피노키오 프로토콜

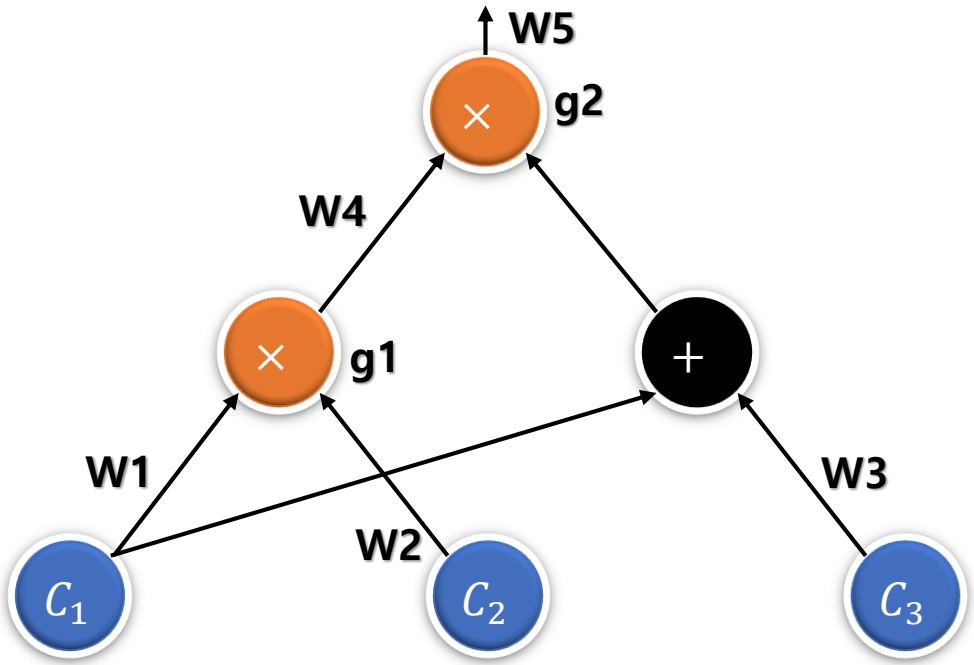
https://youtu.be/dS3nv_exLIA

정의

- 증명자
  → Alice
- 검증자
  → Bob
- 명제
  → $(C_1 \cdot C_2) \cdot (C_1 + C_3) = 7$을 만족하는 $C_1,\ C_2,\ C_3$를 알고 있다.

산술회로(Arithmetic Circuits)

- $(C_1 \cdot C_2) \cdot (C_1 + C_3) = 7$



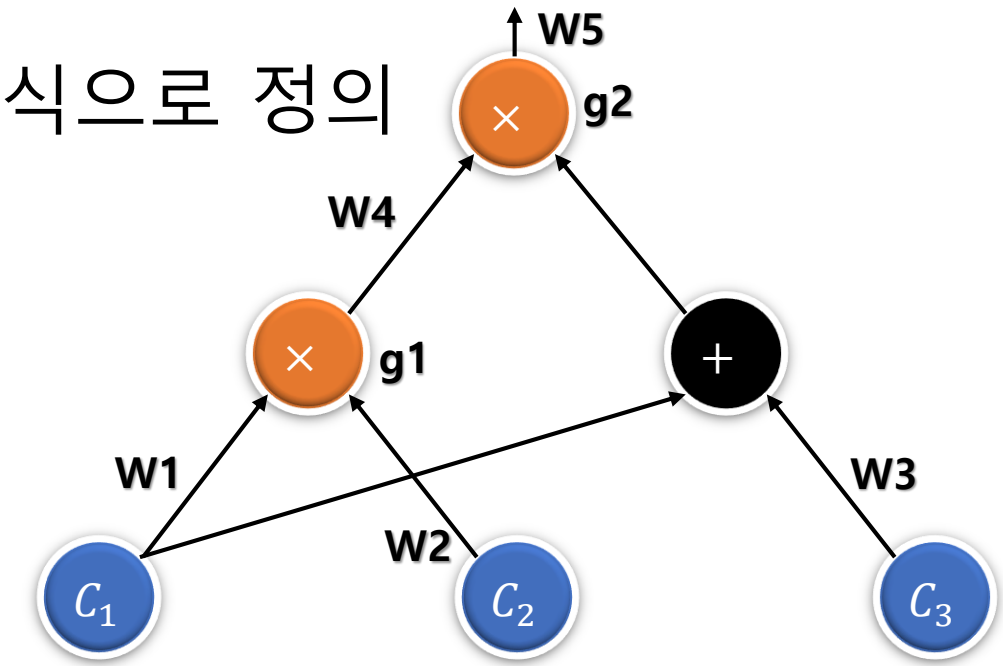
- 하나 이상의 게이트로 들어가는 선의 경우 하나로 정의한다.
- 곱셈 게이트의 두 입력을 Left, Right로 정의한다.
- 덧셈 게이트에서 곱셈 게이트로 가는 출력은 덧셈 게이트의 입력으로 대신한다.

W1, W2, W3, W4, W5 ➔ Legal Assignment

다항식 집합(QAP; Quadratic Arithmetic Program)

1. Target Point 설정
2. 곱셈 게이트와 Target Point 매핑
3. 두 입력, 출력에 해당하는 선을 다항식으로 정의

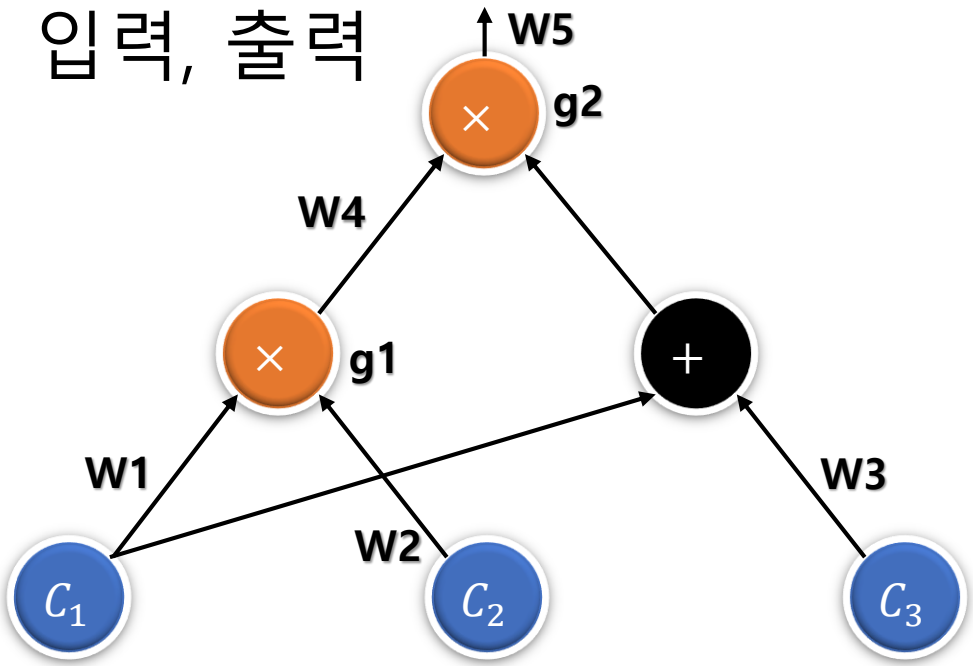
1. {1, 2}
2. {g1, g2} → {1, 2,}
3. L1~L5, R1~R5, O1~O5



다항식 집합(QAP; Quadratic Arithmetic Program)

1. 대응되는 Target Point를 대입할 시 1, 다른 Target Point를 대입할 시 0이 되는 다항식을 만듭니다.
2. 이 다항식을 대응되는 Target Point의 입력, 출력에 할당합니다.

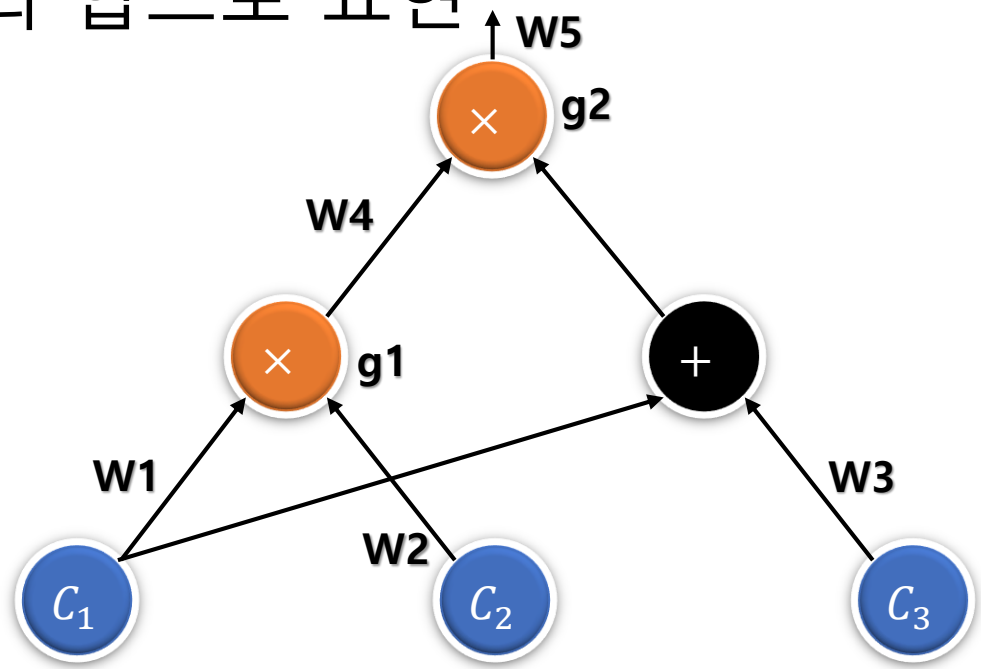
1. {g1, g2} → {1, 2} → {2-X, X-1}
2. {g1; L1, R2, O4 = 2-X}
   {g2; L4, (R1, R3), O5 = X-1}



다항식 집합(QAP; Quadratic Arithmetic Program)

1. 할당되지 않은 식의 경우 0으로 할당
2. L, R, O 를 Legal Assignmet 와의 곱의 합으로 표현

1. $\mathrm{L2}, \mathrm{L3}, \mathrm{L5}, \ldots, 0$
2. $L \coloneqq \sum_1^5 C_i \cdot L_i,$
   $R \coloneqq \sum_1^5 C_i \cdot R_i,$
   $O \coloneqq \sum_1^5 C_i \cdot O_i$



최종 다항식

$$L \coloneqq \sum_1^5 C_i \cdot L_i,$$
$$R \coloneqq \sum_1^5 C_i \cdot R_i,$$
$$O \coloneqq \sum_1^5 C_i \cdot O_i$$

{g1; L1, R2, O4 = 2-X}
{g2; L4, (R1, R3), O5 = X-1}

- $P \coloneqq L \cdot R - O$
  - 의미
    0을 만드는 다항식
  - 특징
    모든 Target Point에서 0이 된다 ⇔ 모든 Ci가 Legal Assignment 이다.

타겟 다항식 T(X)

- P(a) = 0 이 성립하려면, $P = (X - a) \cdot H$
- T가 P의 약수라면,
  $T(X) \coloneqq (X - 1) \cdot (X - 2)$
- Alice는 QAP를 만족하는 Assignment를 알고 있음을 증명할 수단이 생김

QAP 검증

- $P(s) = H(s) \cdot T(s)$

- 잘못된 Assignments를 사용하는 경우
  잘못된 L, R, O, P ⇔ T는 P의 약수가 아님

- Schwartz-Zippel Lemma

피노키오 프로토콜

1. Alice chooses polynomials L,R,O,H

2. Bob chooses a random point $s \in Fp$, and computes E(T(s))

3. Alice sends Bob the hidings of all these polynomials evaluated at s, i.e. E(L(s)),E(R(s)),E(O(s)),E(H(s))

4. Bob checks if the desired equation holds at ss. That is, he checks whether $E(L(s) \cdot R(s) - O(s)) = E(T(s) \cdot H(s))$

다항식 검증

- $F = L + X^{d+1} \cdot R + X^{d+2} \cdot O$
- L, R, O의 계수들을 분리
- 선형결합
  $F := \sum_1^5 C_i \cdot F_i$

피노키오 프로토콜 2

1. Bob chooses a random β, and sends to Alice the hidings $E(\beta \cdot F1(s)),\ldots,E(\beta \cdot Fm(s))$

2. He then asks Alice to send him the element $E(\beta \cdot F(s))$

Assignment 숨기기

- $L_z \coloneqq L + \delta_1 \cdot \mathrm{T}$
  $R_z \coloneqq R + \delta_2 \cdot \mathrm{T}$
  $O_z \coloneqq O + \delta_3 \cdot \mathrm{T}$

동형암호

- H(S)와 T(S)의 검증