Bachelor's Thesis Opponent's Report

Title: A study on "A New Public-Key Cryptosystem via Mersenne Numbers"
Author: Filip Richter

Thesis content

Thesis describes recently published proposal of a public-key cryptosystem based on complexity of expressing a number as quotient of numbers with small equal weights. Cryptosystem computations are performed in fields with Mersenne prime order. Both single-bit and multiple-bit versions of the cryptosystem are presented. Main part of the thesis deals with published attacks on the single-bit version. One of these attacks is of meet-in-the-middle type, where the problem is translated to the task of finding small weight numbers with particular binary representations which products with public key have small Hamming distance. The other attack uses LLL algorithm for finding small vectors in a lattice constructed with rotations of public key and with specific partitions of indices of binary representations of field elements. Asymptotic analysis of meet-in-the-middle attack is included. Attached to the thesis are author's implementations of both attacks.

Thesis evaluation

Topic. This cryptosystem proposal and its underlying problem is interesting from both mathematical and cryptologic points of view. This fact is confirmed by publications analyzing the system. Author of the thesis was able to rephrase published results properly and also include his own formulations. By this, in my opinion, author accomplished the purpose of the work.

Author's contribution. In some cases, author provides own proofs of needed statements and completes argumentation omitted from published papers (e.g. proofs of lemmas 2, 7, 11). Author implemented known attacks with some improvements of sub-algorithms (e.g. choosing random partitions for lattice attack).

Mathematical standard. In spite of certain inconsistency in notation, author formulates the related theory correctly. All referred notions are properly defined and statements are derived rigorously.

Use of sources. Author adopted published results, in few cases found own formulation of proofs and filled in some missing argumentation. He also developed own version of some sub-algorithms.

Form. Major part of the thesis is written in a consistent form. There are some formal errors but their amount is tolerable.

Comments

1. In the first chapter, binary representation of an integer b is defined. It follows from the definition that b must be non-negative. This mistake is repeated several times.
2. The first chapter deals with binary representations and weights of elements of the ring $\mathbb{Z}_n$. Here, only the standard representative set of congruence classes modulo n is considered. This fact should be stated explicitly.
3. In the first chapter, symbols n and p are used for Mersenne numbers. This notation is confused for instance in the first part of the proof of Lemma 2.

4. In the second chapter, there is an error in the definition of encryption. It should be: $C = (-1^b)(AH + B)$. This error repeats later in the chapter.

5. Throughout the thesis notation of some basic parameters is not consistent. For instance, notation of public and secret keys changes from upper to lower case letters.

6. Last sentence of the proof of Claim 12 does not make sense.

7. In Definition 20, there should be: $j \in [i_l, i_{l+1}]$.

8. Second remark following Definition 20 is wrong. There should be: $\lfloor \log_2((b_{i_{j+1}}, \ldots, b_{i_j})_2) \rfloor \leq i_{j+1} - i_j$.

Verdict

The work meets the required criteria. I recommend to accept the work as bachelor's thesis.

Opponent will notify chairman of the examination committee of the proposed classification.

Robert El Bashir
12. 6. 2019