

Министерство науки и высшего образования Российской Федерации
**Федеральное государственное бюджетное образовательное учреждение
высшего образования**
«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»

На правах рукописи

Горелкин Богдан Константинович

**АНАЛИЗ УЯЗВИМОСТЕЙ КРИПТОАЛГОРИТМА RSA ПРИ ЕГО
АППАРАТНОЙ РЕАЛИЗАЦИИ**

Магистерская программа

11.04.02 – «Инфокоммуникационные системы беспроводного широкополосного
доступа»

Автореферат магистерской диссертация
на соискание академической степени магистр

Томск 2020

Работа выполнена на кафедре телекоммуникаций и основ радиотехники
ФГБОУ ВО «Томский Государственный Университет Систем Управления и
Радиоэлектроники»

Научный руководитель:

Рогожников Евгений Васильевич

Кандидат технических наук, доцент кафедры ТОР

Рецензент:

Кандидат технических наук, доцент кафедры

РЭТЭМ

Защита состоится «10» июля 2020 г. на заседании Государственной
комиссии по защите магистерских диссертаций при ФГБОУ ВО «Томский
Государственный Университет Систем Управления и Радиоэлектроники» по адресу:
634050, г. Томск, ул. Вершинина, 47.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы диссертации. Важным аспектом при аппаратной реализации криптографических устройств является защита от утечек информации по сторонним каналам. Со стороны температурного канала на данный момент проведено недостаточно исследований и существует необходимость изучить возможность получения полезных данных по температуре криптографического устройства. Защита от атак по побочным каналам, в настоящее время, является приоритетным направлением исследований в области защиты информации.

Цель и задачи исследования. Целью данной работы является анализ полученных данных от встроенного температурного сенсора в процессе выполнения дешифрования на микроконтроллере STM32F070Rb. Для достижения поставленной цели необходимо выполнить следующие задачи:

1. Рассмотреть угрозы безопасности передаваемых данных.
2. Разобрать принцип работы алгоритма RSA.
3. Исследовать атаки по сторонним каналам.
4. Реализовать экспериментальную установку для получения данных со встроенного температурного датчика процессора STM32.
5. Проанализировать полученные результаты.

Объект и предмет исследования. Объектом исследования является аппаратная реализация криптоалгоритма RSA на плате разработчика Nucleo - STM32F070Rb

Методы исследования. Поставленные задачи были выполнены с использованием систем автоматизированного проектирования, таких как μ Vision IDE – Keil, STM32CubeIDE и Code::Blocks.

Научная новизна и значимость полученных результатов. Ранее извлечение полезных данных по температурному каналу производилось только при помощи дополнительного оборудования. В данной работе используется встроенный температурный сенсор микроконтроллера STM32F070Rb.

Практическая значимость полученных результатов. Результаты диссертационной работы могут повлиять на выбор процессоров, используемых при создании устройств в индустрии «интернета вещей».

Основные положения, выносимые на защиту:

1. Ключ криптографического алгоритма может быть вычислен при помощи данных, собранных по сторонним каналам. В данной работе получены новые экспериментальные данные температуры процессора при дешифровании сообщений микроконтроллером STM32F070Rb,

Личный вклад магистранта. Основные результаты диссертации получены лично автором. Совместно с научным руководителем Рогожниковым Евгением Васильевичем и Sébastien Pillement обсуждалась методология работы.

Моделирование и обработка данных проведены непосредственно автором данной работы

Апробация результатов диссертации. По результатам моделирования работы был сделан доклад на Международной научно-технической конференции «Научная сессия ТУСУР», г. Томск, 2020.

Структура и объем диссертации. Диссертационная работа состоит из 99 страницы, 63 рисунка, 7 таблиц, 47 источников, 4 приложений.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во **введении** показаны сферы применения IoT, а следовательно и исследуемого криптоалгоритма, таким образом обоснована значимость и также отображена актуальность научной работы. Сформулированы цели и задачи исследования.

В **первой главе** приведен теоретический обзор безопасности и конфиденциальности передаваемых/собираемых данных с устройств, приведены основы криптостойкости алгоритмов шифрования, с точки зрения математики.

Во **второй главе** рассмотрен математический аппарат работы RSA алгоритма и приведен пример выполнения всего алгоритма, реализованного на микроконтроллере STM32.

В **третьей главе** рассмотрены атаки на криптографический устройства по сторонним каналам

В **четвертой главе** выполнена классификация атак по сторонним каналам.

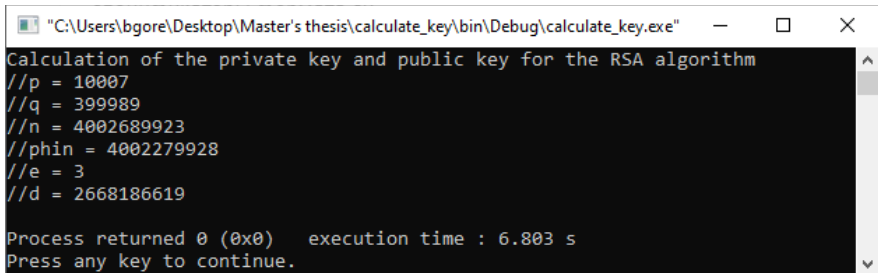
В **пятой главе** совершен литературный обзор по атакам на криптографические устройства со стороны температурного канала

В **шестой главе** описаны процесс получения экспериментальных данных

В **седьмой главе** производится анализ полученных данных

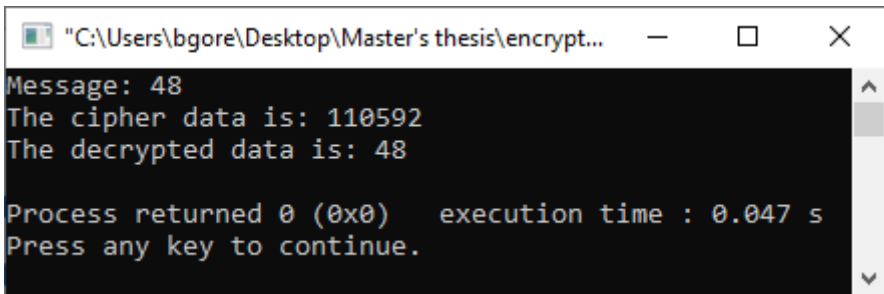
.На рисунке 1 продемонстрированы результаты расчетов параметров ключей для RSA алгоритма при работе с целочисленными типами данных. На рисунке 2

показан результат шифрования символа «0» (48 в десятичном представлении согласно ASCII таблице) рассчитанными ключами,



```
"C:\Users\b gore\Desktop\Master's thesis\calculate_key\bin\Debug\calculate_key.exe"
Calculation of the private key and public key for the RSA algorithm
//p = 10007
//q = 399989
//n = 4002689923
//phin = 4002279928
//e = 3
//d = 2668186619
Process returned 0 (0x0) execution time : 6.803 s
Press any key to continue.
```

Рисунок 1 – Нахождение ключей шифрования



```
"C:\Users\b gore\Desktop\Master's thesis\encrypt..."
Message: 48
The cipher data is: 110592
The decrypted data is: 48
Process returned 0 (0x0) execution time : 0.047 s
Press any key to continue.
```

Рисунок 2 – Результат шифрования

Рисунок 3 демонстрирует получение значений с АЦП при помощи ПДП от температурного датчика дешифрующего устройства, реализованного на STM32.

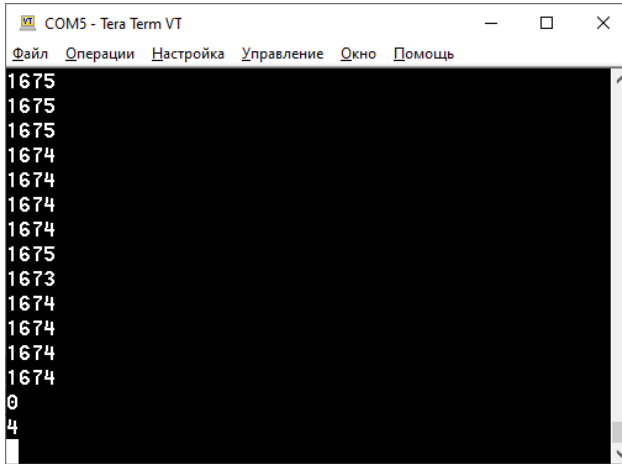


Рисунок 3 – Сравнение выходной мощности

В **пятой главе** производится анализ полученных результатов. На рисунке 4 продемонстрированы усредненные графики роста температуры, при дешифровании целочисленных данных по ключам рисунка из рисунка 1.

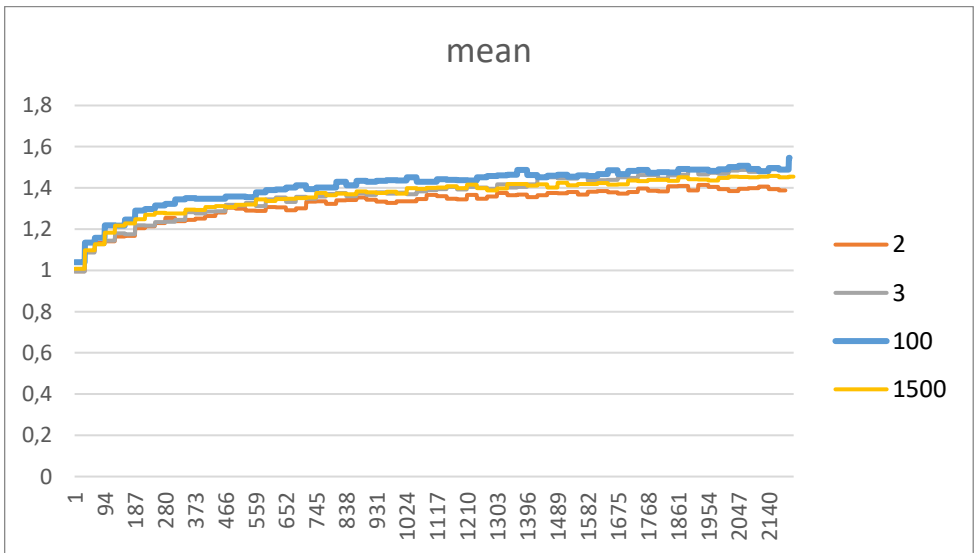


Рисунок 4 – Усредненные значения температуры

В таблице 1 отображены результаты шифрования символов 0-9 при использовании различных ключей. Рисунки 5-8 демонстрируют изменения температуры процессора при дешифровании сообщений таблицы 1..

Таблица 1 – Шифрование данных таблицы 5.1 разными ключами

Experiment		1	2	3	4
p		11	103	4993	10007
q		13	107	4999	10009
n		143	11021	24960007	100160063
$\varphi(n)$		120	10812	24950016	100140048
e		7	5	5	5
d		103	4325	19960013	60084029
Symbol	ASCII	Encrypted data			
0	48	126	9469	5203898	54483842
1	49	36	7019	7915172	82155123
2	50	41	10566	12979916	12019811
3	51	116	1825	20545160	44545062
4	52	13	1574	5803927	79723843
5	53	92	3648	18835381	17555241
6	54	76	8122	9884898	58524772
7	55	55	10410	4084235	2484060
8	56	56	1385	1611622	49931461
9	57	73	562	2651889	731679

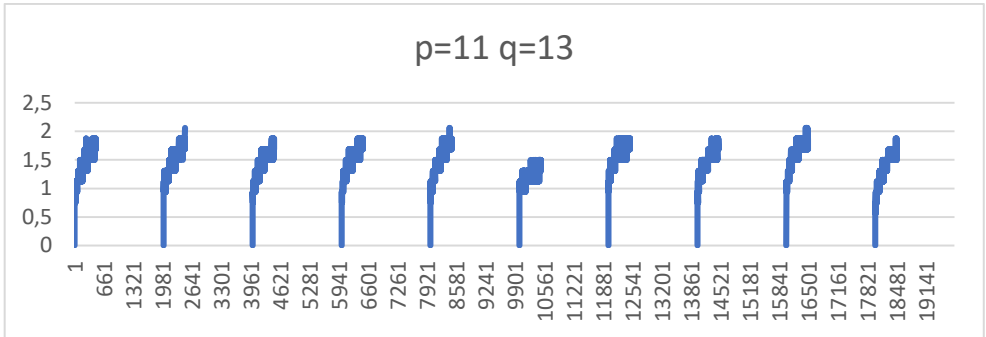


Рисунок 5– Графики роста температуры при $p=11 \quad q=13$

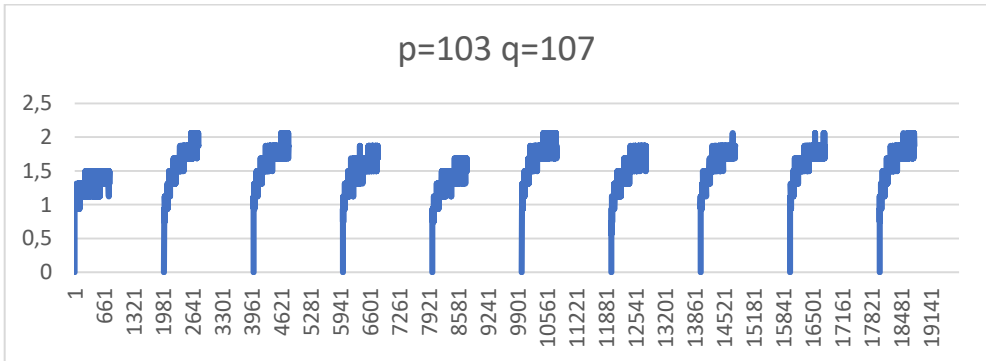


Рисунок 6 – Графики роста температуры при $p=103 \quad q=107$

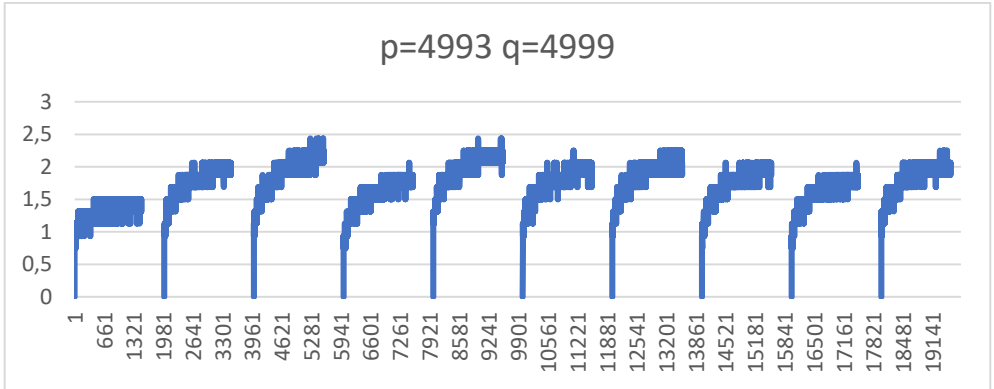


Рисунок 7 – Графики роста температуры при $p=4993$ $q=4999$

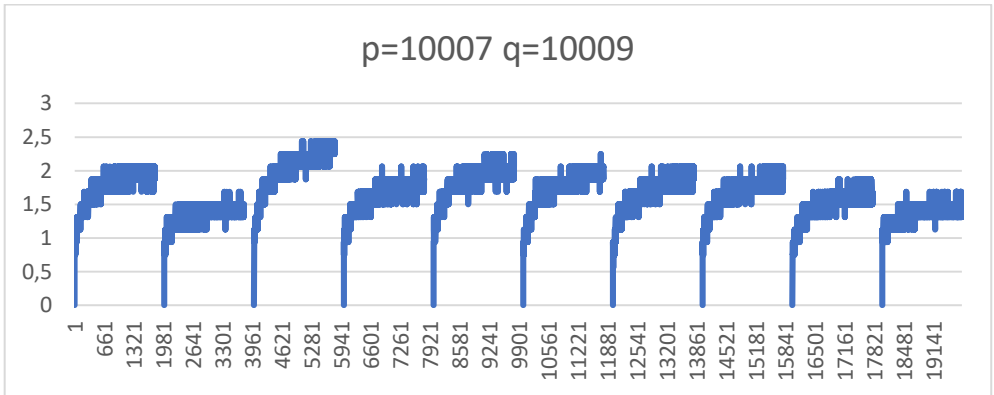


Рисунок 8 – Графики роста температуры при $p=10007$ $q=10009$

Рисунок 9 демонстрирует схему подключения осциллографа к Nucleo – STM32F070Rb для измерения тока, потребляемого процессором в режиме ожидания (Рисунок 10).

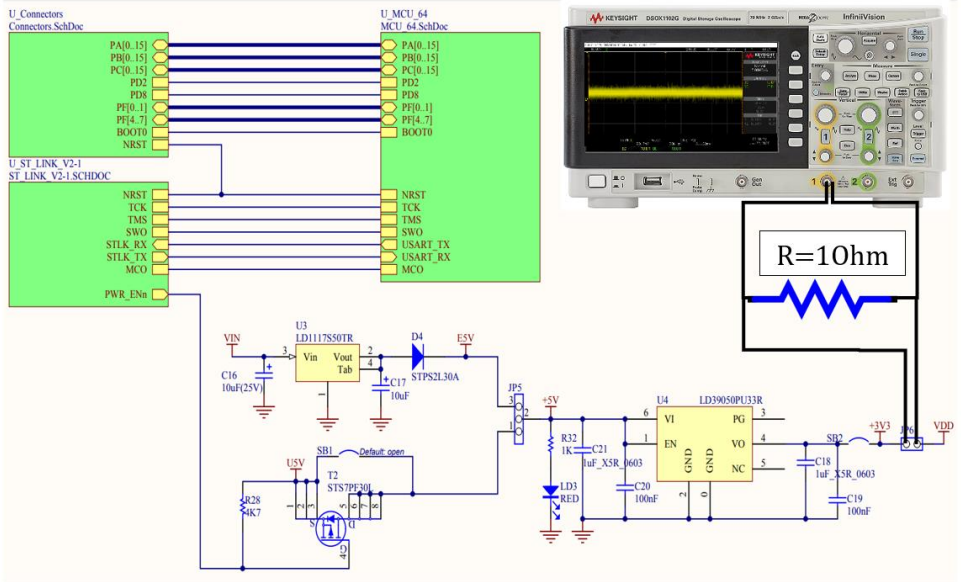


Рисунок 9 – Схема измерения потребляемого тока процессором

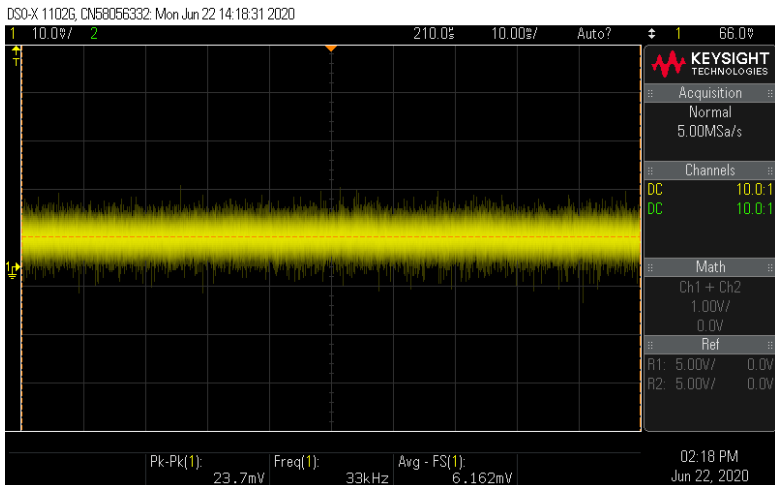


Рисунок 10 – Потребляемый ток процессором в режиме ожидания

В таблице 2 показано изменение температуры и потребляемого тока, в зависимости от данных, которые дешифруются.

Таблица 2 – Изменение температуры и потребляемого тока при дешифровании

№	Шифруемые значения	Дешифруемые значения	Изменение температуры	Потребляемый ток	Количество полученных измерений
1	2	8	1,59	20,352	2191
2	3	27	1,59	20,886	2200
3	100	1000000	1,64	21,087	2204
4	1500	375000000	1,54	20,842	2216
5	4002689921	4002689915	1,59	20,538	2208
6	4002689920	4002689896	1,59	20,595	2205
7	133964360	2147483647	1,59	20,341	2222
8	1024	1073741824	1,49	19,647	2210

Рисунок 11 показывает зависимость температуры процессора от потребляемого тока.

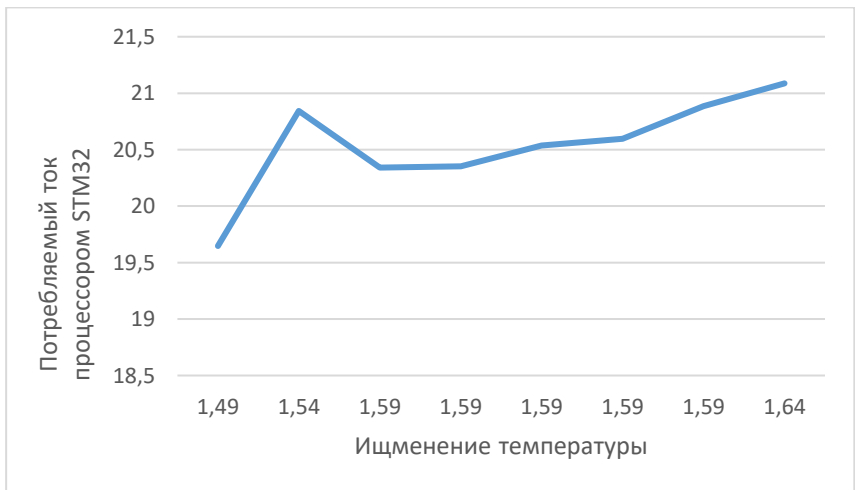


Рисунок 11 – Зависимость температуры от потребляемого тока процессором

ВЫВОДЫ

При аппаратной реализации любого криптографического устройства, даже с самым математически сложным криптоалгоритмом, невозможно избежать утечки информации по побочным каналам. Однако данную информацию можно сделать неразборчивой и предотвратить несанкционированный доступ. Так, встроенный температурный датчик можно использовать не только в корыстных целях, но и для предотвращения несанкционированного доступа. К криптографическому устройству можно добавить защитный алгоритм, который срабатывает при изменении температуры, когда повышается вероятность извлечения ключей шифрования.

Уязвимость RSA, на данный момент, обусловлена не алгоритмом, а его практической реализацией. При использовании больших ключей с математической точки зрения требуется большое количество усилий и ресурсов для факторизации полупростого числа. Однако использование сторонних данных, возникающих в процессе выполнения алгоритма на устройстве, могут позволить злоумышленнику извлечь полезную информацию и получить ключи шифрования даже самого сложного алгоритма.

При пассивной атаке на температурный канал криптографического устройства извлечь ключи шифрования не предоставляется возможным, однако температурный анализ устройства в совокупности с другими сторонними каналами может помочь извлечь ключи шифрования. Так, например, при атаке по времени вычислений в совокупности с температурным каналом можно выяснить, вносились ли специальная задержка вычислений для защиты от атак по времени или нет.

Активные атаки по температурному каналу уже были исследованы []. При активных атаках удалось успешно извлечь ключи шифрования RSA на основе ошибочных вычислений. В исследованиях Michael Hutter и Jorn-Marc Schmidt в 2014 году был использован внешний температурный датчик, который нарушал целостность процессора. Использование встроенных датчиков температуры для

подобного рода атак может быть более перспективным, т.к. визуальная целостность устройства не будет нарушена.

В целом, необходимо подчеркнуть, что решения по безопасности для Internet of Things еще не полностью изучены. По мере развития технологии и ее роли в современном мире, необходимо продолжать научные исследования и предлагать современные решения, способные улучшить ситуацию в сфере безопасности интернета вещей.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1. Горелкин Б.К., Рогожников Е.В. Алгоритм асимметричного шифрования rsa на микроконтроллере stm32f070rb// «Научная сессия ТУСУР – 2020» (Томск, 25-27 мая 2020 г.)// В печати.