Leakage Squeezing Revisited

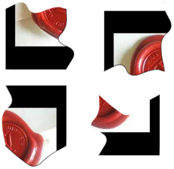
Vincent Grosso[1], François-Xavier Standaert[1], Emmanuel Prouff[2].

[1] ICTEAM/ELEN/Crypto Group, Université catholique de Louvain, Belgium.
[2] ANSSI, 51 Bd de la Tour-Maubourg, 75700 Paris 07 SP, France.

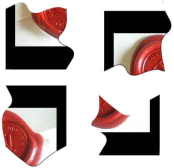
CARDIS 2013, Berlin.

Secret Sharing

Secret Sharing



Secret Sharing



$P($  $|$  $) = P($  $)$

Boolean Secret Sharing

Let X be a variable and M a random value uniformly chosen among the possible values of X.

Boolean Secret Sharing

Let X be a variable and M a random value uniformly chosen among the possible values of X.

Then X can be shared with the vector $(X \oplus M, M)$.

Boolean Secret Sharing

Let X be a variable and M a random value uniformly chosen among the possible values of X.

Then X can be shared with the vector $(X \oplus M, M)$.

M is random $\Rightarrow$ no information on X is available from the observation of M.

Boolean Secret Sharing

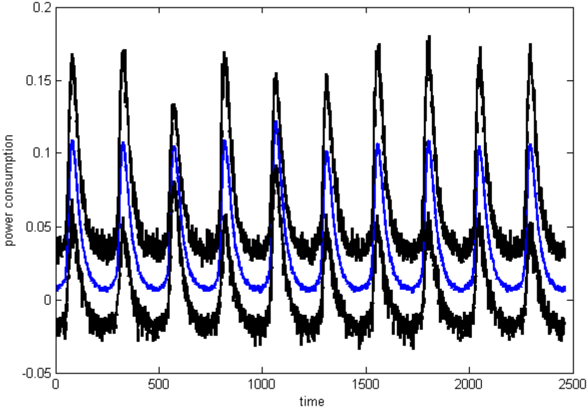
Let X be a variable and M a random value uniformly chosen among the possible values of X.

Then X can be shared with the vector $(X \oplus M, M)$.

M is random $\Rightarrow$ no information on X is available from the observation of M.

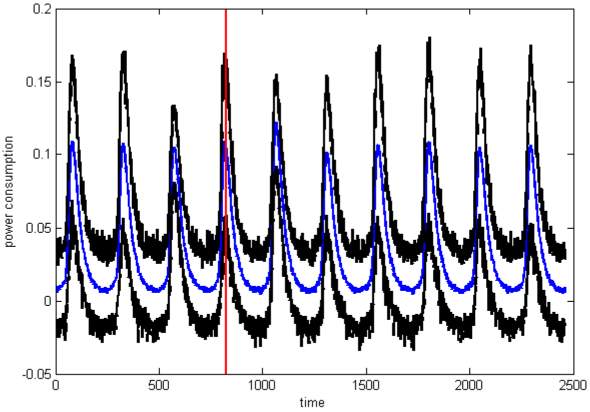
$X \oplus M$ one-time-pad of $X \Rightarrow$ no information on X is available from the observation of $X \oplus M$.

Masking ≃ Computing on Shared Values



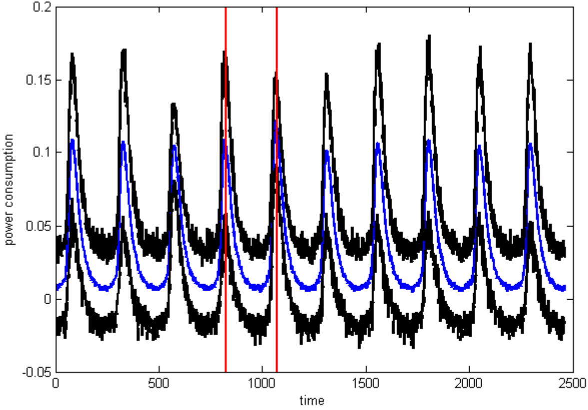
Traces contain information plus some noise.

Masking ≃ Computing on Shared Values



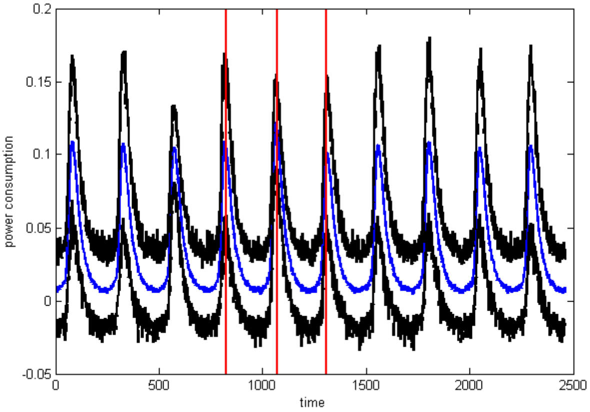
Unprotected device: unidimensional leakage is sufficient to mount an attack.

Masking ≃ Computing on Shared Values



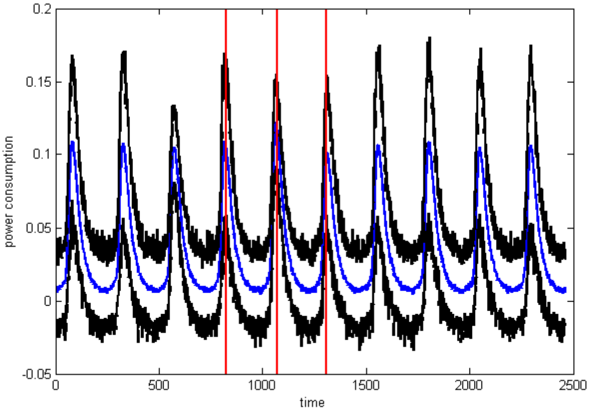
Protected software device with 2 shares: ideally bi-dimensional leakages are sufficient to mount an attack.

Masking $\simeq$ Computing on Shared Values



Protected software device with 3 shares: ideally tri-dimensional leakages are sufficient to mount an attack.

Masking ≃ Computing on Shared Values



Dimension of an attack : number of leakage points used.

Order (statistical)

Let X_i be r random variables, then the central mixed moment of orders $d_1, \ldots, d_r$ is defined by:

$$\mathsf{E}((X_1 - \mathsf{E}(X_1))^{d_1} \times \cdots \times (X_r - \mathsf{E}(X_r))^{d_r}).$$

Order (statistical)

Let X_i be r random variables, then the central mixed moment of orders $d_1, \ldots, d_r$ is defined by:

$$\mathsf{E}((X_1 - \mathsf{E}(X_1))^{d_1} \times \cdots \times (X_r - \mathsf{E}(X_r))^{d_r}).$$

The order of an attack is the smallest statical moment order ($d = \sum_i d_i$) used in the attack.

Order (statistical)

Let X_i be r random variables, then the central mixed moment of orders $d_1, \ldots, d_r$ is defined by:

$$\mathsf{E}((X_1 - \mathsf{E}(X_1))^{d_1} \times \cdots \times (X_r - \mathsf{E}(X_r))^{d_r}).$$

The order of an attack is the smallest statical moment order $(d = \sum_i d_i)$ used in the attack.

If we have noisy random variables, the moment becomes harder to estimate as the order increases.

Application to attack

- Order $\widetilde{\leftrightarrow}$ data complexity.
- Dimension $\widetilde{\leftrightarrow}$ computational complexity.

Application to attack

- Order $\widetilde{\leftrightarrow}$ data complexity.
- Dimension $\widetilde{\leftrightarrow}$ computational complexity.

The data complexity of a successful attack increases exponentially with the order of the attack (with noise as a basis).

Outline

1. Leakage squeezing
2. Assumption fulfilled
3. On the adversary condition
4. On the physical condition

Outline

1. Leakage squeezing
2. Assumption fulfilled
3. On the adversary condition
4. On the physical condition

Motivation

- Masking security holds if all masks are uniformly distributed $\Rightarrow$ strong randomness requirements in masked implementation. Leakage squeezing proposes to reduce the amount of entropy (i.e. the number of masks).
- Less masks can lead to more efficient implementation
- Preserved security order under two conditions:
  - Unidimensional leakage.
  - Linear leakage.

On the security conditions

- Unidimensional leakage only 1 share, adversarial condition:
  - points of interest are difficult to find
  - implementation always leak on all shares

  What happen if adversary obtain leakage on both shares?

On the security conditions

- Unidimensional leakage only 1 share, adversarial condition:
  - points of interest are difficult to find
  - implementation always leak on all shares

  What happen if adversary obtain leakage on both shares?

  Similar security as uniform masking :)

On the security conditions

- Unidimensional leakage only 1 share, adversarial condition:
  - points of interest are difficult to find
  - implementation always leak on all shares

  What happen if adversary obtain leakage on both shares?
  Similar security as uniform masking :)

- Linear leakage, physical condition:
  - classical hypothesis (Hamming weight leakage) for adversary but not for evaluation
  - cryptographic designers can hardly control the leakage function

  What happen if the leakage function is not linear?

On the security conditions

- Unidimensional leakage only 1 share, adversarial condition:
  - points of interest are difficult to find
  - implementation always leak on all shares

  What happen if adversary obtain leakage on both shares?
  Similar security as uniform masking :)

- Linear leakage, physical condition:
  - classical hypothesis (Hamming weight leakage) for adversary but not for evaluation
  - cryptographic designers can hardly control the leakage function

  What happen if the leakage function is not linear?
  The security order decrease, depending on the degree of the leakage function :(

Target

$C_{12} = \{\texttt{0x03}, \texttt{0x18}, \texttt{0x3f}, \texttt{0x55}, \texttt{0x60}, \texttt{0x6e}, \texttt{0x8c}, \texttt{0xa5}, \texttt{0xb2}, \texttt{0xcb}, \texttt{0xd6}, \texttt{0xf9}\}$ [NGD11]. Univariate security of order 2, if linear leakage.

$C_{16} = \{\texttt{0x10}, \texttt{0x1f}, \texttt{0x26}, \texttt{0x29}, \texttt{0x43}, \texttt{0x4c}, \texttt{0x75}, \texttt{0x7a}, \texttt{0x85}, \texttt{0x8a}, \texttt{0xb3}, \texttt{0xbc}, \texttt{0xd6}, \texttt{0xd9}, \texttt{0xe0}, \texttt{0xef}\}$ [BCG13]. Univariate security of order 3, if linear leakage.

Modification of hypothesis

- Multivariate (higher dimension) attacks. $\Rightarrow$ Adversarial condition.
  $I_1 = I(X \oplus m) + N_1,$

Modification of hypothesis

- Multivariate (higher dimension) attacks. $\Rightarrow$ Adversarial condition.
  $l_1 = l(X \oplus m) + N_1$, $l_2 = l(m) + N_2$

Modification of hypothesis

- Multivariate (higher dimension) attacks. $\Rightarrow$ Adversarial condition.
  $l_1 = l(X \oplus m) + N_1$, $l_2 = l(m) + N_2$

- Polynomial leakage. $\Rightarrow$ Physical condition.
  Let X be an internal value, X_i denotes the value of the i^{th} bit of X.
  For a linear leakage $\exists \{a_i\}_i$ s.t.

  $l(X) = \sum_i a_i X_i$

Modification of hypothesis

- Multivariate (higher dimension) attacks. $\Rightarrow$ Adversarial condition.
  $l_1 = l(X \oplus m) + N_1,\ l_2 = l(m) + N_2$

- Polynomial leakage. $\Rightarrow$ Physical condition.
  Let X be an internal value, X_i denotes the value of the i^{th} bit of X.
  For a polynomial leakage $\exists \{a_i\}_i, \{b_{i,j}\}_{i,j}, \ldots$ s.t.
  $l(X) = \sum_i a_i X_i$

  $+ \sum_i \sum_j b_{i,j} X_i \times X_j + \sum_i \sum_j \sum_k c_{i,j,k} X_i \times X_j \times X_k$

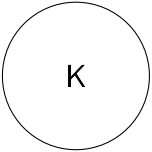
  For uniform masking, polynomial leakage does not mix different shares. It has thus no incidence on security order.

Framework

- Mutual information.

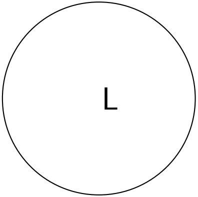
Framework

- Mutual information.



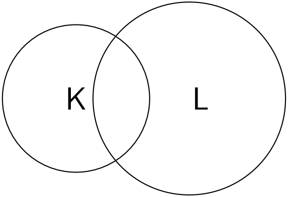
Framework

- Mutual information.



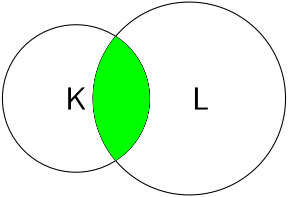
Framework

- Mutual information.



Framework

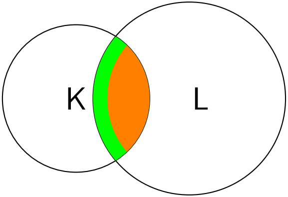
- Mutual information.



The maximum information available.

Framework

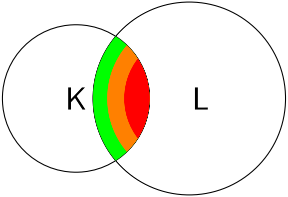
- Perceived information.



The maximum information available.

Framework

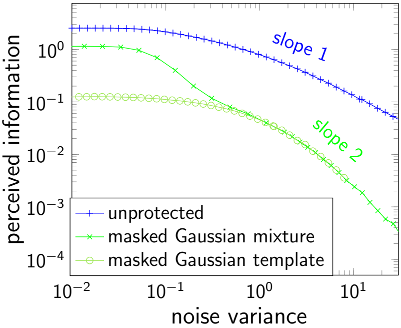
- Perceived information.



The maximum information available.

- Security analysis.
Resistance against nowadays adversary.

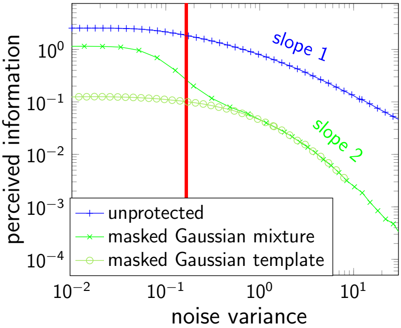
Intuition on information analysis

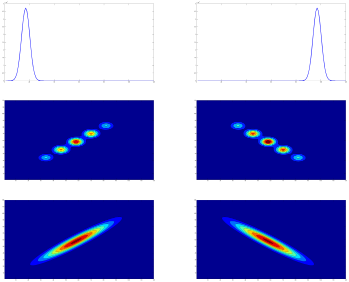


Information analysis can help to find the order of the smallest informative moment.

$$E((X + \sigma^2)^d)$$

Intuition on information analysis



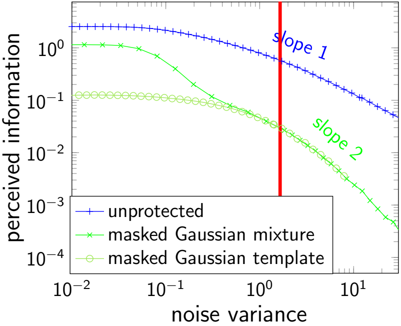


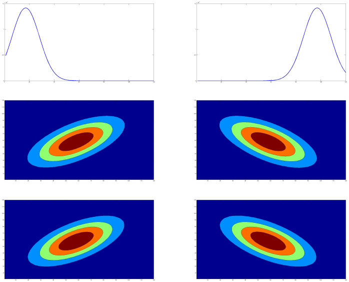
For unprotected device mean are different.

For protected device mean are equals but covariance are different.

Having the full distribution can help to discriminate keys ⇒ information in higher order.

Intuition on information analysis





For unprotected device difference is still in the mean.
For protected full distribution and Gaussian template model are close $\Rightarrow$ few information in higher order.

Outline

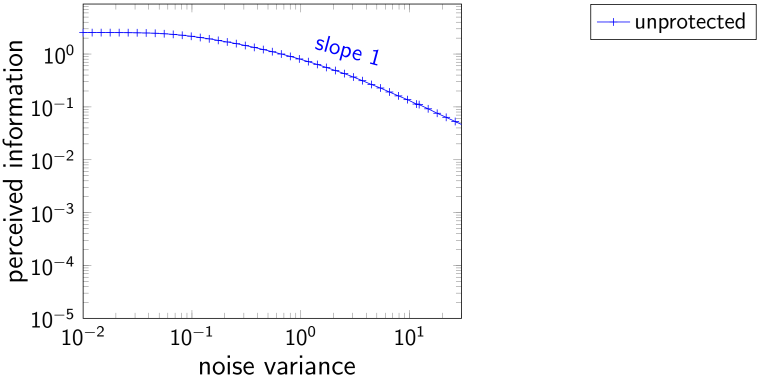
Hypothesis

- univariate leakage on 1 share :

$$l_1 = l(X \oplus m) + N$$

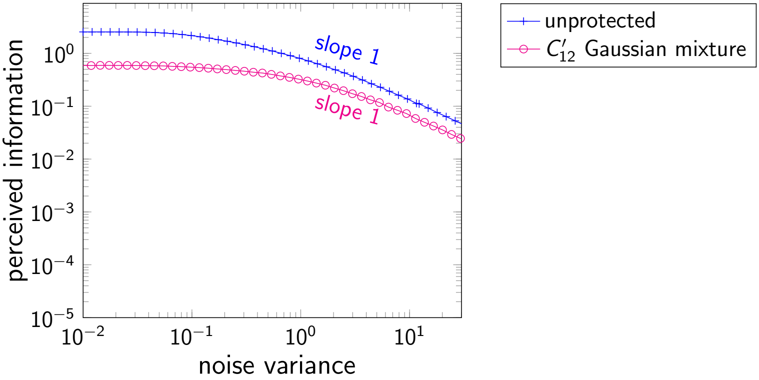
- leakage function is linear (Hamming weight)

Univariate case



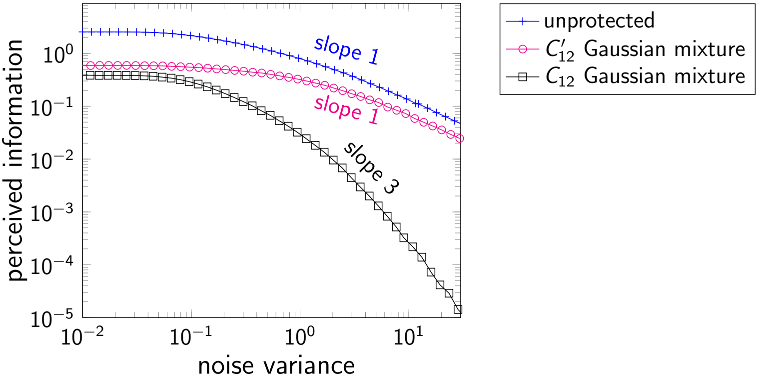
$$l_1 = H_w(X \oplus m) + N$$

Univariate case



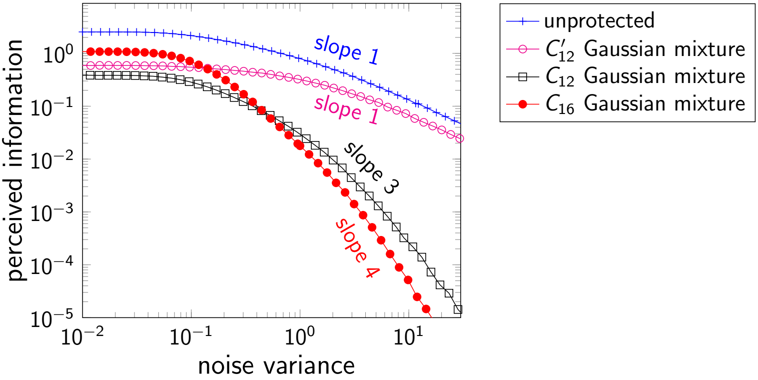
If random subset is used, then information about the key is available in the mean.

Univariate case



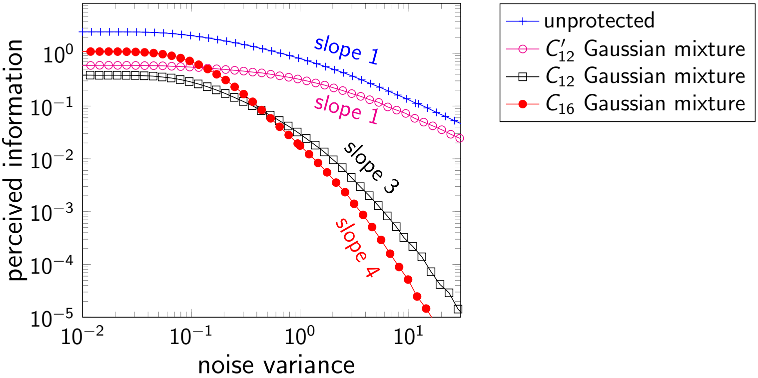
If carefully chosen subset is used, then information about the key is available in higher moment.

Univariate case



If carefully chosen subset is used, then information about the key is available in higher moment.

Univariate case



Such an attack is impossible for masking with 256 masks.
Since only 1 share is observed.

Conclusion classical Hypothesis

- C_{12}: information in 3^{rd} moment
- C_{16}: information in 4^{th} moment

As expected from previous works on leakage squeezing

Outline

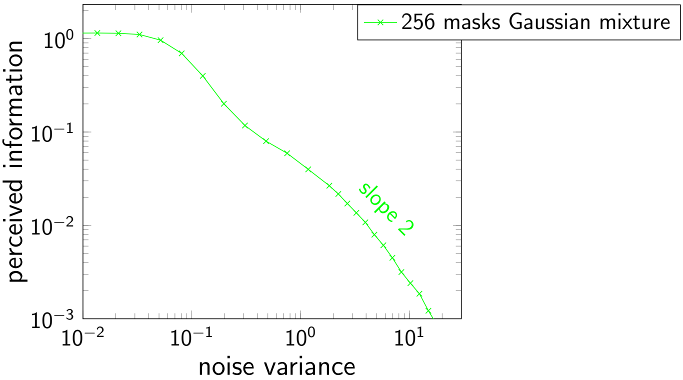
Hypothesis

- bivariate leakage on both shares :

$$l_1 = l(X \oplus m) + N_1, l_2 = l(m) + N_2$$

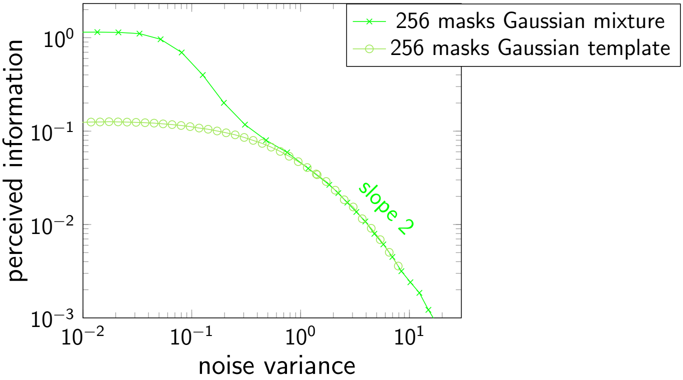
- leakage function is linear (Hamming weight)

Bivariate case



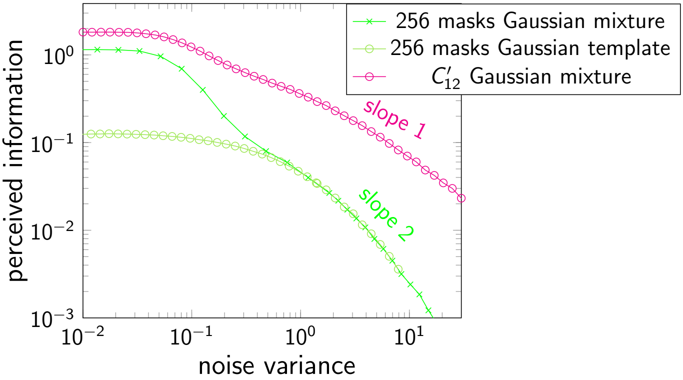
$$l_1 = H_w(X \oplus m) + N_1,\ l_2 = H_w(m) + N_2$$

Bivariate case



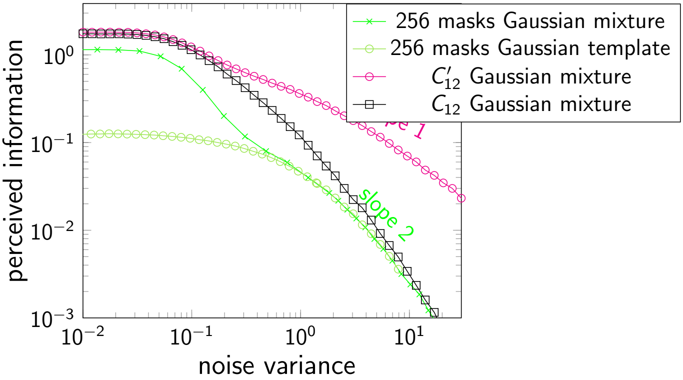
Using Gaussian mixture allows us to obtain more information for low noise. ∃ useful information in higher moments that gradually vanishes as noise increasing.

Bivariate case



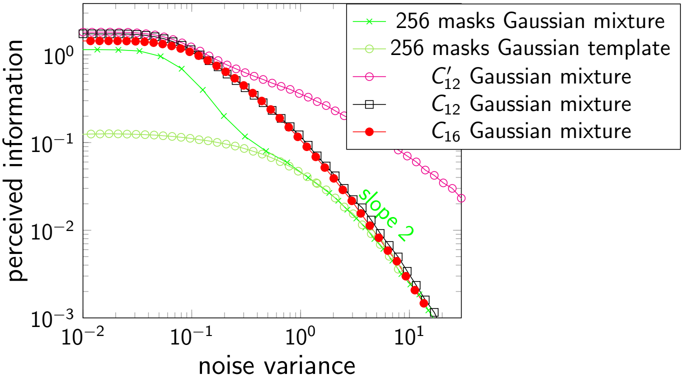
If random subset is used, then information about the key is available in the mean.

Bivariate case



If carefully chosen subset is used, then information about the key is available in the covariance matrix.

Bivariate case



If carefully chosen subset is used, then information about the key is available in the covariance matrix.

Conclusion adversarial condition

- C_{12}: information in 2^{nd} moment
- C_{16}: information in 2^{nd} moment
- uniform masking: information in 2^{nd} moment

The results are similar as for uniform masking :)

Outline

1. Leakage squeezing
2. Assumption fulfilled
3. On the adversary condition
4. On the physical condition

Hypothesis

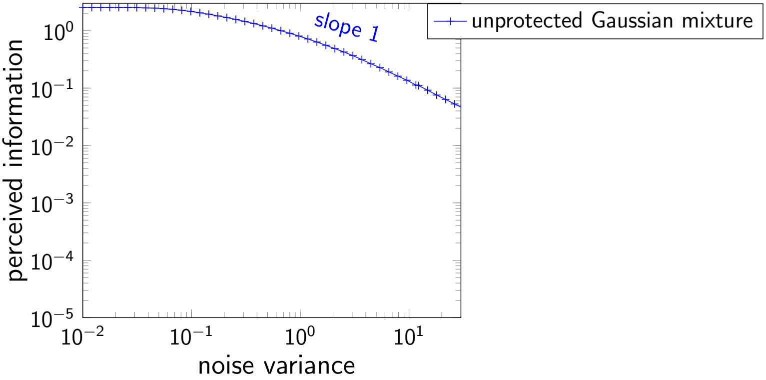
- univariate leakage on 1 share :

$$l_1 = l(X \oplus m) + N$$

- leakage function is polynomial

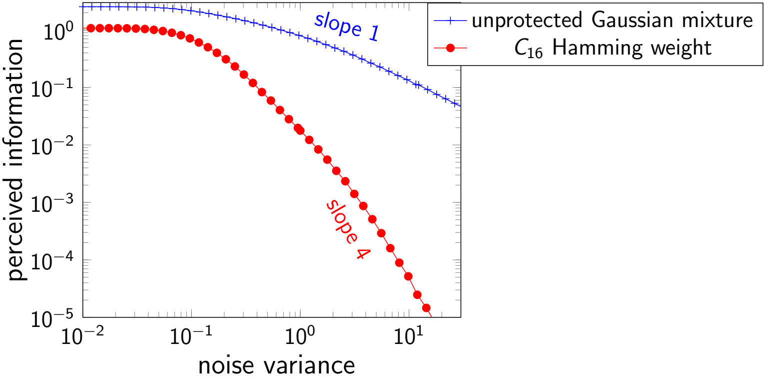
$$l(X) = \sum_i aX_i + \sum_i \sum_j bX_i \times X_j + \sum_i \sum_j \sum_k cX_i \times X_j \times X_k$$

Polynomial leakage case



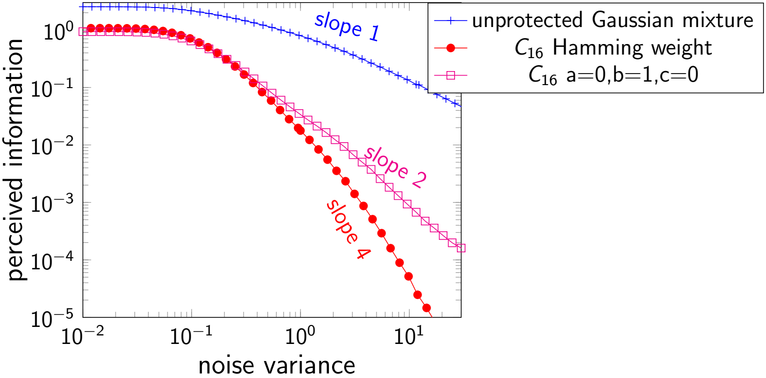
$$l(X) = \sum_i aX_i + \sum_i \sum_j bX_i \times X_j + \sum_i \sum_j \sum_k cX_i \times X_j \times X_k$$

Polynomial leakage case



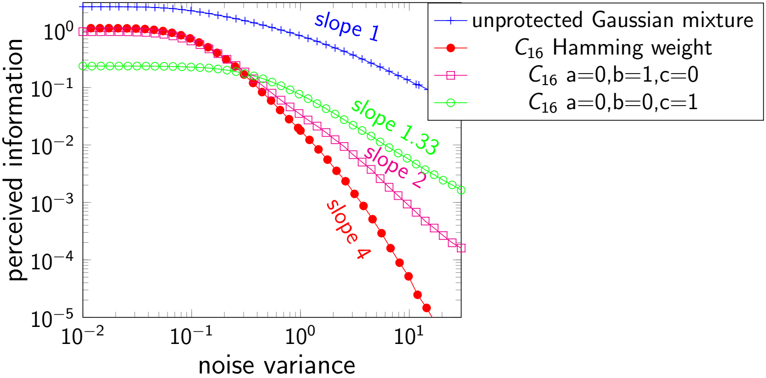
If $a = 1$, $b = 0$ and $c = 0$ we have Hamming weight model.

Polynomial leakage case



If $a = 0$, $b = 1$ and $c = 0$ the degree of the leakage function is 2, hence the slope of the IT curve is $\frac{4}{2}$.

Polynomial leakage case



If $a = 0$, $b = 0$ and $c = 1$ the degree of the leakage function is 3, hence the slope of the IT curve is $\frac{4}{3}$.

Conclusion physical condition

- Security order decreases with the degree of the polynomial deg_p.
- If the security for linear leakage function is of order d then the security order becomes $d' = d/deg_p$

$$\mathsf{E}((X)^d) = \mathsf{E}((X^{deg_p})^{d'})$$

- No impact for uniform masking.

The security order is decreasing depending on the degree of the leakage function :(

Conclusion

- Assumption fulfilled:
  - uniform masking $\Rightarrow$ no attack
  - leakage squeezing $\Rightarrow$ attack of large order

  As excepted from previous works on leakage squeezing.

Conclusion

- Assumption fulfilled:
  - uniform masking $\Rightarrow$ no attack
  - leakage squeezing $\Rightarrow$ attack of large order

  As excepted from previous works on leakage squeezing.

- On the adversary condition :
  - uniform masking $\Rightarrow$ attack of second order
  - leakage squeezing $\Rightarrow$ attack of second order with small degradation for low noise

  Similar security :)

Conclusion

- Assumption fulfilled:
  - uniform masking ⇒ no attack
  - leakage squeezing ⇒ attack of large order

  As excepted from previous works on leakage squeezing.

- On the adversary condition :
  - uniform masking ⇒ attack of second order
  - leakage squeezing ⇒ attack of second order with small degradation for low noise

  Similar security :)

- On the physical condition :
  - uniform masking ⇒ no attack
  - leakage squeezing ⇒ smaller slope of the curve

  Reduction of the slope depending on the degree of the leakage function:(

Shivam Bhasin, Claude Carlet, and Sylvain Guilley.
Theory of masking with codewords in hardware: low-weight dth-order correlation-immune boolean functions.
Cryptology ePrint Archive, Report 2013/303, 2013. http://eprint.iacr.org/.

Maxime Nassar, Sylvain Guilley, and Jean-Luc Danger.
Formal analysis of the entropy / security trade-off in first-order masking countermeasures against side-channel attacks.
In Daniel J. Bernstein and Sanjit Chatterjee, editors, *INDOCRYPT*, volume 7107 of *LNCS*, pages 22–39. Springer, 2011.

Emmanuel Prouff and Matthieu Rivain.
A generic method for secure SBox implementation.

In Sehun Kim, Moti Yung, and Hyung-Woo Lee, editors, *WISA*, volume 4867 of *LNCS*, pages 227–244. Springer, 2007.