Сафина Л.Р.
НГУ, совместная лаборатория Parallels-НГУ
Научный руководитель:
Кренделев С.Ф.

Реализации трехпроходного протокола обмена ключами

Общие сведения

- Множество сообщений - вектора в пространстве F^n, где F - некоторое конечное поле
- Пусть $F = Z_p$ (p - простое число)
- Ключом будем называть любое взаимно однозначное отображение $H : F^n \to F^n$
- Два участника – Алиса и Боб

Трехпроходной протокол обмена данными

- Необходимое условие: обратимые, коммутирующие отображения (назовем их H и K)
- Передаем вектор $v \in F^n$
- Алиса передает $x = H(v)$
- Боб посылает Алисе $y = K(x) = K(H(v))$
- Алиса пересылает $z = H^{-1}(y) = H^{-1}(K(H(v))) = K(v)$
- Боб получает $v = K^{-1}(z) = K^{-1}(K(z))$

Коммутирующие отображения линейной алгебры

- Простейшими взаимно однозначными отображениями являются линейные отображения

Построение коммутирующих отображений линейной алгебры

- $S : F^n \to F^n$ - линейное отображение
- Сопоставим S матрицу $\overline{S}$
- Выбираем полиномы $f(x), g(x)$
- Матрицы $f(\overline{S}), g(\overline{S})$ - коммутируют

Коммутирующие линейные отображения в трехпроходном протоколе

- Алиса и Боб обмениваются параметрами p, n и матрицей $\bar{S}$
- Вычисляются обратимые матрицы $f(\bar{S})$ (Алиса) и $g(\bar{S})$ (Боб)
- Применяется протокол

- Схема легко вскрывается (за $O(n^3)$ шагов)
- Можно использовать для идентификации

Пример вскрытия коммутирующих линейных отображений

- Поле Z_5
- Матрица $S = \begin{pmatrix} 0 & 1 \\ 2 & 2 \end{pmatrix}$ с неприводимым характеристическим многочленом
- $S^2 = \lambda S + \mu E$
- Алиса генерирует полином $pS + qE$, а Боб – $rS + tE$, где коэффициенты $p, q, r, t \in Z_5$

Пример вскрытия коммутирующих линейных отображений

- Пересылается вектор $v \in Z_5^2$
- Алиса посылает $x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = (pS + qE)\begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$
- Боб посылает $y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = (rS + tE)\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$
- К этому моменту злоумышленник знает матрицу S, числа p, n, вектора x, y

Пример вскрытия коммутирующих линейных отображений

- Злоумышленник также знает

$$y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = (rS + tE)\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = rS\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + t\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = r\begin{pmatrix} u_1 \\ u_2 \end{pmatrix} + t\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

(где $S\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} u_1 \\ u_2 \end{pmatrix}$)

- Значит, известна система уравнений

$$\begin{cases} ru_1 + tx_1 = y_1 \\ ru_2 + tx_2 = y_2 \end{cases}$$ и можно вычислить r, t

- На последнем шаге Алисы можно вычислить p, q и вектор v

Нелинейные коммутирующие отображения

- $H_p^{\lambda}[x_1, x_2, ..., x_n]$- пространство однородных многочленов степени λ от n переменных над полем Z_p
- $T : Z_p^n \to Z_p^n$ - невырожденное линейное отображение индуцирует невырожденное линейное отображение $T^* : H_p^{\lambda}[x_1, x_2, ..., x_n] \to H_p^{\lambda}[x_1, x_2, ..., x_n]$
- T^*- замена переменных, в алгебре называется симметрической степенью и обозначается $T^* = T^{[\lambda]}$

Нелинейные коммутирующие отображения

- Если T обратимо, то и T^* - обратимо
- Если R, S коммутируют, то и R^*, S^* коммутируют
- Размерность пространства $H_p^{\lambda}[x_1, x_2, ..., x_n]$ равна $N_n^{\lambda} = \begin{pmatrix} n+\lambda-1 \\ \lambda \end{pmatrix} = \frac{(n+\lambda-1)!}{\lambda!(n-1)!}$

Схема реализации протокола с использованием нелинейных коммутирующих отображений

- Выбирается векторное пространство размерности N_p^{λ} и реализуется как $H_p^{\lambda}[x_1, x_2, ..., x_n]$
- Выбирается матрица S и два полинома от матрицы $A = f(S), B = g(S)$
- Матрицы A, B коммутируют, следовательно также коммутируют и A^*, B^*
- Применяем протокол

Пример использования пространства однородных многочленов

- Поле Z_5
- Матрица $S = \begin{pmatrix} 0 & 1 \\ 2 & 2 \end{pmatrix}$ с неприводимым характеристическим многочленом
- Степень однородности $\lambda = 2$, переменных $n = 2$
- Базисом служат x^2, xy, y^2
- Функция $f(x, y) = ax^2 + bxy + cy^2$

Пример использования пространства однородных многочленов

- Вид отображения $S^*(f(x,y))$

$$\begin{cases} x = 0 \cdot u + 1 \cdot v \\ y = 2 \cdot u + 2 \cdot v \end{cases}$$

- Сделаем замену переменных для базиса

$$\begin{cases} x^2 = v^2 \\ xy = 2uv + 2v^2 \\ y^2 = 4u^2 + 3uv + 4v^2 \end{cases}$$

Пример использования пространства однородных многочленов

- Тогда отображение $S^*(f(x,y))$ принимает вид $S^*(f(x,y)) = a \cdot v^2 + b \cdot (2uv + 2v^2) + c \cdot (4u^2 + 3uv + 4v^2) =$

$$= u^2 \cdot 4c + uv \cdot (2b + 3c) + v^2 \cdot (a + 2b + 4c)$$

- $S^*(f(x,y))$ можно сопоставить $\begin{pmatrix} 0 & 0 & 4 \\ 0 & 2 & 3 \\ 1 & 2 & 4 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix}$

Другие варианты реализации с использованием нелинейных отображений

- $\Omega_p^{\lambda}[x_1, x_2, ..., x_n]$- пространство дифференциальных форм порядка λ с постоянными коэффициентами
- $T : Z_p^n \to Z_p^n$ - невырожденное линейное отображение индуцирует невырожденное линейное отображение
  $T^* : \Omega_p^{\lambda}[x_1, x_2, ..., x_n] \to \Omega_p^{\lambda}[x_1, x_2, ..., x_n]$
- В алгебре T^* называется кососимметрической степенью, обозначается $T^* = T^{(\lambda)}$

Другие варианты реализации с использованием нелинейных отображений

- Если T обратимо, то и T^* - обратимо
- Если R, S коммутируют, то и R^*, S^* коммутируют
- Схема применима и при использовании дифференциальных форм

- Рассматривается пространство дифференциальных форм с коэффициентами из пространства однородных полиномов

Пример использования пространства дифференциальных форм

- Поле Z_5
- Матрица $S = \begin{pmatrix} 0 & 0 & 4 \\ 2 & 0 & 0 \\ 0 & 1 & 2 \end{pmatrix}$ с неприводимым характеристическим многочленом

$$\det \begin{pmatrix} -\lambda & 0 & 4 \\ 2 & -\lambda & 0 \\ 0 & 1 & 2-\lambda \end{pmatrix} = \lambda^2(2-\lambda)+8 = -\lambda^3+2\lambda^2+3 = g(\lambda)$$

$$g(0)=3; g(1)=4; g(2)=3; g(3)=4; g(4)=1$$

- Базис $dx \wedge dy, dx \wedge dz, dy \wedge dz$

Пример использования пространства дифференциальных форм

- $S^2 = \begin{pmatrix} 0 & 0 & 4 \\ 2 & 0 & 0 \\ 0 & 1 & 2 \end{pmatrix} \begin{pmatrix} 0 & 0 & 4 \\ 2 & 0 & 0 \\ 0 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 4 & 3 \\ 0 & 0 & 3 \\ 2 & 2 & 4 \end{pmatrix}$
- Произвольный полином от матрицы S имеет вид

$$f(S) = \alpha E + \beta S + \gamma S^2 = \alpha \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} + \beta \begin{pmatrix} 0 & 0 & 4 \\ 2 & 0 & 0 \\ 0 & 1 & 2 \end{pmatrix} + \gamma \begin{pmatrix} 0 & 4 & 3 \\ 0 & 0 & 3 \\ 2 & 2 & 4 \end{pmatrix} =$$

$$= \begin{pmatrix} \alpha & 4\gamma & 4\beta + 3\gamma \\ 2\beta & \alpha & 3\gamma \\ 2\gamma & \beta + 2\gamma & \alpha + 2\beta + 4\gamma \end{pmatrix}$$

Пример использования пространства дифференциальных форм

- Получаем замену переменных

$$\begin{cases} x = \alpha \cdot u + 4\gamma \cdot v + (4\beta + 3\gamma) \cdot w \\ y = 2\beta \cdot u + \alpha \cdot v + 3\gamma \cdot w \\ z = 2\gamma \cdot u + (\beta + 2\gamma) \cdot v + (\alpha + 2\beta + 4\gamma) \cdot w \end{cases}$$

- Вид дифференциалов

$$\begin{cases} dx = \alpha \cdot du + 4\gamma \cdot dv + (4\beta + 3\gamma) \cdot dw \\ dy = 2\beta \cdot du + \alpha dv + 3\gamma \cdot dw \\ dz = 2\gamma \cdot du + (\beta + 2\gamma) \cdot dv + (\alpha + 2\beta + 4\gamma) \cdot dw \end{cases}$$

Пример использования пространства дифференциальных форм

- Учитываем условия

$$du \wedge du = dv \wedge dv = dw \wedge dw = 0$$

$$du \wedge dv = -dv \wedge du$$

$$du \wedge dw = -dw \wedge du$$

$$dv \wedge dw = -dw \wedge dv$$

Пример использования пространства дифференциальных форм

$$dx \wedge dy = (\alpha \cdot du + 4\gamma \cdot dv + (4\beta + 3\gamma) \cdot dw) \wedge$$
$$(2\beta \cdot du + \alpha dv + 3\gamma \cdot dw) = [\alpha^2 - 3\beta\gamma] du \wedge dv +$$
$$+[3\alpha\gamma - 2\beta(4\beta + 3\gamma)] du \wedge dw + [2\gamma^2 - \alpha(4\beta + 3\gamma)] dv \wedge dw$$

$$dx \wedge dz = (\alpha \cdot du + 4\gamma \cdot dv + (4\beta + 3\gamma) \cdot dw) \wedge$$
$$(2\gamma \cdot du + (\beta + 2\gamma) \cdot dv + (\alpha + 2\beta + 4\gamma) \cdot dw) =$$
$$= [\alpha(\beta + 2\gamma) - 3\gamma^2] du \wedge dv + [\alpha(\alpha + 2\beta + 4\gamma) -$$
$$-(4\beta + 3\gamma)2\gamma] du \wedge dw + [4\gamma(\alpha + 2\beta + 4\gamma) -$$
$$-(4\beta + 3\gamma)(\beta + 2\gamma)] dv \wedge dw$$

Пример использования пространства дифференциальных форм

$$dy \wedge dz = (2\beta \cdot du + \alpha dv + 3\gamma \cdot dw) \wedge (2\gamma \cdot du +$$

$$+(\beta + 2\gamma) \cdot dv + (\alpha + 2\beta + 4\gamma) \cdot dw) = [2\beta(\beta + 2\gamma) -$$

$$-2\alpha\gamma]du \wedge dv + [2\beta(\alpha + 2\beta + 4\gamma) - \gamma^2]du \wedge dw +$$

$$+[\alpha(\alpha + 2\beta + 4\gamma) - 3\gamma(\beta + 2\gamma)]dv \wedge dw$$

- Матрица S^* имеет вид

$$S^* = \begin{pmatrix} \alpha^2 - 3\beta\gamma & 3\alpha\gamma - 2\beta(4\beta + 3\gamma) & 2\gamma^2 - \alpha(4\beta + 3\gamma) \\ \alpha(\beta + 2\gamma) - 3\gamma^2 & \alpha(\alpha + 2\beta + 4\gamma) - (4\beta + 3\gamma)2\gamma & 4\gamma(\alpha + 2\beta + 4\gamma) - (4\beta + 3\gamma)(\beta + 2\gamma) \\ 2\beta(\beta + 2\gamma) - 2\alpha\gamma & 2\beta(\alpha + 2\beta + 4\gamma) - \gamma^2 & \alpha(\alpha + 2\beta + 4\gamma) - 3\gamma(\beta + 2\gamma) \end{pmatrix}$$

Пример использования пространства дифференциальных форм

- Если теперь известен вектор $x = (x_1, x_2, x_3)$ на входе и вектор $y = (y_1, y_2, y_3)$ на выходе , то получаем систему уравнений $y = S^* x$ для определения коэффициентов α, β, γ
- Это три квадратичных уравнения для трех неизвестных

Спасибо за внимание!