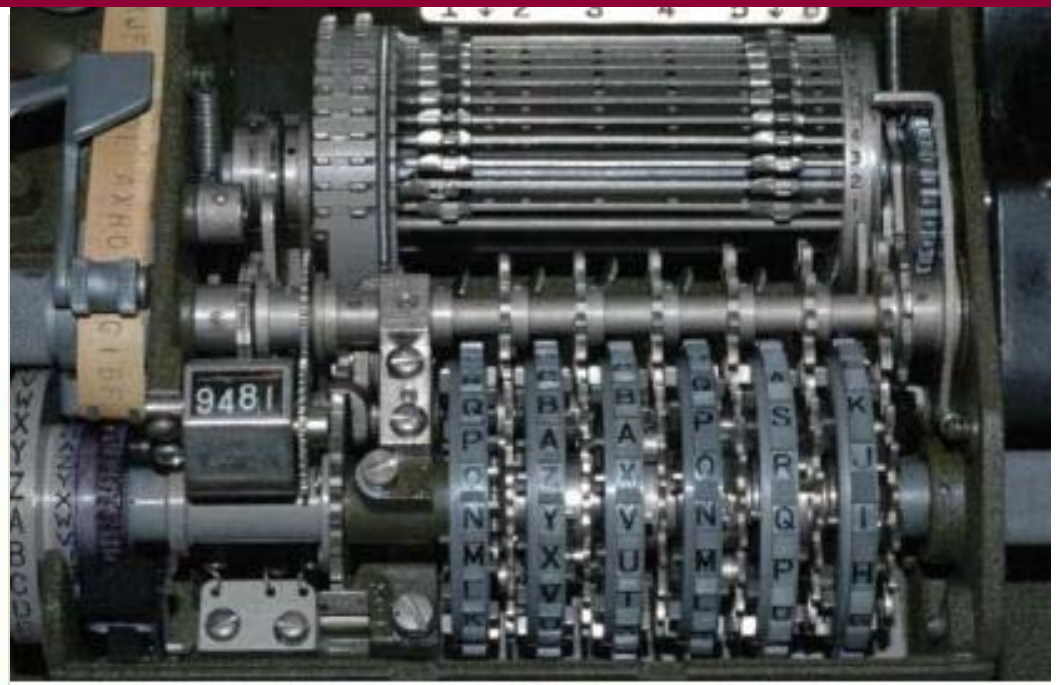
Криптоанализ по побочным каналам

Side Channel Attacks

Ассоциация РусКрипто

Операция «ENGULF», проведенная британской контрразведкой MI-5 в 1956г.

HAGELIN M-209 CIPHER MACHINE (GVG / PD)

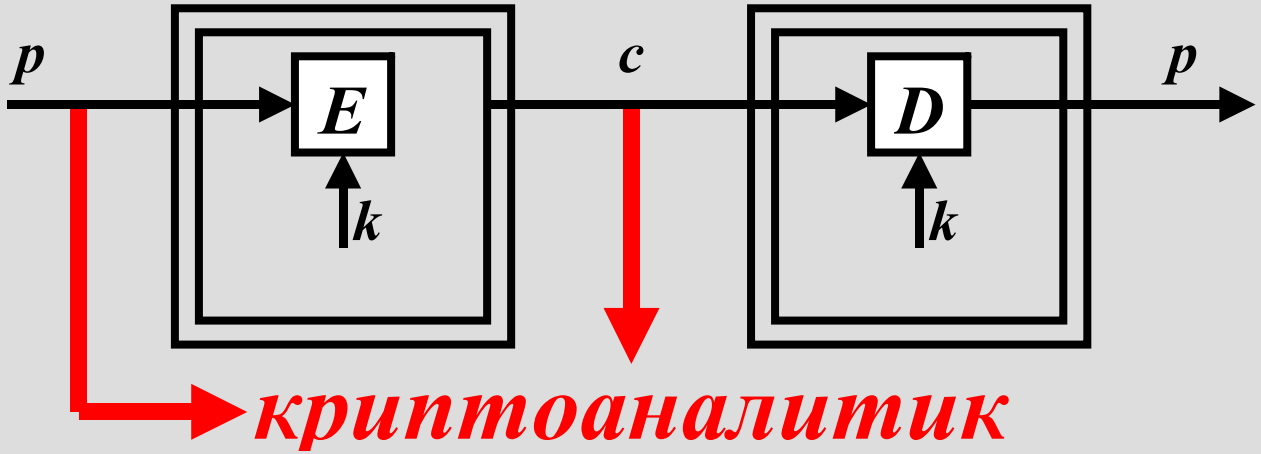


Источник:

P. Wright. Spy Catcher: The Candid Autobiography of a Senior Intelligence Officer. Viking Press,1987.

Ассоциация РусКрипто

Классический криптоанализ



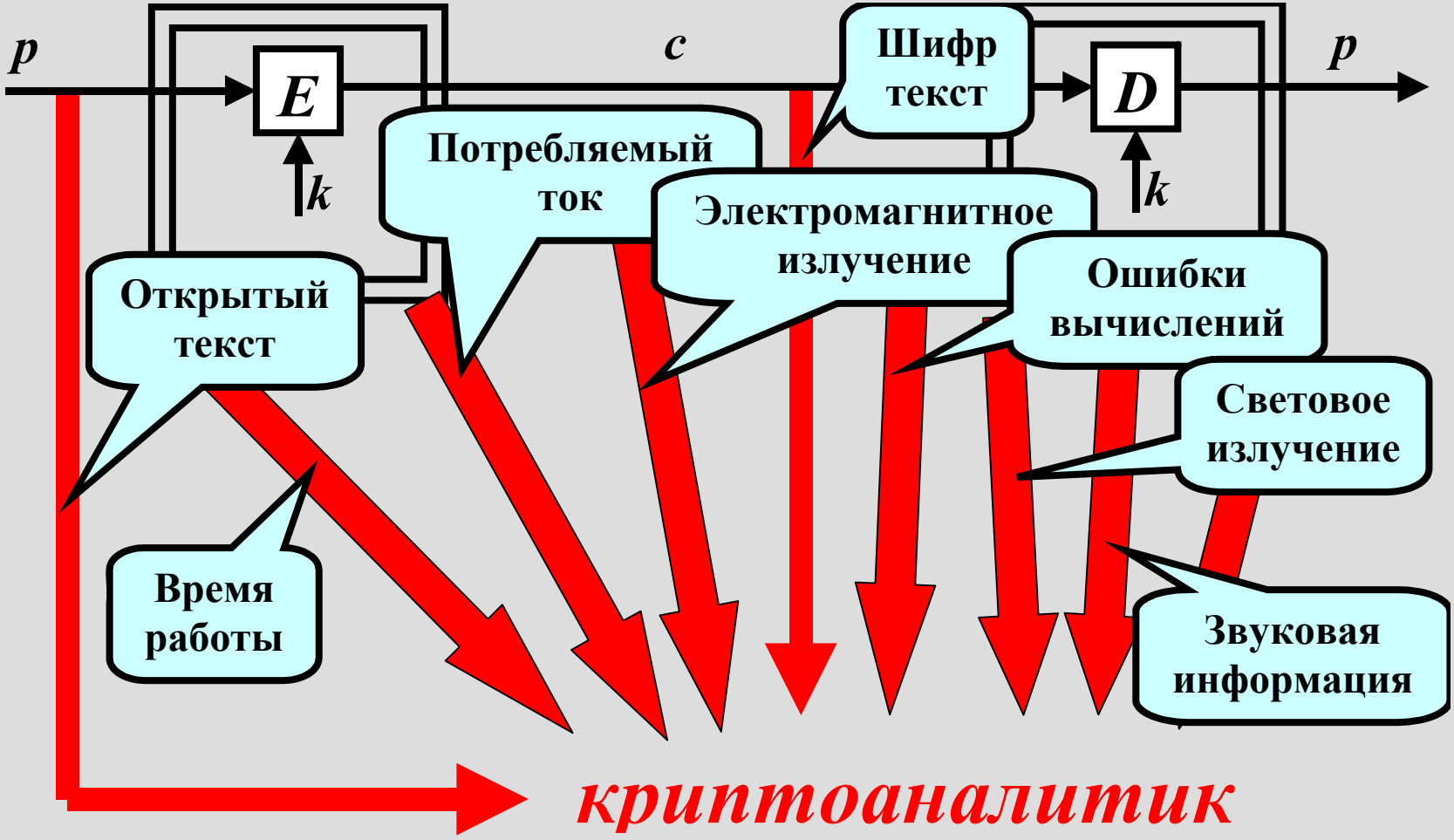
- Криптоанализ только по шифртексту (Ciphertext only attack)
- Криптоанализ по известному открытому тексту (Known plaintext attack)
- Криптоанализ по выбранному открытому тексту (Chosen plaintext attack)
- Криптоанализ по выбранному шифртексту (Chosen ciphertext attack)

Побочные информационные каналы
Side Channels

- ***Атаки по сторонним или побочным каналам*** (side channel attacks, SCA) – это вид криптографических атак, использующих информацию, полученную по ***сторонним или побочным каналам***.
- Под информацией из побочных каналов понимается информация, которая может быть получена с устройства шифрования и не является при этом ни открытым текстом, ни шифртекстом.

Ассоциация РусКрипто

Побочные информационные каналы
Side Channels



Побочные информационные каналы
Side Channels

- Обычный криптоанализ рассматривает криптоалгоритмы как чисто математические объекты, в то время как криптоанализ по побочным каналам также принимает во внимание их реализацию. Поэтому атаки SCA также называют ***атаками на реализацию*** (implementation attacks).

Побочные информационные каналы
Side Channels

- На практике SCA на много порядков более эффективны, чем традиционные атаки, основанные только на математическом анализе шифрующего алгоритма. Атаки по побочным каналам используют особенности реализации для извлечения секретных параметров, задействованных в вычислениях. Такой подход менее обобщённый, поскольку привязан к конкретной реализации, но как правило более мощный, чем классический криптоанализ.

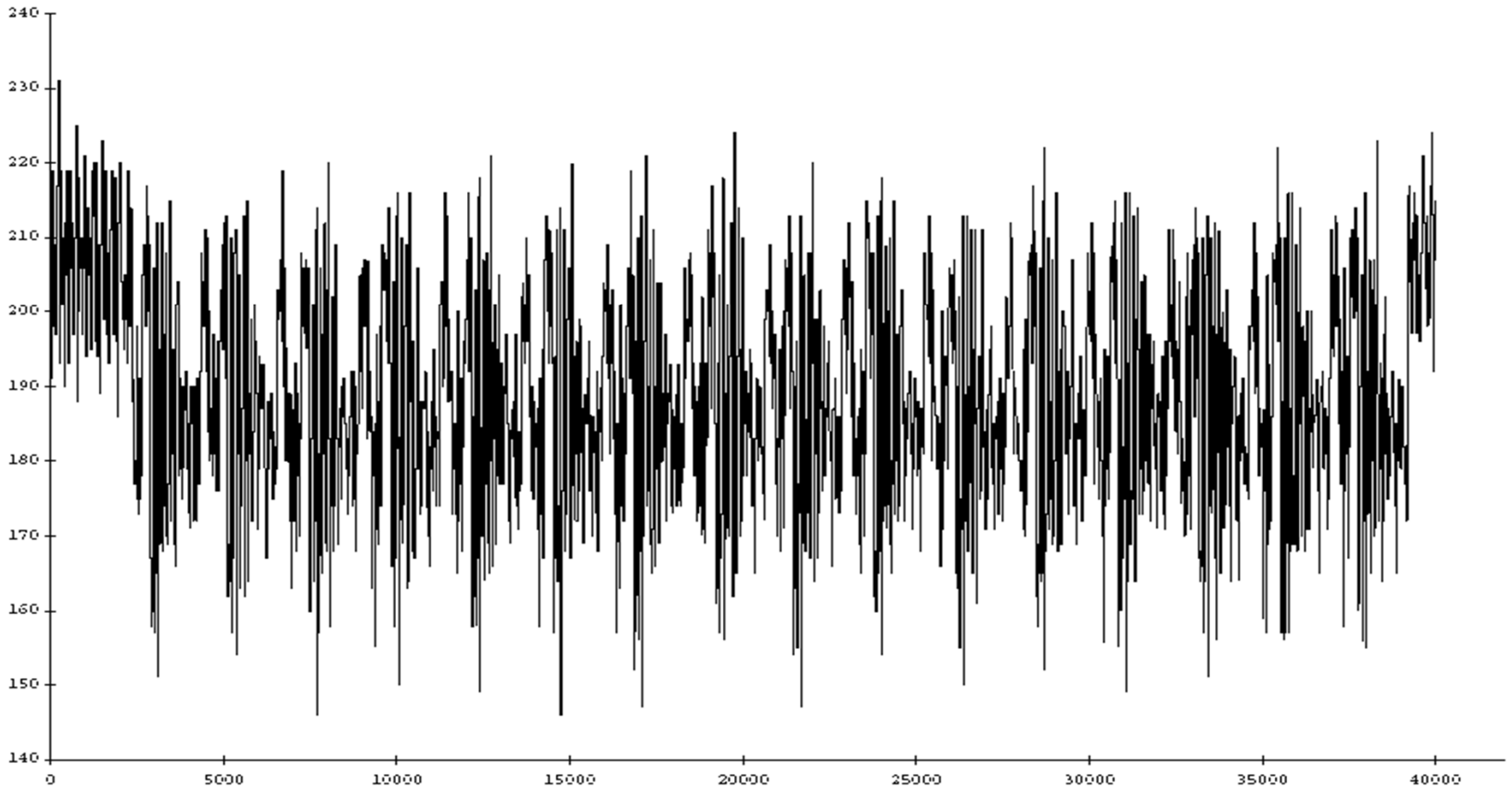
Классификация атак по побочным каналам

Атаки по побочным каналам классифицируются по следующим трём типам:

- По контролю над вычислительным процессом: ***пассивные*** и ***активные***.
- По способу доступа к модулю: ***агрессивные*** (invasive), ***полуагрессивные*** (semi-invasive) и ***неагрессивные*** (non-invasive).
- По методу, применяемому в процессе анализа: ***простые*** – simple side channel attack (***SSCA***) и ***разностные*** – differential side channel attack (***DSCA***).

Ассоциация РусКрипто

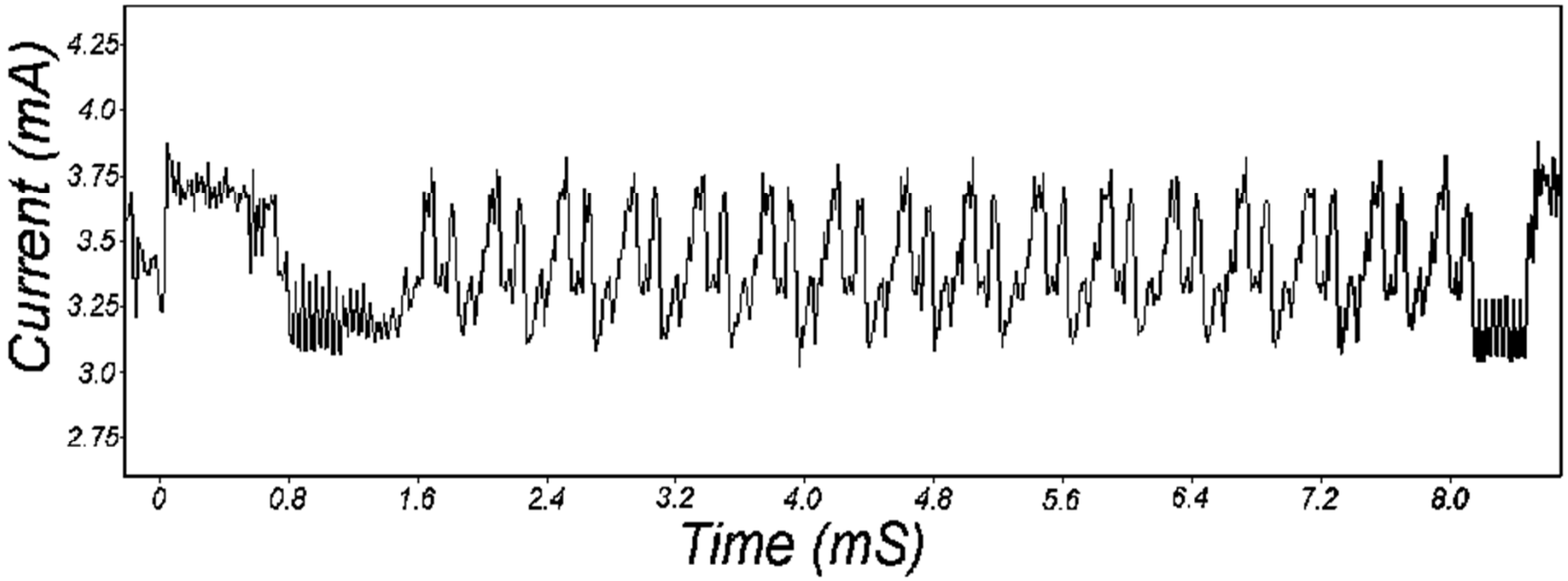
Побочные информационные каналы
Side Channels



Electric consumption measured on the 16 rounds of a DES computation

Ассоциация РусКрипто

Побочные информационные каналы
Side Channels



SPA trace showing an entire DES operation.

Криптоанализ по побочным каналам
Side Channel Attacks

- Атаки по энергопотреблению (Power Analysis Attacks)
- Атаки по времени исполнения (Timing Attacks)
- Атаки по ошибкам вычислений (Fault Attacks)
- Атаки по электромагнитному излучению (ElectroMagnetic Analysis)
- Атаки по ошибкам в канале связи (Error Message Attacks)
- Атаки по кэш-памяти (Cache-based Attacks)
- Акустические атаки (Acoustic Attacks)
- Атаки по световому излучению (Visible Light Attacks)

Атаки по времени исполнения (Timing Attacks)

P. Kocher. *Timing attacks on implementations of Diffie-Hellmann, RSA, DSS, and other systems*. CRYPTO'96, LNCS 1109, pp.104-113, 1996.

Вычисление $y = a^x$
по схеме Горнера:

$x = (x_{n-1}, x_{n-2}, \ldots, x_1, x_0)$

$R \leftarrow 1$
for $i = n-1$ to 0
  $R \leftarrow R^2$
  if $x_i = 1$ then $R \leftarrow R \cdot a$
next i
$y = R$

Нахождение веса x:

Если бит $x_i = 1$ — выполняется дополнительная инструкция

Атаки по времени исполнения (Timing Attacks)

Определение всего x:

Математическая модель:

t_i – независимые одинаково распределенные случайные величины, равные времени вычисления i-й итерации в схеме Горнера. Задавая значения $x_{b-1}, \ldots, x_1, x_0$, можно вычислить параметры случайной величины $r_{b-1}+\ldots+r_1+r_0$, где r_i распределены так же, как t. Рассмотрим дисперсию случайной величины $(t_{n-1}+\ldots+t_1+t_0)-(r_{b-1}+\ldots+r_1+r_0)=$

$=(t_{n-1}+\ldots+t_{b+1}+t_b)+(t_{b-1}-r_{b-1})+\ldots+(t_1-r_1)+(t_0-r_0)$

Она равна $(n-b+2(b-c))D_t=(n+b-2c)D_t$,

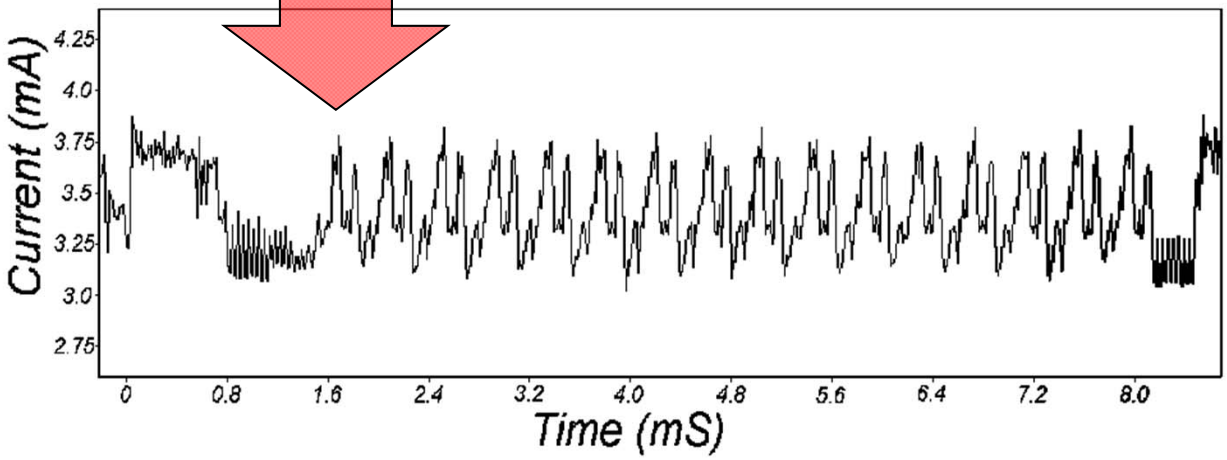
где c – число угаданных битов в $x_{b-1}, \ldots, x_1, x_0$, а D_t – дисперсия случайной величины t.

Ассоциация РусКрипто

Атаки по мощности (энергопотреблению) (Power Analysis Attacks)

Простая атака по мощности ***Simple Power Analysis (SPA)***

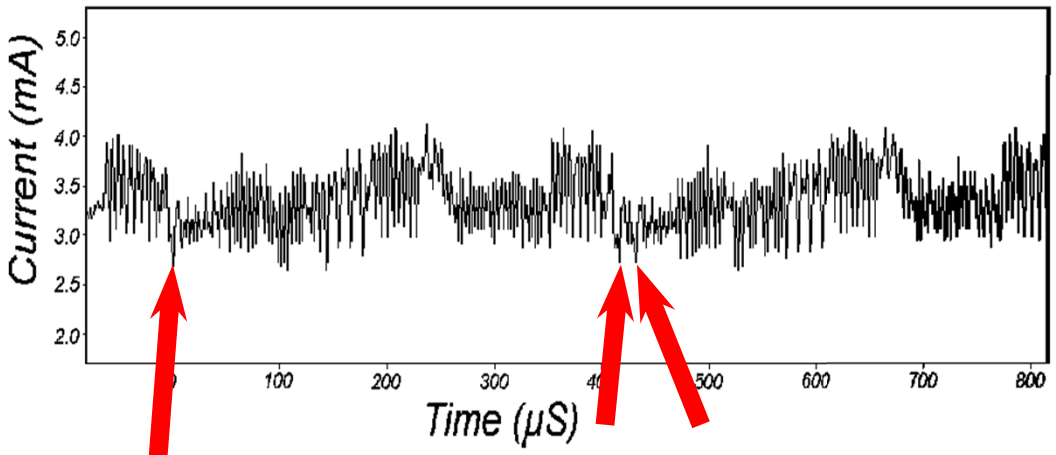
Разностная атака по мощности ***Differential Power Analysis (DPA)***



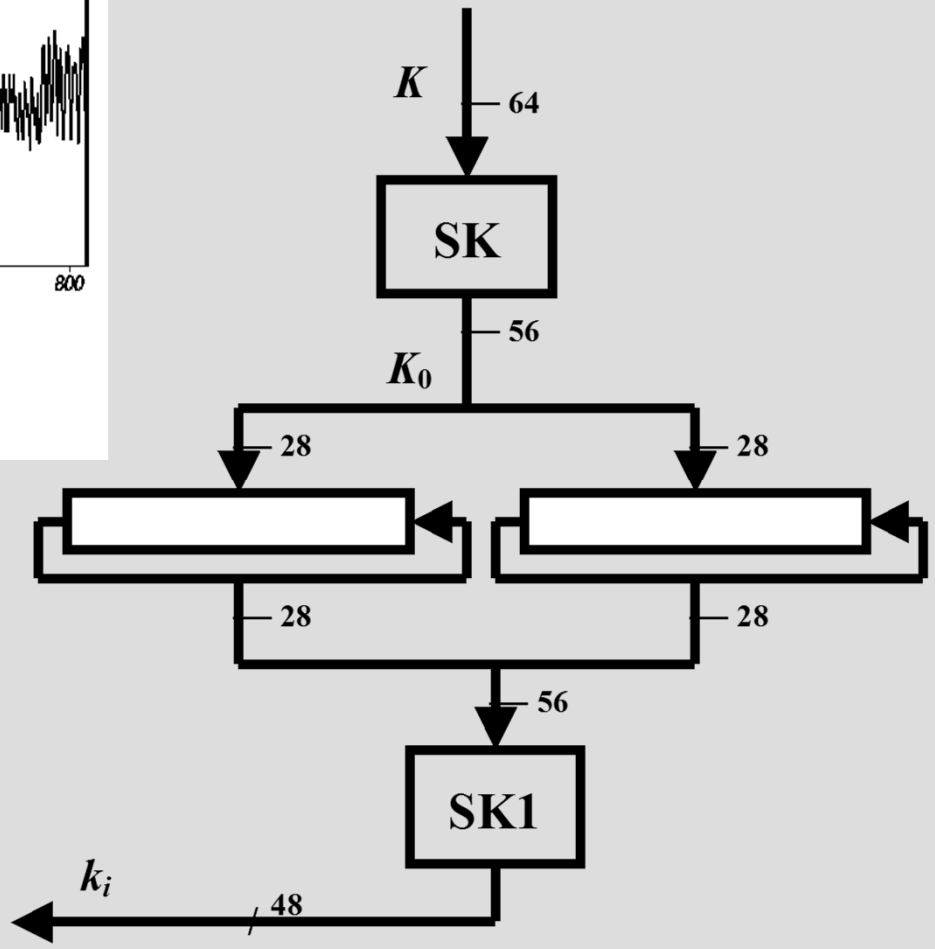
SPA trace showing an entire DES operation.

Ассоциация РусКрипто

Простая атака по мощности
Simple Power Analysis (SPA)



SPA trace showing DES rounds 2 and 3.

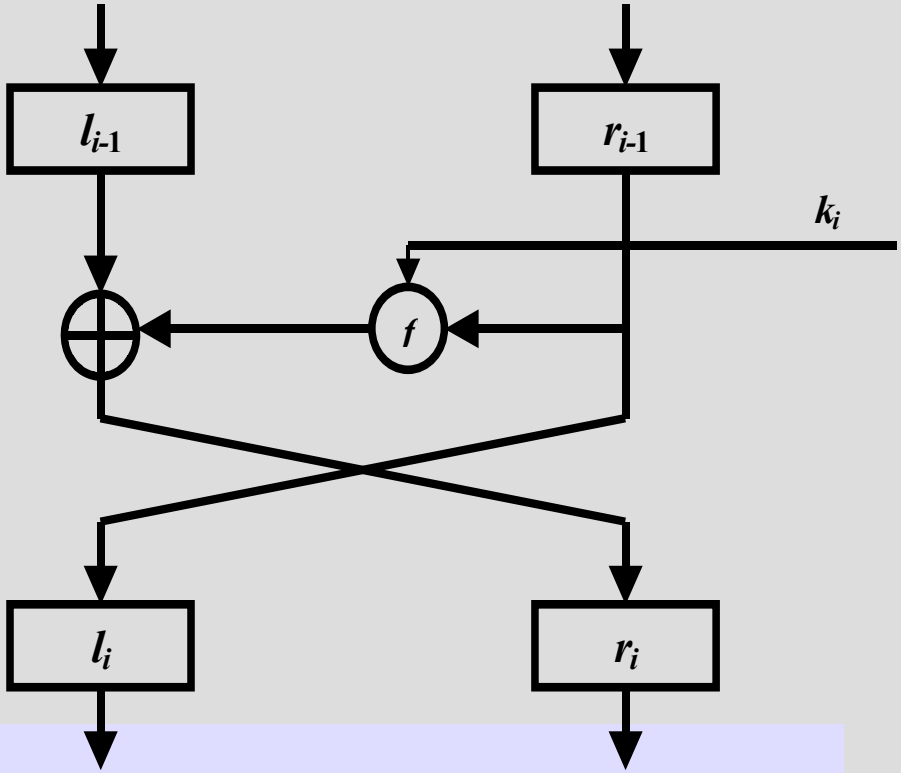


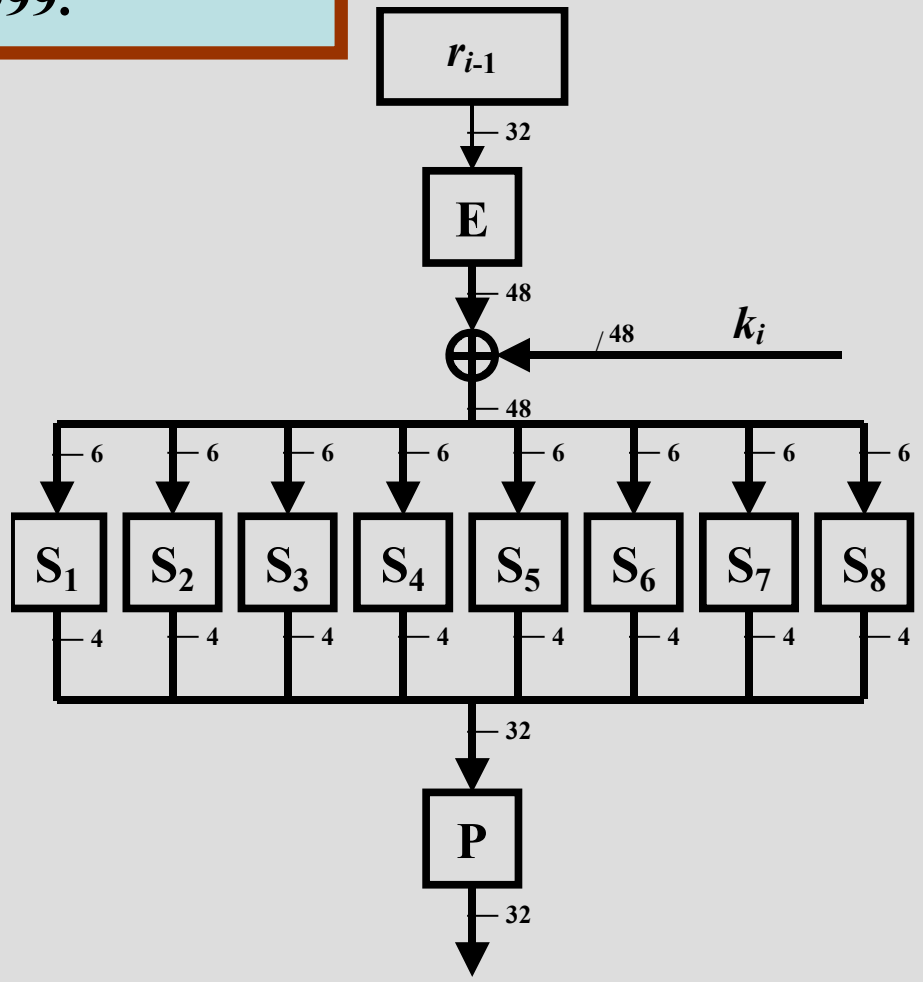
Алгоритм выработки цикловых ключей DES

Ассоциация РусКрипто

Разностная атака по мощности
Differential Power Analysis (DPA)

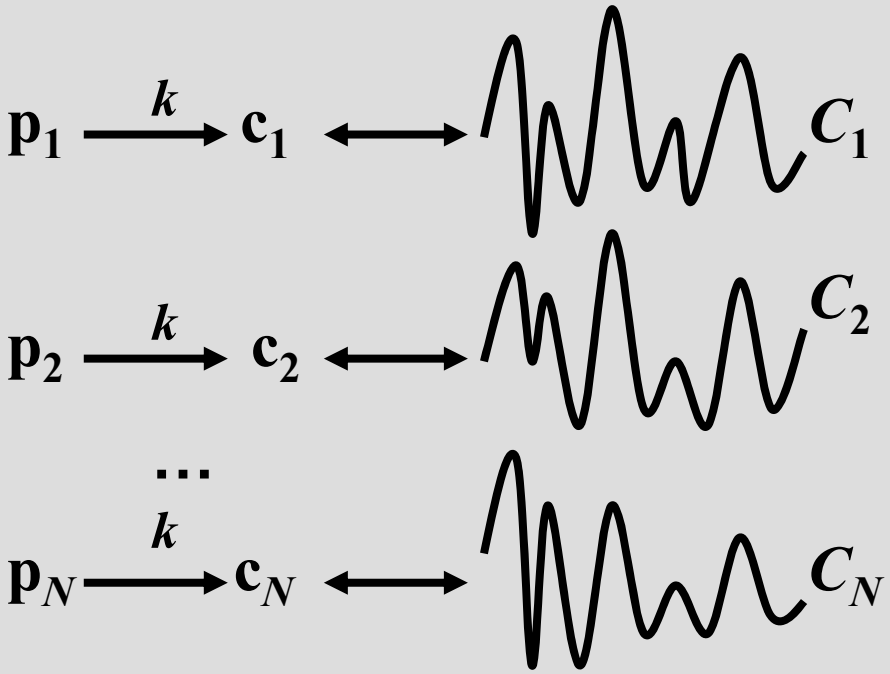
P. Kocher, J. Jaffe, B. Jun. *Differential power analysis.* CRYPTO'99, LNCS 1666, pp.388-397, 1999.

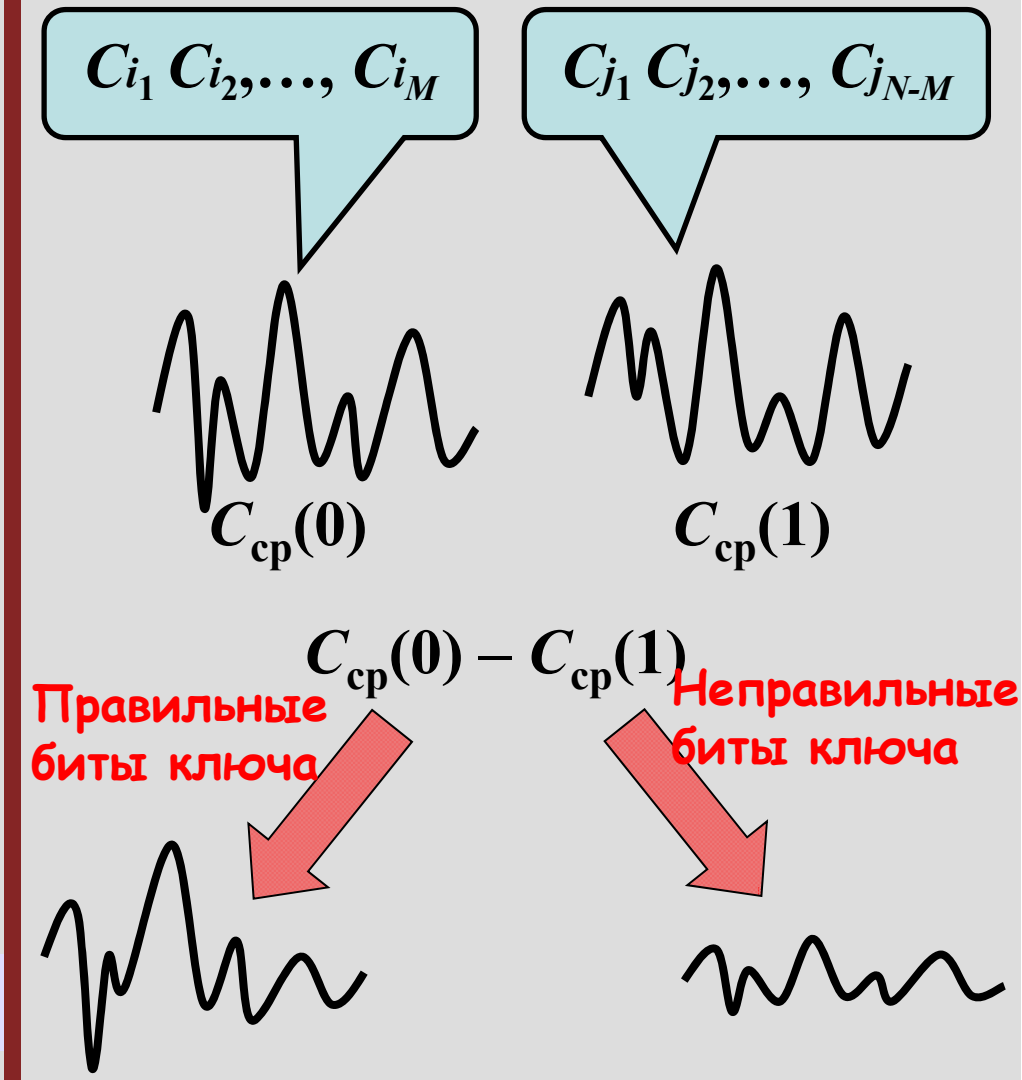




Ассоциация РусКрипто

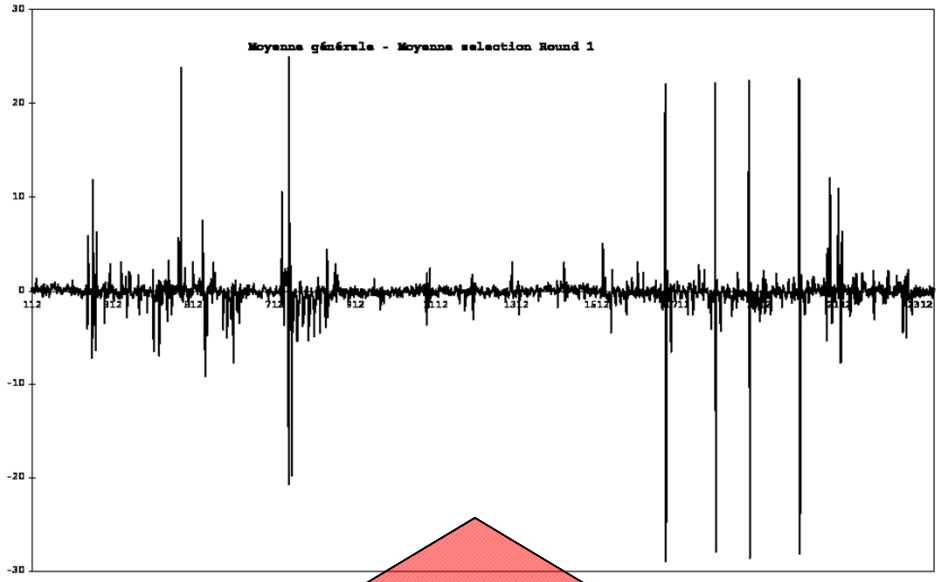
Разностная атака по мощности
Differential Power Analysis (DPA)



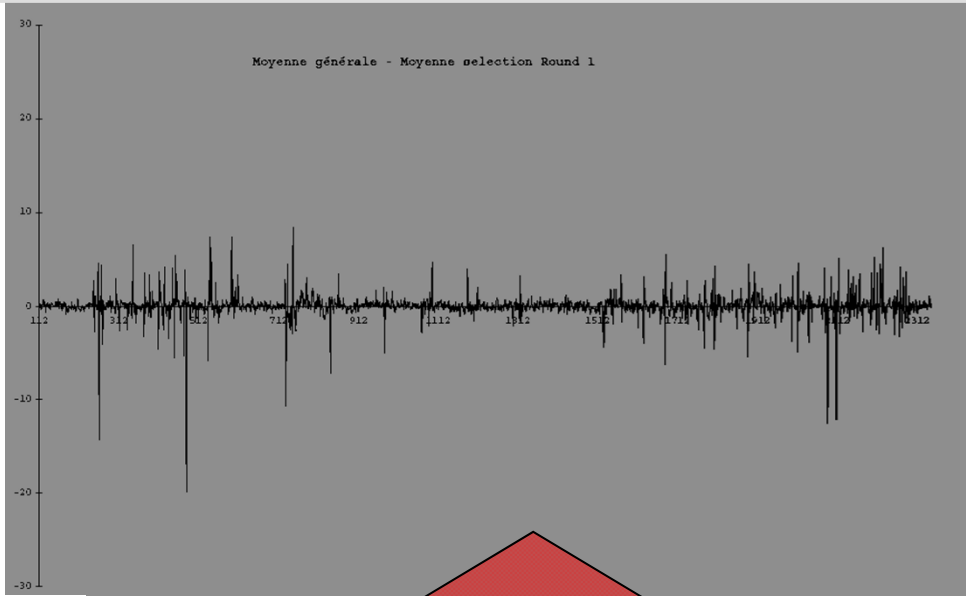


Ассоциация РусКрипто

Разностная атака по мощности
Differential Power Analysis (DPA)



Difference of the curves MC and MC' when the 6 bits are correct



An example of difference of the curves MC and MC' when the 6 bits are false

Правильные биты ключа

Неправильные биты ключа

Противодействие атакам по сторонним каналам

- Атаки по времени исполнения (Timing Attacks)
- Атаки по энергопотреблению (Power Analysis Attacks)
- Атаки по ошибкам вычислений (Fault Attacks)
- Атаки по электромагнитному излучению (ElectroMagnetic Analysis)
- Атаки по ошибкам в канале связи (Error Message Attacks)
- Атаки по кэш-памяти (Cache-based Attacks)
- Акустические атаки (Acoustic Attacks)
- Атаки по световому излучению (Visible Light Attacks)

Ассоциация РусКрипто

Предотвращение атак по внешнему каналу

- Маскирование (Blinding)
- Вычисления, не зависящие от данных
- Условные переходы
- Добавление задержек
- Уравнивание времени умножения и возведения в квадрат
- Балансировка потребляемой мощности
- Добавление шума
- Экранирование
- Выполнение шифрования дважды