CMSC 5719 Seminar
Chinese University of Hong Kong

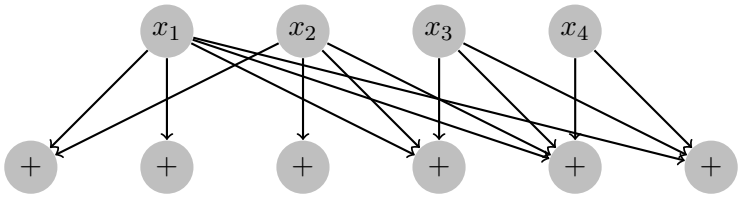
Homework questions
due on 13 February 2012

Problem 1 When Julius Caesar was getting ready for battle, he sent his soldiers the following message:

```
PHHWPHDWWJHUXELFRQ
```

Can you figure out what he said?

Problem 2 Recall the toy one-bit public-key encryption scheme we showed in class. To encrypt a bit, Alice chooses a random "seed" x of four bits and applies the following circuit to it. In this question + represents addition modulo two, namely the XOR operation:



To encrypt zero, Alice sends the resulting output plus some noise. To output one, Alice first flips all bits of the output, then sends out the result plus some noise. To decrypt, Bob XORs the three first bits of the encryption.

(a) Assume there is no noise. Suppose $e_1, e_2, \ldots, e_{10}$ are encryptions of bits $m_1, m_2, \ldots, m_{10}$, respectively. Show that if Bob decrypts $e_1 + e_2 + \cdots + e_{10}$ (here + is bitwise XOR), he obtains the message $m_1 + m_2 + \cdots + m_{10}$.

(b) Now suppose Alice applies independent noise of rate 0.1 to her encryptions. This means the bit at each of the six positions of the encryption is changed independently at random with probability 0.1 (and stays the same with probability 0.9. Recall that this noise is necessary to keep the encryptions secure. If Alice sends such a noisy encryption e, there is some probability that Bob will decrypt e incorrectly. Can you calculate this probability?

(c) Now Alice creates ten encryptions $e_1, \ldots, e_{10}$ applying noise of rate 0.1 to each one of them. In part (a), you showed that if there was no noise, $e_1 + \cdots + e_{10}$ would decrypt to $m_1 + \cdots + m_{10}$. In the presence of noise, what is the probability that $e_1 + \cdots + e_{10}$ does not decrypt to $m_1 + \cdots + m_{10}$?