ТЕХНОЛОГИИ СОЗДАНИЯ И ПРИМЕНЕНИЕ ВЫЧИСЛИТЕЛЬНЫХ ОШИБОК В МИКРОКОНТРОЛЛЕРЕ, РЕАЛИЗУЮЩЕМ КРИПТОГРАФИЧЕСКИЙ АЛГОРИТМ RSA

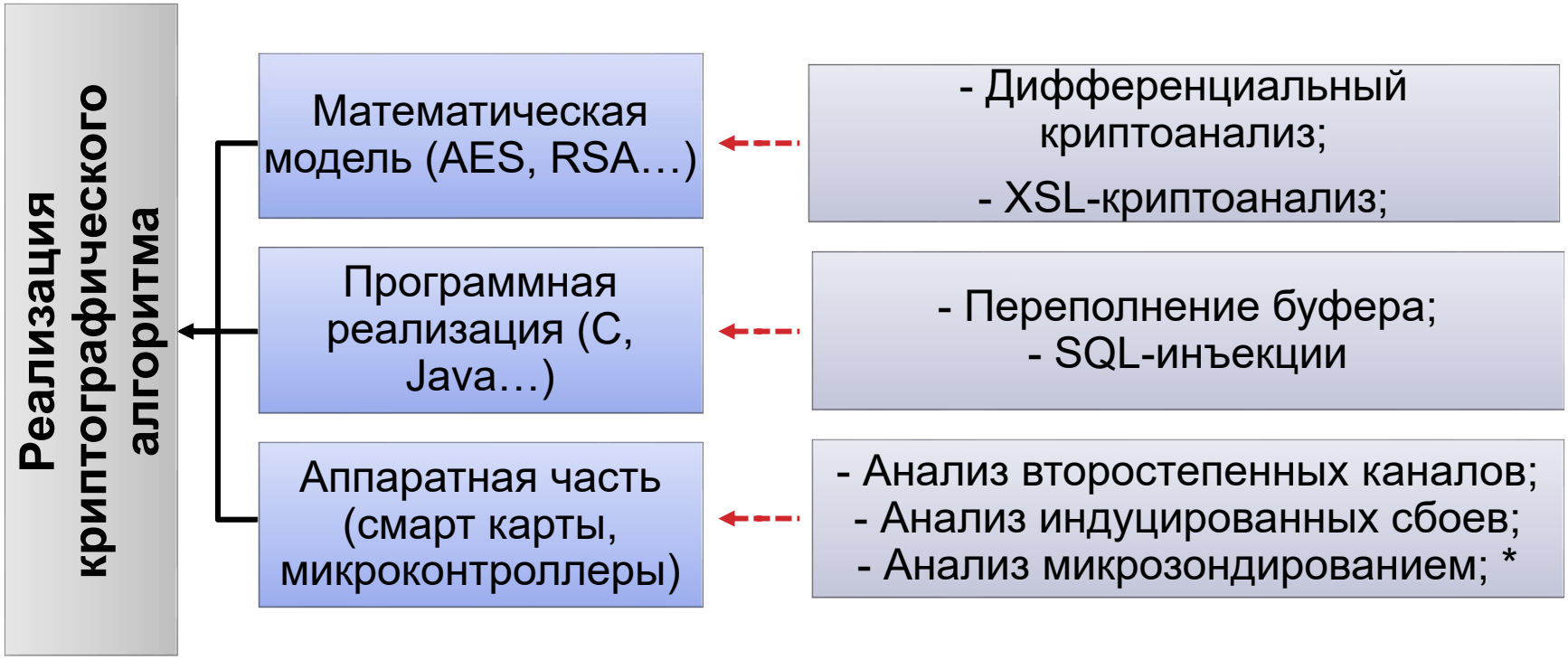
Елена Васильевна Тришина, эксперт по безопасности компании STMicroelectronics, Rousset, elena.trichina@orange.fr

Роман Геворкович Коркикян, аспирант Санкт Петербургского государственного университета телекоммуникаций им. Проф. М.А. Бонч Бруевича, стажер компании STMicroelectronics, Rousset, korkikjan@gmail.com

Научный руководитель: Леонид Георгиевич Осовецкий, д.т.н., профессор, зам. декана по науке факультета информационных систем и технологий, Санкт-Петербургский государственный университет телекоммуникаций им.проф.М.А.Бонч-Бруевича, leoned.osovetsky@gmail.Com

СОДЕРЖАНИЕ

ОБОБЩЕННАЯ СХЕМА ПРОГРАММНЫХ РЕАЛИЗАЦИЙ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ

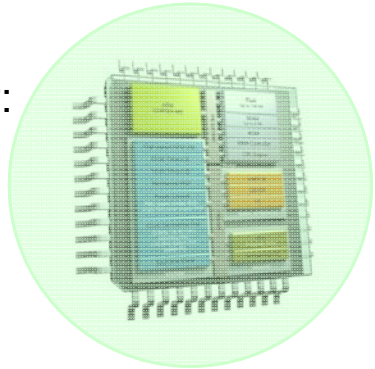


* Данная классификация используется в лекциях профессора Renauld Pacalet университета Eurecom http://soc.eurecom.fr/HWSec/. Русский вариант терминов был взят со статьи Б. Киви, Что показало вскрытие // Хакер-спец, №(11)36, 2003, с. 56-61.

АНАЛИЗ ИНДУЦИРОВАННЫХ СБОЕВ. ОБЩЕЕ ОПИСАНИЕ

Нормальные внешние условия

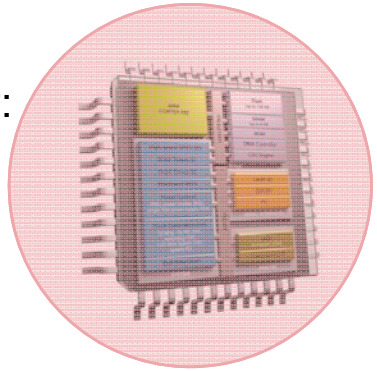
Исходный текст:
A1 0B C9 75



Шифротекст:
18 C9 01 56

Экстремальные внешние условия

Исходный текст:
A1 0B C9 75



Шифротекст:
18 D8 01 47

Изображение взято с сайта http://catalog.gaw.ru/

АНАЛИЗ ИНДУЦИРОВАННЫХ СБОЕВ. ОБЩЕЕ ОПИСАНИЕ

- **Было показано, что ключи некоторых криптографических алгоритмов могут быть вычислены, если в определенный момент времени удается создать необходимую ошибку:**
  - **Изменение *бита*:** E.Biham and A.Shamir, *Differential fault analysis of secret key cryptosystems*, 1997
  - **Изменение *одного или нескольких байт*:** G. Piret and J.-J. Quisquater, *A differential fault attack technique against SPN structures, with application to the AES and KHAZAD*, 2003
  - ***Произвольная ошибка*:** D. Boneh, R.A. Demillo, R.J. Lipton, *On the importance of checking cryptographic protocols for faults*, 1997
  - …
- **«Практичность» анализа индуцированных сбоев была подтверждена работами:**
  - M.Agoyan et al., *Single-bit DFA using multiple-byte laser fault injection*, 2010
  - C. Aumulle et al., *Fault attacks on RSA with CRT: concrete results and practical countermeasures*, 2002
  - A. Barenghi et al. *Low voltage fault attacks to AES and RSA on general purpose processors*, 2010
  - …

СОДЕРЖАНИЕ

АНАЛИЗ ИНДУЦИРОВАННЫХ СБОЕВ. ЦЕЛЬ РАБОТЫ

- **Цель - проверить возможность введения ошибок в современный микроконтроллер общего назначения с 32х битной логикой;**
- **Акцент на возможности введения нескольких ошибок за время одной операции шифрования (дешифровки), так как это бы позволило обойти некоторые систем защиты;**
- **Был выбран шифр RSA, реализованный с помощью китайской теореме об остатках, так как эта реализация позволяет увеличить скорость работы примерно в 4 раза*. Также из-за большой длины ключа алгоритм RSA часто реализован именно программным способов.**
- **Необходимо было найти секретный ключ алгоритма RSA (d,p,q), используемый для *дешифровки* сообщения.**

* J.-J. Quisquater and C. Couvreur. Fast decipherment algorithm for RSA public-key cryptosystem. *IEE Electronics Letters*, 18(21), pp. 905–907, 1982.

СОДЕРЖАНИЕ

1. Метод индуцированных сбоев.
2. Постановка задачи.
3. **Алгоритм CRT-RSA, способ его анализа, защита от метода индуцированных сбоев (6 слайдов).**
4. Описание микроконтроллера и оборудования.
5. Создание вычислительных ошибок с помощью лазера.
6. Создание вычислительных ошибок с помощью генератора импульсов.

ШИФР RSA

Алгоритм создания открытого и секретного ключей:

1. **Выбрать два простых числа p и q.**
2. **Вычислить их произведение $N = pq$, называемое модулем.**
3. **Вычислить значение функции Эйлера $\varphi(N) = (p-1)(q-1)$.**
4. **Выбрать число e ($1 < e < \varphi(N)$), взаимно простое с $\varphi(N)$.**
5. **Вычислить число d: $de = 1 \pmod{\varphi(N)}$.**

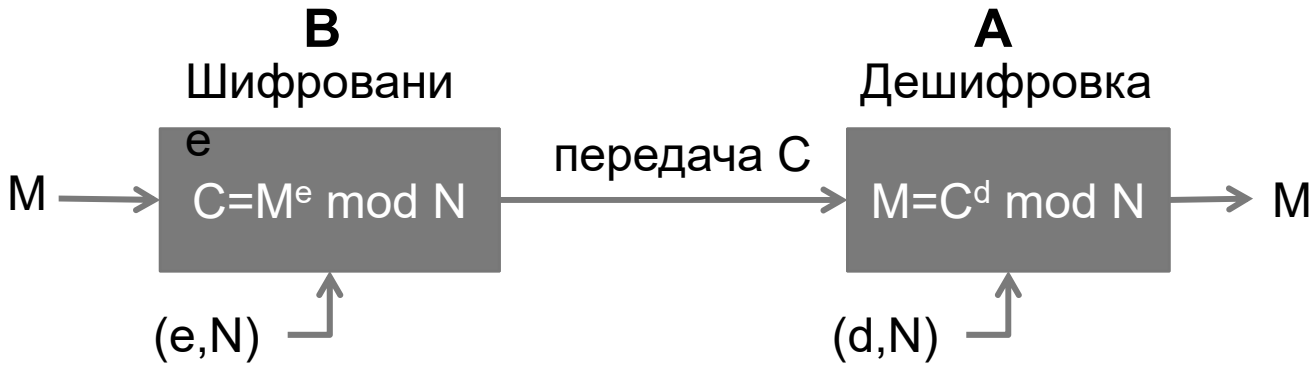
Пара (e,N) публикуется в качестве открытого ключа RSA.

Пара (d,N) играет роль секретного ключа RSA.

ШИФР RSA

Схема RSA

Отправка сообщения *M* от стороны B к стороне A:



Шифрование

1. Берется открытый ключ (*e,N*)
2. Вычисляется значение
$$C = M^e \bmod N$$
3. Значение C передается на сторону A

Дешифровка

1. На основании полученного значения C и секретного ключа (*d,N*) вычисляется:
$$M = C^d \bmod N$$

ШИФР RSA, РЕАЛИЗОВАННЫЙ С ПОМОЩЬЮ КИТАЙСКОЙ ТЕОРЕМЫ ОБ ОСТАТКАХ

- **Вычисление $M = C^d \bmod N$ очень ресурсоемкая операция, поэтому в 1982 был предложен метод*, позволяющий ускорить выполнение этой операции примерно в 4 раза. Он основан на китайской теореме об остатках (Chinese Reminder Theorem), поэтому такая реализация алгоритма носит название CRT RSA:**

$$M_p = C^{d \bmod (p-1)} (\bmod p)$$

$$M_q = C^{d \bmod (q-1)} (\bmod q)$$

$$M = (M_p \cdot q \cdot (q^{-1} \bmod p) + M_q \cdot p \cdot (p^{-1} \bmod q)) (\bmod N)$$

* J.-J. Quisquater and C. Couvreur. Fast decipherment algorithm for RSA public-key cryptosystem. *IEE Electronics Letters*, 18(21), pp. 905–907, 1982.

ШИФР RSA, РЕАЛИЗОВАННЫЙ С ПОМОЩЬЮ КИТАЙСКОЙ ТЕОРЕМЫ ОБ ОСТАТКАХ. МЕТОД АНАЛИЗА*

Правильная операция дешифровки

$$M_p = C^{d \bmod (p-1)} (\bmod p)$$

$$M_q = C^{d \bmod (q-1)} (\bmod q)$$

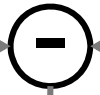
$$M = (M_p \cdot q \cdot (q^{-1} \bmod p) + M_q \cdot p \cdot (p^{-1} \bmod q)) (\bmod N)$$

Операция дешифровки, с ошибкой

$$M'_p = C^{d \bmod (p-1)} (\bmod p)$$

$$M_q = C^{d \bmod (q-1)} (\bmod q)$$

$$M' = (M'_p \cdot q \cdot (q^{-1} \bmod p) + M_q \cdot p \cdot (p^{-1} \bmod q)) (\bmod N)$$



$$M - M' = (M_p - M'_p) \cdot q \cdot (q^{-1} \bmod p) (\bmod N)$$

$$GCD((M - M'), N) = GCD(((M_p - M'_p) \cdot q \cdot (q^{-1} \bmod p)), pq) = q$$

* JD. Boneh, R.A. Demillo, R.J. Lipton, *On the importance of checking cryptographic protocols for faults*, 1997

ЗАЩИТА АЛГОРИТМА CRT RSA ОСНОВАННАЯ НА СРАВНЕНИИ*.

Математическое выражение	Описание
$M_p = C^{d \bmod (p-1)} (\bmod p)$ $M_q = C^{d \bmod (q-1)} (\bmod q)$ $M = (M_p \cdot q \cdot (q^{-1} \bmod p) +$ $+ M_q \cdot p \cdot (p^{-1} \bmod q)) (\bmod N)$	Стандартная дешифровка сообщения C.
$e_p = d_p^{-1} \bmod (p-1)$ $e_q = d_q^{-1} \bmod (q-1)$ $C_p = M^{e_q} \bmod p$ $C_q = M^{e_p} \bmod q$ $C' = \left((C_p - C_q) \cdot i_q \cdot \bmod p\right) q + C_q$	Повторное вычисление исходного сообщения (операция занимает мало времени из за длины e) для сравнения
if C' == C then *return M* *else* *return ErrorMessage;*	Сравнение исходного и заново рассчитанного сообщения.

* A. Boscher, H. Handschuh, and E. Trichina, "Fault resistant RSA Signatures: Chinese Remaindering in both directions," 2010. http://eprint.iacr.org

ШИФР RSA, РЕАЛИЗОВАННЫЙ С ПОМОЩЬЮ КИТАЙСКОЙ ТЕОРЕМЫ ОБ ОСТАТКАХ

- **Впервые этот метод был описан в статье: D. Boneh, R.A. Demillo, R.J. Lipton, *On the importance of checking cryptographic protocols for faults*, 1997**
- **Создав произвольную вычислительную ошибку во время операции дешифровки CRT RSA, злоумышленник может вычислить оба простых числа, образующих модуль N.**
- **В 1999 году было показано*, что злоумышленнику не обязательно знать правильный результат дешифровки.**
- **Насколько практична эта атака мы попытались понять в нашем исследовании.**

* M. Joye, A.K. Lenstra, J.-J. Quisquater, Chinese remaindering based cryptosystems in the presence of faults // Journal of Cryptology, vol. 12, no. 4, 1999, pp. 241-245

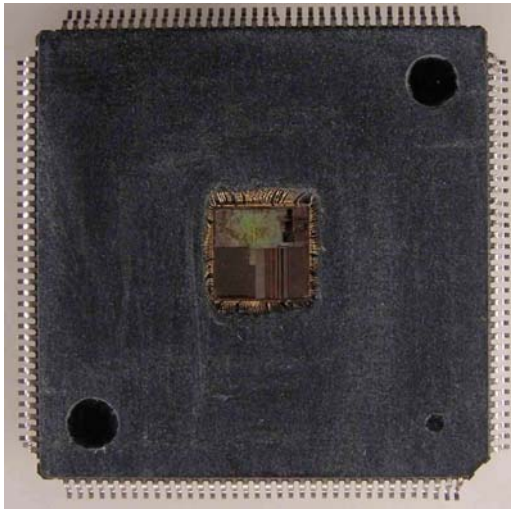
СОДЕРЖАНИЕ

1. Метод индуцированных сбоев.
2. Постановка задачи.
3. Алгоритм CRT-RSA, способ его анализа, защита от метода индуцированных сбоев.
4. **Описание микроконтроллера и оборудования (7 слайдов).**
5. Создание вычислительных ошибок с помощью лазера.
6. Создание вычислительных ошибок с помощью генератора импульсов.

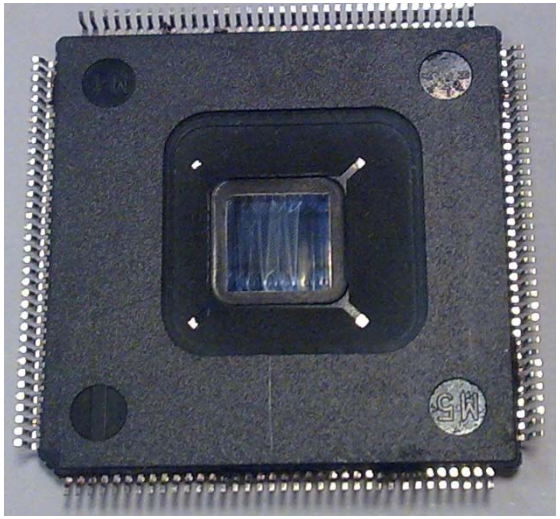
ОПИСАНИЕ МИКРОКОНТРОЛЛЕРА

- **Основан на ARM Cortex-M3, 32х битная логика, 130нм технологический процесс;**
- **512 Кб Flash, 64 Кб SRAM, различная периферия (АЦП, USB, I^2C, таймеры и др.);**
- **Внутренний независимый осциллятор, система мониторинга питания, система прерываний;**
- **Является микроконтроллером общего назначения;**

Фронтальная поверхность



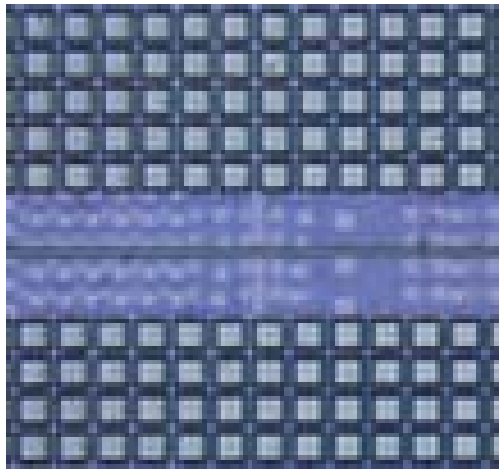
Задняя поверхность

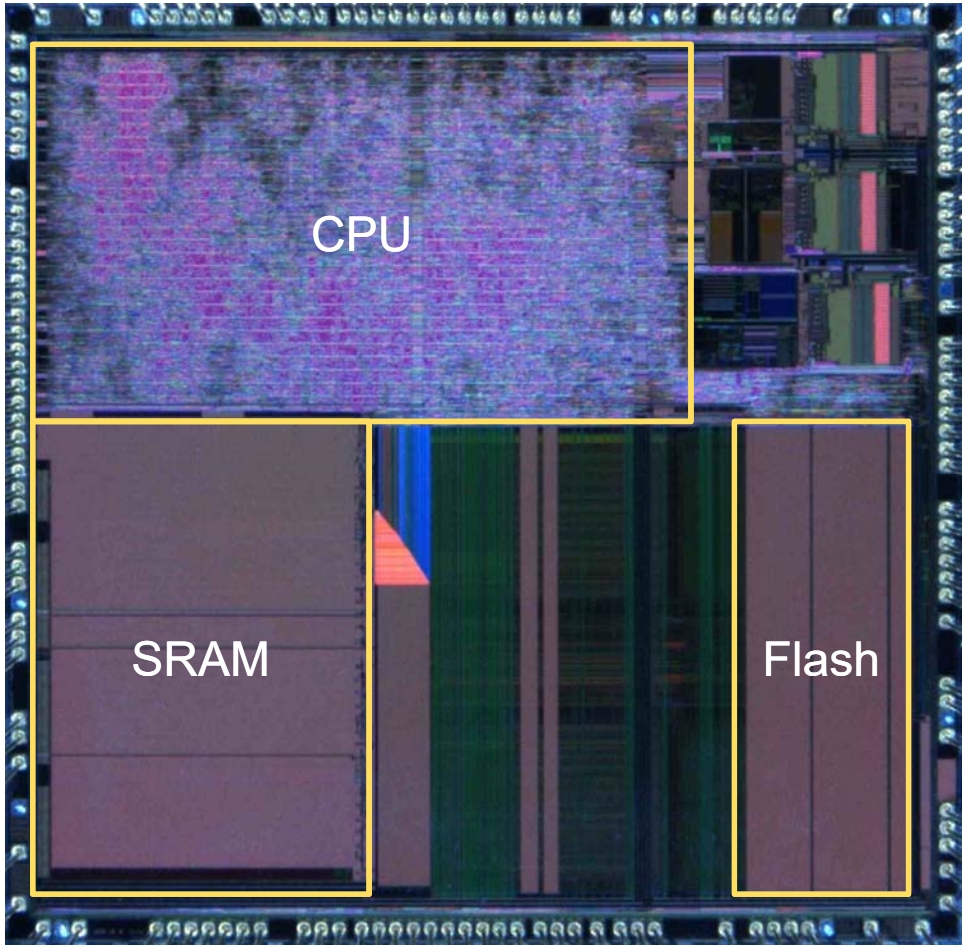


* Декапсуляция чипа проводилась в лаборатории CMP Charpak, Gardanne, France. Химическая (фронтальная часть) с помощью аппарата JetEtch II, механическая (задняя поверхность) с помощью аппарата ASAP-1

ОПИСАНИЕ МИКРОКОНТРОЛЛЕРА

- **Ядро выполнено таким образом, что невозможно понять его составляющие;**
- **Области памяти покрыты металлическими ячейками;**



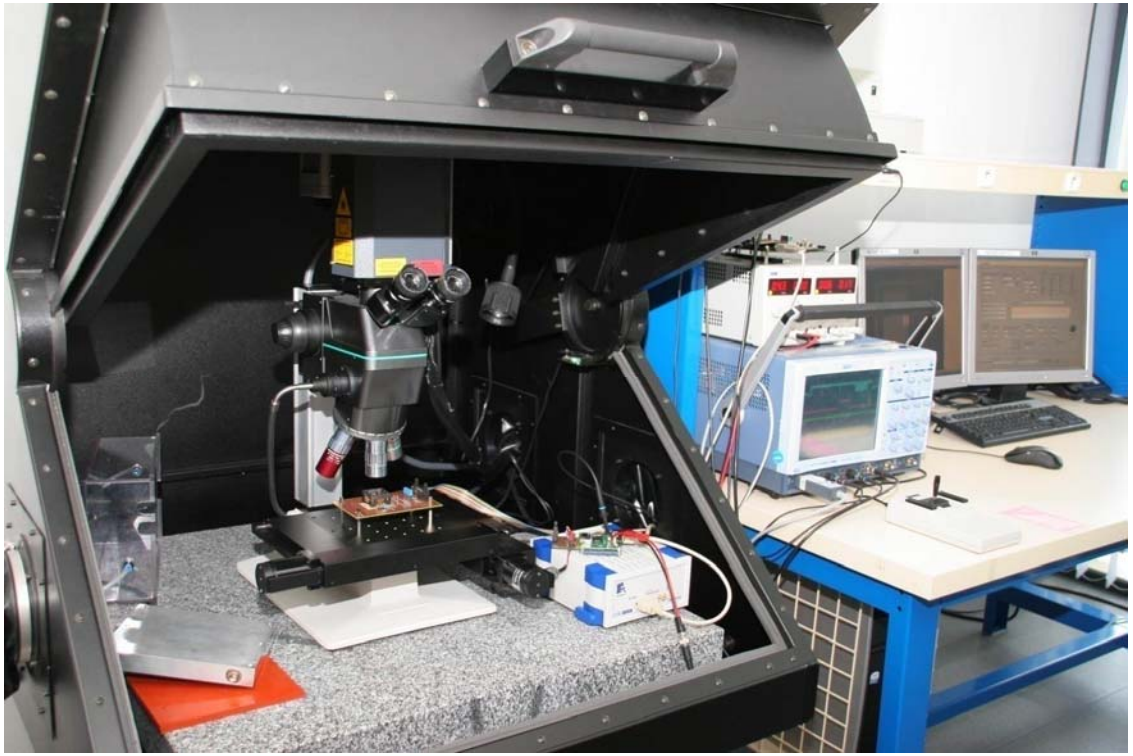


ЛАЗЕРНАЯ УСТАНОВКА. ОБЩИЕ СВЕДЕНИЯ

- Все эксперименты проводились в центре микроэлектроники CMP Charpak, Gardanne, Франция.
- Один из способов введения ошибок в микроконтроллер – облучение его с помощью лазера (фотоэлектронный и термический эффекты);
- Длина волны и другие параметры лазера зависят от используемых технологий и метода создания ошибок (если есть доступ к кремниевому слою, то обычно используется инфракрасный лазер, если нет, то, возможно, лазер зеленого спектра);
- В нашем случае мы опробовали оба метода (облучение верхнего слоя микроконтроллера и облучение его кремниевого слоя). Так как облучению подвергалась одна и та же зона, то ошибки были одинаковыми;

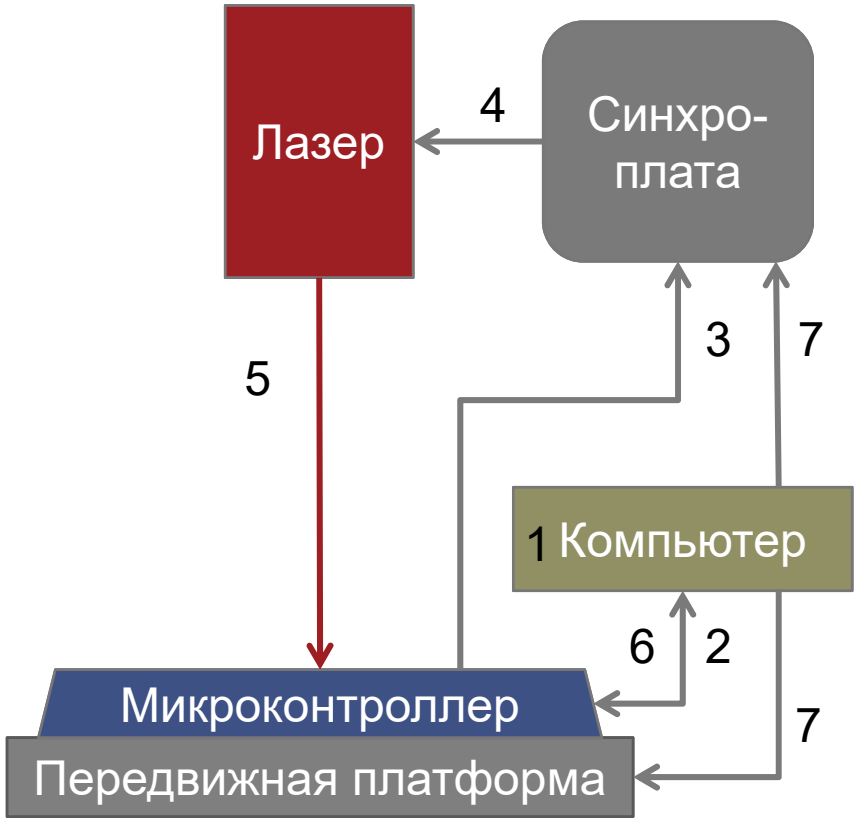
ЛАЗЕРНАЯ УСТАНОВКА. ОБЩИЕ СВЕДЕНИЯ

- **Оборудование:**
  - Лазер (зеленый, инфракрасный) с различными линзами увеличения;
  - Осциллограф (10 ГГц);
  - Подвижная платформа (шаг 1мкм);
  - Компьютер, синхро-плата;
- **Диаметр зоны, облучаемой лазером может устанавливаться от 0 до 2500 мкм.**
- **Время воздействия лазера 5 нс.**
- **Использовали 20x - 100x увеличение и диаметр зоны лазера от 5.5 мкм (размер чипа 4x4 мм).**



ЛАЗЕРНАЯ УСТАНОВКА. ПРИНЦИП РАБОТЫ

1. **Все оборудование подключено и готово к работе (микроконтроллер ждет исходного текста от компьютера);**
2. **Компьютер посылает исходный текст на чип;**
3. **Чип начинает выполнение алгоритма и в определенный момент времени создает триггер на одном из своих выходов, который посылается на синхро-плату;**
4. **После получения сигнала от микроконтроллера, синхно-плата с заранее заданной задержкой генерирует сигнал для лазера;**
5. **Лазер распознает сигнал от синхро-платы и выстреливает, после выстрела сразу начинает перезаряжаться;**
6. **Чип заканчивает вычисления и отправляет результат обратно на компьютер, который сохраняется;**
7. **Компьютер изменяет значение задержки на синхро-плате, меняет положение платформы (если задано) и алгоритм возвращается на шаг 1.**

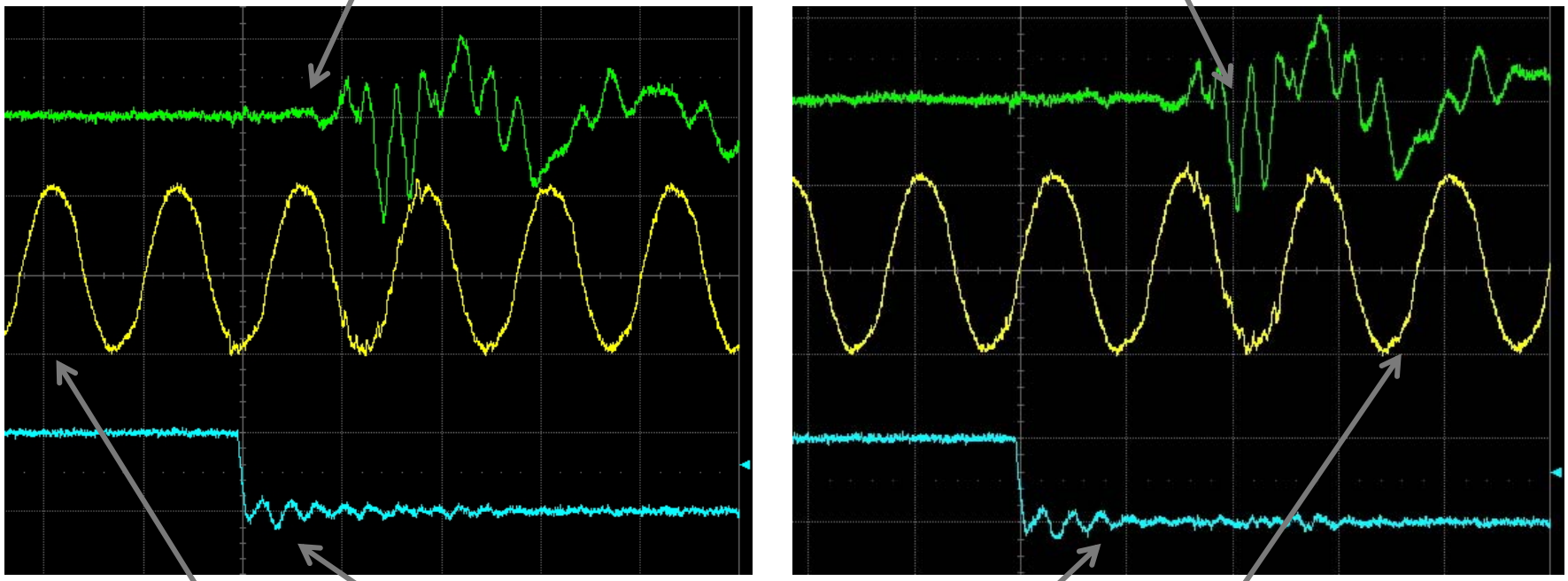


ЛАЗЕРНАЯ УСТАНОВКА. ПРИНЦИП РАБОТЫ

- Начало всех вычислений на микроконтроллере регистрируется с помощью триггера на одном из его выходов;
- Различные задержки триггера от синхро-платы нужны для того, чтобы облучать чип во время выполнения различных инструкций (необходимо найти ту, которая даст нужную ошибку);
- Подвижная платформа необходима для того, чтобы автоматически перемещать чип и облучать различные части микроконтроллера, так как поиск уязвимой зоны это самое сложное;
- Время задержки и область перемещения платформы задаются на компьютере, поэтому после запуска эксперимента необходимо лишь следить за тем, чтобы чип не завис и оборудование работало исправно (можно контролировать с помощью осциллоскопа).

ЛАЗЕРНАЯ УСТАНОВКА. ДАННЫЕ С ОСЦИЛЛОСКОПА

Сигнал, помогающий регистрировать непосредственное излучение лазера



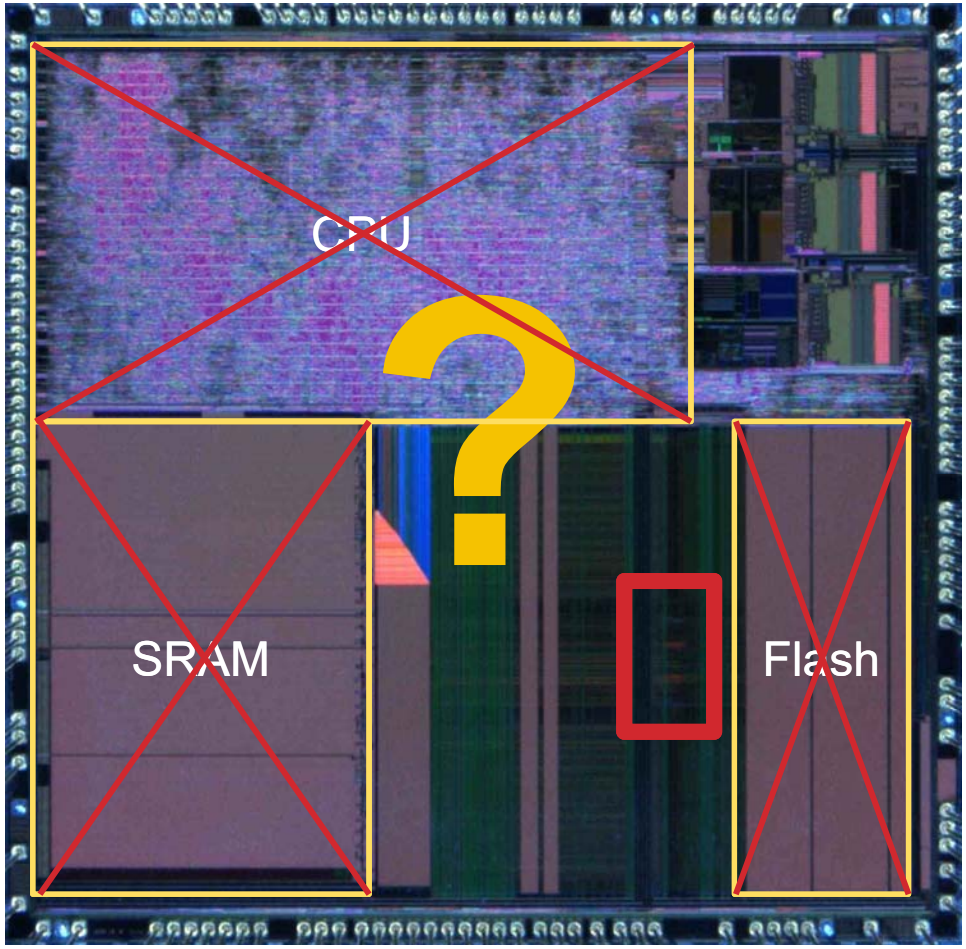
Триггер на выходе чипа

Тактовый сигнал (синхросигнал) 8 МГц

СОДЕРЖАНИЕ

СОЗДАНИЕ ВЫЧИСЛИТЕЛЬНОЙ ОШИБКИ. ОБЛАСТЬ ОБЛУЧЕНИЯ

- Какую часть чипа нужно облучить, чтобы получить вычислительную ошибку?
- Область CPU – чип зависал или перегорал;
- Область памяти – ни одной ошибки;
- После нескольких месяцев была обнаружена область, облучение которой приводит к ошибкам. Область занимает 0.125% от поверхности чипа.



СОЗДАНИЕ ВЫЧИСЛИТЕЛЬНОЙ ОШИБКИ. ТИПЫ ОШИБОК

- **На практике удалось получить следующие типы ошибок:**
  - Изменение одного байта переменной;
  - Изменение нескольких байт переменной (в том числе и переменной, использующейся для сдвига в области памяти);
  - Пропуск инструкции;
- **Этих типов ошибок было достаточно, чтобы успешно вычислить ключа алгоритма CRT RSA, разработанного без защиты от введения сбоев;**

ШИФР RSA, РЕАЛИЗОВАННЫЙ С ПОМОЩЬЮ КИТАЙСКОЙ ТЕОРЕМЫ ОБ ОСТАТКАХ. МЕТОД АНАЛИЗА*

Правильная операция дешифровки

$$M_p = C^{d \bmod (p-1)} (\bmod p)$$

$$M_q = C^{d \bmod (q-1)} (\bmod q)$$

$$M = (M_p \cdot q \cdot (q^{-1} \bmod p) + M_q \cdot p \cdot (p^{-1} \bmod q)) (\bmod N)$$

Операция дешифровки, с ошибкой

$$M'_p = C^{d \bmod (p-1)} (\bmod p)$$

$$M_q = C^{d \bmod (q-1)} (\bmod q)$$

$$M' = (M'_p \cdot q \cdot (q^{-1} \bmod p) + M_q \cdot p \cdot (p^{-1} \bmod q)) (\bmod N)$$

$$M - M' = (M_p - M'_p) \cdot q \cdot (q^{-1} \bmod p) (\bmod N)$$

$$GCD((M - M'), N) = GCD(((M_p - M'_p) \cdot q \cdot (q^{-1} \bmod p)), pq) = q$$

* JD. Boneh, R.A. Demillo, R.J. Lipton, *On the importance of checking cryptographic protocols for faults*, 1997

ПРИМЕР УСПЕШНОГО СОЗДАНИЯ ВЫЧИСЛИТЕЛЬНОЙ ОШИБКИ

Данные об операции дешифровки алгоритма CRT RSA 512, представленные в шестнадцатеричной форме

Исходный шифротекст =

```
12 9D 1B F0 A5 29 A7 2E D6 06 6F 35 4D 7E 50 8F
51 3A 70 51 FA 7C 97 A9 63 74 04 03 24 97 9C E1
53 F6 53 35 AB DE 30 45 17 7B F2 EE DF FF 18 A5
12 3B 8B 42 6B 74 9A 4B 20 8D 0D 18 4E 7A F8 B0
```

Дешифровка сообщения с ошибкой №1

```
4B E2 61 70 9F B7 70 25 62 2A 01 5F 90 8C BD 8D
DD 8D E4 1E 30 9D 68 AD 84 62 2C 33 8E 47 21 22
64 1D ED B6 42 1F 94 87 FA CF 6D 72 64 40 FF 56
21 0F C3 50 AB 91 0D 8A 95 DD 08 57 A0 B4 F2 1B
```

Правильно дешифрованное сообщение =

```
3A 7A 11 F7 04 FE 17 AD 5A BB 2D A1 18 6A 01 F6
41 41 54 66 1D 1E 17 47 10 E0 65 FA 31 A7 2E A9
0B FF 04 54 5E 15 3B 9F 28 89 07 E8 0B 84 17 81
76 12 7D 28 4B ED 5A 18 62 47 07 3C 1E 2E 3D 79
```

Дешифровка сообщения с ошибкой №2

```
11 5A AD CC 3E 9A B2 B8 93 1B 8E 61 B7 F9 7F C2
A6 FA B3 A8 2B 64 2C CE 63 80 84 F6 46 3F 6F FF
EC 93 B8 73 1A 35 11 E7 8B 7E 78 80 B9 8D 75 97
AE EF DF 84 3C C1 84 39 D6 51 71 D2 9B 7D 18 B3
```

Модуль N

```
51 68 A0 CC 86 A1 38 90 71 E8 83 44 C2 87 F0 67
D9 A5 10 40 0C B7 5D 3D 47 B3 4C FA EE F0 97 60
F6 36 25 F4 78 DD 39 AD 7C E0 64 CD 3F EC EE DB
0A B7 22 FF E6 35 AA 18 E0 23 B6 A8 E9 2B 72 7D
```

Открытое значение e

```
01 00 01
```

ЗАЩИТА АЛГОРИТМА CRT RSA ОСНОВАННАЯ НА СРАВНЕНИИ*.

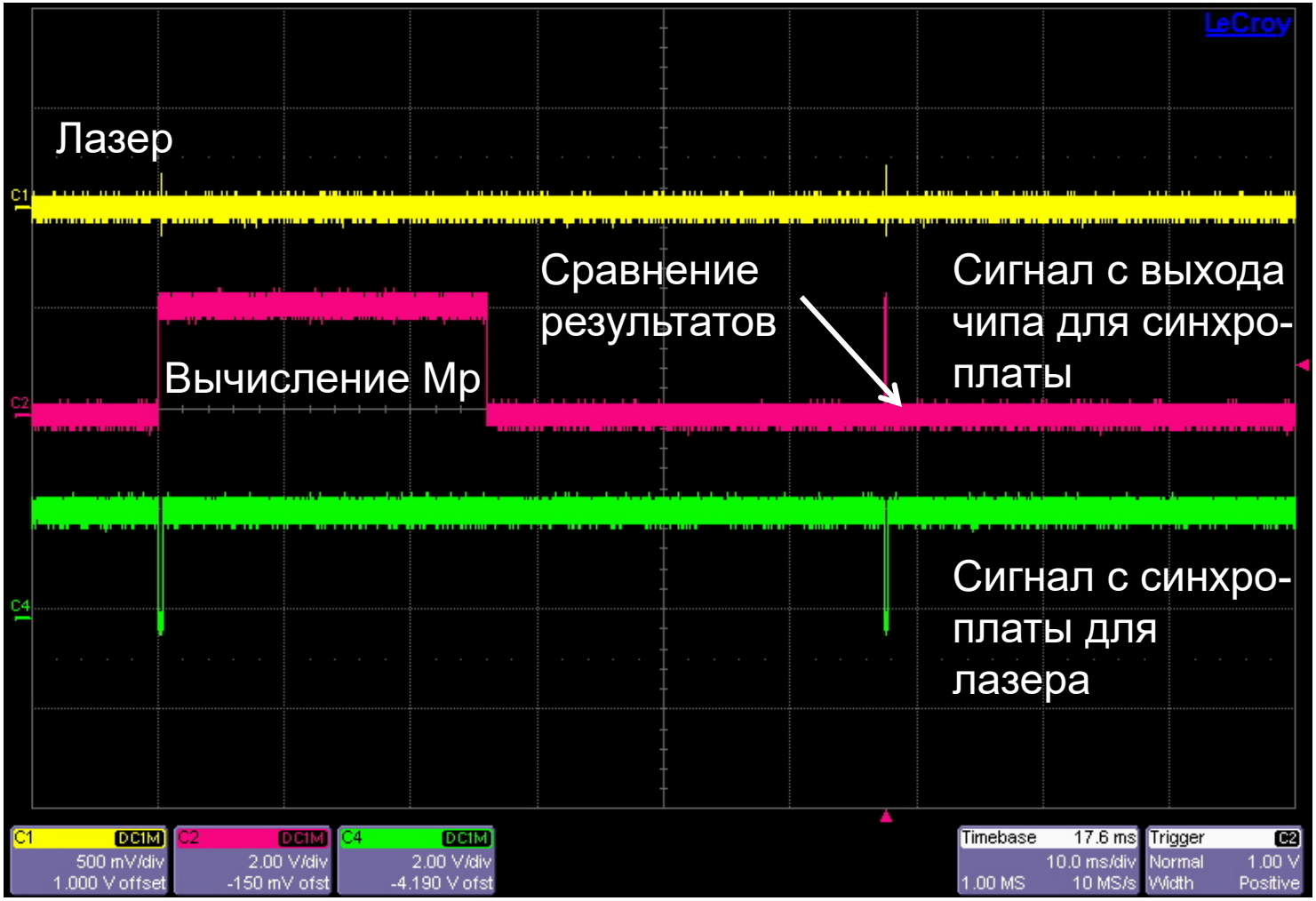
Математическое выражение	Описание
$M_p = C^{d \bmod (p-1)} (\bmod p)$ $M_q = C^{d \bmod (q-1)} (\bmod q)$ $M = (M_p \cdot q \cdot (q^{-1} \bmod p) +$ $+ M_q \cdot p \cdot (p^{-1} \bmod q)) (\bmod N)$	Стандартная дешифровка сообщения C.
$e_p = d_p^{-1} \bmod (p-1)$ $e_q = d_q^{-1} \bmod (q-1)$ $C_p = M^{e_q} \bmod p$ $C_q = M^{e_p} \bmod q$ $C' = \left((C_p - C_q) \cdot i_q \cdot \bmod p\right) q + C_q$	Повторное вычисление исходного сообщения (операция занимает мало времени из за длины e) для сравнения
if C' == C then *return M* *else* *return ErrorMessage;*	Сравнение исходного и заново рассчитанного сообщения.

* A. Boscher, H. Handschuh, and E. Trichina, "Fault resistant RSA Signatures: Chinese Remaindering in both directions," 2010. http://eprint.iacr.org

ЗАЩИТА АЛГОРИТМА CRT RSA ОСНОВАННАЯ НА СРАВНЕНИИ. КОД

```
0x08001160 A9FD      ADD      r1,sp,#0x3F4
0x08001162 A82B      ADD      r0,sp,#0xAC
0x08001164 F000F881  BL.W     CompareBig (0x0800126A)
   509:                  if (i == 0)     {
   510:                   /* write to vector of char */
0x08001168 B930      CBNZ     r0,0x08001178
   511:                           W32_to_W8(m.w,P_pOutput,P_pPrivCRTKey->modulus_size);
   512:                  } else {
0x0800116A 4639      MOV      r1,r7
0x0800116C F1060008  ADD      r0,r6,#0x08
0x08001170 6822      LDR      r2,[r4,#0x00]
0x08001172 F000FCF8  BL.W     W32_to_W8 (0x08001B66)
0x08001176 E003      B        0x08001180
   513:                            printf("Fault %d\n",i);
   514:                  }
   515:          }
0x08001178 4601      MOV      r1,r0
0x0800117A A004      ADR      r0,{pc}+2  ; @0x0800118C
0x0800117C F002FC24  BL.W     __1printf (0x080039C8)
```

ЗАЩИТА АЛГОРИТМА CRA RSA ОСНОВАННАЯ НА СРАВНЕНИИ. ПРИМЕР ЭКСПЕРИМЕНТА



ЗАЩИТА АЛГОРИТМА CRA RSA ОСНОВАННАЯ НА СРАВНЕНИИ. РЕЗУЛЬТАТЫ

- **Типы ошибок, которые удалось получить в результате облучения лазером поверхности микроконтроллера, позволили обойти защиту, основанную на сравнении;**
- **Сложность в том, что первая ошибка изменяет значение Mp, поэтому время выполнения всего алгоритма тоже изменяется, и, как следствие, изменяется момент сравнения результатов. Это усложняет работу злоумышленника.**

ВЫВОДЫ ПО РЕЗУЛЬТАТАМ РАБОТЫ С ЛАЗЕРОМ

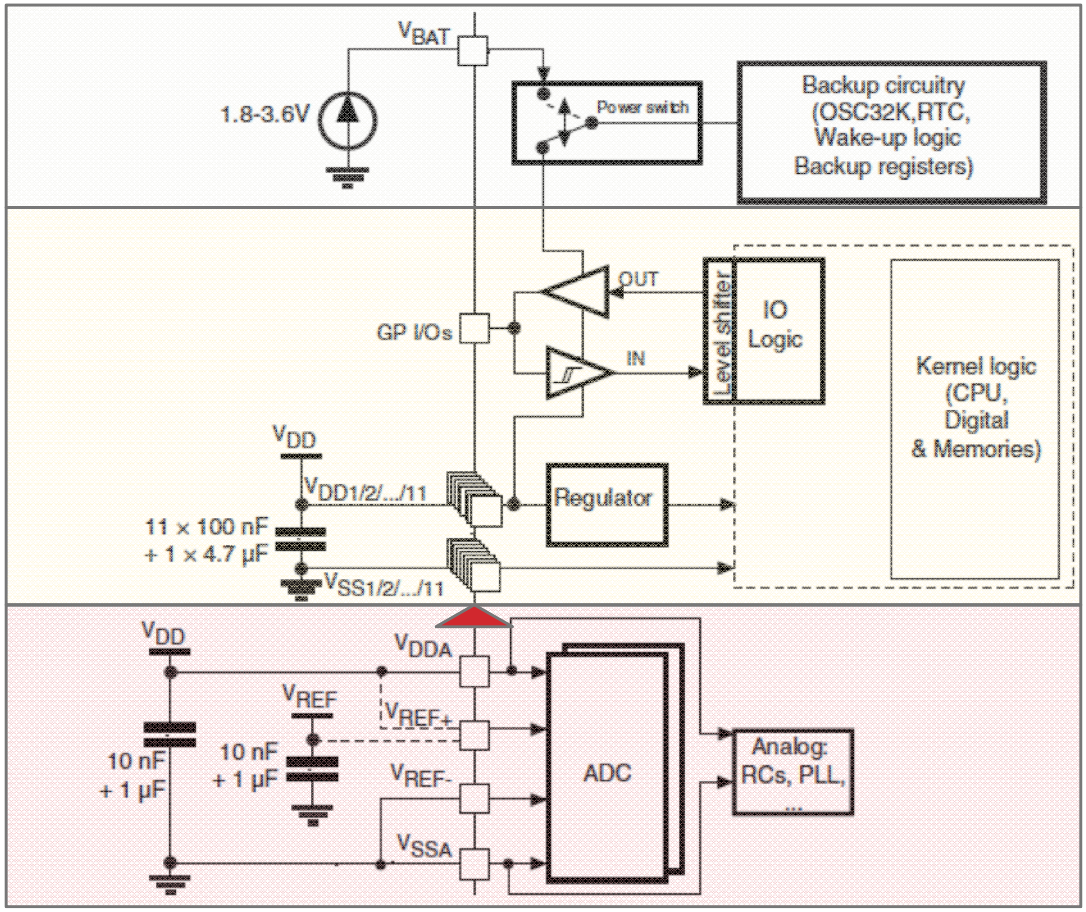
- **Было доказано, что секретный ключ алгоритма CRT RSA, может быть найден, если в микроконтроллер, выполняющий операцию дешифровки, удается ввести произвольную вычислительную ошибку;**
- **Используемые современные технологии производства микроконтроллеров усложняют, но полностью не исключают метод индуцированных сбоев;**
- **Программная защита, основанная на сравнении, может быть преодолена с помощью двух введенных ошибок за одну операцию дешифровки;**
- **Необходимо использовать другие системы защиты;**

СОДЕРЖАНИЕ

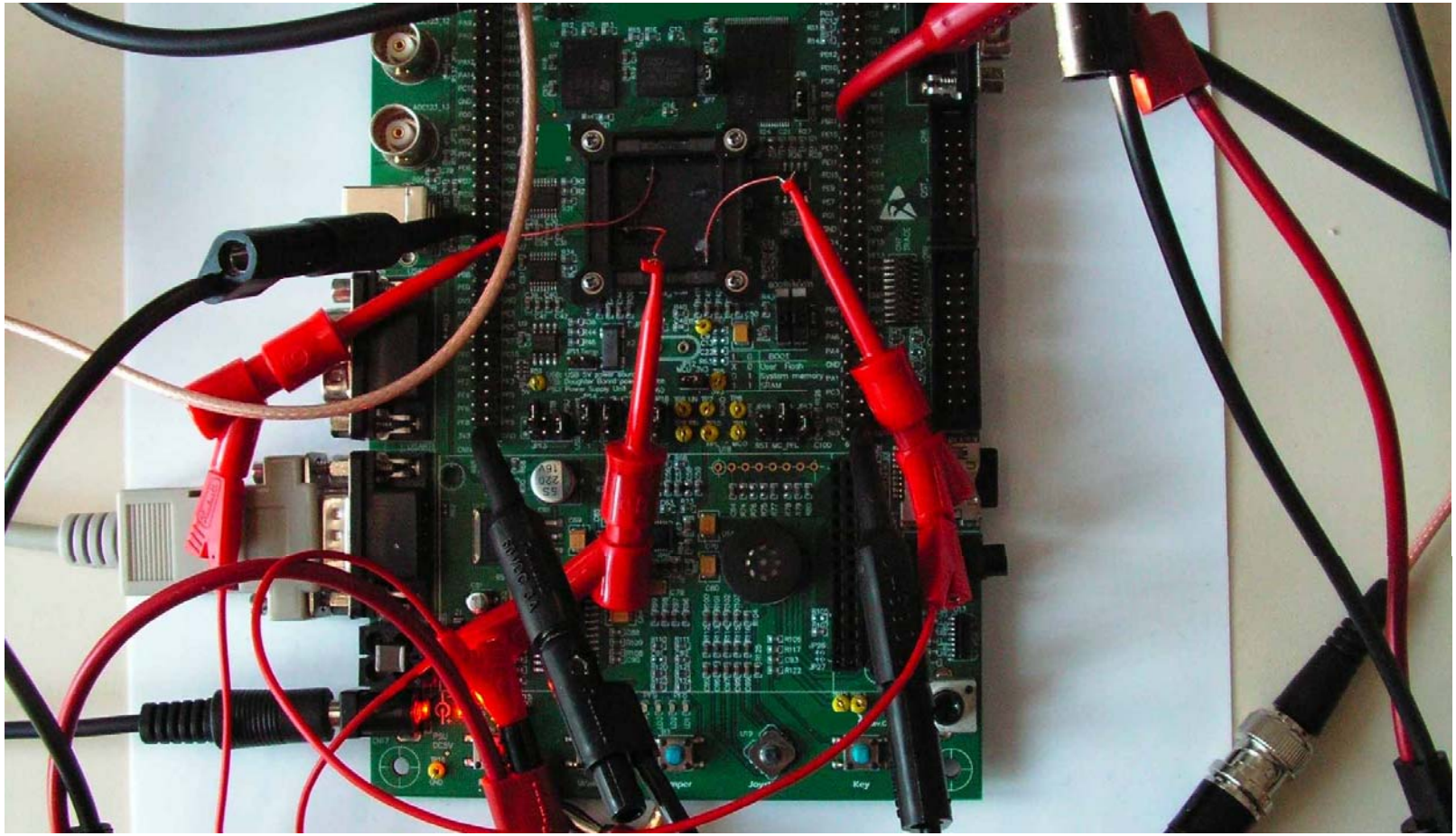
1. Метод индуцированных сбоев.
2. Постановка задачи.
3. Алгоритм CRT-RSA, способ его анализа, защита от метода индуцированных сбоев.
4. Описание микроконтроллера и оборудования.
5. Создание вычислительных ошибок с помощью лазера.
6. **Создание вычислительных ошибок с помощью генератора импульсов (8 слайдов).**

СИСТЕМА ПИТАНИЯ МИКРОКОНТРОЛЛЕРА. ОБЩЕЕ ОПИСАНИЕ

- Система питания может быть условно разбита на три части: резервная, цифровая и аналоговая;
- Согласно документации напряжение в цифровой области от 2.4 до 3.6 В.
- Мониторинг питания ведется в цифровой области;
- По результатам анализа было обнаружено, что цифровая и аналоговая зоны связаны между собой с помощью диода;
- Если цифровая область питается на уровне 1.7 В все равно ошибок не наблюдается;

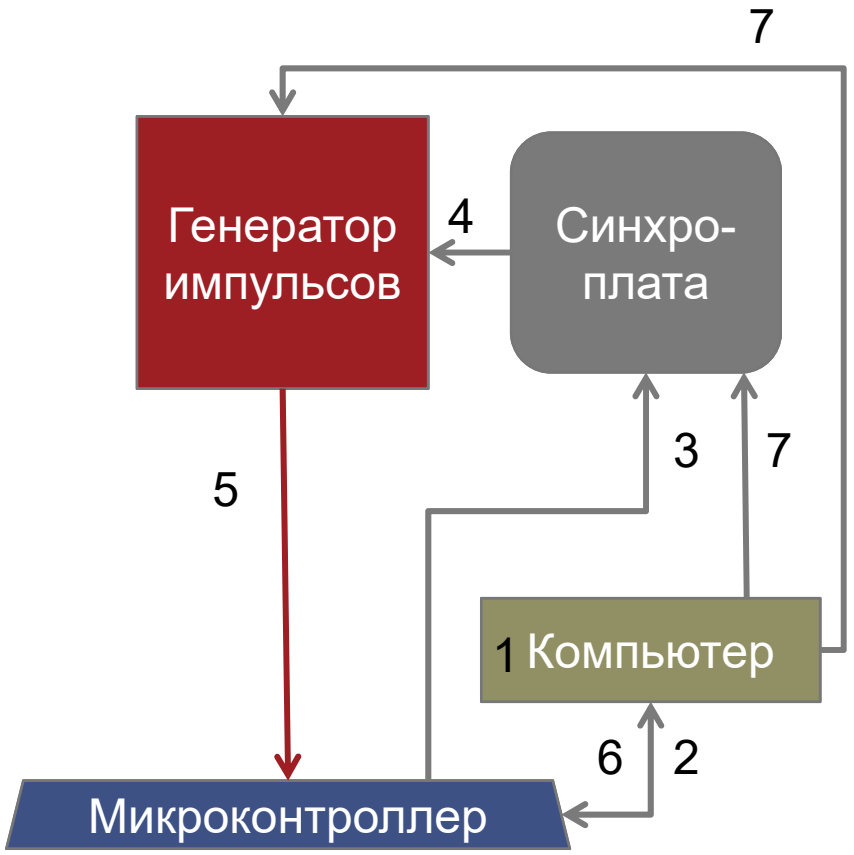


ОПИСАНИЕ УСТАНОВКИ. ВНЕШНИЙ ВИД СИСТЕМЫ



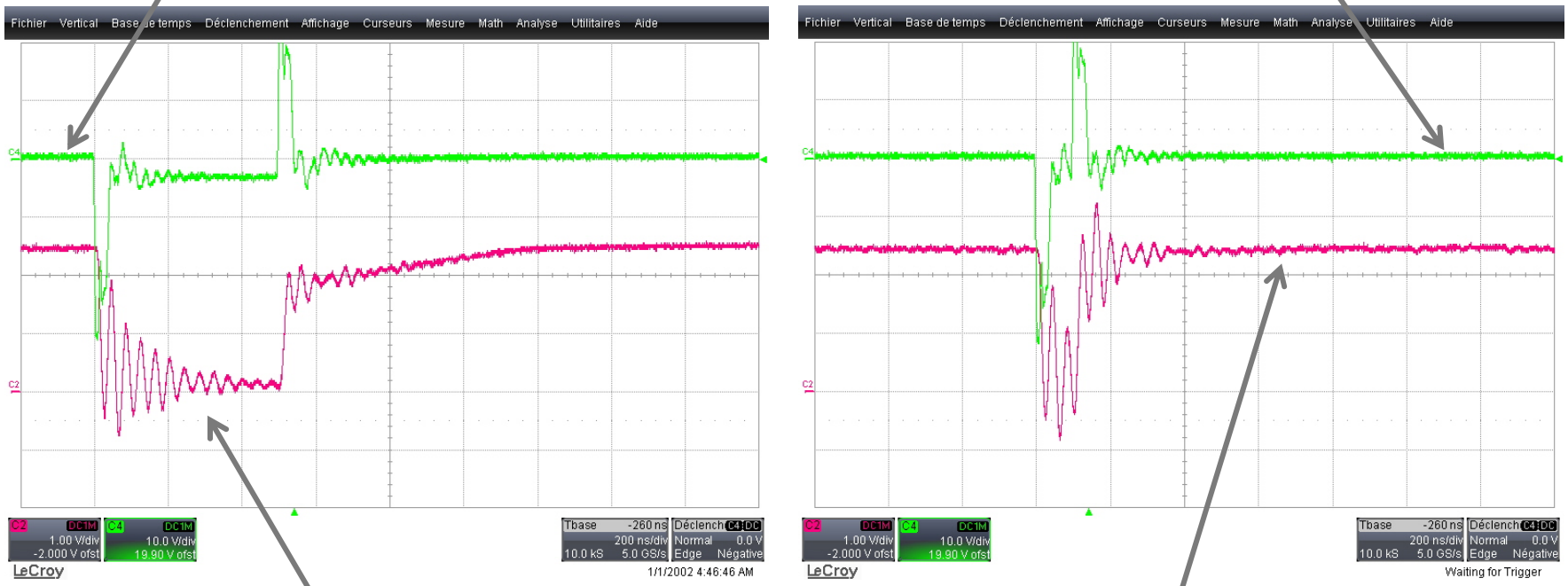
ИМПУЛЬСНАЯ УСТАНОВКА. ПРИНЦИП РАБОТЫ

1. **Все оборудование подключено и готово к работе (микроконтроллер ждет исходного текста от компьютера);**
2. **Компьютер посылает исходный текст на чип;**
3. **Чип начинает выполнение алгоритма и в определенный момент времени создает триггер на одном из своих выходов, который посылается на синхро-плату;**
4. **После получения сигнала от микроконтроллера, синхно-плата с заранее заданной задержкой генерирует сигнал для генератора импульсов;**
5. **Генератор импульсов распознает сигнал от синхро-платы и создает импульс;**
6. **Чип заканчивает вычисления и отправляет результат обратно на компьютер, который сохраняется;**
7. **Компьютер изменяет значение задержки на синхро-плате, меняет значение импульса и алгоритм возвращается на шаг 1.**



ПРИМЕР СОЗДАНИЯ ИМПУЛЬСА

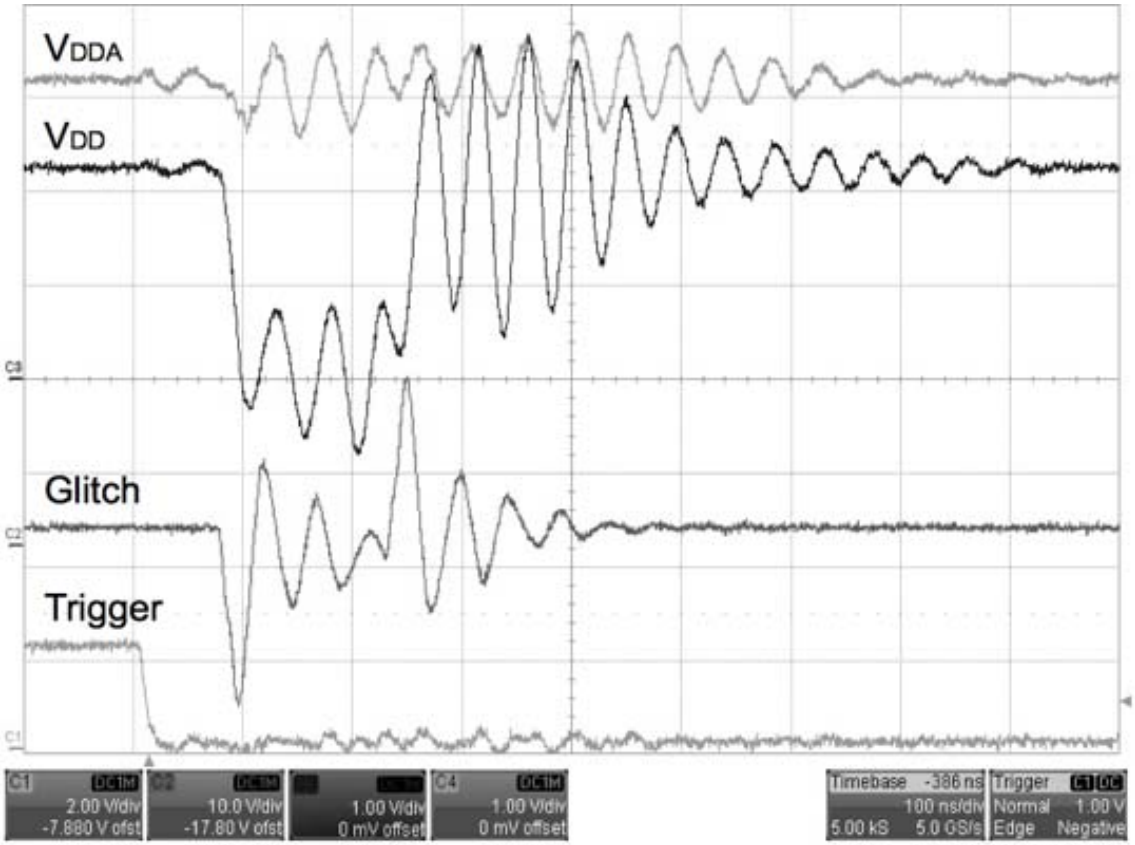
Импульсы разной длины, но одинаковой амплитуды



Падение напряжения в цифровой зоне

ПРИМЕР СОЗДАНИЯ ИМПУЛЬСА

Импульс приводил к колебаниям как в цифровой так и в аналоговой зоне, но из-за наличия диода, аналоговая зона реагировала гораздо меньше, поэтому она не всегда распознавала ошибку в питании.

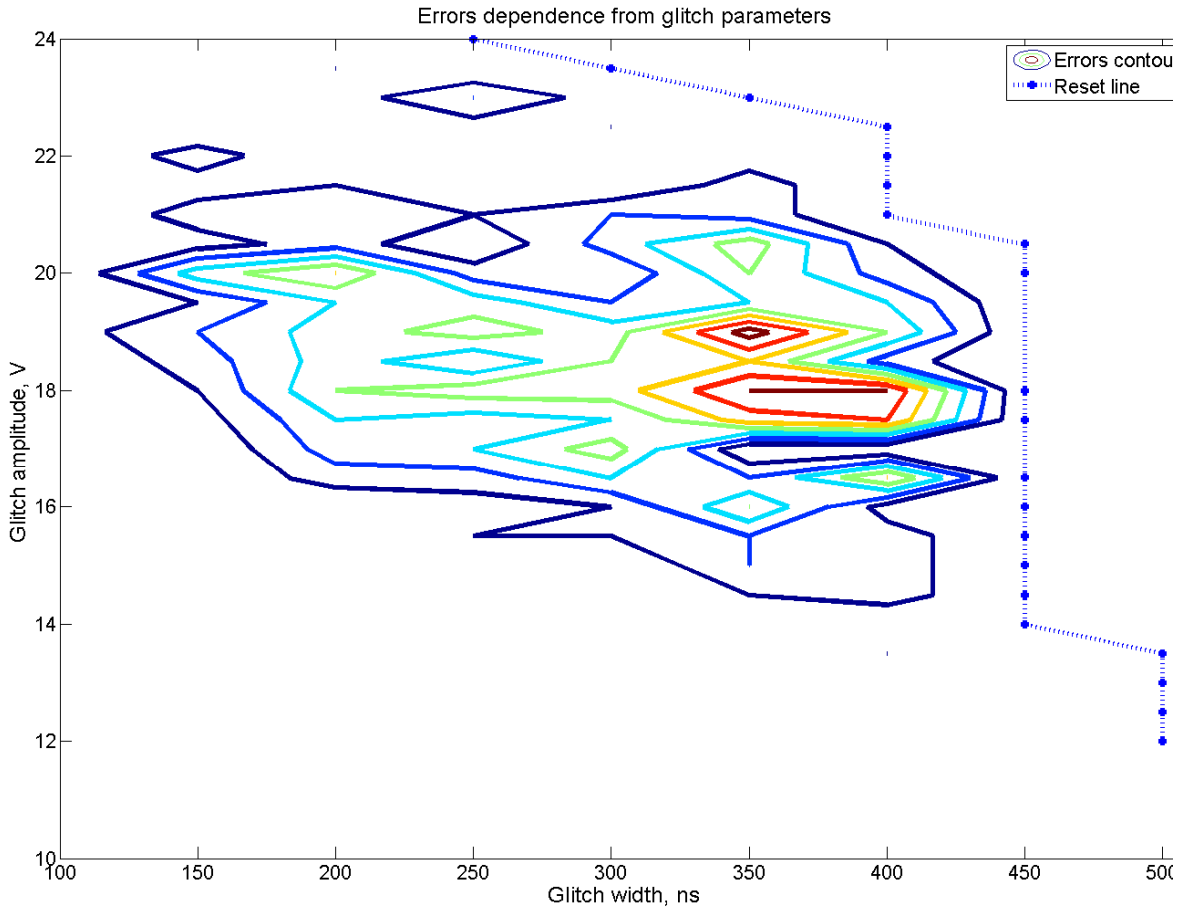


ПАРАМЕТРЫ ИМПУЛЬСА, ПРИВОДЯЩИЕ К ОШИБКАМ

Условные обозначения:

Синяя линия – одна ошибка из 10;

Красная - 10 из 10;



ТИПЫ ОШИБОК, ПОЛУЧЕННЫЕ С ПОМОЩЬЮ ГЕНЕРАТОРА ИМПУЛЬСОВ

- **Самая типичная ошибка это изменение одного или нескольких байт переменной (может быть значения в регистре или считанного из памяти);**
- **Крайне редкая ошибка – пропуск инструкции (одна на несколько тысяч);**

ВЫВОДЫ ПО РЕЗУЛЬТАТАМ РАБОТЫ С ГЕНЕРАТОРОМ ИМПУЛЬСОВ

- **Ключ алгоритма CRT RSA без защиты может быть легко получен (около 400 различных ошибок за один час работы);**
- **Ключа алгоритма CRT RSA с защитой, основанной на сравнении, получить не удалось (из-за нехватки времени), но такая возможность существует, хоть и невелика;**
- **Данный метод удобно применять когда требуется изменить несколько переменных за время одной операции шифрования, так как можно создавать импульсы определенной частоты (гораздо быстрее чем перезарядка лазера);**

СПАСИБО ЗА ВНИМАНИЕ!