Binary Decisions Diagrams for Algebraic Attacks

Oleksandr Kazymyrov, Håvard Raddum

May 7, 2014
Winter School in Information Security
Finse, Norway

Current State

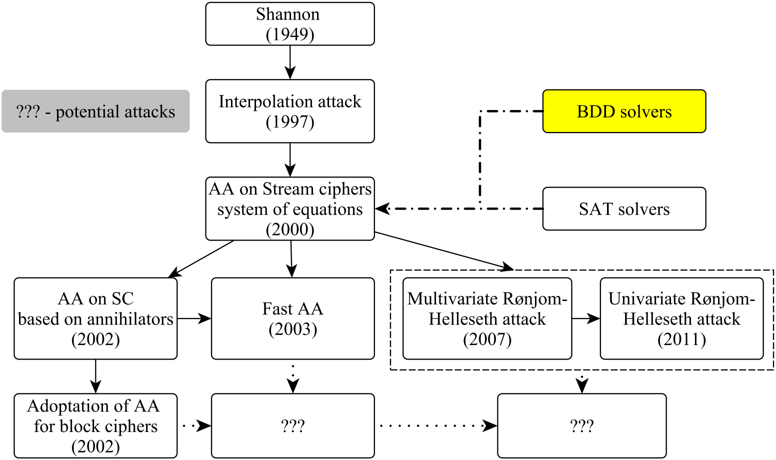


Figure : Development of Algebraic Attack

Binary Decisions Diagram (BDD)

$$f(x_1, x_2, x_3) = x_1x_3 + x_1 + x_2 + x_3 + 1$$

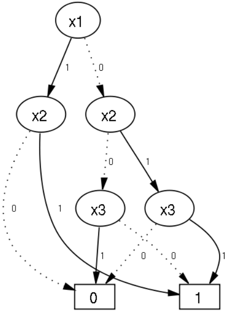


Figure : Binary decision diagram for f function

BDD in Cryptology

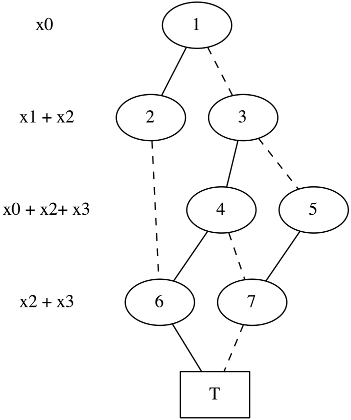
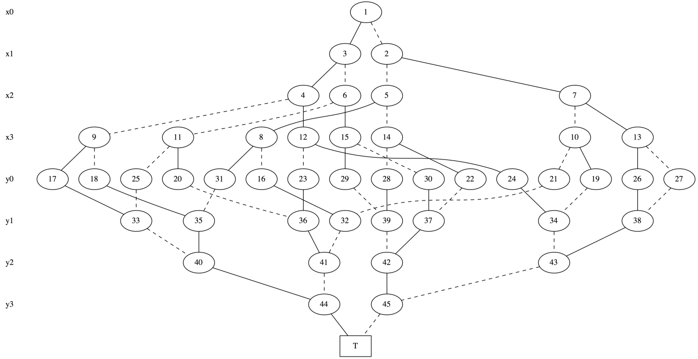


Figure : Example of a BDD with four levels

S-box Representation Using BDD

$$\text{S-box} = \{5, C, 8, F, 9, 7, 2, B, 6, A, 0, D, E, 4, 3, 1\}$$



Previous Results For Stream Ciphers

Binary decision diagram (BDD)-based cryptanalysis of

- A5/1 (GSM keystream generator)
- E0 (Bluetooth keystream generator)
- Trivium (eSTREAM Portfolio, Profile 2)
- Grain (eSTREAM Portfolio, Profile 2)
- ...

Previous Results For Block Ciphers

N.T. Courtois, G.V. Bard [1]

The 6-round DES (with 20 fixed key bits) was attacked by algebraic attack in several minutes with the help of conversion to SAT and applying MiniSat 2.0.

E. Kleiman, [2]

The MiniAES (16-bit version) was attacked by XL and XSL methods.
"This results in a large sparse system of linear equations over the field $GF(2)$ with an unknown number of extraneous solutions that need to be weeded out."

New Results of AA via BDD Representation

DES

- Our best result is finding the key of 6-round DES using 8 chosen plaintext/ciphertext pairs without fixing or guessing any variables.
- The average complexity is $2^{20.571}$ nodes, which is equivalent to $\sim$ 1 minute on MacBook Air 2013 with 8GB RAM.

MiniAES

10-round MiniAES was totally broken via the BDD method using 1 known plaintext/ciphertext pair on regular PC. The average memory complexity is $2^{24.961}$ nodes.

New Results of AA via BDD Representation

Table : Complexities for solving reduced-round DES-systems. Each cell shows the minimum, **average** and maximum complexity observed over 100 instances.

rounds \ # texts	1	2	3	4	5	6	7	8
4	$2^{22.651}$ $\mathbf{2^{22.715}}$ $2^{22.770}$	$2^{10.800}$ $\mathbf{2^{14.506}}$ $2^{17.473}$	$2^{9.281}$ $\mathbf{2^{10.606}}$ $2^{13.006}$	$2^{9.585}$ $\mathbf{2^{10.257}}$ $2^{12.029}$	$2^{9.748}$ $\mathbf{2^{9.805}}$ $2^{9.892}$	$2^{9.976}$ $\mathbf{2^{10.070}}$ $2^{10.412}$	$2^{10.103}$ $\mathbf{2^{10.203}}$ $2^{10.978}$	$2^{10.283}$ $\mathbf{2^{10.381}}$ $2^{10.446}$
5		$2^{19.472}$ $\mathbf{2^{22.110}}$ $2^{23.805}$	$2^{13.831}$ $\mathbf{2^{16.455}}$ $2^{19.329}$	$2^{11.440}$ $\mathbf{2^{13.526}}$ $2^{15.618}$	$2^{12.126}$ $\mathbf{2^{13.995}}$ $2^{16.633}$	$2^{12.289}$ $\mathbf{2^{14.212}}$ $2^{16.758}$	$2^{12.583}$ $\mathbf{2^{14.410}}$ $2^{16.882}$	$2^{12.749}$ $\mathbf{2^{14.704}}$ $2^{17.414}$
6						$2^{24.506}$ $\mathbf{2^{24.929}}$ $2^{25.352}$	$2^{22.206}$ $\mathbf{2^{22.779}}$ $2^{24.324}$	$2^{19.932}$ $\mathbf{2^{20.571}}$ $2^{21.915}$

Open Problems and Further Development

- Development of general methodology and justification of theoretical bounds:
  - Does there exist a generic algorithm giving an order of BDDs that yield low complexity when applying linear absorption?
  - Is it possible to analytically estimate the complexity of solving a BDD system of equations, or do we have to actually run the solver to find out?
  - Which ciphers are most vulnerable against this type of algebraic attacks?
- More block ciphers, stream ciphers and hash functions can be attacked

References

1. Courtois, N.T., Bard, G.V., *Algebraic cryptanalysis of the Data Encryption Standard*, Cryptography and Coding, LNCS 4887, pp. 152–169, Springer (2007).
2. Kleiman, E., *High Performance Computing techniques for attacking reduced version of AES using XL and XSL methods*, Graduate Theses and Dissertations (2010) `http://lib.dr.iastate.edu/etd/11473`.