Master's Thesis Opponent's Report

Title: Cryptography based on semirings
Author: Bc. Martin Mach

The thesis studies versions of key exchange protocols over tropical algebras. Namely, the two variants of Stickel's key exchange protocol are analyzed where the computations are performed in semigroups of tropical matrices.

First, published attacks on the full version of Stickel's protocol are explored. It is found that success rate of the attacks is high for matrices with some entries negative but it sharply declines when non-negative matrices are used. This observation is supported by results of author's computer experiments and is explained also theoretically as powers of tropical matrices with negative entries behave in a specific way. Author proposes his own version of a published attack to address the non-negative case. Complexity of the proposal is analyzed and an asymptotic estimate is given (see below comments and questions on Algorithm 9).

The next sections focus on simplified version of key exchange called Fast Stickel's protocol. Again, behaviour of powers of tropical matrices is crucial for security of the protocol. The impact of cyclicity of irreducible tropical matrices on efficiency of attacks is pointed out. The estimates of cyclicity and transience of irreducible tropical matrices determine complexity of the attacks. Author tries to extend the theory to reducible matrices using the notion of partially constant matrix. An interesting hypothesis on powers of reducible tropical matrices with two diagonal blocks is formulated though it is neither proved nor rejected.

Attack on Fast Stickel's protocol with irreducible matrices is proposed and an estimate of its asymptotic complexity is proven. The idea is then extended to reducible matrices with two diagonal blocks. The conditions of attack's success are given as well as an estimate of its complexity.

The final section formulates some problems connected to the complexity of breaking Fast Stickel's protocol. The situation is analogous to the classical Diffie-Hellman theory. Also, an estimate of solving discrete logarithm problem for irreducible tropical matrices is established.

Thesis is well written except for minor language flaws. Theoretical results are complemented by computer experiments and a number of examples. In few cases, structure of the text and used formulations should be more rigorous (see the comments below). Thesis contains interesting theoretical results and proposals although some of the posed questions remained open.

The work meets the required criteria. I recommend to accept the work as master's thesis. *Opponent will notify chairman of the examination committee of the proposed classification.*

Comments

1. In Definition 3, it seems that multiplication by ε is not explicitly determined.
2. In the statement of Lemma 1, what is the exact meaning of "the value of an element"?
3. Definition 9 should precede Definition 8.

4. The opening of subsection 1.4 mentiones one-way functions and their use in public-key cryptography. Multiplication of integers is given as an example of such function. However, this does not map elements of the same set. The correct example should be encryption of messages with public-key.

5. The use of variable y in Definition 14 is confusing.

6. In the description of the second step of Algorithm 9, the minimum should have a different index set.

7. The third step of Algorithm 9 seems to be superfluous since it is a special case of step 4.

8. In Algorithm 9, an approximation of minimal cover is constructed by picking sets with maximal sizes. It comes to mind that picking sets which provide maximal increase of the covered area could be a better choice.

9. In proof of Theorem 10 the word "field" is used for (two-dimensional) arrays.

10. The closing paragraph of subsection 2.4 concludes that the described attack has high success rate and low complexity. It should be emphasized that succes rate of the attack remains unproved.

11. In the last but one paragraph of subsection 2.5 it should be "exponential in log d".

12. From the formulations surrounding Claim 15 it is not clear whether this is a proven statement. In such a case the rigorous prove should be given.

13. In the paragraph following Claim 15 should be "the least common multiple".

14. Proof of Lemma 16 is omitted. Author should cite published statements from which this can be derived.

15. To make the analysis in subsection 4.2 complete, the case with equal products of average costs of a step in critical cycles of diagonal blocks should be also discussed.

16. The formulation of problem (P3) in section 5 does make sence only using the statement in subsequent Remark which should precede the problem formulation.

Robert El Bashir
5. 9. 2019