

基于开源鸿蒙操作系统的充电场站智能终端加解密自适应策略设计与实现

刘田豹, 李 孜, 王靖杨, 何明阳, 宋梓航, 陈昊佺, 席 萌

(四川中电启明星信息技术有限公司, 四川 成都 610000)

摘要: 硬件加解密技术具备安全性高、运算速度快和稳定性强等优势, 但也存在加密算法固定、灵活性欠佳以及修改部署成本高昂等问题。基于国产 RK3568 主控芯片与开源鸿蒙操作系统, 就充电场站对加密安全的需求, 将不同速率及算法支持的加解密芯片进行集成, 并设计一套基于国产主控芯片 RK3568 为调度核心, 依据需求自适应动态进行加解密芯片调度的优化方案。实验验证及试点表明, 系统运行状态良好, 可自由选择切换加解密方案, 并能够并行处理加解密需求, 进一步提高系统效率。

关键词: 电子技术; 加解密芯片及系统; 分级处理策略; 资源调度优化; 国产 RK3568

Design and implementation of adaptive encryption and decryption strategy for intelligent terminals in charging stations based on open-Harmony

LIU Tianbao, LI Zi, WANG Jingyang, HE Mingyang, SONG Zihang, CHEN Haoqu, XI Meng

(Aostar Information Technologies Co.,Ltd., Chengdu 610000, China)

Abstract: Hardware encryption and decryption technology offers advantages such as high security, fast operation speed, and strong stability. However, it also has limitations, including fixed encryption algorithms, lack of flexibility, and high costs for modification and deployment. Based on the domestic RK3568 main control chip and the open-source HarmonyOS, this study addresses the encryption security requirements of charging stations by integrating encryption and decryption chips that support different rates and algorithms. A dynamic and adaptive optimization scheme was designed, with the RK3568 chip as the core scheduler, to dynamically allocate encryption and decryption tasks based on demand. Experimental verification and pilot tests demonstrate that the system operates efficiently, allowing for flexible switching between encryption and decryption schemes while processing multiple encryption and decryption tasks in parallel, thereby further improving system efficiency.

Keywords: electronic technology; encryption and decryption chips and Systems; hierarchical processing strategy; resource scheduling optimization; domestic RK3568

0 引言

充电场站智能终端作为充电场站核心控制设备, 融合了物联网、大数据、通信等前沿技术, 是实现充电场站智能化管理与高效运营的关键^[1]。其功能涵盖充电控制与管理、用户交互服

务、数据采集与分析、场站管理以及能源管理与优化等多个方面^[2]。作为一种边缘设备, 充电场站智能终端流通的数据通常具有高度的敏感性。因此, 充电场站智能终端有较高的隐私加密需求, 以保证用户和系统的数据安全^[3]。

随着集成电路技术的高速发展和各行业对信息安全要求的不断提高,相比于基于CPU或MCU等通用处理器的可编程软件加密方案,硬件加解密芯片具有安全、高速、低耗能和高可信度等优点,可以有效增加黑客攻击和破解的难度,进而提高智能终端的安全性,确保用户个人信息和应用数据安全。因此,加解密芯片正越来越多地应用于各种智能终端中。然而,单个硬件加密芯片通常只能执行特定一个或几个种类的加密算法。智能终端一旦设计并嵌入某种加解密芯片,后期很难根据不同场景需求快速对其运行的加密算法进行变更乃至扩展^[4]。从长远来看,硬件加密的算法固定性和高更改成本缺陷也逐渐暴露出来。

本文提出了一种充电场站智能终端加解密方式自适应策略。在充电场站智能终端设计场景中,针对上述问题,从硬件和软件两方面对系统安全性进行改进。在硬件层面,通过集成多片可执行不同加解密方法且加解密速率各异的加解密芯片,缓解因替换加密芯片需重写硬件及改版导致的算法替换难题。在软件层面,设计了一种与上述模式相匹配的自适应策略,一方面,使得系统可以根据不同业务场景快速灵活地调度不同加解密芯片,实现不同速率加解密运算;另一方面,通过并行调用加解密芯片,实现并行加解密,进一步提高系统加解密性能上限。该设计解决了硬件加解密处理的灵活性和效率问题,提升了充电场站的数据安全。

1 国内外研究现状

1.1 国内研究现状

将多种相似功能芯片集成于一个系统,以此提升系统性能与功能扩展性,增强系统适应性,成为了一种新的系统研发思路。苏州海特公司提出一种网络安全主板系统,集成多种加密算法芯片,能依据交互数据灵活调整工作模式,增减子单元数量,满足金融、医疗等高要求行业需求。在加密领域,许多金融机构与科技公司合作,将物理加密卡分割为多个虚拟加密卡,配合多种国密算法,根据数据特性与传输环境调整加密策略^[5]。

除此之外,国内并无其他相关策略的系统及配套软件的研究。

1.2 国外研究现状

国外在多加密芯片集成领域有部分技术。Intel的SGX可以通过CPU集成多个安全飞地,实现多加密引擎并行处理,支持AES、RSA等算法协同工作。NVIDIA的GPU加速方案通过CUDA整合多个加密核,在服务器端实现每秒百万次加密运算,但其调度策略依赖固定优先级队列,存在成本较高、难以应用于车网终端的问题。

2 系统硬件设计

2.1 整体硬件架构

本系统核心板以国产RK3568工业级处理器作为主控芯片进行设计,采用四核64位Cortex-A55架构,主频2.0 GHz,集成瑞芯微自研NPU,具有1TOPS算力和丰富接口,可满足轻量级端侧AI计算。

遵循国家电网Q/GDW 11709.1—2017《电动汽车充电计费控制单元技术条件》要求,该充电场站安全智能终端加解密系统硬件整体设计如图1所示,RK3568核心板作为关键枢纽,通过总线与外部芯片实现互联互通。

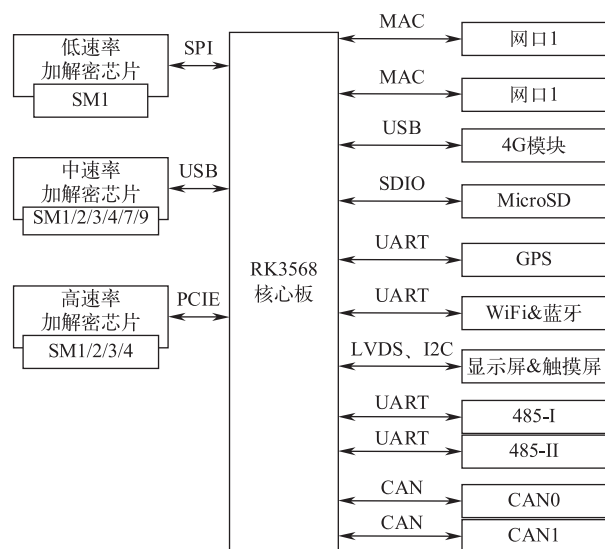


图1 充电场站智能终端硬件架构图

Fig. 1 Hardware architecture diagram of intelligent terminal for charging station

系统具有灵活的对接适配能力。核心板通过GPIO、MAC、USB、SDIO、UART、I2C等接口，与各类数据源进行对接，提供信息流通支撑。核心板通过MAC总线扩展出两个以太网口，以满足网络通信的需求；通过UART串口与外部对接，实现车联网智能终端所需相关通信及控制等功能。其中，UART1作为调试口，用于系统调试与维护；UART2和UART3作为两个485通信口，用于工业环境中的数据传输；UART4集成GPS模块，为终端提供定位功能；UART5集成WiFi蓝牙模块，为系统提供无线通信能力。

在数据加解密处理方面，将RK3568通过SPI、USB、PCIE总线分别连接不同加解密芯片。其中，SPI总线用于扩展低速率加解密芯片，该芯片专为实现低速SM1国密算法设计，满足特定场景下对低速对称数据加密的需求；USB总线连接的中速率加解密芯片，能够支持SM1、SM2、SM3、SM4、SM7、SM9等多种国密算法^[6-11]，可适应多样化的加密要求；PCIE总线与高速率加解密芯片相连，支持高速SM1、SM2、SM3、SM4等多种国密算法。通过RK3568系统中的调度算法，可将加解密任务分派给三个加密芯片并行处理。

2.2 低速率加解密芯片硬件设计

系统选用SC1716Y作为低速率加解密芯片。SC1716Y是国网内部专用芯片，集成实现了SM1算法模块，能够完成低速的数据加解密任务。

如图2所示，SC1716Y使用四根SPI数据总线，即主出从入（MOSI）、主入从出（MISO）、时钟信号（CLK）和片选信号（CS0）。其中，MOSI和MISO负责数据的传输；CLK负责提供时钟同步信号，确保数据传输的准确性和稳定性；CS0负责芯片选定信号传输，在系统连接多个设备进行并行管理时实现有效控制。

为了灵活管理芯片的电力供应,确保其在稳定的电压环境下工作,芯片采用晶闸管S8550进行供电控制。当需要对芯片进行断电或复位操作时,SC1716Y通过控制信号接口SPI2 Control输

入相应的控制信号，从而实现对芯片状态的精准控制。

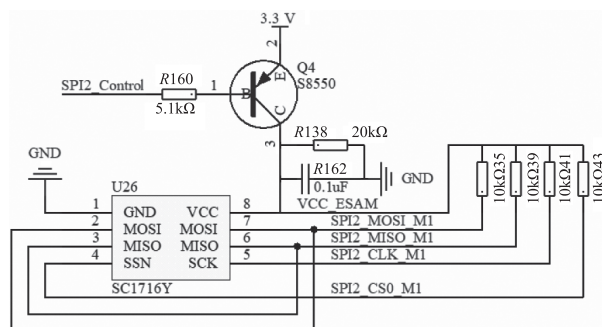


图2 低速率加解密芯片

Fig. 2 Low-speed secure chip

2.3 中速率加解密芯片硬件设计

系统采用HSCTU作为中速率加解密芯片，其控制支持电路如图3所示。该芯片支持SM1、SM2、SM3、SM4、SM9国密算法及AES、DES、ECC、RSA、SHA国际加密算法，这些算法包括对称、非对称和杂凑算法，可以满足不同场景下复杂的数据交互和加密需求。此外，相比于SC1716Y，HSCTU具有更丰富的算力资源，能够提供更快的加解密计算速度；HSCTU还具有较大的片上存储资源，可以作为复杂算法，用于高效处理大量数据。

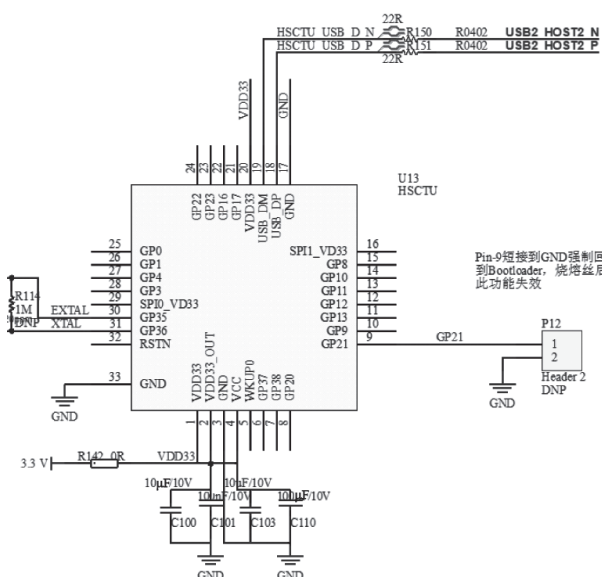


图3 中速率加解密芯片

Fig. 3 Medium-speed secure chip

在系统中，HSCTU通过一对USB2.0的数据线总线与RK3568相连。另有一个GP21调试接口引出，用于后期芯片升级程序或调试，其他电源引脚接入相应的退耦电容，以避免不必要的干扰。

2.4 高速率加解密芯片硬件设计

系统采用PLUTO-08-A1作为高速率加解密芯片，如图4所示，通过PCIE总线与RK3568相连。PLUTO-08-A1作为密码卡，加密能力强，支持SM1、SM3、SM4、SM7、SM9国密算法及AES、DES、ECC、SHA国际加密算法。此

芯片提供多种算法性能级别，用户能按需灵活配置。值得一提的是，该芯片本身支持多进程任务并行，且任务间资源隔离，能够极大提升系统并发处理能力。

在本系统中，采用两对数据线PCIE20_TX、PCIE20_RX，实现PLUTO-08-A1的数据收发，一对时钟线PCIE20_REFCLK保障数据同步，确保高速传输稳定准确。同时，配备一个唤醒信号与一个复位信号，便于芯片电源管理与状态控制，在系统启动、待机及异常恢复时调用。

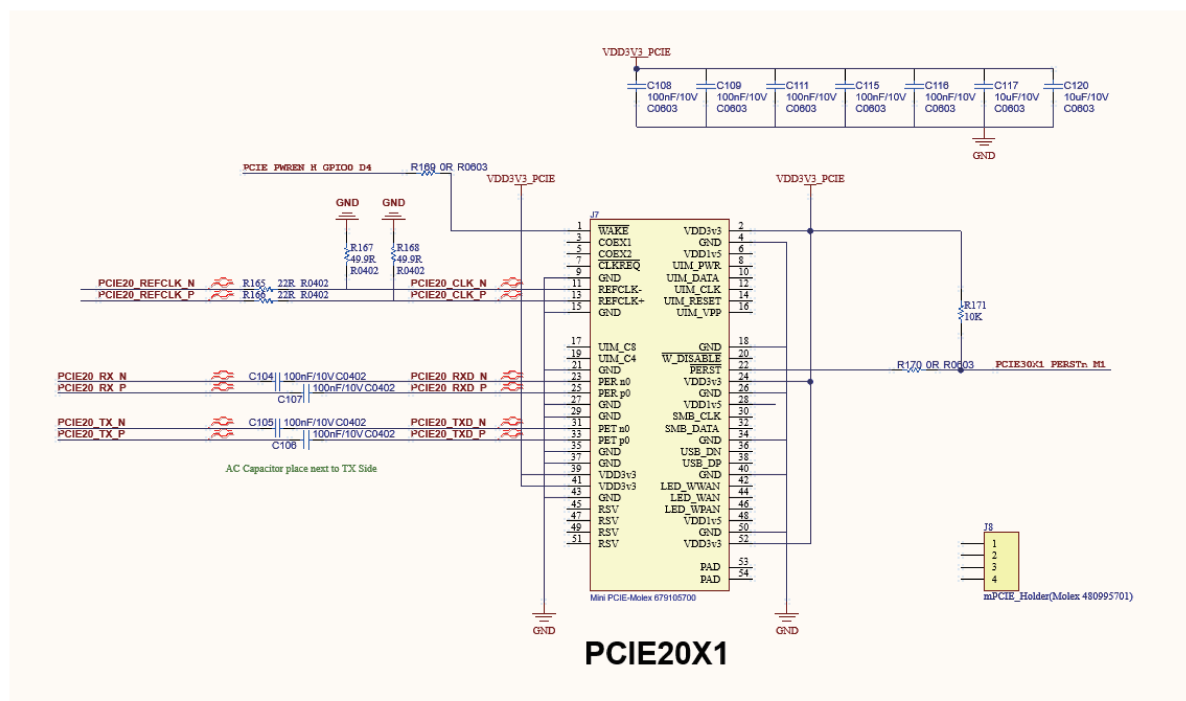


图4 高速率加解密芯片

Fig. 4 High-speed secure chip

3 系统软件设计

3.1 加解密系统软件架构

为提升多芯片与多种加解密调度程序的维护便捷性和运行效率，首先采用软件定义硬件技术构建加解密模块的模型。基于SPI、USB、PCIE三种硬件接口类型，在采用开源鸿蒙操作系统基础上，将加解密芯片定义为三类软件模型，并以JSON文件形式保存。模型涵盖信息包括芯片

厂商、支持的加解密算法及对应接口信息、加解密速率、最大处理字节数、通信协议以及是否使能等。为便于管理与调度，定义了加解密模块的四种性能等级，即低速率、中速率、高速率以及并行速率，分别对应通过SPI通信的SC1716Y、USB通信的HSCTU、PCIE通信的PLUTO-08-A1以及多模块并行加解密控制状态。更具体的软件加解密控制系统的运行流程架构如图5所示。

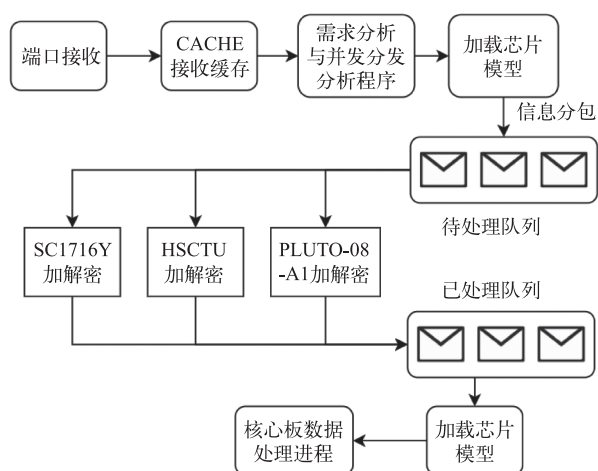


图5 加解密系统架构运行流程

Fig. 5 Operation flow of the encryption and decryption system architecture

当任意通信端口接收到待加密数据后，系统调度程序首先将数据存入缓存区。随后，系统遍历检查所有可用的加密芯片，依据待加密数据包中的加解密需求及当前芯片占用和调度情况进行分析，基于调度算法，选取最优化总体吞吐量的处理芯片，或者将任务拆分后由多个芯片分别处理；接着，系统基于调度结果，对待处理数据加载对应需求芯片的软件模型，标记并存入待处理队列。在加解密算法运算结束后，将处理结果置入结果序列，交由系统中相关的数据返回进程做进一步处理。

3.2 加解密任务分发控制

(1) 相同加密算法在不同加密芯片方式下的实现时间计算

在实际应用场景中，对于同一种算法需求的数据，系统可能会调配不同速率的加解密芯片，实现并发处理。为制定科学合理的任务分配策略，需估算不同加解密核心运行算法的耗时，下面以SM1为例，其余算法同理。

已知三个芯片都支持SM1算法，假设三个芯片同时通过SM1处理加密数据。设三个加密芯片分别以对应接线的满带宽状态从RK3568核心板获取待加密信息，并在完成加解密后立即返回验证结果。已知通常情况下，SPI、USB、PCIE的带宽分别为10 Mbit/s、100 Mbit/s和3 800 Mbit/s。

在每个数据包为64 B的条件下，三个加解密芯片的SM1算法处理性能分别为20 Mbit/s、26 Mbit/s和30 Mbit/s。

低速核心受限于SPI接线的带宽，其最高吞吐量有限，在需生成大量加密密文时，无法在1 s内传输完所有加密信息。此时，其耗时可以粗略计算为

$$T_{\text{slow}} = \frac{V}{B_s} \quad (1)$$

式中， V 为加解密结果体积； B_s 为SPI带宽。

对于中速和高速加解密芯片，其理论耗时为

$$T_{\text{M/H}} = \frac{V}{C_{\text{M/H}}} \quad (2)$$

式中， $T_{\text{M/H}}$ 为中速和高速加解密芯片处理耗时； $C_{\text{M/H}}$ 为对应加解密芯片处理速度。

将上述数据代入，对于处理结果为100 Mbit的加解密任务，由于SM1是对称加密算法，处理结果仍为100 Mbit，此时，系统计算得出预算的低、中、高速加解密芯片的耗时分别为10 s、3.84 s和0.02 s，系统将基于上述预估结果进行调度。

(2) 加密并行调度算法

结合充电场站场景，本文设计了一种针对性的调度算法。在充电场站的实际应用场景中，由于非对称加密安全性高，对称加密速度快，为充分发挥两者优势，本方案将两类算法结合互补使用。在密钥交换与信息交互环节，终端自启动时生成SM2密钥对并公布公钥。当新节点与终端对接时，新节点先以自身标识等作为种子，通过SM2算法获得自身密钥对。随后，终端与节点之间利用SM2算法交换安全需求等级，选择对称加密算法，预估加解密信息量等关键信息。

完成信息交互后，进入算法与芯片选择阶段。系统为每个加解密芯片设置独立的待处理消息队列。当各加解密芯片消息处理队列均为空时，根据安全需求确定对称加密算法。除非特殊指定，若消息安全性要求极高，采用SM1算法；若安全性要求一般，默认采用SM4算法；若消息来源计算能力有限，采用SM7算法。

芯片选择依据数据量大小, 具体为: 数据量小于1 MB时, 优先调用SC1716Y芯片执行SM1算法进行加解密; 数据量在1~10 MB之间时, 优先选用HSCTU芯片; 若数据量大于10 MB, 优先选用 PLUTO-08-A1芯片。当某个加解密芯片消息队列为空, 或默认芯片处于拥塞状态且该芯片能执行满足安全性需求的加密算法时, 进入并行处理状态。通过式(1)、式(2)分别计算默认芯片和转调任务给空闲芯片的加解密耗时, 将任务调度至使系统总耗时更短的芯片进行处

理, 以此优化系统整体性能。

4 实验验证

本文基于所述硬件架构, 使用C语言实现系统配套的加解密自适应策略软件, 整体实现系统并行测试, 以检验设计的正确性和可行性。

4.1 实验场景

本实验基于RK3568核心板的充电场站智能终端, 终端的最终配置信息见下表。

表 多芯片加解密系统速度测试

Tab. Multi-core encryption chip encryption and decryption speed test

(单位: Mbit/s)

算法	模式	64 B	128 B	256 B	512 B	1 024 B	1 536 B	2 048 B	4 096 B	8 192 B	16 384 B
SM1	ecb	34.91	64.7	143.12	210.07	270.25	330.5	354.15	240.21	291.96	331.28
	cbc	34.63	64.31	141.89	213.26	282.61	320.89	351.26	241.47	292.03	330.37
SM4	ecb	81.28	142.78	267.25	481	918.71	1 244.56	1 469.91	2 356.05	2 439.35	2 407.6
	cbc	69.88	135.1	252.3	463.69	864.49	1 193.61	1 452.85	2 302.08	2 324.14	2 443.12
SM7	ecb	12.03	17.33	22.28	25.97	28.45	29.42	30.06	30.08	32.77	32.77
	cbc	11.56	16.84	21.85	25.77	28.29	29.29	29.97	29.88	32.68	32.77
AES	ecb	13.16	20.41	28.23	34.84	39.59	41.42	42.55	42.65	45.02	45.88
	cbc	12.35	19.46	27.31	34.12	39.11	41.07	42.28	42.63	44.3	45.88
DES	ecb	13.08	20.07	27.41	33.36	37.66	39.14	40.34	40.98	42.6	45.88
	cbc	12.73	19.61	26.96	33.26	37.48	39	40.21	40.96	42.7	45.88

本次实验环境以RK3568作为主控芯片, 设计了多种加解密芯片为载体。该终端配置具有四核心, 主频可达 2.0 GHz, 物理内存总量为 2 GB, eMMC存储大小为16 GB, 采用开源鸿蒙操作系统。

在测试中, 通过网线将计算机与充电场站智能终端的网口相连以完成数据交互, 在计算机侧使用超级终端工具进行命令输入和结果查看。

4.2 PCIE高速加解密性能验证

模拟运行系统后, 通过在模拟实验包的config.ini中的performance字段增加sm4_ECB_test=y和sm4_cbc_test=y的方式, 先后选中测试模式ecb与cbc运行SM1、SM4、SM7、AES、DES加密算法, 并进行运行速度测验。cbc相较于ecb, 多一步将数据分为多节, 后一节与前一节异或运算后才代入计算。最后, 在ssh调试口上运行测试程序test_symm_cp_pert, 使其模拟运行不同结果长度目标的多种称加解密算法。测试程序开

启100个线程, 每个线程以一定速度注入待加解密字段模拟场站场景, 运行结束显示100个线程在2 s内总共进行运算的数据量, 吞吐量单位为Mbit/s。

本系统的自适应调度算法在多芯片协同处理中表现出显著优化效果。一般而言, 随着加密内容包的提升, 单个包的信息提取速度更快, 加解密效率更高, 但会逐渐接近一个瓶颈。而在本文所述系统中, 首先, 由于调度系统的动态任务分配机制, 多个不同速率芯片形成协同处理网络, 吞吐量提速态势会保持更久, 最终接近一个更高的速度上限。另外, 可能会出现吞吐量异常下降后继续上升的现象, 这是因为任务调度后高速芯片完成任务, 而中速芯片还存在部分未完成加密内容, 造成总体吞吐量短暂下降。实验数据证实了上述猜想, 具体表现为:

1) SM1算法在2 048 B时ecb模式达354.15 Mbit/s, 4 096 B骤降至240.21 Mbit/s后回升至331.28 Mbit/s。这种“下降-回升”曲线直接

印证了调度系统的分流机制。当数据量突破 1 MB 阈值时，系统将20%任务转调至中速芯片，虽然瞬时速度下降，但通过多芯片协同，整体吞吐量提升，增速曲线符合理论耗时对比模型的预测。

2) SM4算法在1 024 B时ecb模式达918.71 Mbit/s，16 384 B时稳定在2 407.6 Mbit/s；cbc模式通过并行预处理策略，在16 384 B达到2 443.12 Mbit/s。这种持续增长态势验证了数据量分级调度策略的有效性，系统在10 MB阈值后遵循高速芯片优先原则，通过预判性任务拆分实现cbc模式的反超，体现了混合调度策略的优势。

3) SM7算法在1 024 B前快速增长（ecb达28.45 Mbit/s），之后增速趋缓并稳定在32.77 Mbit/s。这一趋势反映了系统对轻量级算法实施的小数据优先策略。64 B时HSCTU芯片处理占比达 85%，确保低延迟响应；当数据量超过1 MB后，通过错峰调度维持稳定输出，体现了资源受限场景下的适应性优化。

4) 国际算法AES/DES在512 B后增速显著放缓，但通过混合调度策略仍实现性能提升。AES-ECB 在16 384 B时达45.88 Mbit/s，较单芯片处理提升22%；DES算法在4 096 B后出现波动，但调度系统通过动态调整任务队列，仍保障最终吞吐量与AES持平。

综上所述，实验数据表明，本系统的自适应调度算法通过数据量分级调度与动态分流机制，有效提升了多芯片协同处理能力。

5 结束语

本研究基于国产RK3568主控芯片与开源鸿蒙操作系统，针对充电场站智能终端的安全通信需求，设计并实现了一套自适应加解密策略，解决了所述场景硬件加密算法需求高、硬件支持算法固定且算力有限的问题。通过集成多种支持不同速率和算法的加解密芯片，结合软件定义硬件的思想，系统能够根据业务场景动态调度加解密任务，提升了系统的灵活性和效率。实验结果表明，该方案不仅能够满足充电场站对高安全性和高效处理的需求，而且能够通过并行加解密进一

步优化系统性能。

参考文献

[1] 杨校辉, 邱俊宏, 张娟, 等. 一种基于综合能源优化调配的充电站运营管理系统研究[J]. 电力系统保护与控制, 2021, 49(5): 173-179.

[2] 王伟贤, 朱洁, 田贺平, 等. 电动汽车充电桩-后台服务管理中心信息安全防护方案设计与实现[J]. 电力建设, 2019, 40(5): 55-62.

[3] 周衍涛, 戴军, 苑惠丽, 等. 城市电动汽车充电设施需求预测与规划布局研究[J]. 电力系统保护与控制, 2021, 49(24): 177-187.

[4] 盛戈皞, 钱勇, 罗林根, 等. 面向新型电力系统的数字化电力设备关键技术及其发展趋势[J]. 高压电压技术, 2023, 49(5): 1765-1778.

[5] 李建立, 莫燕南, 栗涛, 等. 基于国密算法SM2、SM3、SM4的高速混合加密系统硬件设计[J]. 计算机应用研究, 2022, 39(9): 2818-2825, 2831.

[6] 闫永昭, 郑金州. 基于国密SM1算法的CPU卡应用[J]. 现代电子技术, 2013, 36(15): 82-83, 87.

[7] 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.

[8] 王小云, 于红波. SM3密码杂凑算法[J]. 信息安全研究, 2016, 2(11): 983-994.

[9] 吕述望, 苏波展, 王鹏, 等. SM4分组密码算法综述[J]. 信息安全研究, 2016, 2(11): 995-1007.

[10] 王洁民, 陈坚. 基于我国自主密码算法的RFID安全应用系统研究[J]. 计算机应用与软件, 2010, 27(9): 53-55, 74.

[11] 袁峰, 程朝辉. SM9标识密码算法综述[J]. 信息安全研究, 2016, 2(11): 1008-1027.

作者简介

刘田豹（1982—），男，硕士，高级工程师，研究方向为配用电自动化、智能硬件等。
(收稿日期：2025-02-16)