Науково-технічний семінар

"Синтез, обробка та відображення інформаційних моделей" (ІнфоСинтез)

(Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України,
Харківський університет Повітряних Сил ім. І. Кожедуба)

e-mail: infosintez@hups.edu.ua

Чергове засідання 25.12.2007

1. ***Корольов Р.В.**, ад'юнкт науково-організаційного відділу Харківського університету Повітряних Сил ім.І.Кожедуба.* **Метод швидкого формування послідовностей псевдовипадкових чисел з використанням алгоритмів надмірного кодування.**

Методи формування послідовностей псевдовипадкових чисел (ППВЧ) одержали широке практичне використання в багатьох областях науки і техніки: у криптографічних засобах захисту інформації, при формуванні великих ансамблів слабокорелірованних дискретних сигналів, для забезпечення правильності функціонування компонентів інформаційної системи, забезпечення неможливості відслідкування інформаційних відтоків, захист авторських прав, прав власників інформації і ін. До методів формування ППВЧ пред'являються жорсткі вимоги: висока стійкість вживаних алгоритмів до відновлення секретних ключових даних, висока швидкість формування ППВЧ, простота практичної реалізації в програмному і апаратному вигляді і ін. Аналіз результатів багаторічного криптографічного проекту NESSIE показує, що найбільшу стійкість забезпечують методи формування ППВЧ засновані на застосуванні модулярної арифметики. Використання цього підходу дозволяє звести завдання відновлення секретних ключових даних, параметрізуючих роботу генератора ППВЧ, до рішення одного з теоретіко-складних завдань модулярної арифметики (факторизації і/або дискретне логарифмування). У теж час даний напрям крім високих показників стійкості зв'язаний з необхідністю реалізації обчислень над великими числами, що істотно (на 3-5 порядків) знижує швидкість формування ППВЧ. Практична реалізація генераторів ППВЧ, що використовують модулярну арифметику, так само украй скрутна, особливо на процесорах малої розрядності. Альтернативним напрямом досліджень є методи формування ППВЧ, засновані на використанні алгоритмів надмірного кодування. Завдання формування кодового слова надмірного коду ефективно розв'язується алгоритмами поліноміальної складності. У цей час завдання декодування випадкового коду (надмірного коду загального положення) належить до класу теоретіко-складних завдань з експоненціальною складністю рішення. Основна ідея побудови генератора ППВЧ полягає у використанні алгоритмів надмірного кодування для формування ППВЧ і зведення завдання відновлення секретних ключових даних до рішення теоретіко-складної задачі декодування випадкового коду.

Пропонується метод швидкого формування ППВЧ з використанням алгоритмів надмірного кодування, розглянуті практичні алгоритми формування ППВЧ і структурні схеми відповідних генераторів. В результаті проведених дослідження встановлено, що пропонований метод дозволяє забезпечити доказову стійкість за рахунок зведення завдання відновлення секретних ключових даних до рішення теоретіко-складної задачі декодування випадкового коду.

2. ***Кужель І.Є.**, ад'юнкт науково-організаційного відділу Харківського університету Повітряних Сил ім.І.Кожедуба.* **Розробка та дослідження алгебраїчних згортувальних кодів, заданих через многочлен Гоппи.**

Ефективним засобом підвищення перешкодостійкості інформації в АСУВ є методи згортувального кодування. Вони дозволяють ефективно виправляти складні комбінації помилок і найбільший енергетичний виграш.

Математичний апарат згортувального кодування дозволяє задавати потокові теоретико-кодові схеми для ефективного криптографічного захисту інформаційного потоку символів. Криптографічний захист інформації в таких схемах поєднується з перешкодостійким кодуванням.

Для побудови криптографічно стійкої криптосистеми методи згортувального кодування повинні легко описуватися в поліноміальному і матричному вигляді, мати швидкі алгоритми кодування і декодування і формувати велике число різних кодів з фіксованими параметрами. Більшість відомих згортувальних кодів одержано шляхом перебору і тестування по вільній кодовій відстані. Проте складність переборного методу швидко від довжини кодового обмеження і, відповідно, його застосування абсолютно непридатне для побудови потокових теоретико-кодових схем.

Досліджуються алгебраїчні методи, побудови згортувальних кодів, аналізуються їх можливості по побудові потокових теоретико-кодових схем. Розробляються і досліджуються алгебраїчні методи побудови згортувальних кодів, заданих через многочлен Гоппи. Виводяться аналітичні вирази, що встановлюють взаємозв'язок між параметрами недвійкових кодів Гоппи і заданими згортувальними кодами. Розробляються потокові теоретико-кодові схеми на алгебраїчних згортувальних кодах, заданих через многочлен Гоппи.

Наступне засідання семінару відбудеться 29.01.2008 у аудиторії 101-В ГНК (програма засідання буде доведена додатково)

Схема оформлення статей
у фахові наукові видання Харківського університету Повітряних Сил ім. Івана Кожедуба
(журнал "Системи озброєння та військова техніка", "Збірник наукових праць ХУПС",
тематичний збірник "Системи обробки інформації"; переліки 1, 16, 17 наукових фахових видань України)

УДК (кегль – 12 пт)

← *пустий рядок – **10** пт*

А.А. Іванов[1], Б.Б. Петров[2] (кегль – 12 пт)

← *пустий рядок – **8** пт*

[1]*Харківський університет Повітряних Сил ім. І. Кожедуба, Харків*
[2]*Національна академія оборони України, Київ (кегль – 12 пт, накреслення – курсив)*

← *пустий рядок – **12** пт*

НАЗВА СТАТТІ (КЕГЛЬ – 12 ПТ; НАКРЕСЛЕННЯ – "НАПІВЖИРНЕ", ПО ЦЕНТРУ)

← *пустий рядок – **12** пт*

Анотація (мовою основного тексту статті, обсягом до 6 рядків): кегль – 10 пт; накреслення – "курсив", вирівнювання – за шириною; відступ зліва – 1,5 см, без абзацного відступу.

← *пустий рядок – **9** пт*

перелік ключових слів (кегль – 10 пт, накреслення – курсив, напі

← *пустий рядок – **12** пт*

Вимоги до набору

Формат аркуша: А4 (21 × 29,7 см).

Параметри сторінки (відступи від краю): зліва – 2,25 см; справа – 2,25 см; зверху – 2 см; знизу – 2,5 см.

Шрифт статті – *Times New Roman*; накреслення – пряме; кегль – 10 пт міжрядковий інтервал (множник) – 1,1.

Текст статті розташовується у два стовпчики однакової ширини – 8 см, відстань між стовпчиками – 0,5 см; відступ першого рядка абзацу – 0,75 см.

Підзаголовок (кегль – 12 пт): накреслення – напівжирне; відступів немає; вирівнювання – центроване; зверху та знизу відокремлюється **6** пунктами.

Не використовуйте для форматування тексту пропуски, табуляцію тощо. Не встановлюйте ручне перенесення слів, не використовуйте колонтитули. Між значенням величини та одиницею її вимірювання ставте нерозривний пропуск (Ctrl + Shift + пропуск).

УВАГА! Остання сторінка статті заповнюється не менш, ніж на 3/4.

Набір формул: редактор формул *MS Equation*. **Забороняється** використовувати для набору формул графічні об'єкти, кадри й таблиці.

В меню "*Размер* → *Определить*" ввести такі розміри:

Обычный – 10 пт; Крупный индекс – 8 пт;
Мелкий индекс – 7 пт; Крупный символ – 14 пт;
Мелкий символ – 10 пт.

Стиль формул – "прямий", тобто в меню "*Стиль* → *Определить"* поля "Формат символов" – пусті.

Табличний заголовок (9 кегль) – **обов'язковий**.

Рисунки **обов'язково** супроводжуються центрованими підрисунковими підписами (кегль – 9) (рис. 1).

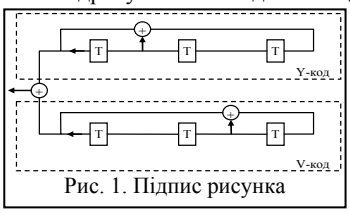

Рис. 1. Підпис рисунка

Таблиця 1

Динаміка змін

Інтервал	1	2
Параметр	180	168

Не допускаються кольорові та фонові рисунки.

Допускається розташування великих рисунків, формул та таблиць в одну колонку (до 16,5 см).

Список літератури виділяється підзаголовком "**Список літератури**" та оформлюється (кегль – 9 пт, курсив) згідно з міждержавним стандартом ГОСТ 7.1-84:

1. Косенко О.О. Петренко А.А. Назва статті // Системи обробки інформації. – Х.: ХУПС, 2007. – № 9 (67). – С. 111-117.

Структура рукопису

Відповідно до постанови ВАК України від 15.01.2003 № 7-05/1 текст статті повинен мати таку структуру: ***постановка проблеми*** *у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями*; ***аналіз останніх досліджень і публікацій***, *на які спирається автор*; ***формулювання мети статті*** (*постановка завдання*); ***виклад основного матеріалу*** *дослідження*; ***висновки*** *з даного дослідження і перспективи подальших розвідок*. Текст статті розбивається на відповідні розділи із підзаголовками, які виділені напівжирним шрифтом.

Після останнього аркушу статті на новому аркуші наводяться відомості про рецензента, авторів та інформація для Українського реферативного журналу (9 кегль) згідно із зразком.

Рецензент: д-р техн. наук, проф. М.І. Сидоренко, Інститут радіофізики та електроніки НАН України, Харків.

Автор*: КЛІМЕНКО Іван Миколайович*
Об'єднаний науково-дослідний інститут Збройних Сил, Харків, кандидат технічних наук, доцент, начальника відділу.
Роб. тел. – 333-33-33, дом. тел. – 777-77-77, E-mail – kim@ic.ua.

УДК 581.341
Кліменко І.М. **Аналіз ризиків при забезпеченні інформаційної безпеки //** Системи обробки інформації. – 2008. – Вип. 00 (00). – С. 00-00. – Рос.
Розглядається один з алгоритмів оцінки і визначення прийнятності рівня ризику при забезпеченні інформаційної безпеки.
Табл. 2. Іл. 3. Бібліогр. 7 назв.

Клименко И.Н. **Анализ рисков при обеспечении информационной безопасности** // Системы обработки информации. – 2008. – Вып. 00 (00). – С. 00-00. – Рус.
Рассматривается один из алгоритмов оценки и определения принятия уровня риска при обеспечении информационной безопасности.

Klimenko I.M. **Analysis of risks when ensuring information safety** // Sistemi obrobki informacii. – 2005. – Issue 00 (00). – P. 00-00. – Rus.
Is considered one of the algorithms of evaluation and determinations of acceptability of risk level when ensuring information safety.

Подання матеріалів

Обсяг рукопису – від 3 до 10 аркушів українською, російською або англійською мовами (у журналі "Системи озброєння та військова техніка" – тільки українська).

Для публікації необхідно представити статтю у електронній формі з роздрукованим екземпляром. Рукопис супроводжується ***експертним висновком, рецензією доктора наук (професора), витягом з протоколу засідання кафедри (відділу).***

Подані матеріали автору не повертаються.