EDA领域中可满足性问题求解方法研究

王秀芹[1] 王 昊[2] 马光胜[3]
(渤海大学信息科学与工程学院 锦州 121013)[1] (黑龙江科技学院电气与信息工程学院 哈尔滨 150027)[2]
(哈尔滨工程大学计算机科学与技术学院 哈尔滨 150001)[3]

摘 要 可满足性问题是理论计算机和人工智能中的著名问题,很多问题都可以通过可满足性求解方法解决。对EDA领域中可满足性问题的求解技术进行了研究。总结了目前主要的求解方法,并对不同的方法进行了详细的分类和比较。讨论了该领域研究中存在的问题,并指出了近期研究热点和未来发展趋势。

关键词 布尔可满足性,电子设计自动化,求解方法
中图法分类号 TP407 **文献标识码** A

Survey on Solving SAT Problems in EDA

WANG Xiu-qin[1] WANG Hao[2] MA Guang-sheng[3]
(College of Information Science and Engineering, Bohai University, Jinzhou 121013, China)[1]
(College of Electrical and Information Engineering, Heilongjiang Institute of Science and Technology, Harbin 150027, China)[2]
(College of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China)[3]

Abstract Boolean satisfiability is a famous problem in theory computer and artificial intelligence, many problems can be solved by the means of solving SAT problems. In this paper, the solving technology for SAT problems in EDA fields was studied. Major solving approaches were summarized, and these different approaches were sorted and compared. Problems existed in this fields were discussed, hot research issues and the development trends in the future were pointed out.

Keywords Boolean satisfiability, EDA, Solving approach

逻辑公式的SAT(Satisfiability,可满足性)问题是计算机科学和人工智能中的著名问题,属于经典的NP完全问题,在最坏情况下,其复杂度呈指数增长。由于可满足性问题的广泛存在,可满足性问题求解方法正受到越来越多的关注。

EDA(Electronic Design Automation)公司和一些大学的研发组织为了解决EDA中的各种问题,广泛研究了可满足性问题的模型和算法,提出了很多成功的求解器,如GRASP[1],SATO[2],Chaff[3],BerkMin[4]等。国内也对SAT问题极其关注,提出了各种新的或改进的SAT求解方法。EDA领域中的许多问题如自动测试向量生成(Automatic Test Pattern Generation,ATPG)、等价验证、模型检查和逻辑综合等问题都可以转化为可满足性问题进行解决。本文针对EDA中主要的SAT问题解决方法进行系统研究。

1 可满足性问题

可满足性问题是指对给定的一个布尔公式φ,确定是否存在一个可满足性赋值A,使得该公式得到满足。如果存在,则这样的一个赋值A称为公式φ的一个解,此时公式φ称为可满足的;否则,称公式φ为不可满足的。

2 SAT问题求解方法

可满足性求解算法有基于随机算法的局部算法和基于DPLL的完备算法。在EDA领域,主要应用基于DPLL的完备算法,它主要由变量决策、布尔推理、冲突分析等几个过程实现。

根据使用的模型和技术的不同,目前EDA领域中的可满足性问题的求解方法可以细分为以下几种。

2.1 基于CNF的SAT求解方法

把EDA中电路功能和约束转化为CNF(Conjunction Normal Form)描述,然后应用基于CNF的通用SAT求解器求解。除了需要对电路描述到CNF公式描述方法的转换进行研究外,更主要的是对SAT算法本身的改进进行研究。

zChaff是由普林斯顿大学SAT研究小组提供的软件包,是Chaff算法的实现[5],是当前研究成果的主要体现。该求解器和其中的基于VSIDS(Variable State Independent Decaying Sum,独立变量状态衰减和)的决策制定、两文字观察、非字典顺序回溯和第一个UIP冲突分析、快速重新开始策略等技术是目前很多研究工作的基础。

国内对SAT算法的改进工作主要有丁敏[6]等结合DPLL算法和失败性文字检查技术,提出了一个可满足性问题求解器。邵明[7]等针对求解SAT的调查传播算法对参数步长敏感的问题,探测了步长对算法有效性和效率的影响规律。罗二海[8]等提出了一种动静态结合变量排序的改进

到稿日期:2008-10-27 返修日期:2009-03-16 本文受国家自然科学基金(60273081),黑龙江省自然科学基金(QC2008C98)资助。
王秀芹(1978-),女,博士,CCF会员,主要研究方向为VLSI计算机辅助设计,E-mail:sd_wxq@sina.com;王 昊(1976-),男,讲师,主要研究方向为数字信号处理和集成电路设计等;马光胜(1944-),男,教授,主要研究方向为EDA理论和算法等。

SAT算法。

2.2 基于电路的SAT求解方法

基于电路的SAT求解器直接作用于电路结构，使用电路专用启发引导搜索过程。

(1) 基于AIGs的SAT求解器

AIGs (And Inverter Graphs，与非图)是一种半正则的数据结构。Kuehlmann A[9,10]用统一AIGs表示问题，把BDD扫描、AIGs结构变换和基于DPLL算法的SAT求解器技术集成在一起。Berkeley大学开发的综合和验证工具ABC工具[11]以AIGs模型为主，集成了组合逻辑综合、顺序逻辑综合、技术映射和重定时功能。

(2) 电路拓扑结构及信号相关信息应用

UCSB(University of California at Santa Barbara)的SoC设计和测试实验室从事电路SAT求解器研究，其中Lu Feng[12-14]等提出了信号相关引导的基于电路的SAT求解器C-SAT。该求解器直接对电路进行处理，通过使用电路拓扑信息和信号相关信息引导赋值决策。采用随机模拟的方法把电路中可能相关(相等或互补)的信号分为一组，在赋值决策过程中对需要确认的同一组信号，同时进行赋值决策，这种方法大大减少了搜索空间，是一个非常有效的SAT求解器。

国内研究对电路结构信息的利用主要有以下工作。卢永江等在原有静态隐含技术的基础上，引入了关联节含及隐含过程加速策略[15]，利用静态隐含技术来提取有用子句作为预处理，加快基于AIGs的电路等价验证过程；在文献[16-18]中通过从电路拓扑结构中提取适当的启发信息，选择合适的割集和量化变量，进行组合电路等价验证。柯宪明[19]等通过对电路的模拟蕴含学习，快速地将许多间接的蕴含关系转化成子句，减少SAT解决器的搜索空间并加速BCP过程。郑飞君[20]等对具有较多输出的复杂电路，使用输出分组技术将共享较多内部节点的输出转化为一个子问题，对每一个子问题，使用将C2SAT和AIGs结构简化、BDD等技术结合的验证算法来解决。

2.3 混合求解方法

(1) 基于CNF和基于电路的结合

将基于CNF的SAT求解器和基于电路的SAT求解器结合，利用二者的优点，形成混合SAT求解器，包含了有效的基于电路的BCP技术和基于CNF求解器中的冲突分析技术[21]。原始电路问题表示成一个简单的门级网表，而学习的冲突子句用CNF表示。BCP引擎由关于门的查找表和对冲突子句的两文字观察方案组成。这种布尔问题的混合表示允许利用基于电路和基于CNF二者的决策启发。

CirCUs是一个基于DPLL的混合SAT求解器，它采用了AIGs，CNF子句和BDD 3种不同的表示，利用各自的优点处理不同的问题。用CirCUs进行BMC时，以AIGs形式展开电路模型，用BDD扫描和初始状态传播进行优化，除去冗余，要检测属性的约束可用AIGs图的一部分或附加的CNF子句表示。

(2) BDD和SAT结合

BDD适合于解决小规模的电路，而SAT适合解决中、大规模的电路。李光辉[22]提出了一种基于电路宽度的启发式策略，根据电路宽度判断电路的复杂性，通过启发式策略实现SAT算法与BDD算法的交替，充分发挥两者的优势。

(3) SAT和模拟技术结合

李光辉提出了一种结合逻辑模拟和布尔可满足性的黑盒验证方法[23]。吴洋把可满足性问题求解技术和传统基于模拟的方法结合，提出了基于布尔可满足性的增量式电路诊断方法[24]，通过对可满足解依据电路结构信息筛选分级，提高了多错误诊断定位的分辨率和准确性。

(4) DPLL和随机局部算法结合

DPLL算法具有完备性，但是求解速度不高，局部搜索算法不完备，但求解速度快。文献[25]提出随机局部搜索算法WALKSAT和DPLL算法的混合求解方法，利用随机算法的快速性改进DPLL算法。文献[26]提出混合求解方法是用局部搜索识别子句的一个子集，把这个子集通过增量式接口传递给DPLL求解器，DPLL求解器对子集进行求解，所获得的解又反馈给局部搜索求解器，帮助其跳出局部最优点。荆明娥[27]等结合DPLL算法完备性和局部搜索算法快速的特点，提出利用近似解加速求解SAT问题的启发式完全算法。首先利用局部搜索算法快速地得到一个近似解，并将该近似解作为完全算法的初始输入，用于其中分支变量的相位决策。

(5) 添加或利用电路结构信息

大多数电路验证任务是从问题的逻辑电路描述开始的，在使用通用的基于CNF的SAT求解器求解问题时，从逻辑电路到CNF的转化过程丢失了一些关于电路结构方面的有用信息。

文献[28]根据电路结构信息，利用可观无关性，把不需要分支的变量标记为“惰性变量”，未加标记的为自由变量，从而用动态或静态的较少搜索空间，提高了可满足性求解工具的性能。刘歆[29]在求解ATPG问题时，在CNF SAT算法中使用结构信息，在CNF公式之上增加一个附加层，维护有关的电路信息(如节点的扇入、扇出信息)和节点变量赋值的确认关系。Velev M N[30-32]在把电路的布尔公式转换到CNF公式的编码时，考虑利用电路中信号的不可观性。文献[33-36]通过模拟和SAT相结合的方法进行可观无关项的计算，从而优化电路。文献[37]在基于CNF的SAT求解器中考虑电路可观无关项Cir-ODCs，在CNF表示中添加Cir-ODCs条件。文献[38]把提取的电路结构信息用于可满足问题的预处理，通过变量代换的方法减少CNF公式中的中间变量，减小可满足问题的规模。文献[39]在基于CNF的SAT求解器基础上，实现了一个新的基于电路的SAT求解器QuteSAT，主要针对电路结构的蕴涵属性，提出新的文字观察策略，用简单的J-frontier算法修剪不相关的决策变量。

2.4 借鉴ATPG算法

SAT引擎与ATPG引擎有很多相同之处，二者的特征比较如表1所列[40-43]。简单来说，ATPG引擎的主要优势是含有电路的结构信息，这些结构信息可以用来引导搜索过程，从而更快地找到解，但是算法复杂度高；而SAT引擎具有先进的蕴涵技术，算法简单，复杂度低，缺点是含有电路的结构信息少。

表1 SAT求解器和ATPG求解器特征比较

特征	SAT	ATPG
冲突分析	是	是
先进的蕴涵	是	否
结构信息	一些	是
VSIDS	是	相似

随机重新开始	是	否
算法复杂度	低	高
电路重新建模	假定	很小
决策排序	在子句中出现次数	概率

ATPG 算法的研究有很多成熟有效的思想和研究成果可供借鉴。在 ATPG 算法中，蕴涵、确认和传播是 3 个基本和重要的操作。ATPG 直接在电路结构上求解可满足性问题，与电路结构关系很紧密，其算法也具有这个特点。

随着集成电路门数目呈指数增加，ATPG 所需要的时间迅速增加，这使得经典算法如 FAN 和 PODEM 到达了它们的极限，使得很多人转向用 SAT 方法解决 ATPG 问题。而 SAT 电路结构信息的利用将大大提高 SAT 求解器的效率。

2.5 字级和位级混合

RTL 电路由数据通路和控制逻辑组成，RTL 的 SAT 问题是一个既有字变量又有位变量，包含电路自身约束和验证性质约束在内的混合 SAT 问题。这些问题已经不能单独由布尔 SAT 求解器解决，而是采用基于 SMT 或基于电路结构搜索的混合求解方法加以解决。文献[44]对 RTL 混合可满足性求解器研究进行了详细论述，将基于电路结构搜索的混合 SAT 求解方法采取的策略分为：1) 字域和位域分别用不同的方法求解；2) 统一用字域方法求解；3)将位域的方法扩展至字位混合域 3 种。

2.6 硬件实现的 SAT 求解方法

由于 SAT 算法的执行时间很大程度上影响着 SAT 应用的范围，于是一些研究人员提出用硬件来加速的方法。硬件 SAT 求解器在算法上分为基于 DPLL 算法和基于 WSAT 算法；在编程模型上分为专有实例和专有应用；在执行模型上分为硬件实现和软硬件实现；重配置模式上分为静态配置、动态配置、部分静态部分动态配置等；使用的硬件有单 FPGA、多 FPGA 等[45]。

文献[46]提出一个基于 FPGA 的 SAT 求解器，以子句估算和冲突分析为基础，通过深度优先搜索和冲突非字典序回溯有效修剪搜索空间，另外利用可重配置 FPGA 的细粒度和并行性执行冲突分析。日本的研究人员提出的 FPGA 求解器是基于 WSAT 算法的，主要针对规模大的可满足性问题[47]。与大部分硬件求解器需要对所有的子句使用相同数目的评估器并行评估不同的是，该文中只对值会发生改变的子句并行评估；在流水线电路中同时执行 4 个独立的求解尝试。后来增加使用了多线程执行和实例数据快速下载的功能[48]。

2.7 并行求解方法

随着集成电路技术、网络技术的发展，多核、多线程 CPUs 应用和网格计算应用越来越多。这些技术为分布式、并行求解器的实现提供了条件。

一些研究人员已经提出了分布式求解器 PSATO[49]，Satz[50]，PaSAT[51]，基于网格的求解器 GridSAT[52]，GrADSAT[53]和 ZetaSAT[54]，基于多处理器的 PICHAFF[55]，多线程求解器 MiraXT[56,57]等并行求解器，用于解决规模大的困难问题。可满足性问题并行化求解是一个有前途的研究方向。

3 存在的问题和未来发展

随着集成电路复杂性增加，对形式化验证、测试、综合技术要求也越来越高。由于可满足性问题复杂性的增加，要求其求解技术不断提高。另外，越来越多的困难问题也需要更快的求解方法来解决。

从目前研究所取得的成果上看，未来研究可以结合以下几个方面：(1)专用化。专用知识对提高求解效率往往有很大帮助，利用电路结构信息或其它如布线、FPGA 布尔映射具体问题的特定信息，实现专用的 SAT 求解器。(2)多种技术合并。随着越来越多新算法的出现，把很多推理方法合并到一个框架中，对实践中碰到的有些 SAT 实例可能是一个有效的方法。在怎样合并不同的推理引擎和怎样使不同的引擎相互协作方面有很多问题需要解决。(3)位级和字级混合。对 RTL 级的字位级混合的求解方面的研究历史还很短，这是目前一个很有前途的研究方向。(4)新技术。利用硬件加速、并行化求解、抽象等新技术，寻求新的解决方法。

结束语 本文对 EDA 领域中的可满足性问题的各种求解方法进行了深入研究，并对已有的各种求解技术进行了分析，为进一步研究指明方向。

参 考 文 献

[1] Marques-Silva J P, Sakallah K A. GRASP: a Search Algorithm for Propositional Satisfiability [J]. IEEE Transactions on Computers, 1999, 48(5): 506-521

[2] Zhang Hantao. SATO: an Efficient Propositional Prover [C]// The 17th International Conference of Automated Deduction. Townsville, 1997: 272-275

[3] Moskewicz M W, Madigan C F, Zhao Ying, et al. Chaff: Engineering an Efficient SAT Solver [C]// Design Automation Conference. Las Vegas, 2001: 530-535

[4] Goldberg E, Novikov Y. BerkMin: a Fast and Robust Sat-solver [C]// Design Automation and Test in Europe. Acropolis, 2002: 142-149

[5] Mahajan Y S, Fu Zhaohui, Malik S. Zchaff2004: An Efficient SAT Solver[C]// Computer Science: Theory and Applications of Satisfiability Testing. Vancouver, 2005: 360-375

[6] 丁敏，唐璞山，周电. 结合高级正向推理过程的可满足性问题解决器[J]. 中国科学 E 辑信息科学，2005，35(4)：426-438

[7] 邵明，李光辉，李晓维. 求解可满足问题的调查传播算法以及步长的影响规律[J]. 计算机学报，2005，28(5)：849-855

[8] 罗二海，荆明娥，唐璞山，等. 动静态结合排序决策的可满足性问题解决器[J]. 计算机辅助设计与图形学学报，2006，18(10)：1472-1477

[9] Kuehlmann A, Ganai M K, Paruthi V. Circuit-based Boolean Reasoning[C]// Proceedings of the Design Automation Conference. Las Vegas, 2001: 232-237

[10] Kuehlmann A, Ganai M K, Krohm F, et al. Robust Boolean Reasoning for Equivalence Checking and Functional Property Verification [J]. IEEE Transactions on Computer-Aided Design, 2002, 21(12): 1377-1394

[11] http://www.eecs.berkeley.edu/~alanmi/abc/

[12] Lu Feng, Wang L-C, Cheng Kwang-Ting, et al. A Circuit SAT Solver with Signal Correlation Guided Learning [C]// Design, Automation and Test in Europe. 2003: 892-897

[13] Lu Feng, Wang L-C, Cheng Kwang-Ting, et al. A Signal Correlation Guided ATPG Solver and its Applications for Solving Difficult Industrial Cases[C]// Proceedings of Design Automation Conference. 2003: 436-441

[14] Lu Feng, Wang L-C, Cheng Kwang-Ting, et al. A Signal Corre-

lation Guided Circuit-SAT Solver [J]. Journal of Universal Computer Science, 2004, 10(12): 1629-1654

[15] 卢永江, 竺红卫, 严晓浪, 等. 利用改善的静态隐含策略加速等价性验证[J]. 电路与系统学报, 2005, 10(3): 47-51

[16] 卢永江. 超大规模集成电路形式验证的方法研究[D]. 杭州: 浙江大学, 2005

[17] 卢永江, 严晓浪, 葛海通, 等. 结合无依赖性割集和量化的等价性验证[J]. 计算机辅助设计与图形学学报, 2005, 17(10): 2215-2219

[18] 杨军, 郑飞君, 卢永江, 等. 结合通用割集和专用割集的组合电路验证方法[J]. 浙江大学学报, 2006, 40(9): 1511-1515

[19] 柯宪明, 唐璞山. 结合模拟蕴含技术的电路验证方法[J]. 微电子学与计算机, 2007, 27(2): 58-62

[20] 郑飞君, 严晓浪, 葛海通. 使用输出分组和电路可满足性的等价性验证算法[J]. 计算机辅助设计与图形学学报, 2005, 17(11): 2484-2488

[21] Ganai M K, Zhang Lin-tao, Ashar P, et al. Combining Strengths of Circuit-based and CNF-based Algorithms for a High Performance SAT Solver [C] // Proceedings of Design Automation Conference. New Orleans, 2002: 747-750

[22] 李光辉, 李晓维. 电路宽度制导的布尔推理[J]. 计算机辅助设计与图形学学报, 2004, 16(11): 1568-1574

[23] 李光辉, 邵明, 李晓维. 验证包含黑盒的电路设计的有效方法[J]. 计算机学报, 2004, 27(6): 803-811

[24] 吴洋, 唐璞山. 基于布尔可满足性的电路设计错误诊断算法[J]. 计算机辅助设计与图形学学报, 2006, 18(9): 1383-1390

[25] Ferris B, Froehlich J. Walksat as an Informed Heuristic to DPLL in SAT Solving[OL]. http://www.cs.washington.edu/homes/bdferris/ papers/ WalkSAT-DPLL.pdf

[26] Fang Lei, Hsiao M S. A New Hybrid Solution to Boost SAT Solver Performance[C] // Design, Automation and Test in Europe. Nice, 2007: 1307-1313

[27] 荆明娥, 周电, 唐璞山, 等. 利用近似解加速求解 SAT 问题的启发式完全算法[J]. 计算机辅助设计与图形学学报, 2007, 19(9): 1184-1189

[28] Gupta A, Gupta A, Yang Zijiang, et al. Dynamic Detection and Removal of Inactive Clauses in SAT with Application in Image Computation[C]//Design Automation Conference. Las Vegas, 2001: 536-541

[29] 刘歆. 数字电路的故障测试模式生成方法研究[D]. 武汉: 华中科技大学, 2004

[30] Velev M N. Encoding Global Unobservability for Efficient Translation to SAT[C] // The Seventh International Conference on Theory and Applications of Satisfiability Testing. Vancover, 2004: 213-216

[31] Velev M N. Efficient Translation of Boolean Formulas to CNF in Formal Verification of Microprocessors [C] // Asia and South Pacific Design Automation Conference. Yokohama, 2004: 609-614

[32] Velev M N. Exploiting Signal Unobservability for Efficient Translation to CNF in Formal Verification of Microprocessors [C] // Design, Automation and Test in Europe. Paris, 2004

[33] Saluja N, Khatri S. A Robust Algorithm for Approximate Compatible Observability Don't care (CODC) Computation[C] // Design Automation Conference. San Diego, 2004: 422-427

[34] Mishchenko A, Brayton R. SAT-based Complete Don't-care Computation for Network Optimization [C] // Design, Automation and Test in Europe. Munich, 2005: 418-413

[35] Safarpour S, Fey G, Veneris A, et al. Utilizing Don't Care States in SAT-based Bounded Sequential Problems [C] // Great Lakes Symposium on. VLSI. Boston, 2005: 264-269

[36] Mishchenko A, Zhang J S, Sinha S, et al. Using Simulation and Satisfiability to Compute Flexibilities in Boolean Networks [J]. IEEE Transactions on CAD of Integrated Circuits and Systems, 2006, 25(5): 743-755

[37] Fu Zhao-hui, Yu Yin-lei, Malik S. Considering Circuit Observability Don't Cares in CNF Satisfiability [C] // Design, Automation and Test in Europe. Munich, 2005: 1108-1113

[38] Ostrowski R, Gr'egoire' Eric, Mazure B. Recovering and Exploiting Structural Knowledge from CNF Formulas[C] // International Conference on Principles and Practice of Constraint Programming. Ithaca, 2002: 185-199

[39] Wu Chi-an, Lin Ting-hao, Lee Chih-Chun, et al. QuteSAT: a Robust Circuit-based SAT Solver for Complex Circuit Structure [C] // Design, Automation and Test in Europe. Munich, 2007: 1313-1318

[40] Drechsler R, Fey G. Automatic Test Pattern Generation[C] // 6th International School on Formal Methods for the Design of Computer, Communication, and Software Systems. Bertinoro, 2006: 30-55

[41] Biere A, Kunz W. SAT and ATPG: Boolean Engines for Formal Hardware Verification[C] // International Conference on Computer- Aided Design. San Jose, 2002: 782-785

[42] Parthasarathy G, Huang Chung-Yang, Cheng Kwang-Ting. An Analysis of ATPG and SAT Algorithms for Formal Verification [C] // Proceedings of High-Level Design Validation and Test Workshop. Monterey, 2001: 177-182

[43] 邓雨春, 杨士元, 王红, 等. 在形式验证和 ATPG 中的布尔可满足性问题[J]. 计算机辅助设计与图形学学报, 2003, 15(10): 1207-1212

[44] 邓澍军, 吴为民, 边计年. RTL 验证中的混合可满足性求解[J]. 计算机辅助设计与图形学学报, 2007, 19(3): 273-278

[45] Skliarova I, de Brito Ferrari A. Reconfigurable Hardware SAT Solvers: A Survey of Systems [J]. IEEE Transactions on computers, 2004, 53(11): 1449-1461

[46] Safar M, Shalan M, El-Kharashi M, et al. A Hardware Accelerator for SAT Solving[C] // International Conference on Computer Engineering and Systems. Croatia, 2006: 132-135

[47] Kanazawa K, Maruyama T. An FPGA Solver for WSAT Algorithms[C] // Proceedings of the 2005 International Conference on Field Programmable Logic and Applications. Tampere, 2005: 83-88

[48] Kanazawa K, Maruyama T. An FPGA Solver for Large SAT Problems[C] // International Conference on Field-Programmable Logic and Applications. Madrid, 2006: 303-308

[49] Zhang Han-tao, Bonacina M P, Hsiang J. PSATO: A Distributed Pro-positional Prover and its Application to Quasigroup Problems [J]. Journal of Symbolic Computation, 1996, 21(4): 543-560

[50] Jurkowiak B, Li Chu-min, Utard G. Parallelizing Satz Using Dynamic Workload Balancing [C] // The 4th International Symposium on Theory and Applications of Satisfiability Testing. Boston, 2001: 205-211

[51] Sinz C, Blochinger W, Küchlin W. PaSAT - Parallel SAT-Checking with Lemma Exchange: Implementation and Applications [C] // The 4th International Symposium on Theory and Applications of Satisfiability Testing. Boston, 2001: 212-217

(下转第 31 页)

$(Q_1, Q_2)^{\frac{r}{x}\cdot\frac{r}{x}}$)的事件，由于 H_2 是随机预言，因此 B 在事件 H 未发生的前提下获胜的概率为 $\Pr[B\ wins\ |\neg H]=1/2$，又 $\Pr[B\ wins]\leqslant\Pr[H]+\frac{1}{2}(1-\Pr[H])=\frac{1}{2}+\frac{1}{2}\Pr[H]$，$\Pr[B\ wins]\geqslant\Pr[B\ wins\ |\neg H]\Pr[\neg H]=\frac{1}{2}(1-\Pr[H])=\frac{1}{2}-\frac{1}{2}\Pr[H]$，因此 $\Pr[H]\geqslant|2\Pr[B\ wins]-1|=Adv(B)\geqslant\varepsilon$。由于 B 对 H_2 最多作了 q_2 次不同询问，因此在事件 H 发生的前提下，A 输出 q_1-BDHI 实例的正确解 $e(P_1,P_2)^{1/x}$ 的概率为 $1/q_2$。

易见，A 获胜的优势 $Adv(A)=Adv(B)\cdot\Pr[H]\geqslant\varepsilon'/q_2$。

综上，若存在针对 BasicCBE 的 Type II IND-CBE-CPA 敌手，则必然存在一个多项式时间算法可以求解 1-BDHI 问题，这与 p-BDHI 假设相矛盾，因此 BasicCBE 是 Type II IND-CBE-CPA 安全的。

对于方案 FullCBE 的安全性，有如下结论。

定理 2 若 H_3 为随机预言，且 BasicCBE 是 IND-CBE-CPA 安全的，则方案 FullCBE 是 IND-CBE-CCA 安全的。

由于方案 FullCBE 是在方案 BasicCBE 的基础之上应用 Fujisaki-Okamoto 变换[11]获得的，文献[10]已证明了 Fujisaki-Okamoto 变换能够将 IND-CBE-CPA 安全的 CBE 方案的安全性增强为 IND-CBE-CCA 安全的，因此定理 2 显然是成立的。

5 性能评价

表 1 给出了该方案与已有 CBE 方案[1-3]的性能对比，其中 p，e，m 和 h 分别表示线对运算、指数运算、乘运算以及 Hash 运算；r 表示加密中所使用的随机数。可以看出，该方案的总体性能，尤其是加密算法，要优于已有的 CBE 方案。

表 1 本文方案与其它方案的性能比较

方案	加密	解密	密文长度
文献[1]	2p+1m+1e+4h	1p+1m+3h	$\|M\|+\|r\|+\|G_1\|$
文献[2]	3m+2e+2h+S+MAC	3p+2m+2h+R+MAC	$\|M\|+3\|G_1\|+\|com\|+\|tag\|$
文献[3]	3m+2e+3h+sig	3p+2m+1h+vfy	$\|M\|+3\|G_1\|+\|vk\|+\|s\|$
本文方案	2m+2e+3h	1p+1m+1e+2h	$\|M\|+\|r\|+\|G_1\|$

结束语 提出了一个高效的基于线对的 CBE 方案，并在随机预言模型中给出了安全性证明。在 p-BDHI 假设下，该方案被证明是 IND-CBE-CCA 安全的。在方案效率上，本文方案仅在解密时计算一个线对，将方案的线对计算的次数降至最少，而已有的其它方案都需要 3 个线对计算，因此本文方案是高效的，其总体性能要优于现有的其它方案。

无线对 CBE 方案的设计目前仍是一个公开问题，因此这方面的研究将是下一步的工作重点。此外，标准模型下安全的高效 CBE 方案的构造也将是另一研究重点。

参 考 文 献

[1] Gentry C. Certificate-based Encryption and the Certificate Revocation Problem. Proceedings[C]// Advances in Cryptology - EUROCRYPT 2003. Warsaw, Poland, 2003

[2] Morillo P, Râfols C. Certificate-based Encryption without Random Oracles[R]. Cryptology ePrint Archive, 2006/12

[3] Galindo D, Morillo P, Râfols C. Improved Certificate-based Encryption in the Standard Model [J]. Journal of System and Software, 2008, 81(7): 1218-1226

[4] Al-Riyami S, Paterson K G. CBE from CL-PKE: A Generic Construction and Efficient Schemes. Proceedings[C]// Public Key Cryptography-PKC 2005. Les Diablerets, Switzerland, 2005

[5] Joux A. A One Round Protocol for Tripartite Diffe-Hellman[C]// Proceedings Fourth International Symposium on Algorithmic Number Theory. Leiden, Netherlands, 2000

[6] Sakai R, Kasahara M. ID Based Cryptosystems with Pairing on Elliptic Curve[R]. Cryptology ePrint Archive, 2003/054

[7] Chen L Q, Cheng Z H. Security Proof of Sakai-Kasahara's Identity-based Encryption Scheme[R]. Cryptology ePrint Archive, 2005/226

[8] Boneh D, Boyen X. Efficient Selective-ID Secure Identity Based Encryption without Random Oracles. Proceedings[C]// Advances in Cryptology - EUROCRYPT 2004. Interlaken, Switzerland, 2004

[9] ElGamal T E. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. Proceedings[C]// Advances in Cryptology -CRYPTO'84. California, USA, 1985

[10] Lu Yang, Li Jiguo, Xiao Junmo. Generic Construction of Certificate-based Encryption. Proceedings[C]// 9th International Conference for Young Computer Scientists. Zhangjajie, China, 2008

[11] Fujisaki E, Okamoto T. How to Enhance the Security of Public Key Encryption at Minimum Cost. Proceedings[C]// Public Key Cryptography - PKC'99. Kamakura, Japan, 1999

[12] Bellare M, Rogaway P. Random Oracles are Practical: A Paradigm for Designing Efficient Protocols. Proceedings[C]// ACM CCS 1993. Virginia, USA, 1993

[13] Barreto P S L M, Kim H Y, Lynn B, et al. Efficient Algorithms for Pairing-based Cryptosystems. Proceedings[C]// Advances in Cryptology - CRYPTO 2002. California, USA, 2002

[14] MIRACL, Multiprecision Integer and Rational Arithmetic C/C++ Library. http://indigo.ie/mscott/

(上接第 20 页)

[52] Chrabakh W, Wolski R. GridSAT: A Chaff-based Distributed SAT Solver for the Grid[C]// Proceedings of the ACM/IEEE Conference on Supercomputing. Phoenix, 2003: 1-13

[53] Chrabakh W, Wolski R. GrADSAT: A Parallel SAT Solver for the Grid[R]. UCSB 2003-05 (pdf). http://www.cs.ucsb.edu/~chrabakh/

[54] Wolfgang B, Wolfgang W, Wolfgang K, et al. ZetaSAT - Boolean Satisfiability solving on Desktop Grids [C]// International Symposium on Cluster Computing and the Grid. Cardiff, 2005: 1079-1086

[55] Tobias S, Bernd B. PICHAFF2 - A Hierarchical Parallel SAT Solver [C]// International Workshop on Microprocessor Test and Verification. Austin, 2004: 56-61

[56] Tobias S, Matthew L, Bernd B. PaMira - a Parallel SAT Solver with Knowledge Sharing[C]// International Workshop on Microprocessor Test and Verification. Austin, 2005: 29-36

[57] Matthew L, Tobias S, Bernd B. Multithreaded SAT Solving[C]// The 12th Asia and South Pacific Design Automation Conference. Yokohama, 2007: 926-931