- **課題（量子関連）**

　将来、量子計算機が実用化すると、パスワードの候補を試す探索が高速化され、従来より短時間で破られる可能性が高まる。さらにGPU等の並列計算でも、照合（正しいかどうかの判定）が単純だと大量試行が容易になる。したがって「候補を試す回数」だけでなく、「候補1件を検証する処理そのものを重くして、試行単価を上げる」ことが課題である。

- **課題の解決手段**

　パスワード等から、まず大きな二次元のビット格子（0/1のマス目）を作る。次にその格子を、多数ステップにわたって次の2つを組み合わせて複雑に変化させる。毎ステップ、入力に基づく乱数で格子の並び替え（回転・反転・行列による入れ替え等）を行う。

同じく入力に基づき、セルオートマトンの更新ルールを選びながら状態遷移させる。
これにより、少しでも入力が違うと最終結果が大きく変わり、しかも計算・メモリ負荷が高いため、攻撃者が大量試行しにくくなる。

- **作品の紹介**

　本作品は、パスワードをそのまま照合する代わりに、パスワードから「大きなビット模様」を生成し、それを入力依存の並び替えとセルオートマトンで何度も進化させた最終模様（またはそのハッシュ）で本人確認する認証方式である。狙いは、将来の量子計算機やGPUによる高速な総当たりでも、1回の検証が重く、規則性も残りにくい評価関数を作って攻撃コストを押し上げる点にもある。

耐量子セルオートマトン認証方式