Template Attacks using Classification Algorithms

Elif Özgen, Louiza Papachristodoulou, Lejla Batina

Digital Security – Radboud University Nijmegen
Technical University Eindhoven
louizap@cs.ru.nl

5 May 2016

Outline

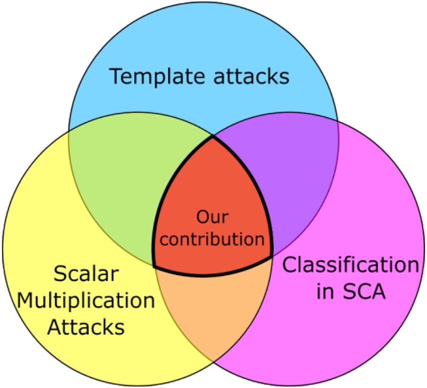
Introduction

Previous Work: OTA with Pearson correlation

Our contribution: OTA with Classification Algorithms

Conclusions - Future Research

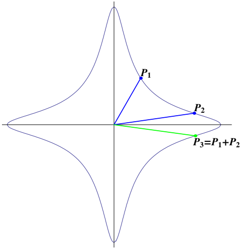
Our Contribution



ECDLP and scalar multiplication

- Let E be an EC over a finite field $\mathbb{F}_q$, $G =< P >$ a cyclic subgroup of $E(\mathbb{F}_q)$ and $Q \in G$.
- Scalar multiplication $kP = \underbrace{P + P + ... + P}_{k\text{-times}}$
- **ECDLP:** Given P, Q on an EC, find $k \in \mathbb{Z}$ such that $Q = kP$.
- Typical EC cryptosystem

P : fixed system parameter
Q : public key
k : secret key



Template Attacks

Chari, Rao, Rohatgi, “Template Attacks” [2002]

- Combination of statistical modelling and power-analysis attack techniques
- Models of signal and noise
- Use experimental device identical to the DUT
- Template-Building Phase
  Templates correspond to each possible value of unknown key
- Template-Matching Phase
  Use iterative classification

Common classifiers

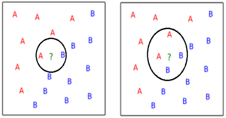
- Euclidean Distance
  $d(\mathbf{p}, \mathbf{q}) = \sqrt{\sum_{i=1}^{n} (q_i - p_i)^2})$
- Pearson correlation
  $\rho_{(X,Y)} = \dfrac{cov(X, Y)}{\sigma_X \sigma_Y}$
- Machine Learning techniques
  1. Classification Algorithms (e.g. Naïve Bayes, kNN, SVM)
  2. Clustering Algorithms (e.g. Centroid-, Distibution-based)

Classification Algorithms

1. Naïve Bayes Classifier: function that combines the naive Bayes probability model with a decision rule. Common rule: pick the hypothesis that is most probable; the maximum value of the a posteriori probability

$$p(c_k|\mathbf{x}) = \frac{p(c_k)\ p(\mathbf{x}|c_k)}{p(\mathbf{x})}$$

2. *k*-Nearest Neighbour



3. SVM outputs an optimal hyperplane which categorizes new examples, i.e. one that gives the largest minimum distance to the training points

Acquisition Setup

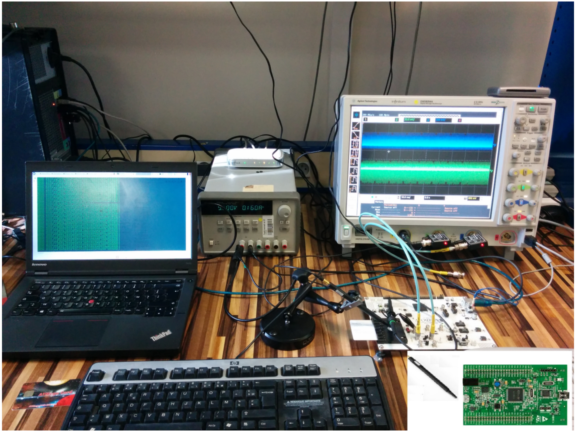


Figure: Acquisition with STM32F4

OTA on double-and-add-always

Optimized double-add-always on twisted Edwards curve

```
Input: $P$,
    $k = (k_{x-1}, k_{x-2}, ..., k_0)_2$
Output: $Q = kP$
$R_0 \leftarrow P$
for $i = x - 2$ downto 0 do
    $R_0 \leftarrow 2R_0$
    $R_1 \leftarrow R_0 + P$
    $R_0 \leftarrow R_{k_i}$
end for
return $R_0$
```

$k = 100$

$R_0 = P$

$R_0 = 2P, R_1 = 3P,$ return $2P$

$R_0 = 4P, R_1 = 5P,$ return $4P$

$k = 110$

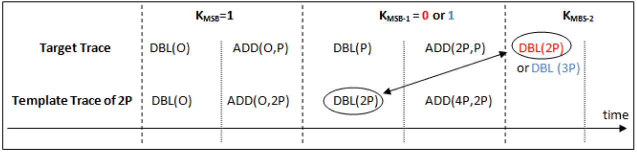
$R_0 = P$

$R_0 = 2P, R_1 = 3P,$ return $3P$

$R_0 = 6P, R_1 = 7P,$ return $6P$

Attack methodology

1. Profiling of the device.
2. Acquire target and template traces.
3. Template Matching of template traces with the corresponding part of the target trace.



K_{MSB}=1

K_{MSB-1} = 0 or 1

K_{MBS-2}

Target Trace: DBL(O) | ADD(O,P) | DBL(P) | ADD(2P,P) | DBL(2P) or DBL (3P)

Template Trace of 2P: DBL(O) | ADD(O,2P) | DBL(2P) | ADD(4P,2P)

Figure: Correlation of $(i+1)$-iteration of target with 1^{st} or 2^{nd}-iteration of template

Template for multiplication operation

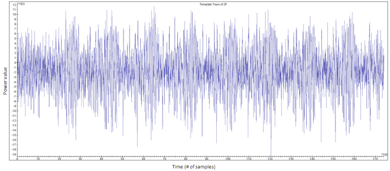


Figure: Multiplication pattern for $k = 0$

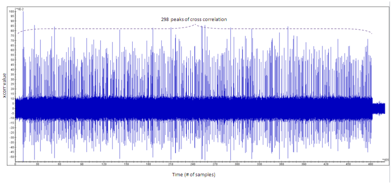


Figure: Cross correlation of multiplication with target trace

OTA on Ed25519 curve with Power Analysis

- ATMega163 with NaCl implementation of twisted Edwards curve with unified formulas.
- Correct bit assumptions: $84 - 88\%$, wrong: $50 - 72\%$
- Pattern matching threshold: 80%

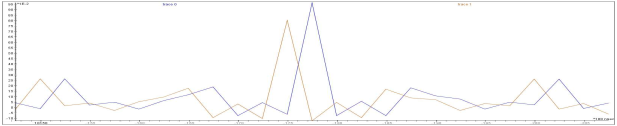


Figure: Pattern match of P to $2P$ (blue) and to $3P$ (brown) for MSB 1000

[L. Batina, L. Chmielewski, L. Papachristodoulou, P. Schwabe and M. Tunstall. Online Template Attacks. In INDOCRYPT 2014 - 15th International Conference on Cryptology in India, pages 21-36, 2014.]

Practical OTA on BP256r1 of mbedTLS with EM Analysis

- Horizontal: 100% success rate with one template trace per bit
- Vertical: Average template traces
- Use 2 averaged templates per key-bit
- Error detection and correction

Number of average traces	1	10	50	100
Success Rate	69%	80,70%	91,60%	99,80%

Table: Different success rates according to the number of average template traces on BP curve.

[M. Dugardin, L. Papachristodoulou, Z. Najm, L. Batina, J.L. Danger, S. Guilley. Dismantling real-world ECC with Horizontal and Vertical Template Attacks. COSADE 2016]

Cross-Correlation

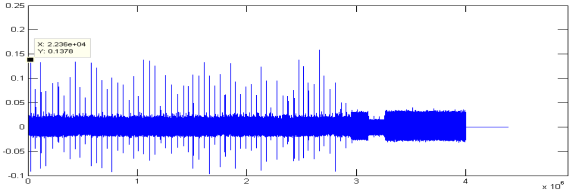


Figure: Cross-correlation of multiplication pattern with the template trace 2***P***

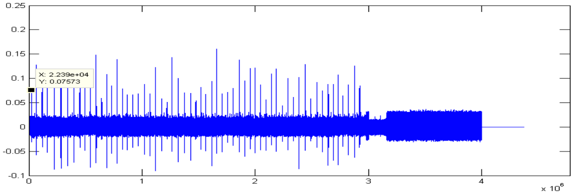


Figure: Cross-correlation of multiplication pattern with the template trace 3***P***

Experimental Results

♯Templates	Naïve Bayes	kNN ($k = 4$)	SVM
160	2[1,0]	2[1,0]	2[1.084593, -1.084593]
80	2[1,0]	2[1,0]	2[1.040720, -1.040720]
40	2[1,0]	2[1,0]	2[0.675875, -0.675875]
20	2[1,0]	2[1,0]	2[0.554645, -0.554645]

Table: Different success rates according to the number of average template traces on BP curve.

Conclusions - Future research

- Classification algorithms and ML techniques in general are very promising for SCA. In our experiments, 100% success rate with average of 20 template traces.
- Work with different distinguishers for HW implementations and automate the technique.
- Implement countermeasures (randomization of scalar, randomization of input point, use isomorphic curves) and evaluate their practical resistance.

Thank You!