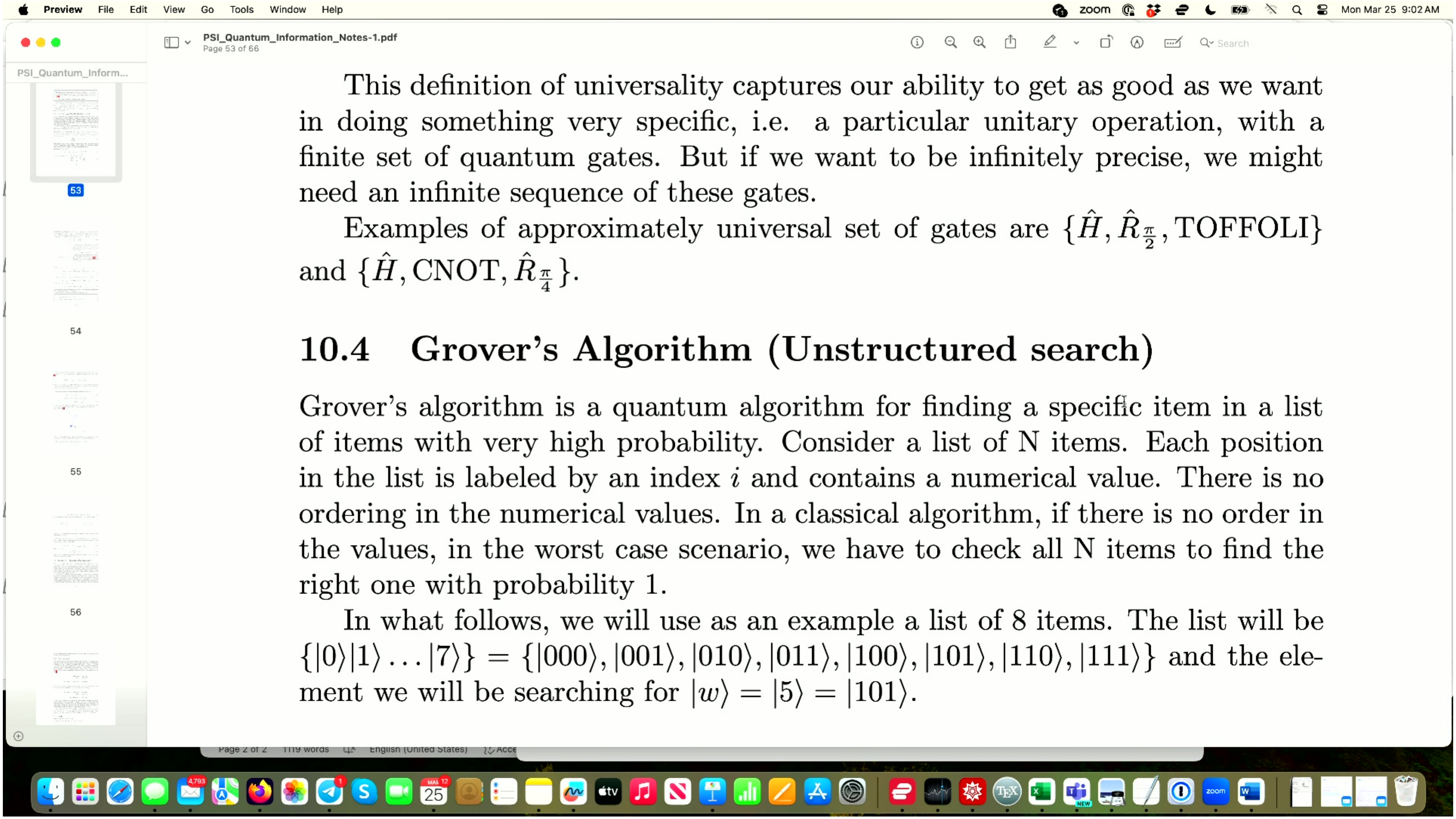
Title: Quantum Information Lecture

Speakers: Eduardo Martin-Martinez

Collection: Quantum Information 2023/24

Date: March 25, 2024 - 9:00 AM

URL: https://pirsa.org/24030061


Preview File Edit View Go Tools Window Help
Mon Mar 25 9:02 AM
PSI_Quantum_Information_Notes-1.pdf
Page 53 of 66
PSI_Quantum_Inform...
53
54
55
56
Search

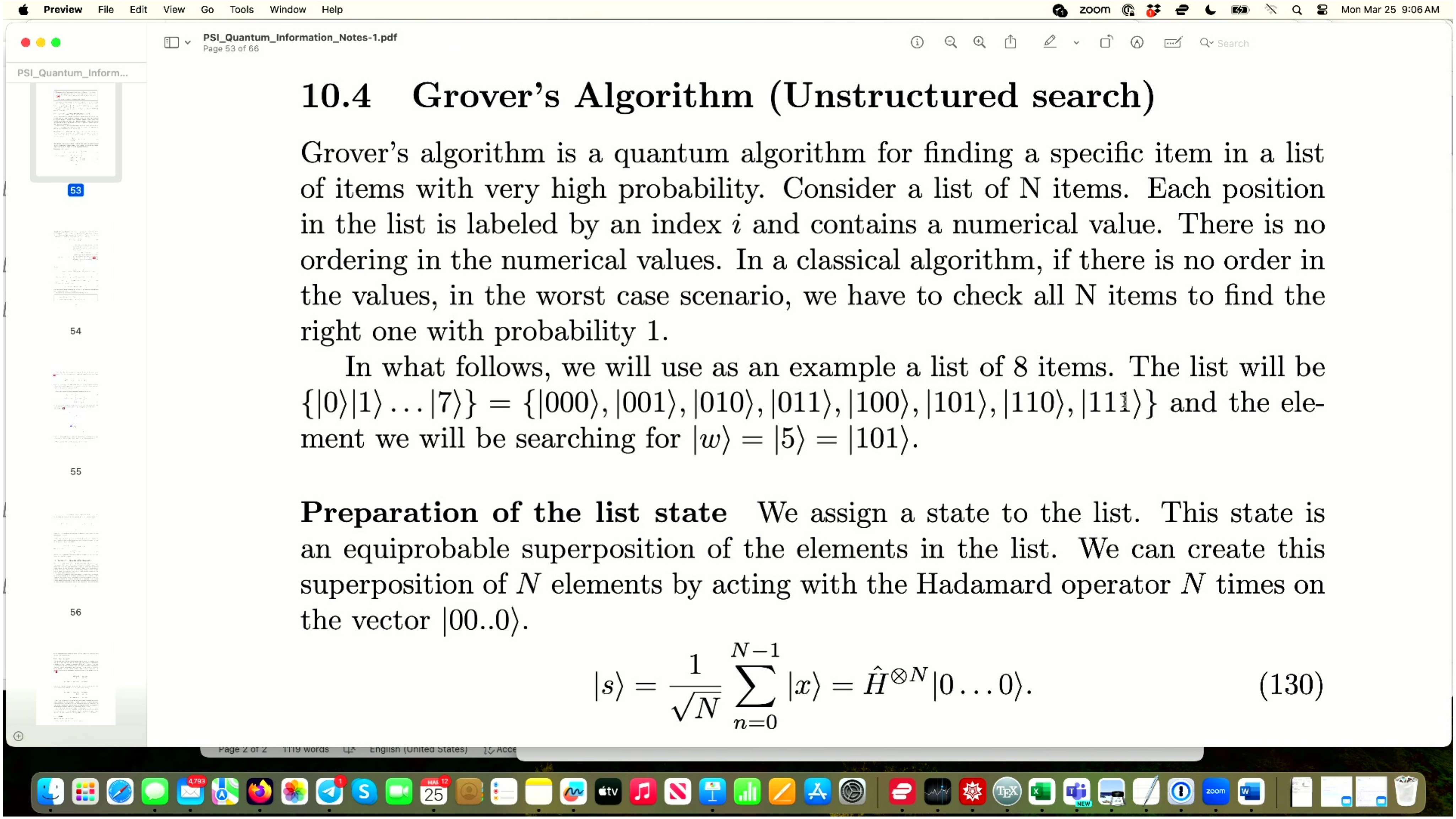
This definition of universality captures our ability to get as good as we want in doing something very specific, i.e. a particular unitary operation, with a finite set of quantum gates. But if we want to be infinitely precise, we might need an infinite sequence of these gates.

Examples of approximately universal set of gates are $\{\hat{H}, \hat{R}_{\frac{\pi}{2}}, \text{TOFFOLI}\}$ and $\{\hat{H}, \text{CNOT}, \hat{R}_{\frac{\pi}{4}}\}$.

10.4 Grover's Algorithm (Unstructured search)

Grover's algorithm is a quantum algorithm for finding a specific item in a list of items with very high probability. Consider a list of N items. Each position in the list is labeled by an index i and contains a numerical value. There is no ordering in the numerical values. In a classical algorithm, if there is no order in the values, in the worst case scenario, we have to check all N items to find the right one with probability 1.

In what follows, we will use as an example a list of 8 items. The list will be $\{|0\rangle|1\rangle \ldots |7\rangle\} = \{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle\}$ and the element we will be searching for $|w\rangle = |5\rangle = |101\rangle$.


Preview File Edit View Go Tools Window Help
Mon Mar 25 9:06 AM
PSI_Quantum_Information_Notes-1.pdf
Page 53 of 66
PSI_Quantum_Inform...
53
54
55
56

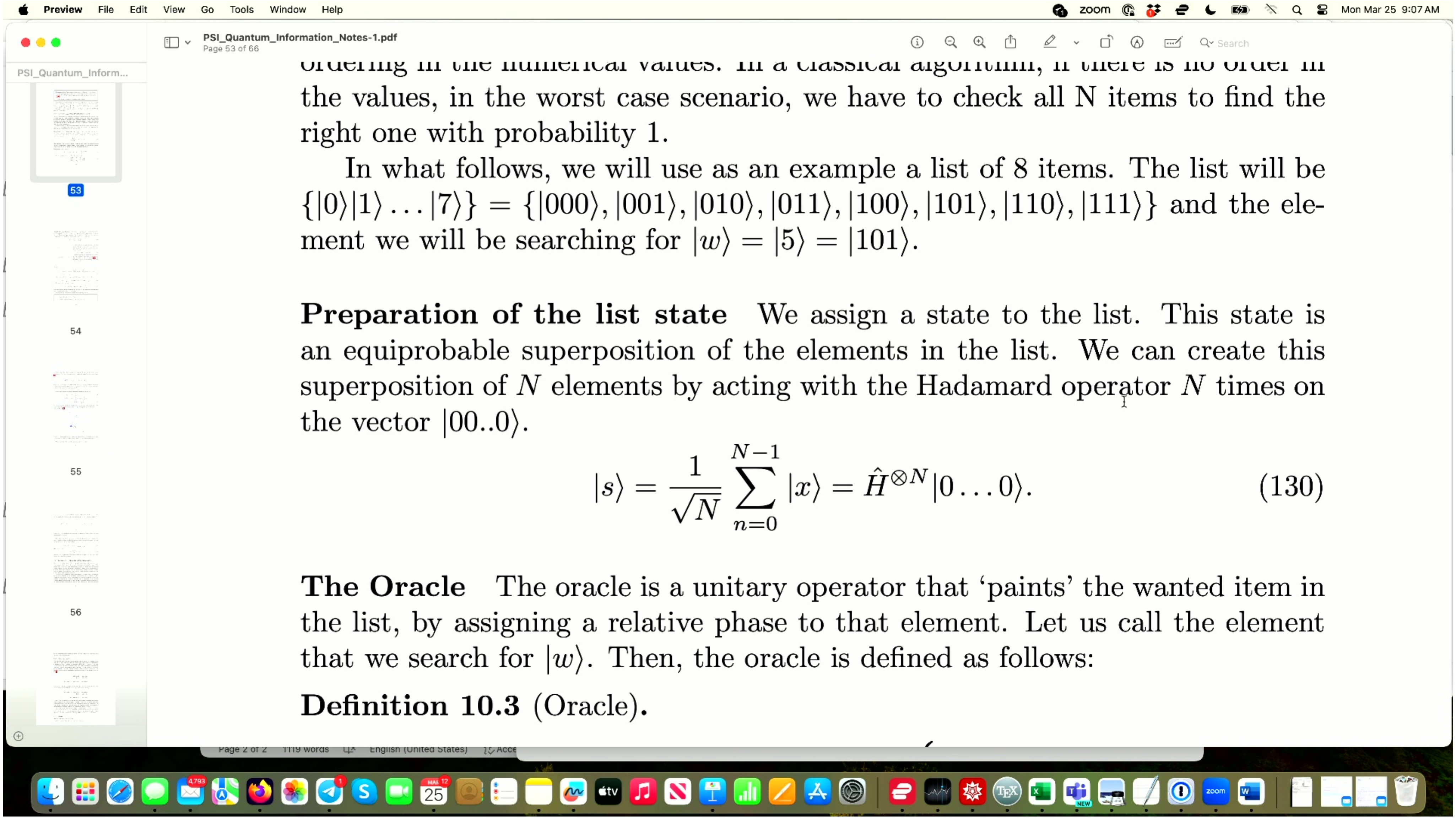
10.4 Grover's Algorithm (Unstructured search)

Grover's algorithm is a quantum algorithm for finding a specific item in a list of items with very high probability. Consider a list of N items. Each position in the list is labeled by an index i and contains a numerical value. There is no ordering in the numerical values. In a classical algorithm, if there is no order in the values, in the worst case scenario, we have to check all N items to find the right one with probability 1.

In what follows, we will use as an example a list of 8 items. The list will be $\{|0\rangle|1\rangle \ldots |7\rangle\} = \{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle\}$ and the element we will be searching for $|w\rangle = |5\rangle = |101\rangle$.

Preparation of the list state We assign a state to the list. This state is an equiprobable superposition of the elements in the list. We can create this superposition of N elements by acting with the Hadamard operator N times on the vector $|00..0\rangle$.

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} |x\rangle = \hat{H}^{\otimes N} |0 \ldots 0\rangle. \qquad (130)$$



ordering in the numerical values. In a classical algorithm, if there is no order in the values, in the worst case scenario, we have to check all N items to find the right one with probability 1.

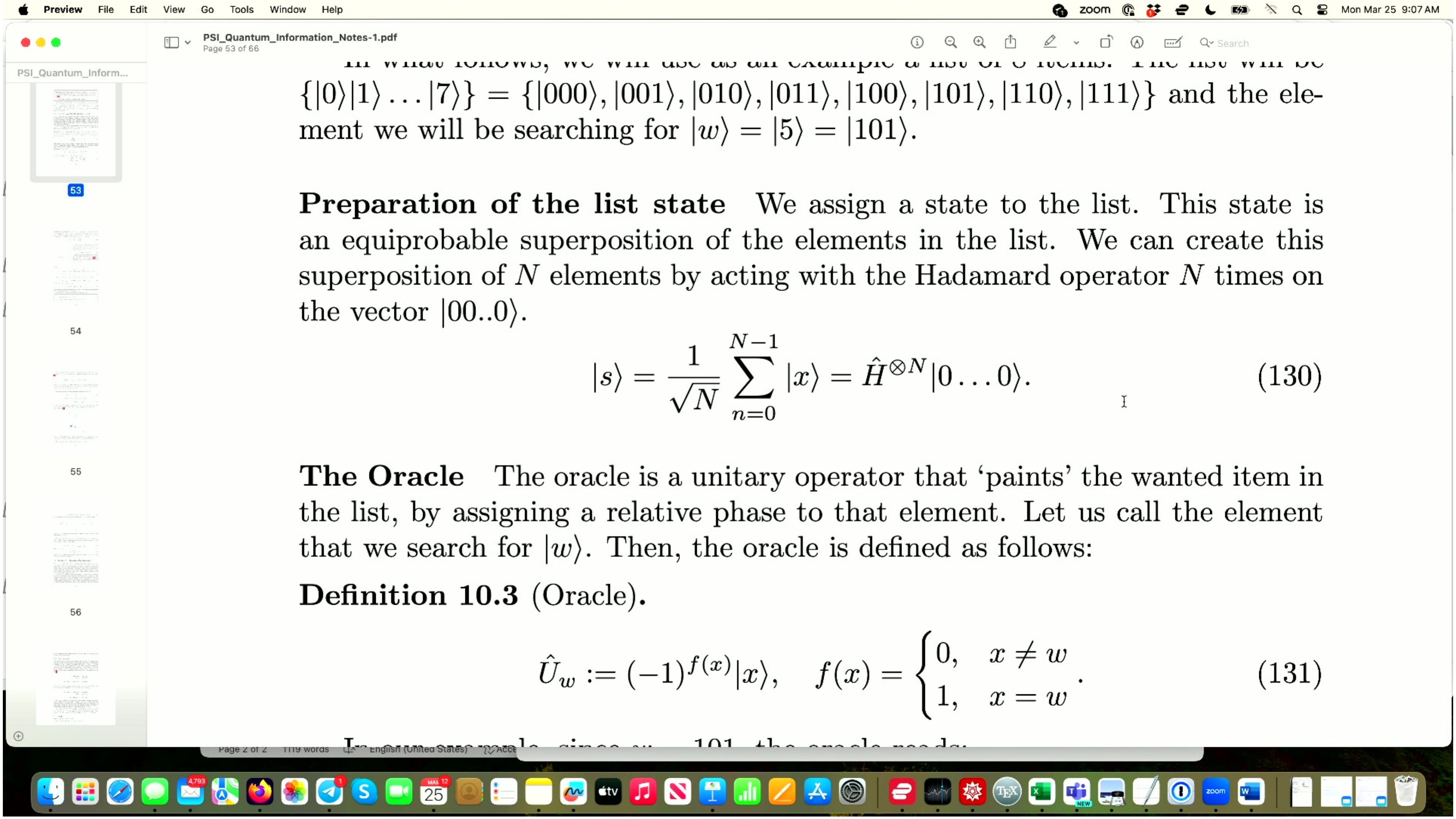
In what follows, we will use as an example a list of 8 items. The list will be $\{|0\rangle|1\rangle\ldots|7\rangle\} = \{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle\}$ and the element we will be searching for $|w\rangle = |5\rangle = |101\rangle$.

Preparation of the list state We assign a state to the list. This state is an equiprobable superposition of the elements in the list. We can create this superposition of N elements by acting with the Hadamard operator N times on the vector $|00..0\rangle$.

$$|s\rangle = \frac{1}{\sqrt{N}}\sum_{n=0}^{N-1}|x\rangle = \hat{H}^{\otimes N}|0\ldots0\rangle. \tag{130}$$

The Oracle The oracle is a unitary operator that 'paints' the wanted item in the list, by assigning a relative phase to that element. Let us call the element that we search for $|w\rangle$. Then, the oracle is defined as follows:

Definition 10.3 (Oracle).


Preview File Edit View Go Tools Window Help
Mon Mar 25 9:07 AM
PSI_Quantum_Information_Notes-1.pdf
Page 53 of 66
PSI_Quantum_Inform...
53
54
55
56

In what follows, we will use as an example a list of 8 items. The list will be $\{|0\rangle|1\rangle\ldots|7\rangle\} = \{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle\}$ and the element we will be searching for $|w\rangle = |5\rangle = |101\rangle$.

Preparation of the list state We assign a state to the list. This state is an equiprobable superposition of the elements in the list. We can create this superposition of N elements by acting with the Hadamard operator N times on the vector $|00..0\rangle$.

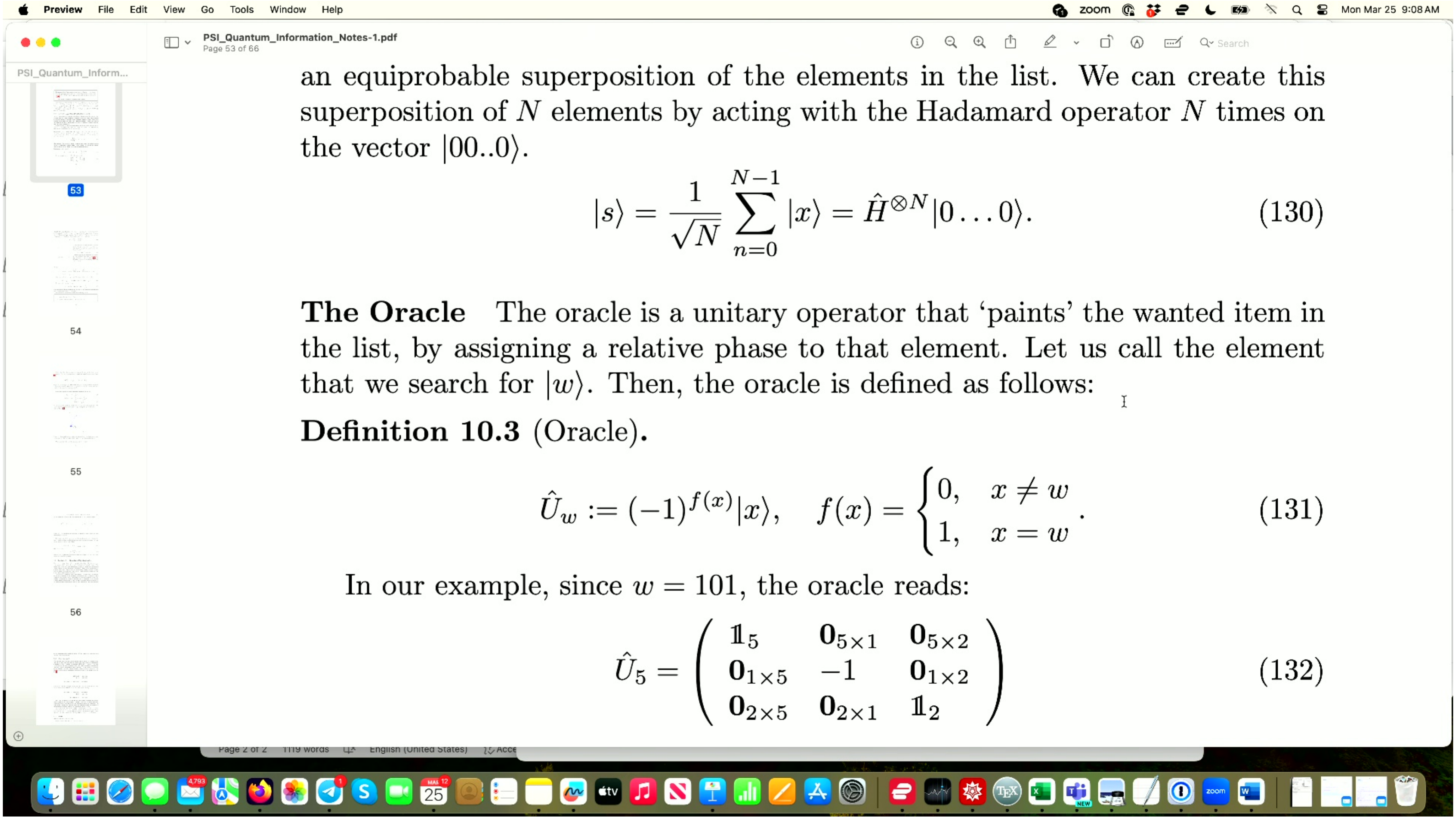
$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} |x\rangle = \hat{H}^{\otimes N}|0\ldots0\rangle. \tag{130}$$

The Oracle The oracle is a unitary operator that 'paints' the wanted item in the list, by assigning a relative phase to that element. Let us call the element that we search for $|w\rangle$. Then, the oracle is defined as follows:

Definition 10.3 (Oracle).

$$\hat{U}_w := (-1)^{f(x)}|x\rangle, \quad f(x) = \begin{cases} 0, & x \neq w \\ 1, & x = w \end{cases}. \tag{131}$$

In our example, since $w = 101$, the oracle reads:



Preview File Edit View Go Tools Window Help
zoom
Mon Mar 25 9:08 AM
PSI_Quantum_Information_Notes-1.pdf
Page 53 of 66
Search
PSI_Quantum_Inform...
53
54
55
56
Page 2 of 2 1119 words English (United States)

an equiprobable superposition of the elements in the list. We can create this superposition of N elements by acting with the Hadamard operator N times on the vector $|00..0\rangle$.

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} |x\rangle = \hat{H}^{\otimes N} |0 \dots 0\rangle. \tag{130}$$

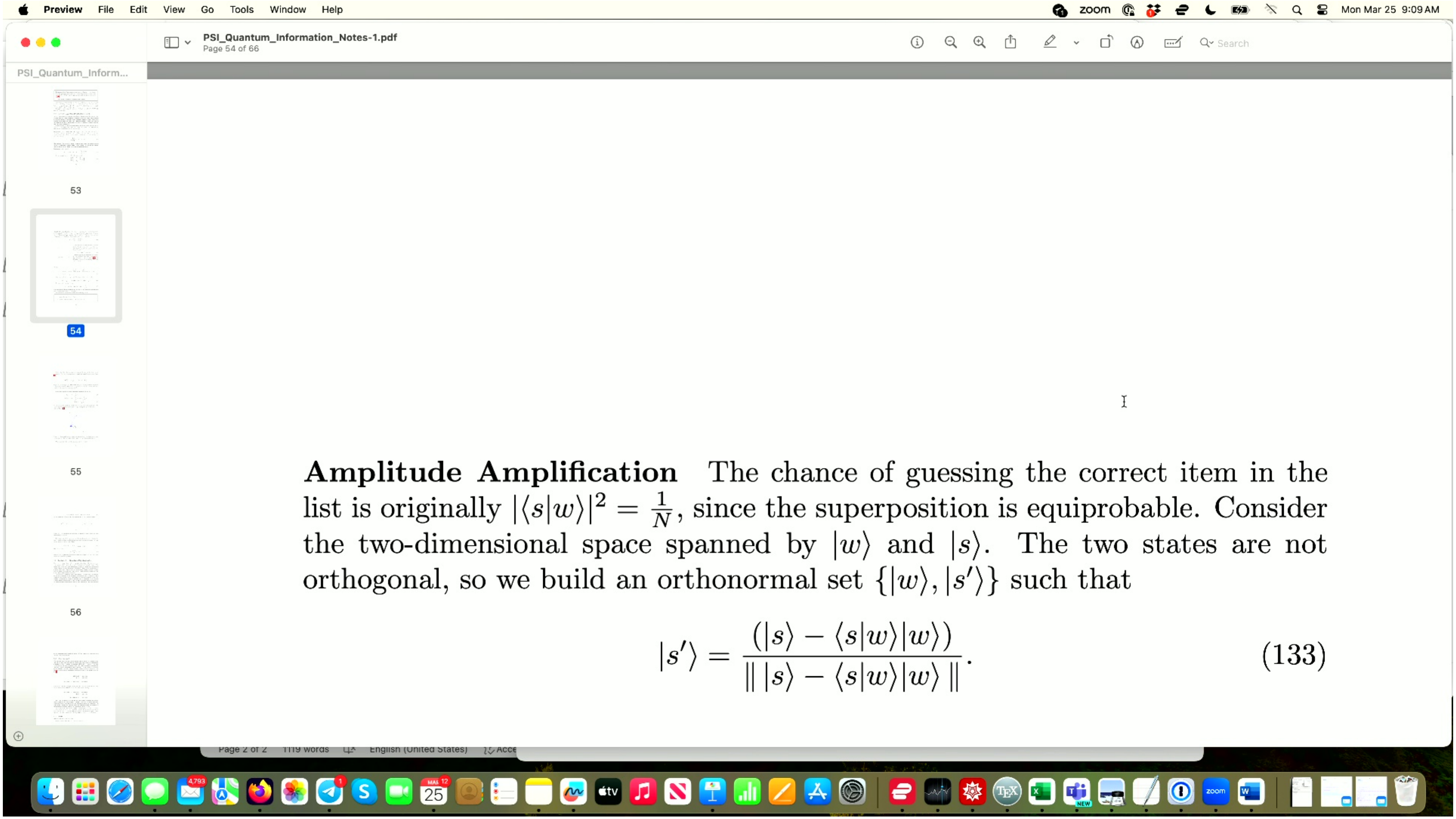
The Oracle The oracle is a unitary operator that 'paints' the wanted item in the list, by assigning a relative phase to that element. Let us call the element that we search for $|w\rangle$. Then, the oracle is defined as follows:

Definition 10.3 (Oracle)**.**

$$\hat{U}_w := (-1)^{f(x)} |x\rangle, \quad f(x) = \begin{cases} 0, & x \neq w \\ 1, & x = w \end{cases}. \tag{131}$$

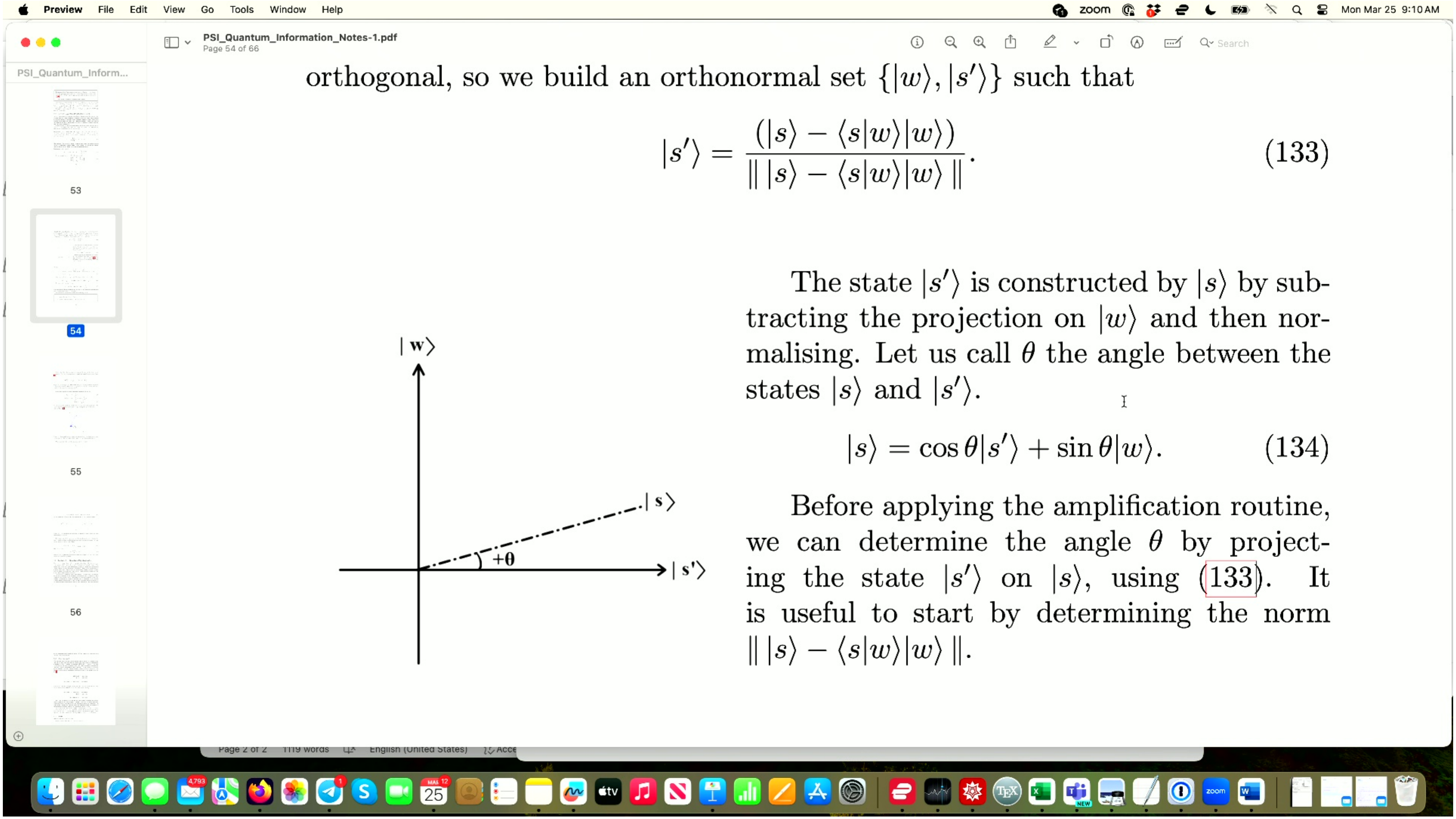
In our example, since $w = 101$, the oracle reads:

$$\hat{U}_5 = \begin{pmatrix} \mathbb{1}_5 & \mathbf{0}_{5\times 1} & \mathbf{0}_{5\times 2} \\ \mathbf{0}_{1\times 5} & -1 & \mathbf{0}_{1\times 2} \\ \mathbf{0}_{2\times 5} & \mathbf{0}_{2\times 1} & \mathbb{1}_2 \end{pmatrix} \tag{132}$$



Amplitude Amplification The chance of guessing the correct item in the list is originally $|\langle s|w\rangle|^2 = \frac{1}{N}$, since the superposition is equiprobable. Consider the two-dimensional space spanned by $|w\rangle$ and $|s\rangle$. The two states are not orthogonal, so we build an orthonormal set $\{|w\rangle, |s'\rangle\}$ such that

$$|s'\rangle = \frac{(|s\rangle - \langle s|w\rangle|w\rangle)}{\| \, |s\rangle - \langle s|w\rangle|w\rangle \, \|}. \qquad (133)$$



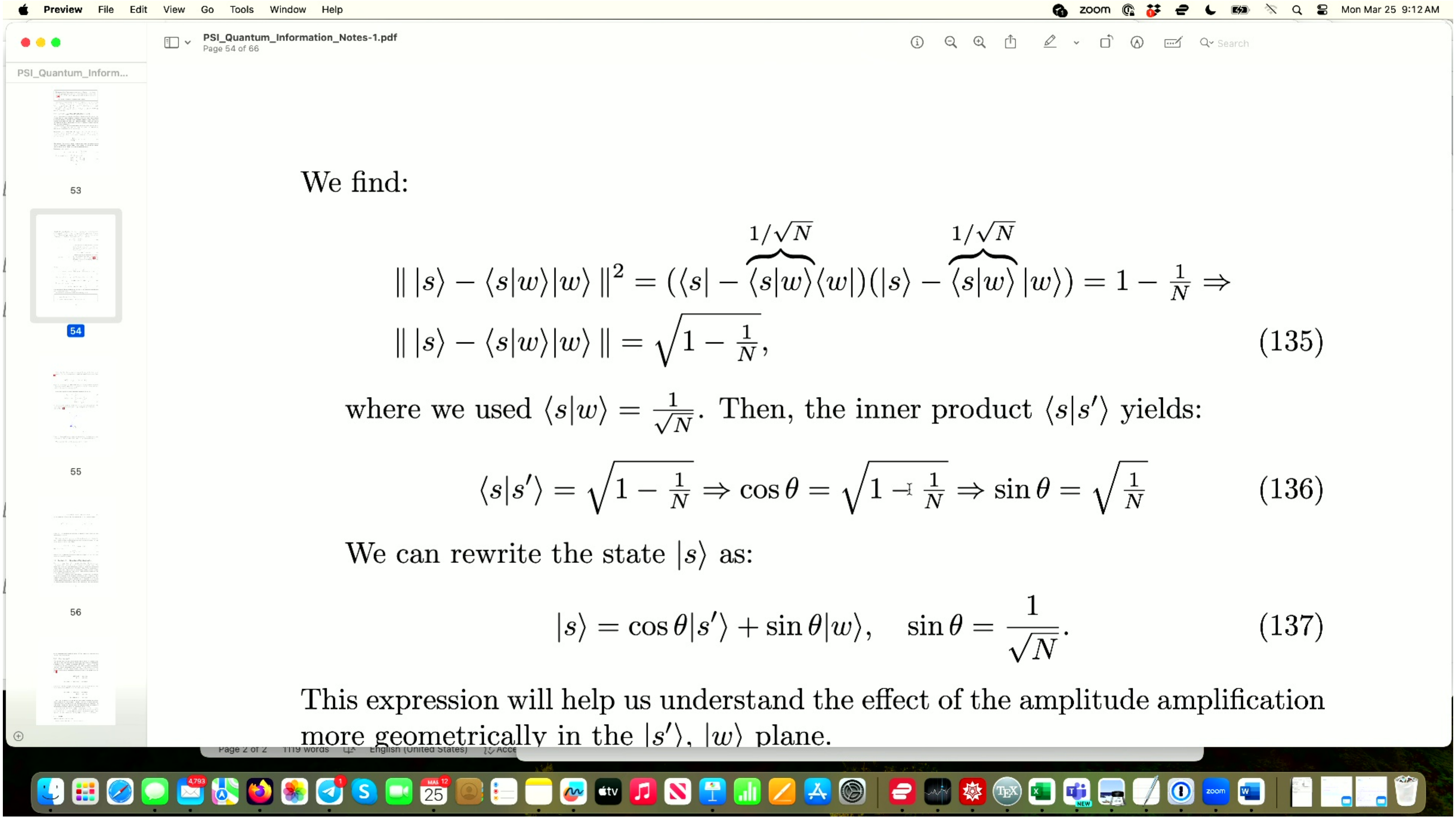
orthogonal, so we build an orthonormal set $\{|w\rangle, |s'\rangle\}$ such that

$$|s'\rangle = \frac{(|s\rangle - \langle s|w\rangle|w\rangle)}{\|\,|s\rangle - \langle s|w\rangle|w\rangle\,\|}. \qquad (133)$$

The state $|s'\rangle$ is constructed by $|s\rangle$ by subtracting the projection on $|w\rangle$ and then normalising. Let us call θ the angle between the states $|s\rangle$ and $|s'\rangle$.

$$|s\rangle = \cos\theta|s'\rangle + \sin\theta|w\rangle. \qquad (134)$$

Before applying the amplification routine, we can determine the angle θ by projecting the state $|s'\rangle$ on $|s\rangle$, using (133). It is useful to start by determining the norm $\|\,|s\rangle - \langle s|w\rangle|w\rangle\,\|$.


Preview File Edit View Go Tools Window Help
Mon Mar 25 9:12 AM
PSI_Quantum_Information_Notes-1.pdf
Page 54 of 66
PSI_Quantum_Inform...
53
54
55
56

We find:

$$\|\,|s\rangle - \langle s|w\rangle|w\rangle\,\|^2 = (\langle s| - \overbrace{\langle s|w\rangle}^{1/\sqrt{N}}\langle w|)(|s\rangle - \overbrace{\langle s|w\rangle}^{1/\sqrt{N}}|w\rangle) = 1 - \frac{1}{N} \Rightarrow$$

$$\|\,|s\rangle - \langle s|w\rangle|w\rangle\,\| = \sqrt{1-\frac{1}{N}}, \qquad (135)$$

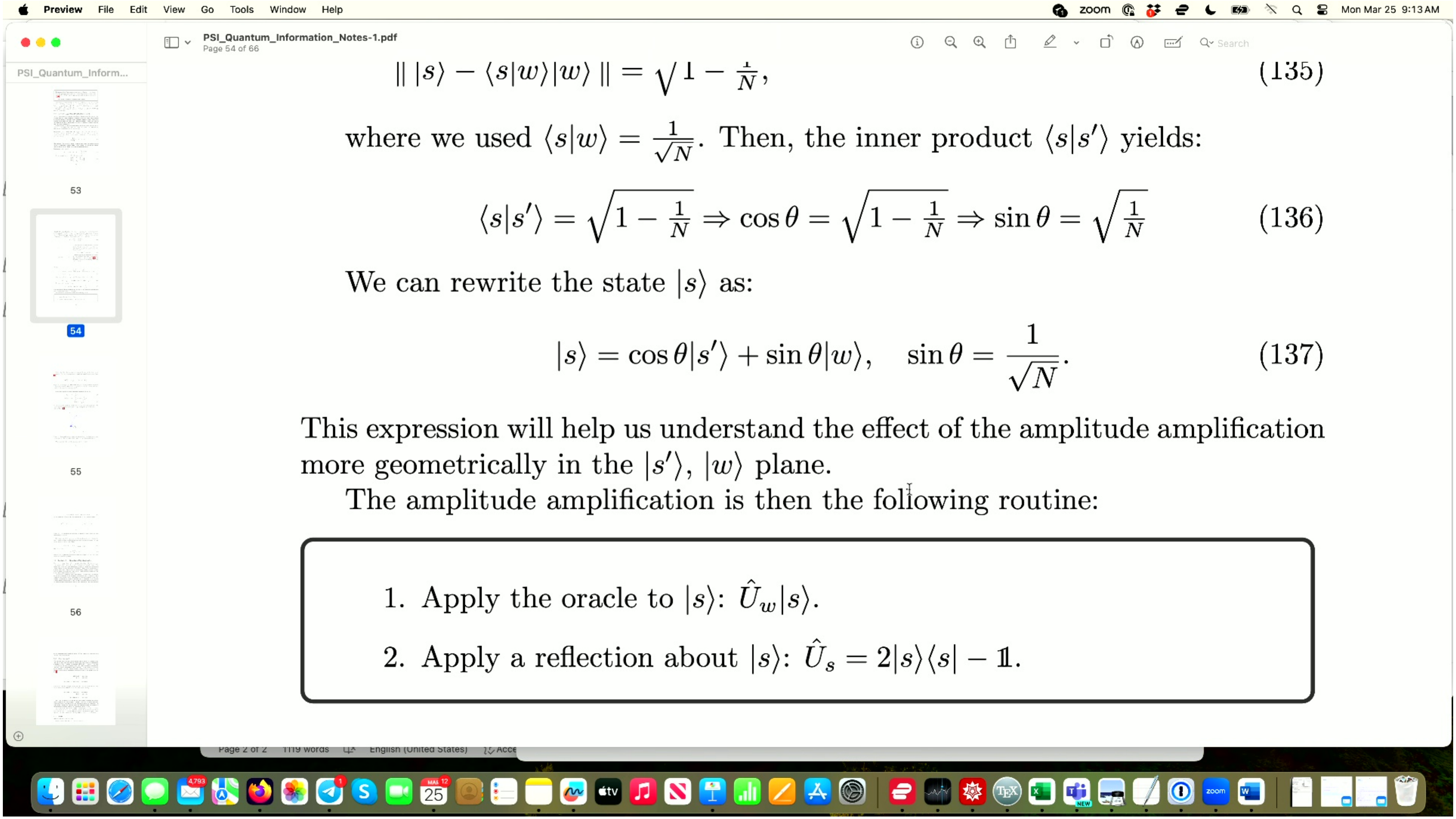
where we used $\langle s|w\rangle = \frac{1}{\sqrt{N}}$. Then, the inner product $\langle s|s'\rangle$ yields:

$$\langle s|s'\rangle = \sqrt{1-\frac{1}{N}} \Rightarrow \cos\theta = \sqrt{1-\frac{1}{N}} \Rightarrow \sin\theta = \sqrt{\frac{1}{N}} \qquad (136)$$

We can rewrite the state $|s\rangle$ as:

$$|s\rangle = \cos\theta|s'\rangle + \sin\theta|w\rangle, \quad \sin\theta = \frac{1}{\sqrt{N}}. \qquad (137)$$

This expression will help us understand the effect of the amplitude amplification more geometrically in the $|s'\rangle$, $|w\rangle$ plane.



$$\| \, |s\rangle - \langle s|w\rangle |w\rangle \, \| = \sqrt{1 - \frac{1}{N}}, \tag{135}$$

where we used $\langle s|w\rangle = \frac{1}{\sqrt{N}}$. Then, the inner product $\langle s|s'\rangle$ yields:

$$\langle s|s'\rangle = \sqrt{1 - \frac{1}{N}} \Rightarrow \cos\theta = \sqrt{1 - \frac{1}{N}} \Rightarrow \sin\theta = \sqrt{\frac{1}{N}} \tag{136}$$

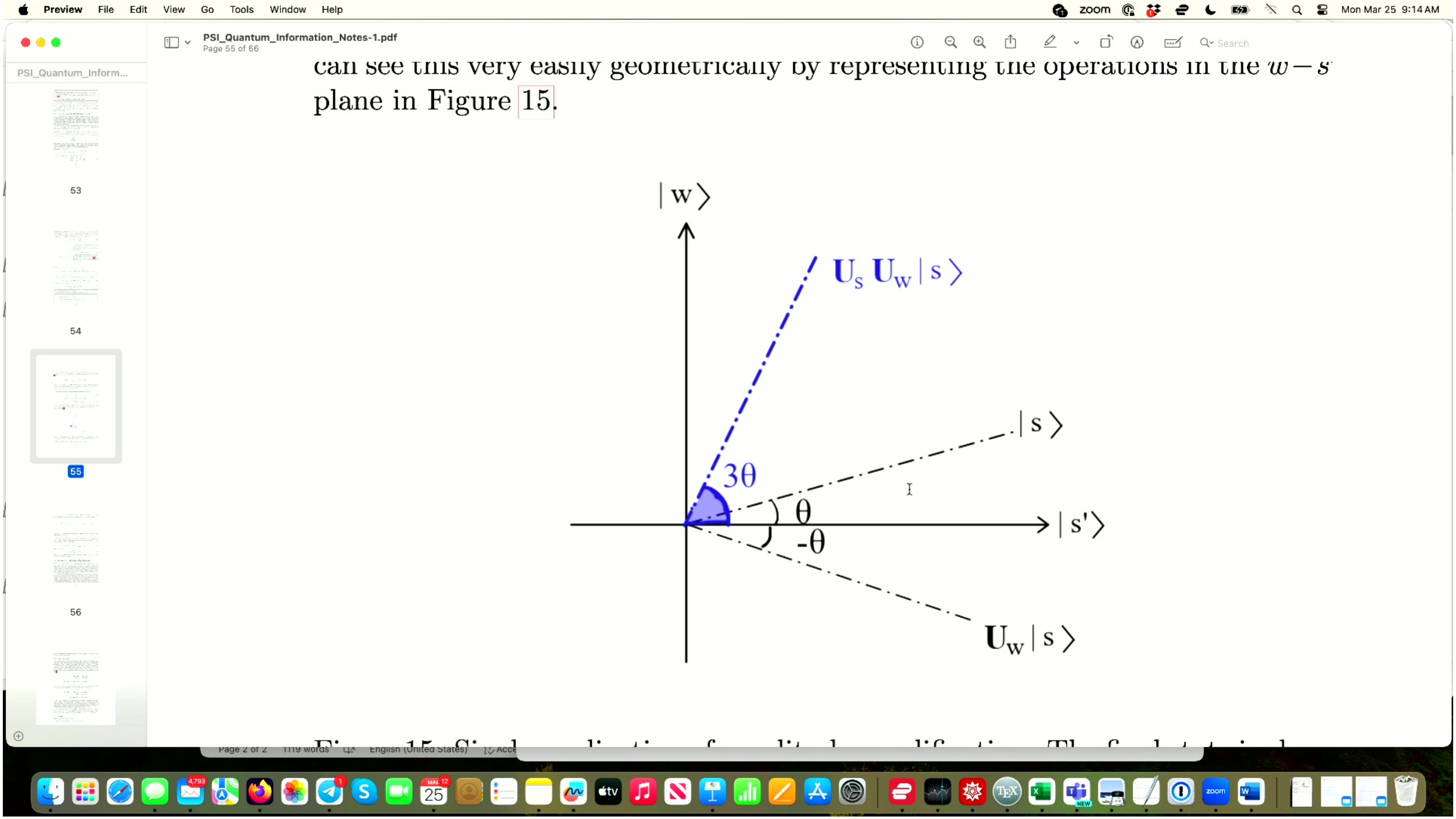
We can rewrite the state $|s\rangle$ as:

$$|s\rangle = \cos\theta|s'\rangle + \sin\theta|w\rangle, \quad \sin\theta = \frac{1}{\sqrt{N}}. \tag{137}$$

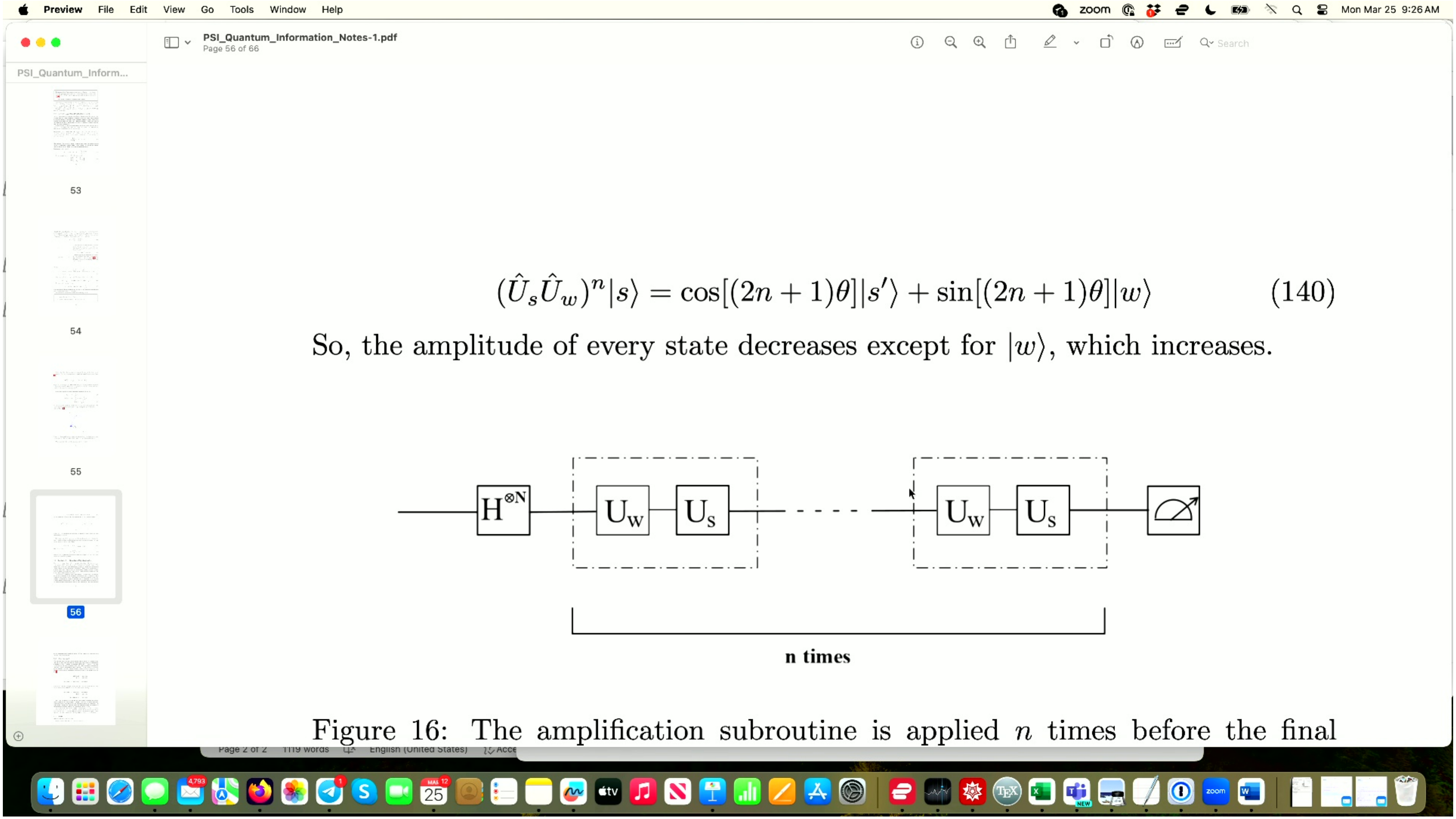
This expression will help us understand the effect of the amplitude amplification more geometrically in the $|s'\rangle$, $|w\rangle$ plane.

The amplitude amplification is then the following routine:

1. Apply the oracle to $|s\rangle$: $\hat{U}_w|s\rangle$.
2. Apply a reflection about $|s\rangle$: $\hat{U}_s = 2|s\rangle\langle s| - \mathbb{1}$.



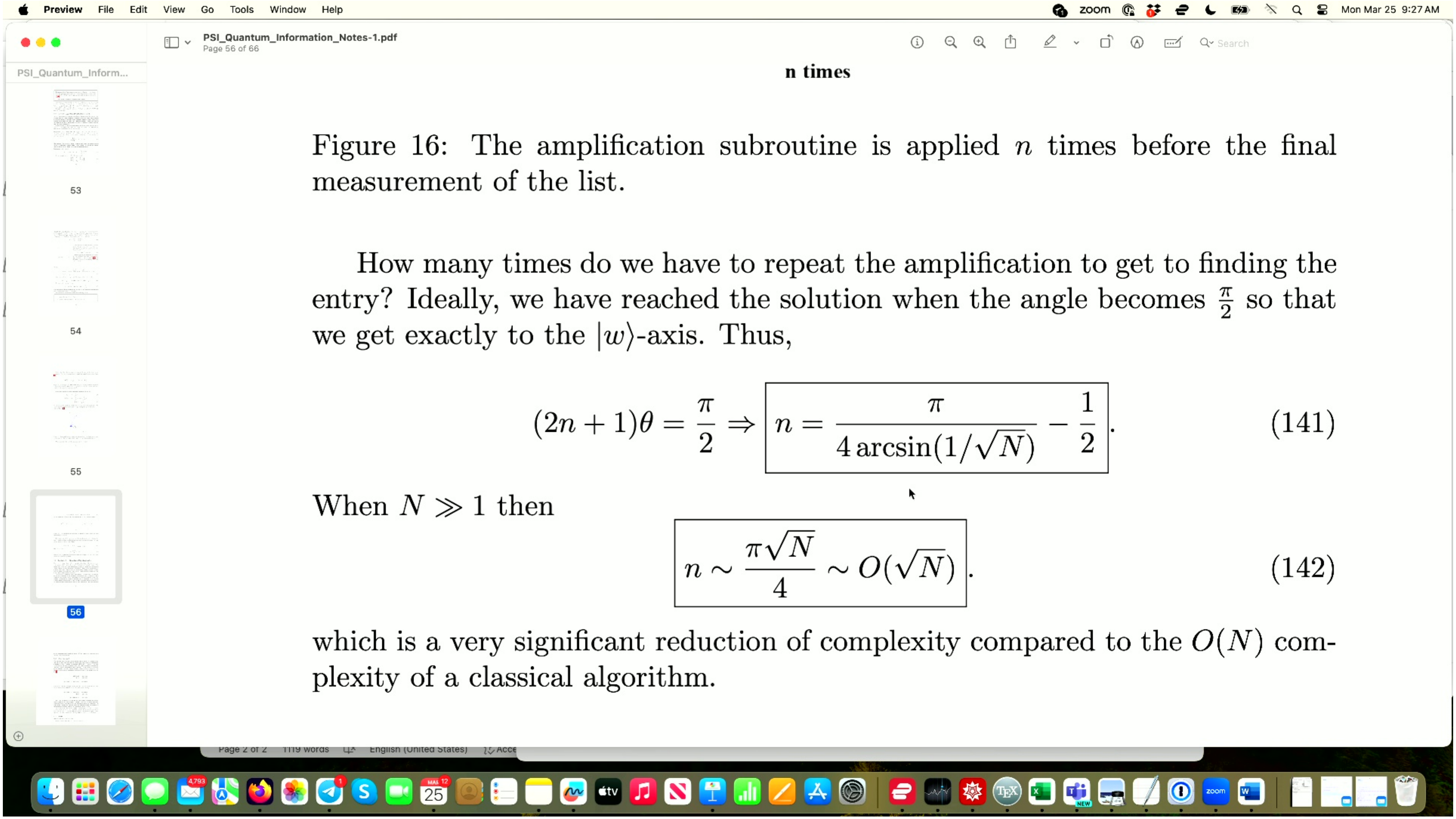
can see this very easily geometrically by representing the operations in the $w - s$ plane in Figure 15.


Preview File Edit View Go Tools Window Help
zoom
Mon Mar 25 9:26 AM
PSI_Quantum_Information_Notes-1.pdf
Page 56 of 66
Search
PSI_Quantum_Inform...
53
54
55
56
$H^{\otimes N}$
U_w
U_s
U_w
U_s
n times
Page 2 of 2 1119 words English (United States)

$$(\hat{U}_s\hat{U}_w)^n|s\rangle = \cos[(2n+1)\theta]|s'\rangle + \sin[(2n+1)\theta]|w\rangle \tag{140}$$

So, the amplitude of every state decreases except for $|w\rangle$, which increases.

Figure 16: The amplification subroutine is applied n times before the final



n times

Figure 16: The amplification subroutine is applied n times before the final measurement of the list.

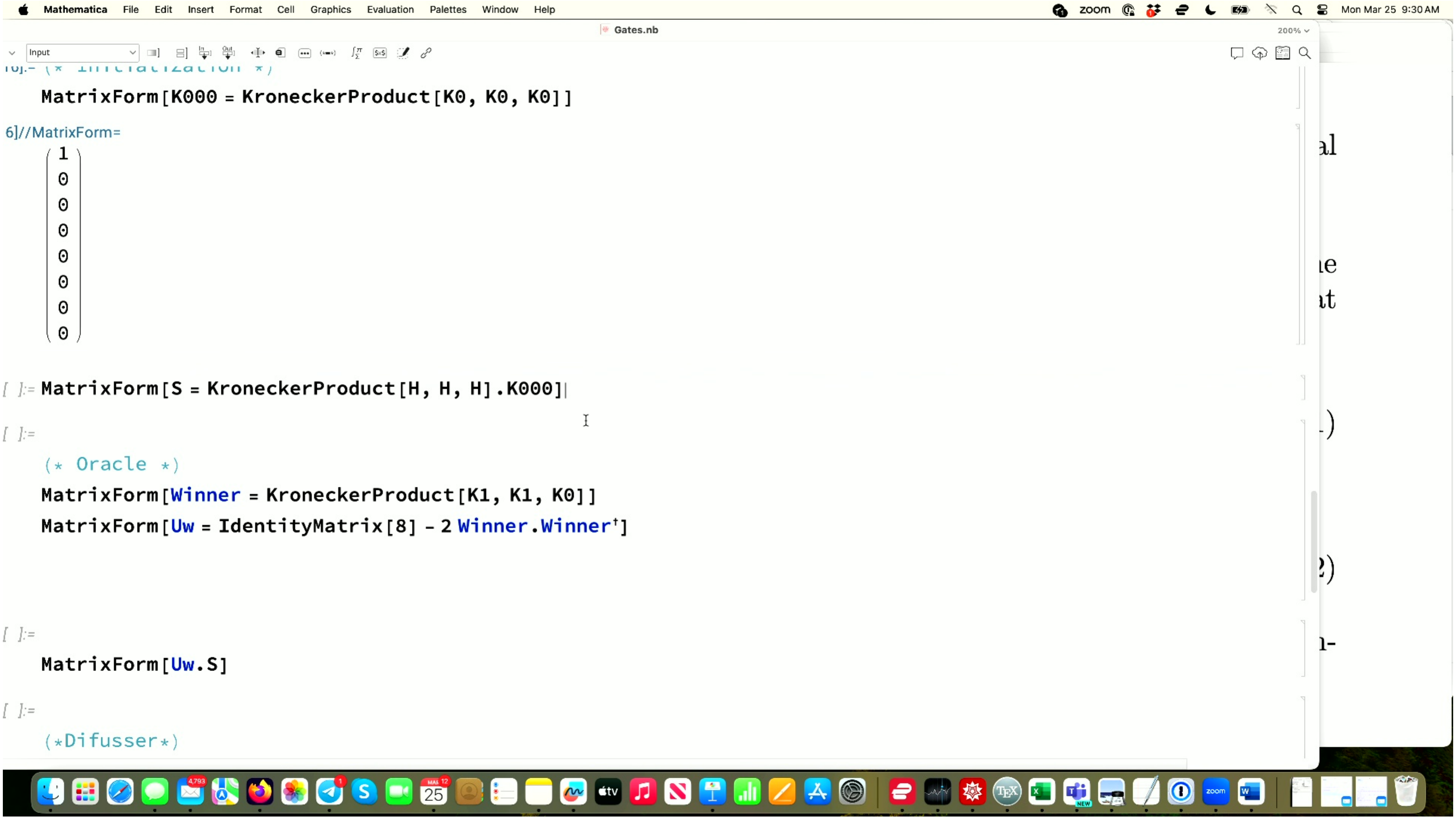
How many times do we have to repeat the amplification to get to finding the entry? Ideally, we have reached the solution when the angle becomes $\frac{\pi}{2}$ so that we get exactly to the $|w\rangle$-axis. Thus,

$$(2n+1)\theta = \frac{\pi}{2} \Rightarrow \boxed{n = \frac{\pi}{4\arcsin(1/\sqrt{N})} - \frac{1}{2}}. \tag{141}$$

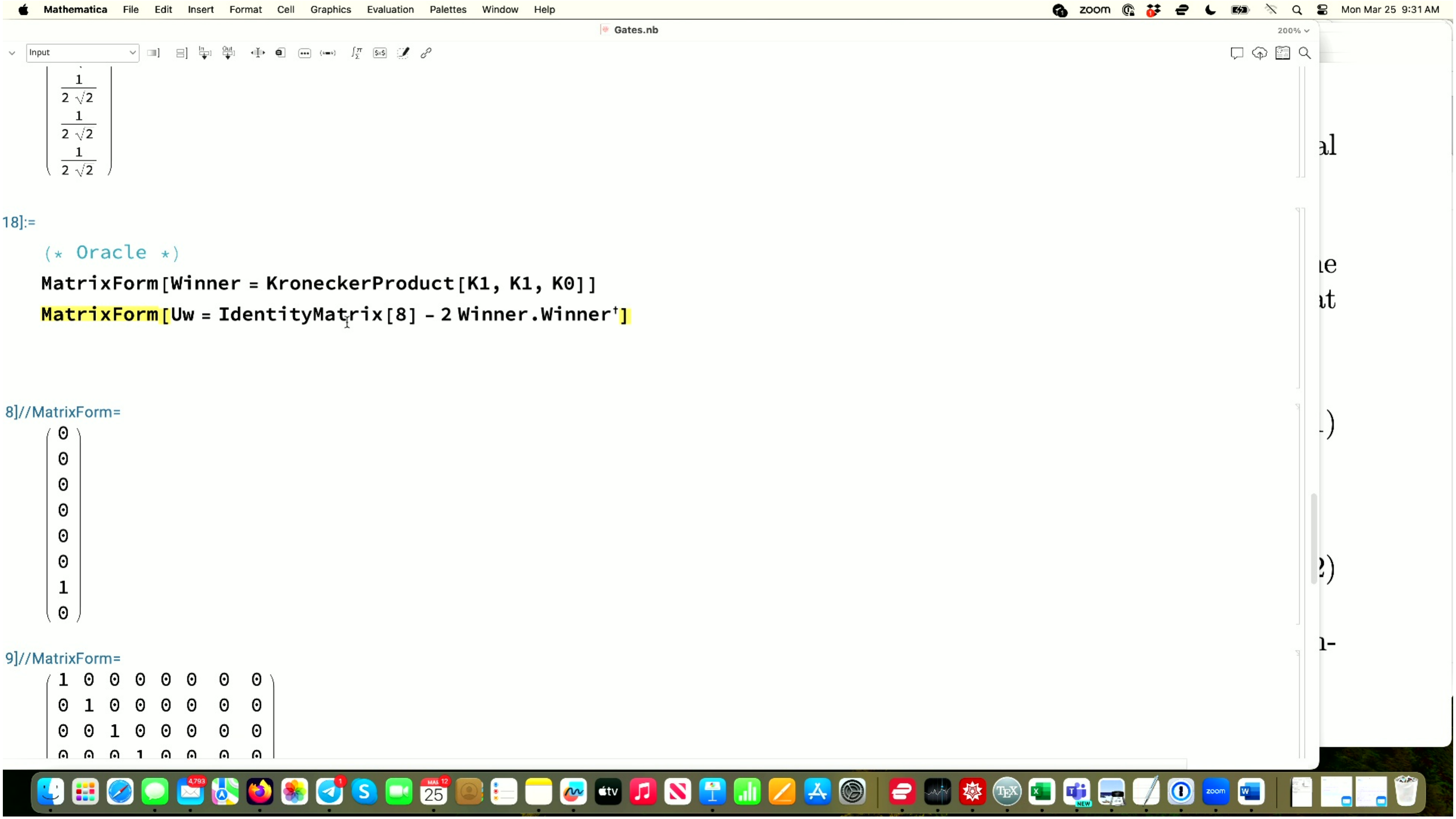
When $N \gg 1$ then

$$\boxed{n \sim \frac{\pi\sqrt{N}}{4} \sim O(\sqrt{N})}. \tag{142}$$

which is a very significant reduction of complexity compared to the $O(N)$ complexity of a classical algorithm.



```
16]:= (* Initialization *)
      MatrixForm[K000 = KroneckerProduct[K0, K0, K0]]

6]//MatrixForm=
      ( 1 )
      ( 0 )
      ( 0 )
      ( 0 )
      ( 0 )
      ( 0 )
      ( 0 )
      ( 0 )

In[ ]:= MatrixForm[S = KroneckerProduct[H, H, H].K000]

In[ ]:=
      (* Oracle *)
      MatrixForm[Winner = KroneckerProduct[K1, K1, K0]]
      MatrixForm[Uw = IdentityMatrix[8] - 2 Winner.Winner†]

In[ ]:=
      MatrixForm[Uw.S]

In[ ]:=
      (*Difusser*)
```

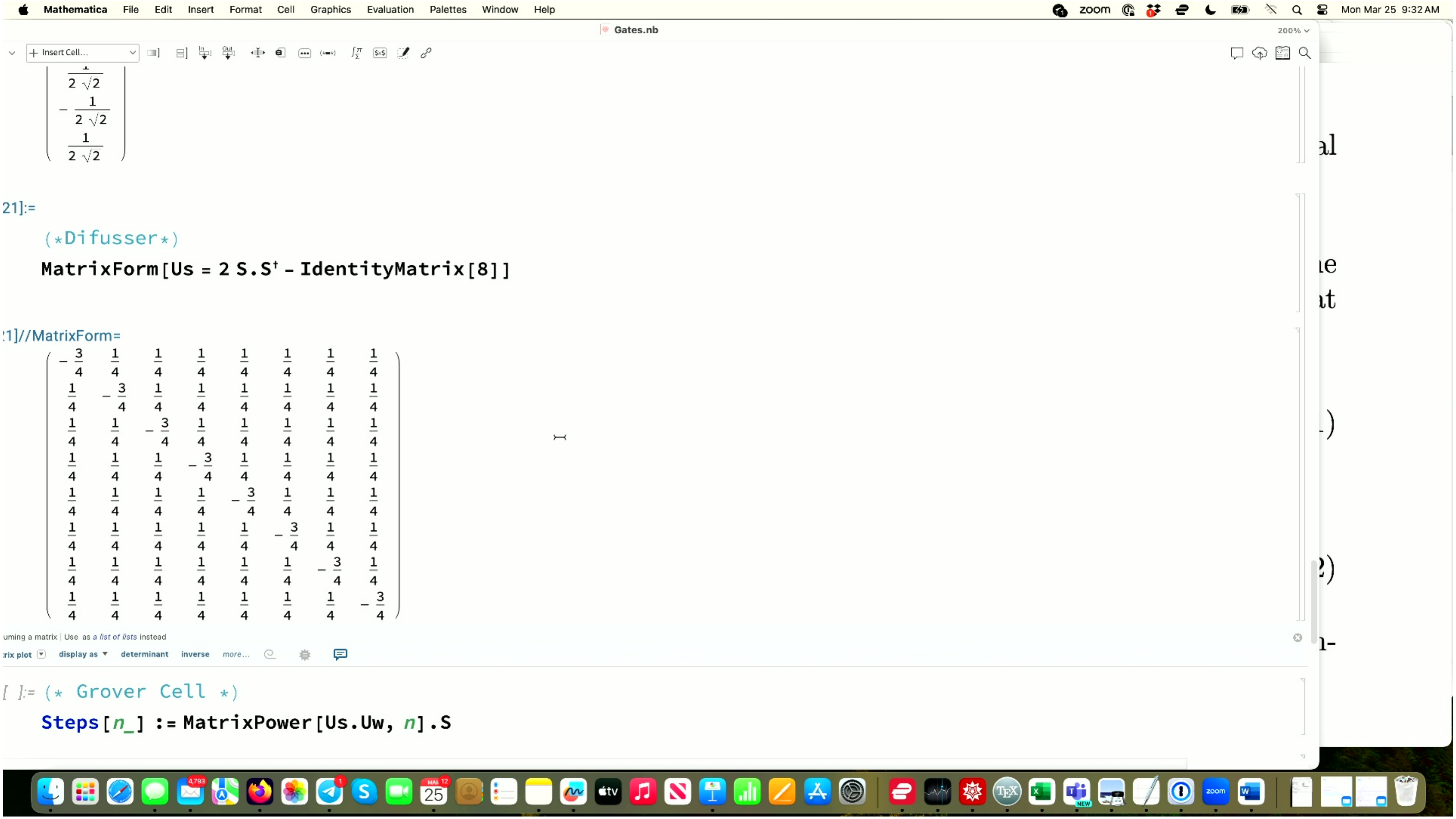

Mathematica File Edit Insert Format Cell Graphics Evaluation Palettes Window Help
zoom
Mon Mar 25 9:31 AM
Gates.nb
200%
Input

$$\begin{pmatrix} \vdots \\ \frac{1}{2\sqrt{2}} \\ \frac{1}{2\sqrt{2}} \\ \frac{1}{2\sqrt{2}} \end{pmatrix}$$

```
18]:=
(* Oracle *)
MatrixForm[Winner = KroneckerProduct[K1, K1, K0]]
MatrixForm[Uw = IdentityMatrix[8] - 2 Winner.Winner†]
```

```
8]//MatrixForm=
( 0 )
( 0 )
( 0 )
( 0 )
( 0 )
( 0 )
( 1 )
( 0 )
```

```
9]//MatrixForm=
( 1  0  0  0  0  0  0  0 )
( 0  1  0  0  0  0  0  0 )
( 0  0  1  0  0  0  0  0 )
( 0  0  0  1  0  0  0  0
```



$$\begin{pmatrix} \frac{1}{2\sqrt{2}} \\ -\frac{1}{2\sqrt{2}} \\ \frac{1}{2\sqrt{2}} \end{pmatrix}$$

21]:=

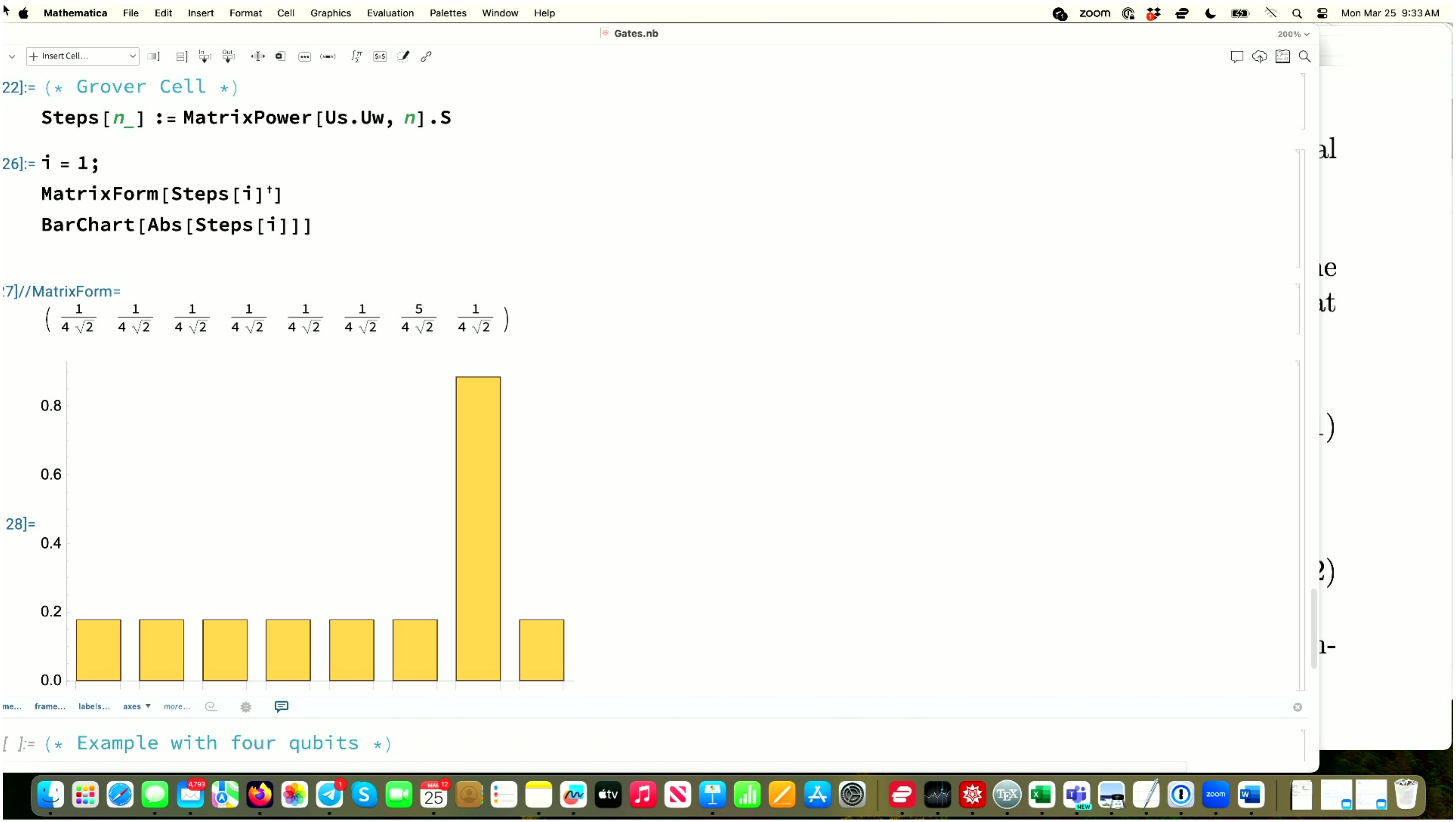
```
(*Difusser*)
MatrixForm[Us = 2 S.S† - IdentityMatrix[8]]
```

1]//MatrixForm=

$$\begin{pmatrix} -\frac{3}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & -\frac{3}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} & -\frac{3}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & -\frac{3}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & -\frac{3}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & -\frac{3}{4} & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & -\frac{3}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & -\frac{3}{4} \end{pmatrix}$$

uming a matrix | Use as a *list of lists* instead

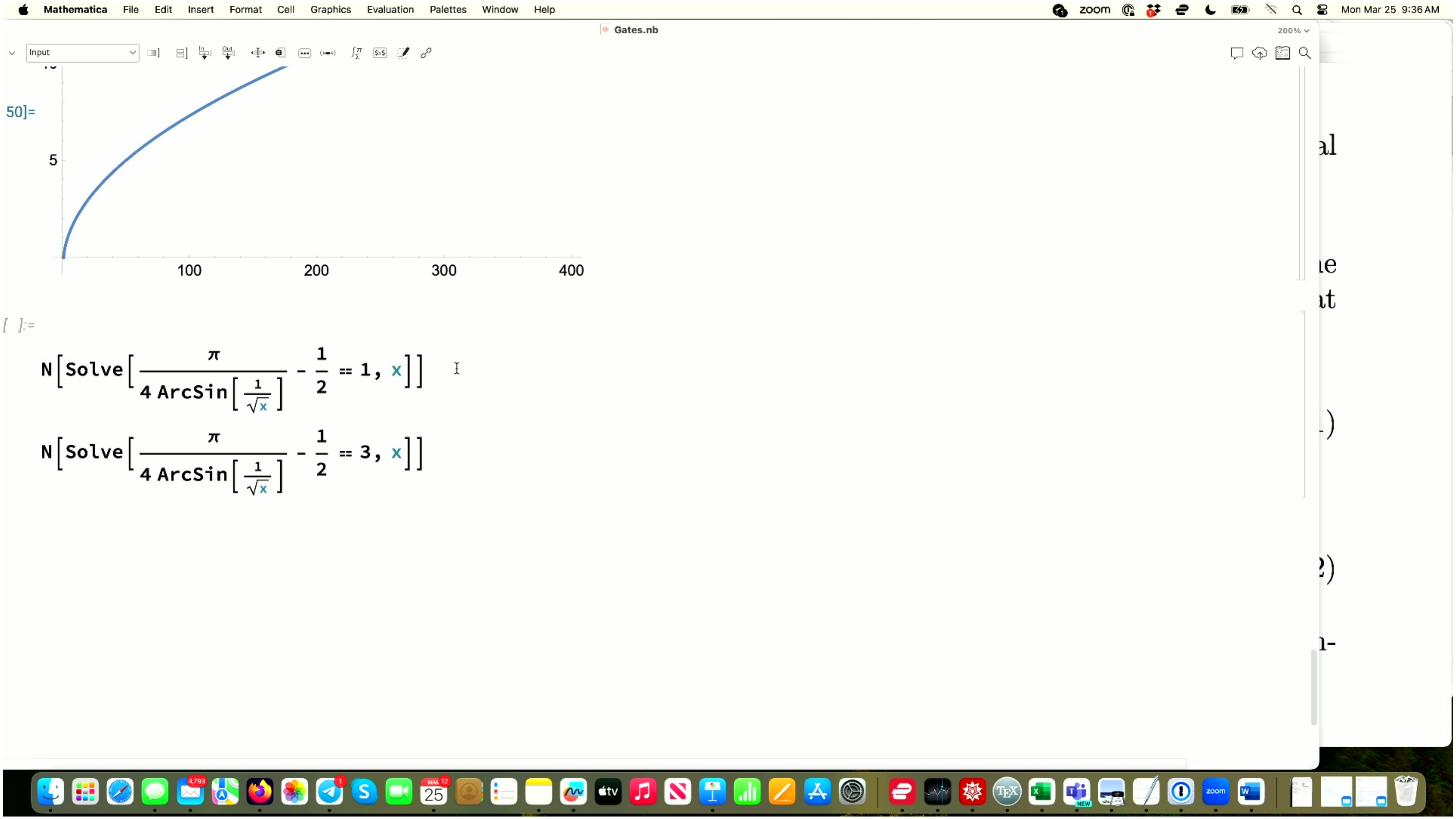
```
[ ]:= (* Grover Cell *)
Steps[n_] := MatrixPower[Us.Uw, n].S
```


Mathematica File Edit Insert Format Cell Graphics Evaluation Palettes Window Help
Mon Mar 25 9:33 AM
Gates.nb
200%
Insert Cell...
0.8
0.6
0.4
0.2
0.0
me... frame... labels... axes more...

```
22]:= (* Grover Cell *)
      Steps[n_] := MatrixPower[Us.Uw, n].S

26]:= i = 1;
      MatrixForm[Steps[i]†]
      BarChart[Abs[Steps[i]]]

:7]//MatrixForm=
```

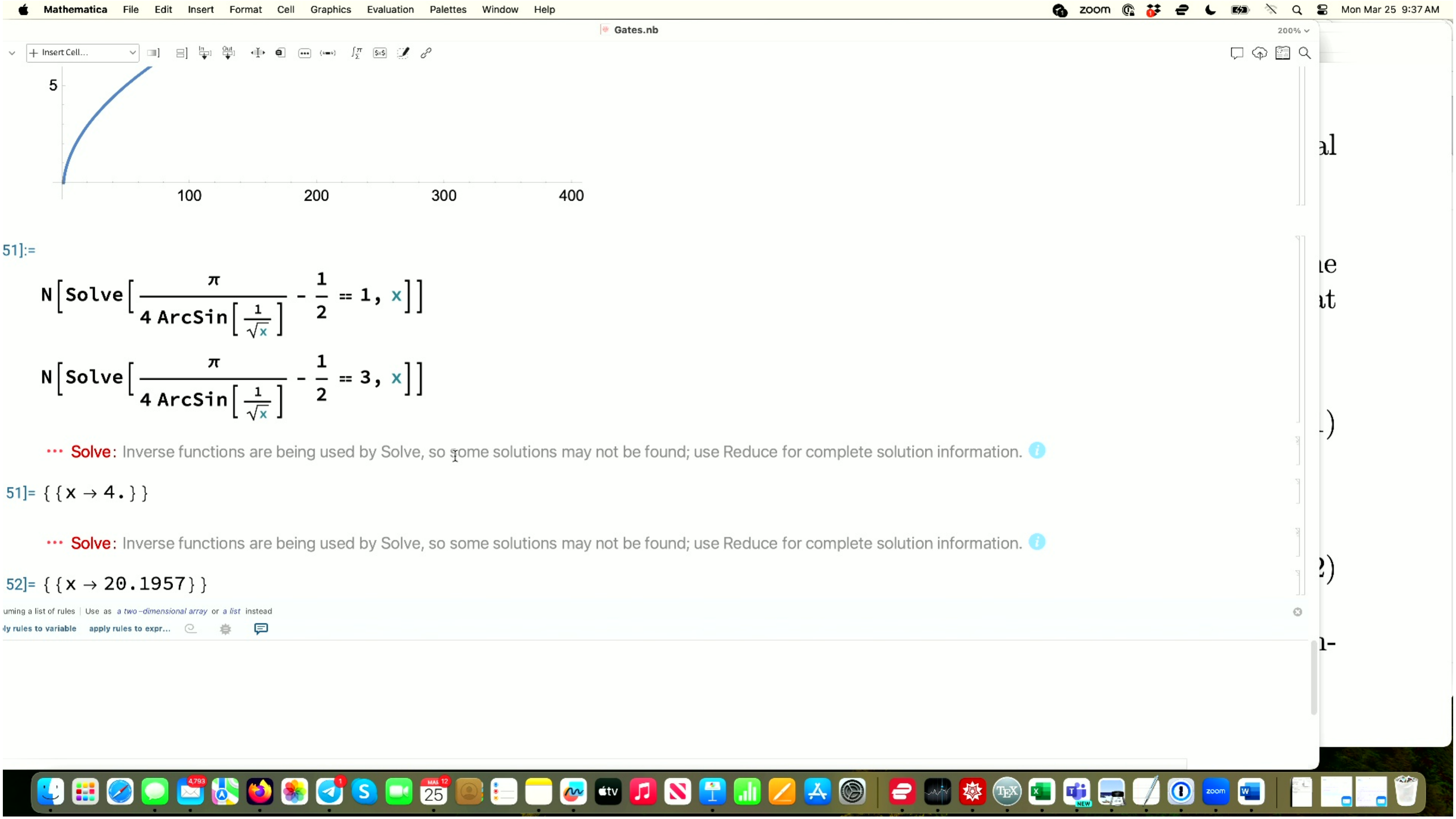
$$\begin{pmatrix} \frac{1}{4\sqrt{2}} & \frac{1}{4\sqrt{2}} & \frac{1}{4\sqrt{2}} & \frac{1}{4\sqrt{2}} & \frac{1}{4\sqrt{2}} & \frac{1}{4\sqrt{2}} & \frac{5}{4\sqrt{2}} & \frac{1}{4\sqrt{2}} \end{pmatrix}$$

```
28]=

[ ]:= (* Example with four qubits *)
```


Mathematica File Edit Insert Format Cell Graphics Evaluation Palettes Window Help
zoom
Mon Mar 25 9:36 AM
Gates.nb
200%
Input
50]=
5
100
200
300
400
[ ]:=
al
le
at
)
2)
n-

$$N\left[\text{Solve}\left[\frac{\pi}{4\,\text{ArcSin}\left[\frac{1}{\sqrt{x}}\right]}-\frac{1}{2}==1,\ x\right]\right]$$

$$N\left[\text{Solve}\left[\frac{\pi}{4\,\text{ArcSin}\left[\frac{1}{\sqrt{x}}\right]}-\frac{1}{2}==3,\ x\right]\right]$$

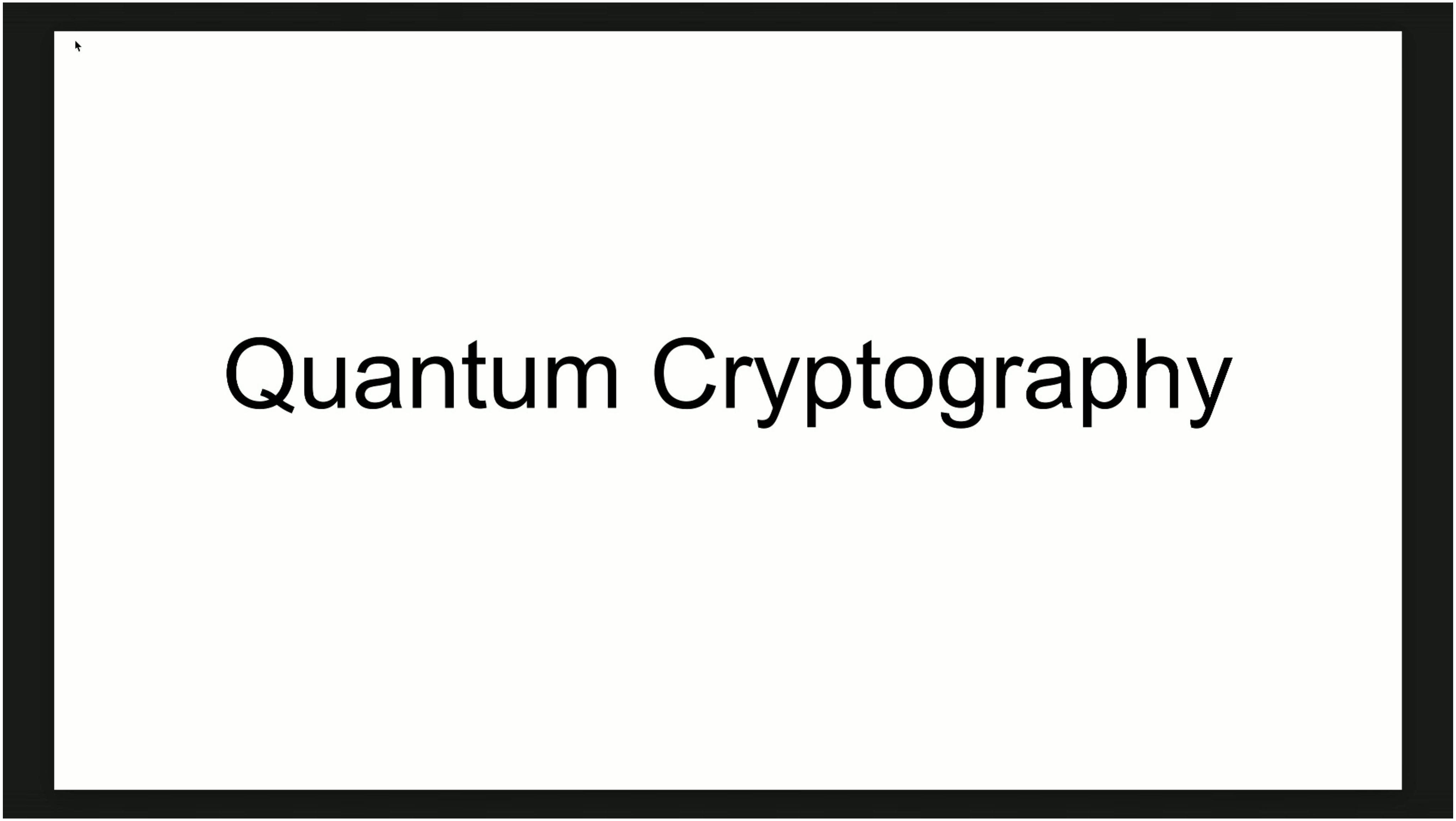

Mathematica File Edit Insert Format Cell Graphics Evaluation Palettes Window Help
zoom
Mon Mar 25 9:37 AM
Gates.nb
200%
Insert Cell...
5
100
200
300
400
uming a list of rules | Use as a two-dimensional array or a list instead
ly rules to variable
apply rules to expr...
al
e
at
.)
2)
n-

51]:=

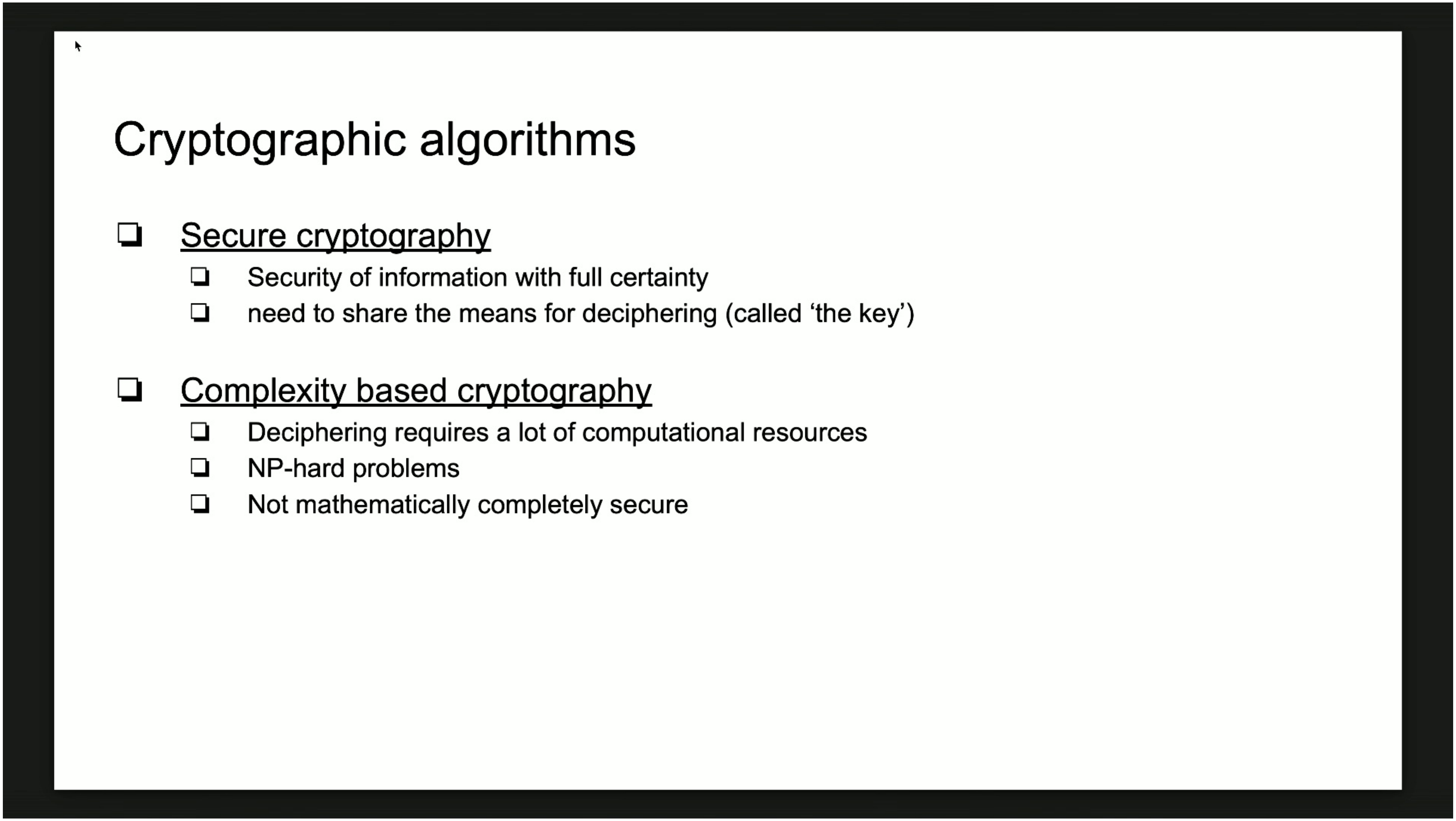
$$\mathtt{N}\left[\mathtt{Solve}\left[\frac{\pi}{4\,\mathtt{ArcSin}\left[\frac{1}{\sqrt{x}}\right]}-\frac{1}{2}==1,\ x\right]\right]$$

$$\mathtt{N}\left[\mathtt{Solve}\left[\frac{\pi}{4\,\mathtt{ArcSin}\left[\frac{1}{\sqrt{x}}\right]}-\frac{1}{2}==3,\ x\right]\right]$$

```
··· Solve: Inverse functions are being used by Solve, so some solutions may not be found; use Reduce for complete solution information.

51]= {{x → 4.}}

··· Solve: Inverse functions are being used by Solve, so some solutions may not be found; use Reduce for complete solution information.

52]= {{x → 20.1957}}
```



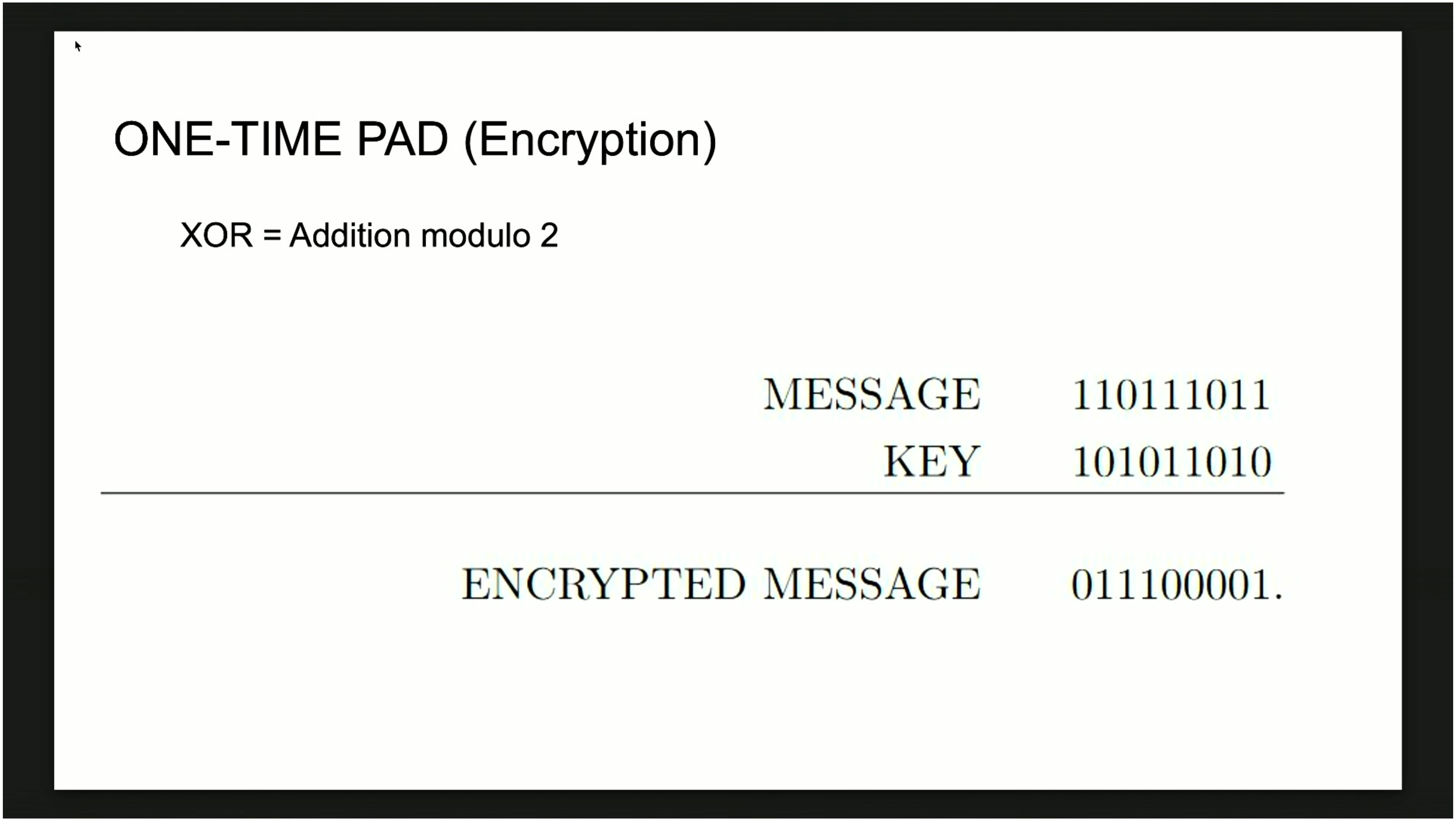
Quantum Cryptography



Cryptographic algorithms

- <u>Secure cryptography</u>
  - Security of information with full certainty
  - need to share the means for deciphering (called ‘the key’)

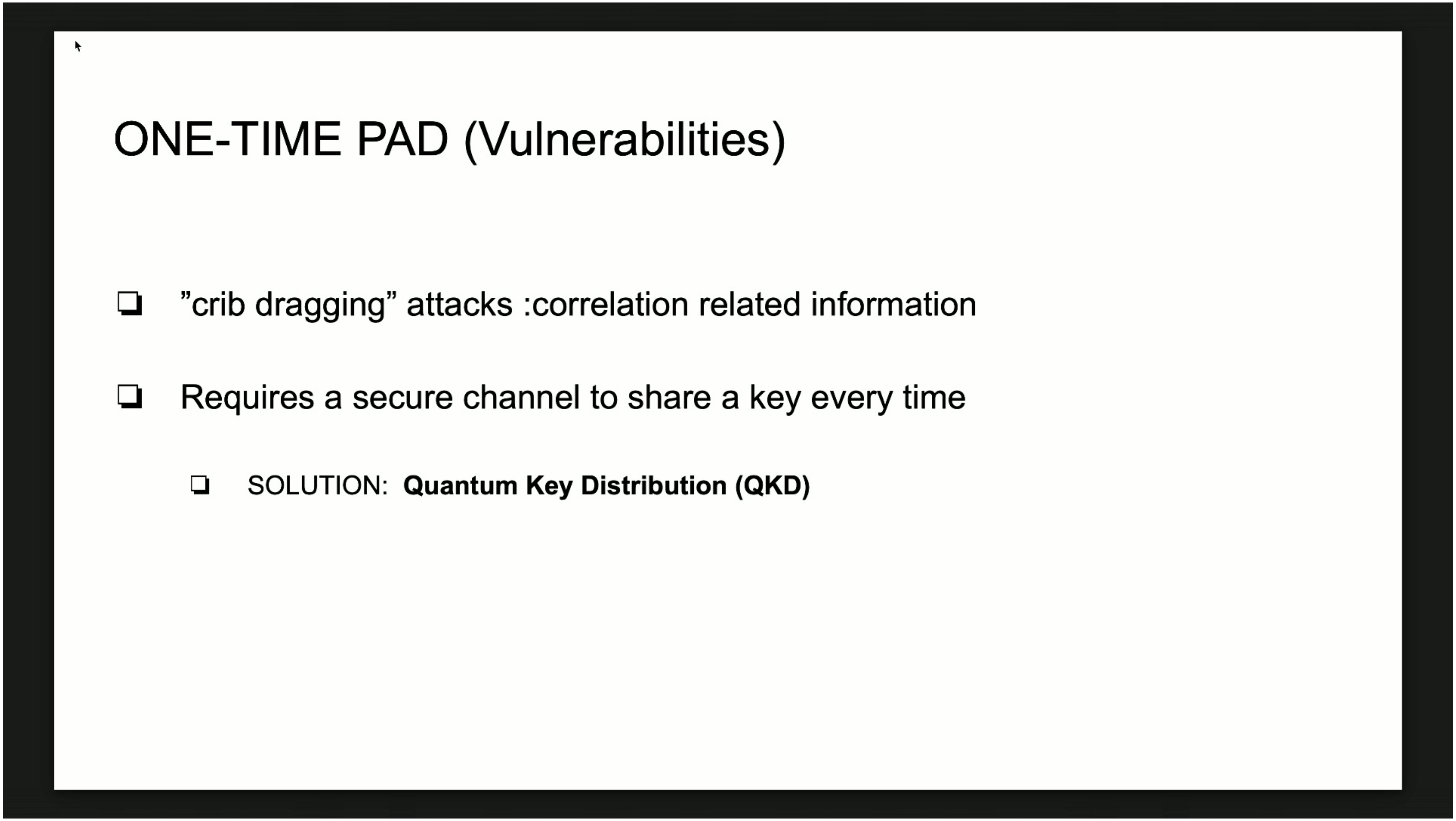
- <u>Complexity based cryptography</u>
  - Deciphering requires a lot of computational resources
  - NP-hard problems
  - Not mathematically completely secure



ONE-TIME PAD (Encryption)

XOR = Addition modulo 2

MESSAGE	110111011
KEY	101011010
ENCRYPTED MESSAGE	011100001.



ONE-TIME PAD (Vulnerabilities)

❑ ”crib dragging” attacks :correlation related information

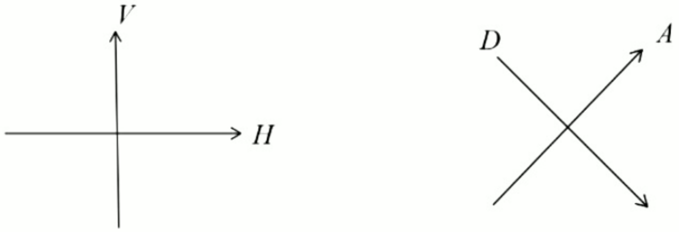
❑ Requires a secure channel to share a key every time

  ❑ SOLUTION: **Quantum Key Distribution (QKD)**

BB84

BB84

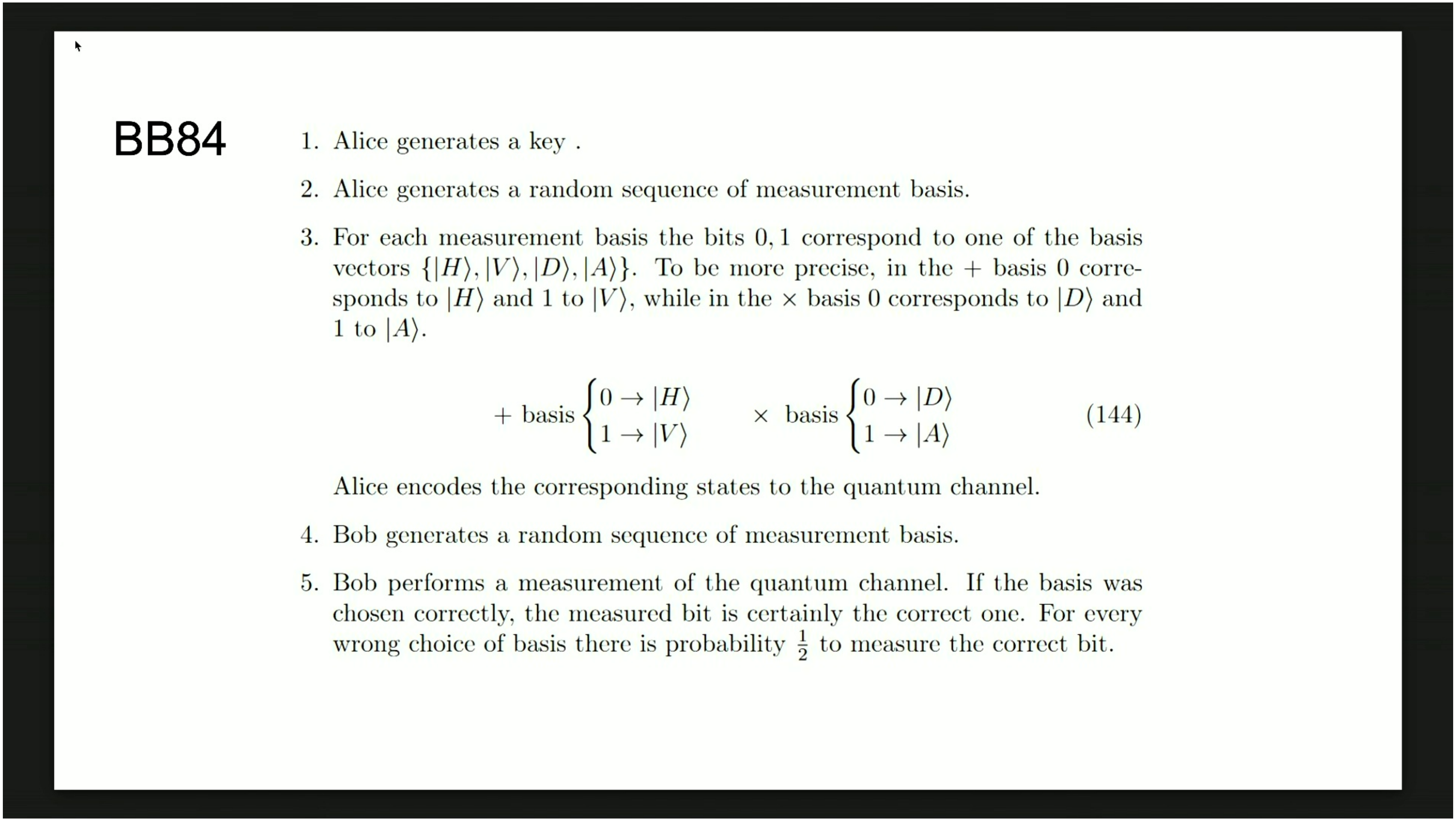
$$
\begin{aligned}
|V\rangle &= \frac{1}{\sqrt{2}}\left(|A\rangle + |D\rangle\right) \\
|H\rangle &= \frac{1}{\sqrt{2}}\left(|A\rangle - |D\rangle\right)
\end{aligned}
\tag{143}
$$



$|V\rangle \leftrightarrow 1$
$|H\rangle \leftrightarrow 0$

$|A\rangle \leftrightarrow 1$
$|D\rangle \leftrightarrow 0$

Figure 17: Vertical-horizontal basis and diagonal-antidiagonal basis.

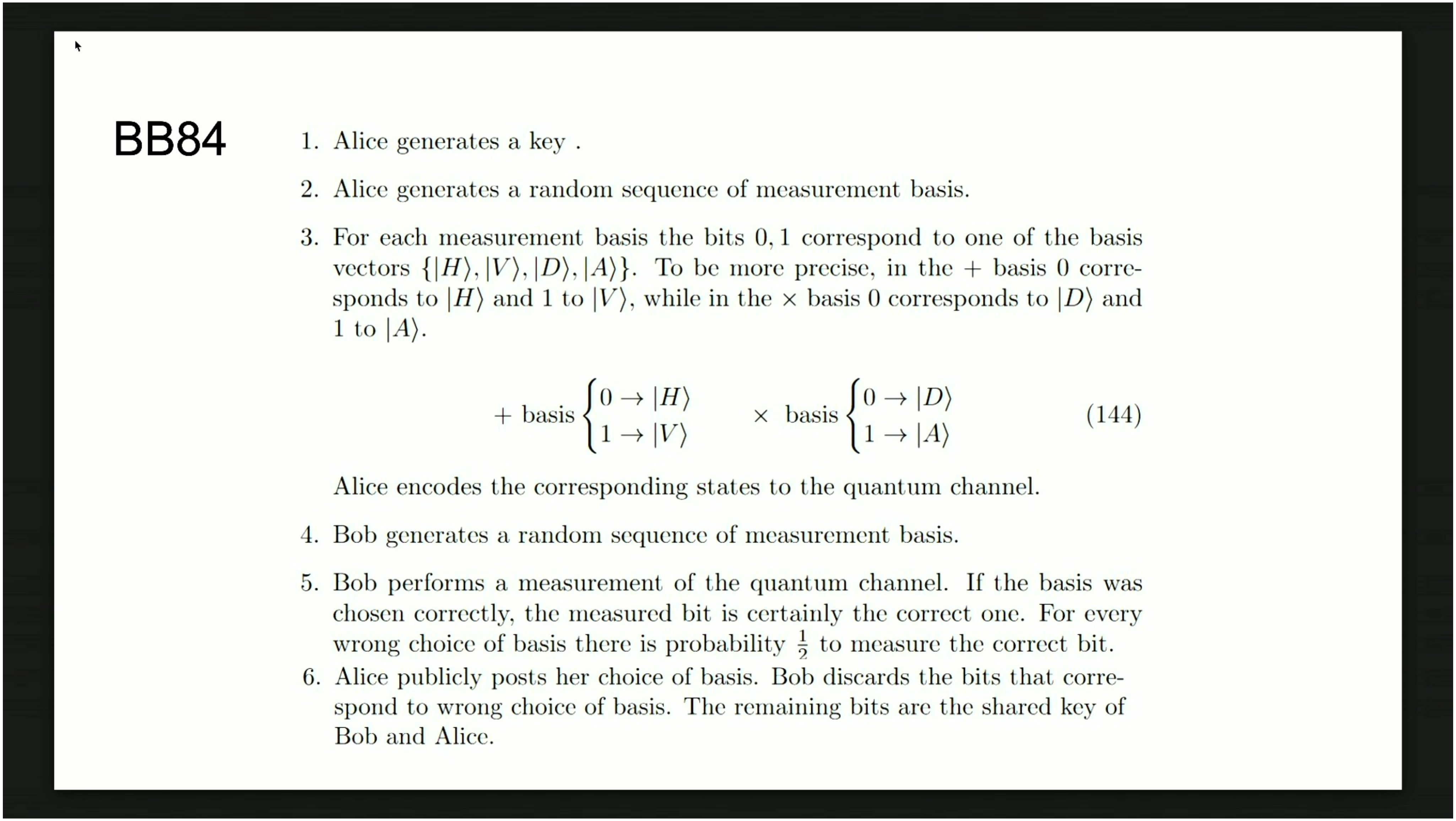


BB84

1. Alice generates a key .
2. Alice generates a random sequence of measurement basis.
3. For each measurement basis the bits $0, 1$ correspond to one of the basis vectors $\{|H\rangle, |V\rangle, |D\rangle, |A\rangle\}$. To be more precise, in the + basis 0 corresponds to $|H\rangle$ and 1 to $|V\rangle$, while in the × basis 0 corresponds to $|D\rangle$ and 1 to $|A\rangle$.

   $$+ \text{ basis} \begin{cases} 0 \rightarrow |H\rangle \\ 1 \rightarrow |V\rangle \end{cases} \qquad \times \text{ basis} \begin{cases} 0 \rightarrow |D\rangle \\ 1 \rightarrow |A\rangle \end{cases} \tag{144}$$

   Alice encodes the corresponding states to the quantum channel.
4. Bob generates a random sequence of measurement basis.
5. Bob performs a measurement of the quantum channel. If the basis was chosen correctly, the measured bit is certainly the correct one. For every wrong choice of basis there is probability $\frac{1}{2}$ to measure the correct bit.

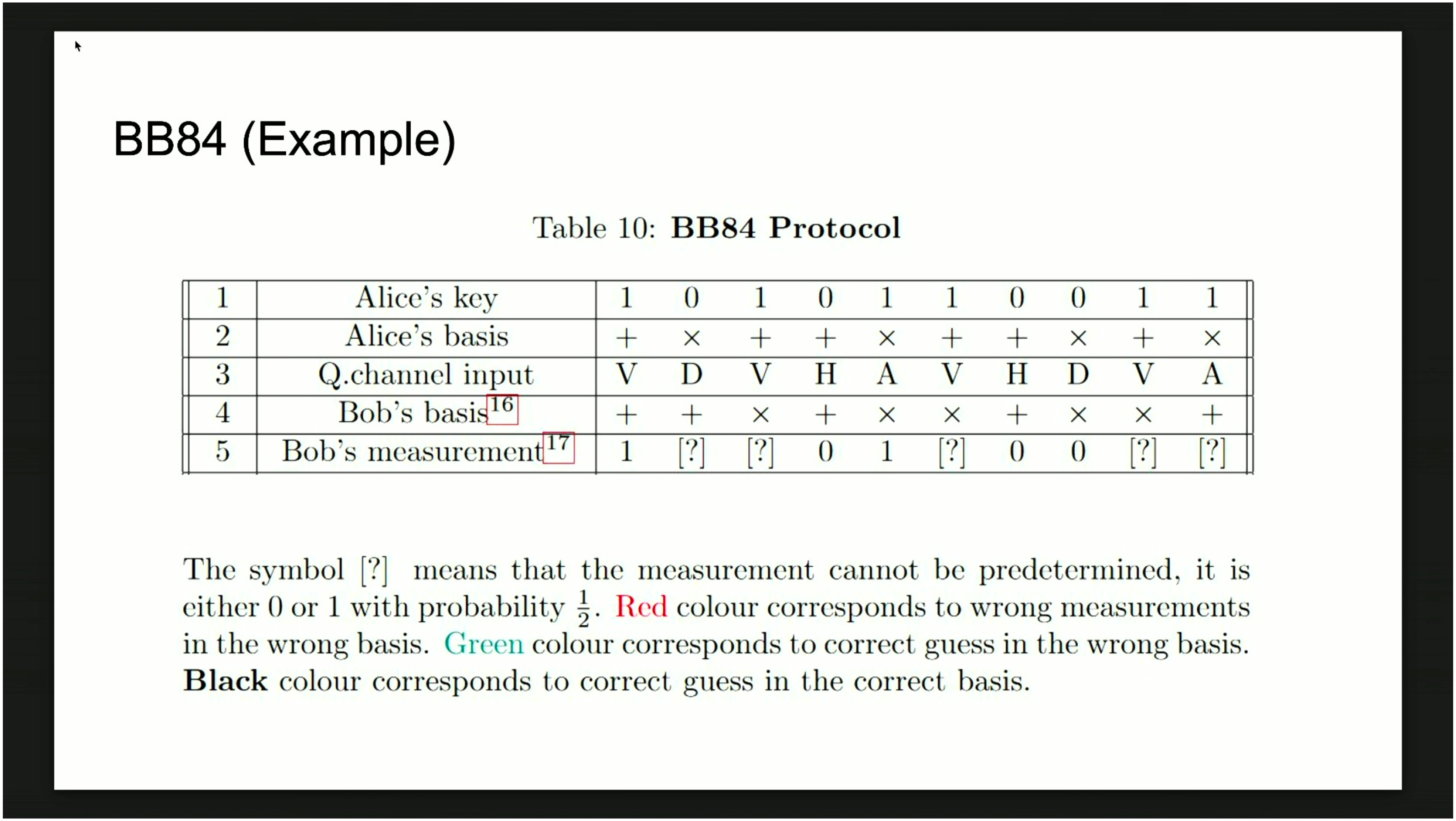


BB84

1. Alice generates a key .
2. Alice generates a random sequence of measurement basis.
3. For each measurement basis the bits $0, 1$ correspond to one of the basis vectors $\{|H\rangle, |V\rangle, |D\rangle, |A\rangle\}$. To be more precise, in the $+$ basis 0 corresponds to $|H\rangle$ and 1 to $|V\rangle$, while in the $\times$ basis 0 corresponds to $|D\rangle$ and 1 to $|A\rangle$.

   $$+\ \text{basis} \begin{cases} 0 \to |H\rangle \\ 1 \to |V\rangle \end{cases} \qquad \times\ \text{basis} \begin{cases} 0 \to |D\rangle \\ 1 \to |A\rangle \end{cases} \tag{144}$$

   Alice encodes the corresponding states to the quantum channel.
4. Bob generates a random sequence of measurement basis.
5. Bob performs a measurement of the quantum channel. If the basis was chosen correctly, the measured bit is certainly the correct one. For every wrong choice of basis there is probability $\frac{1}{2}$ to measure the correct bit.
6. Alice publicly posts her choice of basis. Bob discards the bits that correspond to wrong choice of basis. The remaining bits are the shared key of Bob and Alice.

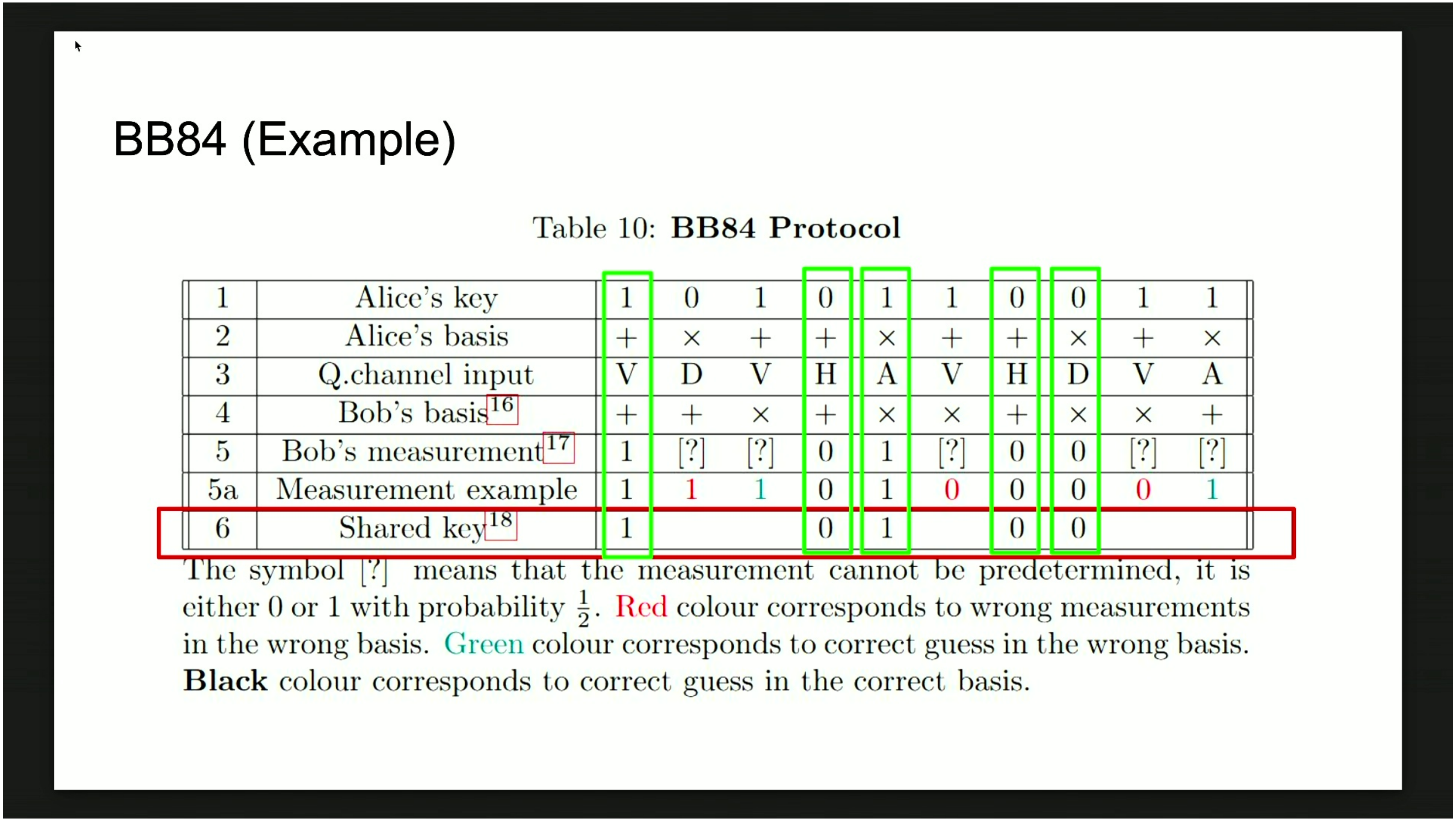


BB84 (Example)

Table 10: **BB84 Protocol**

1	Alice's key	1	0	1	0	1	1	0	0	1	1
2	Alice's basis	+	×	+	+	×	+	+	×	+	×
3	Q.channel input	V	D	V	H	A	V	H	D	V	A
4	Bob's basis[16]	+	+	×	+	×	×	+	×	×	+
5	Bob's measurement[17]	1	[?]	[?]	0	1	[?]	0	0	[?]	[?]

The symbol [?] means that the measurement cannot be predetermined, it is either 0 or 1 with probability $\frac{1}{2}$. Red colour corresponds to wrong measurements in the wrong basis. Green colour corresponds to correct guess in the wrong basis. **Black** colour corresponds to correct guess in the correct basis.

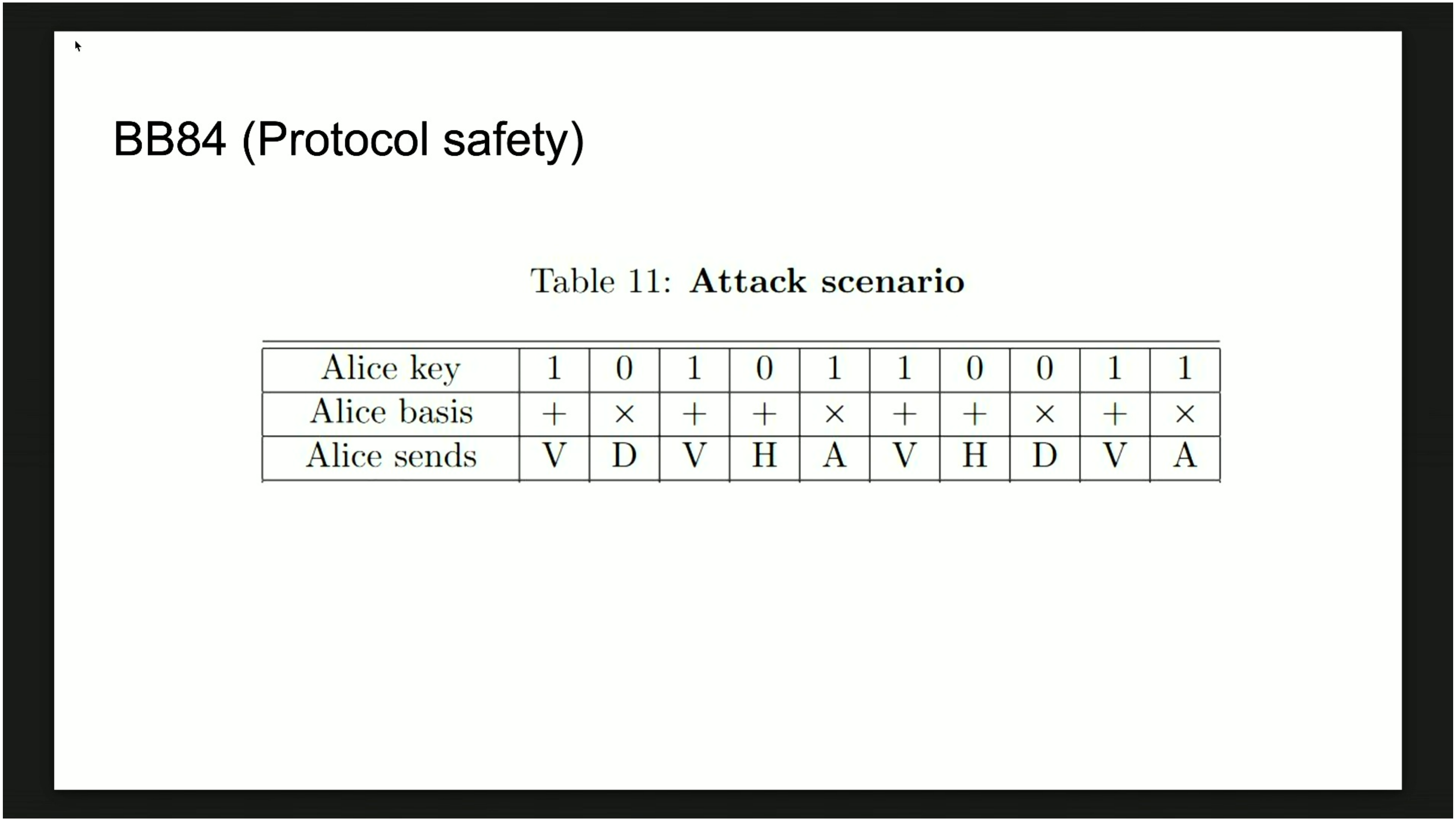


BB84 (Example)

Table 10: **BB84 Protocol**

1	Alice's key	1	0	1	0	1	1	0	0	1	1
2	Alice's basis	+	×	+	+	×	+	+	×	+	×
3	Q.channel input	V	D	V	H	A	V	H	D	V	A
4	Bob's basis[16]	+	+	×	+	×	×	+	×	×	+
5	Bob's measurement[17]	1	[?]	[?]	0	1	[?]	0	0	[?]	[?]
5a	Measurement example	1	1	1	0	1	0	0	0	0	1
6	Shared key[18]	1			0	1		0	0		

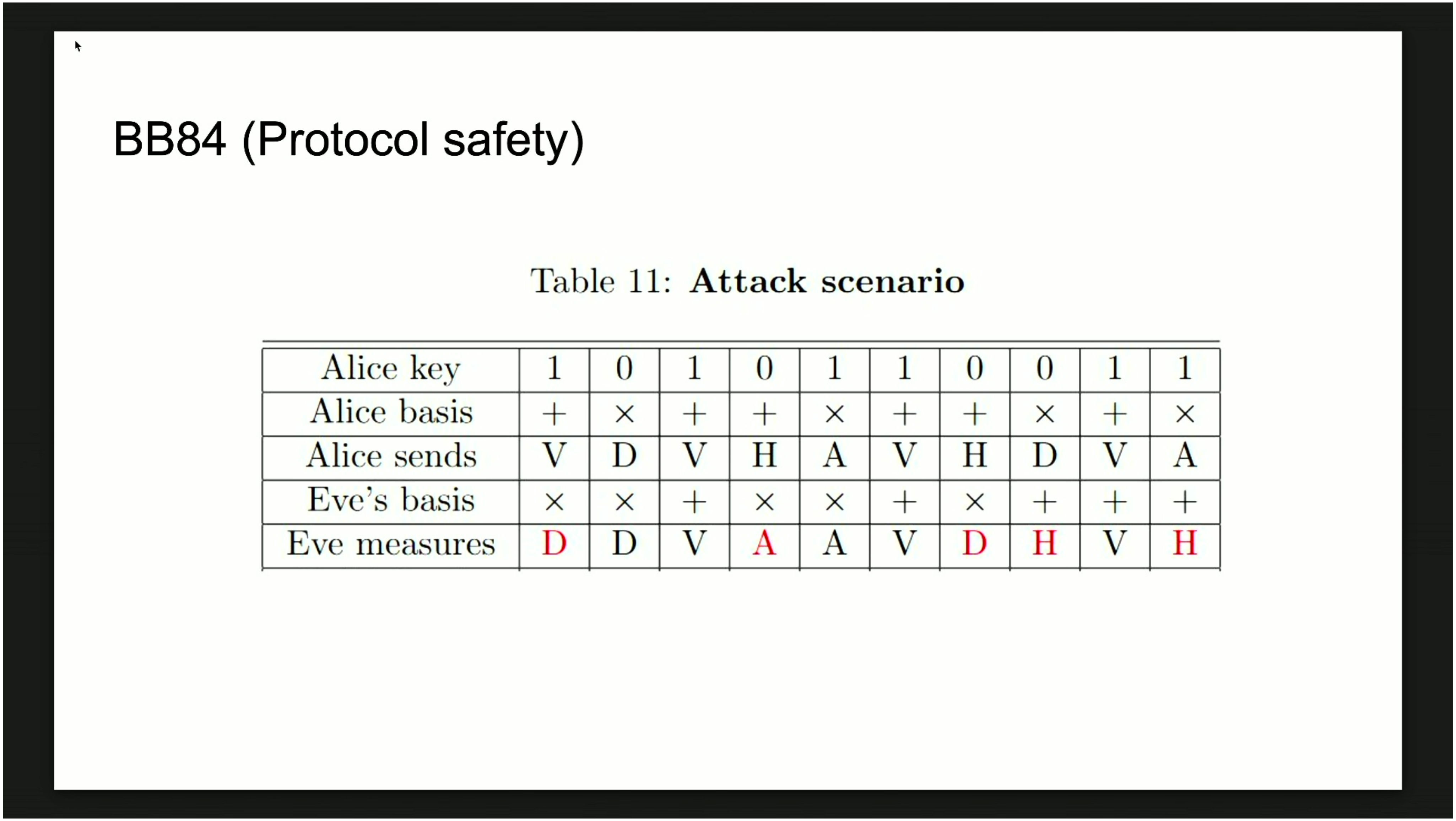
The symbol [?] means that the measurement cannot be predetermined, it is either 0 or 1 with probability $\frac{1}{2}$. Red colour corresponds to wrong measurements in the wrong basis. Green colour corresponds to correct guess in the wrong basis. **Black** colour corresponds to correct guess in the correct basis.



BB84 (Protocol safety)

Table 11: **Attack scenario**

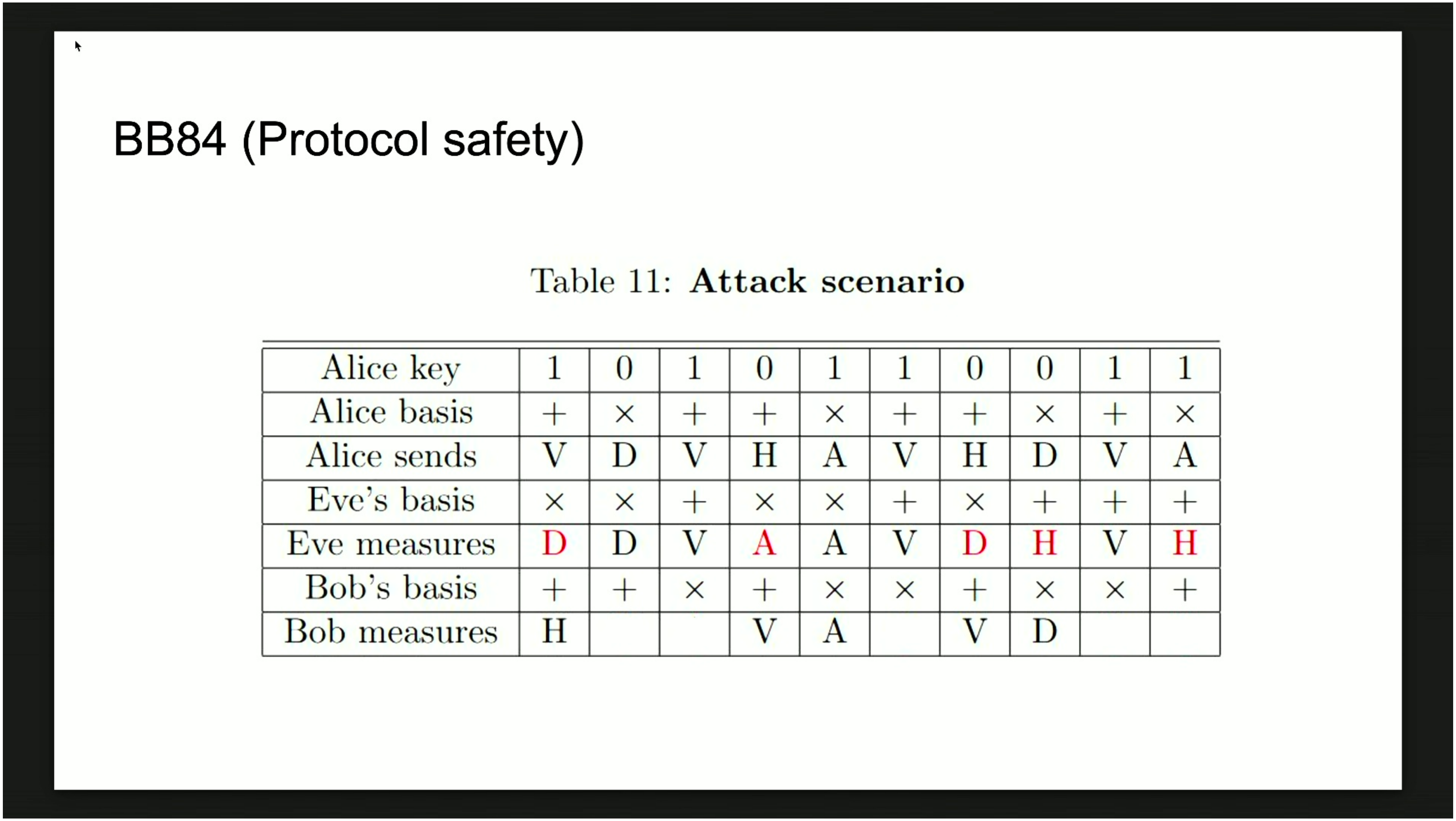
Alice key	1	0	1	0	1	1	0	0	1	1
Alice basis	$+$	$\times$	$+$	$+$	$\times$	$+$	$+$	$\times$	$+$	$\times$
Alice sends	V	D	V	H	A	V	H	D	V	A



BB84 (Protocol safety)

Table 11: **Attack scenario**

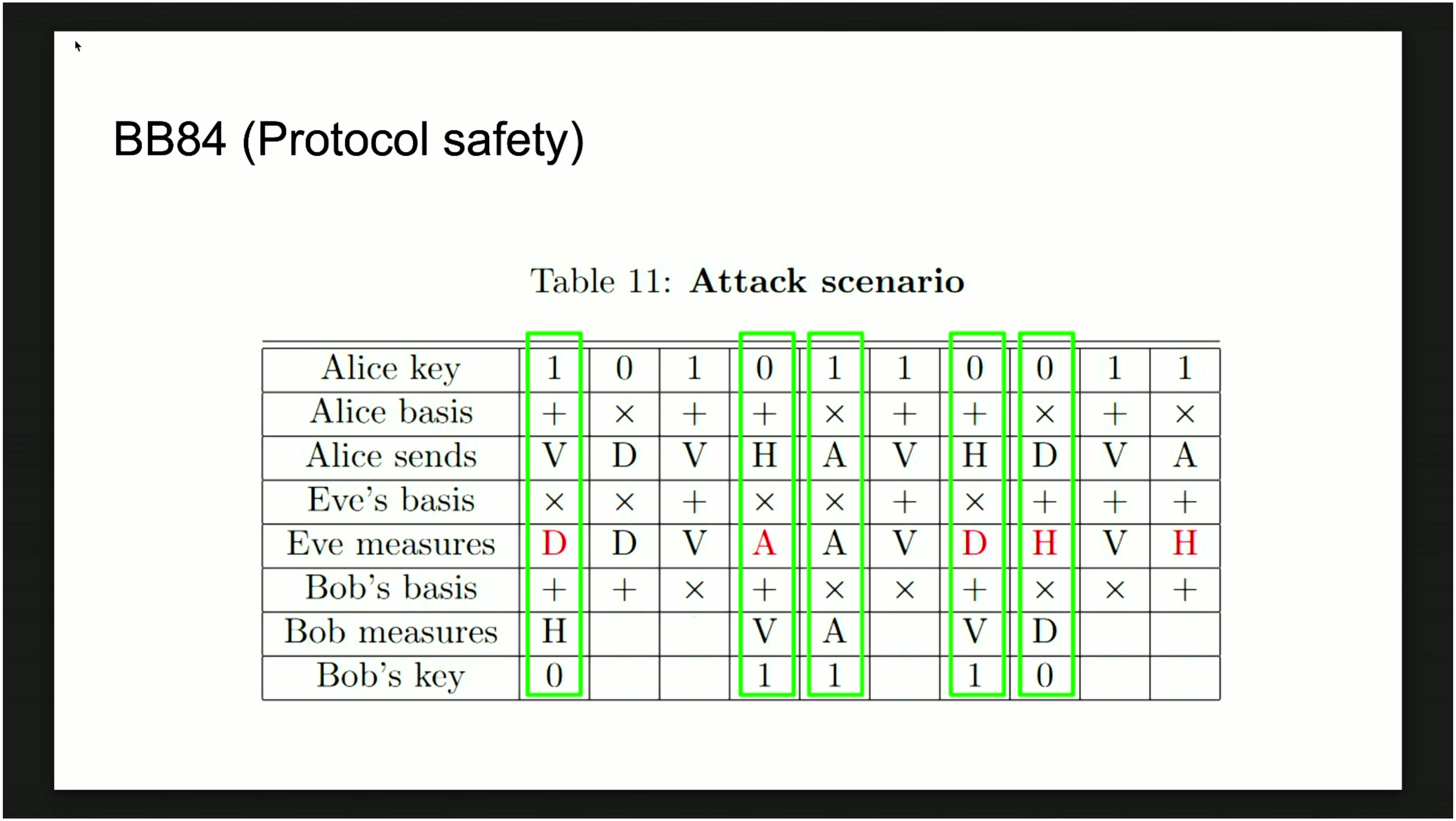
Alice key	1	0	1	0	1	1	0	0	1	1
Alice basis	+	×	+	+	×	+	+	×	+	×
Alice sends	V	D	V	H	A	V	H	D	V	A
Eve's basis	×	×	+	×	×	+	×	+	+	+
Eve measures	D	D	V	A	A	V	D	H	V	H



BB84 (Protocol safety)

Table 11: **Attack scenario**

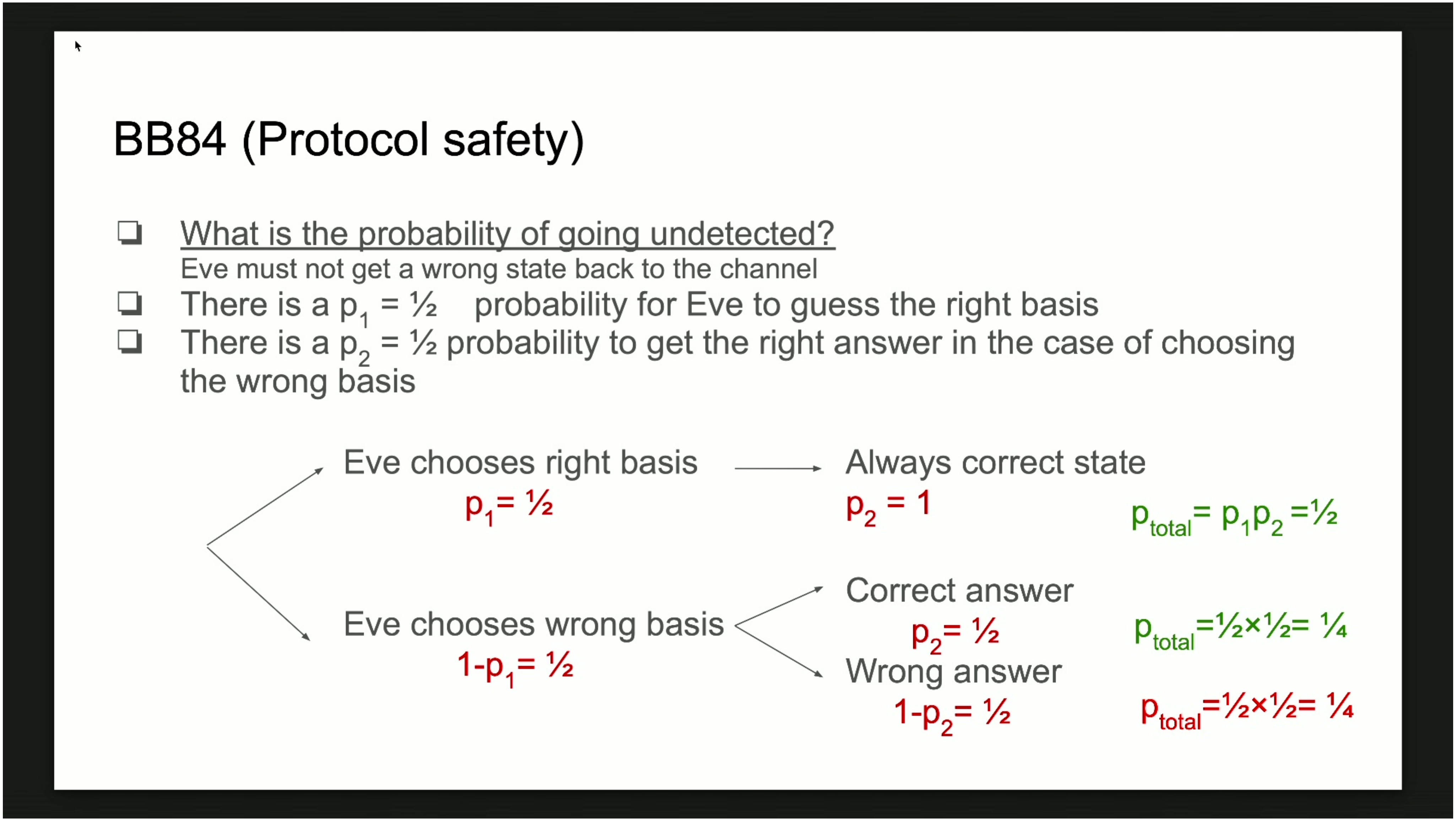
Alice key	1	0	1	0	1	1	0	0	1	1
Alice basis	+	×	+	+	×	+	+	×	+	×
Alice sends	V	D	V	H	A	V	H	D	V	A
Eve's basis	×	×	+	×	×	+	×	+	+	+
Eve measures	D	D	V	A	A	V	D	H	V	H
Bob's basis	+	+	×	+	×	×	+	×	×	+
Bob measures	H			V	A		V	D		



BB84 (Protocol safety)

Table 11: **Attack scenario**

Alice key	1	0	1	0	1	1	0	0	1	1
Alice basis	+	×	+	+	×	+	+	×	+	×
Alice sends	V	D	V	H	A	V	H	D	V	A
Eve's basis	×	×	+	×	×	+	×	+	+	+
Eve measures	D	D	V	A	A	V	D	H	V	H
Bob's basis	+	+	×	+	×	×	+	×	×	+
Bob measures	H			V	A		V	D		
Bob's key	0			1	1		1	0		



BB84 (Protocol safety)

- ❑ What is the probability of going undetected?
  Eve must not get a wrong state back to the channel
- ❑ There is a $p_1 = ½$ probability for Eve to guess the right basis
- ❑ There is a $p_2 = ½$ probability to get the right answer in the case of choosing the wrong basis

Eve chooses right basis

$p_1 = ½$

Always correct state

$p_2 = 1$

$p_{total} = p_1 p_2 = ½$

Eve chooses wrong basis

$1-p_1 = ½$

Correct answer

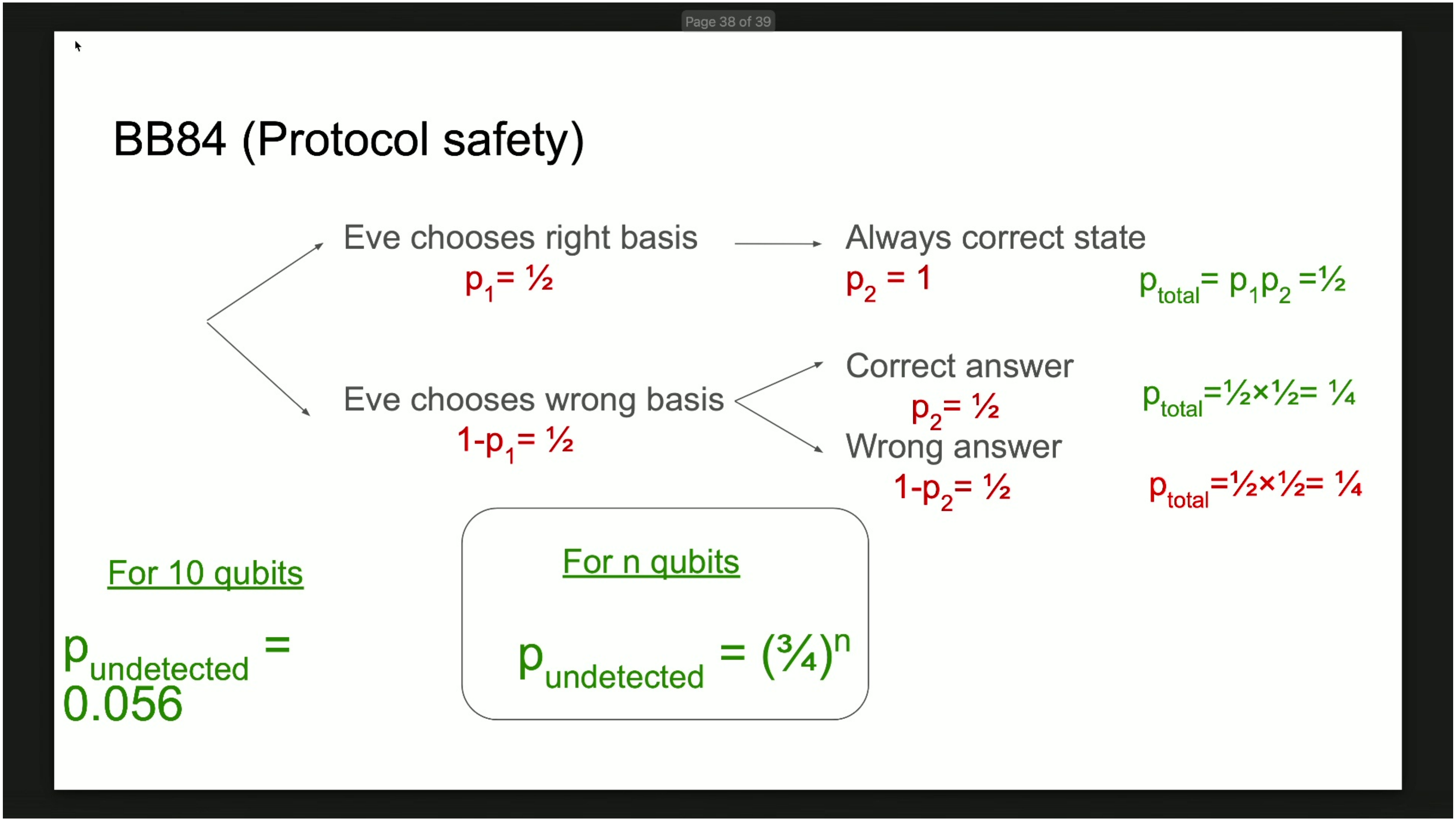
$p_2 = ½$

$p_{total} = ½ \times ½ = ¼$

Wrong answer

$1-p_2 = ½$

$p_{total} = ½ \times ½ = ¼$



BB84 (Protocol safety)

Eve chooses right basis $p_1 = ½$ → Always correct state $p_2 = 1$ $p_{total} = p_1 p_2 = ½$

Eve chooses wrong basis $1 - p_1 = ½$

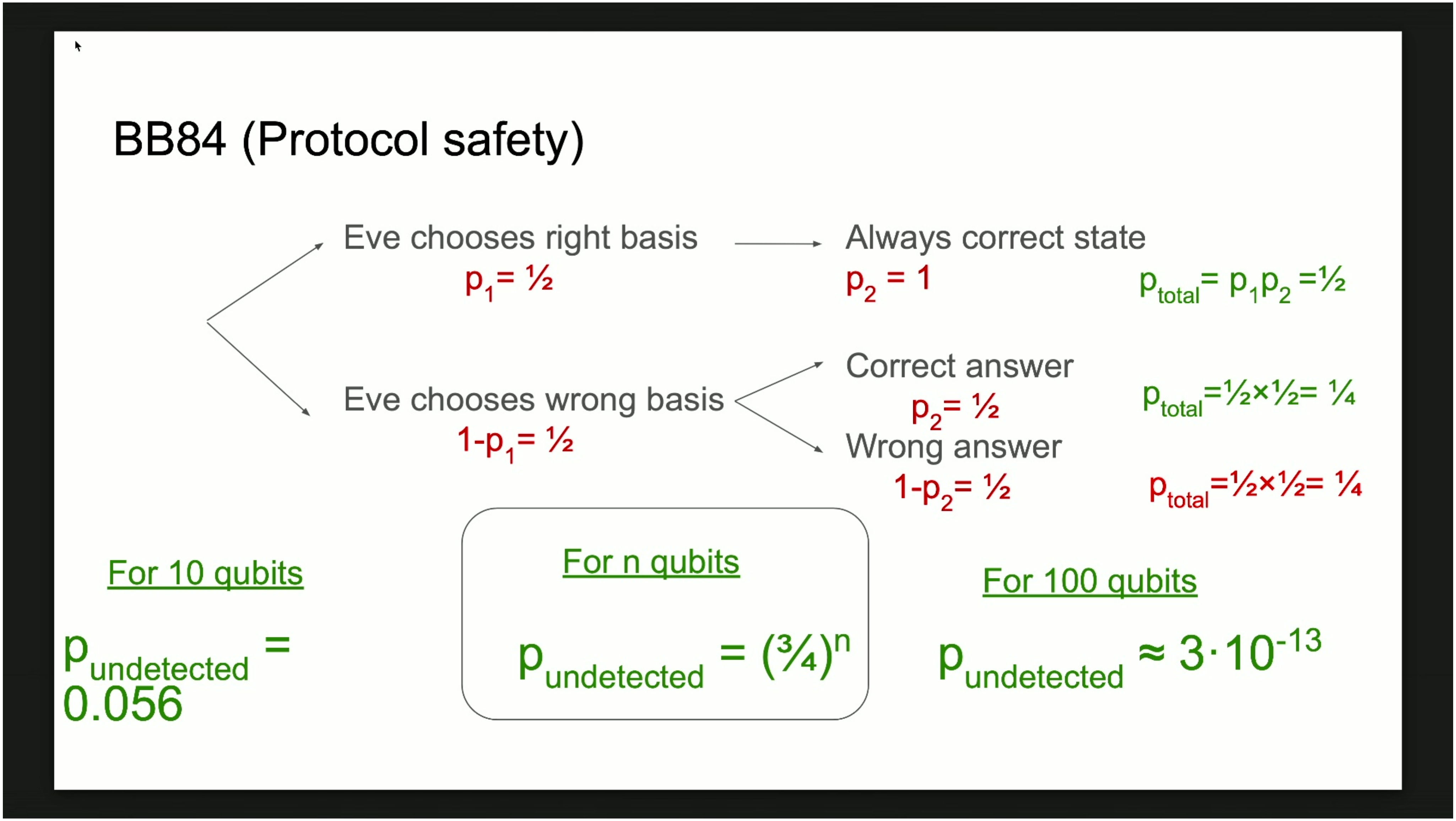
- Correct answer $p_2 = ½$ $p_{total} = ½ \times ½ = ¼$
- Wrong answer $1 - p_2 = ½$ $p_{total} = ½ \times ½ = ¼$

For 10 qubits

$p_{undetected} = 0.056$

For n qubits

$p_{undetected} = (¾)^n$



BB84 (Protocol safety)

Eve chooses right basis $p_1 = \frac{1}{2}$ → Always correct state $p_2 = 1$ $p_{total} = p_1 p_2 = \frac{1}{2}$

Eve chooses wrong basis $1 - p_1 = \frac{1}{2}$

Correct answer $p_2 = \frac{1}{2}$ $p_{total} = \frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$

Wrong answer $1 - p_2 = \frac{1}{2}$ $p_{total} = \frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$

For 10 qubits

$p_{undetected} = 0.056$

For n qubits

$p_{undetected} = (\frac{3}{4})^n$

For 100 qubits

$p_{undetected} \approx 3 \cdot 10^{-13}$