面向时序逻辑的门级信息流分析方法

毛保磊，慕德俊，胡　伟，南秦博，高　昂
(西北工业大学自动化学院,陕西西安,710072)

摘要　利用门级信息流追踪逻辑基础理论,研究了门级信息流时序逻辑扩展问题,在确定系统时钟作为基础可信源情况下,给出了扩展 4 种典型触发器的实现方案。针对 IWLS 测试向量集使用 Synopsys 综合编译器,生成 90 nm 标准库文件,对门级信息流跟踪逻辑的面积、时间延迟和功耗等参数进行了评估。与未经优化的原始 GLIFT 编码相比,在引入时序逻辑之后,电路的平均面积消耗降低了 50% 以上,时间延迟减少 13% 左右,获得的面积和时间延迟信息反映了在逻辑门级层次上实现细粒度信息流控制的复杂性;而仿真获得的功耗对比结果表明追踪逻辑的功耗达到原始逻辑的 5～20 倍左右,功耗问题需要进一步研究和优化。

关键词　信息流控制;时序逻辑;嵌入式安全
DOI　10.3969/j.issn.1009-3516.2013.03.016
中图分类号　TP314　　**文献标志码**　A　　**文章编号**　1009-3516(2013)03-0068-05

Gate Level Information Flow Control Research Based on Sequential Logic

MAO Bao-lei, MU De-jun, HU Wei, NAN Qin-bo, GAO Ang
(School of Automation, Northwestern Polytechnical University, Xian 710072, China)

Abstract: The timing logic problem of gate-level information flow is investigated based on basic GLIFT theory, the implementation of four typical triggers is given when the system clock is trusted. The gate-level information flow tracking logic area, time delay and power consumption are evaluated for the test vectors of the IWLS set using Synopsys compiler to generate 90 nm standard library files. Compared with the original GLIFT code, the average area of the circuit is reduces more than 50%, time delay is reduces about 13% when timing logic is introduced. The obtained area and time delay information reflect the complexity of fine-grained control of information flow; the simulation results of power consumption comparison show that the power consumption of the tracking logic reaches about 5 to 20 times the original logic, the power consumption issues need further research and optimization.

Key words: information flow control; sequential logic; embedded system security

应用在通信、汽车、航空、航天领域的嵌入式设备通常只关注其功能性,忽略了安全性,因而导致各种安全事故甚至灾难。在传统计算机保护领域中使用的信息流策略也逐渐应用在嵌入式系统保护中。信息流策略不仅能对关键信息和机密信息实现有效访问控制,而且对于数据流向和数据使用严格约束,同时信息流策略具有良好的数学描述,适合对于系统的安全属性进行建模和验证,及时排除系统设计

收稿日期:2012-11-12
基金项目:国家自然科学基金资助项目(61203233);航空科学基金资助项目(2012ZC53042);教育部高校博士点基金资助项目(20126102110036)
基金项目:毛保磊(1987－),男,河南郑州人,博士生,主要从事嵌入式系统安全和可靠性分析研究.
E-mail:maobaolei524@gmail.com

缺陷[1]。

Denning D.E.提出了信息流的概念,建立了信息流动的格模型[2]。Bell 和 LaPadula 提出的 BLP 模型从机密性角度描述了多级安全信息流。华保健设计了类 C 的安全语言 PointerC[3]。基于 Java 语言构造的在编译时执行类型检查的编译器 Jif 已经实现[4]。Histar 系统将系统资源划分为 6 个内核对象模块,并按照控制策略添加标签,实现信息在进程、网络设备、地址空间等资源间的安全流动[5]。Flume 系统实现了在 linux 操作系统上的用户空间基于进程、管道和文件描述符等标准操作系统抽象层次的安全策略[6]。ARM 处理器已经在核内实现了可信计算域 Trustzone[7],监控可信域与不可信域信息流动。Raksha 系统采用扩展指令集的方法,在 Leon SPARC V8 处理器上实现动态数据流控制[8]。RIFLE 则将存在的隐式流转化为显式流进行动态信息流控制[9]。M. Tiwari 等从系统硬件和底层对嵌入式系统的安全性进行探讨,提出一种从系统底层开始对信息流的安全性进行分析和控制的思路[10]。胡伟等从比特位信息流安全控制的理论方面进行阐述,定义和分析门级信息流追踪技术的性质,提供了门级信息流追踪技术基本布尔函数的形式化分析和量化分析方法。并且针对生成门级逻辑的算法复杂性进行了分析和证明[11]。归纳不同层次信息流的实现和性能见表 1。

表 1　基于信息流策略的安全系统[4,6-13]

Tab.1　Secure systems based on information flow policy

抽象层次	监控对象	典型实现(时间开销)	应用方法
应用	应用层,Web 应用	TAJ(1～3 倍)	静态(基于编译和执行)
编译,语言	类型系统	Jif(1 倍)	静态(基于编译和执行)
操作系统	内核基元	TaintDroid(135%), Flume(4～35 倍)	动态(基于编译和执行)
体系架构	操作指令	Trustzone,Raksha(134%),RIFLE(1～2 倍)	动态(基于执行)
逻辑门,功能单元	安全基础	GLIFT(1～2 倍)	动态

1　门级信息流分析

1.1　门级信息流技术的组合逻辑验证基础

门级信息流追踪技术就是将数据信息从数据的二进制位开始进行可信性或机密性分析,将其机密性或者可信性作为数据的属性标签进行标记。在将信息流分析从字节粒度降低到基于二进制位时,数据的安全属性可能呈现出与我们主观认为不一致的地方。以或门为例 a,b 是原始输入,a_t,b_t 分别代表 a,b 的安全属性,当 a 可信时,a_t 值为 0,当 a 不可信时,a_t 值为 1,o_t 表示追踪逻辑结果是否可信,可信为 0,不可信为 1.通常认为,只要在输入端存在着不可信的信息,那么计算出来的结果也肯定是不可信的,但是,门级信息流追踪的分析则指出,对于数据可信属性的判定不仅依赖于其属性标签,在一定范围内与数据本身也存在关联。以第 7 行为例,当 a_t 为 1 时,表示 a 的值不可信,可能 a 的值由 1 被篡改为 0,这时考察 a 分别为 0,1 时的值对应着的原始逻辑输出 o 的值,如果 2 种情况下 o 的值相同,表示 o 的输出是可信的,o_t 为 0,否则 o_t 为 1.本例中 o 的输出相同,o_t 为 1.由表 2 的分析我们可以得到或门对应的信息流追踪组合逻辑,见图 1。

表 2　二输入或门真值表

Tab.2　2-input OR-gate truth table

#	a	b	a_t	b_t	O_t
1	0	0	0	0	0
2	0	0	0	1	1
3	0	0	1	0	1
4	0	0	1	1	1
5	0	1	0	0	0
6	0	1	0	1	1
7	0	1	1	0	0
8	0	1	1	1	1
9	1	0	0	0	0
10	1	0	0	1	0
11	1	0	1	0	1
12	1	0	1	1	1
13	1	1	0	0	0
14	1	1	0	1	0
15	1	1	1	0	0
16	1	1	1	1	1

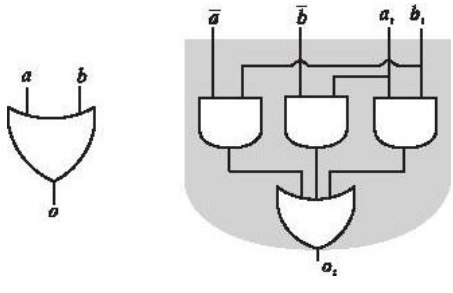

图 1　原始逻辑与门信息流追踪逻辑

Fig.1　Original and GLIFT logic of OR-gate

下面以 $sh(f)$ 表示 f 的安全属性进行形式化描

述可得:

或门 $sh(g+h)=\bar{g}\cdot sh(h)+\bar{h}\cdot sh(g)+sh(g)\cdot sh(h)$ (1)

与门 $sh(g\cdot h)=g\cdot sh(h)+h\cdot sh(g)+sh(g)\cdot sh(h)$ (2)

异或门 $sh(g\otimes h)=sh(h)+sh(g)$ (3)

1.2 门级信息流的时序逻辑电路设计

基于组合逻辑的信息流安全验证方法虽然已经得到系统研究,但是并没有给出时序逻辑电路详细的分析。时序逻辑是实现 CPU 处理单元的基础组成部分,完成门级信息流分析的时序逻辑扩展将为下一阶段构造完整的安全处理器奠定基础。

首先选择触发器中使用最广泛而且形式最简单的 D 触发器。

D 触发器特征方程为:

$$Q^{n+1}=D \tag{4}$$

时钟信号取自系统基准时钟,以其作为基础的可信源。当一个时钟脉冲作用后,D 触发器输出状态取值为 D 端输入,其状态转换过程与简单赋值语句是一致的。所以,门级信息流追踪 D 触发器转换方程为:

$$sh(Q^{n+1})=sh(D) \tag{5}$$

set 和 reset 信号作为可信输入源,对应 D 触发器的寄存器级描述见图 2。

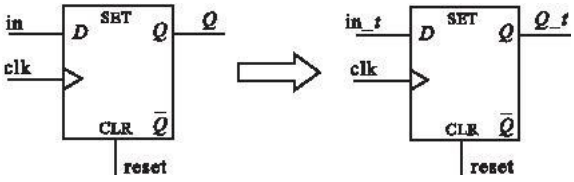

图 2 D 触发器原始逻辑与追踪逻辑

Fig.2 Original and GLIFT logic of D flip-flop

T 触发器特征方程:

$$Q^{n+1}=T\oplus Q^{n} \tag{6}$$

由于 T 触发器不含有除时钟之外的任何形式的条件约束,应用异或门安全属性形式化描述方程(1)扩展 T 触发器,可得 T 触发器转换方程:

$$sh(Q^{n+1})=sh(T)+sh(Q^{n}) \tag{7}$$

J-K 触发器特征方程:

$$Q^{n+1}=\bar{K}Q^{n}+J\overline{Q^{n}} \tag{8}$$

形式类似于二选一选择器,应用文献[11]中二选一选择器扩展的转化方程如下:

$$sh(Q^{n+1})=\overline{Q^{n}}sh(J)+Q^{n}sh(\bar{K})+JKsh(Q^{n})+\overline{JK}sh(Q^{n})+sh(\bar{K})sh(Q^{n})+sh(J)sh(Q^{n}) \tag{9}$$

R-S 触发器特征方程:

$$\begin{cases} Q^{n+1}=S+\bar{R}Q^{n} \\ SR=0 \end{cases} \tag{10}$$

由于约束条件的存在,不易于公式进行拓展,利用门级信息流追踪的原始定义可得:

$$sh(Q^{n+1})=f(R,S,Q^{n},sh(R),sh(S),sh(Q^{n}))=\sum_{m}(1,2,3,6,7,9,11,12,13,14,15,18,19,22,23,27,29,31,37,38,39,44,45,46,47) \tag{11}$$

2 实验评估

为了评估引入时序逻辑后对门级信息流追踪逻辑的影响,我们采用 IWLS 测试向量集进行测试[14],IWLS 测试向量集中包含着组合逻辑和时序逻辑电路,更加接近实际应用电路。在获得面积、时间、功耗信息之后,我们将其与单独的组合逻辑进行对比,发现引入时序逻辑后追踪逻辑的面积消耗减少,延迟变小。

针对 IWLS 测试向量集我们使用 Synopsys 综合编译器,生成 90 nm 标准库文件。获得面积和时间延迟信息如下:

由表 3 测试数据,追踪逻辑的布线面积达到原始逻辑的 2.69 到 5.39 倍,但是追踪逻辑时间延时一般在 1～2 ns 之内,其追踪逻辑与原始逻辑延迟比最高到 5.31 倍。可见追踪逻辑开销远高于原始逻辑,代价高昂。与未经优化的原始 GLIFT 编码相比,在引入时序逻辑之后,电路的平均面积消耗降低了 50% 以上,时间延迟减少 13% 左右,与优化过的经过新编码的 GLIFT 比较,IWLS 测试集的面积消耗和时间延迟仍然需要改进。

同时由图 3 能量功耗对比可见,追踪逻辑的功耗达到原始逻辑的 5～20 倍左右,这是因为追踪逻辑电路中不仅包含着原始逻辑的电路,而且存在着规模更大的对应着原始逻辑的追踪逻辑电路。

图 3 原始逻辑电路与追踪逻辑电路能耗分析
(纵轴是以 10 为底的对数指数表示)

Fig.3 Power analysis of IWLS benchmarks and related GLIFT (the vertical axis is in logarithmic scale)

表 3　IWLS 测试集原始逻辑与追踪逻辑面积和延迟测试

Tab. 3　Area and delay tests of IWLS benchmarks and related GLIFT

测试项	面积/um²			延迟/ns		
	原始逻辑	追踪逻辑	比值	原始逻辑	追踪逻辑	比值
s27	141	460	3.25	0.20	0.46	2.30
s208	531	1614	3.04	0.50	1.42	2.84
s298	909	3127	3.44	0.11	0.13	1.18
s386	675	2 772	4.11	0.40	0.74	1.85
s641	1 507	6 582	4.37	0.62	1.77	2.85
s713	1 507	6 582	4.37	0.62	1.77	2.85
s838	2 194	6 675	3.04	1.14	4.31	3.78
s1196	3 836	15 472	4.03	0.57	1.54	2.70
s1238	3 755	14 566	3.88	0.60	1.39	2.32
s1423	5 458	19 710	3.61	0.92	2.30	2.50
s1488	2 675	12 847	4.80	0.54	1.07	1.98
s1494	2 756	12 750	4.63	0.54	1.09	2.02
s5378	11 204	38 194	3.41	0.62	1.45	2.34
s9234	9 063	31 323	3.46	0.41	0.53	1.29
s13207	11 715	51 997	4.44	0.26	1.38	5.31
s15850	6 499	35 034	5.39	0.11	0.48	4.36
s35932	120 742	447 622	3.71	0.35	0.58	1.66
s38417	93 604	251 795	2.69	0.37	0.52	1.41
s38584	83 778	324 957	3.88	0.37	1.35	3.65
平均			3.87			2.59

3　结语

论文针对门级信息流时序逻辑扩展问题给出了一种简单的实现方法。将系统的基准时钟作为可信来源,分别完成了 D 触发器、T 触发器、J-K 触发器和 R-S 触发器的对应追踪逻辑的实现,并结合 IWLS 测试集评估了相关的面积、延迟和功耗,实验表明引入时序逻辑后追踪逻辑的面积消耗减少,延迟变小。

参考文献(References):

[1] 肖军模,刘军,周海刚.网络信息安全[M]. 北京:机械工业出版社,2006.
XIAO Junmo, LIU Jun, ZHOU Haigang. Network information security [M]. Beijing: China machine press, 2006. (in Chinese)

[2] 张迎周,刘玲玲. 信息流安全技术回顾与展望[J]. 南京邮电大学学报:自然科学版,2011,31(5):87-96.
ZHANG Yingzhou, LIU Lingling. Review and prospect for information flow security technology [J]. Journal of Nanjing university of posts and telecommunications:natural science edition, 2011,31(5):87-96. (in Chinese)

[3] 华保健,陈意云,李兆鹏,等. 安全语言 Pointer C 的设计及形式证明[J]. 计算机学报,2008,31(4):556-564.
HUA Baojian, CHEN Yiyun, Li Zhaopeng, et al. Design and proof of a safe programming language Pointer C[J]. Chinese journal of compu ters, 2008,31(4):556-564. (in Chinese)

[4] Myers A C, Nystrom N, Zheng L, et al. Jif:java information flow[EB/OL]. [2013-1-20]. http://www.cs.cornell.edu/jif.

[5] Nickolai Zeldovich, Silas Boyd-Wickizer, Eddie Kohler, et al. Making information flow explicit in hi star[C]//Proc 7th symposium on operating systems design and implementation. Seattle, USA: USENIX association Berkeley, 2006: 263-278.

[6] Maxwell Krohn, Alexander Yip. Information flow control for standard OS abstractions [C]//Proc SOSP'07. Washington DC:ACM press, 2007: 321-334.

[7] Tiago Alves, Don Felton. Trust zone: integrated hardware and software security enabling trusted computing in embedded systems [J]. Information quarterly, 2004(4): 18-24.

[8] Michael Dalton, Hari Kannan Raksha. A flexible information flow architecture for software security [C]//Proc 34th ISCA. California: ACM press, 2007: 482-493.

[9] Neil Vachharajani Matthew J Bridges. RIFLE: an architectural framework for user-centric information-flow security information-flow security[C]//Proceedings of the 37th international symposium on microarchitecture (MICRO-37'04). Portland: IEEE/ACM press, 2004: 243-254.

[10] Mohit Tiwari, Hassan M G Wassel, Bita Mazloom, et al. Complete information flow tracking from the gates up[C]//Proc 14th ASPLOS. Washington, DC: ACM press, 2009: 109-120.

[11] Wei Hu, Jason Oberg. Theoretical fundamentals of gate level information flow tracking[J]. IEEE trans on CAD, 2011, 30(8): 1128-1140.

[12] William Enck, Peter Gilbert, Byung-Gon Chun, et al. Taint Droid: an information-flow tracking system for realtime privacy monitoring on smartphones [C]//Proceeding of the 9th USENIX symposium on operating systems design and implementation. Vancouver, BC, Canada: USENIX association Berkeley, 2010: 393-408.

[13] Tripp O, Pistoia M, Fink S J, et al. Effective taint analysis of web applications[C]//Programming language design and implementation. Dublin, Ireland: ACM press, 2010: 87-97.

[14] IWLS benchmark [S/OL]. (2005-06-08)[2012-11-12]. http://iwls.org/iwls2005/benchmarks.html.

(编辑:徐楠楠)

(上接第 45 页)

[2] 田宏伟,敬忠良,胡士强,等.基于多速率运动模型的多帧最邻近数据关联算法[J].上海交通大学学报,2005, 39(3):413-416.
TIAN Hongwei, JING Zhongliang, HU Shiqiang, et al. Multiple scan nearest eighbor data association algorithm Based on multirate kinematic model[J]. Journal of Shanghai jiaotong university, 2005, 39(3): 413-416. (in Chinese)

[3] 杨万海.多传感器数据融合及其应用[M]. 西安:西安电子科技大学出版社,2004.
YANG Wanhai. Multi-sensor data fusion and applications[M]. Xi'an: Xidian university publishing house, 2004. (in Chinese)

[4] 夏佩伦.目标跟踪与信息融合[M]. 北京:国防工业出版社,2010.
XIA Peilun. Target tracking and information fusion [M]. Beijing: National defense industrial press, 2010. (in Chinese)

[5] 石章松,刘忠.目标跟踪与数据融合理论及方法[M]. 北京:国防工业出版社,2010.
SHI Zhangsong, LIU Zhong. Method and thoery of target tacking and data fusion[M]. Beijing: National defense industrialpress, 2010. (in Chinese)

[6] Bar Shalom Y, Li X R. Multitarget-multisensor tracking principles techniques[J]. Control system IEEE, 1996, 11(2): 41-44.

[7] Ilke Turkmen, Kerim Guney Cheap. Joint probabilistic data association with adaptive neuro-fuzzy inference system state filter for tracking multiple targets in cluttered environment[J]. International journal of electronics and communications, 2004, 58(5): 349-357.

[8] 廖辉荣,李国林.多目标跟踪中联合概率数据关联优化算法[J].计算机仿真,2011, 28(11): 14-18.
LIAO Huirong, LI Guolin. Joint probability algorithm in data association based on DHN artificial nerve network[J]. Computer simulation, 2011, 28(11): 14-18. (in Chinese)

[9] 王耀南.智能信息处理技术[M].北京:高等教育出版社,2003.
WANG Yaonan. Intelligent information processing technology [M]. Beijing: Higher education press, 2003. (in Chinese)

(编辑:田新华)