Algebraic Attack in Presence of Non-Linear and Noisy Equations

Zahra Eskandari
Ferdowsi University of Mashhad

February 2020

Outline

- **Algebraic Attack**
- **Cube Attack**
- **Non-BlackBox Cube Attack**
- **Non-Linear and Noisy Equations**
- **Probabilistic Cube Attack**
- **Conclusion & Future Works**

Algebraic Attack

- Write the cipher as a system of polynomial equations
- Recover the secret key by solving equation system: NP-Hard
  - Gröbner basis algorithms(Buchberger, F4 and F5)
  - XL and XSL
  - SAT Solver based and Optimization approaches

In high rounds:

- Large Equation System
- Explosion in memory space
- Exponential time complexity

- Cube Attack: Offline Equation Extraction

Cube Attack

- Phase 1: Linear Equation Extraction
  - Ciphertext bit as a polynomial function of Plaintext and Key

$$C_{\mathrm{i}} = p(\mathrm{P}, K)$$

$$I \subset P, x = P \cup K, \mathrm{C_i} = t_I . Ps(I) + q(x)$$

$$Ps(I) = \sum_{v \epsilon C_I} p(\mathrm{P}, K)(mod\ 2) = p(W, K) \xrightarrow{W=\{i\epsilon P | i \notin I\}=0,} \mathrm{p(K)}$$

- Phase 2: Solving extracted equations by Gaussian Elimination

Challenges of Cube Attack

- High complexity of linear equation extraction
  - Heuristic selection of set I : Random Walk
    - Test a large number of cubes for high rounds
  - BlackBox manner
- Lack of linear equations in high rounds
  - Secret bits are confused complicatedly
  - Ciphertext bit is more dense

Non-BlackBox Equation Extraction by Division property

- Division property (Todo, 2015)
  - Successful approach to find integral distinguishers in non-blackbox manner
    - Determine initial Division Property D_{K_0} based on set I
    - Obtain D_{K_i} from the propagation rules in accordance with the round function after i rounds
    - Determine existence of integral distinguishers in r-round via a valid propagation trail:

$$K_0 \rightarrow K_1 \rightarrow K_2 \rightarrow \cdots K_r$$

  - High-growth rate of the problem: difficulty in evaluation of the propagation

- Efficient and Automatic Evaluation of propagation (Eskandari, 2018)
  - SAT-based approach to find Integral Distinguishers using division property
  - Map searching for propagation trail to a SAT problem
  - 30 primitives with different design strategies
  - Find several new or improved distinguishers with lower data complexity

Non-BlackBox Equation Extraction by Division property (Cont.)

- Employing division property in cube attacks(Eskandari,2019)
  - Adapting SAT-based approach to extract cube distinguishers in block ciphers
    - Considering key variables and key schedule function in the propagation trail
  - Decrease the complexity because of non-blackbox manner
  - Apply to lightweight block cipher KATAN32
    - Cube distinguishers are extended to higher rounds

Rounds	Number of extracted Eq.	Cube Att. Time complexity	Ref.
60	41	2^{39}	(Bard, 2010)
71	3	-	(Bard, 2010)
72	44	2^{36}	Here
90	3	-	Here

Cube size	Distinguisher type	Rounds	Ref.
31	constant cube distinguisher	83	(Ahmadiyan, 2015)
31	zero-sum integral distinguisher	99	(Sun , 2016)
31	constant cube distinguisher	101	Here

Challenges of Cube Attack

- High complexity of linear equation extraction
  - Heuristic selection of set I : Random Walk
    - Test a large number of cubes for high rounds
  - BlackBox manner
- Lack of linear equations in high rounds
  - Secret bits are confused complicatedly
  - Ciphertext bit is more dense

Nonlinear and Noisy EQ

- To prevent complexity of Non-Linear equations solving
  - probabilistic linearization
    - Linearization of nonlinear terms
    - Elimination of other terms and considering equation as noisy one
    - Extracting linear equation with high probability
- Generating probabilistic equation system

Nonlinear and Noisy EQ(Cont.)

- Solving probabilistic equation system: Noisy equation system
  - MAX-POSSO: Finding the solution that satisfies the maximum number of equations
    - Consider noisy polynomial system $\mathrm{F} = \{f_1, f_2 , \dots , f_m \}$
    - Define noise vector $e = (e_1, e_2 , \dots , e_m)$
    - Find e with the smallest Hamming weight that $\{f_1 + e_1, f_2 + e_2 , \dots , f_m + e_m\}$ has a solution
  - Approaches to solve noisy equation system
    - Optimization approaches (Albrecht, 2011)
    - Coding approaches (Yuan, 2016)
    - ISBS (Huang, 2017)

- Incremental solving & backtracking search tree (Huang, 2017)
  - Higher success rate and more efficient in comparison to others
  - Height of the search tree is dependent on the number of probabilistic equations
    - Not efficient at high error rates: near 6 hours for 20 nonlinear equations

Nonlinear and Noisy EQ(Cont.)

- To enhance the efficiency and practicality of ISBS
  - Considering the probability of equations in the search tree
  - Linearize nonlinear equations
  - Consistency checking instead of partial solving
- Near half an hour for solving equation system with 19 probabilistic equations

Probabilistic Cube Attack

- Phase 1: Linear equation extraction- deterministic and probabilistic-
- Phase 2: Solving probabilistic linear equation system using improved ISBS
  - Assigning proper noise values to probabilistic equations efficiently

- Improve the results to higher round (Eskandari, 2020)

Cipher	Rounds	Time Complexity	Approach
KATAN32	80	2^{36}	Cube Attack
	85	2^{37}	Probabilistic Cube Attack

Conclusion & Future Works

- Probabilistic cube attack utilizing Non-Linear and Noisy equations
  - Extend original cube attacks to higher round
- Open problem: can we extend algebraic attack to higher round utilizing Noisy and lower degree equations?
- Application of noisy equations solving in Side Channel attacks

Thanks for Your Attention