Proceedings of the 10th International Scientific and Practical Conference «Science, Education, Innovation: Topical Issues and Modern Aspects»

(April 16-18, 2024). Tallinn, Estonia

No 196

INFORMATION AND WEB TECHNOLOGIES

Метод забезпечення безпеки програм згідно оборотної логіки

Савенко Олег Станіславович[1], Кучерук Дмитро Віталійович[2], Ярецька Наталія Олександрівна[3]

[1] д.т.н., професор, декан факультету інформаційних технологій; *Хмельницький національний університет;* Україна

[2] здобувач магістерського ступеня, 2 курс, кафедра комп'ютерної інженерії та інформаційних систем; *Хмельницький національний університет;* Україна

[3] к.ф.-м.н., доцент, доцент кафедри вищої математики та комп'ютерних застосувань; *Хмельницький національний університет;* Україна

Анотація. В роботі розглянуто оборотну логіку в CMOS та запропоновано реалізацію адіабатичної динамічної диференціальної логіки для додатків для більш сильного пом'якшення атак DPA.

Ключові слова: *оборотна логіка, адіабатична динамічна диференціальна логіка, CMOS.*

Вступ. Виробництво економічно ефективних безпечних інтегрованих мікросхем, таких як смарт-карти, вимагає від розробників апаратного забезпечення врахування компромісів у розмірі, безпеці та енергоспоживанні. Для створення успішних проектів, орієнтованих на безпеку, апаратне забезпечення низького рівня повинно містити вбудовані механізми захисту, які доповнюють криптографічні алгоритми, такі як AES і Triple DES, запобігаючи атакам на бокових каналах, таким як диференціальний аналіз потужності (DPA). Динамічна логіка затьмарює вихідні сигнали та роботу схеми, знижуючи ефективність атаки DPA. Тому було запропоновано реалізацію адіабатичної динамічної диференціальної логіки для додатків у безпечному дизайні для більш сильного пом'якшення атак DPA.

Оборотні логічні структури. Принципи квантової механіки керують фізичними обмеженнями обчислювальних схем і систем. Ці системи розсіюють енергію через стирання бітів у своїх взаємопов'язаних примітивних структурах, що є важливим фактором, оскільки щільність транзисторів зростає. Збільшення ентропії в цих середовищах безпосередньо пов'язане з ймовірністю того, що квантова частинка займе будь-який із

INFORMATION AND WEB TECHNOLOGIES

своїх станів. Щоб створити ідеальний універсальний комп'ютер, який розсіює довільно низьку енергію, має бути реалізована обертова логіка, оскільки закони фізики вказують на оборотність у часі.

Оборотні логічні структури є задовільними для проектування та реалізації в обчислювальних структурах та організації, коли ці правила проектування забезпечують оборотність логічної структури [1]. Таким чином, універсальна обчислювальна машина може бути реалізована для того, щоб ідеально моделювати кожну кінцево реалізовану фізичну систему, оскільки кожен електрон у квантовому комп'ютері представлений постійним унітарним оператором у гамільтоновому просторі [2].

Основний принцип оборотного обчислення полягає в тому, що бієктивний пристрій з однаковою кількістю вхідних і вихідних ліній не матиме розсіювання тепла. Електродинаміка системи дозволяє передбачити всі майбутні стани на основі відомих минулих станів, і система досягає кожного можливого стану. Є дві окремі, але однаково важливі парадигми оборотної логіки. По-перше, це логічна оборотність, яка використовує принципи, які керують оборотною логічною структурою, щоб визначити логічні обчислення, необхідні для здійсненних проектів. По-друге, це фізична оборотність, яка передбачає розробку фізичної структури, вхідні значення якої можуть однозначно визначатися виходом кожного обчислювального циклу, і розсіювання енергії якої не перевищує бар'єр Ландауера (kTln(2) джоулів на обчислювальний цикл). Різниця між цими двома парадигмами є важливою, оскільки логічно-обертова структура все ще може перевищувати бар'єр Ландауера. Наприклад, CMOS – це інвертор, розроблений за технологією, що працює при кімнатній температурі, VDD якого становить 1 В і має вихідну ємність 100 пФ, буде розсіювати $5 \cdot 10^{-11}$ Джоулів на перехід стану, що в $1{,}75 \cdot 10^{10}$ разів більше, ніж kTln(2), навіть якщо інвертори логічно оборотні.

Реалізацією оборотної логіки в CMOS, де струм (що протікає через схему) контролюється, щоб мінімізувати розсіювання енергії через перемикання є – адіабатична логіка. Існують значні дослідження щодо проектування та аналізу локально оптимальних адіабатичних елементів для пом'якшення атак бічних каналів. Однак жодна з цих робіт не розглядала використання адіабатичної логіки в реалізації гнучких і програмованих політик апаратної безпеки. Адіабатична логіка також не застосовувалася в додатках апаратної безпеки, таких як надійні системи голосування та стандарти шифрування даних.

INFORMATION AND WEB TECHNOLOGIES

Адіабатичну теорему вперше представили Борн і Фок [3]. Вони описують фізичну систему такою, що залишається у своєму миттєвому власному стані, якщо дане збурення діє на неї досить повільно і якщо існує розрив між власним значенням і рештою спектра гамільтоніана. Тому, уповільнюючи зміну умов системи, система сама адаптується до нової конфігурації, змінюючи щільність ймовірності. Це означає, що якщо система починається у власному стані початкового гамільтоніана, вона закінчиться у відповідному власному стані кінцевого гамільтоніана [4].

В роботі розглянуто питання про те, чи можна маніпулювати схемами перемикання потоку електронів оборотно за допомогою логічних структур CMOS. Представлені результати симуляції прикладу адіабатичної логіки, де бінарна комутаційна мережа розсіює менше kTln(2) джоулів енергії за подію комутації. Також, розглянуто допустимість послідовної логіки в оборотних обчислювальних системах. Я представляють суто математичний доказ того, що послідовні оборотні логічні структури фізично можливі. Розроблено набір обчислювальних логічних примітивів, щоб забезпечити підтримку фізичної оборотності для всіх оборотних логічних структур із шляхами зворотного зв'язку.

Диференціальний аналіз потужності. Використання енергоспоживання для отримання компрометуючої інформації відоме як атака диференціального аналізу потужності (DPA). Зловмисник аналізує інформацію, отриману з деталей практичної реалізації безпечних алгоритмів [5]. Більшість сучасних обчислювальних систем використовують технологію CMOS, і динамічне споживання енергії вентилем CMOS пропорційне його вхідним сигналам. Таким чином, аналіз вихідної потужності дозволяє зловмиснику визначити кореляцію між даними та ключем, оскільки перемикання в вентилях CMOS залежить від цих вхідних даних. Коли зловмиснику відомий відкритий текст і круглий підключ, він може визначити вхідні дані для логічної функції та вивести їх вихід за допомогою таблиці пошуку. Алгоритми відкритого ключа можна аналізувати за допомогою DPA шляхом співвіднесення значень кандидатів для проміжних обчислень із вимірюванням енергоспоживання. Для операцій модульного піднесення до степеня можна перевірити припущення бітів експоненти, перевіривши, чи співвідносяться прогнозовані проміжні значення з фактичним обчисленням.

Ефективність атаки DPA можна продемонструвати за допомогою простого звичайного інвертора. Напруга живлення звичайного інвертора CMOS становить 0,95 В при 1 МГц. Середня потужність звичайного інвертора становить $2{,}0617 \cdot 10^{-8}$ Вт, з

піковим підвищенням $P_{Peak_{rise}}$ =4,5604·10^{-6} Вт, та піковим падінням $P_{Peak_{fall}}$ =1,0325·10^{-5} Вт, викликаючи P_{diff} =5,7644·10^{-6} Вт. Це означає, що пік потужності, коли вхід перемикається з 1 на 0, становить 5,7644·10^{-6} Вт перевищує пікову потужність, коли вхід перемикається з 0→1. Тому зловмисник може правильно визначити логічне розташування схеми.

Основним недоліком усунення DPA-атак на програмному рівні є те, що зміни потужності та струму, які аналізуються зловмисником, відбуваються на апаратному рівні, і жоден програмний алгоритм, яким би ефективним він не був, не може вплинути на роботу затвору CMOS після отримання вхідного сигналу. Наприклад, вставлення випадкових переривань процесу для запобігання послідовній роботі алгоритму [6] можна обійти методами повторної синхронізації та інтеграції [5]. Крім того, бітове маскування [7] можна подолати за допомогою атак DPA.

Запобігання атакам DPA. Таким чином, найефективніший підхід до запобігання атакам DPA полягає в тому, щоб включити логіку на основі безпеки в саму апаратну реалізацію, щоб ускладнити для зловмисника визначення необхідної інформації для визначення вхідних даних. Три найважливіші показники, які слід враховувати при розробці схем CMOS для цієї мети, це споживана потужність, площа та робоча частота, оскільки

$$E_{diss}=C_L \cdot V_{dd}^2 \cdot f,$$

де C_L – ємність навантаження, V_{dd} – напруга живлення, а f – робоча частота.

В роботі також розглядається два алгоритми синтезу для оборотної та адіабатичної логіки: 1) надійну модель поведінки для фундаментального затвору Integrated Qubit (IQ) для проектування локально оборотних логічних структур; 2) метод оптимізації для оборотного логічного синтезу на основі бібліотеки Integrated Qubit (IQ). Причому моделювання затвору IQ, на відміну від затвору Control-V або затвору Тоффолі, дозволяє створити більш надійну модель, яка точніше відображає теоретичну оборотну обчислювальну структуру. А алгоритм на основі бібліотеки IQ працює за O(N) часу та знижує квантову вартість синтезованої схеми до 45%. Алгоритм паралельного адіабатичного синтезу для адіабатичної логіки з двома шлюзами, покращує вартість схеми на 36,85% порівняно з попередніми тестами. Також була застосована техніка прямого зміщення тіла, [8], до звичайного інвертора, щоб

INFORMATION AND WEB TECHNOLOGIES

продемонструвати ефективність зміщення тіла в динамічній диференціальній логіці.

Результати. Було показано, що PMOS- і NMOS-транзистори для регулювання порогової напруги (VTH) контролюють підпорогові витоки й уникають значного розсіювання статичної потужності й оптимізують продуктивність системи. Це пояснюється тим, що порогова напруга є функцією напруги джерела в організмі, яку можна модулювати для підвищення продуктивності за допомогою прямого зміщення. Додатковою перевагою є те, що вплив ефектів короткого каналу зменшується в міру застосування зміщення, що також зменшує коливання порогової напруги.

Крім того, було показано, що зміщення корпусу в транзисторах покращує вразливість схеми CMOS проти атак DPA. Оскільки порогова напруга підтягуючих транзисторів, що використовуються для відновлення заряду, змінюється пороговою напругою, саме відновлення погіршується, збільшуючи різницю між піковим і середнім енергоспоживанням і робить схему більш уразливою до атак аналізу потужності. Реалізуючи корпусне зміщення в транзисторах PMOS, динамічне енергоспоживання було зменшено в середньому на 50%, а також зменшено залежність даних від енергоспоживання.

Висновок. Оборотна логіка є багатообіцяючою парадигмою обчислювального дизайну, яка представляє метод побудови комп'ютерів, які виробляють довільно низьке розсіювання тепла. Основний принцип оборотних обчислень полягає в тому, що біективний пристрій з однаковою кількістю вхідних і вихідних ліній створює обчислювальне середовище, де електродинаміка системи дозволяє передбачати всі майбутні стани на основі відомих минулих станів, і система досягає всіх можливих станів, що призводить до відсутності розсіювання тепла. Оборотна логіка має важливе значення в майбутніх реалізаціях CMOS [149], квантових обчислень, оптичних обчислень і ДНК-обчислень, оскільки ці структури потрібні для подолання бар'єру kTln(2) для розсіювання енергії.

Отже, в дослідженні розглянуто дизайн та проведений аналіз із використанням високоефективної адіабатичної динамічної логіки (PADDL) для пом'якшення атак DPA.

References:

[1] T. Toffoli, "Reversible Computing," Technical Report MIT/LCS/TM-151, 1980.
[2] R. Feynman, "Simulating Physics with Computers," International

INFORMATION AND WEB TECHNOLOGIES

Journal of Theoretical Physics, 1982.
[3] M. Born and V. A. Fock (1928). "Beweis des Adiabatensatzes". Zeitschrift für Physik A 51 (3-4): 165-180.
[4] T. Kato, "On the Adiabatic Theorem of Quantum Mechanics". Journal of the Physical Society of Japan 5 (6): 435-439, 1950.
[5] C. Clavier, J.-S. Coron, and N. Dabbous, "Differential power analysis in the presence of hardware countermeasures," in CHES '00. London, UK, UK: Springer-Verlag, 2000, pp. 252-263.
[6] J. Daemen and V. Rijmen, "Resistance Against Implementation Attacks: A Comparative Study of the AES Proposals", in Proc. of the Second Advanced Encryption Standard (AES) Candidate Conf. March 1999.
[7] S. Chari, C.S. Jutla, J.R. Rao, and P. Rohatgi, "Towards Sound Approaches to Counteract Power-Analysis Attacks", in Proc. of CRYPTO '99, Lecture Notes in Computer Science, vol. 1666, 1999, pp. 398-412.
[8] Tschanz, J.W.; Kao, J.T.; Narendra, S.G.; Nair, R.; Antoniadis, D.A.; Chandrakasan, A.P.; De, V.; "Adaptive body bias for reducing impacts of die-to-die and within-die parameter variations on microprocessor frequency and leakage," Solid-State Circuits, IEEE Journal of , vol.37, no.11, pp. 1396- 1402, Nov 2002.