频繁的更新可能减少中断时段，但其代价为需要更多的带宽以发送频繁的更新。

一个解决方案提供了一种方法，不使用附加的带宽而提供用于在每个加密的广播内容分组内实现 SK 更新的足够的信息。因此，中断时段可能不一定需要附加的带宽而最小化。在此揭示的四个示例实施例，用于实现 SK 更新，有各种优势和劣势。所有的四个实施例提供了足够安全的方法。第一实施例去除了终断时段，并不使用附加的带宽以更新 SK 值。其它的实施例可能在高度使用时段有中断时期。第一实施例很简单地能与 IPSec 合并。

根据用于实现 SK 更新的第一实施例，上述的问题的解决是通过定义 SK，它作为广播访问密钥（BAK）和 ESP 头部内的 SPI 的函数对给定的 IPSec 分组进行加密。这样，不是在分开的流内提供 SK，SK 从内容流中计算得到。假设 MS 已经如上所述

接收到了 BAK，则 MS 能立即为每个内容分组计算 SK，而不需要等待附加的 SK 更新信息。这有效地去除了任何 SK 用于新广播接收的更新等待时间。一旦 MS 接收到内容分组，则 MS 可以立即确定 SK 并对内容解密。

足以在 MS 处计算 SK 的信息在 IPSec 分组内被提供。IPSec 分组使用 IP 封装安全性有效负荷(ESP)且在 RFC 1827 内有所规定，题为“IP Encapsulating Security Payload(ESP)”，R. Atkinson, 1995 年 8 月，如上所述。ESP 是一种提供 IP 数据报完整性和机密性的机制。在一些情况下，它还可以提供 IP 数据报的验证。图 9A 根据一实施例说明一 IPSec 分组 600，包括 IP 头部 602、ESP 头部 604 和有效负荷 606。封装安全性有效负荷（ESP）可能出现在 IP 头部后和最后传输层协议前的任何位置。一般，ESP 包括后接封装数据的未加密头部。

ESP 头部字段 604 包括安全性关联标识符，被称为 SPI。根据上述的第一实施例，包含广播内容的 IPSec 分组包括与 SK 相关的 SPI，被称为 SPI_SK。图 9B 说明对应的 32 位 SPI_SK 610 的格式。SPI_SK 610 被分解为两个部分 SPI_RAND 612 和 BAK_ID 614。SPI_RAND 612 是统计随机的随机数，且还用于计算用于对对应的广播内容或有效负荷加密或解密的 SK。SPI_RAND 参数允许内容服务器（CS）经常通过改变 SPI_RAND 值改变内容的有效的 SK 值，从而向 MS 提供了立即计算 SK 值需要的参数。另外，SPI_RAND 实现了 SKI_RANDOM 的角色，如上所述。SPI_RAND 的随机性保证了攻击者不能以较高的准确性预测 SK 的值。由于 SPI 已经是 IPSec 加密分组内的标准参数，即为 ESP 规定的，本实施例不会需要一般与将 SK 作为分开的流发送相关联的附加带宽。BAK_ID 指明哪个 BAK 值用于计算 SK 值。在一实施例中，BAK_ID 是一个四位标记，其中每个标记与 BAK 值相关联。当 MS 实现预订时，MS 在内存存储单元内存储每个接收到的 BAK_ID 以及对应的 BAK 值。根据一实施例，MS 包括用于存储与每个对应 BAK_ID 标识的 BAK 值的查询表（LUT）。BAK LUT 包含在 UIM 内的安全存储器内。

图 9D 说明 BAK LUT 630。LUT 630 内的每项标识了 BAK_ID、对应的 BAK 值和组合的有效期的超时。引入超时是因为 BAK_ID 的小数值。另外的实施例可能避免在 BAK LUT 内使用超时值。在一实施例中，只使用 BAK_ID 的 16 个值。如果每个月发布一个新的 BAK，则 BAK_ID 的值可能在 16 个月后重复。在那时，可能会有所混淆哪个 BAK 值时有效的。超时提供了暂停时间，在这时间后新的项替代过期项。一个原因是因为 CS 可能希望在它们成为有效之前将 BAK 值发送到 MS。另外，CS 可能希望有多个同时有效的 BAK 值，其中不同的 BAK 值可能用于计算不同的 BAK 值。如

果 BAK LUT 不包含对应 BAK_ID 的当前 BAK，则 MS 可能执行获取有效 BAK 的预订。

在从 SPI_SK 抽取了 SPI_RAND 和 BAK_ID 后并获取了对应 BAK_ID 的 BAK 后，UIM 使用密码函数 g 从 BAK 和 SPI_RAND 计算 SK 的值：

$$SK = g(BAK, SPI\_RAND) \quad (10)$$

在一实施例中，函数 g(BAK,SPI_RAND)对应用零填充到 128 位的 SPI_RAND 的加密，它使用带有作为密钥的 BAK 的 AES 加密算法：

$$SK = AES(BAK, SPI\_RAND). \quad (11)$$

在另一实施例中，函数 g(BAK,SPI_RAND)对应计算应用到 BAK 和 SPI_RAND 连接的 SHA－1 的输出的 128 个最不重要比特：

$$SK = SHA(BAK, SPI\_RAND). \quad (12)$$

这样，UIM 不需要为 MS 接收到的每个分组计算 SK 的值。MS 将每个 SPI_SK 值与对应的 SK 值存储在内存存储单元内，诸如查询表（LUT）内。MS 可能将 SPI_SK 和 SK 值作为安全性关联数据库（SAD）内的安全性关联存储，SAD 是一 LUT，其中 MS 存储其它应用需要的一般安全性关联。安全性关联根据目的地地址和 SPI 经索引。当新的 SK 从 SPI_SK 的新值生成时，旧的安全性关联由包含新的 SPI_SK 和 SK 值的安全性关联替换。或者，MS 可能在 SK_LUT 内存储 SPI_SK 和 SK 值，分配给每个广播信道一个 SK_LUT。图 9C 说明 SK LUT 620。LUT 620 内的每个项标识 SPI_SK 以及对应的 SK 值。当 MS 接收到广播内容分组时，ME 首先检查 SAD 和 SK LUT 以了解该表格是否包含等于接收到的分组的 SPI 的 SPI_SK 值。如果表格包含该值，则 ME 使用该值，否则 UIM 计算 SK 的新值。CS 可能还有 BAK LUT、SAD 或 SK_LUT。

图 10 和 11 说明用于实现 SK 更新的一实施例。图 10 说明 CS 的操作方法 700。对于每个 IP 分组，CS 确定用于导出 SK 的 BAK，并在步骤 702 确定对应 BAK 的 BAK_ID。BAK_ID 可能是任何类型的标识符，它能区别多个 BAK 值。CS 在步骤 706 处通过实现预订将 BAK 和 BAK_ID 发送到单个用户处。用户可能在预订时段之前或期间的不同时间实现预订。步骤 702 和 706 可能发生在预订时段开始前。在步骤 710，CS 为 SPI_RAND 值选择一个随机值。如果 BAK_ID 使用 b 位表示，则 SPI_RAND 使用（32－b）位表示。SPI_RAND 值不应在一个 BAK 时段期间重复。在步骤 712 处，一旦 SPI_RAND 和 BAK_ID 是已知的，CS 将它们组合（例如将 BAK_ID 与 SPI_RAND 串接）以形成 SPI_SK。在步骤 714 处，CS 通过使用加密函数将 SPI_RAND 与对应 BAK_ID 的 BAK 组合以形成 SK 而形成 SK。CS 然后在步骤 716 用 SK 对广播消息或消息的部分加密，然后在步骤 718 处发送加密的消息。值得注意的是加密的广播消息是包括

IP 头部和 ESP 头部的 IP 分组的部分。ESP 头部包括 SPI_SK。在判决菱形 720 处，CS 决定是否要改变 SK。如果 CS 决定不改变 SK，则 CS 进行到步骤 716。如果 CS 决定改变 SK，则 CS 进行到判决菱形 724，在此 CS 决定是否改变 BAK。如果 CS 决定不改变 BAK，则 CS 进行到步骤 710。如果 CS 决定改变 BAK，则 CS 进行到步骤 702。

图 11 说明在接收机处对应的操作，诸如 MS 处。方法 750 在步骤 752 处开始，当接收机接收到包含在 ESP 头部内的 SPI_SK 的 IP 分组时。值得注意的是接收机从 IP 分组抽取 SPI_SK 信息。在接收到 SPI_SK 时，接收机首先检查对应接收到的 SPI_SK 值的 SK 是否被存储在存储器内。

在一实施例中，SPI_SK 被存储在图 4 的 ME 306 单元内存储的 SK LUT 内，在另一实施例中，SPI_SK 被存储在安全性关联数据库内：这两个表格在图 11 内由 SPI 表格标明。在判决菱形 754 处实现 SPI 表格的检查。如果 SK 值在接收机处被存储在存储器内，接收机能在步骤 756 处使用存储的 SK 值对内容分组的有效负荷解码。如果接收机没有存储在存储器内的 SK 值，则接收机在步骤 758 从 SPI_SK 抽取 BAK_ID 和 SPI_RAND。在步骤 760，接收机然后检查 BAK LUT 是否有对应 BAK_ID 的有效 BAK 项。如果 BAK LUT 具有对应 BAK_ID 的有效 BAK，则接收机选择该值并进行到步骤 764。如果 BAK LUT 没有对应 BAK_ID 的有效 BAK，诸如当用户希望预订该时段，则接收机实现预订以获得有效的 BAK，如步骤 762 示出。新的 BAK 与 BAK_ID 一起被存储在 BAK_LUT 内，且接收机进行到步骤 764。在步骤 764，接收机将对应 BAK_ID 值的 BAK（即接收到的 SPI_SK 内的 BAK_ID）与 SPI_RAND 值组合以计算新的 SK。接收机然后使用新的 SK 值以在步骤 766 对内容分组的有效负荷解密。接收机还将由对应 SPI_SK 索引的该 SK 值以及可能 IPSec 分组的目的地地址。

SK 直接从 BAK 和内容分组内的 SPI_SK 值计算而得。BAK 改变没有 SK 改变这么频繁，例如 BAK 可能一个月改变一次。因此，接收机能立即从内容分组确定 SK 值，而没有附加延时，且不需要更多的带宽以发送 SK 更新。

根据一实施例，SK 计算给出为：

$$SK=f(SPI\_SK, BAK), \qquad (13)$$

其中函数被定义为使用 BAK 的 SPI_SK 的加密。由于 SPI_SK 由 SPI_RAND 和 BAK_ID 组成，则等式（13）可能给出为：

$$SK=f(SPI\_RAND, BAK\_ID) \qquad (14)$$

用于实现 SK 更新的第二示例实施例引入对 SK 计算附加的随机性方面，其中 SK 被定义为 BAK、SPI_RAND 和附加参数 RAND 的函数。RAND 参数对几个 SK 值保持

恒定。RAND 使得更多不同的 SK 值能通过改变 SPI_SK 和 RAND 从单个 BAK 值中导出。如果没有使用 RAND，则最多有 2^{32} 的 SK 值可以通过改变 SPI 从单个 BAK 中导出。然而，如果使用 96 位的 RAND，则可以有多达 2^{218} 个 SK 值从单个 BAK 中通过改变 SPI_RAND 和 RAND 而导出。（这些数字不计及用于表示 BAK_ID 的 SPI 的位）。现在，不是 SPI_SK 只标识 BAK，SPI_SK 必须还包含标识 RAND 的信息。为了实现 RAND 值，SPI_SK 形成有三个部分：1）BAK_ID 标识要使用的 BAK 值；2）RAND_ID 标识要使用的 RAND；以及 3）SPI_RAND 值提供在 SPI_SK 内频繁改变的随机性。

图 12 说明 IP 分组的 SPI_SK 800 部分，包括 SPI_RAND 802、BAK_ID 804 和 RAND_ID 806。SPI_RAND 802 和 BAK_ID 804 如上所述。为了维持 SPI_SK 在预定或特定的位长，SPI_RAND 802 可能使用比图 9B 内允许 RAND_ID 806 使用的 SPI_RAND 612 少的位数。RAND_ID 806 对应于用于计算 SK 的 RAND 值，且可能是四位标记或其它标识符。RAND_ID 和对应的 RAND 值被存储在接收机处的 LUT 内。图 12B 说明 RAND LUT 820。RAND LUT 820 包括每个 RAND 值的项，列出 RAND_ID 和与 RAND 值相关的超时。

图 13 说明 CS 的操作。对于每个 IP 分组，发射机确定用于导出 SK 的 BAK，并在步骤 902 确定对应 BAK 的 BAK_ID。BAK_ID 可能是任何类型的标识符，它能区别多个 BAK 值。CS 通过在步骤 904 处实现预订而将 BAK 和 BAK_ID 发送到单个用户。用户可能在预订时段前或期间的不同时刻实现预订。步骤 902 和 904 可能在预订时段开始前发生。在步骤 906，发射机选择 RAND 值，并确定对应的 RAND_ID。CS 可能将 RAND 和 RAND_ID 单独发送到 MS 或将 RAND 和 RAND_ID 发送到广播信道上进行广播。RAND 值不需要是机密的，所以它不用被加密。如果广播 RAND 和 RAND_ID，则不应在重发间有许多时间，使得 MS 在获得 RAND 值前不需要等待很长时间。广播 RAND 和 RAND_ID 会在时间上使用很大带宽。然而，如果有大量用户调谐到信道，则需要大量带宽将 RAND 单独发送到每个用户。结果是，如果有大量用户调谐到该信道，则 RAND 和 RAND_ID 只能被广播。在步骤 910，CS 选择 SPI_RAND 的随机值。

一旦 SPI_RAND、BAK_ID 和 RAND_ID 已知，在步骤 912，发送机将其组合（例如将 RAND_ID 和 BAK_ID 串接为 SPI_RAND）以形成 SPI_SK。CS 使用密码函数以组合 SPI_RAND、BAK（用 BAK_ID 标识）和 RAND（以 RAND_ID 标识）以形成 SK。CS 然后在步骤 916 用 SK 对广播消息或消息部分加密，并在步骤 918 发送加密的消息。值得注意的是加密的广播消息是 IP 分组的一部分，IP 分组包括 IP 头部和 ESP 头部。ESP 头部包括 SPI_SK。在判决菱形 920 处，CS 决定是否要改变 SK。如果 CS

决定不改变 SK，则 CS 进行到步骤 916。如果 CS 决定改变 SK，则 CS 进行到判决菱形 922，在此 CS 决定是否改变 RAND。如果 CS 决定不改变 RAND，则 CS 进行到步骤 910。如果 CS 决定改变 RAND，则 CS 进行到判决菱形 924，在此 CS 决定是否改变 BAK。如果 CS 决定不改变 BAK，则 CS 进行到步骤 906。如果 CS 决定改变 BAK，则 CS 回到步骤 902。

图 14 说明在接收机处的对应操作，诸如 MS 处。方法 950 开始于当接收机在步骤 952 处接收到包含在 ESP 头部内的 SPI_SK 的 IP 分组时。值得注意的是接收机从 IP 分组抽取 SPI_SK 信息。在接收到 SPI_SK 时，在判决菱形 952 处，接收机首先检查是否对应接收到的 SPI_SK 值的 SK 被存储在内存内。在一实施例中，SPI_SK 被存储在 SK LUT，该 LUT 存储于图 4 的 ME 单元 306 内，在另一实施例中，SPI_SK 被存储在安全性相关数据库内，这些表格在图 14 内被标为 SPI 表格。检查 SK LUT 是在判决菱形 954 处实现的。如果 SK 值在接收机处存储在内存内，则在步骤 956 处，接收机能使用存储的 SK 值对内容分组的有效负荷解密。如果接收机没有 SK 值存储在内存内，则接收机在步骤 958 从 SPI_SK 抽取 BAK_ID 和 SPI_RAND。在步骤 960，接收机然后检查 BAK LUT 是否有对应 BAK_ID 的合法的 BAK 项。如果 BAK LUT 具有对应 BAK_ID 的合法的 RAND，则接收机选择该值，并进行到步骤 964。如果 BAK LUT 没有对应 BAK_ID 的合法 BAK，则（假如用户希望预订该时段）接收机实现预订以获得合法的 BAK，如步骤 962 示出。新的 BAK 于 BAK_ID 存储在 BAK_LUT 内，且接收机进行到步骤 864。在步骤 964，接收然后检查 RAND LUT 是否有对应 RAND_ID 的合法 RAND 项。如果 RAND LUT 具有对应 RAND_ID 的合法 RAND，则接收机选择该值并进行到步骤 964。如果 RAND LUT 没有对应 RAND_ID 的合法 RAND，则接收机获得 RAND 和 RAND_ID，要么通过从 CS 请求该值，要么从广播请求该值，如步骤 966 示出。新的 RAND 值于 RAND_ID 存储在 RAND_LUT 内，接收机进行到步骤 968。接收机组合对应 BAK_ID 值的 BAK、对应 RAND_ID 值的 RAND（即在接收到的 SPI_SK 内的 RAND_ID）和 SPI_RAND 值（也在接收到的 SPI_SK 内）以在步骤 968 处形成新的 SK。在步骤 970 处，接收机然后使用新的 SK 值以对内容分组的有效负荷解密。接收机还存储该由对应 SPI_SK 索引的 SK 值和可能的 IPSec 分组的目的地地址。

RAND 的改变的频度没有 SPI_RAND 高。RAND 值对于所有监听广播的移动站一样。因此，RAND 可能被广播到所有移动站，且不一定是按每接收者特别加密的。因此，如果有足够的移动站收听广播流，则让空中接口几次向所有移动站广播 RAND 值会比需要每个移动站单独从 CS 请求 RAND 值更有效。

根据一实施例，SK 计算给出如下：

$$SK=f(SPI\_SK, BAK, RAND), \quad (15)$$

其中函数被定义为使用 BAK 对 SPI_SK 加密。由于 SPI_SK 是由 SPI_RAND、BAK_ID 和 RAND_ID 组成的。等式（15）还可以给出为：

$$SK=f(SPI\_RAND, BAK\_ID, RAND\_ID, RAND) \quad (16)$$

值得注意的是使用 RAND 值可能引入一些“中断时段”，因为接收机需要在改变时接收 RAND 值。然而，这些时段比 SK 在分开的流上更新以及接收机等待周期性更新的频度要低。RAND 被设计成比 SK 值的改变要慢，因此对 RAND 的更新不那么频繁地被发送。当 MS 由于丢失信号、调谐到另一信道或响应中断（诸如电话呼叫）而停止收听信道时，CS 会希望减少产生的“中断”的概率。中断最可能发生在 RAND 值的生存期的开始。为了解决这点，CS 可能在新 RAND 成为合法时更频繁地重新广播新的 RAND 值。在 RAND 的生存期结束时，可能必须广播当前 RAND 值和下一 RAND 值。RAND 值不应是可预测的，且 CS 应能在 RAND 成为合法的前短时间开始发送 RAND。

如上所述，根据第三示例实施例，SK 从 BAK、系统时间和被称为 SK_RAND 的广播随机值导出。图 7C 说明了在支持广播服务的无线通信系统内更新用于安全性加密的密钥的方法。该方法 440 实现如图 7E 给出的时间段。BAK 以时间周期 T1 周期性地被更新。在 BAK 经计算且在 T1 超时时开始计时器 t1。使用变量计算被称为 SK_RAND 的 SK，它以时间周期 T2 被周期性更新。当 SK_RAND 经生成，且 T2 处超时时，计时器 t2 开始。在一实施例中，SK 进一步以时间周期 T3 的周期性地被更新。当每个 SK 经生成且在时间 T3 超时时开始计时器 t3。SK_RAND 在 CS 处经生成，且被周期性地提供给 MS。MS 和 CS 使用 SK_RAND 以生成 SK，如下将详述。

当更新可应用的 BAK 值时第一计时器 t1 被重设。在两个 BAK 更新间的时间长度是 BAK 的更新时段。在示例实施例中，BAK 更新时段是一个月，然而，其它的实施例可能实现系统的最优操作需要的任何时间周期，或满足各种系统准则。

继续图 7C，方法 440 在步骤 442 处开始计时器 t2 以开始 SK_REG 时间段 T2。在步骤 444 处，CS 生成 SK_RAND 并将该值提供给发射电路以在整个系统内传输。计时器 t3 在步骤 446 处开始，以开始 SK 时段 T3。在步骤 448，CS 然后使用当前 SK 对 BC 加密。加密的积是 EBC，其中 CS 提供 ECB 给发射电路用于在系统内传输。如果计时器 t2 在判决菱形 450 处超时，则处理回到步骤 442。在 t2 小于 T2 时，如果计时器 t3 在判决菱形 452 处超时，则处理回到步骤 446，否则处理回到 450。

图 7D 说明 MS 接入广播服务的操作。方法 460 首先在步骤 462 处用 CS 处值使

计时器 t2 和 t3 同步。在步骤 464 处，MS 的 UIM 接收 CS 生成的 SK_RAND。在步骤 466 处，UIM 使用 SK_RAND、BAK 和一时间测量生成 SK。UIM 将 SK 传递到 MS 的 ME。在步骤 468，UIM 然后使用 SK 对接收到的 EBC 解密以抽取原始的 BC。当计时器 t2 在步骤 470 超时时，处理回到步骤 462。当计时器 t2 小于 T2 时，如果计时器 t3 在步骤 472 超时，则计时器 t3 在步骤 474 处开始并回到 466。

密钥管理和更新在图 8C 内说明，其中 CS 应用函数 508 以生成 SK_RAND 值，该值是 CS 和 MS 使用的中间值以计算 SK。尤其是，函数 508 应用 BAK 值、SK_RAND 和时间因子。虽然图 8C 内的实施例应用计时器以确定何时更新 SK，其它的实施例可以使用其它的措施以提供周期性更新，例如错误或其它事件的发生。CS 提供给每个订户 SK_RAND 值，其中驻留在每个 UIM 内的函数 518 应用如 CS 的函数 508 相同的函数。函数 518 对 SK_RAND、BAK 和计时器值进行操作以生成存储在 ME 内的内存位置内的 SK，诸如 ME_1 540 的 MEM_1 542。

如上所述，根据第四示例实施例，SK 使用 BAK 经加密以形成 SKI，SKI 被发送到 MS。在示例实施例中，SK 在使用 BAK 加密的 IPSec 分组内被发送。CS 还可能广播可以用于标识用 SK 加密的数据对应的 SPI。该实施例不需要进一步讨论。

在上述的示例实施例中，CS 可能选择如 CS 期望的那样更新 SK。SK 改变越频繁，CS 越能防止攻击者发布 SK 值。有时攻击者可能会比其它时间更考虑发布 SK 值的好处。这源于广播的内容的性质。例如，在重大时间发生时，未预订的用户会对接收 HSBS 上的新闻更感兴趣，因此，会比其它时间更愿意支付非法接入费用。在这些时候，CS 可能通过比正常更频繁地改变 SK 而增加费用和不便性以阻止攻击者和未预订用户。CS 必须知道，这限于 UIM 的处理能力。如果 CS 太频繁地改变 SK，则 UIM 会不能实时计算 SK 值，则用户会不能实时对内容进行解密。

本领域内的技术人员可以理解信息和信号可能使用各种不同的科技和技术表示。例如，上述说明中可能涉及的数据、指令、命令、信息、信号、比特、码元和码片最好由电压、电路、电磁波、磁场或其粒子、光场或其粒子、或它们的任意组合来表示。

本领域的技术人员还可以理解，这里揭示的结合这里描述的实施例所描述的各种说明性的逻辑框、模块、电路和算法步骤可以用电子硬件、计算机软件或两者的组合来实现。为清楚地说明硬件和软件的可互换性，各种说明性的组件、方框、模块、电路和步骤一般按照其功能性进行阐述。这些功能性究竟作为硬件或软件来实现取决于整个系统所采用的特定的应用程序和设计约束。技

术人员可以以多种方式对每个特定的应用实现描述的功能，但该种实现决定不应引起任何从本发明范围的偏离。

各种用在此的说明性实施例揭示的逻辑框、模块和电路的实现或执行可以用：通用处理器、数字信号处理器(DSP)或其它处理器、专用集成电路(ASIC)、现场可编程门阵列(FPGA)或其它可编程逻辑器件、离散门或晶体管逻辑、离散硬件组件或任何以上的组合以实现在此描述的功能。通用处理器最好是微处理器，然而或者，处理器可以是任何常规的处理器、控制器、微控制器或状态机。处理器可以实现为计算设备的组合，例如 DSP 和微处理器的组合、多个微处理器、一个或多个结合 DSP 内核的微处理器或任何该种配置。

在此用实施例揭示的方法步骤或算法可能直接在硬件内、处理器执行的软件模块或两者的组合内执行。软件模块可以驻留于 RAM 存储器、快闪(flash)存储器、ROM 存储器、EPROM 存储器、SPI_SKPROM 存储器、寄存器、硬盘、移动盘、CD-ROM、或本领域中已知的其它任意形式的存储媒体中。一示范处理器最好耦合到处理器使处理器能够从存储介质读取写入信息。或者，存储介质可能整合到处理器。处理器和存储介质可驻留于专用集成电路 ASIC 中。ASIC 可以驻留于用户终端内。或者,处理器和存储介质可以驻留于用户终端的离散元件中。

上述优选实施例的描述使本领域的技术人员能制造或使用本发明。这些实施例的各种修改对于本领域的技术人员来说是显而易见的，这里定义的一般原理可以被应用于其它实施例中而不使用创造能力。因此，本发明并不限于这里示出的实施例，而要符合与这里揭示的原理和新颖特征一致的最宽泛的范围。

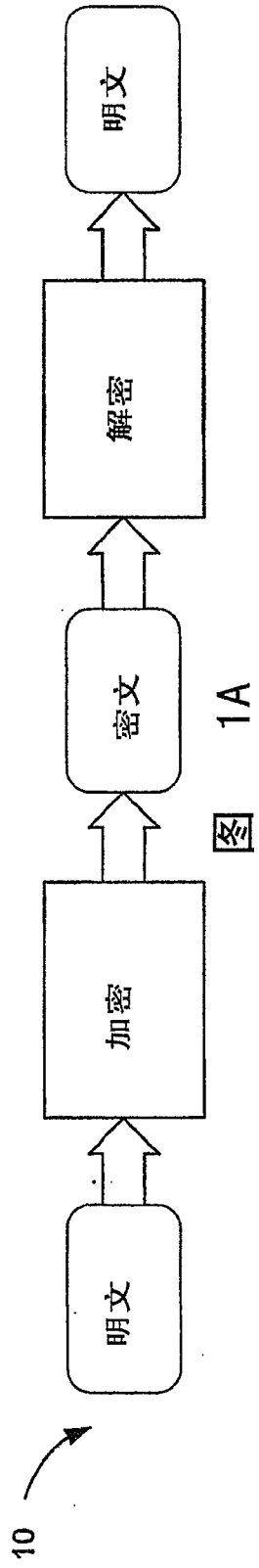


图 1A

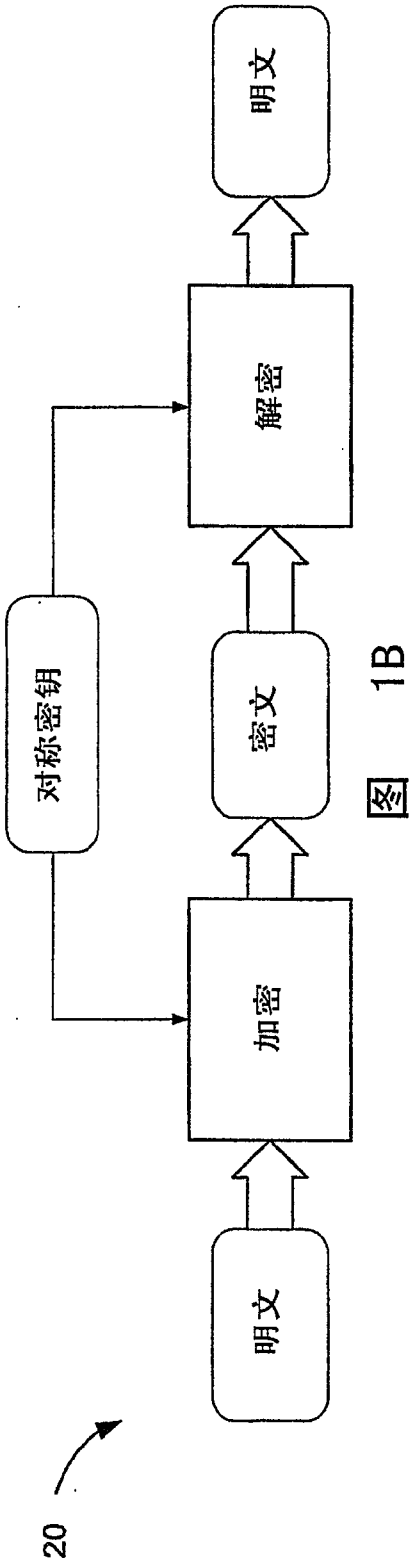


图 1B

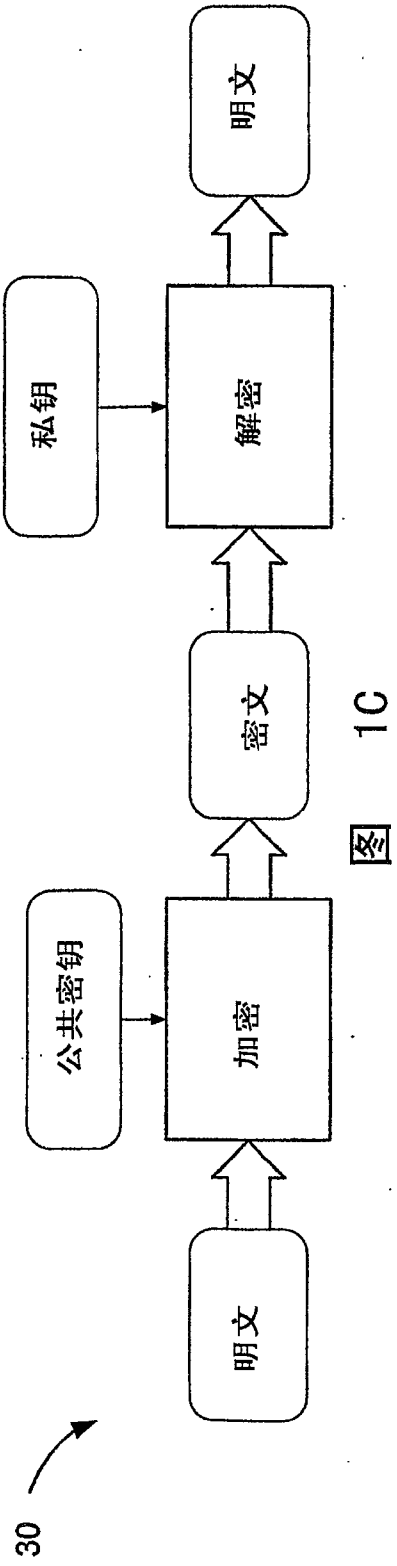


图 1C

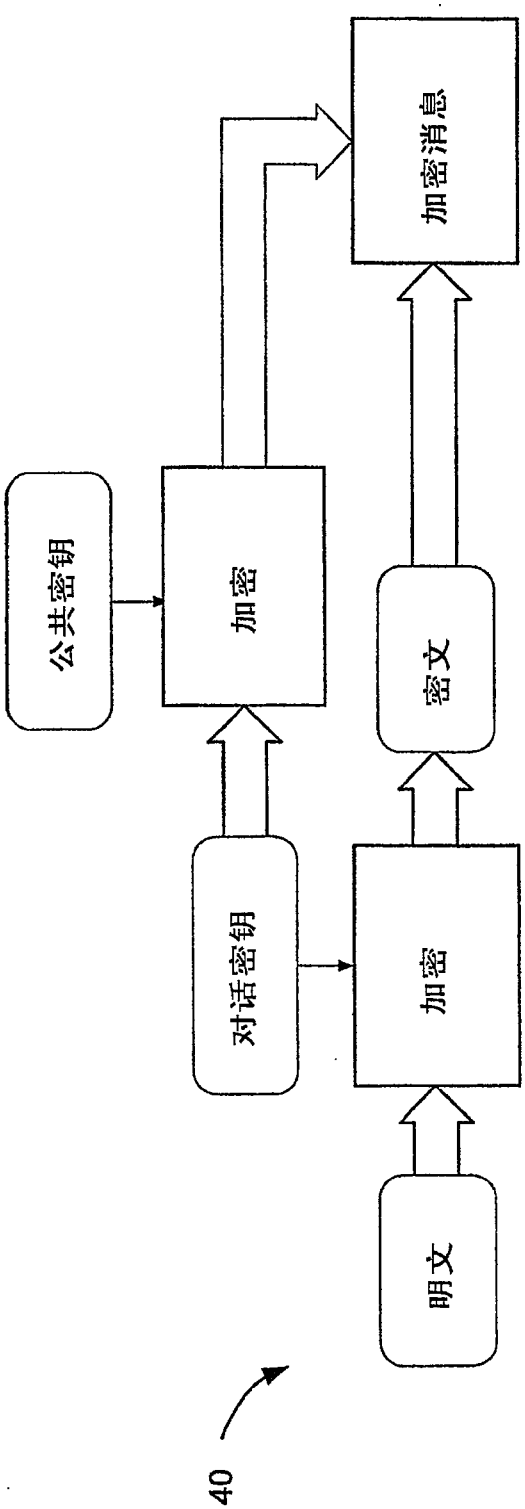


图 1D

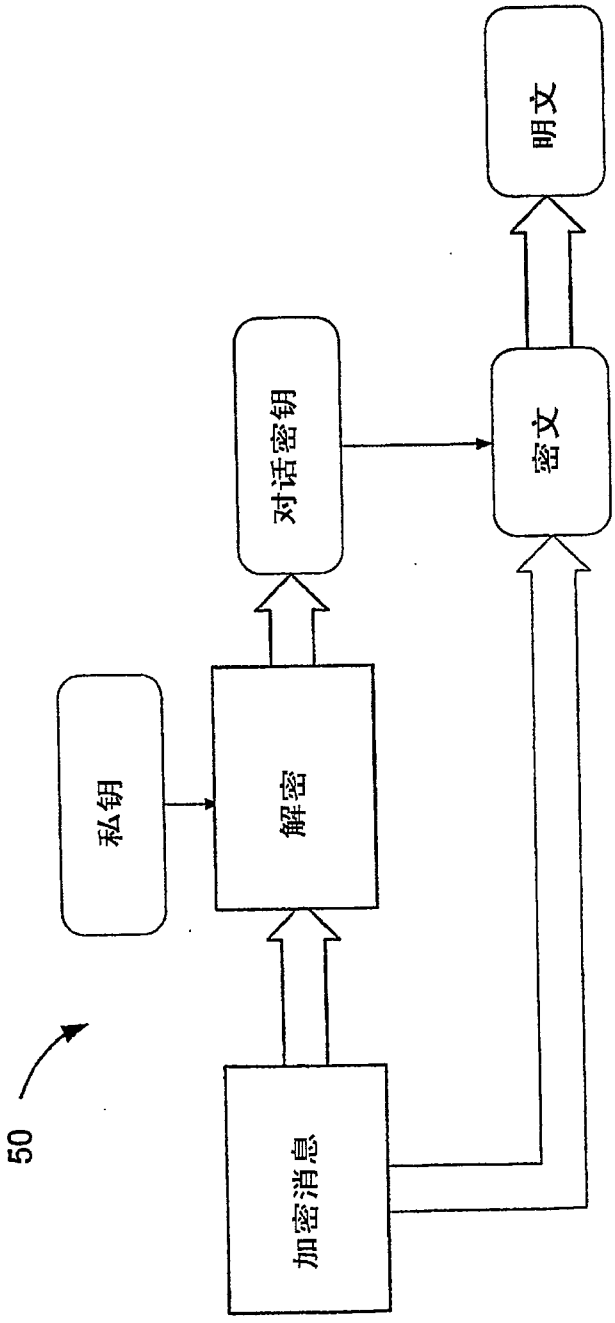


图 1E

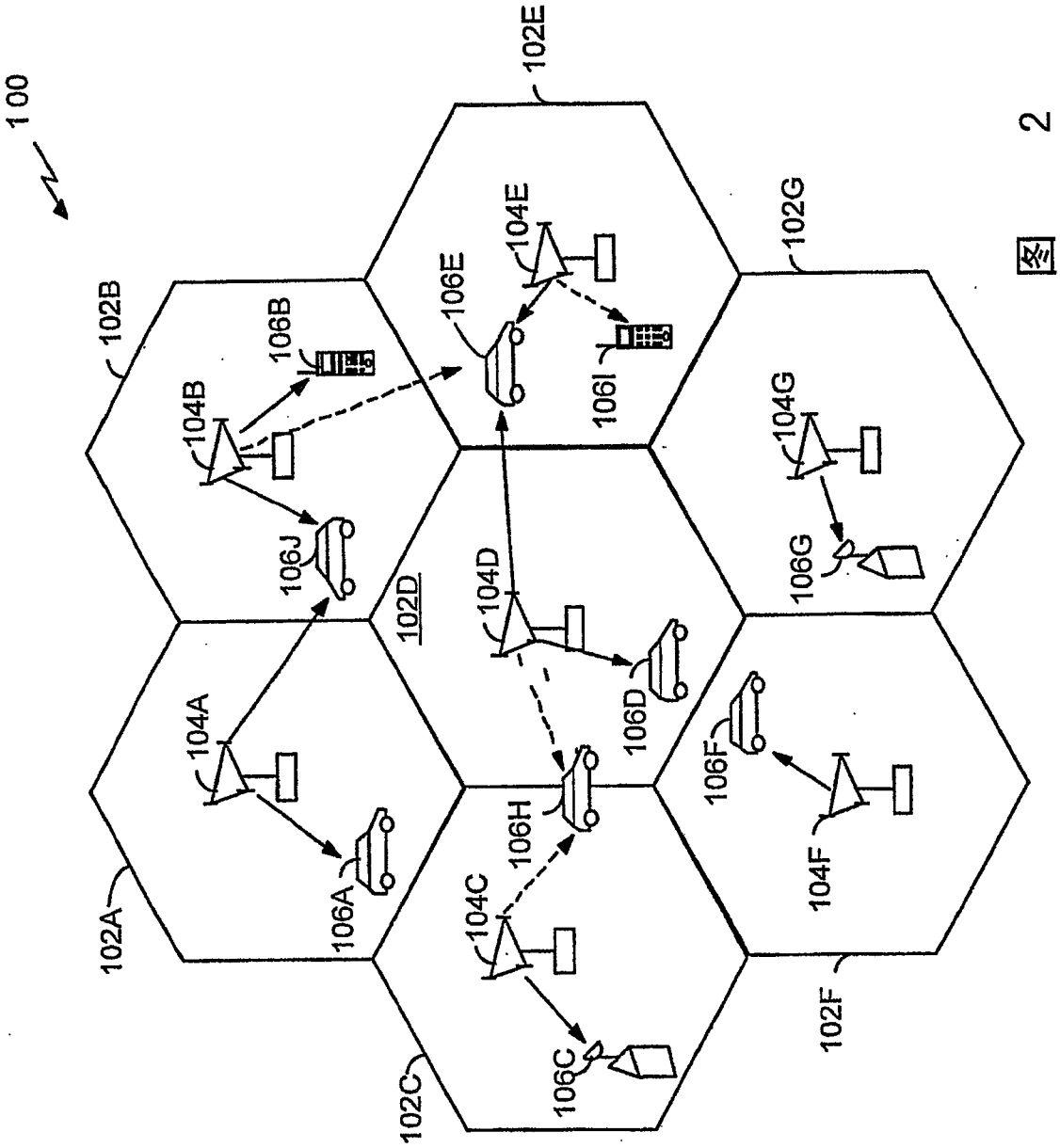

100
102A
102B
102C
102D
102E
102F
102G
104A
104B
104C
104D
104E
104F
104G
106A
106B
106C
106D
106E
106F
106G
106H
106I
106J

图 2

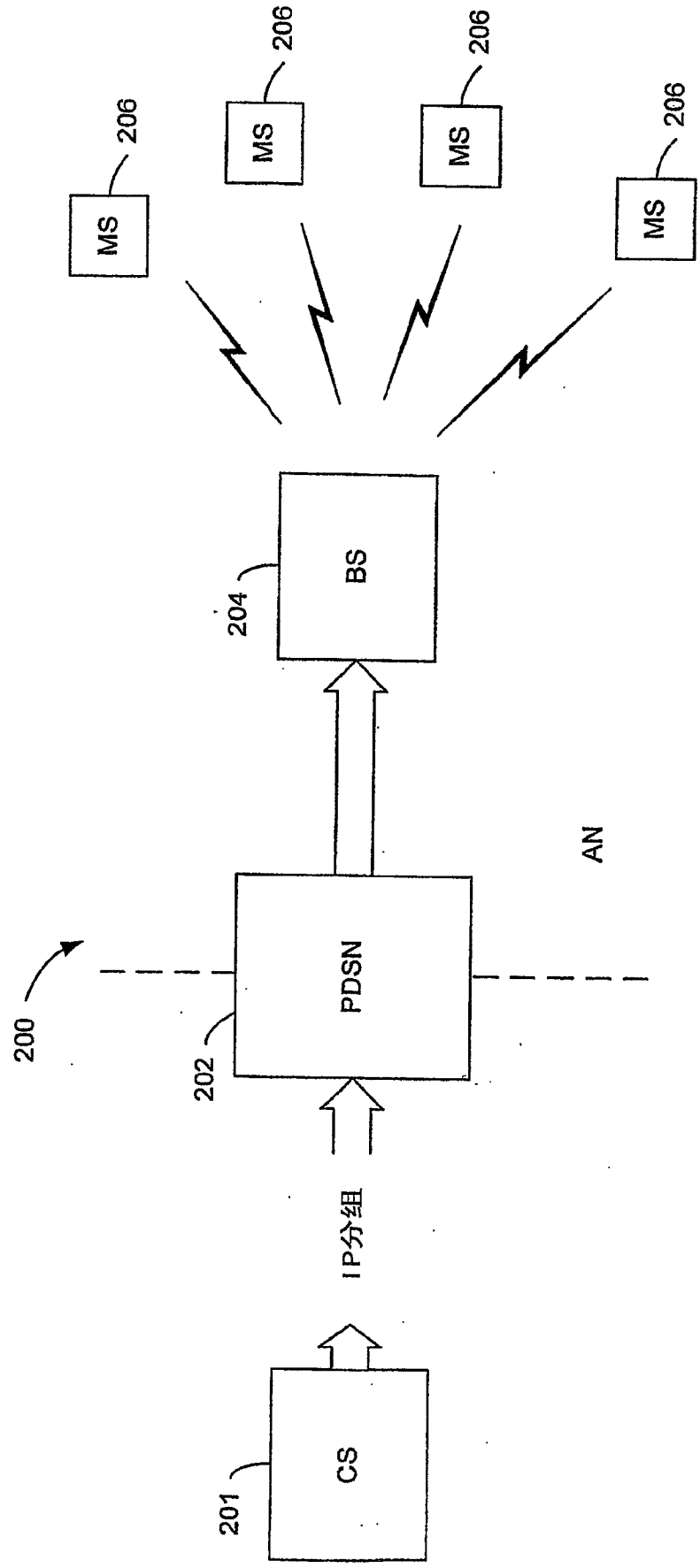


图 3

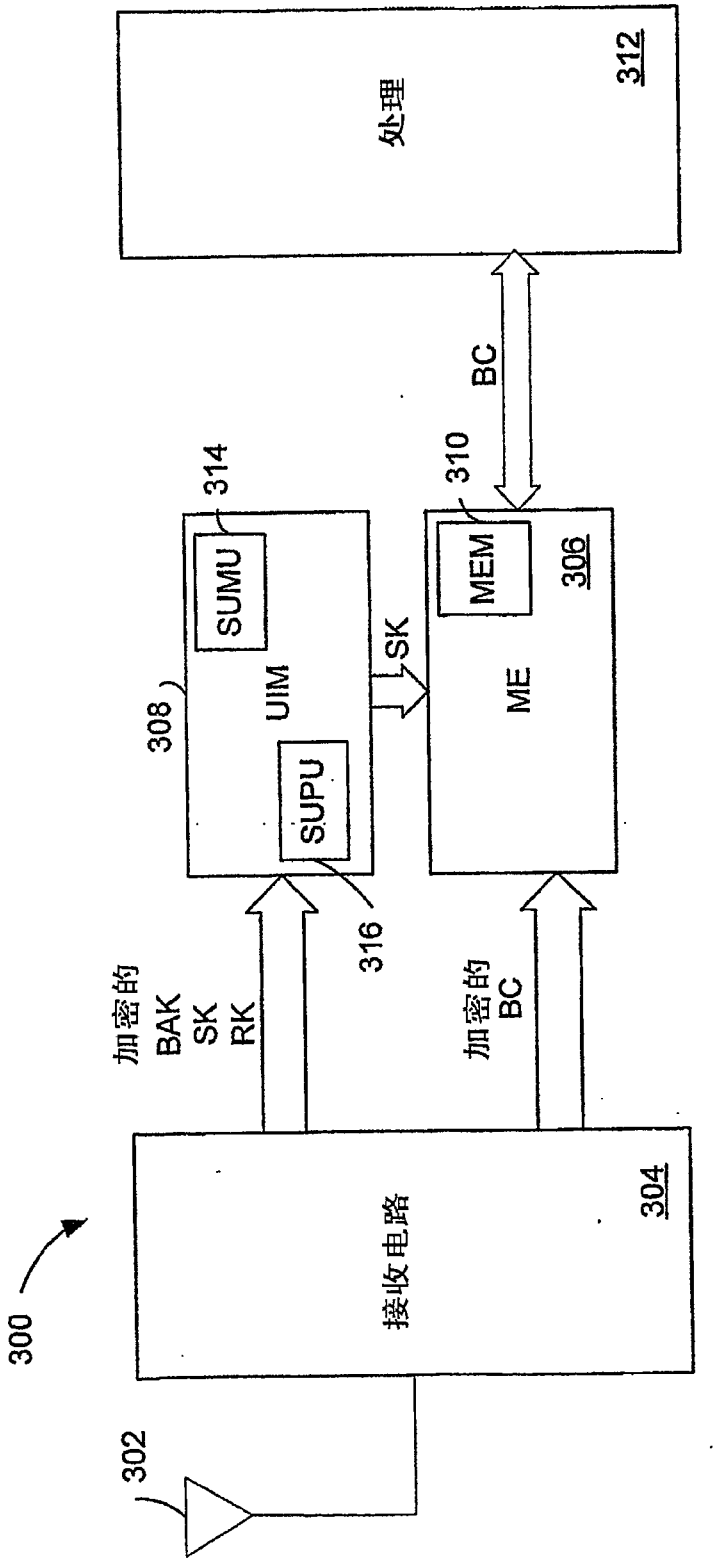

300
302
接收电路
304
加密的
BAK
SK
RK
加密的
BC
316
308
UIM
SUMU
SUPU
314
SK
310
ME
MEM
306
BC
处理
312

图 4

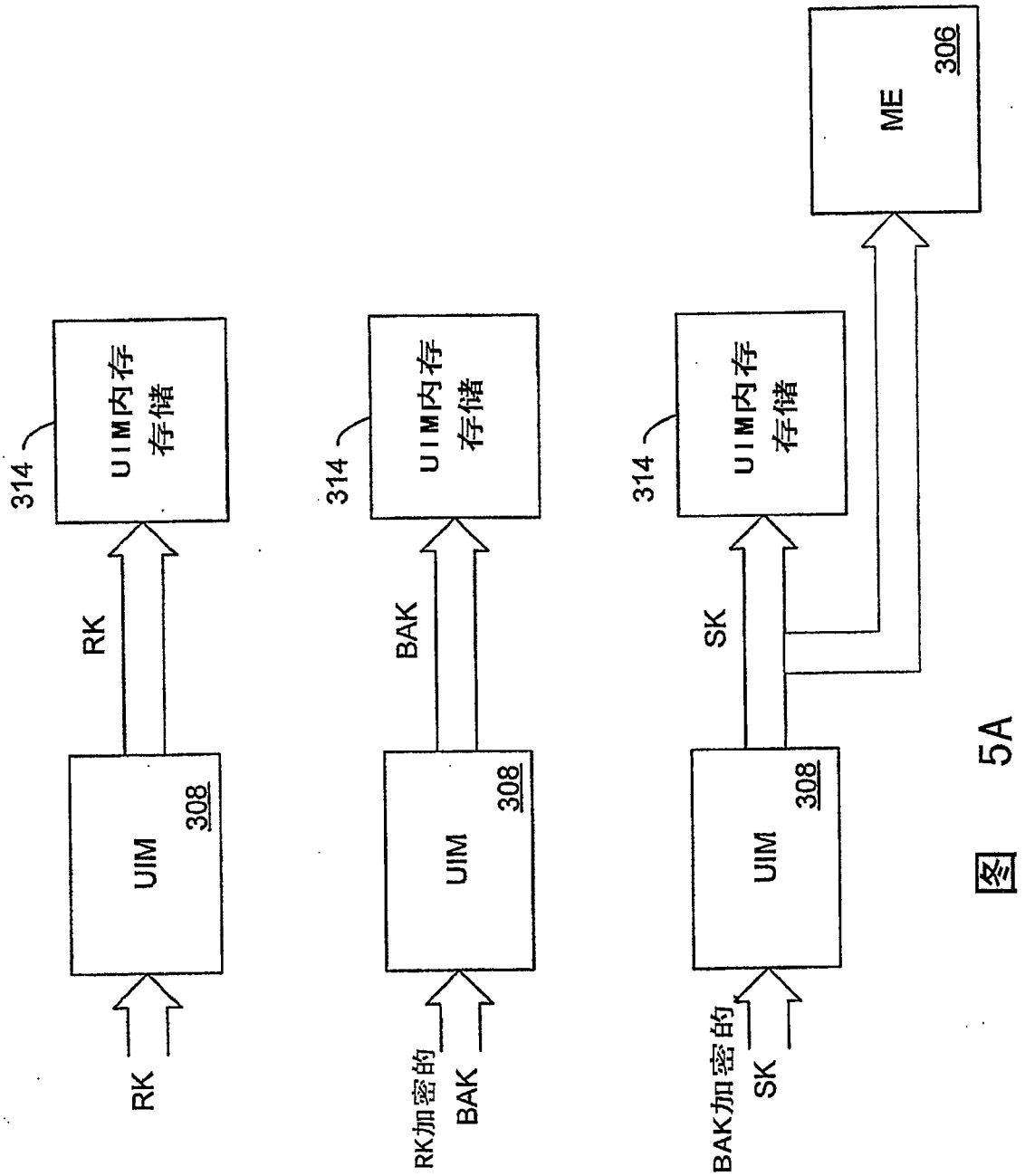

RK
UIM
308
RK
314
UIM内存存储
RK加密的BAK
UIM
308
BAK
314
UIM内存存储
BAK加密的SK
UIM
308
SK
314
UIM内存存储
ME
306

图 5A

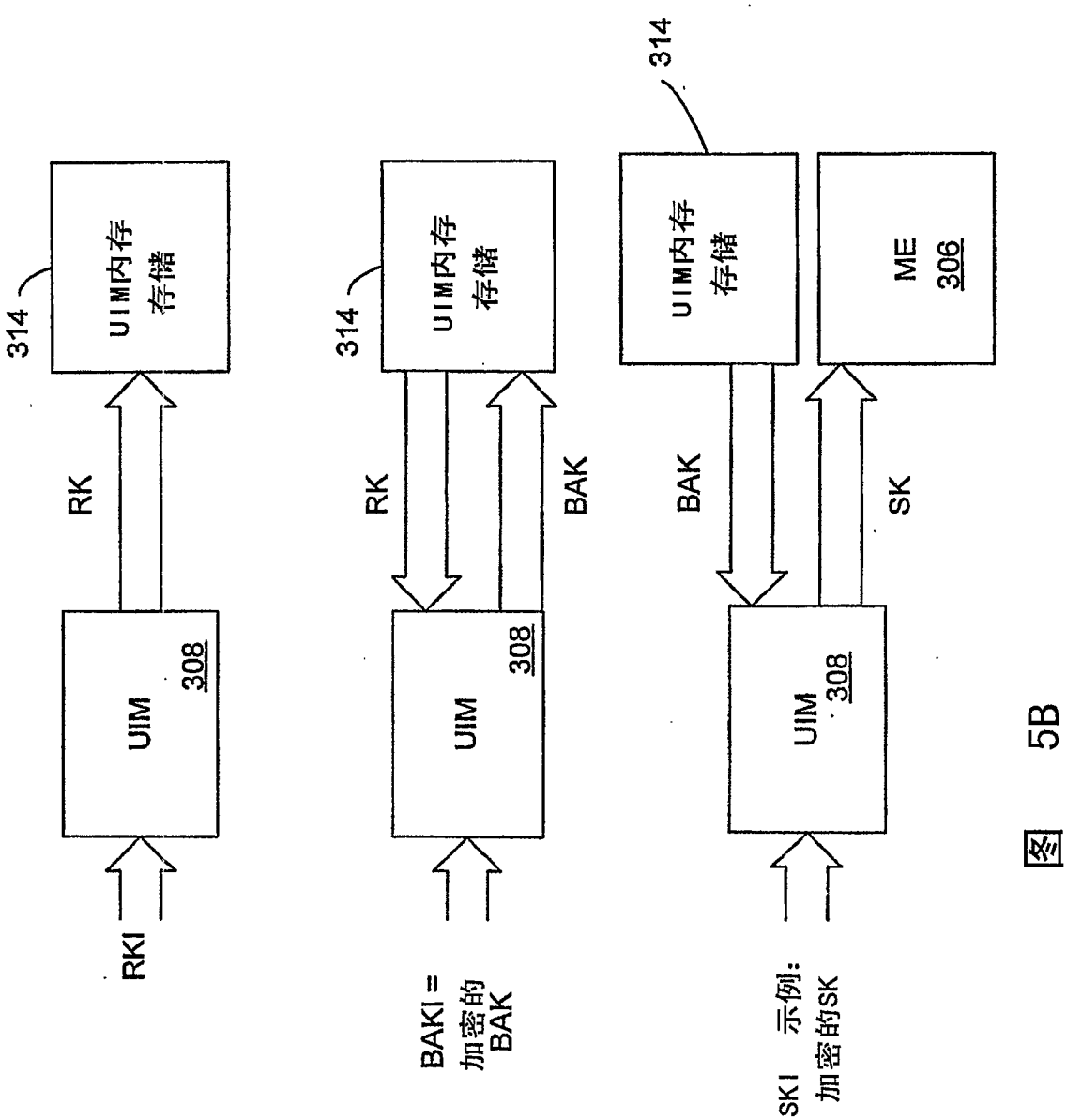

314
UIM内存存储
RK
UIM
308
RKI
314
UIM内存存储
RK
BAK
UIM
308
BAKI = 加密的BAK
314
UIM内存存储
ME
306
BAK
SK
UIM
308
SKI 示例：加密的SK

图 5B

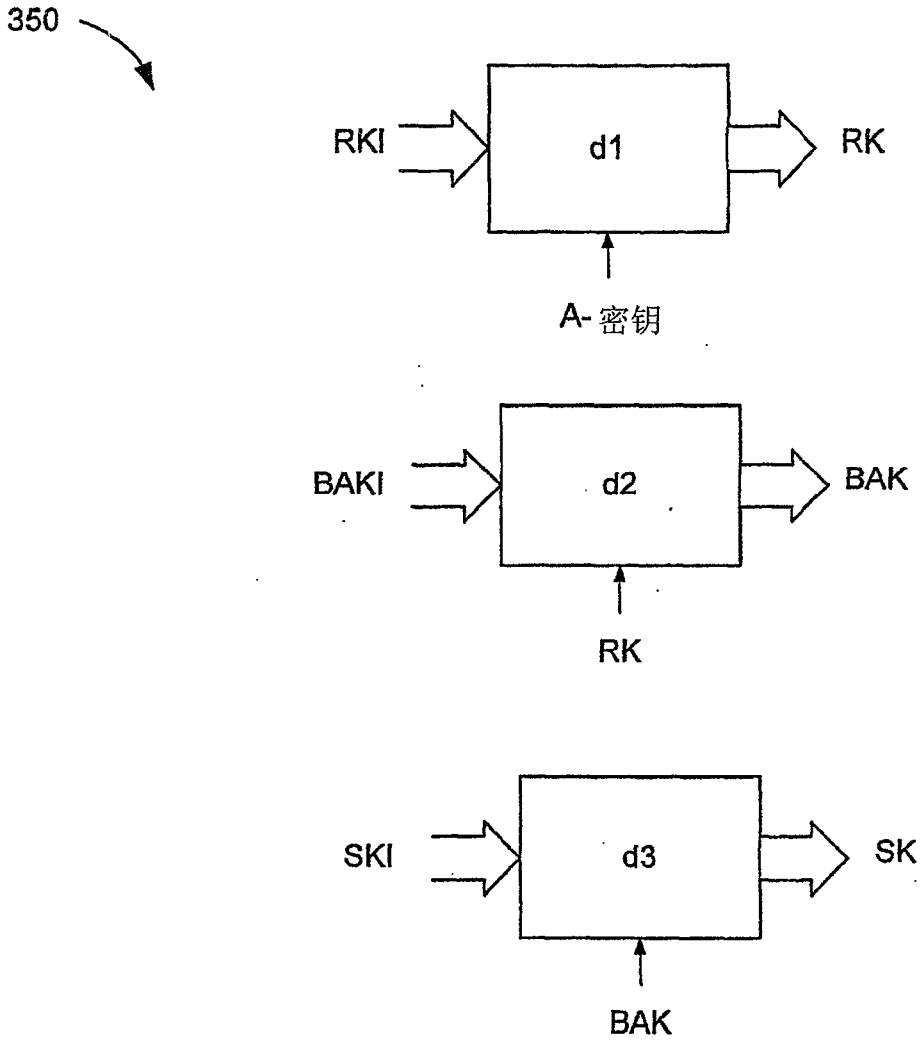


图 6

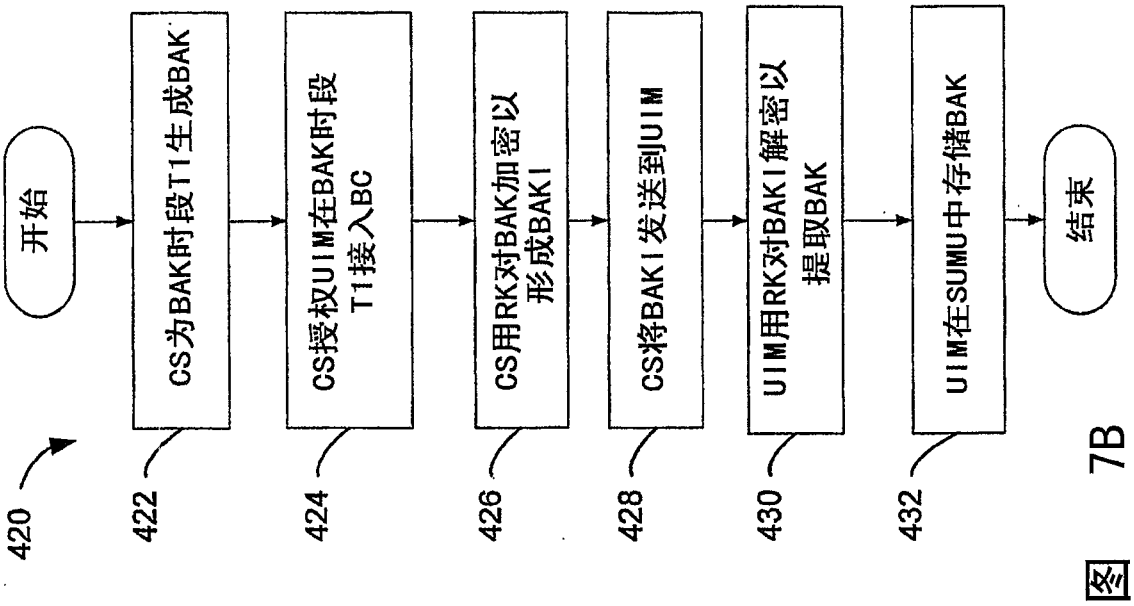

开始
CS为BAK时段T1生成BAK
CS授权UIM在BAK时段T1接入BC
CS用RK对BAK加密以形成BAK1
CS将BAK1发送到UIM
UIM用RK对BAK1解密以提取BAK
UIM在SUMU中存储BAK
结束
420
422
424
426
428
430
432

图 7B

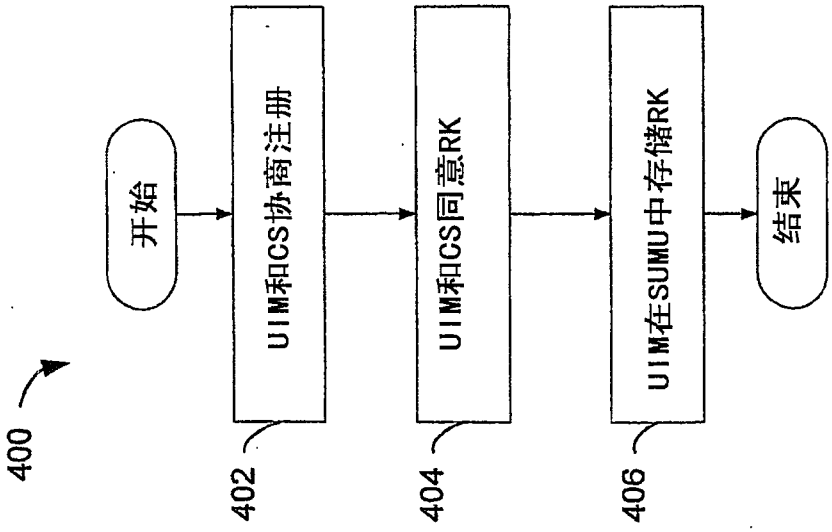

开始
UIM和CS协商注册
UIM和CS同意RK
UIM在SUMU中存储RK
结束
400
402
404
406

图 7A

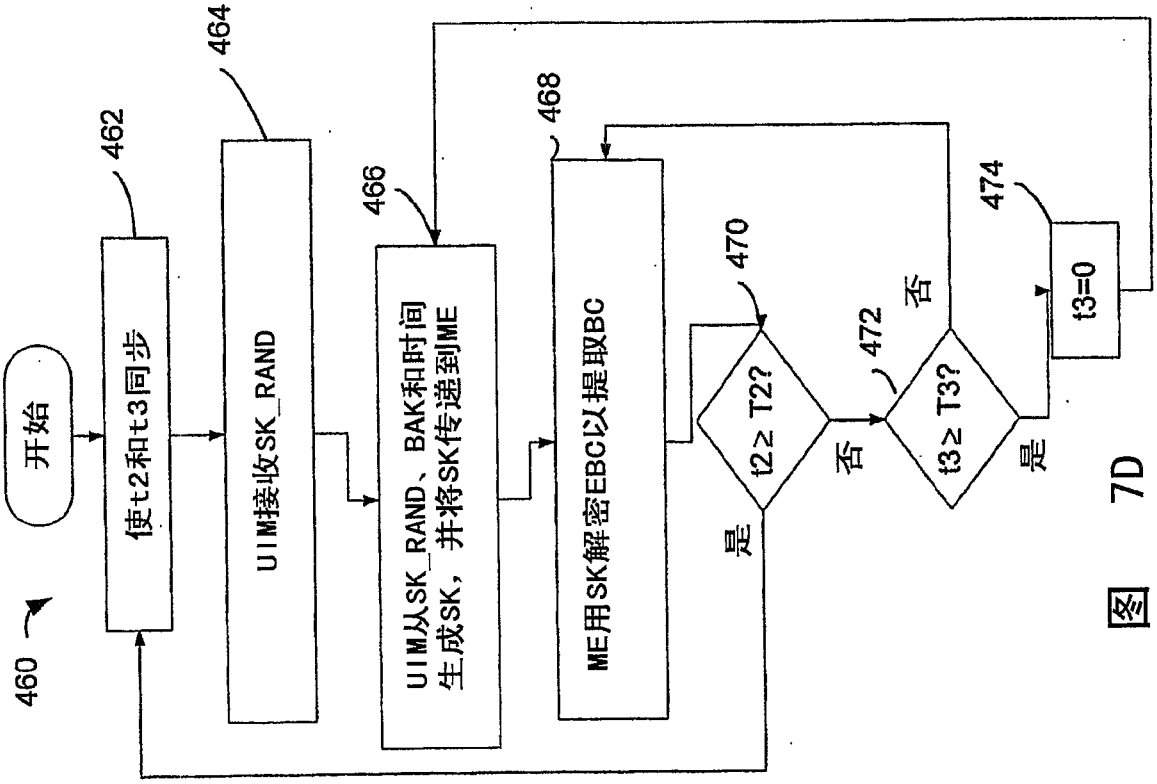

460
开始
462
使t2和t3同步
464
UIM接收SK_RAND
466
UIM从SK_RAND、BAK和时间
生成SK，并将SK传递到ME
468
ME用SK解密EBC以提取BC
470
t2≥ T2?
否
是
472
t3≥ T3?
否
是
474
t3=0

图 7D

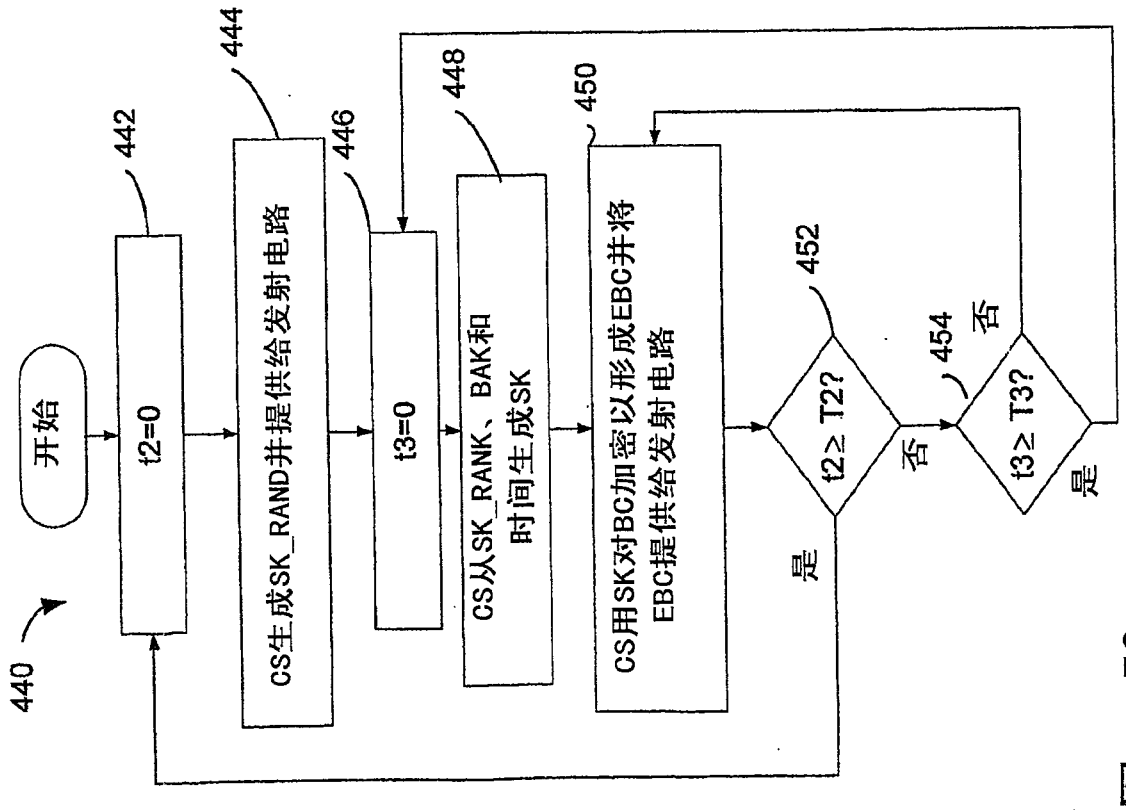

440
开始
442
t2=0
444
CS生成SK_RAND并提供给发射电路
446
t3=0
448
CS从SK_RANK、BAK和
时间生成SK
450
CS用SK对BC加密以形成EBC并将
EBC提供给发射电路
452
t2≥ T2?
否
是
454
t3≥ T3?
否
是

图 7C

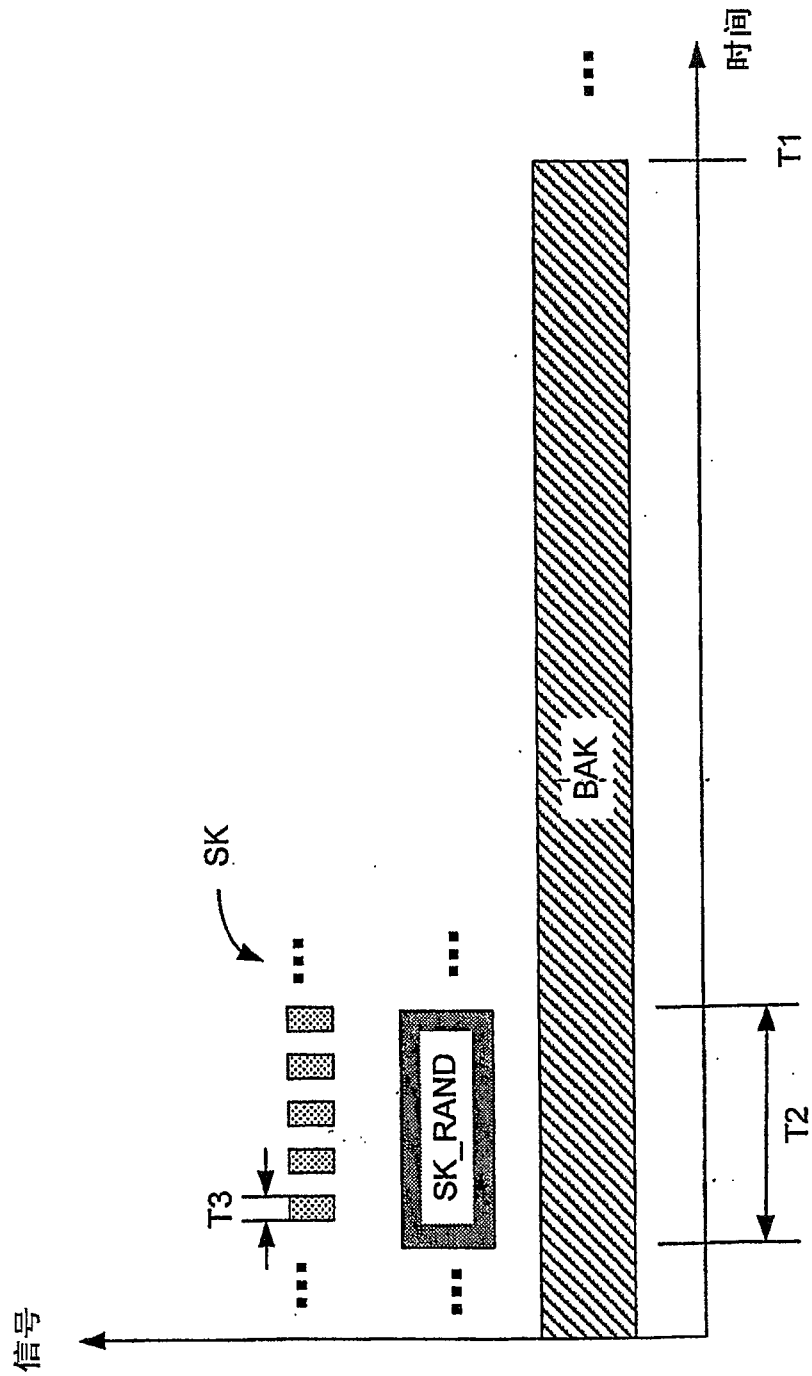


图 7E

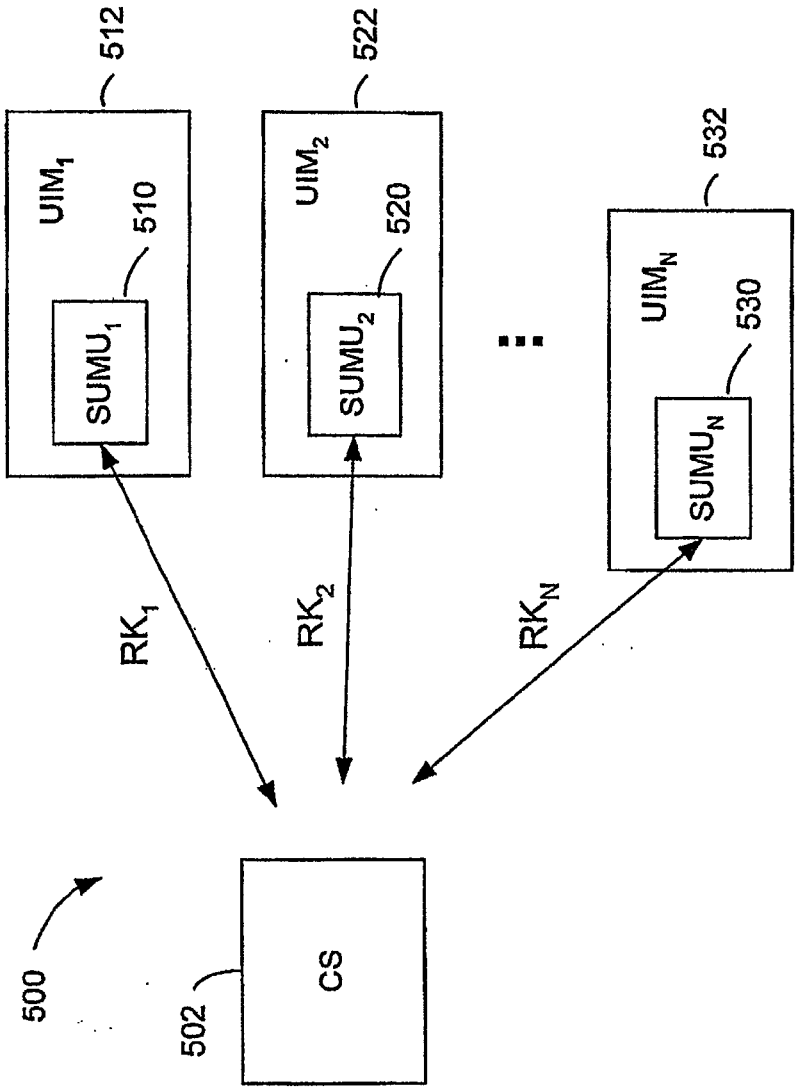

512
522
532
UIM1
510
SUMU1
UIM2
520
SUMU2
UIMN
530
SUMUN
RK1
RK2
RKN
500
502
CS

图 8A

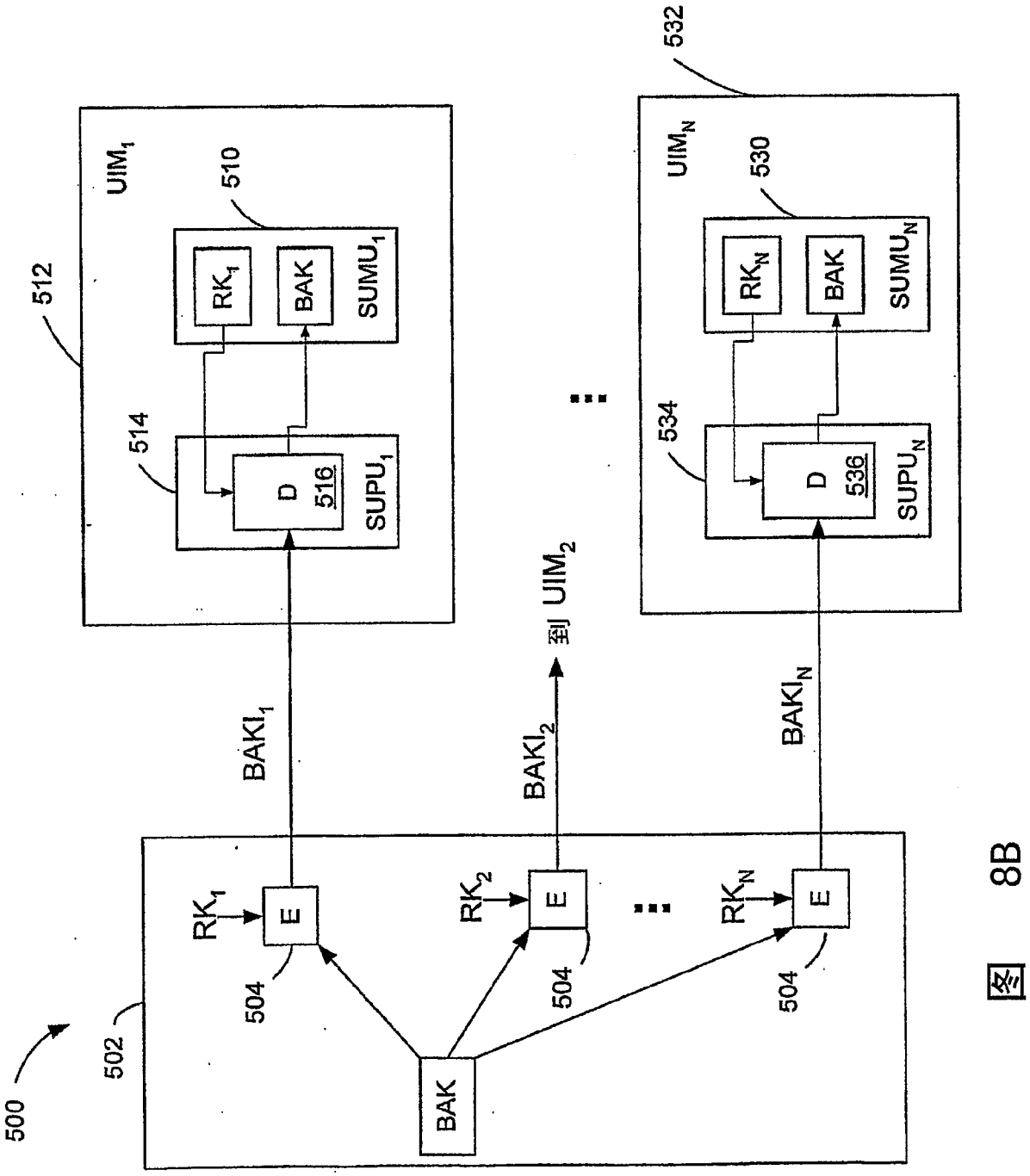

500
502
BAK
RK1
E
504
RK2
E
504
RKN
E
504
BAKI1
BAKI2
到 UIM2
BAKIN
UIM1
512
510
RK1
BAK
SUMU1
514
D
516
SUPU1
UIMN
532
530
RKN
BAK
SUMUN
534
D
536
SUPUN

图 8B

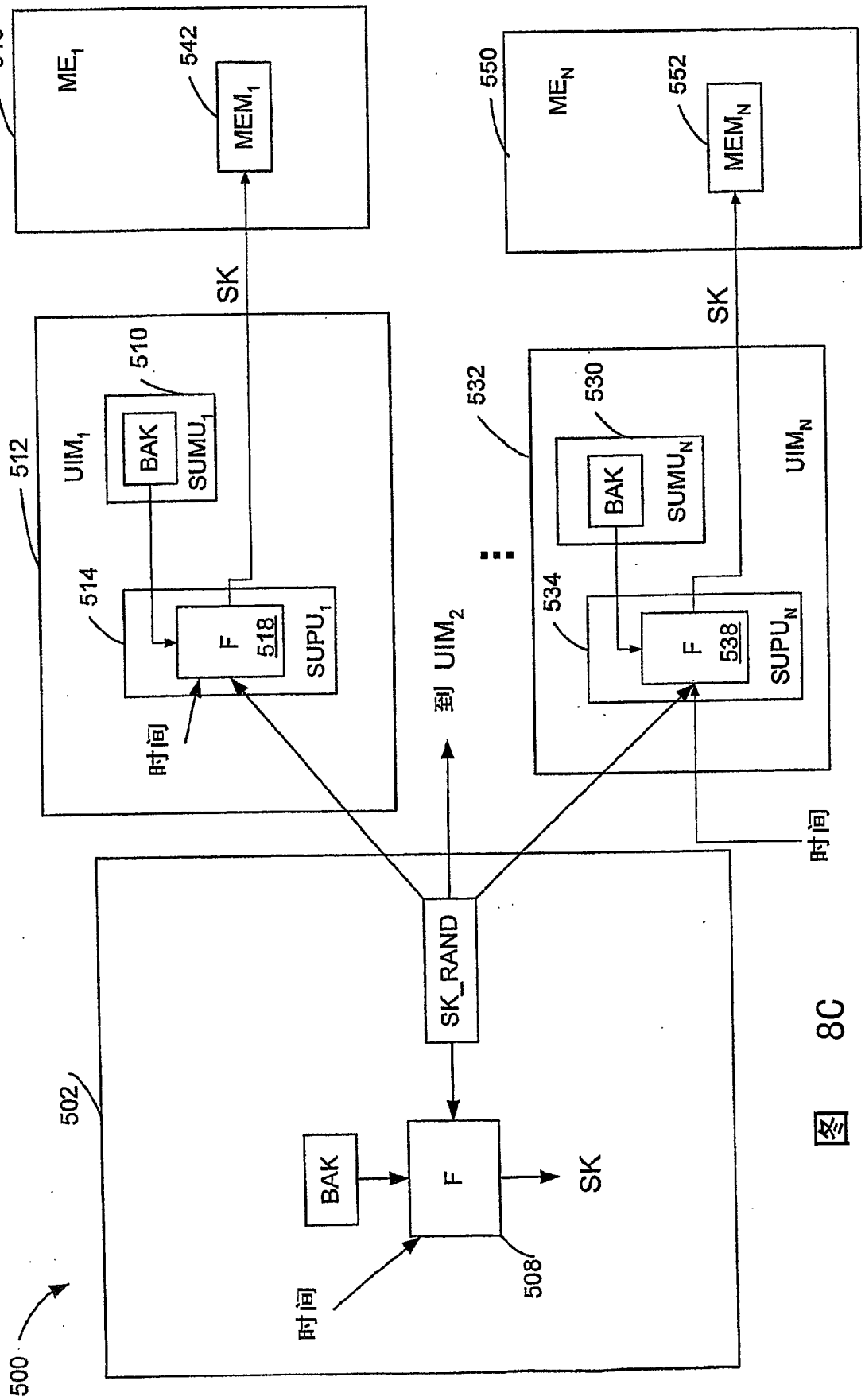

500
502
BAK
F
SK
时间
508
SK_RAND
到 UIM2
540
ME1
542
MEM1
550
MEN
552
MEMN
SK
512
UIM1
510
BAK
SUMU1
514
F
518
SUPU1
时间
532
UIMN
530
BAK
SUMUN
534
F
538
SUPUN
时间

图 8C

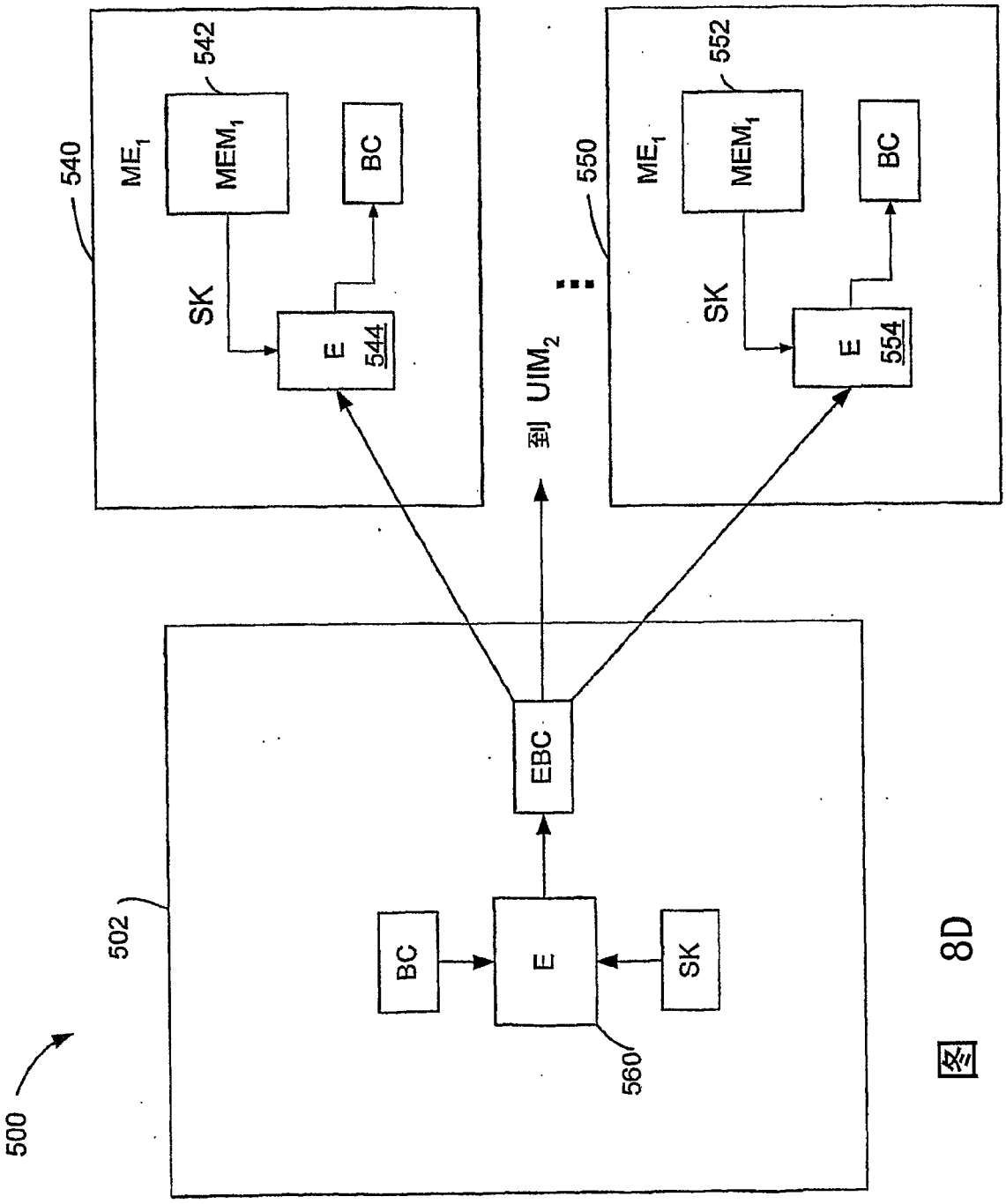

500
502
BC
E
SK
560
EBC
到 UIM2
540
ME1
MEM1
542
SK
E
544
BC
550
ME1
MEM1
552
SK
E
554
BC

图 8D

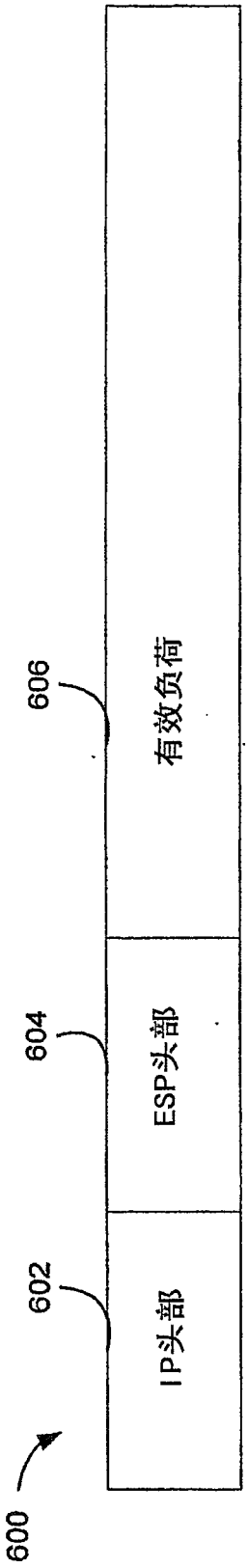

600
602
IP头部
604
ESP头部
606
有效负荷

图 9A

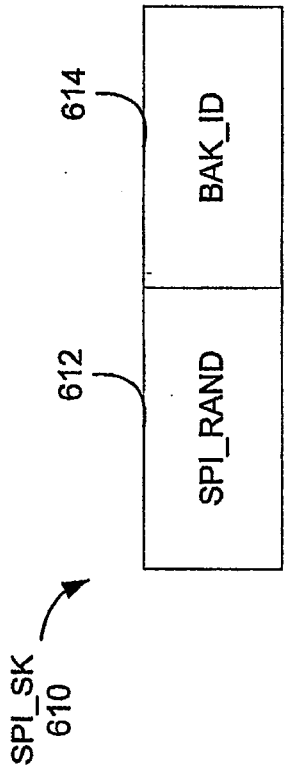

SPI_SK
610
612
SPI_RAND
614
BAK_ID

图 9B

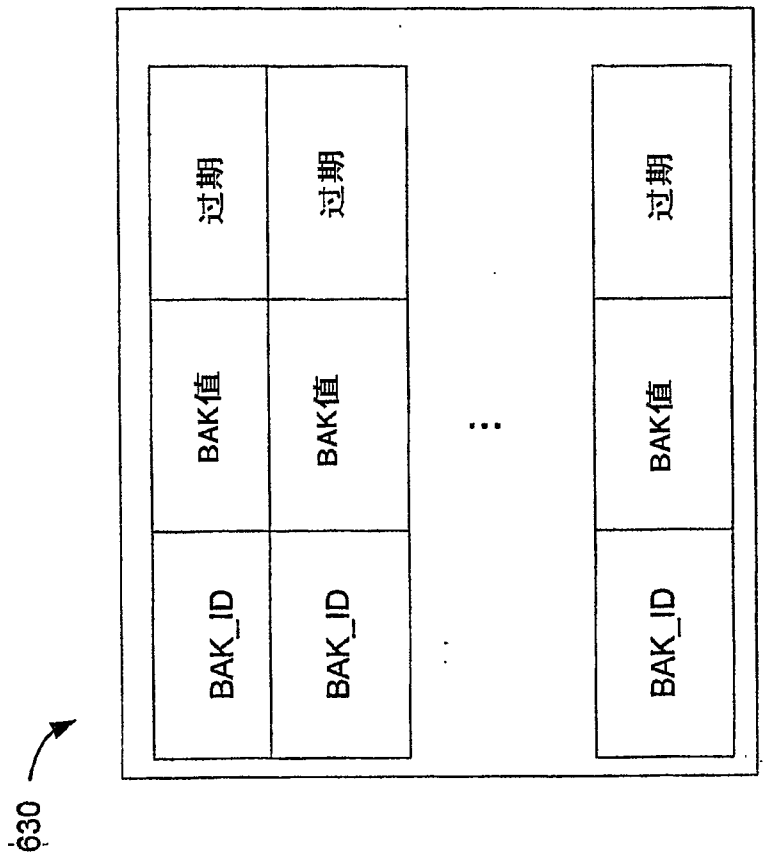

630
BAK_ID
BAK值
过期
BAK_ID
BAK值
过期
BAK_ID
BAK值
过期

图 9D

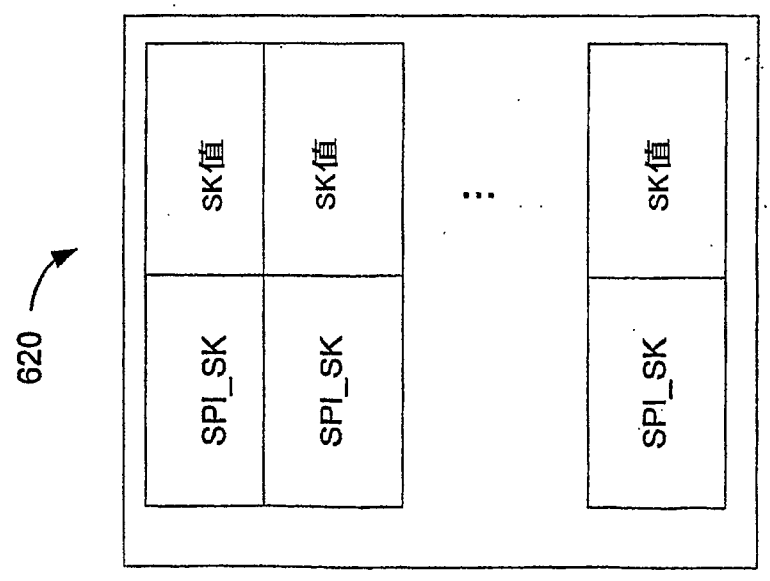

620
SPI_SK
SK值
SPI_SK
SK值
SPI_SK
SK值

图 9C

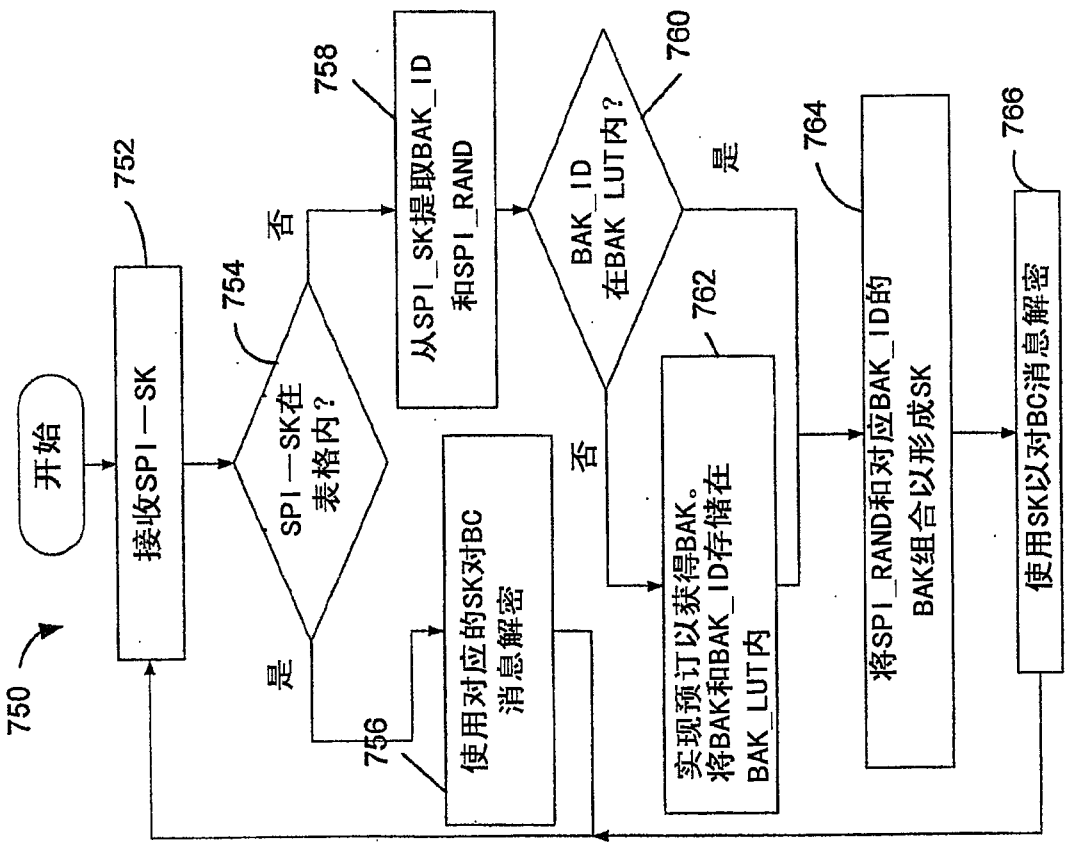

750
开始
752
接收SPI—SK
754
SPI—SK在表格内？
是
否
756
使用对应的SK对BC消息解密
758
从SPI_SK提取BAK_ID和SPI_RAND
760
BAK_ID在BAK_LUT内？
是
否
762
实现预订以获得BAK。将BAK和BAK_ID存储在BAK_LUT内
764
将SPI_RAND和对应BAK_ID的BAK组合以形成SK
766
使用SK以对BC消息解密

图 11

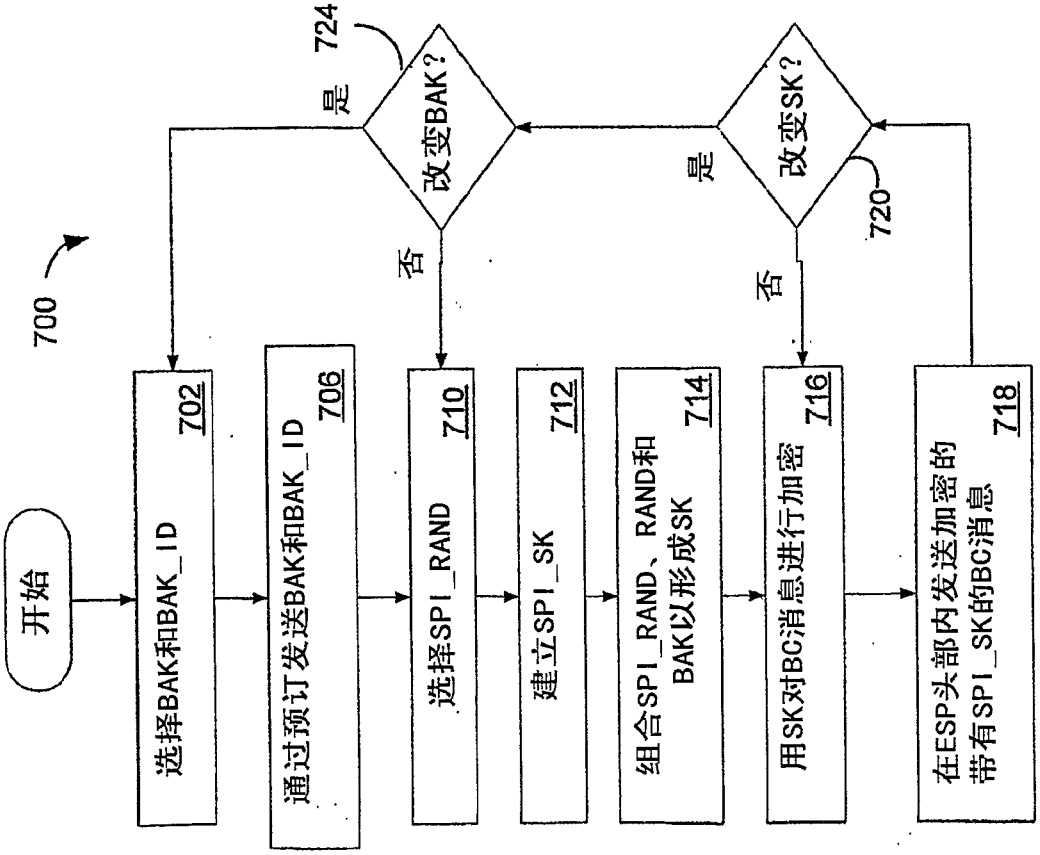

700
开始
702
选择BAK和BAK_ID
706
通过预订发送BAK和BAK_ID
710
选择SPI_RAND
712
建立SPI_SK
714
组合SPI_RAND、RAND和BAK以形成SK
716
用SK对BC消息进行加密
718
在ESP头部内发送加密的带有SPI_SK的BC消息
720
改变SK？
是
否
724
改变BAK？
是
否

图 10

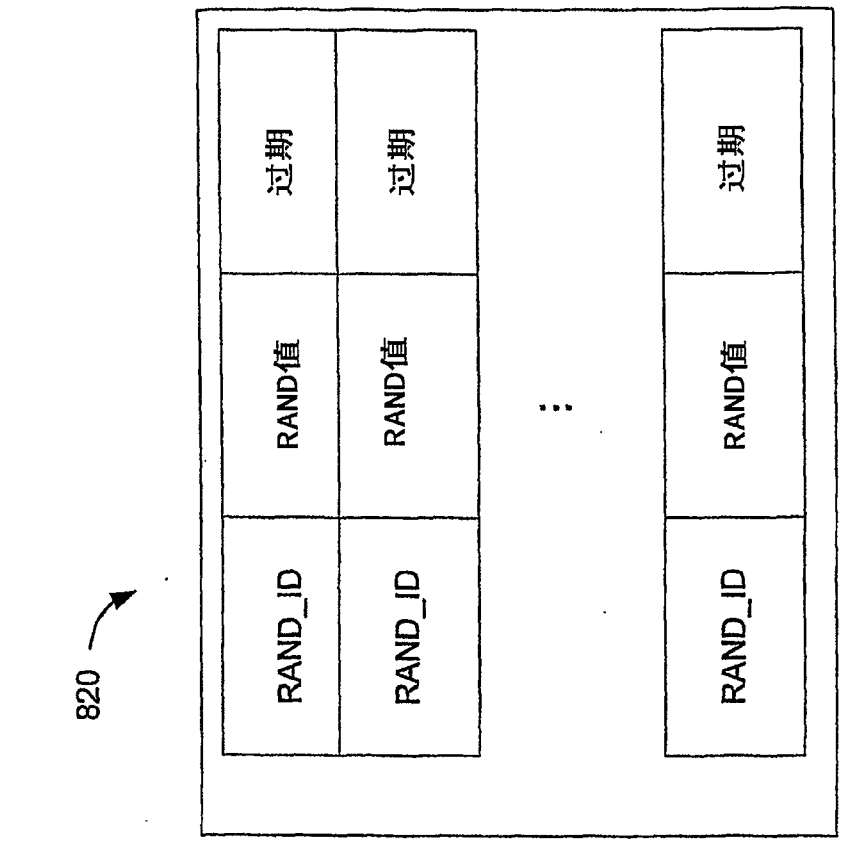

820
RAND_ID
RAND值
过期
RAND_ID
RAND值
过期
RAND_ID
RAND值
过期

图 12B

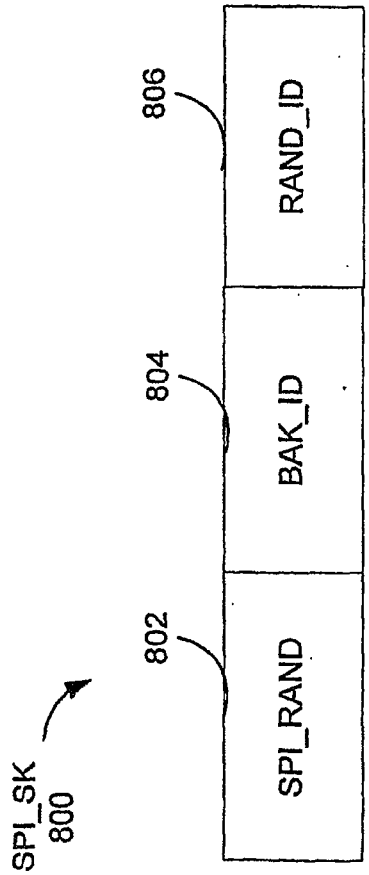

SPI_SK
800
802
SPI_RAND
804
BAK_ID
806
RAND_ID

图 12A

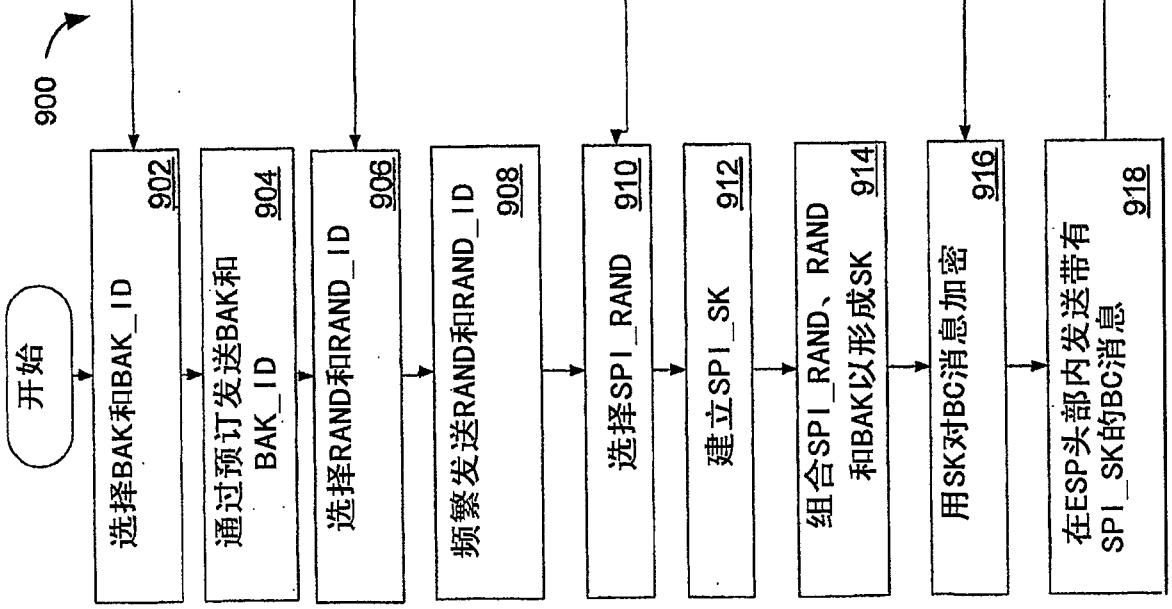

开始
900
选择BAK和BAK_ID
902
通过预订发送BAK和BAK_ID
904
选择RAND和RAND_ID
906
频繁发送RAND和RAND_ID
908
选择SPI_RAND
910
建立SPI_SK
912
组合SPI_RAND、RAND和BAK以形成SK
914
用SK对BC消息加密
916
在ESP头部内发送带有SPI_SK的BC消息
918
改变SK?
920
改变RAND?
922
改变BAK?
924
是
否

图 13

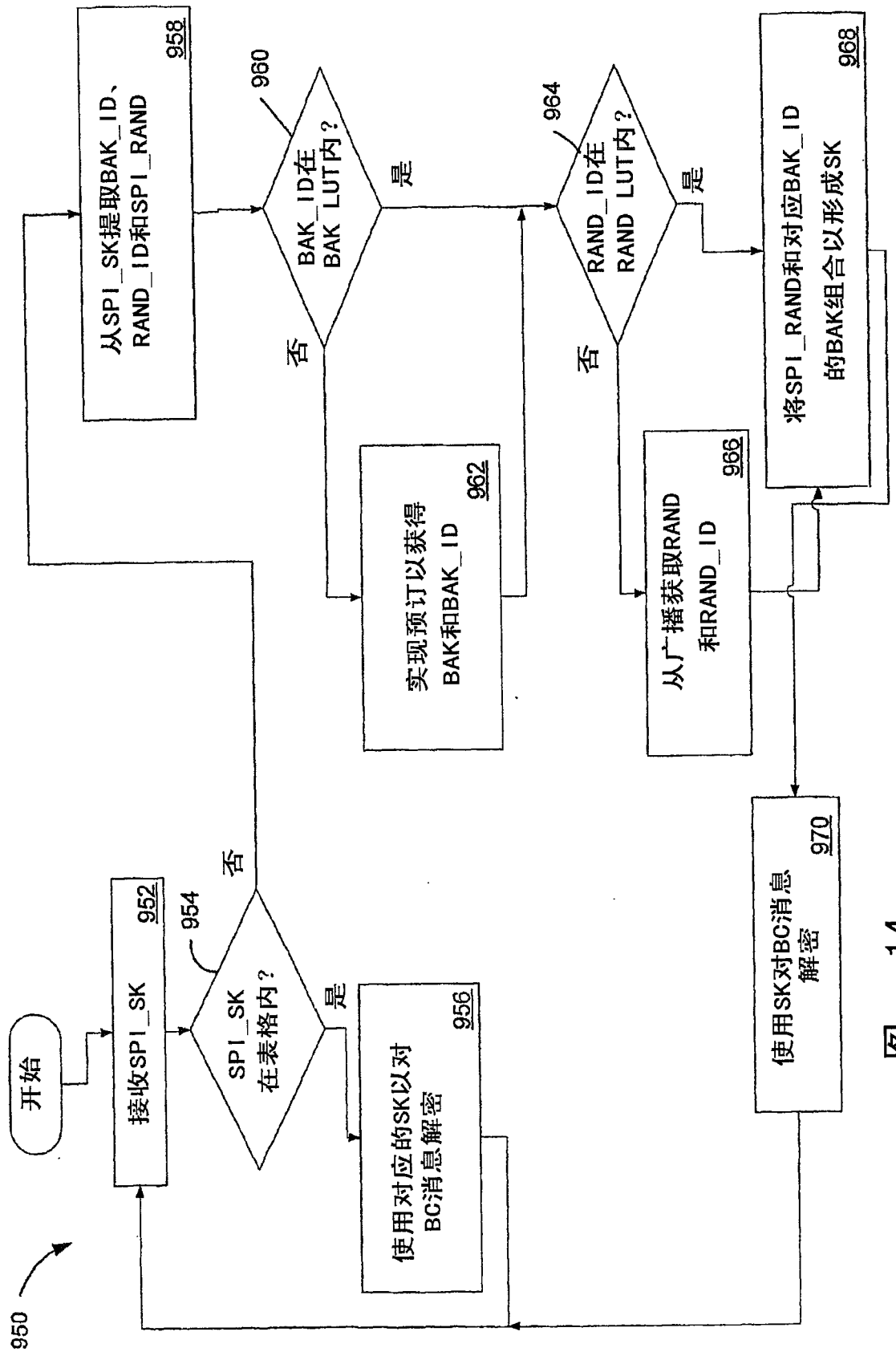

950
开始
接收SPI_SK
952
SPI_SK
在表格内？
954
否
是
使用对应的SK以对
BC消息解密
956
从SPI_SK提取BAK_ID、
RAND_ID和SPI_RAND
958
BAK_ID在
BAK LUT内？
960
否
是
实现预订以获得
BAK和BAK_ID
962
RAND_ID在
RAND LUT内？
964
否
是
从广播获取RAND
和RAND_ID
966
将SPI_RAND和对应BAK_ID
的BAK组合以形成SK
968
使用SK对BC消息
解密
970

图 14