

Estimating the Signal-to-Noise ratio under repeated sampling of the same centered signal: applications to side-channel attacks on a cryptoprocessor

Gilles R. Ducharme, Philippe Maurine

▶ **To cite this version:**

Gilles R. Ducharme, Philippe Maurine. Estimating the Signal-to-Noise ratio under repeated sampling of the same centered signal: applications to side-channel attacks on a cryptoprocessor. IEEE Transactions on Information Theory, 2018, 64 (9), pp.6333-6339. 10.1109/TIT.2018.2851217 . hal-01830075

HAL Id: hal-01830075
https://hal.science/hal-01830075

Submitted on 31 Mar 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Estimating the Signal-to-Noise ratio under repeated sampling of the same centered signal : applications to side-channel attacks on a cryptoprocessor

Gilles R. Ducharme, IMAG, Univ Montpellier, CNRS, Montpellier, France
Philippe Maurine, LIRMM, Univ Montpellier, CNRS, Montpellier, France

***Abstract*—This paper introduces an estimator of the signal-to-noise ratio in the framework where a noisy source emits the same signal a number n of times. The estimator has the structure of a U-statistic from which derives many desirable properties : it is unbiased, consistent and, being a Rao-Blackwellisation of existing proposals, is closer to optimal variance-wise. However, its variance is numerically difficult to evaluate and two approximations are obtained to facilitate its use in practice. These allow to quantify the improvement in variance, which is found to be substantial as the estimator needs roughly one third of the data previously required to perform similarly. Moreover, a simulation shows that the estimator is approximately normally distributed for n as small as 10, which allows for accurate inference. The estimator is then applied to data arising in a cryptanalysis, where the numerical security of a cryptoprocessor is tested against a side-channel attack. This problem is a representative of situations where the signal-to-noise ratio must be precisely estimated for small n. We derive a rigorous data-driven approach that is shown to much enhance the efficiency of standard side-channel attacks.**

***Index Terms*—Asymptotic normality, Cryptanalysis, Side-channel attack, Signal-to-noise ratio, U-statistic.**

I. Introduction

We assume the following framework: a received signal $\boldsymbol{M} = (M_1, ..., M_T)'$ (the prime denotes transposition) is observed at various time points t in the range $\{1, ..., T\}$. This received signal consists of an unknown deterministic signal $\boldsymbol{\tau} = (\tau_1, ..., \tau_T)'$ perturbed by a random noise $\boldsymbol{\eta} = (\eta_1, \ldots, \eta_T)'$. Hence the model is

$$\boldsymbol{M} = \boldsymbol{\tau} + \boldsymbol{\eta}. \tag{1}$$

We assume that the signal can be centered, i.e. $\sum_t \tau_t = 0$, and that $\boldsymbol{\eta}$ obeys the T-dimensional multinormal distribution, $\boldsymbol{\eta} \sim N_T(\mathbf{0}, \sigma_\eta^2 \mathbf{I})$ with expectation $\mathbf{0}$ and covariance matrix $\sigma_\eta^2 \mathbf{I}$, where $\mathbf{I}$ denotes the T-dimensional identity matrix. The signal-to-noise ratio is defined as

$$SNR = \boldsymbol{\tau}'\boldsymbol{\tau}/(T\sigma_\eta^2). \tag{2}$$

In our context, we further assume the same signal $\boldsymbol{\tau}$ of fixed length T is emitted n times, each time perturbed by a different random noise $\boldsymbol{\eta}$. Also $T > 2$ for reasons to be explained in Section **??**. This context is encountered in particular in cryptanalysis and more precisely in side-channel attacks (SCA) on cryptoprocessors (Diop et al. [**?**]), which is our motivating application. In SCA, a plaintext is sent for encryption to a cryptoprocessor, which mingles it with a secret key and produces the signal $\boldsymbol{\tau}$. An attacker tries to spy on this signal but gets to observe a version $\boldsymbol{M}$ of $\boldsymbol{\tau}$ perturbed with random noise $\boldsymbol{\eta}$. The experiment can be replicated n times, thus generating $\boldsymbol{M}_i = \boldsymbol{\tau} + \boldsymbol{\eta}_i$, $i = 1, ..., n$ where nothing can be assumed about $\boldsymbol{\tau}$ beyond its centering. For more details, see Section **??**.

Estimating the SNR is an important and difficult problem in signal processing. Here, we introduce the estimator

$$\widehat{SNR} = \frac{2}{n(n-1)} \sum_{i=1}^{n} \sum_{j=i+1}^{n} h(\boldsymbol{M}_i, \boldsymbol{M}_j), \tag{3}$$

where

$$h(\boldsymbol{M}_i, \boldsymbol{M}_j) = \frac{(T-2)\left\|\boldsymbol{M}_i + \boldsymbol{M}_j\right\|^2}{2T\left\|\boldsymbol{M}_i - \boldsymbol{M}_j\right\|^2} - \frac{1}{2}, \tag{4}$$

and $\|\cdot\|^2$ is the squared Euclidean norm. We establish its stochastic behavior and show that $\widehat{SNR}$ has theoretical and practical advantages over competitors, e.g. those of Diop et al. [**?**], Simon and Dolinar [**?**] and Coppola et al. [**?**]. In particular, we show it is unbiased and approximately normal for n as small as 10. We also show that (**??**) derives from an application of the Rao-Blackwell theorem so its variance is improved with respect to the competitors. This variance is however numerically difficult to evaluate and two simplified expressions are obtained. A comparison shows that these are close to the exact values and that our estimator requires roughly three times less data to perform similarly as these competitors. These advantages allow to establish accurate confidence intervals and derive powerful statistical tests pertaining to the SNR. Then, $\widehat{SNR}$ is applied to data arising in a cryptanalysis, where the numerical security of a cryptoprocessor is tested against a side-channel attack. This problem is a representative of situations where the SNR must be precisely estimated for small n. We derive a rigorous and principled data-driven approach that is shown to much enhance the efficiency of standard side-channel attacks.

The paper is organized as follows. Section **??** recalls some useful statistical results. Section **??** derives the theoretical properties of $\widehat{SNR}$ and presents the two approximations. Section **??** explains how accurate statistical inference can be produced about the SNR. Section **??** investigates the variance improvement of our estimator. Side-channel attacks (SCA)

on cryptoprocessors, the motivating application of the present work, are explained in Section **??**. A new data-driven $\widehat{SNR}$-based SCA is presented to illustrates the usefulness of the methods of the paper. A conclusion closes the paper.

II. Preliminary statistical results

A. Stochastic behavior of a U-statistic

An expression of the form (**??**) is a U-statistic. The function $h(\cdot,\cdot)$ is its kernel and is of order 2. Many theoretical results about the stochastic behavior of U-statistics are listed in Chapter 5 of Serfling [**?**]. In particular, let U_n be a U-statistic of order 2 whose variance exists and such that (hereafter $\mathbb{E}(X)$ and $\mathbb{V}(X)$ denote the expectation and variance of the random quantity X)

$$\mathbb{E}(h(\boldsymbol{M}_i,\boldsymbol{M}_j)) = \theta. \tag{5}$$

Then U_n is an unbiased estimator of θ, i.e. $\mathbb{E}(U_n) = \theta$. Moreover, setting $h_1(\boldsymbol{m}_1) = \mathbb{E}\left[h(\boldsymbol{m}_1,\boldsymbol{M}_2)\right]$ (here $\boldsymbol{m}_1$ is a fixed value of $\boldsymbol{M}_1$) with $\widetilde{h}_1(\boldsymbol{m}_1) = h_1(\boldsymbol{m}_1) - \theta$, we have

$$\mathbb{V}(U_n) = \frac{2}{n(n-1)}\left[2(n-2)\zeta_1^2 + \zeta_2^2\right], \tag{6}$$

where $\zeta_1^2 = \mathbb{E}(\widetilde{h}_1^2(\boldsymbol{M}_1))$ and $\zeta_2^2 = \mathbb{V}(h(\boldsymbol{M}_1,\boldsymbol{M}_2))$. Important for statistical inference is the fact that if $\zeta_1 > 0$, U_n is approximately normally distributed with expectation θ and variance $\mathbb{V}(U_n)$, whose dominant term is $4\zeta_1^2/n$.

B. Stochastic behavior of quadratic forms in normally distributed random vectors.

We recall that if $\boldsymbol{Z} \sim N_T(\boldsymbol{0},\sigma^2\mathbf{I})$, then $\|\boldsymbol{Z}+\boldsymbol{\mu}\|^2/\sigma^2$ has the non-central chi-square distribution $\chi^2_T(\boldsymbol{\mu}'\boldsymbol{\mu}/\sigma^2)$ with T degrees of freedom. We also recall for convenience the following well-known theorem.

Theorem 1. *Let $W_1 \sim\chi^2_{d_1}(\delta^2)$ and $W_2 \sim \chi^2_{d_2}(0)$ be independent random variables. Then $F = (d_2W_1)/(d_1W_2) \sim F^{d_1}_{d_2}(\delta^2)$, the non-central Fisher distribution with degrees of freedom (d_1,d_2) and non-centrality parameter δ^2. Moreover*

$$\mathbb{E}(F) = \frac{d_2(d_1+\delta^2)}{d_1(d_2-2)}, \qquad \text{if } d_2 > 2, \tag{7}$$

$$\mathbb{V}(F) = \frac{2d_2^2\left[(d_1+\delta^2)^2 + (d_1+2\delta^2)(d_2-2)\right]}{d_1^2(d_2-4)(d_2-2)^2} \qquad \text{if } d_2 > 4. \tag{8}$$

Finally $\mathbb{E}(F)$ and $\mathbb{V}(F)$ exists when $d_2 > 2$ and $d_4 > 4$ respectively.

III. Stochastic behavior of the estimator

A. Bias

Write $V(\boldsymbol{\eta}_i,\boldsymbol{\eta}_j) = \left\|\boldsymbol{\eta}_i+\boldsymbol{\eta}_j+\mathbf{2}\boldsymbol{\tau}\right\|^2 / \left\|\boldsymbol{\eta}_i-\boldsymbol{\eta}_j\right\|^2$ and rewrite $h(\boldsymbol{M}_i,\boldsymbol{M}_j) = h(\boldsymbol{\eta}_i,\boldsymbol{\eta}_j) = \frac{(T-2)}{2T}V(\boldsymbol{\eta}_1,\boldsymbol{\eta}_2) - \frac{1}{2}$, $h_1(\boldsymbol{M}_i) = h_1(\boldsymbol{\eta}_i)$, etc. It is easy to see that

$$\begin{pmatrix} \boldsymbol{\eta}_i-\boldsymbol{\eta}_j \\ \boldsymbol{\eta}_i+\boldsymbol{\eta}_j+2\boldsymbol{\tau} \end{pmatrix} \sim N_{2T}\left(\begin{pmatrix} 0 \\ 2\boldsymbol{\tau} \end{pmatrix}, 2\sigma_\eta^2\begin{pmatrix} \mathbf{I} & 0 \\ 0 & \mathbf{I} \end{pmatrix}\right). \tag{9}$$

From Section **??**, $\left\|\boldsymbol{\eta}_i-\boldsymbol{\eta}_j\right\|^2$ is distributed as a $2\sigma_\eta^2\chi^2_T(0)$ while $\left\|\boldsymbol{\eta}_i+\boldsymbol{\eta}_j+\mathbf{2}\boldsymbol{\tau}\right\|^2$ has for distribution a $2\sigma_\eta^2\chi^2_T(2\rho)$, upon introducing the notation $\rho = \boldsymbol{\tau}'\boldsymbol{\tau}/\sigma_\eta^2 = T\times SNR$. Thus, $V(\boldsymbol{\eta}_i,\boldsymbol{\eta}_j)$ is distributed as $\chi^2_T(2\rho)/\chi^2_T(0)$, where the two χ^2 are independent. From Theorem **??**, this is the stochastic representation of a non-central Fisher distribution with both degrees of freedom equal to T and non-centrality parameter 2ρ. Using (**??**) shows that $\widehat{SNR}$ is unbiased when $T > 2$.

B. The term ζ_2^2

From (**??**), when $T > 4$,

$$\zeta_2^2 = \frac{T^2+2\rho(\rho-2)+T(4\rho-1)}{T(T-4)}. \tag{10}$$

C. The term ζ_1^2

Let $\widetilde{\boldsymbol{\eta}}_1$ denote the fixed value of the random $\boldsymbol{\eta}_1$ corresponding to $\boldsymbol{m}_1$ and set $x = \boldsymbol{\tau}'\widetilde{\boldsymbol{\eta}}_1$, $y = \widetilde{\boldsymbol{\eta}}_1'\widetilde{\boldsymbol{\eta}}_1$. After completing the square and using the notation $\Psi_d(\cdot;\delta^2)$ for the cumulative distribution function of a $\chi^2_d(\delta^2)$, we get

$$\begin{aligned}\mathbb{P}\left[V(\tilde{\boldsymbol{\eta}}_1,\boldsymbol{\eta}_2) \le v\right] &= \\ &\mathbb{P}\left[\left\|\boldsymbol{\eta}_2+\tilde{\boldsymbol{\eta}}_1+2\boldsymbol{\tau}\right\|^2 \le v\left\|\boldsymbol{\eta}_2-\tilde{\boldsymbol{\eta}}_1\right\|^2\right] \\ &= \begin{cases} \Psi_T\left(b(v);\delta^2(v)\right) & \text{if } v \ge 1 \\ 1-\Psi_T\left(b(v);\delta^2(v)\right) & \text{if } v < 1, \end{cases}\end{aligned} \tag{11}$$

where

$$\delta^2(v) = \frac{4}{(1-v)^2}\left(\rho+(1+v)x+(1+v)^2y/4\right), \tag{12}$$

$$b(v) = \frac{4v}{(1-v)^2}\left(\rho+2x+y\right), \tag{13}$$

after noticing that the term σ_η^2 appears solely through $\boldsymbol{\tau}/\sigma_\eta$ and $\widetilde{\boldsymbol{\eta}}_1/\sigma_n$, so that scale invariance allows to set $\sigma_\eta^2 = 1$ without loss of generality.

Write $V(\tilde{\boldsymbol{\eta}}_1) = \mathbb{E}\left(V(\tilde{\boldsymbol{\eta}}_1,\boldsymbol{\eta}_2)\right)$. The positiveness of $V(\cdot,\cdot)$ entails $V(\tilde{\boldsymbol{\eta}}_1) = \int_0^\infty \mathbb{P}\left[V(\tilde{\boldsymbol{\eta}}_1,\boldsymbol{\eta}_2) \le v\right] dv$ which can in principle be computed via (**??**). Moreover because $\mathbb{E}\left(h_1(\boldsymbol{\eta}_1)\right) = SNR$, we have $\mathbb{E}\left(V(\boldsymbol{\eta}_1)\right) = (2\rho+T)/(T-2)$, so that

$$\zeta_1^2 = \left(\frac{T-2}{2T}\right)^2 \times \left[\mathbb{E}\left(V^2(\boldsymbol{\eta}_1)\right) - \left((2\rho+T)/(T-2)\right)^2\right]. \tag{14}$$

It is shown in the Appendix that

$$\mathbb{E}\left(V^2(\boldsymbol{\eta}_1)\right) = \int_0^{\infty}\int_{-\sqrt{\rho y}}^{\sqrt{\rho y}} \left\{\int_0^1 (1-\Psi_T\left(b(v);\delta^2(v)\right)dv + \int_1^{\infty}\Psi_T\left(b(v);\delta^2(v)\right)dv\right\}^2 \times \frac{\Gamma(\frac{T}{2})}{\sqrt{\pi}\Gamma(\frac{T-1}{2})}(1-x^2/\rho y)^{(T-3)/2}/\sqrt{\rho y} \times \psi_T(y;0)dxdy. \quad (15)$$

This triple integral is difficult to evaluate numerically. A first approximation is based on the following proposition whose proof is in the Appendix.

Proposition 1.

$$V(\tilde{\boldsymbol{\eta}}_1) = \frac{T+4x+y+4\rho}{T+y} + O(T^{-1/2}). \quad (16)$$

Injecting into $\mathbb{E}(h_1^2(\boldsymbol{\eta}_1))$ leads to the explicit expression :

$$\zeta_1^2 = \frac{(T-2)^2}{T^3}\rho [2(\rho-1) - 2e^{T/2}(T(\rho-1)-\rho)E_{T/2}(T/2) - T\rho e^{T/2}\left(E_{T/2}(T/2)\right)^2] + O(T^{-1/2}), \quad (17)$$

where $E_n(z)$ denotes the exponential integral function.

This approximation is only first order accurate and, for small T, is degraded by the asymmetry of a non-central χ^2. As shown in the Appendix, a Cornish-Fisher expansion leads to :

Proposition 2. *Let* $c = -2^3/(6\sqrt{T})$. *Then*

$$V(\tilde{\boldsymbol{\eta}}_1) \simeq \frac{1}{(T+y)^2 - 2c^2(T+2y)}\left\{c^2(4y+8x-2T) + (T+y)(T+4x+y+4\rho) + 4\left[c^2(T^2(2x+y+\rho)(1+y(4x+y+4\rho)) + 2T\left(3x^2+y^2+3y\rho+\rho^2+4x(y+\rho)\right) - 2c^2\left(2y\rho-2x^2+T(2x+y+\rho)\right)\right]^{1/2}\right\}. \quad (18)$$

Injecting into $\mathbb{E}(h_1^2(\boldsymbol{\eta}_1)))$ does not yield an explicit expression but turns out to be easy to evaluate numerically.

We numerically evaluate the accuracy of these two approximations for ζ_1. First the value of the triple integral defining ζ_1 is evaluated by 2000 Monte Carlo replications for various values of T and SNR. Then the two approximations are computed. The results appear in Table **??**, where MC refers to the Monte Carlo values of ζ_1.

As expected, the 1^{st} order approximation is less accurate, but can be useful when $T\geq$ 25 . The 2^{nd} order approximation offers much improvement in all investigated cases.

IV. Inference for SNR

Summing up, $\widehat{SNR}$ is an unbiased and consistent estimator of SNR approximately distributed as

$$N\left(SNR, \hat{\sigma}^2_{SNR} = \frac{2}{n(n-1)}\left[2(n-2)\hat{\zeta}_1^2 + \hat{\zeta}_2^2\right]\right), \quad (19)$$

where $\hat{\zeta}_1, \hat{\zeta}_2$ are obtained by plugging in the value of $\widehat{SNR}$ in (**??**) and (**??**).

Statistical inference about SNR derives from (**??**). Let z_α denote the α-th quantile of the $N(0,1)$ distribution. A two-sided confidence interval of approximate level $1-\alpha$ is

$$\widehat{SNR} \pm z_{1-\alpha/2}\hat{\sigma}_{SNR}. \quad (20)$$

Similarly the null hypothesis $H_0 : SNR \leq \theta_0$ can be rejected at approximate level α in favor of $H_1 : SNR > \theta_0$ when

$$\mathcal{Z}_n = \frac{(\widehat{SNR} - \theta_0)}{\hat{\sigma}_{SNR}} > z_{1-\alpha/2}. \quad (21)$$

Adaptation to other inference problems is obvious. The only point that remains to clarify regards the accuracy of the risks associated with these inferential procedures.

To investigate this, a simulation study was performed. For the pairs (SNR, T) listed in Table **??**, samples of size $n = 10$ and 20 where taken according to model (**??**). 95% confidence intervals (**??**) were computed using the 1^{st} and 2^{nd} order approximation and their coverage probabilities obtained from 5000 replications. Results appear in Table **??** and show that the true coverage probabilities are close to nominal for n as small as 10 when $SNR \geq 1$ and the 2^{nd} order approximation is used. When $SNR<1$, these approximations are less precise because the distribution of $\widehat{SNR}$ is bounded to the left. The 1^{st} order approximation performs close to nominal when $T \geq 25$. In view of these results, we recommend the 2^{nd} order approximation while the explicit and convenient 1^{st} order approximation can be used when $T \geq 25$.

V. Improvement in variance

Another unbiased estimator of SNR is

$$\widehat{SNR}_{i,i+1} = \frac{2}{n}\sum_{\substack{i=1\\ i:odd}}^{n} h(\boldsymbol{M}_i, \boldsymbol{M}_{i+1}), \quad (22)$$

which is a variant of proposals in e.g. Diop et al. [**?**] or Simon and Dolimar [**?**]. The central limit theorem ensures that the confidence interval $\widehat{SNR}_{i,i+1} \pm z_{1-\alpha/2}\sqrt{2}\hat{\zeta}_2/\sqrt{n}$ also has approximate level $1-\alpha$.

Computationally, $\widehat{SNR}_{i,i+1}$ and its other linear (e.g. a single sum of terms) variants are easier to work with, but inferior to $\widehat{SNR}$. First, they are not invariant to the pairs taken in $h(\cdot,\cdot)$, a serious flaw, and their variance is larger than that of $\widehat{SNR}$. To see this, note that the set of all $\boldsymbol{M}_i$, ranked by their first component, is a sufficient statistic. From general results on U-statistic (see Serfling [**?**], Theorem, p.176), $\widehat{SNR}$ in (**??**) is the expectation of $h(\boldsymbol{M}_i, \boldsymbol{M}_j)$ conditioned on this

TABLE I
VALUES OF ζ_1 BY MONTE-CARLO (MC) SIMULATIONS (2000 REPLICATIONS) ALONG WITH THOSE OBTAINED FROM THE 1^{st} AND 2^{nd} ORDER APPROXIMATIONS, FOR VARIOUS VALUES OF T AND SNR.

SNR	Approx.	0.1	1.0	5.0	10.0	25.0	50.0	100.0	200.0
T = 5	MC	0.132	0.551	1.877	3.660	8.636	16.78	33.38	65.86
	2^{nd}	0.149	0.555	1.883	3.476	8.221	16.12	32.90	63.47
	1^{st}	0.083	0.311	1.078	2.000	4.752	9.332	18.49	36.80
T = 10	MC	0.106	0.403	1.379	2.555	6.041	11.84	23.61	46.79
	2^{nd}	0.105	0.394	1.340	2.476	5.860	11.49	22.75	45.26
	1^{st}	0.080	0.303	1.042	1.933	4.592	9.017	17.86	35.56
T = 25	MC	0.066	0.248	0.851	1.585	3.747	7.316	14.64	28.99
	2^{nd}	0.065	0.247	0.843	1.560	3.696	7.251	14.36	28.58
	1^{st}	0.059	0.224	0.766	1.420	3.372	6.619	13.11	26.10
T = 50	MC	0.046	0.174	0.595	1.103	2.612	5.119	10.23	20.32
	2^{nd}	0.046	0.174	0.594	1.100	2.607	5.115	10.13	20.16
	1^{st}	0.043	0.166	0.567	1.050	2.492	4.892	9.690	19.29

TABLE II
ACTUAL COVERAGE PROBABILITIES (BASED ON 5000 REPLICATIONS) OF 95% CONFIDENCE INTERVAL (**??**) USING THE 1^{st} AND 2^{nd} ORDER APPROXIMATION FOR ζ_1.

		SNR								
T	n	Approx.	0.1	1	5	10	25	50	100	200
5	10	1^{st}	94.6	90.2	90.9	91.8	91.2	91.3	90.8	91.6
		2^{nd}	98.9	96.6	94.7	95.1	94.5	95.4	95.2	95.1
	20	1^{st}	90.7	85.2	87.8	86.4	86.1	85.8	85.6	85.2
		2^{nd}	98.2	95.8	93.9	94.5	94.2	93.9	94.8	94.1
10	10	1^{st}	89.9	89.4	91.2	91.7	90.1	91.9	91.3	90.8
		2^{nd}	98.1	96.8	95.8	94.9	94.2	95.0	94.4	94.3
	20	1^{st}	88.2	90.7	90.9	91.7	91.3	91.7	91.4	90.6
		2^{nd}	98.9	96.3	93.4	94.1	94.1	94.3	94.2	94.1
25	10	1^{st}	92.2	93.6	94.4	94.1	93.4	93.5	92.9	92.8
		2^{nd}	98.0	96.4	94.9	94.5	94.9	95.1	94.7	95.0
	20	1^{st}	92.5	93.3	92.2	92.5	93.2	92.9	92.9	92.6
		2^{nd}	98.8	96.4	94.1	94.1	94.4	94.2	94.8	94.9
50	10	1^{st}	94.1	93.8	93.6	94.1	94.3	94.0	94.4	94.4
		2^{nd}	97.7	96.4	94.5	94.7	95.0	94.8	95.4	95.2
	20	1^{st}	93.9	94.9	94.4	93.6	94.4	94.2	94.3	94.4
		2^{nd}	98.3	96.9	94.9	94.4	95.2	95.1	95.6	95.0

sufficient statistic. The Rao-Blackwell theorem ensures that this conditional expectation has a smaller variance than linear competitors and thus improves on them. We can quantify this improvement in variance by exploiting expression (i) of Lemma A in Serfling [**?**], p. 183, which yields :

$$\mathbb{V}(\widehat{SNR}) \approx \frac{4\zeta_1^2}{n} \leq \frac{2\zeta_2^2}{n} = \mathbb{V}(\widehat{SNR}_{i,i+1}). \qquad (23)$$

The ratio $\sqrt{2}\zeta_1/\zeta_2$ compares the length of confidence interval (**??**) to that based on $\widehat{SNR}_{i,i+1}$, It serves as a measure of the relative efficiency of statistical inferences (confidence interval, hypotheses test) based on $\widehat{SNR}$. Table **??** shows the values of this ratio for the pairs (SNR, T) in Table **??**, with a ratio of 0.5 indicating that a statistical procedure based on a linear estimator requires a sample of size $4n$ to perform similarly to one based on n received signal using $\widehat{SNR}$. The average of the entries in this table is approximately 0.55 showing that, overall, statistical inference based on $\widehat{SNR}$ requires roughly over three times less observations to perform similarly.

Note that other estimators of the SNR in the present context have been proposed, notably some based on correlations (Bershad and Rockmore [**?**]). Their stochastic behavior is largely unknown and will not investigate here.

VI. APPLICATION TO SIDE CHANNEL ATTACKS

Cryptoprocessors perform the calculations ciphering sensitive information. They apply algorithms that use secret keys and if an opponent obtains the key, the ciphered information

TABLE III
RATIO OF LENGTHS OF CONFIDENCE INTERVALS BASED ON $\widehat{SNR}$ AND $\widehat{SNR}_{i,i+1}$.

SNR	0.1	1.0	5.0	10.0	25.0	50.0	100.0	200.0
T = 5	0.18	0.32	0.33	0.34	0.33	0.37	0.33	0.33
T = 10	0.33	0.55	0.58	0.57	0.57	0.57	0.57	0.57
T = 25	0.36	0.62	0.66	0.66	0.66	0.66	0.66	0.65
T = 50	0.37	0.63	0.68	0.68	0.68	0.68	0.69	0.68

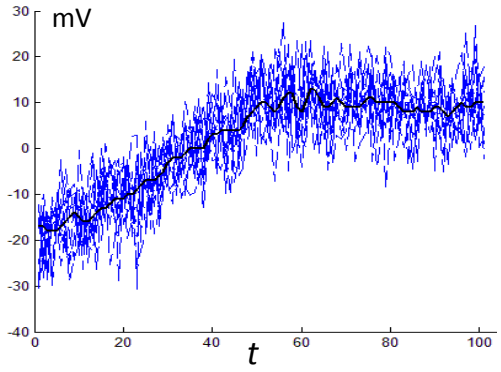


Fig. 1. EM curves ($n = 10$) from an AES

can easily be transformed back into plaintext. When the cryptoprocessor is ciphering, the plaintext, mingled with the secret key, gets converted into an analog signal $\boldsymbol{\tau}$. This conversion can leak information about $\boldsymbol{\tau}$ to be exploited by an opponent to recover the key. This is referred to as a side-channel attack (SCA) and constitutes one form of cryptanalysis. Among the most successful SCA are those based on the electromagnetic (EM) emanations as the cryptoprocessor manipulates the text/key combination.

EM-based SCA are easy to perform cryptanalyses because the attacker can send the plaintext for encryption a number n of times and observe, through an inexpensive sensor, the emanated EM radiations at various time points. The resulting EM curves $\boldsymbol{M}_i$, $i = 1, ..., n$, are modeled as in (**??**), where the $\boldsymbol{\eta}_i$ are random noises arising from various causes. The process is calibrated to provide a centered $\boldsymbol{\tau}$.

If the attacker can separate the noise from $\boldsymbol{\tau}$, parts of the key can be recovered. To give an idea of how this can be done, Figure **??** shows a sample of $n = 10$ EM curves $\boldsymbol{M}_i$ (in blue) while a cryptoprocessor was ciphering the same plaintext with the AES algorithm. The black curve is the (unknown to an attacker) signal $\boldsymbol{\tau}$. The AES algorithm involves so-called "rounds" and the oscillations of the black curve are related to the calculations performed during the last round using a part of the secret key. The knowledge of these oscillations, coupled with some other available informations, can reveal the calculations being performed and thus that part of the key. This indicates that a sophisticated SCA on the blue curves could be successful in exploiting the leakage to recover the key. The whole SCA process is however rather involved; we refer the interested reader to e.g. Brier et al. [**?**] for details.

When dealing with noisy measurements, filtering is a preprocessing technique that seeks to reduce the noise by focussing on the frequencies that best carry the signal. In general, a fruitful filtering requires some a priori knowledge about the informative frequencies, otherwise these may get filtered out. This is especially true in EM-based SCA where a small change in the position of the sensor can drastically alter the EM curves. In the present SCA context, as in many other applications, such a priori knowledge is unfortunately often unavailable.

Tiran et al. [**?**] have devised an approach to detect the informative frequencies in a EM-based SCA. They theorize a quantity they refer to as the Leakage-to-Noise Ratio (LNR) = $\boldsymbol{\tau}'_*\boldsymbol{\tau}_*/(T\sigma^2_\eta)$, where $\boldsymbol{\tau}_*$ is the part of $\boldsymbol{\tau}$ that is informative about the key. They argue that, in general, $LNR \leq SNR$. Then they translate by Fast Fourier (FF) transform the time domain received signal $\boldsymbol{M}_i$ of length T into the frequency domain over an interval $[F_{MIN}, F_{MAX}]$ whose bounds are chosen in relation with T. For the frequency interval of width δf centered on f, they introduce the quantity $LNRp(f) = SNR(f)/f$, where $SNR(f)$ is the SNR computed from the data at frequency f and the division by f penalizes the large frequencies. Thus large values of $LNRp(f)$ are indicative of interesting frequencies. They evaluate from the FF transformed $\boldsymbol{M}_i$ a crude approximation of $SNR(f)$ and retain only those frequencies where the corresponding $LNRp(f)$ is greater than an $ad\ hoc$ threshold. They set all others frequencies to zero and translate back the results into the time domain to get filtered signal that are then processed by a standard SCA to extract the leaked information about the secret key.

Here we use $\widehat{SNR}$ to supplement their approach with a better estimate of $LNRp(f)$ and exploit its stochastic properties to derive a rigorous and data-driven way of identifying the candidate frequencies to be retained. Our goal is to illustrate that the efficiency of standard SCA can be enhanced by the methods of the paper.

For this, we develop a multiple testing procedure based on (**??**) to test all pairs of hypotheses $H_0(f) : LNRp(f) \leq \lambda_0$ vs $H_1(f) : LNRp(f) > \lambda_0$ in the grid of values $f \in [F_{MIN}, F_{MAX}]$. The f values for which the tests reject $H_0(f)$ are the candidate frequencies carrying leakage information. Setting $\widehat{LNRp}(f) = \widehat{SNR}(f)/f$, the test statistic $\mathcal{Z}^*_n(f) = f \times (\widehat{LNRp}(f) - \lambda_0)/\hat{\sigma}_{SNR}$ is under $H_0(f)$ approximately $N(0, 1)$ and $H_0(f)$ gets rejected when $\mathcal{Z}^*_n(f) > z_{\alpha^*}$ where α^* is taken to control the risk of at least one false rejection (a family-wise Type 1 error) in this multiple testing situation.

To show the efficiency of the above data-driven filtering approach, an experiment was conducted in the following way. Recall from Section **??** that with $n = 10$, asymptotic normality offers a good approximation to the distribution of $\widehat{SNR}$. In a preliminary study, two sets of $n = 10$ EM curves of length $T = 3000$ were collected above an AES mapped into a cryptoprocessor-emulating FPGA (field-programmable gate array) device. The first set was collected with the EM sensor positioned far from the FPGA surface in order to obtain noisy data while the second set was collected with the sensor much closer to get small noise measurements. The $\widehat{SNR}(f)$ values were then computed for the 499 frequencies in $[0.8MHz, 400MHz]$ by steps of $0.8MHz$ with

$\delta f = 0.8MHz$. Here $\widehat{SNR}(f)$ varies from 1.21 to 14781, so it is reasonable to use the explicit first order approximation for ζ_1^2 given by (**??**). Also we took the standard $\alpha = 5\%$ with $\alpha^* = 1 - \alpha/499$, derived from the Bonferroni inequality. Subject-matter considerations, coupled with the attractive equilibrium between signal and noise, lead to the choice $\lambda_0 = 1$.

Panel (a) of Figure **??** shows the evolutions of $\sqrt{\widehat{LNRp}(f)}$ (the square root is used for increased clarity) with f for the noisy measurements while Panel (b) shows the same for the small noise data. The black dots correspond to the frequencies f where $H_0(f)$ has been rejected at level α^*. They suggest that measurements should be filtered so as to retain the frequencies in $[0.8; 54MHz] \cup [130MHz, 160MHz] \cup [240MHz, 260MHz]$ for noisy measurements, while for small noise, measurements should be filtered so as to keep frequencies $[0.8, 104MHz] \cup [120MHz, 260MHz] \cup [300MHz, 360MHz]$, if one aims at preserving the leakage that can be exploited by the subsequent SCA.

With this knowledge gained from the filtering step, a full-fledged SCA called a correlation power analysis (Brier et al. [**?**]) was applied to 5000 new EM-curves observed from the same apparatus and on their corresponding 5000 filtered measurements as described above. This allowed to compute the global Guessing Entropy (gGE), a figure of the merit of an attack, which is used to compare the efficiency of the SCA with and without filtering. The Guessing Entropy (GE) gives the average position of the correct sub-key of 8 bits in the ranking of the 256 possible sub-keys provided by the SCA. If the rank of a sub-key is one, the SCA successfully discloses the sub-key. The gGE is the average of the 16 GE values obtained for each of the 16 sub-keys constituting the whole 128 bits AES key. When gGE = 1, the whole key has been correctly disclosed by the SCA. Note that in SCA, the security of a ciphering device is typically evaluated using information theoretic metrics such as the entropy, while actual attacks are evaluated by empirical security metrics such as the above guessing entropy. See Standaert et al. [**?**] for a complete description of this and other information metrics and their relationships in the context of SCA.

Figure **??** shows the evolutions of the gGE with the number of processed curves for noisy and small noise data, with and without application of our data-driven filtering method. With small noise data, our method leads to a slight improvement in the convergence rate toward success (e.g. gGE = 1.0 with 3200 measurements with filtering versus 4000 without) of the SCA. For noisy data, the improvement is more significant.

VII. Conclusion

This paper proposes a new unbiased estimator of the SNR. Being a Rao-Blackwellisation, the estimator improved linear competitors variance-wise. THis operator is idempotent so that using it on $\widehat{SNR}$ gives back the same estimator. However, one intriguing possibility arises from the realization that one could extend (**??**) to a third (fourth etc.) order unbiased U-statistic that could yield further improved estimators of the SNR, perhaps initiating a convergence process toward optimality. More research is needed to evaluate the cost-benefit of this idea.

Acknowledgements

The authors would like to thank Prof. Serge B. Provost from The Western University, Ontario (Canada), for his helpful suggestion regarding the distribution of $V(\boldsymbol{\eta}_1)$. They also acknowledge the contribution of two anonymous reviewers and the associate editors for comments that led to much improvements.

References

[1] Bershad, N.J., Rockmore, A.J. (1974) : On estimating signal-to-noise ratio using the sample correlation coefficient. *IEEE Trans. Inf. Theory,* IT-20; 112-113.

[2] Brier, E., Clavier, C., Olivier, F. (2004) : Correlation power analysis with a leakage model. In *International Workshop on Cryptographic Hardware & Embedded Systems* (CHES)-2004 : Joye, M., Quisquater, J.-J. (eds.). LNCS, vol. 3156, pp. 16–29. Springer, Heidelberg.

[3] Coppola, R., Tabor, R., Buchsbaum, M.S. (1978) : Signal to Noise Ratio and Response Variability Measurements in Single Trial Evoked Potentials. *Electroencephalography and Clinical Neurophysiology*, 44: 214-222.

[4] Diop, I., Carbone, M., Ordas, S., Linge, Y. Liardet, P.Y., Maurine, P. (2015) : Collision for Estimating SCA Measurement Quality and Related Applications. In *Smart Card Research and Advanced Applications* - 14th International Conference, CARDIS 2015, Bochum, Germany, Revised Selected Papers.

[5] Serfling, R. J. (1980) : *Approximation Theorems of Mathematical Statistics*. Wiley, New York.

[6] Simon, M.K., Dolinar, S. (2006) : Signal-to-Noise Ratio Estimation. Chapter 6 in *Autonomous Software-Defined Radio Receivers for Deep Space Applications*, Jon Hamkins and Marvin K. Simon, editors, DESCANSO Monograph Series, Pasadena, California: NASA Jet Propulsion Laboratory.

[7] Standaert F.X., Malkin T.G., Yung M. (2009) : A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks. In: Joux A. (eds) $Advances\ in\ Cryptology$ - EUROCRYPT 2009. Lecture Notes in Computer Science, vol 5479. Springer, Berlin, Heidelberg.

[8] Tiran, S., Ordas, S., Teglia, Y., Agoyan, M., Maurine, P. (2014) : A model of the leakage in the frequency domain and its application to CPA and DPA. *J. Cryptographic Engineering.* **4**, 3, p.197-212.

[9] Watson, G.S. (1983) : *Statistics on Spheres*. Wiley, New York.

Appendix

We prove (**??**). In principle, the evaluation of $\mathbb{E}\left(V^2(\boldsymbol{\eta}_1)\right)$ requires a T-fold integration over the density of $\boldsymbol{\eta}_1$. But $\delta^2(v)$ and $b(v)$ being functions of x, y solely we need only the joint density $f_{(X,Y)}(x, y)$, where $X = \boldsymbol{\tau}'\boldsymbol{\eta}_1, Y = \boldsymbol{\eta}_1'\boldsymbol{\eta}_1$ and, by scale invariance, $\boldsymbol{\eta}_1 \sim N_T(\mathbf{0}, \mathbf{I})$. Now the marginal density of Y is easily seen to be that of a $\chi^2_T(0)$:

$$_T(y; 0) = \frac{1}{2^{T/2}\Gamma(\frac{T}{2})} y^{T/2-1} e^{-y/2}, \qquad y > 0.$$

As for the conditional density of $(X \mid Y = y)$, we use the following argument. The random vector $\boldsymbol{\eta}_1$ has the stochastic representation $\boldsymbol{\eta}_1 = \sqrt{Y}U$, where $\boldsymbol{U} = \boldsymbol{\eta}_1 / \|\boldsymbol{\eta}_1\|$ and Y and $\boldsymbol{U}$ are independent with $\boldsymbol{U}$ being a directional vector uniformly distributed over the T-dimensional unit sphere. Hence if $\boldsymbol{t}$ denotes the unit vector $\boldsymbol{\tau}/\|\boldsymbol{\tau}\|$, the event $\{X = x\}$ = $\{\boldsymbol{t}'\boldsymbol{\eta}_1/\|\boldsymbol{\eta}_1\| = x/(\|\boldsymbol{\tau}\|\,\|\boldsymbol{\eta}_1\|)\} = \left\{\boldsymbol{t}'\boldsymbol{U} = x/(\|\boldsymbol{\tau}\|\sqrt{Y})\right\}$. From this we get

$$f_{(X|Y)}(x \mid y) = \mathbb{P}\left[\boldsymbol{t}'\boldsymbol{U} = x/\sqrt{\rho Y} \mid Y = y\right], \qquad (24)$$

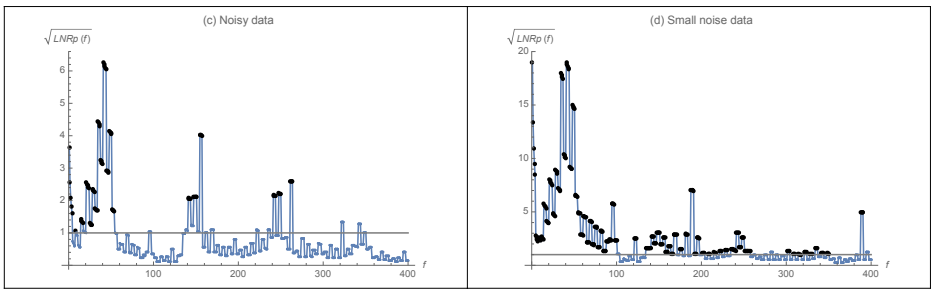


Fig. 2. (a) $\sqrt{\widehat{LNRp}(f)}$ for noisy measurements (b) $\sqrt{\widehat{LNRp}(f)}$ for small noise measurements. The gray line is the threshold value $\lambda_0 = 1$. The dots correspond to values of f where $H_0(f)$ are rejected at a family-wise error rate of 5%.

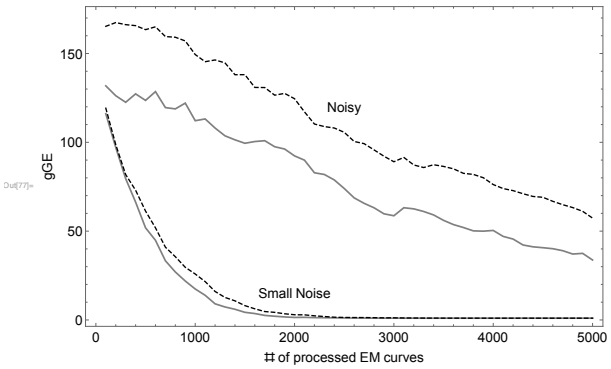


Fig. 3. Evolutions of the gGE for noisy and small noise data, with (solid) and without (dashed) application of our data-driven $SNR-$based filtering method.

Now the independence between Y and $\boldsymbol{U}$ allows getting rid of the conditioning :

$$f_{(X|Y)}(x \mid y) = \mathbb{P}\left[\boldsymbol{t}'\boldsymbol{U} = x/\sqrt{\rho y}\right],$$

while the uniformity of $\boldsymbol{U}$ yields for $-\sqrt{\rho y} < x < \sqrt{\rho y}$ (see Watson [**?**], p. 45, eq. 2.2.7),

$$\mathbb{P}\left[\boldsymbol{t}'\boldsymbol{U} = x/\sqrt{\rho y}\right] = \frac{\Gamma(\frac{T}{2})}{\sqrt{\pi}\Gamma(\frac{T-1}{2})}(1 - x^2/\rho y)^{(T-3)/2}/\sqrt{\rho y}. \quad (25)$$

Hence $f_{(X,Y)}(x, y) =$

$$\frac{\Gamma(\frac{T}{2})}{\sqrt{\pi}\Gamma(\frac{T-1}{2})}(1 - x^2/\rho y)^{(T-3)/2}/\sqrt{\rho y} \times \psi_T(y; 0), \quad (26)$$

over the domain $y > 0, -\sqrt{\rho y} < x < \sqrt{\rho y}$. The result follows from collecting the above.

Next, we prove Propositions **??** and **??**. A normalized non-central χ^2 approaches a $N(0, 1)$ as its degree of freedom increases. Here this translates into

$$\Psi_T\left(b(v); \delta^2(v)\right) \quad \simeq \quad \Phi\left(\frac{b(v) - (T + \delta^2(v))}{\sqrt{2(T + 2\delta^2(v))}}\right), \quad (27)$$

where $T + \delta^2(v)$ and $2(T + 2\delta^2(v))$ are respectively the expectation and variance of the $\chi^2_T(\delta^2(v))$ and $\Phi(\cdot)$ is the CDF of the standard $N(0, 1)$ distribution. Now the relation $\Phi(0) = 1/2$ suggest solving for v the equation

$$b(v) - (T + \delta^2(v)) = 0,$$

which leads to (**??**). As for Proposition 2, the asymmetry of the $\chi^2_T(\delta^2(v))$ suggests solving for v the equation

$$\frac{b(v) - (T + \delta^2(v))}{\sqrt{2(T + 2\delta^2(v))}} = c$$

for some constant c near 0 to be determined. Now, the two terms Cornish-Fisher expansion of a $\chi^2_T(\delta^2(v))$ at $1/2$ is $-\kappa/6 + O(T^{-1})$, where $\kappa = \sqrt[3]{2}(T + 3\delta^2(v))/\sqrt[3]{T + 2\delta^2(v)}$. Analysis of κ shows that it is rather stable over a large range of (SNR, T) values and that $c = -2^3/(6\sqrt{T})$ provides a good compromise .

View publication stats