

AIを用いたAES暗号に対する新たな攻撃手法

A new attacking method for the AES with AI

岡山大学 野上 保之 日下 卓也 城市 翔 生田 健

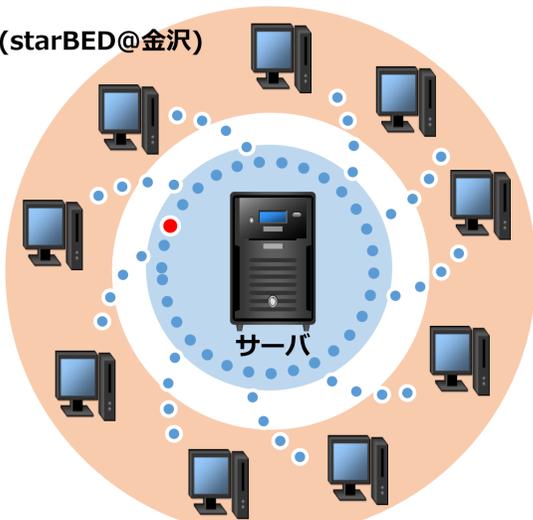
新たな攻撃手法

114bit楕円曲線暗号の攻撃実験

クライアント(starBED@金沢)

各クライアントが膨大な点情報をサーバに送信

同じ点があれば鍵の解読に成功



約3000コアを用いて数ヶ月をかけて鍵を解読

膨大なリソースが必要

AIを用いた鍵の推定

A6C0987BE21
D9FF381A0E7
CB623DE1451
A89EF9D0BE2
F41A33EACC5
65B

01001010
10110100
100011100110
010100110111
010111101001
010100101001

各データ

AIが学習データを元に暗号の鍵を瞬時に予測

少ないリソースで解読可能

Deep Learning によるAES暗号の鍵の推定

学習

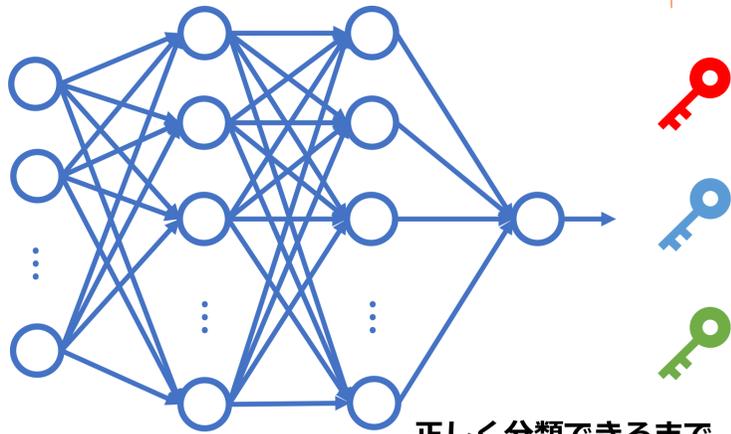
推定



AES波形データ

エラー

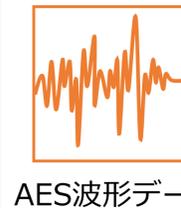
ニューラルネットワーク



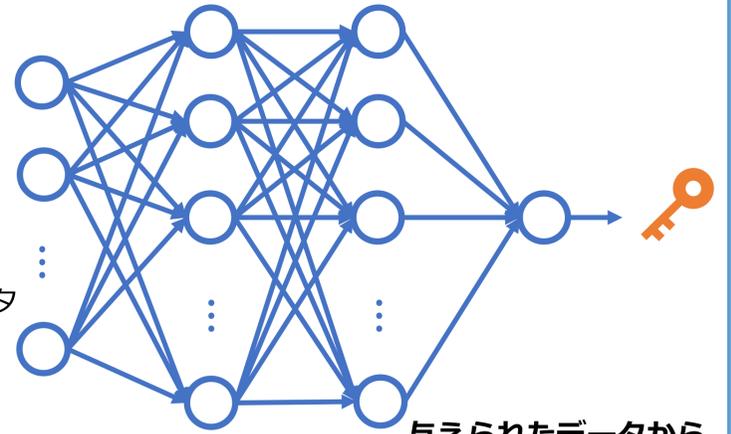
正しく分類できるまでトレーニングを繰り返す



ニューラルネットワーク



AES波形データ



与えられたデータから鍵を予測



今後の展望

GPUを用いた学習の効率化

GPU

大量のデータを複数のプロセッサで同時かつ並列に処理することが可能



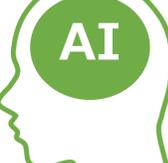
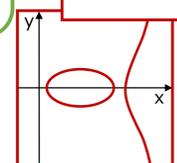
NAVIDA Tesla V100

学習の効率化・高速化

様々な暗号への応用

AIを用いてAES暗号の鍵の解読に成功

328578758
923843829
567659258
432475503
249558304



RSA暗号や楕円曲線暗号なども鍵の解読が可能かどうか検討