DPA Contest 2008 – 2009
Less than 50 traces allow to recover the key

Christophe Clavier [1] [2]

[1] Institut d'Ingénierie Informatique de Limoges (3iL)

[2] Université de Limoges – XLIM

Lausanne – September 7, 2009

Description of the method

The proposed solution uses a maximum likelihood criterion

Description of the method

The proposed solution uses a maximum likelihood criterion

Given a consumption model (Hamming distance between L_i and R_i), we compute for each key guess k its *a posteriori* probability $Pr(k|traces)$

- Predicted value assuming k is evaluated for each trace
- Sum of squared differences between predictions and observations:
  - → a posteriori probability of the traces given the key
  - → a posteriori probability of the key given the traces (Bayes)

Description of the method

The proposed solution uses a maximum likelihood criterion

Given a consumption model (Hamming distance between L_i and R_i), we compute for each key guess k its *a posteriori* probability $Pr(k|traces)$

- Predicted value assuming k is evaluated for each trace
- Sum of squared differences between predictions and observations:
  - → a posteriori probability of the traces given the key
  - → a posteriori probability of the key given the traces (Bayes)

We select the key achieving highest probability (Least Square Method)

Description of the method

The proposed solution uses a maximum likelihood criterion

Given a consumption model (Hamming distance between L_i and R_i), we compute for each key guess k its *a posteriori* probability $Pr(k|traces)$

- Predicted value assuming k is evaluated for each trace
- Sum of squared differences between predictions and observations:
    - → a posteriori probability of the traces given the key
    - → a posteriori probability of the key given the traces (Bayes)

We select the key achieving highest probability (Least Square Method)

Is this method new?

Description of the method

The proposed solution uses a maximum likelihood criterion

Given a consumption model (Hamming distance between L_i and R_i), we compute for each key guess k its *a posteriori* probability $Pr(k|traces)$

- Predicted value assuming k is evaluated for each trace
- Sum of squared differences between predictions and observations:
  - → a posteriori probability of the traces given the key
  - → a posteriori probability of the key given the traces (Bayes)

We select the key achieving highest probability (Least Square Method)

Is this method new?

- Already mentionned by Bevan and Knudsen (ICISC'02)
- Major differences:
  - We guess the full 56-bit key (particularly suited to hardware DES)
  - We focus on two points of interest (end of first round & end of DES)

An innovative key space exploration

Computing the probabilities of all 2^{56} keys is not practicable!

An innovative key space exploration

Computing the probabilities of all 2^{56} keys is not practicable!

Partial exploration of the key space:

- Oriented iterative walk (heuristic)
- Given a key candidate k_i
  - Search for a better one k_{i+1} in a neighbourhood of k_i
  - Repeat the process until $k_{i+1} = k_i$ (stability)
- Starting from a random k_0, the best key encountered may not be the correct one (particularly with few traces)
- Explore a largest key space portion by considering several initial key candidates (increase probability of success)
- Other heuristic methods are possible: genetic algorithms, simulated annealing,...

Our results

We posted three solutions to the *Representative Order* category

(average score on 100 runs with randomly chosen traces)

They are all variants of the maximum likelihood method

Our results

We posted three solutions to the *Representative Order* category
(average score on 100 runs with randomly chosen traces)

They are all variants of the maximum likelihood method

Solution 1 (dpa_contest.representative.1.c)

- posted on August 18, 2009
- uses a bivariate known model with 3 points of interest
- key recovered with only 42.42 curves on average
- assume a strong adversary model
  - previous caraterization of the consumption function
  - need a device with fixed known key

Our results

Solution 2 (dpa_contest.representative.3.c)

- posted on August 30, 2009 (together with solution 3)
- uses a bivariate unknown model with 2 points of interest
- key recovered with 46.06 curves on average
- do not assume a strong adversary model!
  - model parameters are infered on-the-fly by linear regression

Our results

Solution 2 (dpa_contest.representative.3.c)

- posted on August 30, 2009 (together with solution 3)
- uses a bivariate unknown model with 2 points of interest
- key recovered with 46.06 curves on average
- do not assume a strong adversary model!
  - model parameters are infered on-the-fly by linear regression

Solution 3 (dpa_contest.representative.4.c)

- same as solution 2 with a univariate model
- key recovered with 53.42 curves on average

Our results

Solution 2 (dpa_contest.representative.3.c)

- posted on August 30, 2009 (together with solution 3)
- uses a bivariate unknown model with 2 points of interest
- key recovered with 46.06 curves on average
- do not assume a strong adversary model!
  - model parameters are infered on-the-fly by linear regression

Solution 3 (dpa_contest.representative.4.c)

- same as solution 2 with a univariate model
- key recovered with 53.42 curves on average

Conclusion

- Maximum likelihood method combined with full-key guessing strategy showed to be efficient to tackle the *DPA contest* challenge
- Further details about the method available in the source comments

DPA Contest 2008 – 2009
Less than 50 traces allow to recover the key

Christophe Clavier [1] [2]

[1] Institut d'Ingénierie Informatique de Limoges (3iL)
[2] Université de Limoges – XLIM

Lausanne – September 7, 2009