Solutions to HW10 Problems

BILL, RECORD LECTURE!!!!

BILL RECORD LECTURE!!!

HW10, Problem 2

PRG: $G(b_1 \cdots b_n) = b_1 \cdots b_n(\sum_{i=1}^{n} b_i \pmod 4$ written in binary$)$.

HW10, Problem 2

PRG: $G(b_1 \cdots b_n) = b_1 \cdots b_n(\sum_{i=1}^{n} b_i \pmod 4$ written in binary).

Give poly strategy for E for PRG-Game that wins $> \frac{1}{2}$ the time.

HW10, Problem 2

PRG: $G(b_1 \cdots b_n) = b_1 \cdots b_n(\sum_{i=1}^{n} b_i \pmod 4$ written in binary).

Give poly strategy for E for PRG-Game that wins $> \frac{1}{2}$ the time.
Note when E is SURE that she wins and when she is NOT sure.

HW10, Problem 2

PRG: $G(b_1 \cdots b_n) = b_1 \cdots b_n(\sum_{i=1}^{n} b_i \pmod 4$ written in binary).

Give poly strategy for E for PRG-Game that wins $> \frac{1}{2}$ the time.
Note when E is SURE that she wins and when she is NOT sure.
Prove that E wins OVER half the time.

HW10, Problem 2 SOLUTION

HW10, Problem 2 SOLUTION

1. E sees $b_1 \cdots b_n b_{n+1} b_{n+2}$ and $c_1 \cdots c_n c_{n+1} c_{n+2}$.

HW10, Problem 2 SOLUTION

1. E sees $b_1 \cdots b_n b_{n+1} b_{n+2}$ and $c_1 \cdots c_n c_{n+1} c_{n+2}$.
2. E computes $b_1 + \cdots + b_n \pmod 4$, in binary $b'_{n+1} b'_{n+2}$.

HW10, Problem 2 SOLUTION

1. E sees $b_1 \cdots b_n b_{n+1} b_{n+2}$ and $c_1 \cdots c_n c_{n+1} c_{n+2}$.
2. E computes $b_1 + \cdots + b_n \pmod 4$, in binary $b'_{n+1} b'_{n+2}$.
3. E computes $c_1 + \cdots + c_n \pmod 4$, in binary $c'_{n+1} c'_{n+2}$.

HW10, Problem 2 SOLUTION

1. E sees $b_1 \cdots b_n b_{n+1} b_{n+2}$ and $c_1 \cdots c_n c_{n+1} c_{n+2}$.
2. E computes $b_1 + \cdots + b_n \pmod 4$, in binary $b'_{n+1} b'_{n+2}$.
3. E computes $c_1 + \cdots + c_n \pmod 4$, in binary $c'_{n+1} c'_{n+2}$.
4. $b_{n+1} b_{n+2} \neq b'_{n+1} b'_{n+2}$: E outputs $\vec{b}$. KNOWS won.

HW10, Problem 2 SOLUTION

1. E sees $b_1 \cdots b_n b_{n+1} b_{n+2}$ and $c_1 \cdots c_n c_{n+1} c_{n+2}$.
2. E computes $b_1 + \cdots + b_n \pmod 4$, in binary $b'_{n+1} b'_{n+2}$.
3. E computes $c_1 + \cdots + c_n \pmod 4$, in binary $c'_{n+1} c'_{n+2}$.
4. $b_{n+1} b_{n+2} \ne b'_{n+1} b'_{n+2}$: E outputs $\vec{b}$. KNOWS won.
5. $c_{n+1} c_{n+2} \ne c'_{n+1} c'_{n+2}$: E outputs $\vec{c}$. KNOWS won.

HW10, Problem 2 SOLUTION

1. E sees $b_1 \cdots b_n b_{n+1} b_{n+2}$ and $c_1 \cdots c_n c_{n+1} c_{n+2}$.
2. E computes $b_1 + \cdots + b_n \pmod 4$, in binary $b'_{n+1} b'_{n+2}$.
3. E computes $c_1 + \cdots + c_n \pmod 4$, in binary $c'_{n+1} c'_{n+2}$.
4. $b_{n+1} b_{n+2} \neq b'_{n+1} b'_{n+2}$: E outputs $\vec{b}$. KNOWS won.
5. $c_{n+1} c_{n+2} \neq c'_{n+1} c'_{n+2}$: E outputs $\vec{c}$. KNOWS won.
6. If neither occurs then then E clueless! Outputs $\vec{b}$ and hopes.

HW10, Problem 2 SOLUTION

1. E sees $b_1 \cdots b_n b_{n+1} b_{n+2}$ and $c_1 \cdots c_n c_{n+1} c_{n+2}$.
2. E computes $b_1 + \cdots + b_n \pmod 4$, in binary $b'_{n+1} b'_{n+2}$.
3. E computes $c_1 + \cdots + c_n \pmod 4$, in binary $c'_{n+1} c'_{n+2}$.
4. $b_{n+1} b_{n+2} \neq b'_{n+1} b'_{n+2}$: E outputs $\vec{b}$. KNOWS won.
5. $c_{n+1} c_{n+2} \neq c'_{n+1} c'_{n+2}$: E outputs $\vec{c}$. KNOWS won.
6. If neither occurs then then E clueless! Outputs $\vec{b}$ and hopes.

Pr E LOSES is $\le$ pr rand string A picked, $r_1 \cdots r_{n+2}$ has $\sum_{i=1}^{n} r_i \mod 4 = r_{n+1} r_{n+2}$.

HW10, Problem 2 SOLUTION

1. E sees $b_1 \cdots b_n b_{n+1} b_{n+2}$ and $c_1 \cdots c_n c_{n+1} c_{n+2}$.
2. E computes $b_1 + \cdots + b_n \pmod 4$, in binary $b'_{n+1} b'_{n+2}$.
3. E computes $c_1 + \cdots + c_n \pmod 4$, in binary $c'_{n+1} c'_{n+2}$.
4. $b_{n+1} b_{n+2} \ne b'_{n+1} b'_{n+2}$: E outputs $\vec{b}$. KNOWS won.
5. $c_{n+1} c_{n+2} \ne c'_{n+1} c'_{n+2}$: E outputs $\vec{c}$. KNOWS won.
6. If neither occurs then then E clueless! Outputs $\vec{b}$ and hopes.

Pr E LOSES is $\le$ pr rand string A picked, $r_1 \cdots r_{n+2}$ has $\sum_{i=1}^{n} r_i \mod 4 = r_{n+1} r_{n+2}$.
Number of strings A can pick is 2^{n+2}.

HW10, Problem 2 SOLUTION

1. E sees $b_1 \cdots b_n b_{n+1} b_{n+2}$ and $c_1 \cdots c_n c_{n+1} c_{n+2}$.
2. E computes $b_1 + \cdots + b_n \pmod 4$, in binary $b'_{n+1} b'_{n+2}$.
3. E computes $c_1 + \cdots + c_n \pmod 4$, in binary $c'_{n+1} c'_{n+2}$.
4. $b_{n+1} b_{n+2} \ne b'_{n+1} b'_{n+2}$: E outputs $\vec{b}$. KNOWS won.
5. $c_{n+1} c_{n+2} \ne c'_{n+1} c'_{n+2}$: E outputs $\vec{c}$. KNOWS won.
6. If neither occurs then then E clueless! Outputs $\vec{b}$ and hopes.

Pr E LOSES is $\le$ pr rand string A picked, $r_1 \cdots r_{n+2}$ has $\sum_{i=1}^{n} r_i \mod 4 = r_{n+1} r_{n+2}$.
Number of strings A can pick is 2^{n+2}.
Number of strings A can pick with that property is 2^n since last two bits determined by 1st n bits.

HW10, Problem 2 SOLUTION

1. E sees $b_1 \cdots b_n b_{n+1} b_{n+2}$ and $c_1 \cdots c_n c_{n+1} c_{n+2}$.
2. E computes $b_1 + \cdots + b_n \pmod 4$, in binary $b'_{n+1} b'_{n+2}$.
3. E computes $c_1 + \cdots + c_n \pmod 4$, in binary $c'_{n+1} c'_{n+2}$.
4. $b_{n+1} b_{n+2} \ne b'_{n+1} b'_{n+2}$: E outputs $\vec{b}$. KNOWS won.
5. $c_{n+1} c_{n+2} \ne c'_{n+1} c'_{n+2}$: E outputs $\vec{c}$. KNOWS won.
6. If neither occurs then then E clueless! Outputs $\vec{b}$ and hopes.

Pr E LOSES is $\le$ pr rand string A picked, $r_1 \cdots r_{n+2}$ has
$\sum_{i=1}^{n} r_i \mod 4 = r_{n+1} r_{n+2}$.
Number of strings A can pick is 2^{n+2}.
Number of strings A can pick with that property is 2^n since last two bits determined by 1st n bits.
Prob E loses is $\le \frac{2^n}{2^{n+2}} = \frac{1}{4}$.

HW10, Problem 2 SOLUTION

1. E sees $b_1 \cdots b_n b_{n+1} b_{n+2}$ and $c_1 \cdots c_n c_{n+1} c_{n+2}$.
2. E computes $b_1 + \cdots + b_n \pmod 4$, in binary $b'_{n+1} b'_{n+2}$.
3. E computes $c_1 + \cdots + c_n \pmod 4$, in binary $c'_{n+1} c'_{n+2}$.
4. $b_{n+1} b_{n+2} \ne b'_{n+1} b'_{n+2}$: E outputs $\vec{b}$. KNOWS won.
5. $c_{n+1} c_{n+2} \ne c'_{n+1} c'_{n+2}$: E outputs $\vec{c}$. KNOWS won.
6. If neither occurs then then E clueless! Outputs $\vec{b}$ and hopes.

Pr E LOSES is $\le$ pr rand string A picked, $r_1 \cdots r_{n+2}$ has $\sum_{i=1}^{n} r_i \mod 4 = r_{n+1} r_{n+2}$.
Number of strings A can pick is 2^{n+2}.
Number of strings A can pick with that property is 2^n since last two bits determined by 1st n bits.
Prob E loses is $\le \frac{2^n}{2^{n+2}} = \frac{1}{4}$.
Prob E wins is $\ge \frac{3}{4}$.

HW10, Problem 3

Not going over it- but tell me how it turned out.

HW10, Problem 4a

A & B do Public Key LWE. $p = 37$, $m = 4$, $\gamma = 4$.

HW10, Problem 4a

A & B do Public Key LWE. $p = 37$, $m = 4$, $\gamma = 4$.
A's private key: $(1, 3, 5, 8, 22)$.

HW10, Problem 4a

A & B do Public Key LWE. $p = 37$, $m = 4$, $\gamma = 4$.
A's private key: $(1, 3, 5, 8, 22)$.
Noisy equations Al makes public are:

$$2k_1 + 4k_2 + 6k_3 + 8k_4 + 18k_5 \sim 24 \pmod{37}$$

$$3k_1 + 6k_2 + 9k_3 + 15k_4 + 20k_5 \sim 0 \pmod{37}$$

$$4k_1 + 5k_2 + 6k_3 + 7k_4 + 9k_5 \sim 7 \pmod{37}$$

$$10k_1 + 9k_2 + 8k_3 + 7k_4 + 6k_5 \sim 7 \pmod{37}$$

HW10, Problem 4a

A & B do Public Key LWE. $p = 37$, $m = 4$, $\gamma = 4$.
A's private key: $(1, 3, 5, 8, 22)$.
Noisy equations Al makes public are:

$$2k_1 + 4k_2 + 6k_3 + 8k_4 + 18k_5 \sim 24 \pmod{37}$$

$$3k_1 + 6k_2 + 9k_3 + 15k_4 + 20k_5 \sim 0 \pmod{37}$$

$$4k_1 + 5k_2 + 6k_3 + 7k_4 + 9k_5 \sim 7 \pmod{37}$$

$$10k_1 + 9k_2 + 8k_3 + 7k_4 + 6k_5 \sim 7 \pmod{37}$$

B wants to send $b = 0$. Chooses 1st & 3rd eq.

HW10, Problem 4a

A & B do Public Key LWE. $p = 37$, $m = 4$, $\gamma = 4$.
A's private key: $(1, 3, 5, 8, 22)$.
Noisy equations Al makes public are:

$$2k_1 + 4k_2 + 6k_3 + 8k_4 + 18k_5 \sim 24 \pmod{37}$$

$$3k_1 + 6k_2 + 9k_3 + 15k_4 + 20k_5 \sim 0 \pmod{37}$$

$$4k_1 + 5k_2 + 6k_3 + 7k_4 + 9k_5 \sim 7 \pmod{37}$$

$$10k_1 + 9k_2 + 8k_3 + 7k_4 + 6k_5 \sim 7 \pmod{37}$$

B wants to send $b = 0$. Chooses 1st & 3rd eq.

What does he send?

HW10, Problem 4a, SOLUTION

B adds 1st and 3rd eq and adds $\frac{bp}{2} = 0$ to the RHS :

$$2k_1 + 4k_2 + 6k_3 + 8k_4 + 18k_5 \sim 24 \pmod{37}$$

$$4k_1 + 5k_2 + 6k_3 + 7k_4 + 9k_5 \sim 7 \pmod{37}$$

HW10, Problem 4a, SOLUTION

B adds 1st and 3rd eq and adds $\frac{bp}{2} = 0$ to the RHS :

$$2k_1 + 4k_2 + 6k_3 + 8k_4 + 18k_5 \sim 24 \pmod{37}$$

$$4k_1 + 5k_2 + 6k_3 + 7k_4 + 9k_5 \sim 7 \pmod{37}$$

$$6k_1 + 9k_2 + 12k_3 + 15k_4 + 27k_5 \sim 31 + 0 = 31 \pmod{37}$$

HW10, Problem 4a, SOLUTION

B adds 1st and 3rd eq and adds $\frac{bp}{2} = 0$ to the RHS :

$$2k_1 + 4k_2 + 6k_3 + 8k_4 + 18k_5 \sim 24 \pmod{37}$$

$$4k_1 + 5k_2 + 6k_3 + 7k_4 + 9k_5 \sim 7 \pmod{37}$$

$$6k_1 + 9k_2 + 12k_3 + 15k_4 + 27k_5 \sim 31 + 0 = 31 \pmod{37}$$

B sends $(6, 9, 12, 15, 27; 31)$

HW10, Problem 4b

B wants to send $b = 1$. Uses 1st and 4th eqs. What does B send?

HW10, Problem 4b

B wants to send $b = 1$. Uses 1st and 4th eqs. What does B send?

SOLUTION

B adds 1st and 4th eqs and adds $\frac{bp}{2} = \frac{37}{2} = 18$ to RHS.

$$2k_1 + 4k_2 + 6k_3 + 8k_4 + 18k_5 \sim 24 \pmod{37}$$

$$10k_1 + 9k_2 + 8k_3 + 7k_4 + 6k_5 \sim 7 \pmod{37}$$

HW10, Problem 4b

B wants to send $b = 1$. Uses 1st and 4th eqs. What does B send?

SOLUTION

B adds 1st and 4th eqs and adds $\frac{bp}{2} = \frac{37}{2} = 18$ to RHS.

$$2k_1 + 4k_2 + 6k_3 + 8k_4 + 18k_5 \sim 24 \pmod{37}$$

$$10k_1 + 9k_2 + 8k_3 + 7k_4 + 6k_5 \sim 7 \pmod{37}$$

$$12k_1 + 13k_3 + 14k_3 + 15k_4 + 24k_5 \sim 31 + 18 = 12 \pmod{37}$$

HW10, Problem 4b

B wants to send $b = 1$. Uses 1st and 4th eqs. What does B send?

SOLUTION

B adds 1st and 4th eqs and adds $\frac{bp}{2} = \frac{37}{2} = 18$ to RHS.

$$2k_1 + 4k_2 + 6k_3 + 8k_4 + 18k_5 \sim 24 \pmod{37}$$

$$10k_1 + 9k_2 + 8k_3 + 7k_4 + 6k_5 \sim 7 \pmod{37}$$

$$12k_1 + 13k_3 + 14k_3 + 15k_4 + 24k_5 \sim 31 + 18 = 12 \pmod{37}$$

B sends $(12, 13, 14, 15, 24; 12)$

HW10, Problem 4c

A receives $17k_1 + 11k_2 + 15k_3 + 21k_4 + 29k_5 \sim 25 \pmod{37}$. What bit did B send?

HW10, Problem 4c

A receives $17k_1 + 11k_2 + 15k_3 + 21k_4 + 29k_5 \sim 25 \pmod{37}$.
What bit did B send?

SOLUTION

A plugs in her private key $(1, 3, 5, 8, 22)$ and sees if what she gets is close to 25 or around 18 away from 25.

$$17 \times 1 + 11 \times 3 + 15 \times 5 + 21 \times 8 + 29 \times 22 \equiv 6$$

6 around 18 away from from 25, so the bit is 1.

HW10, Problem 4d

This turns out to be a terrible set of equation for secrecy. This is NOT because the the p, n, m are too small. There is ANOTHER reason. Speculate on what that is.

HW10, Problem 4d

This turns out to be a terrible set of equation for secrecy. This is NOT because the the p, n, m are too small. There is ANOTHER reason. Speculate on what that is.

Discuss

HW10, Problem 5

A, B, E playing cards scenario.
A and B want to establish a secret key of n bits.
What is m such that if start with (m, m, m) then can get n bits?

HW10, Problem 5

A, B, E playing cards scenario.
A and B want to establish a secret key of n bits.
What is m such that if start with (m, m, m) then can get n bits?

You wrote program for this.

HW10, Problem 5

A, B, E playing cards scenario.
A and B want to establish a secret key of n bits.
What is m such that if start with (m, m, m) then can get n bits?

You wrote program for this.

Discuss what you found.