An adaptive attack on Wiesner's quantum money

Thomas Gimpel, Marius Gebhardt

Institut für Physik der Universität Augsburg

Reference: Brodutch, A.; Nagaj, D.; Sattath, O.; Unruh, D.
"An adaptive attack on Wiesner's quantum money",
Quantum Information & Computation 16(11&12): 1048-1070 (2016)

Quantum money

- *Goal*: Create money which is impossible to forge
- *Method*: Use quantumsystem
- *No-Cloning Theorem* should prohibit copying

S. Wiesner proposed system with single-qubit memory and single qubit measurement:

- Bank creates public serial number s with private key $k^{(s)} \in \{0, 1, +, -\}^n$
- The Banknote then is $(s, |\$_s\rangle)$ with $|\$_s\rangle = |k_1^{(s)}\rangle \otimes ... \otimes |k_n^{(s)}\rangle$

Quantum Money: Security

- Banknote gets validated by the bank, which measures each qubit in corresponding basis and sends the banknote back after successful validation
- Measuring in the false basis would change the qubit and later Validation would fail
  $\Rightarrow$ Use interaction free measurement
- *Loophole*: Bank returns correctly validated banknote

Elitzur-Vaidman bomb quality tester

- General Idea: Detect some property without disturbing it.
  $\Rightarrow$ e.g. Detect a photon that never interacted with an object.
- Using quantum zeno effect
  $\Rightarrow$ One can be sure about the system's property
- Problem: There might be a light activated bomb
- Principal aim of the algorithm: Reducing the probability of the bomb to detonate but nevertheless gaining information if there is a bomb

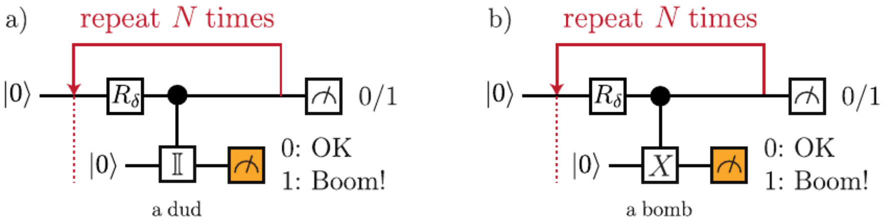

Figure: A quality-testing procedure for bombs: run N rounds and end with a measurement of the first register. a) A dud can't explode, and the first register slowly rotates from $|0\rangle$ to $|1\rangle$. b) With a live bomb, we can really trigger the bomb by flipping the second register to $|1\rangle$. This does not happen often as δ is small, and we are much more likely to measure $|0\rangle$ on the second register. The first register is then also projected back to $|0\rangle$.

After first round:

- Dud: $(\cos\delta\,|0\rangle + \sin\delta\,|1\rangle)\,|0\rangle$
- Bomb: $\cos\delta\,|0\rangle\,|0\rangle + \sin\delta\,|1\rangle\,|1\rangle \Rightarrow$ probability of explosion: $\sin^2\delta$
- No explosion $\Rightarrow$ both registers get projected to $|0\rangle\,|0\rangle$

Probability of no Explosion after N steps:

$$(1-\sin^2\delta)^N \geq 1 - \frac{\pi^2}{4N}; \quad \delta = \frac{\pi}{2N}$$

- This behavior is called *quantum Zeno effect*
- After N steps we measure the first register: $|1\rangle \Rightarrow$ dud, $|0\rangle \Rightarrow$ bomb

Bomb-testing attack on quantum money

- Goal: Find state of i^{th} qubit $|\alpha\rangle$ of quantummoney $|\$\rangle$ without going to jail (changing it)
- Procedure is similar to Elitzur-Vaidman's bomb tester

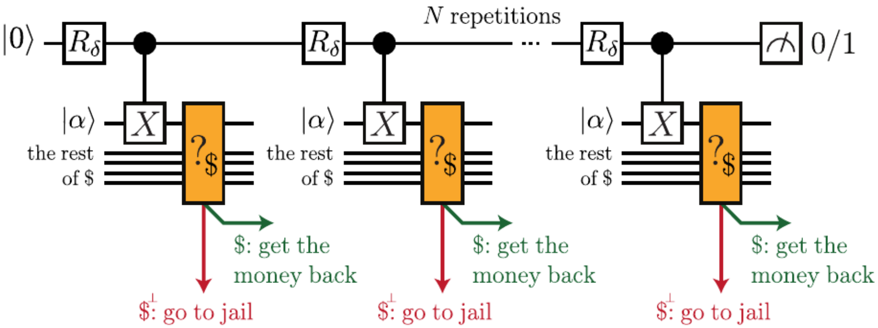

Figure: An adaptive attack on Wiesner's quantum money with a strict testing procedure. We can identify whether the qubit $|\alpha\rangle$ is in the state $|+\rangle$ without going to jail (being detected). If we do not identify it, we can use controlled-$(-X)$ instead to test for $|-\rangle$ If we do not detect it either, we just measure the qubit in the computational basis.

What happens to the four possible states with the X-Operation

- $|0\rangle, |1\rangle$: Flipping maps the states $|0\rangle \leftrightarrow |1\rangle$, this is the "bomb" case
  $\Rightarrow$ Successful validation will keep first register in $|0\rangle$
- $|+\rangle$: Flip does nothing ("Dud" case) $\Rightarrow$ First register will move to $|1\rangle$
- $|-\rangle$: Flip gives minus sign. Initial states is $|0\rangle |-\rangle$
  - First iteration:

$$R_\delta \otimes \mathbb{I} : ((\cos\delta)|0\rangle + (\sin\delta)|1\rangle)|-\rangle$$

$$\mathrm{CNOT} : ((\cos\delta)|0\rangle - (\sin\delta)|1\rangle)|-\rangle$$

    First register is rotated by $-\delta$ compared to $|0\rangle$
  - Second iteration will rotate first register back to $|0\rangle$
    $\Rightarrow$ after even number of iteration fist register is $|0\rangle$

$\Rightarrow$ We can identify if $|\alpha\rangle$ is in the $|+\rangle$ state

- We can test for $|-\rangle$ using the controlled-$(-X)$ operation
- If we can rule out $|+\rangle$ and $|-\rangle$ we can measure in the $\{|0\rangle, |1\rangle\}$ basis
- We can submit a banknote for validation where all qubits are slightly changed
- If we want to have a success rate of $1 - f$ we need $N = \frac{\pi^2 n}{2f}$ verification rounds (n: Number of qubits)

Protective Measurement Attack

- Uses weak interaction between the probe state and the money state with the unitary operator $U = \mathrm{e}^{-\mathrm{i}\delta(\sigma_x \otimes A)}$
- At each step the validation protects the money state by projecting it back to its original state with high probability
- The probe state evolves linear with the weakness parameter δ, whereas the chance of getting caught will be quadratic in δ

Process

- $$|0\rangle|\alpha\rangle \xrightarrow{e^{-i\delta(\sigma_x\otimes A)}} \approx |0\rangle|\alpha\rangle - i\delta|1\rangle A|\alpha\rangle$$
  $$\xrightarrow{\text{bank measures } \{|\alpha\rangle\langle\alpha|, \mathbb{1}-|\alpha\rangle\langle\alpha|\}} \approx \left(e^{-i\delta\langle A\rangle\sigma_x}|0\rangle\right)\otimes|\alpha\rangle$$
  $$\xrightarrow{\text{repeat } N \text{ times}} \approx \left(e^{-ic\langle A\rangle\sigma_x}|0\rangle\right)\otimes|\alpha\rangle$$
  $$\text{with } \delta = \frac{c}{N}$$
- The probe system is now rotated proportional to $\langle A\rangle$
- Then approximate $\langle A\rangle = \langle\alpha|A|\alpha\rangle$ and thus $|\alpha\rangle$

Calculations

- With $A = P - P^{\perp}$,the Taylor series of e^{P} and $P^2 = P$ we get

$$U = \mathrm{e}^{-\mathrm{i}\delta(\sigma_x \otimes A)} = \mathrm{e}^{-\mathrm{i}\delta(\sigma_x \otimes P - \sigma_x \otimes P^{\perp})} = \mathrm{e}^{-\mathrm{i}\delta\sigma_x \otimes P}\mathrm{e}^{\mathrm{i}\delta\sigma_x \otimes P^{\perp}} =$$
$$= (\mathrm{e}^{-\mathrm{i}\delta\sigma_x} \otimes \mathrm{e}^{P})(\mathrm{e}^{\mathrm{i}\delta\sigma_x} \otimes \mathrm{e}^{P^{\perp}}) =$$
$$= \left[\mathrm{e}^{-\mathrm{i}\delta\sigma_x} \otimes (\mathbb{1} + (e-1)P)\right]\left[\mathrm{e}^{\mathrm{i}\delta\sigma_x} \otimes (\mathbb{1} + (e-1)P^{\perp})\right] =$$
$$= \mathrm{e}^{-\mathrm{i}\delta\sigma_x} \otimes P + \mathrm{e}^{\mathrm{i}\delta\sigma_x} \otimes P^{\perp}$$

- $$W\left|\varphi_k\right\rangle = (\mathbb{1} \otimes \langle\alpha|)U\left|\varphi_k\right\rangle\left|\alpha\right\rangle = \sqrt{p_k}\left|\varphi_{k+1}\right\rangle =$$
$$= (\mathbb{1} \otimes \langle\alpha|)(\mathrm{e}^{-\mathrm{i}\delta\sigma_x} \otimes P + \mathrm{e}^{\mathrm{i}\delta\sigma_x} \otimes P^{\perp})(\left|\varphi_k\right\rangle \otimes \left|\alpha\right\rangle) =$$
$$= (\mathbb{1} \otimes \langle\alpha|)(\mathrm{e}^{-\mathrm{i}\delta\sigma_x}\left|\varphi_k\right\rangle P\left|\alpha\right\rangle + \mathrm{e}^{\mathrm{i}\delta\sigma_x}\left|\varphi_k\right\rangle P^{\perp}\left|\alpha\right\rangle) =$$
$$= \langle\alpha|P|\alpha\rangle\,\mathrm{e}^{-\mathrm{i}\delta\sigma_x}\left|\varphi_k\right\rangle + \langle\alpha|P^{\perp}|\alpha\rangle\,\mathrm{e}^{\mathrm{i}\delta\sigma_x}\left|\varphi_k\right\rangle$$

Calculations

- $$W\left|\varphi_k\right\rangle = \langle\alpha|P|\alpha\rangle\, e^{-i\delta\sigma_x}\left|\varphi_k\right\rangle + \langle\alpha|P^{\perp}|\alpha\rangle\, e^{i\delta\sigma_x}\left|\varphi_k\right\rangle \Rightarrow$$
  $$W = \langle\alpha|P|\alpha\rangle\, e^{-i\delta\sigma_x} + \langle\alpha|P^{\perp}|\alpha\rangle\, e^{i\delta\sigma_x} =$$
  $$= \langle\alpha|P|\alpha\rangle\left(\cos\delta\mathbb{1} - i\sin\delta\sigma_x\right) + \langle\alpha|P^{\perp}|\alpha\rangle\left(\cos\delta\mathbb{1} + i\sin\delta\sigma_x\right) =$$
  $$= \cos\delta\mathbb{1}\,\langle\alpha|P + P^{\perp}|\alpha\rangle - i\sin\delta\,\langle\alpha|P - P^{\perp}|\alpha\rangle =$$
  $$= \cos\delta\mathbb{1} - i\sin\delta\,\langle A\rangle\,\sigma_x$$
- $$\lambda_{\mp} = \cos\delta \mp i\,\langle A\rangle\sin\delta$$
  $$\Rightarrow \text{ eigenstates: } \quad \left|+\right\rangle, \left|-\right\rangle$$

Calculations

- $$W^N \left|\varphi_0\right\rangle = \prod_{k=0}^{N-1} \sqrt{p_k} \left|\varphi_N\right\rangle = \sqrt{p_{\text{pass}}} \left|\varphi_N\right\rangle$$

- $$\lambda_{\mp}^N = (\underbrace{\cos\delta \mp i\sin\delta \left\langle A\right\rangle}_{1+i\langle A\rangle\delta-\frac{\delta^2}{2}-\frac{1}{6}i\langle A\rangle\delta^3})^N = (\underbrace{e^{\mp i\delta\langle A\rangle}}_{1+i\langle A\rangle\delta-\frac{\langle A\rangle^2\delta^2}{2}-\frac{1}{6}i\langle A\rangle\delta^3} + \mathcal{O}(\delta^2))^N =$$
$$= \left(e^{\mp i\delta\langle A\rangle}(1+\mathcal{O}(\delta^2))\right)^N = e^{\mp iN\delta\langle A\rangle}(1 + N\times\mathcal{O}(\delta^2)) =$$
$$= e^{\mp ic\langle A\rangle} + \mathcal{O}(N^{-1})$$

Calculations

- Look at a new Matrix: $\begin{pmatrix} \cos(c\langle A\rangle) & -\mathrm{i}\sin(c\langle A\rangle) \\ -\mathrm{i}\sin(c\langle A\rangle) & \cos(c\langle A\rangle) \end{pmatrix}$

  $\Rightarrow$ eigenvalues: $\cos(c\langle A\rangle) \mp \mathrm{i}\sin(c\langle A\rangle) = \mathrm{e}^{\mp \mathrm{i}c\langle A\rangle}$
- $$W^N = \mathrm{e}^{-\mathrm{i}c\langle A\rangle\sigma_x} + \mathcal{O}(\frac{1}{N}) \quad \text{(rotation with phase shift)}$$
- $$\sqrt{p_{\text{pass}}}\,|\varphi_N\rangle = \mathrm{e}^{-\mathrm{i}c\langle A\rangle\sigma_x}|\varphi_0\rangle + \mathcal{O}\left(\frac{1}{N}\right)|\tilde{\varphi}\rangle$$
- $$\Rightarrow p_{\text{pass}} = 1 - \mathcal{O}\left(\frac{1}{N}\right)$$
- $$|\varphi_N\rangle = \mathrm{e}^{-\mathrm{i}c\langle A\rangle\sigma_x}|\varphi_0\rangle + \mathcal{O}\left(\frac{1}{N}\right)|\varphi\prime\rangle =$$
  $$= \cos\left(c\langle A\rangle\right)|0\rangle - \mathrm{i}\sin\left(c\langle A\rangle\right)|1\rangle + \mathcal{O}\left(\frac{1}{N}\right)|\varphi\prime\rangle$$

Approximating $\langle A\rangle$ and thus $|\alpha\rangle$

- After N validation rounds with weak coupling ($c = \frac{\pi}{8}$):

$$|\varphi_N\rangle = \cos\left(\frac{\pi}{8}\langle A\rangle\right)|0\rangle - i\sin\left(\frac{\pi}{8}\langle A\rangle\right)|1\rangle + \mathcal{O}\left(\frac{1}{N}\right)|\tilde{\varphi}\rangle$$

- Estimate $\langle A\rangle$ by measuring the probe state in the σ_y basis:

$$\bar{p}_{y+} = \frac{1}{2}\left[1 - \sin\left(\frac{\pi}{4}\langle A\rangle\right)\right] + O\left(\frac{1}{N}\right)$$

- Repeat estimation $m \ll N$ times to get:

$$\left|\langle A\rangle - \frac{4}{\pi}\arcsin\left(1 - 2p_y^{(m)}\right)\right| \leq \nu + O\left(\frac{1}{N}\right)$$

- Overall failure probability is $p_{\text{fail}} = \mathcal{O}\left(\frac{m}{N}\right)$

Example: the four Wiesner money states

- Choose $A = \sigma_x$, $c = \frac{\pi}{2}$ and $|\varphi_0\rangle = |0\rangle$
- $\langle 0|\sigma_x|0\rangle = \langle 1|\sigma_x|1\rangle = 0$ and $\langle +|\sigma_x|+\rangle = -\langle -|\sigma_x|-\rangle = 1$
- Thus if $|\alpha\rangle$ was initially $|+\rangle$ or $|-\rangle$, the final probe state will be $W^N |0\rangle = \mp \mathrm{i} |1\rangle$
- If $|\alpha\rangle$ was $|0\rangle$ or $|1\rangle$, the probe state will remain close to $|0\rangle$
- By measuring the final probe state $|\varphi_N\rangle$ we can identify the basis of the money state, which allows us to measure the money state $|\alpha\rangle$ in that basis directly

Comparison of the two attacks

- BT-attack does not work for general unknown states or if the range of states is continuous
- PM-attack does not have this problem, but in general only estimates the money state (however modifications like in our example can be used to identify a state instead of estimating it)
- In the processes suggested by this paper the BT-attack does not have an advantage over the PM-attack in terms of resources, but neither methods are optimized (might be an advantage for the BT-attack in the future)