产品名称Product name	密级Confidentiality level
SSC密码运算加速卡	授权公开
产品版本Product version	Total 6 pages共6页
V1.2	

SSC密码运算加速卡介绍手册

拟制:	陈金强	日期：	2017.4.23
审核:	马亚飞	日期：	2017.11.23
审核:		日期：	
批准:	余小龙	日期：	2018.04.25

深圳数字电视国家工程实验室股份有限公司

修订记录

日期	修订版本	描述	作者
2017年4月20日	1.0.0	初稿	陈金强
2017年11月23日	1.1.0	添加介绍	马亚飞
2018年4月25日	1.2.0	补充介绍	马亚飞

目录

1. 概述

SSC 密码运算加速卡是深圳数字电视国家工程实验室开发的高性能低功耗 PCIe 接口单芯片密码运算加速卡，提供密码运算加速以及可选的密钥安全管理功能。可应用于网络安全应用，区块链，数据中心等领域。本文档描述了加速卡的功能和性能。

2. 简介

SSC 加速卡基于单芯片方案开发研制，内置硬件加速处理引擎，相比传统的加速卡集成度更高，更稳定，具有更低的功耗和成本优势。加速卡支持两种接口访问（DIP 开关配置），以太网接口和 PCIe 接口。

加速卡若采用 PCIe 接口使用，加速卡与主机相连后可以作为一个完整的主机对外提供高性能的安全应用服务。

加速卡若采用以太网方式访问，则可作为独立安全系统运行。

主机系统连接的示意图如下图 1 所示：

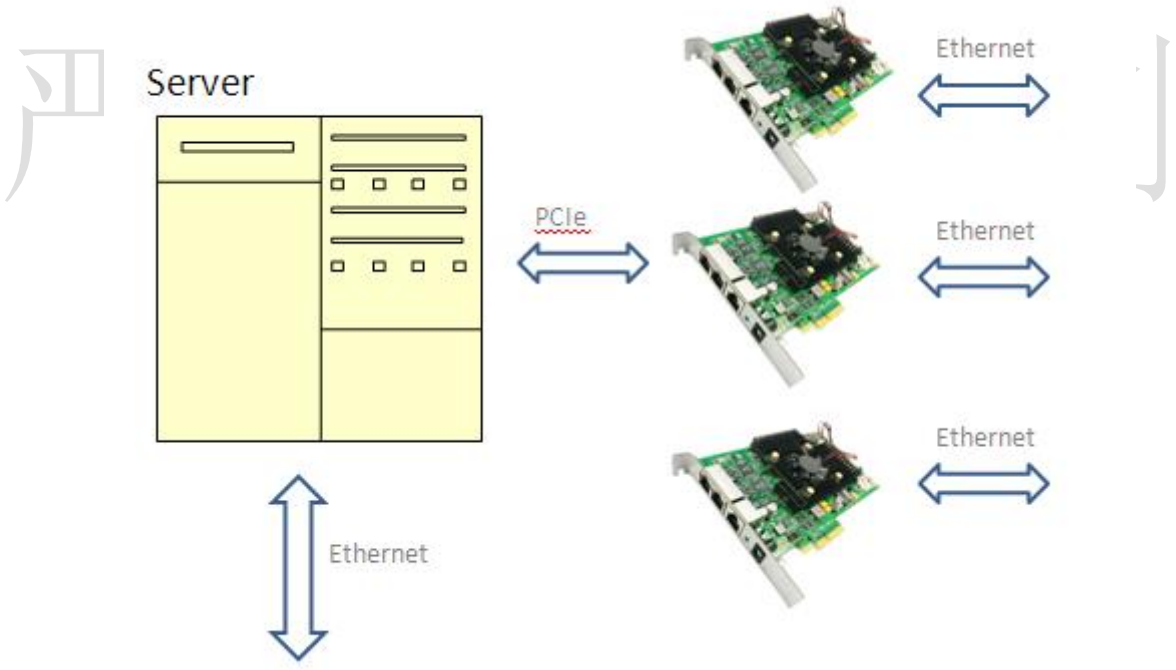

图 1 支持 PCIe 或 Ethernet 访问（取决于硬件 DIP 开关）

2.1. 结构

加速卡硬件结构如下图所示：

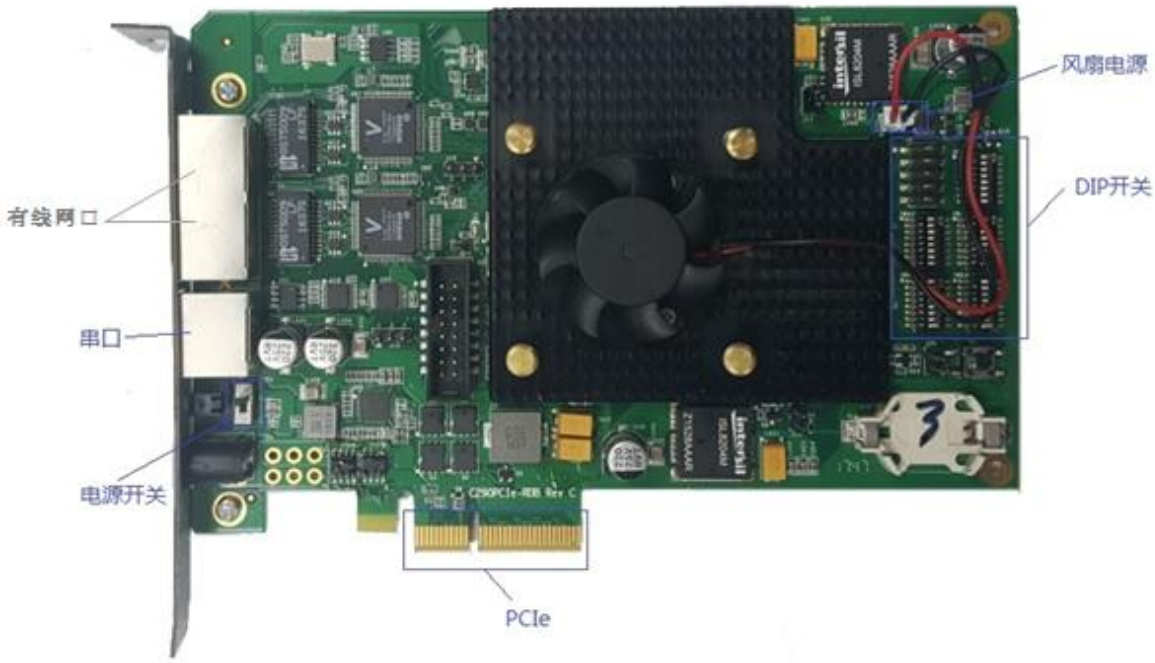

图2 加速卡板子布局

2.2. 特性

- 内置 3 个安全引擎，每个引擎有 15 个公钥硬件加速器，以及共 80 个对称密码加速器；
- NIST 认证的随机数发生器；
- RSA（最大支持 4096 位）签名验签算法；
- ECC 密码算法（素数域最大 1024 位长，二元域最大 1024 位长）；
- 支持 DH，ECDH 算法；
- 支持 AES，SHA256 等国际主流对称加密算法
- 四通道的 DMA 控制器；
- PCIe 2.0 的连接器规格： Edge Free / Multi-lane PCIe X1 Connector : Support X1、X2、 X4；
- PCIe 电源：不低于 40 瓦的供电电源，避免电源供电不足出现异常；
- 功耗：加速卡高峰功耗在 30 瓦左右；
- 支持多卡无缝运行，性能倍增，最多支持一台服务器 128 张卡；
- 支持 Host 端 Linux 系列操作系统；
- 兼容 openssl 接口，支持 openssl 同步和异步操作接口；
- 工作条件：
  - 工作环境温度：0℃-45℃；

- 工作环境相对湿度：45%-75%；
- 存贮环境温度：0℃-80℃；
- 存贮环境相对湿度：20%-95%；
- 可靠性指标：MTBF 大于等于 20000 小时。

2.3. 安全

- 支持安全启动和安全存储特性；
- Tamper 监测；
- 防芯片侧信道攻击；
- 安全可信结构：
  - 安全监视器；
  - 安全 fuse 处理器；
  - battery-backed secret key；
  - Internal boot ROM with ISBC code；
  - CCSR 访问控制；
  - 支持安全 DEBUG；

2.4. 性能

下表单卡性能指标是根据内核测试工具进行统计的部分结果，应用层（openssl）测试性能基本与其一致，详细参考我们的测试报告（测试结果与主机的性能有关，本测试结果基于 Pentium 双核 E5500 @2.8GHz,4G 内存）：

测试主机	Intel(R) Pentium(R) CPU G840 @ 2.80GHz	
	性能	执行命令
RSA2048 Public	331125.82 次/s	c29x_driver_perf_profile.sh RSA_PUB_OP_2K -m 0x2 -t 1 -s 10
RSA2048 Private	31695.72 次/s	c29x_driver_perf_profile.sh RSA_PRV_OP_2K -m 0x2 -t 1 -s 10
ECDSAP256 sign	90826.52 次/s	c29x_driver_perf_profile.sh ECDSA_SIGN_TEST -m 0x2 -t 1 -s 10
ECDSAP256 verify	67204.30 次/s	c29x_driver_perf_profile.sh ECDSA_VERIFY_TEST -m 0x2 -t 1 -s 10