Харківський національний економічний університет
Університет ЛІОН 2 ім. Люм'єра
Віденський університет прикладних технічних наук
Представництво «Microsoft Україна»
Асоціація «Інформаційні технологій України»
Співтовариство ІТ-директорів України
АО «СПАЭРО плюс»

ПЕРША МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

«ПРОБЛЕМИ Й ПЕРСПЕКТИВИ РОЗВИТКУ ІТ-ІНДУСТРІЇ»

м. Харків, 18–19 листопада 2009 р.

Матеріали конференції

Харків
2009

УДК 004

Проблеми й перспективи розвитку IT-індустрії: *матеріали 1-ї Міжнародної науково-практичної конференції [«Проблеми й перспективи розвитку IT-індустрії»], (Харків, 18 – 19 листоп. 2009 р.) / редкол.: В.С. Пономаренко (відп. ред.)* – Харків: ХНЕУ, 2009. – 360 с.

Опубліковані матеріали, що охоплюють широке коло проблем, пов'язаних з інформаційними системами та технологіями. Представлені результати теоретичних та експериментальних досліджень в області моделювання бізнес-процесів, геоінформаційних технологій, захисту інформації, технологій мультимедійних видань, дистанційній освіті.

Матеріали публікуються в авторській редакції.

Проблемы и перспективы развития IT-индустрии: *материалы 1-й Международной научно-практической конференции [«Проблемы и перспективы развития IT-индустрии»], (Харьков, 18-19 ноября 2009 г.) / редкол.: В.С. Пономаренко (отв. ред.)* – Харьков: ХНЭУ, 2009. – 360 с.

Опубликованы материалы, охватывающие широкий круг проблем, связанных с информационными системами и технологиями. Представлены результаты теоретических и практических исследований в области моделирования бизнес-процессов, геоинформационных технологий, защиты информации, технологий мультимедийных изданий, дистанционного образования.

Материалы публикуются в авторской редакции.

Problems and prospects of the development of IT industry: materials of 1-st International scientifically-practical conference [«Problems and prospects of development of IT-industry»], (Kharkov, November, 18-19th, 2009) / Khark. Nation. Econ. Univ.; editor: V.S. Ponomarenko [etc.]. – Kh.: Publish house SevNTU, 2009. – 360 p.

The materials, covered the wide content of problems, which are gathered with information technologies are published in this article. The results of theoretical and practical discoveries in the analysis and synthesys of managered and information systems, systems of support of given decisions are represented here.

The matherials are published in the author's redaction.

Друкується за рішенням вченої ради ХНЕУ,
протокол №2 від 26.10.2009 р.

УДК 003.26

В.А. Лужецький, д.т.н., професор
зав. каф. захисту інформації,
Вінницький національний технічний університет
м. Вінниця, Україна
Ю.В. Баришев, аспірант
Вінницький національний технічний університет
м. Вінниця, Україна
yuriy.baryshev@gmail.com

УЗАГАЛЬНЕНА МОДЕЛЬ СТІЙКОГО ПАРАЛЕЛЬНОГО ХЕШУВАННЯ

Одна з вимог, що найбільш часто висувається до процесу обчислення хеш-значення, є його швидкість. Очевидно, що при цьому основна вимога до хешування, стійкість, повинна залишатись сталою. В процесі криптоаналізу хешування була розроблена атака, що базується на "парадоксі дня народження". Відповідно до цього парадоксу знаходження колізій для n-розрядного хеш-значення можливо здійснити за $2^{n/2}$ ітерацій. Для того, щоб досягти бажаної стійкості до цієї атаки, необхідно збільшити розрядність вихідного хеш-значення вдвічі. Остання процедура є незручною з точки зору швидкісних характеристик хешування, тому в [1] було запропоноване "каскадування", тобто розпаралелення процесу обчислень хеш-значень та конкатенація результатів на останній ітерації. Такий підхід зняв питання стосовно швидкості хешування до 2004 року, коли Жукс винайшов атаку з використанням мультиколізій [2]. Відповідно актуальною задачею є знаходження конструкції, тобто математичної моделі, хешування, яка б дозволила паралельно обчислювати хеш-значення за допомогою різних процесорів та отримувати результуюче хеш-значення шляхом їх конкатенації.

Розглянемо хешування теоретично доведеної стійкості, що використовує операцію піднесення до степеня за модулем великого простого числа, прикладом чого може бути хешування, реалізоване в [3]. Очевидно, що операція піднесення до степеня великої розрядності вимагає достатньо багато часу для виконання обчислень. При передачі даних в режимі реального часу таке хешування може бути неприйнятним через великі часові витрати на його виконання при сучасній апаратурі. В той же час, піднесення до степеня числа з суттєво меншою розрядністю буде виконуватись швидко, але в зв'язку з невеликою розрядністю воно буде зламано порівняно легко. Розпаралелення обчислень, подібне до каскадування могло б забезпечити підвищену швидкість хешування, оскільки обчислення б виконувались над операндами меншої розрядності, а тому б це виконувалося б швидше. Проте для цього воно повинно запобігати атакам, подібним до атаки

Жукса. Тому пропонується замість одного каналу хешування великої розрядності використовувати декілька каналів хешування, в кожному з яких буде виконуватись піднесення числа малої розрядності до степеня за модулем простого числа, що буде меншим, ніж у випадку з одним каналом. Особливістю такого впровадження стане те, що результат і-го раунду, обчислений за допомогою кожного каналу, впливатиме на результат обчислення в усіх каналах, що може бути узагальнене у вигляді такої моделі хешування для q каналів:

$$\begin{cases} h_i^{(1)} = f^{(1)}\left(h_{i-1}^{(1)}, h_{i-1}^{(2)}, \ldots, h_{i-1}^{(q)}, m_i, c_i^{(1)}\right) \\ h_i^{(2)} = f^{(2)}\left(h_{i-1}^{(1)}, h_{i-1}^{(2)}, \ldots, h_{i-1}^{(q)}, m_i, c_i^{(2)}\right) \\ \ldots \\ h_i^{(q)} = f^{(q)}\left(h_{i-1}^{(1)}, h_{i-1}^{(2)}, \ldots, h_{i-1}^{(q)}, m_i, c_i^{(q)}\right), \end{cases} \quad (1)$$

де $f^{(1)}(\cdot), f^{(2)}(\cdot), \ldots, f^{(q)}(\cdot)$ – функції ущільнення, які мають сталу довжину вихідного значення та обчислюються приблизно за однаковий час;

m_i – і-й блок інформаційних даних, що хешуються;

$c_i^{(1)}, c_i^{(2)}, \ldots, c_i^{(q)}$ – псевдовипадкові числа, що використовуються з метою протидії атакам з попередньою підготовкою криптоаналітика.

Атака Жукса є неможливою для конструкції (1), оскільки, знайшовши колізію в одному з каналів обчислення на певній ітерації, зловмисник не може використати її на наступній ітерації для цього ж каналу, щоб побудувати мультиколізії, не перевіривши чи викличе це ж повідомлення колізію в інших $q-1$ каналах з урахуванням їх взаємного впливу.

Список літератури: 1. B. Preneel. Analysis and Design of Cryptographic Hash Functions. PhD thesis, Katholieke Universiteit Leuven, 1993 // Режим доступу до ресурсу – http://homes.esat.kuleuven.be/~preneel/phd_preneel_feb1993.pdf. 2. A. Joux. Multicollisions in Iterated Hash Functions. Application to Cascaded Constructions. In M. K. Franklin, editor, CRYPTO'04, volume 3152 of Lecture Notes in Computer Science, pages 306-316. Springer, 2004. 3. Патент України на корисну модель № 18693 МПК G 09 C 1/00. Спосіб ключового хешування теоретично доведеної стійкості / Стасєв Ю.В., Кузнецов О.О., Євсеєв С.П., Чевардін В.Є., Малахов С.В., Гришко А.В.; заявник та патентовласник Харківський університет повітряних сил. – №u200605734 ; заявл. 25.05.06 ; опубл. 15.11.06, Бюл. №11.