(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
2013 年 5 月 10 日 (10.05.2013)

WIPO | PCT

(10) 国际公布号
WO 2013/064063 A1

(51) 国际专利分类号:
H04L 12/26 (2006.01)

(21) 国际申请号: PCT/CN2012/083805

(22) 国际申请日: 2012 年 10 月 31 日 (31.10.2012)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201110341828.X 2011 年 11 月 2 日 (02.11.2011) CN

(71) 申请人: **中国银联股份有限公司 (CHINA UNIONPAY CO., LTD.)** [CN/CN]; 中国上海市浦东新区含笑路 36 号银联大厦, Shanghai 200135 (CN)。

(72) 发明人: **陆辉 (LU, Hui)**; 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 **吴金坛 (WU, Jintan)**; 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 **吕苏 (LV, Su)**; 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 **尹祥龙 (YIN, Xianglong)**; 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 **许丹 (XU, Dan)**; 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。

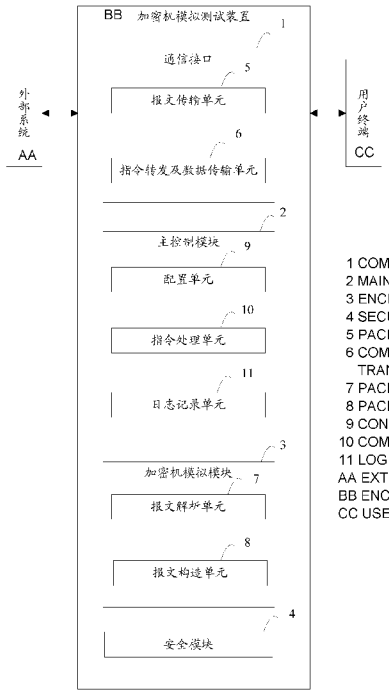
(74) 代理人: **中国专利代理（香港）有限公司 (CHINA PATENT AGENT (HK) LTD.)**; 中国香港特别行政区湾仔港湾道 23 号鹰君中心 22 字楼, Hong Kong (CN)。

(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, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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, 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。

[见续页]

(54) **Title**: ENCRYPTOR SIMULATION TEST DEVICE AND METHOD

(54) **发明名称** : 加密机模拟测试装置及方法



1 COMMUNICATION INTERFACE
2 MAIN CONTROL MODULE
3 ENCRYPTOR SIMULATION MODULE
4 SECURITY MODULE
5 PACKET TRANSMISSION UNIT
6 COMMAND FORWARDING AND DATA TRANSMISSION UNIT
7 PACKET PARSING UNIT
8 PACKET CONSTRUCTION UNIT
9 CONFIGURATION UNIT
10 COMMAND PROCESSING UNIT
11 LOG RECORDING UNIT
AA EXTERNAL SYSTEM
BB ENCRYPTOR SIMULATION TEST DEVICE
CC USER TERMINAL

图 1 / FIG. 1

(57) **Abstract**: Provided are an encryptor simulation test device and method, the encryptor simulation test device comprising a communication interface, an encryptor simulation module, a security module and a main control module; the encryptor simulation module parses the received request packet, transmits the parsed packet data to the security module, constructs a response packet based on the security processing result data from the security module, and transmits the response packet to an external system via the communication interface. The encryptor simulation test device and method of the present invention are flexible to configure and have a high analytical precision.

(57) **摘要**: 本发明提出了一种加密机模拟测试装置及方法，所述加密机模拟测试装置包括：通信接口、加密机模拟模块、安全模块和主控制模块。其中，所述加密机模拟模块用于解析接收到的请求报文，并将解析出的报文数据传送到安全模块，以及基于来自所述安全模块的安全处理结果数据构造应答报文，并将所述应答报文经所述通信接口传送到外部系统。本发明所公开的加密机模拟测试装置及方法配置灵活且具有高的分析精确度。

WO 2013/064063 A1

(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, 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, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

加密机模拟测试装置及方法

技术领域

本发明涉及模拟测试装置及方法，更具体地，涉及加密机模拟测试装置及方法。

背景技术

目前，随着数据应用的日益广泛以及不同领域（例如金融领域）的业务种类的日益丰富，使用加密机（特别是硬件加密机）以完成安全性信息（即对安全性要求较高的信息）的交互日益普遍，因而，针对加密机（特别是硬件加密机）的测试系统及方法变得越来越重要。

现有的加密机（特别是硬件加密机）测试装置及方法通常将测试终端连接到真实的加密机上，进而实施相关测试。

然而，上述现有的方案具有如下问题：（1）无法自由模拟各种加密机的输出（即真实的加密机通常只能输出正确处理的结果，但在测试过程中，往往需要测试系统对错误结果是否正确处理）；（2）由于加密机种类繁多且调试设置步骤通常并不相同，故针对不同的加密机需要掌握不同的操作方法，从而导致使用不便且成本增加；（3）从安全角度出发，常规的加密机通常被集成在机箱内，并且除通信接口外不提供其他交互通道，因而在常规测试中，虽然测试人员可以通过解析通信日志和/或应用日志来分析测试过程中产生的问题，但是如果遇到加密机返回错误，则通常难于仅根据加密机的错误应答码来较准确地定位所述问题（即难于模拟错误结果的输出）。

因此，存在如下需求：提供一种配置灵活且具有高的分析精确度的加密机模拟测试装置及方法。

发明内容

为了解决上述现有技术方案所存在的问题，本发明提出了一种加密机模拟测试装置及方法。

本发明的目的是通过以下技术方案实现的：

一种加密机模拟测试装置，所述加密机模拟测试装置包括:

通信接口，所述通信接口用于以预定的通信格式接收来自外部系统的请求报文，并将所述请求报文传送到加密机模拟模块，以及将来自所述加密机模拟模块的应答报文以所述预定的通信格式传送回所述外部系统;

加密机模拟模块，所述加密机模拟模块用于解析接收到的所述请求报文，并将解析出的报文数据传送到安全模块，以及基于来自所述安全模块的安全处理结果数据构造应答报文，并将所述应答报文传送到所述通信接口;

安全模块，所述安全模块用于处理所述解析出的报文数据以获得所述安全处理结果数据，并将所述安全处理结果数据传送回所述加密机模拟模块;

主控制模块，所述主控制模块用于在所述加密机模拟测试装置启动时基于预定的配置文件初始化所述加密机模拟测试装置，以及监控与数据处理过程相关的信息并维护日志文件。

在上面所公开的方案中，优选地，所述通信接口进一步用于接收来自用户终端的控制指令，并将所述控制指令传送到所述主控制模块。

在上面所公开的方案中，优选地，所述主控制模块进一步用于执行接收到的所述控制指令，并将执行结果经所述通信接口传送回所述用户终端。

在上面所公开的方案中，优选地，所述通信接口进一步包括报文传输单元，其中，所述报文传输单元用于基于所述预定的通信格式从所述请求报文中提取出报文体，并将所述报文体传送到所述加密机模拟模块，以及将接收到的所述应答报文以所述预定的通信格式传送到所述外部系统。

在上面所公开的方案中，优选地，所述通信接口进一步包括指令转发及数据传输单元。所述指令转发及数据传输单元用于接收来自所述用户终端的控制指令，并将所述控制指令传送到所述主控制模块，以及将来自所述主控制模块的执行结果传送到所述用户终端。

在上面所公开的方案中，优选地，所述执行结果包括执行结果状态指示和/或执行结果数据。

在上面所公开的方案中，优选地，所述加密机模拟模块进一步包括:

报文解析单元，所述报文解析单元用于基于预定参数解析接收到的所述请求报文，并将解析出的报文数据传送到所述安全模块;

报文构造单元，所述报文构造单元用于基于预定参数和接收到的所述安全处理结果数据构造所述应答报文，并将所述应答报文传送到所述通信接口。

在上面所公开的方案中，优选地，所述预定参数包括密钥参数和/或异常模拟控制参数。

在上面所公开的方案中，优选地，所述解析出的报文数据包括指令码、密钥和安全数据。

在上面所公开的方案中，优选地，所述控制指令包括配置指令和/或日志指令。

在上面所公开的方案中，优选地，所述主控制模块进一步包括:

配置单元，所述配置单元用于在所述加密机模拟测试装置启动时基于预定的配置文件初始化所述加密机模拟测试装置;

日志记录单元，所述日志记录单元用于监控与数据处理过程相关的信息并将所述与数据处理过程相关的信息记录在所述日志文件中。

在上面所公开的方案中，优选地，所述主控制模块进一步包括指令处理单元，所述指令处理单元用于基于接收到的所述配置指令更新和/或重新读取所述配置文件，以及基于接收到的所述日志指令将统计信息输出到所述日志文件。

在上面所公开的方案中，优选地，所述安全模块进一步用于基于所述解析出的报文数据，根据所述指令码使用所述密钥对所述安全数据进行处理，以获得所述安全处理结果数据。

在上面所公开的方案中，优选地，所述预定的通信格式是以下通信格式之一:（a）由报文长度字段、报文头字段和报文体字段构成报文通信接口；（b）由报文长度字段、报文体字段构成报文通信接口；（c）仅由报文体字段构成报文通信接口（即无报文长度字段和报文头字段）。

在上面所公开的方案中，优选地，所述配置单元基于所述配置文件配置所述预定的通信格式。

在上面所公开的方案中，优选地，所述配置单元基于所述配置文件配置所述预定参数。

在上面所公开的方案中，优选地，所述配置文件包括环境变量、日志路径、

日志级别标志以及线程数目中的至少一个。

在上面所公开的方案中，优选地，所述日志文件包括用于记录通信报文的通信日志和用于记录处理过程中的异常情况信息的应用日志。

在上面所公开的方案中，优选地，所述指令处理单元还用于基于所述控制指令而将所述日志文件经所述通信接口传送到所述用户终端。

在上面所公开的方案中，优选地，所述配置单元基于所述配置文件配置所述安全模块使用的安全加密算法。

在上面所公开的方案中，优选地，所述加密机模拟模块进一步用于为多个加密机接口规范中的每个定义动态链接库，所述动态链接库中的每个用于以对应的所述加密机接口规范解析所述请求报文以及构造所述应答报文。

在上面所公开的方案中，优选地，所述加密机模拟模块进一步用于基于所述配置文件加载所述动态链接库中的一个作为工作动态链接库，从而以所述工作动态链接库所对应的加密机接口规范解析所述请求报文以及构造所述应答报文。

本发明的目的也可以通过以下技术方案实现：

一种加密机模拟测试方法，所述加密机模拟测试方法包括以下步骤：

（A1）以预定的通信格式接收来自外部系统的请求报文；

（A2）解析接收到的所述请求报文以获得解析出的报文数据；

（A3）处理所述解析出的报文数据以获得安全处理结果数据；

（A4）基于所述安全处理结果数据构造应答报文；

（A5）将所述应答报文以所述预定的通信格式传送回所述外部系统。

在上面所公开的方案中，优选地，所述方法进一步包括：接收并执行来自用户终端的控制指令，并将执行结果传送回所述用户终端。

在上面所公开的方案中，优选地，所述步骤（A1）进一步包括：基于所述预定的通信格式从所述请求报文中提取出报文体。

在上面所公开的方案中，优选地，所述执行结果包括执行结果状态指示和/或执行结果数据。

在上面所公开的方案中，优选地，所述步骤（A2）进一步包括：基于预定参数解析接收到的所述请求报文。

在上面所公开的方案中，优选地，所述预定参数包括密钥参数和/或异常模拟控制参数。

在上面所公开的方案中，优选地，所述解析出的报文数据包括指令码、密钥和安全数据。

在上面所公开的方案中，优选地，所述控制指令包括配置指令和/或日志指令。

在上面所公开的方案中，优选地，所述方法进一步包括：基于预定的配置文件执行初始化操作。

在上面所公开的方案中，优选地，所述方法进一步包括：监控与数据处理过程相关的信息并将所述与数据处理过程相关的信息记录在日志文件中。

在上面所公开的方案中，优选地，所述方法进一步包括：基于接收到的所述配置指令更新和/或重新读取所述配置文件，以及基于接收到的所述日志指令将统计信息输出到所述日志文件。

在上面所公开的方案中，优选地，所述步骤（A3）进一步包括：基于所述解析出的报文数据，根据所述指令码使用所述密钥对所述安全数据进行处理，以获得所述安全处理结果数据。

在上面所公开的方案中，优选地，所述步骤（A4）进一步包括：基于预定参数和所述安全处理结果数据构造所述应答报文。

在上面所公开的方案中，优选地，所述预定的通信格式是以下通信格式之一：（a）由报文长度字段、报文头字段和报文体字段构成报文通信接口；（b）由报文长度字段、报文体字段构成报文通信接口；（c）仅由报文体字段构成报文通信接口（即无报文长度字段和报文头字段）。

在上面所公开的方案中，优选地，所述方法进一步包括：基于所述配置文件配置所述预定的通信格式。

在上面所公开的方案中，优选地，所述方法进一步包括：基于所述配置文件配置所述预定参数。

在上面所公开的方案中，优选地，所述配置文件包括环境变量、日志路径、日志级别标志以及线程数目中的至少一个。

在上面所公开的方案中，优选地，所述日志文件包括用于记录通信报文的

通信日志和用于记录处理过程中的异常情况信息的应用日志。

在上面所公开的方案中，优选地，所述方法进一步包括：基于所述控制指令而将所述日志文件传送到所述用户终端。

在上面所公开的方案中，优选地，所述方法进一步包括：基于所述配置文件配置所使用的安全加密算法。

在上面所公开的方案中，优选地，所述方法进一步包括：为多个加密机接口规范中的每个定义动态链接库，所述动态链接库中的每个用于以对应的所述加密机接口规范解析所述请求报文以及构造所述应答报文。

在上面所公开的方案中，优选地，所述方法进一步包括：基于所述配置文件加载所述动态链接库中的一个作为工作动态链接库，从而以所述工作动态链接库所对应的加密机接口规范解析所述请求报文以及构造所述应答报文。

本发明所公开的加密机模拟测试装置及方法具有如下优点：（1）支持 3 种常用的加密机通讯接口规范，并可灵活配置；（2）支持多种安全加密算法，并可根据需求自由配置安全处理结果；（3）实时记录通信日志及应用日志，从而具有高的分析精确度；（4）具有高的数据处理性能。综上所述，相对于使用真实的加密机进行测试，本发明所公开的加密机模拟测试装置及方法可以更自由模拟加密机的各种行为。

附图说明

结合附图，本发明的技术特征以及优点将会被本领域技术人员更好地理解，其中：

图1为根据本发明的实施例的加密机模拟测试装置的结构图；

图2为根据本发明的实施例的加密机模拟测试方法的流程图。

具体实施方式

图1是根据本发明的实施例的加密机模拟测试装置的结构图。如图1所示，本发明所公开的加密机模拟测试装置包括通信接口1、主控制模块2、加密机模拟模块3和安全模块4。其中，所述通信接口1用于以预定的通信格式接收来自外部系统的请求报文，并将所述请求报文传送到所述加密机模拟模块3，以及

将来自所述加密机模拟模块3的应答报文以所述预定的通信格式传送回所述外部系统。所述加密机模拟模块3用于解析接收到的所述请求报文，并将解析出的报文数据传送到所述安全模块4，以及基于来自所述安全模块4的安全处理结果数据构造应答报文，并将所述应答报文传送到所述通信接口1。所述安全模块4用于处理所述解析出的报文数据以获得所述安全处理结果数据，并将所述安全处理结果数据传送回所述加密机模拟模块3。所述主控制模块2用于在所述加密机模拟测试装置启动时基于预定的配置文件初始化所述加密机模拟测试装置，以及监控与数据处理过程相关的信息并维护日志文件。

优选地，在本发明所公开的加密机模拟测试装置中，所述通信接口1进一步用于接收来自用户终端的控制指令，并将所述控制指令传送到所述主控制模块2。

优选地，在本发明所公开的加密机模拟测试装置中，所述主控制模块2进一步用于执行接收到的所述控制指令，并将执行结果经所述通信接口1传送回所述用户终端。

优选地，在本发明所公开的加密机模拟测试装置中，所述通信接口1进一步包括报文传输单元5。其中，所述报文传输单元5用于基于所述预定的通信格式从所述请求报文中提取出报文体，并将所述报文体传送到所述加密机模拟模块3，以及将接收到的所述应答报文以所述预定的通信格式传送到所述外部系统。

优选地，在本发明所公开的加密机模拟测试装置中，所述通信接口1进一步包括指令转发及数据传输单元6。所述指令转发及数据传输单元6用于接收来自所述用户终端的控制指令，并将所述控制指令传送到所述主控制模块2，以及将来自所述主控制模块2的执行结果传送到所述用户终端。示例性地，所述执行结果包括执行结果状态指示（即执行成功或执行失败）和/或执行结果数据。

优选地，在本发明所公开的加密机模拟测试装置中，所述加密机模拟模块3进一步包括报文解析单元7和报文构造单元8。其中，所述报文解析单元7用于基于预定参数解析接收到的所述请求报文，并将解析出的报文数据传送到所述安全模块4。所述报文构造单元8用于基于预定参数和接收到的所述安全处理结

果数据构造所述应答报文，并将所述应答报文传送到所述通信接口1。

示例性地，在本发明所公开的加密机模拟测试装置中，所述预定参数包括密钥参数和/或异常模拟控制参数。

示例性地，在本发明所公开的加密机模拟测试装置中，所述解析出的报文数据包括指令码、密钥和安全数据（即加解密数据）。

示例性地，在本发明所公开的加密机模拟测试装置中，所述控制指令包括配置指令和/或日志指令。

优选地，在本发明所公开的加密机模拟测试装置中，所述主控制模块2进一步包括配置单元9和日志记录单元11。其中，所述配置单元9用于在所述加密机模拟测试装置启动时基于预定的配置文件初始化所述加密机模拟测试装置（例如基于预定的配置文件初始化所述通信接口1、所述加密机模拟模块3以及所述安全模块4等）。所述日志记录单元11用于监控与数据处理过程相关的信息并将所述与数据处理过程相关的信息记录在所述日志文件中。

优选地，在本发明所公开的加密机模拟测试装置中，所述主控制模块2进一步包括指令处理单元10。所述指令处理单元10用于基于接收到的所述配置指令更新和/或重新读取所述配置文件，以及基于接收到的所述日志指令将统计信息输出到所述日志文件。

优选地，在本发明所公开的加密机模拟测试装置中，所述安全模块4进一步用于基于所述解析出的报文数据，根据所述指令码使用所述密钥对所述安全数据进行处理，以获得所述安全处理结果数据。

优选地，在本发明所公开的加密机模拟测试装置中，所述预定的通信格式是以下通信格式之一：（a）由报文长度字段、报文头字段和报文体字段构成报文通信接口；（b）由报文长度字段、报文体字段构成报文通信接口；（c）仅由报文体字段构成报文通信接口（即无报文长度字段和报文头字段）。

优选地，在本发明所公开的加密机模拟测试装置中，所述配置单元9基于所述配置文件配置所述预定的通信格式。

优选地，在本发明所公开的加密机模拟测试装置中，所述配置单元9基于所述配置文件配置所述预定参数。

示例性地，在本发明所公开的加密机模拟测试装置中，所述配置文件包括

环境变量、日志路径、日志级别标志以及线程数目中的至少一个。

优选地，在本发明所公开的加密机模拟测试装置中，所述日志文件包括用于记录通信报文的通信日志和用于记录处理过程中的异常情况信息的应用日志。

优选地，在本发明所公开的加密机模拟测试装置中，所述指令处理单元10还用于基于所述控制指令而将所述日志文件经所述通信接口1传送到所述用户终端。

优选地，在本发明所公开的加密机模拟测试装置中，所述配置单元9基于所述配置文件配置所述安全模块4使用的安全加密算法。

示例性地，在本发明所公开的加密机模拟测试装置中，所述加密机模拟模块3进一步用于为多个加密机接口规范（例如报文组装格式规范）中的每个定义动态链接库，所述动态链接库中的每个用于以对应的所述加密机接口规范解析所述请求报文以及构造所述应答报文。

示例性地，在本发明所公开的加密机模拟测试装置中，所述加密机模拟模块3进一步用于基于所述配置文件加载所述动态链接库中的一个作为工作动态链接库，从而以所述工作动态链接库所对应的加密机接口规范解析所述请求报文以及构造所述应答报文。

示例性地，在本发明所公开的加密机模拟测试装置中，所述加密机模拟模块3采用了统一的接口函数定义，并且对于每一种加密机接口规范，定义对应的解析的动态链接库，随后根据配置参数，决定具体加载哪一个动态链接库，从而链接采用统一接口的不同功能处理函数，以实现模拟不同种类的加密机（特别是硬件加密机）的处理行为。由上可见，由于采用了统一的公开接口，测试人员可以根据特定的需要，自行实现处理功能，以完成相应的测试，因此具有较高的应用灵活性。

示例性地，在本发明所公开的加密机模拟测试装置的基本工作原理如下：（1）所述通信接口 1 以预定的通信格式接收来自外部系统的请求报文，并将所述请求报文传送到所述加密机模拟模块 3 （例如基于 TCP/IP 协议从 TCP 上读取两字节的长度位数据，并将其转换为报文的长度，随后从 TCP 中提取指令长度的数据，从而将提取出的报文体传送到所述加密机模拟模块 3）；（2）

所述加密机模拟模块 3 解析接收到的所述请求报文，并将解析出的报文数据传送到所述安全模块 4；（3）所述安全模块 4 处理所述解析出的报文数据以获得所述安全处理结果数据，并将所述安全处理结果数据传送回所述加密机模拟模块 3；（4）所述加密机模拟模块 3 基于来自所述安全模块 4 的安全处理结果数据构造应答报文，并将所述应答报文传送到所述通信接口 1；（5）所述通信接口 1 将来自所述加密机模拟模块 3 的应答报文以所述预定的通信格式传送回所述外部系统。

图2为根据本发明的实施例的加密机模拟测试方法的流程图。如图2所示，本发明所公开的加密机模拟测试方法包括如下步骤：（A1）以预定的通信格式接收来自外部系统的请求报文；（A2）解析接收到的所述请求报文以获得解析出的报文数据；（A3）处理所述解析出的报文数据以获得安全处理结果数据；（A4）基于所述安全处理结果数据构造应答报文；（A5）将所述应答报文以所述预定的通信格式传送回所述外部系统。

优选地，在本发明所公开的加密机模拟测试方法中，所述方法进一步包括：接收并执行来自用户终端的控制指令，并将执行结果传送回所述用户终端。

优选地，在本发明所公开的加密机模拟测试方法中，所述步骤（A1）进一步包括：基于所述预定的通信格式从所述请求报文中提取出报文体。

示例性地，在本发明所公开的加密机模拟测试方法中，所述执行结果包括执行结果状态指示（即执行成功或执行失败）和/或执行结果数据。

优选地，在本发明所公开的加密机模拟测试方法中，所述步骤（A2）进一步包括：基于预定参数解析接收到的所述请求报文。

示例性地，在本发明所公开的加密机模拟测试方法中，所述预定参数包括密钥参数和/或异常模拟控制参数。

示例性地，在本发明所公开的加密机模拟测试方法中，所述解析出的报文数据包括指令码、密钥和安全数据（即加解密数据）。

示例性地，在本发明所公开的加密机模拟测试方法中，所述控制指令包括配置指令和/或日志指令。

优选地，在本发明所公开的加密机模拟测试方法中，所述方法进一步包括：基于预定的配置文件执行初始化操作。

优选地，在本发明所公开的加密机模拟测试方法中，所述方法进一步包括：监控与数据处理过程相关的信息并将所述与数据处理过程相关的信息记录在日志文件中。

优选地，在本发明所公开的加密机模拟测试方法中，所述方法进一步包括：基于接收到的所述配置指令更新和/或重新读取所述配置文件，以及基于接收到的所述日志指令将统计信息输出到所述日志文件。

优选地，在本发明所公开的加密机模拟测试方法中，所述步骤（A3）进一步包括：基于所述解析出的报文数据，根据所述指令码使用所述密钥对所述安全数据进行处理，以获得所述安全处理结果数据。

优选地，在本发明所公开的加密机模拟测试方法中，所述步骤（A4）进一步包括：基于预定参数和所述安全处理结果数据构造所述应答报文。

优选地，在本发明所公开的加密机模拟测试方法中，所述预定的通信格式是以下通信格式之一：（a）由报文长度字段、报文头字段和报文体字段构成报文通信接口；（b）由报文长度字段、报文体字段构成报文通信接口；（c）仅由报文体字段构成报文通信接口（即无报文长度字段和报文头字段）。

优选地，在本发明所公开的加密机模拟测试方法中，所述方法进一步包括：基于所述配置文件配置所述预定的通信格式。

优选地，在本发明所公开的加密机模拟测试方法中，所述方法进一步包括：基于所述配置文件配置所述预定参数。

示例性地，在本发明所公开的加密机模拟测试方法中，所述配置文件包括环境变量、日志路径、日志级别标志以及线程数目中的至少一个。

优选地，在本发明所公开的加密机模拟测试方法中，所述日志文件包括用于记录通信报文的通信日志和用于记录处理过程中的异常情况信息的应用日志。

优选地，在本发明所公开的加密机模拟测试方法中，所述方法进一步包括：基于所述控制指令而将所述日志文件传送到所述用户终端。

优选地，在本发明所公开的加密机模拟测试方法中，所述方法进一步包括：基于所述配置文件配置所使用的安全加密算法。

示例性地，在本发明所公开的加密机模拟测试方法中，所述方法进一步包

括：为多个加密机接口规范（例如报文组装格式规范）中的每个定义动态链接库，所述动态链接库中的每个用于以对应的所述加密机接口规范解析所述请求报文以及构造所述应答报文。

示例性地，在本发明所公开的加密机模拟测试方法中，所述方法进一步包括：基于所述配置文件加载所述动态链接库中的一个作为工作动态链接库，从而以所述工作动态链接库所对应的加密机接口规范解析所述请求报文以及构造所述应答报文。

尽管本发明是通过上述的优选实施方式进行描述的，但是其实现形式并不局限于上述的实施方式。应该认识到：在不脱离本发明主旨和范围的情况下，本领域技术人员可以对本发明做出不同的变化和修改。

权利要求

1. 一种加密机模拟测试装置，所述加密机模拟测试装置包括:

通信接口，所述通信接口用于以预定的通信格式接收来自外部系统的请求报文，并将所述请求报文传送到加密机模拟模块，以及将来自所述加密机模拟模块的应答报文以所述预定的通信格式传送回所述外部系统;

加密机模拟模块，所述加密机模拟模块用于解析接收到的所述请求报文，并将解析出的报文数据传送到安全模块，以及基于来自所述安全模块的安全处理结果数据构造应答报文，并将所述应答报文传送到所述通信接口;

安全模块，所述安全模块用于处理所述解析出的报文数据以获得所述安全处理结果数据，并将所述安全处理结果数据传送回所述加密机模拟模块;

主控制模块，所述主控制模块用于在所述加密机模拟测试装置启动时基于预定的配置文件初始化所述加密机模拟测试装置，以及监控与数据处理过程相关的信息并维护日志文件。

2. 根据权利要求1所述的加密机模拟测试装置，其特征在于，所述通信接口进一步用于接收来自用户终端的控制指令，并将所述控制指令传送到所述主控制模块。

3. 根据权利要求2所述的加密机模拟测试装置，其特征在于，所述主控制模块进一步用于执行接收到的所述控制指令，并将执行结果经所述通信接口传送回所述用户终端。

4. 根据权利要求3所述的加密机模拟测试装置，其特征在于，所述通信接口进一步包括报文传输单元，其中，所述报文传输单元用于基于所述预定的通信格式从所述请求报文中提取出报文体，并将所述报文体传送到所述加密机模拟模块，以及将接收到的所述应答报文以所述预定的通信格式传送到所述外部系统。

5. 根据权利要求4所述的加密机模拟测试装置，其特征在于，所述通信接口进一步包括指令转发及数据传输单元。所述指令转发及数据传输单元用于接收来自所述用户终端的控制指令，并将所述控制指令传送到所述主控制模块，以及将来自所述主控制模块的执行结果传送到所述用户终端。

6. 根据权利要求5所述的加密机模拟测试装置，其特征在于，所述执行结果包括执行结果状态指示和/或执行结果数据。

7. 根据权利要求6所述的加密机模拟测试装置，其特征在于，所述加密机模拟模块进一步包括:

报文解析单元，所述报文解析单元用于基于预定参数解析接收到的所述请求报文，并将解析出的报文数据传送到所述安全模块;

报文构造单元，所述报文构造单元用于基于预定参数和接收到的所述安全处理结果数据构造所述应答报文，并将所述应答报文传送到所述通信接口。

8. 根据权利要求7所述的加密机模拟测试装置，其特征在于，所述预定参数包括密钥参数和/或异常模拟控制参数。

9. 根据权利要求8所述的加密机模拟测试装置，其特征在于，所述解析出的报文数据包括指令码、密钥和安全数据。

10. 根据权利要求9所述的加密机模拟测试装置，其特征在于，所述控制指令包括配置指令和/或日志指令。

11. 根据权利要求10所述的加密机模拟测试装置，其特征在于，所述主控制模块进一步包括:

配置单元，所述配置单元用于在所述加密机模拟测试装置启动时基于预定的配置文件初始化所述加密机模拟测试装置;

日志记录单元，所述日志记录单元用于监控与数据处理过程相关的信息并将所述与数据处理过程相关的信息记录在所述日志文件中。

12. 根据权利要求11所述的加密机模拟测试装置，其特征在于，所述主控制模块进一步包括指令处理单元，所述指令处理单元用于基于接收到的所述配置指令更新和/或重新读取所述配置文件，以及基于接收到的所述日志指令将统计信息输出到所述日志文件。

13. 根据权利要求12所述的加密机模拟测试装置，其特征在于，所述安全模块进一步用于基于所述解析出的报文数据，根据所述指令码使用所述密钥对所述安全数据进行处理，以获得所述安全处理结果数据。

14. 根据权利要求13所述的加密机模拟测试装置，其特征在于，所述预定的通信格式是以下通信格式之一: （a）由报文长度字段、报文头字段和报文

体字段构成报文通信接口；（b）由报文长度字段、报文体字段构成报文通信接口；（c）仅由报文体字段构成报文通信接口（即无报文长度字段和报文头字段）。

15. 根据权利要求14所述的加密机模拟测试装置，其特征在于，所述配置单元基于所述配置文件配置所述预定的通信格式。

16. 根据权利要求15所述的加密机模拟测试装置，其特征在于，所述配置单元基于所述配置文件配置所述预定参数。

17. 根据权利要求16所述的加密机模拟测试装置，其特征在于，所述配置文件包括环境变量、日志路径、日志级别标志以及线程数目中的至少一个。

18. 根据权利要求17所述的加密机模拟测试装置，其特征在于，所述日志文件包括用于记录通信报文的通信日志和用于记录处理过程中的异常情况信息的应用日志。

19. 根据权利要求18所述的加密机模拟测试装置，其特征在于，所述指令处理单元还用于基于所述控制指令而将所述日志文件经所述通信接口传送到所述用户终端。

20. 根据权利要求19所述的加密机模拟测试装置，其特征在于，所述配置单元基于所述配置文件配置所述安全模块使用的安全加密算法。

21. 根据权利要求20所述的加密机模拟测试装置，其特征在于，所述加密机模拟模块进一步用于为多个加密机接口规范中的每个定义动态链接库，所述动态链接库中的每个用于以对应的所述加密机接口规范解析所述请求报文以及构造所述应答报文。

22. 根据权利要求21所述的加密机模拟测试装置，其特征在于，所述加密机模拟模块进一步用于基于所述配置文件加载所述动态链接库中的一个作为工作动态链接库，从而以所述工作动态链接库所对应的加密机接口规范解析所述请求报文以及构造所述应答报文。

23. 一种加密机模拟测试方法，所述加密机模拟测试方法包括以下步骤：

（A1）以预定的通信格式接收来自外部系统的请求报文；

（A2）解析接收到的所述请求报文以获得解析出的报文数据；

（A3）处理所述解析出的报文数据以获得安全处理结果数据；

（A4）基于所述安全处理结果数据构造应答报文；

（A5）将所述应答报文以所述预定的通信格式传送回所述外部系统。

24. 根据权利要求23所述的加密机模拟测试方法，其特征在于，所述方法进一步包括：接收并执行来自用户终端的控制指令，并将执行结果传送回所述用户终端。

25. 根据权利要求24所述的加密机模拟测试方法，其特征在于，所述步骤（A1）进一步包括：基于所述预定的通信格式从所述请求报文中提取出报文体。

26. 根据权利要求25所述的加密机模拟测试方法，其特征在于，所述执行结果包括执行结果状态指示和/或执行结果数据。

27. 根据权利要求26所述的加密机模拟测试方法，其特征在于，所述步骤（A2）进一步包括：基于预定参数解析接收到的所述请求报文。

28. 根据权利要求27所述的加密机模拟测试方法，其特征在于，所述预定参数包括密钥参数和/或异常模拟控制参数。

29. 根据权利要求28所述的加密机模拟测试方法，其特征在于，所述解析出的报文数据包括指令码、密钥和安全数据。

30. 根据权利要求29所述的加密机模拟测试方法，其特征在于，所述控制指令包括配置指令和/或日志指令。

31. 根据权利要求30所述的加密机模拟测试方法，其特征在于，所述方法进一步包括：基于预定的配置文件执行初始化操作。

32. 根据权利要求31所述的加密机模拟测试方法，其特征在于，所述方法进一步包括：监控与数据处理过程相关的信息并将所述与数据处理过程相关的信息记录在日志文件中。

33. 根据权利要求32所述的加密机模拟测试方法，其特征在于，所述方法进一步包括：基于接收到的所述配置指令更新和/或重新读取所述配置文件，以及基于接收到的所述日志指令将统计信息输出到所述日志文件。

34. 根据权利要求33所述的加密机模拟测试方法，其特征在于，所述步骤（A3）进一步包括：基于所述解析出的报文数据，根据所述指令码使用所述密钥对所述安全数据进行处理，以获得所述安全处理结果数据。

35. 根据权利要求34所述的加密机模拟测试方法，其特征在于，所述步骤

（A4）进一步包括：基于预定参数和所述安全处理结果数据构造所述应答报文。

36. 根据权利要求35所述的加密机模拟测试方法，其特征在于，所述预定的通信格式是以下通信格式之一：（a）由报文长度字段、报文头字段和报文体字段构成报文通信接口；（b）由报文长度字段、报文体字段构成报文通信接口；（c）仅由报文体字段构成报文通信接口（即无报文长度字段和报文头字段）。

37. 根据权利要求36所述的加密机模拟测试方法，其特征在于，所述方法进一步包括：基于所述配置文件配置所述预定的通信格式。

38. 根据权利要求37所述的加密机模拟测试方法，其特征在于，所述方法进一步包括：基于所述配置文件配置所述预定参数。

39. 根据权利要求38所述的加密机模拟测试方法，其特征在于，所述配置文件包括环境变量、日志路径、日志级别标志以及线程数目中的至少一个。

40. 根据权利要求39所述的加密机模拟测试方法，其特征在于，所述日志文件包括用于记录通信报文的通信日志和用于记录处理过程中的异常情况信息的应用日志。

41. 根据权利要求40所述的加密机模拟测试方法，其特征在于，所述方法进一步包括：基于所述控制指令而将所述日志文件传送到所述用户终端。

42. 根据权利要求41所述的加密机模拟测试方法，其特征在于，所述方法进一步包括：基于所述配置文件配置所使用的安全加密算法。

43. 根据权利要求42所述的加密机模拟测试方法，其特征在于，所述方法进一步包括：为多个加密机接口规范中的每个定义动态链接库，所述动态链接库中的每个用于以对应的所述加密机接口规范解析所述请求报文以及构造所述应答报文。

44. 根据权利要求43所述的加密机模拟测试方法，其特征在于，所述方法进一步包括：基于所述配置文件加载所述动态链接库中的一个作为工作动态链接库，从而以所述工作动态链接库所对应的加密机接口规范解析所述请求报文以及构造所述应答报文。


加密机模拟测试装置
1
通信接口
5
报文传输单元
6
指令转发及数据传输单元
外部系统
用户终端
2
主控制模块
9
配置单元
10
指令处理单元
11
日志记录单元
3
加密机模拟模块
7
报文解析单元
8
报文构造单元
4
安全模块

图 1

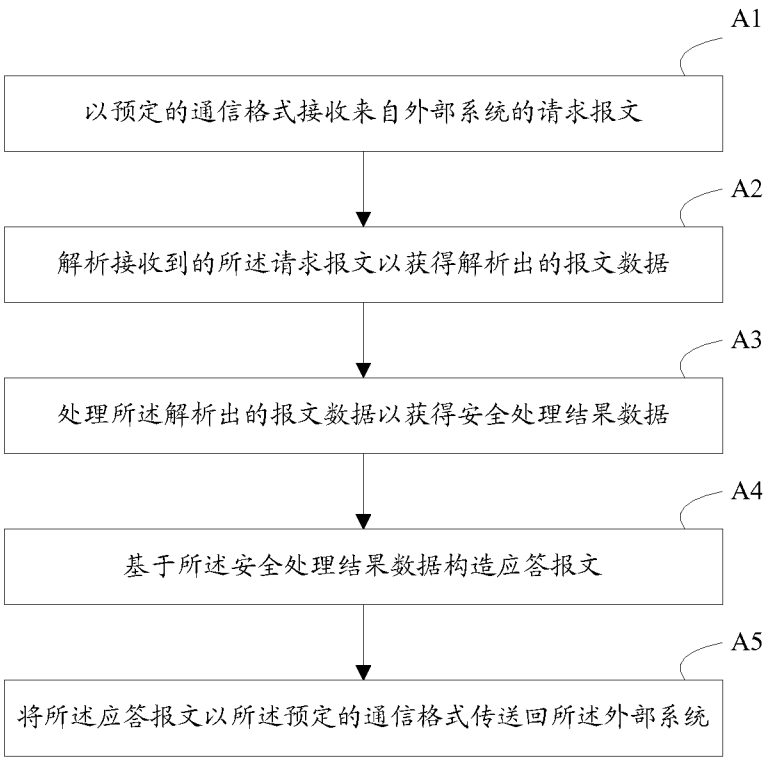

A1
以预定的通信格式接收来自外部系统的请求报文
A2
解析接收到的所述请求报文以获得解析出的报文数据
A3
处理所述解析出的报文数据以获得安全处理结果数据
A4
基于所述安全处理结果数据构造应答报文
A5
将所述应答报文以所述预定的通信格式传送回所述外部系统

图 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2012/083805

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/26 (2006.01) 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)

IPC: H04L, H04W, G06F

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)

CPRSABS, CNABS, CNKI, VEN: encryption equipment, encrypt+, encod+, security, emulat+, simulat+, test+, request+, pars+, analy+, key, response

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 101534227 A (BEIJING STAR-NET RUIJIE NETWORKS TECHNOLOGY CO., LTD.), 16 September 2009 (16.09.2009), see description, pages 8-9 and 13, and figure 7	1-44
Y	WO 2007073623 A1 (ZTE CORP. et al.), 05 July 2007 (05.07.2007), see description, pages 6-8	1-44
Y	US 2008137543 A1 ((CISC) CISCO TECHNOLOGY INC.), 12 June 2008 (12.06.2008), see description, pages 3-5	2-22, 24-44
A	US 2006206906 A1 ((IBMC) INT BUSINESS MACHINES CORP.), 14 September 2006 (14.09.2006), see the whole document	1-44

☐ 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
21 January 2013 (21.01.2013)	**07 February 2013 (07.02.2013)**
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 **FAN, Wenjing** Telephone No.: (86-10) **62411255**

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

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2012/083805

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101534227 A	16.09.2009	CN 101534227 B	20.07.2011
WO 2007073623 A1	05.07.2007	CN 101305542 A	12.11.2008
		CN 101305542 B	26.01.2011
US 2008137543 A1	12.06.2008	US 7801050 B2	21.09.2010
US 2006206906 A1	14.09.2006	US 7484226 B2	27.01.2009

国际检索报告

国际申请号
PCT/CN2012/083805

A. 主题的分类

H04L12/26 (2006.01) 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)

IPC: H04L, H04W, G06F

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）)

CPRSABS,CNABS,CNKI,VEN: 加密机，加密设备，加密，模拟，仿真，测试，请求，解析，密钥，应答，答复，响应，安全，encrypt+, encod+, security, emulat+, simulat+, test+, request+, pars+, analy+, key, response

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
Y	CN101534227A (北京星网锐捷网络技术有限公司) 16.9 月 2009 (16.09.2009) 参见说明书第 8-9、13 页，图 7	1-44
Y	WO2007073623A1 (中兴通讯股份有限公司等) 05.7 月 2007 (05.07.2007) 参见说明书第 6-8 页	1-44
Y	US2008137543A1 ((CISC) CISCO TECHNOLOGY INC) 12.6 月 2008 (12.06.2008) 参见说明书第 3-5 页	2-22，24-44
A	US2006206906A1 ((IBMC) INT BUSINESS MACHINES CORP) 14.9 月 2006 (14.09.2006) 参见全文	1-44

☐ 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
21.1 月 2013 (21.01.2013)	**07.2 月 2013 (07.02.2013)**
ISA/CN 的名称和邮寄地址： 中华人民共和国国家知识产权局 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 范文婧 电话号码：(86-10) **62411255**

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2012/083805

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN101534227A	16.09.2009	CN101534227B	20.07.2011
WO2007073623A1	05.07.2007	CN101305542A	12.11.2008
		CN101305542B	26.01.2011
US2008137543A1	12.06.2008	US7801050B2	21.09.2010
US2006206906A1	14.09.2006	US7484226B2	27.01.2009