(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2017 年 11 月 23 日 (23.11.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/197689 A1

(51) 国际专利分类号:
H04W 12/04 (2009.01) *H04W 88/02* (2009.01)
H04W 12/06 (2009.01)

(21) 国际申请号: PCT/CN2016/085725

(22) 国际申请日: 2016 年 6 月 14 日 (14.06.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201610333585.8 2016年5月18日 (18.05.2016) CN

(71) 申请人: 中兴通讯股份有限公司 (ZTE CORPORATION) [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(72) 发明人: 孙东平 (SUN, Dongping); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦中兴通讯股份有限公司转交, Guangdong 518057 (CN)。

(74) 代理人: 北京安信方达知识产权代理有限公司 (AFD CHINA INTELLECTUAL PROPERTY LAW OFFICE); 中国北京市海淀区学清路8号B座1601A, Beijing 100192 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

根据细则4.17的声明:
— 关于申请人有权申请并被授予专利 (细则4.17(ii))
— 发明人资格 (细则4.17(iv))

本国际公布:
— 包括国际检索报告 (条约第21条(3))。

(54) **Title:** SIM CARD PROCESSING METHOD AND APPARATUS, TERMINAL, AND ESAM CHIP

(54) **发明名称**: 一种SIM卡处理方法、装置、终端及ESAM芯片

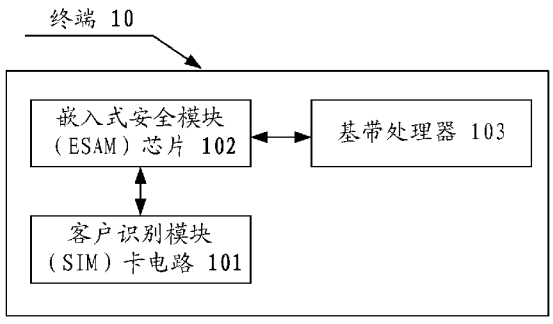

图 1

10 TERMINAL
101 SUBSCRIBER IDENTITY MODULE (SIM) CARD CIRCUIT
102 EMBEDDED SECURITY MODULE (ESAM) CHIP
103 BASEBAND PROCESSOR

(57) **Abstract:** Provided are a subscriber identity module (SIM) card processing method and apparatus, a terminal, and an ESAM chip. The method comprises: when it is detected that an SIM card is inserted, reading the card number of the SIM card inserted into a terminal; and using an embedded security module (ESAM) chip used for authenticating the card number of the SIM card to authenticate the read card number of the SIM card.

(57) **摘要**: 本申请提供了一种客户识别模块SIM卡处理方法、装置、终端及ESAM芯片，该方法包括：检测到有SIM卡插入，读取插入终端的SIM卡的卡号；采用用于对SIM卡的卡号进行认证的嵌入式安全模块ESAM芯片，对读取到的SIM卡的卡号进行认证。

WO 2017/197689 A1

一种 SIM 卡处理方法、装置、终端及 ESAM 芯片

技术领域

本申请涉及但不限于通信领域，尤其涉及一种客户识别模块 SIM（Subscriber Identity Module，简称为 SIM）卡处理方法、装置、终端及嵌入式安全模块 ESAM（Embedded Secure Access Module，简称为 ESAM）芯片。

背景技术

在相关技术中，由于经常发生终端（例如，手机）丢失、被盗的现象，因此，很多终端都设置有对插入的 SIM 卡进行鉴权认证的功能。但是，对终端接入的 SIM 卡进行鉴权时，一般采用软件算法的方式进行鉴权。这些功能即使设定了，一般也是可以通过软件代码进行破解的。一旦被破解，丢失或者被盗的终端依然可以使用。

因此，在相关技术中，存在通过软件算法的方式对 SIM 卡进行鉴权，无法保证鉴权的安全性和可靠性的问题。

发明内容

以下是对本文详细描述的主题的概述。本概述并非是为了限制权利要求的保护范围。

本发明实施例提供了一种 SIM 卡处理方法、装置、终端及 ESAM 芯片，解决了在相关技术中，通过软件算法的方式对 SIM 卡进行鉴权，无法保证鉴权的安全性和可靠性的问题。

一种终端，包括：客户识别模块 SIM 卡电路，基带处理器，和嵌入式安全模块 ESAM 芯片，其中：所述 SIM 卡电路，设置为检测到有 SIM 卡插入时，读取接入终端的所述 SIM 卡的卡号；所述 ESAM 芯片，连接至所述 SIM 卡电路和所述基带处理器，设置为对读取到的所述 SIM 卡的卡号进行认证。

可选地，所述 ESAM 芯片对读取到的所述 SIM 卡的卡号进行认证包括：根据用于标识 ESAM 芯片的 ESAM 标识 ID 以及与 ESAM 芯片绑定的 SIM 卡的卡号的绑定关系，对读取到的所述 SIM 卡的卡号进行认证。

其中，根据用于标识 ESAM 芯片的 ESAM 标识 ID，以及与 ESAM 芯片绑定的 SIM 卡的卡号的绑定关系，对读取到的所述 SIM 卡的卡号进行认证包括:

根据获取到的所述SIM卡的卡号、所述ESAM芯片中存储的所述ESAM ID以及用于加密的密钥进行计算得到密文。

比较计算得到的密文与预定密文是否相同；其中，所述预定密文包括:在所述 ESAM 芯片中，根据所述绑定关系中预先存储的 SIM 卡的卡号、所述 ESAM ID 以及所述密钥计算得到的密文。

在比对结果为计算得到的密文与所述预定密文相同时，确定对所述 SIM 卡的卡号认证成功；以及在比对结果为计算得到的密文与所述预定密文不相同时，确定对所述 SIM 卡的卡号认证失败。

可选地，所述 ESAM 芯片根据获取到的所述 SIM 卡的卡号、所述 ESAM 芯片中存储的所述 ESAM ID 以及用于加密的密钥进行计算得到密文包括:

生成用于计算所述密文的随机数。

采用生成的所述随机数，根据获取到的所述 SIM 卡的卡号、所述 ESAM 芯片中存储的所述 ESAM ID，以及用于加密的密钥进行计算得到密文。

可选地，所述终端还包括：基带处理器。

所述基带处理器，设置为在所述 ESAM 芯片对读取到的所述 SIM 卡的卡号进行认证之后，根据所述 ESAM 芯片发送的用于通知所述基带处理器对所述终端的软件进行销毁通知，进行所述终端的软件的销毁。

可选地，所述 ESAM 芯片，还设置为通知所述基带处理器进行所述终端的软件的销毁，并在接收到所述基带处理器返回的、用于指示所述终端的软件销毁完成的指示消息后，断开与所述 SIM 卡电路以及与所述基带处理器的通信路径。

一种客户识别模块 SIM 卡处理方法，包括：检测到有 SIM 卡插入时，读取插入终端的 SIM 卡的卡号；采用用于对 SIM 卡的卡号进行认证的嵌入式安全模块 ESAM 芯片，对读取到的所述 SIM 卡的卡号进行认证。

可选地，采用用于对 SIM 卡的卡号进行认证的 ESAM 芯片，对获取到

的所述 SIM 卡的卡号进行认证包括: 根据用于标识 ESAM 芯片的 ESAM 标识 ID 以及与 ESAM 芯片绑定的 SIM 卡的卡号的绑定关系，对读取到的所述 SIM 卡的卡号进行认证。

其中，根据用于标识 ESAM 芯片的 ESAM 标识 ID，以及与 ESAM 芯片绑定的 SIM 卡的卡号的绑定关系，对读取到的所述 SIM 卡的卡号进行认证包括:

根据获取到的所述 SIM 卡的卡号、所述 ESAM 芯片中存储的所述 ESAM ID 以及用于加密的密钥进行计算得到密文。

比较计算得到的密文与预定密文是否相同；其中，所述预定密文包括: 在所述 ESAM 芯片中，根据所述绑定关系中预先存储的 SIM 卡的卡号、所述 ESAM ID 以及所述密钥计算得到的密文。

在比对结果为计算得到的密文与所述预定密文相同时，确定对所述 SIM 卡的卡号认证成功; 以及在比对结果为计算得到的密文与所述预定密文不相同时，确定对所述 SIM 卡的卡号认证失败。

可选地，根据获取到的所述 SIM 卡的卡号、所述 ESAM 芯片中存储的所述 ESAM ID，以及用于加密的密钥进行计算得到密文包括: 生成用于计算所述密文的随机数; 采用生成的所述随机数，根据获取到的所述 SIM 卡的卡号、所述 ESAM 芯片中存储的所述 ESAM ID，以及用于加密的密钥进行计算得到密文。

可选地，所述方法还包括: 在采用用于对 SIM 卡的卡号进行认证的嵌入式安全模块 ESAM 芯片，对获取到的所述 SIM 卡的卡号进行认证之后，在对所述 SIM 卡的卡号认证失败时，控制所述终端进行销毁操作。

其中，在对所述 SIM 卡的卡号认证失败时，控制所述终端进行销毁操作，包括:

向所述终端的基带处理器发送通知消息，其中，所述通知消息用于通知所述基带处理器对所述终端的软件进行销毁。

在接收到所述基带处理器返回的、用于指示所述终端的软件销毁完成的指示消息后，断开与所述终端的 SIM 卡电路以及与所述终端的基带处理器

的通信路径。

一种客户识别模块 SIM 卡处理装置，包括，获取模块，设置为检测到有 SIM 卡插入时，读取插入终端的 SIM 卡的卡号。

认证模块，设置为采用用于对 SIM 卡的卡号进行认证的嵌入式安全模块 ESAM 芯片，对读取到的所述 SIM 卡的卡号进行认证。

可选地，所述认证模块采用用于对 SIM 卡的卡号进行认证的 ESAM 芯片，对获取到的所述 SIM 卡的卡号进行认证包括：根据用于标识 ESAM 芯片的 ESAM 标识 ID 以及与 ESAM 芯片绑定的 SIM 卡的卡号的绑定关系，对获取到的所述 SIM 卡的卡号进行认证。

其中，所述认证模块包括：计算单元、比对单元和确定单元。

所述认证模块根据用于标识 ESAM 芯片的 ESAM 标识 ID，以及与 ESAM 芯片绑定的 SIM 卡的卡号的绑定关系，对读取到的所述 SIM 卡的卡号进行认证包括：

计算单元，设置为根据获取到的所述 SIM 卡的卡号、所述 ESAM 芯片中存储的所述 ESAM ID 以及用于加密的密钥进行计算得到密文。

比对单元，设置为比较计算得到的密文与预定密文是否相同；其中，所述预定密文包括：在所述 ESAM 芯片中，根据所述绑定关系中预先存储的 SIM 卡的卡号、所述 ESAM ID 以及所述密钥计算得到的密文。

确定单元，设置为在比对结果为计算得到的密文与所述预定密文相同时，确定对所述 SIM 卡的卡号认证成功；以及在比对结果为计算得到的密文与所述预定密文不相同时，确定对所述 SIM 卡的卡号认证失败。

可选地，所述计算单元包括：生成子单元，设置为生成用于计算所述密文的随机数；计算子单元，设置为采用生成的所述随机数，根据获取到的所述 SIM 卡的卡号、所述 ESAM 芯片中存储的所述 ESAM ID，以及用于加密的密钥进行计算得到密文。

可选地，所述装置还包括：控制模块。

所述控制模块，设置为在认证模块对获取到的所述 SIM 卡的卡号进行认证之后，在对所述 SIM 卡的卡号认证失败时，控制所述终端进行销毁操

作。

所述控制模块包括：通知单元和断开单元。

其中，所述控制模块在对所述 SIM 卡的卡号认证失败时，控制所述终端进行销毁操作包括：

通知单元，设置为向所述终端的基带处理器发送通知消息，其中，所述通知消息用于通知所述基带处理器对所述终端的软件进行销毁；断开单元，设置为在接收到所述基带处理器返回的、用于指示所述终端的软件销毁完成的指示消息后，断开与所述终端的 SIM 卡电路以及与所述终端的基带处理器的通信路径。

一种嵌入式安全模块 ESAM 芯片。该 ESAM 芯片包括前述任一项所述客户识别模块 SIM 卡处理装置。

一种计算机可读存储介质，存储有计算机可执行指令，所述计算机可执行指令被处理器执行时实现所述的客户识别模块 SIM 卡处理方法。

该存储介质设置为存储用于执行以下步骤的程序代码：检测到有 SIM 卡插入时，读取插入终端的 SIM 卡的卡号；采用用于对 SIM 卡的卡号进行认证的嵌入式安全模块 ESAM 芯片，对读取到的所述 SIM 卡的卡号进行认证。

可选地，存储介质还设置为存储用于执行以下步骤的程序代码：采用用于对 SIM 卡的卡号进行认证的 ESAM 芯片，对获取到的所述 SIM 卡的卡号进行认证包括：根据用于标识 ESAM 芯片的 ESAM 标识 ID 以及与 ESAM 芯片绑定的 SIM 卡的卡号的绑定关系，对获取到的所述 SIM 卡的卡号进行认证。

其中，根据用于标识 ESAM 芯片的 ESAM 标识 ID，以及与 ESAM 芯片绑定的 SIM 卡的卡号的绑定关系，对读取到的所述 SIM 卡的卡号进行认证包括：

根据获取到的所述SIM卡的卡号、所述ESAM芯片中存储的所述ESAM ID 以及用于加密的密钥进行计算得到密文。

比较计算得到的密文与预定密文是否相同；其中，所述预定密文包括：

在所述 ESAM 芯片中，根据所述绑定关系中预先存储的 SIM 卡的卡号、所述 ESAM ID 以及所述密钥计算得到的密文。

在比对结果为计算得到的密文与所述预定密文相同时，确定对所述 SIM 卡的卡号认证成功；以及在比对结果为计算得到的密文与所述预定密文不相同时，确定对所述 SIM 卡的卡号认证失败。

可选地，存储介质还被设置为存储用于执行以下步骤的程序代码：根据获取到的所述 SIM 卡的卡号、所述 ESAM 芯片中存储的所述 ESAM ID 以及用于加密的密钥进行计算得到密文包括：生成用于计算所述密文的随机数；采用生成的所述随机数，根据获取到的所述 SIM 卡的卡号、所述 ESAM 芯片中存储的所述 ESAM ID，以及用于加密的密钥进行计算得到密文。

可选地，存储介质还被设置为存储用于执行以下步骤的程序代码：在采用用于对 SIM 卡的卡号进行认证的嵌入式安全模块 ESAM 芯片，对获取到的所述 SIM 卡的卡号进行认证之后，在对所述 SIM 卡的卡号认证失败时，控制所述终端进行销毁操作。

其中，在对所述 SIM 卡的卡号认证失败时，控制所述终端进行销毁操作，包括：向所述终端的基带处理器发送通知消息，其中，所述通知消息用于通知所述基带处理器对所述终端的软件进行销毁。在接收到所述基带处理器返回的、用于指示所述终端的软件销毁完成的指示消息后，断开与所述终端的 SIM 卡电路以及与所述终端的基带处理器的通信路径。

通过本发明实施例方案，在终端的 SIM 卡电路和基带处理器之间设置一个 ESAM 芯片，通过 ESAM 芯片对终端接入的 SIM 卡的卡号进行认证，由于 ESAM 芯片具有安全性高，不易被破解的优点，因此，可以解决在相关技术中，通过软件算法的方式对 SIM 卡进行鉴权，无法保证鉴权的安全性和可靠性的问题，达到提高 SIM 卡鉴权的安全性和可靠性的效果。

附图概述

图 1 是根据本发明实施例的终端的结构框图；

图 2 是根据本发明实施例的 SIM 卡处理方法的流程图；

图 3 是根据本发明可选实施例的 SIM 卡处理方法的流程图；

图 4 是根据本发明实施例的 SIM 卡处理装置的结构框图一;

图 5 是根据本发明实施例的 SIM 卡处理装置中认证模块 44 的结构框图;

图 6 是根据本发明实施例的 SIM 卡处理装置中计算单元 52 的结构框图;

图 7 是根据本发明实施例的 SIM 卡处理装置的结构框图二。

本发明的实施方式

下文中将结合附图对本发明的实施例进行详细说明。需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互任意组合。

需要说明的是，本发明实施例的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。

实施例 1

本实施例所提供的终端可以是移动终端、计算机终端或者类似的运算装置。图 1 是根据本发明实施例的终端的结构框图。如图 1 所示，终端 10 可以包括一个或多个（图中仅示出一个）SIM 卡电路 101、一个或多个（图中仅示出一个）ESAM 芯片 102、以及基带处理器 103。本领域普通技术人员可以理解，图 1 所示的结构仅为示意，其并不对上述终端的结构造成限定。例如，终端 10 还可包括比图 1 中所示更多或者更少的组件(例如，基带部分、射频部分、显示部分、外设部分、子板等)，或者具有与图 1 所示不同的配置。

SIM 卡电路 101，设置为检测到有 SIM 卡插入，读取插入的 SIM 卡的卡号；ESAM 芯片 102，分别连接到 SIM 卡电路 101 和基带处理器 103，设置为对读取到的 SIM 卡的卡号进行认证。

通过本发明实施例的上述技术方案，在终端 10 的 SIM 卡电路 101 和基带处理器之间设置 ESAM 芯片，通过 ESAM 芯片对 SIM 卡电路 101 中插入的 SIM 卡的卡号进行认证。由于 ESAM 芯片具有安全性高，不易被破解的优点，可以解决在相关技术中，存在通过软件算法的方式对 SIM 卡进行鉴权，无法保证鉴权的安全性和可靠性的问题，达到提高 SIM 卡鉴权的安全性和可靠性的效果。

终端 10 可以包括一个或多个 SIM 卡电路 101，当包含多个 SIM 卡电路 101 时，每个 SIM 卡电路 101 中可插入相同或者不同运营商(例如移动、联通等)的 SIM 卡，只要 SIM 卡电路 101 可以识别并读取插入的 SIM 卡所对应的卡号即可。

终端 10 可以包括一个或多个 ESAM 芯片 102，当包含多个 ESAM 芯片 102，每个 ESAM 芯片 102 可以分别连接至不同的 SIM 卡电路 101。也就是说，根据不同的需求，终端 10 中的一个或多个 SIM 卡电路 101 可连接至同一 ESAM 芯片 102，或者不同的 SIM 卡电路 101 连接至不同的 ESAM 芯片 102，只要满足 ESAM 芯片 102 分别连接至 SIM 卡电路 101 和基带处理器 103 即可。ESAM 芯片 102 可以通过总线与和 SIM 卡电路 101 及基带处理器 103 相连。

可选地，ESAM 芯片 102 还设置为根据用于标识 ESAM 芯片的 ESAM ID 以及与 ESAM 芯片绑定的 SIM 卡的卡号的绑定关系，对读取到的 SIM 卡的卡号进行认证。

ESAM 芯片硬件安全性获得了ITSECEAL5 级认证，可见其安全性是值得肯定的。同时，ESAM 芯片还具有身份识别的功能。在 ESAM 芯片内部存储了唯一的标号(ESAM 的 ID)，这个唯一的标号是 ESAM 芯片出厂前设定的，是唯一的，如同人的身份证，是无法改变的，同时可以防止 SEMA/DEMA、SPA/DPA、DFA 和时序等措施的攻击破解，保证了安全性和唯一性。

在将用于标识 ESAM 芯片的 ESAM 标识 ID，以及 SIM 卡的卡号进行绑定时，需要分发该 SIM 卡的运营商将 SIM 卡号和 ESAM 芯片的 ESAM ID 绑定在一起，并将相应的绑定信息写入 ESAM 芯片。

当终端丢失或者被盗后，一般使用时会更换其他的 SIM 卡。当检测到有 SIM 卡插入时，读取插入的 SIM 卡的卡号。ESAM 芯片根据用于标识 ESAM 芯片的 ESAM ID，以及与 ESAM 芯片绑定的 SIM 卡的卡号的绑定关系，对读取到的 SIM 卡的卡号进行认证，并在对读取到的 SIM 卡的卡号认证。

通过本发明实施例的上述技术方案，根据用于标识 ESAM 芯片的 ESAM

ID，以及与 ESAM 芯片绑定的与 SIM 卡的卡号的绑定关系，对读取到的 SIM 卡的卡号进行认证，保证了对插入的 SIM 卡的卡号认证的准确性，保证了对 SIM 卡认证的安全性和可靠性。

可选地，在 ESAM 芯片 102 对读取的 SIM 卡的卡号认证失败时，控制终端进行销毁操作。

需要说明的是，上述控制终端进行销毁操作可以包括多种，例如，可以包括对终端的锁定操作和对终端的毁坏操作。其中，该锁定操作可以是对一些重要应用进行限制使用的限定操作。而该毁坏操作则是对终端硬件进行破坏的破坏操作。当终端的拥有者再次得到终端，需要对终端再次使用时，对于上述锁定操作，需要携带终端、绑定时所使用的相关证件及 SIM 卡到运营商安排的地点或者别的相关部门对限定操作进行解锁操作。而对于上述毁坏操作，则需要携带终端、绑定时所使用的相关证件及 SIM 卡到运营商安排的地点或者别的相关部门对破坏操作进行硬件恢复操作处理，该毁坏操作的硬件恢复相比于锁定操作的解锁操作相对来说，可能需要耗费较长时间。

通过本发明实施例的上述技术方案，能够解决终端数据的自动销毁功能容易被破解的问题，进而保证了用户的隐私和财产安全。

可选地，基带处理器 103 根据 ESAM 芯片 102 的通知，进行终端中安装的软件的自动销毁，例如，卸载或者部分卸载终端 10 上已经安装的客户端、清除终端 10 中保存的账号和密码、格式化终端 10 中存储的文件、格式化终端 10 的操作系统等。

通过本发明实施例的上述技术方案，实现了对终端 10 中安装的软件的销毁，清除了可能泄露用户隐私的图片、视频等数据以及可能导致用户财产损失的用户银行账户、虚拟账户相关的账号(例如各银行账号、支付宝、微信、互联网金融相关的账号以及游戏账号)和密码信息以及商业信息等，有针对性地保证了用户的隐私及财产安全。

可选地，ESAM 芯片 102 还可以设置为通知基带处理器 103 进行终端 10 中安装的软件的销毁，并在接收到基带处理器 103 返回的、用于指示终端的软件销毁完成的指示消息后，断开与 SIM 卡电路 101 以及与基带处理器 103 的通信路径。例如，通过将 ESAM 芯片 102 的内部熔丝短路，断开

与 SIM 卡电路 101 以及与基带处理器 106 的通信路径。

通过本发明实施例的上述技术方案，由于 ESAM 芯片 102 连接在 SIM 卡电路 101 以及基带处理器 103 之间，当 SIM 卡电路 10 与基带处理器 106 之间的通信路径断开后，SIM 卡电路 101 将不能正常工作。同时，由于 ESAM 芯片 102 与基带处理器 103 之间的通信路径断开，基带处理器 103 将检测不到 ESAM 芯片 102，而检测到 ESAM 芯片 102 是下载版本的必要条件，故检测不到 ESAM 芯片 102 也将无法完成下载功能，此时的终端成为板砖，防止了丢失终端被使用，而不能使用的终端不具备可交易的价值，因此，降低了因为偷窃终端而造成的伤害事故的数量。

实施例 2

在本实施例中提供了一种客户识别模块 SIM 卡处理方法，图 2 是根据本发明实施例的 SIM 卡处理方法的流程图，如图 2 所示，该流程包括步骤 S201-S202:

步骤 S201，检测到有 SIM 卡插入时，读取插入终端的 SIM 卡的卡号。

步骤 S202，采用用于对 SIM 卡的卡号进行认证的嵌入式安全模块 ESAM 芯片，对读取到的 SIM 卡的卡号进行认证。

可选地，上述步骤 S202 可以包括：根据用于标识 ESAM 芯片的 ESAM ID，以及与 ESAM 芯片绑定的 SIM 卡的卡号的绑定关系，对读取到的 SIM 卡的卡号进行认证。

其中，根据用于标识 ESAM 芯片的 ESAM 标识 ID，以及与 ESAM 芯片绑定的 SIM 卡的卡号的绑定关系，对读取到的所述 SIM 卡的卡号进行认证包括:

根据获取到的 SIM 卡的卡号、ESAM 芯片中存储的 ESAM ID 以及用于加密的密钥进行计算得到密文。

比较计算得到的密文与预定密文是否相同；其中，所述预定密文包括：在所述 ESAM 芯片中，根据所述绑定关系中预先存储的 SIM 卡的卡号、所述 ESAM ID 以及所述密钥计算得到的密文。

在比对结果为计算得到的密文与预定密文相同时，确定对 SIM 卡的卡

号认证成功；以及在比对结果为计算得到的密文与预定密文不相同时，确定对 SIM 卡的卡号认证失败。

可选地，还可以根据其他多种方式对获取到的 SIM 卡的卡号进行认证，例如，可以根据用于标识 ESAM 芯片的 ESAM ID，ESAM 芯片绑定的用户的用户 ID 以及 SIM 卡的卡号的绑定关系，或者，根据 ESAM 芯片绑定的用户的用户 ID 以及 SIM 卡的卡号的绑定关系，或者，直接根据 ESAM 芯片中绑定 SIM 卡的卡号，对获取到的 SIM 卡的卡号进行认证。而上述用户 ID 可以是用户的身份证或者其他可以为唯一标识用户身份的证件的号码。

通过使用密钥加密以及加密结果比对的方式，增加了对获取到的 SIM 卡的卡号认证的安全性以及认证结果的可靠性。

可选地，上述步骤 S202 还可以包括:

生成用于计算密文的随机数。

采用生成的随机数，根据获取到的 SIM 卡的卡号、ESAM 芯片中存储的 ESAM ID，以及用于加密的密钥进行计算得到密文。

通过生成用于计算密文的随机数，在计算密文时使用了上述随机数，由于随机数的产生是随机的，保证了对获取到的 SIM 卡的卡号认证的安全性以及认证结果的可靠性。

可选地，在步骤 S202 以后，该方法还可以包括：在对所述 SIM 卡的卡号认证失败时，控制所述终端进行销毁操作。

其中，在对所述 SIM 卡的卡号认证失败时，控制所述终端进行销毁操作包括:

向终端的基带处理器发送通知消息，其中，通知消息用于通知基带处理器对终端的软件进行销毁。

在接收到基带处理器返回的、用于指示终端的软件销毁完成的指示消息后，断开与终端的 SIM 卡电路以及与终端的基带处理器的通信路径。

可选地，基带处理器可以采用多种方式对终端的软件进行销毁，例如，可以通过以下方式的至少之一对终端的软件进行销毁: 卸载或者部分卸载终端上已经安装的客户端、清除终端中保存的账号和密码、格式化终端中存储

的文件、格式化终端的操作系统。

可选地，可以采用多种方式断开与终端的 SIM 卡电路以及与终端的基带处理器的通信路径，例如，可以将 ESAM 芯片的内部熔丝短路。

可选地，上述步骤的执行主体可以为 ESAM 芯片或者嵌入有上述 ESAM 芯片的终端等，但不限于此。

基于上述实施例及可选实施方式，为说明方案的整个流程交互，在本优选实施例中，提供了一种 SIM 卡处理方法，图 3 是根据本发明可选实施例的 SIM 卡处理方法的流程图，需要说明的是，在该 SIM 卡处理方法中，终端以手机为例进行说明。如图 3 所示，该流程包括步骤 S301-S313:

步骤 S301：进入客户端，进行自动销毁设置，可以选择卸载某些客户端、格式化文件、账号密码的清除和删除手机操作系统。

步骤 S302：检测是否有 SIM 卡的插入，通过 SIM 卡的中断信号进行相应的检测。

步骤 S303：ESAM 模块的内部小系统对 SIM 卡号进行读取。

步骤 S304：ESAM 模块内部产生一组随机数，用于密文的验证。

步骤 S305：将读取到的 SIM 卡号，结合原先绑定的身份证，ESAM 本身的 ID 进行密钥的计算。

步骤 S306：将计算出的密文和原先设置的密文进行比较；如果两者的密文相同，则转到 S307 和 S308；密文不同则转到 S309。

步骤 S307：密文相同，对读取的 SIM 卡的卡号认证成功，可以进行数据传输工作.

步骤 S308：认证后，手机可以正常使用，流程结束。

步骤 S309：计算的密文和原先设定的密文不一样，对读取的 SIM 卡的卡号认证失败，启动相关的销毁流程。例如，可以先进行软件的销毁工作，进行应用程序 app 的卸载，账号密码的清除，格式化文件以及手机操作系统的删除。

步骤 S310：判断软件销毁是否完成，如果没完成，返回 S309，如果软

件销毁完成，则跳转到 S311。

步骤 S311：ESAM 模块内部的熔丝短路，启动相应的硬件销毁。

步骤 S312：ESAM 模块停止了工作，也就切断了 SIM 卡电路和基带处理器之间的通信，手机无法进行与 SIM 相关的工作了。

步骤 S313：手机完成销毁。由于 ESAM 模块内部熔丝短路后，基带处理器无法检测到 ESAM 模块，即使重新刷机，整个手机系统也不会启动。

例如，机主 A 的手机丢了，机主 A 的手机号码是 15888888888，身份证 300001199911113333，ESAM 的 ID 是 IS400500600，机主 A 在购买手机的时候办理了启动自动销毁的功能，并在营业厅将手机号码、ESAM 的 ID 和身份证进行了绑定。且对自动销毁的模式也进行了设置，当 SIM 卡号不对时，将卸载支付宝等全部应用，同时格式化存储的文件和手机系统，ESAM 自动销毁也进行了启动，这是机主 A 对自己手机的自动销毁项进行的设置。有一天，机主 A 的手机丢了，被 B 捡到了，B 将自己的手机卡插进了 A 的手机，此时，手机会检测有 SIM 卡的插入，检测后进行 SIM 卡号的读取，并将读取的 SIM 卡号和机主 A 的身份证号、ESAM 的 ID 号码进行密文的计算，然后将计算的密文和原先设定的密文进行比较，比较后，发现密文不一样，SIM 卡的卡号认证失败，此时启动自动销毁，先进行软件自动销毁，主要是卸载支付宝等应用程序，格式化存储的数据和手机系统，完成后进行 ESAM 的自动销毁，此时，ESAM 内部熔丝短路，完成销毁，同时也断开了 SIM 卡电路和基带处理器之间的通路，手机成为板砖。

通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到根据上述实施例的方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明实施例的技术方案本质上或者说对相关技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质（如 ROM/RAM、磁碟、光盘）中，包括多个指令用以使得一台终端设备（可以是手机，计算机，服务器，或者网络设备等）执行本发明实施例所述的方法。

实施例 3

在本实施例中还提供了一种客户识别模块 SIM 卡处理装置及 ESAM 芯片，该装置用于实现上述实施例及优选实施方式，已经进行过说明的不再赘述。如以下所使用的，术语“模块”可以实现预定功能的软件和/或硬件的组合。尽管以下实施例所描述的装置较佳地以软件来实现，但是硬件，或者软件和硬件的组合的实现也是可能并被构想的。

图 4 是根据本发明实施例的 SIM 卡处理装置的结构框图一，如图 4 所示，该装置包括：获取模块 41、认证模块 42，下面对该装置进行说明。

获取模块 41，设置为检测到有 SIM 卡插入时，读取插入终端的 SIM 卡的卡号；认证模块 42，连接至上述获取模块 41，设置为采用用于对 SIM 卡的卡号进行认证的嵌入式安全模块 ESAM 芯片，对读取到的 SIM 卡的卡号进行认证。

图 5 是根据本发明实施例的 SIM 卡处理装置中认证模块 44 的结构框图，该认证模块 4 采用用于对 SIM 卡的卡号进行认证的 ESAM 芯片，对获取到的所述 SIM 卡的卡号进行认证包括：根据用于标识 ESAM 芯片的 ESAM 标识 ID 以及与 ESAM 芯片绑定的 SIM 卡的卡号的绑定关系，对获取到的 SIM 卡的卡号进行认证。如图 5 所示，该认证模块 42 包括计算单元 51、比对单元 52 和确定单元 53，下面对该认证模块 42 进行说明。

计算单元 51，设置为根据获取到的 SIM 卡的卡号、ESAM 芯片中存储的 ESAM ID，以及用于加密的密钥进行计算得到密文；比对单元 52，连接至上述计算单元 51，设置为比较计算得到的密文与 ESAM 芯片中根据绑定关系中预先存储的 SIM 卡的卡号、ESAM ID 以及密钥计算得到的预定密文是否相同；确认单元 53，连接至上述比对单元 52，设置为在比对结果为计算得到的密文与预定密文相同时，确定对上述 SIM 卡的卡号认证成功；以及在比对结果为计算得到的密文与上述预定密文不相同时，确定对 SIM 卡的卡号认证失败。

图 6 是根据本发明实施例的 SIM 卡处理装置中计算单元 51 的结构框图，如图 6 所示，该计算单元 51 包括生成子单元 61 和计算子单元 62，下面对该计算单元 51 进行说明。

生成子单元 61，设置为生成用于计算密文的随机数；计算子单元 62，

连接至上述生成子单元 61，设置为采用生成的随机数，根据获取到的 SIM 卡的卡号、ESAM 芯片中存储的 ESAM ID，以及用于加密的密钥进行计算得到密文。

图 7 是根据本发明实施例的 SIM 卡处理装置的结构框图二，如图 7 所示，该装置还包括控制模块 43，设置为在对 SIM 卡的卡号认证失败时，控制终端进行销毁操作。该控制模块 43 包括通知单元 71、断开单元 72，下面对该控制模块 43 进行说明。

通知单元 71，设置为向终端的基带处理器发送通知消息，其中，上述通知消息用于通知上述基带处理器对终端的软件进行销毁；断开单元 74，连接至上述通知单元 71，设置为在接收到基带处理器返回的、用于指示终端的软件销毁完成的指示消息后，断开与终端的 SIM 卡电路以及与终端的基带处理器的通信路径。

可选地，上述基带处理器对终端的软件进行销毁包括以下以下一种或多种：卸载或者部分卸载终端上已经安装的客户端、清除终端中保存的账号和密码、格式化终端中存储的文件、格式化终端的操作系统；或者，断开与终端的 SIM 卡电路以及与终端的基带处理器的通信路径包括：将 ESAM 芯片的内部熔丝短路。

需要说明的是，上述每个模块是可以通过软件或硬件来实现的，对于后者，可以通过以下方式实现，但不限于此：上述模块均位于 ESAM 芯片中；或者，上述每个模块以任意组合的形式分别位于不同的 ESAM 芯片中，而上述 ESAM 芯片位于包括 SIM 卡电路和基带处理器的终端之中。

一种计算机可读存储介质，存储有计算机可执行指令，所述计算机可执行指令被处理器执行时实现所述的客户识别模块 SIM 卡处理方法。

本发明实施例还提供了一种存储介质。可选地，在本实施例中，上述存储介质可以被设置为存储用于执行以下步骤的程序代码：

S1，检测到有 SIM 卡插入时，读取插入终端的 SIM 卡的卡号。

S2，采用用于对 SIM 卡的卡号进行认证的嵌入式安全模块 ESAM 芯片，对读取到的 SIM 卡的卡号进行认证。

可选地，存储介质还被设置为存储用于执行以下步骤的程序代码：

采用用于对 SIM 卡的卡号进行认证的 ESAM 芯片，对获取到的 SIM 卡的卡号进行认证包括：

根据用于标识 ESAM 芯片的 ESAM 标识 ID 以及与 ESAM 芯片绑定的 SIM 卡的卡号的绑定关系，对读取到的 SIM 卡的卡号进行认证。

其中，根据用于标识 ESAM 芯片的 ESAM 标识 ID，以及与 ESAM 芯片绑定的 SIM 卡的卡号的绑定关系，对读取到的所述 SIM 卡的卡号进行认证包括：

S1，根据获取到的 SIM 卡的卡号、ESAM 芯片中存储的 ESAM ID，以及用于加密的密钥进行计算得到密文。

S2，比较计算得到的密文与预定密文是否相同；其中，所述预定密文包括：在所述 ESAM 芯片中，根据所述绑定关系中预先存储的 SIM 卡的卡号、所述 ESAM ID 以及所述密钥计算得到的密文。

S3，在比对结果为计算得到的密文与预定密文相同时，确定对 SIM 卡的卡号认证成功；以及在比对结果为计算得到的密文与预定密文不相同时，确定对 SIM 卡的卡号认证失败

可选地，存储介质还被设置为存储用于执行以下步骤的程序代码：

根据获取到的 SIM 卡的卡号、ESAM 芯片中存储的 ESAM ID，以及用于加密的密钥进行计算得到密文包括：

S1，生成用于计算密文的随机数。

S2，采用生成的随机数，根据获取到的 SIM 卡的卡号、ESAM 芯片中存储的 ESAM ID，以及用于加密的密钥进行计算得到密文。

可选地，存储介质还被设置为存储用于执行以下步骤的程序代码：在采用用于对 SIM 卡的卡号进行认证的嵌入式安全模块 ESAM 芯片，对获取到的 SIM 卡的卡号进行认证之后，在对所述 SIM 卡的卡号认证失败时，控制所述终端进行销毁操作。

其中，在对 SIM 卡的卡号认证失败时，控制终端进行销毁操作，包括：

S1，向终端的基带处理器发送通知消息，其中，通知消息用于通知基带处理器对终端的软件进行销毁。

S2，在接收到基带处理器返回的、用于指示终端的软件销毁完成的指示消息后，断开与终端的SIM卡电路以及与终端的基带处理器的通信路径。

可选地，在本实施例中，上述存储介质可以包括但不限于：U盘、只读存储器（ROM，Read-Only Memory）、随机存取存储器（RAM，Random Access Memory）、移动硬盘、磁碟或者光盘等各种可以存储程序代码的介质。

可选地，在本实施例中，处理器根据存储介质中已存储的程序代码执行：获取插入终端的SIM卡的卡号；采用用于对SIM卡的卡号进行认证的嵌入式安全模块ESAM芯片，对获取到的SIM卡的卡号进行认证。

可选地，在本实施例中，处理器根据存储介质中已存储的程序代码执行：采用用于对SIM卡的卡号进行认证的ESAM芯片，对获取到的SIM卡的卡号进行认证包括：根据用于标识ESAM芯片的ESAM ID以及与ESAM芯片绑定的SIM卡的卡号的绑定关系，对获取到的SIM卡的卡号进行认证，包括：根据获取到的SIM卡的卡号、ESAM芯片中存储的ESAM ID，以及用于加密的密钥进行计算得到密文；比较计算得到的密文与ESAM芯片中根据绑定关系中预先存储的SIM卡的卡号、ESAM ID以及密钥计算得到的预定密文是否相同；在比对结果为计算得到的密文与预定密文为相同的情况下，确定对SIM卡的卡号认证成功；和/或在比对结果为计算得到的密文与预定密文为不相同的情况下，确定对SIM卡的卡号认证失败。

可选地，在本实施例中，处理器根据存储介质中已存储的程序代码执行：根据获取到的SIM卡的卡号、ESAM芯片中存储的ESAM ID，以及用于加密的密钥进行计算得到密文包括：生成用于计算密文的随机数；采用生成的随机数，根据获取到的SIM卡的卡号、ESAM芯片中存储的ESAM ID，以及用于加密的密钥进行计算得到密文。

可选地，在本实施例中，处理器根据存储介质中已存储的程序代码执行：在采用用于对SIM卡的卡号进行认证的嵌入式安全模块ESAM芯片，对获取到的SIM卡的卡号进行认证之后，还包括：控制终端进行销毁操作，包括：向终端的基带处理器发送通知消息，其中，通知消息用于通知基带处理

器对终端的软件进行销毁；在接收到基带处理器返回的、用于指示终端的软件销毁完成的指示消息后，断开与终端的 SIM 卡电路以及与终端的基带处理器的通信路径。

可选地，本实施例中的示例可以参考上述实施例及可选实施方式中所描述的示例，本实施例在此不再赘述。

本领域普通技术人员可以理解上述实施例的全部或部分步骤可以使用计算机程序流程来实现，所述计算机程序可以存储于一计算机可读存储介质中，所述计算机程序在相应的硬件平台上（如系统、设备、装置、器件等）执行，在执行时，包括方法实施例的步骤之一或其组合。

可选地，上述实施例的全部或部分步骤也可以使用集成电路来实现，这些步骤可以被分别制作成一个个集成电路模块，或者将它们中的多个模块或步骤制作成单个集成电路模块来实现。

上述实施例中的装置/功能模块/功能单元可以采用通用的计算装置来实现，它们可以集中在单个的计算装置上，也可以分布在多个计算装置所组成的网络上。

上述实施例中的装置/功能模块/功能单元以软件功能模块的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。上述提到的计算机可读取存储介质可以是只读存储器，磁盘或光盘等。

工业实用性

通过本发明实施例方案，在终端的 SIM 卡电路和基带处理器之间设置一个 ESAM 芯片，通过 ESAM 芯片对终端接入的 SIM 卡的卡号进行认证，由于 ESAM 芯片具有安全性高，不易被破解的优点，因此，可以解决在相关技术中，通过软件算法的方式对 SIM 卡进行鉴权，无法保证鉴权的安全性和可靠性的问题，达到提高 SIM 卡鉴权的安全性和可靠性的效果。

权 利 要 求 书

1.一种终端，包括客户识别模块SIM卡电路，基带处理器，和嵌入式安全模块ESAM芯片；

所述SIM卡电路，设置为检测到有SIM卡插入时，读取插入终端的所述SIM卡的卡号；

所述ESAM芯片，连接至所述SIM卡电路和所述基带处理器，设置为对读取到的所述SIM卡的卡号进行认证。

2.根据权利要求1所述的终端，其中，所述ESAM芯片对读取到的所述SIM卡的卡号进行认证包括：根据用于标识ESAM芯片的ESAM标识ID，以及与ESAM芯片绑定的SIM卡的卡号的绑定关系，对读取到的所述SIM卡的卡号进行认证；

其中，根据用于标识ESAM芯片的ESAM 标识ID，以及与ESAM芯片绑定的SIM卡的卡号的绑定关系，对读取到的所述SIM卡的卡号进行认证包括：

根据获取到的所述SIM卡的卡号、所述ESAM芯片中存储的所述ESAM ID以及用于加密的密钥进行计算得到密文；

比较计算得到的密文与预定密文是否相同；其中，所述预定密文包括：在所述ESAM芯片中，根据所述绑定关系中预先存储的SIM卡的卡号、所述ESAM ID以及所述密钥计算得到的密文；

在比对结果为计算得到的密文与所述预定密文相同时，确定对所述SIM卡的卡号认证成功；以及在比对结果为计算得到的密文与所述预定密文不相同时，确定对所述SIM卡的卡号认证失败。

3.根据权利要求2所述的终端，其中，所述ESAM芯片根据获取到的所述SIM卡的卡号、所述ESAM芯片中存储的所述ESAM ID以及用于加密的密钥进行计算得到密文包括：

生成用于计算所述密文的随机数；

采用生成的所述随机数，根据获取到的所述SIM卡的卡号、所述ESAM芯片中存储的所述ESAM ID，以及用于加密的密钥进行计算得到密文。

4.根据权利要求 1 所述的终端，所述终端还包括：基带处理器；

所述基带处理器，设置为在所述 ESAM 芯片对读取到的所述 SIM 卡的卡号进行认证之后，根据所述 ESAM 芯片发送的用于通知所述基带处理器对所述终端的软件进行销毁的通知，进行所述终端的软件的销毁。

5.根据权利要求 1 至 3 中任一项所述的终端，

所述 ESAM 芯片，还设置为通知所述基带处理器进行所述终端的软件的销毁，并在接收到所述基带处理器返回的、用于指示所述终端的软件销毁完成的指示消息后，断开与所述 SIM 卡电路以及与所述基带处理器的通信路径。

6.一种客户识别模块 SIM 卡处理方法，该方法包括：

检测到有 SIM 卡插入时，读取插入终端的 SIM 卡的卡号；

采用用于对 SIM 卡的卡号进行认证的嵌入式安全模块 ESAM 芯片，对读取到的所述 SIM 卡的卡号进行认证。

7.根据权利要求 6 所述的 SIM 卡处理方法，其中，所述采用用于对 SIM 卡的卡号进行认证的 ESAM 芯片，对获取到的所述 SIM 卡的卡号进行认证包括：

根据用于标识 ESAM 芯片的 ESAM 标识 ID，以及与 ESAM 芯片绑定的 SIM 卡的卡号的绑定关系，对读取到的所述 SIM 卡的卡号进行认证；

其中，根据用于标识 ESAM 芯片的 ESAM 标识 ID，以及与 ESAM 芯片绑定的 SIM 卡的卡号的绑定关系，对读取到的所述 SIM 卡的卡号进行认证包括：

根据获取到的所述 SIM 卡的卡号、所述 ESAM 芯片中存储的所述 ESAM ID 以及用于加密的密钥进行计算得到密文；

比较计算得到的密文与预定密文是否相同；其中，所述预定密文包括：在所述 ESAM 芯片中，根据所述绑定关系中预先存储的 SIM 卡的卡号、所述 ESAM ID 以及所述密钥计算得到的密文；

在比对结果为计算得到的密文与所述预定密文相同时，确定对所述 SIM 卡的卡号认证成功；以及在比对结果为计算得到的密文与所述预定密文不相

同时，确定对所述 SIM 卡的卡号认证失败。

8.根据权利要求 7 所述的 SIM 卡处理方法，其中，所述根据获取到的所述 SIM 卡的卡号、所述 ESAM 芯片中存储的所述 ESAM ID 以及用于加密的密钥进行计算得到密文包括:

生成用于计算所述密文的随机数;

采用生成的所述随机数，根据获取到的所述 SIM 卡的卡号、所述 ESAM 芯片中存储的所述 ESAM ID，以及用于加密的密钥进行计算得到密文。

9.根据权利要求 6 所述的 SIM 卡处理方法，所述方法还包括: 在采用用于对 SIM 卡的卡号进行认证的嵌入式安全模块 ESAM 芯片，对获取到的所述 SIM 卡的卡号进行认证之后，在对所述 SIM 卡的卡号认证失败时，控制所述终端进行销毁操作; 其中，在对所述 SIM 卡的卡号认证失败时，控制所述终端进行销毁操作包括:

向所述终端的基带处理器发送通知消息，其中，所述通知消息用于通知所述基带处理器对所述终端的软件进行销毁;

在接收到所述基带处理器返回的、用于指示所述终端的软件销毁完成的指示消息后，断开与所述终端的 SIM 卡电路以及与所述终端的基带处理器的通信路径。

10.一种客户识别模块 SIM 卡处理装置，包括:

获取模块，设置为检测到有 SIM 卡插入时，读取插入终端的 SIM 卡的卡号;

认证模块，设置为采用用于对 SIM 卡的卡号进行认证的嵌入式安全模块 ESAM 芯片，对读取到的所述 SIM 卡的卡号进行认证。

11.根据权利要求 10 所述的 SIM 卡处理装置，其中，所述认证模块采用用于对 SIM 卡的卡号进行认证的 ESAM 芯片，对获取到的所述 SIM 卡的卡号进行认证包括: 根据用于标识 ESAM 芯片的 ESAM 标识 ID 以及与 ESAM 芯片绑定的 SIM 卡的卡号的绑定关系，对获取到的所述 SIM 卡的卡号进行认证;

其中，所述认证模块包括: 计算单元、比对单元和确定单元;

所述认证模块根据用于标识 ESAM 芯片的 ESAM 标识 ID，以及与 ESAM 芯片绑定的 SIM 卡的卡号的绑定关系，对读取到的所述 SIM 卡的卡号进行认证包括:

所述计算单元，设置为根据获取到的所述 SIM 卡的卡号、所述 ESAM 芯片中存储的所述 ESAM ID 以及用于加密的密钥进行计算得到密文;

所述比对单元，设置为比较计算得到的密文与预定密文是否相同;其中，所述预定密文包括：在所述 ESAM 芯片中，根据所述绑定关系中预先存储的 SIM 卡的卡号、所述 ESAM ID 以及所述密钥计算得到的密文;

所述确定单元，设置为在比对结果为计算得到的密文与所述预定密文相同时，确定对所述 SIM 卡的卡号认证成功;以及在比对结果为计算得到的密文与所述预定密文不相同时，确定对所述 SIM 卡的卡号认证失败。

12.根据权利要求 11 所述的 SIM 卡处理装置，其中，所述计算单元包括:

生成子单元，设置为生成用于计算所述密文的随机数;

计算子单元，设置为采用生成的所述随机数，根据获取到的所述 SIM 卡的卡号、所述 ESAM 芯片中存储的所述 ESAM ID，以及用于加密的密钥进行计算得到密文。

13.根据权利要求 10 所述的 SIM 卡处理装置，所述装置还包括：控制模块;

所述控制模块，设置为在认证模块对获取到的所述 SIM 卡的卡号进行认证之后，在对所述 SIM 卡的卡号认证失败时，控制所述终端进行销毁操作;

所述控制模块包括：通知单元和断开单元;

其中，所述控制模块在对所述 SIM 卡的卡号认证失败时，控制所述终端进行销毁操作包括:

所述通知单元，设置为向所述终端的基带处理器发送通知消息，其中，所述通知消息用于通知所述基带处理器对所述终端的软件进行销毁;

所述断开单元，设置为在接收到所述基带处理器返回的、用于指示所述终端的软件的销毁完成的指示消息后，断开与所述终端的 SIM 卡电路以及

与所述终端的基带处理器的通信路径。

14. 一种嵌入式安全模块 ESAM 芯片，包括权利要求 10 至 13 中任意一项所述的 SIM 卡处理装置。

15、一种计算机可读存储介质，存储有计算机可执行指令，所述计算机可执行指令被处理器执行时实现权利要求 6 至 9 任意一项所述的客户识别模块 SIM 卡处理方法。

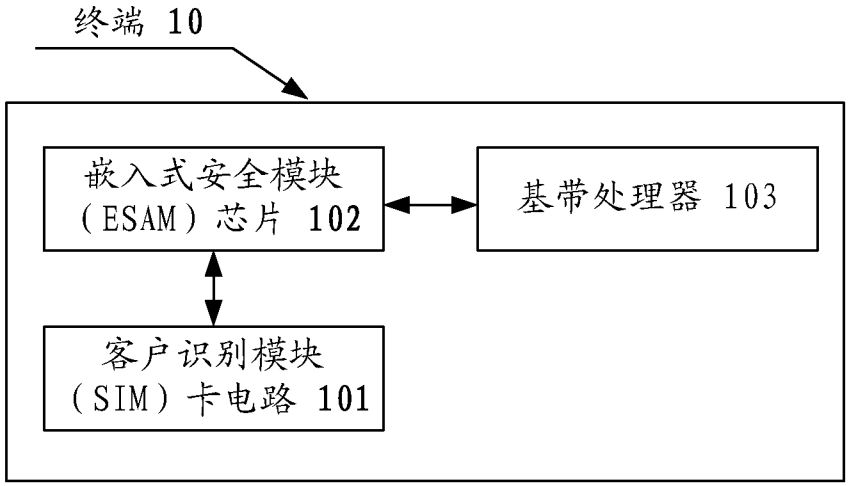
终端 10
嵌入式安全模块（ESAM）芯片 102
基带处理器 103
客户识别模块（SIM）卡电路 101

图 1

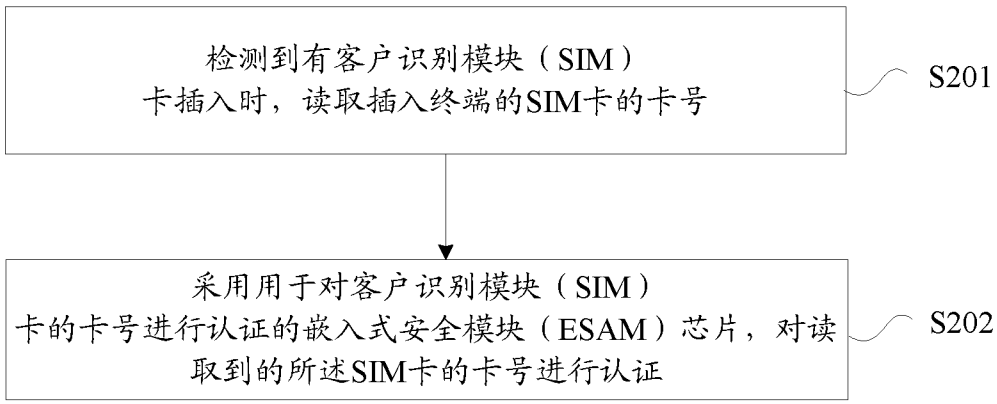
检测到有客户识别模块（SIM）卡插入时，读取插入终端的SIM卡的卡号
S201
采用用于对客户识别模块（SIM）卡的卡号进行认证的嵌入式安全模块（ESAM）芯片，对读取到的所述SIM卡的卡号进行认证
S202

图 2

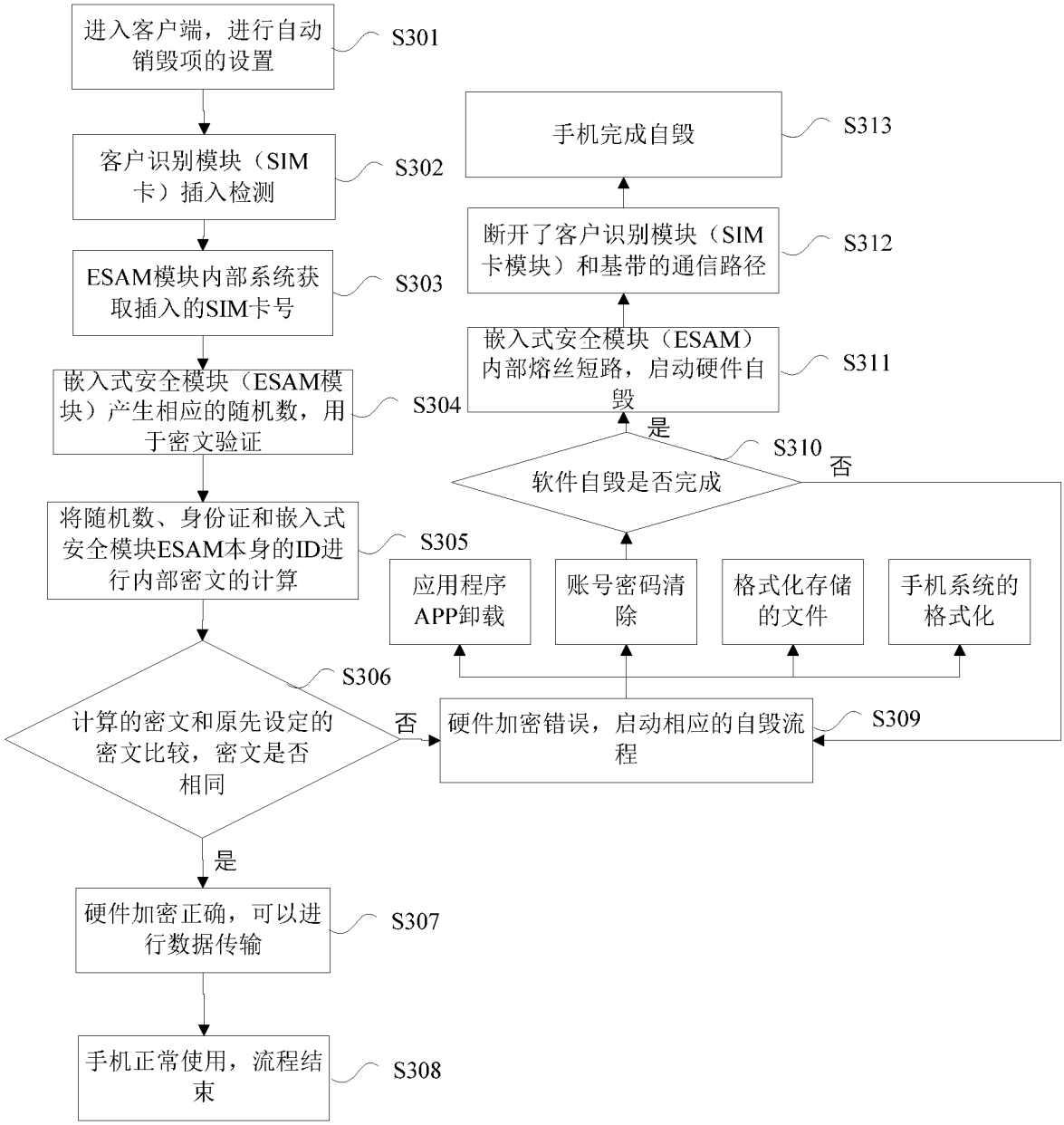
进入客户端，进行自动销毁项的设置
S301
客户识别模块（SIM卡）插入检测
S302
ESAM模块内部系统获取插入的SIM卡号
S303
嵌入式安全模块（ESAM模块）产生相应的随机数，用于密文验证
S304
将随机数、身份证和嵌入式安全模块ESAM本身的ID进行内部密文的计算
S305
计算的密文和原先设定的密文比较，密文是否相同
S306
否
是
硬件加密正确，可以进行数据传输
S307
手机正常使用，流程结束
S308
硬件加密错误，启动相应的自毁流程
S309
应用程序APP卸载
账号密码清除
格式化存储的文件
手机系统的格式化
软件自毁是否完成
S310
否
是
嵌入式安全模块（ESAM）内部熔丝短路，启动硬件自毁
S311
断开了客户识别模块（SIM卡模块）和基带的通信路径
S312
手机完成自毁
S313

图 3

图 4

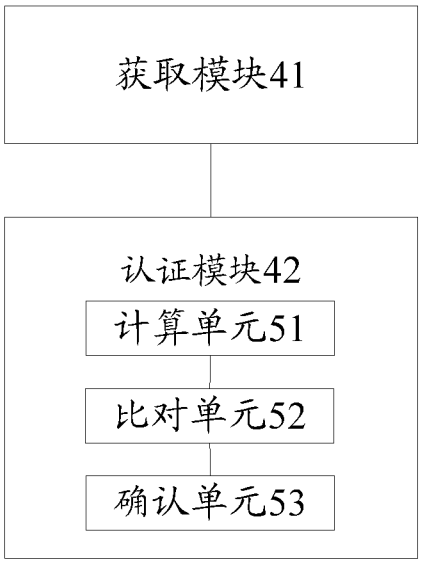

图 5

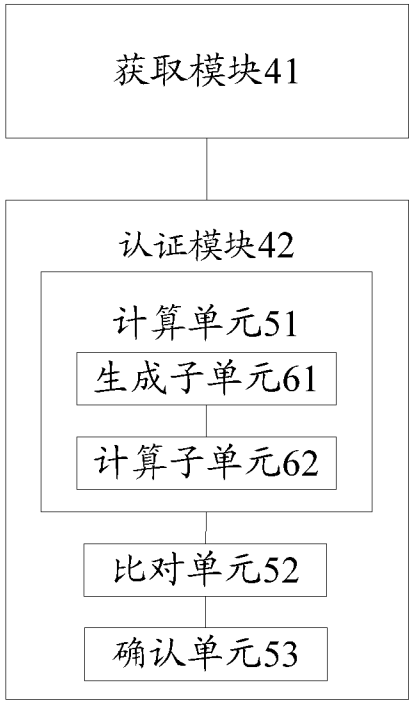
获取模块41
认证模块42
计算单元51
生成子单元61
计算子单元62
比对单元52
确认单元53

图 6


获取模块41
认证模块42
控制模块43
通知单元71
断开单元72

图 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/085725

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/04 (2009.01) i; H04W 12/06 (2009.01) i; H04W 88/02 (2009.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W; H04Q; H04L; G07B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNKI, CNPAT, EPODOC, WPI: subscriber identity card, embedded security chip, phone card, ESAM chip, card number, identification, serial number, random number, IMSI, ID, embedded secure access module, subscriber identity module, SIM card, authentication, CPU card, random

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 101521886 A (WATCHDATA SYSTEM CO., LTD. et al.), 02 September 2009 (02.09.2009), description, page 7, line 20 to page 9, line 12	1, 4-6, 9, 10, 13-15
X	CN 101605328 A (XIAMEN STELCOM INFORMATION & TECHNOLOGY CO., LTD.), 16 December 2009 (16.12.2009), description, page 2, lines 5-20	1, 4-6, 9, 10, 13-15
X	CN 101511083 A (WATCHDATA SYSTEM CO., LTD.), 19 August 2009 (19.08.2009), description, page 7, line 7 to page 8, line 7	1, 4-6, 9, 10, 13-15
A	CN 102104864 A (ZTE CORP.), 22 June 2011 (22.06.2011), the whole document	1-15
A	CN 102377566 A (RT. HITECH (BEIJING) CO., LTD.), 14 March 2012 (14.03.2012), the whole document	1-15
A	CN 103258354 A (WUXI CHANGDA INFORMATION TECHNOLOGY CO., LTD.), 21 August 2013 (21.08.2013), the whole document	1-15

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 November 2016 (23.11.2016)	**04 February 2017 (04.02.2017)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **XING, Zhaoxia** Telephone No.: (86-10) **010-62413304**

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/085725

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101521886 A	02 September 2009	None	
CN 101605328 A	16 December 2009	None	
CN 101511083 A	19 August 2009	None	
CN 102104864 A	22 June 2011	WO 2010148779 A1	29 December 2010
CN 102377566 A	14 March 2012	None	
CN 103258354 A	21 August 2013	None	

国际检索报告

国际申请号
PCT/CN2016/085725

A. 主题的分类

H04W 12/04(2009.01)i; H04W 12/06(2009.01)i; H04W 88/02(2009.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04W; H04Q; H04L; G07B

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNKI,CNPAT,EPODOC,WPI:用户识别卡，嵌入式安全芯片，SIM卡，CPU卡，电话卡，ESAM芯片，认证，鉴权，卡号，标识，序列号，随机数，IMSI,ID,embedded secure access module，subscriber identity module，SIM card，authentication，CPU card，random

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	CN 101521886 A (北京握奇数据系统有限公司等) 2009年 9月 2日 (2009-09-02) 说明书第7页第20行-第9页第12行	1、4-6、9、10、13-15
X	CN 101605328 A (厦门敏讯信息技术股份有限公司) 2009年 12月 16日 (2009-12-16) 说明书第2页第5-20行	1、4-6、9、10、13-15
X	CN 101511083 A (北京握奇数据系统有限公司) 2009年 8月 19日 (2009-08-19) 说明书第7页第7行-第8页第7行	1、4-6、9、10、13-15
A	CN 102104864 A (中兴通讯股份有限公司) 2011年 6月 22日 (2011-06-22) 全文	1-15
A	CN 102377566 A (北京融通高科科技发展有限公司) 2012年 3月 14日 (2012-03-14) 全文	1-15
A	CN 103258354 A (无锡昶达信息技术有限公司) 2013年 8月 21日 (2013-08-21) 全文	1-15

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2016年 11月 23日	2017年 2月 4日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 行朝霞 电话号码 (86-10)010-62413304

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/085725

检索报告引用的专利文件	公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN 101521886 A	2009年 9月 2日	无	
CN 101605328 A	2009年 12月 16日	无	
CN 101511083 A	2009年 8月 19日	无	
CN 102104864 A	2011年 6月 22日	WO 2010148779 A1	2010年 12月 29日
CN 102377566 A	2012年 3月 14日	无	
CN 103258354 A	2013年 8月 21日	无	