Quantum-computer algorithm of Shor

The factorization of an integer N is assumed to be difficult, since every **known classical algorithm** grows **exponentially** with the size of the integer N.

This is the basis of most of the adopted **cryptographical tools** that are thus **assumed** to be **relatively secure**.

Quantum-computer algorithm of Shor

The factorization of an integer N is assumed to be difficult, since every **known classical algorithm** grows **exponentially** with the size of the integer N.

This is the basis of most of the adopted **cryptographical tools** that are thus **assumed** to be **relatively secure**.

The algorithm of Shor is based on 3 tricks:

1. **Transformation of the problem** into finding the period of a function.

Quantum-computer algorithm of Shor

The factorization of an integer N is assumed to be difficult, since every **known classical algorithm** grows **exponentially** with the size of the integer N.

This is the basis of most of the adopted **cryptographical tools** that are thus **assumed** to be **relatively secure**.

The algorithm of Shor is based on 3 tricks:

1. **Transformation of the problem** into finding the period of a function.

2. Use of the **Fourier transform** in order to determine this period.

Quantum-computer algorithm of Shor

The factorization of an integer N is assumed to be difficult, since every **known classical algorithm** grows **exponentially** with the size of the integer N.

This is the basis of most of the adopted **cryptographical tools** that are thus **assumed** to be **relatively secure**.

The algorithm of Shor is based on 3 tricks:

1. **Transformation of the problem** into finding the period of a function.

2. Use of the **Fourier transform** in order to determine this period.

3. Use of **quantum parallelism** for 1. and 2.

Trick 1: Transformation of the problem (I)

For an **integer** N and an **arbitrarily chosen integer** $y \leq N$

(with $\gcd(y, N) = 1 =$ greatest common divisor of y and N)

there is a large probability that

$$\gcd(y^{r/2} + 1, N) \cdot \gcd(y^{r/2} - 1, N) \;=\; u \cdot v \;=\; N$$

and thus u **and** v **are the factors searched for**,
if r **is the period of the function** $f(a) = y^a \bmod N$.

Trick 1: Transformation of the problem (I)

For an **integer** N and an **arbitrarily chosen integer** $y \leq N$

(with $\gcd(y,N)=1=$ greatest common divisor of y and N)

there is a large probability that

$$\gcd(y^{r/2}+1,N)\cdot\gcd(y^{r/2}-1,N) \;=\; u\cdot v \;=\; N$$

and thus u **and** v **are the factors searched for**,
if r **is the period of the function** $f(a) = y^a \bmod N$.

Notes:

- The integer y can be chosen arbitrarily, provided it has no common divisor (other than 1) with N.

Trick 1: Transformation of the problem (I)

For an **integer** N and an **arbitrarily chosen integer** $y \leq N$

(with $\gcd(y, N) = 1 =$ greatest common divisor of y and N)

there is a large probability that

$$\gcd(y^{r/2} + 1, N) \cdot \gcd(y^{r/2} - 1, N) \;=\; u \cdot v \;=\; N$$

and thus u **and** v **are the factors searched for**,
if r **is the period of the function** $f(a) = y^a \bmod N$.

Notes:

- The integer y can be chosen arbitrarily, provided it has no common divisor (other than 1) with N.
- Not every choice of y leads to a success, i. e. there are integers that will not work ("failures").

Trick 1: Transformation of the problem (II)

Example: $N = 15 \rightarrow y = 2, 4, 7, 8, \underline{11}, 13,$ or 14.

Trick 1: Transformation of the problem (II)

Example: $N = 15 \rightarrow y = 2, 4, 7, 8, \underline{11}, 13,$ or 14.

Arbitrary choice of $\boldsymbol{y}$**=11:**

Trick 1: Transformation of the problem (II)

Example: $N = 15 \rightarrow y = 2, 4, 7, 8, \underline{11}, 13,$ or 14.

Arbitrary choice of y=11:

$$\begin{aligned}
11^0 \bmod 15 &= 1 \bmod 15 = (0 \cdot 15 + 1) \bmod 15 = 1 \\
11^1 \bmod 15 &= 11 \bmod 15 = (0 \cdot 15 + 11) \bmod 15 = 11 \\
11^2 \bmod 15 &= 121 \bmod 15 = (8 \cdot 15 + 1) \bmod 15 = 1 \\
11^3 \bmod 15 &= 1331 \bmod 15 = (88 \cdot 15 + 11) \bmod 15 = 11
\end{aligned}$$

$$\longrightarrow r = 2 \text{ (für } y = 11) \longrightarrow \text{gcd}(11^{2/2} \pm 1, 15)$$

$$\longrightarrow \text{gcd}(12, 15) \cdot \text{gcd}(10, 15) = 3 \cdot 5 = 15$$

Trick 1: Transformation of the problem (III)

Example: $N = 15 \rightarrow y = 2, 4, \underline{7}, 8, 11, 13,$ oder 14.

Alternatively, choose $\boldsymbol{y}$=7 (instead of $\boldsymbol{y} = 11$).

Trick 1: Transformation of the problem (III)

Example: $N = 15 \rightarrow y = 2, 4, \underline{7}, 8, 11, 13,$ oder 14.

Alternatively, choose y=7 (instead of $y = 11$).

$$
\begin{aligned}
7^0 \bmod 15 &= 1 \bmod 15 = (0 \cdot 15 + 1) \bmod 15 = 1 \\
7^1 \bmod 15 &= 7 \bmod 15 = (0 \cdot 15 + 7) \bmod 15 = 7 \\
7^2 \bmod 15 &= 49 \bmod 15 = (3 \cdot 15 + 4) \bmod 15 = 4 \\
7^3 \bmod 15 &= 343 \bmod 15 = (22 \cdot 15 + 13) \bmod 15 = 13 \\
7^4 \bmod 15 &= 2401 \bmod 15 = (160 \cdot 15 + 1) \bmod 15 = 1 \\
7^5 \bmod 15 &= 16807 \bmod 15 = (1120 \cdot 15 + 7) \bmod 15 = 7
\end{aligned}
$$

$$\longrightarrow r = 4 \text{ (für } y = 7) \longrightarrow \gcd(7^{4/2} \pm 1, 15)$$

$$\longrightarrow \gcd(50, 15) \cdot \gcd(48, 15) = 5 \cdot 3 = 15$$

Trick 1: Transformation of the problem (III)

Example: $N = 15 \rightarrow y = 2, 4, \underline{7}, 8, 11, 13,$ oder 14.

Alternatively, choose y=7 (instead of $y = 11$).

$$
\begin{aligned}
7^0 \bmod 15 &= 1 \bmod 15 = (0 \cdot 15 + 1) \bmod 15 = 1 \\
7^1 \bmod 15 &= 7 \bmod 15 = (0 \cdot 15 + 7) \bmod 15 = 7 \\
7^2 \bmod 15 &= 49 \bmod 15 = (3 \cdot 15 + 4) \bmod 15 = 4 \\
7^3 \bmod 15 &= 343 \bmod 15 = (22 \cdot 15 + 13) \bmod 15 = 13 \\
7^4 \bmod 15 &= 2401 \bmod 15 = (160 \cdot 15 + 1) \bmod 15 = 1 \\
7^5 \bmod 15 &= 16807 \bmod 15 = (1120 \cdot 15 + 7) \bmod 15 = 7
\end{aligned}
$$

$$\longrightarrow r = 4 \text{ (für } y = 7) \longrightarrow \gcd(7^{4/2} \pm 1, 15)$$

$$\longrightarrow \gcd(50, 15) \cdot \gcd(48, 15) = 5 \cdot 3 = 15$$

Note: The choice of $y = 14$ results in a failure !

Trick 2: Quantum Fourier transform QFT (I)

Problem: the efforts to find the period r grow exponentially with the size of N !

Trick 2: Quantum Fourier transform QFT (I)

Problem: the efforts to find the period r grow exponentially with the size of N !

Solution: Make use of the very specific properties of the (quantum) Fourier transform.

Trick 2: Quantum Fourier transform QFT (I)

Problem: the efforts to find the period r grow exponentially with the size of N !

Solution: Make use of the very specific properties of the (quantum) Fourier transform.

The **Quantum Fourier transform (QFT)**

$$\sum_{j=0}^{K-1} x_j \,|\, j \,\rangle \xrightarrow{\text{QFT}} \sum_{k=0}^{K-1} y_k \,|\, k \,\rangle \,, \; y_k \;=\; \sum_{j=0}^{K-1} x_j \, \mathrm{e}^{2\pi i \, \frac{jk}{K}}$$

is completely analogous to the classical discrete Fourier transform (DFT), except the fact that in the **QFT** the **amplitudes** are transformed.

Trick 2: Quantum Fourier transform (II)

Relevant properties of the (Q)FT:

1. A possible period r in $x_{0,1,\ldots,K-1}$ changes into a period K/r in the $y_{0,1,\ldots,K-1}$.

Trick 2: Quantum Fourier transform (II)

Relevant properties of the (Q)FT:

1. A possible period r in $x_{0,1,\ldots,K-1}$ changes into a period K/r in the $y_{0,1,\ldots,K-1}$.

2. A constant shift transforms into a phase factor

$$\sum_{j=0}^{K-1} x_j \,|\, j+l \,\rangle \xrightarrow{\text{QFT}} \sum_{k=0}^{K-1} \mathrm{e}^{2\pi i \frac{k\,l}{K}} y_k \,|\, k \,\rangle \;,$$

but the (measurable) probabilities remain unchanged
($|\mathrm{e}^{2\pi i \frac{k\,l}{K}} y_k|^2 = |y_k|^2$).

Efficiency of the Quantum Fourier transform QFT

Efficiency:

- Classical discrete fast Fourier transform: scales as $K\,2^K$.
- **Quantum Fourier transform (QFT):** scales as K^2.

Efficiency of the Quantum Fourier transform QFT

Efficiency:

- Classical discrete fast Fourier transform: scales as $K\,2^{K}$.
- **Quantum Fourier transform (QFT):** scales as K^{2}.

Quantum parallelism transforms a *difficult* into a *simple* problem.

Efficiency of the Quantum Fourier transform QFT

Efficiency:

- Classical discrete fast Fourier transform: scales as $K\,2^K$.
- **Quantum Fourier transform (QFT):** scales as K^2.

Quantum parallelism transforms a *difficult* into a *simple* problem.

Fourier transforms are really of massive practical interest !

Efficiency of the Quantum Fourier transform QFT

Efficiency:

- Classical discrete fast Fourier transform: scales as $K\,2^K$.
- **Quantum Fourier transform (QFT):** scales as K^2.

Quantum parallelism transforms a *difficult* into a *simple* problem.

Fourier transforms are really of massive practical interest !

Problem: The results of the QFT (the amplitudes y_k) are not directly accessible (wave-function collapse) !

Shor for factorizing 15 (I): 2 registers

The Shor algorithm given explicitly for the example of factorizing the number $N = 15$.

Two registers are needed:

Register 1: $k = 3$ qubits for representing the numbers 0 to 7 $(\leq N/2)$

Shor for factorizing 15 (I): 2 registers

The Shor algorithm given explicitly for the example of factorizing the number $N = 15$.

Two registers are needed:

Register 1: $k = 3$ qubits for representing the numbers 0 to 7 $(\leq N/2)$

Register 2: $m = 4$ qubits for the numbers 0 to 15 $(\leq N)$

Shor for factorizing 15 (I): 2 registers

The Shor algorithm given explicitly for the example of factorizing the number $N = 15$.

Two registers are needed:

Register 1: $k = 3$ qubits for representing the numbers 0 to 7 ($\leq N/2$)

Register 2: $m = 4$ qubits for the numbers 0 to 15 ($\leq N$)

Choose a number $y \leq 15$ (with $\gcd(y, 15) = 1$), e. g. $y = 11$.

Shor for factorizing 15 (I): 2 registers

The Shor algorithm given explicitly for the example of factorizing the number $N = 15$.

Two registers are needed:

Register 1: $k = 3$ qubits for representing the numbers 0 to 7 $(\leq N/2)$

Register 2: $m = 4$ qubits for the numbers 0 to 15 $(\leq N)$

Choose a number $y \leq 15$ (with $\gcd(y, 15) = 1$), e. g. $y = 11$.

The Shor algorithm can be split into 4 steps:

1. Initialization: Set all 7 qubits to $|\,0\,\rangle$:

$|\,0000000\,\rangle$ $(= |\,\Psi_1\,\rangle_1 |\,\Phi_1\,\rangle_2)$.

Shor for factorizing 15 (II): Input preparation

2. Prepare input: Put the 1st register into the superposition of $|\,0\,\rangle$ and $|\,1\,\rangle$, i. e. the integers 0 to 7:

$$|\,0000000\,\rangle \;\rightarrow\; \frac{1}{\sqrt{8}}\Big(\underbrace{|\,000\,\rangle}_{|\,0\,\rangle}+\underbrace{|\,001\,\rangle}_{|\,1\,\rangle}+\underbrace{|\,010\,\rangle}_{|\,2\,\rangle} + \cdots + \underbrace{|\,111\,\rangle}_{|\,7\,\rangle}\Big)\,|\,0000\,\rangle$$

$$|\,\Psi_1\,\rangle_1|\,\Phi_1\,\rangle_2 \;\rightarrow\; \frac{1}{\sqrt{2^k}}\sum_{a=0}^{2^k-1}|\,a\,\rangle_1|\,0\,\rangle_2$$

Shor for factorizing 15 (III): evaluate $f(a)$

3. **Evaluate $f(a)$** $= y^a \,\mathrm{mod} N$ (here $11^a \,\mathrm{mod} 15$) for all a in the 1st register $(0 \ldots 7)$ simultaneously (quantum parallelism). Store the result in the 2nd register:

Shor for factorizing 15 (III): evaluate $f(a)$

3. **Evaluate $f(a)$** $= y^a \,\mathrm{mod} N$ (here $11^a \,\mathrm{mod} 15$) for all a
in the 1st register $(0 \ldots 7)$ simultaneously (quantum parallelism).
Store the result in the 2nd register:

$$\frac{1}{\sqrt{8}}\Big(\underbrace{|\,000\,\rangle}_{|\,0\,\rangle} \underbrace{|\,0001\,\rangle}_{|\,1\,\rangle} + \underbrace{|\,001\,\rangle}_{|\,1\,\rangle} \underbrace{|\,1011\,\rangle}_{|\,11\,\rangle} + \underbrace{|\,010\,\rangle}_{|\,2\,\rangle} \underbrace{|\,0001\,\rangle}_{|\,1\,\rangle} + \cdots + \underbrace{|\,111\,\rangle}_{|\,7\,\rangle} \underbrace{|\,1011\,\rangle}_{|\,11\,\rangle} \Big)$$

Shor for factorizing 15 (III): evaluate $f(a)$

3. Evaluate $f(a)$ $= y^a \bmod N$ (here $11^a \bmod 15$) for all a
in the 1st register $(0 \ldots 7)$ simultaneously (quantum parallelism).
Store the result in the 2nd register:

$$\frac{1}{\sqrt{8}}\Big(\underbrace{|\,000\,\rangle}_{|\,0\,\rangle}\underbrace{|\,0001\,\rangle}_{|\,1\,\rangle} + \underbrace{|\,001\,\rangle}_{|\,1\,\rangle}\underbrace{|\,1011\,\rangle}_{|\,11\,\rangle}$$

$$+ \underbrace{|\,010\,\rangle}_{|\,2\,\rangle}\underbrace{|\,0001\,\rangle}_{|\,1\,\rangle} + \cdots + \underbrace{|\,111\,\rangle}_{|\,7\,\rangle}\underbrace{|\,1011\,\rangle}_{|\,11\,\rangle}\Big)$$

$$= \frac{1}{\sqrt{8}}\Big(\Big[\underbrace{|\,000\,\rangle}_{|\,0\,\rangle} + \underbrace{|\,010\,\rangle}_{|\,2\,\rangle} + \underbrace{|\,100\,\rangle}_{|\,4\,\rangle} + \underbrace{|\,110\,\rangle}_{|\,6\,\rangle}\Big]\underbrace{|\,0001\,\rangle}_{|\,1\,\rangle}$$

$$+ \Big[\underbrace{|\,001\,\rangle}_{|\,1\,\rangle} + \underbrace{|\,011\,\rangle}_{|\,3\,\rangle} + \underbrace{|\,101\,\rangle}_{|\,5\,\rangle} + \underbrace{|\,111\,\rangle}_{|\,7\,\rangle}\Big]\underbrace{|\,1011\,\rangle}_{|\,11\,\rangle}\Big)$$

Shor for factorizing 15 (IV): r in 1st register (1)

The result of the simultaneous evaluation of $f(a) = y^a \bmod N$ (here $11^a \bmod 15$) for all a in 1st register $(0 \ldots 7)$ is in the 2nd register:

Shor for factorizing 15 (IV): r in 1st register (1)

The result of the simultaneous evaluation of $f(a) = y^a \bmod N$ (here $11^a \bmod 15$) for all a in 1st register $(0\ldots7)$ is in the 2nd register:

$$\frac{1}{\sqrt{8}}\left(\left[\underbrace{|\,000\,\rangle}_{|\,0\,\rangle}+\underbrace{|\,010\,\rangle}_{|\,2\,\rangle}+\underbrace{|\,100\,\rangle}_{|\,4\,\rangle}+\underbrace{|\,110\,\rangle}_{|\,6\,\rangle}\right]\underbrace{|\,0001\,\rangle}_{|\,1\,\rangle}\right.$$

$$\left.+\left[\underbrace{|\,001\,\rangle}_{|\,1\,\rangle}+\underbrace{|\,011\,\rangle}_{|\,3\,\rangle}+\underbrace{|\,101\,\rangle}_{|\,5\,\rangle}+\underbrace{|\,111\,\rangle}_{|\,7\,\rangle}\right]\underbrace{|\,1011\,\rangle}_{|\,11\,\rangle}\right)$$

Shor for factorizing 15 (IV): r in 1st register (1)

The result of the simultaneous evaluation of $f(a) = y^a \bmod N$ (here $11^a \bmod 15$) for all a in 1st register ($0 \ldots 7$) is in the 2nd register:

$$\frac{1}{\sqrt{8}}\Bigg(\Big[\underbrace{|\,000\,\rangle}_{|\,0\,\rangle} + \underbrace{|\,010\,\rangle}_{|\,2\,\rangle} + \underbrace{|\,100\,\rangle}_{|\,4\,\rangle} + \underbrace{|\,110\,\rangle}_{|\,6\,\rangle}\Big]\;\underbrace{|\,0001\,\rangle}_{|\,1\,\rangle}$$

$$+\Big[\underbrace{|\,001\,\rangle}_{|\,1\,\rangle} + \underbrace{|\,011\,\rangle}_{|\,3\,\rangle} + \underbrace{|\,101\,\rangle}_{|\,5\,\rangle} + \underbrace{|\,111\,\rangle}_{|\,7\,\rangle}\Big]\;\underbrace{|\,1011\,\rangle}_{|\,11\,\rangle}\Bigg)$$

$$|\,\Psi_3\,\rangle_1|\,\Phi_3\,\rangle_2 \;=\; \frac{1}{\sqrt{2^k}} \sum_{a=0}^{2^k-1} |\,a\,\rangle_1|\,y^a \bmod N\,\rangle_2$$

$$\overset{A<\frac{2^k-l}{r}}{=} \sum_{l=0}^{r-1}\left[\frac{1}{\sqrt{r(A+1)}}\sum_{j=0}^{A}|\,l+jr\,\rangle_1\right]|\,y^l \bmod N\,\rangle_2$$

Shor for factorizing 15 (IV): r in 1st register (1)

The result of the simultaneous evaluation of $f(a) = y^a \bmod N$ (here $11^a \bmod 15$) for all a in 1st register ($0 \ldots 7$) is in the 2nd register:

$$\frac{1}{\sqrt{8}}\Bigg(\Big[\underbrace{|\,000\,\rangle}_{|\,0\,\rangle} + \underbrace{|\,010\,\rangle}_{|\,2\,\rangle} + \underbrace{|\,100\,\rangle}_{|\,4\,\rangle} + \underbrace{|\,110\,\rangle}_{|\,6\,\rangle}\Big]\,\underbrace{|\,0001\,\rangle}_{|\,1\,\rangle}$$

$$+\Big[\underbrace{|\,001\,\rangle}_{|\,1\,\rangle} + \underbrace{|\,011\,\rangle}_{|\,3\,\rangle} + \underbrace{|\,101\,\rangle}_{|\,5\,\rangle} + \underbrace{|\,111\,\rangle}_{|\,7\,\rangle}\Big]\,\underbrace{|\,1011\,\rangle}_{|\,11\,\rangle}\Bigg)$$

$$|\,\Psi_3\,\rangle_1|\,\Phi_3\,\rangle_2 \;=\; \frac{1}{\sqrt{2^k}}\sum_{a=0}^{2^k-1}|\,a\,\rangle_1|\,y^a \bmod N\,\rangle_2$$

$$\overset{A<\frac{2^k-l}{r}}{=}\;\sum_{l=0}^{r-1}\left[\frac{1}{\sqrt{r(A+1)}}\sum_{j=0}^{A}|\,l+jr\,\rangle_1\right]|\,y^l \bmod N\,\rangle_2$$

Register 1 contains now the period r of interest, but only for identical measurement results in register 2!

Shor for factorizing 15 (V): r in 1st register (2)

The searched for **period r** (here $r = 2$) is the distance between the components ($|0\rangle, |2\rangle, |4\rangle, |6\rangle$ or $|1\rangle, |3\rangle, |5\rangle, |7\rangle$) in the 1st register for a **single** state of the 2nd register (1 or 11).

$$\frac{1}{\sqrt{8}}\left(\left[\underbrace{|000\rangle}_{|0\rangle}+\underbrace{|010\rangle}_{|2\rangle}+\underbrace{|100\rangle}_{|4\rangle}+\underbrace{|110\rangle}_{|6\rangle}\right]\underbrace{|0001\rangle}_{|1\rangle}\right.$$
$$\left.+\left[\underbrace{|001\rangle}_{|1\rangle}+\underbrace{|011\rangle}_{|3\rangle}+\underbrace{|101\rangle}_{|5\rangle}+\underbrace{|111\rangle}_{|7\rangle}\right]\underbrace{|1011\rangle}_{|11\rangle}\right)$$

$$|\Psi_3\rangle_1|\Phi_3\rangle_2 \overset{A<\frac{2^k-l}{r}}{=} \sum_{l=0}^{r-1}\left[\frac{1}{\sqrt{r(A+1)}}\sum_{j=0}^{A}|l+jr\rangle_1\right]|y^l \bmod N\rangle_2$$

Only the multiple repetition of the experiment yields the period r.

Shor for factorizing 15 (V): r in 1st register (2)

The searched for **period r** (here $r = 2$) is the distance between the components ($|0\rangle, |2\rangle, |4\rangle, |6\rangle$ <u>or</u> $|1\rangle, |3\rangle, |5\rangle, |7\rangle$) in the **1st register** for a **single** state of the **2nd register** (1 <u>or</u> 11).

$$\frac{1}{\sqrt{8}}\left(\left[\underbrace{|000\rangle}_{|0\rangle}+\underbrace{|010\rangle}_{|2\rangle}+\underbrace{|100\rangle}_{|4\rangle}+\underbrace{|110\rangle}_{|6\rangle}\right]\underbrace{|0001\rangle}_{|1\rangle}\right.$$

$$\left.+\left[\underbrace{|001\rangle}_{|1\rangle}+\underbrace{|011\rangle}_{|3\rangle}+\underbrace{|101\rangle}_{|5\rangle}+\underbrace{|111\rangle}_{|7\rangle}\right]\underbrace{|1011\rangle}_{|11\rangle}\right)$$

$$|\Psi_3\rangle_1 |\Phi_3\rangle_2 \overset{A<\frac{2^k-l}{r}}{=} \sum_{l=0}^{r-1}\left[\frac{1}{\sqrt{r(A+1)}}\sum_{j=0}^{A}|l+jr\rangle_1\right]|y^l \bmod N\rangle_2$$

Only the multiple repetition of the experiment yields the period r.

The mean number of necessary repetitions grows **exponentially** with the number of digits of N !

Shor for factorizing 15 (VI): QFT

4. Application of the QFT onto register 1:

$$\longrightarrow \quad \frac{1}{2}\Bigg(\Big[\underbrace{|\,000\,\rangle}_{|\,0\,\rangle} + \underbrace{|\,100\,\rangle}_{|\,4\,\rangle}\Big]\underbrace{|\,0001\,\rangle}_{|\,1\,\rangle}$$

$$+\Big[\underbrace{|\,000\,\rangle}_{|\,0\,\rangle} + \underbrace{\mathrm{e}^{i\pi}\,|\,100\,\rangle}_{-\,|\,4\,\rangle}\Big]\underbrace{|\,1011\,\rangle}_{|\,11\,\rangle}\Bigg)$$

$$|\,\Psi_4\,\rangle_1 |\,\Phi_4\,\rangle_2 \;=\; \frac{1}{r}\sum_{l=0}^{r-1}\left[\sum_{j=0}^{r-1}\mathrm{e}^{2\pi i \frac{l\,j}{r}}\,|\,j\,\frac{2^k}{r}\,\rangle_1\right]|\,y^l \bmod N\,\rangle_2$$

Shor for factorizing 15 (VI): QFT

4. Application of the QFT onto register 1:

$$\longrightarrow \frac{1}{2}\Bigg(\Big[\underbrace{|\,000\,\rangle}_{|\,0\,\rangle}+\underbrace{|\,100\,\rangle}_{|\,4\,\rangle}\Big]\underbrace{|\,0001\,\rangle}_{|\,1\,\rangle}$$

$$+\Big[\underbrace{|\,000\,\rangle}_{|\,0\,\rangle}+\underbrace{e^{i\pi}\,|\,100\,\rangle}_{-|\,4\,\rangle}\Big]\underbrace{|\,1011\,\rangle}_{|\,11\,\rangle}\Bigg)$$

$$|\,\Psi_4\,\rangle_1|\,\Phi_4\,\rangle_2 \;=\; \frac{1}{r}\sum_{l=0}^{r-1}\left[\sum_{j=0}^{r-1} e^{2\pi i\frac{l\,j}{r}}\,|\,j\,\frac{2^k}{r}\,\rangle_1\right]|\,y^l \bmod N\,\rangle_2$$

Independent of register 2 **every measurement** yields either $\mathbf{0}$ or a multiple of the new period $2^k/r$ (here 4 due to $r=2$ and $k=3$):

- $|\,0\,\rangle \equiv |\,000\,\rangle$: failure $\longrightarrow$ new attempt.

Shor for factorizing 15 (VI): QFT

4. Application of the QFT onto register 1:

$$\longrightarrow \quad \frac{1}{2}\left(\left[\underbrace{|\,000\,\rangle}_{|\,0\,\rangle} + \underbrace{|\,100\,\rangle}_{|\,4\,\rangle} \right] \underbrace{|\,0001\,\rangle}_{|\,1\,\rangle} + \left[\underbrace{|\,000\,\rangle}_{|\,0\,\rangle} + \underbrace{e^{i\pi}\,|\,100\,\rangle}_{-\,|\,4\,\rangle} \right] \underbrace{|\,1011\,\rangle}_{|\,11\,\rangle} \right)$$

$$|\,\Psi_4\,\rangle_1 |\,\Phi_4\,\rangle_2 \;=\; \frac{1}{r} \sum_{l=0}^{r-1} \left[\sum_{j=0}^{r-1} e^{2\pi i \frac{l\,j}{r}} \,|\, j\,\frac{2^k}{r}\,\rangle_1 \right] |\, y^l \bmod N\,\rangle_2$$

Independent of register 2 **every measurement** yields either **0** or a multiple of the new period $2^k/r$ (here 4 due to $r = 2$ and $k = 3$):

- $|\,0\,\rangle \equiv |\,000\,\rangle$: failure $\longrightarrow$ new attempt.
- $|\,4\,\rangle \equiv |\,100\,\rangle$: $r = 2^{k=3}/4 = 8/4 = 2$ **(success!)**.

Shor for factorizing 15 (VII): analysis

$$|\,\Psi_4\,\rangle_1|\,\Phi_4\,\rangle_2 \;=\; \frac{1}{r}\sum_{l=0}^{r-1}\left[\,\sum_{j=0}^{r-1} \mathrm{e}^{2\pi i\frac{l\,j}{r}}\,|\,j\,\frac{2^k}{r}\,\rangle_1\right]|\,y^l\,\mathrm{mod}N\,\rangle_2$$

Problem: measurement yields $|\,j\,\frac{2^k}{r}\,\rangle$ with $j = 0, 1, \ldots, r-1$.

Shor for factorizing 15 (VII): analysis

$$|\,\Psi_4\,\rangle_1 |\,\Phi_4\,\rangle_2 \;=\; \frac{1}{r}\sum_{l=0}^{r-1}\left[\,\sum_{j=0}^{r-1} \mathrm{e}^{2\pi i\frac{l\,j}{r}}\,|\,j\,\frac{2^k}{r}\,\rangle_1\right]|\,y^l \bmod N\,\rangle_2$$

Problem: measurement yields $|\,j\,\frac{2^k}{r}\,\rangle$ with $j = 0, 1, \ldots, r-1$.

$j = 0 \rightarrow$ failure, but the probability decreases for increasing N.

Shor for factorizing 15 (VII): analysis

$$|\,\Psi_4\,\rangle_1|\,\Phi_4\,\rangle_2 \;=\; \frac{1}{r}\sum_{l=0}^{r-1}\left[\,\sum_{j=0}^{r-1} \mathrm{e}^{2\pi i\frac{l\,j}{r}}\,|\,j\,\frac{2^k}{r}\,\rangle_1\right]|\,y^l \,\mathrm{mod} N\,\rangle_2$$

Problem: measurement yields $|\,j\,\frac{2^k}{r}\,\rangle$ with $j = 0, 1, \ldots, r-1$.

$j = 0 \rightarrow$ failure, but the probability decreases for increasing N.

Larger $N \longrightarrow$ generally larger period r and larger j.

Example $N = 15$ with $y = 11$: no problem, since $r = 2 \rightarrow j = 0, 1$.

Shor for factorizing 15 (VII): analysis

$$|\,\Psi_4\,\rangle_1|\,\Phi_4\,\rangle_2 \;=\; \frac{1}{r}\sum_{l=0}^{r-1}\left[\,\sum_{j=0}^{r-1} \mathrm{e}^{2\pi i\frac{l\,j}{r}}\,|\,j\,\frac{2^k}{r}\,\rangle_1\right]|\,y^l \bmod N\,\rangle_2$$

Problem: measurement yields $|\,j\,\frac{2^k}{r}\,\rangle$ with $j = 0, 1, \ldots, r-1$.

$j = 0 \rightarrow$ failure, but the probability decreases for increasing N.

Larger $N \longrightarrow$ generally larger period r and larger j.

Example $N = 15$ with $y = 11$: no problem, since $r = 2 \rightarrow j = 0, 1$.

r from $j \cdot 2^k/r$: method of continued fractions.

Shor for factorizing 15 (VII): analysis

$$|\,\Psi_4\,\rangle_1|\,\Phi_4\,\rangle_2 \;=\; \frac{1}{r}\sum_{l=0}^{r-1}\left[\,\sum_{j=0}^{r-1} \mathrm{e}^{2\pi i\frac{l\,j}{r}}\,|\,j\,\frac{2^k}{r}\,\rangle_1\right]|\,y^l \bmod N\,\rangle_2$$

Problem: measurement yields $|\,j\,\frac{2^k}{r}\,\rangle$ with $j = 0, 1, \ldots, r-1$.

$j = 0 \rightarrow$ failure, but the probability decreases for increasing N.

Larger $N \longrightarrow$ generally larger period r and larger j.

Example $N = 15$ with $y = 11$: no problem, since $r = 2 \rightarrow j = 0, 1$.

r from $j \cdot 2^k/r$: method of continued fractions.

Important: 2^k and r grow exponentially with N,
but $2^k/r$ only polynomially!

Shor for factorizing 15 (VII): analysis

$$|\,\Psi_4\,\rangle_1|\,\Phi_4\,\rangle_2 \;=\; \frac{1}{r}\sum_{l=0}^{r-1}\left[\,\sum_{j=0}^{r-1} \mathrm{e}^{2\pi i\frac{l\,j}{r}}\,|\,j\,\frac{2^k}{r}\,\rangle_1\right]|\,y^l \bmod N\,\rangle_2$$

Problem: measurement yields $|\,j\,\frac{2^k}{r}\,\rangle$ with $j = 0, 1, \ldots, r-1$.

$j = 0 \rightarrow$ failure, but the probability decreases for increasing N.

Larger $N \longrightarrow$ generally larger period r and larger j.

Example $N = 15$ with $y = 11$: no problem, since $r = 2 \rightarrow j = 0, 1$.

r from $j \cdot 2^k/r$: method of continued fractions.

Important: 2^k and r grow exponentially with N,
but $2^k/r$ only polynomially !

Number of operations incl. probability for failures grows only polynomially with N !!!