УДК 628.916:681.518.5

Дослідження поліномів для сигнатурної алгебри в кінцевому полі галуа gf(3)

Рисований О. М., Шканд Д. О.

Національний технічний університет «Харківський політехнічний інститут»
вул. Кирпичова, 2, Харків, Україна, 61000
E-mail: rysov81524@gmail.com , shkand.daria@gmail.com

Вступ. Сигнатурна математика використовується в криптографії, теорії чисел, в структурах алгебри та хешуванні.

У криптографії та теорії чисел сигнатурна математика використовується тоді, коли операції над підписами (signatures) виконуються у кінцевих полях, наприклад, у схемах цифрових підписів (DSA, ECDSA, EdDSA), де операції відбуваються над елементами кінцевих полів. І тут “сигнатурна математика” представляє собою арифметику підписів у GF(p).

В алгебраїчних структурах або хешуванні сигнатура може означати унікальний числовий відбиток (хеш, контрольна сума, вектор ознак), а сигнатурна математика – це набір правил операцій над такими відбитками, що виконуються за модулем поля [1-2].

Велике значення сигнатурна математика в GF(3) має в кодах Ріда-Соломона (варіанти над GF(3)), у поліноміальному хешуванні, в електронних підписах та контрольних сумах, у криптографії над кінцевими полями, у системах із тризначною логікою (наприклад, для квантових обчислень або квантових обчислень). А в генераторах чисел застосування елементів кінцевого поля різко збільшує довжину генерованої послідовності.

Мета роботи – аналіз поліномів для сигнатурної алгебри в кінцевому полі Галуа GF(3).

Матеріали дослідження. У всіх областях, які застосовують поліноміальні (сигнатурні) обчислення, використовуються ненаведені поліноми [3]. Ненаведений поліном - це поліном, який не можна розкласти на множники меншою мірою GF(3).

Це пов'язано з тим, що тільки такі поліноми генерують максимальну кількість своїх станів і ці стани підпорядковані правилам арифметики кінцевих полів. Наявність такої властивості дозволяє обчислювати будь-який стан, а при контролі та діагностиці – виявляти та часто локалізувати помилки, що виникли.

Операції в GF(3) виконуються над багаточленами з коефіцієнтами {0,1,2} за модулем неприведеного багаточлена, наприклад x^2+1 неприведен в GF(3) т.я. жодне значення x∈{0,1,2} не робить його рівним нулю.

Розширені поля на основі GF(3) використовуються:

– для трьох систем, квантових або аналогових уявлень (тернарна структура (три значення));

– для збільшення щільності інформації (одне значення в $GF(3^n)$ кодує більше біт, ніж в $GF(2^n)$);

– для стійкості до лінійних атак (тризначні операції складніше звести до бінарної лінійної алгебри);

– для нелінійних підпису та кодування (при побудові схем багаточленів над $GF(3^n)$ з'являються сильні нелінійні залежності, що корисно захисту).

У роботі визначено, що у мультиваріантних (багаточленних) сигнатурних схемах (наприклад, Rainbow, UOV) можна використовувати поля не тільки $GF(2^n)$, але й $GF(3^n)$. У цьому випадку кожен елемент підпису - це вектор з $GF(3^n)$; операції над підписами – квадратичні поліноми над цим полем. Таким чином, використання $GF(3^n)$ робить простір рішень складнішим для атаки, підвищує ентропію підпису, створює нелінійність у тернарній арифметиці.

Усі класичні генератори псевдовипадкових послідовностей у своїй основі мають регістр зсуву із зворотними зв'язками за правилом обраного поліному. У цьому випадку, на складність технічної реалізації не впливає наявність коефіцієнтів у записі поліномів. Значення мають лише кількість та вид (у разі нелінійних перетворень) зворотних зв'язків. Тому, змінюється складність суматора за модулем поля. Наприклад, довжина генерованої послідовності для degP(x) = 5 дорівнює 242. Однак, не усі P(X) з degP(X) = 5 генерують таку довжину. Це залежить від властивостей полінома (такі P(X) повинні бути примітивними та ненаведеними).

Регістри зсуву з зворотними зв'язками описуються двома матрицями: матрицею з'єднань (зв'язків) та матрицею вихідних станів (перевірочна матриця).

В роботі обчислено, що для $P(X) \in \deg P(X) = 4$ з $T_{max} = 3^{\deg P(x)} - 1 = 80$ налічується всього 16 поліномів, у яких матриці зв'язків першого ступеня мають види:

$$P(X) = 10011,\ S = \begin{Vmatrix} h_2 h_{79} h_{80} h_1 \end{Vmatrix};$$
$$P(X) = 10021,\ S = \begin{Vmatrix} h_2 h_{79} h_{80} h_1 \end{Vmatrix};$$
$$P(X) = 11001,\ S = \begin{Vmatrix} h_2 h_3 h_4 h_1 \end{Vmatrix};$$
$$P(X) = 11121,\ S = \begin{Vmatrix} h_2 h_7 h_{15} h_1 \end{Vmatrix};$$
$$P(X) = 11221,\ S = \begin{Vmatrix} h_2 h_{68} h_{66} h_1 \end{Vmatrix};$$
$$P(X) = 12001,\ S = \begin{Vmatrix} h_2 h_3 h_4 h_1 \end{Vmatrix};$$
$$P(X) = 12111,\ S = \begin{Vmatrix} h_2 h_{17} h_{55} h_1 \end{Vmatrix};$$
$$P(X) = 12211,\ S = \begin{Vmatrix} h_2 h_{38} h_{66} h_1 \end{Vmatrix};$$
$$P(X) = 10012,\ S = \begin{Vmatrix} h_{42} h_{39} h_{40} h_{41} \end{Vmatrix};$$
$$P(X) = 10022,\ S = \begin{Vmatrix} h_{42} h_{39} h_{40} h_{41} \end{Vmatrix};$$
$$P(X) = 11002,\ S = \begin{Vmatrix} h_{42} h_{43} h_{44} h_{41} \end{Vmatrix};$$
$$P(X) = 11122,\ S = \begin{Vmatrix} h_{42} h_{57} h_{55} h_{41} \end{Vmatrix};$$
$$P(X) = 11222,\ S = \begin{Vmatrix} h_{42} h_{38} h_{36} h_{41} \end{Vmatrix};$$
$$P(X) = 12002,\ S = \begin{Vmatrix} h_{42} h_{43} h_{44} h_{41} \end{Vmatrix};$$
$$P(X) = 12112,\ S = \begin{Vmatrix} h_{42} h_{57} h_{15} h_{41} \end{Vmatrix};$$
$$P(X) = 12212,\ S = \begin{Vmatrix} h_{42} h_{68} h_{26} h_{41} \end{Vmatrix}.$$

Висновки. Таким чином, у роботі отримані наукові результати по визначенню поліномів для сигнатурної алгебри в кінцевих полях Галуа, наведено залежності стовпців перевірочної матриці для формування матриці зв'язків першого ступеню.

Бібліографічні посилання

1. Рисований О.М. Метод генерування нелінійної псевдовипадкової послідовності без використання зворотних зв'язків / О.М. Рисований // Системи управління, навігації та зв'язку. – Полтава : ПНТУ ім. Ю. Кондратюка. –2018. – №4 (50).– С. 144-146.

2. Рисований О.М. Метод синтезу генераторів у кінцевому полі GF(3) зі спрощенням блоків множення / О.М. Рисований // Сучасні інформаційні системи // – Харків: НТУ «ХПІ» – 2018. – Том 2, №3. – С. 76-79.

3. Рисований О.М., Коломійцев Л.В., Альошин Г.В. та інш. Метод підвищення ефективності управління безпілотним літальним апаратом на основі використання нелінійного псевдовипадкового генератора // Scientific Collection «InterConf», (149): with the Proceedings of the 11 th International Scientific and Practical Conference «International Forum: Problems and Scientific Solutions» (April 6-8, 2023; Melbourne, Australia) by the SPC «InterConf». CSIRO Publishing House, 2023 - 282-290 p.