(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 104486072 A
(43)申请公布日 2015.04.01

(21)申请号 201410846069.6

(22)申请日 2014.12.31

(71)申请人 宁波保税区攀峒信息科技有限公司
地址 315800 浙江省宁波市宁波保税区兴业三路6号314室

(72)发明人 倪龙

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 9/00(2006.01)

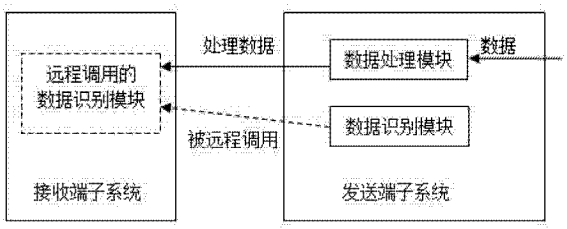
权利要求书2页 说明书4页 附图1页

(54)发明名称

一种保密通信系统

(57)摘要

本发明提供一种保密通信系统，发送端子系统、接收端子系统，发送端子系统包括数据处理模块和与之相应的可被远程调用的数据识别模块，要发送的原始数据先经数据处理模块处理然后再发送，接收端子系统接收到处理数据后远程调用数据识别模块进行识别，从而获得原始数据或其可识别同义形式或者通过远程调用的数据识别模块的展示功能展示以获取信息。上述数据处理模块、数据识别模块可以拿出一个或都拿出组成服务端子系统，需要时从服务端子系统远程调用。本发明还提供了上述保密通信系统的保密通信终端。本发明的保密通信系统和终端，较现有通道加密、端到端加密等方式，成本低，保密技术和强度可以根据需要灵活选配，可用于私人、商务等各种场合。



保密通信系统

CN 104486072 A

1.一种保密通信系统，其特征在于：

包括发送端子系统、接收端子系统，发送端子系统包括数据处理模块和与之相应的可被远程调用的具有识别经数据处理模块处理后的处理数据功能的数据识别模块，发送端子系统将要发送的原始数据先经数据处理模块处理然后再发送，接收端子系统接收到处理数据后远程调用发送端子系统的数据识别模块进行识别，从而获得原始数据或原始数据的可识别同义形式或者无法获得原始数据或原始数据的可识别同义形式但远程调用的数据识别模块还具有展示功能并只能通过该功能展示以获取信息；

或者包括发送端子系统、接收端子系统和服务端子系统，服务端子系统包括可被远程调用的数据处理模块和与之相应的可被远程调用的具有识别经数据处理模块处理后的处理数据功能的数据识别模块，发送端子系统将要发送的原始数据先经远程调用服务端子系统的数据处理模块处理然后再发送，接收端子系统接收到处理数据后远程调用服务端子系统的数据识别模块进行识别，从而获得原始数据或原始数据的可识别同义形式或者无法获得原始数据或原始数据的可识别同义形式但远程调用的数据识别模块还具有展示功能并只能通过该功能展示以获取信息；

或者包括发送端子系统、接收端子系统和服务端子系统，发送端子系统包括数据处理模块，服务端子系统包括与发送端子系统数据处理模块相应的可被远程调用的具有识别经发送端子系统的数据处理模块处理后的处理数据功能的数据识别模块，发送端子系统将要发送的原始数据先经数据处理模块处理然后再发送，接收端子系统接收到处理数据后远程调用服务端子系统的数据识别模块进行识别，从而获得原始数据或原始数据的可识别同义形式或者无法获得原始数据或原始数据的可识别同义形式但远程调用的数据识别模块还具有展示功能并只能通过该功能展示以获取信息；

或者包括发送端子系统、接收端子系统和服务端子系统，服务端子系统包括数据处理模块，发送端子系统包括与服务端子系统数据处理模块相应的可被远程调用的具有识别经服务端子系统的数据处理模块处理后的处理数据功能的数据识别模块，发送端子系统将要发送的原始数据先经远程调用服务端子系统的数据处理模块处理然后再发送，接收端子系统接收到处理数据后远程调用发送端子系统的数据识别模块进行识别，从而获得原始数据或原始数据的可识别同义形式或者无法获得原始数据或原始数据的可识别同义形式但远程调用的数据识别模块还具有展示功能并只能通过该功能展示以获取信息。

2.一种保密通信终端，其特征在于：

包括发送端子系统，

发送端子系统包括数据处理模块和与之相应的可被远程调用的具有识别经数据处理模块处理后的处理数据功能的数据识别模块，发送端子系统将要发送的原始数据先经数据处理模块处理然后再发送给与之通信的其它终端并提示自身的数据识别模块用作上述处理数据识别同时将自身的数据识别模块供与之通信的其它终端远程调用，

或发送端子系统包括数据处理模块但不包括与之相应的可被远程调用的具有识别经数据处理模块处理后的处理数据功能的数据识别模块，发送端子系统将要发送的原始数据先经数据处理模块处理然后再发送给与之通信的其它终端并提示本通信系统内非自身的与之相应的数据识别模块用作上述处理数据识别，

或发送端子系统不包括数据处理模块但包括与之相应的可被远程调用的具有识别经

数据处理模块处理后的处理数据功能的数据识别模块，发送端子系统将要发送的原始数据先经远程调用本通信系统内非自身的可供远程调用的数据处理模块处理然后再发送给与之通信的其它终端并提示自身的数据识别模块用作上述处理数据识别同时将自身的数据识别模块供与之通信的其它终端远程调用，

或发送端子系统既不包括数据处理模块又不包括与之相应的可被远程调用的具有识别经数据处理模块处理后的处理数据功能的数据识别模块，发送端子系统将要发送的原始数据先经远程调用本通信系统内非自身的可供远程调用的数据处理模块处理然后再发送给与之通信的其它终端并提示本通信系统内非自身的与之相应的数据识别模块用作上述处理数据识别；

同时／或者包括接收端子系统，接收端子系统接收到与之通信的其它终端发送来的处理数据后远程调用该终端指示的数据识别模块进行识别，从而获得原始数据或原始数据的可识别同义形式或者无法获得原始数据或原始数据的可识别同义形式但远程调用的数据识别模块还具有展示功能并只能通过该功能展示以获取信息。

3. 根据权利要求 1 所述的保密通信系统或权利要求 2 所述的保密通信终端，其特征在于：

其中的数据处理模块包括数据加密步骤，同时数据识别模块包括与之相应的数据解密步骤；

同时／或者数据识别模块具有通信数据删除功能和／或通信数据保存功能。

一种保密通信系统

技术领域

[0001] 本发明属于电子产品领域，尤其涉及一种保密通信系统。

背景技术

[0002] 通信保密在一些场合非常必要，尤其在涉及个人隐私、商业秘密、国家秘密的时候。当前常用的通信保密方法有两种方式，一是通道加密，二是端到端加密。通道加密是指数据在传输过程中是加密的，其加密过程对于通信用户来说是透明的。端到端加密是指在发送端加密然后在接收端解密，其加密过程是用户自己控制的。但所采用的加密技术都是可以破解的，尽管付出的代价有大有小，其代价包括破译时间成本和直接经济成本。目前不能破解的加密技术只有一种一次一密(one-time pad)。一次一密指在流密码当中使用与消息长度等长的随机密钥， 密钥本身只使用一次。具体而言，首先选择一个随机位串作为密钥，然后将明文转变成一个位串，比如使用明文的 ASCII 表示法。最后，逐位计算这两个串的异或值，结果得到的密文不可能被破解，因为即使有了足够数量的密文样本，每个字符的出现概率都是相等的，每任意个字母组合出现的概率也是相等的。这种方法被称为“一次一密”。其优点是由于使用与消息等长的随机密钥， 产生与原文没有任何统计关系的随机输出，因此一次一密方案不可破解，其缺陷是密钥在传递和分发上存在很大困难。因此一次一密这种方式在使用上还是存在许多不便，因此目前通道加密和端到端加密中都没有采用。当前，随着互联网的发展和普及，基于互联网的各种通信方式越来越被人们所采用，甚至依赖，邮件、即时通信软件、社交软件，许多商业系统、政府乃至军事系统都延伸到了互联网上，所以互联网上的泄密、入侵事件层出不穷。

发明内容

[0003] 本发明的目的在于解决通信保密程度不高、一次一密这种方式难以有效应用的问题。本发明的思路是采用远程调用的方式实现密钥的传递，从而达到通信保密的目的。本发明的保密通信系统技术方案如下：

包括发送端子系统、接收端子系统，是否包括其它子系统不限，下同。发送端子系统包括数据处理模块和与之相应的可被远程调用的具有识别经自身的数据处理模块处理后的处理数据功能的数据识别模块，所谓相应是指两个模块可配合使用，如数据处理模块用于数据加密，而数据识别模块则用于数据解密，以识别数据处理模块加密了的数据，下同。发送端子系统将要发送的原始数据先经自身的数据处理模块处理然后再发送，当然发送的是处理后的数据，下同。接收端子系统接收到处理数据后远程调用发送端子系统的数据识别模块进行识别，从而获得原始数据，也可以是原始数据的可识别同义形式，比如现在有些软件把文字转化图形，从而防止拷贝和敏感词检测，还有的在文字中夹杂一些字符，计算机难以区别其与正常字符，但肉眼能够轻易识别；还可以是无法获得原始数据或原始数据的可识别同义形式但远程调用的数据识别模块还具有展示功能并只能通过该功能展示以获取信息，这种情况是为了防止接收方私自保留通信信息，这样通信信息仅一次使用有效，这里

的一次是指整个远程调用数据识别模块识别的这一次。

[0004] 前述方案也可以在变动一下，将数据处理模块、数据识别模块放到另一个子系统 --- 服务端子系统当中，这时保密通信系统就包括发送端子系统、接收端子系统和服务端子系统，服务端子系统包括可被远程调用的数据处理模块和与之相应的可被远程调用的具有识别经数据处理模块处理后的处理数据功能的数据识别模块，发送端子系统将要发送的原始数据先经远程调用服务端子系统的数据处理模块处理然后再发送，接收端子系统接收到处理数据后远程调用服务端子系统的数据识别模块进行识别，从而获得原始数据或原始数据的可识别同义形式或者无法获得原始数据或原始数据的可识别同义形式但远程调用的数据识别模块还具有展示功能并只能通过该功能展示以获取信息。

[0005] 前述两种方案可以折中，即将数据处理模块、数据识别模块其中一个模块放到另一个子系统 --- 服务端子系统当中，这样就存在两种情况，这时保密通信系统同样包括发送端子系统、接收端子系统和服务端子系统。第一种情况是：发送端子系统包括数据处理模块，服务端子系统包括与发送端子系统数据处理模块相应的可被远程调用的具有识别经发送端子系统的数据处理模块处理后的处理数据功能的数据识别模块，发送端子系统将要发送的原始数据先经数据处理模块处理然后再发送，接收端子系统接收到处理数据后远程调用服务端子系统的数据识别模块进行识别，从而获得原始数据或原始数据的可识别同义形式或者无法获得原始数据或原始数据的可识别同义形式但远程调用的数据识别模块还具有展示功能并只能通过该功能展示以获取信息。第二种情况是：发送端子系统包括与服务端子系统数据处理模块相应的可被远程调用的具有识别经服务端子系统的数据处理模块处理后的处理数据功能的数据识别模块，发送端子系统将要发送的原始数据先经远程调用服务端子系统的数据处理模块处理然后再发送，接收端子系统接收到处理数据后远程调用发送端子系统的数据识别模块进行识别，从而获得原始数据或原始数据的可识别同义形式或者无法获得原始数据或原始数据的可识别同义形式但远程调用的数据识别模块还具有展示功能并只能通过该功能展示以获取信息。

[0006] 可以参照数据保密通信系统技术方案制成相应的保密通信终端，其技术方案是：

包括发送端子系统；发送端子系统包括数据处理模块和与之相应的可被远程调用的具有识别经数据处理模块处理后的处理数据功能的数据识别模块，即包括后面要用的两个模块：数据处理模块、数据识别模块，是否包括其它的数据处理模块、数据识别模块不限，发送端子系统将要发送的原始数据先经数据处理模块处理然后再发送给与之通信的其它终端并提示自身的数据识别模块用作上述处理数据识别同时将自身的数据识别模块供与之通信的其它终端远程调用。发送端子系统也可以包括数据处理模块但不包括与之相应的可被远程调用的具有识别经数据处理模块处理后的处理数据功能的数据识别模块，即包括了后面要用的数据处理模块、但不包括后面要用的数据识别模块，是否包括或不包括其它的数据处理模块、数据识别模块不限，发送端子系统将要发送的原始数据先经数据处理模块处理然后再发送给与之通信的其它终端并提示本通信系统内非自身的与之相应的数据识别模块用作上述处理数据识别。发送端子系统也可以不包括数据处理模块但包括与之相应的可被远程调用的具有识别经数据处理模块处理后的处理数据功能的数据识别模块，即不包括后面要用的数据处理模块、但包括了后面要用的数据识别模块，是否包括或不包括其它的数据处理模块、数据识别模块不限，发送端子系统将要发送的原始数据先经远程调用本

通信系统内非自身的可供远程调用的数据处理模块处理然后再发送给与之通信的其它终端并提示自身的数据识别模块用作上述处理数据识别同时将自身的数据识别模块供与之通信的其它终端远程调用。发送端子系统也可以既不包括数据处理模块又不包括与之相应的可被远程调用的具有识别经数据处理模块处理后的处理数据功能的数据识别模块，即不包括后面要用的两个模块：数据处理模块、数据识别模块，是否不包括其它的数据处理模块、数据识别模块不限，发送端子系统将要发送的原始数据先经远程调用本通信系统内非自身的可供远程调用的数据处理模块处理然后再发送给与之通信的其它终端并提示本通信系统内非自身的与之相应的数据识别模块用作上述处理数据识别。保密通信终端也可同时包括接收端子系统或者仅包括接收端子系统，接收端子系统接收到与之通信的其它终端发送来的处理数据后远程调用该终端指示的数据识别模块进行识别，从而获得原始数据或原始数据的可识别同义形式或者无法获得原始数据或原始数据的可识别同义形式但远程调用的数据识别模块还具有展示功能并只能通过该功能展示以获取信息。

[0007] 上述方案还可以进一步具体化，比如其中的数据处理模块包括数据加密步骤，同时数据识别模块包括与之相应的数据解密步骤，当前有关数据加解密的算法的研究及成果很多，可以根据保密的场合和需要拿过来用，够用就好，无须在任何场合都选那种加密强度很高难以破解的算法。比如让数据识别模块具有通信数据删除功能和 / 或通信数据保存功能，有些场合需要保密的信息看后就要销毁，怎么来保证销毁，靠当事人的自觉是不靠谱的，靠当事人一方的程序自动删除也是有问题的，只有依靠远程调用数据识别模块删除才能确保信息会删除；至于保存功能，由于信息最终是由数据识别模块处理的，因此也利于信息的保存，如果是可靠的用户，有时也需要这个保存功能。

[0008] 本发明的保密通信系统和终端，由于采用远程调用数据识别模块来识别处理后的数据，在远程调用过程中可以实现一次一密所需要与消息长度等长的随机密钥的分发和传输，这种方式下，对于所传输信息的加密就不需要采用那些复杂的加密算法，相应解密也可以很简单，而在远程调用的过程中一般需要具有一定强度的加密算法对等长随机密钥进行加密。而且可远程调用的数据识别模块是可以随时变化的，比如接口不换但识别算法更换，或者接口和算法都更换，当然最简单的方式是更换密钥，所以这次调用成功识别，下次再调用不一定会成功，这样就进一步增强了难破解性。由于可以采用一次一密方式，这样就较现有通道加密、端到端加密等方式其保密性能有了飞跃。本发明也采用其它的数据处理方式，简单的变换加密等、将文字转换为图片、在文字中插入不影响人眼识别的字符，等等，保密技术和强度可以根据需要灵活选配，成本低，可用于私人、商务乃至军事等各种场合。

附图说明

[0009] 图 1 为一种保密通信系统结构图；

图 2 为一种保密通信终端结构图。

具体实施方式

[0010] 实施例 1

一种保密通信系统

基于微软的 NetMeeting 即时通信终端程序改造一下，使其具有一个数据加密功能和

数据解密和展示功能，数据解密和展示功能做成一个可以远程调用的过程 -- 数据解密和展示过程。对话的双方程序一样，但加密解密的密钥不一样，可以由使用者自行设置。在通话时，甲方通过键入的图文通过按发送按钮发送后，先通过甲方数据加密功能用自己设置加密密钥加密然后再发送出加密文本并指示乙方远程调用自己的数据解密和展示过程，乙方收到加密文本后然后远程调用甲方的数据解密和展示过程（由于甲方舍得解密密钥和乙方不一样所以调用的过程和自身供远程调用的过程在数据流上有差别）进行解密和展示，退出此远程调用过程相关数据都销毁，此过程中不在乙方保存任何数据。

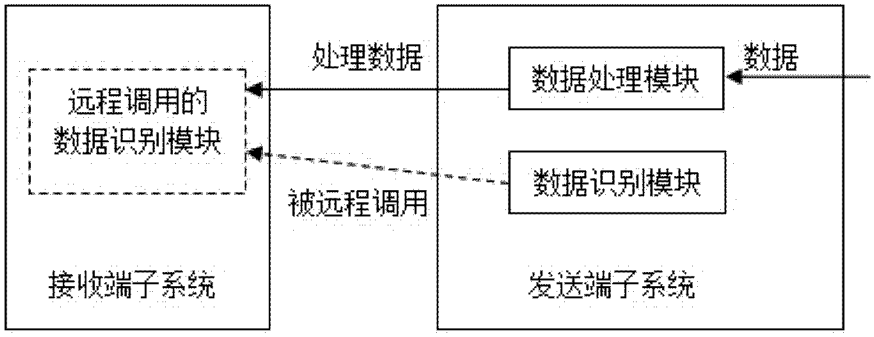

处理数据
数据处理模块
数据
远程调用的
数据识别模块
数据识别模块
被远程调用
接收端子系统
发送端子系统
保密通信系统

图 1

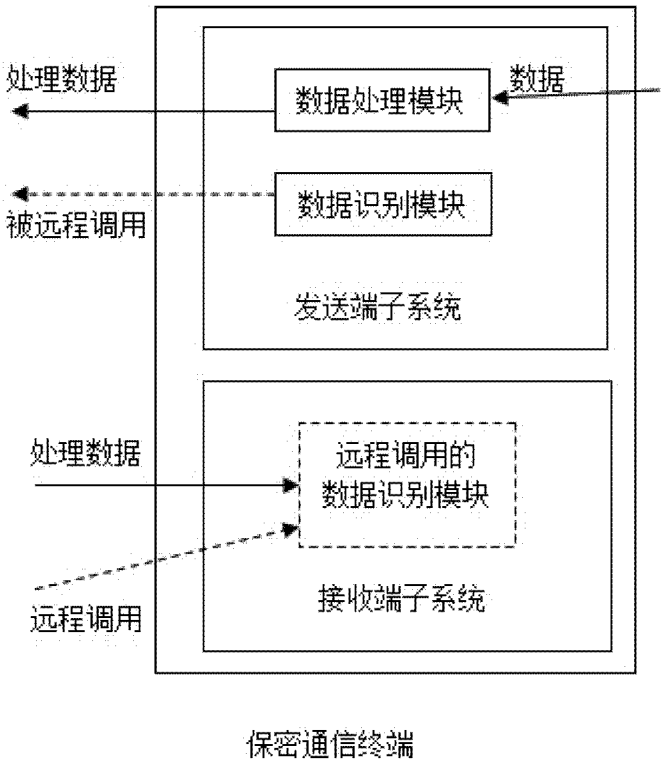

处理数据
数据处理模块
数据
数据识别模块
被远程调用
发送端子系统
处理数据
远程调用的
数据识别模块
远程调用
接收端子系统
保密通信终端

图 2