 引 言 IPSe[1]作为一种实现VPN的安全协议体系，目前已在VPN设备中广泛使用。但是，随着千兆位高速网络的技术发展，对VPN设备在时效性等方面提出了更高的要求。 因此，必须从体系结构等方面，研究新的技术方法实现IPSec。在IPSec安全设备中，SoC技术将是一种较好的选择。soC将系统的CPU、I/O接口、存储器、算法、协议处理等模块全部集成到单一半导体芯片上，实现IPSec协议的全部功能，成为构筑IPSec安全设备的核心部件，极大地提高了高速V。PN网络的安全性、可靠性、时效性以及较高的性能价格比。 1 IPSec协议 IPSec协议是因特网工程任务组(IETF)针对TCP/IP协议没有安全机制的严重缺陷而专门制定的IP安全标准，用以在IP层实现访问控制、无连接完整性、数据源验证、抗重播、数据加密和有限的业务流机密性等多种安全服务。该标准由一系列协议组成，各协议之间的关系如图1所示。 *基金项目：“ 十五 ”期间国家密码发展基金密码理论研究课题“ 密码soc芯片的体系结构和安全性研究 ”。 有关协议的解释如下： ①AH[2] (Authentication Header)是一个安全协议头，在传输模式下为IP层数据流提供数据完整性、数据源身份认证、一些可选的和有限的抗重播服务。 ②EsP[3] (Encapsulating Security Payload)是一个插入到IP数据报内部的协议头，为IP层流量数据提供机密性、数据源身份认证、抗重播以及数据完整性等安全服务。 ③认证与加密算法是IPSec实现安全数据传输的核心，其中，加密算

法用于ESP，可以采用DES、IDEA等密码算法；认证算法用于AH，可以采用3DES、RC5等算法。④IKE[4](Internet Key Exchange)是密钥交换协议，用于在IPSec通信双方建立共享安全参数及验证过的密钥，以建立一种安全关联关系。⑤DoI(Domain of Interpretation)是一个单独的文档，用于存放IKE协商的参数。⑥SA(Security ASSOCiation)是安全关联协议，是主机、路由器两个应用IPS ec实体之间的一种单向逻辑连接。sA有安全策略库(sPDB)和安全关联库(sADB)，存储了安全策略的具体细节，包括保护的内容、保护的方式、保护通信数据的主体等策略。2 SoC技术 目前，SoC平台主要用于CSoC、SoPC、EPGA等芯片开发。其中，CSoC称为可配置系统级芯片，一般包括1个处理器内核、可编程逻辑阵列和其它一些通用部件；SoPC是可编程的单芯片系统，如Altera的Nios内核模块；EPGA是以FPGA为主体的SoC芯片。使用这些SoC开发平台，可以充分利用系统级芯片集成度高和性能优越的特点，灵活设计开发各种专用Soc芯片。(1)开发平台的选择 SoC平台开发套件包括：各种工具与资源软件、可以重构的硬件电路结构验证平台和使用说明书等。其可用软件资源包括：供选用的多种嵌入式处理器核，硬件模块设计语言及其编译器，仿真、综合和布局、布线工具等；设计语言包括HDL、C/C 等。开发平台的选择取决于器件的来源：当选用商品化器件时，可以选择Altera的SOPC开发环境QUARTUSII；当选择自主研发Soc时，应使用相关的专用开发平台。(2)lP库的选择 IP库的选择应针对器件类型，选择通用的IP核。对安全性要求较高的算法模块，应采取访问控制、抗解剖分析等技术措施；对可变逻辑模块，应采用FPGA

，以保证可编程的特点。 (3)芯片结构的选择 SoC的主体部分由CPU和ASIC组成。在设计过程中，芯片结构的选择应从系统应用规划、协议处理速度要求、便于实现、Vetilog HDL编程实现结构化，以及所用逻辑模块的实际结构等几个角度入手。 Altera的SoC芯片[5]构成如图2所示。 (4)软硬件系统设计 SoC的基本结构是具有一个成多个微处理器，以及可编程硬件逻辑，因此，在SoC设计中必须进行软硬件的协同设计。软硬件协同设计的技术性很强，它既有SoC设计的灵活性，又有SoC设计中难以揣摩、充满变数的复杂性，将涉及到硬件资源的规划和整个系统性能的实现。 (5)系统集成设计 系统集成设计的关键技术，主要是IP核的无缝连接系统设计和相关的可测试技术，包括紧密耦合、传输特性、时钟综合和测试接口等。 (6)低功耗管理设计 低功耗设计是对有相关要求的器件进行的一种设计技术，设计中主要通过一些系统状态、桥接控制等来实现。