Solutions to HW09 Problems

BILL, RECORD LECTURE!!!!

BILL RECORD LECTURE!!!

HW09, Problem 2a

A & B do PRIV-LWE with $\vec{k} = (11, 100, 39, 4)$, $p = 1009$, $\gamma = 2$.
All $\equiv$ are mod 1009.

HW09, Problem 2a

A & B do PRIV-LWE with $\vec{k} = (11, 100, 39, 4)$, $p = 1009$, $\gamma = 2$.
All $\equiv$ are mod 1009.
a) A wants to send 1. Random vector is $(1, 2, 3, 4)$. e is 2. What does she send B?

HW09, Problem 2a

A & B do PRIV-LWE with $\vec{k} = (11, 100, 39, 4)$, $p = 1009$, $\gamma = 2$.
All $\equiv$ are mod 1009.
a) A wants to send 1. Random vector is $(1, 2, 3, 4)$. e is 2. What does she send B?
SOLUTION

HW09, Problem 2a

A & B do PRIV-LWE with $\vec{k} = (11, 100, 39, 4)$, $p = 1009$, $\gamma = 2$.
All $\equiv$ are mod 1009.
a) A wants to send 1. Random vector is $(1, 2, 3, 4)$. e is 2. What does she send B?
SOLUTION
A computes

HW09, Problem 2a

A & B do PRIV-LWE with $\vec{k} = (11, 100, 39, 4)$, $p = 1009$, $\gamma = 2$.
All $\equiv$ are mod 1009.
a) A wants to send 1. Random vector is $(1, 2, 3, 4)$. e is 2. What does she send B?

SOLUTION

A computes

$$C = (11, 100, 39, 4) \cdot (1, 2, 3, 4) = 11 + 200 + 117 + 16 = 344 \equiv 344.$$

HW09, Problem 2a

A & B do PRIV-LWE with $\vec{k} = (11, 100, 39, 4)$, $p = 1009$, $\gamma = 2$.
All $\equiv$ are mod 1009.
a) A wants to send 1. Random vector is $(1, 2, 3, 4)$. e is 2. What does she send B?

SOLUTION

A computes

$$C = (11, 100, 39, 4) \cdot (1, 2, 3, 4) = 11 + 200 + 117 + 16 = 344 \equiv 344.$$

$$D \equiv C + e + \frac{bp}{4} = 344 + 2 + \frac{1009}{4} = 346 + 252 = 598.$$

HW09, Problem 2a

A & B do PRIV-LWE with $\vec{k} = (11, 100, 39, 4)$, $p = 1009$, $\gamma = 2$.
All $\equiv$ are mod 1009.
a) A wants to send 1. Random vector is $(1, 2, 3, 4)$. e is 2. What does she send B?

SOLUTION

A computes

$$C = (11, 100, 39, 4) \cdot (1, 2, 3, 4) = 11 + 200 + 117 + 16 = 344 \equiv 344.$$

$$D \equiv C + e + \frac{bp}{4} = 344 + 2 + \frac{1009}{4} = 346 + 252 = 598.$$

A sends $(1, 2, 3, 4; 598)$.

HW09, Problem 2b

A & B do PRIV-LWE with $\vec{k} = (11, 100, 39, 4)$, $p = 1009$, $\gamma = 2$.
All $\equiv$ are mod 1009.

HW09, Problem 2b

A & B do PRIV-LWE with $\vec{k} = (11, 100, 39, 4)$, $p = 1009$, $\gamma = 2$.
All $\equiv$ are mod 1009.
b) A wants to send 0. Random vector is $(5, 10, 41, 3)$. e is -1.
What does she send B?

HW09, Problem 2b

A & B do PRIV-LWE with $\vec{k} = (11, 100, 39, 4)$, $p = 1009$, $\gamma = 2$.
All $\equiv$ are mod 1009.
b) A wants to send 0. Random vector is $(5, 10, 41, 3)$. e is -1.
What does she send B?
SOLUTION

HW09, Problem 2b

A & B do PRIV-LWE with $\vec{k} = (11, 100, 39, 4)$, $p = 1009$, $\gamma = 2$.
All $\equiv$ are mod 1009.
b) A wants to send 0. Random vector is $(5, 10, 41, 3)$. e is -1.
What does she send B?
SOLUTION
A computes

HW09, Problem 2b

A & B do PRIV-LWE with $\vec{k} = (11, 100, 39, 4)$, $p = 1009$, $\gamma = 2$.
All $\equiv$ are mod 1009.
b) A wants to send 0. Random vector is $(5, 10, 41, 3)$. e is -1.
What does she send B?

SOLUTION

A computes

$$C = (11, 100, 39, 4) \cdot (5, 10, 41, 3) = 55 + 1000 + 1599 + 12 = 2666 \equiv 648.$$

HW09, Problem 2b

A & B do PRIV-LWE with $\vec{k} = (11, 100, 39, 4)$, $p = 1009$, $\gamma = 2$.
All $\equiv$ are mod 1009.
b) A wants to send 0. Random vector is $(5, 10, 41, 3)$. e is -1.
What does she send B?

SOLUTION

A computes

$$C = (11, 100, 39, 4) \cdot (5, 10, 41, 3) = 55 + 1000 + 1599 + 12 = 2666 \equiv 648.$$

$$D \equiv C + e + \frac{bp}{4} = 648 - 1 + 0 = 647.$$

HW09, Problem 2b

A & B do PRIV-LWE with $\vec{k} = (11, 100, 39, 4)$, $p = 1009$, $\gamma = 2$.
All $\equiv$ are mod 1009.
b) A wants to send 0. Random vector is $(5, 10, 41, 3)$. e is -1.
What does she send B?
SOLUTION
A computes

$$C = (11, 100, 39, 4) \cdot (5, 10, 41, 3) = 55+1000+1599+12 = 2666 \equiv 648.$$

$$D \equiv C + e + \frac{bp}{4} = 648 - 1 + 0 = 647.$$

A sends $(5, 10, 41, 3; 647)$.

HW09, Problem 2c

A & B do PRIV-LWE with $\vec{k} = (11, 100, 39, 4)$, $p = 1009$, $\gamma = 2$.
All $\equiv$ are mod 1009.

HW09, Problem 2c

A & B do PRIV-LWE with $\vec{k} = (11, 100, 39, 4)$, $p = 1009$, $\gamma = 2$.
All $\equiv$ are mod 1009.
c) B gets $(12, 39, 44, 19; 779)$ from A. What bit did A send?

HW09, Problem 2c

A & B do PRIV-LWE with $\vec{k} = (11, 100, 39, 4)$, $p = 1009$, $\gamma = 2$.
All $\equiv$ are mod 1009.
c) B gets $(12, 39, 44, 19; 779)$ from A. What bit did A send?
SOLUTION

HW09, Problem 2c

A & B do PRIV-LWE with $\vec{k} = (11, 100, 39, 4)$, $p = 1009$, $\gamma = 2$.
All $\equiv$ are mod 1009.
c) B gets $(12, 39, 44, 19; 779)$ from A. What bit did A send?
SOLUTION
B knows secret key (11,100,39,4) so he computes:

HW09, Problem 2c

A & B do PRIV-LWE with $\vec{k} = (11, 100, 39, 4)$, $p = 1009$, $\gamma = 2$.
All $\equiv$ are mod 1009.
c) B gets $(12, 39, 44, 19; 779)$ from A. What bit did A send?
SOLUTION
B knows secret key (11,100,39,4) so he computes:

$$(11, 100, 39, 4) \cdot (12, 39, 44, 19) = 5824 \equiv 779$$

HW09, Problem 2c

A & B do PRIV-LWE with $\vec{k} = (11, 100, 39, 4)$, $p = 1009$, $\gamma = 2$.
All $\equiv$ are mod 1009.
c) B gets $(12, 39, 44, 19; 779)$ from A. What bit did A send?
SOLUTION
B knows secret key (11,100,39,4) so he computes:

$$(11, 100, 39, 4) \cdot (12, 39, 44, 19) = 5824 \equiv 779$$

779 is 0 away from 779 and $0 < 2$. So the bit is 0.

HW09, Problem 3a

A & B do PRIV-LWE with $\vec{k} = (10, 201, 89, 8)$, $p = 2003$, $\gamma = 4$. Everything is mod 2003.

HW09, Problem 3a

A & B do PRIV-LWE with $\vec{k} = (10, 201, 89, 8)$, $p = 2003$, $\gamma = 4$.
Everything is mod 2003.
A &B think that E might be tampering with messages!

HW09, Problem 3a

A & B do PRIV-LWE with $\vec{k} = (10, 201, 89, 8)$, $p = 2003$, $\gamma = 4$.
Everything is mod 2003.
A &B think that E might be tampering with messages!
Give an algorithm so that, if B gets $(r_1, r_2, r_3, r_4; D)$, he will output one of the following

HW09, Problem 3a

A & B do PRIV-LWE with $\vec{k} = (10, 201, 89, 8)$, $p = 2003$, $\gamma = 4$.
Everything is mod 2003.
A &B think that E might be tampering with messages!
Give an algorithm so that, if B gets $(r_1, r_2, r_3, r_4; D)$, he will output one of the following

- A probably sent a 0.

HW09, Problem 3a

A & B do PRIV-LWE with $\vec{k} = (10, 201, 89, 8)$, $p = 2003$, $\gamma = 4$.
Everything is mod 2003.
A &B think that E might be tampering with messages!
Give an algorithm so that, if B gets $(r_1, r_2, r_3, r_4; D)$, he will output one of the following

- A probably sent a 0.
- A probably sent a 1.

HW09, Problem 3a

A & B do PRIV-LWE with $\vec{k} = (10, 201, 89, 8)$, $p = 2003$, $\gamma = 4$.
Everything is mod 2003.
A &B think that E might be tampering with messages!
Give an algorithm so that, if B gets $(r_1, r_2, r_3, r_4; D)$, he will output one of the following

- A probably sent a 0.
- A probably sent a 1.
- E definitely tampered with the message.

HW09, Problem 3a

A & B do PRIV-LWE with $\vec{k} = (10, 201, 89, 8)$, $p = 2003$, $\gamma = 4$.
Everything is mod 2003.
A &B think that E might be tampering with messages!
Give an algorithm so that, if B gets $(r_1, r_2, r_3, r_4; D)$, he will output one of the following

- A probably sent a 0.
- A probably sent a 1.
- E definitely tampered with the message.

SOLUTION

HW09, Problem 3a

A & B do PRIV-LWE with $\vec{k} = (10, 201, 89, 8)$, $p = 2003$, $\gamma = 4$.
Everything is mod 2003.
A &B think that E might be tampering with messages!
Give an algorithm so that, if B gets $(r_1, r_2, r_3, r_4; D)$, he will output one of the following

- A probably sent a 0.
- A probably sent a 1.
- E definitely tampered with the message.

SOLUTION
B receives $(r_1, r_2, r_3, r_4; D)$.

HW09, Problem 3a

A & B do PRIV-LWE with $\vec{k} = (10, 201, 89, 8)$, $p = 2003$, $\gamma = 4$.
Everything is mod 2003.
A &B think that E might be tampering with messages!
Give an algorithm so that, if B gets $(r_1, r_2, r_3, r_4; D)$, he will output one of the following

- A probably sent a 0.
- A probably sent a 1.
- E definitely tampered with the message.

SOLUTION
B receives $(r_1, r_2, r_3, r_4; D)$.
B finds the bit as usual: computes $C \equiv \vec{r} \cdot \vec{k}$.

HW09, Problem 3a

A & B do PRIV-LWE with $\vec{k} = (10, 201, 89, 8)$, $p = 2003$, $\gamma = 4$.
Everything is mod 2003.
A &B think that E might be tampering with messages!
Give an algorithm so that, if B gets $(r_1, r_2, r_3, r_4; D)$, he will output one of the following

- A probably sent a 0.
- A probably sent a 1.
- E definitely tampered with the message.

SOLUTION
B receives $(r_1, r_2, r_3, r_4; D)$.
B finds the bit as usual: computes $C \equiv \vec{r} \cdot \vec{k}$.
If $|D - C| \le 4$ then output **A probably sent a 0.**

HW09, Problem 3a

A & B do PRIV-LWE with $\vec{k} = (10, 201, 89, 8)$, $p = 2003$, $\gamma = 4$.
Everything is mod 2003.
A &B think that E might be tampering with messages!
Give an algorithm so that, if B gets $(r_1, r_2, r_3, r_4; D)$, he will output one of the following

- A probably sent a 0.
- A probably sent a 1.
- E definitely tampered with the message.

SOLUTION

B receives $(r_1, r_2, r_3, r_4; D)$.
B finds the bit as usual: computes $C \equiv \vec{r} \cdot \vec{k}$.
If $|D - C| \leq 4$ then output **A probably sent a 0.**
If $|D - (C + \frac{p}{4})| \leq 4$ then output **A probably sent a 1.**

HW09, Problem 3a

A & B do PRIV-LWE with $\vec{k} = (10, 201, 89, 8)$, $p = 2003$, $\gamma = 4$.
Everything is mod 2003.
A &B think that E might be tampering with messages!
Give an algorithm so that, if B gets $(r_1, r_2, r_3, r_4; D)$, he will output one of the following

- A probably sent a 0.
- A probably sent a 1.
- E definitely tampered with the message.

SOLUTION
B receives $(r_1, r_2, r_3, r_4; D)$.
B finds the bit as usual: computes $C \equiv \vec{r} \cdot \vec{k}$.
If $|D - C| \le 4$ then output **A probably sent a 0.**
If $|D - (C + \frac{p}{4})| \le 4$ then output **A probably sent a 1.**
If NEITHER then output *E tampered with the message.*

HW09, Problem 3b

A & B do PRIV-LWE with $\vec{k} = (10, 201, 89, 8)$, $p = 2003$, $\gamma = 4$.
Everything is mod 2003.

HW09, Problem 3b

A & B do PRIV-LWE with $\vec{k} = (10, 201, 89, 8)$, $p = 2003$, $\gamma = 4$.
Everything is mod 2003.
b) Use your algorithm on the following:
$(1, 2, 3, 4; 5)$.
$(11, 40, 99, 101; 245)$.

HW09, Problem 3b

A & B do PRIV-LWE with $\vec{k} = (10, 201, 89, 8)$, $p = 2003$, $\gamma = 4$.
Everything is mod 2003.
b) Use your algorithm on the following:
$(1, 2, 3, 4; 5)$.
$(11, 40, 99, 101; 245)$.

SOLUTION

$(1, 2, 3, 4; 5)$.

$$C \equiv (1, 2, 3, 4) \cdot (10, 201, 89, 8) \equiv 711.$$

This is NOT close to 5, nor is $711 + 500 \equiv 1211$, so TAMPERED WITH.

HW09, Problem 3b

A & B do PRIV-LWE with $\vec{k} = (10, 201, 89, 8)$, $p = 2003$, $\gamma = 4$.
Everything is mod 2003.
b) Use your algorithm on the following:
$(1, 2, 3, 4; 5)$.
$(11, 40, 99, 101; 245)$.

SOLUTION

$(1, 2, 3, 4; 5)$.

$$C \equiv (1, 2, 3, 4) \cdot (10, 201, 89, 8) \equiv 711.$$

This is NOT close to 5, nor is $711 + 500 \equiv 1211$, so TAMPERED WITH.

$(11, 40, 99, 101; 245)$.

$$C \equiv (11, 40, 99, 101) \cdot (10, 201, 89, 8) \equiv 1745.$$

1745 is NOT 245.
But $1745 + 500 \equiv 242$ IS close to 245. (It needs to be within 4 and it is) So A probably sent 1.

HW09, Problem 4

A & B do PRIV-LWE with $\vec{k} = (11, 100, 39, 4)$, $p = 1009$, $\gamma = 2$.
All math is mod 1009.

HW09, Problem 4

A & B do PRIV-LWE with $\vec{k} = (11, 100, 39, 4)$, $p = 1009$, $\gamma = 2$.
All math is mod 1009.
E sees A send $(7, 13, 22, 100; 618)$.

HW09, Problem 4

A & B do PRIV-LWE with $\vec{k} = (11, 100, 39, 4)$, $p = 1009$, $\gamma = 2$.
All math is mod 1009.
E sees A send $(7, 13, 22, 100; 618)$.
She later finds out that this decoded to 0.

HW09, Problem 4

A & B do PRIV-LWE with $\vec{k} = (11, 100, 39, 4)$, $p = 1009$, $\gamma = 2$.
All math is mod 1009.
E sees A send $(7, 13, 22, 100; 618)$.
She later finds out that this decoded to 0.
Write down what she knows about k_1, k_2, k_3, k_4.

SOLUTION

A knows

$$7k_1 + 13k_2 + 22k_3 + 100k_4 \in \{618-2, 618-1, 618, 618+1, 618+2\}$$

HW09, Problem 4

A & B do PRIV-LWE with $\vec{k} = (11, 100, 39, 4)$, $p = 1009$, $\gamma = 2$.
All math is mod 1009.
E sees A send $(7, 13, 22, 100; 618)$.
She later finds out that this decoded to 0.
Write down what she knows about k_1, k_2, k_3, k_4.
SOLUTION
A knows

$7k_1+13k_2+22k_3+100k_4 \in \{618-2, 618-1, 618, 618+1, 618+2\}$

so

$$7k_1 + 13k_2 + 22k_3 + 100k_4 \in \{616, 617, 618, 619, 620\}$$