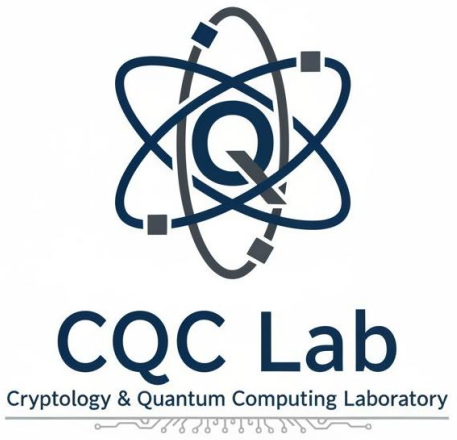
Cryptanalysis in the NISQ era:
Breaking the A5-GMR-2 Cipher using Quantum Annealing

이동재

dongjae.lee@kangwon.ac.kr

2025. 09. 22.

온라인 초청 강연 @한성대학교



NISQ

- Noisy Intermediate-Scale Quantum
  - 양자 컴퓨팅의 현 상태
    - Term coined by John Preskill
  - Quantum processor containing up to 1,000 qubits

NISQ

- Noisy Intermediate-Scale Quantum
  - 양자 컴퓨팅의 현 상태
    - Term coined by John Preskill
  - Quantum processor containing up to 1,000 qubits
  - **No quantum error correction**

- Opposite of Falut-Tolerant Quantum Computing (FTQC)

Limitation of NISQ

- Difficult to scale for general-purpose quantum algorithms
  - Shor's algorithm is not feasible on NISQ devices
- Error correction is not guaranteed to succeed in the future
- Even if error correction becomes practical, the required number of physical qubits per logical qubit could be large

Post-quantum Cryptography

- In cryptography, we typically assume the worst-case scenario
  - Design for FTQC-level threats

Why Study Cryptanalysis in the NISQ Era?

- It's not just curiosity

- Evaluate the realistic, near-term threat posed by quantum computing

- NISQ-compatible algorithms behave quite differently from FTQC algorithms

⇒ This opens up possibilities for discovering new types of attacks or unknown vulnerabilities

Why Study Cryptanalysis in the NISQ Era?

- It's not just curiosity

- Evaluate the realistic, near-term threat posed by quantum computing

- NISQ-compatible algorithms behave quite differently from FTQC algorithms

⇒ This opens up possibilities for discovering new types of attacks or unknown vulnerabilities

Quantum Dongjae Attack

NISQ Algorithm 1

- Quantum approximate optimization algorithm
  - It is an algorithm designed to solve **combinatorial optimization problems**
  - It gained attention by showing the potential to solve NP-hard problems such as Max-Cut

NISQ Algorithm 2

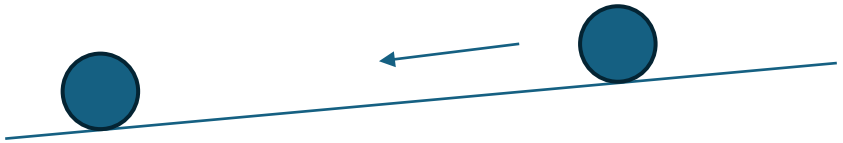
- Quantum Annealing
  - 양자 역학의 원리 중 특히 quantum adiabatic theorem에 따라 조합 최적화 문제의 해를 찾는 방식
    - Quantum Adiabatic Theorem: 어떤 시스템(양자 상태)를 아주 천천히 변화시키면, 가장 안정적인 상태를 벗어나지 않는다는 원리

Quantum Annealing

평평한 바닥 위에 공을 두면 공은 가만히 있는다.

모든 곳의 위치 에너지가 같다.

Quantum Annealing



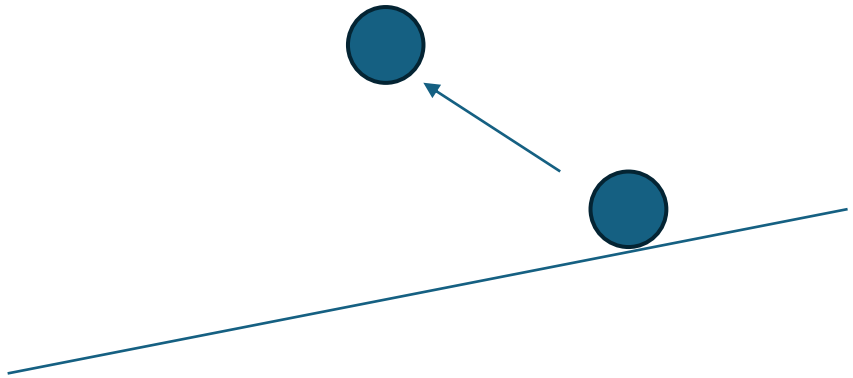
바닥을 서서히 기울이면 공은 경사를 따라 굴러간다.

위치 에너지가 가장 낮은 곳으로 이동한다

Quantum Annealing

그리고 (위치 에너지가) 가장 낮은 지점에서 멈춘다

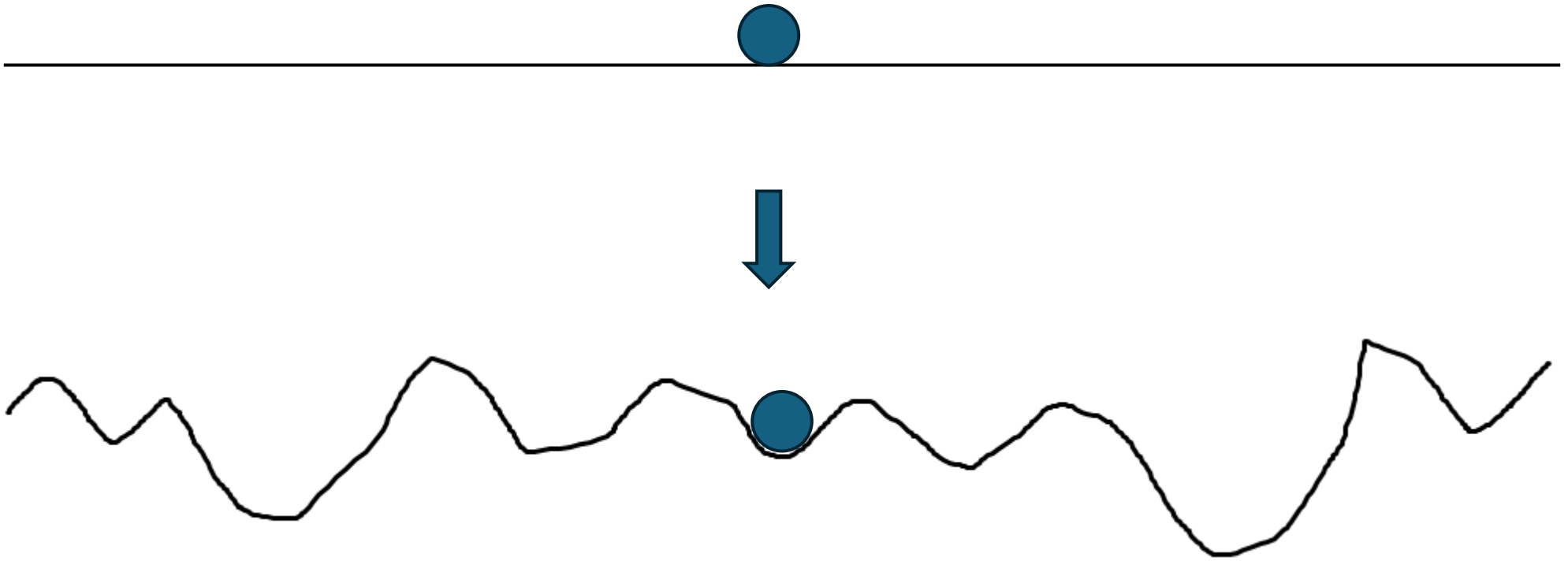
Quantum Annealing



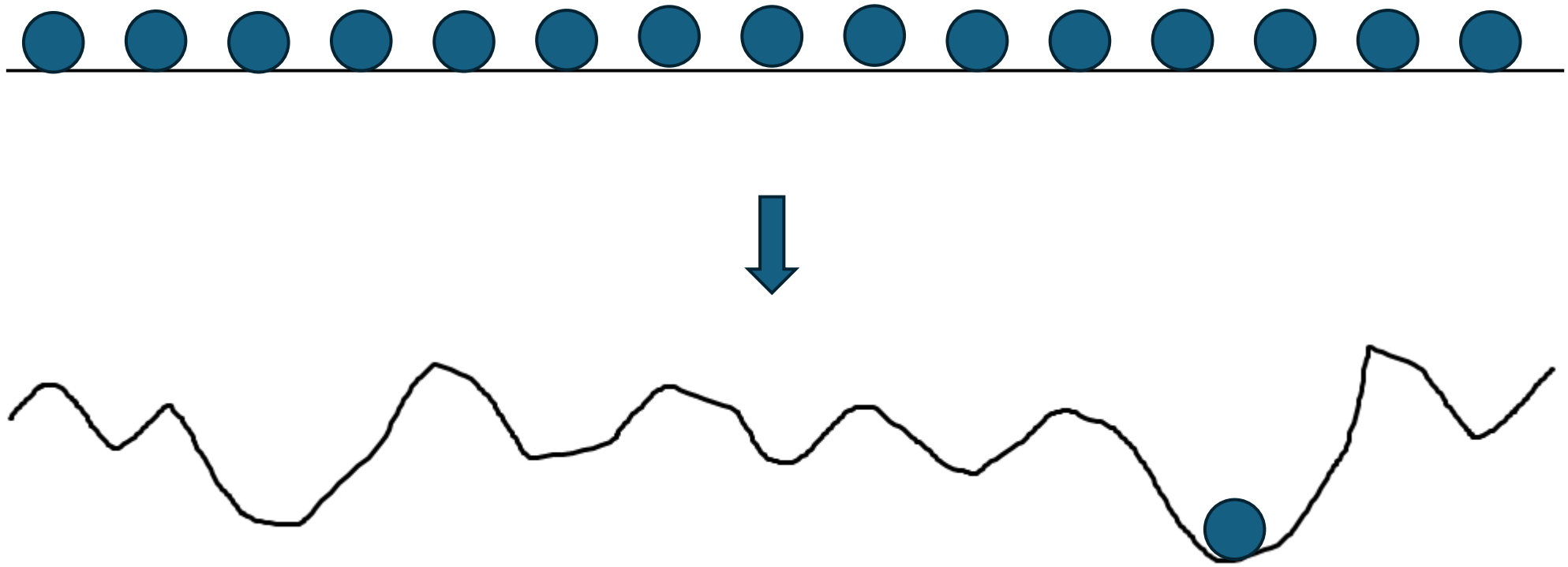
바닥을 갑자기 들어올리면, 공은 튕겨져 나간다.

Quantum Annealing

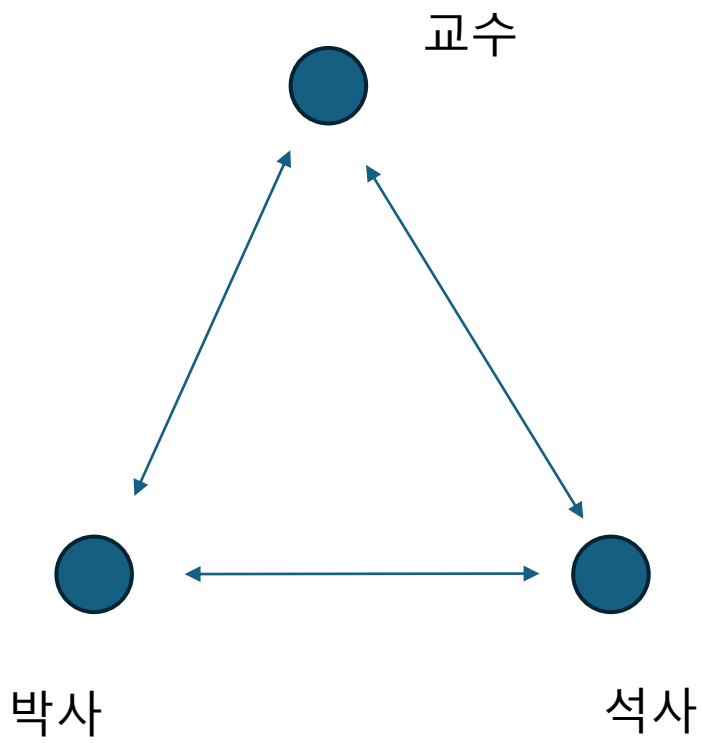
Quantum Annealing



Quantum Annealing



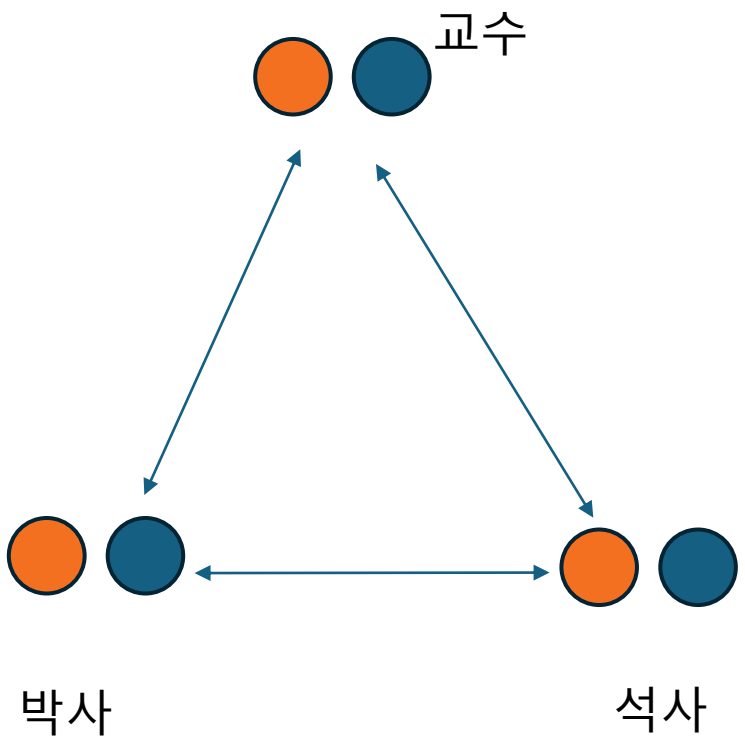
Quantum Annealing



교수 1, 박사 1, 석사 1명으로 구성된 연구팀의 역량이 다음과 같이 결정된다고 하자.

교수의 역량 + 박사의 역량 + 석사의 역량
+ 교수와 박사의 시너지
+ 교수와 석사의 시너지
+ 박사와 석사의 시너지

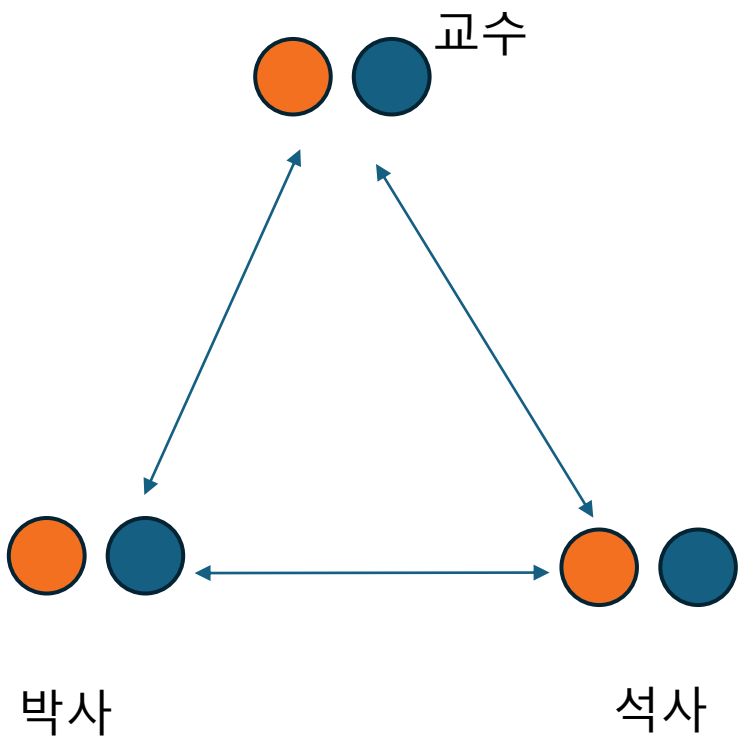
Quantum Annealing



이때, 각 구성원이
예민 모드가 있고 둔감 모드가 있다고 하자.

어떤 상태냐에 따라 개인 역량이 달라지고,
어떤 상태 조합이냐에 따라 시너지가 달라진다.

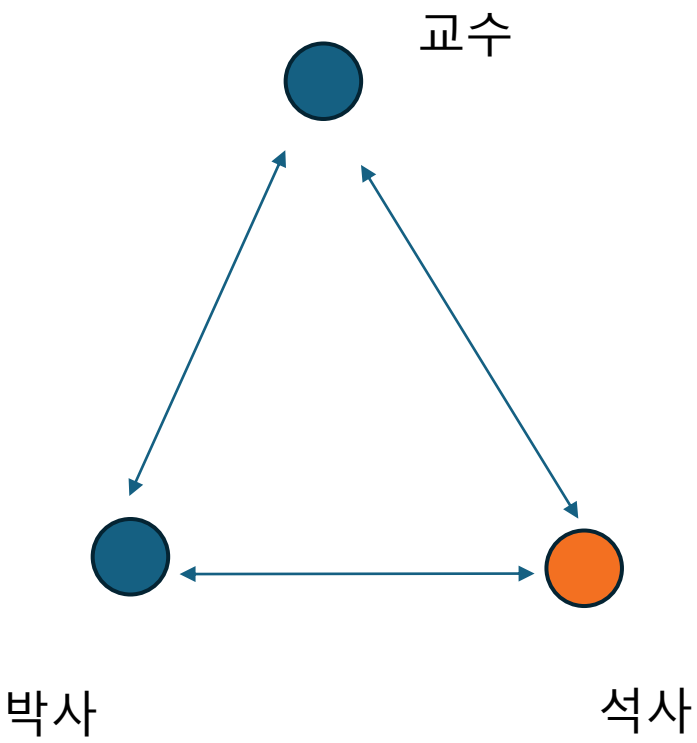
Quantum Annealing



이 연구팀을 방에 가둬 놓고

우수한 연구결과가 나올때 까지 문을 열어주지 않는다면,

Quantum Annealing

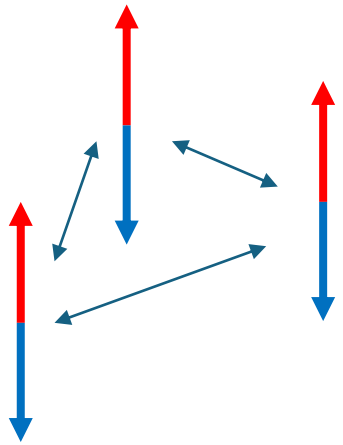


시행착오를 거치면서 최적의 상태 조합에 도달할 것이다.

Quantum Annealing

$$y = -5x_1 + 3x_2 - 8x_3 + 4x_1x_2 + 9x_2x_3$$

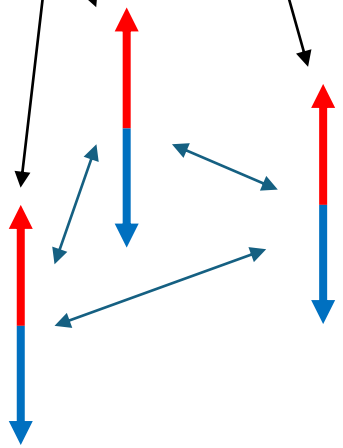
위의 식을 최소화 시키는 binary $x_1, x_2, x_3 \in \{0,1\}$ 은 무엇인가?



Quantum Annealing

$$y = -5x_1 + 3x_2 - 8x_3 + 4x_1x_2 + 9x_2x_3$$

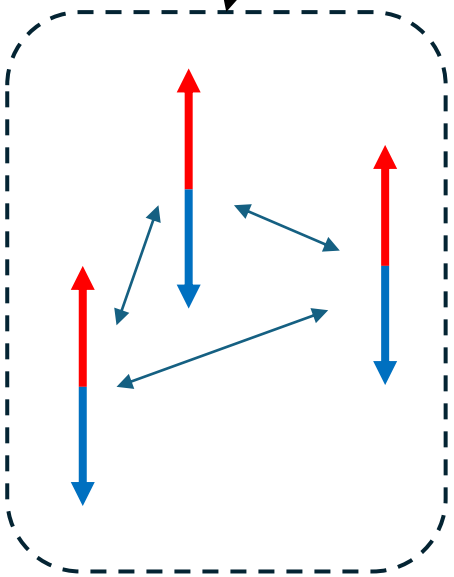
위의 식을 최소화 시키는 binary $x_1, x_2, x_3 \in \{0,1\}$ 은 무엇인가?



Quantum Annealing

$$y = -5x_1 + 3x_2 - 8x_3 + 4x_1x_2 + 9x_2x_3$$

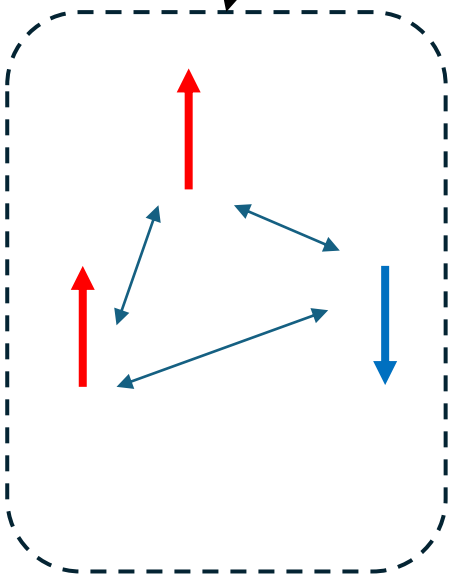
위의 식을 최소화 시키는 binary $x_1, x_2, x_3 \in \{0,1\}$ 은 무엇인가?



Quantum Annealing

$$y = -5x_1 + 3x_2 - 8x_3 + 4x_1x_2 + 9x_2x_3$$

위의 식을 최소화 시키는 binary $x_1, x_2, x_3 \in \{0,1\}$ 은 무엇인가?

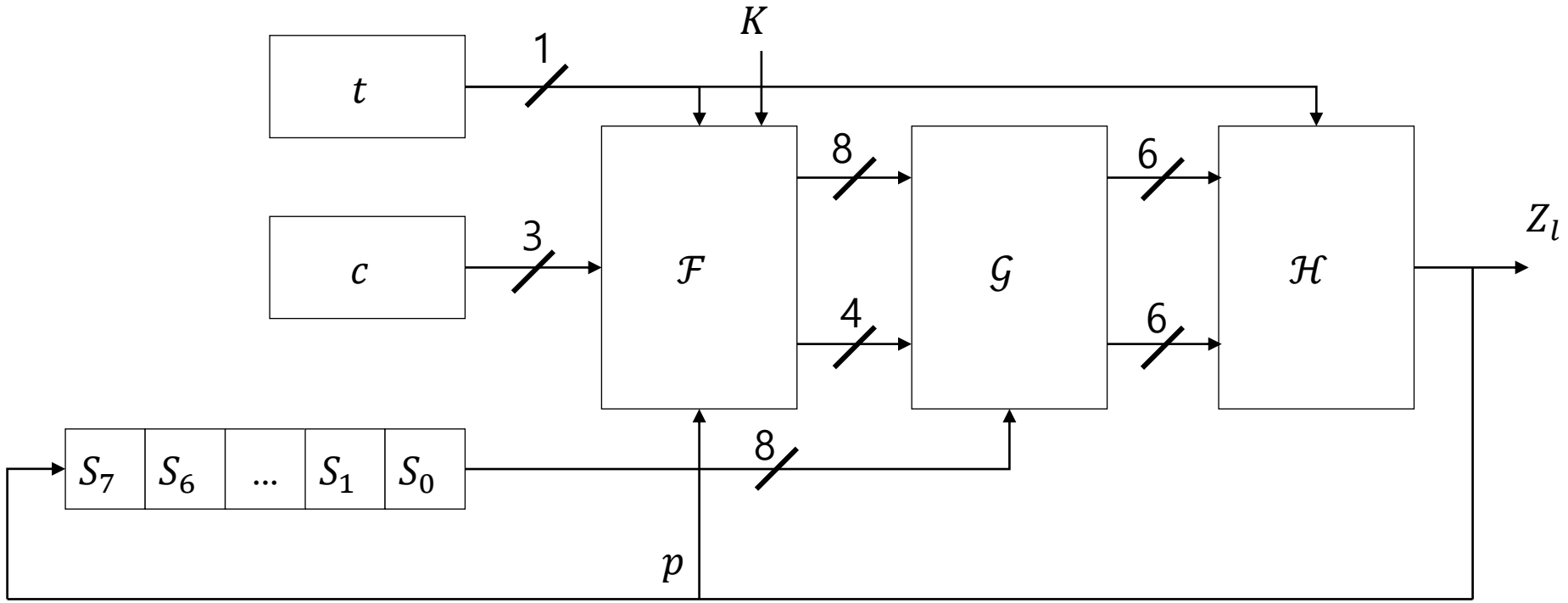


Quantum Annealer

- Quantum Annealing 방식을 활용한 양자 컴퓨터는 D-Wave 사에서 제조한 것이 유일
  - 4400+ 큐비트로 구성된 quantum processor

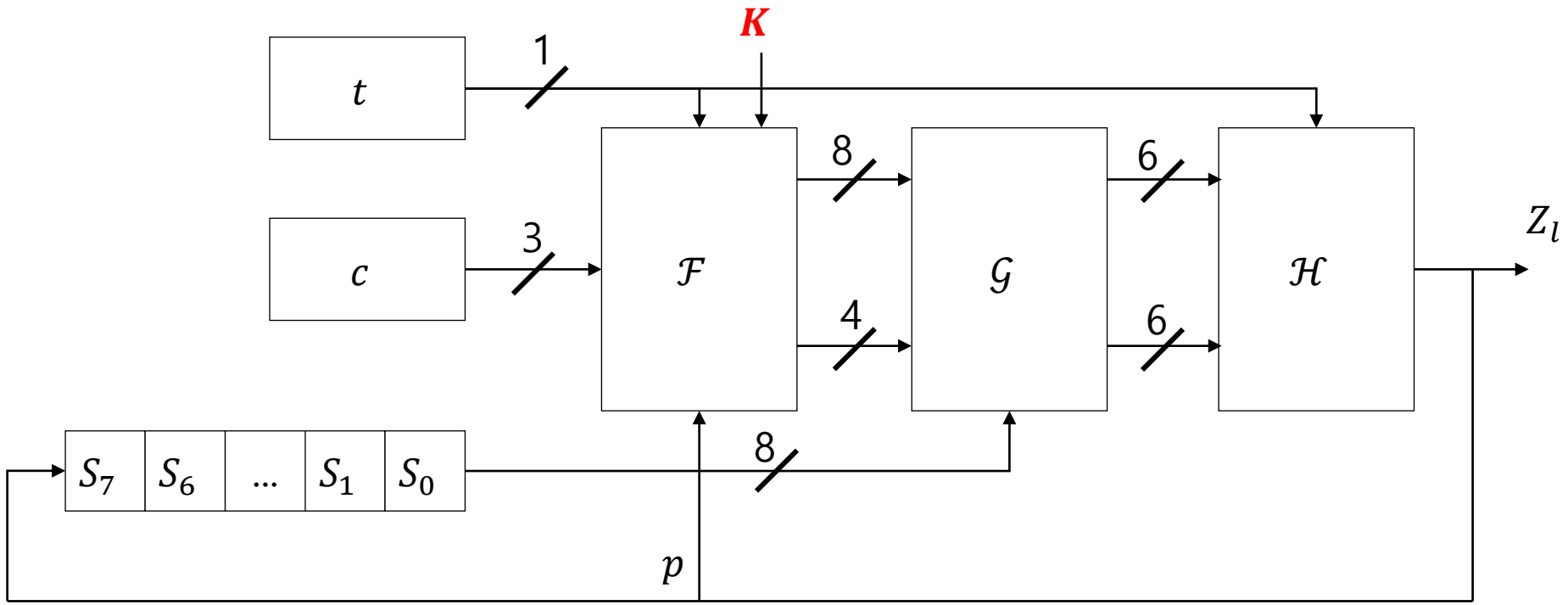
A5-GMR-2

- A stream cipher used for the GMR-2 satellite communication system



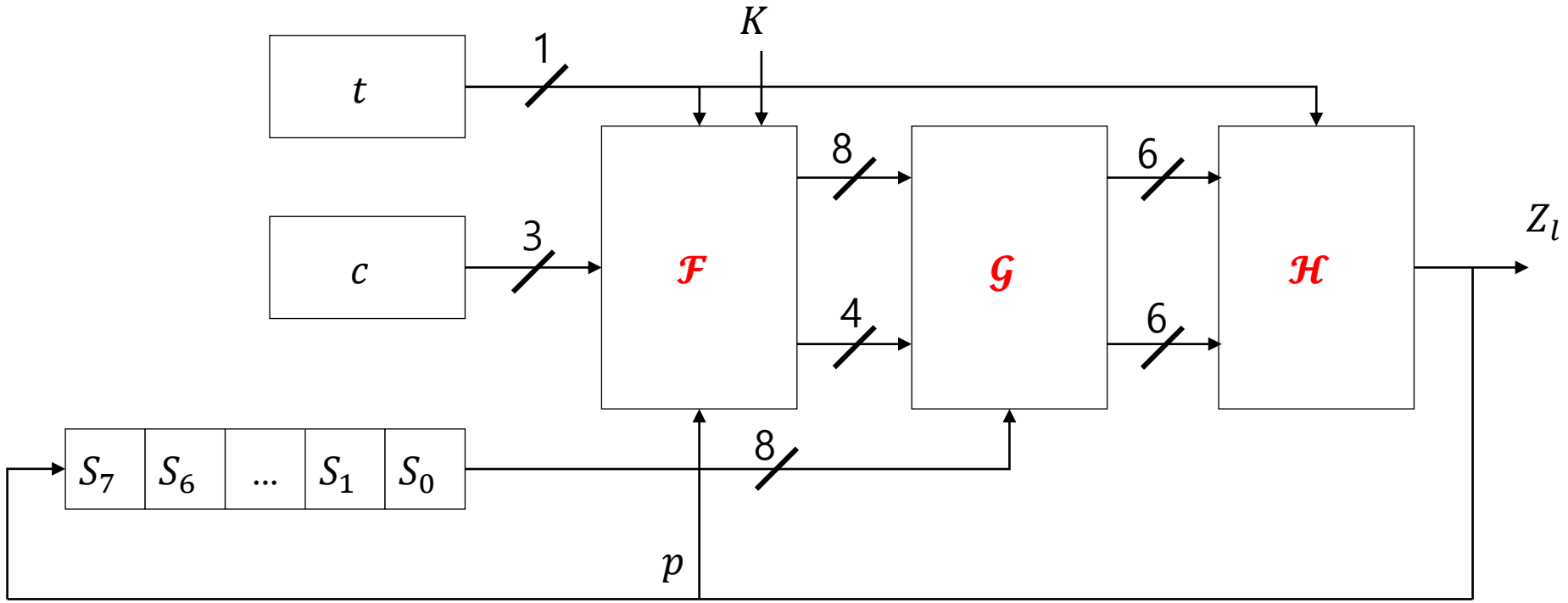
A5-GMR-2

- A stream cipher used for the GMR-2 satellite communication system



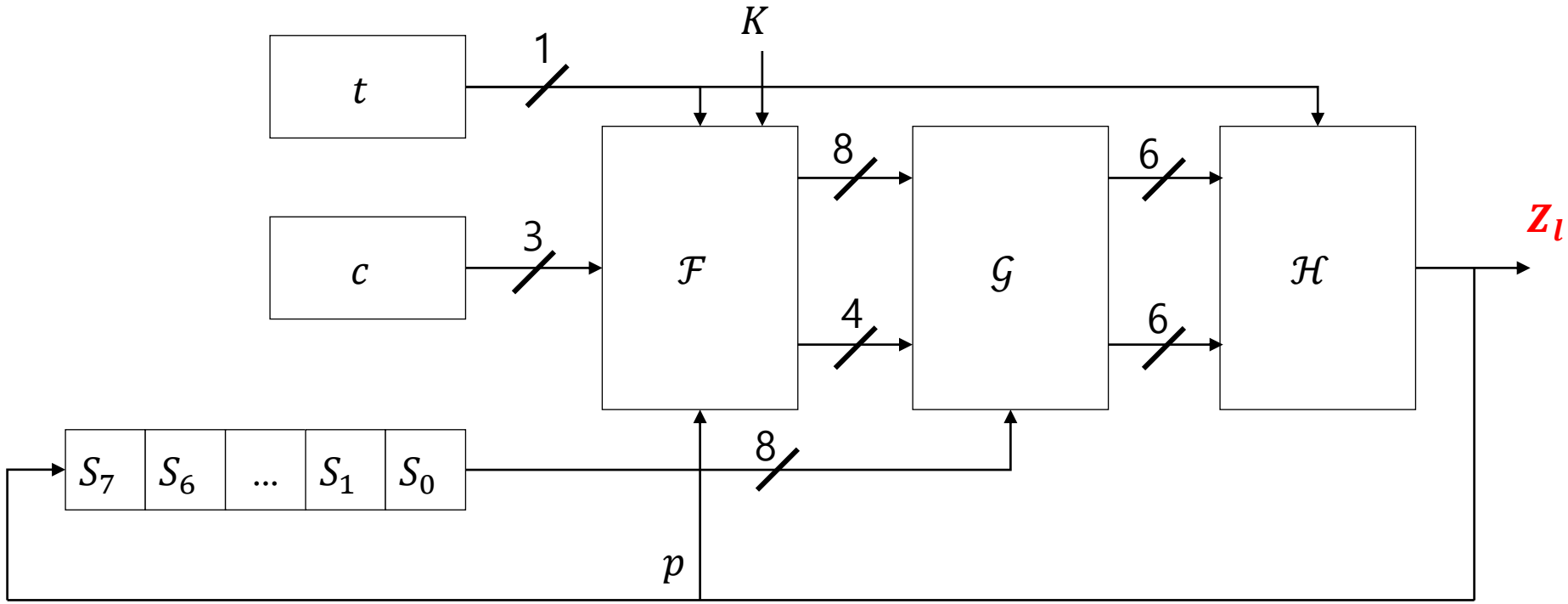
A5-GMR-2

- A stream cipher used for the GMR-2 satellite communication system

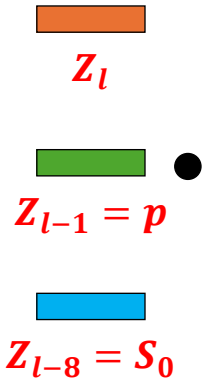


A5-GMR-2

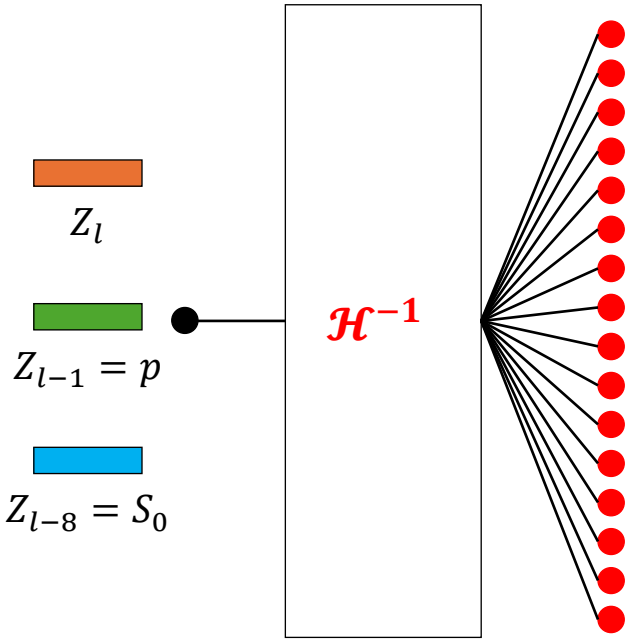
- A stream cipher used for the GMR-2 satellite communication system



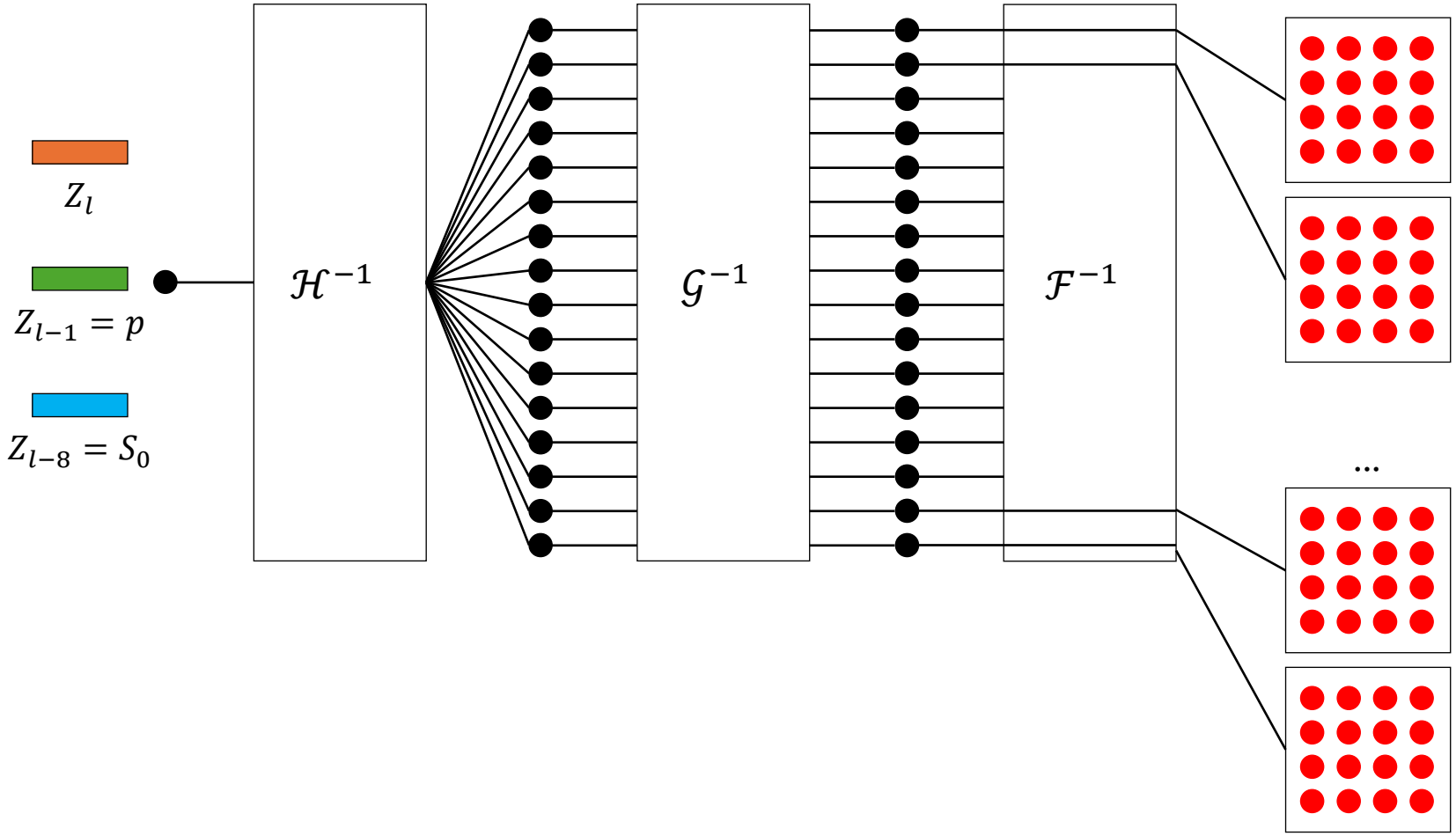
Inversion Attack on A5-GMR-2



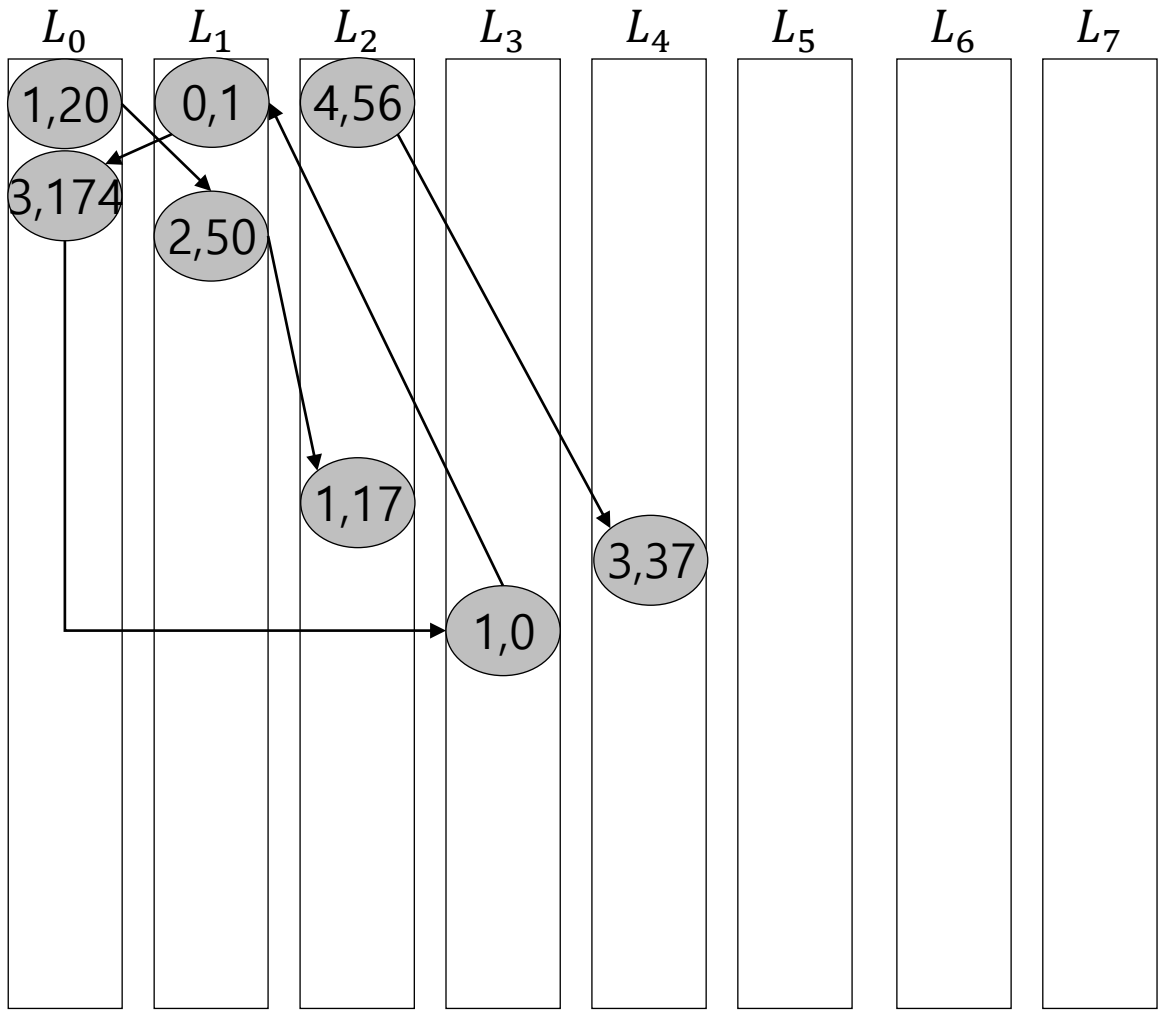
Inversion Attack on A5-GMR-2



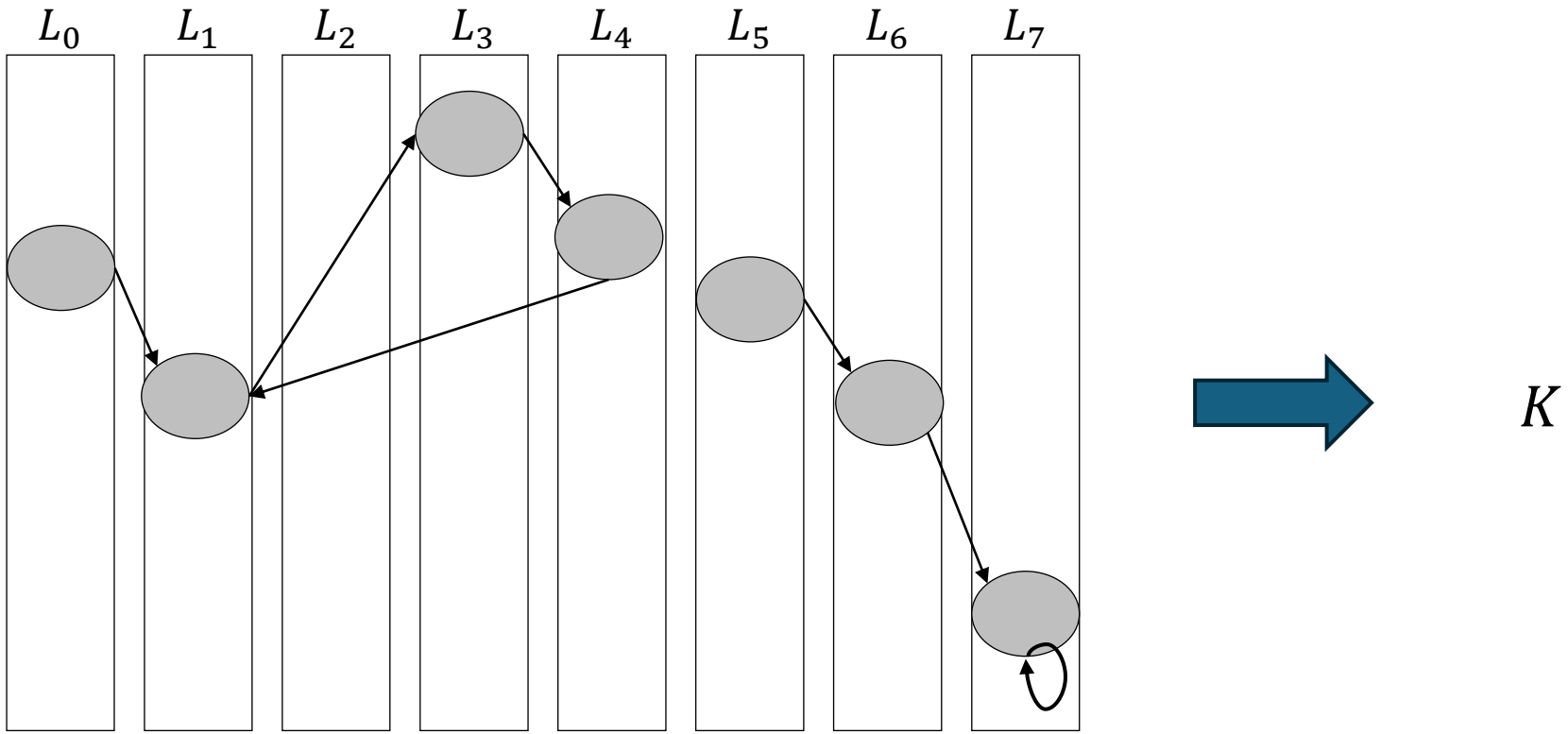
Inversion Attack on A5-GMR-2



Inversion Attack on A5-GMR-2



Inversion Attack on A5-GMR-2



어떤 조건을 만족하는 노드 집합을 찾으면 키 복구로 연결됨

Challenges

Known Keystream Attack on A5-GMR-2 → Reduce the attack to a graph problem → Construct Combinatorial Optimization Problem

→ Implement QA on an available quantum platform → Evaluate the results

→ Search for more applicable ciphers or problems

QUBO

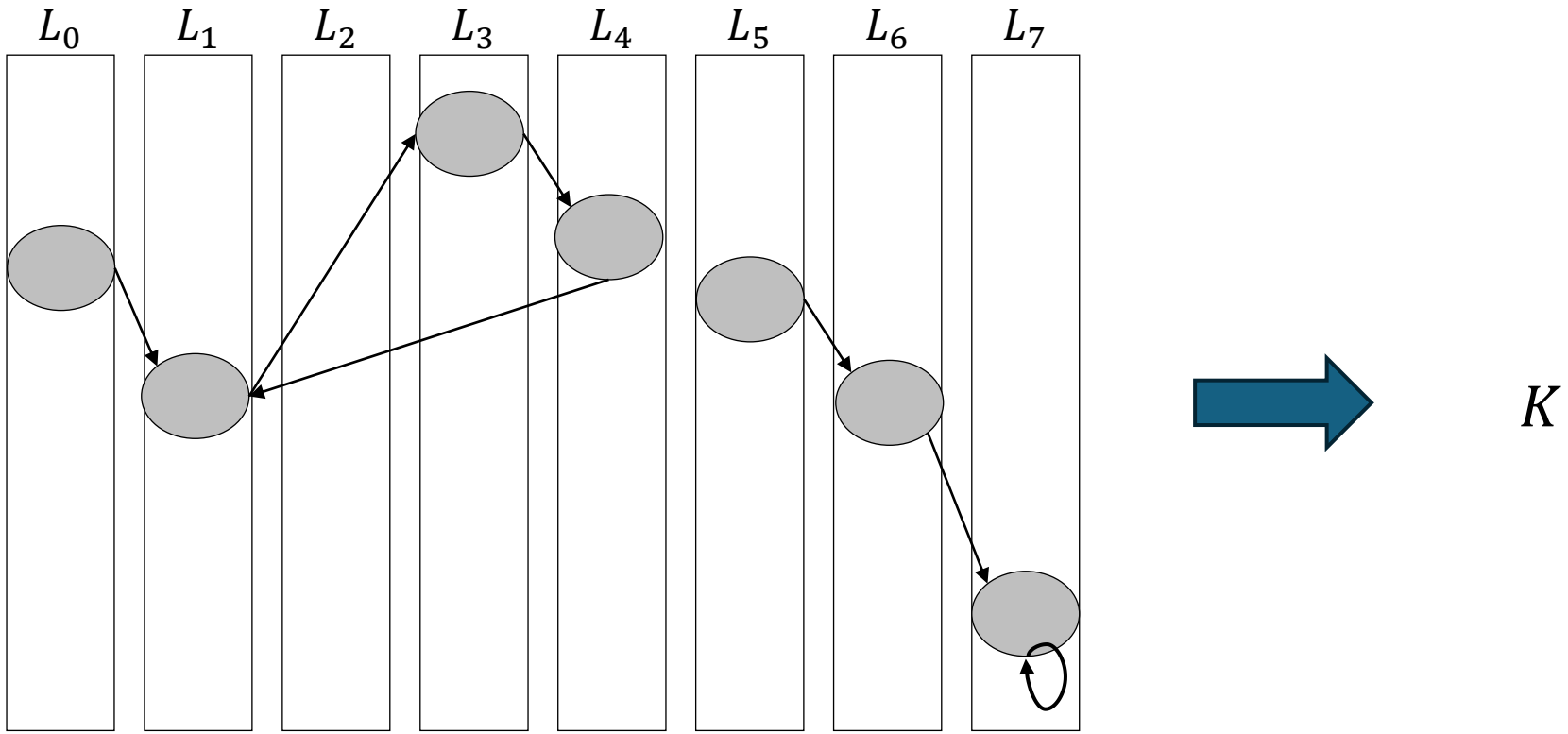
- **QUBO (Quadratic Unconstrained Binary Optimization)**

$$\text{QUBO: minimize/maximize} \quad y = x^t Q x \quad x\text{는 binary.}$$

$$\text{Minimize} \quad y = -5x_1 - 3x_2 - 8x_3 - 6x_4 + 4x_1x_2 + 8x_1x_3 + 2x_2x_3 + 10x_3x_4$$

- 예시
  - NP-hard로 분류되는 문제
  - 풀고자하는 문제를 QUBO로 나타낼 수 있으면 QA를 적용할 수 있음
  - 그러나 QUBO는 제약 조건이 없는 문제이므로, 페널티를 부과하여 이를 구현

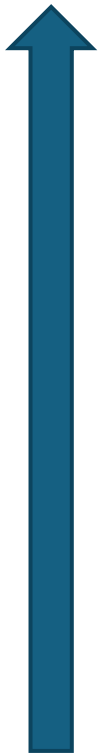
Inversion Attack on A5-GMR-2



어떤 조건을 만족하는 노드 집합을 찾으면 키 복구로 연결됨

Inversion Attack on A5-GMR-2

어떤 조건을 만족하는 노드 집합이 최적해에 대응되는 QUBO 문제를 구축



어떤 조건을 만족하는 노드 집합을 찾으면 키 복구로 연결됨

Inversion Attack on A5-GMR-2

어떤 조건을 만족하는 노드 집합이 최적해에 대응되는 QUBO 문제를 구축

각 노드를 하나의 이진 변수에 대응 -> 선택하면 1, 선택하지 않으면 0

어떤 조건을 만족하는 노드 집합을 찾으면 키 복구로 연결됨

Inversion Attack on A5-GMR-2

어떤 조건을 만족하는 노드 집합이 최적해에 대응되는 QUBO 문제를 구축

모든 1차항의 계수를 -1로 설정

각 노드를 하나의 이진 변수에 대응 -> 선택하면 1, 선택하지 않으면 0

어떤 조건을 만족하는 노드 집합을 찾으면 키 복구로 연결됨

Inversion Attack on A5-GMR-2

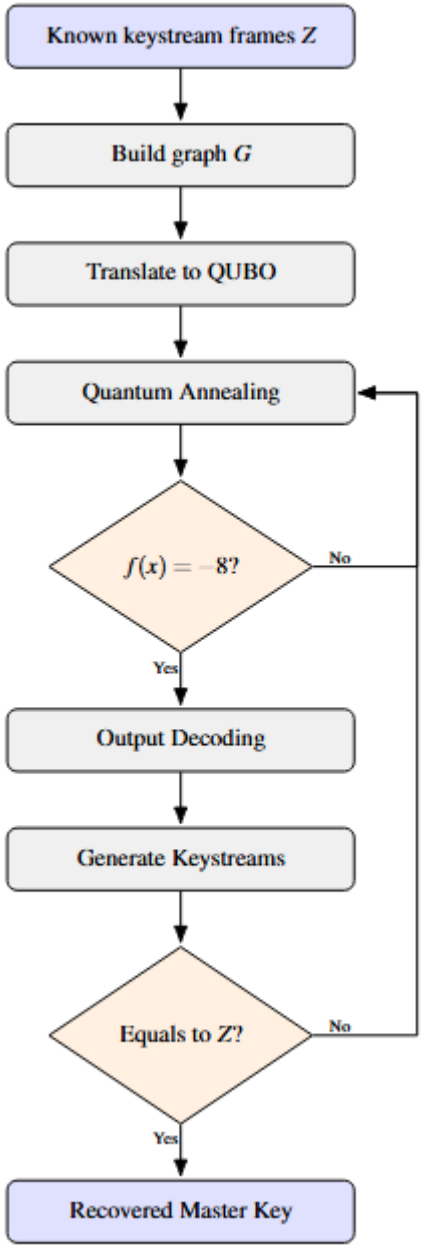
어떤 조건을 만족하는 노드 집합이 최적해에 대응되는 QUBO 문제를 구축

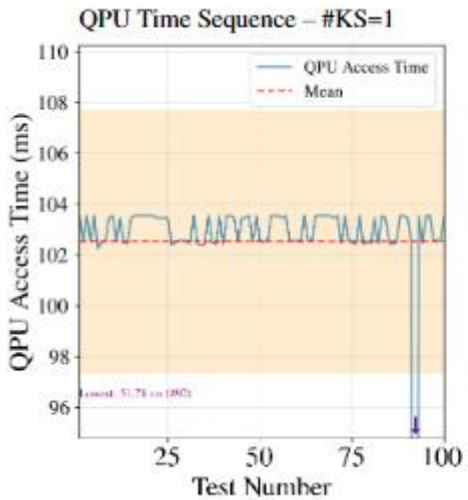
어떤 조건을 만족하지 않을 때에만 1인 수식에 penalty를 곱하여 목적함수에 추가

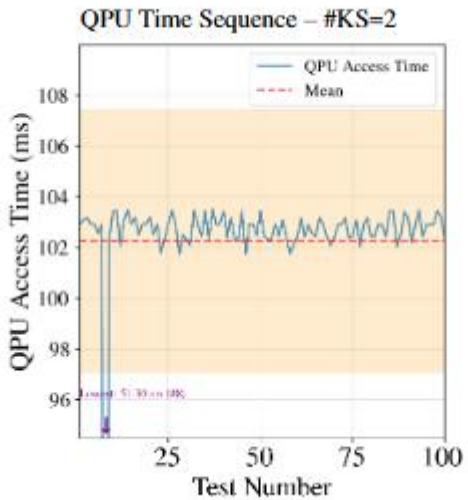
모든 1차항의 계수를 -1로 설정

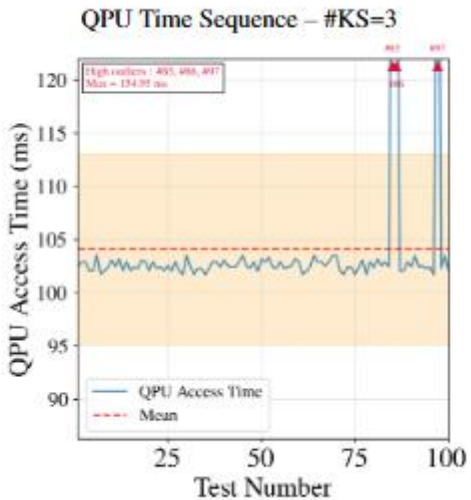
각 노드를 하나의 이진 변수에 대응 -> 선택하면 1, 선택하지 않으면 0

어떤 조건을 만족하는 노드 집합을 찾으면 키 복구로 연결됨


Known keystream frames Z
Build graph G
Translate to QUBO
Quantum Annealing
$f(x) = -8$?
No
Yes
Output Decoding
Generate Keystreams
Equals to Z?
No
Yes
Recovered Master Key


QPU Time Sequence – #KS=1
QPU Access Time
Mean
QPU Access Time (ms)
Test Number


QPU Time Sequence – #KS=2
QPU Access Time
Mean
QPU Access Time (ms)
Test Number


QPU Time Sequence – #KS=3
QPU Access Time
Mean
QPU Access Time (ms)
Test Number

감사합니다

dongjae.lee@kangwon.ac.kr