Efficient Stochastic Methods: Profiled Attacks Beyond 8 Bits

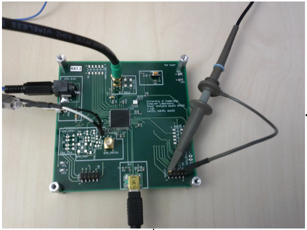
CARDIS 2014

Omar Choudary Markus G. Kuhn

UNIVERSITY OF CAMBRIDGE

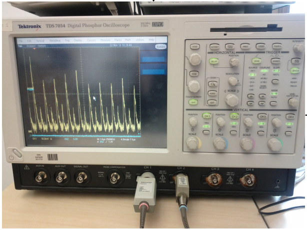
Paris, 6 November 2014

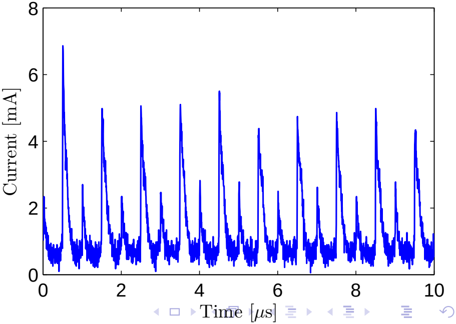
Framework for SCA – 8-bit target



Executed Code:

```
movw r30, r24
ld r8, 0
ld r9, k
ld r10, 0
ld r11, 0
```





Introduction

- Template Attacks (TA) [Chari et al., '02] very powerful
- Stochastic Model (SM) [Schindler et al., '05] very efficient
  $\Rightarrow$ i.e. much fewer traces required than for TA during profiling
- PCA and LDA [Archambeau et al., '06, '08]
  great compression methods for TA
- There were no efficient (supervised) implementations of PCA or LDA for SM (until now...)

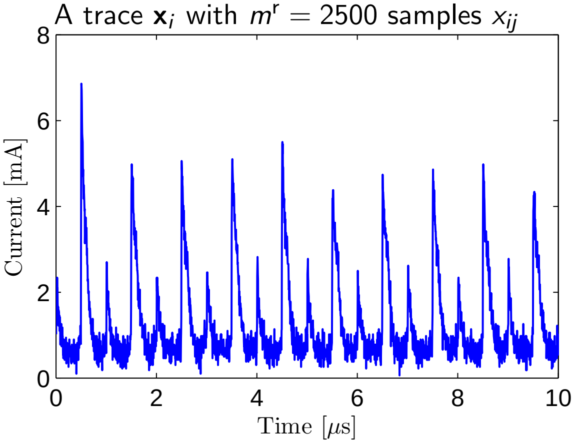
Introduction

- Contributions:
  - Efficient methods for implementing PCA and LDA with SM
  - Evaluation on 8-bit
    - comparing several compressions with SM/TA, including PCA/LDA
  - Evaluation on 16-bit target
    - Show that SM are feasible on 16-bit and possibly larger targets (at least computationally)
    - Comparing 16-bit attack with two 8-bit attacks
    - Evaluation of extended 16-bit model
- Overall, we provide the most efficient kind of profiled attack

Profiled attacks

1. Select/Detect the target data (e.g. a key byte, S-box output)
2. Profile training device
   - Collect traces (and most likely compress them)
   - Build a model of the leakage for each target value
3. Attack target device (same type as training device)
   - Compare leakage with model
   - Decide that target data is the one with best match

Template attacks – acquisition



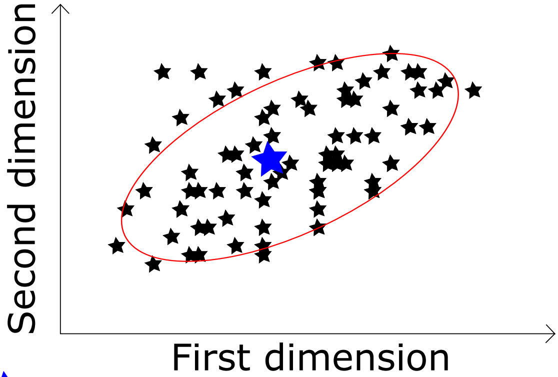
For each k obtain n_{p} such traces

Template attacks – compression

1. Goal is to reduce size from $m^{\mathrm{r}} = 2500$ to $m \ll m^{\mathrm{r}}$
   $\Rightarrow$ E.g. $m = 4$ (for PCA)
2. Common approaches
   1. sample selection
   2. PCA
   3. LDA

Template attacks – model

Data space for a single k, 2 variables (leakage samples)

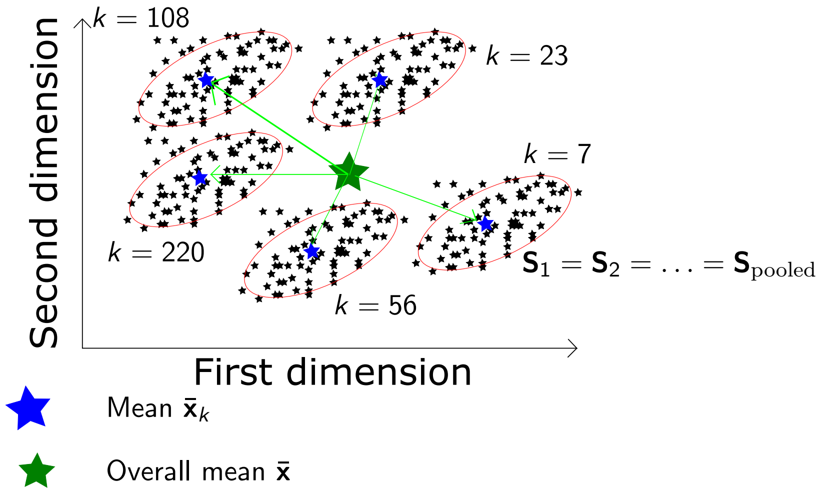


Mean $\bar{\mathbf{x}}_k$

Ellipse from eigenvectors of covariance matrix $\mathbf{S}_k$

Template attacks – model

Data space for several k, 2 variables (leakage samples)



Template attacks – attack

For each k compute linear discriminant score:

$$\mathrm{d}_{\mathrm{LINEAR}}^{\mathrm{joint}}(k \mid \mathbf{X}_{k\star}) = \bar{\mathbf{x}}_k' \mathbf{S}_{\mathrm{pooled}}^{-1} \left(\sum_{\mathbf{x}_i \in \mathbf{X}_{k\star}} \mathbf{x}_i \right) - \frac{n_{\mathrm{a}}}{2} \bar{\mathbf{x}}_k' \mathbf{S}_{\mathrm{pooled}}^{-1} \bar{\mathbf{x}}_k$$

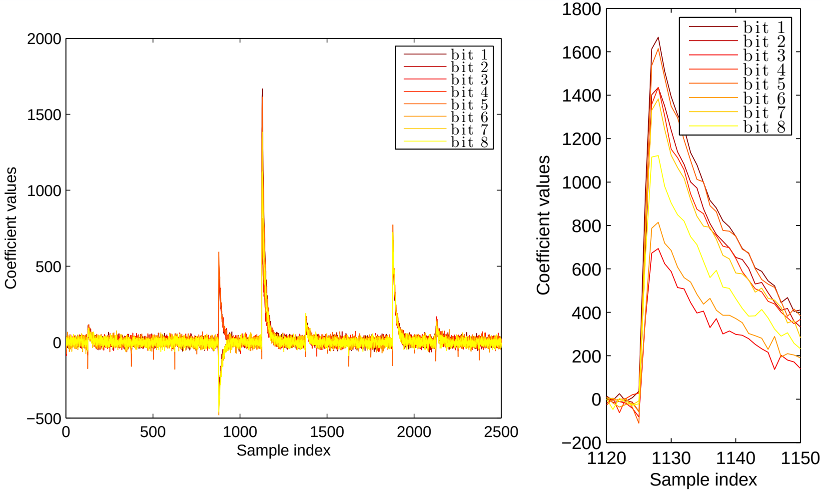
$\mathbf{X}_{k\star}$ contains n_{a} leakage traces for attack

$$k\star = \arg\max_k \mathrm{d}_{\mathrm{LINEAR}}^{\mathrm{joint}}(k \mid \mathbf{X}_{k\star})$$

Stochastic method – model

- Model each leakage sample as $x_j = \delta_j(k) + \rho_j$
- $\delta_j(k) = \sum_{b=0}^{u-1} \beta_{jb} \cdot g_{jb}(k)$
  - g_{jb} provides the model (usually bit selection)
  - Coefficients β_{jb} obtained from least-squares approximation i.e. minimize $(x_{ij} - \delta_j(k^i))^2$ over all traces $\mathbf{x}_i$
- $\hat{\mathbf{x}}'_k = [\delta_1(k), \ldots, \delta_m(k)]$
  - $\hat{\mathbf{x}}_k$ replaces $\bar{\mathbf{x}}_k$ (from TA)

Stochastic method – model

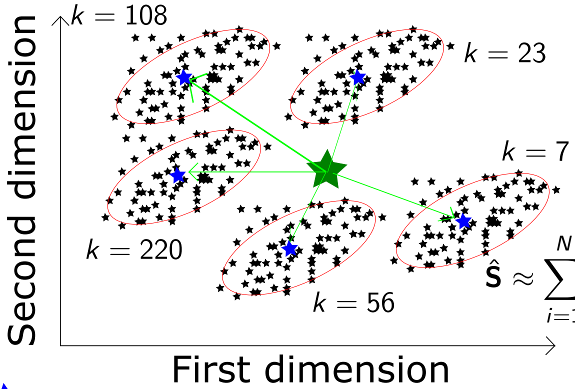


Only $u = 9$ parameters to approximate $(\beta_{j0}, \ldots, \beta_{j9})$

Fewer traces to match TA results (when model fits hardware well)

Stochastic method – model

Data space for several k, 2 variables (leakage samples)



$$\hat{\mathbf{S}} \approx \sum_{i=1}^{N} (\mathbf{x}_i - \hat{\mathbf{x}}_k)(\mathbf{x}_i - \hat{\mathbf{x}}_k)'$$

Stochastic 'mean' $\hat{\mathbf{x}}_k$

Ellipse from eigenvectors of covariance matrix $\hat{\mathbf{S}}$

Stochastic method – attack

For each k compute linear discriminant score:

$$\mathrm{d}_{\mathrm{LINEAR}}^{\mathrm{joint}}(k \mid \mathbf{X}_{k\star}) = \hat{\mathbf{x}}_k' \hat{\mathbf{S}}^{-1} \left(\sum_{\mathbf{x}_i \in \mathbf{X}_{k\star}} \mathbf{x}_i \right) - \frac{n_{\mathrm{a}}}{2} \hat{\mathbf{x}}_k' \hat{\mathbf{S}}^{-1} \hat{\mathbf{x}}_k$$

$\mathbf{X}_{k\star}$ contains n_{a} leakage traces for attack

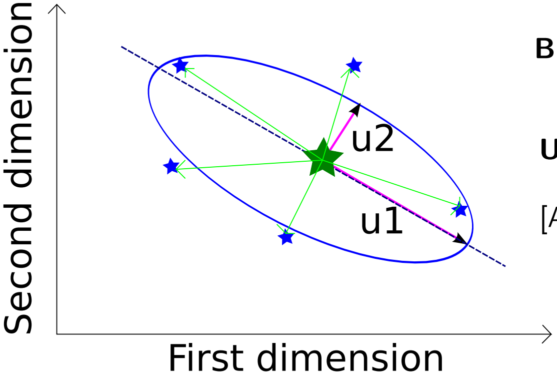
$$k\star = \arg\max_k \mathrm{d}_{\mathrm{LINEAR}}^{\mathrm{joint}}(k \mid \mathbf{X}_{k\star})$$

Stochastic method – compression

1. So far the usual method was sample selection
2. A single PCA proposal, but unsupervised (sub-optimal)
3. Our contribution: PCA and LDA for SM in supervised (efficient) manner
    - Goal is to maintain profiling efficiency of SM

Principal Component Analysis (PCA) – TA

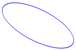
Data space for several k, 2 variables (leakage samples)



$$\mathbf{B} = \sum_{k \in \mathcal{S}} (\bar{\mathbf{x}}_k^{\mathrm{r}} - \bar{\mathbf{x}}^{\mathrm{r}})(\bar{\mathbf{x}}_k^{\mathrm{r}} - \bar{\mathbf{x}}^{\mathrm{r}})'$$

$$\mathbf{U} = [\mathbf{u}_1, \mathbf{u}_2] = \mathrm{SVD}(\mathbf{B})$$

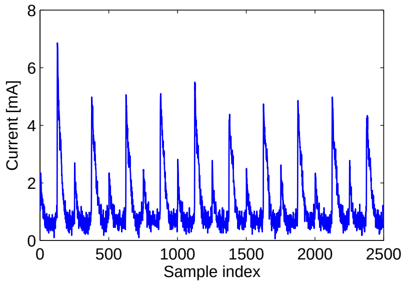
[Archambeau et al. '06]

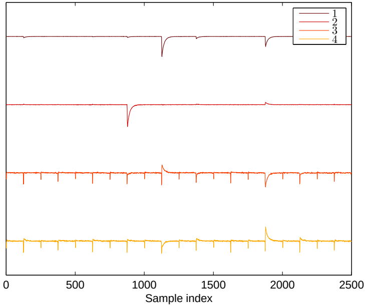
 Ellipse from *treatment* matrix **B** (covariance of means)

Principal Component Analysis (PCA) – TA

$$\mathbf{x}^{\mathrm{r}}_{ki} \in \mathbb{R}^{m^{\mathrm{r}}}$$

$$\mathbf{U}^m = [\mathbf{u}_1, \ldots, \mathbf{u}_m]$$

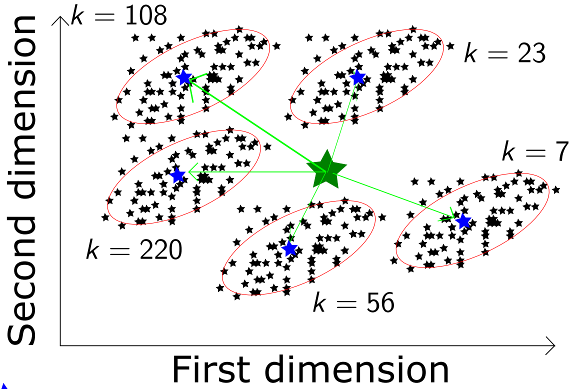




$$\mathbf{x}_{ki} = \mathbf{U}^{m\prime}\mathbf{x}^{\mathrm{r}}_{ki} \in \mathbb{R}^m, m \ll m^{\mathrm{r}} \text{ (e.g. } m^{\mathrm{r}} = 2500, m = 4)$$

SM PCA – unsupervised approach [Heuser et al. '12]

Data space for several k, 2 variables (leakage samples)

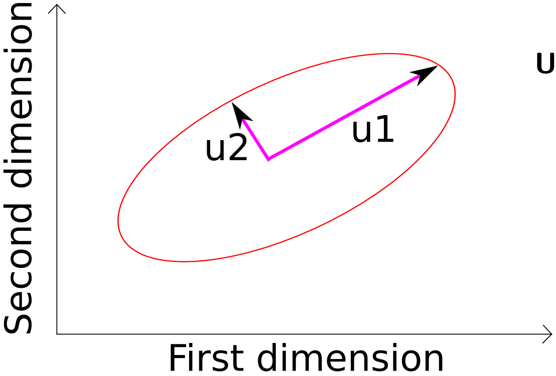


 Stochastic 'mean' $\hat{\mathbf{x}}_k$

 Ellipse from eigenvectors of covariance matrix $\hat{\mathbf{S}}$

SM PCA – unsupervised approach [Heuser et al. '12]

Data space for several k, 2 variables (leakage samples)



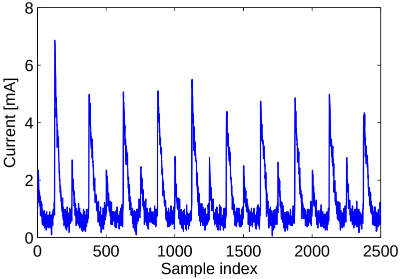
$$\mathbf{U} = [\mathbf{u}_1, \mathbf{u}_2] = \mathrm{SVD}(\hat{\mathbf{S}})$$

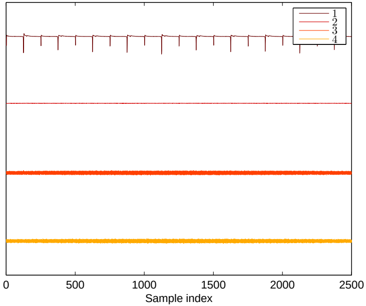
Ellipse from eigenvectors of covariance matrix $\hat{\mathbf{S}}$

SM PCA – unsupervised approach [Heuser et al. '12]

$\mathbf{x}_i^{\mathrm{r}} \in \mathbb{R}^{m^{\mathrm{r}}}$

$\mathbf{U}^m = [\mathbf{u}_1, \dots, \mathbf{u}_m]$





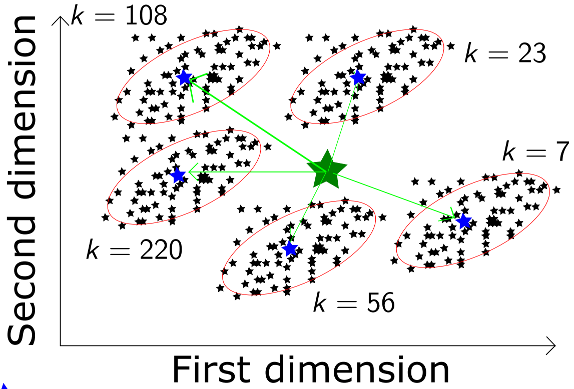
$\mathbf{x}_i = \mathbf{U}^{m\prime} \mathbf{x}_i^{\mathrm{r}} \in \mathbb{R}^m, m \ll m^{\mathrm{r}}$

$x_j = \delta_j(k) + \rho_j, \ldots \Rightarrow \hat{\mathbf{x}}_k, \hat{\mathbf{S}}$

Doesn't identify leakage, only removes correlation

SM PCA – supervised (our approach)

Data space for several k, 2 variables (leakage samples)

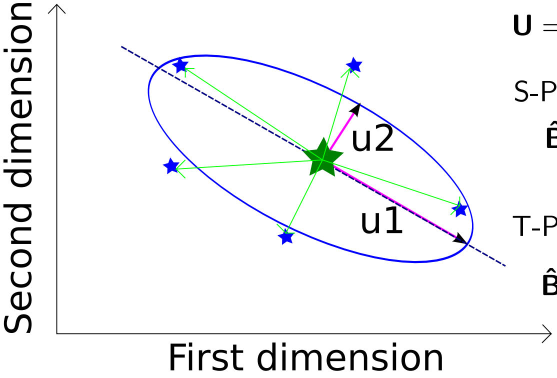


Stochastic 'mean' $\hat{\mathbf{x}}_k$

Ellipse from eigenvectors of covariance matrix $\hat{\mathbf{S}}$

SM PCA – supervised (our approach)

Data space for several k, 2 variables (leakage samples)



$$\mathbf{U} = [\mathbf{u}_1, \mathbf{u}_2] = \mathrm{SVD}(\hat{\mathbf{B}})$$

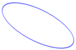
S-PCA:

$$\hat{\mathbf{B}} = \sum_{k \in \mathcal{S}} (\hat{\mathbf{x}}_k^{\mathrm{r}} - \hat{\mathbf{x}}^{\mathrm{r}})(\hat{\mathbf{x}}_k^{\mathrm{r}} - \hat{\mathbf{x}}^{\mathrm{r}})'$$

T-PCA:

$$\hat{\mathbf{B}} = \sum_{k \in \mathcal{S}_s} (\bar{\mathbf{x}}_k^{\mathrm{r}} - \bar{\mathbf{x}}^{\mathrm{r}})(\bar{\mathbf{x}}_k^{\mathrm{r}} - \bar{\mathbf{x}}^{\mathrm{r}})'$$

$$(\mathcal{S}_s \subset \mathcal{S})$$

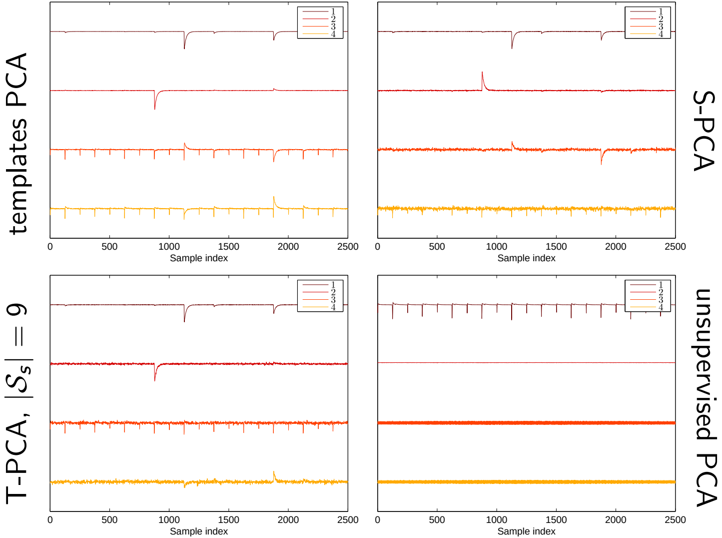

Ellipse from covariance matrix $\hat{\mathbf{B}}$

SM PCA – supervised (our approach)

3 main steps for SM PCA (supervised approach):

1. Compute $\hat{\mathbf{B}}$ as an approximation of $\mathbf{B}$ (from TA) – efficiently!
2. Compress traces
   - $\mathbf{U}^m = [\mathbf{u}_1, \ldots, \mathbf{u}_m] = \mathrm{SVD}(\hat{\mathbf{B}})$
   - $\mathbf{x}_i = \mathbf{U}^{m\prime}\mathbf{x}_i^{\mathrm{r}} \in \mathbb{R}^m, m \ll m^{\mathrm{r}}$
3. Use stochastic model on compressed traces
   - $x_j = \delta_j(k) + \rho_j$
   - $\Rightarrow \hat{\mathbf{x}}_k, \hat{\mathbf{S}}$

SM PCA – supervised (our approach)



Fisher's Linear Discriminant Analysis (LDA) – SM

3 main steps for SM LDA (supervised approach):

1. Compute $\hat{\mathbf{B}}$ (as for PCA) and $\hat{\mathbf{S}}^{\mathrm{r}}$
2. Compress traces
   - $\mathbf{U}^m = [\mathbf{u}_1, \ldots, \mathbf{u}_m] = \mathrm{SVD}({\hat{\mathbf{S}}^{\mathrm{r}}}^{-1}\hat{\mathbf{B}})$
   - $\mathbf{x}_i = \mathbf{U}^{m\prime}\mathbf{x}_i^{\mathrm{r}} \in \mathbb{R}^m, m \ll m^{\mathrm{r}}$
3. Use stochastic model on compressed traces
   - $x_j = \delta_j(k) + \rho_j$
   - $\Rightarrow \hat{\mathbf{x}}_k, \hat{\mathbf{S}}$

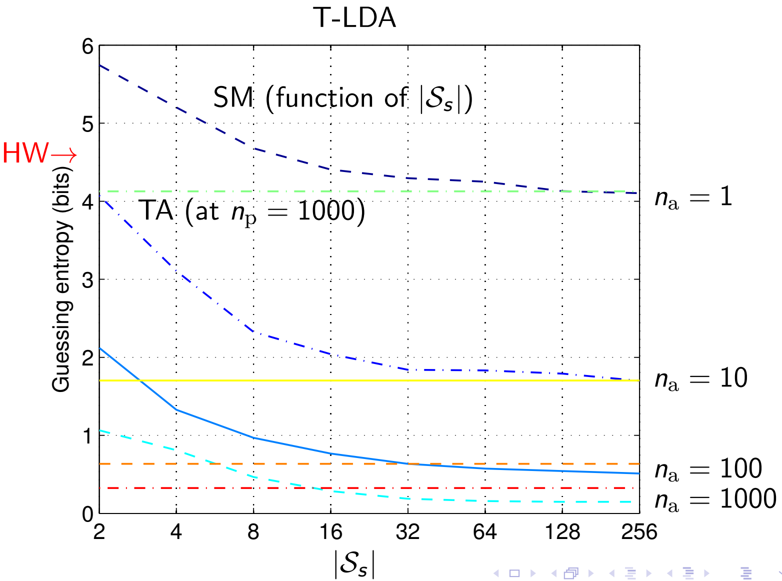
Depending on estimation of $\hat{\mathbf{B}}, \hat{\mathbf{S}}$ we have S-LDA or T-LDA.

SM PCA and LDA – supervised (our approach)

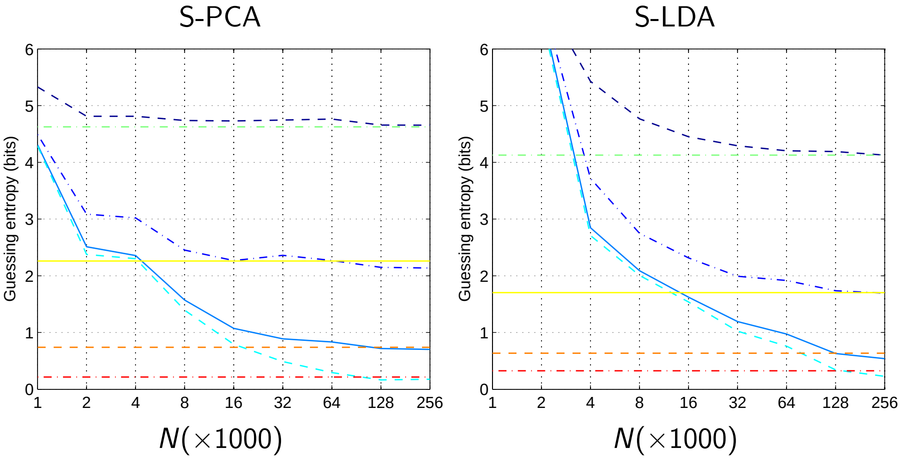
Method	Step 1	Step 2	Step 3
S-PCA	Estimate $\hat{\mathbf{B}}$ (SM)	$\mathbf{U} = \mathrm{SVD}(\hat{\mathbf{B}})$	Compute $\hat{\mathbf{x}}_k, \hat{\mathbf{S}}$
T-PCA	Estimate $\hat{\mathbf{B}}$ (TA)		
S-LDA	Estimate $\hat{\mathbf{B}}, \hat{\mathbf{S}}^{\mathrm{r}}$ (SM)	$\mathbf{U} = \mathrm{SVD}({\hat{\mathbf{S}}^{\mathrm{r}}}^{-1}\hat{\mathbf{B}})$	(SM)
T-LDA	Estimate $\hat{\mathbf{B}}, \hat{\mathbf{S}}^{\mathrm{r}}$ (TA)		

Note: stochastic model ‘sandwich’ for S-PCA and S-LDA

Results – 8-bit target

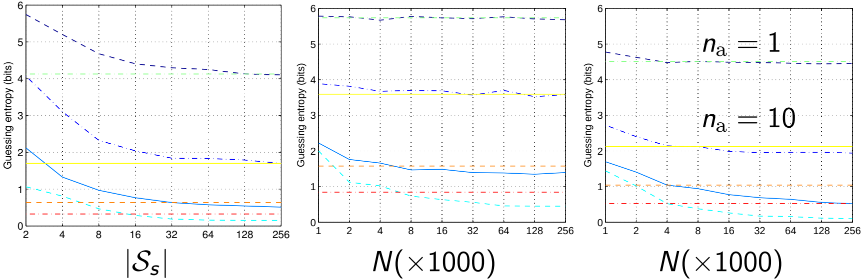


Results – 8-bit target



Results – 8-bit target

T-LDA ($N = 16000$) 1ppc 20ppc



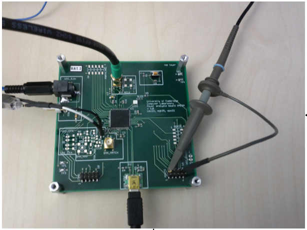
Overall, SM reaches TA boundary with considerably fewer traces

SM LDA is best method at low n_{a}

Attacks on 16-bit target

- TA are not feasible on much more than 8-bit
  $\Rightarrow$ Need to acquire n_p traces for each possible value k
  $\Rightarrow$ E.g. for 16-bit, to compute $\bar{\mathbf{x}}_0, \bar{\mathbf{x}}_1, \ldots, \bar{\mathbf{x}}_{65535}$
- SM may allow profiling with a relatively small number N of traces
  $\Rightarrow$ Even for 16-bit (or larger) targets
  $\Rightarrow$ In such cases, SM may be the only possible profiled attack

Attacks on 16-bit target



Executed Code:

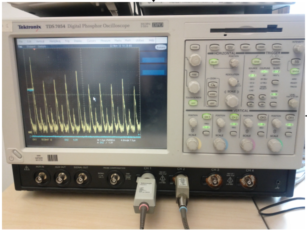
movw r30, r24

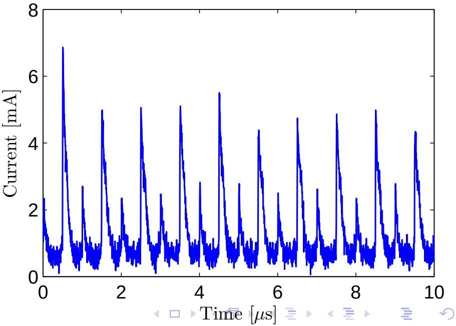
ld r8, 0

ld r9, k_1

ld r10, k_2

ld r11, 0

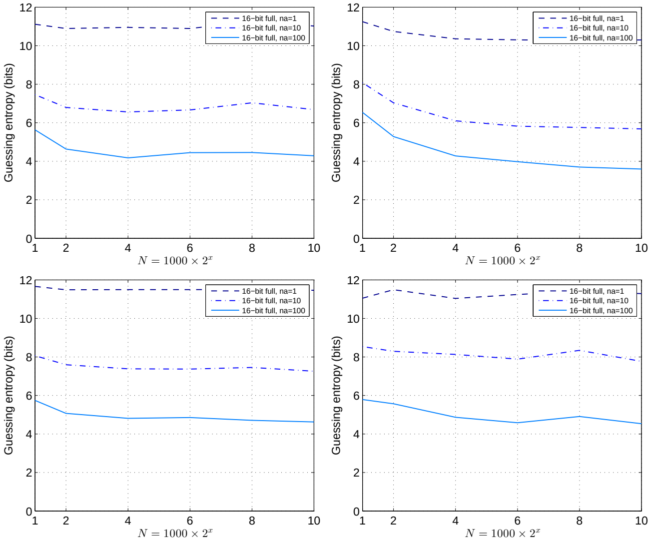




Results – 16-bit target

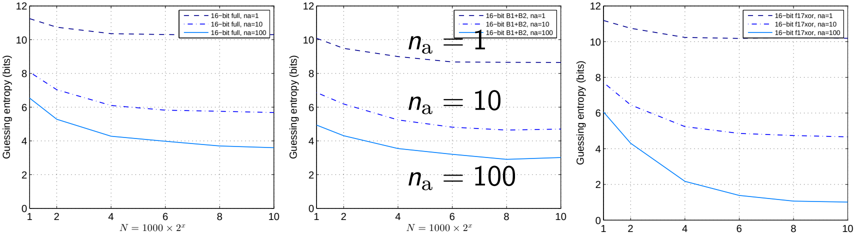
S-PCA | S-LDA

20ppc | T-LDA



Results – 16-bit target

S-LDA $\mathcal{F}_{17}$ S-LDA 8+8 S-LDA $\mathcal{F}_{17x}$

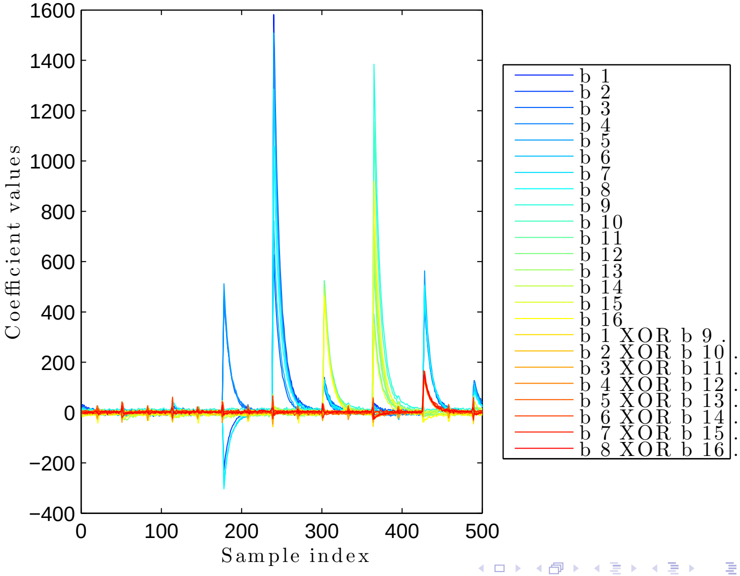


Note: attack on 2 consecutive bytes, not a 16-bit bus

Naively running a 16-bit attack in this case is not the best (large number of parameters)

But adding the XOR between bytes to the model works best ($\mathcal{F}_{17x}$)

Results – 16-bit target



Conclusions

- We have shown how to obtain very efficient profiled attacks
  $\Rightarrow$ combining PCA and LDA with stochastic models
  $\Rightarrow$ Main steps of S-PCA computation (including guessing entropy) for 16-bit target take less than 7 minutes
- Algorithm choice:
  - The stochastic model 'sandwich' S-LDA seems generally efficient (8 and 16-bit)
  - For low number of bits (e.g. 8-bit) T-LDA seems best
- For attacks on more than one byte we should enhance the model (e.g. include XOR)
- TODO: try on 16-bit bus

Questions?

Omar Choudary: omar.choudary@cl.cam.ac.uk

Markus G. Kuhn: markus.kuhn@cl.cam.ac.uk

`http://www.cl.cam.ac.uk/research/security/`