基于门级信息流分析的多值逻辑形式化方法研究

邰瑜, 慕德俊, 胡伟, 毛保磊, 郭蓝天

(西北工业大学 深圳研究院, 广东 深圳 518057)

摘 要:硬件系统设计规模的增大使得测试和验证覆盖率难以保证,所隐含的安全漏洞容易导致敏感信息泄露。门级信息流分析方法能够实现对硬件中全部逻辑信息流精确度量,防止有害信息流所引发的信息泄露。现有的工作主要研究布尔逻辑系统下门级信息流分析的基本理论、生成算法、跟踪逻辑形式化及检测验证等问题。然而,在硬件系统的设计和验证中通常需要采用多值逻辑描述电路的逻辑状态,基于门级信息流分析方法,采用构造方法生成系统的信息流模型,研究多值逻辑标签传播问题,分别构建针对四值逻辑和九值逻辑的标签传播规则集,对门级信息流跟踪逻辑进行形式化描述,通过分析多值逻辑传播规则的逻辑特性对基本门信息流跟踪逻辑进行扩展。

关 键 词:门级信息流分析;多值逻辑;标签传播规则;形式化描述;GLIFT 逻辑
中图分类号:TP309 **文献标志码**:A **文章编号**:1000-2758(2017)05-0884-06

硬件电路设计规模的增长导致系统测试和验证覆盖率难以保证,使硬件系统中可能隐含的设计缺陷、安全脆弱点及恶意代码等安全漏洞难以检测。而这些安全漏洞为攻击者提供了更多的切入点,成为黑客攻击系统的突破口。例如,Web 浏览器由于算术操作在运行时的变化泄露了登录凭证[1]。传统硬件系统在设计阶段并未充分考虑安全性需求,更加注重目标设计的正确性和功能性指标[2],从而使其隐含的安全漏洞在系统受到攻击时导致敏感信息泄露或引发系统失效。信息流跟踪(information flow tracking,IFT)方法根据输入及其标签在系统运算中的传播,通过输出标签类型确定输出的安全属性[3]。该方法能够有效监控信息在系统中的流动,防止有害信息流对系统造成的破坏。门级信息流跟踪(gate level information flow tracking,GLIFT)方法,从逻辑门级抽象层次精确地监控每个二进制位信息的流动,通过对电路中全部逻辑信息流进行精确地度量,捕捉有害的信息流动来检测和消除设计中潜在的安全漏洞[4]。

国外已经对 GLIFT 方法进行了大量研究。现有门级信息流分析方法的基本理论包括信息流分析逻辑的性质定理、形式化描述、生成算法及复杂度理论等[5]。其次,利用 GLIFT 方法检测和消除交叉信任环境下片上系统的时序信息流,设计了隔离硬件时序信道的测试框架[6]。SecVerilog 允许设计者通过可验证的可变类型函数定义为不同的操作描述自己的标签传播规则[7]。RTLIFT 通过现有的 EDA 工具,在寄存器传输级使用精确的信息流跟踪规则自动生成 IFT 逻辑[8]。此外,GLIFT 已被用于研究逻辑综合对硬件信息流跟踪的质量和复杂性的影响[9]。国内关于门级信息流跟踪信的研究相对较少,采用信息理论度量对 RSA 的时间隐通道进行了量化分析,对信息泄露进行了精确度量[10]。提出了一种自底向上的信息流方法来保证设计安全嵌入式系统,能够在整个系统堆栈中证明抽象级别的安全属性[11]。

现有的研究主要针对布尔逻辑系统下的门级信息流跟踪的标签传播问题、基本门 GLIFT 逻辑的形式化描述、门级信息流生成算法进行了讨论。然而,不足之处在于实际的数字电路设计和验证中,通常需要采用多值逻辑对电路的状态进行描述和仿真,现有研究无法满足硬件电路设计的需求。本文研究

收稿日期:2017-03-01 **基金项目**:国家自然科学基金(61303224、61672433)、国家密码发展基金(MMJJ20170210)与深圳市科创委基础研究基金(201703063000517)资助
作者简介:邰瑜(1982—),西北工业大学博士研究生,主要从事硬件安全及逻辑优化研究。

多值逻辑系统下门级信息流分析的标签传播问题,构建面向多值逻辑系统的污染传播规则,对多值逻辑系统下基本门的 GLIFT 逻辑进行形式化描述。

1　信息流逻辑系统

1.1　信息流格模型

信息流分析是一种通过静态验证来强化信息流安全策略的方法,通常采用格模型来描述信息流策略[12]。任一信息流策略都可采用形如 $L=(SC,\subseteq)$ 的安全格(security lattice) 来描述。其中,SC 是安全类的集合以表示不同数据类型的安全级别;是定义在该安全类集上的偏序关系,规定了不同安全类之间许可的数据流向,即只允许信息在同一安全类之内或者向更高级别的安全类流动。定义函数 $L:x\rightarrow SC$ 表示安全数据对象 x 所属的安全类。箭头'→'表示由安全策略和安全格偏序关系定义的信息流动的方向。本文利用线性安全格对多值逻辑的门级信息流进行分析,设{U→C→S→T}为一个线性安全格,U、C、S、T 表示安全格中不同的安全等级,SC={U,C}、SC={U,C,S}、SC={U,C,S,T}分别为二级、三级和四级线性安全格,二级到四级线性安全格下基于门级信息流跟踪方法的二输入与门 AND-2 的标签传播规则如表 1 所示。

表 1　二级到四级线性安全格下 AND-2 的标签传播规则

A^{a_t}	B^{b_t}							
	0^U	1^U	0^C	1^C	0^S	1^S	0^T	1^T
0^U	0^U	0^U	0^U	0^U	0^U	0^U	0^U	0U
1^U	0^U	1^U	0^C	1^C	0^S	1^S	0^T	1^T
0^C	0^U	0^C	0^C	0^C	0^C	0^C	0^C	0^C
1^C	0^U	1^C	0^C	1^C	0^S	1^S	0^T	1^T
0^S	0^U	0^S	0^C	0^S	0^S	0^S	0^S	0^S
1^S	0^U	1^S	0^C	1^S	0^S	1^S	0^T	1^T
0^T	0^U	0^T	0^C	0^T	0^S	0^T	0^T	0^T
1^T	0^U	1^T	0^C	1^T	0^S	1^T	0^T	1^T

以二级线性安全格{U,C}和二输入与门 AND-2 为例,表 1 的第二行和第二列,若 AND-2 任一输入为 0^U,则其输出固定为 0^U,与另一个输入无关。可见,门级信息流分析方法在计算输出的安全标签时不仅考虑输入的安全标签,还考虑了输入对输出的实际影响,能够更准确地对系统中实际存在的信息流进行度量,比传统保守的信息流分析方法更为准确。

1.2　多值逻辑系统

门级信息流的逻辑运算是定义在布尔逻辑系统下的,实际的数字电路设计与验证中通常需要采用多值逻辑来描述电路的逻辑状态,表 2 给出了 IEEE 标准定义的九种逻辑状态。如表 2 斜体所示,不确定态'X'、逻辑'0'、逻辑'1'和高阻态'Z'构成的四值逻辑系统是实际应用中最常用的多值逻辑系统。本文分别在四值逻辑和九值逻辑系统下对污染传播问题和 GLIFT 逻辑的形式化描述进行研究。

表 2　IEEE 标准定义的九值逻辑系统

符号	英文名称	中文名称
U	Uninitialized	未初始化
X	Forcing unknown	不确定态
0	Forcing 0	低电位
1	Forcing 1	高电位
Z	High impedace	高阻态
W	Weak unknown	弱不确定态
L	Weak 0	弱低电位
H	Weak 1	弱高电位
-	Don't care	无关电位

2　GLIFT 多值逻辑形式化分析

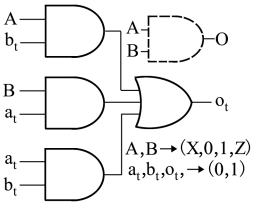
本文基于门级信息流分析方法,采用构造方法生成多值逻辑系统下的门级信息流模型,分析污染标签在信息流传播中的运算规则,并对多值逻辑 GLIFT 逻辑进行了形式化描述。

2.1　多值逻辑的门级信息流分析

GLIFT 方法在门级抽象层次上采用标签传播策略进行精确的信息流分析。每个输入二进制位数据都分配有一位的标签,此标签即被称为该数据位的污染标志表示其安全级别,标签随数据在系统中参与运算而流动和传播。当数据的污染为逻辑真('1')时,称该数据所包含的信息是受污染的(tainted);当数据的污染为逻辑假('0')时,则称此数据未受污染(untainted)。任何污染的输入都对输出产生影响,并随着输入传播到数据的输出。

四值逻辑情况下考虑如图 1a)所示二输入与门 AND-2 及其 GLIFT 逻辑;图 1b)为四值逻辑下与门包含污染信息的部分真值表,a_t、b_t 和 o_t 分别表示输入 A、B 和输出 O 的污染标签。四值逻辑下 A、B 和 O 的取值域为(X,0,1,Z),污染标签要么是未受污染('0')或受污染('1'),因此其污染标签 at、bt 和 ot 的值为(0,1)。

考虑图 1b)第二行(A = 1; B = 1; a_t = 0; b_t = 0),当 2 个输入都是未受污染的,则输出可确定是未受污染的。类似地,当 2 个输入都是受污染的,则输出必然是受污染的,如第七行(A = 0; B = X; a_t = 1; b_t = 1)所示。第一行(A = 0; B = X; a_t = 0; b_t = 1),输入 B 是受污染的,输入 A 是未受污染的,输出是未受污染的的(o_t = 0),此时受污染的输入没有对输出产生影响,未受污染的输入 A 阻止了受污染的输入 B 的污染信息流至输出。第三行(A = 1; B = 0; a_t = 0; b_t = 1)和第五行(A = 1; B = X; a_t = 0; b_t = 1)中未受污染的 A(a_t = 0)和受污染的 B(b_t = 1)的输出 O 都是受污染的(o_t = 1);第六行(A = 0; B = X; a_t = 1; b_t = 0)中受污染的 A(a_t = 1)和未受污染的 B(b_t = 0)的输出 O 也是受污染的(o_t = 1),此时观察到输出的标签是受污染的,因此被污染的输入对输出产生了影响,输出被标记为受污染的。真值表表明输出的污染不仅涉及输入的污染同时也依赖于输入本身,通过真值表可以得到与门的 GLIFT 逻辑电路如图 1a)所示。



a) AND-2 及其 GLIFT 逻辑

#	A	o_t	b_t	a_t	O	o_t
1	0	0	X	0	0	0
2	1	0	1	0	1	0
3	1	0	0	1	0	1
4	1	0	X	0	X	0
5	1	0	X	1	X	1
6	0	1	X	0	0	1
7	0	1	X	1	0	1
8	X	0	X	1	X	1

b) AND-2 部分真值表

图 1 四值逻辑下与门 AND-2 的信息流分析

2.2 系统构造方法

构造方法如图 2 所示,给定采用硬件语言(VHDL 或 Verilog)描述的硬件设计,首先需采用逻辑综合工具,根据硬件的技术/工艺规范将设计映射为门级网表。同时,该构造方法需要创建一个包含基本逻辑单元的信息流模型库,并由基本的 GLFIT 库集成为复杂信息流模型库。然后,为该门级网表中的各逻辑单元离散式地实例化信息流模型,生成相应的门级信息流分析逻辑。基于门级信息流分析的多值逻辑系统可以进行形式化描述,并在其基础上对设计中底层硬件实现的全部逻辑信息流进行准确度量,捕捉包括硬件相关时间隐通道在内的全部逻辑信息流,从而检测信息流安全策略是否被违反,为设计修改提供指导。

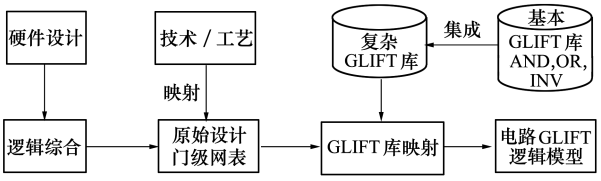


图 2 逻辑电路信息流模型的生成方法

2.3 多值逻辑污染传播规则

相对于布尔逻辑,四值逻辑增加了不确定态‘X’和高阻态‘Z’,表 3 定义了包含不确定态‘X’和高阻态‘Z’在内的四值逻辑的与、或、非运算规则。

表 3 四值逻辑系统下的与、或、非运算规则

AND-2	X	0	1	Z	OR-2	X	0	1	Z	NOT
X	X	0	X	X	X	X	X	1	X	X
0	0	0	0	0	0	X	0	1	X	1
1	X	0	1	X	1	1	1	1	1	0
Z	X	0	X	X	Z	X	X	1	X	X

根据 GLIFT 方法的基本原理,当且仅当受污染的输入对输出存在影响时,污染信息才能流向输出,输出才会受到污染,因此,由表 3 可得到 AND-2 在四值逻辑系统下的污染传播规则,如表 4 所示,其中“U”表示未受污染,‘T’表示受污染。

表 4 AND-2 在四值逻辑系统下的标签传播规则

A^{a_t}	B^{b_t}							
	0^U	0^T	1^U	1^T	X^U	X^T	Z^U	Z^T
0^U	0^U	0^U	0^U	0^U	0^U	0^U	0^U	0^U
0^T	0^U	0^T	0^T	0^T	0^T	0^T	0^T	0^T
1^U	0^U	0^T	1^U	1^T	X^U	X^T	X^U	X^T
1^T	0^U	0^T	1^T	1^T	X^T	X^T	X^T	X^T
X^U	0^U	0^T	X^U	X^T	X^U	X^T	X^U	X^T
X^T	0^U	0^T	X^T	X^T	X^T	X^T	X^T	X^T
Z^U	0^U	0^T	X^U	X^T	X^U	X^T	X^U	X^T
Z^T	0^U	0^T	X^T	X^T	X^T	X^T	X^T	X^T

表中第 4、6、8 行输出结果的污染标签是相应一致的,第 5、7、9 行输出结果的污染标签也是相应一致的;同时第 4、6、8 列输出结果的污染标签是相应一致的,第 5、7、9 列输出结果的污染标签也是相应一致的。可见,不确定态‘X’和高阻态‘Z’的污染传播规则与逻辑‘1’状态上的标签传播规则是完全一致的。

九值逻辑是在四值逻辑基础上增加了未初始化

'U',弱不确定态'W',弱低电位'L',弱高电位'H'和无关电位'-'5 种逻辑状态。表 5 给出了 IEEE-1164 定义的九值逻辑系统下与运算规则。

表 5　九值逻辑系统下的与运算规则

AND-2	0	1	X	Z	U	W	L	H	-
0	0	0	0	0	0	0	0	0	0
1	0	1	X	X	U	X	0	1	X
X	0	X	X	X	U	X	0	X	X
Z	0	X	X	X	U	X	0	X	X
U	0	U	U	U	U	U	0	U	U
W	0	X	X	X	U	X	0	X	X
L	0	0	0	0	0	0	0	0	0
H	0	1	X	X	U	X	0	1	X
-	0	X	X	X	U	X	0	X	X

采用 GLIFT 方法对九值逻辑系统下的标签传播规则进行分析,与四值逻辑类似,可以得到九值逻辑系统下的标签传播规则集。多值逻辑系统下的标签传播规则的一致性有助于对 GLIFT 逻辑的描述。

2.4　多值逻辑系统下的 GLIFT 逻辑

在二级安全格下以与门 AND-2、或门 OR-2、非门 NOT 为例,采用四值逻辑对门级信息流分析 GLIFT 逻辑进行形式化描述。如表 2 所示二级安全格,布尔逻辑系统下以 A、B 和 O 表示与门的输入和输出,以 a_t、b_t 和 o_t 分别表示它们的污染标签,当污染标签为'0'时未受污染,当污染标签为'1'时受污染。则由表 2 可推导出 AND-2 在布尔逻辑系统下 GLIFT 逻辑可采用(1)式来描述。

$$o_t = Ab_t + Ba_t + a_tb_t \tag{1}$$

四值逻辑系统下若输入 A 是受污染的逻辑'0'或逻辑'1',输入 B 是未受污染的不确定态'X',根据(1)式计算得到的输出的污染标签为不确定态'X'。而根据污染标签的定义,一个变量要么是受污染的,要么是未受污染的,因此,其污染标签的取值不能为不确定态'X'。因此,(1)式给出的 AND-2 的 GLIFT 逻辑不能用于多值逻辑系统下的污染传播。根据表 4 中不确定态'X'和高阻态'Z'上的污染传播规则与逻辑'1'状态上的污染传播规则一致性的结论,可对 AND-2 的 GLIFT 逻辑进行扩展,即当变量为不确定态'X'或高阻态'Z'时,将其置为逻辑'1'。AND-2 在二级安全格和四值逻辑系统下 GLIFT 逻辑可用(2)式来描述。

$$o_t = A_{XZ}b_t + B_{XZ}a_t + a_tb_t$$
$$(A_{XZ} = A_{XZ} === X \parallel A_{XZ} === Z)\ ?\ 1 : A; \tag{2}$$
$$B_{XZ} = (B_{XZ} === X \parallel B_{XZ} === Z)\ ?\ 1 : B)$$

对于或门 OR-2,可根据不确定态'X'和高阻态'Z'的逻辑或运算规则推导四值逻辑系统下 OR-2 的污染传播规则,进而对 OR-2 的 GLIFT 逻辑进行描述。或可利用与门和或门的逻辑对称性导出四值逻辑系统下 OR-2 的 GLIFT 逻辑,此时不确定态'X'或高阻态'Z'变量的值应置为逻辑'0'。OR-2 在四值逻辑系统下 GLIFT 逻辑可用(3)式来描述。

$$o_t = \overline{A_{XZ}}b_t + \overline{B_{XZ}}a_t + a_tb_t$$
$$(A_{XZ} = A_{XZ} === X \parallel A_{XZ} === Z)\ ?\ 0 : A; \tag{3}$$
$$B_{XZ} = (B_{XZ} === X \parallel B_{XZ} === Z)\ ?\ 0 : B)$$

考虑非门的逻辑表达式为 $O=\overline{A}$,输入 A 的污染标签 ,由于非门的输出总是跟随输入发生变化,输出标签取决于输入的污染标签,所以非门在四值逻辑系统下 GLIFT 逻辑可用(4)式来描述。

$$o_t = a_t \tag{4}$$

在推导四值逻辑系统下基本门的 GLIFT 逻辑时,应将不确定态'X'或高阻态'Z'变量的值置为当前逻辑门的无关输入项(Don't care),即将该变量直接从 GLIFT 逻辑中消去。

在九值逻辑系统下对于基本逻辑门,定义在逻辑'L'状态上的标签传播规则与定义在逻辑'0'上的标签传播规则完全一致,定义在逻辑'H'状态上的标签传播规则与定义在逻辑'1'上的标签传播规则完全一致,此时不需要对原有的 GLIFT 逻辑进行任何修改。以逻辑与门为例,定义在逻辑'U'、'X'、'Z'、'W'和'-'状态上的标签传播规则与定义在逻辑'1'上的标签传播策略是完全一致的,在污染传播中应将这些转态转换为逻辑'1'。

3　实验分析

本文采用 Mentor Graphics ModelSim 逻辑仿真工具验证四值逻辑系统下门级信息流分析的标签传播规则与扩展的 GLIFT 逻辑一致性。比较仿真结果与表 4 所示的污染传播规则的一致性。如图 3 所示,从仿真图可以看出,输入 B 的输入依次为'0'、'1'、'X'、'Z'且污染标签 bt 分别取'0'和'1',当输入 A = 1,污染标签 $a_t = 0$ 时,此时,输出 O = 0011XXXX,输出污染标签 $o_t = 01010101$;当输入 A =X,污染标签 $a_t = 0$ 时,输出 O = 00XXXXXX,输出污染标签 $o_t = 01010101$,即图 3 中的 GLIFT 逻辑在

表 4 中对应第 4 行和第 6 行且验证了这两行污染传播规则具有是一致性;当输入 A = 1,污染标签 a_t = 1 时,此时,输出 O = 0011XXXX,输出污染标签 o_t = 01111111;当输入 A = X,污染标签 a_t = 1 时,输出 O = 00XXXXXX,输出污染标签 o_t = 01111111;即图 3 中的 GLIFT 逻辑在表 4 中对应第 5 行和第 7 行且验证该两行污染传播规则具有具有一致性。表 4 中的标签传播规则可由图 3 得到,仿真实验验证了四值逻辑系统 GLIFT 逻辑扩展方法的有效性。

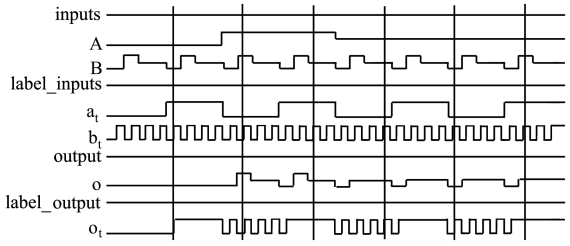


图 3 四值逻辑系统下的 GLIFT 逻辑

进一步采用仿真工具对九值逻辑的标签传播规则与扩展的 GLIFT 逻辑的一致性进行验证。如图 4 所示,输入 B = 01XZUWLH-且污染标签 b_t 分别取‘0’和‘1’,当输入 A = 1,污染标签 a_t = 0 时,则输出 O = 0011XXXXUUXX0011XX,输出污染标签 o_t = 010101010101010101;当输入 A = X,污染标签为 a_t = 0 时,此时,输出 O = 00XXXXXXUUXX00XXXX,输出污染标签 o_t = 010101010101010101,即图 4 中的 GLIFT 逻辑在与九值逻辑系统下的标签污染传播规则具有一致性;当输入 A = 1,污染标签 a_t = 1 时,则输出 O = 0011XXXXUUXX0011XX,输出污染标签 o_t = 011111110111011111;当输入 A = X,污染标签 a_t = 1 时,此时,输出 O = 00XXXXXXUUXX00XXXX,输出污染标签 o_t = 011111110111011111;即图 4 中的 GLIFT 逻辑在九值逻辑系统下的标签污染传播规则是一致的。相应地,九值逻辑的门级信息流分析逻辑可在图 4 中得到验证。

由表 2 和表 3,在多值逻辑下门级信息流分析的标签传播中,应将逻辑‘X’、‘Z’或逻辑‘U’、‘X’、‘Z’、‘W’、‘-’状态设置为当前逻辑门的无关项,使污染标签可以在多值逻辑环境下随信息流传播。仿真实验表明该扩展方法是有效的。

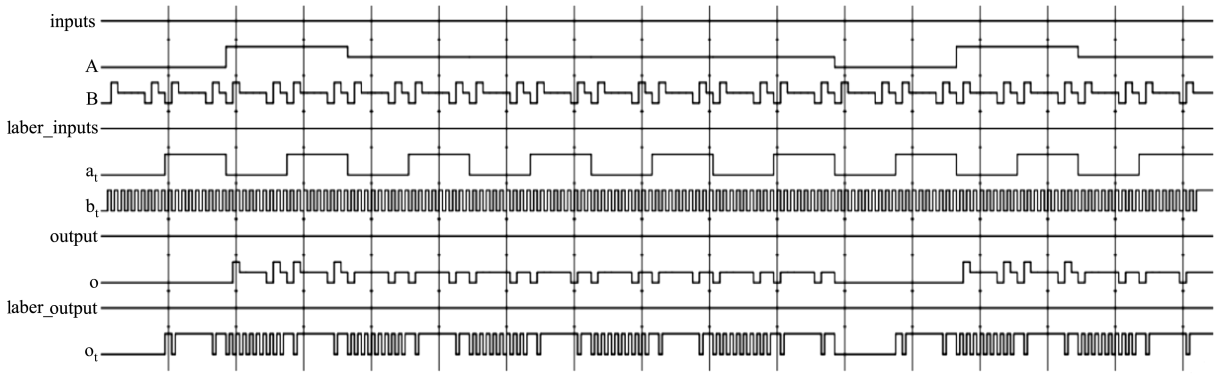


图 4 九值逻辑系统下的 GLIFT 逻辑

4 结 论

布尔逻辑系统下的门级信息流分析方法能够在电路门级层面上有效监控系统中全部的逻辑信息流动,实现对硬件中全部逻辑信息流的精确度量,防止敏感信息泄露。本文分析了多值逻辑系统下的门级信息流标签传播问题,将标签传播规则扩展到多值逻辑系统;采用构造方法生成 GLIFT 逻辑,对比多值逻辑状态下的 GLIFT 逻辑,对部分逻辑输出进行了扩展以便对多值逻辑系统下的 GLIFT 逻辑进行形式化描述;仿真实验表明该分析方法与多值逻辑系统的标签传播规则是一致的。

参考文献:

[1] Andrysco M, Kohlbrenner D, Mowery K, et al. On Subnormal Floating Point and Abnormal Timing[C]//IEEE Symposium on Security and Privacy, 2015: 623-639

[2] Hwang D D, Schaumont P, Tiri K, et al. Securing Embedded Systems[J]. IEEE Security and Privacy, 2006, 4(2): 40-49

[3] Sabelfeld A, Myers A. Language-Based Information-Flow Security[J]. IEEE Journal on Selected Areas in Communications, 2003 21(1): 5-19

[4] Tiwari M, Wassel H W, Mazloom B, et al. Complete Information Flow Tracking from the Gates up[C]//The 14th International Conference on Architectural Support for Programming Languages and Operating Systems, 2009: 109-120

[5] Hu W, Oberg J, Irturk A, et al. Theoretical Fundamentals of Gate Level Information Flow Tracking[J]. IEEE Trans on Computer-Aided Design of Integrated Circuits and Systems, 2011, 30(8):1128-1140

[6] Oberg J, Sherwood T, Kastner R. Eliminating Timing Information Flows in a Mix-Trusted System-on-Chip[J]. IEEE Design & Test, 2013, 30(2):55-62

[7] Zhang D, Wang Y, Suh G E, et al. A Hardware Design Language for Timing-Sensitive Information-Flow Security[J]. ACM SIGARCH Computer Architecture News, 2015, 43(1): 503-516

[8] Ardeshiricham A, Hu W, Marxen J, et al. Register Transfer Level Information Flow Tracking for Provably Secure Hardware Design[C]//Design, Automation & Test in Europe Conference & Exhibition, 2017: 1691-1696

[9] Hu W, Becker A, Ardeshiricham A, et al. Imprecise Security: Quality and Complexity Tradeoffs for Hardware Information Flow Tracking[C]//IEEE/ACM International Conference on Computer-Aided Design, 2016: 1-8

[10] Mao B, Hu W, Althoff A, et al. Quantifying Timing-Based Information Flow in Cryptographic Hardware[C]//IEEE/ACM International Conference on Computer-Aided Design, 2015: 552-559

[11] Mu D, Hu W, Mao B, et al. A Bottom-up Approach to Verifiable Embedded System Information Flow Security[J]. IET Information Security, 2014, 8(1): 12-17

[12] Denning D E. Cryptography and Data Security[M]. Boston, Addison-Wesley Longman Publishing Co Inc, 1982

Gate Level Information Flow Analysis for Formal Method of Multi-Valued Logic System

Tai Yu, Mu Dejun, Hu Wei, Mao Baolei, Guo Lantian

(Shenzhen Research Institute, Northwestern Polytechnical University, Shenzhen 518057, China)

Abstract: The testing and verification coverage is hard to guarantee in the design phase due to the continuous increasing in the scale of integrated circuits. Consequently, the security vulnerabilities residing in hardware designs tend to cause leakage of sensitive information or system failure. As a solution, gate level information flow tracking (GLIFT) can precisely measure and effectively control all the information flows in the underlying hardware to prevent information leakage resulting from these harmful flows of information. However, preliminary research mainly focused on the basic theories of GLIFT and generation algorithms for tracking logic formalization under the Boolean logic system, while digital circuits are typically described using multi-valued logic system during hardware design and verification. This paper proposes to expand the gate level logic information flow analysis method for multi-valued logic system. We derive the label propagation rule set for four-valued and nine-valued logic systems by extending the minimum label propagation set for Boolean logic. In addition, the formal descriptions of GLIFT logic for primitive gates are amended in order to support the features of multi-valued logic in label propagation in computing hardware.

Keywords: gate level information flow analysis; multi-valued logic; label propagation rules; formal description; GLIFT logic