Quantum neural distinguisher for S-PRESENT
+
암호연구회 실험

https://youtu.be/L4M10DJxt_s

Quantum neural distinguisher for S-PRESENT

암호연구회 실험 (일부)

Quantum neural distinguisher for S-PRESENT

Quantum neural distinguisher for S-PRESENT

- 배경 지식 및 제안 기법 설명은 다른 세미나에서 많이 해서 스킵하고 실험 결과에 대해 설명드리겠습니다.
- (작성 중인 SCIE 논문에 추가할 예정)
- **S-PRESENT 3라운드에 대한 실험 결과**
  (더 많은 라운드에 대해, 클래식으로는 가능하지만 퀀텀으로는 시간이 오래 걸려서 현재 3라운드만 검증됨)
- **입력 차분 : 0x0007**
- **정확도 7% 향상, 과적합 해결, 파라미터 32% 감소**

		Classical	Quantum
Accuracy	Training	84.2	98.5
	Validation	79.7	95.7
	Test	87.0	94.0
The number of parameters		37377	25393
Epoch		20	20
Description		Accuracy improved by 7%, Overfitting reduced, The number of parameters reduced by 32%	

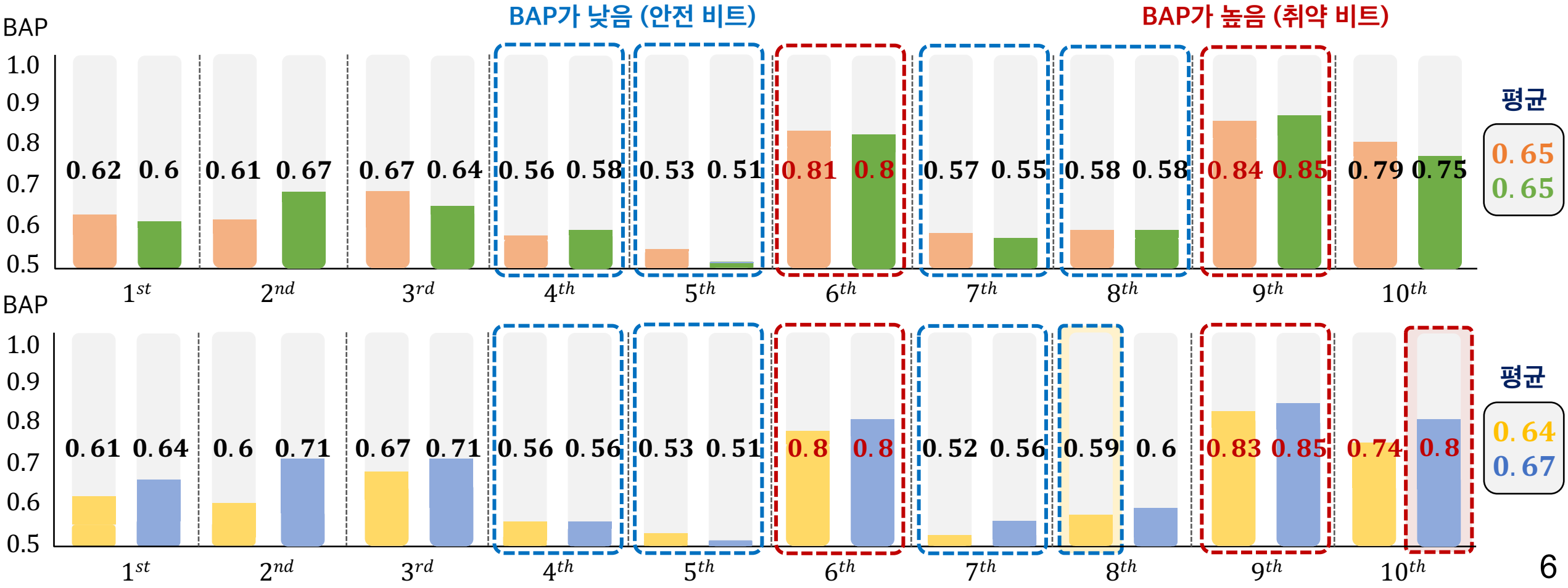
암호연구회 실험 (일부)

Classical vs Quantum (New)

Classical (MLP, # of data : 28500, # of param : 55092)
Quantum (Random, # of data : 28500, # of param : 43956)
Classical (MLP, # of data : 19950, # of param : 55092)
Quantum (Strongly, # of data : 19950, # of param : 44276)

안전 비트 : ~ 0.6
취약 비트 : 0.8 ~

- Quantum NN의 학습 시간이 매우 오래 걸려서, Epoch을 줄인 후 결과 비교 (25, 25, 35, 35)
- Quantum NN의 **파라미터**가 Classical에 비해 **약 19.7% 감소**
- **데이터 수가 상대적으로 적은 경우 (19950)**, quantum이 평균적으로 **3% 더 높은 BAP 달성**
- Classical에서는 **검출되지 않던 취약 비트 검출 가능**, 전반적으로 높은 정확도



Epoch별 취약 비트 (얽힘만 있는 경우)

of data : Tr (19950), Val (14000), Ts (1050)

Epoch \ Bit	1	2	3	4	5	6	7	8	9	10
15	O	O		O	O	X	O	O	X	
20				O	O	X	O	O	X	
25				O	O	X	O	O	X	
30				O	O	X	O	O	X	
35				O	O	X	O	O	X	
100				O		X	O		X	X

Epoch \ Bit	1	2	3	4	5	6	7	8	9	10
10	O	O		O	O	X	O	O	X	
15	O			O	O	X	O	O	X	
20	O			O	O	X	O	O	X	
25				O	O	X	O	O	X	
30				O	O	X	O	O	X	X
35				O	O	X	O		X	X

Classical NN

- In every epoch, 4,7은 안전
- In every epoch, 6,9는 취약
- In 35 epoch, 4,5,7,8은 안전, 6, 9는 취약
- In 100 epoch, **5, 8은 안전 비트 탈락**, **10이 취약 비트로 검출**

Quantum NN (Only entanglement)

- In every epoch, 4,5,7은 안전
- In every epoch, 6, 9는 취약
- In 30 epoch, **10이 취약 비트로 검출**
- In 35 epoch, **8은 안전 비트 탈락** (Classical에 비해 빨리 탈락)

- **Quantum에서 더 적은 epoch만으로 취약 비트 검출 (30 epoch)**
- Epoch을 늘릴 수록 안전 비트가 줄어들고, 취약 비트가 증가
- 그러나 quantum은 100번의 epoch을 실행하기는 어려움
- Classical에서는 100 epoch이 가능했기 때문에 **5번째 비트가 안전 비트가 아니었으나**,
  35 epoch만 학습한 quantum에서는 안전 비트로 판별됨 (더 적게 학습되어서 예측 확률이 낮은 상태)

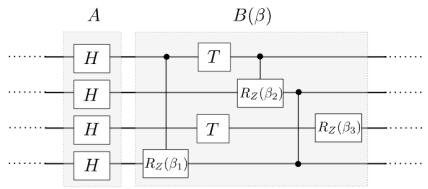
Hadamard 게이트 추가

- **양자 회로 맨 앞에 중첩이 추가되어야 함** (임베딩 회로의 맨 앞에 중첩 추가)
  - **Method 1 : 진폭 임베딩 앞에 Hadamard 추가**
    → 2^N개의 feature를 N개의 큐비트에 임베딩
  - **Method 2 : 중첩 게이트가 포함된 임베딩 회로** (IQP 회로, QAOA 임베딩 회로 ; Pennylane 제공)
    - **IQP 회로**
      → N개의 feature를 N개의 큐비트에 임베딩
      → 맨 앞에 Hadamard 게이트가 있고 각 큐비트에 회전 게이트 적용 후, 원하는 얽힘 게이트 설정 가능
    - **QAOA 임베딩**
      → N개의 feature를 $N+\alpha$개의 큐비트에 임베딩
      → N개의 feature를 임베딩한 큐비트 외의 큐비트에 Hadamard 게이트가 적용

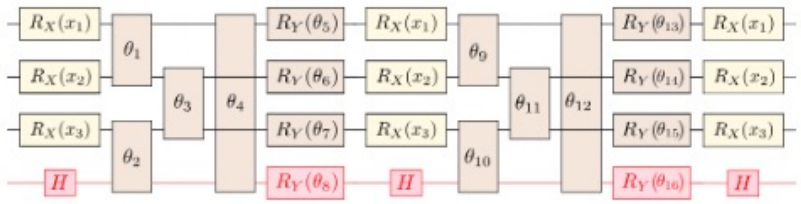
  - 현재 많은 큐비트를 사용한 학습은 어려움
  - 따라서 **Method 1을 우선적으로 실험 중**

A 고정, B 매개변수화

단일 큐비트 게이트가 고정된 예는 소위 *IQP(Instantaneous Quantum Polynomial)* 회로입니다. 여기서AHadamard 게이트와B매개변수화된 대각선 1 및 2 큐비트 게이트로 구성됩니다(Shepherd & Bremner(2008) , Havlicek et al.(2018)).



*IQP 회로
https://pennylane.ai/qml/glossary/circuit_ansatz.html



*QAOA 회로
https://docs.pennylane.ai/en/stable/code/api/pennylane.QAOAEmbedding.html

IQP / QAOA 회로 적용?

- 앞서 언급한 IQP, QAOA 임베딩 또한 각 임베딩과 같이 **많은 큐비트를 필요로 함**

- **큐비트를 적게 쓸 경우**
  → 임베딩 할 수 있는 feature가 감소

- **큐비트를 많이 쓸 경우**
  → 최대 16 큐비트 정도이며, 학습 소요 시간이 매우 클 것으로 예상 (큐비트 수가 n배 증가 시, 학습 소요 시간 n배 증가)

- **IQP 임베딩 및 QAOA 사용 시 오래 걸리는 문제를 해결하기 위해 4 큐비트만 사용한다면?**
  - 해당 임베딩이 적은 큐비트로도 효과적일 수도 있으므로 **현재 학습 중**
  - **만약 적은 큐비트로 효과적이지 않다면,** 더 많은 큐비트를 사용해서 학습하기에는 수많은 학습 시간이 필요하게 됨
  - IQP 임베딩에 대해 4 큐비트, 4 회로, 10 레이어로 1 epoch에 약 20000~40000초 소요 예상, 파라미터 38084 개
  - QAOA도 가능하면… 실험해볼 예정

Epoch별 취약 비트 (중첩+얽힘 있는 경우)

Epoch \ Bit	1	2	3	4	5	6	7	8	9	10
15	O	O		O	O	X	O	O	X	
20				O	O	X	O	O	X	
25				O	O	X	O	O	X	
30				O	O	X	O	O	X	
35				O	O	X	O	O	X	
100				O		X	O		X	X

Epoch \ Bit	1	2	3	4	5	6	7	8	9	10
10										
15										
20										
25										
30										
35										

Classical NN

- In every epoch, 4,7은 안전
- In every epoch, 6,9는 취약
- In 35 epoch, 4,5,7,8은 안전, 6, 9는 취약
- In 100 epoch, **5, 8은 안전 비트 탈락**, **10이 취약 비트로 검출**

Quantum NN (Entanglement + Superposition)

- 3일 후 완료 됨

- …

Epoch별 취약 비트 (얽힘 vs 중첩+얽힘 있는 경우)

Epoch \ Bit	1	2	3	4	5	6	7	8	9	10
10	O	O		O	O	X	O	O	X	
15	O			O	O	X	O	O	X	
20	O			O	O	X	O	O	X	
25				O	O	X	O	O	X	
30				O	O	X	O	O	X	X
35				O	O	X	O		X	X

Quantum NN (Only entanglement)

- In every epoch, 4,5,7은 안전
- In every epoch, 6, 9는 취약
- In 30 epoch, **10이 취약 비트로 검출**
- In 35 epoch, **8은 안전 비트 탈락**

- …

Epoch \ Bit	1	2	3	4	5	6	7	8	9	10
10										
15										
20										
25										
30										
35										

Quantum NN (Entanglement + Superposition)

- 3일 후 완료 됨

노이즈 있는 경우에 대한 실험

- 시뮬레이터 돌아가는지 확인하려고 얽힘만 있는 경우에 대해 실행했을 때 (키 공간 줄여서 실험했었음), **정확도가 비슷한 수준이어서 노이즈 모델을 지원하는 게 맞는지 확인 중**
- 중첩 포함된 케이스에 대한 실험이 끝나면 다시 돌려볼 예정

향후 계획

- 다음과 같은 내용 추가할 예정
- **S-AES**는 자원 부족 및 소요 시간으로 인해 현재로서는 불가능함을 보이기 위해 시간 및 자원 측정 예정
- **얽힘 vs 얽힘 + 중첩**
  - 학습이 약 50% 정도 진행 되었음 (한 번 학습에 너무 오래 걸려서 여러 번 실험은 불가능할 것 같음)
  - 학습 다 되면 세미나에 넣으려고 했는데 학습이 다 안 끝나서, 끝나면 한 번 정리해서 말씀드리겠습니다..
    (10/11일 기준, 3~4일이면 지금 학습 중인 것은 끝남, 1 epoch에 25000초 이상 소요)
- 중첩 포함된 회로에는 **IQP, QAOA, Hadamard+amplitude 임베딩**이 있음
  - 적은 feature만 임베딩할 수 있는 IQP, QAOA도 실험해보고 효과적인 것 같으면 중첩 회로끼리도 비교

감사합니다.

(세미나 늦지 않겠습니다 죄송합니다..
실험도 빨리 진행하도록 하겠습니다.)