Leveraging Reinforcement Learning to Identify Novel Advancements in Quantum Cryptography: A Case Study from QCrypt Conferences

Our study focuses on enhancing institutional capacities for exploring emerging quantum cryptography technologies, utilizing advanced techniques like reinforcement learning and topic modeling to identify and prioritize innovative cryptographic solutions. The key objective is to extract actionable insights from available data, enabling experts to anticipate and address organizational needs through the use of technological advancements. The research centers on quantum communication technologies, specifically aiming to identify innovations relevant to cryptographic applications. Our method integrates three main components: (1) topic modeling to extract core themes from relevant literature, (2) expert knowledge to refine the analysis, and (3) reinforcement learning (RL) to prioritize key topics based on entropy changes.

To implement this approach: 1) we first gathered articles published by 2022 from reputable databases like Scopus and Web of Science, refining them into a corpus for creating the initial topic model (CTP1), 2) the focus shifted to quantum cryptography, where a TF-IDF technique used to assign weights to critical cryptographic terms, particularly those related to quantum communication protocols. This process re-evaluated the initial topic model, emphasizing the most promising topics for technological potential, and 3) reinforcement learning was applied to optimize the selection of topics based on the maximum entropy change, with predefined thresholds guiding the identification of papers aligned with selected topics.

Our validation involved testing the relevance of topics selected by RL with articles from the 2023 and 2024 QCrypt conferences, focusing on weighted terms like "protocol" and "security enhancements with new protocols." We observed how the RL process evolved from CTP1 to CTP3, with iterations reflecting shifts in key topics and the discovery of novel advancements in security protocols.

Results show that the integration of keywords from the cryptography protocols and security protocols texts into the cryptography model yielded three models (CTP1 → CTP2 → CTP3), where the highest entropy changes within the models indicated promising advancements in protocols. The steps and outputs of the process are visually represented in the attached flowchart, illustrating how RL-guided selection has effectively identified trends in quantum cryptography, particularly in protocols. High rewards based on topic scores confirm the robustness of the RL approach in tracking novel developments across conference papers.

Entropy changes:

Entropy changes are used to inform Reinforcement Learning (RL) policy decisions in topic selection by measuring uncertainty in a topic's word distribution. High entropy reflects broad or ambiguous topics with evenly distributed words, signaling a need for exploration and refinement. Low entropy indicates well-defined topics with concentrated word distributions, suggesting these can be exploited for clarity and precision. Tracking entropy helps the RL agent focus on refining underdeveloped topics and reinforcing those that are clear. The entropy formula used to calculate the uncertainty of a topic's word distribution is: $H(T) = -\sum_{i=1}^{n} \mathrm{P}(\mathrm{wi} \mid \mathrm{T}) log \mathrm{P}(\mathrm{wi} \mid \mathrm{T})$

The cryptography topic model with three top terms is presented below.

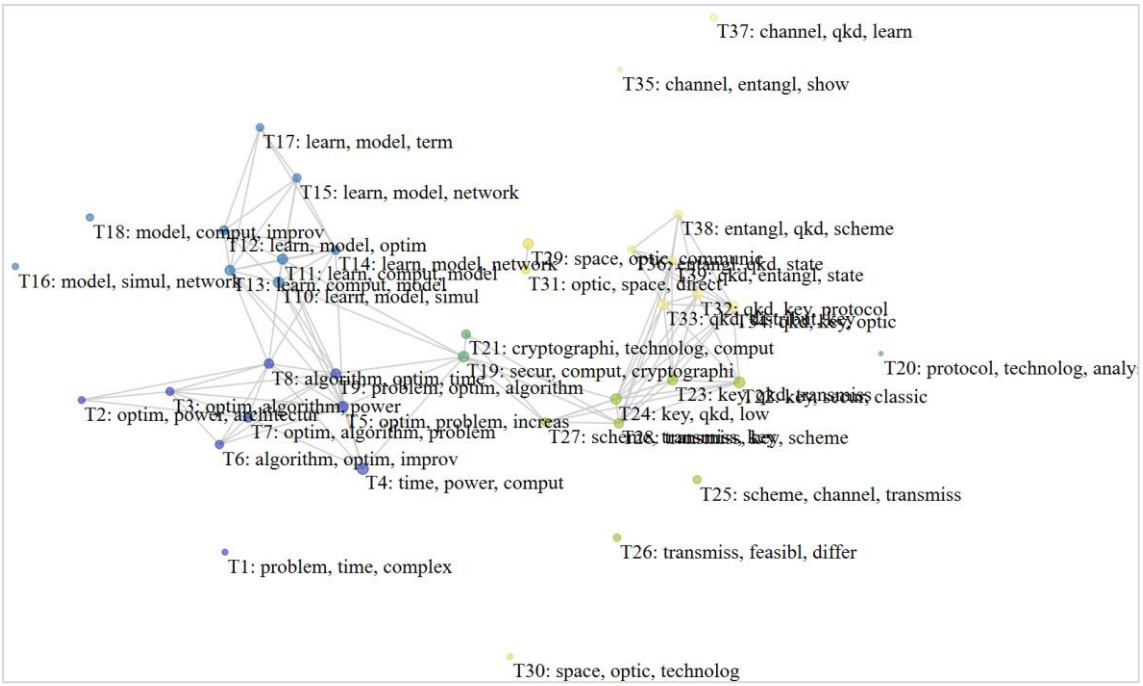


Figure 1: The network of the topics in initial topic model

The below flowchart outlines two iterations of a cryptography-related topic model process using reinforcement learning (RL) to explore novel protocol advancements.

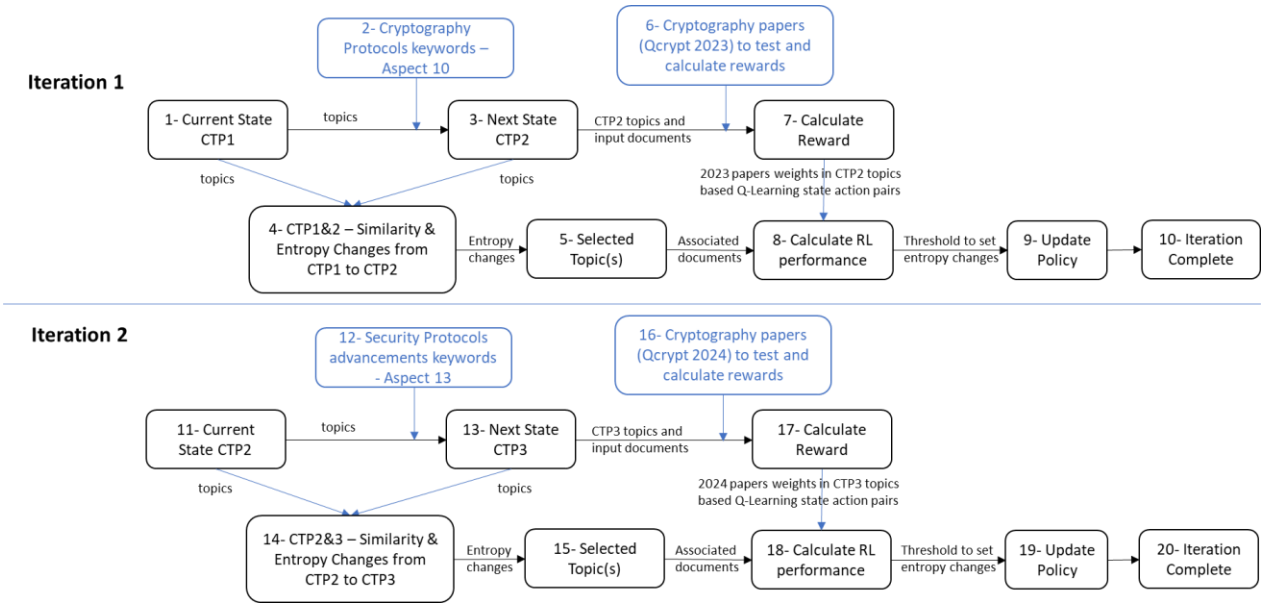


Figure 2: Iterative refinement of cryptography topic model using RL

First Iteration (Top Half):

1. **Current State (CTP1):** The model starts with the current cryptography topic model (CTP1).
2. **Aspect 10:** Cryptography protocols weighted keywords
3. **Next State (CTP2):** Based on cryptography protocols keywords (Aspect 10), the model transitions to a new state (CTP2).
4. **Similarity & Entropy Changes (CTP1 to CTP2):** A comparison between CTP1 and CTP2 evaluates similarity and entropy changes.
5. **Selected Topic(s):** Topics are chosen based on the analysis.
6. **QCrypt 2023 Papers:** Cryptography papers are used to calculate RL rewards.
7. **Reward:** The reward is calculated based on weights of most associated documents.
8. **RL Performance:** Compare the findings based on selected topics and associated documents and advancements in QCrypt 2023 published papers.
9. **Update Policy:** Based on the findings, the RL policy (e.g., maximum entropy change) is updated.
10. **Iteration Completion:** The first iteration concludes.

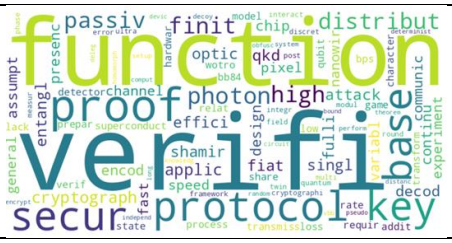
Second Iteration (Bottom Half):

11. **Current State (CTP2):** The second iteration begins with the updated state (CTP2) from the first iteration.
12. **Aspect 13:** Cryptography security protocols weighted keywords
13. **Next State (CTP3):** Using new security protocol advancement keywords (Aspect 13), the model moves to the next state (CTP3).
14. **Similarity & Entropy Changes (CTP2 to CTP3):** A similar comparison evaluates changes between CTP2 and CTP3.
15. **Selected Topic(s):** Relevant topics are selected.
16. **QCrypt 2024 Papers:** Updated cryptography papers (QCrypt 2024) are used to test and calculate rewards.
17. **Reward:** The reward is calculated based on weights of most associated 2024 documents.
18. **RL Performance:** Compare the findings based on selected topics and associated documents and advancements in QCrypt 2024 published papers.
19. **Update Policy & Iteration Completion:** The RL policy (e.g., maximum entropy change) is updated.
20. **Iteration Completion:** The second iteration concludes.

This process involves refining the cryptography topic model by leveraging RL to assess changes, adjust based on protocol advancements, and improve performance across two iterations.

Table 1: State Descriptions for Each Iteration in the Process

Step/Iteration 1	
1- Current State CTP1	CTP1
2- Cryptography Protocols keywords	**Aspect 10:** verifi-0.029, function-0.022, proof-0.022, protocol-0.02, secur-0.019, key-0.019, base-0.019, photon-0.018, distribut-0.017, high-0.017

	
3- Next State CTP2	CTP2
4- CTP1&2 – Similarity & Entropy Changes from CTP1 to CTP2	CTP1&2
5- Selected Topic(s) based on RL policy (max entropy changes) ***Top 5 selected topics:*** all unique documents, Average entropy, and top keywords	According the last column in CTP1&2, protocols topic model, top 5 topics with max entropy changes include: *topic number, entropy change, keyword (weight in the topic)* T37, Entropy score:223.6217, Topic Keywords: photon(0.015), qkd(0.014), key(0.011), state(0.010), protocol(0.010) T34, Entropy score:215.79414, Topic Keywords: key(0.416), protocol(0.397), secur(0.385), distribut(0.371), optic(0.365) T10, Entropy score:124.20075, Topic Keywords: high(0.068), state(0.060), base(0.057), effici(0.055), perform(0.054) T24, Entropy score:91.34865, Topic Keywords: qkd(0.187), secur(0.170), distribut(0.160), key(0.145), rate(0.127) T38, Entropy score:41.2685, Topic Keywords: photon(0.188), qkd(0.185), entangl(0.178), key(0.161), distribut(0.141) Docs(QCrypt 2023): 32, 10, 12, 2, 34, 33, 8, 20, 22, 28, 5, 3 Entropy score(Avg):139.24675 Keywords: system(2.48), design(1.86), framework(1.35), size(1.16), receiv(1.16), integr(1.12), channel(1.05), high(1.04), sourc(0.93), hash(0.88)
6- Cryptography papers (Qcrypt 2023) to test and calculate rewards	QCrypt2023_Papers / 2023.qcrypt.net
7- Calculate Reward: *each top 5 selected topics*,	Reward:37(0.433), 34(0.417), 10(0.387), 24(0.405), 38(0.358) - Avg(0.4) [Max in topics(0.586) - Min (0.323)]

max and min of entropy changes within 39 topics	
8- RL performance	Compare documents of 2023 and aspect 10 keywords
9- Update Policy	We keep the policy on top 5 max entropy changes and min on 0.3
10- Iteration Complete	
Iteration 2	
11- Current State CTP2	CTP2
12- Security Protocols advancements keywords	**Aspect 13:** independ-0.03, classic-0.026, key-0.025, pair-0.024, technolog-0.024, challeng-0.021, secur-0.02, protocol-0.02, share-0.02, set-0.02 
13- Next State CTP3	CTP3
14- CTP2&3 – Similarity & Entropy Changes from CTP2 to CTP3	CTP2&3
15- Selected Topic(s) based on RL policy (max entropy changes)	According the last column in CTP2&3, protocols topic model, top 5 topics with max entropy changes include: *topic number, entropy change, keyword (weight in the topic)* T32, Entropy score:51.086, Topic Keywords: secur(0.713), qkd(0.632), protocol(0.612), key(0.551), photon(0.538) T1, Entropy score:26.68507, Topic Keywords: studi(0.003), comput(0.002), promis(0.001) T2, Entropy score:19.9535, Topic Keywords: classic(0.010), function(0.010), present(0.009), final(0.009), studi(0.009) T12, Entropy score:16.15191, Topic Keywords: approach(0.065), classic(0.063), system(0.062), differ(0.061), propos(0.059) T17, Entropy score:15.8209, Topic Keywords: network(0.025), comput(0.025), classic(0.024), model(0.022), state(0.021)

Top 5 selected topics: all unique documents, Average entropy, and top keywords	Docs(QCrypt 2024): 16, 11, 12, 22, 21, 35, 33, 9, 10, 18, 26, 24, 4, 14, 29, 28 Entropy score(Avg):25.93948 Keywords: key(2.28), commit(1.6), state(1.52), model(1.26), pseudorandom(1.16), singl(1.12), bound(1.01), system(0.99), channel(0.91), high(0.9)
16- Cryptography papers (Qcrypt 2024) to test and calculate rewards	QCrypt2024_Papers / 2024.qcrypt.net
17- Calculate Reward: *each top 5 selected topics*, max and min of entropy changes within 39 topics	Reward:32(0.38), 1(0.36), 2(0.367), 12(0.398), 17(0.414) - Avg(0.384) [Max in topics(0.591) - Min (0)]
18- RL performance	Compare documents of 2024 and aspect 10 keywords
19- Update Policy	We keep the policy on top 5 max entropy changes and min on 0.3
20- Iteration Complete	

Table 1 outlines a detailed, step-by-step process of two iterations in cryptography topic modeling, demonstrating how reinforcement learning (RL) was applied to optimize topic selection based on entropy changes. The goal is to refine the cryptography topics over multiple iterations and extract valuable insights, especially in the context of cryptography protocols and security advancements.

Table Breakdown:

Iteration 1 (CTP1 to CTP2):

- We start with an initial topic model (CTP1) that uses Aspect 10 keywords (e.g., "protocol," "key," "photon") related to cryptography protocols.
- A transition is made to the next state (CTP2), where entropy changes (i.e., shifts in topic distribution and coherence) are calculated between CTP1 and CTP2.
- The RL algorithm identifies the top 5 topics with the highest entropy changes. These topics (e.g., T37, T34, T10) represent the most significant shifts in the cryptography landscape based on the selected protocol keywords.
- Rewards are calculated for each topic, with an average reward of 0.4 based on max and min entropy changes. This reward reflects how well each topic has shifted toward relevant and informative distributions.

Iteration 2 (CTP2 to CTP3):

- The second iteration begins with CTP2 and shifts to CTP3, using updated keywords from Aspect 13, which represent advancements in security protocols.
- Similar to the first iteration, RL selects the top 5 topics with the highest entropy changes (e.g., T32, T1, T12), reflecting advancements in security technologies and cryptography mechanisms.
- The average reward in this iteration is slightly lower (0.384), but the model continues to optimize based on maximum entropy changes to refine the understanding of emerging topics in cryptography.

Survey on Cryptography Topic Modeling Iterations

This survey aims to gather feedback from experts and participants regarding the effectiveness of the cryptography topic modeling process, with a particular emphasis on verifying the findings presented in Table 1 of the project statement (link below). Your insights will play a crucial role in refining the methodology and ensuring the relevance of the topics identified through the reinforcement learning approach.

The survey is organized into sections for ease of completion, concentrating on various aspects such as the relevance of topics, the verification of findings, the methodology used, and overall satisfaction.

Thank you for participating in this survey. Your feedback is vital for evaluating the effectiveness of the topic modeling process and its relevance to advancements in cryptography.

Here is the link to the project and its results: Project

Section 1: Respondent Information

1. Name (Optional):
2. Affiliation/Organization:
3. Role/Position:
    - Researcher
    - Practitioner
    - Educator
    - Other (please specify): _____
4. Years of Experience in Cryptography: ___ years

Section 2: Topic Relevance

5. How relevant do you find the selected topics from Iteration 1 (CTP1 to CTP2) based on Aspect 10 keywords? *Use keywords related to the selected topics to refine your search or follow the links to view relevant documents.*
    - Very Relevant
    - Relevant
    - Neutral
    - Not Relevant
    - Not Relevant at All
6. How relevant do you find the selected topics from Iteration 2 (CTP2 to CTP3) based on Aspect 13 keywords? *Use keywords related to the selected topics to refine your search or follow the links to view relevant documents.*
    - Very Relevant
    - Relevant
    - Neutral
    - Not Relevant
    - Not Relevant at All
7. Which of the following topics from Iteration 1 do you believe reflects significant advancements in cryptography protocols? (Select all that apply)

- T37
- T34
- T10
- T24
- T38
- Other (please specify): _____

8. Which of the following topics from Iteration 1 do you believe reflects significant advancements in cryptography protocols? (Select all that apply)
    - T32
    - T1
    - T2
    - T12
    - T17
    - Other (please specify): _____
9. Please rate the relevance of the top keywords associated with each selected topic in conveying important cryptography concepts.
    - Very Relevant
    - Relevant
    - Neutral
    - Not Relevant
    - Not Relevant at All

Section 3: Entropy and Information Gain

10. Do you believe the entropy changes observed between **CTP1 and CTP2, iteration 1**, accurately reflect significant shifts in the field of cryptography protocols? (Look at entropy scores in select topics, step 5)
    - Strongly Agree
    - Agree
    - Neutral
    - Disagree
    - Strongly Disagree
11. Do you believe the entropy changes observed between **CTP2 and CTP3, iteration 2**, accurately reflect significant shifts in the field of cryptography protocols? (Look at entropy scores in select topics, step 15)
    - Strongly Agree
    - Agree
    - Neutral
    - Disagree
    - Strongly Disagree
12. Did the observed entropy changes influence your understanding of trends in cryptography?
    - Yes, significantly
    - Yes, moderately
    - Neutral
    - No, not much
    - No, not at all

Section 4: Reinforcement Learning Methodology

13. How effective do you find the application of reinforcement learning in enhancing topic selection across iterations?
    - Very Effective
    - Effective
    - Neutral
    - Ineffective
    - Very Ineffective
14. How would you rate the clarity of the RL policy for selecting top topics based on maximum entropy changes?
    - Very Clear
    - Clear
    - Neutral
    - Unclear
    - Very Unclear
15. How satisfied are you with the calculated rewards for selected topics based on entropy changes?
    - Very Satisfied
    - Satisfied
    - Neutral
    - Dissatisfied
    - Very Dissatisfied

Section 5: Applicability and Impact

16. How applicable do you find the findings from this iterative process to your own research or work in the field of cryptography?
    - Highly Applicable
    - Applicable
    - Neutral
    - Not Applicable
    - Not Applicable at All
17. What improvements or additional features would you suggest for future iterations of the topic modeling process? (Open-ended response)

18. Are there any specific areas in cryptography that you believe require further exploration through topic modeling? (Open-ended response)

Section 6: Overall Satisfaction

19. Overall, how satisfied are you with the findings presented in the iterations?
    - Very Satisfied
    - Satisfied
    - Neutral
    - Dissatisfied
    - Very Dissatisfied
20. Do you have any additional comments or feedback regarding the topic modeling iterations? (Open-ended response)
