(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 107070642 B
(45)授权公告日 2020.07.21

(21)申请号 201611214674.7

(22)申请日 2016.12.26

(65)同一申请的已公布的文献号
申请公布号 CN 107070642 A

(43)申请公布日 2017.08.18

(73)专利权人 贵州银行股份有限公司
地址 550006 贵州省贵阳市观山湖区长岭北路贵阳国际会议展览中心SOHO区D1栋出版集团大厦三层

(72)发明人 张晖 冯六军 吴贤佳 臧晗 卢松坚

(74)专利代理机构 贵阳中新专利商标事务所 52100
代理人 李亮 程新敏

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

(56)对比文件
CN 102868521 A,2013.01.09
CN 103780618 A,2014.05.07
CN 105933113 A,2016.09.07
US 6442690 B1,2002.08.27
US 2015139238 A1,2015.05.21

审查员 王相君

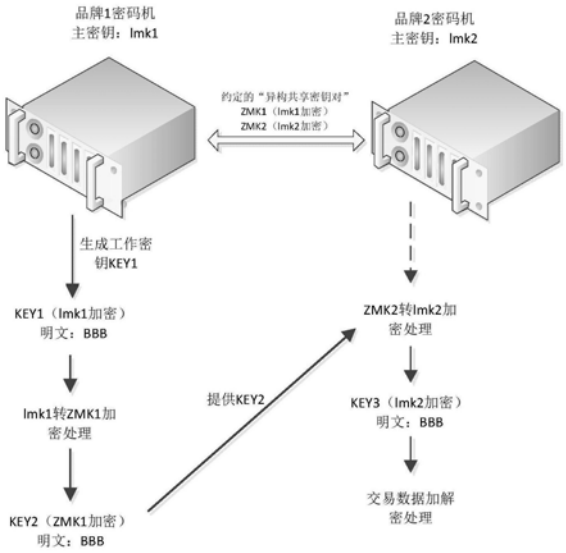
权利要求书1页 说明书4页 附图3页

(54)发明名称

多品牌密码机异构资源池复用技术

(57)摘要

本发明公开了一种多品牌密码机异构资源池复用技术。本发明实现了不同品牌的密码机数据兼容数据互用，拓展了密码的使用范围。对于金融交易行业来说，本发明将很大程度地改变了金融交易行业密码机的使用方式，密码机使用将不再受限于现有已使用的某个品牌，也不会依赖于某个品牌密码机，采用了本发明技术后，金融交易行业原有的交易系统可引入性能更高的新品牌密码机，并且减少了因引入新品牌密码机而带来的系统改造工作量。不仅如此，金融交易行业相关部门采用本发明后，可对现有使用的不同品牌密码机进行整合，形成密码机集聚，统一提供给所有业务系统调用，从而在不购买新的密码机情况下提高业务系统的处理效率，使得密码机资源最大化利用，并且减低购买密码机的成本。



CN 107070642 B

1.一种多品牌密码机异构资源池复用方法,其特征在于,包括如下步骤:

1)约定异构共享密钥对:由连接在同一服务器且使用两种以上不同品牌的密码机的工作设备组成的工作平台,在该工作平台中的任意一个密码机组A产生一对非对称密钥对,即公钥PK及私钥VK;在该工作平台内的另一个品牌的密码机组B则产生异构共享密钥对中的ZMK1,密码机组B对ZMK1进行转加密处理,将密码机组B本地主密钥加密的ZMK1转公钥PK加密,得到Key1,再将公钥PK加密的Key1在密码机组A中进行转加密,转为密码机组A本地主密钥加密,得到ZMK2;ZMK1与ZMK2共同组成共享密钥;

2)工作密钥产生:服务器调用密码机A产生工作密钥后,对工作密钥进行“密码机异构”处理,得到明文一致密文不同的工作密钥对,然后再把工作密钥对下发给工作设备,具体方案如下:

a)两种不同品牌密码机约定一对传输保护密钥ZMK1和ZMK2;两种不同品牌的密码机约定一把明文相同的传输保护密钥,密文是由各品牌密码机本地主密钥加密保护,该对传输保护密文为“异构共享密钥对”;

b)由密码机A随机产生一把工作密钥KEY1,该工作密钥由密码机A本地主密钥LMK1加密;

c)通过密码机A将KEY1从LMK1加密转为ZMK1加密,得到明文相同但密文不同的工作密钥KEY2;

d)由于ZMK1和ZMK2是明文相同的“异构共享密钥对”,这样就通过密码机B将把KEY2从ZMK2加密转为LMK2加密,LMK2是密码机B的本地主密钥;

e)因为工作密钥的明文在转加密前后是保持不变的,所以密码机A生成的工作密钥就能用于密码机B的运算中;

3)工作设备的工作密钥调用:工作设备根据密码机适用于情况,分别调用工作密钥对中对应的密码机主密钥加密的工作密钥。

2.根据权利要求1所述的多品牌密码机异构资源池复用方法,其特征在于:共享密钥每天都进行一次更新,更新的策略为:密码机组A生成一把公私钥对,密码机组B生成一把本地密钥加密的ZMK,密码机组B对ZMK进行转加密得到A组加密机的公钥加密的ZMK,并传输给密码机组A,密码机组A进行转加密得到本地密钥加密的ZMK,于是两组密码机便约定了一把共享ZMK密钥。

多品牌密码机异构资源池复用技术

技术领域

[0001] 本发明涉及密码学技术领域，尤其是一种多品牌密码机异构资源池复用技术。

背景技术

[0002] 目前，密码机在金融交易领域中使用广泛，其主要功能是实现对网络上传输的信息进行保护或鉴别，以保证金融信息的正确性，能够有效防止对通信数据的非法窃取或篡改，特别在银行、移动、电信、社保、交通等多个行业的电子支付计算机网络系统中其安全作用不可替代。

[0003] 但随着密码机加密技术的不断发展和推广，通过国家商用密码主管部门鉴定并批准使用的国内自主开发的密码机设备也随之增加，金融行业中使用密码机的品牌百花齐放。在密码机推广和使用过程中，不可避免的会遇到如下问题：

[0004] 1、各品牌密码机产生的数据不能直接互用

[0005] 密码机在产生工作密钥时，先随机产生该工作密钥的明文，然后用密码机的本地主密钥加密该明文得到工作密钥的密文。由于不同品牌密码机的本地主密钥不同，一个品牌密码机产生的工作密钥不能直接参与例外一个品牌密码机的运算。

[0006] 密码机对数据进行加解密运行时，都会用到本密码机产生的工作密钥进行运行，由于一个品牌密码机产生的工作密钥不能直接用于另外一个品牌密码机，所以导致该品牌密码机产生的数据也不能直接用于另外一个品牌密码机运行中。

[0007] 2、被设备“绑架”，更换密码机品牌难度大

[0008] 金融行业部门某业务系统在已经使用一个品牌密码机的情况下想改换另外一个品牌密码机时，由于原来的数据由原有品牌密码机产生的或加解密运行得到的，若更换另外一个品牌密码机或引用新品牌密码机，那么原有的数据则不能复用，需要使用新品牌密码机产生，如此对金融行业部门带来严重的安全隐患问题，容易引发交易事故，并且增加了金融行业部门运维人员的工作难度和工作量。不仅如此，密码机品牌更换难度大，使得金融行业部门会对已使用的品牌密码机形成依赖关系。

[0009] 3、密码机资源浪费

[0010] 部分金融行业部门会使用多个品牌密码机，而同一品牌的多台密码机采用“密码机复用”的方式进行工作，但由于业务系统较多业务交易量大，同一品牌的密码数量有限，在业务交易高峰期，同一品牌密码机由于资源不足可能导致交易失败，而另外一个品牌密码机因为使用频率不高，存在资源空余情况，但因为数据不兼容，资源空余的密码机却不能参与工作，由此出现了密码机资源浪费情况。

发明内容

[0011] 本发明的目的是：提供了一种多品牌密码机异构资源池复用技术，它能实现不同品牌的密码机数据兼容数据互用，拓展了密码的使用范围，以克服现有技术不足。

[0012] 本发明是这样实现的：多品牌密码机异构资源池复用技术，其特征在于，包括如下

步骤：

[0013] 1)约定异构共享密钥对：由连接在同一服务器且使用两种以上不同品牌的密码机的工作设备组成的工作平台，在该工作平台中的任意一个密码机A组产生一对非对称密钥对，即公钥PK及私钥VK；在该工作平台内的另一个品牌的密码机B组则产生异构共享密钥对中的ZMK1，密码机组B对ZMK1进行转加密处理，将密码机组B本地主密钥加密的ZMK1转公钥PK加密，得到Key1，再将公钥PK加密的Key1在密码机组A中进行转加密，转为密码机组A本地主密钥加密，得到ZMK2；ZMK1与ZMK2共同组成共享密钥；

[0014] 2)工作密钥产生：服务器调用密码机A产生工作密钥后，对工作密钥进行“密码机异构”处理，得到明文一致密文不同的工作密钥对，然后再把工作密钥对下发给工作设备，具体方案如下：

[0015] a)两种不同品牌密码机约定一对传输保护密钥ZMK1和ZMK2；两种不同品牌的密码机约定一把明文相同的传输保护密钥，密文是由各品牌密码机本地主密钥加密保护，该对传输保护密位为“异构共享密钥对”；

[0016] b)由密码机A随机产生一把工作密钥KEY1，该工作密钥由密码机A本地主密钥LMK1加密；

[0017] c)通过密码机A将KEY1从LMK1加密转为ZMK1加密，得到明文相同但密文不同的工作KEY2；

[0018] d)由于ZMK1和ZMK2是明文相同的“异构共享密钥对”，这样就通过密码机B将把KEY2从ZMK2加密转为LMK2加密，LMK2是密码机B的本地主密钥；

[0019] e)因为工作密文的明文在转加密前后是保持不变的，所以密码机A生成的工作密钥就能用于密码机B的运算中。

[0020] 3)工作设备的工作密钥调用：工作设备根据密码机适用于情况，分别调用工作密钥对中对应的密码机主密钥加密的工作密钥。

[0021] 共享密钥每天都进行一次更新，更新的策略为：密码机组A生成一把公私钥对，密码机组B生成一把本地密钥加密的ZMK，密码机组B对ZMK进行转加密得到A组加密机的公钥加密的ZMK，并传输给密码机组A，密码机组A进行转加密得到本地密钥加密的ZMK，于是两组密码机便约定了一把共享ZMK密钥。

[0022] 本发明的原理是：虽然不同品牌密码机的指令格式和主密钥不同，但是密码机的加解密算法是通用相同的，并且对数据加解密运算时，密码机是使用工作密钥明文进行运算的，基于上述两个原理，品牌1密码机生成的工作密钥密文经过一系列特殊处理，能用于品牌2密码机的数据加解密运算中，这一系列处理过程，称“密码机异构”。

[0023] “密码机异构”技术实现原理：所有的密码机都能实现工作密钥转加密功能，可以把本地主密钥加密的工作密钥密文转为通讯密钥加密的密文，虽然转加密前后的工作密钥密文不同，但是工作密钥明文却保持不变。基于该原理，两种品牌密码机约定一对明文相同但密文用各自本地主密钥加密的通讯密钥，该对通讯密钥我们称“异构共享密钥对”。该密钥的作用是，把品牌1密码机本地主密钥加密的工作密钥转为“异构共享密钥对”加密，再把“异构共享密钥对”加密后的工作密钥转加密为品牌2密码机本地主密钥加密，因为工作密文的明文在转加密前后是保持不变的，所以品牌1密码机生成的工作密钥就能用于品牌2密码机运算中。

[0024] 密码机对数据进行加解密运算时，先用本地主密钥解密工作密钥得到工作密钥的明文，然后使用工作密钥明文对数据进行加解密运行。由于品牌1密码机的工作密钥经过“密码机异构”处理后可以直接用于品牌2密码运算，所以品牌1密码机产生的数据也能直接用于品牌2密码运算中，本发明称该处理流程为“数据异构处理”。

[0025] 与现有的技术相比，本发明实现了不同品牌的密码机数据兼容数据互用，拓展了密码的使用范围。对于金融交易行业来说，本发明将很大程度地改变了金融交易行业密码机的使用方式，密码机使用将不再受限于现有已使用的某个品牌，也不会依赖于某个品牌密码机，采用了本发明技术后，金融交易行业原有的交易系统可引入性能更高的新品牌密码机，并且减少了因引入新品牌密码机而带来的系统改造工作量。不仅如此，金融交易行业相关部门采用本发明后，可对现有使用的不同品牌密码机进行整合，形成密码机集聚，统一提供给所有业务系统调用，从而在不购买新的密码机情况下提高业务系统的处理效率，使得密码机资源最大化利用，并且减低购买密码机的成本。本发明原理简单，操作难度低，适用性广，使用效果好。。

附图说明

[0026] 附图1为密码机异构处理示意图；

[0027] 附图2为密码机非异构处理数据示意图；

[0028] 附图3为数据异构处理示意图；

[0029] 附图4为“共享密钥对”的生成示意图；

[0030] 附图5为业务系统工作密钥调用说明示意图；

[0031] 附图6为“异构共享密钥”更换策略示意图。

具体实施方式

[0032] 下面结合附图对本发明作进一步的详细说明，但不作为对本发明的任何限制

[0033] 本发明的实施例：多品牌密码机异构资源池复用技术，贵州银行在2016年内对行内业务系统进行“国密改造”中，需要对行内业务系统使用密码机情况也行进改造。由于贵州银行行内所有业务系统原先使用的密码机为“卫士通”品牌密码机，改造后，所有行内业务系统必须同时支持“卫士通”品牌密码机交易处理和“科友”品牌密码机交易处理。

[0034] 由于贵州银行行内所有业务系统交易处理时调用密码机使用的工作密钥由行内的“通讯管理平台”(即工作平台)调用卫士通密码机生成的，所以本次改造需要对“通讯管理平台”进行“密码机异构”改造。改造后的“通讯管理平台”同时支持“卫士通”品牌密码机和“科友”品牌密码机。

[0035] 处理方案：

[0036] 1、约定“异构共享密钥对”

[0037] 如图4所示，改造后的“通讯管理平台”存在两组密码机组，分别为“卫士通”品牌密码机组A和“科友”品牌密码机组B。密码机组A产生一对非对称密钥对(公钥:PK，私钥:VK)，密码机组B产生“异构共享密钥对”中的ZMK1。密码机组B对ZMK1进行转加密处理，把密码机组B本地主密钥加密的ZMK1转PK加密，得到Key1。把PK加密的Key1在密码机组A中进行转加密，转为密码机组A本地主密钥加密，得到ZMK2。如此产生了“异构共享密钥对”ZMK1和ZMK2；

如图1所示，ZMK1和ZMK2是“异构共享密钥对”，KEY1是“卫士通”密码机生成的工作密钥，其密文由“卫士通”密码机主密钥lmk1加密，KEY1经过两次转加密后为KEY3，由“科友”密码机主密钥lmk2加密。KEY1和KEY1虽然由不同的品牌密码机主密钥加密，但明文一致，都可以用于数据加解密处理。

[0038] 2、工作密钥产生

[0039] “通讯管理平台”调用“卫士通”密码机产生工作密钥后，对工作密钥进行“密码机异构”处理，得到明文一致密文不同的工作密钥对，然后再把工作密钥对下发工业务系统。

[0040] 3、业务系统工作密钥调用

[0041] 如图5所示，行内业务系统根据密码机品牌适用于情况，分别调用工作密钥对中的“卫士通”密码机主密钥加密的工作密钥和“科友”密码机主密钥加密的工作密钥。例如，若调用“科友”品牌密码机，则使用“科友”密码机主密钥加密的工作密钥进行交易数据加解密运行。

[0042] 但是，如图2所示，如是采用密码机非异构处理，当两个不同品牌密码机不使用“密码机异构”技术进行数据互用时，密钥KEY1是品牌1密码机主密钥加密，明文数据data由KEY1加密得到密文数据DATA1。把KEY1和密文数据DATA1提供给品牌2密码机进行解密，由于KEY1是品牌1密码机主密钥加密的，所以品牌2密码机使用KEY1进行解密计算时，会解密失败。

[0043] 如图3所示，当两个不同品牌密码机使用“密码机异构”技术后进行数据互用时，密钥KEY1是品牌1密码机主密钥加密，KEY3是品牌2密码机主密钥加密，明文数据data由KEY1加密得到密文数据DATA1。把密文数据DATA1提供给品牌2密码机进行解密，由于密钥KEY1和KEY3的密钥明文是一致的，所以KEY3对DATA1数据解密时，解密成功，得到明文数据data。

[0044] 4、“异构共享密钥”一天一更换策略

[0045] 如图6所示，为了提高安全，“异构共享密钥”必须支持一天一换，共享密钥更新的策略如下：密码机组A生成一把公私钥对，密码机组B生成一把本地密钥加密的ZMK，密码机组B对ZMK进行转加密得到A组加密机的公钥加密的ZMK，并传输给密码机组A，密码机组A进行转加密得到本地密钥加密的ZMK，于是两组密码机便约定了一把共享ZMK密钥。

[0046] 以上所述，仅是本发明的较佳实例而已，并非对本发明做任何形式上的限制，任何未脱离本发明技术方案内容，依据本发明的技术实质对以上实施例所作的任何简单修改、等同变化与修饰，均仍属于本发明技术方案的范围内。

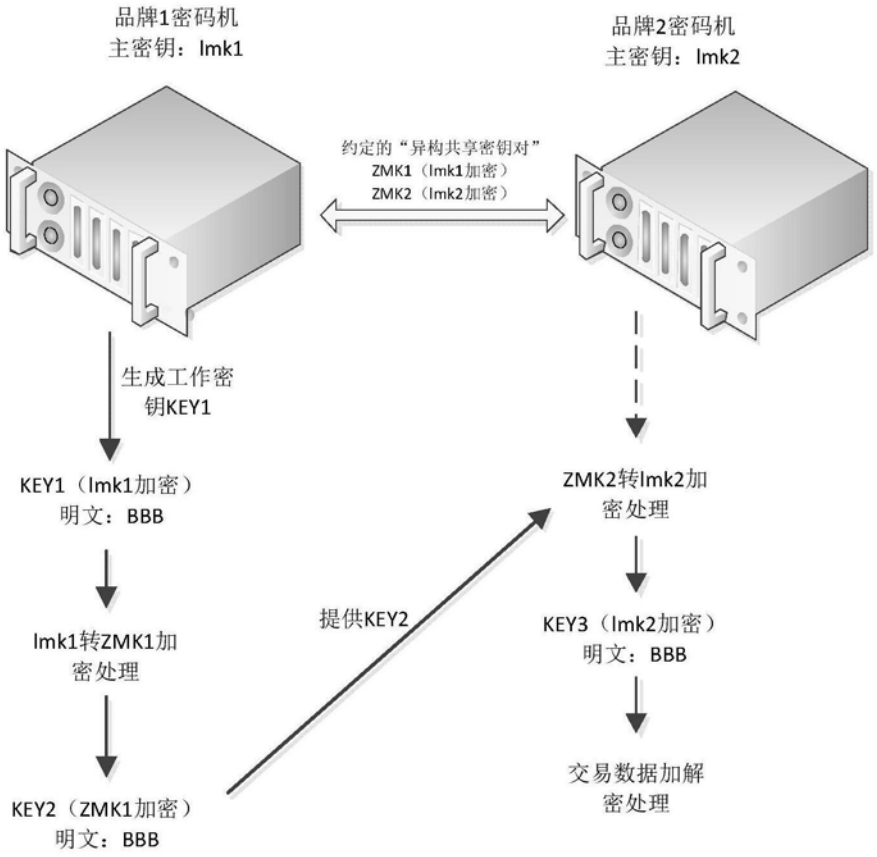

品牌1密码机
主密钥：lmk1
品牌2密码机
主密钥：lmk2
约定的“异构共享密钥对”
ZMK1（lmk1加密）
ZMK2（lmk2加密）
生成工作密钥KEY1
KEY1（lmk1加密）
明文：BBB
lmk1转ZMK1加密处理
KEY2（ZMK1加密）
明文：BBB
提供KEY2
ZMK2转lmk2加密处理
KEY3（lmk2加密）
明文：BBB
交易数据加解密处理

图1

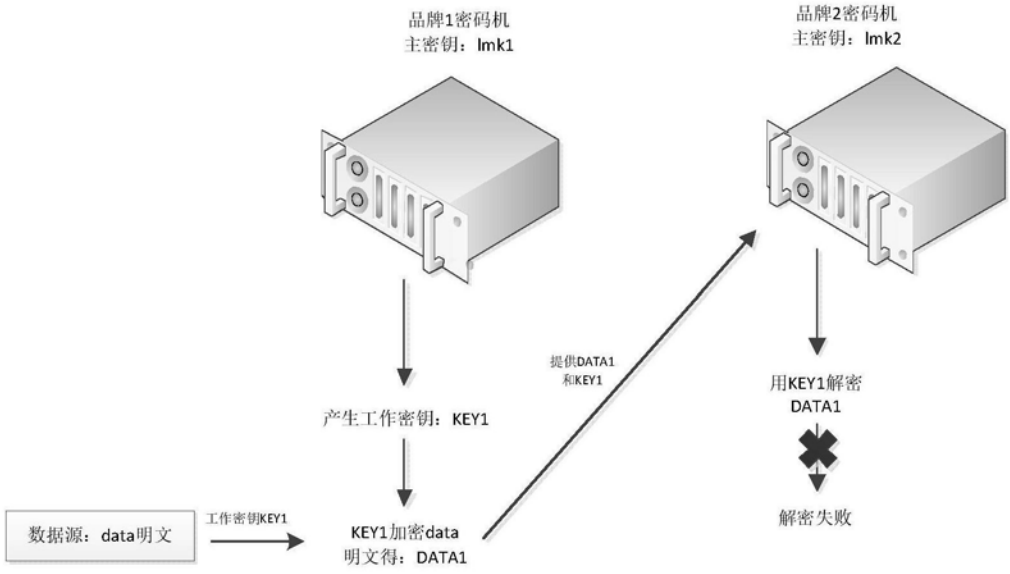

品牌1密码机
主密钥：lmk1
品牌2密码机
主密钥：lmk2
产生工作密钥：KEY1
提供DATA1和KEY1
用KEY1解密DATA1
解密失败
数据源：data明文
工作密钥KEY1
KEY1加密data
明文得：DATA1

图2

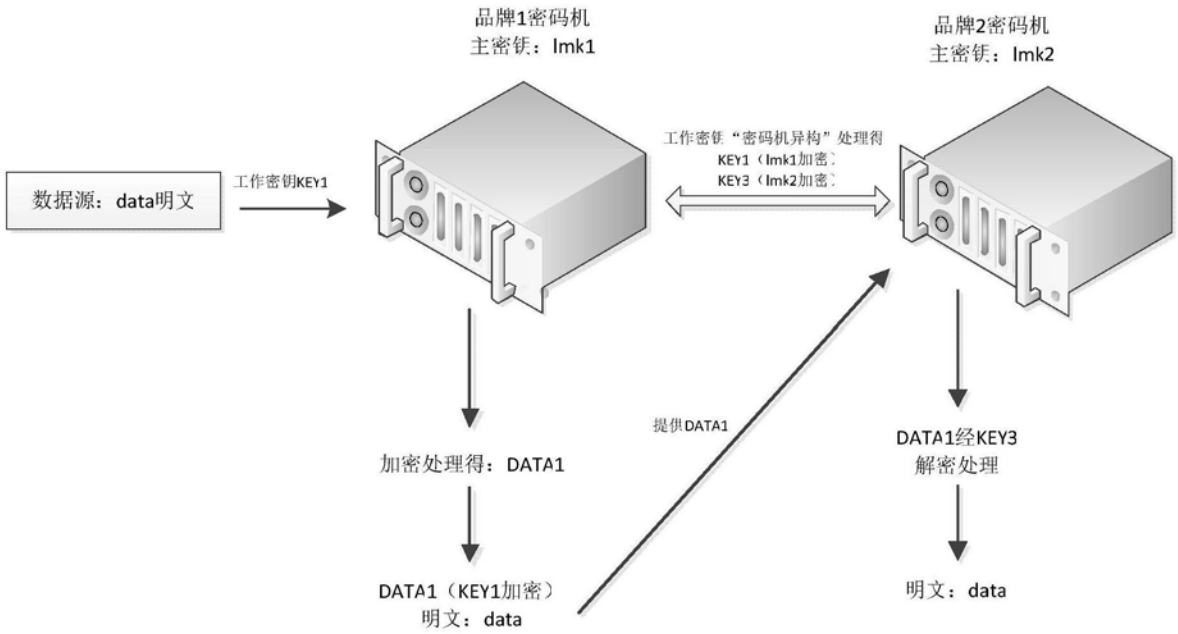

品牌1密码机
主密钥：lmk1
品牌2密码机
主密钥：lmk2
数据源：data明文
工作密钥KEY1
工作密钥“密码机异构”处理得
KEY1（lmk1加密）
KEY3（lmk2加密）
加密处理得：DATA1
提供DATA1
DATA1经KEY3
解密处理
DATA1（KEY1加密）
明文：data
明文：data

图3

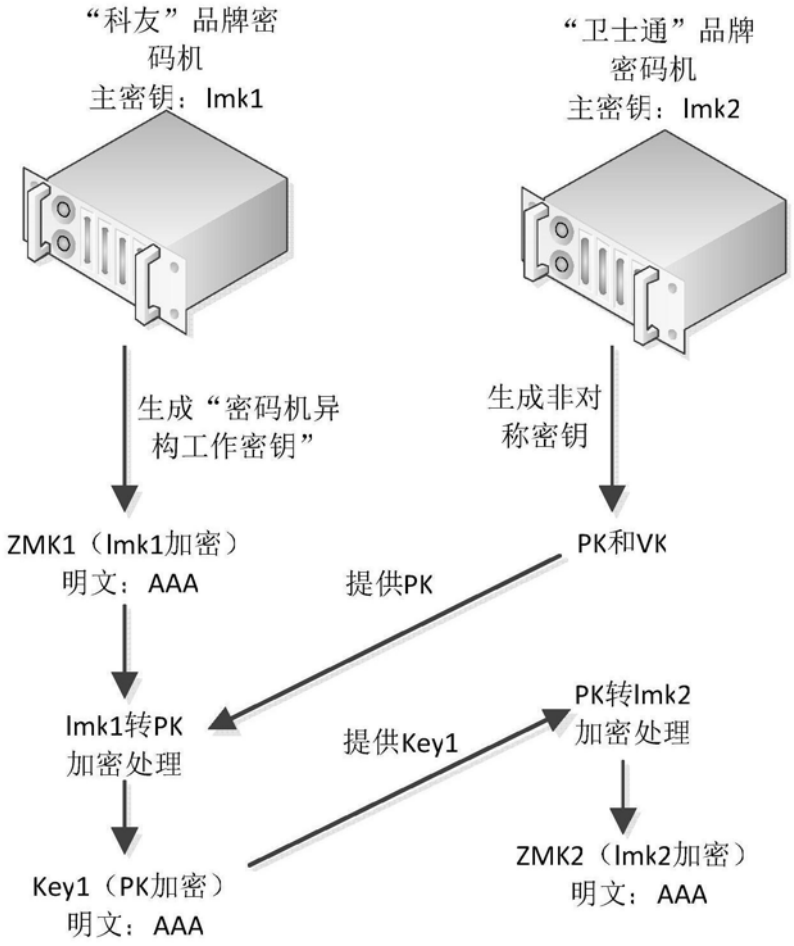

“科友”品牌密
码机
主密钥：lmk1
“卫士通”品牌
密码机
主密钥：lmk2
生成“密码机异
构工作密钥”
生成非对
称密钥
ZMK1（lmk1加密）
明文：AAA
PK和VK
提供PK
lmk1转PK
加密处理
提供Key1
PK转lmk2
加密处理
Key1（PK加密）
明文：AAA
ZMK2（lmk2加密）
明文：AAA

图4

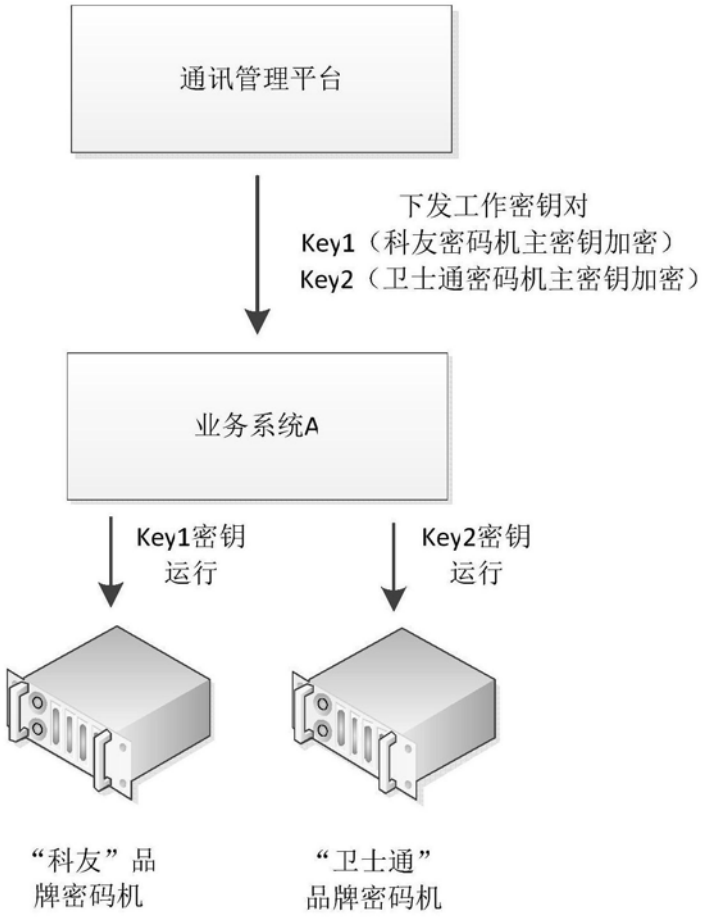

通讯管理平台
下发工作密钥对
Key1（科友密码机主密钥加密）
Key2（卫士通密码机主密钥加密）
业务系统A
Key1密钥
运行
Key2密钥
运行
“科友”品
牌密码机
“卫士通”
品牌密码机

图5

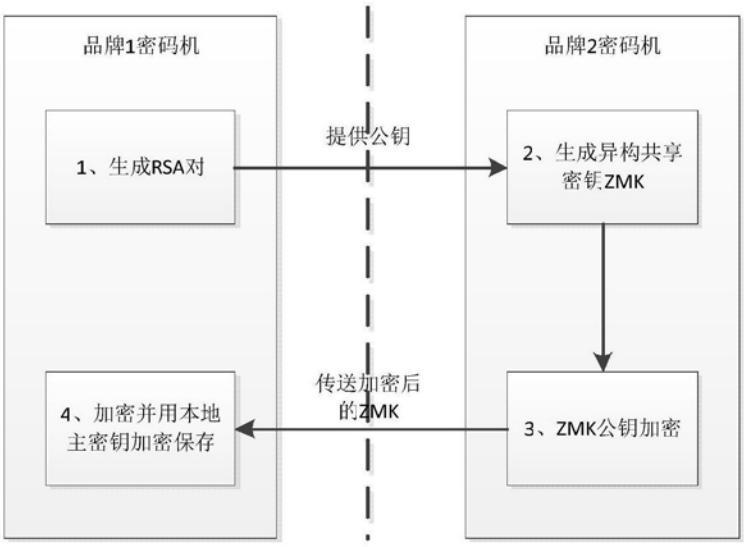

品牌1密码机
品牌2密码机
1、生成RSA对
提供公钥
2、生成异构共享
密钥ZMK
传送加密后
的ZMK
4、加密并用本地
主密钥加密保存
3、ZMK公钥加密

图6