УДК: 005

ТЕХНОЛОГІЇ ЗЛОМУ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ ЧЕРЕЗ АНАЛІЗ ДИНАМІКИ СПОЖИВАННЯ ПОТУЖНОСТІ ПРИ ЇХ РЕАЛІЗАЦІЇ

Гринь Я.В.
Національний технічний університет України «Київський політехнічний інститут», Україна, Київ

Проаналізовано дві технології злому криптографічних алгоритмів: простий аналіз споживання потужності (SPA -Simple Power Analysis) та диференційний аналіз споживання потужності (DPA - Differentional Power Analysis). Розглянуто ефективні методи протидії.

Ключові слова: простий аналіз споживання потужності (SPA - Simple Power Analysis), диференційний аналіз споживання потужності (DPA - Differentional Power Analysis), сила струму, термінальні компоненти, мікроконтролер, смарт-карти, реконструкція .

Гринь Я.В. Технологии взлома криптографических алгоритмов через анализ динамики потребления мощности при их реализации / Национальный технический университет Украины «Киевский политехнический институт», Украина, Киев.

Проанализированы две технологии взлома криптографических алгоритмов: простой анализ потребления мощности (SPA - Simple Power Analysis) и дифференциальный анализ потребления мощности (DPA - Differentional Power Analysis). Рассмотрены методы противодействия.

Ключевые слова: the simple analysis of consuming of power (SPA - Simple Power Analysis), differential analysis of consuming of power (DPA - Differentional Power Analysis), current intensity, terminal components, the microcontroller, smart cards, reconstruction.

Hryn Y. V. Technologies of cracking of cryptographic algorithms through the analysis of dynamics of consuming of power in case of their implementation / National technical university of Ukraine "Kiev polytechnic institute", Ukraine, Kiev.

Two technologies of cracking of cryptographic algorithms are analyzed: the simple analysis of consuming of power (SPA - Simple Power Analysis) and differential analysis of consuming of power (DPA - Differentional Power Analysis). Counteraction methods are considered.

Keywords: symmetric cryptographic algorithm of data, secret key, reconstruction of key elements, differential analysis, polymorphic implementation, stochasticity, cycle.

Вступ. Значну частину термінальних компонентів комп'ютерних систем і мереж складають портативні обчислювальні пристрої - мікроконтролери та смарт-карти, особливістю яких є те, що в кожний момент часу в них виконується лише один процес, тобто об'єктивно існує зв'язок між даними, що оброблюються і потужністю, яку споживає обчислювальний пристрій.

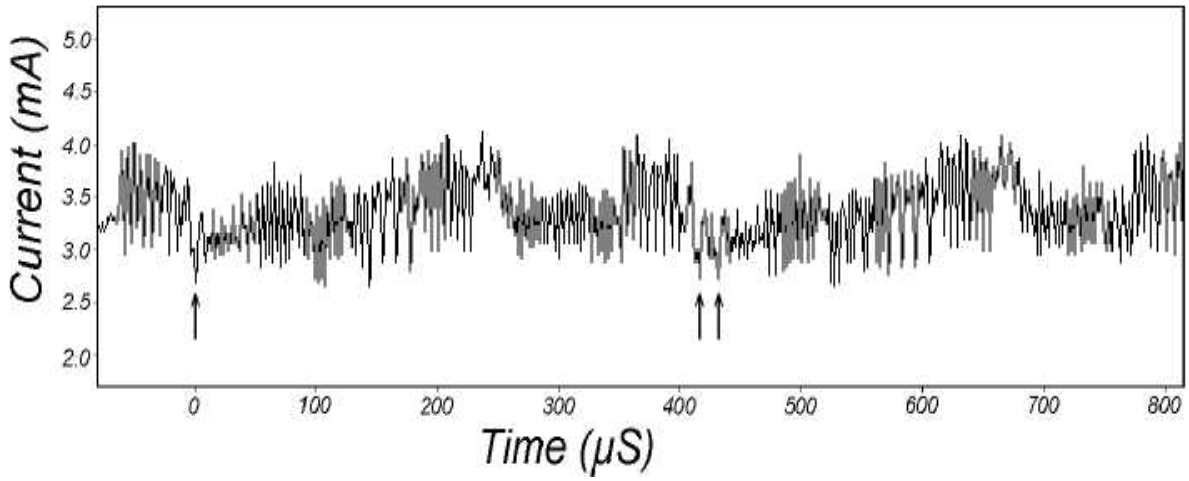
Сила струму, що споживається портативним обчислювальним пристроєм в момент виконання команди, залежить від типу команди і від кодів операндів та результату. Для портативних обчислювальних пристроїв відносно просто виконати вимірювання динаміки споживання потужності під час виконання програми і поставити у відповідність командам, що виконуються.

Мета. Розглянути технології злому криптографічних алгоритмів через динаміку споживання потужності при їх реалізації.

Існує дві технології такої реконструкції: простий аналіз споживання потужності (SPA -Simple Power Analysis) та диференційний аналіз споживання потужності (DPA - Differentional Power Analysis).

Сутність першої полягає у відновленні за осцилограмою споживання потужності послідовності команд, що виконуються програмою. На рис.1 наведено реальну осцилограму споживання потужності мікроконтролером при виконанні 2-го та 3-го циклів алгоритму DES. Стрілками позначені значення потужності, що співвідносяться з командами зсуву лівої та правої частин ключа. Чітко видно, що на 2-му циклі зсув виконується один раз, а 3-му - два рази.

Ефективність SPA в плані реконструкції даних визначається залежністю порядку виконання програми від цих даних. Наприклад, в основі алгоритмів несиметричного шифрування, цифрового підпису та ідентифікації віддалених абонентів лежить операція модулярного експоненціювання: A^E mod M n-розрядних чисел. Процедура обчислення полягає в виконанні n циклів, в кожному з яких реалізується операція піднесення до квадрату і, залежно від поточного біту експоненти - E множення на А. Зафіксувавши номери циклів, на яких виконується операція множення достатньо просто реконструювати двійковий код E, яка в згаданих вище алгоритмах являє собою секретний код.



Технологія DPA полягає у встановлені статичних залежностей між розрядами даних та потужністю, що споживається обчислювальним пристроєм під час виконання кожної з команд. Тобто ця технологія попереднього статистичного дослідження впливу розрядів даних на споживання потужності в кожний момент часу за умови, що програма не змінюється. Сам процес реконструкції даних за допомогою виявлених залежностей також являє собою статистичний аналіз. Відповідно, такий процес може бути ефективним лише за умови незмінності даних. Існує ряд модифікацій і різновидів технології DPA.

Рис.1. Приклад реальної осцилограми споживання потужності мікроконтролером при виконанні 2-го та 3-го циклів алгоритму DES

Активне використання технологій SPA і DPA ініціює розробку апаратних та програмних засобів протидії. Застосування апаратних засобів ускладнює структуру портативних обчислювальних компонент та помітно збільшує їх вартість. Тому на практиці більшого розповсюдження набули програмні засоби протидії SPA та DPA. Основними критеріями ефективності таких засобів є рівень захисту, що забезпечується їх застосуванням та об'єм додаткових обчислювальних ресурсів, потрібних для їх реалізації.

Для протидії DPA - технології, що має за основу статистичний аналіз, найбільш ефективними є методи, що базуються на введенні випадковості.

До цієї групи методів протидії відносяться:

- маскування значень даних, що використовуються при кожному виконанні програми (ключів криптографічних алгоритмів) випадковими кодами, які змінюються при кожному запуску програми. Маскування - найбільш простий метод протидії DPA, що потребує найменших додаткових ресурсів для своєї

реалізації, хоча існує проблема “зняття маски” для одержання коректного результату. В останні роки з’явилась технологія незаконного доступу до даних - диференційний аналіз споживання потужності (DPA) другого порядку, при використанні якої маскування ключів випадковим кодом не забезпечує їх ефективного захисту від реконструкції;

- стохастичний програмний поліморфізм, що застосовується в двох формах: випадкова вставка команд, що не впливають на результат, але ускладнюють прив’язку моменту виміру потужності до конкретної команди програми; випадкова зміна послідовності виконання незалежних по даним команд.

Найбільш ефективним засобом протидії SPA і DPA є друга форма програмного поліморфізму, тобто випадкова зміна при кожному виконанні програми послідовності виконання команд, яка не впливає на результат. Такий поліморфізм дозволяє ефективно протидіяти DPA високих порядків.

Основним недоліком стохастичного поліморфізму, як засобу протидії SPA і DPA, є значний об’єм обчислювальних ресурсів на його реалізацію. Значною мірою цей недолік зумовлений тим, що в опублікованих дослідженнях задача поліморфної реалізації розв’язується в загальному вигляді, без урахування особливостей конкретного алгоритму. При такій постановці поліморфна реалізація постає доволі складною задачею, розв’язання якої пов’язано з аналізом графу залежності операцій по даним. В ряді публікацій такий аналіз пропонується виконувати динамічно. При такому підході застосування поліморфізму, як засобу протидії незаконній реконструкції ключів криптографічних алгоритмів аналізом споживання потужності, обмежене значним об’ємом потрібних для цього обчислювальних ресурсів, суттєво більшим в порівнянні з іншими методами.

Разом з тим, слід враховувати, що кількість криптографічних алгоритмів, що використовуються в протоколах інформаційного обміну з термінальними компонентами комп’ютерних систем і мереж відносно невелика. Тому обґрунтованою представляється розробка методу ефективної поліморфної реалізації для кожного алгоритму в рамках загальних принципів. Такий підхід дозволяє повною мірою враховувати структуру алгоритму, особливості його обчислювальних процедур, надає можливість проводити цілеспрямовані еквівалентні його перетворення і отримати в результаті ефективну реалізацію програмного поліморфізму, сумірну за витратами обчислювальних ресурсів з іншими методами.

Висновок. Отже, характерна особливість обчислювальних процедур алгоритмів симетричного шифрування полягає в тому, що послідовність операцій не залежить від коду ключа. Це означає, що найбільшу потенційну загрозу з точки зору можливості реконструкції коду ключа становлять технології диференційного аналізу споживання потужності.

Всього існує дві технології такої реконструкції: простий аналіз споживання потужності (SPA -Simple Power Analysis) та диференційний аналіз споживання потужності (DPA - Differentional Power Analysis) і це дозволяє нам зробити наступні висновки:

1) ефективність SPA в плані реконструкції даних визначається залежністю порядку виконання програми від цих даних;
2) технологія DPA полягає у встановлені статичних залежностей між розрядами даних та потужністю, що споживається обчислювальним пристроєм під час виконання кожної з команд. Тобто ця технологія попереднього статистичного дослідження впливу розрядів даних на споживання потужності в кожний момент часу за умови, що програма не змінюється;
3) активне використання технологій SPA і DPA ініціює розробку апаратних та програмних засобів протидії. Застосування апаратних засобів ускладнює структуру портативних обчислювальних компонент та помітно збільшує їх вартість.

Література:

1. Зензинов О. С., Іванов М. А., Стандарт криптографічного захисту XXI століття - AES. Кінцеві поля. М.: КУДИЦ-ОБРАЗ.- 2002 - 174 с.

2. Іванов М.А. Криптографічні методи захисту інформації в комп'ютерних системах і мережах.-М.: Кудіц-Образ, 2001.-368 с.

3. Іванов М.А., Чугунков І.В. Теорія, застосування і оцінка якості генераторів псевдовипадкових послідовностей. М.: КУДИЦ-ОБРАЗ.- 2003 - 260 с.

4. Молдовян А.А., Молдовян Н.А. Введення в асиметричні алгоритми шифрування. С-Пб .: БХВ-Петербург, - 2004.-322 с.

5. Akkar M.L., Bevan R., Goubin L. Two Power Attacks against One-Mask Methods. // 11th International Workshop, Fast Software Encryption (FSE-2004), LNCS-3017. Delhi, India,-2004.- R.332-34.

References:

1. Zenzynov O. S., Ivanov M. A., Standart kryptohrafichnoho zakhystu XXI stolittia - AES. Kintsevi polia. M.: KUDYTs-OBRAZ.- 2002 - 174 s..

2. Ivanov M.A. Kryptohrafichni metody zakhystu informatsii v kompiuternykh systemakh i merezhakh.-M.: Kudits-Obraz, 2001.-368 s..

3. Ivanov M.A., Chuhunkov I.V. Teoriia, zastosuvannia i otsinka yakosti heneratoriv psevdovypadkovykh poslidovnostei. M .: KUDYTs-OBRAZ.- 2003 - 260s..
4. Moldovian A.A., Moldovian N.A. Vvedennia v asymetrychni alhorytmy shyfruvannia. S-Pb .: BKhV-Peterburh, - 2004.-322s..
5. Akkar M.L., Bevan R., Goubin L. Two Power Attacks against One-Mask Methods. // 11th International Workshop, Fast Software Encryption (FSE-2004), LNCS-3017. Delhi, India,-2004.- R.332-34.