计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.210100030

国密算法在资源公钥基础设施(RPKI)中的应用

冷 峰[1,2,3] 张明凯[2] 延志伟[2] 张翠玲[2] 曾 宇[1,2]
1 中国科学院计算机网络信息中心 北京 100190
2 中国互联网络信息中心 北京 100190
3 中国科学院大学 北京 100049
(lengfeng@cnnic.cn)

摘 要 近年来域间路由劫持事件频发,路由系统的安全性受到广泛重视。RPKI系统作为一种路由安全验证系统,通过和现有的路由广播策略的有效结合,可大幅降低路由劫持的风险。RPKI系统当前在设计和开发上针对密码算法的选择做了特殊的约定,其中签名算法仅限于使用RSA非对称加密算法,哈希算法仅限于使用SHA-256算法。随着密码算法的不断升级更新,以及新密码算法的推出,预期RPKI系统在未来版本中会逐步纳入更多新的算法来满足安全、性能以及用户定制化部署的需求。文中将国密算法与RPKI结合,通过建立一套完善的密码算法测试环境,对国密算法应用性能与标准RFC定义的算法进行多维度的横向比较,探讨国密算法在RPKI中应用的可行性、大规模部署环境下的优化改进方式以及对现有RPKI系统中密码体系的未来发展的展望。

关键词:RPKI;非对称加密;哈希算法;路由安全;性能测试
中图法分类号 TP393

Application of Chinese Cryptographic Algorithm in RPKI

LENG Feng[1,2,3],ZHANG Ming-kai[2],YAN Zhi-wei[2],ZHANG Cui-ling[2] and ZENG Yu[1,2]
1 Computer Network Information Center,Chinese Academy of Sciences,Beijing 100190,China
2 China Internet Network Information Center,Beijing 100190,China
3 University of Chinese Academy of Science,Beijing 100049,China

Abstract The security of routing systems attracts extensive attention worldwide with increasing inter-domain routing hijacking incidents in recent years. As a routing security verification system,the RPKI system can greatly reduce the risk of routing hijacking by working with existing routing broadcast strategies. The signature algorithm is limited to the RSA asymmetric encryption algorithm,and the hash algorithm is limited to the SHA-256 algorithm. With the upgrading of cryptographic algorithms,it is reasonable to expected that the RPKI system will gradually accept more algorithms to meet security and performance requirements. This article introduces the SM2 and SM3 algorithms,also known as Chinese commercial cryptographic algorithms,into RPKI system,and establishes a complete set of cryptographic algorithm testing environment from multi-dimensional aspect to compare Chinese commercial cryptographic performance with standard RFC defined algorithms. After performance evaluation and comparison,we discuss the algorithm feasibility,optimization and improvement methods in large-scale deployment environments,and the prospect of the future development of the existing crypto system in RPKI system.

Keywords RPKI,Asymmetric encryption,Hash algorithm,Routing security,Performance test

1 引言

近年来,针对路由系统的网络安全事件层出不穷,域间路由劫持时有发生,比如2006年的Con-Edison路由劫持事件[1]、2008年的YouTube流量劫持事件[2]以及2018年4月Amazon路由劫持事件[3]等。劫持事件的发生主要由于边界网关协议(Border Gateway Protore,BGP)本身设计上的缺陷导致。BGP协议被广泛用于当前互联网域间路由信息的交互,其缺乏必要的验证策略以实现对路由信息交换的管理。互联网码号资源公钥证书体系(Resource Public Key Infrastructure,RPKI)的诞生就是为了缓解自治域间路由劫持的安全风险,通过对PKI(Public Key Infrastructu)正确性进行核验,从而降低路由劫持事件的发生。

根据RFC7935[4]定义,当前RPKI系统在设计和开发上针对加密算法的选择做了特殊的约定。签名算法仅限于使用RSA非对称加密算法,哈希算法仅限于使用SHA-256算法(简称为标准算法)。2010年由国家密码管理局推出了一系列国产加密算法,其中包括非对称加密算法SM2[8]及哈希算法SM3[9],借助于SM2我们可以实现对于数据的签名和验证,而SM3则可以获取数据的散列值用于数据签名。两种国

基金项目:北京市科技新星计划项目(Z191100001119113)
This work was supported by the Beijing Nova Program of Science and Technology(Z191100001119113).
通信作者:曾宇(zengyu@cnnic.cn)

密算法组合后可以实现对于标准算法的替换，通过建立完善的测试环境，实现标准算法和国密算法的对比，验证国密算法在 RPKI 体系中的适配情况，以及对 RPKI 中的核心功能——证书签名和验证进行功能测试和压力测试，并根据测试结论对其应用情况进行分析。

2　RPKI 与加密算法

2.1　RPKI 简介

RPKI 系统本身包括三大基本组件：认证权威(Certificate Authority，CA)、依赖方(Relying Party，RP)和资料库(Repository)。三大组件之间的交互关系如图 1 所示。

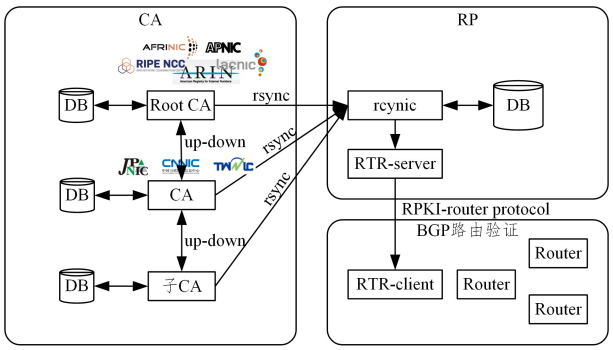

图 1　RPKI 系统的三大组件

Fig. 1　Components of RPKI system

这三大组件通过签发、传送、存储、验证各种数字对象(包括各种签名对象和证书)来彼此协作，共同完成 RPKI 的功能。其中三大组件的核心功能介绍如下：

(1)CA 通过签发 RC(Resource Certificate)证书来表明互联网码号资源(Internet Number Resource，INR)分配关系，也可以直接通过签发路由起源认证(Route Origin Authorization，ROA)来授权某个 ISP 针对自己的一部分 IP 地址前缀发起源路由通告。

(2)RP 负责从 Repository 中获取数字对象，并将其处理成 IP 地址块与 AS 号的真实授权关系，用于 BGP 路由信息的发布。

(3)Repository 负责存储这些承载了 INR 分配/授权信息的 RC 证书/ROA 等数字对象，供 RP 服务下载。

2.2　RPKI 证书与数字签名对象

在 RPKI 体系中包含两类证书[10]：一类是 CA 证书，用以证明某个实体对 IP 地址和 AS 号的所有权；一类为终端实体(End Entity，EE)证书，用以对 IP 地址前缀的路由源信息添加签名。在 RPKI 中，验证关系由 IP 地址分配关系决定，并通过对传统的 X.509 证书进行扩展实现。RFC3779[5] 约定了如何使用 X.509 证书来携带 IP 地址和 AS 号信息，详细规范了 IP 地址和 AS 号作为扩展域在 X.509 证书中的编码格式。

RPKI 体系数字签名对象 ROA 包含一个 AS 号同一个或多个 IP 地址前缀之间的“绑定关系”。其真实性由 ROA 中 IP 地址前缀对应的 EE 证书添加签名加以保证。与传统的 PKI 证书体系一样，证书撤销列表(CRL)文件和存储证书及资源清单(Manifest)文件的生成也需要用到加密算法。

2.3　密码算法应用

RPKI 内部主要采用签名算法和哈希算法完成整个证书的签名和验证。其中证书、CRL(Certificate Revocation List)、CMS(Content Management System)签名对象和证书请求使用的签名算法为 RSA PCKS＃1 v1.5(见 RFC3447 8.2)，哈希算法采用 SHA-256 算法完成，同时 CA 在产生 key ID 时使用的是 SHA-1 算法[6]。

在证书、CRL 和证书请求中，哈希算法和数字签名算法是一并标示的，用 sha256WithRSAEncryption 来表示。在 CMS 签名数据中，哈希算法(用于生成消息摘要)和数字签名算法是分别标示的，其中哈希算法表示为 id-sha256，签名算法表示为 rsaEncryption，sha256WithRSAEncryption。

根据 RFC7935 对 RPKI 密码算法的规定，目前 RPKI 只支持 RSA(2048 位密钥)签名算法与 SHA-256 哈希算法的密码算法组合。其中 RSA 密钥对必须是模长为 2048 位，指数为 65537 的密钥。公钥包括算法和公钥两个字段，格式遵从 RFC4055[7] 的规定，编码方式为 DER。私钥格式没有作出统一规定。针对 RPKI 中签名的格式，证书中的签名字段和 CMS 签名数据签署者信息中的签名字段分别遵从 RFC 4055 和 RFC 5652 的规定。RFC7935 中定义了针对未来算法扩展方面的介绍，算法迁移的操作可以参考 RFC6916 实现。但自 RPKI 诞生以来尚未提出新的密码算法。如需扩展新引入的密码算法可参考 RFC7935 中对 RSA(2048 位密钥)签名算法和 SHA-256 哈希算法表示方法的规定。

3　国密算法的应用

当前全球五大区域互联网注册机构(Regional Internet Registry，RIR)均部署了 RPKI 服务。针对 RPKI 社区的开源项目也逐渐增多，部分开源软件可以同时作为 CA 以及 RP 完成整个安全业务的管理，部分软件则只适用于某一些服务功能，比如只能作为 RP 软件同步证书和验证证书使用，或者支持 RTR 协议，实现路由信息到路由设备的下发管理等。

表 1　开源软件现状调研

Table 1　Open resource software survey

软件名称	CA	RP	RTR	语言
RPKI. NET Toolkit	支持	支持	支持	Python
PRKI Took	支持	支持	支持	Rust
RPSTIR	不支持	支持	支持	C
RPKI Validator	不支持	支持	支持	Java
OctoRPKI	不支持	支持	不支持	Go

本文针对国密算法的协议扩展和性能测试，主要基于 Cloudflare 公司开源的 OctoRPKI 开源解决方案，借助于其 RPKI 组件库可进行针对证书的签名和验证测试，修改组件库的内置算法实现，从而完成国密算法和标准算法的性能对比。

3.1　协议扩展

为测试国密算法在整个 RPKI 体系中的应用情况，本文搭建了一整套完善的实验环境，用于模拟线上 RPKI 的证书签名和验证流程。整个实验环境可以看作一个独立的服务系统，主要提供两个接口。第一个接口为输入用户自定义 IP 段与 AS 号的绑定信息，输出对应的签名证书；第二个接口为输入签名证书，输出签名证书的验证结果。

我们在此系统上实现针对上述接口的功能性测试和压力负载测试。该环境除了 ROA 证书生成和验证过程，内部还集成了从自签名的根证书到二级组织证书和单独的 ROA 签名证书的多层证书链认证管理，并在整个业务处理逻辑中实

现标准算法与国密算法的切换处理，从而实现独立的测试。图 2 描述了测试环境包含的三层证书结构。

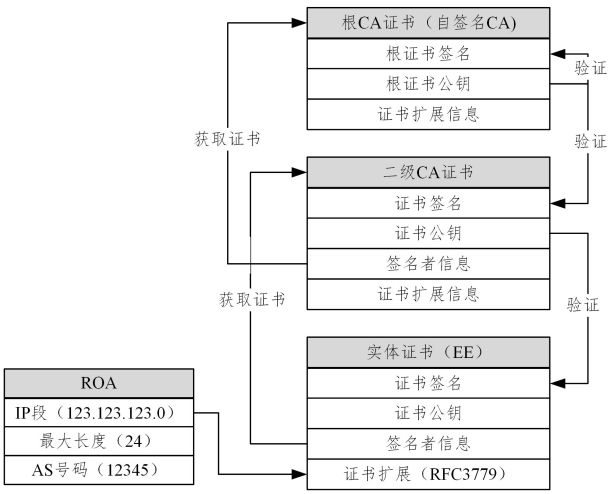

图 2 密钥签名证书验证流程

Fig. 2 Key signature certificate verification process

3.2 ROA 签名

针对功能需求中接口 1 的设计，将整个生成 ROA 证书的流程划分为以下 6 个主要步骤。

(1)初始化根证书，首先生成一对公私密钥对，针对标准算法为 RSA 密钥对(使用 2048 位密钥长度)，针对国密算法则为 SM2 密钥对(使用 256 位密钥长度)。对于根证书，这里需要设置其 IP 段(0.0.0.0/0)与 AS 号范围($[0,2^{32}-1]$)作为其授权管理域。

(2)设置根 CA 的指向存储资源对象库的路径(Subject Information Access，SIA)信息，生成对应的根 CA 证书撤销列表；根据 RFC3779 要求这些信息经过 ASN.1 编码后写入 x.509 证书的扩展区。

(3)生成二级证书，设置证书的签名 CA(父级)为根证书，使用 AIA(权威信息访问)来记录父级证书的访问路径。生成对应的二级 CA 证书撤销列表。测试环境中这些访问路径均以 KV 的形式存储，便于快速定位其证书数据。

(4)使用根证书公钥对证书进行签名，生成的证书哈希值用于更新 Manifest 清单信息，这里标准算法使用的是 SHA-256，国密算法采用 SM3 哈希算法完成。

(5)获取用户输入的 ROA 信息，使用 CMS 格式进行编码处理。

(6)生成一对公私密钥，并创建 ROA 签名证书，使用二级证书对该证书进行签名处理，并利用该证书对步骤(5)中创建的 CMS 信息进行签名。

上述处理流程中步骤(1)－步骤(4)实现测试环境的初始化，只需要执行一次；步骤(5)－步骤(6)为重复测试执行步骤，用户每次输入一个新 ROA 信息，则为其创建一个独立的实体证书，并返回信息编码处理后的 ROA 证书内容，完成整个的签名过程。对标准算法与国密算法签名部分的性能测试对比将仅围绕创建 ROA 证书的部分展开。

对于上述步骤(5)－步骤(6)进行持续压力测试，对比每秒可生成 ROA 证书签名的次数，在同样的测试条件下结果如图 3 所示。测试结果表明国密算法(SM2＋SM3 组合)在整个签名过程中性能表高于 RFC 标准算法(RSA2048＋SHA256)，性能提升约 4 倍。

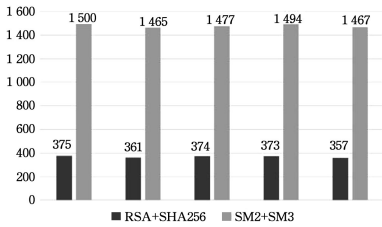

图 3 ROA 证书生成性能测试

Fig. 3 ROA generation performance test

通过对测试性能分析可以发现，密码算法在生成 ROA 证书过程中的主要瓶颈在于采用 RSA 或国密 SM2 的签名效率方面。在证书生成流程中，包含两次完整的签名操作，一是 ROA 编码后的 CMS 消息摘要信息的 RSA 签名，签名用于验证 ROA 信息的完整性；二是父级 CA 对于 ROA 证书公钥的签名，该签名用于验证 ROA 证书的有效性。在标准算法中两次签名总计占用测试总时间的 40.52%和 32.68%，在国密算法中两次签名时间占总时间的 40.00%和 34.55%。

3.3 ROA 验证

针对功能需求中接口 2 验证 ROA 签名的流程，从获取到 ROA 证书开始，对数据进行处理后按照信任链逐层进行验证。主要的执行步骤如下。

(1)获取 ROA 证书，进行 CMS 格式的解码，提取其中的 IP，AS 等扩展信息，验证数据字段是否有效(取值范围以及是否缺失数据)，并提取其中的公钥证书信息及签名者证书信息。

(2)检查该 ROA 证书是否在证书撤销列表中(CRL 证书同样需要验证)。

(3)获取证书中的摘要信息，使用签名算法，比如标准 SHA-256 算法或者国密 SM3 算法对封装的数据信息进行重新计算。

(4)获取签名信息，使用证书公钥，比如标准算法 RSA 或者国密算法 SM2，对签名信息进行核验，检查是否能够通过签名验证。利用证书链继续完成其上一级签名证书的核验。

(5)取得父级签名者证书，并对 ROA 证书完整性进行签名校验，同时验证 IP 及 AS 信息是否有效(有效的父级管理范围内)。如果验证成功，继续沿着证书信任链上移，获取签名证书父证书。

重复步骤(4)－步骤(5)，直到到达根证书，如果父证书为根证书，代表其不包含任何有效的父证书，则直接使用该证书与内置的 TAL 中信任证书进行算法比较，检查是否有效。如果根证书验证成功，则整个验证过程成功，否则返回失败信息。

如果整个验证过程中没有出现错误(验证签名失败，证书过期或证书撤销等无效结果)，则证明信任链及 ROA 均验证成功。为实现独立的验证签名过程性能测试，整个测试流程去除了初始化信任链，以及对应的 Manifest 文件和 CRL 证书撤销文件生成的过程，验证过程同时会直接检查这些已存在文件的信息。所有证书将存储在内存中处理，以提供高效的查找和定位。

图 4 给出了标准算法和国密算法在 ROA 证书验证流程中的性能数据。通过对运行程序的性能分析，标准算法在验证 ROA 证书流程中相对于国密算法具有明显的优势，整体的验证效率约为国密算法的 5.7 倍。国密算法执行的性能瓶

颈在于其 SM2 验证签名效率方面相对于 RSA2048 较低。与生成签名证书相同，在执行证书验证的流程中，同样包含两次完整的签名验证操作。同时该测试中也包含了对于数据的 ASN.1 解码以及证书的数据提取等操作。

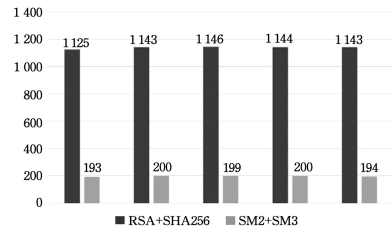

图 4　ROA 证书校验性能测试

Fig. 4　ROA verification performance test

由上述两项测试可以看出，国密算法在验证 ROA 签名方面效率不及标准算法，而在生成签名方面较标准算法执行效率更高。这也与对两种算法进行单纯的性能测试的结论相一致。结合 RPKI 而言，线上服务运行时 CA 以签名为主，RP 则以验签为主。RP 在获取到证书并完成证书签名验证后，将数据传递给路由器等设备加载。CA 一旦生成完成证书后，后续进行变更的频率较低，而后续主要是大量 RP 的验证。所以验证签名效率的提升是国密算法在 RPKI 中应用的关键。

国密算法尽管在实际测试中存在验证签名效率较低的问题，但是验证签名的频率与实际部署的环境和架构设计模式有直接关系。基于 HTTPS 的 RPKI 缓存下发机制[11]现在已经逐步成熟且得到较大规模的应用[12]，集中式的 RP 可以为更多的边缘节点提供路由解析验证，借助于 HTTPS 成熟的缓存机制和 CDN 分发网络，可以大幅度地降低边缘路由验证的代价，从而减少实际进行验证签名的次数，国密算法和标准算法在此模式下的均摊成本将趋于一致。

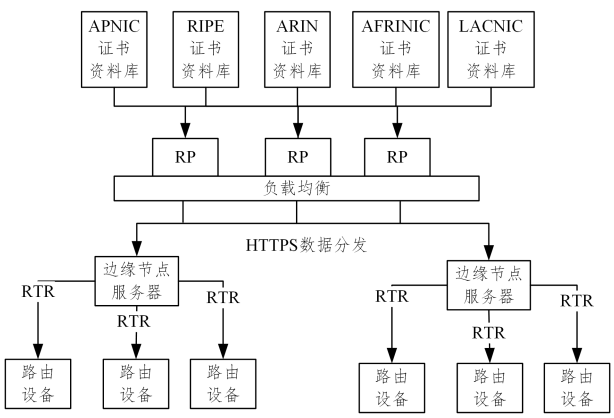

图 5　系统部署架构图

Fig. 5　System deployment architecture diagram

同时部署方面借助于负载均衡设备可以提供高可靠的传输保障，分层的设计也可以有效降低单层的负载压力，减轻五大区证书下载和同步的负担。这种模式下整个传输过程中数据的安全性由 HTTPS 保证，而 RP 的角色更侧重作为一个验证和分发中心，为网络内所有的边缘节点提供路由验证的服务。

结束语　当前 RPKI 系统由于相关标准的实现规定，仅支持使用一种加密和签名算法，不同系统组件之间的交互也完全依赖于相同算法完成。但是通过扩展我们可以实现算法的升级和替换，提供更灵活的选择空间。通过对证书签名和验证过程的性能测试分析发现，尽管国密算法在签名阶段的表现优于标准算法，但在验证阶段却相对较差。总体来看，选择国密算法对于以签名 ROA 为主的 CA 服务来说会有部分性能方面的提升，但是对于以验证为主的 RP 服务则可导致验证效率的降低。大规模部署环境下，特别是基于 HTTPS 的数据下发方式，国密算法签名和验证的效率将得到大幅度的提升和优化，解决性能方面的短板，从而提升整体算法的可实施性。另外当前国际标准对于 RPKI 的密钥算法的约束，在未来会随着密码算法的逐步更迭而放开，使其能够更好地兼容不同类型的密码算法，同时密码算法的发展也需要不同服务之间提供一定的密钥协商流程以及软件算法的支持，这些都是 RPKI 体系后续需要逐步完善的地方。

参 考 文 献

[1] Towards uncovering BGP Hijacking attacks [EB/OL]. https://pastel.archives-ouvertes.fr/tel-01412800/-document. 2016.

[2] RIPE NCC YouTube Hijacking: A RIPE NCC RIS case study [EB/OL]. https://www.ripe.net/publication-s/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study [2008].

[3] ThousandEyes, Anatomy of a BGP Hijack on Amazon's Route 53 DNS Service [EB/OL]. https:/-/medium.com/thusandeyes/anatomy-of-a-bgp-hijack-on-amazons-route-53-dns-servicea5eebb3e9375. 2018.

[4] APNIC RFC7935[EB/OL]. https://tools.ietf.org/ht-ml/rfc79-35. 2016.

[5] BBN TechnologiesRFC3779[EB/OL]. https://tool-s.ietf.org/html/rfc 3779. 2004.

[6] QIN X W. Head First RPKI[M]. Publishing house of electronics industry, 2018.

[7] RSA Laboratories [EB/OL]. https://tools.ietf.org/-html/rfc 4055. 2005.

[8] Public Key cryptographic algorithm SM2 based on elliptic curves Part 2: Digital signature algorithm[S]. Beijing: Chinese Standard Publishing House, 2012.

[9] Information security techniques—SM3 cryptographic hash algorithm[S]. Beijing: Chinese Standard Publishing house, 2012.

[10] MA D. RPKI Overview[J]. Telecommunications Network Technology, 2012.

[11] GENG X J, MA D, MAO W, et al. RPKI Cache Update Mechanism Based on HTTPS[J]. Computer Systems and Applications, 2019, 28(9): 72-80.

[12] Cloudflare RIPE79 Cloudflare and RPKI at scale [EB/OL]. https://ripe79.ripe.net/presentations /40-RIPE79-Cloudflares-RPKI-validator.pdf.

LENG Feng, born in 1982, Ph.D, is a member of China Computer Federation. His main research interests include internet infrastructure resources and network security.

ZENG Yu, born in 1973, Ph.D, researcher, Ph.D supervisor, is a member of China Computer Federation. His main research interests include computer architecture, network security and digital economy.