Quantum Machine Learning versus Machine Learning for Intrusion Detection in 5G Environments

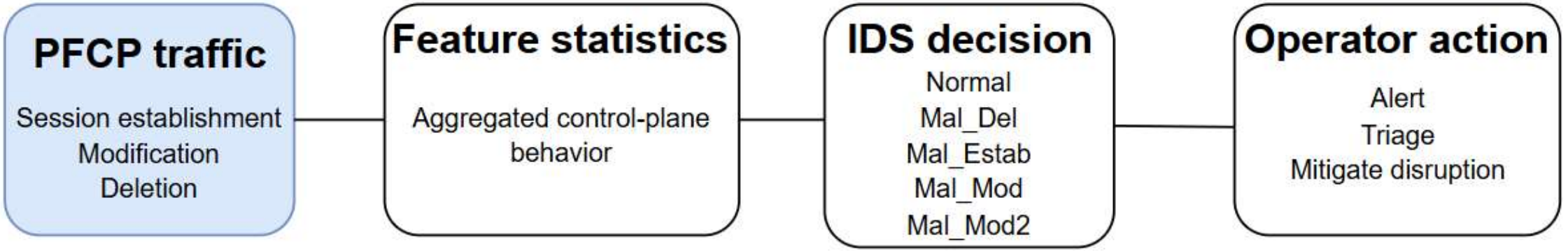
Ioannis D. Leonidas, Panagiotis Radoglou-Grammatikis, Evangelos K. Markakis, Michail-Alexandros Kourtis, Thomas Lagkas, Georgios Th. Papadopoulos, Vasileios Argyriou, Panagiotis Sarigiannidis



Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101225776, SecQDevOps: Trustworthy Quantum DevOps for Secure Software and Hardware Quantum Engineering. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the granting authority. Neither the European Union nor the granting authority can be held responsible for them.

Motivation



- PFCP is a high value 5G Core target
- Control plane attacks can disrupt the user plane services the operator need to keep alive

Why this is hard?

- High dimensional statistics, multiclass attack taxonomies, latency constraints make PFCP IDS a realistic testbed for comparing representations

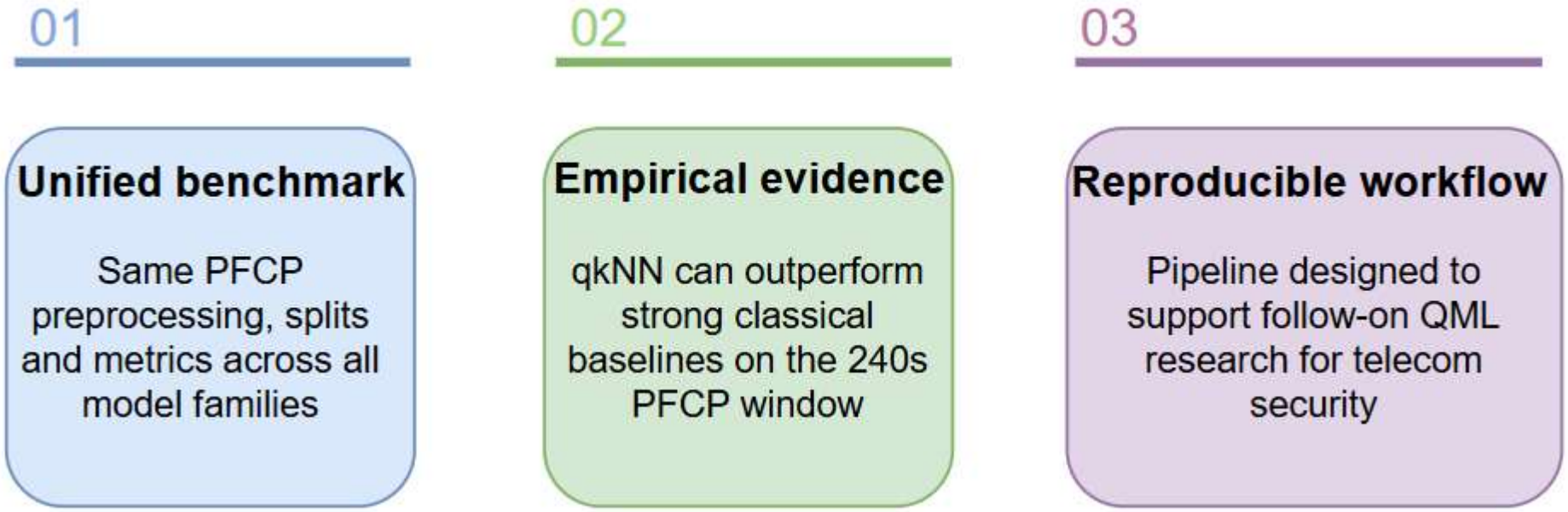
Main question

Can quantum-inspired or quantum models give useful decision boundaries for realistic 5G Core IDS?

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101225776, SecQDevOps: Trustworthy Quantum DevOps for Secure Software and Hardware Quantum Engineering. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the granting authority. Neither the European Union nor the granting authority can be held responsible for them.

Our contribution



Positioning

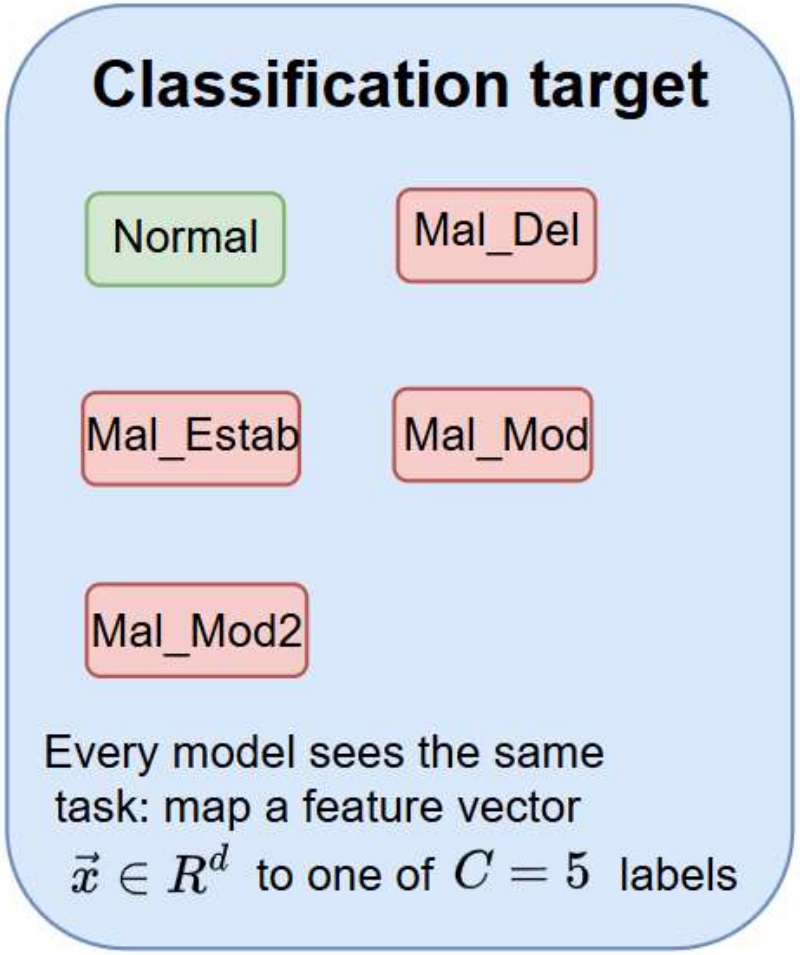
This paper separates analytic quantum-inspired kernels, parametrized quantum classifiers, and trainable quantum kernels. The result is a practical comparison, not a claim that QML is universally superior.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101225776, SecQDevOps: Trustworthy Quantum DevOps for Secure Software and Hardware Quantum Engineering. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the granting authority. Neither the European Union nor the granting authority can be held responsible for them.

Dataset and task formulation

- PFCP APP Layer
  - Multiclass detection over aggregation-window datasets
- Dataset input
  - 35 original features
  - 10 PFCP statistical features, with PCA, to fit NISQ quantum circuits
- Windows
  - 15sec, 60sec, 120sec, 240sec
- Classes
  - Normal + 4 PFCP attack classes
- Metrics
  - Accuracy, macro precision, macro recall, macro F1



Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101225776, SecQDevOps: Trustworthy Quantum DevOps for Secure Software and Hardware Quantum Engineering. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the granting authority. Neither the European Union nor the granting authority can be held responsible for them.

Model families compared

Classical ML baselines

RBF-SVM

XGBoost

Strong reference points with mature optimization and low deployment friction

Quantum-inspired kernels

qkNN

analytic SWAP-test kernel

Quantum motivated similarity, evaluated fully classically

Trainable QML algorithms

Parametrized quantum classifiers

Hardware efficient ansatz

Data reuploading ansatz

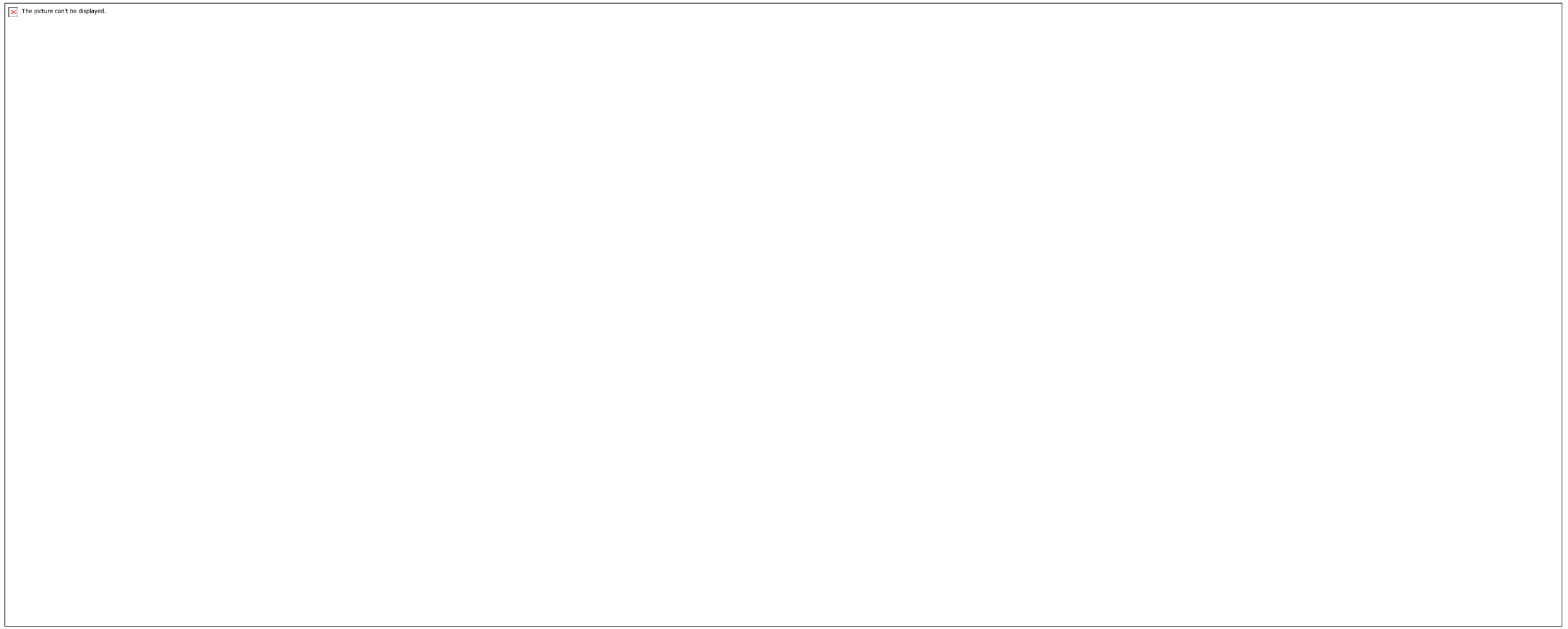
Quantum kernel alignment methods

More expressive but sensitive to scaling, optimization and runtime

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101225776, SecQDevOps: Trustworthy Quantum DevOps for Secure Software and Hardware Quantum Engineering. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the granting authority. Neither the European Union nor the granting authority can be held responsible for them.

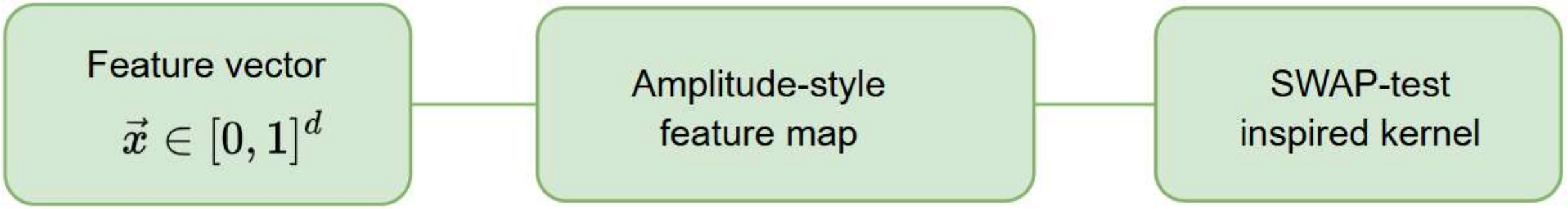
End-to-end evaluation pipeline



Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101225776, SecQDevOps: Trustworthy Quantum DevOps for Secure Software and Hardware Quantum Engineering. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the granting authority. Neither the European Union nor the granting authority can be held responsible for them.

qkNN: Quantum-inspired similarity



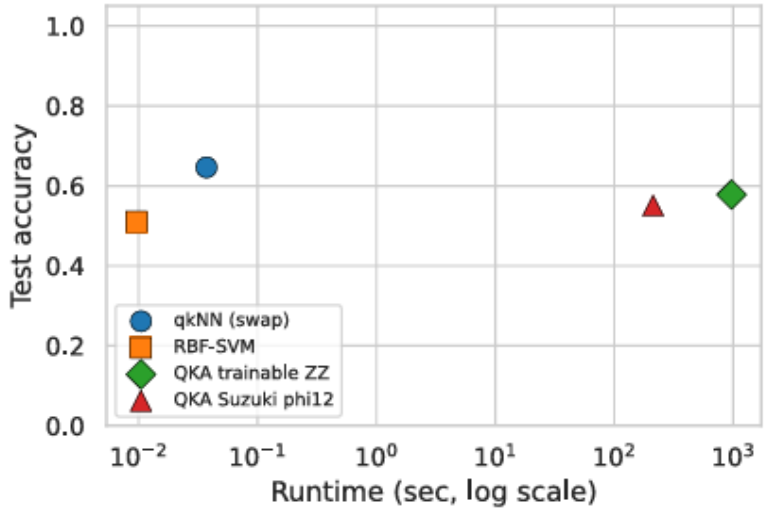
$$K(\vec{x}, \vec{x'}) = \prod_{j=1}^{d} \left(\sqrt{x_j x'_j} + \sqrt{(1 - x_j)(1 - x'_j)} \right)$$

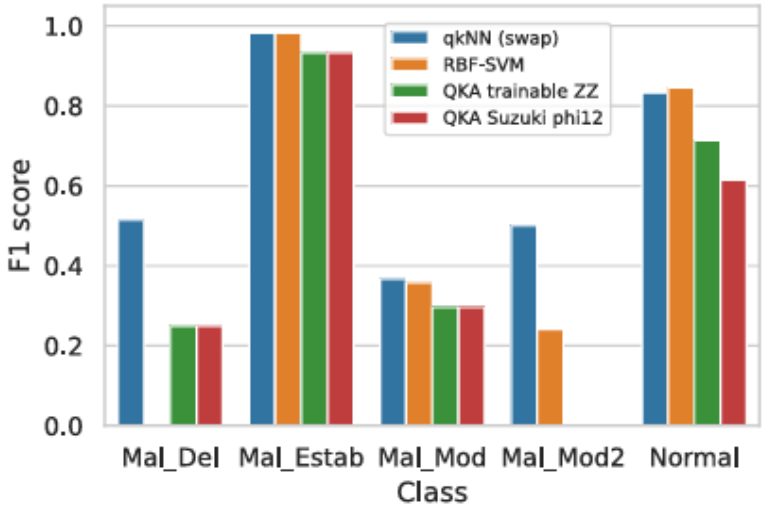
Then, select top-k most similar training samples and perform similarity-weighted voting

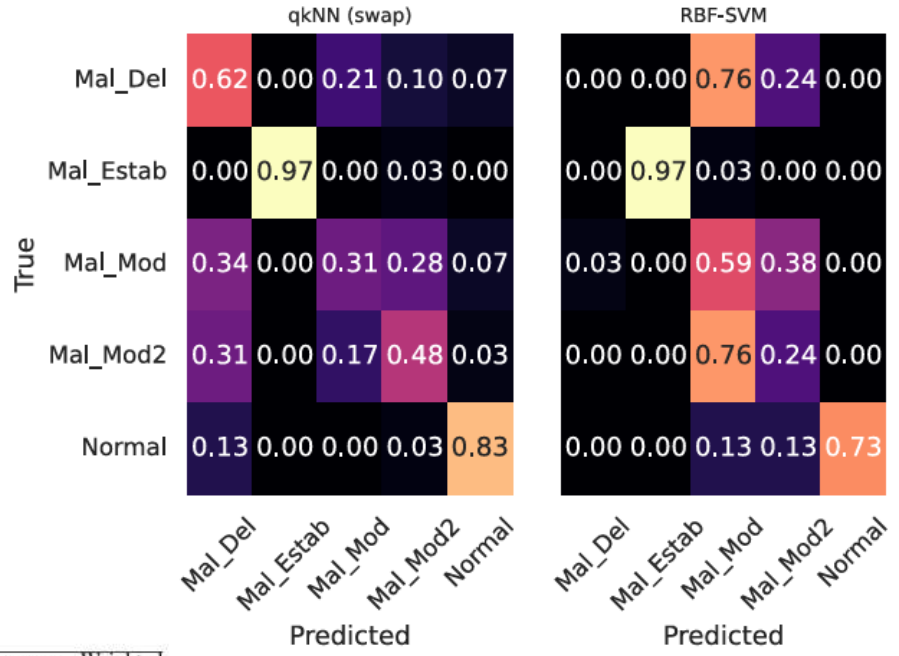
Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101225776, SecQDevOps: Trustworthy Quantum DevOps for Secure Software and Hardware Quantum Engineering. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the granting authority. Neither the European Union nor the granting authority can be held responsible for them.

Main result: 240sec PFCP window







qkNN
62.1% accuracy
61.6% macro F1
Outperforms xgboost and rbf-svm on this time window

TABLE V
PFCP 240S WINDOW RESULTS.

Method	Accuracy	Macro Precision	Macro Recall	Macro F1	Weighted F1
svm-rbf	0.5510	0.5429	0.5478	0.5169	0.5216
qknn	**0.6211**	**0.6355**	**0.6175**	**0.6157**	**0.6195**
qka trainable ZZ	0.4125	0.5221	0.4125	0.4263	0.4263
qka suzuki phi12	0.4500	0.4981	0.4500	0.4460	0.4460
xgboost	0.5986	0.6215	0.5952	0.6029	0.6068
hardware efficient ansatz	0.5027	0.4937	0.4989	0.4613	0.4668
multi class ansatz	0.5177	0.5462	0.5139	0.4949	0.5000
data reuploading ansatz	0.5075	0.5126	0.5037	0.4740	0.4793

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101225776, SecQDevOps: Trustworthy Quantum DevOps for Secure Software and Hardware Quantum Engineering. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the granting authority. Neither the European Union nor the granting authority can be held responsible for them.

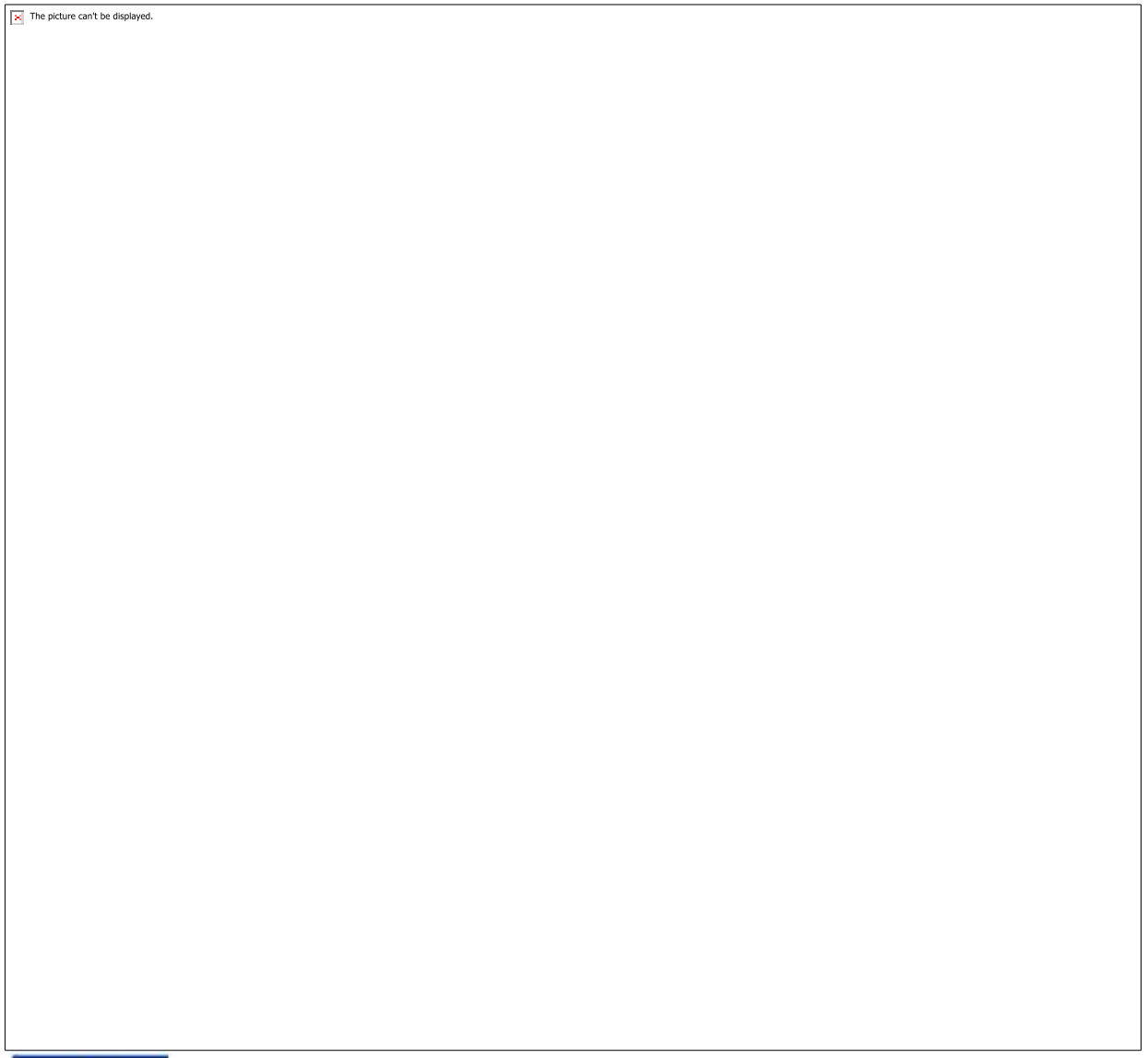
Results across aggregation windows

Method	15sec Acc/F1 (%)	60sec Acc/F1 (%)	120sec Acc/F1 (%)	240sec Acc/F1 (%)
qkNN	**63.14 / 63.46**	58 / 57.99	**59.49 / 60.55**	**62.11 / 61.57**
XGBoost	61.5 / 61.91	**59.33 / 59.61**	58.23 / 58.86	59.86 / 60.29
RBF-SVM	54.2 / 51.43	55.35 / 47.16	53.16 / 48.23	55.1 / 51.69
Best PQC	55.11 / 48.49	57 / 53.93	52.5 / 48.8	51.77 / 49.49
Best QKA	58.75 / 55.06	52 / 49.44	51.25 / 46.65	45 / 44.6

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101225776, SecQDevOps: Trustworthy Quantum DevOps for Secure Software and Hardware Quantum Engineering. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the granting authority. Neither the European Union nor the granting authority can be held responsible for them.

Trainable quantum machine learning algorithms



- Ansatz variants tested
  - Hardware-efficient ansatz (HEA)
    - Encodes the input once, then applies repeatable trainable layers
  - Data-reuploading ansatz (DRA)
    - Alternates data encoding and trainable blocks across layers
  - Multiclass ansatz
    - Assigns each class to a computational basis bitstring and predicts using state overlap probabilities
- Observed results
  - PQCs are competitive but not dominant on PFCP intrusion detection
  - Across windows, trainable QML algorithms shows higher sensitivity to scaling, optimization and circuit design than qknn or xgboost

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101225776, SecQDevOps: Trustworthy Quantum DevOps for Secure Software and Hardware Quantum Engineering. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the granting authority. Neither the European Union nor the granting authority can be held responsible for them.

Key takeaways

- Quantum inspired kernels are competitive with classical baselines
  - They can add a useful similarity bias without quantum hardware or quantum circuit training
- Trainable quantum machine learning algorithms are fragile
  - PQCs and QKA methods need stronger optimization, scaling, and validation under noise
- Telecom based IDS needs realistic benchmarks
  - PFCP multiclass detection is a better stress test than toy or generic datasets

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101225776, SecQDevOps: Trustworthy Quantum DevOps for Secure Software and Hardware Quantum Engineering. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the granting authority. Neither the European Union nor the granting authority can be held responsible for them.

Conclusion & Next steps

- Conclusion
  - Quantum inspired kernels are competitive with classical baselines for PFCP intrusion detection
  - Trainable quantum algorithms are promising but not yet robust enough in this setting
- Future work
  - Test the algorithms on TCP-IP layer datasets
  - Study the scale of the algorithms under realistic hardware noise
  - Improve on scaling strategies

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101225776, SecQDevOps: Trustworthy Quantum DevOps for Secure Software and Hardware Quantum Engineering. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the granting authority. Neither the European Union nor the granting authority can be held responsible for them.



Co-funded by
the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101225776, SecQDevOps: Trustworthy Quantum DevOps for Secure Software and Hardware Quantum Engineering. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the granting authority. Neither the European Union nor the granting authority can be held responsible for them.



Co-funded by
the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101225776, SecQDevOps: Trustworthy Quantum DevOps for Secure Software and Hardware Quantum Engineering. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the granting authority. Neither the European Union nor the granting authority can be held responsible for them.



Co-funded by
the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101225776, SecQDevOps: Trustworthy Quantum DevOps for Secure Software and Hardware Quantum Engineering. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the granting authority. Neither the European Union nor the granting authority can be held responsible for them.



Co-funded by
the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101225776, SecQDevOps: Trustworthy Quantum DevOps for Secure Software and Hardware Quantum Engineering. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the granting authority. Neither the European Union nor the granting authority can be held responsible for them.



Co-funded by
the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101225776, SecQDevOps: Trustworthy Quantum DevOps for Secure Software and Hardware Quantum Engineering. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the granting authority. Neither the European Union nor the granting authority can be held responsible for them.



Co-funded by
the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101225776, SecQDevOps: Trustworthy Quantum DevOps for Secure Software and Hardware Quantum Engineering. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the granting authority. Neither the European Union nor the granting authority can be held responsible for them.



Co-funded by
the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101225776, SecQDevOps: Trustworthy Quantum DevOps for Secure Software and Hardware Quantum Engineering. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the granting authority. Neither the European Union nor the granting authority can be held responsible for them.



Co-funded by
the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101225776, SecQDevOps: Trustworthy Quantum DevOps for Secure Software and Hardware Quantum Engineering. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the granting authority. Neither the European Union nor the granting authority can be held responsible for them.



Co-funded by
the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101225776, SecQDevOps: Trustworthy Quantum DevOps for Secure Software and Hardware Quantum Engineering. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the granting authority. Neither the European Union nor the granting authority can be held responsible for them.