计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.190700110

一种基于云端加密的 FPGA 自适应动态配置方法

陈利锋[1]　朱路平[2]
1 复旦大学计算机国家级实验教学示范中心　上海 200433
2 91045 部队　上海 200940

摘　要　在需要进行大量数据并行计算的算法(如云计算、机器学习算法、人工智能算法等)中,FPGA 作为一种提升性能的重要技术手段,得到了广泛的应用。FPGA 配置方式中,需要在存储器中读取配置数据,然后将其写入 FPGA 中。作为技术成果的实际体现,FPGA 的配置数据可能被非法获取,从而导致研究成果泄露的问题。为了较好地应对这个问题,文中提出了一种有效的基于云加密的 FPGA 配置方法。该方法通过云端加密 APP 对配置数据文件进行加密管理,在需要配置 FPGA 的时候,由微处理器通过云端服务器的访问端口获取加密的配置数据,并使用内置在微处理器的解密算法进行解密,然后用解密后的数据对 FPGA 进行动态配置。该方法将 FPGA 的配置数据存储于云端服务器,在云服务器上通过加密手段进行严格的数据保护和文件保护,由此提供了灵活而强大的加密保护功能;微处理器从云端通过加密通道获取数据,将加密数据解密后再用于 FPGA 的配置,整个过程中配置数据都是处于加密状态,数据泄密的风险得到了有效控制。这样,既实现了对配置数据最大限度保护,防止其被非法获取和使用,又实现了对 FPGA 的远程动态配置。所提方法在阿里云和腾讯云平台得到了实际验证,其不仅保密效果好,而且能灵活配置。

关键词:FPGA 动态配置;云存储安全;对称加密;非对称加密;数据保护
中图法分类号　G201

Encrypted Dynamic Configuration Method of FPGA Based on Cloud

CHEN Li-feng[1] and ZHU Lu-ping[2]
1 National Demonstration Center for Experimental Computer Education, Fudan University, Shanghai 200433, China
2 Troops 91045, Shanghai 200940, China

Abstract　In the field of parallel computing which needs a lot of data, such as cloud computing, machine learning algorithm, artificial intelligence computing, etc., as an important technical means to improve performance, FPGA has been widely used. In the configuration of FPGA, configuration data need to be read from memory and then written into the FPGA. As a practical embodiment of technological achievements, configuration data has the problem of how to prevent data from being illegally acquired, leading to the leakage of research property. In order to deal with this problem, this paper proposes an effective method of FPGA configuration based on cloud encryption. This method encrypts and manages the configuration data file by cloud-based encryption APP. When configuring the FPGA, the microprocessor obtains the encrypted configuration data through the access port of the cloud-based server, and decrypts it using the decryption algorithm built in the microprocessor. Then, the decrypted data are used dynamically to config the FPGA. The method described in this paper stores the configuration data of the FPGA in the cloud server, and carries out strict data protection and file protection through encryption means on the cloud server, thus providing a flexible and powerful encryption protection capability. The microprocessor obtains data from the cloud through encryption channel, decrypts the encrypted data and then uses it for the configuration of FPGA. In the whole process, the configuration data are encrypted, and the risk of data leakage is effectively controlled. Thus, the configuration data can be protected to the maximum extent to prevent illegal acquisition and use, meanwhile the remote dynamic configuration of the FPGA can be realized. The proposed method has been verified in Aliyun and Tencent cloud platforms, which achieves good confidentiality and flexible configuration.

Keywords　Dynamic configuration of FPGA, Cloud storage security, Symmetric encryption, Asymmetric encryption, Data protection

到稿日期:2019-07-17　返修日期:2019-09-17　本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
基金项目:"核高基"重大专项(KCH230110)
This work was supported by the Sub Project of HGJ Major Project(KCH230110).
通信作者:陈利锋(chenlf@fudan.edu.cn)

1 背景

FPGA 器件是专用集成电路中的一种半定制电路，是可编程的逻辑列阵。FPGA 的基本结构包括可编程输入输出单元、可配置逻辑块、数字时钟管理模块、嵌入式块 RAM、布线资源、内嵌专用硬核和底层内嵌功能单元。FPGA 具有布线资源丰富、可重复编程、集成度高和投资较低的特点，在数字电路设计领域得到了广泛的应用[1-2]。在 FPGA 的应用系统中，每次上电后，都需要通过专门的配置方法将配置数据传输给 FPGA 芯片，传输完成后，FPGA 芯片才能实现预定的逻辑功能。FPGA 的配置方法有多种，其中的在线下载模式通过 JTAG 下载线将 sof 文件下载到 FPGA 内部的 RAM 内部运行，掉电程序丢失，主要用于前期的调试阶段；外部 Flash 配置模式是将 sof 文件下载到外部 Flash 中，上电 FPGA 主动读取 Flash 加载程序的方式，掉电程序不丢失；外部微处理器配置模式利用外部微处理器来给 FPGA 发送配置数据。

上述几种 FPGA 配置方式都存在如何防止配置数据被非法获取甚至被非法使用的问题[3-5]。如果能够采用基于云端加密的 FPGA 动态配置方法，配置数据存储于云端，被严格保护；在上电配置的时候，微处理器从云端通过加密通道获取数据，将加密数据解密后再直接用于 FPGA 的配置。这样，配置数据能够最大限度地得到保护，防止被非法获取和使用。

2 方法概述

本文的设计目标是，将 FPGA 的配置数据存储于云端，借助云存储和云加密的技术手段对数据进行保护，从而实现对配置数据的保护，防止其被非法访问和非法使用。

本文方法使用了一个加密的云端服务器，该服务器存储了加密的 FPGA 配置数据文件。服务器提供了加密的访问接口，供远程客户端通过加密协议来获取数据。微处理器通过 Internet 网络从云端服务器获取数据。获取数据的过程包括两个阶段：1）使用内置的加密协议传输通信密钥；2）使用通信密钥来传输 FPGA 配置数据。微处理器内置对称加密解密协议，用于解析通信密钥；同时还内置了非对称加密解密协议，用于解析 FPGA 配置数据。

微处理器通过 Internet 网络从云端服务器获取数据，再通过解密算法[6-8]完成数据解密，并将解密后的 FPGA 配置数据存储在微处理器的内存中，然后分块将 FPGA 配置数据配置到 FPGA 中。微处理器直接进行 FPGA 配置的工作方式结合使用微处理器的 GPIO，可以灵活地控制 FPGA，实现全局或部分的配置更新，也可以实现运行态配置，达到了动态配置的目的。微处理器可以自动检测云端服务器上的配置数据更新，自动完成对 FPGA 的配置更新；还可以接受云端服务器的动态指令，完成动态 FPGA 配置。

3 系统结构

图 1 展示了一种基于云端加密的 FPGA 动态配置方法的系统结构，包括以下 5 个组成部分。

（1）云端服务器：一个通信管理 APP 和相关 FPGA 配置数据文件。

（2）云端的通信协议 API：实现了 TCP 通信控制、通信的加密解密算法等功能。

（3）通信网络：用于建立从云端服务器到微处理器的双向加密通信通道。

（4）FPGA 配置的微处理器节点：包含 TCP 通信控制、微处理器、FPGA 及配置电路。

（5）微处理器端通信协议 API：实现了 TCP 通信控制、通信的加密解密算法等功能。

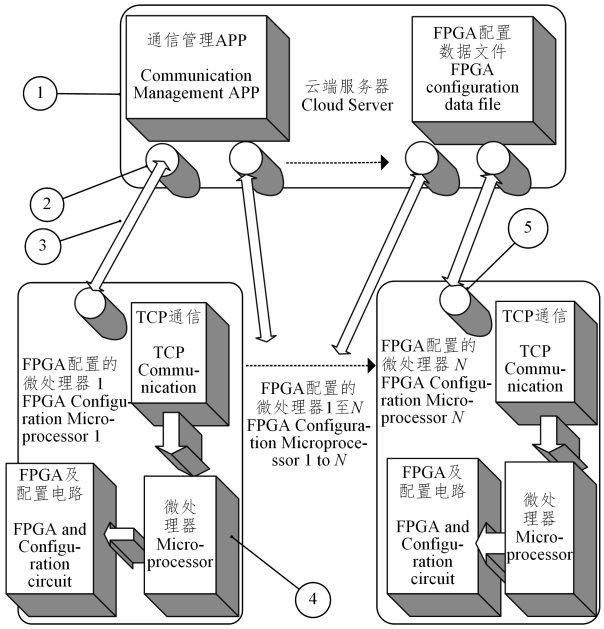


图 1 系统结构图

Fig. 1 System structure diagram

4 云端加密

（1）云端服务器由一个通信管理 APP 和相关 FPGA 配置数据文件构成。服务器软件的功能包括：通过 TCP 协议为远程微处理器端提供访问接口；对称加密解密协议，用于密钥传输；非对称加密解密协议，用于数据加密；FPGA 配置数据文件的加密保存及管理。

4.1 加密算法

文中所提系统中的密钥传输使用了对称加密算法。对称加密指加密方和解密方使用同样的密钥来进行加密和解密。在对称加密算法中，数据发信方将明文（原始数据）和加密密钥（mi yue）一起经过特殊加密算法处理后，使其变成复杂的加密密文发送出去。常用的对称加密算法有：AES，RC4，3DES。密钥传输示意图如图 2 所示。

如图 2 所示，此种方式属于对称加密，双方拥有相同的密钥，信息得到安全传输。但由于此种方式存在以下缺点：

（1）使用不同的客户端且服务器数量庞大，所以双方都需要维护大量的密钥，维护成本很高；

（2）因每个客户端、服务器的安全级别不同，密钥极易泄露。

因此本文方法仅使用对称加密算法来进行密钥的传输，利用了对称加密算法加密解密速度快、传输时间极短、使用简便的优点。

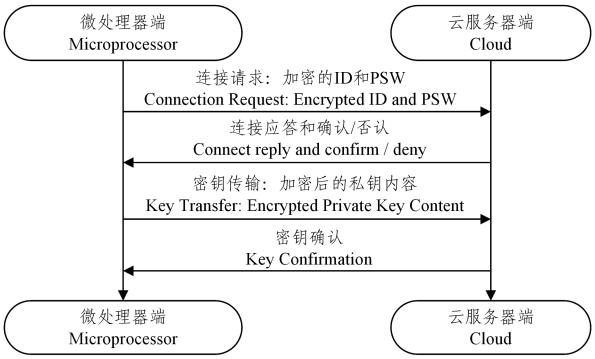


图 2 密钥传输示意图

Fig. 2 Key transmission schematic

4.2 数据加密

对于数据的加密传输，本文采用了非对称加密方法。非对称加密算法实现机密信息交换的基本过程是：

(1)甲方生成一对密钥并将其中的一把作为公用密钥向其他方公开；

(2)得到该公用密钥的乙方使用该密钥对机密信息进行加密后再发送给甲方；

(3)甲方再用自己保存的另一把专用密钥对加密后的信息进行解密；

(4)甲方只能用其专用密钥解密由其公用密钥加密后的任何信息。

非对称加密算法有 RSA，DSA/DSS 。

如图 3 所示，云端服务器用公钥对请求内容加密，微处理器端使用私钥对内容进行解密。密钥的设计只针对单次配置文件传输有效。每一次重新连接云端服务器，都会产生新的私钥供当次传输使用。这样的加密方式有效保证了数据的安全性。

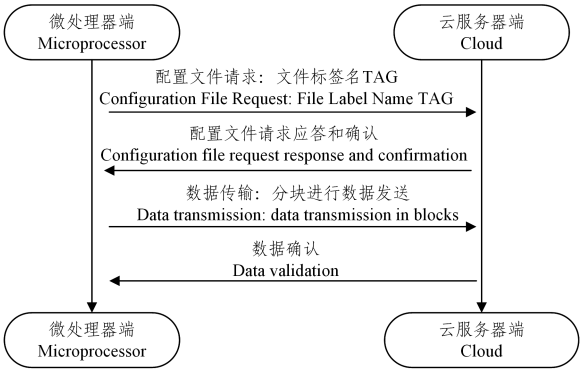


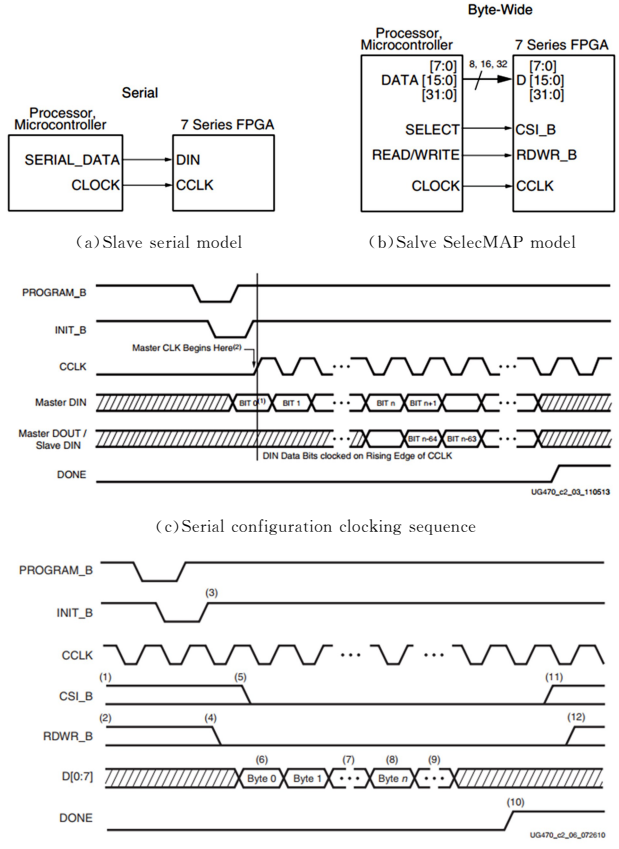
图 3 数据传输示意图

Fig. 3 Data transmission schematic diagram

5 自适应动态 FPGA 配置

本文所提方法采用了自身具有强加密功能的单片机作为主控微处理器，同时配置了网络通信模块，包括有线网络通信、无线网络通信或移动数据通信。微处理器通过通信网络与云端服务器进行 TCP/IP 通信。通信的过程包括两个阶段：1)使用内置的加密协议传输通信密钥；2)使用通信密钥传输 FPGA 配置数据。微处理器从云端服务器获得了 FPGA 配置数据后，通过微处理器与 FPGA 的硬件接口完成对 FPGA 的全局或局部配置更新。

微处理器对 FPGA 的配置包括 SerialMode 和 Byte-WideMode 两种方式[9]，前一种数据以串行方式传输，接口简洁，但是速度较慢；后一种数据以并行方式传输，接口信号多，但是速度较快[10-13]。



(a)Slave serial model (b)Salve SelecMAP model

(c)Serial configuration clocking sequence

(d)Continuous ×8 SelectMAP data Loading

图 4 微处理器对 FPGA 的配置模式及时序[14]

Fig. 4 Configuration mode and timing between microprocessor and FPGA[14]

为了提高 FPGA 配置更新的自动化效果，本文设计了 3 种配置更新机制。

(1)自动比对更新。微处理器定时检查云端服务器，自动比对从云端服务器获得的 FPGA 配置数据的版本号，以判断是否需要对 FPGA 进行更新配置。如果发现配置有更新，就启动更新过程对 FPGA 进行配置。

(2)远程指令更新。在这种方式里，微处理器可以接受云端服务器的指令，用户在云端 APP 里发布该指令，并可以选择执行该命令的目标 FPGA 节点，然后向相应节点上的微处理器发送强制更新命令。节点上的微处理器收到强制更新命令后，启动新过程，强制进行 FPGA 的更新配置。

(3)局部运行态更新。前两种更新方式是全局的配置更新，在更新过程中 FPGA 的原有内部逻辑会被全部擦除和置换。某些节点不希望或者不允许擦除全部逻辑，则会使用一种更精细的更新配置方式——局部运行态更新[15-16]。这种更新方式中，局部配置块的大小以 4 Slice 为单位增加。另外，在逻辑的设计中，需要给局部可重配置预留配置资源，包括时钟、IOBs 互联资源[17-18]。配置的过程中，需要微处理器根据

配置时序的要求擦除该块的逻辑，并发送块配置数据流，完成局部配置更新。

结束语 本文提出的方法将云端服务器、对称加密、非对称加密、微处理器的功能结合成一个整体，将 FPGA 的配置数据存储于云端严格进行保护；微处理器通过加密通道从云端获取数据，将加密数据解密后再用于 FPGA 的配置，既实现了对配置数据的最大限度保护，防止其被非法获取和使用，又实现了对 FPGA 的远程动态配置。所提方案不仅保密效果好，而且能灵活配置的效果。云平台可以采用开放的公共云平台，例如阿里云、腾讯云等，本文在实现过程中采用了阿里云、腾讯云作为测试平台，实现了预期的加密配置功能。

参 考 文 献

[1] DI H. Research on Data Encryption Based on Cloud Computing Platform[J]. Journal of Changchun Normal University, 2017, 36(3): 55-58.

[2] MENG Q, MA J F, CHEN K F, et al. A comparison scheme of Internet of things encrypted data based on cloud computing platform[J]. Journal of Communications, 2018, 4: 65-70.

[3] ZHANG Y. Fuzzy searchable encryption algorithm for privacy information of cloud platform [J]. Electronic Technology and Software Engineering, 2018(8): 214-214.

[4] ZHAO T G, DING Y W. Research on cloud storage security cross encryption algorithm [J]. Software Guide, 2018, 17(10): 204-208.

[5] DENG C Z, LEI Q. Construction and implementation of RSA cloud storage security platform loaded with random oracle model [J]. Journal of Huaihua University, 2019, 38(5): 65-69.

[6] JI P, LV X M, SU S T, et al. A new sequence preserving encryption algorithm based on coding tree in cloud environment [J]. Computer Engineering, 2018, 44(12): 288-293.

[7] DU Y Z, DU X H, YANG Z. Information flow control and Implementation Based on attribute encryption in cloud computing environment [J]. Computer Engineering, 2018(3): 27-36.

[8] ZHANG H Y. Application of data encryption technology in computer network communication security [J]. Digital Technology and Application, 2018(12).

[9] LU Y, CHEN Y, LI T, et al. Convolutional Neural Network Construction Method for Embedded FPGAs Oriented Edge Computing. Journal[J]. Journal of Computer Research and Development, 2018, 55(3): 551-562.

[10] GU L, XU G L, WANG Y R. Dynamic Reconfiguration Theory and Research Development of FPGA[J]. Computer Measurement and Control, 2007(11): 1-4.

[11] LIU K, CAI X J, ZHANG Z Y, et al. NVM verification architecture design and verification based on high performance SOC FPGA array [J]. Computer Research and Development, 2018, 55(2): 265-272.

[12] LU Q S, XU Y S. Design of target recognition and tracking system based on FPGA [J]. Modern Electronic Technology, 2018(18): 3-8.

[13] CUI G X. Design of online hardware practice teaching platform based on FPGA[J]. Experimental Teaching and Innovation, 2017, 36(4): 153-156.

[14] Xilinx Corp. Xilinx FPGAs Configuration User Guide, UG470 (v1. 13. 1)[EB/OL]. https://www. xilinx. com/support/documentation/.

[15] PANG Y Y, WANG S J, PENG X Y. Research on design method of remote reconfigurable system based on SOPC [J]. Journal of Electronic Measurement and Instruments, 2010(6): 548-554.

[16] ZHANG Y, FAN J H, LV Z M, et al. Overview of FPGA dynamic partial reconfiguration technology [J]. Computer and Modernization, 2014(3): 49-53.

[17] XIONG J B, ZHANG Y Y, TIAN Y L, et al. Cloud data security de duplication based on role symmetric encryption[J]. Journal of Communications, 2018, 39(5): 59-73.

[18] COMPTON K, HAUCK S. Reconfigurable Computing: A Survey of Systems and Software[J]. ACM Computing Surveys, 2002, 2(2): 936-938.

CHEN Li-feng, born in 1977, doctor. His main research interests include embedded system application, and machine learning.