CRYPTO WORKS (MAMME, Spring 2020): ASSIGNED EXERCISES TO EACH GROUP

(when I do not say the contrary, references to exercises in the book refer to the version 0.4 in Atenea: https://atenea.upc.edu/pluginfile.php/3090839/mod_resource/content/1/BonehShoup_0_4_for_FME_Crypto.pdf)

- Group 1: Almirall, González, Mijares, Sánchez.

- Exercise 4.13 of the book
- Exercise 11.6 of the book
- Exercise 13.14 of the book
- Exercise 3, Exam of October'2018: https://atenea.upc.edu/pluginfile.php/3090291/mod_resource/content/1/Crypto_exam_october_2018.pdf

- Group 2: Altarriba, Gonzalvo, Mir, Segarra.

- Exercise 7.9 (page 140) in: https://web.engr.oregonstate.edu/~rosulekm/crypto/chap7.pdf
- Exercise 11.1 of the book
- Exercise 13.6 of the book
- Exercise 4 (parts a,b), Exam of December'2015: https://atenea.upc.edu/pluginfile.php/3089195/mod_resource/content/1/exam_Crypto_December_2015.pdf

- Group 3: Costantini, Herrerias, Ott, Tobar.

- Exercise 3.17 of the book
- Exercise 11.13 of the book
- Exercise 13.10 of the book
- Exercise 4, Exam of January'2016: https://atenea.upc.edu/pluginfile.php/3089196/mod_resource/content/1/exam_Crypto_January_2016.pdf

- Group 4: Gamboa, Irizar, Oviedo, Torrents.

- Exercise 4.8 of the book
- Exercise 12.17 of the book (maybe exercise 11.7 can be an inspiration)
- BLS is similar to FDH-RSA in some sense: they are both deterministic signature schemes, and the security reduction (in the random oracle model) to the underlying hard problem (either the RSA problem or the CDH problem) is not tight: the basic proof has a factor q_H in the relation between the success probabilities; this can be improved to a factor of q_S. (Here q_H is the number of Hash queries and q_S is the number of signature queries, done by the attacker against the signature scheme).

Similarly to problem 13.10 of the book, describe a probabilistic version of BLS whose security in the random oracle model can be tightly related to the hardness of the CDH problem.

- Exercise 4, Exam of December'2014: https://atenea.upc.edu/pluginfile.php/3089194/mod_resource/content/1/exam_Crypto_december_2014.pdf

- Group 5: Gómez, Masip, Palfner, Vilar.

- Exercise 3.22 of the book
- Exercise 11.15 of the book
- Exercise 15.6 from **version 0.5** of the book
- Exercise 4, Exam of December'2016: https://atenea.upc.edu/pluginfile.php/3089198/mod_resource/content/1/Crypto_exam_december_2016.pdf