Cryptographic Protocols

Homework 2

1. Let us define the following variation of the DDH game:

\[ \text{DDH}_{G,A}^* \]

\[ \begin{align*}
(x, y, r, s) &\leftarrow U\mathbb{Z}_q^2; \\
z_0 &\leftarrow rs; z_1 &\leftarrow U\mathbb{Z}_q; \\
b &\leftarrow \{0, 1\}; \\
b' &\leftarrow A(g^x, g^y, g^{x+}, g^{y+}, g^{z+b}); \\
\text{return} & b = b';
\end{align*} \]

Assuming the same terminology as in the lecture slides, show that if \( G \) is a \((t, \varepsilon)\)-DDH group, then it is also \((t', \varepsilon')\)-DDH* group. Reduction should be efficient and please also provide a precise expression for \( t' \) and \( \varepsilon' \). (2pt)

2. The Secure Bidding course has the curious property that a student can set the amount of points they would like to get for the course. However, there’s a catch: the students have to encrypt their “bids” of grades by Elgamal, using the parameters given by the professor, with the following rules:

- Students choose numbers 0-100 as their number of points. However, the passing grade is 40: anything less will make you fail.
- The student with the lowest point request will fail the course. If there is a tie, these students will all fail.
- The student with the highest points request will take an exam, where he needs to at least get the number of points he requested, to pass the course. If there is a tie, these students will all take the exam.
- If there is a tie for some other points, only the person who submitted their points request first will pass the course.
- Every other student who requests a valid passing number will pass the course.

Four lazy students taking the course would like to pass the course without any of them taking the exam. By some great slice of fortune, they know that only two students, Alice and Bob, have submitted their values, say \( A \) and \( B \). Moreover, they know some other facts about these bids

(a) \( B \) is approximately \( 1.5 \cdot A \), with \( A \) at least 40.
(b) \( A \) is a multiple of 5, while \( B \) is a multiple of 7.
(c) Devise a strategy for these four students to pass without an exam, and give four ciphertexts denoting their encrypted bids according to this strategy.
(d) Is it always possible for 5 students to pull off the same feat? (3pt)
3. Implement lifted Elgamal encryption using the following template: 

https://courses.cs.ut.ee/MTAT.07.014/2018_fall/uploads/Main/elgamal_lift_template.txt

Decryption should work for short messages. Feel free to introduce modifications to the template. (2p)

4. Implement homomorphic polynomial evaluation using lifted Elgamal (function `homomorphic_poly` in the template). Namely a function should take as an input lifted Elgamal ciphertexts encrypting messages $m, m^2, \ldots, m^n$ and coefficients $k_0, \ldots, k_n$, and output a ciphertext encrypting a message $\sum_{i=0}^{n} k_i m^i$. Final ciphertext should also be rerandomized before outputting. Make sure that decryption gives the correct value. (2p)