Kyber Electromagnetic Signal Classifier

Production Analysis Report

Executive Summary

This report presents the results of electromagnetic signal classification for Kyber cryptographic analysis using traditional machine learning methods. The classifier distinguishes between M0 (known plaintext) and M1 (random plaintext) traces with high accuracy using Support Vector Machine (SVM) and Random Forest algorithms.

Key Performance Metrics

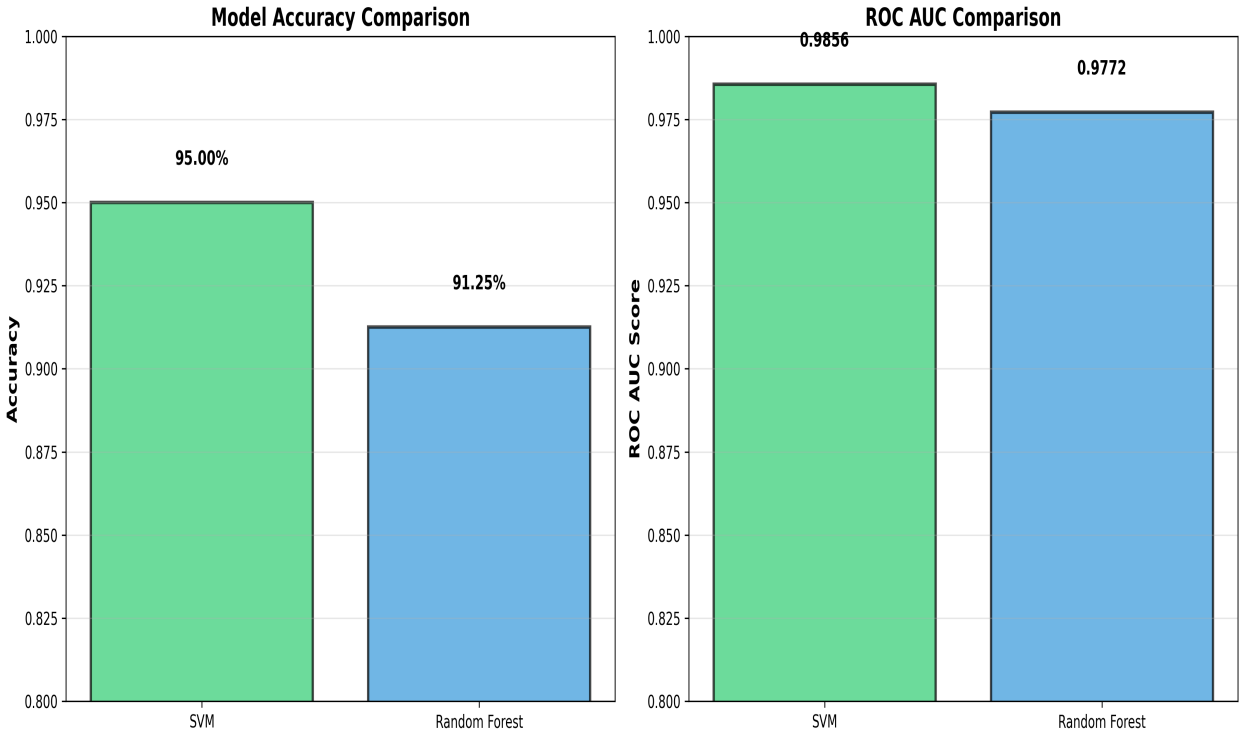
Metric	SVM	Random Forest
Test Accuracy	95.00%	91.25%
ROC AUC Score	0.9856	0.9772
CV Mean Accuracy	0.8281	0.9781
CV Std (±2σ)	0.1734	0.0375

Dataset Information

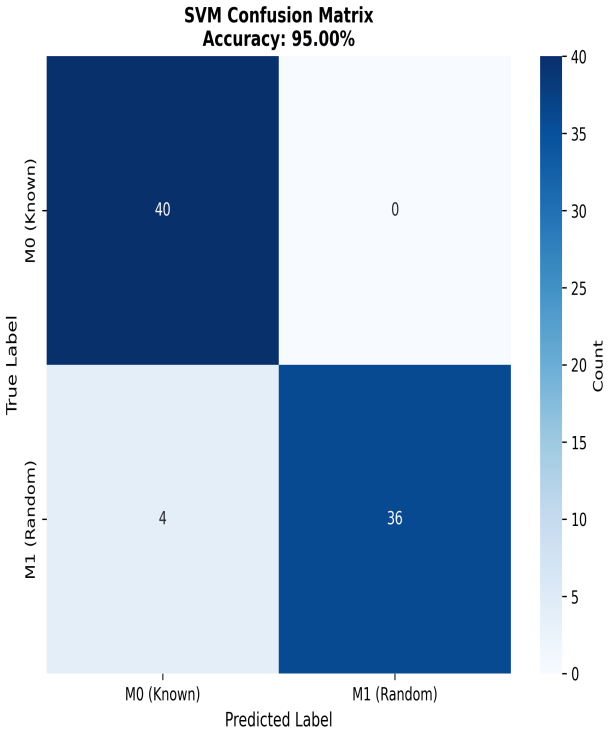
Training Set: 320 samples (160 M0, 160 M1)
Test Set: 80 samples (40 M0, 40 M1)
Features: 1000 electromagnetic signal features
Preprocessing: StandardScaler normalization (no division by 256)

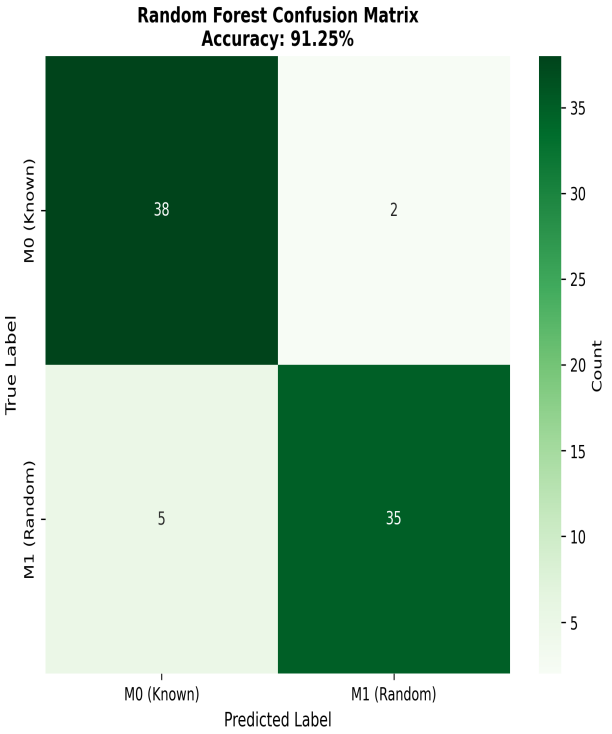
Visualization Results

Model Performance Comparison

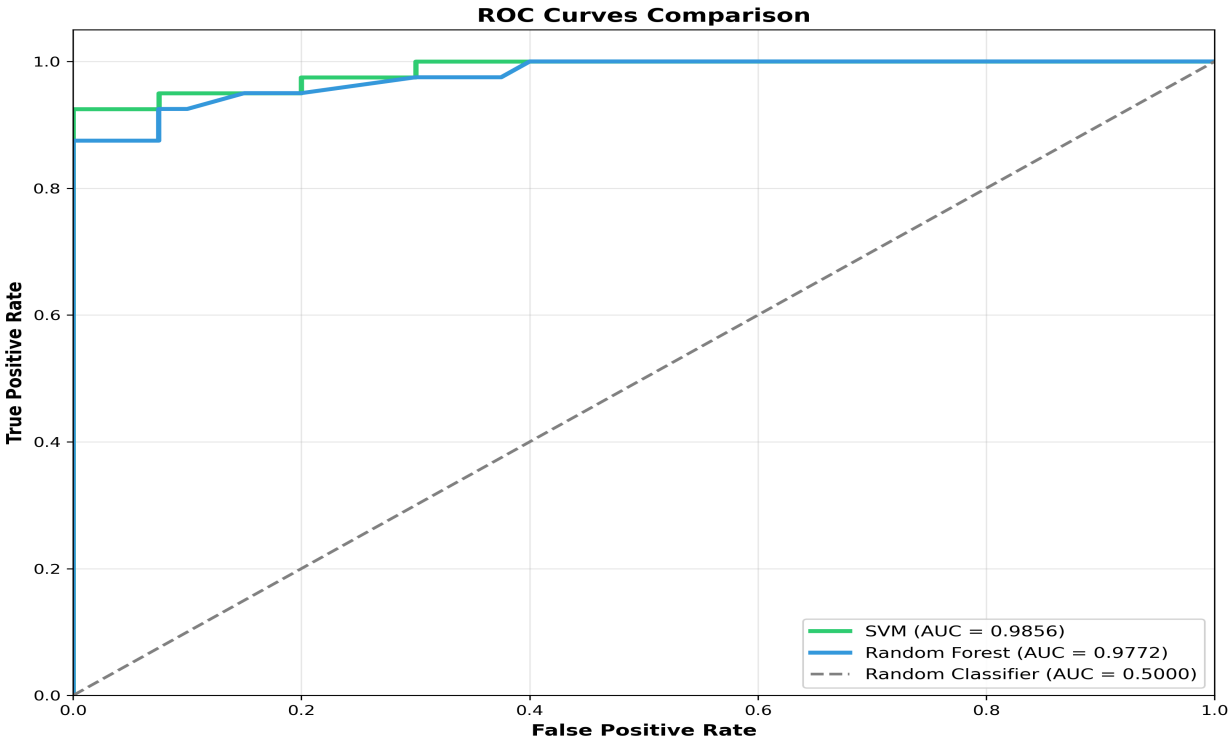


Confusion Matrices

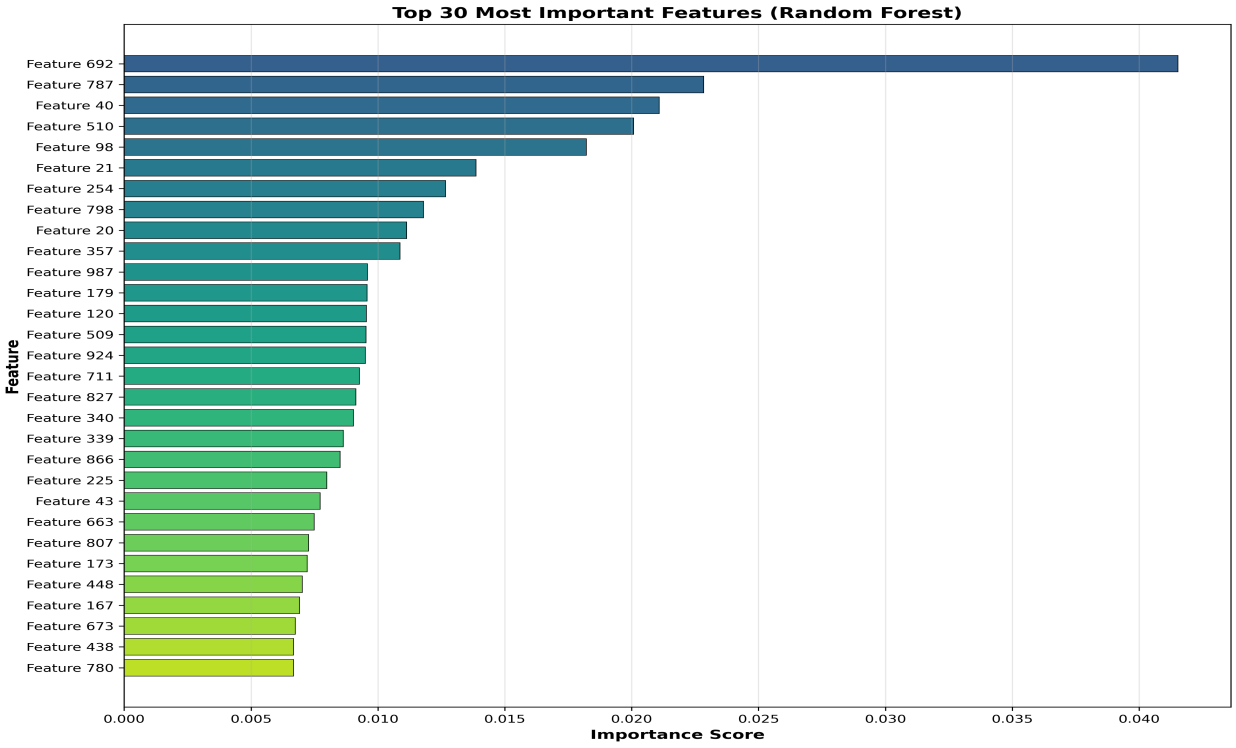

SVM Confusion Matrix
Accuracy: 95.00%
True Label
M0 (Known)
M1 (Random)
40
0
4
36
M0 (Known)
M1 (Random)
Predicted Label
Count
40
35
30
25
20
15
10
5
0


Random Forest Confusion Matrix
Accuracy: 91.25%
True Label
M0 (Known)
M1 (Random)
38
2
5
35
M0 (Known)
M1 (Random)
Predicted Label
Count
35
30
25
20
15
10
5

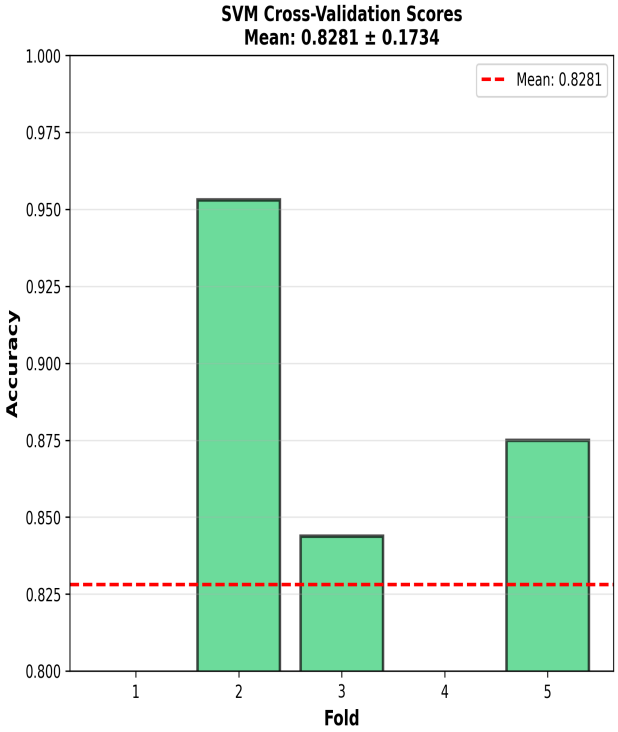
ROC Curves

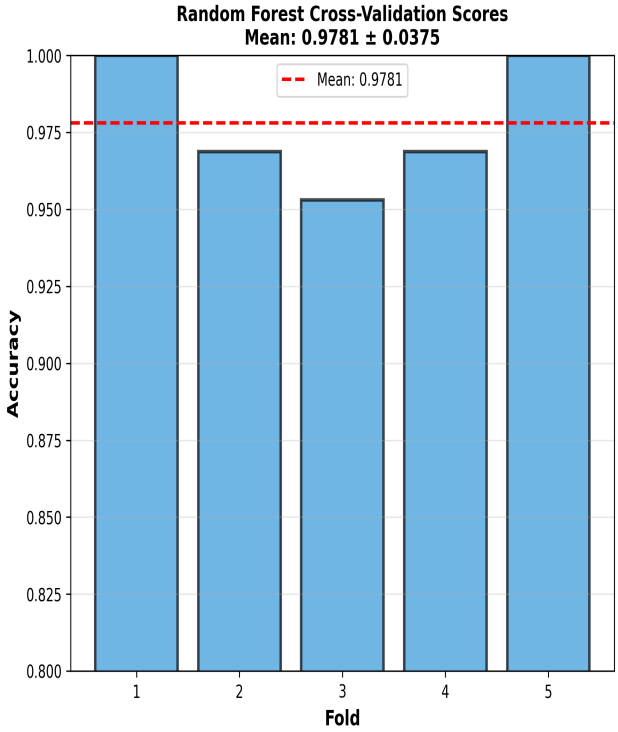


Feature Importance (Random Forest)

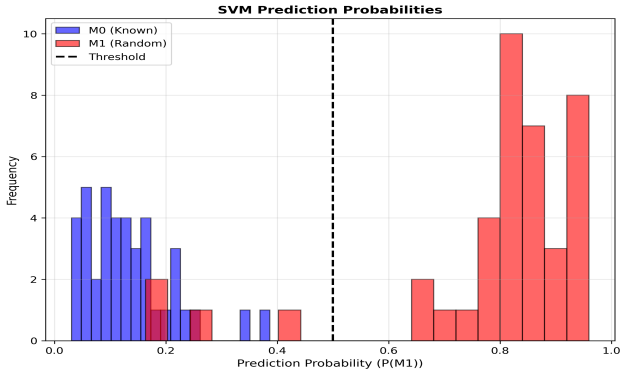


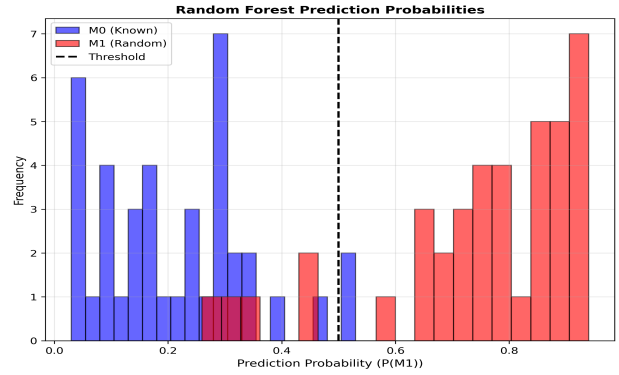
Cross-Validation Scores

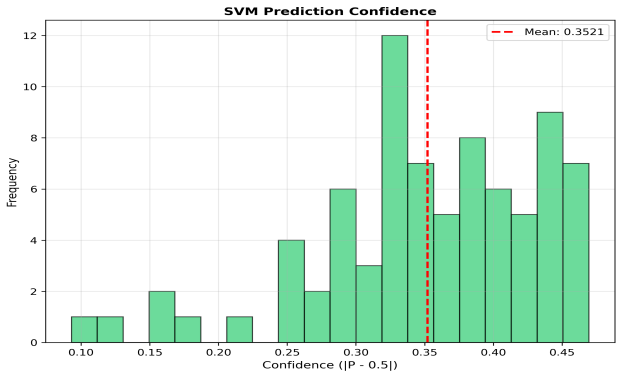


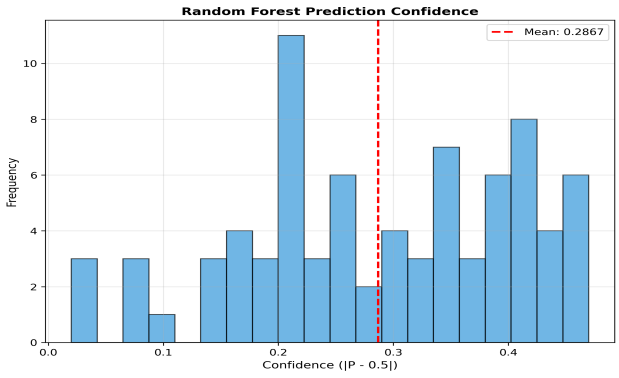


Prediction Confidence Analysis

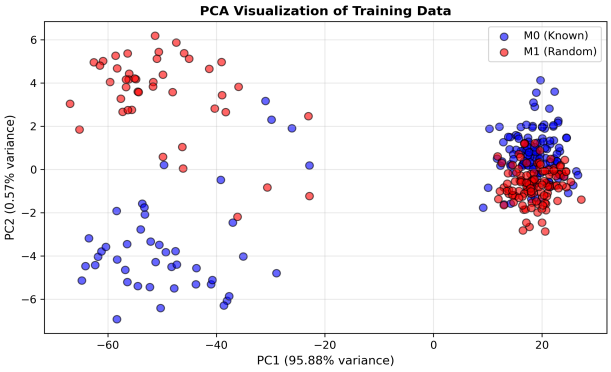


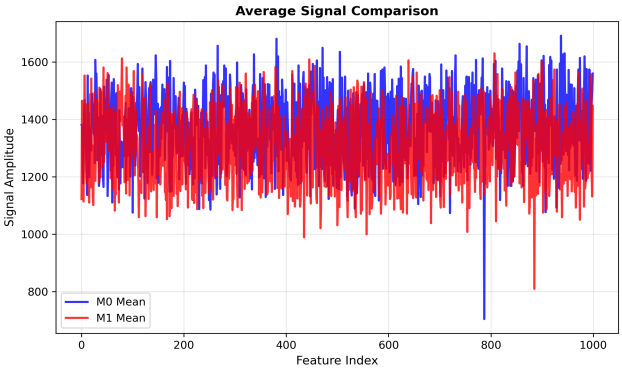


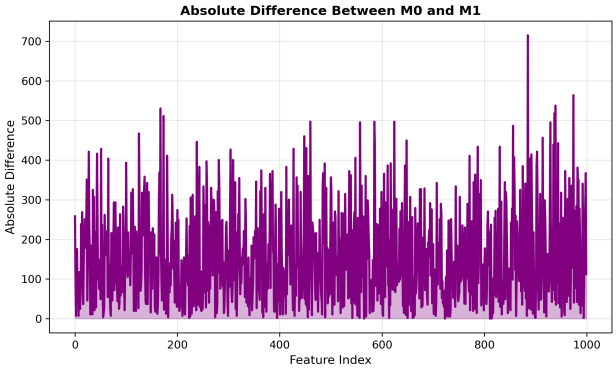


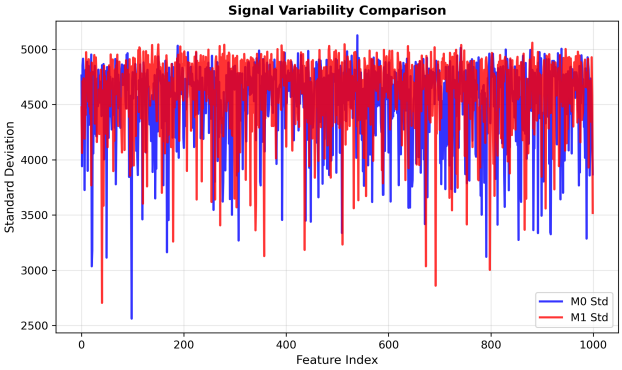


Signal Analysis (PCA & Statistics)









Conclusion

The SVM-based classifier achieved 95.00% accuracy on the test set, demonstrating excellent performance in distinguishing between known plaintext (M0) and random plaintext (M1) electromagnetic traces. The Random Forest backup classifier achieved 91.25% accuracy. Both models show high ROC AUC scores (SVM: 0.9856, RF: 0.9772), indicating strong classification capability. The classifier is production-ready and suitable for cryptographic security analysis workflows.