МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ «КПІ»
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»
ОДЕСЬКА НАЦІОНАЛЬНА АКАДЕМІЯ ЗВ'ЯЗКУ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ ПОЛІТЕХНІЧНИЙ УНІВЕРСИТЕТ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ
ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

ПРАЦІ

IV Міжнародної науково-практичної конференції

«ОБРОБКА СИГНАЛІВ І НЕГАУССІВСЬКИХ ПРОЦЕСІВ»

Пам'яті професора Ю.П. Кунченка

22 - 24 травня 2013 р.,
м. Черкаси, Україна

Черкаси ЧДТУ **2013**

УДК 621.3;681.3;519.2;519.6
П70

Відповідальний редактор **Заболотній С.В.,** к.т.н., доцент, ЧДТУ.

Праці IV Міжнародної науково-практичної конференції «Обробка сигналів і
П70 негаусівських процесів», присвяченої пам'яті професора Ю.П. Кунченка: Тези доповідей. – М-во освіти і науки України, Черкас. держ. технол. ун-т. – Черкаси : ЧДТУ, 2013. – 212 с.

У виданні відображено результати актуальних наукових і прикладних досліджень, пов'язаних із опрацюванням інформації, зокрема, наукової школи професора Ю.П. Кунченка з обробки сигналів і негаусівських процесів, що охоплюють широке коло сучасних аспектів розвитку науково-технічного прогресу: створення математичних моделей сигналів та систем; синтез і аналіз методів та алгоритмів обробки сигналів та статистичних даних; розробка апаратних та програмних засобів опрацювання сигналів та даних; комп'ютерне моделювання.

Для наукових співробітників, інженерно-технічних працівників, аспірантів і студентів-старшокурсників, що спеціалізуються в галузях радіотехніки, телекомунікацій, інформатики, автоматичного управління та історії техніки.

УДК 621.3;681.3;519.2;519.6

- скорочення довжини необхідних антенних кабелів, що в типовому випадку вдвічі покращує радіопараметри станції;
- на 20% компактніше і легше типової базової станції;
- виконання, що дозволяє її використовувати поза приміщеннями в будь-яких погодних умовах;
- модульність, масштабованість та компактність базових станцій.

Література

1. Тихвинский В.О., Терентьев С.В., Юрчук А.Б. Сети мобильной связи LTE: технологии и архитектура. – М.: Эко-Трендз, 2010. – 284с.: ил.
2. Тихвинский В.О., Терентьев С.В., Минаев И.В. Стандартизация, спецификации, эволюция технологии и архитектура базовой сети LTE // Сети и средства связи, № 2(10). Специальный выпуск «Сети доступа». – 2009. – № 3.

УДК 003.26: 004.424.47

МЕТОД КЛЮЧОВОГО ХЕШУВАННЯ ТЕОРЕТИЧНО ДОВЕДЕНОЇ СТІЙКОСТІ НА ОСНОВІ ЕЛІПТИЧНИХ КРИВИХ

Лужецький В.А., Олексюк А.О.
Вінницький національний технічний університет,
21029, м. Вінниця, вул. Хмельницьке шосе 95, (0432)513293
E-mail: aneliyaoleksyuk@gmail.com

У зв'язку зі швидким розвитком інформаційних технологій, захисту інформації приділяється підвищена увага. Хеш-функції відіграють значну роль в автентифікації повідомлень та цифровому підписуванні. З появою успішних атак на традиційні хеш-функції, постала задача створення нових більш захищених методів хешування. Математичний апарат еліптичних кривих є потужним механізмом для створення стійких хеш-функцій, за рахунок того, що базується на проблемі дискретного логарифмування в групі точок еліптичної кривої, для якої існує теоретично доведена оцінка складності.

Оскільки процес хешування є ітеративним багатокроковим процесом, при якому на кожному кроці виконуються однотипні обчислення, то в даному методі перед початком хешування пропонується виконати передобчислення значень точок еліптичної кривої, для того щоб спростити обчислення на кожній ітерації.

Суть методу, що пропонується, полягає в такому:

- дані подають у вигляді послідовності $M=\{m_1, m_2, \ldots, m_N\}$;
- на кожній ітерації обчислюється проміжне хеш-значення за формулою:

$$h_i = (h_{i-1} \oplus m_i) \cdot P = K_i P, \qquad (1)$$

де i =1,2, …, N;

У блок пам'яті заносяться попередньо обчислені значення точок еліптичної кривої. Формування адрес, для запису і зчитування даних для блоку пам'яті забезпечує лічильник. На вхід блоку додавання за модулем 2 подаються i-й блок даних та секретне значення h_0, далі за допомогою блоку додавання за модулем 2 формується значення K_i, яке передається в регістр зсуву. Цифри a_j коду K_i послідовно з'являються на виході регістру зсуву і визначається чи потрібно виконувати додавання чергового значення $2^j P$ до раніше накопиченого значення суми точок еліптичної кривої. Узгодження роботи всіх блоків спеціалізованого процесора забезпечується блоком керування.

Запропонований метод дозволяє пришвидшити процедуру хешування даних у 3 рази. Оскільки значна частка механізмів автентифікації користувачів та даних використовує методи хешування, то це забезпечує пришвидшення процедури автентифікації.

Література

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке С. 2-е узд./ Брюс Шнайер.– СПб.: Вильямс, 2000. – 789с. – ISBN 5-89392-055-4.
2. Патент України на корисну модель № 649225 М. кл. G 09 C 1/00. Спосіб ключового хешування теоретично доведеної стійкості на основі еліптичних кривих/ Лужецький В.А., Баришев Ю.В., Черняхович К.В., Олексюк А.О.; заявник та патентовласник Вінницький національний технічний університет. – №u201104428; заявл 11.04.2011; опубл. 25.11.2011р., бюл. №22.

АДАПТИВНОЕ ОБНАРУЖЕНИЕ ИМПУЛЬСНЫХ РАДИОСИГНАЛОВ ПРИ НЕКОГЕРЕНТНОМ ПРИЕМЕ НА ФОНЕ НЕГАУССОВСКИХ ПОМЕХ

Мартыненко С.С.
Черкасский государственный технологический университет
бул. Шевченка, 460, Черкассы, 18006, тел. (0472)730261
E-mail: smartynenko@ukr.net

В большинстве случае при оптимальном приеме импульсных радиосигналов говорить о когерентном приеме не совсем корректно. Из-за наличия помех в каналах связи начальная фаза сигнала может быть или неизвестной или изменяться по одному из известных законов распределения вероятностей. В работах [1, 2] представлены алгоритмы обнаружения импульсных сигналов на фоне негауссовских сигналов при некогерентном приеме. При этом считалось, что фаза принимаемых импульсов изменялась по равномерному закону в интервале $[-\pi;\pi]$. В качестве априорной