УДК 004.056.55

Чуднівець Д. Р.
Кирилащук Т. Г.

КОЛІЗІЇ ДЛЯ ХЕШ-ФУНКЦІЙ

Вінницький національний технічний університет

Анотація

У тезах розглядається проблема криптографічної стійкості та наводяться практичні колізії для популярних хеш-функцій, таких як MD4, MD5, HAVAL-128 та RIPEMD. Досліджуються вразливості цих алгоритмів, що дозволяють генерувати різні повідомлення, які дають однакове значення хешу при оригінальних векторах ініціалізації. Запропонований підхід демонструє надзвичайно високу ефективність атак: колізії для повної версії HAVAL-128 знаходяться всього за 64 обчислення , для MD4 - за допомогою ручних розрахунків , а для MD5 генерація колізій займає близько години на комп'ютері IBM P690. Крім того, практично доведено, що повна версія алгоритму RIPEMD також не є стійкою до колізій.

Ключові слова*: криптографічні файлові системи, GPU, шифрування даних, режим CTR, спекулятивне шифрування, продуктивність системи.*

Abstract

The theses consider the problem of cryptographic security and present practical collisions for popular hash functions, such as MD4, MD5, HAVAL-128, and RIPEMD. The vulnerabilities of these algorithms are investigated, which allow generating different messages that produce the same hash value with the original initialization vectors. The proposed approach demonstrates extremely high attack efficiency: collisions for the full version of HAVAL-128 are found in just 64 computations, for MD4 - using hand calculations, and for MD5, collision generation takes about an hour on an IBM P690 computer. Furthermore, it is practically proven that the full version of the RIPEMD algorithm is also not collision-free.

Keywords*: collisions, hash functions, MD4, MD5, HAVAL-128, RIPEMD, cryptanalysis, information security.*

Вступ

Сучасні системи захисту інформації значною мірою покладаються на використання криптографічних хеш-функцій, тому їхня надійність є критично важливим аспектом для забезпечення цілісності даних та електронного цифрового підпису. Однією з головних вимог до таких алгоритмів є стійкість до колізій, що має гарантувати практичну неможливість створення двох різних повідомлень із однаковим значенням хешу. Проте розвиток методів криптоаналізу демонструє, що низка широко відомих алгоритмів хешування, таких як MD4, MD5, HAVAL-128 та RIPEMD, містять вразливості. Це зумовлює необхідність детального дослідження методів знаходження колізій для оцінки реальної криптографічної стійкості цих стандартів та запобігання загрозам інформаційній безпеці.

Результати дослідження

У сучасному інформаційному суспільстві забезпечення цілісності даних значною мірою спирається на використання криптографічних хеш-функцій, проте результати дослідження переконливо демонструють, що низка поширених алгоритмів є вразливою до генерації колізій. Зокрема, алгоритм MD5, розроблений як посилена версія MD4 , раніше піддавався криптоаналізу, який дозволяв знаходити лише псевдоколізії або колізії для специфічно обраних векторів ініціалізації. Натомість запропонований метод вперше дозволяє знаходити реальні колізії, що складаються з двох різних повідомлень довжиною 1024 біти зі стандартним вектором ініціалізації. Процес знаходження таких колізій є надзвичайно ефективним: на комп'ютері IBM P690 генерація першої частини займає близько

однієї години, а пошук блоків, що остаточно формують колізію, триває від 15 секунд до 5 хвилин. Важливо зазначити, що ця атака є універсальною і успішно працює для будь-якого заданого початкового значення.

Подібна вразливість була виявлена і в алгоритмі HAVAL, який розроблений для стиснення повідомлень довільної довжини та продукує хеші довжиною від 128 до 224 біт. Раніше криптоаналітикам вдавалося успішно атакувати лише скорочену версію HAVAL-128. У рамках даного дослідження вперше було здійснено злам повної версії алгоритму, причому для знаходження колізії потрібно виконати лише близько 64 обчислень. Знайдені приклади демонструють, що зміна вхідного повідомлення на певну різницю з ненульовими значеннями на конкретних позиціях призводить до формування ідентичних хешів. Щодо алгоритму MD4, попередні атаки дозволяли знаходити колізії з ймовірністю 1 до понад 4 мільйонів. Завдяки новому підходу пошук колізії для MD4 спростився настільки, що його можна виконати за допомогою звичайних ручних розрахунків.

Крім того, дослідження охопило алгоритм RIPEMD, розроблений у рамках проекту RIPE. Раніше було доведено вразливість лише його двораундової версії , проте нові результати підтверджують, що повна версія RIPEMD також не є стійкою до колізій. Принципи запропонованого методу свідчать про те, що й інші хеш-функції не мають ідеального рівня безпеки. Зокрема, колізію для алгоритму SHA-0 можна знайти за 2 у 40 ступені обчислень, а для HAVAL-160 - з ймовірністю 1 до 2 у 32 ступені.

Висновки

У результаті дослідження доведено вразливість до колізій популярних хеш-функцій, зокрема MD4, MD5, HAVAL-128 та RIPEMD. Запропоновані методи атаки дозволяють знаходити реальні колізії зі стандартними векторами ініціалізації та вирізняються високою обчислювальною ефективністю. Зокрема, злам повної версії HAVAL-128 потребує лише 64 обчислень , для MD4 достатньо ручних розрахунків , а генерація колізій для MD5 займає близько години машинного часу. Також доведено, що повна версія RIPEMD не є стійкою до колізій. Отримані результати підтверджують, що досліджені алгоритми не забезпечують ідеального рівня криптографічної безпеки. Це ставить під загрозу цілісність даних та надійність систем, що їх використовують, і вимагає переходу на більш стійкі сучасні стандарти.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Boer B. den, Bosselaers A. Collisions for the Compression Function of MD5 // Eurocrypto. – 1993.
2. Dobbertin H. Cryptanalysis of MD4 // Fast Software Encryption, LNCS 1039. – Springer-Verlag, 1996.
3. Dobbertin H. Cryptanalysis of MD5 compress // Rump session of Eurocrypt'96. – 1996.
4. Rivest R. L. The MD5 Message Digest Algorithm, Request for Comments (RFC) 1321. – Internet Activities Board, Internet Privacy Task Force, 1992.
5. Zheng Y., Pieprzyk J., Seberry J. HAVAL - A One-way Hashing Algorithm with Variable Length of Output // Auscrypto'92. – 1992.

Чуднівець Денис Русланович – студент групи 2БС-24б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: bournovich@gmail.com

Науковий керівник: ***Кирилащук Тетяна Геннадіївна*** – асистент кафедри захисту інформації, Вінницький національний технічний університет, Вінниця, e-mail: kgt0998@gmail.com

Chudnivets Denis – student of group 2BS-24B, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: bournovich@gmail.com

Scientific Supervisor: ***Kyrylashchuk Tatyana*** – assistant of the Information Security Department, Vinnytsia National Technical University, Vinnytsia, e-mail: kgt0998@gmail.com