УДК 681.3.06

О.О. Кузнецов, Ю.М. Рябуха, Р.В. Корольов

Харківський університет Повітряних Сил ім. І Кожедуба, Харків

МЕТОД ФОРМУВАННЯ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ ІЗ ЗАСТОСУВАННЯМ ПЕРЕТВОРЕНЬ У ГРУПІ ТОЧОК ЕЛІПТИЧНИХ КРИВИХ

Відповідно до основних положень Концепції національної безпеки України першочерговими завданнями у галузі інформатизації та розвитку зв'язку є побудова комплексних систем захисту інформації. Головною особливістю у вирішенні комплексу завдань, що стоять в цій області, є висока складність, яка обумовлена жорсткими імовірнісно-тимчасовими вимогами, що пред'являються до форми і способів обробки і передачі інформації, до її своєчасності та безпеки.

Особливе місце серед вирішуваних завдань займає розробка перспективних методів і алгоритмів формування псевдовипадкових чисел (ПВЧ), які використовуються: для забезпечення правильності функціонування компонентів інформаційної системи, зокрема для забезпечення відсутності недокументованих можливостей; для забезпечення невідстежуваності інформаційних потоків в системі; для захисту авторських прав, прав власників інформації та ін.; у криптографічних засобах захисту інформації при забезпеченні конфіденційності, цілісності, автентичності і доступності інформаційних технологій. Питанням розробки ефективних методів формування ПВЧ присвячено багато робіт, в яких розглянуті різні підходи, що засновані на використанні: рекурентних регістрів з лінійними і нелінійними зворотними зв'язками; конгруентних перетворень; математичного апарату булевої алгебри і нелінійних криптографічних функцій; блоків ускладнень (блоків замін) сучасних симетричних шифрів та інші. У той же час, формовані відомими методами ПСЧ не завжди володіють максимальним періодом. Крім того, поява ефективних атак на симетричні шифри автоматично веде до уразливості відповідних генераторів ПСЧ.

Інший напрямок полягає у зведенні завдання відновлення таємного правила формування ПСЧ до рішення добре відомого теоретіко-складного завдання, наприклад, завдання факторизації, дискретного логарифмування та інших. Подібні методи (засновані на доказово стійких перетвореннях) найбільш перспективні по стійкості до негативних дій зловмисників і, як показують проведені дослідження, володіють високими показниками статистичної безпеки. У той же час доказово стійкі генератори (ДСГ) обчислювально складні в реалізації (на 3-4 порядки в порівнянні з класичними підходами) і не дозволяють формувати ПВЧ максимального періоду. Виникає протиріччя, коли існуючий математичний апарат, відомі методи і алгоритми формування ПСЧ не дозволяють повною

мірою забезпечити високі показники ефективності. Для вирішення виявленого протиріччя необхідна наукова розробка перспективних методів формування ПВЧ, конкретна реалізація яких дозволить будувати доказово стійкі генератори з потрібними властивостями. Перспективним напрямом в цьому сенсі є доказово стійкі генератори ПВЧ із застосуванням перетворень у групі точок еліптичних кривих, завдання відновлення таємного правила формування ПВЧ в яких зводиться до рішення теоретіко-складного завдання дискретного логарифмування у групі точок еліптичних кривих. В даній роботи викладаються основні результати, що отримані при розробці нового методу формування ПВЧ, досліджується його ефективність та проводяться порівняльні дослідження із іншими генераторами.

Виробляються практичні рекомендації із застосування отриманих результатів та впровадження їх у комплексні системи захисту інформації..

Список літератури

1. Болотов А.А. Элементарное введение в эллиптическую криптографию: Протоколы криптографии на эллиптических кривых / А.А. Болотов, С.Б. Гашков, А.Б. Фролов. – М.: КомКнига, 2006. – 280 с.

2. Соловьев Ю.П. Эллиптические кривые и современные алгоритмы теории чисел / Ю.П. Соловьев, В.А. Садовничий, Е.Т. Шавгулидзе, В.В. Белокуров. – М.: Ижевск: Институт компьютерных исследований, 2003. –192 с.

3. Алгоритмические основы эллиптической криптографии / [Болотов А.А. и др.]. – М.: МЭИ, 2000. – 100 с.