

Hyperledger Fabric 平台的国密算法嵌入研究

曹琪, 阮树骅, 陈兴蜀, 兰晓, 张红霞, 金泓健

(1. 四川大学网络空间安全学院, 四川 成都 610065;
2. 四川大学网络空间安全研究院, 四川 成都 610065)

摘要: Hyperledger Fabric 是企业级商用区块链项目提供支撑的且可扩展的联盟链平台, 密码算法为该平台的核心, 保证上链数据的安全和不可篡改, 但原始 Fabric 平台缺乏对国密算法的支持。因此, 设计并实现了 Fabric 平台的国密算法的嵌入和支持。首先, 通过分析 Fabric 平台中组件间交互逻辑和密码算法的调用场景, 提出了在该平台嵌入国密支持的设计思路; 其次, 基于同济开源国密实现源码, 为 Fabric 平台 BCCSP 添加 SM2、SM3 和 SM4 算法模块与接口; 再次, 将 Fabric 平台的各组件上层应用的密码算法调用接口与对应国密算法接口相关联, 实现上层应用对国密算法调用的支持; 最后, 通过创建 fabric-gm 联盟链测试实例验证 Fabric 平台中嵌入的国密算法模块和接口的正确性及有效性, 并与原生 Fabric 平台镜像构建的测试实例进行了性能比较。实验结果表明, 嵌入的国密算法模块和接口可用、正确且生成的国密证书有效, 与原生 Fabric 平台镜像相比, 网络启动时间增加 3%, 毫秒级单位下的交易时间开销增加 1 倍, 动态证书生成时间增加 9%, 各项性能指标均在可接受范围内。

关键词: 区块链; Hyperledger Fabric; SM2; SM3; SM4

中图分类号: TP309.2

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2021007

Embedding of national cryptographic algorithm in Hyperledger Fabric

CAO Qi, RUAN Shuhua, CHEN Xingshu, LAN Xiao, ZHANG Hongxia, JIN Hongjian

1. School of Cyber Science and Engineering, Sichuan University, Chengdu 610065, China
2. Cybersecurity Research Institute, Sichuan University, Chengdu 610065, China

Abstract: Hyperledger Fabric is an extensible alliance blockchain platform and provides support for enterprise-level commercial blockchain projects. The cryptographic algorithm is the core technologies of the platform, ensuring the security and non-tampering of the data on the chain. But the original Fabric platform lacks the national

收稿日期: 2020-05-24; 修回日期: 2020-09-18

通信作者: 阮树骅, ruanshuhua@scu.edu.cn

基金项目: 国家自然科学基金(61802270); 中央高校基础研究经费(SCU2018D018, 2019SCU12069)

Foundation Items: The National Natural Science Foundation of China(61802270), The Fundamental Research Funds for the Central Universities(SCU2018D018, 2019SCU12069)

论文引用格式: 曹琪, 阮树骅, 陈兴蜀, 等. Hyperledger Fabric 平台的国密算法嵌入研究[J]. 网络与信息安全学报, 2021, 7(1): 65-75.

CAO Q, RUAN S H, CHEN X S, et al. Embedding of national cryptographic algorithm in Hyperledger Fabric[J]. Chinese Journal of Network and Information Security, 2021, 7(1): 65-75.

cryptographic algorithm support. The embedding and support of the national cryptographic algorithm of the Fabric platform was designed and implemented. Firstly, the interaction logic of between components and the invocation scenario of each type of cryptographic algorithm in the Fabric platform were analyzed, an idea of embedding national cryptographic algorithm support for the platform was proposed. Secondly, the modules and interfaces for SM2, SM3 and SM4 were added to BCCSP of the Fabric platform based on the open source code of national cryptographic algorithm implementation. Thirdly, the interface of cryptographic algorithm invoked by the upper layer of each component is associated to the interface of corresponding national cryptographic algorithms, which realized the invocation support of national cryptographic algorithm for the upper layer applications. Finally, the correctness and effectiveness of the embedded national cryptographic algorithm were verified by creating a fabric-gm test instance. And compared with the performances of the test instance built by the mirror of the native Fabric platform. The experimental results show that the embedded national cryptographic algorithm interfaces are corrected and the generated national cryptographic certificates are effective. Moreover, compared with the native Fabric platform, the network start up time increases by about 3%. In the millisecond unit, the transaction time cost increases by about one time, the dynamic certificate generation time increases by about 9%, and all the performance are within the acceptable range.

Keywords: blockchain, Hyperledger Fabric, SM2, SM3, SM4

1 引言

Hyperledger Fabric^[1] (简称 Fabric 平台) 是由 IBM 牵头、旨在为企业级商用区块链应用场景打造的许可分布式账本支撑平台, 也是目前联盟链^[2]的典型代表。在克服了公有链吞吐量低^[3]、交易公开而导致的无隐私性和私有链^[4]的强中心化等问题的同时, 它以模块化和可插拔的特性, 可向上提供高度的机密性、灵活性及可扩展性^[5], 使 Fabric 平台满足广泛行业的商业应用诉求。密码技术是 Fabric 平台实现的核心技术之一, 是 Fabric 上层应用开发的基础支撑技术。基于密码技术, Fabric 实现了一种基于证书的身份管理与一种“执行-排序-验证”并行执行的新交易模式, 保证了对链上的每一步操作进行严格的身份与权限验证, 进而保证该平台上数据的安全与不可篡改。但目前原生的 Fabric 平台仅支持通用的国际密码算法, 缺乏对国家密码算法 (简称国密算法) 支持。同时, 我国政府和技术监管和自主可控方面对从事区块链系统建设、服务运营的机构提出了国密算法规范要求^[6], 因此, 将我国自主研发的国产密码算法嵌入 Fabric 平台显得尤为必要。

目前, 已有国内学者或机构主要针对 Hyperledger Fabric 1.0 开展了 SM2^[7-8]、SM3^[9-10]等国密算法的嵌入工作。其中, 具有代表性的是苏州同济区块链研究院^[11]开源的 Fabric 1.0 的国

密嵌入代码。在此基础上, 张青禾^[12]基于支持国密的 Fabric1.0 提出了一种隐私保护方案。张梦一^[13]基于支持国密的 Fabric1.0 实现了一种通用积分管理系统。但上述工作仅针对 Fabric 平台的部分组件进行了针对性应用的国密嵌入支持, 不具有通用性, 且未实现整个平台的国密算法支持, 无法支持广泛的商用应用。

本文通过分析 Fabric 平台组件间交互逻辑与密码算法的调用场景, 提出了 Fabric 平台国密算法嵌入的设计思路, 对 Fabric 平台核心组件区块链密码服务提供者^[1] (BCCSP, blockchain cryptographic service provider) 嵌入国密 SM2、SM3 及 SM4^[14]算法模块与接口, 并将 Fabric 平台各组件的上层密码调用关联到国密算法接口, 进而实现了 Fabric 平台的国密算法支持。

2 相关工作

2.1 Fabric 平台架构及组件间交互逻辑

Fabric 平台由 Fabric 联盟链网络^[15]、Fabric-CA^[16]以及 Fabric-SDK^[17]3 部分组成, 组件间交互逻辑如图 1 所示, 展示了 Fabric 联盟链网络典型的交易流程。

1) Fabric 联盟链网络^[1,15]是 Fabric 平台的核心组成部分, 依赖于底层密码算法为上链数据提供不可篡改等特性。

2) Fabric-CA^[16]是 Fabric 平台的证书颁发机

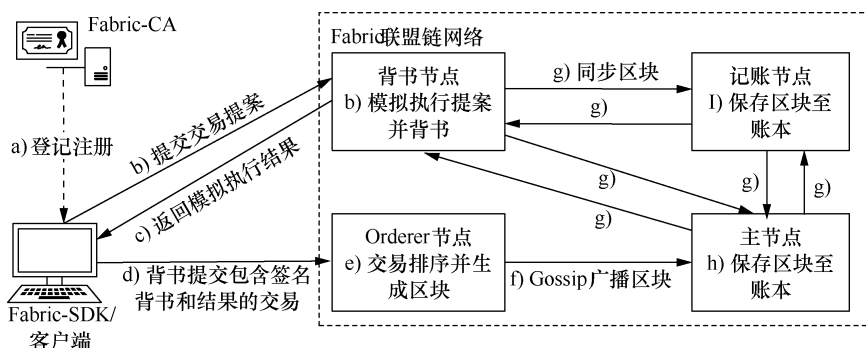


图1 Fabric 平台组件间交互逻辑图
Figure 1 The interaction logic between components in the Fabric

构,用于网络成员身份证书的动态管理,包括证书的动态颁发与吊销等。

3) Fabric-SDK^[17]是为开发人员编写和测试链码应用程序提供的一个结构化、可配置的库环境,并作为 Fabric 平台的客户端。

从图 1 可以看出, Fabric-SDK 向 Fabric-CA 进行网络成员动态身份证书的注册,并向 Fabric 联盟链网络发起交易等操作。在交易处理的每个环节上都会进行签名验签操作,并对交易信息进行权限与格式检查,需要大量调用密码算法。因此,为了实现 Fabric 平台对国密算法的支持,需要分别实现 Fabric 联盟链网络、Fabric-CA 及 Fabric-SDK 对国密算法的支持。

这里需要强调的是关于网络成员身份证书的动态管理问题, Fabric 本身维护了一个在网络启动时用于静态生成节点证书的二进制证书生成工具 **cryptogen**,通过该工具可生成各节点证书,从而实现对任何上链操作的身份验证,但是在系统要求动态添加节点用户时,该方式存在反复修改配置文件并重启网络更新配置的问题。故在实际应用中,可使用 Fabric-CA 代替 **cryptogen** 证书生成方式,实现动态管理 Fabric 联盟链网络中节点身份证书,进而为 Fabric 平台提供可动态颁发与吊销的动态成员管理功能。

2.2 Fabric 联盟链网络的安全与密码服务

Fabric 联盟链网络技术架构如图 2 所示,与本文研究工作关系最为密切的是区块链密码服务提供者 **BCCSP**^[1]模块,基于 **BCCSP** 可实现 Fabric 联盟链网络共同的安全与密码服务,为上层应用提供安全的、可插拔的成员身份管理(MSP, membership service provider)、共识服务和链码服务^[18]。

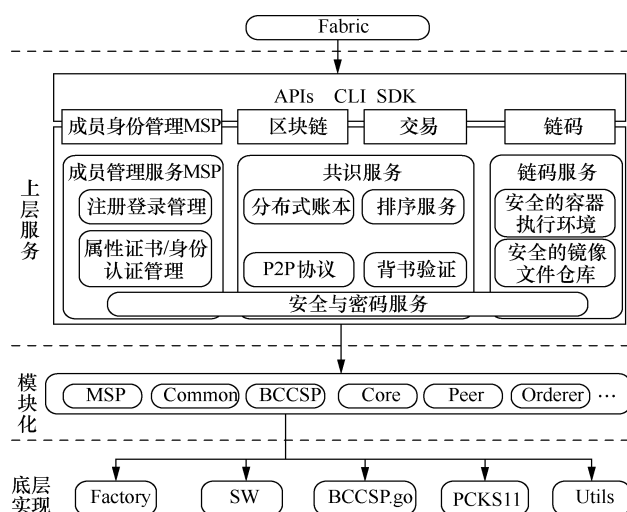


图2 Fabric 联盟链网络技术架构
Figure 2 The technology architecture of the Fabric alliance chain network

BCCSP 模块封装了基于软件实现的 **SW** 和基于硬件实现的 **PCAS11** 两类 **BCCSP** 实例,每类实例提供包括密钥的生命周期管理、哈希、签名验证及加解密等 4 大类功能接口供上层服务调用。**BCCSP** 模块支持的密码算法主要有哈希密码算法、对称密码算法和非对称密码算法 3 类,各类密码算法支持的应用场景如图 3 所示,可通过 **CSP** 选项来指定 **BCCSP** 选取的实例,如国密算法实例,从而为上层应用提供相应的国密算法调用的支持。为了在 Fabric 联盟链网络中嵌入国密支持,首先需要在 **BCCSP** 底层实现中嵌入基于国密的 **BCCSP** 实例,并提供国密 **SM3**、**SM2** 和 **SM4** 的功能接口,其次需要将上层应用的密码算法调用接口与国密接口关联,从而最终实现基于国密的 Fabric 联盟链网络共同的安全与密码服务。

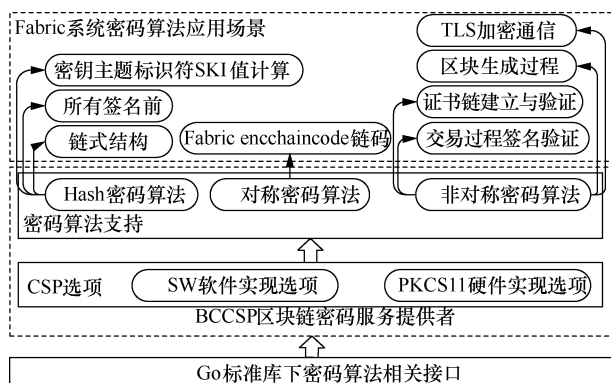


图3 Fabric平台支持的密码算法及使用场景
Figure 3 Cryptographic algorithms support and usage scenarios in the Fabric

3 Fabric平台国密算法嵌入设计思路

本文将嵌入了国密支持的 Fabric 平台称为 Fabric-gm, 具体的 Fabric-gm 平台实现过程同时考虑了 Fabric-gm 联盟链网络、Fabric-CA-gm 和 Fabric-SDK-gm 三类组件的国密嵌入实现, 国密算法嵌入设计思路如图 4 所示, 主要工作有以下 4 个部分。

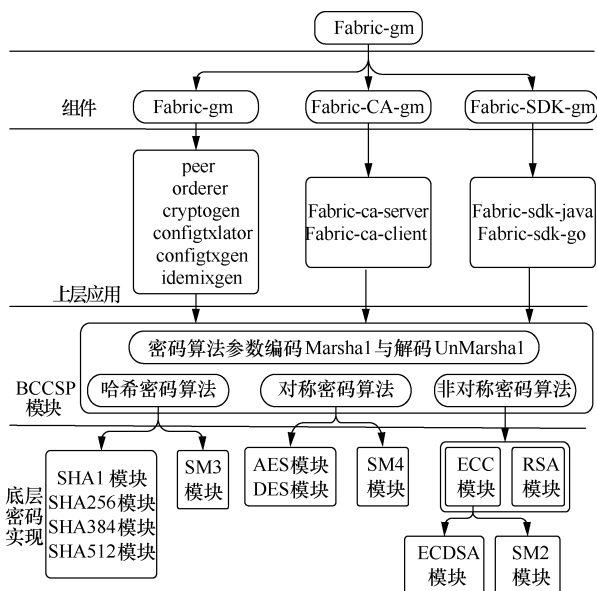


图4 Fabric平台国密算法嵌入设计思路
Figure 4 The embedding scheme of the GM in the Fabric

1) 基于 Go 标准的底层国密算法嵌入: 可依据 SM 系列国密算法的标准规范文件, 设计并实现基于 Go 标准的国密算法, 包括常用的加解密算法 (SM4、SM2)、哈希算法 (SM3) 以及签名验签算法 (SM2) 等。在这部分工作中, 本文对

开源实现(指同济区块链研究院对国密 SM2、SM3 和 SM4 算法的开源实现)的底层国密算法实例^[19]进行了正确性验证, 并在 BCCSP 模块的国密实例中采用了该算法实例。

2) BCCSP 模块的国密算法接口嵌入: 分别在 BCCSP 模块的哈希算法子模块、对称密码算法子模块和非对称密码算法子模块下, 添加相关的国密 SM3 模块、SM4 模块和 SM2 模块的调用接口。

3) 上层应用的国密算法接口嵌入: 在上层程序与应用中, 添加相关的国密算法接口调用, 将原哈希、签名验签等密码算法接口与国密 SM3、SM2 算法接口关联, 以实现上层应用对国密算法调用的支持。

4) 对嵌入国密算法及相关调用接口后的 Fabric 平台源码进行编译, 形成支持国密算法的可执行文件, 并打包成 Fabric-gm 镜像文件, 部署支持国密算法的 Fabric-gm 平台, 通过基于国密接口的加解密、签名验签及哈希对比等实验验证所嵌入的国密算法的正确性、可用性和有效性。

4 Fabric平台国密算法嵌入实现

4.1 Fabric 联盟链网络国密算法嵌入实现

4.1.1 BCCSP 国密算法相关接口实现

Fabric 联盟链网络 BCCSP 模块国密算法相关接口实现如图 5 所示。将基于同济实现的底层国密算法 GSM 代码封装成支持国密算法的 BCCSP 实例, 即在 CSP 选项添加 GM 软件实现选项并在该选项下添加 bccsp-gm 实例, 提供 SM2 非对称加密算法选项 (用于数字签名及验证)、SM3 哈希算法选项、SM4 对称加密算法选项以及与 X.509 证书相关的各类国密算法与服务支持的接口, 如图 5 所示。特别地, 国密证书生成和国密证书与密钥转换接口, 不仅提供了已封装的国密证书生成接口, 还提供了将 X.509 证书和密钥转换成 SM2 国密证书和密钥的接口。

4.1.2 Fabric 联盟链网络上层应用国密算法调用支持

Fabric 联盟链网络上层应用的国密算法支持主要分为网络启动过程和交易流程的国密算法调用支持两个部分。

网络启动过程要求证书生成工具 cryptogen

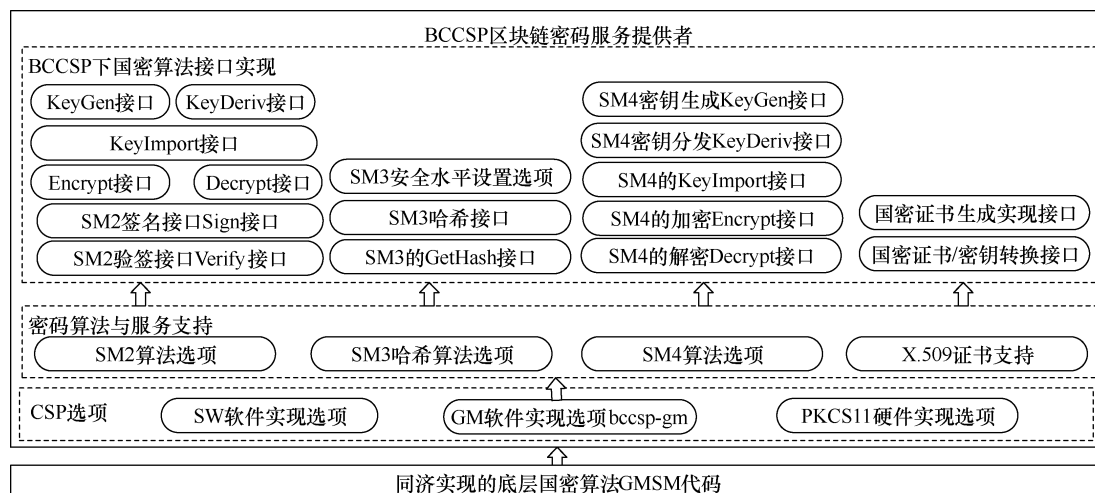


图5 BCCSP 国密算法接口实现示意
Figure 5 The GM interface implementation for BCCSP

能够为对应的网络节点生成国密身份证书与密钥。因此,相关的国密算法调用支持主要包括以下内容:

1) 修改 example 和 sampleconfig 文件下的网络结构配置参数,保证其 BCCSP 实例指向 BCCSP-gm 实例;

2) 修改 common 文件下 CA 结构体、证书生成与加载及 MSP 证书链,保证能够生成支持国密的 cryptogen,进而为各网络节点生成对应的国密身份证书与密钥。

交易流程要求对一次完整交易中涉及的交易发起、执行、不同类型网络节点签名与验签、通道管理、账本管理、区块生成、基于 Gossip 的区块分发、链码调用等处理操作都进行基于国密的身份与权限验证。因此,相关的国密算法调用支持主要包括以下内容。

1) Common 模块: 在 channel.go 中添加国密 SM3 算法的调用支持,在 csp.go 中添加 SM2 的密钥获取方法,保证默认密钥加载选项指向国密 SM2 接口。

2) Core 模块: 在 server.go 中添加国密 X.509 格式的证书解析方法。

3) MSP 模块: 在 cert.go 中添加国密 X.509 格式的证书反序列化方法,在 identities.go 添加指向 SM3 哈希算法的实现。

4) Common、Core、MSP、Peer、Orderer、Gossip 等模块的密码算法调用修改指向 bccsp-gm

提供的国密接口,从而实现各上层应用的国密算法调用支持。

将 4.1.1 节和 4.1.2 节修改后的源码重新编译,生成支持国密的二进制文件,并打包生成用于环境部署的 Fabric-gm 镜像文件,从而实现国密支持嵌入。

4.2 Fabric-CA 国密算法嵌入实现

4.2.1 Fabric-CA 的国密算法接口实现

首先,在 Fabric-CA 组件的 lib 文件下添加国密 CA 验证方法,新添 gmca.go 文件,该文件封装了基于国密算法的签名、证书生成、证书请求与转换等国密 GM 实现方法与接口。

同时,修改 Fabric-CA 客户端和服务端的 config.go 配置文件的 BCCSP 的 default 和 CSR 选项字段需要指向国密 GM 实例和新国密接口。

此外,在 Fabric-CA 组件中的 util 文件下添加基于国密算法的证书与密钥管理方法,添加的方法如图 6 所示,并修改令牌创建与验证代码,为 Fabric-CA 上层应用对国密算法接口的调用提供支持。

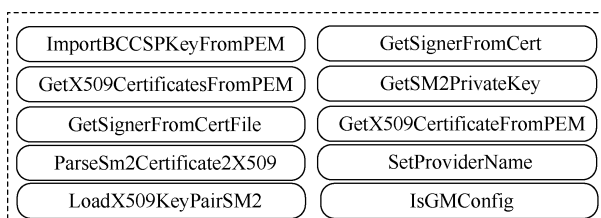


图6 fabric-CA 组件下 util 文件新添方法示意
Figure 6 The new methods added to the util file

4.2.2 Fabric-CA 上层应用国密算法调用支持

Fabric-CA 动态证书申请流程如图 7 所示, 上层应用的国密算法调用支持主要包括以下 4 个阶段。



图 7 Fabric-CA 动态证书申请流程
Figure 7 The flowchart of dynamic certificate application for the Fabric-CA

1) Fabric-CA 服务器初始化启动阶段的国密算法调用支持。

2) Enroll (注册) 管理员注册阶段的国密算

法调用支持。

3) Register (用户登记) 阶段的国密算法调用支持。

4) Enroll (注册) 普通用户注册阶段的国密算法调用支持。

Fabric-CA 服务器初始化启动阶段国密调用流程如图 8 所示, 图上虚线箭头表示间接调用, 实线箭头表示直接调用, 灰色背景部分为新添的国密算法调用支持, 以 CA 服务器初始化部分为例, 通过修改证书有效性检测、根密钥生成以及添加 CA 部分调用的接口或方法, 可实现将该 CA 指向 BCCSP-gm 及新添的国密证书与密钥处理方法, 进而实现该部分对国密算法的调用支持。通过对注册处理程序和监听与服务部分进行类似的操作, 最终可实现该阶段的国密调用支持。

Enroll (注册) 阶段的国密算法调用流程如图 9 的 Enroll 操作部分所示, 该阶段主要涉及管理员注册和用户注册。因此, 该阶段的操作主要有:

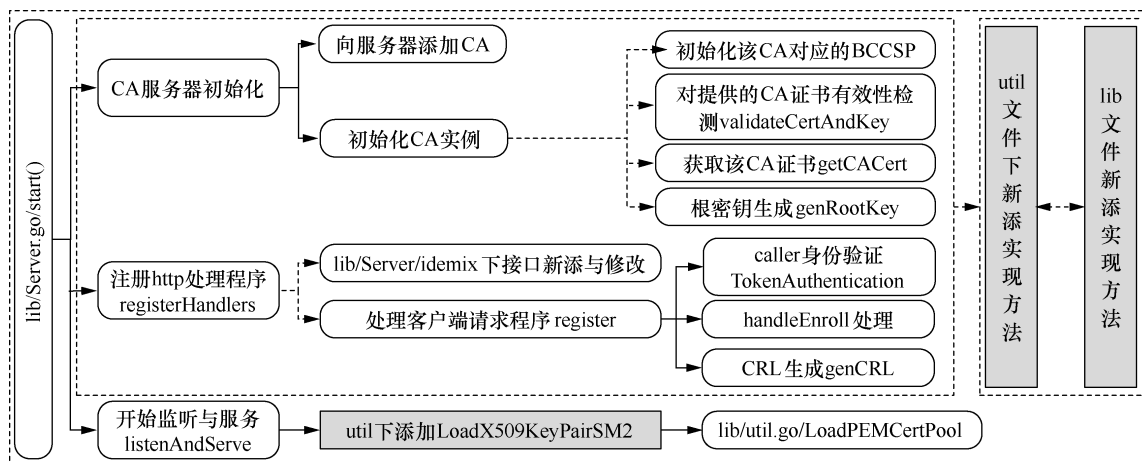


图 8 Fabric-CA 服务器初始化启动阶段的国密调用流程
Figure 8 The invoking flowchart of the GM during the Fabric-CA initial phase

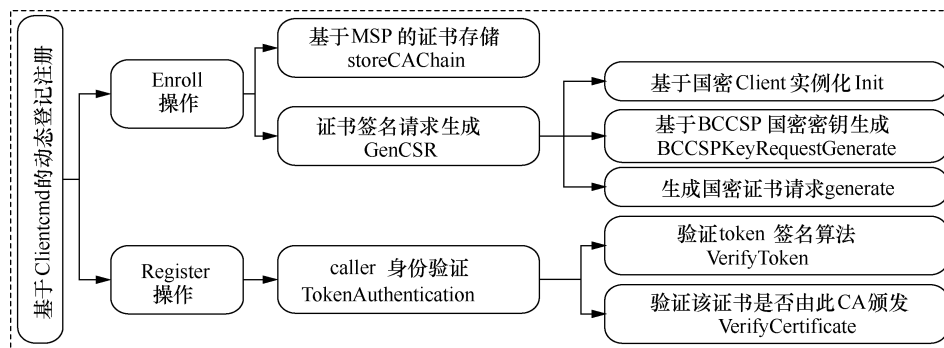


图 9 Enroll 与 Register 国密调用流程
Figure 9 The invoking flowchart of the GM during the enroll and register phase

① 实例化支持国密的 Fabric-CA 客户端；② 修改 CSR 的生成代码和基于 MSP 的证书存储代码；③ 修改图 9 中注册阶段所涉及的函数以及相关函数中的子调用，添加对国密算法相关接口的调用，从而实现对国密密钥/证书请求与生成的支持。

Register（用户登记）阶段的国密算法调用流程如图 9 的 Register 操作部分所示，该阶段仅在管理员身份验证部分存在密码算法的调用，因此，直接修改图 9 中 Register 操作下调用函数及其子调用，添加对国密算法相关接口的调用，就能够实现基于国密的通信凭证 token 创建、签名及证书验证等操作。

5 功能测试与性能分析

本文所有实验均在虚拟化环境下进行。宿主机配置: Win10 x86_64、Intel Core i5-8400 CPU @ 2.80 GHz 2.81 GHz。虚拟机配置: Ubuntu 16.04.05 x86_64, CPU 可用核数为 1, 内存 4 GB。

5.1 Fabric 联盟链网络国密算法嵌入实现

5.1.1 国密算法接口测试

国密算法接口测试对 Fabric-gm 平台上 BCCSP 下添加的国密 SM3、SM4 及 SM2 接口的可用性和有效性进行评估,测试实验如下。

(1) SM3 哈希算法接口测试

首先，进行 Fabric-gm 平台上 SM3 哈希算法接口调用可用性验证，验证上层应用调用的哈希算法指向国密 SM3 哈希算法接口。图 10 的长方形框内显示了 Fabric-gm 平台默认的哈希选项为国密 SM3 哈希算法接口，即 Fabric-gm 平台上层应用调用的哈希算法指向了国密 SM3 哈希算法接口，使用国密 SM3 哈希算法进行签名验签及标识 ID 值计算等操作过程。



图 10 Fabric-gm 上的 SM3 哈希接口调用可用性验证
Figure 10 The verification of usability for SM3 interface

其次, 进行 Fabric-gm 平台上 SM3 哈希算法

接口有效性验证, 验证上层应用调用的国密 SM3 哈希算法计算的正确性。将测试消息设定为“Hello World”, 分别使用 GmSSL^[20]函数库和 Fabric-gm 平台的 SM3 哈希算法接口计算测试消息的哈希值, 比较计算结果。图 11(a)为基于 GmSSL 的 SM3 哈希函数计算得到的结果, 图 11(b)为基于 Go test 测试调用 BCCSP 下哈希算法接口的哈希计算结果, 由计算结果可知, 两者对同一测试消息计算的哈希结果一致, 因此, Fabric-gm 平台的 SM3 哈希算法接口是可用且有效的, 可被正确使用。

```
[root@localhost gm]# printf "Hello World" | gmsssl sm3
(stdin)= 77015816143ee627f4fa410b6dad2bdb9fcbdf1e061a452a686b8711a484c5d7
[root@localhost gm]#
```

(a) 基于GmSSL的SM3哈希函数计算结果

```
[root@localhost gm]# go test -v -run TestHasher
=== RUN TestHasher
=== PAUSE TestHasher
=== CONT TestHasher

Input data:Hello World 测试输入数据
=====gm/hasher=====
InitData:48656c6c6f20576f726c64原始数据对应hex/byte
hash:77015816143ee627f4fa410b6dad2dbb9fcbdf1e061a452a686b8711a484c5d7
--- PASS: TestHasher (0.00s) 哈希值
PASS
ok      github.com/hyperledger/fabric/bccsp/gm 0.005s
[root@localhost gm]#
```

(b) 基于Fabric-gm/BCCSP 下哈希算法接口的哈希计算结果

图 11 Fabric-gm 上的 SM3 哈希接口有效性验证

Figure 11 The verification of validity for SM3 in the Fabric-gm

(2) SM4 算法接口测试

验证 Fabric-gm 平台上 BCCSP 下添加的国密 SM4 算法接口的可用性和有效性。调用 BCCSP 下的 KeyGen 接口生成 SM4 算法密钥，再调用 SM4 的 Encrypt 接口和 Decrypt 接口进行数据的加解密操作。测试结果如图 12 所示，首先，SM4 密钥生成成功，其次，基于该 SM4 密钥对明文数据进行加解密操作，解密后数据与明文数据一致，因此，验证了 Fabric-gm 平台的 SM4 算法相关接口是可用且有效的，可被正确使用。

```
[root@localhost ~]# go test -v -run TestSM4KeyGenerator
=== RUN TestSM4KeyGenerator
=== PASS TestSM4KeyGenerator
=== CONT TestSM4KeyGenerator

KeyLen:32  密钥长度

K:{{203 191 219 38 179 236 114 236 87 16 174 213 197 215 103 229 255 137 62 188 219 154 174 186 199 30 34 17 247 212 223 218}} false)
          十进制制式的SM4密钥
SM4_privkey:{{203 191 219 38 179 236 114 236 87 16 174 213 197 215 103 229 255 137 62 188 219 154 174 186 199 30 34 17 247 212 223 218}}
    PASS: TestSM4KeyGenerator (0.00s)
PASS
ok   github.com/hyperledger/fabric/bccsp/gm 0.000s

[root@localhost ~]# go test -v -run TestSM4_Encrypt_Decrypt调用生成的SM4密钥进行加解密
=== RUN TestSM4_Encrypt_Decrypt
=== PASS TestSM4_Encrypt_Decrypt
=== CONT TestSM4_Encrypt_Decrypt

Key:{{203 191 219 38 179 236 114 236 87 16 174 213 197 215 103 229 255 137 62 188 219 154 174 186 199 30 34 17 247 212 223 218}}
          加载SM4密钥
Key:cbf6b26c3c72e257318aed5c0e767047f83b3c0e9a0ba6c71b6221137f4d6da 十六进制制式的SM4密钥
plaintext:abcdeghijklmnop 原始明文信息
Encrypted data:2037261a1eb39326f6f780d99  SM4加密后的密文信息

Decrypted data:abcdeghijklmnop 解密后数据
    PASS: TestSM4_Encrypt_Decrypt (0.00s)
PASS
ok   github.com/hyperledger/fabric/bccsp/gm 0.000s
```

图 12 Fabric-gm/BCCSP 上的 SM4 算法接口可用性和有效性验证结果
Figure 12 The verification of availability and validity for SM4 in the Fabric-gm/BCCSP

(3) SM2 算法接口测试

验证 Fabric-gm 平台上 BCCSP 下添加的国密 SM2 算法接口的可用性和有效性。调用 BCCSP 下 KeyGen 生成 SM2 算法密钥，再调用 signGMSM2 和 verifyGMSM2 接口进行签名验签操作。测试结果如图 13 所示，签名过程中的 R 值与验签过程中的 r 值相等，表明 BCCSP 下 SM2 算法相关接口被成功使用，因此，验证了 Fabric-gm 平台的 SM2 算法相关接口是可用且有效的，可被正确使用。

```
[root@localhost gm]# go test -v -run TestVerifySM2
=== RUN TestVerifySM2
=== PAUSE TestVerifySM2
=== CONT TestVerifySM2
msg: [104 101 108 108 111 32 119 111 114 108 106]
签名值: (R,S) 序列化后的值
sigma_R: [48 70 2 33 0 222 108 124 80 78 253 42 140 139 60 28 119 144 20 191 227 170 6 150 151 16 86 141 0 127 251 11
0 23 210 78 20 193 2 33 0 240 142 228 107 22 228 80 67 207 70 202 214 166 187 5 33 228 98 235 73 128 25 112 214 108
117 69 207 68 218 115 126]
签名中的R值
sigma_S: [10880755242847461857522794947656930126259853128903291063325679053792654029694
SmVerify_x(r): [1006051298501424444154379414366966799801623903390983898107186295950327276737]
签名中的S值
验签中的r值
Sign_Verify_Success: true
PASS: TestVerifySM2 (0.00s)
ok      github.com/hyperledger/fabric/bccsp/gm 0.009s
[root@localhost gm]#
```

图 13 Fabric-gm/BCCSP 上的 SM2 算法接口有用性和有效性验证结果
Figure 13 The verification of availability and validity for SM2 in the Fabric-gm/BCCSP

5.1.2 国密算法证书有效性测试

测试验证是否能够成功生成国密证书，包含两方面的内容。

(1) 证书生成工具 cryptogen 对国密算法支持的验证

如图 14 所示，证书生成工具 cryptogen 中的签名与哈希算法分别指向 SM2 和 SM3 算法，表明基于 cryptogen 工具生成节点证书的 Fabric-gm 联盟链网络实现了对国密证书生成操作的支持。

```
[root@localhost bin]# cryptogen generate --config=./crypto-config.yaml
org1.example.com
org2.example.com
[root@localhost bin]# gmsl x509 -in ./crypto-config/ordererOrganizations/example.com/msp/admincerts/Admin
@example.com-cert.pem -inform pem -noout -text
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
1d:e7:c7:db:2a:e8:6e:fc:d1:a5:c1:b2:9a
Signature Algorithm: sm2sign-with-sm3
Issuer: C = US, ST = California, L = San Francisco, O = example.com, CN = ca.example.com
Validity
Not Before: Jun 6 08:28:00 2020 GMT
Not After: Jun 4 08:28:00 2030 GMT
Subject: C = US, ST = California, L = San Francisco, CN = Admin@example.com
Subject Public Key Info:
Public Key Algorithm: id-ecPublicKey
Public-Key: (256 bit)
pub:
04:e0:4f:a0:b3:79:7a:7d:67:27:a7:30:de:b5:55:
ee:de:3d:46:5a:97:08:73:bc:53:75:05:df:f7:a9:
b6:eb:b2:35:bf:5e:5b:66:9c:76:63:69:05:82:23:
5a:39:0b:6a:71:11:47:e3:f8:a6:97:1b:5a:d3:fa:
51:17:b4:a6:30
ASN1 OID: sm2p256v1
NIST CURVE: SM2
X509v3 extensions:
X509v3 Key Usage: critical
Digital Signature
X509v3 Basic Constraints: critical
CA:FALSE
X509v3 Authority Key Identifier:
keyid:F6:90:15:6D:E7:9F:0F:7B:46:14:1A:AF:EC:8A:A9:CB:71:14:02:FC:B9:24:C7:29:2B:8A:70:6D
54:79:C6:6C
Signature Algorithm: sm2sign-with-sm3
30:45:02:20:7e:36:65:89:e2:46:18:de:63:6d:fb:e1:c1:a2:
f4:58:06:44:33:e8:2f:18:39:59:29:40:b5:c1:0a:3a:d1:ca:
02:21:00:e3:fb:26:70:7f:45:3a:a5:f5:93:39:b7:48:f2:b4:
85:e5:b2:2a:a3:6a:4a:51:c2:88:25:b8:c4:69:47:9a:e3
[root@localhost bin]#
```

图 14 fabric-gm/cryptogen 支持国密证书生成
Figure 14 The GM certificate in the fabric-gm/cryptogen

(2) Fabric-CA-gm 动态证书生成测试

在 Fabric-CA-gm 容器内，首先，通过 fabric-ca-client 命令注册名为 JimTest 新用户；其次，将该新用户的证书信息复制至容器外，利用 Gmsl 命令展示此证书信息。如图 15 所示，该证书的签名与哈希算法指向国密 SM2 和 SM3 算法，表明 Fabric-CA-gm 实现了对国密动态证书生成操作的支持。

综上所述，Fabric-gm 和 Fabric-CA-gm 基于国密算法的证书链成功建立。

```
[root@localhost fabric]# docker cp 7d95f8b3269d:/root/ca/root
[root@localhost fabric]# gmsl x509 -in /root/ca/jimtest/signcerts/cert.pem -inform pem -noout -text
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
1e:e6:5d:05:69:72:3a:15:18:97:12:0e:96:c7:4a:24:06:bb:f0:d1
Signature Algorithm: sm2sign-with-sm3
Issuer: C = US, ST = California, L = San Francisco, O = Org1.example.com, CN = ca.org1.example.com
Validity
Not Before: Jun 6 08:51:23 2020 GMT
Not After: Jul 18 00:51:23 2020 GMT
Subject: C = US, ST = North Carolina, O = Hyperledger, OU = Fabric, CN = JimTest
Subject Public Key Info:
Public Key Algorithm: id-ecPublicKey
Public-Key: (256 bit)
pub:
04:03:68:c7:e6:f4:d9:fe:61:ae:23:7d:59:a8:27:
12:7d:3a:e9:15:fe:10:ed:cf:ab:88:d5:4b:ee:04:
b4:dc:4c:e7:57:a2:6e:4e:37:15:77:09:46:fc:5b:
96:73:9b:53:de:32:51:94:65:ee:fd:cf:08:c8:7a:
30:37:79:0e:84
ASN1 OID: sm2p256v1
NIST CURVE: SM2
X509v3 extensions:
X509v3 Authority Key Identifier:
keyid:26:14:C6:B6:26:B3:E9:61:74:EB:35:1D:C3:17:4F:A2:56:5E:E9:98:8B:73:52:5C:FC:65:66:F
B:8A:4F:11:4F
X509v3 Subject Alternative Name:
DNS:rdhfb3269d
Signature Algorithm: sm2sign-with-sm3
30:44:02:20:16:b9:52:54:91:c1:08:0e:ef:d9:5c:fb:13:61:
b2:57:38:e7:05:cf:0d:b4:59:7d:b7:a9:ef:bf:ae:21:15:53:
02:20:11:58:77:8d:37:56:f7:75:a2:21:f4:4c:5b:7f:79:3f:
31:64:10:8a:f9:50:cf:c8:89:a9:7f:c7:6c:f8:4c:74
[root@localhost fabric]#
```

图 15 Fabric-CA-gm 支持国密证书生成
Figure 15 The GM certificate supported by the Fabric-CA-gm

5.1.3 Fabric-gm 联盟链测试网络正常启动验证

通过命令 ./byfn.sh up -a 依次执行 Fabric-gm 联盟链测试网络启动时的节点容器（包括 CA 容器）创建、节点密钥证书生成验证、链码实例化及一次完整的交易等过程。执行结果如图 16 所示，表明 Fabric-gm 联盟链测试网络能够正常启动。

```
[root@localhost fabric-gm-testnetwork]#
===== Query successful on peer1.org2 on channel 'mychannel' =====
----- All GOOD, BYFN execution completed -----
[root@localhost fabric-gm-testnetwork]#
```

图 16 Fabric-gm 联盟链测试网络正常启动验证
Figure 16 The normal startup verification for the Fabric-gm testing network

5.2 国密嵌入性能对比测试

5.2.1 系统时间开销对比测试

基于联盟链测试网络启动时间探索系统时间开销在国密嵌入前后的变化。

联盟链测试网络启动时间定义: 从 byfn.sh 开始执行开始, 经历证书生成、容器创建、通道创建、节点配置以及链码安装实例化等过程, 直至完成一次链码查询为止, 被称为联盟链测试网络的启动时间。

在虚拟环境下分别部署基于国密算法的 Fabric-gm 平台和原生 Fabric 平台开发环境, 保证两种环境下联盟链测试网络的结构配置信息和链码不变。基于每种环境重复启动联盟链测试网络 10 次, 求均值。测试结果显示: ① Fabric-gm 环境下的联盟链测试网络启动时间均值为 109.6 s; ② 原生 Fabric 环境下联盟链测试网络启动时间均值为 106.1s。综上, Fabric-gm 平台环境下联盟链测试网络的启动时间相较于原生 Fabric 平台环境下增加 3%, 因此, Fabric-gm 平台的系统时间开销在可接受范围内。

5.2.2 系统运算性能开销对比测试

SM2 和 SM3 算法主要用于 Fabric-gm 平台中的交易发起、执行和证书生成阶段, 因此, 基于 SDK 客户端发起交易与证书动态生成时间来探索系统运算性能开销在国密嵌入前后的变化。针对同样的交易内容和用户证书信息进行时间开销测试, 每项测试各进行 1 000 次, 分别求得测试均值, 测试结果如表 1 所示, Fabric-gm 平台相较于原生 Fabric 平台其平均交易时间开销增加 1 倍, 管理员用户证书动态生成时间增加 10%, 普通用户证书动态生成时间增加 8%, 平均动态证书生成时间增加 9%, 但增加的时间量级为毫秒级, 因此, Fabric-gm 平台的运算性能开销在可接受范围内。

表 1 系统运算性能开销结果

Table 1 The results of system operation performance overhead

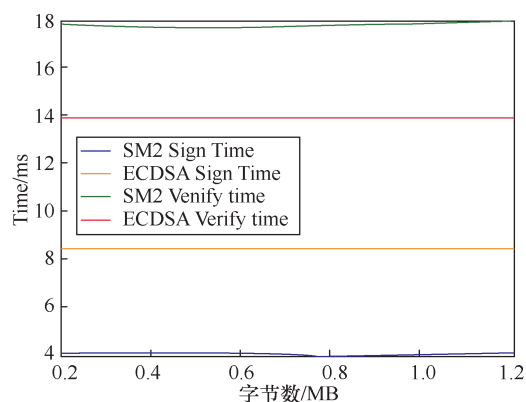
运算性能开销计算模式		国密 SDK	原生 SDK
交易时间开销		53.741 ms	23.534 ms
动态证书生成 时间开销	管理员用户	114.838 ms	103.872 ms
	普通用户	199.285 ms	184.206 ms

5.2.3 系统性能影响原因分析

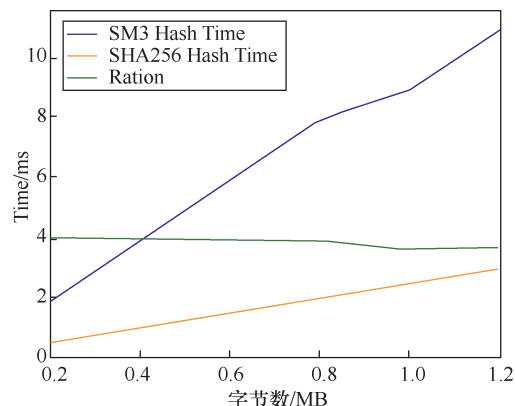
支持国密的 Fabric-gm 平台性能提升或减损可能的原因有以下两方面: ① SM2 和 SM3 国密算法效率本身与对应的 ECDSA 和 SHA256 算法效率存在差异; ② 不同版本的 SM2 和 SM3 国密

算法实现存在算法效率差异。

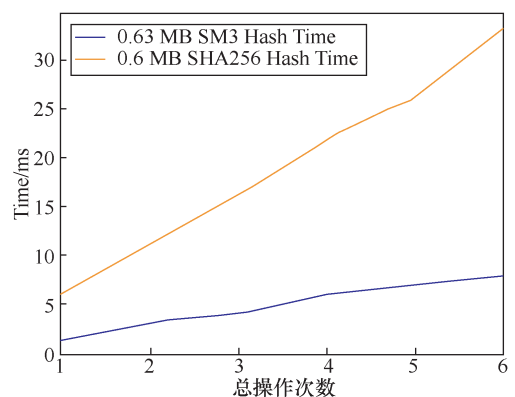
Fabric 平台原生密码算法与同济实现的国密算法的效率对比分析实验结果如图 17 所示, 分析有如下发现。



(a) SM2与ECDSA时间开销对比



(b) SM3与SHA256时间开销对比



(c) 多次哈希时间开销对比

图 17 密码算法时间开销对比

Figure 17 The comparison of cryptographic algorithm time overhead

1) 各密码算法签名、验签以及哈希操作的时间开销基本保持在毫秒级。

2) 图 17(a)表明, 在基于 ECDSA 和 SM2 的

不同字节数规模的数据的签名验签实验中,两者的时间开销均不随着字节数的增加而增加;基于 SM2 签名操作的效率优于 ECDSA 签名,但 ECDSA 的验签操作效率略高于 SM2 的验签操作。

3) 图 17(b)表明, SM3 和 SHA256 哈希操作时间开销均随着字节数的增加而近线性增长, SM3 时间开销高于 SHA256,同等条件下, SM3 哈希时间开销约为 SHA256 的 4 倍;图 17(c)表明,哈希调用的次数增加其时间开销近线性增长。Fabric 平台中单个交易哈希计算次数和区块大小规模有限,因此不会出现系统时间开销无限增加的情况。

Fabric 平台中密码算法调用场景如节 2.2 所述,哈希算法在多应用场景中被频繁调用,哈希算法调用不仅发生在所有基于 SM2 和 ECDSA 的签名验签过程中,还存在于区块链的链式结构形成和特殊 ID 值计算的过程中,远大于 ECDSA 和 SM2 算法调用频率。由图 17 的分析结果可知, SM2 与 ECDSA 的算法效率差异较小,而 SM3 与 SHA256 在同等条件下算法差异近 4 倍左右。因此,在时间开销单位为毫秒级别的基础上,同济实现的 SM3 哈希算法可能是导致 Fabric-gm 性能减损的主要原因之一。此外,文献[21]中结果表明,不同版本的 SM3 实现具有不同的算法效率,因此后期可尝试优化 SM3 的实现,以使 Fabric-gm 平台获得更接近或略优于原生 Fabric 平台的系统性能。

6 结束语

本文提出了对 Fabric 平台实现国密嵌入的思路,并基于该思路针对长期稳定版本 Fabric release1.4 开展了国密算法的嵌入工作:① 基于同济开源国密实现源码,在 Fabric 平台的 BCCSP 下添加 SM2、SM3 和 SM4 算法模块与接口;② 将 Fabric 平台的各组件上层调用的密码算法接口与对应国密算法接口相关联,实现上层应用对国密算法调用的支持。实验结果表明, Fabric 平台国密嵌入后,测试网络启动、交易以及动态证书生成等过程都成功调用了基于国密算法实现的加解密、签名验签及哈希接口,与原系统相比,改造后的系统时间开销和系统运算性能开销均在可接受范围。此外,本文对系统性能影响的原因进行对比实验分析,国密算法本身效率和原生 Fabric

平台的密码算法之间存在差异性,且不同版本的国密算法实现同样存在差异性,从而可能对平台的性能造成一定的影响。未来,将已嵌入国密的 Fabric-gm 平台与产业应用相结合,加速产业应用落地并提升生产效益。

参考文献:

- [1] hyperledger-fabricdocs documentation[EB].
- [2] 董友康,张大伟,韩臻,等. 基于联盟区块链的董事会电子投票系统[J]. 网络与信息安全学报, 2017, 3(12): 31-37.
DONG Y K, ZHANG D W, HAN Z, et al. Board voting system based on the consortium blockchains[J]. Chinese Journal of Network and Information Security, 2017, 3(12): 31-37.
- [3] 潘晨, 刘志强, 刘振, 等. 区块链可扩展性研究:问题与方法[J]. 计算机研究与发展, 2018, 55(10):7-18.
PAN C, LIU Z Q, LIU Z, et al. Research on scalability of blockchain technology: problems and methods[J]. Journal of Computer Research and Development, 2018, 55(10):7-18.
- [4] GUEGAN D. Public blockchain versus private blockchain[J]. documents de travail du centre deconomie de la sorbonne, 2017.
- [5] An introduction to hyperledger[EB].
- [6] 中华人民共和国金融行业标准. 金融分布式账本技术安全规范[EB].
Financial industry standard of the people's Republic of China. Security specification for financial distributed ledger technology[EB].
- [7] 国家密码管理局. SM2 椭圆曲线公钥密码算法[EB].
State Cryptography Administration. Public key cryptographic algorithm sm2 based on elliptic curves[EB].
- [8] 郭青霄,张大伟,常亮,等. 基于 SM2 的代理保护代理签名的设计与实现[J]. 网络与信息安全学报, 2017, 3(9): 47-54.
GUO Q X, ZHANG D W, CHANG L, et al. Design and implementation of proxy-protected proxy signature based on SM2[J]. Chinese Journal of Network and Information Security, 2017, 3(9): 47-54.
- [9] 国家密码管理局. SM3 密码杂凑算法[EB].
State Cryptography Administration. SM3 Cryptographic hash algorithm[EB].
- [10] 邵梦丽,殷新春,李艳梅. SM3 杂凑算法的 SoPC 组件实现[J]. 网络与信息安全学报, 2017, 3(5): 47-53.
SHAO M L, YIN X C, LI Y M. Implementation of SM3 algorithm based on SoPC component[J]. Chinese Journal of Network and Information Security, 2017, 3(5): 47-53.
- [11] Tongji blockchain Research Institute. Hyperledger-Fabric-gm[EB].
- [12] 张青禾. 区块链中的身份识别和访问控制技术研究[D]. 北京: 北京交通大学, 2018.
ZHANG Q H. Research on identification and access control in blockchain[D]. Beijing: Beijing Jiaotong University, 2018.
- [13] 张梦一. 基于区块链的通用积分管理系统[D]. 济南: 山东大学, 2019.
ZHANG M Y. General integration management system based on blockchain[D]. Jinan: Shandong University, 2019.
- [14] 国家密码管理局. SM4 分组密码算法[EB].
State Cryptography Administration. SM4 Block cipher algorithm[EB].
- [15] ANDROULAKI E, BARGER A, BORTNIKOV V, et al. Hyper-

ledger Fabric: a distributed operating system for permissioned blockchains[C]//Proceedings of the Thirteenth EuroSys Conference (EuroSys '18). Association for Computing Machinery.2018: 1-15.

[16] hyperledger-fabric-ca documentation[EB].

[17] Hyperledger Fabric SDKs[EB].

[18] 陈剑雄, 张董朱, 深度探索区块链 Hyperledger 技术与应用[M]. 北京: 机械工业出版社, 2018.

CHEN J X, ZHANG D Z. In-depth exploration of blockchain Hyperledger technology and application[M],BeiJing:China Machine Press,2018.

[19] 同济区块链研究院. 国密 SM2、SM3 和 SM4 算法实现[EB].

Suzhou Tongji blockchain Research Institute. Implementation of SM2, SM3 and SM4 algorithms[EB].

[20] GUAN Z. GmSSL[EB].

[21] SM2 算法与原生 RSA、ECDSA 算法的比较[EB].

Comparison of SM2 algorithm with RSA and ECDSA[EB].



陈兴蜀(1968-), 女, 贵州六枝人, 博士, 四川大学教授、博士生导师, 主要研究方向为云计算与大数据安全、可信计算与信息保障。



兰晓(1990-), 女, 四川自贡人, 博士, 四川大学助理研究员, 主要研究方向为应用密码学、安全多方计算、认证密钥协商协议、区块链安全。

[作者简介]



曹琪(1996-), 女, 四川广安人, 四川大学硕士生, 主要研究方向为区块链安全及应用、网络行为分析。



张红霞(1996-), 女, 河北邢台人, 四川大学硕士生, 主要研究方向为区块链安全及应用、网络行为分析。



阮树骅(1966-), 女, 浙江绍兴人, 四川大学副教授、硕士生导师, 主要研究方向为云计算与大数据安全、区块链安全。



金泓键(1996-), 男, 重庆人, 四川大学硕士生, 主要研究方向为区块链安全及应用、大数据分析。