团　　体　　标　　准

T/EMCG 001.4.2019

移动智能终端密码模块技术框架
第 4 部分：密钥多端协同计算保护技术架构

Technical framework of cryptographic module in mobile smart terminal

Part 4: Key protection based on multi-party computation

2019-07-05 发布　　2019-07-05 实施

中关村网络安全与信息化产业联盟　发布

目 次

前　言

T/EMCG 001-2019《移动智能终端密码模块技术框架》分为 5 个部分：

第 1 部分：总则

第 2 部分：密钥加密本地保护技术架构

第 3 部分：密钥加密云保护技术架构

第 4 部分：密钥多端协同计算保护技术架构

第 5 部分：基于安全芯片的技术架构

本部分为 T/ EMCG 001-2019《移动智能终端密码模块技术框架》的第 4 部分。

本部分由中关村网络安全与信息化产业联盟企业移动计算工作组（EMCG）提出。

本部分由参与 T/ EMCG 001-2019《移动智能终端密码模块技术框架》标准制定的单位投票表决通过。

本部分主要起草单位：中关村网络安全与信息化产业联盟企业移动计算工作组（EMCG）、北京江南天安科技有限公司、中国科学院信息工程研究所、奇安信科技集团股份有限公司、江苏通付盾科技有限公司、北京握奇数据股份有限公司、卫士通信息产业股份有限公司、鼎桥通信技术有限公司等。

本部分主要起草人：刘宗斌、张晶、李强、王克、史晗晖、张凡、傅文斌、李勃、鲁洪成、李向荣、张令臣等。

引　言

密码技术使用的安全性除了算法自身安全性外还取决于算法正确实现和安全参数可靠保护。在开放移动网络和便携移动终端系统环境中，如何安全设计、实现和使用密码模块，如何保护敏感安全参数成为移动智能终端密码模块设计和实现的核心问题。

为了解决移动智能终端缺乏可靠密钥保护环境的问题，引入密钥多端协同计算机制，由两端或三端协同生成用户 SM2 私钥，并由各方独立保存，协同完成数字签名等密码运算，保证移动智能终端用户私钥的安全，满足 GM/T 0028 -2014 标准要求。

移动智能终端密码模块技术框架
第4部分：密钥多端协同计算保护技术架构

1 范围

T/EMCG 001-2019《移动智能终端密码模块技术框架》的本部分规范了移动智能终端密钥多端协同计算保护技术架构组成、主要工作流程，以及满足GM/T 0028-2014标准各安全域的具体要求。

本规范是GM/T 0028-2014在移动智能终端中实现密码模块的具体展开和补充，适用于指导密码模块制造厂家设计、实现移动智能终端密码模块，也可作为移动智能终端使用密码模块的参考。

2 规范性引用文件

下列文件中的条款通过T/EMCG 001-2019《移动智能终端密码模块技术框架》的本部分的引用而成为本部分的条款。

GM/T 0003-2012 SM2椭圆曲线公钥密码算法

GM/T 0005-2012 随机性检测规范

GM/T 0009-2012 SM2密码算法使用规范

GM/T 0019-2012 通用密码服务接口规范

GM/T 0028-2014 密码模块安全技术要求

GM/T 0030-2014 服务器密码机技术规范

T/ EMCG 001-2019《移动智能终端密码模块技术框架 第 1 部分：总则》

3 术语和定义

3.1

非对称密钥对 asymmetric key pair

一对相关的密钥，其中私有密钥规定私有变换，公开密钥规定公开变换。

[GB/T 25069-2010，定义2.2.2.33]

3.2

服务器密码机 cryptographic server；

又称主机加密服务器，能够独立或并行为多个应用实体提供密码服务和密钥管理的设备。

[GM/T 0030-2014，定义3.1]

3.3

数字签名 digital signature

附加在数据单元上的数据，或是对数据单元所作的密码变换，这种数据或变换允许数据单元的接收者用以确认数据单元的来源和完整性，并保护数据防止被人（例如接收者）伪造或抵赖。

[GB/T 25069-2010，定义2.2.2.176]

3.4

密钥多端协同计算保护 key protection based on multi-party computation；KPBMC

将一个密钥由多方联合生成，每一方产生各自的密钥分量并独立保存，使用时多方使用各自密钥分量协同完成密码计算（如数字签名），任何一方，任何时候都不能获得完整的密钥，从而降低密钥在一方保存存在的泄露风险。本标准采用密钥多端协同计算保护以解决移动智能终端软件密码组件密钥保护环境不安全问题。

3.5

移动智能终端密码组件 mobile smart terminal cryptographic components；MST-CC

部署在移动智能终端中的密码组件，或独立构成，或与服务端密码组件（SS-CC、TPSS-CC）一起构成移动智能终端密码模块。

3.6

个人特征数据 personal profile data；PPD

个人知道或独具的因素，如PIN码，手势码，以及个人的生物特征，如指纹、脸部特征等。

3.7

服务端密码组件 server side cryptographic components；SS-CC

部署在服务端中的密码组件，与移动智能终端密码组件（MST-CC）一起构成移动智能终端密码模块。

3.8

第三方服务端密码组件 third party server side cryptographic components；TPSS-CC

部署在第三方服务端中的密码组件，与移动智能终端密码组件（MST-CC）、服务端密码组件（SS-CC）一起构成移动智能终端密码模块。

3.9

用户私钥 user private key

在某一移动智能终端使用者的非对称密钥对中，只应由该用户掌握和使用的密钥。正常情况下，私钥不应泄露。

3.10

私钥分量

在密钥多端协同计算保护中，由协同的某方生成的部分密钥数据，所有分量一起组合构成用户私钥。如，本标准中移动智能终端密码组件（MST-CC）产生的私钥分量、服务端密码组件（SS-CC）产生的私钥分量。

3.11

用户公钥 user public key

在移动应用用户非对称密钥对中，能够公开的密钥。

4 符号和缩略语

下列符号和缩略语适用于T/EMCG 001-2019《移动智能终端密码模块技术框架》的本部分。

CC 密码组件（cryptographic components）
CMMST 移动智能终端密码模块（cryptographic module of mobile smart terminal）
CSP 关键安全参数（critical security parameter）
KPBMC 密钥多端协同计算保护（key protection based on multi-party computation）
MST 移动智能终端（mobile smart terminal）
MST-CC 移动智能终端密码组件（mobile smart terminal cryptographic components）
PIN 个人身份识别码（personal identification number）
PPD 个人特征数据（personal profile data）
SDK 软件开发套件（software development kit）
SS-CC 服务端密码组件（server side cryptographic components）
TPSS-CC 第三方服务端密码组件（third party server side cryptographic components）

5 概述

5.1 引言

在基于密钥多端协同计算保护的移动智能终端密码模块（CMMST of key protection based on multi-party computation；CMMST-KPBMC）中，两端或三端协同生成用户（SM2）私钥分量，各方独立保存各自生成的私钥分量，协同完成数字签名、数据加解密等核准的密码服务功能。密码运算过程中在任意一方不会出现完整的用户私钥信息,从而保证移动智能终端用户私钥的安全,满足 GM/T 0028 -2014 对安全一、二级密码模块的要求。

CMMST-KPBMC 包括密钥双端协同计算保护和密钥三端协同计算保护。

5.2 密钥双端协同计算保护

5.2.1 技术架构

CMMST-KPBMC 密钥双端协同计算技术架构由移动智能终端密码组件（MST-CC）和服务端密码组件（SS-CC）组成。MST-CC 以软件形式部署在 MST 中，实现 MST-CC 私钥分量生成、协同签名与协同解密等功能；SS-CC 基于服务器密码机，实现 SS-CC 私钥分量生成、协同签名与协同解密等功能。密钥双端协同计算保护技术架构如图 1所示。

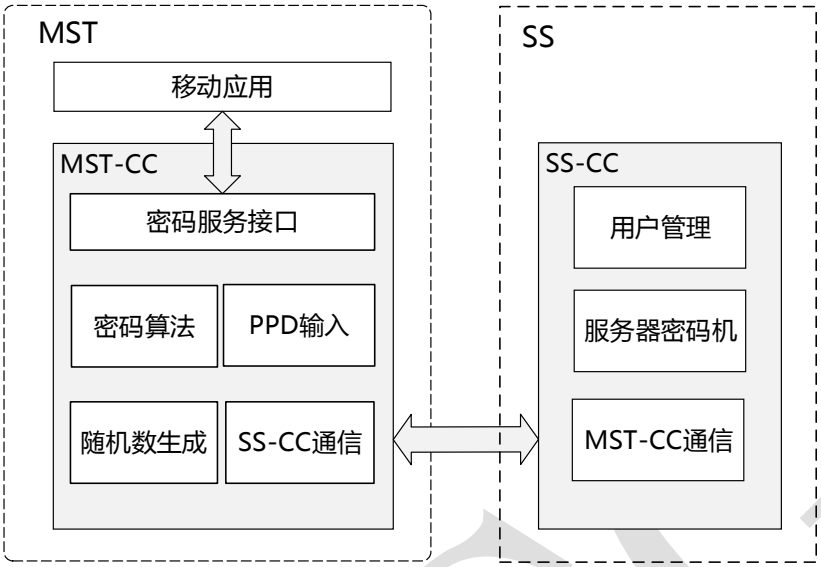

图 1 密钥双端协同计算保护技术架构

5.2.1.1 移动智能终端密码组件 MST-CC

MST-CC完成MST-CC私钥分量生成、与SS-CC协同数字签名及数据加解密等功能，至少包括完成以下功能的模块：

（1）密码服务接口。移动应用通过调用密码服务接口请求密码服务。

（2）密码算法。实现核准的密码算法，如SM2、SM3、SM4算法。

（3）PPD输入。采用输入试错锁定、界面劫持告警，收集移动用户个人特征数据（如PIN码）。

（4）随机数生成。为密码计算生成满足要求的随机数。

（5）SS-CC通信。实现与SS-CC通信。

5.2.1.2 服务端密码组件 SS-CC

SS-CC基于服务器密码机实现SS-CC私钥分量生成、协同签名与协同解密等功能，至少包括完成以下功能的模块：

（1）用户密钥管理。维护移动应用用户信息、密钥分量状态，根据MST-CC服务请求提供移动应用密码服务。

（2）服务器密码机。用户私钥协同生成、SS-CC私钥分量加解密、协同数据签名、协同数据解密等需要的密码计算在密码机中完成。

（3）MST-CC通信。实现与MST-CC通信。

5.2.2 基本工作流程

本标准 CMMST-KPBMC 密钥双端协同计算保护基本工作流程包括协同密钥生成、协同数据签名与协同数据解密流程。数据验签符合 GMT 0003.2-2012 SM2 椭圆曲线公钥密码算法 第 2 部分：数字签名算法；数据加密符合 GMT 0003.4-2012 SM2 椭圆曲线公钥密码算法 第 4 部分：公钥加密算法。

符号说明：

[*]：点乘操作

[-]：点减操作

[+]：点加操作

5.2.2.1 协同密钥生成流程

符号定义：

d_{A1}、d_{A2}——用户 A 的 MST-CC 私钥分量、SS-CC 私钥分量

P_A——用户 A 公钥

协同密钥生成基本流程：

1) MST-CC向SS-CC发送密钥生成请求；
2) 根据具体协同计算算法进行协同密钥生成，生成双端部分私钥d_{A1}、d_{A2}，以及公钥P_A；
3) SS-CC生成移动应用用户ID，将ID发送给MST-CC；
4) SS-CC使用密码机加密保存d_{A2}；
5) MST-CC保存用户ID，用户输入PPD，并用该PPD参与运算对d_{A1}进行加密保存，将公钥P_A输出给移动应用。

具体实现算法参见附录 B，部分步骤可以调整顺序或合并执行。

5.2.2.2 协同数据签名流程

符号定义：

d_{A1}、d_{A2}——用户 A 的 MST-CC 私钥分量、SS-CC 私钥分量

1) MST-CC取出用户ID，将用户ID发送给SS-CC；
2) SS-CC根据用户ID选择并恢复相应的SS-CC私钥分量d_{A2}；
3) MST-CC用户确认签名信息后输入PPD，使用PPD恢复签名私钥分量d_{A1}；
4) 根据具体协同计算算法利用d_{A1}和d_{A2}进行协同数据签名，生成签名值。

具体实现算法参见附录 B，部分步骤可以调整顺序或合并执行。

5.2.2.3 协同数据解密流程

符号定义：

d_{A1}、d_{A2}——MST-CC 私钥分量、SS-CC 私钥分量

1) MST-CC取出用户ID，将用户ID发送给SS-CC；
2) SS-CC根据用户ID选择相应的SS-CC私钥分量d_{A2}；
3) MST-CC用户确认签名信息后输入PPD，使用PPD恢复签名私钥分量d_{A1}；
4) 根据具体协同计算算法利用d_{A1}和d_{A2}进行协同数据解密，得到密文。

具体实现算法参见附录 B，部分步骤可以调整顺序或合并执行。

5.3 密钥三端协同计算保护

5.3.1 技术架构

CMMST-KPBMC 将用户私钥分为三个密钥分量，分别由 MST-CC、SS-CC 及第三方服务端密码组件（TPSS-CC）生成，三端协同进行数字签名计算。

CMMST-KPBMC 密钥三端协同计算保护可进一步降低密钥分量非法组合带来的安全风险，用户可在两端协同计算基础上引入第三端机构参与密钥协同计算和保护，加强服务端密钥管理的可信度。

CMMST-KPBMC 密钥三端协同计算保护技术架构由 MST-CC、SS-CC 及 TPSS-CC 组成，如图 所示：

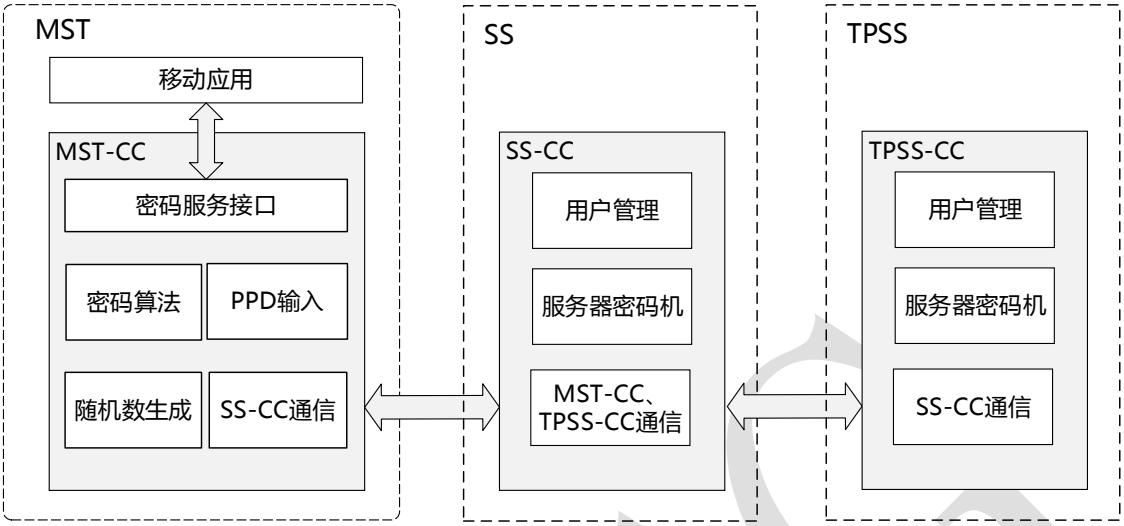

图 2 CMMST-KPBMC 密钥三端协同计算保护技术架构

5.3.1.1 移动智能终端密码组件 MST-CC

MST-CC 为软件组件，部署在移动智能终端中，负责 MST-CC 用户私钥分量生成，并与 SS-CC、TPSS-CC 协同密钥计算。MST-CC 至少包括完成以下功能的模块：

（1） 密码服务接口。移动应用通过调用密码服务接口请求密码服务。

（2）密码算法。实现核准的密码算法，如 SM2、SM3、SM4 算法。

（3） PPD 输入。采用输入试错锁定、界面劫持告警，收集移动用户个人特征数据（如 PIN 码）。

（4）随机数生成。为密码计算生成满足要求的随机数。

（5）SS-CC 通信。实现与 SS-CC 通信。

5.3.1.2 服务端密码组件 SS-CC

SS-CC 部署在服务器中，负责生成 SS-CC 用户私钥分量，参与三端协同数字签名计算。SS-CC 至少包括完成以下功能的模块：

（1） 用户密钥管理。对注册的移动应用用户及其私钥分量进行管理。

（2） 服务器密码机。执行密钥计算，满足 GM/T 0030-2014《服务器密码机技术规范》。

（3） MST-CC、TPSS-CC 通信。实现与 MST-CC、TPSS-CC 通信。

5.3.1.3 第三方服务端密码组件 TPSS-CC

TPSS-CC 部署在服务器中，协同 SS-CC、MST-CC 实现相应私钥分量生成、数字签名计算。TPSS-CC 至少包括完成以下功能的模块：

（1） 用户密钥管理。对注册的移动应用用户及其私钥分量进行管理。

（2） 服务器密码机。执行密钥计算，满足 GM/T 0030-2014《服务器密码机技术规范》。

（3） SS-CC 通信模块。实现与 SS-CC 通信。

5.3.2 基本工作流程

本标准 CMMST-KPBMC 密钥三端协同计算保护基本工作流程包括三端协同密钥生成和三端协同数据签名流程。三端数据验签符合 GMT 0003.2-2012 SM2 椭圆曲线公钥密码算法 第 2 部分：数字签名算法。

5.3.2.1 三端协同密钥产生流程

本流程生成的用户私钥符合 GMT 0003.2-2012 SM2 椭圆曲线公钥密码算法要求。

符号定义：

d_{A1} 、d_{A2} 、d_{A3}——分别为用户 A 的 MST-CC、SS-CC、TPSS-CC 私钥分量

P_A——用户 A 公钥

三端协同密钥产生流程：

1) MST-CC 输入用户 PPD，产生私钥分量 d_{A1}，向 SS-CC 传递必要参数并发送密钥生成请求
2) SS-CC 根据 PPD 生成用户 ID，产生私钥分量 d_{A2}，密码机加密保存 d_{A2}；
   向 TPSS-CC 传递必要参数并发送密钥生成请求；
3) TPSS-CC 产生私钥分量 d_{A3}，密码机加密保存 d_{A3}；
   产生公钥 P_A 并验证公钥合法性，如公钥不合法，重新生成 d_{A3}；
4) TPSS-CC 将 P_A 传递给 SS-CC；
5) SS-CC 将 P_A、用户 ID 传递给 MST-CC；
6) MST-CC 对 d_{A1} 进行（加密）保护，将用户公钥 P_A 输出给移动应用。

具体实现算法参见附录 C，部分步骤可以调整顺序或合并执行。

5.3.2.2 三端协同数据签名流程

本流程数据签名符合 GMT 0003.2-2012 SM2 椭圆曲线公钥密码算法要求。

符号定义：

d_{A1} 、d_{A2} 、d_{A3}——分别为用户 A 的 MST-CC、SS-CC、TPSS-CC 私钥分量

三端协同数据签名流程：

1) MST-CC取出用户ID，向SS-CC发签名请求
2) SS-CC向TPSS-CC发签名请求；
3) TPSS-CC根据用户ID查找并恢复私钥分量d_{A3}，做部分签名计算发送给SS-CC；
4) SS-CC根据用户ID查找并恢复私钥分量d_{A2}，做部分签名计算发送给MST-CC；
5) MST-CC输入用户PPD，使用PPD恢复私钥分量d_{A1}，和SS-CC、TPSS-CC协同得出签名值。

具体实现算法参见附录C，部分步骤可以调整顺序或合并执行。

6 密码模块规格

6.1 密码模块类型

CMMST-KPBMC 是混合软件密码模块，包括 MST-CC、SS-CC 及 TPSS-CC 软件模块及服务器密码机。

6.2 密码边界

密钥双端协同计算保护 CMMST-KPBMC 边界为 MST-CC、SS-CC 的可执行文件或文件集以及服务器密码机，如**错误!未找到引用源。**灰色框所示。

（1） MST-CC 至少包括完成以下功能的模块：密码服务接口，密码算法，PPD 输入，随机数生成，SS-CC 通信。

（2） SS-CC 至少包括完成以下功能的模块：用户密钥管理，服务器密码机，MST-CC 通信。

（3） MST-CC、SS-CC 软件模块运行在独立的进程空间中，使用操作系统进程间通信接口与密码边界外进行数据交换。

密钥三端协同计算保护 CMMST-KPBMC 边界为 MST-CC、SS-CC、TPSS-CC 的可执行文件或文件集以及服务器密码机，如图 5 灰色框所示。

（1） MST-CC 至少包括完成以下功能的模块：密码服务接口，密码算法，PPD 输入，随机数生成，SS-CC 通信。

（2） SS-CC 至少包括完成以下功能的模块：用户密钥管理，服务器密码机，MST-CC、TPSS-CC 通信。

（3） TPSS-CC 至少包括完成以下功能的模块：用户密钥管理，服务器密码机，SS-CC 通信；

（4） MST-CC、SS-CC、TPSS-CC 软件模块运行在独立的进程空间中，使用操作系统进程间通信接口与密码边界外进行数据交换。

6.3 工作模式

CMMST-KPBMC 运行于密码模块核准的工作模式下。

7 密码模块接口

7.1 物理和逻辑接口

CMMST-KELP 逻辑接口分布在 MST-CC、SS-CC 及 TPSS-CC 上，各方逻辑接口类型相同。

7.2 接口类型

CMMST-KPBMC 接口类型为混合软件模块接口类型。

7.3 接口定义

CMMST-KPBMC 接口定义参照 GM/T 0019-2012 通用密码服务接口规范。

7.4 可信信道

对于 CMMST-KPBMC 此项无要求。

8 角色、服务和鉴别

8.1 角色

CMMST-KPBMC 支持密码主管角色、移动应用用户角色。

密码主管：负责对 SS-CC、TPSS-CC 进行操作，以及 CMMST-KPBMC 系统管理。（三端协同计算密码模块有两个密码主管，分别对 SS-CC、TPSS-CC 进行操作。）

移动应用用户：使用 MST-CC 实现私钥分量生成、数据签名/验签及加解密等。

8.2 服务

8.2.1 服务通用要求

CMMST-KPBMC满足GM/T 0028-2014 7.4.3要求。

8.2.2 旁路能力

CMMST-KPBMC不提供旁路能力或功能。

8.2.3 自启动密码服务能力

CMMST-KPBMC不提供自启动密码服务能力或功能。

8.2.4 软件/固件加载

CMMST-KPBMC不提供加载外部软件/固件功能。

8.3 鉴别

CMMST-KPBMC 除满足 GM/T 0028-2014 7.4.4 对安全二级的要求外，还具备以下功能：

（1） MST-CC采用PPD对移动应用用户身份进行鉴别。

（2） SS-CC及TPSS-CC采用硬件Token（令牌）对密码主管进行身份认证。

9 软件 / 固件安全

CMMST-KPBMC 满足 GM/T 0028 -2014 7.5 对安全一、二级的技术要求。

10 运行环境

CMMST-KPBMC 运行于可修改的运行环境，需满足 GM/T 0028 -2014 7.6 对安全二级的技术要求。

MST-CC、SS-CC 以及 TPSS-CC 的软件模块须运行在独立的进程空间中，依托操作系统的访问控制机制。

11 物理安全

MST-CC 不涉及物理安全。

SS-CC、TPSS-CC 中的服务器密码机需满足 GM/T 0028 -2014 7.7 安全二级技术要求。

12 非侵入式安全

MST-CC 不涉及非侵入式安全。

SS-CC、TPSS-CC 中的服务器密码机满足 GM/T 0028 -2014 7.8 安全二级技术要求。

13 敏感安全参数管理

CMMST-KPBMC 敏感安全参数（SSP）包括：

d_{A1}——用户 MST-CC 私钥分量

d_{A2}——用户 SS-CC 私钥分量

d_{A3}——用户 TPSS-CC 私钥分量

P_A——用户公钥

PPD——用户个人特征数据

遵照 GM/T 0028-2014 7.9.1 要求，CMMST-KPBMC 对以上敏感安全参数进行管理。

（1） 关键安全参数（CSP）d_{A1}、PPD 在 MST-CC 内保护，防止非授权的访问、使用、泄露、修改

和替换。

（2） 关键安全参数（CSP）d_{A2}、d_{A3}在服务器密码机中生成，防止非授权的访问、使用、泄露、修改和替换。

（3） 公开安全参数（PSP）P_A在保存在 MST-CC 内，防止非授权修改和替换。

（4） 使用移动应用用户 PPD 与 d_{A1}使用相关联。

（5） 使用服务器密码机硬件 Token（令牌）将密码主管角色与 d_{A2}、d_{A3}相关联。

13.1随机比特生成器

满足 GM/T 0005-2012 随机性检测要求。

13.2敏感安全参数的生成

CMMST-KPBMC 敏感安全参数遵照 GM/T 0028－2014 7.9.3 要求生成。

（1） d_{A1}、d_{A2}、d_{A3}分别在 MST-CC、SS-CC、TPSS-CC 中生成。

（2） 密钥双端协同计算架构公钥 P_A在移动端生成。

（3） 密钥三端协同计算保护架构公钥 P_A在服务端生成。

（4） PPD 由 MST-CC 接收用户输入生成。

13.3敏感安全参数的建立

CMMST-KPBMC 敏感安全参数遵照 GM/T 0028—2014 7.9.4 要求建立。

13.4敏感安全参数的输入输出

CMMST-KPBMC 敏感安全参数遵照 GM/T 0028－2014 7.9.5 要求输入输出。

（1） d_{A1}、d_{A2}、d_{A3}不输出到密码模块外。

（2） PPD 输入防护须采用输入试错锁定机制，设置试错次数。

13.5敏感安全参数的存储

CMMST-KPBMC 敏感安全参数遵照 GM/T 0028－2014 7.9.6 要求存储。

（1） d_{A1}、d_{A2}、d_{A3}分别在MST-CC、SS-CC、TPSS-CC中存储。

（2） 至少使用PPD对d_{A1}进行（加密）保护。

（3） 使用服务器密码对d_{A2}、d_{A3}进行（加密）保护。

（4）d_{A2}、d_{A3}应实现禁用或者销毁。

13.6敏感安全参数置零

遵照 GM/T 0028－2014 7.9.7 要求，CMMST-KPBMC 没有未受保护的敏感安全参数，不需置零操作。

14 自测试

CMMST-KPBMC 除满足 GM/T 0028 -2014 7.10 对安全二级的技术要求外，还符合以下要求：

（1） 在协同生成用户私钥的同时，应生成自测试密钥。

（2） 软件每次启用、测试网络连通性后，应当对随机数进行自测试。

（3） 软件每次启用、测试网络连通性后，应当使用自测试密钥进行功能自测试。

15 生命周期保障

符合密钥多端协同计算技术架构的密码模块需满足 GM/T 0028 -2014 7.11 对安全二级的技术要求。

16 对其他攻击的缓解

符合密钥多端协同计算技术架构的密码模块需满足 GM/T 0028 -2014 7.12 对安全二级的技术要求，本技术框架对于 GM/T 0028 -2014 未定义的其他攻击不提供缓解机制。

附录 A
（资料性附录）
应用示例（移动智能终端数据签名系统）

A.1 应用需求

在满足国家和行业合规要求基础上，解决移动智能终端硬件密码模块成本高、携带不方便的问题。

A.2 密码模块应用架构

CMMST-KPBMC 应用部署架构如图 3 所示：

（1） CMMST-KPBMC 移动端密码组件（MST-CC）为移动智能终端移动应用 APP 提供密码服务 API-SDK。

（2） CMMST-KPBMC 服务端密码组件（SS-CC）与应用系统进行业务对接。

（3） SS-CC 使用服务器密码机进行多方密钥协同运算。

（4） 当移动应用需要对数据进行签名时，用户通过输入指纹（或 PIN 码）启动 MST-CC 与 SS-CC 进行协同计算电子签名。

（5） 在对 PC 端的认证及签名应用时，通过移动应用 app 扫码 PC 浏览器，再输入指纹（或 PIN 码）进行确认，实现密码认证及签名功能。

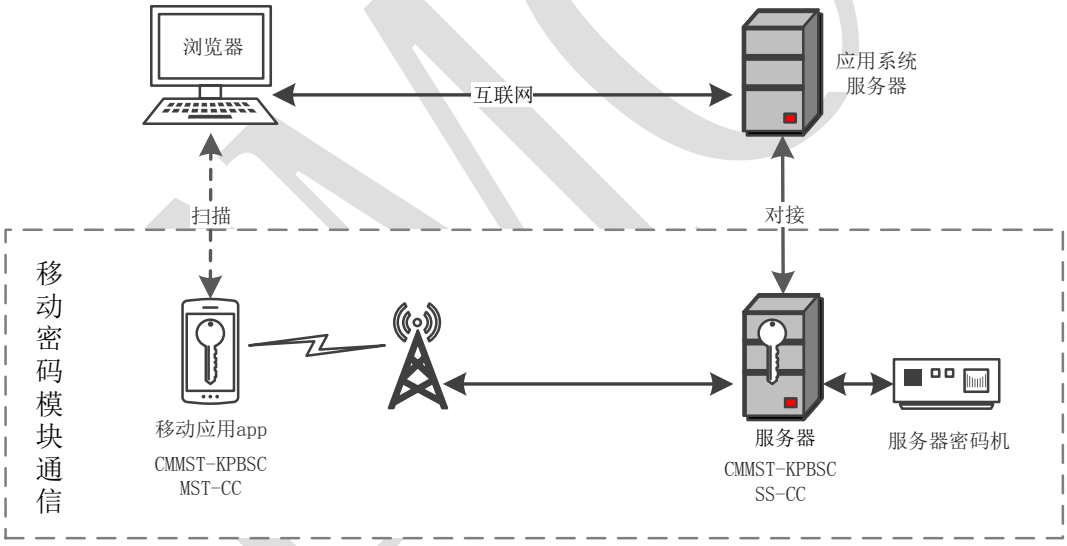

图 3 CMMST-KPBMC 应用架构

A.3 适用场景

A.3.1 手机银行

银行集成 CMMST-KPBMC，可通过在手机上刷指纹方式实现转账，其安全性与使用外置硬件密码设备相同。CMMST-KPBMC 对用户数字签名私钥进行协同计算保护，通过多方联合计算形成数字签名，完成带有数字签名的、符合金融行业标准要求的移动端大额转账。

A.3.2 OA 办公

可用 CMMST-KPBMC 实现 OA 办公登录系统、流程审批等密码应用。

用户登录 OA 系统时，可使用手机对着电脑屏幕进行扫码，再输入指纹确定，可完成用户身份鉴别登录 OA 系统，这时的多因素的强身份认证是由 CMMST-KPBMC 完成的。

在 OA 流程审批过程中，如用户在 PC 上签署“同意此项申请”，就可用手机扫码方式，在手机端书写审批意见，再输入指纹确认，这时的 PC 上的审批意见经过用户电子签名，保证审批意见不可伪造、不可抵赖。

A.3.3 互联网金融

在互联网金融中，如保险、理财等产品，需要在手机端签署电子合同。CMMST-KPBMC 使用第三方 CA 的数字证书，实现对合同原始数据，包括个人身份信息、签字、现场拍照、录像等信息进行数字签名，这些信息的数字签名符合《电子签名法》，可作为司法证据。

附录 B
（参考性附录）
SM2 双端协同计算流程示例

B.1 协同密钥生成流程

本流程生成的用户私钥符合 GMT 0003.2-2012 SM2 椭圆曲线公钥密码算法要求。

符号定义：

d_{A1}、d_{A2}——用户 A 的 MST-CC 私钥分量、SS-CC 私钥分量

P_A——用户 A 公钥

错误!未找到引用源。所示 MST-CC 和 SS-CC 协同密钥生成流程：

1) MST-CC向SS-CC发送密钥生成请求-CC；
2) SS-CC生成移动应用用户ID，生成签名密钥对，产生签名私钥分量d_{A2}，计算对应的公钥分量P_{A2}，服务器密码机加密保存d_{A2}；
3) SS-CC将用户ID，P_{A2}发送给MST-CC；
4) MST-CC保存用户ID，产生签名私钥分量d_{A1}，计算完整的签名公钥P_A；
5) MST-CC用户输入PPD，并用该PPD参与运算对d_{A1}进行加密保存，将公钥P输出给移动应用。

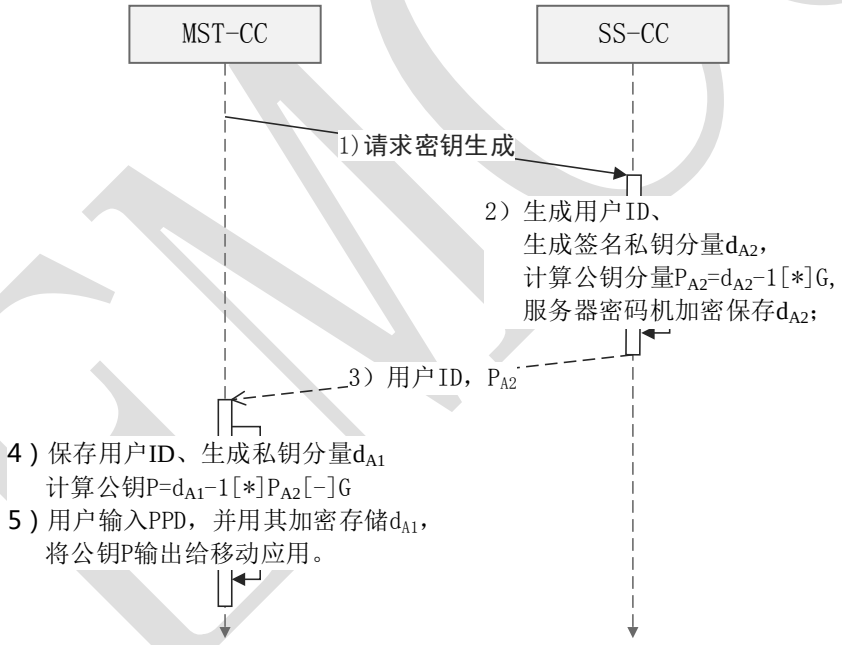

图 4 SM2 协同密钥生成流程

B.2 协同数据签名流程

本流程数据签名符合 GMT 0003.2-2012 SM2 椭圆曲线公钥密码算法要求。

符号定义：

d_{A1}、d_{A2}——用户 A 的 MST-CC 私钥分量、SS-CC 私钥分量

错误!未找到引用源。所示 MST-CC 和 SS-CC 协同签名流程：

1) MST-CC取出用户ID，计算签名数据摘要e，生成随机数k_1，并计算点乘数据Q_1；

2) MST-CC将用户ID，Q_1和e发送给SS-CC；
3) SS-CC生成随机数k_2、k_3，利用Q_1和消息摘要e，计算部分签名r，并根据用户ID取出SS-CC私钥分量d_{A2}，生成随机数k_2、k_3，计算部分签名s_2和s_3；
4) 发送r、s_2和s_3给MST-CC；
5) MST-CC用户确认签名信息后输入PPD，使用PPD恢复签名私钥分量d_{A1}，利用d_{A1}、r、s_2和s_3，得出签名值（r，s）。

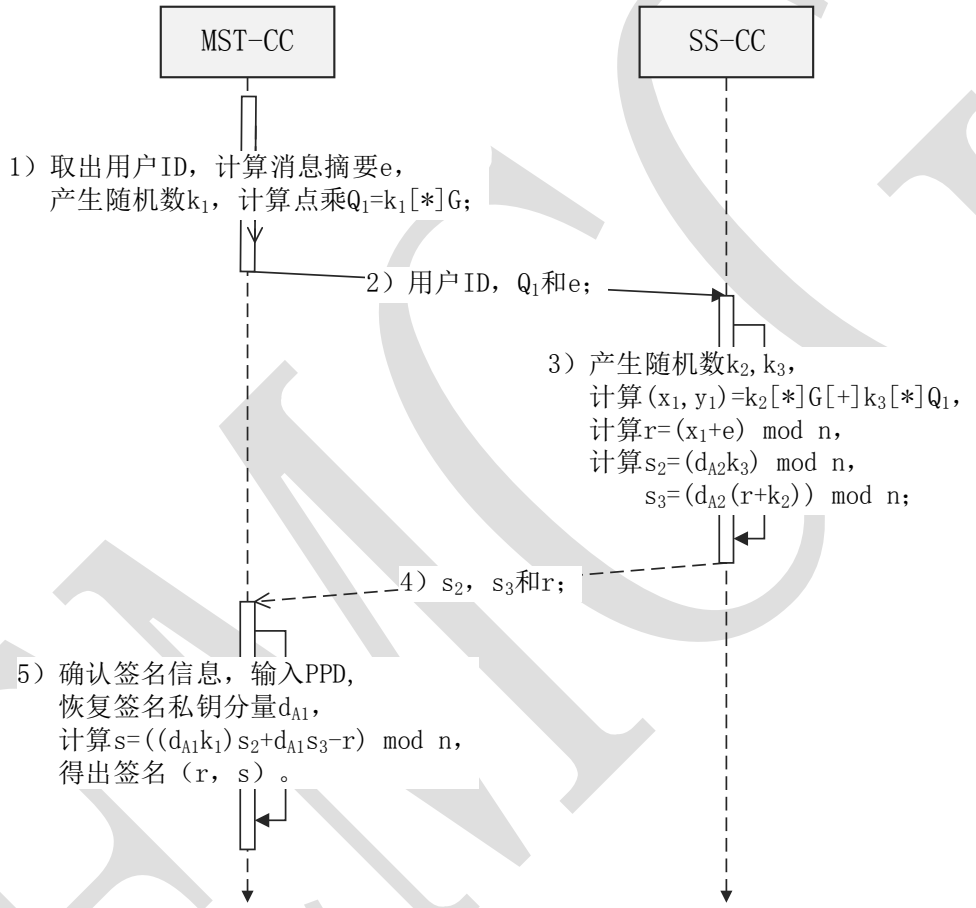

图 5 SM2 协同数字签名流程

B.3 协同数据解密流程

本流程数据解密符合 GMT 0003.2-2012 SM2 椭圆曲线公钥密码算法要求。

符号定义：

d_{A1}、d_{A2}——MST-CC 私钥分量、SS-CC 私钥分量

如**错误!未找到引用源。**所示 MST-CC 与 SS-CC 协同数据解密流程：

1) MST-CC从密文C中提取C_1；
2) MST-CC生成随机数k，利用k计算T_1，发送T_1到SS-CC；
3) SS-CC利用d_{A2}、T_1，计算得到部分明文T_2，并发送T_2回MST-CC；
4) MST-CC用户输入PPD；

5) MST-CC利用PPD恢复私钥分量d_{A1}，

6) 利用私钥分量d_{A1}和T_2进行解密，得出明文T。

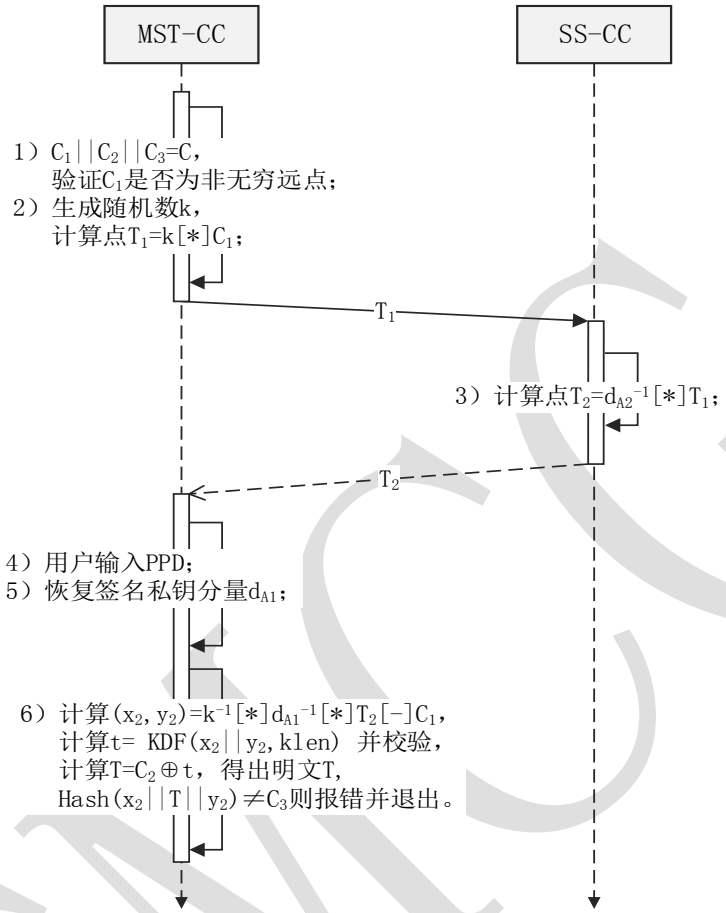

图 6 SM2 协同数据解密流程

附录 C
（参考性附录）
SM2 三端协同计算流程示例

C.1 三端协同密钥产生流程

本流程生成的用户私钥符合 GMT 0003.2-2012 SM2 椭圆曲线公钥密码算法要求。

符号定义：

d_{A1} 、d_{A2} 、d_{A3}——分别为用户 A 的 MST-CC、SS-CC、TPSS-CC 私钥分量

P_A——用户 A 公钥

f()——SM2 椭圆曲线的单向函数

P()——公钥产生函数

Q_{Ai}——用户 A 公钥分量

三端协同密钥产生流程如图7所示：

7) MST-CC 输入用户 PPD，产生私钥分量 d_{A1}、Q_{A0}；
8) 计算 $Q_{A1}=f(Q_{A0}, d_{A1})$，将 PPD、Q_{A1} 传递给 SS-CC；
9) SS-CC 根据 PPD 生成用户 ID，产生私钥分量 d_{A2}，密码机加密保存 d_{A2}；
   计算 $Q_{A2}=f(Q_{A1}, d_{A2})$；将用户 ID、Q_{A2} 传递给 TPSS-CC；
10) TPSS-CC 产生私钥分量 d_{A3}，密码机加密保存 d_{A3}；
    计算 $Q_{A3}=f(Q_{A2}, d_{A3})$；
    产生公钥 $P_A=P(Q_{A3})$并验证公钥合法；
11) 如公钥不合法，重新生成 d_{A3}；
12) TPSS-CC 将 P_A 传递给 SS-CC；
13) SS-CC 将 P_A、用户 ID 传递给 MST-CC；
14) 使用 PPD 对 d_{A1} 进行（加密）保护，将用户公钥 P_A 输出给移动应用。

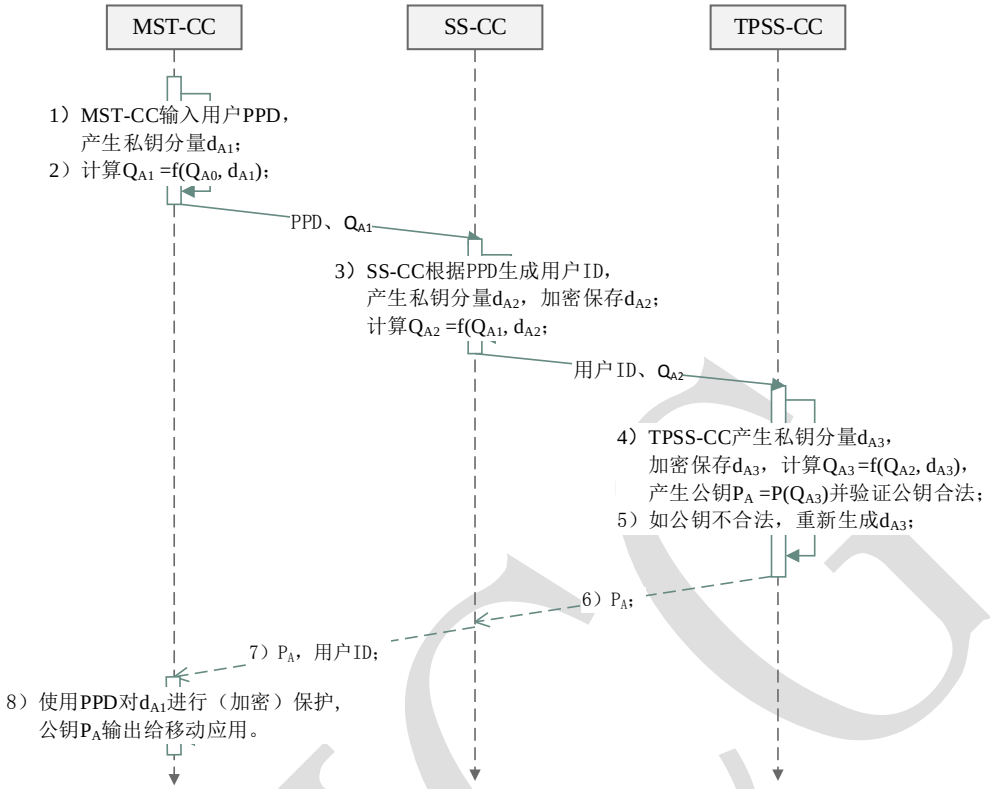

图 7 三端协同密钥产生流程

C.2 三端协同数据签名流程

本流程数据签名符合 GMT 0003.2-2012 SM2 椭圆曲线公钥密码算法要求。

符号定义：

d_{A1} 、d_{A2} 、d_{A3}——分别为用户 A 的 MST-CC、SS-CC、TPSS-CC 私钥分量

fr()——单向函数

fs()——安全函数

R_0、S_4——初值、常数

fk()、g()——表达函数

三端协同数据签名流程如**错误!未找到引用源。**所示：

6) MST-CC取出用户ID，计算签名数据摘要e，产生随机数K_1；

7) 计算R_1= fr (R_0,K_1)，将用户ID，e,和R_1发送给SS-CC；

8) SS-CC产生随机数K_2，计算R_2= fr(R_1, k_2)，将用户ID，e和R_2发送给TPSS-CC；

9) TPSS-CC产生随机数K_3，计算R_3= fr(R_2, k_3)=(x_1,y_1)，r =x_1 + e mod n，根据用户ID查找并恢复私钥分量d_{A3}，计算S_3=fs(S_4, d_{A3}, K_3)，将r, S_3发送给SS-CC；

10)SS-CC根据用户ID查找并恢复私钥分量d_{A2}，计算:S_2=fs(S_3, d_{A2} , K_2)，将r, S_2发送给MST-CC；

11)MST-CC输入用户PPD，使用PPD恢复私钥分量d_{A1}，计算S_1=fs(S_2, d_{A1}, K_2)，得出签名值s = h(S_1, r)。

注：SM2_Sign(e, d_A, k) =(r, s)最终等效值，随机数可表达为：k =fk(K_1, K_2, K_3)，用户A私钥d_A可表达为： d_A= g(d_{A1}, d_{A2}, d_{A3}) 。

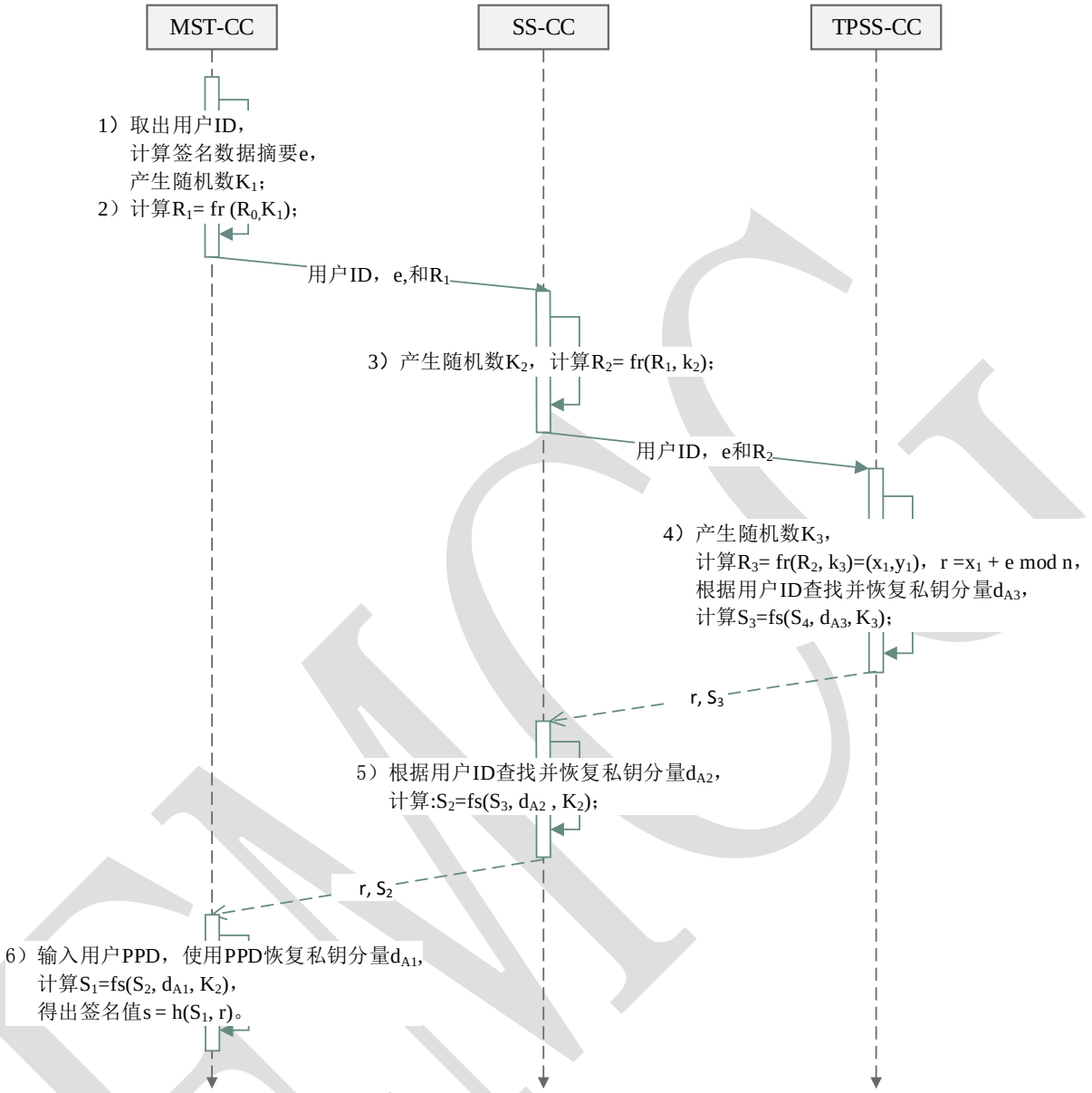

图 8 三端协同数据签名流程

参考文献

[1] GM/T 0029-2014 签名验签服务器技术规范

[2] GB/T 25069-2010 信息安全技术_术语