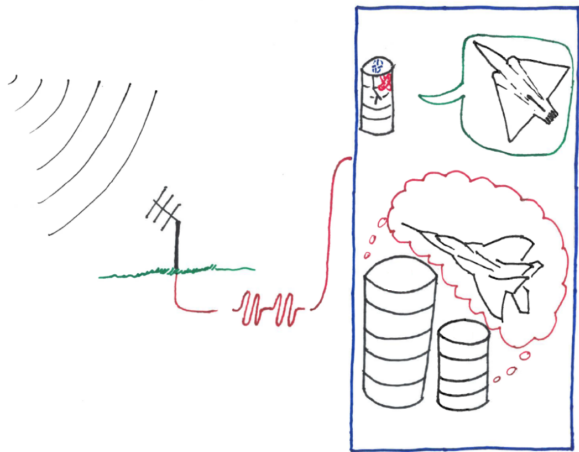




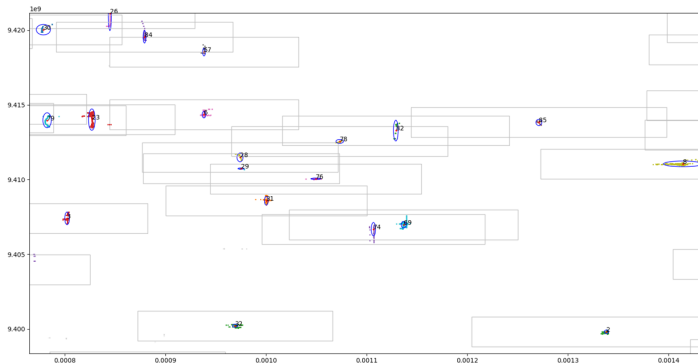
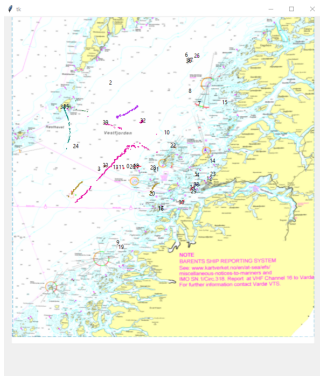
FFI Norwegian Defence
Research Establishment

Private recognition and comparison of radar signatures

Martin Strand



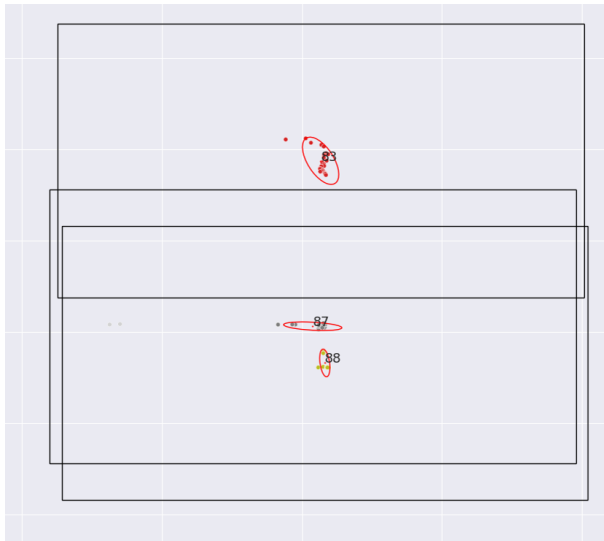
Proxy: Ships between Lofoten and Bodø



Summer students 2023

Their task

1. Start with the ship data, and create reasonable signatures
2. Match signals to signatures using MPC, share the end result
3. If time: Partition the database, match across several sources



MPC for dummies



$$a + b$$



$$a \cdot b$$



$$\frac{a}{b}$$

Mahalanobis distance and CCDF

Assumptions

The RF/PRI samples come from a 2D normal distribution Q around $\mu = (\mu_1, \mu_2)$ with covariance matrix $\Sigma = \begin{pmatrix} \sigma_{11} & \sigma_{12} \\ \sigma_{21} & \sigma_{22} \end{pmatrix}$.

$$D_x = D(x, Q) = \sqrt{(x - \mu)^T \Sigma^{-1} (x - \mu)}$$

Can show:

$$\Sigma = CC^T, \quad C = \begin{pmatrix} l_{11} & 0 \\ l_{21} & l_{22} \end{pmatrix}$$

$$\bar{F}_{\chi^2_2}(D_x^2) = e^{-\|\eta\|_2^2}$$

where $\eta = C^{-1}(x - \mu)$.

Efficient distance computation

Let $y_1 = x_1 - \mu_1$ and $y_2 = x_2 - \mu_2$. Then

$$\Gamma = \sigma_{11} (\sigma_{22}\sigma_{11} - \sigma_{21}^2)$$
$$\Gamma \|\eta\|_2^2 = y_1^2 (\sigma_{22}\sigma_{11} - \sigma_{21}^2) + (y_2^2 \sigma_{11} + 2y_1 y_2 \sigma_{21}) \sigma_{11} + y_1^2 \sigma_{21}^2$$

Summary for humans

We can do hypothesis testing with a single division. Score!

Sorting

MP-SPDZ: Oblivious Radix Sort

- $\mathcal{O}(n \log n)$
- Exponential communication/round behaviour in number of parties

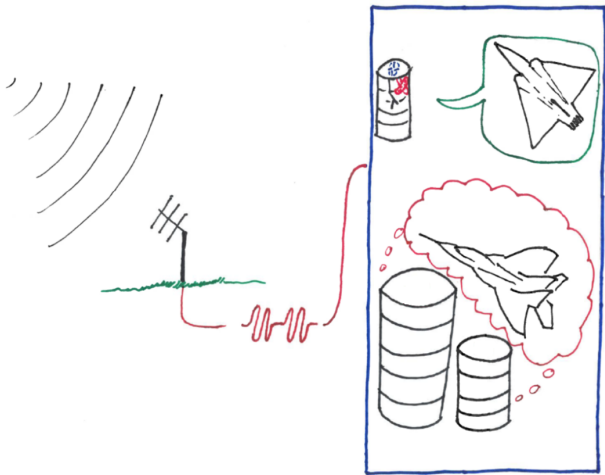
New: Sparse Oblivious Keyword Sort

- $\mathcal{O}(n \log^2 n)$
- Non-exponential in number of parties

Demo time!

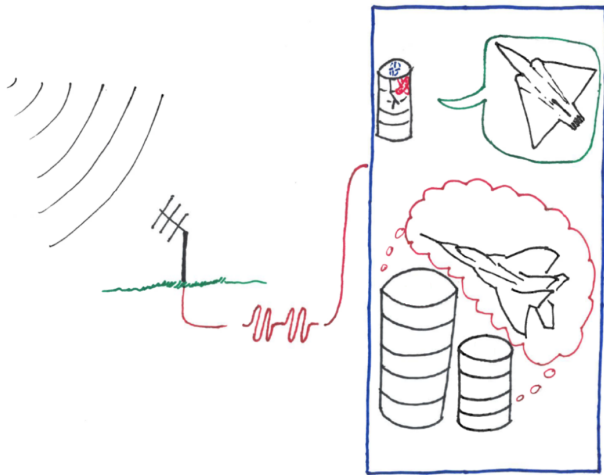
What will we see?

- Two parties
 - One knows the signal
 - One has a database
- Output: Friend/foe identification of the vessel



The next steps

- Some more adjustments
- Optimisation: Currently ~10,000 rounds
- Not production code
- Analyse: What leaks from the process?
- Write it up and submit somewhere!



We're hiring!

What we want

- Must have good MS, preferably PhD
- Must get security clearance
- Formal announcement later this fall

$$P = \mathcal{P}(\{\text{PQC, protocols, MPC, FHE, lightweight, side ch.}\}) \setminus \{\emptyset\}$$
$$\exists I \in P \text{ s.t. } I \cup \{\text{applications}\} \subseteq \text{interests}_{\text{you}}$$

What you get

- Decent amount of autonomy (!)
- Permanent position (!!), paid with real money (!!!)
- Not just publish-publish-publish (!!!!)