Correlated Extra-Reductions Defeat Blinded Regular Exponentiation

Margaux Dugardin, Sylvain Guilley, Jean-Luc Danger, Zakaria Najm, and Olivier Rioul

CHES 2016 - Santa Barbara, CA

Overview

Introduction

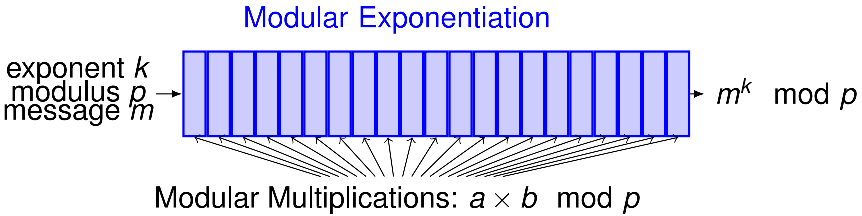
- Montgomery Modular Multiplication
- Montgomery eXtra-reduction
- State of the art of attack exploiting eXtra-reduction

Our work

- Idea of the attack
- New information given by study of the eXtra-reduction
- Experimental part and results

Conclusion

Montgomery Modular Multiplication



Montgomery Modular Multiplication

Definition (Montgomery Transformation [Mon85])

For any prime modulus p, the Montgomery form of $a \in \mathbb{F}_p$ is $\phi(a) = a \times R \mod p$ for some constant R greater than and co-prime with p.

Used case is $R = 2^{\lceil \log_2(p) \rceil}$

Definition (Montgomery Modular Multiplication [Mon85])

Let $\phi(a)$ and $\phi(b)$ two elements of $\mathbb{F}_p$ in Montgomery form. The MMM of $\phi(a)$ and $\phi(b)$ is $\phi(a) \times \phi(b) \times R^{-1} \mod p$.

Montgomery Modular Multiplication

The MMM can be implemented in two steps:

(*i*) compute $D = \phi(a) \times \phi(b)$, then

(*ii*) reduce D using Montgomery reduction which returns $\phi(c)$.

Montgomery reduction

In the Algorithm 1, the pair (R^{-1}, v) is such that $RR^{-1} - vp = 1$.

Algorithm 1 Montgomery Reduction (Alg. 14.32 of [MvOV96])

Input: $D = \phi(a) \times \phi(b)$
Output: $\phi(c) = \phi(a) \times \phi(b) \times R^{-1} \bmod p$

$m \leftarrow (D \bmod R) \times v \bmod R$
$U \leftarrow (D + m \times p) \div R$ ▷ Invariant: $0 \leq U < 2p$
if $U \geq p$ **then**
    $C \leftarrow U - p$ ▷ eXtra-reduction
else
    $C \leftarrow U$
end if
return C

Montgomery reduction

In the Algorithm 1, the pair (R^{-1}, v) is such that $RR^{-1} - vp = 1$.

Algorithm 2 Montgomery Reduction (Alg. 14.32 of [MvOV96])

Input: $D = \phi(a) \times \phi(b)$

Output: $\phi(c) = \phi(a) \times \phi(b) \times R^{-1} \bmod p$

1: $m \leftarrow (D \bmod R) \times v \bmod R$
2: $U \leftarrow (D + m \times p) \div R$ ▷ Invariant: $0 \leq U < 2p$
3: **if** $U \geq p$ **then**
4: $\quad C \leftarrow U - p$ $\boxed{X = 1}$ ▷ eXtra-reduction
5: **else**
6: $\quad C \leftarrow U$ $\boxed{X = 0}$
7: **end if**
8: **return** C

Montgomery eXtra-reduction

Example (of software implementation)

- Conditional final substraction: OpenSSL
  (File `crypto/bn/bn_mont.c`)

```
if (BN_ucmp(ret, &(mont->N)) >= 0)
{
    if (!BN_usub(ret,ret,&(mont->N))) goto err;
}
```

$X = 1$

- Real or dummy final subtraction: mbedTLS
  (File `library/bignum.c`)

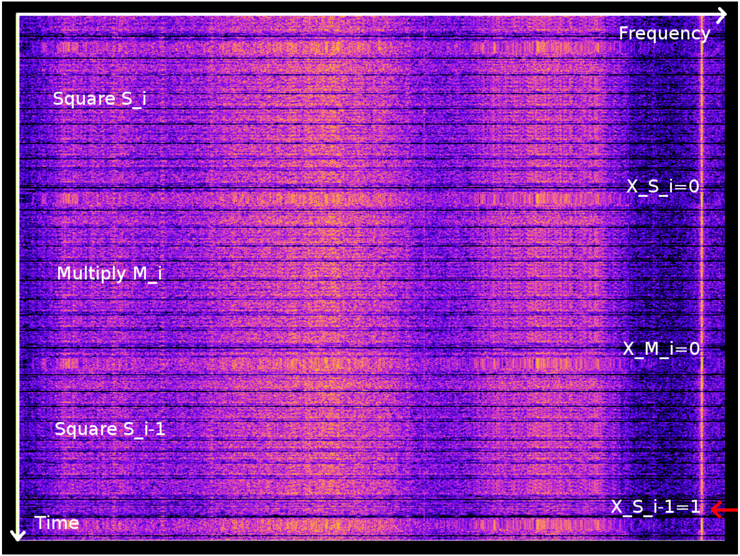
```
if( mpi_cmp_abs( A, N ) >= 0 )
mpi_sub_hlp( n, N->p, A->p );
else
/* prevent timing attacks */
mpi_sub_hlp( n, A->p, T->p );
```

$X = 1$

$X = 0$

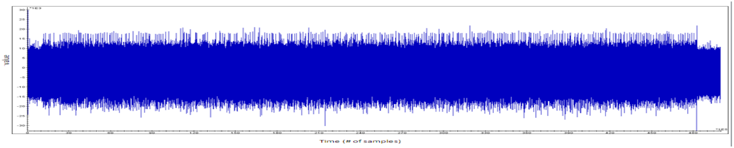
1. Spectrogram on global power consumption acquisition

OpenSSL on ARM Cortex-M0



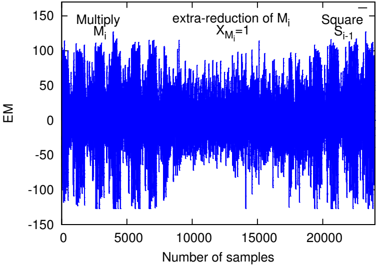
THALES TELECOM ParisTech

2. Electromagnetic analysis against `mbedTLS` on ARM Cortex-M4



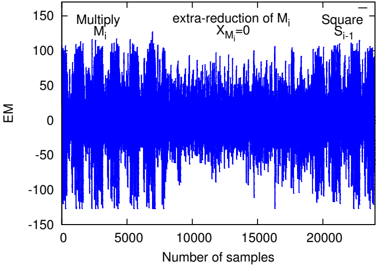
Real subtraction

$X_{M_i} = 1$



Dummy subtraction

$X_{M_i} = 0$



Attack on RSA exploiting timing and eXtra-reduction

	CRT	Key Protection	DPA protected Blinded Message	SPA protected Constant Time
Kocher	No	No	No	No
Schindler 1	Yes	No	No	No
Schindler 2	Yes	Yes	No	No
Schindler 3	Yes	No	Yes	No
???	Yes	No	Yes	Yes

References:

- Kocher: [Koc98]
- Schindler 1: [SKQ01, SW03, ASK05, AS08]
- Schindler 2: [Sch15]
- Schindler 3: [Sch00, WT01, Sch02]

Bias theory

How to differentiate between a multiply and a square using eXtra-reduction?

Proposition (Probability of extra-reduction in a multiply and a square operation [Sch00, Lemma 1])

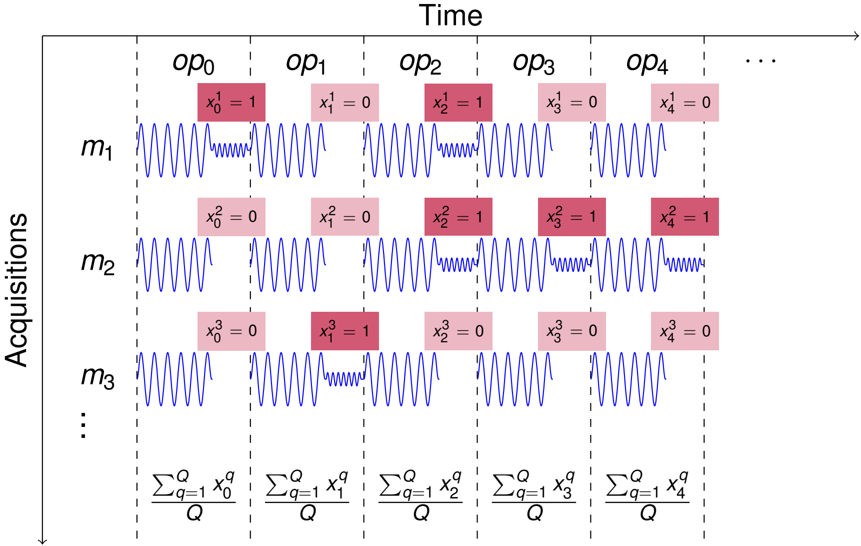
- Multiply of two random numbers:

$$\mathbb{P}(X_M = 1) = \frac{p}{4R},$$

- Square of one random number:

$$\mathbb{P}(X_S = 1) = \frac{p}{3R}.$$

Schindler 3: Attack on blinded message

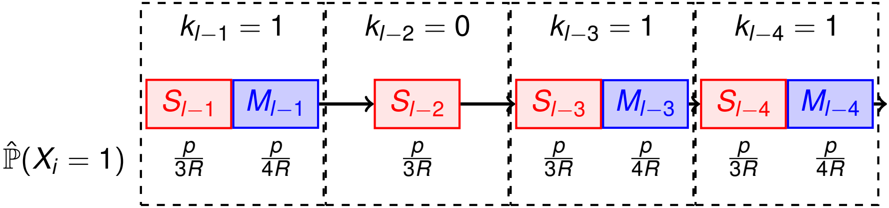


Schindler 3: Attack on blinded message

Algorithm 3 Probability estimation using histogram method

Input: We take Q acquisitions using random messages $m_1, \dots, m_Q$
Output: Estimated probability

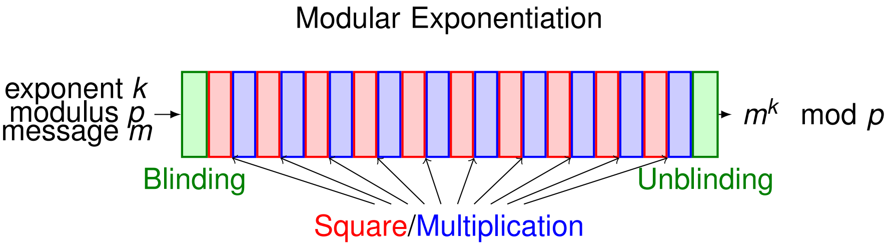
for each operation noted by i **do**
    for each acquisition $q \in \{1, \dots, Q\}$ **do**
        Detect if an eXtra-reduction is present $x_i^q = 1$ or absent $x_i^q = 0$
    end for
    Compute the means $\hat{\mathbb{P}}(X_i = 1) = \frac{\sum_{q=1}^{Q} x_i^q}{Q}$
end for
return $\hat{\mathbb{P}}(X_i = 1)$



Summary of state-of-the-art

To protect against:

- Kocher, Schindler 1 and Schindler 2, the message must be blinded,
- Schindler 3, the exponentiation modular algorithm must be regular.



One classical blinded regular algorithm

Algorithm 4 Blinded Square and Multiply Always Left-to-Right

Input: $m, k = (k_l k_{l-1} \ldots k_0)_2, p$ $\quad (k_l = 1)$

Output: $m^k \mod p$

$m^* \leftarrow BLINDING(m)$
$R_0 \leftarrow 1$
$R_1 \leftarrow m^*$
for $i = l - 1$ **downto** 0 **do**
    $R_1 \leftarrow R_1 \times R_1 \mod p$ $\quad \triangleright$ Square S_i
    $R_{k_i} \leftarrow R_1 \times m^* \mod p$ $\quad \triangleright$ Multiply M_i
end for
$R_1 \leftarrow UNBLINDING(R_1)$
return R_1

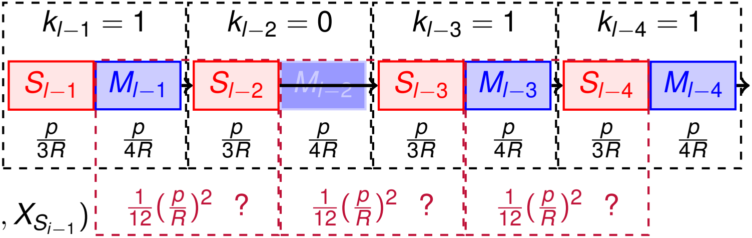
In Square and Multiply Always (SMA)

Only the for-loop part:

	$k_{l-1} = 1$		$k_{l-2} = 0$		$k_{l-3} = 1$		$k_{l-4} = 1$	
	S_{l-1}	M_{l-1}	S_{l-2}	M_{l-2}	S_{l-3}	M_{l-3}	S_{l-4}	M_{l-4}
$\mathbb{P}(X_i = 1)$	$\frac{p}{3R}$	$\frac{p}{4R}$	$\frac{p}{3R}$	$\frac{p}{4R}$	$\frac{p}{3R}$	$\frac{p}{4R}$	$\frac{p}{3R}$	$\frac{p}{4R}$

In Square and Multiply Always (SMA)

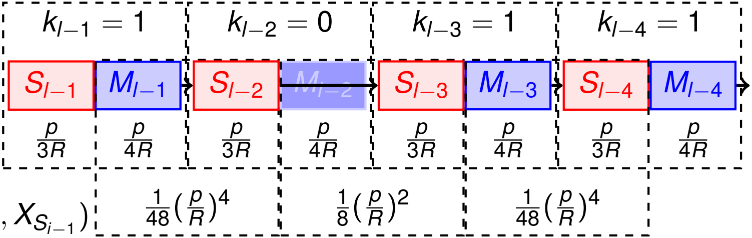
Only the for-loop part:



$$\mathbb{P}((X_{M_i}, X_{S_{i-1}}) = (1,1))$$

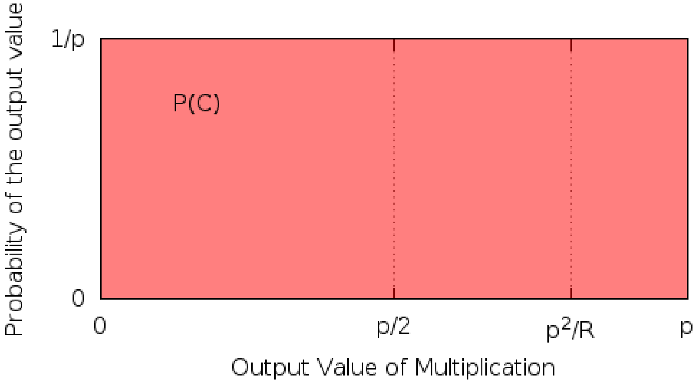
In Square and Multiply Always (SMA)

Only the for-loop part:



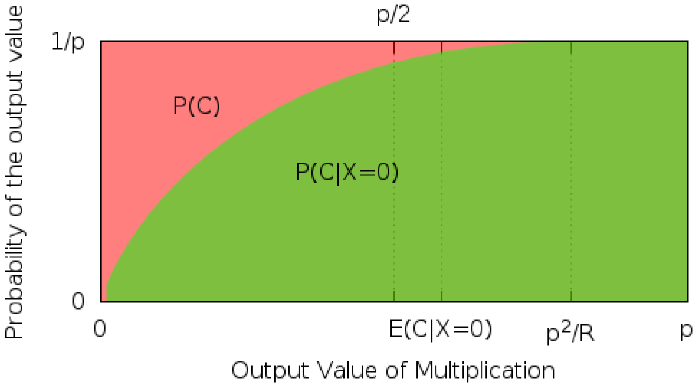
$\mathbb{P}((X_{M_i}, X_{S_{i-1}}) = (1,1))$

Distribution of the multiplication output



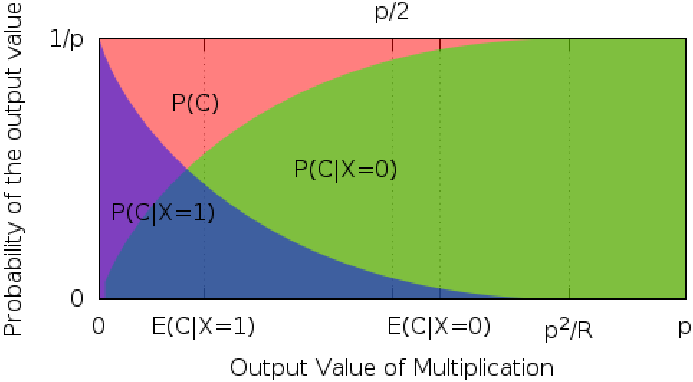
- $C = A \times B \mod p, \quad \mathbb{E}(C) = \frac{p}{2}$

Distribution of the multiplication output



- $C = A \times B \mod p, \quad \mathbb{E}(C) = \frac{p}{2}$
- $C|X = 0, \quad \mathbb{E}(C|X = 0) = \frac{(p/2)-(p^3/18R^2)}{1-(p/4R)}$

Distribution of the multiplication output

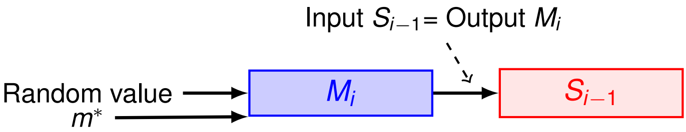


- $C = A \times B \mod p, \quad \mathbb{E}(C) = \frac{p}{2}$
- $C|X = 0, \quad \mathbb{E}(C|X = 0) = \frac{(p/2)-(p^3/18R^2)}{1-(p/4R)}$
- $C|X = 1, \quad \mathbb{E}(C|X = 1) = \frac{2p^2}{9R}$

THALES TELECOM ParisTech

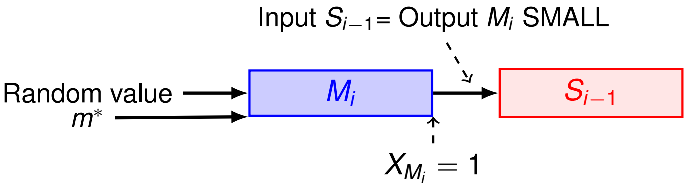
New observations

- Case $k_i = 1$:



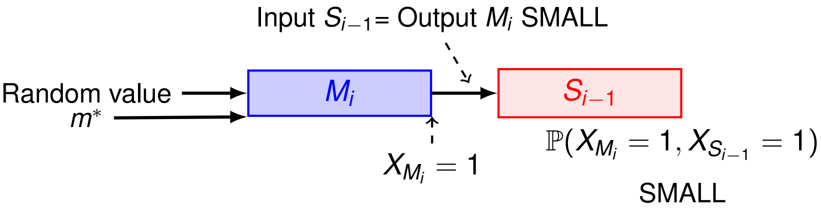
New observations

- Case $k_i = 1$:



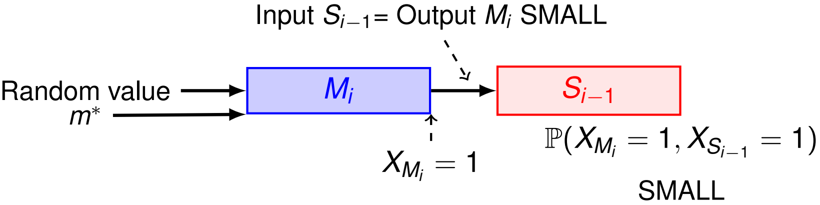
New observations

- Case $k_i = 1$:

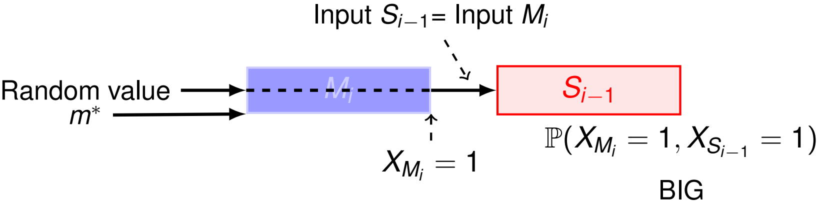


New observations

- Case $k_i = 1$:



- Case $k_i = 0$:



Theorem (Joint Probability of Extra-Reduction in Multiplication Followed by a Square)

Case $k_i = 1$:

$\mathbb{P}(X_{M_i}, X_{S_{i-1}})$	$X_{S_{i-1}} = 0$	$X_{S_{i-1}} = 1$
$X_{M_i} = 0$	$1 - \frac{7}{12}\frac{p}{R} + \frac{1}{48}\left(\frac{p}{R}\right)^4$	$\frac{p}{3R} - \frac{1}{48}\left(\frac{p}{R}\right)^4$
$X_{M_i} = 1$	$\frac{p}{4R} - \frac{1}{48}\left(\frac{p}{R}\right)^4$	$\frac{1}{48}\left(\frac{p}{R}\right)^4$

Case $k_i = 0$:

$\mathbb{P}(X_{M_i}, X_{S_{i-1}})$	$X_{S_{i-1}} = 0$	$X_{S_{i-1}} = 1$
$X_{M_i} = 0$	$1 - \frac{7}{12}\frac{p}{R} + \frac{1}{8}\left(\frac{p}{R}\right)^2$	$\frac{p}{3R} - \frac{1}{8}\left(\frac{p}{R}\right)^2$
$X_{M_i} = 1$	$\frac{p}{4R} - \frac{1}{8}\left(\frac{p}{R}\right)^2$	$\frac{1}{8}\left(\frac{p}{R}\right)^2$

Example with $p \simeq R$

Case $k_i = 1$:

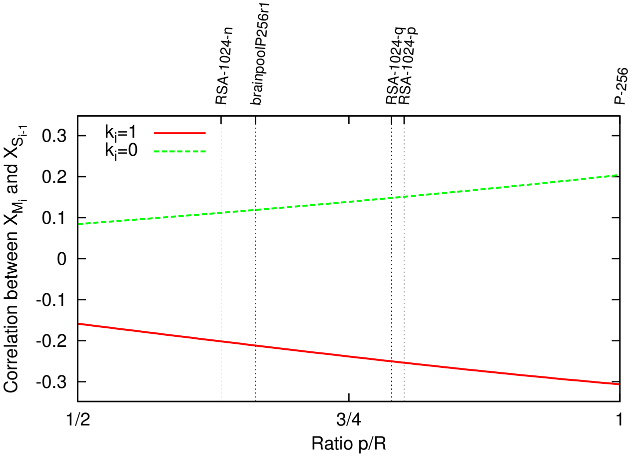
$\mathbb{P}(X_{M_i}, X_{S_{i-1}})$	$X_{S_{i-1}} = 0$	$X_{S_{i-1}} = 1$
$X_{M_i} = 0$	$\frac{21}{48}$	$\frac{15}{48}$
$X_{M_i} = 1$	$\frac{11}{48}$	$\frac{1}{48}$

Case $k_i = 0$:

$\mathbb{P}(X_{M_i}, X_{S_{i-1}})$	$X_{S_{i-1}} = 0$	$X_{S_{i-1}} = 1$
$X_{M_i} = 0$	$\frac{26}{48}$	$\frac{10}{48}$
$X_{M_i} = 1$	$\frac{6}{48}$	$\frac{6}{48}$

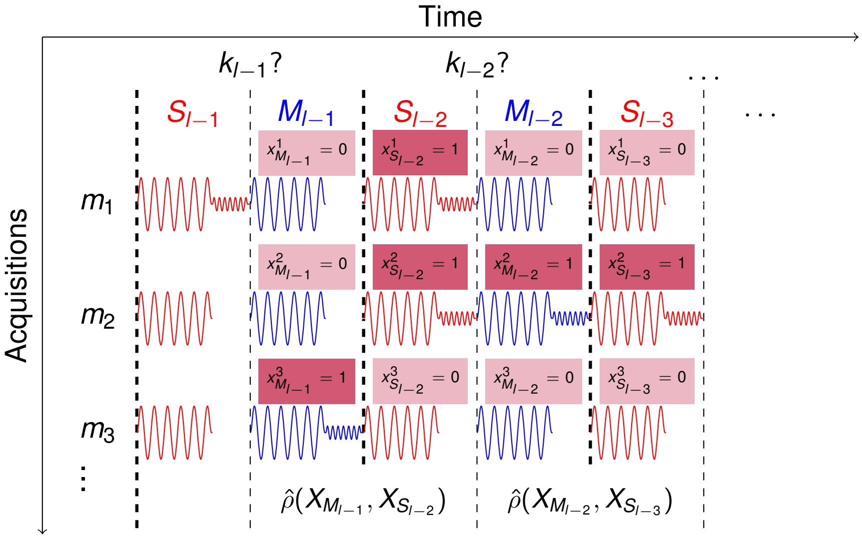
Pearson correlation

$$\rho(X_{M_i}, X_{S_{i-1}}) = \frac{\mathbb{P}(X_{M_i} = 1, X_{S_{i-1}} = 1) - (\mathbb{P}(X_{M_i} = 1) \times \mathbb{P}(X_{S_{i-1}} = 1))}{\sqrt{\mathbb{P}(X_{M_i} = 1)(1 - \mathbb{P}(X_{M_i} = 1))}\sqrt{\mathbb{P}(X_{S_{i-1}} = 1)(1 - \mathbb{P}(X_{S_{i-1}} = 1))}}$$



THALES TELECOM ParisTech

Exploitation of the bias



Exploitation of the bias

Algorithm 5 ρ-estimation using bi-variate histogram method

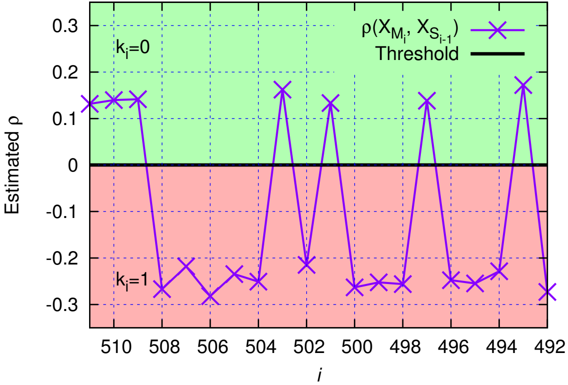
Input: $(\underline{x_{M_i}}, \underline{x_{S_{i-1}}})$, a set of Q pairs of $(l-1)$ bits

Output: A rho estimation $\hat{\rho}(X_{M_i}, X_{S_{i-1}})$ for each iteration

for $i = l - 1$ **downto** 1 **do**
  $\hat{\mathbb{P}}(X_{M_i}, X_{S_{i-1}}) \leftarrow 0$
  for $q = 1$ **to** Q **do**
    $\hat{\mathbb{P}}(X_{M_i} = x^q_{M_i}, X_{S_{i-1}} = x^q_{S_{i-1}}) \leftarrow \hat{\mathbb{P}}(X_{M_i} = x^q_{M_i}, X_{S_{i-1}} = x^q_{S_{i-1}}) + 1$
  end for
  $\hat{\mathbb{P}}(X_{M_i}, X_{S_{i-1}}) \leftarrow \hat{\mathbb{P}}(X_{M_i}, X_{S_{i-1}}) \ / \ Q$ ▷ Normalization
  $\hat{\rho}(X_{M_i}, X_{S_{i-1}}) \leftarrow \dfrac{\hat{\mathbb{P}}(X_{M_i}{=}1, X_{S_{i-1}}{=}1) - (\hat{\mathbb{P}}(X_{M_i}{=}1) \times \hat{\mathbb{P}}(X_{S_{i-1}}{=}1))}{\sqrt{\hat{\mathbb{P}}(X_{M_i}{=}1)(1-\hat{\mathbb{P}}(X_{M_i}{=}1))}\sqrt{\hat{\mathbb{P}}(X_{S_{i-1}}{=}1)(1-\hat{\mathbb{P}}(X_{S_{i-1}}{=}1))}}$
  ▷Pearson coefficient
end for

Exploitation of the bias

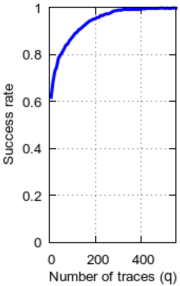
Estimated Pearson correlations using 1000 randoms queries for `RSA-1024-p` for the first 20 iterations



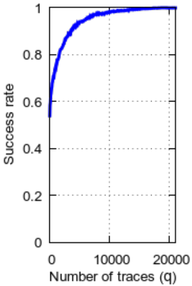
Exploitation of the bias

$$\mathbb{P}(N) = \mathbb{P}(N_{M_i} = 1) = \mathbb{P}(N_{S_{i-1}} = 1)$$

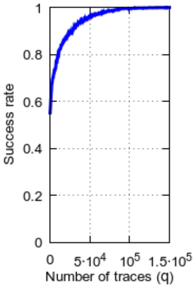
$$k \rightarrow \boxed{\mathbb{P}_{k_i}(X_{M_i}, X_{S_{i-1}})} \rightarrow \overset{\text{i.i.d}}{(\underline{x_{M_i}}, \underline{x_{S_{i-1}}})} \rightarrow \boxed{\text{Add } (N_{M_i}, N_{S_{i-1}})} \rightarrow \overset{\text{i.i.d}}{(\underline{y_{M_i}}, \underline{y_{S_{i-1}}})} \rightarrow \boxed{\hat{\rho}} \rightarrow \hat{k}$$



$\mathbb{P}(N) = 10\%$



$\mathbb{P}(N) = 20\%$



$\mathbb{P}(N) = 30\%$

Exploitation of the bias on real measurements

Type of attack side-channel for detection	`SPA-Timing` Openssl	`max-corr` mbedTLS	`min-abs-diff` mbedTLS
Detection probability for one query $= 1 - \mathbb{P}(N)$	100%	82.50%	83.47%
Number of queries (SMA)	≈ 200	≈ 10000	≈ 10000

Conclusion

	CRT	Key Protection	DPA protected Blinded Message	SPA protected Constant Time
Kocher	No	No	No	No
Schindler 1	Yes	No	No	No
Schindler 2	Yes	Yes	No	No
Schindler 3	Yes	No	Yes	No
Our Work	Yes	No	Yes	Yes
???	Yes	Yes	Yes	Yes

In the paper, we detailed

- the attack over Montgomery Ladder Algorithm

Thank you !

THALES

TELECOM ParisTech

References I

Onur Aciiçmez and Werner Schindler, *A vulnerability in RSA implementations due to instruction cache analysis and its demonstration on openssl*, Topics in Cryptology - CT-RSA 2008, The Cryptographers' Track at the RSA Conference 2008, San Francisco, CA, USA, April 8-11, 2008. Proceedings (Tal Malkin, ed.), Lecture Notes in Computer Science, vol. 4964, Springer, 2008, pp. 256–273.

Onur Aciiçmez, Werner Schindler, and Çetin Kaya Koç, *Improving Brumley and Boneh timing attack on unprotected SSL implementations*, Proceedings of the 12th ACM Conference on Computer and Communications Security, CCS 2005, Alexandria, VA, USA, November 7-11, 2005 (Vijay Atluri, Catherine Meadows, and Ari Juels, eds.), ACM, 2005, pp. 139–146.

References II

Paul C. Kocher, *On certificate revocation and validation*, Financial Cryptography, Second International Conference, FC'98, Anguilla, British West Indies, February 23-25, 1998, Proceedings (Rafael Hirschfeld, ed.), Lecture Notes in Computer Science, vol. 1465, Springer, 1998, pp. 172–177.

Peter L. Montgomery, *Modular multiplication without trial division*, Math. Comput. **44** (1985), no. 170, 519–521. MR 86e:11121

Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, October 1996, `http://www.cacr.math.uwaterloo.ca/hac/`.

References III

Werner Schindler, *A timing attack against RSA with the chinese remainder theorem*, Cryptographic Hardware and Embedded Systems - CHES 2000, Second International Workshop, Worcester, MA, USA, August 17-18, 2000, Proceedings (Çetin Kaya Koç and Christof Paar, eds.), Lecture Notes in Computer Science, vol. 1965, Springer, 2000, pp. 109–124.

______, *A combined timing and power attack*, Public Key Cryptography, 5th International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2002, Paris, France, February 12-14, 2002, Proceedings (David Naccache and Pascal Paillier, eds.), Lecture Notes in Computer Science, vol. 2274, Springer, 2002, pp. 263–279.

References IV

- ______, *Exclusive exponent blinding may not suffice to prevent timing attacks on RSA*, Cryptographic Hardware and Embedded Systems - CHES 2015 - 17th International Workshop, Saint-Malo, France, September 13-16, 2015, Proceedings (Tim Güneysu and Helena Handschuh, eds.), Lecture Notes in Computer Science, vol. 9293, Springer, 2015, pp. 229–247.
- Werner Schindler, François Koeune, and Jean-Jacques Quisquater, *Improving divide and conquer attacks against cryptosystems by better error detection / correction strategies*, Cryptography and Coding, 8th IMA International Conference, Cirencester, UK, December 17-19, 2001, Proceedings (Bahram Honary, ed.), Lecture Notes in Computer Science, vol. 2260, Springer, 2001, pp. 245–267.

References V

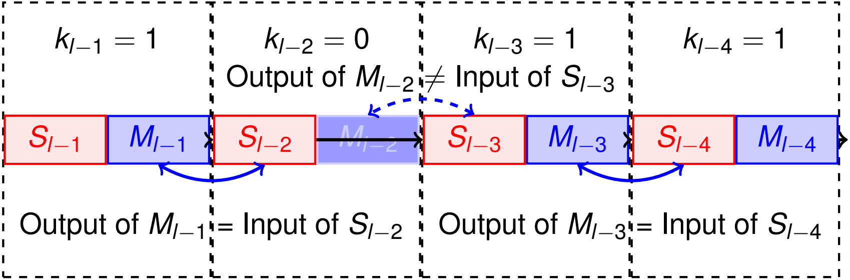
Werner Schindler and Colin D. Walter, *More detail for a combined timing and power attack against implementations of RSA*, Cryptography and Coding, 9th IMA International Conference, Cirencester, UK, December 16-18, 2003, Proceedings (Kenneth G. Paterson, ed.), Lecture Notes in Computer Science, vol. 2898, Springer, 2003, pp. 245–263.

Colin D. Walter and Susan Thompson, *Distinguishing exponent digits by observing modular subtractions*, Topics in Cryptology - CT-RSA 2001, The Cryptographer's Track at RSA Conference 2001, San Francisco, CA, USA, April 8-12, 2001, Proceedings (David Naccache, ed.), Lecture Notes in Computer Science, vol. 2020, Springer, 2001, pp. 192–207.

Details on experimental part

1. Power Analysis on OpenSSL :
   - micro-controller: a dual core LPC43S37 ARM Cortex-M0 / M4
   - scope: PICOSCOPE 6402C
   - sampling rate: 5 GSa/s
2. Electromagnetic Analysis on `mbedTLS` :
   - micro-controller: ARM Cortex-M4
   - scope Tektronix and EM Langer probe
   - sampling rate: 1 GSa/s

In Square and Multiply Always (SMA)



- The input/output value of each operation depend of the key bit value

ECC code example

To apply this biais on ECC: Find consecutives multiply square operation in elliptic curve adding and doubling operation

Algorithm 1: Mixed-Adding in PolarSSL

Input: (X, Y, Z) Jacobian coordinates of one point, (x, y) affine coordinates of the second point
Output: (X_R, Y_R, Z_R) Jacobian coordinates corresponding to the addition result

$T_1 \leftarrow Z \times_p Z$
$T_2 \leftarrow T_1 \times_p Z$
$T_1 \leftarrow T_1 \times_p x$
$T_2 \leftarrow T_2 \times_p y$
$T_1 \leftarrow T_1 -_p X$
$T_2 \leftarrow T_2 -_p Y$
if $T_1 = 0$ **then**
  if $T_2 = 0$ **then**
    $R \leftarrow \mathrm{DBL}(P)$
  else
    $R \leftarrow \infty$
  end if
end if
$\boxed{Z_3 \leftarrow Z \times_p T_1}$
$T_3 \leftarrow T_1 \times_p T_1$
$T_4 \leftarrow T_3 \times_p T_1$
$T_3 \leftarrow T_3 \times_p X$
$T_1 \leftarrow T_3 \times_{pi} 2$
$X_3 \leftarrow T_2 \times_p T_2$
$X_3 \leftarrow X_3 -_p T_1$
$X_3 \leftarrow X_3 -_p T_4$
$T_3 \leftarrow T_3 -_p X_3$
$T_3 \leftarrow T_3 \times_p T_2$
$T_4 \leftarrow T_4 \times_p Y$
$T_3 \leftarrow T_3 -_p T_4$
$X_R \leftarrow X_3$
$Y_R \leftarrow Y_3$
$Z_R \leftarrow Z_3$

Algorithm 2: Doubling in PolarSSL

Input: (X, Y, Z) Jacobian coordinates of the point
Output: (X_R, Y_R, Z_R) Jacobian coordinates corresponding to the doubling of the input point

$T_3 \leftarrow X \times_p X$
$T_2 \leftarrow Y \times_p Y$
$Y_3 \leftarrow T_2 \times_p T_2$
$X_3 \leftarrow X +_p T_2$
$X_3 \leftarrow X_3 \times_p X_3$
$X_3 \leftarrow X_3 -_p Y_3$
$X_3 \leftarrow X_3 -_p T_3$
$T_1 \leftarrow X_3 \times_{pi} 2$
$\boxed{Z_3 \leftarrow Z \times_p Z}$
$X_3 \leftarrow Z_3 \times_p Z_3$
$T_3 \leftarrow T_3 \times_{pi} 3$
$X_3 \leftarrow X_3 \times_p a$
$T_3 \leftarrow T_3 +_p X_3$
$X_3 \leftarrow T_3 \times_p T_3$
$X_3 \leftarrow X_3 -_p T_1$
$X_3 \leftarrow X_3 -_p T_1$
$T_1 \leftarrow T_1 -_p X_3$
$T_1 \leftarrow T_1 \times_p T_3$
$T_3 \leftarrow Y_3 \times_{pi} 8$
$Y_3 \leftarrow T_1 -_p T_3$
$T_1 \leftarrow Y +_p Z$
$T_1 \leftarrow T_1 \times_p T_1$
$T_1 \leftarrow T_1 -_p T_2$
$Z_3 \leftarrow T_1 -_p Z_3$
$X_R \leftarrow X_3$
$Y_R \leftarrow Y_3$
$Z_R \leftarrow Z_3$