(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 101772014 A
(43)申请公布日 2010.07.07

(21)申请号 200810241782.2

(22)申请日 2008.12.31

(71)申请人 深圳易拓科技有限公司
地址 518000 广东省深圳市福田区彩田路 7006 工业区 4、5 层

(72)发明人 宋美华

(74)专利代理机构 深圳鼎合诚知识产权代理有限公司 44281
代理人 龚安义

(51)Int.Cl.
H04W 12/02(2009.01)
H04W 88/02(2009.01)

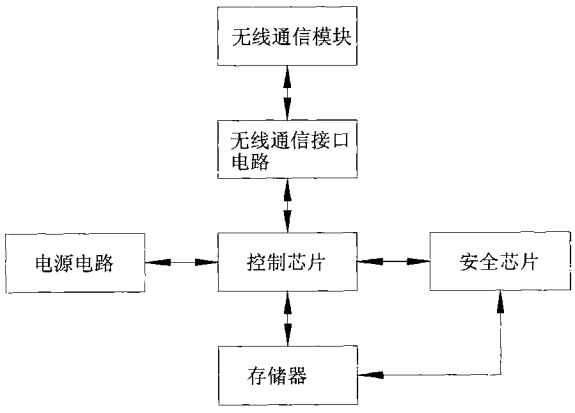
权利要求书 1 页 说明书 2 页 附图 1 页

(54)发明名称

一种提高无线数据传输安全的方法及移动终端

(57)摘要

本发明公开了一种提高无线数据传输安全的方法及移动终端，移动终端包括控制芯片、与控制芯片连接的无线通信模块和存储器，还包括与控制芯片连接的安全芯片，所述安全芯片中具有嵌入式加密解密程序和存储有用户识别信息。本发明在移动终端内设置安全芯片，对接受和发送的无线数据进行加密签名或解密验证，采用硬件加密，不但提高了数据加密传输的速度，而且能对整个数据流进行加密，保证了数据无线传输的安全性。



CN 101772014 A

1. 一种提高无线数据传输安全的移动终端，包括控制芯片、与控制芯片连接的无线通信模块和存储器，其特征在于：还包括与控制芯片连接的安全芯片，所述安全芯片中具有嵌入式加密解密程序。

2. 如权利要求 1 所述的提高无线数据传输安全的移动终端，其特征在于：所述安全芯片中还存储有用户识别信息。

3. 如权利要求 2 所述的提高无线数据传输安全的移动终端，其特征在于：所述安全芯片还与存储器连接。

4. 一种提高无线数据传输安全的方法，其特征在于包括以下步骤：

移动终端接收无线数据步骤：移动终端的控制芯片将接收到的无线传输数据流传输给安全芯片，安全芯片对数据流进行解密验证后将数据流传输给控制芯片，控制芯片将解密验证后的数据流存储在存储器中；

移动终端发送无线数据步骤：移动终端的控制芯片从存储器中读取数据流并将数据流传输给安全芯片，安全芯片对数据流进行加密后将数据流传输给控制芯片，控制芯片将加密后的数据流输出给无线通信模块发送。

5. 如权利要求 4 所述的提高无线数据传输安全的方法，其特征在于：所述移动终端接收无线数据步骤中，安全芯片将解密验证后的数据流输出到并存储在存储器中。

6. 如权利要求 4 所述的提高无线数据传输安全的方法，其特征在于：所述移动终端发送无线数据步骤中，控制芯片通知安全芯片从存储器中读取数据流，控制芯片对数据流进行加密后再传输给控制芯片。

7. 如权利要求 4 所述的提高无线数据传输安全的方法，其特征在于：所述移动终端发送无线数据步骤中，安全芯片还将用户识别信息写入数据流中，对数据流签名后再传输给控制芯片。

一种提高无线数据传输安全的方法及移动终端

技术领域

[0001] 本发明涉及一种数据传输安全的方法，具体是涉及一种提高无线数据传输安全的方法及一种提高无线数据传输安全的移动终端。

背景技术

[0002] 各种手持移动终端如手机、PDA（个人数字助理）以及其他无线上网的可移动计算机，为人们提供了方便的网络接入服务和极大的移动性。但在实际使用中，无线数据传输的安全性、保密性受到了人们的关注，限制了人们对其使用的兴趣。相对于数据的有线传输，无线数据传输过程的数据更容易被非法用户窃取、阅读、篡改等。利用数据加密解决方案是保护数字信息的安全的重要手段。对于移动终端，现有技术的解决方案一般是，用户下载使用专门的加密／解密程序，通过运行这些软件程序对信息数据进行加密／解密并传输，防止非法用户获知信息内容。而这些软件容易被非法程序攻击，一旦这些软件染上病毒，数据的安全性则得不到保障。

发明内容

[0003] 本发明的目的是提出一种提高无线数据传输安全的移动终端，内置有安全芯片，提高数据无线传输的安全性。

[0004] 本发明还提出一种提高无线数据传输安全的方法。

[0005] 本发明的提高无线数据传输安全的移动终端是通过以下技术方案予以解决的。

[0006] 这种提高无线数据传输安全的移动终端，包括控制芯片、与控制芯片连接的无线通信模块和存储器，其特征是，还包括与控制芯片连接的安全芯片，所述安全芯片中具有嵌入式加密解密程序。

[0007] 上述提高无线数据传输安全的移动终端，其中所述安全芯片中还存储有用户识别信息。

[0008] 所述安全芯片还与存储器连接。

[0009] 本发明提出的一种提高无效数据传输安全的方法是通过以下技术方案予以实现的。

[0010] 这种提高无线数据传输安全的方法包括以下步骤：移动终端接收无线数据步骤：移动终端的控制芯片将接收到的无线传输数据流传输给安全芯片，安全芯片对数据流进行解密验证后将数据流传输给控制芯片，控制芯片将解密验证后的数据流存储在存储器中；移动终端发送无线数据步骤：移动终端的控制芯片从存储器中读取数据流并将数据流传输给安全芯片，安全芯片对数据流进行加密后将数据流传输给控制芯片，控制芯片将加密后的数据流通过无线通信模块发送出去。

[0011] 上述的提高无线数据传输安全的方法，其中，所述移动终端接收无线数据步骤中，安全芯片将解密验证后的数据流直接输出并存储在存储器中。

[0012] 所述移动终端发送无线数据步骤中，控制芯片通知安全芯片从存储器中读取数据

流，控制芯片对数据流进行加密后再传输给控制芯片。

[0013] 所述移动终端发送无线数据步骤中，安全芯片还将用户识别信息写入数据流中，对数据流签名后再传输给控制芯片。

[0014] 本发明与现有技术对比所具有的有益效果有：在移动终端内设置安全芯片，对接受和发送的无线数据进行加密签名或解密验证，采用硬件加密，在数据传输的过程中同时对数据进行加密 / 解密，不但提高了数据加密传输的速度，而且能对整个数据流进行加密，保证了数据无线传输的安全性。

附图说明

[0015] 图 1 是具体实施方式中移动终端的模块组成图。

具体实施方式

[0016] 如图 1 所示的一种移动终端，包括控制芯片 (CPU)、存储器，并通过无线通信接口电路连接有无线通信模块，还设有安全芯片，安全芯片通过并行总线与控制芯片连接。控制芯片用于控制数据的接受和发送，安全芯片具有嵌入式加密解密程序，并存储有用户身份识别等信息，用于实现数据的加密认证。

[0017] 移动终端发送数据时，控制芯片从存储器中读取数据流，并将数据流传输给安全芯片。安全芯片对数据流进行加密，并将存储在其内的用户信息添加到数据流中，然后将经过加密验证的数据流传输给控制芯片。控制芯片将加密后的数据流通过无线通信模块发送出去。

[0018] 移动终端接收数据时，控制芯片控制无线通信模块接收无线传输数据，然后将接收到的无线传输数据流传输给安全芯片。安全芯片对数据流进行解密验证，如果解密验证失败，则清除数据并提示；如果解密验证成功，则将解密后的数据流传输给控制芯片。控制芯片将解密验证后的数据流输出存储在存储器中。

[0019] 另一种实施方式中，移动终端接收数据后，安全芯片将解密验证后的数据流直接输出存储在存储器中。移动终端发送数据时，控制芯片控制安全芯片从存储器中读取数据流，控制芯片对数据流进行加密后再传输给控制芯片。这样可以减少安全芯片与控制芯片的数据传输，提高速度。

[0020] 存储器包括移动终端内置或外接的缓存、内存、闪存或移动硬盘等。

[0021] 以上方法可以应用于 WPA(Wi-Fi Protected Access，Wi-Fi 网络安全存取）解决方案、WEP(Wired Equivalent Privacy，有线等效保密）加密技术，增强无线传输的安全性。由于加密解密程序通过安全芯片硬件实现，保证了数据的安全性，如在非对称式加密中，生成的密钥不会传输到芯片外部。

[0022] 以上内容是结合具体的优选实施方式对本发明所作的进一步详细说明，不能认定本发明的具体实施只局限于这些说明。对于本发明所属技术领域的普通技术人员来说，在不脱离本发明构思的前提下，还可以做出若干简单推演或替换，都应当视为属于本发明的保护范围。

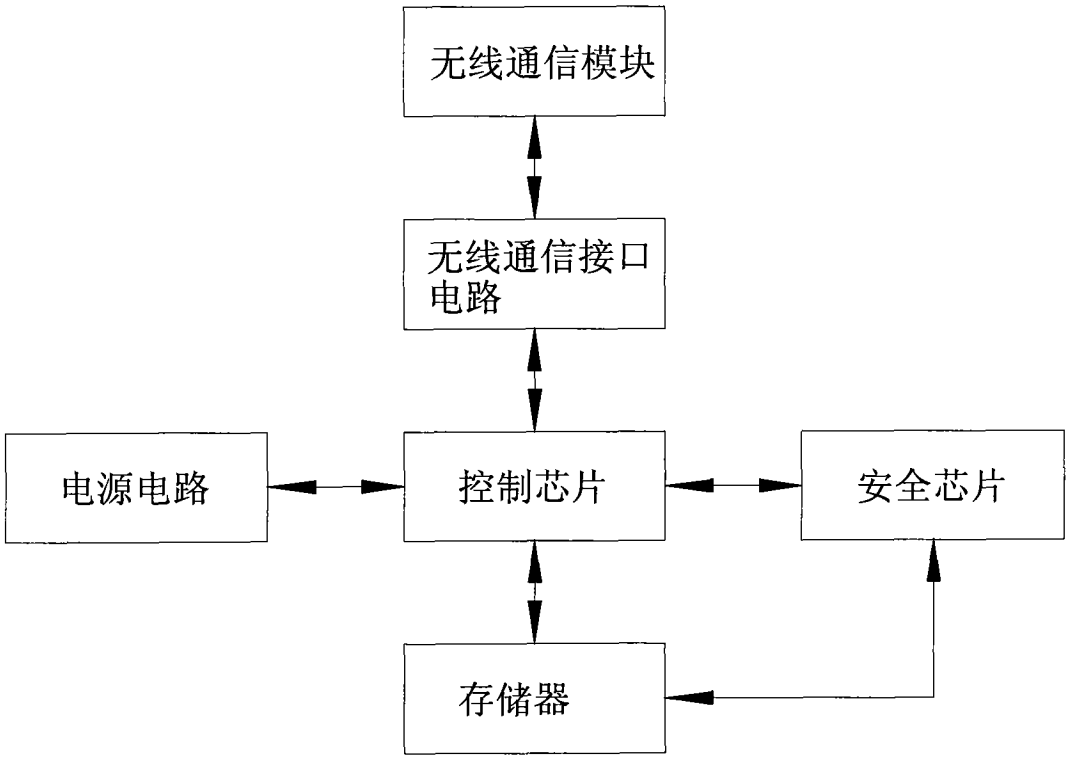


图 1