doi: 10.3969/j.issn.1672-6073.2025.05.016

轻量级公钥基础设施在城市轨道交通网络中的应用

廖志斌[1,2]，崔亦博[1,2]，冯浩楠[1]，郜洪民[1]
（1. 中国铁道科学研究院集团有限公司，北京 100081；2. 广州铁科智控有限公司，广州 510555）

摘 要：为解决城市轨道交通安全设备在开放网络空间中面临的外部设备冒充和信息窃取的风险问题，提出一个基于国密算法的轻量级公钥基础设施的系统方案，以及兼顾行政管理需求的证书签发方案。首先，根据城市轨道交通特点设计分层级的 X.509 格式 SM2 算法签名的证书；然后，以该证书中公开的公钥信息为基础，提出密钥协商三次握手协议，实现完全开放的网络空间中的会话密钥协商；最后，构建域内设备握手和域间设备握手的通信流程，并对其进行效率分析。结果表明：本文提出的系统方案在设备间通信信息完全泄露的情况下，依然能够保证设备间点到点的加密传输；设备间密钥协商过程时间消耗约 214.5 ms，最不利情况下约 2 557.5 ms，该时间消耗远小于列车跨越区域控制中心时的通信重叠区运行时间，效率能够得到有效保障。

关键词：加密传输；城市轨道交通；公钥基础设施；国密算法
中图分类号：U231　　**文献标志码：**A　　**文章编号：**1672-6073(2025)05-0129-07

Application of a Lightweight Public Key Infrastructure in Urban Rail Transit Networks

LIAO Zhibin[1,2], CUI Yibo[1,2], FENG Haonan[1], GAO Hongmin[1]
(1. China Academy of Railway Sciences, Beijing 100081;
2. Guangzhou Railway Sciences Intelligent Controls Co., Ltd., Guangzhou 510555)

Abstract: To mitigate the risks of device impersonation and information eavesdropping faced by urban rail transit safety equipment in open network environments, this paper proposes a system scheme for lightweight Public Key Infrastructure (PKI) based on domestic cryptographic algorithm (SM algorithm), which takes into account the certificate issuance scheme for administrative management needs. First, based on the characteristics of urban rail transit, a hierarchical X.509 certificate system signed with the SM2 algorithm was designed. Then, leveraging the public key information embedded in the certificates, a three-way handshake protocol was proposed to achieve session key negotiation in a fully open network environment. Finally, communication procedures for intra-domain and inter-domain device handshakes were constructed, and their performance (efficiency) was analyzed. The results show that the proposed system still ensures point-to-point encrypted communication between devices even if all inter-device communication data are fully exposed. The device-to-device key negotiation takes approximately 214.5 ms under average conditions and about 2557.5 ms in the worst case; both values are far below the duration of the communication overlap zone when a train transitions between regional control centers, thereby ensuring acceptable efficiency.

Keywords: encrypted transmission; urban rail transit; public key infrastructure; SM algorithm

收稿日期：2025-02-24　修回日期：2025-03-13

第一作者：廖志斌，男，硕士，助理研究员，从事轨道交通信号系统研究工作，lzb_216511@163.com

基金项目：国家重点研发计划(2023YFB4302501-05)；中国国家铁路集团有限公司科技研究开发计划(K2024T005)；中国铁道科学研究院集团有限公司科研项目(2023YJ116)；广州铁科智控有限公司技术研究(KYA23002)

引用格式：廖志斌，崔亦博，冯浩楠，等. 轻量级公钥基础设施在城市轨道交通网络中的应用[J]. 都市快轨交通，2025，38(5)：129-135.
LIAO Zhibin, CUI Yibo, FENG Haonan, et al. Application of a lightweight public key infrastructure in urban rail transit networks[J]. Urban rapid rail transit, 2025, 38(5): 129-135.

轨道交通作为高效、安全、环保的公共交通工具，在国家交通体系中占据越来越重要的地位。轨道交通通信网络与最新通信技术的融合与应用，提升了轨道交通的运营效率和服务质量，为自动化、智能化、无人化的信号系统技术提供了重要支撑。

城市轨道交通列车运行控制系统网络由有线封闭式网络和无线开放式网络组成，该网络为信号安全设备提供了数据传输通道；信号安全设备间，通常使用铁路信号安全协议(railway signal safety protocol，RSSP)的 RSSP-I 和 RSSP-II 作为通信协议。

RSSP-I 基于封闭式网络设计的保护算法，不能满足开放式网络[1]的通信需求。RSSP-II 协议考虑了封闭式和开放式两种网络。信号安全设备应用 RSSP-II 协议需预先写入密钥参数，由于该密钥参数在一个运行区域内(例如城市轨道交通的一条线路)均相同，因此只能通过行政管理手段进行保密。而城市轨道交通中车载和地面的安全设备的通信网络暴露在空中，密钥参数一旦泄露，将导致所有安全设备处于被劫持和伪装的风险当中。

近年来，信息安全受到越来越广泛的关注，根据全国网络安全标准化技术委员会公示的国家标准清单，截至 2024 年 1 月 3 日，我国共发布了 378 项相关标准，信息安全领域形成了完整的标准体系。国铁集团的工电部也积极推进网络安全的研究[2]。

学者们也对信息安全进行了相关研究，张凯[3]提出使用高级加密标准(advanced encryption standard，AES)代替 RSSP 采用的三重数据加密标准(triple data encryption standard，3DES)实现设备间通信数据加密；张成阳等[4-5]则提出使用国产商用密码算法 SM4 进行设备间通信数据加密。无论是 AES 还是 SM4，这些算法只能在加密强度上进行安全提升，并不能解决加密密钥泄露的风险。因此，城市轨道交通安全设备在开放环境下必须解决密钥的机密性传输。对此，屈毅等[6]提出统一密钥生成和系统分发的密钥管理架构，以及完善铁路通信网的安全防护体系的想法。

公钥基础设施(public key infrastructure，PKI)是一个采用公钥管理体制的基础设施，它能够提供鉴别、加密、完整性和不可否认性服务[7]。目前，互联网采用的 PKI 系统，使用主流的 RSA 和 AES 算法，这些算法均是国外提出的密码算法，其核心技术受制于人，加密技术中甚至可能会被放置后门，对国家安全构成严重威胁。为了摆脱密码技术的依赖，国家密码局发展了国产商用密码算法。已经有许多学者对国家商用密码算法进行了应用研究，张宇等[8-9]研究了 SM2 算法高效签名的方案；ZHOU 等[10]在云环境中使用 SM2/3/4 实现了可信计算；孙敏等[11]研究了 SM4 和 SM2 混合加密的算法。各行业不断推进的商用密码算法从根本上摆脱了对国外密码技术和产品的过度依赖，也实现了信息安全自主可控，降低研发、维护等方面的成本，避免潜在的知识产权风险。

本文针对开放网络空间下的密钥泄露问题，采用国密算法，构建公钥基础设施，保障开放网络空间中设备端到端的加密传输，完善通信网的安全防护体系。

1 系统模型

互联网行业的公钥基础设施为一个单向认证模型，用户要求服务器提供凭证，通过公开的密钥算法和公钥信息完成对服务器的真实性认证；服务器对用户则不进行认证，而由服务器本身的应用服务决定是否对未知用户提供服务。但是，城市轨道交通行业中的信号安全设备一般为对等通信设备，通信双方均需认证对端设备。因此，城市轨道交通行业公钥基础设施应用需要建立双向认证的系统模型。参考 Subset-038 标准[12]，本文提出基于公钥基础设施的双向认证系统模型。

双向认证系统模型如图 1 所示。证书颁发机构(certification authority，CA)域定义为一个授权区域，这个授权区域内的所有设备均归属 PKI 设备进行授权和验证。每个 CA 域中的 PKI 设备包含两套非对称密钥，域内密钥对用于不同 CA 域之间的认证和安全传输，域间密钥对用于本 CA 域中的证书授权和验证。

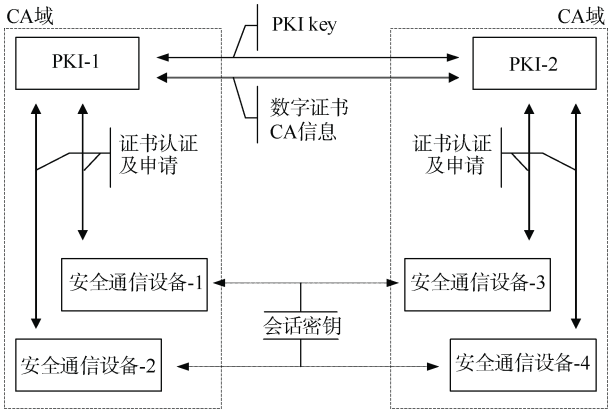


图 1 双向认证系统模型

Figure 1 Mutual authentication system model

每个 CA 域中的设备均共享 PKI 设备的域内公钥。不同 CA 域之间使用 PKI 系统对外交互数字证书信息。每个 PKI 设备均需要保存其他可信 CA 域的自签名证书。安全通信设备(简称设备)-1 与设备 2 属于相同 CA 域，由 PKI-1 管理身份认证所需证书；设备 3 和设备 4 属于另一个 CA 域，由 PKI-2 管理身份认证所需证书。设备 1 与设备 2 通过域内公钥验证双方证书，认证身份；设备 1 和设备 3 与各自归属的 PKI 交互验证双方证书，认证身份；设备间认证完成后，由证书中携带的密钥信息生成会话密钥，进行后续加密通信。

在双向认证系统模型中，设备间通过非对称加密算法协商会话密钥完成连接建立，对称加密算法使用会话密钥完成端到端的数据加密。系统的目标是假设开放空间泄露所有信息的情况下，依然能够保证设备端到端的加密传输。

2　证书签发

2.1　设计原则

PKI 系统需要为每一个设备进行证书签发，让设备获得自身证书凭证，该过程可在封闭网络内自动申请和授权，或者由管理者进行集中管理审核。本系统采用人工授权的方式进行集中管理审核，对每一个系统内新增设备进行确认，该授权仅需要在设备第一次取得自身证书凭证时进行。当设备取得自身证书凭证后，则无需人工干预，并在开放空间中所有数据暴露的情况下，依然能够完成端到端的加密传输。

城市轨道交通系统可简单看作一个集中分布式系统，以一座城市的一条城市轨道交通线路为一个中心，设备分别归属各个中心，各中心之间互相通过骨干网络进行连接。每一条城市轨道交通线路设置独立的 PKI 系统，线路中设备均由 PKI 系统管辖，每个设备的证书由管辖 PKI 系统颁发；各线路的 PKI 系统能够相互通信。当归属不同 PKI 系统的设备进行通信时，设备需要根据对端设备的 PKI 系统进行认证，因此，设备的证书需携带设备归属信息。

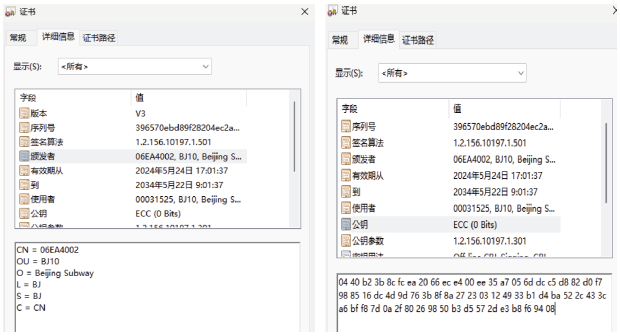
PKI 系统中的设备面临更换或报废时，该设备具备完整接入算法和合法证书，为了防止内部人员错误使用或利用该设备进行非法接入，PKI 系统证书的管理中引入管理者角色，管理设备的准入和移出。

2.2　证书格式

PKI 系统中设备的证书使用 X.509 标准[13]，主要包含 serialNumber(序列号)，signature(签名算法)、subject(主题信息，包含证书颁发者 Name 值)，subjectPublicKeyInfo(证书持有人公钥信息)，subjectUniqueID (持有者标识)，signatureAlgorithm(签名算法)和(signatureValue)签名结果。其中，客户端主要上传包含 serialNumber(序列号)和 subjectPublicKeyInfo 信息的认证请求，由 CA 进行证书签名。

按照 X.509 协议规定，Name 值由 country(C)，state(S)，locality(L)，org(O)，org_unit(OU)，common_name(CN) 6 部分组成。为了满足轨道交通行业需求，将 Name 值各组成部分分别对应为国家、省份、城市、地铁公司、线路名称和设备 ID 这 6 个子项。

证书内容如图 2 示例，颁发者为中国北京的地铁 10 号线编号为 06EA4002 的设备，使用者为 00031525，其中 Name 值按照规划，其子项分别为 CN，BJ，BJ，Beijing Subway，BJ10，06EA4002；签名算法的对象标识符(Object Identifier，OID)为 1.2.156.10197.1.501 代表证书采用了 SM2 签名算法。



(a) 颁发机构Name值　　(b) 证书公钥信息

图 2　签发证书仿真

Figure 2　Certificate issuance simulation

证书请求阶段，客户端随机生成注册密钥对(d_0，P_0)，其中 d_0 为私钥，P_0 为公钥；注册前，使用注册密钥的私钥 d_0 将除 signatureValue 之外的其他数据进行签名，形成 CSR 文件，再使用域内公钥 P_{CA} 进行加密，发送给 PKI。

证书签名阶段，PKI 设备使用域内私钥 d_{CA} 解密客户端 CSR 文件的数据后，使用该数据中的公钥 P_0 进行签名验证，添加必要信息后，使用自身域内私钥 d_{CA} 进行证书签名，得到完整证书信息；然后使用客户端 CSR 文件中的公钥 P_0 进行证书信息的加密，并回传给客户端。客户端收到数据并解密后，将证书信息编码为 base64 格式，并存储为 CRT 证书文件。

证书验证阶段，PKI 系统中的设备 A 收到另一个

设备 B 的通信请求，并获得设备 B 的 CRT 证书信息后，根据 CRT 证书中的 subject 信息判断证书归属关系，若该证书归属于当前 CA 域的 PKI 设备(PKI-1)，则使用域内公钥进行验证；否则设备 A 将设备 B 的 CRT 证书信息发送给 PKI-1，由 PKI-1 交给该 CRT 证书归属的 PKI 设备(PKI-2)进行验证，PKI-2 再将验证结果反馈给 PKI-1，PKI-1 将验证结果反馈给设备，完成验证过程。

2.3 签发流程

证书签发流程只在一个新的设备加入当前CA域时进行。每个安全设备首先随机生成一个公钥，由管理者先将安全设备序列号和公钥，按照行政管理手段加入 PKI 设备中，防止伪造设备取得证书。然后将设备连接到与 PKI 相同的 CA 域中，设备自动与 PKI 设备交互，获得唯一证书。证书签发流程具体如图 3 所示。

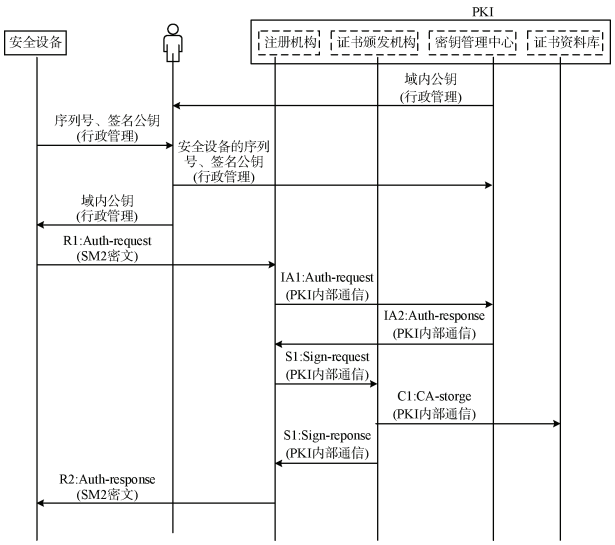


图 3 证书签发流程

Figure 3 Certificate issuance process

PKI 系统的域内公钥为公开信息，任何设备和个人均可持有，该信息不影响网络中数据的机密性。PKI 系统最少包含注册机构(registration authority，RA)，CA，密钥管理中心和证书资料库 4 个功能实体。证书签发流程如下。

1) PKI 将域内密钥对(P_{CA}，d_{CA})随机生成后，秘密保存私钥 d_{CA}，并将公钥 P_{CA} 发送给管理人员。

2) 安全设备通过随机算法，生成一个注册密钥对(d_0，P_0)，安全人员获取安全设备的序列号 SN 和公钥 P_0。

3) 管理人员将安全设备的 P_0 和序列号输入 PKI 系统的密钥管理中心；并将域内公钥 P_{CA} 发送给安全设备。

4) 安全设备使用 P_{CA}，通过 SM2 加密算法，向 PKI 的 RA 发起认证请求(certificate signing request，CSR)，认证请求携带了设备通信密钥对的公钥 P_0、序列号和主题信息，并通过注册密钥对的私钥 d_0 进行签名。

5) PKI 设备的 RA 模块收到请求后，通过序列号向密钥管理中心查询该设备的 P_0，使用公钥 P_0 进行验签。

6) 验证通过后，RA 则将请求发送给 CA 模块；由 CA 模块使用域内密钥对的私钥签发 X.509 格式的证书，一方面将证书保存到资料库，另一方面将证书发送给 RA 模块。

7) RA 模块使用 P_0，通过 SM2 加密算法将证书反馈给安全设备。

当设备需要从系统中退网时，可在证书资料库中证书吊销列表(certificate revocation list，CRL)将证书吊销，或者管理者从证书资料中删除该设备的证书。

3 密钥协商

3.1 密钥协商流程

图 4 为密钥协商三次握手协议，发起设备和响应设备可以是安全设备或者 PKI。发起和响应设备均具有自身非对称密钥对，通过密钥协商后，取得公共会话密钥，并利用该公共密钥使用对称加密算法进行数据传输。

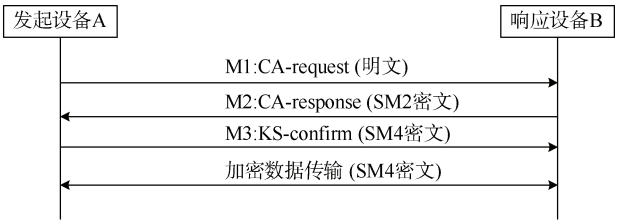


图 4 设备间的密钥协商三次握手

Figure 4 Three-way handshake for key negotiation between devices

设备 A 具备非对称密钥对(d_A，P_A)，设备 B 具备非对称密钥对(d_B，P_B)，设备 A 与设备 B 进行会话密钥 K_s 的协商的具体握手流程如下。

1) 设备 A 将自身证书和随机数 R_a 发送给设备 B，证书中包含发起设备 A 的公钥 P_a，私钥 d_a 由设备 A 秘密保存。

2) 设备 B 对证书验证通过后，使用设备 A 公钥

P_a，通过 SM2 加密算法将自身证书和随机数 R_b 发送给设备 A，证书中包含响应设备 B 的公钥 P_b，私钥 d_b 由设备 B 秘密保存。

3) 设备 A 通过参数 R_a、R_b、d_a 和 P_b 计算会话密钥 K_s，并利用该密钥使用 SM4 算法加密确认消息发给设备 A；设备 B 通过参数为 R_a、R_b、d_b 和 P_a 计算会话密钥 K_s，并利用该密钥使用 SM4 算法解密设备 A 发送的确认消息；设备 A 和设备 B 通过不同参数计算的会话密钥需一致，并由该密钥进行对称加密通信。

3.2 密钥协商机密性

本文借鉴了 Oakley 算法[14]思想进行密钥交换，密钥交换的过程中，仅交换双方的公钥信息，而不泄露任何私钥信息，实现会话密钥的协商。协商关键过程如下。

1) 设备 A 将自身公钥 P_A 和随机数 R_a 发送给设备 B。

2) 设备 B 将自身公钥 P_B 和随机数 R_b 发送给设备 A。

SM2 采用的椭圆曲线公钥算法中，使用的倍点计算公式为

$$P=d\cdot G \tag{1}$$

式中，P 为公钥；d 为私钥；G 为公开的椭圆曲线基点。

倍点计算公式满足交换律和结合律，全局变量 m 和 K 对应的计算式可分别表示为

$$m=d_A\cdot P_B=d_A\cdot d_B\cdot G=d_B\cdot d_A\cdot G=d_B\cdot P_A \tag{2}$$

$$K=R_a\cdot R_b\cdot d_A\cdot P_B=R_a\cdot R_b\cdot m=R_a\cdot R_b\cdot d_B\cdot P_A \tag{3}$$

当双方公钥交换完毕后，互相能够取得相同的全局变量 m。由于设备 A 和设备 B 的私钥没有在传输中出现，因此，即使第三方获取到所有信息，依然无法得到全局变量 m。

3) 为了防止第三方通过统计学攻击手段破解会话密钥，设备 A 和设备 B 在每次协商过程中，均产生一个随机数，该随机数的存在使得相同设备在每次协商过程会生成一个变化的全局变量 K，并使用该全局变量 K 作为密钥生成参数。

4) 使用 SM3 杂凑算法对 K 进行计算，得到对称加密算法的密钥 K_s，至此，完成密钥协商。

从上述流程可知，当所有数据均处于第三方窃取且第三方完全掌握相同算法的情况下，如果需要获取用户数据，则必须破解会话密钥，此时需要得到 K 值。由交换过程可知，第三方能够完全得到 P_A，R_a，P_B，R_b，G 这 5 个参数，由公式(2)可知，其仍需要得到 d_A 或者 d_B 才能得到 K 值。根据椭圆曲线公钥算法[15]，已知 $d_A\cdot G=P_A$ 和 $d_B\cdot G=P_B$，要得到 d_A 或者 d_B 则需要解决椭圆曲线算法中由 P 和 G 获得 d 的逆运算问题。若数字较大如 256 位，该逆运算的计算量将远远大于 RSA 中素数分解的计算量，这也是 SM2 算法加密强度优于 RSA 的基础，因此，可认为难以从公开的数据获取 K 值，也就保证了全开放环境下依然能够保证加密通信的特点。

4 设备通信

4.1 通信流程

本文 PKI 系统中设备间采用非对称加密算法协商会话密钥，对称加密算法通过会话密钥实现数据加密的方式，完成端到端的连接建立和数据交互。其中，非对称密码算法采用 SM2 算法，对称密码算法采用 SM4 算法。

SM2 算法加密强度高，保证会话密钥的机密性；SM4 算法效率高，保证数据传输效率；二者结合能够兼顾安全和效率。

设备间通信时，首先互相交互证书并验证，取得双方的公钥信息；然后通过公钥信息和私钥计算会话密钥；最后进行数据通信。当安全设备属于同一个 CA 域时，仅需要考虑域内 CA 验证，当安全设备属于不同 CA 域时，则需要考虑跨域 CA 验证。

安全设备通信流程如图 5 所示。PKI-1 与安全设备 A 属于同一个 CA 域，PKI-2 与安全设备 B 属于同一

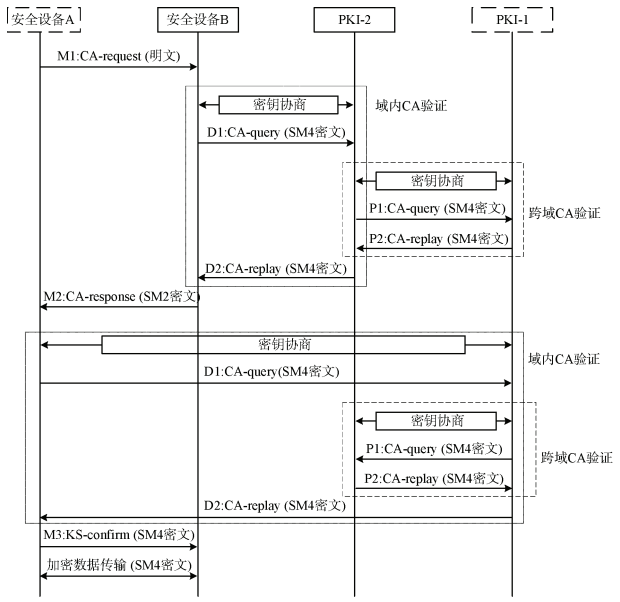


图 5 安全设备通信流程

Figure 5 Transmission process of safety equipment

个 CA 域。跨域通信中，握手过程需要进行跨域 CA 验证。由于本域设备不具备其他 CA 域的域内公钥，因此，本域设备无法对外域设备进行证书验签。当域内设备收到跨域设备的握手请求时，则必须将跨域设备的证书上报给 PKI，由 PKI 向跨域 PKI 进行证书查询。当 PKI-1 和 PKI-2 为同一个 PKI 时，则不需要进行跨域 CA 验证流程。

相比于通用的密钥协商握手，域内 CA 验证增加了向 PKI 查询证书正确性的过程。由于安全设备本身具备域内公钥 P_{CA}，可以进行证书的正确性验证。因此，CA 验证流程仅用于查询证书是否被吊销。

当安全设备从 CA 域中被行政移除，管理人员应在 PKI 系统中将被移除安全设备未过期的证书从证书资料库中标记为吊销，当其他设备查询时，吊销信息将被反馈给查询设备。当查询设备收到的 D2 中的信息为证书错误或证书已吊销，则拒绝握手，通过 M2 消息或 M3 消息拒绝连接。

4.2 效率分析

为了探究本系统在连接建立和数据传输中引起的时延开销，从算法效率和交互频次两个方面进行了分析。使用的测试环境为 1 核(vCPU)、1G 主频和 2GiB 内存安装 Ubuntu20.04 系统的小型工控机。

4.2.1 算法效率

利用 256bit 长度密钥的 SM2 算法对 174 byte 数据分别做了 10、10^2、10^3 和 10^4 次的加密和解密仿真，数据加密后长度变更为 284 byte，加密和解密过程时间消耗情况如表 1 所示。

表 1 SM2 算法加解密效率

Table 1 Encryption and decryption efficiency of SM2 algorithms ms

项目	10 次计算耗时	10^2 次计算耗时	10^3 次计算耗时	10^4 次计算耗时
加解密	15	152	1 503	15 018
加密	10	106	987	9 887
解密	5	50	499	4 996

通过 256 bit 长度密钥的 SM4 算法对 174 byte 数据分别做了 10^4、10^5 和 10^6 次的加解密仿真，时间消耗分别为 33 ms、332 ms 和 3 308 ms。

由 SM2 和 SM4 算法对 174 byte 数据的加解密仿真可知，一次 SM2 的加密和解密约消耗 1 ms 和 0.5 ms，一次 SM2 的数据发送接收需要消耗 1.5 ms；SM4 完成一次加解密数据的时间约为 3.3 μs，每秒钟能够完成 401.3 Mbyte 数据量的加解密，该算法加解密引起的时延可以忽略。

4.2.2 交互频次

由图 5 可知，两个设备间至少需要进行 3 次握手，才能确定会话密钥。一次证书查询需要进行密钥协商的 3 次交互和请求响应的 2 次交互，一共需要 5 次交互。

以车载设备与地面设备进行通信的典型场景为例，PKI 系统中设备间数据传输前协商会话密钥产生的时延分析如下。

令 t_w 为一次无线通信时延，t_l 为一次有线通信时延，t_e 为一次 SM2 数据的加解密时间总和，忽略 SM4 加解密时间。则有以下两种情况：

1) 两个设备属于相同 CA 域时，车载设备与地面设备间握手 3 次交互，两个设备分别与 PKI 设备进行身份查询的 5 次交互，共 13 次交互，其中相同 CA 域中设备间握手总时延 t_s 为

$$t_s=3t_w+t_e+5t_w+t_e+5t_l+t_e=8t_w+5t_l+3t_e \tag{4}$$

2) 两个设备属于不同 CA 域时，车载设备与地面设备间握手 3 次交互，两个设备分别与 PKI 设备进行身份查询的 5 次交互，PKI 设备间 10 次交互，其中跨域场景下设备间握手总时延 t_a 为

$$t_a=3t_w+t_e+5t_w+t_e+5t_l+t_e+10t_l+2t_e=8t_w+15t_l+5t_e \tag{5}$$

设备的跨域时延差 t_d 为

$$t_d=10t_l+2t_e \tag{6}$$

从上述分析可知，设备间握手时延由无线通信时延，有线通信时延和数据加解密时间共同构成。两个设备无论是否跨域均包含同样的无线通信频次，跨域引起的额外开销仅在有线通信时延和数据加解密时延中有所体现。

城市轨道交通系统的主流车地无线通信系统 LTE-M 系统标准[16]规定车地传输时延不超过 300 ms 的概率不小于 98%；而地面有线网络间的时延按照经验在 10 ms 以内。经过估算，两个设备属于相同 CA 域，握手时间 t_s 小于 2 454.5 ms 的概率大于 85%，属于不同 CA 域的握手时间 t_a 小于 2 557.5 ms 的概率大于 85%，t_d 约为 103 ms。按照实际 LTE-M 系统传输性能的现场测试[17]，其传输时延平均约为 20 ms，那么 t_s 约为 214.5 ms，t_a 约为 307.5 ms，t_d 约为 103 ms。以城市轨道交通典型的列车与地面区域控制中心通信为例，列车在初始投用时，设备开机和检车在分钟级，有足够的时间建立与地面设备的连接；列车在跨区域控制中心时，存在约 90 s 时间的通信重叠区，也就是有 90 s 的时间与地面设备

建立连接，也远远大于连接建立所需要的 t_s 时间。当列车连接建立后，SM4 算法引起的时延可忽略不计，因此，PKI 系统中设备间通信的效率能够得到保障。

此外，PKI 系统中设备完成会话密钥协商的时延能够进行优化，设备上线后立即与 PKI 设备进行握手并保存会话密钥，则能够将身份查询的 5 次交互降低为 2 次，相同 CA 域中设备间握手总时延 t_s 将降低 $3t_w+3t_l$ 的时间消耗，按照最不利情况，将降低约 37.9%的时延；不同 CA 域中设备间握手总时延 t_a 将降低 $3t_w+9t_l$ 的时间消耗，按照最不利情况，将降低 38.7%的时延；此外，PKI 中设备通过缓存机制，管理已验证设备的身份信息，可进一步降低设备间密钥协商握手引起的时间消耗。

5 结论

立足于城市轨道交通在开放网络空间数据传输的安全需求，结合城市轨道交通系统中设备按地域归属的特点，提出了一个基于国密算法的轻量级公钥基础设施解决方案。得出如下主要结论：

1) 将城市轨道交通系统看作集中分布式系统建立的设备间双向认证系统模型，能够满足设备从入网、运营和退网的全生命周期管理。

2) 采用的密钥协商流程基于SM2的不可逆特性，使用随机数和公钥自动协商会话密钥，可保障设备间通信的机密性。

3) 应用本文模型，在城市轨道及交通通信系统中设备间数据传输时延处于最大允许边界值的情况下，两个设备属于相同 CA 域，握手时间约为 2 454.5 ms，属于不同 CA 域的握手时间约为 2 557.5 ms；按照 LTE 系统网络平均时延计算，相同 CA 域握手时间约为 214.5 ms，跨域情况下握手时间约为 307.5 ms。握手产生的时延远小于列车跨区域控制中心时的通信重叠运行时间，效率能够得到保障。

参考文献

[1] 国家质量监督检验检疫总局，中国国家标准化管理委员会. 轨道交通 通信、信号和处理系统 第 2 部分：开放式传输系统中的安全相关通信：GB/T 24339.2—2009[S]. 北京：中国标准出版社，2010.
General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China, Standardization Administration of the People's Republic of China. Railway application: Communication signalling and processing systems: Part 2: Safety-related communication in open transmission systems: GB/T 24339.2—2009[S]. Beijing: Standards Press of China, 2010.

[2] 李继元. 铁路通信网络安全防护研究[J]. 中国铁路，2022(6): 94-98.
LI Jiyuan. Research on protection of railway communication network security[J]. China railway, 2022(6): 94-98.

[3] 张凯. RSSP-Ⅱ中消息认证码算法的安全性研究[D]. 兰州交通大学，2020.
ZHANG Kai. Research on the safety of message authentication code algorithm in RSSP-II[D]. Lanzhou: Lanzhou Jiaotong University, 2020.

[4] 张成阳，王金成，黄翌虹，等. 基于国密算法的列车控制系统传输加密研究[J]. 铁道通信信号，2024，60(1): 37-44.
ZHANG Chengyang, WANG Jincheng, HUANG Yihong, et al. Research on transmission encryption for train control system based on national cryptography algorithm[J]. Railway signalling & communication, 2024, 60(1): 37-44.

[5] 苗义烽，宋毅，张芸鹏. 基于国密算法的 TDCS/CTC 系统通信加密技术应用方案研究[J]. 铁道通信信号，2024，60(10): 58-64.
MIAO Yifeng, SONG Yi, ZHANG Yunpeng. Research on application scheme of communication encryption technology based on national cryptographic algorithms for TDCS/CTC system[J]. Railway signalling & communication, 2024, 60(10): 58-64.

[6] 屈毅，张卫军，杨锐. 铁路通信网密码技术应用研究[J]. 中国铁路，2023(10): 91-96.
QU Yi, ZHANG Weijun, YANG Rui. Research on application of railway communication network cryptography[J]. China railway, 2023(10): 91-96.

[7] 国家质量监督检验检疫总局，中国国家标准化管理委员会. 信息技术 安全技术 公钥基础设施 PKI 组件最小互操作规范：GB/T 19771—2005[S]. 北京：中国标准出版社，2005.
General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China, Standardization Administration of the People's Republic of China. Information technology--Security technology--Public key infrastructure--Minimum interoperability specification for PKI components: GB/T 19771—2005[S]. Beijing: Standards Press of China, 2005.

[8] 张宇，汪宗斌，秦体红. 基于 SM2 的高效签密方案[J]. 信息安全研究，2024，10(6): 526-531.
ZHANG Yu, WANG Zongbin, QIN Tihong. An efficient signcryption scheme based on SM2[J]. Journal of information security research, 2024, 10(6): 526-531.

（下转第 152 页）

[4] 王文静, 董子钰, 代森等. 高速列车撒砂装置振动特性及疲劳寿命研究[J]. 机械工程学报, 2023: 1-10.
WANG Wenjing, DONG Ziyu, DAI Sen, et al. Research on vibration characteristics and fatigue life of sanding device of EMU[J]. Journal of mechanical engineering, 2023: 1-10.

[5] LIU Yang, WU Xingwen, LIU Kaicheng, et al. An investigation into vibration-induced fatigue failure of metro vehicle cowcatcher and its structural improvement design[J]. Engineering failure analysis, 2023, 145: 107038.

[6] WEI Lai, SUN Yi, ZENG Jing, et al. Experimental and numerical investigation of fatigue failure for metro bogie cowcatchers due to modal vibration and stress induced by rail corrugation[J]. Engineering failure analysis, 2022, 142: 106810.

[7] CASOLARO A, CAPONE V, IANNUZZO G, et al. Deep learning for time series forecasting: advances and open problems[J]. Information, 2023, 14(11): 598.

[8] TIAN Jing. Quality evaluation of preschool video games based on RNN[J]. Entertainment computing, 2023, 47: 100581.

[9] ZHANG Jiaxuan, LI Shunyong. Air quality index forecast in Beijing based on CNN-LSTM multi-model[J]. Chemosphere, 2022, 308(1): 136180.

[10] BAI S, ZICO KOLTER J, KOLTUN V. An Empirical Evaluation of Generic Convolutional and Recurrent Networks for Sequence Modeling[J]. Arxiv, 2018. DOI: 01271.

（编辑：王艳菊）

（上接第 135 页）

[9] 沈荣耀, 马利民, 王佳慧, 等. 基于国密 SM2 算法的局部可验证聚合签名算法研究[J]. 信息安全研究, 2024, 10(2): 156-162.
SHEN Rongyao, MA Limin, WANG Jiahui, et al. Research on locally verifiable aggregate signature algorithm based on SM2[J]. Journal of information security research, 2024, 10(2): 156-162.

[10] ZHOU M X, RUAN S H, LIU J W, et al. vTPM-SM: an application scheme of SM2/SM3/SM4 algorithms based on trusted computing in cloud environment[C]//2022 IEEE 15th International Conference on Cloud Computing (CLOUD). Barcelona, 2022: 351-356.

[11] 孙敏, 陕童, 续森炜. 基于 I-SM4 和 SM2 的混合加密算法[J]. 计算机科学, 2023, 50(增刊 2): 869-872.
SUN Min, SHAN Tong, XU Senwei. Hybrid Encryption algorithm based on I-SM4 and SM2[J]. Computer science, 2023, 50(S2): 869-872.

[12] European Union Agency for Railways (ERA). SUBSET-038: ERTMS/ETCS System Requirements Specification[S]. Valenciennes: ERA, 2017.

[13] ITU-T. X.509: Information technology–Open Systems Interconnection–The Directory: Public-key and attribute certificate frameworks[S]. Geneva: international telecommunication union, 2019.

[14] KAUFMAN C, HOFFMAN P, NIR Y, et al. Internet Key Exchange Protocol Version 2 (IKEv2): RFC 7296[S]. Fremont: IETF, 2014.

[15] 国家密码管理局. SM2 椭圆曲线公钥密码算法 第 1 部分: 总则: GM/T 0003.1—2012[S]. 北京: 国家密码管理局, 2012.
National Cryptography Administration. Public key cryptographic algorithm SM2 based on elliptic curves-Part 1: General: GM/T 0003.1—2012[S]. Beijing: National Cryptography Administration, 2012.

[16] 中国城市轨道交通协会. 城市轨道交通车地综合通信系统(LTE-M)总体规范 第 1 部分: 系统需求: T/CAMET 04005.1—2018[S]. 北京: 中国城市轨道交通协会, 2018.
China Association of Metros. Long term evolution for metro (LTE-M)-Generic specification Part 1: System requirement: T/CAMET 04005.1—2018[S]. Beijing: China Association of Metros, 2018.

[17] 朱东飞, 洪婷. 城市轨道交通车地通信综合承载系统(LTE-M)性能测试与分析[J]. 城市轨道交通研究, 2017, 20(5): 171-175.
ZHU Dongfei, HONG Ting. Test and analysis of integrated service capacity for trainground communication based on metro LTE-M system[J]. Urban mass transit, 2017, 20(5): 171-175.

（编辑：王艳菊）