urandom

Computer Security Magazine

vol.9

目次

Quantum Covert Lottery meets Grover's algorithm

1 はじめに

"Covert Lottery" とは 2021 年に発表された論文 "*Card-Based Covert Lottery*"[1] で発表されたガチャの 1 つです。これは 2 人プレイヤーの秘密の希望（1 bit）を入力して、もし 2 人の希望が衝突しないのであれば希望通りにし、そうでないならランダムな結果を出力するというプロトコルです。

2 人によるこのプロトコルを量子コンピュータで実装したものを Zenn.dev の記事 [2] にしてから、前回に発行した urandom vol.8 では Covert Lottery を多人数に拡張するために CZ ゲートの多量子ビット版を作るなど基礎的な部分を解説しました。今回の記事ではこの Covert Lottery とグローバーのアルゴリズムについて考えます。

グローバーのアルゴリズム [3] とはショアの素因数分解と並んで量子コンピュータによる加速を代表する有名なアルゴリズムであり、これは N 個の未整列なデータ（配列、リスト）の中からある求めたいデータ（ターゲット）を検索する問題を高速化します。古典コンピュータではこのような問題には平均で $N/2$ 回の検索が必要で、最悪の場合は N 個探すことになります。一方でこのグローバーのアルゴリズムを利用すると約 $\sqrt{N}$ 回[*1]の検索でデータを見つけることができるというものです。グローバーの検索アルゴリズムと Covert Lottery の多人数化には一見するとなんの関係もなさそうですが、最近はこの 2 つを組み合わせることができるのではないかと考えています。

この記事では最初におさらいとして Covert Lottery の性質を解説して、次にグローバーのアルゴリズムについて簡単な例から解説し、やや複雑なものは Qiskit[4] というシミュレーターと Python コードを用いつつ解説します。そしてこの 2 つを使った多人数量子 Covert Lottery の展望と残された課題について述べます。

[*1] "約" となっているのはこのグローバーのアルゴリズムが正しい答えを出力するかどうかが確率的であり、高い確率で $\sqrt{N}$ 回で答えを求められるものの、そうでない可能性があることも考慮してこのような表記にしました。本稿ではこの回数についても議論します。

とある RISC-V の Voltage Fault Injection (C100 版)

1　はじめに

動作中のプロセッサーに供給されている電源電圧をごく短い間変動させ、プロセッサーの挙動がどのように変化するか観察する “Voltage fault injection”（V-FI, VCC glitching）と呼ばれるテスト手法が存在する。時として命令のスキップやデータの変化のような興味深い挙動が観察されることから、V-FI はコンピューターセキュリティにおける関心の対象とされている。

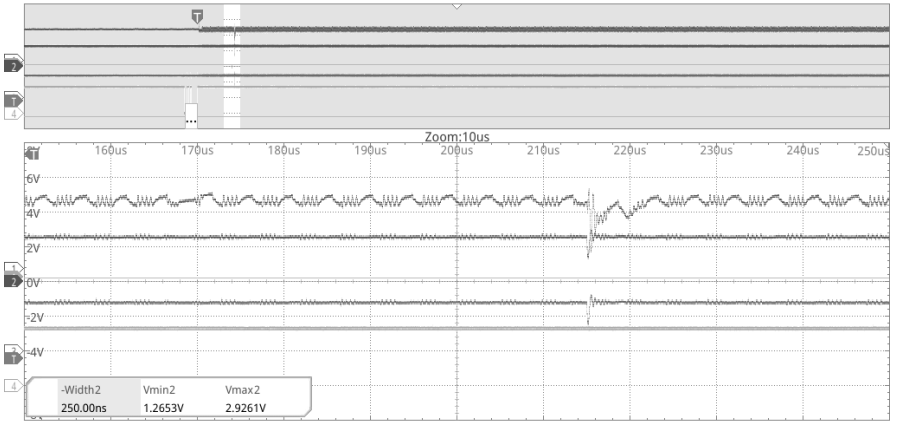

図 1: プロセッサーの電圧を変動させたときのオシロスコープ画像（上 2 本が電流と電圧の測定値）

V-FI は 20 年以上前から研究されているテスト手法であり、V-FI などに対して仕様外挙動が発生しないよう堅牢化されたプロセッサーも一部にあるが、多くのプロセッサーは V-FI に対して何らかの仕様外挙動を示す。最近では、市販の Arm Cortex-M4 プロセッ