Report on “Cryptosystems based on coding theory”

The thesis is on cryptosystems that are based on coding theory. Code-base cryptography is a very important technique that is widely used in cryprosystems. They are one of the important alternatives in post-quantum cryptography which is a very important current branch of cryptography related research. The thesis surveys many fundamental code-based cryptosystems and their variations as well as classical attacks against them.

The thesis starts with a succinct introduction explaining main coding theoretic and cryptographic concepts. Chapter 2 is devoted to description of two important code- based cryptosystems, namely, McEliece and Niederreiter PKC. In Chapter 3, a classical cryptanalysis method due to Stern is explained and with applications to McEliece PKC. Chapter 4 is a core part of the thesis, where the student explains Sidelnikov-Shestakov attack in great detail using multiple sources. Chapter 5 introduces rank-metric variants, known as Gabidulin codes which is another important coding theoretic/cryptographic object that has become popular in recent years. Here Gabidulin/MRD codes and related cryptosytems are introduced as well as attacks (such as the one due to Overbeck) against them. Moreover, the student takes on a comment on Overbeck [Ove 05, p. 52] which states that a variant of Sidelnikov-Shestakov attack could be used against a GGPT system when a parameter X selected to be trivial with complexity $O(n^3)$. The student gives arguments that such an attack does not seem plausible, and gives her own version of an attack with complexity $O(n^6)$. She explains the attack and the complexity analysis in detail, which seem correct according to my detailed checks.

Topic of the thesis: The topic is extremely suitable for a Diploma thesis.

Mathematical content: The mathematical content of the thesis is surely adequate. The student clearly explains the derivations, in much more detail compared to the sources used, in correct, logical and natural ways. For instance in Section 4, Möbius transforms are used after a detailed introduction, to explain Sidelnikov-Shestakov attack, where every detail is presented. Detailed examples are worked out etc. Many interesting mathematical concepts are used overall the thesis, and the student shows that she is comfortable with them.

Citations/References: Many sources are used effectively and carefully cited overall the thesis.

Student’s contribution: Student analyzes in detail a comment of Overbeck (mentioned above) and produces an algorithm for an attack when a variable is selected in a trivial fashion. The contribution is correct. It shows that the student understood the ideas used in the literature and can work with them to prove new results.

A few comments on formal issues (which are not many):

- It is good practice to introduce the abbreviations also in the introduction. It should be possible to read it without consulting the main text.
- Definition 6. It does not define the problem. One should write: “General Decoding Problem is to find the . . . ”
- A few typos:

p. 10: An example $\Longrightarrow$ examples

overall: One should use “ ” instead of ” ”

overall: article errors such as omissions of “a” and “the” in several places

p. 23: representant $\Longrightarrow$ representative

p. 43: previous chapter: I think it should be “previous section”

p. 59: pulic $\Longrightarrow$ public

p. 70: addings $\Longrightarrow$ additions

Conclusion: commented $\Longrightarrow$ commented on

Conclusion: I think saying that such an attack “cannot work” is a bit too strong.

Question 1 *In Section 5.5.2, you comment that the attack based on Sidelnikov-Shestakov attack does not seem to work because “you could not convert the mapping $x \mapsto 1/x$ to a linear mapping $x \mapsto L(x)$.” If one wants to solve*

$$L(x) = 1/x$$

one might convert it to a “quadratic” equation

$$xL(x) = 1.$$

Writing such equation in $\mathbb{F}_p$ variables one gets a “quadratic system” in n variables which can be converted to a linear system in $n^2 + n$ variables. Solving it by Gaussian reduction would give an $O(n^6)$ algorithm as yours. Do you think your algorithm and the above idea are related?

Conclusion: I think the thesis is a very good survey combined with a small but nicely worked out contribution. Although the contribution may not be considered very strong, in my opinion, it warrants awarding of the best grade.

Suggested grade: 1.