УДК 004.056 : 004.424.47

В. А. Лужецький, д-р. техн. наук, проф.;
Ю. В. Баришев, асп.

КРИПТОГРАФІЧНІ ПРИМІТИВИ ДЛЯ РЕАЛІЗАЦІЇ КЕРОВАНОГО ХЕШУВАННЯ

За результатами аналізу відомих конструкцій хешування визначено концепцію керованого хешування. Визначено вимоги до криптографічних примітивів та визначено відповідні їм примітиви для реалізації цієї концепції. Запропоновано приклад моделі множини функцій ущільнення для синтезу за допомогою криптографічних примітивів. Визначено перспективи подальшого дослідження.

Вступ

Сьогодні алгоритми хешування можуть досліджуватись як криптоаналітиками, так і зловмисниками. Останнє дозволяє реалізувати попередню підготовку до атак [1, 2]. Очевидно, що закриття послідовностей операцій, які виконуються під час криптографічних перетворень, могло б стати виходом із ситуації для криптологів, однак це звузить прикладне застосування хешування в електронній комерції. Роботи [1, 3] стали першими спробами приховування від зловмисника шляху ітеративних перетворень за допомогою введення додаткових операндів до конструкції хешування. Однак, введення додаткового операнда [1] не спричинило зміни самих перетворень, які залишаються об'єктом дослідження для зловмисників. Було здійснено спробу побудови «динамічного» хешування, тобто хешування, що залежить від вхідних даних, однак ця спроба виявилася невдалою [4], оскільки вхідні дані відомі криптоаналітикам.

Робота [3], на думку авторів, є найбільш вдалою в цьому напрямі, однак вона орієнтована на симетричне шифрування і криптографічні примітиви, що у ній пропонуються, першочергово зорієнтовані на шифрування. Саме тому хешування, що запропоноване в [3], реалізується на основі шифрів, а отже не враховує специфіки задачі хешування і не може вважатися розв'язком, що наближається до оптимального за критерієм швидкості обробки даних. Відповідно актуальною є розробка керованого хешування «з нуля».

Метою дослідження є підвищення швидкості хешування за рахунок розробки концепції керованого хешування та криптографічних примітивів, які будуть використовуватись для її реалізації.

Для досягнення мети дослідження необхідно розв'язати такі задачі:

– аналіз відомих конструкцій хешування та розробка концепції керованого хешування і конструкцій для її реалізації;

– визначення вимог до криптографічних примітивів, які будуть використовуватись для реалізації керованого хешування;

– аналіз відомих та синтез нових операцій, що можуть бути використані для досягнення мети дослідження.

Концепція керованого хешування

Більшість відомих підходів до побудови хешування «з нуля» базуються на конструкції, тобто математичній моделі, Меркля-Дамгаарда, яка описується формулою [1]

$$h_i = f\left(h_{i-1}, m_i\right), \tag{1}$$

де h_i — проміжне хеш-значення, отримане після обробки *i*-го блока даних m_i; $f\left(\cdot\right)$ — деяка функція ущільнення, що реалізує такі відображення

$$\left\{0;\ 1\right\}^n \times \left\{0;\ 1\right\}^k \to \left\{0;\ 1\right\}^n, \tag{2}$$

де $n,\ k$ — бітова довжина проміжного хеш-значення та блока даних, відповідно.

Ітеративність перетворень, що реалізуються конструкцією (1), стала основною причиною появи

атак з передобчисленнями [1]. Саме тому в роботі [1] пропонувалась нова конструкція, що описується формулою

$$h_i = f\left(h_{i-1}, m_i, c, b\right), \tag{3}$$

де c — деякий параметр хешування, що визначається безпосередньо перед початком процесу; b — кількість вже захешованих бітів даних.

Параметр c повинен виконувати роль «запобіжника» для атак з передобчисленням, оскільки впливає на хід усіх обчислень, а лічильник кількості захешованих біт, що входить до конструкції, — протидіяти перестановці блоків повідомлення [1]. Отже, функція ущільнення, що входить до складу конструкції (3), передбачає реалізацію такого відображення:

$$\{0;\ 1\}^n \times \{0;\ 1\}^k \times \{0;\ 1\}^s \times \{0;\ 1\}^p \to \{0;\ 1\}^n, \tag{4}$$

де $s,\ p$ — бітові довжини параметрів c та b, відповідно.

Відображення (2) та (4) реалізують стале перетворення, тобто кожний блок даних зазнає однакових перетворень у разі його обробки під час ітерацій. У роботах [3, 4] розглядаються варіанти хешування, в яких параметри ітеративних перетворень залежать від певної змінної, в роботі [4] — від блока даних, в роботі [3] — від вектора керування. Оскільки ці підходи відрізняються від підходів, закладених в основу конструкцій (1) та (3), тому пропонується позначати залежність параметрів перетворень від змінної верхнім індексом. Відповідно хешування, в якому параметри залежать від блока даних, позначається таким чином:

$$h_i = f^{m_i}\left(h_{i-1}, m_i\right). \tag{5}$$

Залежність параметрів перетворень від блока даних позначимо у відображенні так:

$$\{0;\ 1\}^n \times \{0;\ 1\}^k \xrightarrow{\{0;\ 1\}^k} \{0;\ 1\}^n. \tag{6}$$

Підхід до хешування, що використовує вектор керування, можна формалізувати у вигляді конструкції

$$h_i = f^{v_i}\left(h_{i-1}, m_i\right), \tag{7}$$

де v_i — вектор керування, який визначає параметри перетворення на i-й ітерації та має довжину w бітів.

Функція ущільнення, що входить до складу конструкції (7), реалізує таке відображення:

$$\{0;\ 1\}^n \times \{0;\ 1\}^k \xrightarrow{\{0;\ 1\}^w} \{0;\ 1\}^n. \tag{8}$$

Очевидно, що можна змінити конструкцію (7) аналогічно тому, як автори [1] змінили конструкцію (1) конструкцією (3) або внести інші зміни, однак все одно нова конструкція відображатиме кероване хешування.

Означення. Хешування, що описується виразом

$$DH = \left\langle M,\ H,\ V,\ \left\{f^v(\cdot)\right\}\right\rangle, \tag{9}$$

де M — множина всіх можливих вхідних блоків даних $\{0;1\}^n$; H — можливі значення всіх проміжних і вихідних хеш-значень $\{0;1\}^k$; V — множина всіх векторів керування $\{0;1\}^w$; $f^v(\cdot)$ — функція ущільнення з параметрами перетворення, що задаються вектором керування $v \in V$, називається *керованим хешуванням*.

Для конкретних реалізацій керованого хешування опис (9) може бути доповнений іншими множинами, наприклад, множиною псевдовипадкових чисел C, що домішуються на кожній ітерації, множиною станів лічильника вже захешованих даних B тощо.

Отже, концепція керованого хешування полягає в тому, що функція ущільнення, яка входить до конструкції, включає перетворення, параметри яких залежать від вектора керування.

Визначення вимог до криптографічних примітивів

Хешування широко використовується для автентифікації, яка, в більшості випадків, виконується в умовах реального часу. Тому для того, щоб відповідати сучасним вимогам прикладного застосування хешування, криптографічні примітиви, які використовуються в процесі хешування, повинні швидко виконуватись на сучасному апаратному забезпеченні, тобто бути природними для універсальних мікропроцесорів.

Результати перетворень, що здійснюються за допомогою криптографічних примітивів, повинні мати рівномірний закон розподілу та бути «збалансованими» [3]. Під збалансованістю розуміється рівна кількість одиниць та нулів у бінарному представленні елементів множини значень.

Необхідно висунути ще одну вимогу, притаманну лише керованому хешуванню — вимогу рівномірності розподілу значень векторів керування та рівномірності їх вибору. Часто будують атаки, використовуючи властивість деяких операцій з втратою бітів, тобто значення певних вхідних бітів не впливають на результат виконання операції. У таких випадках для зловмисників спрощується задача пошуку колізій та праобразів [4], тому всі біти вхідних даних криптографічних примітивів повинні впливати на результат перетворення.

Отже, криптографічні примітиви, що будуть використовуватись для побудови функцій ущільнення, повинні задовольняти такі вимоги:

– бути природними для універсальних мікропроцесорів, а тому швидко виконуватися на них;

– забезпечувати рівномірність та збалансованість результату перетворення;

– забезпечувати вплив усіх вхідних біт на вихідне значення.

Крім цих вимог окремо визначається вимога до формування векторів керування — кожний вектор v_i повинен обиратися з множини V з рівною ймовірністю. З урахуванням сформульованих вимог до криптографічних примітивів проаналізуємо базові операції мікропроцесорів для визначення тих з них, які можуть бути використані як криптографічні примітиви в цьому дослідженні.

Аналіз криптографічних примітивів

Виходячи з вимоги до хешування, яка зумовлена його прикладним застосуванням, як криптографічні примітиви бажано брати операції, які є природними для універсальних процесорів, тобто виконуються за один такт. До таких операцій належать: додавання за модулем 2^n (+); виключне або ($\oplus$); інвертування (~); логічне множення ($\wedge$); логічне додавання ($\vee$); циклічний зсув на u біт праворуч (>>> u); простий зсув на u бітів праворуч/ліворуч (>> u / << u).

Операції +, $\oplus$, а також ~ не забезпечують високого ступеня нелінійності перетворень, тому під час синтезу функції ущільнення $\left\{f^v(\cdot)\right\}$ ці операції необхідно комбінувати з нелінійними. Операції $\wedge$, $\vee$, >>> u, >> u (<< u) є нелінійними, а тому задовольняють вимогу стосовно нелінійності перетворень.

Операції +, $\oplus$, ~ та >>> u забезпечують збалансованість та рівномірність результатів. Операції $\wedge$ та $\vee$ не задовольняють цю вимогу, однак вони можуть використовуватись як криптографічні примітиви за умови однакової частоти виконання цих операцій під час хешування. Простий зсув не забезпечує цю властивість, оскільки «пусті» місця, отримані внаслідок зсуву коду, заповнюються нулями. Останній недолік може бути усунений, якщо ввести різновид зсуву, який забезпечить запис одиниць на місця, які звільняються. Такий зсув нескладно реалізувати як програмно, так і апаратно.

Вимогу забезпечення впливу всіх вхідних біт на вихідний результат забезпечують всі операції, які розглядаються, окрім >> u (<< u).

Отже, із визначених вище криптографічних примітивів для синтезу функцій ущільнення можуть бути використані +, $\oplus$, ~, $\wedge$, $\vee$ та >>> u. Використовуючи набір цих примітивів, пропонується виконувати керування параметрами унарних операцій. Наприклад, нехай синтезовано функцію ущільнення такого вигляду:

$$h_i = h_{i-1} + m_i \ggg u_i \oplus (\sim)c \wedge (\sim)b_i. \qquad (10)$$

Як параметри перетворення, що визначаються вектором керування v_i, пропонується використовувати кількість бітів u_i, на яку зсувається блок даних m_i, а також виконання або не виконання операції інвертування над двома останніми операндами. Реалізацію концепції керованого хешу-

вання можна вважати повною у випадку, коли вектором керування задаватимуться 2^{ω} параметрів перетворення, що, на думку авторів, може бути реалізовано у разі багатоканального хешування.

Висновки

Існує низка атак на процес ітеративного хешування за хеш-значеннями. З метою протистояння цим атакам пропонується концепція керованого хешування. Для досягнення високої швидкості хешування пропонується набір криптографічних примітивів: $+$, $\oplus$, $\sim$, $\wedge$, $\vee$ та $>>>$ *и*. Однією з основних вимог до криптографічних примітивів є забезпечення високої нелінійності перетворень. Автори вважають, що можна забезпечити цю вимогу в цілому для процесу хешування, використовуючи примітиви з відносно невисокою нелінійністю перетворень за рахунок керованості цього процесу. Доведення цієї думки неможливе без синтезованого алгоритму хешування, для якого, в свою чергу, необхідно спочатку виконати попередній відбір криптографічних примітивів. Тому результати таких досліджень будуть наведені у подальших публікаціях.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. E. Biham. A Framework for Iterative Hash Functions: HAIFA [Електронний ресурс] / E. Biham, O. Dunkelman // COSIC internal report, 2007. — 20 с. — Режим доступу до ресурсу : https://www.cosic.esat.kuleuven.be/publications/article-934.pdf.

2. B. Preneel. Analysis and Design of Cryptographic Hash Functions. PhD thesis [Електронний ресурс] / Bart Preneel. — Katholieke Universiteit Leuven, 1993. — 338 с. — Режим доступу до ресурсу : http://homes.esat.kuleuven.be/~preneel/phd_preneel_feb1993.pdf.

3. Молдовян Н. А. Криптография: от примитовов к синтезу алгоритмов / Н. А. Молдовян, А. А. Молдовян, М. А. Еремеев. — СПб. : БХВ-Петербург, 2004. — 448 с.

4. J-P. Aumasson. Cryptanalysis of Dynamic SHA(2) [Електронний ресурс] / J-P. Aumasson, O. Dunkelman, S. Indesteege and B. Preneel // COSIC publications, 2009. — 18 с. — Режим доступу до ресурсу : https://www.cosic.esat.kuleuven.be/publications/article-1277.pdf.

Рекомендована кафедрою захисту інформації

Стаття надійшла до редакції 9.07.10
Рекомендована до друку 11.01.11

Лужецький Володимир Андрійович — завідувач кафедри, ***Баришев Юрій Володимирович*** — аспірант.
Кафедра захисту інформації, Вінницький національний технічний університет, Вінниця