

一种可重构计算平台中的远程比特流安全更新方案

李 磊, 张 雪, 陈 静, 张志鸿

(郑州大学 信息工程学院, 河南 郑州 450001)

摘 要: 针对可重构计算平台的远程比特流更新中如何防止信息被篡改和重放攻击的问题, 提出了可重构计算平台中的远程比特流安全更新方案. 该方案在远程更新配置端采用部分加密策略加密比特流并计算 MAC 值, 通过以太网将信息发往可重构计算平台, 经控制单元验证其完整性后, 将加密的比特流和 MAC 值放入安全配置器中, 最后 FPGA 加电并向控制单元请求获取比特流, 从而完成远程比特流的安全更新. 分析表明, 该方案能够保证更新比特流的完整性和机密性, 并能防止重放攻击.

关键词: 信息安全; FPGA; 可重构技术; 远程比特流更新

中图分类号: TP309

文献标识码: A

文章编号: 1000-7180(2013)12-0064-05

A Secure Solution for Remote Bitstream Updates of Reconfigurable Computing Platform

LI Lei, ZHANG Xue, CHEN Jing, ZHANG Zhi-hong

(School of Information Engineering, Zhengzhou University, Zhengzhou 450001, China)

Abstract: Although FPGA-based reconfiguration computing platform has been shown as a promising technique in high productivity computing field, it may suffer security threats during its bitstream remote update process. A secure scheme is proposed in this paper to prevent tamper and replay attacks during the process of remote bitstream update on reconfigurable computing platform, which encrypts the bitstream partially and calculates the value of MAC when making the configuration at the Remote Updating Configuration End. And then these data is sent to the distributed Control Units on reconfigurable computing platform via network. The encrypted bitstream will be put into security configurator after its integrity was verified by the value of MAC. At the end of the secure update process, FPGAs will makes the requirements to its Control Unit and get the secure bitstream after it is restart. Analysis shows that the scheme proposed can guarantee the integrity and the confidentiality of the bitstream for remote updating and also has the ability of protecting the updating process from replay attacks.

Key words: information security; FPGA; reconfigurable technology; remote bitstream update

1 引言

近年来, 高端计算领域的研究热点逐渐从高性能计算转向到高效能计算(High Productivity Computing). 基于现场可编程门阵列(Field Programmable Gate Arrays, FPGA)的可重构技术是可重构计算体系的关键技术之一, 与传统数字电路系统相比, FPGA 具有可编程、高集成度、高速和高可靠性等优

点. 目前主流的 FPGA 大多基于 SRAM 工艺, 掉电后 FPGA 会失去所有逻辑关系, 所以一般都配备片外的非易失存储器(Non-Volatile Memory, NVM), 用于在断电时保存配置信息, 但片外的 NVM 易受到对手攻击, 从而导致比特流信息泄露.

关于 FPGA 的远程更新及比特流传输的安全, 文献[1]中分别提出了两种不同的比特流更新的安全方案, 但都不够完善和安全. 文献[2]中描述了一

个新颖有效的远程更新 FPGA 配置的安全协议,但并没有给出安全分析,且比特流被存储在 NVM 中,不能保证安全.文献[3]中提出了一种防重放攻击的比特流更新协议,但没有提供保证比特流机密性和完整性的方案.

本文提出一种在 FRCP 平台下的远程比特流安全更新方案.在本方案中,配置信息被存储在 FRCP 的控制单元中,在远程更新配置端对比特流加密并计算 MAC 值,以保证比特流的机密性和完整性,此外,还采用部分加密方案来增加逆向工程的难度和花费.

2 系统架构

2.1 FRCP 系统架构

FRCP 系统架构如图 1 所示.远程更新配置端的决策资源管理模块负责根据应用需求,生成 FRCP 端的新配置.新的配置被封装在比特流数据包中,远程配置管理器用密钥存储器中的密钥加密比特流并计算 MAC 值后,通过以太网将信息送往 FRCP 端的控制单元,控制单元验证 MAC 值正确后,方可将加密的比特流放入安全配置器中.当底层的 FPGA 通电或需要更新时,控制单元根据比特流数据包的控制位信息判断该比特流对应哪一个 FPGA,从而完成比特流的远程更新.

FRCP 端有多个重构组件,每个重构组件由多个 FPGA 组成. FRCP 端运行信息的收集和动态重配置主要是依靠可重构组件内的控制单元实现的,控制单元收集处理器内各部分的状态,并将收集到的信息整理,上报远程更新配置端,为管理决策提供依据.

2.2 FRCP 平台的主要安全威胁

FRCP 平台的安全威胁主要来源于攻击者对

SRAM FPGA 的数据或 IP(Intellectual Property)的攻击.因此,保证 FRCP 平台的安全主要是保证 FPGA 的数据安全和 FPGA 的 IP 核的安全.其中,FPGA 的数据安全包括保护 FPGA 应用程序电路中的数据安全和在通信过程中从外设电路中进出的数据安全.保护 FPGA 的 IP 安全则需保护 FPGA 的比特流信息,以防止设计被克隆或逆向攻击^[4].本文主要关注 FPGA 的远程比特流更新问题,其中面临的主要安全威胁包括窃听、篡改和重放.窃听指攻击者通过网络监听等手段,盗取 FPGA 系统设计.篡改指攻击者篡改经由网络传输的数据,以欺骗 FPGA 系统.而重放则是指攻击者重放监听到的早期信息,获取 FPGA 的信任或将 FPGA 系统配置降级.

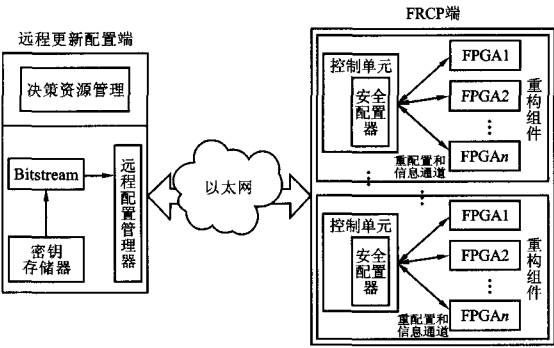


图 1 FRCP 远程比特流更新配置图

3 远程比特流更新安全方案

FRCP 的远程比特流安全更新方案的目标是为 FRCP 的远程配置信息提供一个有效的安全保障,以抵抗克隆、逆向工程、欺骗和重放攻击.

3.1 方案设计概述

FRCP 的远程比特流安全更新的实施方案如图 2 所示,该方案包括三个部分.

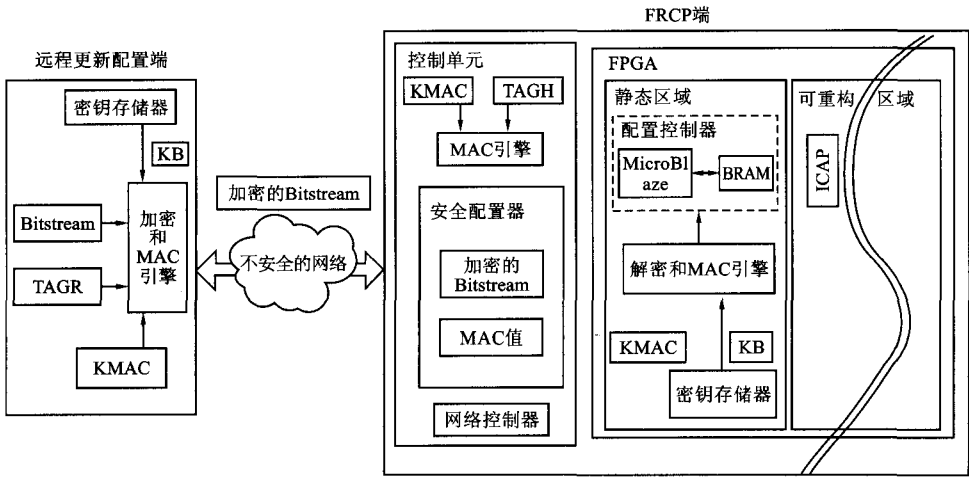


图 2 FRCP 的远程比特流的安全更新

(1) 远程更新配置端: 负责产生和发送加密的比特流信息. 它由密钥存储器、加密和 MAC 引擎以及比特流数据包和版本标识 TAG_R 组成. 其中, 比特流数据包由 FPGA 设备 ID、软硬件版本信息, 再加上控制位信息、数据大小等组成, 记为 B. 密钥存储器存放着各个 FPGA 对应的对称密钥 K_B , K_B 仅被远程更新配置端和对应的 FPGA 所知. K_{MAC} 是生成消息认证码 (Message Authentication Code, MAC) 所需用的密钥, 远程更新配置端、控制单元和 FPGA 利用文献[5]提供的群加密机制共享该密钥, 群内用户可以解密获得由 K_{MAC} 加密的信息, 而群外用户没有解密信息的能力. TAG_R 用来标识比特流的版本, 可以保证比特流版本的新鲜性, 以防止信息传输过程中的欺骗或重放攻击. 加密和 MAC 引擎, 采用硬件实现的, 对比特流进行加密并计算 MAC 值, 以保证比特流的机密性和完整性.

(2) FRCP 端控制单元: 负责接收来自远程更新配置端的信息, 并将加密的比特流发送给 FPGA. 它保存的 TAG_H 是远程更新配置端 TAG_R 的副本, 只能由远程更新配置端的更新指令来触发递增. MAC 引擎用接收到的加密比特流等信息计算 MAC 值, 并与接收到的 MAC 值进行比较, 若是匹配, 将接收到的加密比特流和相应的 MAC 值存储在安全配置器中; 否则, 通知远程更新配置端更新失败. 安全配置器是一个非易失存储器, 用于存储加密比特流和它的 MAC 值. 网络控制器负责管理 FRCP 端和远程更新配置端的数据传输.

(3) FPGA: 它分为静态区域和可重构区域. 其中, 静态区域主要包括配置控制器、解密和 MAC 引擎. 配置控制器负责管理可重构区域的动态或部分重构, 控制部件由软核的 MicroBlaze 实现, BRAM 用来存储 MicroBlaze 使用的数据和指令. 密钥存储器用来存储对称密钥 K_B . 解密和 MAC 引擎负责从控制单元中取得加密比特流等信息, 并进行 MAC 计算和验证, 若验证通过, 就用 K_B 对加密比特流进行解密, 然后发给配置控制器; 否则, 就丢弃此比特流并通知控制单元更新失败, 再由控制单元通知远程更新配置端. 而可重构区域 (即动态部分) 是指在配置控制器的控制下, 能通过 ICAP 进行动态重构和部分重构的组件. 其中 ICAP 是一个在 FPGA 上的内置硬核 IP 模块, 该模块由处理器 MicroBlaze 的软件驱动控制.

3.2 远程更新过程

比特流远程更新过程如图 3 所示. 其中, 远程更新配置端是唯一可以更新 FPGA 配置和 TAG_H 值的实体. 比特流可以分为两部分: 数据部分 (DATE), 表示设计者的设计内容; 控制部分即比特流头部 (HEADER), 长度固定 32 位, 用于携带控制信息和对应的 FPGA 的 ID. 本方案采用比特流数据部分加密而控制部分不加密, 部分加密的策略可增加逆向工程的难度和花费, 提供更好的安全性^[6]. 本文使用文献[7]采用的符号体系, 符号说明如下: $E_K(x)$ 代表用对称密钥 K 对消息 X 进行加密; $D_{K(x)}$ 代表用对称密钥 K 对消息 X 进行解密; B_{DATE} 代表比特流 B 的数据部分; $||$ 代表消息之间的相互连接操作.

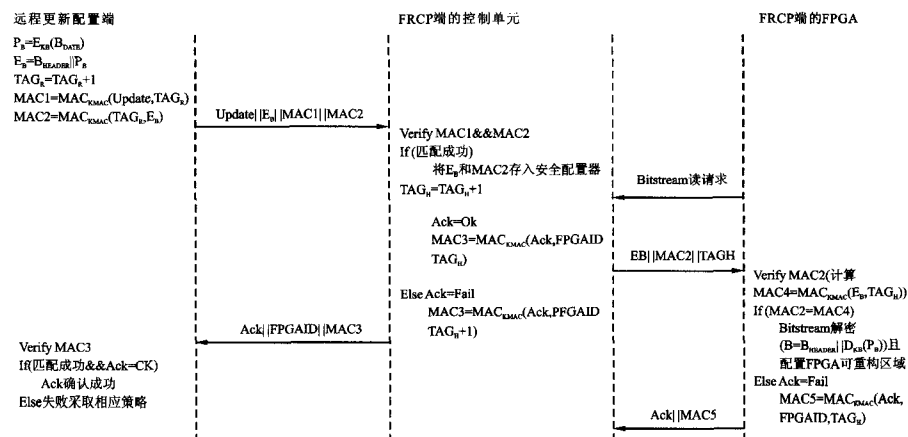


图 3 远程比特流的更新过程

首先, 远程更新配置端进行如下操作:

(1) 部分加密新的比特流 B 先加密比特流的数据部分: $P_B = E_{K_B}(B_{DATE})$, 然后将 P_B 与比特流的头部连接起来, 得到部分加密的比特流: $E_B = B_{HEADER} || P_B$;

(2) TAG_R 的值加 1, 新 TAG_R 值用来标识比特

流 B 的版本, 并将在随后的 MAC 计算中使用;

(3) 生成更新指令 Update, 并计算相应的 MAC 值: $MAC1 = MAC_{K_{MAC}}(Update, TAG_R)$;

(4) 计算加密比特流 E_B 和 TAG_R 的 MAC 值: $MAC2 = MAC_{K_{MAC}}(TAG_R, E_B)$;

(5) 发送 Update、MAC1 和 E_B 、MAC2 到 FRCP 端。

FRCP 端接收到这些信息后,进行如下操作:

(1)解密 Update 指令,得到更新请求;

(2)检查更新请求是否是合法的. 根据 Update、 TAG_H 计算 MAC 值: $MAC_{11} = MAC_{K_{MAC}}(Update, TAG_H + 1)$, 并与 MAC1 比较;

(3)如果更新请求是合法的,即 MAC11 和 MAC1 是匹配的,则根据 E_B 和 TAG_H 计算 MAC 值: $MAC_{21} = MAC_{K_{MAC}}(TAG_H + 1, E_B)$, 并与 MAC2 比较. 否则,在确认消息指令 Ack 中写入 Fail,说明更新失败。

(4)如果 MAC21 和 MAC2 是匹配的,则将 E_B 和它的 MAC 值 MAC2 存入安全配置器中,并使 TAG_H 的值加 1. 新的 TAG_H 值不仅能锁定平台和 FPGA 的新配置比特流,还能与远程更新配置端 TAG_R 的值保持一致. 然后在确认消息指令 Ack 中写入 Ok,并计算 MAC 值: $MAC_3 = MAC_{K_{MAC}}(Ack, FPGAID, TAG_H)$. 如果 MAC21 和 MAC2 不匹配,则在 Ack 中写入 Fail,说明更新失败;生成确认消息指令 Ack, 计算相应的 MAC 值: $MAC_3 = MAC_{K_{MAC}}(Ack, FPGAID, TAG_H + 1)$.

(5)发送 Ack、FPGA ID 和 MAC3 到远程更新配置端。

远程更新配置端收到信息后,检查确认指令 Ack 是否是合法的. 远程更新配置端通过计算 Ack、 TAG_R 、FPGA ID 的 MAC 值: $MAC_{31} = MAC_{K_{MAC}}(Ack, FPGAID, TAG_R)$, 与 MAC3 进行比较得出结果. 如果 MAC31 和 MAC3 是匹配的,且 Ack 的值为 OK,则说明更新成功;否则,说明完整性被破坏,需采取相应的策略。

当 FPGA 通电时,设备需要从控制单元的安全配置器中下载它的配置比特流. 下载过程如图 3 所示,FPGA 端的操作如下:

(1)FPGA 向控制单元发送一个比特流读请求;

(2)FPGA 读取控制单元发送来的部分加密比特流 E_B 、相应的 MAC 值 MAC2 和 TAG_H ;

(3)验证 MAC2 是否是合法的. 计算 E_B 、 TAG_H 的 MAC 值: $MAC_4 = MAC_{K_{MAC}}(E_B, TAG_H)$, 并与

MAC2 比较;

(4)如果 MAC4 和 MAC2 是匹配的,则去掉 E_B 的 32 位头部得到加密的数据部分 P_B ,对 P_B 进行解密后,再连接 32 位头部得到原始比特流 B,即 $B = B_{HEADER} || D_{K_B}(P_B)$. 然后配置控制器利用比特流 B,对 FPGA 的可重构区域进行动态部分配置. 如果 MAC4 和 MAC2 不匹配,则说明 E_B 被篡改,FPGA 置 Ack 的值为 Fail,计算相应的 MAC 值: $MAC_5 = MAC_{K_{MAC}}(Ack, FPGAID, TAG_H)$, 发送 Ack 和 MAC5 给控制单元,通知更新失败。

4 安全分析

本文的远程比特流安全更新方案采用对称加密算法 AES 来保证比特流的机密性,使用消息认证码 MAC 和版本标识 TAG 保证比特流的完整性和版本的新鲜性. 还采用了部分加密的方法,文献[7]证明了部分加密比全部加密的效果要好,尤其是对逆向工程,会增加逆向工程的难度和花费. 本文安全方案假设底层的密钥、加密模块和 MAC 功能是安全的. 因此,安全分析主要针对在远程更新配置端和 FRCP 端之间防止比特流的重放攻击和篡改。

在比特流通信两端进行远程交互的过程中,敌手可伪装成远程更新配置端或是 FRCP 端对比特流进行拦截. 篡改是指攻击者修改比特流信息然后发送,本文安全方案采用 MAC 对信息进行验证,可保证比特流的完整性. 一旦敌手修改信息,通过 MAC 值的计算和匹配就能发现。

重放攻击是指敌手监听并记录比特流信息,然后在某个时刻发送该过期的比特流,此类攻击对系统的危害性很大,会使系统性能降低. 本文安全方案通过在 MAC 的计算过程中使用版本标识 TAG 保证传输比特流的新鲜性,可防止重放攻击. 在安全更新协议交互的报文中包含不同的 TAG 标识,该 TAG 标识被加密封装在 MAC 中,在安全协议通信的两端均可以通过计算 MAC 验证 TAG 标识的合法性,并根据合法的 TAG 标识判断该比特流的新鲜性。

表 1 中给出了本文提出的安全方案与商用的 FPGA 供应商方案^[8]和 Kean 的方案^[9]在抵御攻击和远程更新方面的比较,突出本安全方案的优势。

表 1 各方案比较

	克隆攻击	逆向工程攻击	重放攻击	安全远程更新
FPGA 供应商方案	能防止	能防止	不能防止	密钥需采取措施防止丢失(使用外部电池)
Kean 的方案	能防止	能防止	不能防止	不支持
本文提出方案	能防止	能防止	能防止	支持,不需外部电池

5 结束语

基于 FPGA 的可重构计算平台(FRCP)是一种重要的高效能计算平台,本文针对 FRCP 平台中远程比特流更新面临的窃听、篡改和重放攻击等安全威胁,提出了一种远程比特流安全更新方案.分析表明,本文方案能够保证更新比特流的完整性和机密性,并能防止重放攻击.

参考文献:

- [1] Castillo J, Huerta P, Martinez J. Secure ip downloading for sram fpga[J]. Microprocessors and Microsystems, 2007(31):77-86.
- [2] Drimer S, Kuhn M G. A protocol for secure remote updates of fpga configuration[C]//Proceedings of the 15th International Workshop on Reconfigurable Computing: Architecture, Tools and Applications. Berlin, Heidelberg: Springer Verlag, 2009:50-61.
- [3] Devic F, Torres L, Badrignans B. Secure protocol implementation for remote bitstream update preventing replay attacks on FPGA[C]//Proceeding of the 20th International Conference on Field Programmable Logic and Applications. Italy:Milano, IEEE Computer Society, 2010:179-182.
- [4] 王沁,孙富明. FPGA 设计安全性综述[J]. 小型微型计算机系统, 2010,31(7):1333-1337.
- [5] GuangHuei C, Wen Tsuen C. Secure broadcasting using the secure lock[J]. Transactions on Software Engineering, 1989,15(8):929-934.
- [6] Yip Kun wah, Ng Tung Sang. Partial encryption technique for intellectual property protection of FPGA-based products[J]. IEEE Transactions on Consumer Electronics, 2000, 46(1):183-190.
- [7] Braeken A, Genoe J. Secure remote reconfiguration of an FPGA-based embedded system[C]// 6th International Workshop on Reconfigurable Communication-centric Systems-on-Chip(ReCoSoC). France, Montpellier: IEEE Computer Society, 2011:1-6.
- [8] Xilinx. 7 series FPGA configuration user guide[EB/OL]. [2013-03-10]. http://www.xilinx.com/support/documentation/user_guides/ug470_7Series_Config.pdf.
- [9] Kean T. Secure configuration of field programmable gate arrays[C]// Field-Programmable Logic and Applications. Berlin: Springer, 2001:142-151.

作者简介:

李磊 男, (1974—), 博士, 讲师. 研究方向为网络与信息安全.

张雪 女, (1989—), 硕士研究生. 研究方向为网络与信息安全.

陈静 女, (1977—), 博士, 讲师. 研究方向为 P2P、移动信息安全.

张志鸿 男, (1965—), 博士, 教授. 研究方向为服务计算、移动信息安全.

(上接第 63 页)

- [2] Candes E J, Donoho D L. New tight frames of curvelets and optimal representation of objects with piecewise-singularities[J]. Commun on Pure and Appl Math, 2004, 57(2):219-266.
- [3] Rudin L, Osher S, Fatemi E. Nonlinear total variation based noise removal algorithms[J]. Physica D, 1992 (60):259-268.
- [4] 阮秋琦 作冀颖. 数字图像处理中的偏微分方程方法[J]. 信号处理, 2012, 28(3):301-314.
- [5] Perona P, Malik J. Scale-space and edge detection using an isotropic diffusion[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 1990, 12 (7):629-639.
- [6] 陈利霞, 宋国乡, 丁宣浩, 等. 改进的总变分去噪算法[J]. 光子学报, 2009, 38(4):1001-1004.
- [7] 马少贤, 江成顺. 基于四阶偏微分方程的盲图像恢复模型[J]. 中国图象图形学报, 2010, 15(1):26-30.

作者简介:

周志立 男, (1979—), 讲师. 研究方向为多媒体通信、图像处理.

万登淦 男, (1975—), 助理研究员. 研究方向为计算机算法.