Спецкурс «Алгебраическая криптография» в МГТУ им.Н.Э. Баумана

Пудовкина М.

МГТУ им. Н.Э. Баумана

- Предназначен для студентов 5 курса, специальность «Компьютерная безопасность»

- Две основные части:

  I. Решение систем алгебраических уравнений (САУ).

  II. Применение групп подстановок в криптографии.

Часть I

- Основные понятия и результаты теории систем алгебраических уравнений.
- Системы уравнений и идеалы в кольцах многочленов. Понятие идеала, базиса идеала. Идеалы в кольце многочленов.
- Теорема Гильберта о базисе. Идеал системы.

Теорема Гильберта о базисе. Каждый идеал $I \in \mathrm{K}[x_1,...,x_n]$ допускает конечный базис, т.е. найдутся такие $f_1(x_1,...,x_n),...,f_c(x_1,...,x_n) \in I$, что

$$I = \{ f_1 r_1 + ... + f_c r_c \mid r_1,...,r_c \in \mathrm{K}[x_1,...,x_n] \}.$$

Всякой САУ

$$\begin{cases} p_1(x_1,...,x_n) = 0, \\ p_2(x_1,...,x_n) = 0, \\ ..... \end{cases}$$

ставим в соответствие идеал

$$I = (p_1(x_1,...,x_n), p_2(x_1,...,x_n),...).$$

- Понятие и примеры аффинного алгебраического многообразия.

Пусть $V_n(K)-$ n-мерное пространство над полем K.

Определение. Подмножество $X \subset V_n(K)$ называется аффинным алгебраическим многообразием, если найдётся система S:

$$\begin{cases} p_1(x_1,...,x_n)=0, \\ ..... \\ p_m(x_1,...,x_n)=0, \end{cases}$$

для которой из условия $\overline{x}=(x_1,...,x_n)\in X$ следует, что $\overline{x}$ – решение системы S, и наоборот.

Пусть $X(S)-$ множество решений системы S. Для идеала $I \lhd \mathrm{K}[x_1,...,x_n]$ положим

$$X(I)=\left\{(x_1,...,x_n)\in V_n(\mathrm{K}) \mid f(x_1,...,x_n)=0 \ \forall f\in I\right\}.$$

$$J(X)=\left\{p\in \mathrm{K}[x_1,...,x_n] \mid p(x_1,...,x_n)=0 \forall (x_1,...,x_n)\in X\right\}$$

Утверждение. Системы S_1 и S_2 эквиваленты тогда и только тогда, когда $J(X(S_1))=J(X(S_2))$.

- Радикал идеала и его свойства. Теорема Гильберта о нулях. Применение в теории САУ над алгебраически замкнутым полем.

Пусть $I \lhd \mathrm{K}[x_1,...,x_n]$ – произвольный идеал, K – алгебраически замкнутое поле.

Радикалом идеала I называется множество

$$r(I) = \left\{ f \in \mathrm{K}[x_1,...,x_n] \mid f^t \in I \text{ для некоторого } t \in \mathrm{N} \right\}.$$

Теорема Гильберта о нулях. Над полем K для каждой САУ имеем $J(X(S)) = r(I(S))$.

Эквивалентная формулировка. Для системы

$$\begin{cases} p_1(x_1,...,x_n) = 0, \\ ..... \\ p_m(x_1,...,x_n) = 0, \end{cases}$$

алгебраических уравнений многочлен $f(x_1,...,x_n) = 0$ на всех решениях данной системы тогда и только тогда, когда существуют $r_1,...,r_m \in \mathrm{K}[x_1,...,x_n]$ и $t \in \mathrm{N}$, для которых $f^t = f_1 r_1 + ... + f_m r_m$.

- Лексикографический порядок на множестве одночленов.
- Определение базиса Грёбнера и решение задачи вхождения.
- Бриллиантовая теорема.
- Алгоритм Бухбергера.
- Минимальный редуцированный базис Гребнера.
- Примеры вычисления базисов Гребнера.

Базис $g_1,...,g_m$ идеала $I =< g_1,...,g_m >$ называется *базисом Грёбнера* идеала I, если всякий многочлен $h \in I$ редуцируется к нулю при помощи $g_1,...,g_m$.

Бриллиантовая лемма. Базис $g_1,...,g_m$ идеала I является базисом Грёбнера тогда и тогда, когда в нем нет зацеплений или каждое зацепление разрешимо.

- Семейство алгоритмов XL.
- Применение в криптографии.
- Алгебраическая атака.
- Алгоритмы шифрования: алгоритм Куртуа (Courtois Toy Cipher), Trivium, Bivium,

- Courtois, N. 2006. How fast can be algebraic attacks on block ciphers? Cryptology ePrint Archive, Report 2006=168, http://eprint.iacr.org/2006/168.pdf
- Buchmann, J., Pychkine A., Weinmann R. P. Block ciphers sensitive to Grobner basis attacks. Cryptology ePrint Archive, http://eprint.iacr.org/2005/200
- Courtois N., Patarin J. 2003. About the XL Algorithm over GF(2). In Topics in Cryptology - CT-RSA 2003: The Cryptographers' Track At The RSA Conference 2003; Proceedings. Springer, pp. 141–157.

Часть II. Применение групп подстановок в криптографии

- Основные понятия теории групп подстановок введены в курсе «Дополнительные главы дискретной математики»

- Сплетение групп подстановок. Строение сплетения групп $G \int F$. Примеры использования операции сплетения.

$$\Phi_n = \{f_\pi : V_m \times V_m \to V_m \times V_m \mid f_\pi : (\alpha, \beta) \to (\beta, \beta^\pi \oplus \alpha)\}.$$

$\alpha^{\pi_k} \in \{(\alpha \oplus k)^\pi, \alpha^\pi \oplus k\}$ для любого $\alpha \in V_m$,

$\overline{a} = a_1 a_2, \ldots,$

$$a_i = \begin{cases} 1, \text{ если } i \equiv 1,2 (\mathrm{mod}\, 3), \\ 0, \text{если } i \equiv 0 (\mathrm{mod}\, 3), \end{cases}$$

являющуюся решением рекуррентного соотношения $a_i = a_{i-1} \oplus a_{i-2}$ в $GF(2)$, $a_0 = 0, a_1 = 1$, $i = 2,3,\ldots$

Утверждение 7.1. Пусть $\pi \in S_2 \int S_{2^{m-1}}$, $f_k \in \Phi_n$, $\alpha^{\pi_k} \in \{(\alpha \oplus k)^\pi, \alpha^\pi \oplus k\}$ для любого $k \in V_m$. Тогда

1. $\pi_k \in S_2 \int S_{2^{m-1}}$ для любого $k \in V_m$.
2. $(\alpha, \beta)^{\prod_{i=1}^{l} f_{k_i \oplus \theta_i}} = (\alpha^{(l)} \oplus \sum_{i=1}^{l-1} a_{l-i}\theta_i, \beta^{(l)} \oplus \sum_{i=1}^{l} a_{l-i+1}\theta_i)$,

где $l \in \mathbb{N}$, $(\alpha, \beta)^{\prod_{i=1}^{l} f_{k_i}} = (\alpha^{(l)}, \beta^{(l)})$ и $\theta_i \in \{\vec{0}, \vec{1}\}$, $i = \overline{1,l}$.

Утверждение 7.2. Пусть $\pi \in S_{2^{m-1}} \int S_2$, $f_k \in \Phi_n$, $\alpha^{\pi_k} \in \{(\alpha \oplus k)^{\pi}, \alpha^{\pi} \oplus k\}$ для любого $k \in V_m$. Тогда для любого натурального числа l и любых $k_1, ..., k_l \in V_m$ справедливо включение:

1. $\left(\prod_{j=1}^{l} f_{k_j} \right)^3 \in S_{2^{n-1}} \int S_2$, если $l \not\equiv 0 (\mathrm{mod} 3)$;

2. $\left(\prod_{j=1}^{l} f_{k_j} \right)^2 \in S_{2^{n-1}} \int S_2$, если $l \equiv 0 (\mathrm{mod} 3)$.

Групповые свойства итерационных алгоритмов шифрования

Раундовая функция $g_k = \rho\sigma_k$, где $\sigma_k : \alpha \to \alpha + k$, $k \in V_n$, $n \geq 2$, ρ – некоторая фиксированная подстановка из $S(V_n)$. Пусть $G =< g_k \mid k \in V_n >$, $H_n = \{\sigma_k \mid k \in V_n\}$. $G =< \rho, H_n >$.

Утверждение 8.1. Если группа $G =< \rho\sigma_k \mid k \in V_n >$ импримитивна, то $\{v + U \mid v \in V_n\}$– система блоков импримитивности, где U – некоторое подпространство векторного пространства V_n.

Метод усеченных разностей для алгоритмов шифрования с раундовой функцией $g_k = \rho\sigma_k$ основан на следующем свойстве.

Следствие 8.2 [CarVSV06]**.** Если группа $G =< \rho\sigma_k \mid k \in V_n >$ импримитивна, то существует подпространство $U \subset V_n$, $U \neq \{\vec{0}\}$, такое, что $(\alpha + \beta)^\rho + \beta^\rho \in U$ для любых векторов $\beta \in V_n$, $\alpha \in U$.

Пусть $V_n = V_m^{(1)} \oplus ... + V_m^{(t)}$, $m \cdot t = n$, $\rho = \mu\lambda$, где $\mu, \lambda \in S(V_n)$ и $\mu = (\mu_1, ..., \mu_t)$, $\mu_i \in S(V_m^{(i)})$, $i = \overline{1,t}$, λ– линейное преобразование.

Теорема 8.3. Пусть выполняются следующие свойства: 1) $\vec{0}^{\mu} = \vec{0}$ и $\mu^s = 1$ для некоторого минимального натурального числа $s > 1$; 2) существует число r, $1 \le r < m/s$ такое, что для каждого $i \in \{\overline{1,t}\}$: а) $|\operatorname{Im} \pi_\beta^{(i)}| > 2^{m-r-1}$ для каждого вектора $\beta \in V_m^{(i)} \setminus \{\vec{0}\}$, где $\pi_\beta^{(i)} : V_m^{(i)} \to V_m^{(i)}$, $\pi_\beta^{(i)} : x \to (x+\beta)^{\mu_i} + x^{\mu_i}$; б) не существует собственного подпространства $U \le V_m^{(i)}$ такого, что $U^{\mu_i} = U$ и $\operatorname{co\,dim} U \le sr$; 3) $V_m^{(i_1)} \oplus ... \oplus V_m^{(i_r)}$ не является инвариантным относительно λ для каждого подмножества $\{i_1, ..., i_r\} \subset \{\overline{1,t}\}$, $r \notin \{0, m\}$.

Тогда группа $G = <\rho\sigma_k \mid k \in V_n>$ примитивна.

Следствие 8.4. Группа алгоритма AES примитивна.

По преобразованию λ строится орграф $\Gamma(\lambda)$ (перемешивающий граф). На подстановки μ_i и линейное преобразование λ накладываются следующие условия:

Условие 1. Орграф $\Gamma(\lambda)$ является сильно связанным и наибольший общий делитель длин всех циклов равен 1.

Условие 2. Группы $G(\mu_i)$, $i = \overline{1,n}$, транзитивные.

Теорема 8.5 [Mac07]. Пусть выполнены условия 1, 2 и одно из следующих условий: а) матрица $\hat{\lambda}$ преобразования λ перестановочная; б) $m \geq 3$ и матрица $\hat{\lambda}$ имеет вид $\hat{\lambda} = b \otimes I_m$, где $b-$ обратимая матрица порядка n, $\otimes-$ кронекерово произведение матриц, а I_m- единичная $m \times m$ матрица; в) $2^{mn} < (2^m - 1)^{n-1}(2^m + 2^{m-1} - 2)$;

то G является 2-транзитивной. Если дополнительно

г) $2^{mn} - 1$ не является степенью простого числа,

то $G = A(V_{mn})$.

Теорема 8.8 [Mac07]. Если группа подстановок G является 2-танзитивной, то выполнено условие 1.

Следующая теорема ([Mac07]) позволяет свести проверку 2-транзитивности группы $G(s)$ к проверке связанности графа $\Phi(s)$. Для построения данного графа рассмотрим матрицу $h = (h_{\alpha\beta})$,

$$h_{\alpha\beta} = \sum_{\beta \in V_m} I\{(\alpha+\beta)^s = \beta^s + \lambda\},\ \lambda, \alpha \in V_m \setminus \vec{0},$$

где $I\{A\}$ – индикатор наступления события A. Пусть $\Phi(s)$ – граф, задающийся матрицей смежности $w = hh^T = (w_{\alpha\beta})$: ребро (α, β), $\beta, \alpha \in V_m \setminus \vec{0}$, принадлежит графу $\Phi(s)$ тогда и только тогда, когда $w_{\alpha\beta} > 0$.

Теорема 8.9 [Mac07]. Группа $G(s)$ является 2-транзитивной тогда и только тогда, когда граф $\Phi(s)$ является связанным.

Спасибо за внимание!