Formal Security Proofs via Doeblin Coefficients

Optimal Side-channel Factorization from Noisy Leakage to Random Probing

Julien Béguinot[1], Wei Cheng[2,1], Sylvain Guilley[2,1], Olivier Rioul[1]

[1]***LTCI, Télécom Paris, Institut Polytechnique de Paris****, Palaiseau, France*
[2]***Secure-IC S.A.S.****, Paris, France & San Mateo, CA, USA*

CRYPTO 2024, Santa Barbara, CA, USA

Long version $\Longrightarrow$ ia.cr/2024/199

Context

- **ISW'03** Masking and security proof in the t-threshold probing model

Context

- **ISW’03** Masking and security proof in the t-threshold probing model
- **PR’13** Noisy leakage model (Euclidean norm bias) ; subsequence decomposition

Context

- **ISW'03** Masking and security proof in the t-threshold probing model
- **PR'13** Noisy leakage model (Euclidean norm bias) ; subsequence decomposition
- **DDF'14** Reduction from noisy leakage (total variation information) to the random probing model ; reduction from random probing to t-threshold probing model

Context

- **ISW’03** Masking and security proof in the t-threshold probing model
- **PR’13** Noisy leakage model (Euclidean norm bias) ; subsequence decomposition
- **DDF’14** Reduction from noisy leakage (total variation information) to the random probing model ; reduction from random probing to t-threshold probing model
- **DFS’15** Bound in terms of MI with DDF’14 leveraging Pinsker’s inequality

Context

- **ISW'03** Masking and security proof in the *t*-threshold probing model
- **PR'13** Noisy leakage model (Euclidean norm bias) ; subsequence decomposition
- **DDF'14** Reduction from noisy leakage (total variation information) to the random probing model ; reduction from random probing to *t*-threshold probing model
- **DFS'15** Bound in terms of MI with DDF'14 leveraging Pinsker's inequality
- **PGMP'19** (Average) relative error : direct proof (PR'13) ; indirect proof (DDF'14)

Context

- **ISW'03** Masking and security proof in the *t*-threshold probing model
- **PR'13** Noisy leakage model (Euclidean norm bias) ; subsequence decomposition
- **DDF'14** Reduction from noisy leakage (total variation information) to the random probing model ; reduction from random probing to *t*-threshold probing model
- **DFS'15** Bound in terms of MI with DDF'14 leveraging Pinsker's inequality
- **PGMP'19** (Average) relative error : direct proof (PR'13) ; indirect proof (DDF'14)
- **BCG+'23** Use of Mrs. Gerber's lemma to prove security of encoding using MI

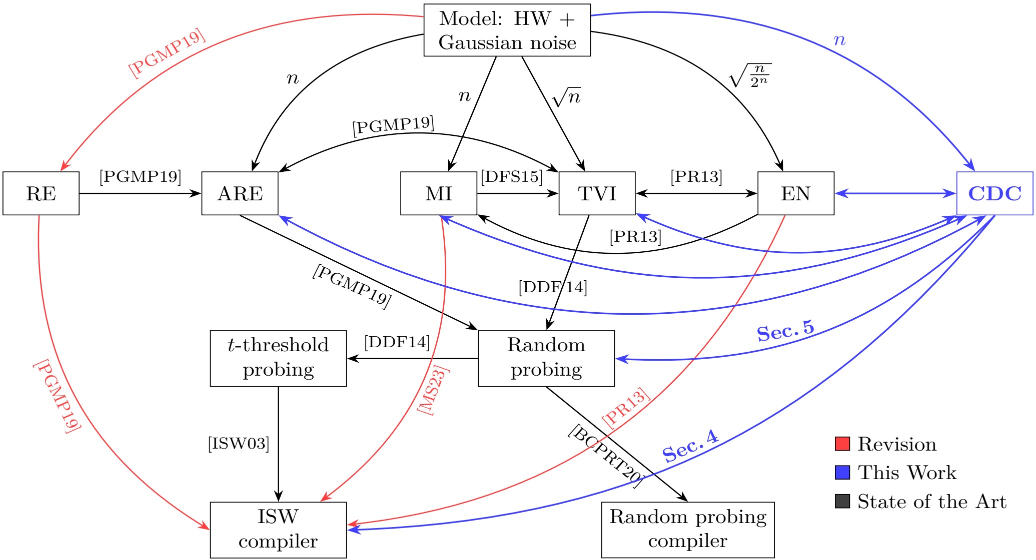
Context

- **ISW'03** Masking and security proof in the t-threshold probing model
- **PR'13** Noisy leakage model (Euclidean norm bias) ; subsequence decomposition
- **DDF'14** Reduction from noisy leakage (total variation information) to the random probing model ; reduction from random probing to t-threshold probing model
- **DFS'15** Bound in terms of MI with DDF'14 leveraging Pinsker's inequality
- **PGMP'19** (Average) relative error : direct proof (PR'13) ; indirect proof (DDF'14)
- **BCG+'23** Use of Mrs. Gerber's lemma to prove security of encoding using MI
- **MS'23** Direct proof (PR'13) for MI extending BCG+'23 to computations

Context

- **ISW'03** Masking and security proof in the t-threshold probing model
- **PR'13** Noisy leakage model (Euclidean norm bias) ; subsequence decomposition
- **DDF'14** Reduction from noisy leakage (total variation information) to the random probing model ; reduction from random probing to t-threshold probing model
- **DFS'15** Bound in terms of MI with DDF'14 leveraging Pinsker's inequality
- **PGMP'19** (Average) relative error : direct proof (PR'13) ; indirect proof (DDF'14)
- **BCG+'23** Use of Mrs. Gerber's lemma to prove security of encoding using MI
- **MS'23** Direct proof (PR'13) for MI extending BCG+'23 to computations
- **Our work** : Complementary Doeblin Coefficient : optimal reduction from noisy leakage to random probing model ; direct proof (PR'13) and indirect proof (DDF'14) + points several flaws in previous derivations from PR'13, DDF'14, DFS'15, PGMP'19 and MS'23.

Context



Model: HW + Gaussian noise
RE
ARE
MI
TVI
EN
CDC
t-threshold probing
Random probing
ISW compiler
Random probing compiler
[PGMP19]
[PGMP19]
[PGMP19]
[PGMP19]
[PGMP19]
[DFS15]
[PR13]
[PR13]
[PR13]
[DDF14]
[DDF14]
[ISW03]
[MS23]
[BCPRT20]
Sec. 5
Sec. 4
n
n
n
$\sqrt{n}$
$\sqrt{\frac{n}{2^n}}$
Revision
This Work
State of the Art

Adversary's Model

Let K be the secret. Adversary obtains side information $(Y_1, \ldots, Y_l)$ about sensitive values $(X_1, \ldots, X_l)$ through $\varphi_i = (X_i \to Y_i)$, $i = 1, \ldots, l$. $\varphi = (\varphi_1, \ldots, \varphi_l)$ is restricted to limit the adversary's abilities :

- **t-threshold probing** : t identity channels and opaque channels otherwise ;
- **$\overline{\mathcal{E}}$-random probing** : $\mathcal{E}$-erasure channels ;
- **δ-noisy** : δ-noisy channels with respect to $\mathscr{D}$ i.e. $\mathscr{D}(X;Y) \leqslant \delta$ where X is uniformly distributed and Y is the output of the side-channel $X \to Y$;
- **(σ, f)-additive** : channels $X \to Y \triangleq f(X) + \sigma N$.

Adversary's Model

Let K be the secret. Adversary obtains side information $(Y_1, \ldots, Y_l)$ about sensitive values $(X_1, \ldots, X_l)$ through $\varphi_i = (X_i \to Y_i)$, $i = 1, \ldots, l$. $\varphi = (\varphi_1, \ldots, \varphi_l)$ is restricted to limit the adversary's abilities :

- ***t*-threshold probing** : t identity channels and opaque channels otherwise ;
- **$\overline{\mathcal{E}}$-random probing** : $\mathcal{E}$-erasure channels ;
- **δ-noisy** : δ-noisy channels with respect to $\mathcal{D}$ i.e. $\mathcal{D}(X;Y) \leqslant \delta$ where X is uniformly distributed and Y is the output of the side-channel $X \to Y$;
- **(σ, f)-additive** : channels $X \to Y \triangleq f(X) + \sigma N$.

Let $\mathrm{rank}(K|Y)$ be the rank of the correct key in the ranking produced by the adversary upon observation Y. The performance of the attack is usually assessed using :

1. Success rate of order o, (SR_o) : $\mathbb{P}_{s,o}(K|Y) \triangleq \mathbb{P}(\mathrm{rank}(K|Y) \leqslant o)$
2. Guessing entropy (GE) : $G(K|Y) \triangleq \mathbb{E}\{\mathrm{rank}(K|Y)\}$

Multiple Leakage Measures

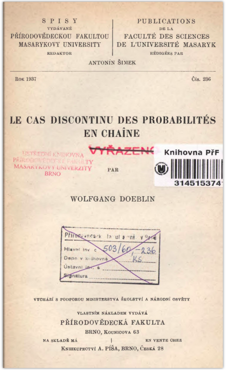
- Mutual Information : $I(X;Y) = D_{\mathrm{KL}}(p_{XY} \| p_X p_Y) = \sum\!\!\!\!\!\!\int p_{XY}(x,y) \log \frac{p_{X,Y}(x,y)}{p_X(x) p_Y(y)}$.
- Total Variation Information : $\Delta(X;Y) = D_{\mathrm{TV}}(p_{XY} \| p_X p_Y) = \frac{1}{2} \| p_{XY} - p_X p_Y \|_1$.
- Maximal Leakage : $\mathcal{L}(X \to Y) = \log \sum\!\!\!\!\!\!\int_y \sup_x p_{Y|X}(y|x)$.
- Euclidean Norm bias : $\beta(X;Y) = \mathbb{E}_Y \| p_{X|Y}(\cdot|Y) - p_X \|_2$.
- Relative Error : $RE(X;Y) = \sup_{x,y} \left| \frac{p_{X|Y}(x|y)}{p_X(x)} - 1 \right|$.
- Average Relative Error : $ARE(X;Y) = \mathbb{E}_Y \left[\sup_x \left| \frac{p_{X|Y}(x|Y)}{p_X(x)} - 1 \right| \right]$.
- Complementary Doeblin Coefficient :

$$\overline{\mathcal{E}}(X \to Y) = 1 - \sum\!\!\!\!\!\!\!\int_y \inf_x p_{Y|X}(y|x) = \mathbb{E}_Y \left[\sup_x \left(1 - \frac{p_{X|Y}(x|Y)}{p_X(x)} \right) \right].$$

TELECOM Paris
IP PARIS

Wolfgang Doeblin (Vincent Döblin)

Here
died at the age of 25
on June 21, 1940
Vincent Döblin
mathematical genius


SPISY VYDÁVANÉ PŘÍRODOVĚDECKOU FAKULTOU MASARYKOVY UNIVERSITY REDAKTOR | PUBLICATIONS DE LA FACULTÉ DES SCIENCES DE L'UNIVERSITÉ MASARYK RÉDIGÉES PAR

ANTONÍN ŠIMEK

ROK 1937 Čís. 236

LE CAS DISCONTINU DES PROBABILITÉS EN CHAÎNE

PAR

WOLFGANG DOEBLIN

VYCHÁZÍ S PODPOROU MINISTERSTVA ŠKOLSTVÍ A NÁRODNÍ OSVĚTY

VLASTNÍM NÁKLADEM VYDÁVÁ PŘÍRODOVĚDECKÁ FAKULTA BRNO, KOUNICOVA 63

NA SKLADĚ MÁ | EN VENTE CHEZ
KNIHKUPECTVÍ A. PÍŠA, BRNO, ČESKÁ 28

The discontinuous case of probability chains (1937)

Wolfgang Döblin, ca. 1935

Erasure Channel

Definition (Erasure Channel)

The channel

$$X \to \boxed{\mathrm{EC}_{\mathcal{E}}^{\perp}} \to Y \tag{1}$$

is said to be an erasure channel with erasure probability $\mathcal{E} \in [0, 1]$ and special erasure symbol $\perp$ if on input x, $\mathrm{EC}_{\mathcal{E}}^{\perp}$ outputs x with probability

$$\overline{\mathcal{E}} = 1 - \mathcal{E} \tag{2}$$

and the special erasure symbol $\perp$ otherwise (with probability $\mathcal{E}$). That is

$$\begin{cases} p_{Y|X}(\perp|x) = \mathcal{E} \\ p_{Y|X}(x|x) = \overline{\mathcal{E}} \end{cases} \qquad (\forall x \neq \perp). \tag{3}$$

Optimal Reduction from Noisy Leakage to Random Probing

Theorem (Optimal Reduction)

Any channel $X \to \boxed{P_{Y|X}} \to Y$ is a stochastically degraded erasure channel :

$$X \to \boxed{\mathrm{EC}_{\mathcal{E}}^{\perp}} \to X' \to \boxed{P_{Y|X'}} \to Y \tag{4}$$

with maximum erasure probability given by the Doeblin Coefficient

$$\mathcal{E}(X \to Y) = \sum\!\!\!\!\!\!\int_y \inf_{x \in \mathcal{X}} p_{Y|X}(y|x). \tag{5}$$

Proof : Achievability

1. Consider a channel $X \to \boxed{P_{Y|X}} \to Y$ with a given Doeblin coeffcient

$$\mathcal{E} = \sum\!\!\!\!\!\!\int_y \inf_{x \in \mathcal{X}} p_{Y|X}(y|x).$$

2.

$$\begin{cases} p_{Y|X'}(y|\perp) = \mathcal{E}^{-1} \inf\limits_{x \in \mathcal{X}} p_{Y|X}(y|x) \\ p_{Y|X'}(y|x) = \overline{\mathcal{E}}^{-1} \left(p_{Y|X}(y|x) - \inf\limits_{x \in \mathcal{X}} p_{Y|X}(y|x) \right) \end{cases}$$

is such that

$$\left(X \to \boxed{P_{Y|X}} \to Y \right) = \left(X \to \boxed{\mathrm{EC}_{\mathcal{E}}} \to X' \to \boxed{P_{Y|X'}} \to Y \right).$$

TELECOM Paris IP PARIS

Proof : Converse

1. Assume that there exists $\varepsilon \in [0,1]$ such that

$$\left(X \to \boxed{P_{Y|X}} \to Y\right) = \left(X \to \boxed{\mathrm{EC}_{\varepsilon}} \to X' \to \boxed{P_{Y|X'}} \to Y\right).$$

2. Then for any pair x, y :

$$p_{Y|X}(y|x) = \overline{\varepsilon} p_{Y|X'}(y|x) + \varepsilon p_{Y|X'}(y|\perp) \geqslant \varepsilon p_{Y|X'}(y|\perp).$$

3. Since it is true for all x :

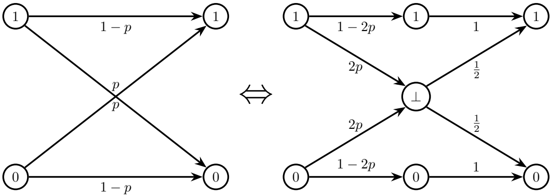
$$\inf_x p_{Y|X}(y|x) \geqslant \varepsilon P_{Y|X}(y|\perp).$$

4. Since $\sum\!\!\!\!\!\int_{y \in \mathcal{Y}} P_{Y|X}(y|\perp) = 1$:

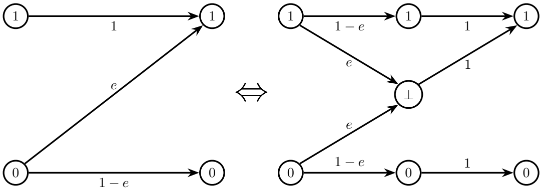
$$\sum\!\!\!\!\!\!\int_{y \in \mathcal{Y}} \inf_{x \in \mathcal{X}} p_{Y|X}(y|x) \geqslant \varepsilon.$$

.

Example with BSC and Z-channel



(a) BSC



(b) Z-Channel

Figure – Illustration of the Theorem

Many Good Properties !

1. **Strengthened-DPI** For any $X \to Y \to Z$, CDC satisfies the following strengthened-DPI
$$\overline{\mathcal{E}}(X \to Z) \leqslant \overline{\mathcal{E}}(X \to Y)\overline{\mathcal{E}}(Y \to Z) \tag{6}$$
2. **Adaptive Single Letterization**
$$\overline{\mathcal{E}}(K \to Y_1, \ldots, Y_q) \leqslant 1 - (1 - \overline{\mathcal{E}})^q \leqslant q\overline{\mathcal{E}} \tag{7}$$
3. **Fano's Inequality** The adversary's advantage is bounded as follows :

$$\begin{array}{ccccc|c}
0 & \leqslant & \mathbb{P}_{s,o}(K|Y) - \mathbb{P}_{s,o}(K) & \leqslant & \overline{\mathcal{E}}(K \to Y)\lambda_{SR_o} & \lambda_{SR_o} = (1 - \mathbb{P}_{s,o}(K)), \\
0 & \leqslant & G(K) - G(K|Y) & \leqslant & \overline{\mathcal{E}}(K \to Y)\lambda_{GE} & \lambda_{GE} = (G(K) - 1), \\
0 & \leqslant & \Delta(K;Y) & \leqslant & \overline{\mathcal{E}}(K \to Y)\lambda_{TVI} & \lambda_{TVI} = (1 - \exp(-H_2(K))),
\end{array}$$

Subsequence Decomposition

For typical block ciphers like the AES, featuring substitution boxes, Prouff and Rivain (EuroCrypt'13) decompose the computations in four different types of subsequences :

- **Type 1** $(z_i \leftarrow g(x_i))_i$ where g is a linear function (of the block cipher)
- **Type 2** $(x_i \leftarrow g(y_i))_i$ where g is an affine function (of Sbox evaluation)
- **Type 3** $(v_{i,j} \leftarrow a_i b_j)_{i,j}$ (First step of non-linear secure multiplication)
- **Type 4** $(t_{i,j} \leftarrow t_{i,j-1} + v_{i,j})_{i,j}$ (Last step of non-linear secure multiplication)

Explicit Algorithm in AES (from MS'24 article)

Algorithm 1 Linear gadget in Prouff & Rivain's proof.

Require: $\mathbf{A}$: $(d+1)$-sharing of A, C: elementary calculation linear with its input.
Ensure: $\mathbf{B}$: $(d+1)$-sharing of $\mathsf{C}(\mathrm{A})$.

for $i = 0, \ldots, d$ **do**
    $\mathrm{B}_i \leftarrow \mathsf{C}(\mathrm{A}_i)$ ▷ Type 1 or 2
end for
$\mathbf{B} \leftarrow \mathsf{Refresh}(\mathbf{B})$ ▷ Assumed to be leak-free
$\mathbf{A} \leftarrow \mathsf{Refresh}(\mathbf{A})$ ▷ Only if A used subsequently.

Algorithm 2 Multiplication gadget in Prouff & Rivain's proof.

Require: $\mathbf{A}, \mathbf{B}$: $(d+1)$-sharing of A, B.
Ensure: C : $(d+1)$-sharing of $\mathrm{A} \times \mathrm{B}$.

for $i = 0, \ldots, d$ **do**
    for $j = 0, \ldots, d$ **do**
        $\mathrm{V}_{i,j} \leftarrow \mathrm{A}_i \times \mathrm{B}_j$ ▷ Cross products (type 3)
    end for
end for
$\mathbf{V} \leftarrow \mathsf{Refresh}(\mathbf{V})$ ▷ Assumed to be leak-free
for $i = 0, \ldots, d$ **do**
    $\mathrm{C}_i = 0$
    for $j = 0, \ldots, d$ **do**
        $\mathrm{C}_i \leftarrow \mathrm{C}_i \oplus \mathrm{V}_{i,j}$ ▷ Compression (type 4)
    end for
end for
$\mathbf{C} \leftarrow \mathsf{Refresh}(\mathbf{C})$ ▷ Assumed to be leak-free
$\mathbf{A}, \mathbf{B} \leftarrow \mathsf{Refresh}(\mathbf{A}), \mathsf{Refresh}(\mathbf{B})$ ▷ Only if A, B used subsequently.

Mrs. Gerber's Lemma for CDC, Type 1 & 2 Subsequences

Let $\mathbf{G} = (G_i)_{i=0}^{d}$ be a d-th order encoding of $G = g(X)$ where g is a given function. Each share leaks independently through the side-channels $(G_i \to Y_i)_{i=0}^{d}$.

$$\overline{\mathcal{E}}(X \to \mathbf{Y}) \leqslant \prod_i \overline{\mathcal{E}}(G_i \to Y_i).$$

Intuition : A shared sensitive value is probed if and only all of its shares are probed.

Type 3 subsequences

Definition (Rook Domination Polynomial)

Let $(E_{i,j})_{0\leqslant i,j\leqslant d}$ be a collection of independent events with respective probabilities $((\overline{\mathcal{E}}_{i,j})_{0\leqslant i,j\leqslant d})$. Let

$$\Upsilon((\overline{\mathcal{E}}_{i,j})_{0\leqslant i,j\leqslant d}) \triangleq \mathbb{P}\left((\cap_{i=0}^{d}\cup_{j=0}^{d} E_{i,j}) \cup (\cap_{j=0}^{d}\cup_{i=0}^{d} E_{i,j})\right). \tag{9}$$

For short $\Upsilon_d(\overline{\mathcal{E}}) \triangleq \Upsilon((\overline{\mathcal{E}}_{i,j})_{0\leqslant i,j\leqslant d})$ when for all i,j we have $\overline{\mathcal{E}}_{i,j} = \overline{\mathcal{E}}$.

Lemma (Type 3 Subsequences)

Consider the channels $((G_i, H_j) \to Y_{i,j})_{0\leqslant i,j\leqslant d}$ *and let* $\mathbf{Y} \triangleq (Y_{i,j})_{0\leqslant i,j\leqslant d}$. *Then one has*

$$\overline{\mathcal{E}}(X \to \mathbf{Y}) \leqslant \Upsilon((\overline{\mathcal{E}}((G_i, H_j) \to Y_{i,j}))_{0\leqslant i,j\leqslant d}). \tag{10}$$

Type 4 subsequences

Let $(V_{i,j})$ be an encoding in $(d+1)^2$ shares of $f(X)$ where f is a given function. Let $\begin{cases} T_{i,0} = V_{i,0} \\ T_{i,j} = T_{i,j-1} \oplus V_{i,j}. \end{cases}$ In particular $(T_{i,d})_{i=0}^{d}$ is a d-th order encoding of $f(X)$.

Lemma (Type 4 Subsequences)

$(V_{i,0}, \ldots, V_{i,d})$ is a d-th order sharing of $T_{i,d}$. Consider $((T_{i,j-1}, V_{i,j}) \to Y_{i,j})_{0 \leqslant i,j \leqslant d}$ and let $\mathbf{Y} = (Y_{i,j})_{0 \leqslant i,j \leqslant d}$ then,

$$\overline{\mathcal{E}}(X \to \mathbf{Y}) \leqslant \prod_{i=0}^{d} \overline{\mathcal{E}}((T_{i,d-1}, V_{i,d}) \to Y_{i,d}). \tag{11}$$

Theorem : Direct Security Proof

Consider an implementation with n_i subsequences of type i and a $\overline{\mathcal{E}}$-noisy with respect to CDC adversary with q queries.

$$0 \leqslant \overline{\mathcal{E}}(K \to \mathbf{Y}) \leqslant 1 - \left(\left(1 - \overline{\mathcal{E}}^{d+1}\right)^{n_1+n_2+n_4} \left(1 - \Upsilon_d(\overline{\mathcal{E}})\right)^{n_3}\right)^q \leqslant 1. \tag{12}$$

(12) is asymptotically equivalent to

$$\overline{\mathcal{E}}(K \to \mathbf{Y}) \leqslant q\left(n_1 + n_2 + \left(2(d+1)^{d+1} - (d+1)!\right) n_3 + n_4\right) \overline{\mathcal{E}}^{d+1}. \tag{13}$$

(12) can be weakened to

$$\overline{\mathcal{E}}(K \to \mathbf{Y}) \leqslant q\left((n_1 + n_2 + n_4) + 2n_3(d+1)^{d+1}\right) \overline{\mathcal{E}}^{d+1}. \tag{14}$$

Theorem : Lower Bound on the Number of Queries

Let

$$\lambda(\overline{\mathcal{E}}, d) = \left(\ln\left(\left(1-\overline{\mathcal{E}}^{d+1}\right)^{n_1+n_2+n_4}\left(1-\Upsilon_d(\overline{\mathcal{E}})\right)^{n_3}\right)\right)^{-1} \tag{15}$$

$$= \left(\left(n_1+n_2+n_4\right)\log\left(1-\overline{\mathcal{E}}^{d+1}\right)+n_3\log\left(1-\Upsilon_d(\overline{\mathcal{E}})\right)\right)^{-1} \tag{16}$$

$$\approx \left(\left(n_1+n_2+n_4+n_3(2(d+1)^{d+1}-(d+1)!)\right)\overline{\mathcal{E}}^{d+1}\right)^{-1}. \tag{17}$$

Number of queries to achieve $\mathbb{P}_{s,o}(K|\mathbf{Y}) = \mathbb{P}_{s,o}$, $G(K|\mathbf{Y}) = G$ or $\Delta(K;Y) = \Delta$ is at least :

$$\begin{aligned} q_{\mathrm{sr}} &\geqslant \lambda(\overline{\mathcal{E}}, d)\ln\left((1-\mathbb{P}_{s,o})^{-1}\lambda_{SR_o}\right), \\ q_{\mathrm{ge}} &\geqslant \lambda(\overline{\mathcal{E}}, d)\ln\left((G-1)^{-1}\lambda_{GE}\right), \\ q_{\mathrm{tvi}} &\geqslant \lambda(\overline{\mathcal{E}}, d)\ln\left(\Delta^{-1}\lambda_{TVI}\right). \end{aligned} \tag{18}$$

TELECOM Paris IP PARIS

Theorem : Indirect Security Proof

Circuit Γ decomposed into $|\Gamma|$ regions with (l_i) wires. Any set of at most t (probed) wires in each region of the circuit is independent with the secret key. Let $\mathscr{A}$ be a $\overline{\mathcal{E}}$-noisy adversary with respect to CDC with q queries.

$$\overline{\mathcal{E}}(K \to \mathbf{Y}) \leqslant \mathrm{fail}(t,(l_i),\overline{\mathcal{E}},q) \triangleq 1 - \prod_{i=1}^{|\Gamma|}\Big(1 - Q_B(t,l_i,\overline{\mathcal{E}})\Big)^q \leqslant q\sum_{i=1}^{|\Gamma|} Q_B(t,l_i,\overline{\mathcal{E}}). \tag{19}$$

TELECOM Paris

IP PARIS

Thank you ! Questions ?

Optimal Side-channel Factorization from Noisy Leakage to Random Probing

Julien Béguinot[1], Wei Cheng[2,1], Sylvain Guilley[2,1], Olivier Rioul[1]

[1]***LTCI, Télécom Paris, Institut Polytechnique de Paris***, *Palaiseau, France*
[2]***Secure-IC S.A.S.***, *Paris, France & San Mateo, CA, USA*

CRYPTO 2024, Santa Barbara, CA, USA

Long version $\Longrightarrow$ ia.cr/2024/199

Optimal Masking Order ?

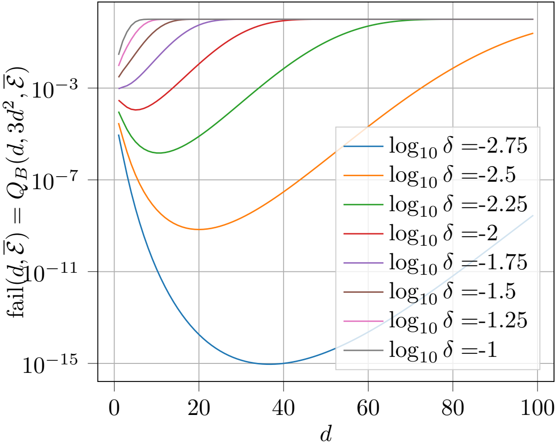


Figure – Bound for a Quadratic Gadget

Lemma : Practical Evaluation

$Y = f(X) + Z$ where Z is a radially symmetric decreasing with survival function S. Then

$$\mathcal{E}(X \to Y) = 2S\left(\frac{\sup_{x\in\mathcal{X}} f(x) - \inf_{x\in\mathcal{X}} f(x)}{2}\right). \tag{20}$$

If $f(X) = \sum_{i=1}^{n} a_i X_i$,

$$\mathcal{E}(X \to Y) = 2S\left(\frac{\|\mathbf{a}\|_1}{2}\right). \tag{21}$$

If $Z \sim \sigma\mathcal{N}(0,1)$,

$$\overline{\mathcal{E}}(X \to Y) = 1 - 2Q\left(\frac{\|\mathbf{a}\|_1}{2\sigma}\right) \overset{\sigma\to\infty}{=} \frac{\|\mathbf{a}\|_1}{\sqrt{2\pi}}\frac{1}{\sigma} + O\left(\sigma^{-3}\right). \tag{22}$$

Lemma : Comparison with Other Leakage Measures

$$\left.\begin{array}{r}\frac{I(X;Y)}{\log|\mathcal{X}|} \leqslant \frac{I(X;Y)}{H(X)} \\ \left.\begin{array}{r}\frac{ARE(X;Y)}{2\gamma_X\lambda_{TVI}} \\ \\ \frac{\beta(X;Y)}{2\lambda_{TVI}}\end{array}\right\} \leqslant \frac{\Delta(X;Y)}{\lambda_{TVI}} \\ \\ \frac{\exp(\mathcal{L}(X\to Y))-1}{|\mathcal{X}|-1}\end{array}\right\} \leqslant \overline{\mathcal{E}}(X\to Y) \leqslant \left\{\begin{array}{l} ARE(X;Y) \leqslant RE(X;Y) \\ \\ \gamma_X\beta(X;Y) \\ \gamma_X\Delta(X;Y) \leqslant \gamma_X\left(\frac{I(X;Y)}{2\log e}\right)^{\frac{1}{2}} \\ \\ (|\mathcal{X}|-1)(\exp\left(\mathcal{L}(X\to Y)\right)-1)\end{array}\right. \tag{23}$$

where H is Shannon entropy, H_2 is the collision entropy, $\lambda_{TVI} = 1 - \exp(-H_2(X))$ and $\gamma_X \triangleq \left(\inf_{x\in\mathcal{X}} p_X(x)\right)^{-1}$. If $X \sim \mathcal{U}(\mathcal{X})$ then $\gamma_X = |\mathcal{X}|$ and $\lambda_{TVI} = 1 - \frac{1}{|\mathcal{X}|}$.

Definition (Kullback-Leibler Divergence and Total Variation Distance)

Let P, Q be two probability distributions with respective pdf or pmf p, q defined over $\mathcal{X}$. The Kullback–Leibler (KL) divergence between P and Q is

$$D_{\mathrm{KL}}(P \| Q) \triangleq \sum\!\!\!\!\!\!\int_{\mathcal{X}} p \log \frac{p}{q} \tag{24}$$

and the total variation distance (TV) between P and Q is

$$D_{\mathrm{TV}}(P \| Q) = \frac{1}{2} \sum\!\!\!\!\!\!\int_{\mathcal{X}} |p - q| = \frac{1}{2} \|p - q\|_1 . \tag{25}$$

TELECOM Paris
IP PARIS

Proof I

Let

$$X \to \boxed{f} \to G \to \boxed{\mathrm{Mask}_d} \to \mathbf{G} \to \boxed{\prod_{i=0}^{d} p_{Y_i|G_i}} \to \mathbf{Y}. \tag{26}$$

By optimal reduction theorem,

$$\left(G_i \to \boxed{P_{Y_i|G_i}} \to Y_i\right) = \left(G_i \to \boxed{\mathrm{EC}^{\perp_i}_{\mathcal{E}_i}} \to G_i' \to \boxed{P_{Y_i|G_i'}} \to Y_i\right) \quad \text{where} \quad \mathcal{E}_i = \mathcal{E}(G_i \to Y_i). \tag{27}$$

$$G \to \boxed{\mathrm{Mask}_d} \to \boxed{\prod_{i=0}^{d} \mathrm{EC}^{\perp_i}_{\mathcal{E}_i}} \to \mathbf{Y}' \to \boxed{\prod_{i=0}^{d} p_{Y_i|G_i}} \to \mathbf{Y}. \tag{28}$$

By DPI,

$$\overline{\mathcal{E}}(X \to \mathbf{Y}) \leqslant \overline{\mathcal{E}}(G \to \mathbf{Y}) \leqslant \overline{\mathcal{E}}(G \to \mathbf{Y}').$$

Proof II

By definition,

$$\overline{\mathcal{E}}(G \to \mathbf{Y}') = \mathbb{E}_{Y'_0,\ldots,Y'_d}\left[\sup_{g\in f(\mathcal{X})}\left(1 - \frac{p(g|Y'_0,\ldots,Y'_d)}{p(g)}\right)\right]. \tag{30}$$

If $\exists i$ s.t. $y'_i = \perp_i$ then $p(g|y'_0,\ldots,y'_d) = p(g)$,

$$\sup_{g\in f(\mathcal{X})}\left(1 - \frac{p(g|y'_0,\ldots,y'_d)}{p(g)}\right) = 0. \tag{31}$$

Otherwise,

$$\begin{cases} p(g|y'_0,\ldots,y'_d) = 1 & \text{if } g = y'_0 + \ldots + y'_d \\ p(g|y'_0,\ldots,y'_d) = 0 & \text{if } g \neq y'_0 + \ldots + y'_d \end{cases} \tag{32}$$

Proof III

So that,

$$\sup_{g\in f(\mathcal{X})}\left(1-\frac{p(g|y'_0,\ldots,y'_d)}{p(g)}\right)=\sup\left(1,1-\frac{1}{p(y'_0+\ldots+y'_d)}\right)=1. \tag{33}$$

As a consequence,

$$\overline{\mathcal{E}}(G\to\mathbf{Y}')=\mathbb{E}_{Y'_0,\ldots,Y'_d}\left[\mathbb{1}_{Y'_0\neq\perp_0,\ldots,Y'_d\neq\perp_d}\right]=\mathbb{P}\left(Y'_0\neq\perp_0,\ldots,Y'_d\neq\perp_d\right)=\prod_{i=0}^{d}\overline{\mathcal{E}}_i. \tag{34}$$

Comparison Leakage Metrics

	$I(X;Y)$	$\Delta(X;Y)$	$\mathcal{L}(X \to Y)$	$\beta(X;Y)$	$RE(X;Y)$	$ARE(X;Y)$	$\overline{\mathcal{E}}(X \to Y)$
T	$\frac{\lvert\mathcal{X}\rvert \log \lvert\mathcal{X}\rvert}{\sqrt{2 \log e I(X;Y)}}$	$\lvert\mathcal{X}\rvert - 1$	$(\lvert\mathcal{X}\rvert - 1)^2$	$2(\lvert\mathcal{X}\rvert - 1)$	$+\infty$	$2(\lvert\mathcal{X}\rvert - 1)$	1
M	$\log \lvert\mathcal{X}\rvert$	$1 - \frac{1}{\lvert\mathcal{X}\rvert}$	$\log \lvert\mathcal{X}\rvert$	$\sqrt{1 - \frac{1}{\lvert\mathcal{X}\rvert}}$	$\lvert\mathcal{X}\rvert - 1$	$\lvert\mathcal{X}\rvert - 1$	1
H	$\frac{n \log e}{8} \frac{1}{\sigma^2}$	$\frac{\sqrt{n}}{2\pi\sigma}$	$\frac{n \log e}{\sqrt{2\pi\sigma}}$	$\sqrt{\frac{n}{2\pi 2^n}} \frac{1}{\sigma}$	$2^n - 1$	$\frac{n}{\sqrt{2\pi\sigma}}$	$\frac{n}{\sqrt{2\pi\sigma}}$