(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 112464291 B
(45)授权公告日 2022.03.22

(21)申请号 202011495037.8

(22)申请日 2020.12.17

(65)同一申请的已公布的文献号
申请公布号 CN 112464291 A

(43)申请公布日 2021.03.09

(73)专利权人 杭州电子科技大学
地址 310018 浙江省杭州市下沙高教园区2号大街

(72)发明人 姚英彪 周红 徐欣 姜显扬 许晓荣

(74)专利代理机构 杭州君度专利代理事务所(特殊普通合伙) 33240
代理人 朱月芬

(51)Int.Cl.
G06F 21/62(2013.01)
G06F 21/60(2013.01)
G06F 21/32(2013.01)
G06F 8/30(2018.01)

(56)对比文件
CN 104868997 A,2015.08.26
CN 111654510 A,2020.09.11
US 2005144464 A1,2005.06.30
US 2005244037 A1,2005.11.03
Li Dongyang et al..A Parallel and Pipelined Architecture for Accelerating Fingerprint Computation in High Throughput Data Storages.《2015 IEEE 23rd Annual International Symposium on Field-Programmable Custom Computing Machines (FCCM)》.2015,

审查员 胡振洲

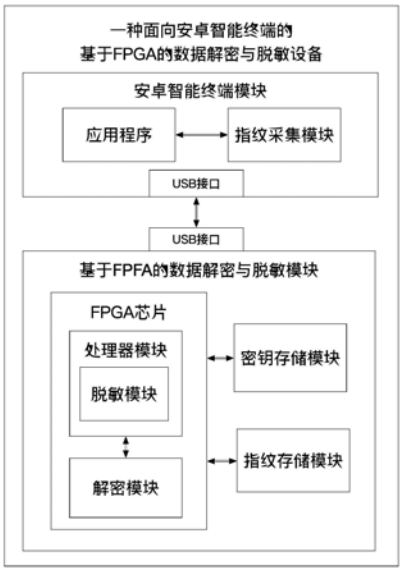
权利要求书1页 说明书5页 附图2页

(54)发明名称

面向安卓智能终端的基于FPGA的数据解密与脱敏设备

(57)摘要

本发明公开了一种面向安卓智能终端的基于FPGA的数据解密与脱敏设备。本发明包括安卓智能终端模块和基于FPGA的数据解密与脱敏模块(FPGA模块);所述的安卓智能终端模块由具有指纹采集功能的安卓智能终端及对应的应用程序组成;所述的FPGA模块包括处理器模块、解密模块、脱敏模块、密钥存储模块和指纹存储模块;所述安卓智能终端模块通过USB接口和FPGA模块连接,所述的秘钥存储模块和指纹存储模块通过QSPI接口与FPGA芯片连接。本发明最大程度上保证了数据的安全性。也就是说,即使在用户智能终端被控后,仍然能够保证关键机密数据以及密钥的安全性。



CN 112464291 B

1.面向安卓智能终端的基于FPGA的数据解密与脱敏设备,其特征在于包括安卓智能终端模块和基于FPGA的数据解密与脱敏模块(FPGA模块);所述的安卓智能终端模块由具有指纹采集功能的安卓智能终端及对应的应用程序组成;所述的FPGA模块包括处理器模块、解密模块、脱敏模块、密钥存储模块和指纹存储模块;所述安卓智能终端模块通过USB接口和FPGA模块连接,所述的密钥存储模块和指纹存储模块通过QSPI接口与FPGA芯片连接;

所述的安卓智能终端模块,用于接收加密以后的密文数据,采集用户的指纹以及展示解密并脱敏后数据;

所述的FPGA模块用于接收安卓智能终端发送的数据以及指令,然后进行处理,所述的处理包括对密文数据的解密、指纹鉴权、解密后数据的脱敏,并将处理结果返回给安卓智能终端模块;具体来说:解密是加密的逆过程,将智能终端发送的密文数据转换为明文数据,脱敏是对明文数据的某些敏感信息通过脱敏规则进行数据变形,实现敏感隐私数据的可靠保护;指纹鉴权用于确保只有授权的用户才能使用设备,进一步保证安卓应用程序和机密数据的安全性。

2.根据权利要求1所述的面向安卓智能终端的基于FPGA的数据解密与脱敏设备,其特征在于所述的密钥存储模块用于存储解密模块解密时所需要的密钥,在数据处理的过程中由FPGA模块进行调用,从而整个过程中安卓智能终端模块始终没有接触到密钥文件,确保了密钥的安全性。

3.根据权利要求2所述的面向安卓智能终端的基于FPGA的数据解密与脱敏设备,其特征在于所述的指纹存储模块用于存储授权用户的指纹数据,在启动时由FPGA模块内的处理器模块调用并进行对比,从而避免授权用户的指纹数据在安卓智能终端模块泄露的风险,保证了使用设备的用户身份的真实性。

4.根据权利要求3所述的面向安卓智能终端的基于FPGA的数据解密与脱敏设备,其特征在于该设备的实现方法明包含以下步骤:

步骤一,打开安卓应用程序,提示用户进行指纹验证,用户在安卓智能终端上录入指纹后,将指纹数据发送给FPGA模块;

步骤二,FPGA模块的处理器从指纹专用存储器里读取授权用户的指纹进行鉴权,并将鉴权结果返回给安卓智能终端模块;

步骤三,安卓智能终端的应用程序根据指纹鉴权结果进行下一步动作;若成功,进行步骤四;若失败则关闭应用程序并结束操作;

步骤四,安卓应用程序上选择需要解密的密文文件和解密算法,然后将解密指令以及密文数据发送给FPGA模块;

步骤五,FPGA模块收到安卓智能终端模块解密指令后,其内部的处理器从密钥存储器中读取解密的密钥,并启动相应的数据解密电路对接收到的密文数据文件进行解密;接着,FPGA内部的处理器启动相应的脱敏模块,对解密后的明文数据进行脱敏处理;最后,FPGA模块将脱敏后的数据发送给安卓智能终端模块;

步骤六,安卓智能终端模块收到脱敏后的明文数据后,将这些数据展示给授权用户。

面向安卓智能终端的基于FPGA的数据解密与脱敏设备

技术领域

[0001] 本发明属于信息安全领域,涉及一种面向安卓智能终端的基于FPGA的数据解密与脱敏设备。

背景技术

[0002] 随着通信网络进入移动互联网时代,通过移动智能终端可以随时随地连接互联网。这使得人们可以方便地通过智能终端进行在线购物、学习、办公等,在这些过程中有很多的数据都涉及到移动智能终端的传输、处理和展示。

[0003] 例如在疫情期间很多公司采取线上办公的方式,需要传输很多的数据,其中有很多数据都涉及到公司的商业机密。但是由于互联网的开放性,这些数据在传输的过程中可能会被篡改或者窃取。这会导致数据的不安全,导致用户的损失。这些安全问题逐步成为制约移动互联网应用发展的阻碍。

[0004] 为了保护这些机密的数据的安全,可以把数据加密以后再进行传输,这样即使数据泄露,窃取者得到的只是加密以后的数据。这样确保了数据在传输过程中的安全。

[0005] 为了保护信息安全,国家商用密码管理办公室制定了一系列密码标准,用于对各种机密数据进行加解密。国密算法是我国自主研发创新的一套数据加密处理系列算法。从SM1-SM4分别实现了对称、非对称、摘要等密码算法。

[0006] SM4分组密码算法是我国自主设计的分组对称密码算法,用于实现数据的加密/解密运算,以保证数据和信息的机密性。要保证一个对称密码算法的安全性的基本条件是其具备足够的密钥长度,SM4算法与AES算法具有相同的密钥长度分组长度128比特,因此在安全性上高于3DES算法。

[0007] 由于安卓系统的开放性,用户可以随意下载并安装应用程序,其中有的应用程序可能被植入了病毒,用于窃取用户的数据。所以在安卓智能终端上对数据解密存在暴露密钥的风险。而且由于SM4等加密算法是公开算法,得到密钥就可以对数据进行解密。因此当密钥被窃取以后数据的安全性同样无法得到保障。

[0008] 此外,当数据解密以后存储在安卓智能终端并进行展示时,数据也有可能会被窃取导致信息的不安全。因此保证解密算法密钥的安全性以及解密以后数据的安全性,是安卓智能终端对机密数据进行解密以后进行展示需要解决的问题。

发明内容

[0009] 为了解决上述问题,本发明公布了一种面向安卓智能终端的基于FPGA的数据解密与脱敏设备,它能够有效的保护用于解密数据的密钥不被泄露,以及将解密以后的数据安全的在安卓智能终端上进行展示。

[0010] 为实现以上发明目的,采用的技术方案是:

[0011] 面向安卓智能终端的基于FPGA的数据解密与脱敏设备,包括安卓智能终端模块和基于FPGA的数据解密与脱敏模块(简称FPGA模块)。所述的安卓智能终端模块由具有指纹采

集功能的安卓智能终端及对应的应用程序组成。所述的FPGA模块包括处理器模块、解密模块、脱敏模块、密钥存储模块和指纹存储模块。所述安卓智能终端模块通过USB接口和FPGA模块连接，所述的秘钥存储模块和指纹存储模块通过QSPI接口与FPGA芯片连接。

[0012] 所述的处理器模块、解密模块、脱敏模块集成在FPGA芯片上。

[0013] 所述的安卓智能终端模块，用于接收加密以后的密文数据，采集用户的指纹以及展示数据。具体来说，安卓智能终端需要向用户提供友好的交互界面，包括指纹采集、密文数据接收、脱敏数据展示、以及与FPGA模块通信等功能。

[0014] 所述的FPGA模块用于接收安卓智能终端发送的数据以及指令，然后进行处理，所述的处理包括密文数据的解密和脱敏、指纹鉴权，并将处理结果返回给安卓智能终端模块。具体来说：解密是加密的逆过程，将智能终端发送的密文数据转换为明文数据，脱敏是对明文数据的某些敏感信息通过脱敏规则进行数据变形，实现敏感隐私数据的可靠保护。此时，即使FPGA模块发回的明文数据在安卓智能终端被窃取，窃取者也无法理解其原本的含义。指纹鉴权用于确保只有授权的用户才能使用设备，进一步保证安卓应用程序和机密数据的安全性。

[0015] 所述的密钥存储模块用于存储解密模块解密时所需要的密钥，在数据处理的过程中由FPGA模块进行调用，这样在整个过程中安卓智能终端模块始终没有接触到密钥文件，确保了密钥的安全性。

[0016] 所述的指纹存储模块用于存储授权用户的指纹数据，在启动时由FPGA模块内的处理器模块调用并进行对比，这样避免授权用户的指纹数据在安卓智能终端模块泄露的风险，保证了使用设备的用户身份的真实性。

[0017] 本发明包含以下步骤：

[0018] 步骤一，打开安卓应用程序，提示用户进行指纹验证，用户在安卓智能终端上录入指纹后，将指纹数据发送给FPGA模块。

[0019] 步骤二，FPGA模块的处理器从指纹专用存储器里读取授权用户的指纹进行鉴权，并将鉴权结果返回给安卓智能终端模块。

[0020] 步骤三，安卓智能终端的应用程序根据指纹鉴权结果进行下一步动作。若成功，进行步骤四；若失败则关闭应用程序并结束操作。

[0021] 步骤四，安卓应用程序上选择需要解密的密文文件和解密算法，然后将解密指令以及密文数据发送给FPGA模块。

[0022] 步骤五，FPGA模块收到安卓智能终端模块解密指令后，其内部的处理器从密钥存储器中读取解密的密钥，并启动相应的数据解密电路对接收到的密文数据文件进行解密。接着，FPGA内部的处理器启动相应的脱敏模块，对解密后的明文数据进行脱敏处理。最后，FPGA模块将脱敏后的数据发送给安卓智能终端模块。

[0023] 步骤六，安卓智能终端模块收到脱敏后的明文数据后，将这些数据展示给授权用户。

[0024] 本发明与现有技术相比，具有如下优点和有益效果：

[0025] 使用安卓智能终端的指纹采集与FPGA模块的指纹识别完成用户的鉴权，确保此安卓应用程序只有授权用户才能打开。与此同时，授权用户的指纹存储在FPGA模块内部的专用存储器上，确保了授权用户的指纹安全性。

[0026] 在FPGA芯片内嵌入微处理器软核，用于完成设备的控制，资源调度，指纹鉴别等功能。同时处理器通过片内高速总线与数据处理部分相连，可以实现数据的快速传输，减少数据的传输时间。

[0027] 利用FPGA可以编程的灵活性，可以在FPGA资源允许的情况下嵌入不同的解密算法，拓展设备的使用范围。

[0028] 密钥存储于专用的存储器中，数据的解密全程在FPGA芯片内实现，安卓智能终端始终不会接触到密钥，确保了密钥的安全性。

[0029] 数据在解密以后进行脱敏处理再返回给安卓终端进行展示，在用户能理解数据原本含义的情况下，最大程度上保证了数据的安全性。也就是说，即使在用户智能终端被控后，仍然能够保证关键机密数据的安全性。

附图说明

[0030] 图1为本发明实施例所述面向安卓智能终端的基于FPGA的数据解密与脱敏设备的结构示意图；

[0031] 图2为本发明实施例的整体工作流程图。

具体实施方式

[0032] 下面结合实施例及附图对本发明作进一步详细的描述，但本发明的实施方式不限于此。

[0033] 如图1所示，一种面向安卓智能终端的基于FPGA的数据解密与脱敏设备，包括安卓智能终端模块和基于FPGA的数据解密与脱敏模块(简称FPGA模块)。所述的安卓智能终端模块由具有指纹采集功能的安卓智能终端及对应的应用程序组成。所述的FPGA模块包括处理器模块、解密模块、脱敏模块、密钥存储模块和指纹存储模块。所述安卓智能终端模块通过USB接口和FPGA模块连接，所述的密钥存储模块和指纹存储模块通过QSPI接口与FPGA芯片连接。

[0034] 所述的安卓智能终端模块，用于接收加密以后的密文文件，采集用户的指纹进行鉴权以及数据的展示功能。具体来说，安卓智能终端需要向用户提供易用的交互界面，包括指纹采集、密文数据接收、脱敏后的数据展示、以及与FPGA模块通信等功能。

[0035] 所述的具有指纹识别功能的安卓智能终端，在此安卓智能终端只负责采集指纹，再将指纹数据发送给FPGA模块，FPGA模块对比以后再返回相应的结果。通过利用安卓智能终端的指纹采集以及FPGA模块的指纹识别功能，实现了用户身份的快速鉴权，确保了只有授权的用户才能使用设备，进一步保证了机密数据的安全性。同时减少了单独使用指纹采集模块的成本。

[0036] 安卓端应用程序由JAVA语言开发，用户可以从手机内存选择需要处理的密文文件，也可以将密文文件从别的应用程序分享至本应用程序进行处理。同时用户可以根据不同的加密的算法在应用程序里选择不同的解密算法。最后把解密指令和需要解密的数据发送给FPGA模块。

[0037] 本实施例中，安卓智能终端使用USB接口通过OTG协议与FPGA设备进行连接，此时安卓智能终端处于主机模式，设备处于从机模式。FPGA设备由安卓智能终端进行供电，无需

外接电源,方便用户使用设备。

[0038] 所述的FPGA内的处理器模块用于接收上述安卓智能终端发送的数据以及指令,并且实现对应的操作。具体有访问指纹专用存储器,将读取到的指纹数据与存储的用户指纹进行对比,并将对比结果进行返回;访问密钥专用存储器,将收到的密文数据及读取到的密钥通过片内高速总线传送给数据解密模块;内置的脱敏模块用于将解密后的数据进行脱敏处理;负责将脱敏完成的指令以及脱敏后的数据返回。本实施例中在FPGA内嵌入Nios II系列32位RISC嵌入式处理器软核,可以节约单独使用处理器的成本,以及可以通过片内Avalon交换式总线实现高速的数据传输。

[0039] 本实施例中选用的FPGA芯片为Altera公司的CycloneIV系列EP4CE10F17C8,该芯片有超过10K的逻辑单元。可以通过Altera公司的Quartus Ⅱ开发软件工具在此芯片上快速的嵌入Nios II系列32位RISC嵌入式处理器软核,其性能超过200DMIPS。该处理器可以通过Avalon交换式总线与数据处理部分连接,并提供高带宽数据路径、多路和实时处理能力。Avalon交换式总线也可用可以通过调用SOPC Builder设计软件自动生成。

[0040] 本实施例中解密模块调用解密IP核对密文数据进行解密操作。其中解密IP核使用Verilog语言,根据解密算法进行编写并进行封装,包括常用的SM4算法、AES算法以及DES算法,供用户使用时选择,后续可以根据实际情况进行增删。

[0041] 脱敏模块对解密完成以后的明文数据进行脱敏操作。数据脱敏是指对某些敏感信息通过脱敏规则进行数据的变形,实现敏感隐私数据的可靠保护。例如,对关键数据采用“***”或利用字典进行转换。由于数据已经进行脱敏处理,可以把数据发送给安卓智能终端进行展示,即使返回的数据在安卓智能终端被窃取,窃取者也无法理解其原本的含义,因为脱敏后的数据只对使用者有意义。

[0042] 本实施例中脱敏模块在处理器内使用软件方式实现,根据脱敏规则编写C函数程序,实现对数据的脱敏处理,可以方便的改写脱敏规则,以适应不同的应用场景。

[0043] 进一步,所述的密钥存储模块用于存储解密时所需要的密钥,在数据处理的过程中由FPGA模块进行调用,这样在整个过程中安卓智能终端始终没有接触到密钥文件,确保了密钥的安全性。所述的指纹存储模块用于存储授权用户的指纹数据,在启动程序时由FPGA模块内的处理器调用并进行对比,这样避免授权用户的指纹数据在安卓终端泄露的风险,确保了使用设备的用户身份的真实性。

[0044] 在本实施例中由于密钥数据大小与指纹数据所需存储空间较小,故采用同一个存储器分不同区分别存储密钥数据与指纹数据。采用QSPI FLASH芯片型号为M25PE16-VMW6TG,大小为16Mbit。在前1Mbit空间存储密钥数据,2-16Mbit空间存储指纹数据。FLASH芯片中存储的数据在写入后掉电也不会丢失,并且可以专用工具重复擦写。

[0045] 如图2所示本实施例的实施步骤如下:

[0046] 步骤一,打开安卓应用程序,提示用户进行指纹验证,用户在安卓智能终端上录入指纹后,将指纹数据发送给FPGA模块。

[0047] 步骤二,FPGA模块的处理器从指纹专用存储器里读取授权用户的指纹进行鉴权,并将鉴权结果返回给安卓智能终端模块。

[0048] 步骤三,安卓智能终端的应用程序根据指纹鉴权结果进行下一步动作。若成功,进行步骤四;若失败则关闭应用程序并结束操作。

[0049] 步骤四，安卓应用程序上选择需要解密的密文文件和解密算法，然后将解密指令以及密文数据发送给FPGA模块。

[0050] 步骤五，FPGA模块收到安卓智能终端模块解密指令后，其内部的处理器从密钥存储器中读取解密的密钥，并启动相应的数据解密电路对接收到的密文文件进行解密。接着，FPGA内部的处理器启动相应的脱敏模块，对解密后的明文数据进行脱敏处理。最后，FPGA模块将脱敏后的数据发送给安卓智能终端模块。

[0051] 步骤六，安卓智能终端模块收到脱敏后的明文数据后，将这些数据展示给授权用户。

[0052] 所述步骤二的具体实施步骤如下：

[0053] 当FPGA内处理器接收到指纹对比指令以及用户指纹数据后处理器从指纹专用存储器里逐个调取指纹数据与收到的用户指纹数据进行对比，如果对比成功则结束对比并发送指纹鉴权成功的指令给安卓智能终端，如果对比完所有的指纹数据都失败则返回指纹鉴权失败的指令给安卓智能终端。

[0054] 所述步骤五的具体实施步骤如下：

[0055] FPGA模块收到安卓智能终端模块得解密指令后，处理器根据收到的解密指令选择使用对应的解密算法IP核以及从密钥专用存储器中读取密钥然后把密文数据以及密钥发给数据解密模块进行解密。其中在FPGA中例化一个双口RAM用于实现处理器和FPGA的数据交互，双口RAM一侧通过Avalon总线连接处理器，另一侧与FPGA解密模块相连，可以实现处理器与FPGA的高速全双工传输。当数据解密完以后解密模块将解密后的明文数据返回给处理器，处理器收到解密完成指令后启动数据脱敏模块对明文数据进行脱敏。脱敏完成以后，处理器向安卓智能终端发送数据脱敏完成指令，并把脱敏后的数据发送给安卓智能终端。

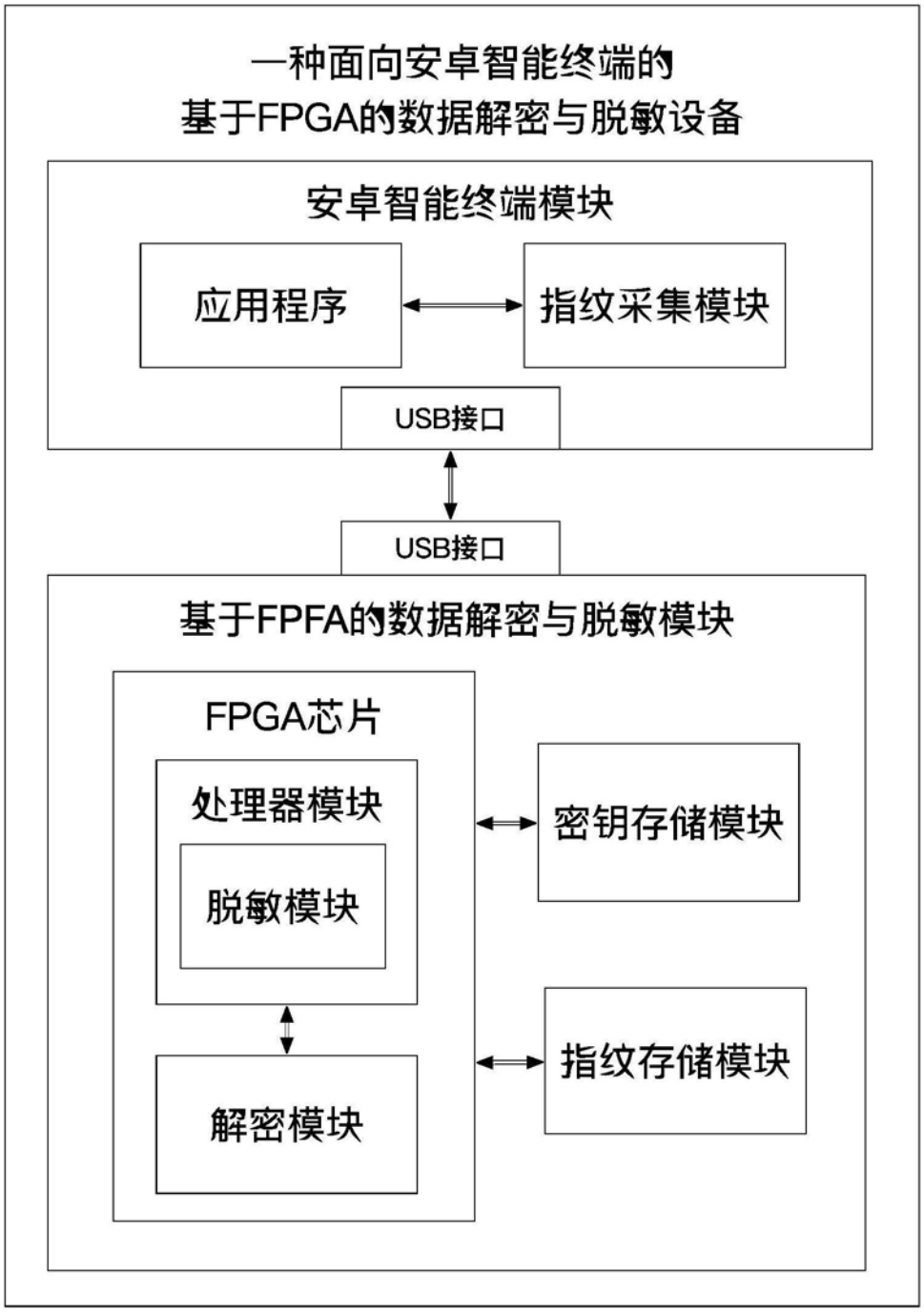

一种面向安卓智能终端的
基于FPGA的数据解密与脱敏设备
安卓智能终端模块
应用程序
指纹采集模块
USB接口
USB接口
基于FPFA的数据解密与脱敏模块
FPGA芯片
处理器模块
脱敏模块
解密模块
密钥存储模块
指纹存储模块

图1

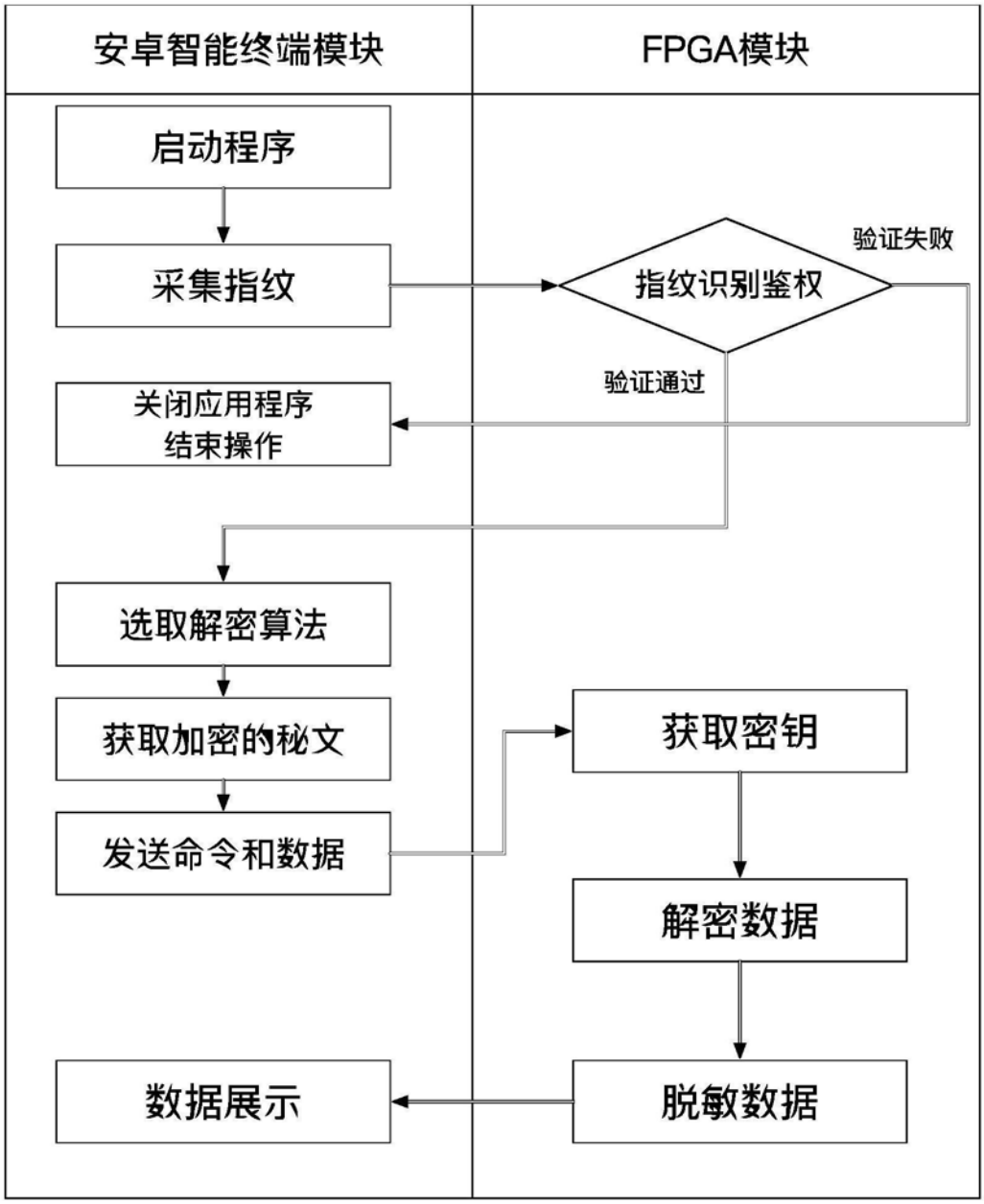

安卓智能终端模块
FPGA模块
启动程序
采集指纹
指纹识别鉴权
验证失败
验证通过
关闭应用程序
结束操作
选取解密算法
获取加密的秘文
发送命令和数据
获取密钥
解密数据
脱敏数据
数据展示

图2