What is the Best Attack?

Orr Dunkelman[1]

[1]Dept. ESAT/SCD-COSIC, K.U.Leuven, Belgium.

Echternach Symmetric Cryptography, January 11, 2008

Outline

The Deciding Cryptographers Problem

- Three cryptographers are sitting down to discussion at their favorite IACR venue. Their program chair informs them that arrangements have been made with the program such that the same scheme is broken by two papers.
- Now they have to decide which of the two papers present a better attack.

How you define the best attack?

Comparing Attacks

Attacks are usually measured by:

- Data complexity
- Time complexity
- Memory complexity

Comparing Attacks

Possible metrics:

- Money!
- “Time-Memory-Data” curves
- Actual implementation
- Everybody making up their metrics?

What Money Can ~~Buy~~ Analyze

Possible costs:

- Design
- Production
- Energy
- Management
- Data acquisition

A New Cost Metric

- The cost should be stated in a cost-per-key manner.
- More precisely, in a cost-per-key-in-a-time-unit manner.

Introducing: DKY — Dollars per key in a year. The cost required to find one key in a year.

Moore's law: computational power increases by a factor 2 every 18 month

Corollary: the cost of computational power decreases by a factor 2 every 18 month

Introducing: DKY_{2008} — Dollars per key in a year (measured in the beginning of 2008).

How the Costs Really Behave

- For a really small amount of available money, exhaustive key search is the best option.
- Thus, the DKY units remain the same.
- Until paying someone to optimize the exhaustive key search software is more efficient.
- Thus, DKY is smaller (and the total cost you pay for each additional speed up is smaller).
- Until FPGA design becomes more cost-effective.
- And then ASIC becomes more cost-effective.
- And after a while, you may wish to use Hellman's time-memory tradeoff (averaging the cost of the pre-processing over many keys).

Discussion

Topics:

- Which costs exist?
- How to estimate them?
- CPUs — one vs. multiple?
- Do we really care?
- ...

Possible Curves

- Hellman's curve — $N^2 = TM^2$.
- Multiple data curve — $N^2 = TM^2D^2$.
- New curve — $N = T^\alpha M^\beta D^\gamma$.

These curves have constraints on the possible values for T, M, and D.

Discussion

Topics:

- Possible values for α, β, γ?
- Dealing with constraints?
- Comparing known plaintexts vs. chosen plaintext/ciphertexts vs. ...
- ...

Current State of Affairs

Our attack requires the least amount of data* for a small increase in the time complexity.
Take $2^{128} - \epsilon$ chosen plaintexts ...
The attack takes 2 minutes.

Why This is Bad for Us

- The resulting papers are very confusing to the reader. The NSA will not be able to use our results!
- When we discuss matters in program committees, this issue has an effect on the scoring.
- Differences between theory and practice lead to wrong optimizations.
- Prevents a real comparison between various attacks.

More Discussion is Needed!

- We do not need a consensus.
- But we do need to have a relatively small set of models.
- How do you measure small?

Thank You For Your Attention

Questions, comments, etc. can be sent to

Fredrik	Thomas	Come	Dan	Guido
Alex	Anne	Claude	Joan	Orr
Christophe	Henri	Helena	Antoine	Dmitry
Lars	Tanja	Arjen	Stefan	Florian
Willi	Ivica	Ludovic	Raphael	Bart
Chirstian	Tom (^{2})	Greg	Michael	Martin
Martijn	Iwata	Gilles	Serge	Ralph
		Erik		

Thanks for the Organization!

Committee:

- Alex
- Joan
- Serge
- Stefan

Local organizers:

- Ragga
- Dimitry