易科腾
EQTINFO

PRODUCT
MANUAL
产品手册

易科腾

EQD CC120 系列密码卡

www.e-quantum.com

产品介绍

EQD CC120 系列密码卡是一款基于国产加密芯片、提供 PCI-E 接口或 M.2 接口的高性能硬件密码模块产品，满足国密标准相关要求，适用于各类密码安全设备和密码应用系统，提供高速的、多任务并行处理的密码运算，可以满足系统数据的签名/验证、加密/解密的要求，确保信息的机密性、完整性、真实性和不可抵赖性，同时提供安全、完善的密钥管理机制，结合 CryptoDev 和 DPDK 还可满足网络安全和 VPN 安全连接等场景的高吞吐数据加解密要求。

产品特点

内禀随机性
双 WNG 系列物理噪声源芯片，可选 QRNG 量子随机数芯片。

高性能大容量
高达 18Gbps 的加解密性能，最多支持 10240 对非对称密钥对，支持用户态 DPDK 高性能加解密转发。

符合商密检测要求
遵循商密规范，符合密评三级要求，商用密码产品认证证书编号 GM003210420220467。

妥善的应急保护
支持过热保护，可适应无风环境工作；支持应急复位、优雅重启。

灵活的接口定制
支持标准 SDF 接口，支持 SDF 扩展接口，支持基于数字信封密钥导入接口。

支持内核态应用
支持内核态 CryptoDev 接口，可在内核调用密码卡编程接口，支持同步/异步调用模式。

支持功能卸载
支持功能 Offload 定制，如 SSL 业务卸载，由密码卡完成相关功能，提升系统/设备的整体性能。

多档性能可选
产品系列囊括低、中、高等多档位性能产品，可适配不用场景、层次的密码卡需求。

高度国产化
产品系列主器件全国产化，安全合规、自主可控，支持全器件国产化定制。

适配管理便捷
提供管理工具的参考源码，提供基于国密 SSL 密钥/证书管理的 Demo 源码。

产品功能

真随机数生成
支持双 WNG 系列物理噪声源芯片、QRNG 量子随机数芯片生成真随机数。

国内外密码算法
国产算法 SM1、SM2、SM3、SM4，国际算法 AES、SHA1、SHA256、RSA1024、RSA2048 等。

三级密钥管理体系
三级密钥分别为系统保护密钥、用户密钥对及密钥加密密钥、会话密钥，逐层加密。

安全密钥存储
用户密钥对及密钥加密密钥通过系统保护密钥加密保护，以密文的形式存储在密码卡中。

密钥备份及恢复
支持密钥的备份和恢复功能，保证安全应用系统的安全性和可靠性。

用户访问权限控制

管理员、操作员、审计员分级的权限控制机制，UKey 联动，提高密码设备的安全性。

SSL 加解密卸载

支持 SSL 加解密卸载，减轻服务器加解密负荷，提升系统整体流量性能。

虚拟化

支持 SR-IOV 技术，最大 VF 数量可达 31 个。

产品参数

表格 1 PCIE 接口密码卡规格参数

PCI-E 接口系列	CC120-L10	CC120-L20	CC120-L30	CC120-M	CC120-G
尺寸（宽×高×深）	180.9mm x 120.8mm x 21.6mm				
外壳结构	PCB+金属封盖，材质铝型材				
MTBF	≥25000 小时				
工作环境	温度 0℃～ 40℃，湿度 30%～90%				
存贮环境温度	温度-40℃～ 55℃，湿度 20%～93%（40℃）				
硬件接口	PCI-E				
算法支持					
支持的非对称算法	SM2_SIGN、SM2_ENC、RSA_SIGN、RSA_ENC				
支持的对称算法	SM1_ECB、SM1_CBC、SM1_CFB、SM1_OFB、SM4_ECB、SM4_CBC、SM4_CFB、SM4_OFB、SM4_GCM、AES128_ECB、AES128_CBC、AES128_CFB、AES128_OFB、AES256_ECB、AES256_CBC、AES256_CFB、AES256_OFB				
支持的摘要算法	SM3、SHA-1、SHA256				
消息认证码算法	HMAC-SM3				
算法性能***					
SM1 加解密（ECB）	390 Mbps	800 Mbps	3 Gbps	10.3 Gbps	10.5 Gbps
SM1 加解密（CBC）	380 Mbps	770 Mbps	3 Gbps	9.9 Gbps	10.1 Gbps
SM2 签名	0.5 万次/秒	1.7 万次/秒	3.4 万次/秒	10 万次/秒	18 万次/秒
SM2 验签	0.2 万次/秒	0.6 万次/秒	1.2 万次/秒	3.8 万次/秒	6.4 万次/秒
SM2 加密	0.1 万次/秒	0.3 万次/秒	0.7 万次/秒	2.3 万次/秒	4 万次/秒
SM2 解密	0.1 万次/秒	0.5 万次/秒	0.9 万次/秒	2.9 万次/秒	5 万次/秒
SM3 杂凑算法	800 Mbps	1.6 Gbps	3 Gbps	12 Gbps	19 Gbps
SM4 加解密（ECB）	600 Mbps	1.2 Gbps	3 Gbps	12 Gbps	16 Gbps

PCI-E 接口系列	CC120-L10	CC120-L20	CC120-L30	CC120-M	CC120-G
SM4 加解密（CBC）	570 Mbps	1.2 Gbps	3 Gbps	12 Gbps	16 Gbps
RSA1024 加密	6400 次/秒	22000 次/秒	45000 次/秒	120000 次/秒	170000 次/秒
RSA1024 解密	110 次/秒	400 次/秒	800 次/秒	2500 次/秒	4200 次/秒
RSA1024 签名	110 次/秒	400 次/秒	800 次/秒	2500 次/秒	4200 次/秒
RSA1024 验签	6400 次/秒	22000 次/秒	45000 次/秒	120000 次/秒	180000 次/秒
RSA2048 加密	3300 次/秒	11000 次/秒	23000 次/秒	70000 次/秒	120000 次/秒
RSA2048 解密	20 次/秒	100 次/秒	200 次/秒	600 次/秒	1000 次/秒
RSA2048 签名	20 次/秒	100 次/秒	200 次/秒	600 次/秒	1000 次/秒
RSA2048 验签	3300 次/秒	11000 次/秒	23000 次/秒	70000 次/秒	120000 次/秒
AES256 加解密	500 Mbps	1 Gbps	2 Gbps	7 Gbps	15 Gbps
HASH（SHA256）	300 Mbps	600 Mbps	3 Gbps	8 Gbps	8 Gbps
随机数生成	14Mbps	19Mbps	30Mbps	33Mbps	35Mbps
随机数源	双随机数源				
量子真随机数*	175Kbps				
权限管理					
管理员数量	3 个		操作员数量	3 个	
容量					
SM2 密钥对**	1024（1k）	2048（2k）	4096（4k）	6144（6k）	10240（10k）
RSA 密钥对**	128	128	256	512	736
密钥加密密钥数量	256	1024（1k）	2048（2k）	4096（4k）	4096（4k）
会话密钥数量	4096（4k）	8192（8k）	16384（16k）	32768（32k）	65000（64k）
文件系统容量	32KB				
虚拟化					
SR-IOV	4	4	4	16	31
架构/系统适配					
CPU 架构	Intel Atom、Xeon、Hygon CPU、飞腾、ARM64。				
操作系统	Ubuntu 18.04/20.04/22.04，CentOS 7.9/8.5/stream-9，统信 UOS，麒麟 Linux 等。				

表格 2 M.2 接口密码卡规格参数

M.2 Key B&M 接口系列	CC120-LM10	CC120-LM20	CC120-LM30	CC120-MM
尺寸（宽×长×高）	30mm×80mm×12.6mm			
外壳结构	PCB+散热器			
MTBF	≥25000 小时			
工作环境	温度 0℃～ 40℃，湿度 30%～90%			

M.2 Key B&M 接口系列	CC120-LM10	CC120-LM20	CC120-LM30	CC120-MM
存贮环境	温度-40℃～ 55℃，湿度 20%～93%（40℃）			
硬件接口	M.2 Key B&M			
算法支持				
支持的非对称算法	SM2_SIGN、SM2_ENC、RSA_SIGN、RSA_ENC			
支持的对称算法	SM1_ECB、SM1_CBC、SM1_CFB、SM1_OFB、SM4_ECB、SM4_CBC、SM4_CFB、SM4_OFB、SM4_GCM、AES128_ECB 、 AES128_CBC 、 AES128_CFB 、 AES128_OFB 、 AES256_ECB 、 AES256_CBC 、 AES256_CFB、AES256_OFB			
支持的摘要算法	SM3、SHA-1、SHA256			
算法性能***				
SM1 加解密（ECB）	390 Mbps	800 Mbps	3 Gbps	10.3 Gbps
SM1 加解密（CBC）	380 Mbps	770 Mbps	3 Gbps	9.9 Gbps
SM2 签名	0.5 万次/秒	1.7 万次/秒	3.4 万次/秒	10 万次/秒
SM2 验签	0.2 万次/秒	0.6 万次/秒	1.2 万次/秒	3.8 万次/秒
SM2 加密	0.1 万次/秒	0.3 万次/秒	0.7 万次/秒	2.3 万次/秒
SM2 解密	0.1 万次/秒	0.5 万次/秒	0.9 万次/秒	2.9 万次/秒
SM3 杂凑算法	800 Mbps	1.6 Gbps	3 Gbps	12 Gbps
SM4 加解密（ECB）	600 Mbps	1.2 Gbps	3 Gbps	12 Gbps
SM4 加解密（CBC）	570 Mbps	1.2 Gbps	3 Gbps	12 Gbps
RSA1024 加密	6400 次/秒	22000 次/秒	45000 次/秒	120000 次/秒
RSA1024 解密	110 次/秒	400 次/秒	800 次/秒	2500 次/秒
RSA1024 签名	110 次/秒	400 次/秒	800 次/秒	2500 次/秒
RSA1024 验签	6400 次/秒	22000 次/秒	45000 次/秒	120000 次/秒
RSA2048 加密	3300 次/秒	11000 次/秒	23000 次/秒	70000 次/秒
RSA2048 解密	20 次/秒	100 次/秒	200 次/秒	600 次/秒
RSA2048 签名	20 次/秒	100 次/秒	200 次/秒	600 次/秒
RSA2048 验签	3300 次/秒	11000 次/秒	23000 次/秒	70000 次/秒
AES256 加解密	500 Mbps	1 Gbps	2 Gbps	7 Gbps
HASH（SHA256）	300 Mbps	600 Mbps	3 Gbps	8 Gbps
随机数生成	14Mbps	19Mbps	25Mbps	33Mbps
随机数源	双随机数源			
权限管理				
管理员数量	3 个	操作员数量	3 个	
容量				
SM2 密钥对**	1024（1k）	2048（2k）	4096（4k）	6144（6k）

M.2 Key B&M 接口系列	CC120-LM10	CC120-LM20	CC120-LM30	CC120-MM
RSA 密钥对**	128	128	256	512
密钥加密密钥数量	256	1024（1k）	2048（2k）	4096（4k）
会话密钥数量	4096（4k）	8192（8k）	16384（16k）	32768（32k）
文件系统容量	32KB			
虚拟化				
SR-IOV	4	4	4	16
架构/系统适配				
CPU 架构	Intel Atom、Xeon、Hygon CPU、飞腾、ARM64。			
操作系统	Ubuntu 18.04/20.04/22.04，CentOS 7.9/8.5/stream-9，统信 UOS，麒麟 Linux 等。			

备注一：

测试环境，CPU：Xeon(R) Silver 4208@2.10GHz；内存：8G；卡线程数：64。

*量子真随机数，由量子随机数芯片产生，仅 PCIE 密码卡可选。

**非对称密钥对，SM2 和 RSA，支持资源划分，常用规格之外可根据实际需要另做调整。

***主表测试数据的包大小为 4096，其他包大小的性能数据见后文副表。

表格 3 密码卡规格参数副表

算法及包大小	L10/LM10	L20/LM20	L30/LM30	M/MM	G
SM1-ECB-256	340 Mbps	700 Mbps	1.4 Gbps	1.6 Gbps	1.6 Gbps
SM1-ECB-512	360 Mbps	750 Mbps	2.3 Gbps	3.1 Gbps	3.2 Gbps
SM1-ECB-1024	370 Mbps	780 Mbps	2.6 Gbps	5.9 Gbps	6 Gbps
SM1-ECB-2048	380 Mbps	800 Mbps	2.9 Gbps	9.8 Gbps	9.9 Gbps
SM1-CBC-256	330 Mbps	680 Mbps	1.4 Gbps	1.5 Gbps	1.6 Gbps
SM1-CBC-512	350 Mbps	720 Mbps	2.3 Gbps	3.1 Gbps	3.2 Gbps
SM1-CBC-1024	360 Mbps	750 Mbps	2.6 Gbps	5.8 Gbps	5.9 Gbps
SM1-CBC-2048	370 Mbps	770 Mbps	2.9 Gbps	9.5 Gbps	9.6 Gbps
SM3-256	590 Mbps	1 Gbps	1.1 Gbps	1.2 Gbps	1.3 Gbps
SM3-512	690 Mbps	1.4 Gbps	2.1 Gbps	2.5 Gbps	2.6 Gbps
SM3-1024	750 Mbps	1.5 Gbps	2.5 Gbps	5 Gbps	5.1 Gbps
SM3-2048	780 Mbps	1.6 Gbps	2.9 Gbps	9.8 Gbps	9.9 Gbps
SM4-ECB-256	440 Mbps	0.9 Gbps	1.4 Gbps	1.6 Gbps	1.6 Gbps
SM4-ECB-512	520 Mbps	1.1 Gbps	2.3 Gbps	3.2 Gbps	3.3 Gbps
SM4-ECB-1024	570 Mbps	1.1 Gbps	2.7 Gbps	6.3 Gbps	7 Gbps
SM4-ECB-2048	600 Mbps	1.2 Gbps	2.9 Gbps	11 Gbps	11 Gbps
SM4-CBC-256	420 Mbps	0.8 Gbps	1.4 Gbps	1.6 Gbps	1.9 Gbps

算法及包大小	L10/LM10	L20/LM20	L30/LM30	M/MM	G
SM4-CBC-512	500 Mbps	1 Gbps	2.3 Gbps	3.3 Gbps	3.6 Gbps
SM4-CBC-1024	570 Mbps	1.2 Gbps	2.6 Gbps	6.1 Gbps	6.2 Gbps
SM4-CBC-2048	600 Mbps	1.3 Gbps	2.9 Gbps	11.2 Gbps	11.6 Gbps
AES256-256	470 Mbps	0.9 Gbps	1.4 Gbps	1.5 Gbps	1.6 Gbps
AES256-512	510 Mbps	1.1 Gbps	2.3 Gbps	3.1 Gbps	3.2 Gbps
AES256-1024	540 Mbps	1.1 Gbps	2.6 Gbps	6 Gbps	6.2 Gbps
AES256-2048	560 Mbps	1.1 Gbps	2.9 Gbps	11.1 Gbps	11.5 Gbps
SHA256-256	240 Mbps	500 Mbps	1.1 Gbps	1.2 Gbps	1.3 Gbps
SHA256-512	270 Mbps	560 Mbps	2.1 Gbps	2.5 Gbps	2.5 Gbps
SHA256-1024	290 Mbps	600 Mbps	2.5 Gbps	4.9 Gbps	5 Gbps
SHA256-2048	300 Mbps	620 Mbps	2.8 Gbps	8 Gbps	8.1 Gbps

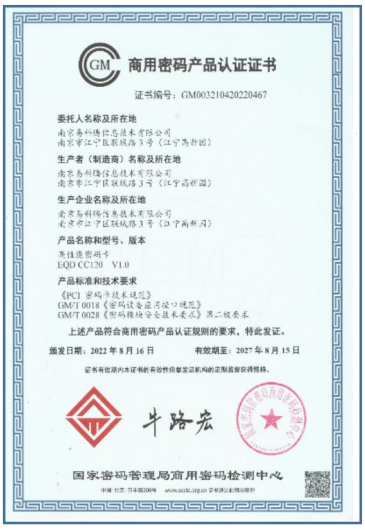
备注二：

副表的 LM10、LM20、LM30、MM 对应 M.2 接口密码卡，L10、L20、L30、M、G 对应 PCIE 密码卡。

不同测试环境下，实测数据会有差异；上述实测环境为 i5-8500，其他与“备注一”所述相同。

小包情况下，性能参数受 CPU 影响明显，改善 CPU 可获得更好表现。

产品资质


商用密码产品认证证书

证书编号：GM003210420220467

委托人名称及所在地

生产者（制造商）名称及所在地

生产企业名称及所在地

产品名称和型号、版本

EQD CC120 V1.0

产品标准和技术要求

《PCI 密码卡技术规范》

GM/T 0018《密码设备应用接口规范》

GM/T 0028《密码模块安全技术要求》第二级要求

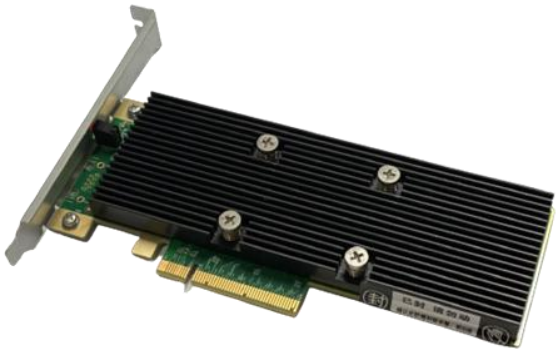
上述产品符合商用密码产品认证规则的要求，特此发证。

颁发日期：2022 年 8 月 16 日　　有效期至：2027 年 8 月 15 日

国家密码管理局商用密码检测中心

商用密码产品认证

产品实物



PCI-E 接口系列

M.2 Key B&M 接口系列

产品应用

EQD CC120 系列密码卡，作为 PKI（Public Key Infrastructure，公钥基础设施）系统的基础密码设备，通过标准接口（接口函数符合《GM/T 0018-2012 密码设备应用接口规范》）为多种密码安全产品和密码应用系统提供密码能力服务，是密码安全应用场景、信息安全系统的基础硬件之一。密码卡可作为服务组件应用于如下几种安全产品。

- 基础密码设备：服务器密码机、金融数据密码机、签名验签服务器等。
- 身份认证设备：安全接入网关、SSL VPN 网关、身份认证网关等。
- 密码服务设备：密钥管理设备、数据库加密网关、安全服务器等。

关于易科腾

南京易科腾信息技术有限公司是一家专注于量子保密通信相关产品研发、生产及销售的高新技术企业。

公司积极响应国家对量子科技与信息安全的战略部署，致力于融合量子通信和现代密码技术，通过将量子密码技术与云、管、端、物等紧密结合，为行业赋能，实现“量子安全+”产业化应用。公司自主研发以量子安全和信创为特色的网络、密码、SD-WAN 和应用产品，形成了多样化的综合解决方案，可为行业组织和个人用户提供量子安全服务。

www.e-quantum.com.cn market@e-quantum.com 025-52771107

版权所有 © 南京易科腾信息技术有限公司 2023。保留一切权利
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播

商标声明
易科腾 EQTINFO 和其他易科腾商标均为南京易科腾信息技术有限公司的商标.
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意
您购买的产品、服务或特性等应受易科腾公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，易科腾公司对本文档内容不做任何明示或默示的声明或保证。
由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。