Crypto-seminar 2014–2015 Fall

Faruk Göloğlu

September 9, 2014

Discrete Logarithm Problem

- In 2013 and 2014, there was quite a bit of developments on the Discrete logarithm problem (DLP) in small characteristic finite fields. Recently, Barbulescu, Gaudry, Joux and Tome came up with a heuristic quasi-polynomial algorithm for DLP in finite fields with small characteristic.

Project 1

Discrete Logarithm Problem

- In 2013 and 2014, there was quite a bit of developments on the Discrete logarithm problem (DLP) in small characteristic finite fields. Recently, Barbulescu, Gaudry, Joux and Tome came up with a heuristic quasi-polynomial algorithm for DLP in finite fields with small characteristic.
- The duty of the student in the project is a study on the following paper.

  R. Barbulescu, P. Gaudry, A. Joux and E. Thome, *A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic*, EUROCRYPT 2014 (Best Paper Award).

Project 1

Discrete Logarithm Problem

- In 2013 and 2014, there was quite a bit of developments on the Discrete logarithm problem (DLP) in small characteristic finite fields. Recently, Barbulescu, Gaudry, Joux and Tome came up with a heuristic quasi-polynomial algorithm for DLP in finite fields with small characteristic.
- The duty of the student in the project is a study on the following paper.

  R. Barbulescu, P. Gaudry, A. Joux and E. Thome, *A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic*, EUROCRYPT 2014 (Best Paper Award).
- Level MSc.

Biclique

- Biclique attack is the best known cryptanalysis of AES, which can be directed towards block ciphers and hash functions. It is a variant of MITM (meet-in-the-middle) attacks.

Biclique

- Biclique attack is the best known cryptanalysis of AES, which can be directed towards block ciphers and hash functions. It is a variant of MITM (meet-in-the-middle) attacks.

$$C = \mathrm{ENC}_{k_2}(\mathrm{ENC}_{k_1}(P))$$
$$P = \mathrm{DEC}_{k_1}(\mathrm{DEC}_{k_2}(C))$$

Project 2

Biclique

- Biclique attack is the best known cryptanalysis of AES, which can be directed towards block ciphers and hash functions. It is a variant of MITM (meet-in-the-middle) attacks.

$$C = \mathrm{ENC}_{k_2}(\mathrm{ENC}_{k_1}(P))$$
$$P = \mathrm{DEC}_{k_1}(\mathrm{DEC}_{k_2}(C))$$

- In this project, the student will perform a study of biclique cryptanalyses based on the following paper:

  A. Bogdanov, D. Khovratovich and C. Rechberger, *Biclique Cryptanalysis of the Full AES*, ASIACRYPT 2011. http://research.microsoft.com/en-us/projects/cryptanalysis/aesbc.pdf

Project 2

Biclique

- Biclique attack is the best known cryptanalysis of AES, which can be directed towards block ciphers and hash functions. It is a variant of MITM (meet-in-the-middle) attacks.

$$C = \mathrm{ENC}_{k_2}(\mathrm{ENC}_{k_1}(P))$$
$$P = \mathrm{DEC}_{k_1}(\mathrm{DEC}_{k_2}(C))$$

- In this project, the student will perform a study of biclique cryptanalyses based on the following paper:

  A. Bogdanov, D. Khovratovich and C. Rechberger, *Biclique Cryptanalysis of the Full AES*, ASIACRYPT 2011. http://research.microsoft.com/en-us/projects/cryptanalysis/aesbc.pdf

- Level MSc.