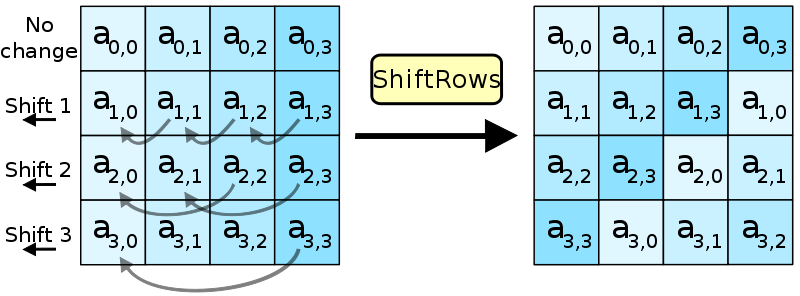
1. Формулировка задачи

Выполнение операции AES ShiftRows над набором из N-матриц. Данные передаются по протоколу TCP.

2. Алгоритм выполнения бизнес-логики

В процедуре ShiftRows байты в каждой строке матрицы циклически сдвигаются влево. Размер смещения байтов каждой строки зависит от её номера. Алгоритм выполнения операции представлен на рисунке 1.

*Рисунок 1 – Алгоритм выполнения операции ShiftRows*

Данный алгоритм применяется для каждой из N матриц.

3. Последовательный вариант исполнения

Исходный код программы-вычислителя представлен в листинге 1.

#include <netdb.h>

#include <netinet/in.h>

#include <stdlib.h>

#include <stdio.h>

#include <string.h>

#include <sys/socket.h>

#include <sys/types.h>

#define PORT 8080

#define SA struct sockaddr

int create() {

int sockfd, connfd, len;

struct sockaddr\_in servaddr, cli;

// socket create and verification

sockfd = socket(AF\_INET, SOCK\_STREAM, 0);

if (sockfd == -1) {

printf("socket creation failed...\n");

exit(0);

}

else

printf("Socket successfully created..\n");

if (setsockopt(sockfd, SOL\_SOCKET, SO\_REUSEADDR, &(int){1}, sizeof(int)) < 0)

printf("setsockport(SO\_REUSEADDR) failed \n");

bzero(&servaddr, sizeof(servaddr));

// assign IP, PORT

servaddr.sin\_family = AF\_INET;

servaddr.sin\_addr.s\_addr = htonl(INADDR\_ANY);

servaddr.sin\_port = htons(PORT);

// Binding newly created socket to given IP and verification

if ((bind(sockfd, (SA\*)&servaddr, sizeof(servaddr))) != 0) {

printf("socket bind failed...\n");

exit(0);

}

else

printf("Socket successfully binded..\n");

// Now server is ready to listen and verification

if ((listen(sockfd, 5)) != 0) {

printf("Listen failed...\n");

exit(0);

}

else

printf("Server listening..\n");

len = sizeof(cli);

// Accept the data packet from client and verification

connfd = accept(sockfd, (SA\*)&cli, &len);

if (connfd < 0) {

printf("server acccept failed...\n");

exit(0);

}

else

printf("server acccept the client...\n");

return connfd;

}

void func(int sockfd)

{

int n = 0;

read(sockfd, &n, sizeof(n));

int width = 0;

read(sockfd, &width, sizeof(width));

int height = 0;

read(sockfd, &height, sizeof(height));

n = ntohl(n);

width = ntohl(width);

height = ntohl(height);

printf("Received header:\n Number of matrices = %d\n Width of each = %d\n Height of each = %d\n", n, width, height);

u\_char \*in = malloc(sizeof(u\_char) \* n \* width \* height);

u\_char \*out = malloc(sizeof(u\_char) \* n \* width \* height);

u\_char buff[height \* width];

for (size\_t i = 0; i < n; i++) {

read(sockfd, in + i \* height \* width, sizeof(buff));

}

process(n, height, width, in, out);

printf("Sending result...\n");

for (size\_t i = 0; i < n; i++) {

write(sockfd, out + i \* height \* width, sizeof(buff));

}

printf("Result send.\n");

free(in);

free(out);

}

void process(int n, int height, int width, u\_char \*in, u\_char \*out) {

printf("Start calculations\n");

int i, j, k;

for(i = 0; i < n; i++) {

for(j = 0; j < height; j++) {

for(k = 0; k < width; k++) {

int current = i \* width \* height + j \* width + k;

if (k + j < width) {

out[current] = in[current + j];

} else {

out[current] = in[current + j - width];

}

}

}

}

printf("Calculations complete\n");

}

// Driver function

int main()

{

int sockfd;

sockfd = create();

func(sockfd);

close(sockfd);

}

Исходный код программы-генератора преведён в листинге 2.

#include <netdb.h>

#include <stdio.h>

#include <stdlib.h>

#include <string.h>

#include <sys/socket.h>

#include <stdbool.h>

#include <time.h>

#include <errno.h>

#include <string.h>

#define SA struct sockaddr

u\_char randomByte()

{

return (u\_char) randInRange( 0, 255 );

}

int randInRange( int min, int max )

{

double scale = 1.0 / (RAND\_MAX + 1);

double range = max - min + 1;

return min + (int) ( rand() \* scale \* range );

}

int create(char\* addr, char\* port) {

int sockfd;

struct sockaddr\_in servaddr, cli;

// socket create and varification

sockfd = socket(AF\_INET, SOCK\_STREAM, 0);

if (sockfd == -1) {

printf("socket creation failed...\n");

exit(0);

}

else

printf("Socket successfully created..\n");

bzero(&servaddr, sizeof(servaddr));

// assign IP, PORT

servaddr.sin\_family = AF\_INET;

servaddr.sin\_addr.s\_addr = inet\_addr(addr);

servaddr.sin\_port = htons(port);

// connect the client socket to server socket

if (connect(sockfd, (SA\*)&servaddr, sizeof(servaddr)) != 0) {

printf("connection with the server failed...\n");

exit(0);

}

else

printf("connected to the server..\n");

return sockfd;

}

void send\_data(int sockfd, int count, int width, int height, int silent)

{

printf("Sending data...");

int n = htonl(count);

write(sockfd, &n, sizeof(n));

int w = htonl(width);

write(sockfd, &w, sizeof(w));

int h = htonl(height);

write(sockfd, &h, sizeof(h));

int sz = width \* height;

u\_char buff[sz];

for(size\_t i = 0; i < count; i++)

{

bzero(buff, sizeof(buff));

for(size\_t j = 0; j < sz; j++)

{

buff[j] = randomByte();

if (!silent) {

if (j % width == 0) {

printf("\n");

}

if (j % sz == 0) {

printf("\n");

}

printf("\t%x", buff[j]);

}

}

write(sockfd, buff, sizeof(buff));

}

printf("\nData have been send.");

}

void receive\_data(int sockfd, int count, int width, int height, int silent) {

int size = width \* height;

u\_char buff[size];

bzero(buff, sizeof(buff));

printf("\nReceiving result...");

u\_char \*in = malloc(sizeof(u\_char) \* count \* width \* height);

for(size\_t i = 0; i < count; i++)

{

read(sockfd, in + i \* size, sizeof(buff));

if (!silent) {

for(size\_t j = 0; j < size; j++) {

if (j % width == 0) {

printf("\n");

}

if (j % size == 0) {

printf("\n");

}

printf("\t%x", in[i \* size + j]);

}

}

}

printf("\nResult received.");

free(in);

}

void save\_report(long int size\_bytes, long int time\_ms) {

FILE \*file;

file = fopen("results.txt", "ab");

if (!file) {

printf("something went wrong: %s", strerror(errno));

exit(1);

}

fprintf(file, "%ld:%ld\n", (long int) size\_bytes, (long int) time\_ms);

fclose(file);

printf("Report saved.\n");

}

int main(int argc, char \*\*argv)

{

int sockfd;

char\* host = argv[1];

int port = atoi(argv[2]);

int count = atoi(argv[3]);

int height = atoi(argv[4]);

int width = atoi(argv[4]);

bool silent = false;

if (argv[5])

silent = true;

sockfd = create(host, port);

clock\_t begin = clock();

send\_data(sockfd, count, width, height, silent);

receive\_data(sockfd, count, width, height, silent);

clock\_t end = clock();

printf("\nElapsed: %ld ms", (long int)(end - begin));

close(sockfd);

printf("\nSocket successfully closed.\n");

save\_report(count \* height \* width, end - begin);

}

График зависимости времени выполнения от размера данных представлен на рисунке 2. Операция проводилась над N матрицами размером 1024x1024, таким образом N – количество данных в Мб. Использовался процессор Intel(R) Core(TM) i5-8500 CPU @ 3.00GHz. Исходные данные для постороения графиков были взяты из сгенерированного файла results.txt. Содержимое файла results.txt приведено в таблице 1.

Таблица 1. Результаты работы программы с последовательным выполнением

|  |  |
| --- | --- |
| Количество данных, Мб | Время выполнения, с |
| 1 | 0.014278 |
| 256 | 2.705722 |
| 512 | 5.534891 |
| 768 | 8.034663 |
| 1024 | 10.726104 |

*Рисунок 2 – График зависимости для варианта программы с последовательным исполнением*