S. KIMMEL

Current Crypto Systems

Alice

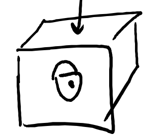
$m \xrightarrow[\text{using } K_{public}]{} \bar{m}_{Bob}$ encrypted for Bob

$\uparrow$ message

K_{public}

Bob

$K_{private}$



$\bar{m}_{bob}$

$\uparrow$ Eve

"If only I could factor..."

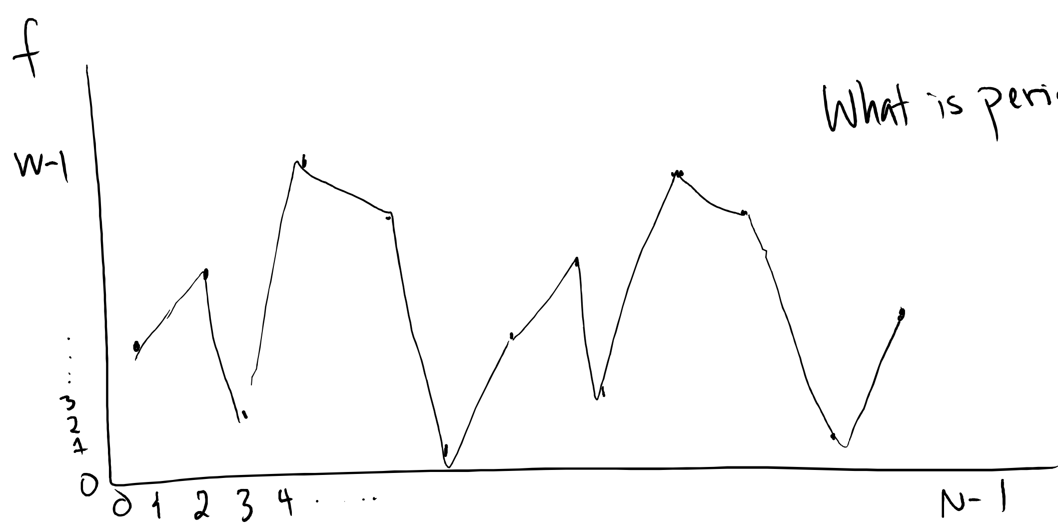
$\bar{m}_{Bob} \longrightarrow m$

$\uparrow$ using $K_{private}$

If you can find the period of a specific function, then can factor, then can break crypto systems

Period Finding Problem

- f has domain $[N]$. Notation: $[N] = \{0, 1, 2, \ldots N-1\}$
- Range of f is $[W]$, In other words: $f: [N] \to [W]$
- f periodic period $r \Rightarrow f(x) = f(x+r)$
- no repeats within a period: $\left(f(i) \neq f(j) \text{ if } |i-j| < r\right)$
- $N > r^2$



What is period?

What is classical query complexity of period finding?

A. $O(\log r)$ B. $O(r)$ C. $O(r^2)$ $O(N)$

- Let U_f act on $N \times R$ dimensional quantum system

$$U_f |x\rangle |y\rangle = |x\rangle |y + f(x) \bmod W\rangle$$

$$\underset{N\text{-dim}}{\uparrow} \quad \underset{W\text{-dim}}{\uparrow}$$

Changing standard basis labels:

Old Label	Vector	New Label
$\vert 00\rangle =$	$\begin{pmatrix}1\\0\\0\\0\end{pmatrix}$	$= \vert 0\rangle$
$\vert 01\rangle =$	$\begin{pmatrix}0\\1\\0\\0\end{pmatrix}$	$= \vert 1\rangle$
$\vert 10\rangle =$	$\begin{pmatrix}0\\0\\1\\0\end{pmatrix}$	$= \vert 2\rangle$

Binary Rep $\Rightarrow$ (old labels)

$\Leftarrow$ Base 10 Rep (new labels)

S. KIMMEL

What is classical query complexity of period finding?

A. $O(\log r)$ B. $O(r)$ C. $O(r^2)$ $O(N)$

$\Uparrow$

Ask $f(1), f(2), f(3)\ldots$ until get a repeat value. Need to look at r values

- Let U_f act on $N \times R$ dimensional quantum system

$$U_f \underbrace{|x\rangle}_{N\text{-dim}} \underbrace{|y\rangle}_{W\text{-dim}} = |x\rangle|y + f(x) \bmod W\rangle$$

✲ Changing standard basis labels:

Old Label	Vector	New Label
$\|00\rangle =$	$\begin{pmatrix}1\\0\\0\\0\end{pmatrix}$	$= \|0\rangle$
$\|01\rangle =$	$\begin{pmatrix}0\\1\\0\\0\end{pmatrix}$	$= \|1\rangle$
$\|10\rangle =$	$\begin{pmatrix}0\\0\\1\\0\end{pmatrix}$	$= \|2\rangle$

Binary Rep $\Rightarrow$

$\Leftarrow$ Base 10 Rep

S.KIMMEL

$f:[100] \to [50]$ Suppose $f(5) = 23$

domain range

$$U_f|5\rangle|30\rangle = |5\rangle|30+23 \bmod 50\rangle$$

$$= |5\rangle|3\rangle$$

$$= \begin{pmatrix} 0\\0\\0\\0\\1\\0\\ \vdots \end{pmatrix} \otimes \begin{pmatrix} 0\\0\\1\\0\\0\\ \vdots \end{pmatrix}$$

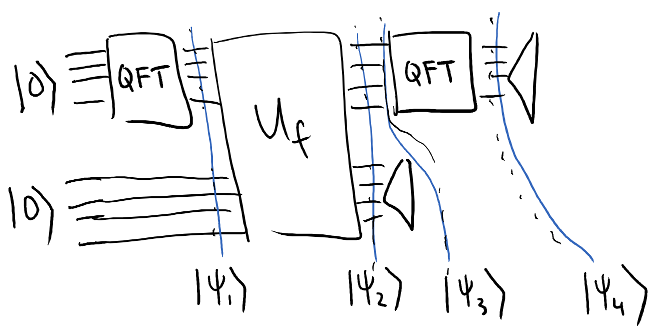
length 100 → ← length 50

S. KIMMEL

Basic Algorithm:

1. Prepare $|0\rangle_A |0\rangle_B$
   A: N-dim, B: W-dim
2. Apply QFT_N to A
3. Apply U_f to A, B
4. Measure B in standard basis
5. Apply QFT_N to A
6. Measure A in standard basis

Q: Write as circuit -



Full Algorithm

1. Run basic algorithm twice. Get outcomes y, y'.
   Do Classical postprocessing on y, y'. Outcome of postprocessing is r with high probability. Check by querying $f(1)$ and $f(r+1)$

S.KIMMEL

Important Unitary: Quantum Fourier Transform for Period Finding

$\boxed{\begin{array}{l} QFT_t \text{ is an } t \times t \text{ unitary} \\ \text{For standard basis state } |x\rangle: \\ QFT_t|x\rangle = \frac{1}{\sqrt{t}} \sum_{y=0}^{t-1} e^{\frac{2\pi i x y}{t}} |y\rangle \end{array}}$

Q: If apply QFT_t to a standard basis state $|x\rangle$ and then measure in standard basis, what is the probability of getting outcome y:

A) $\frac{1}{t}$ B) $\frac{1}{\sqrt{t}}$ C) $\frac{xy}{t}$ d $\frac{y}{t}$

S. KIMMEL

Important Unitary: Quantum Fourier Transform for Period Finding

QFT_t is an $t \times t$ unitary

For standard basis state $|x\rangle$:

$$QFT_t|x\rangle = \frac{1}{\sqrt{t}} \sum_{y=0}^{t-1} e^{\frac{2\pi i x y}{t}} |y\rangle$$

Q: If apply QFT_t to a standard basis state $|x\rangle$ and then measure in standard basis, what is the probability of getting outcome y:

$\boxed{\text{A) } \frac{1}{t}}$ B) $\frac{1}{\sqrt{t}}$ C) $\frac{xy}{t}$ d $\frac{y}{t}$

Because $\left|\frac{e^{\frac{2\pi i x y}{t}}}{\sqrt{t}}\right|^2 = \left|\frac{1}{\sqrt{t}}\right|^2 \left|e^{2\pi i x y/t}\right|^2 = \frac{1}{t}$

S.KIMMEL

QFT Tricks

Q: What is $\sum_{k=0}^{t-1} e^{2\pi i k y/t}$ if $k = n \cdot t$

y is integer

integer n

A) 0 B) 1 C) Depends on y D) t

⇑

Q: What is $\sum_{k=0}^{t-1} e^{2\pi i k y/t}$ if $k \neq nt$.

y is integer

integer n

A) 0 B) 1 C) Depends on y D) t

S. KIMMEL

QFT Tricks

Q: What is $\sum_{k=0}^{t-1} e^{2\pi i k y/t}$ if $k = n \cdot t$

y is integer; n integer

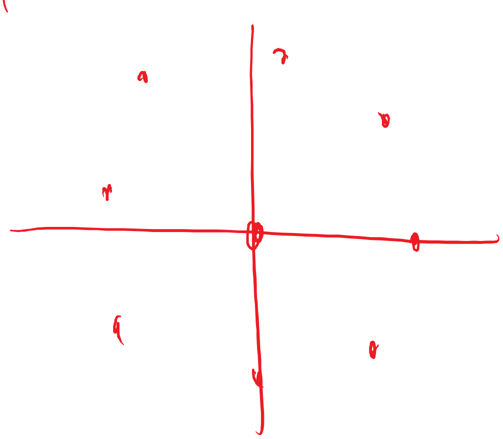
A) 0 B) 1 C) Depends on y D) t

$$\sum_{k=0}^{t-1} e^{2\pi i m t y/t} = \sum_{k=0}^{t-1} \left(e^{2\pi i}\right)^{my} = \sum_{k=0}^{t-1} (1)^{my} = \sum_{k=0}^{t-1} 1 = t$$

Q: What is $\sum_{k=0}^{t-1} e^{2\pi i k y/t}$ if $k \neq n \cdot t$

y is integer; integer n

A) 0 B) 1 C) Depends on y D) t



S. KIMMEL

Math Tricks

- $$\sum_{k=0}^{t-1} e^{\frac{2\pi i k y}{t}} = \sum_{k=0}^{t-1} \left(e^{\frac{2\pi i y}{t}}\right)^k$$

Geometric Series: $\sum_{k=0}^{t-1} r^k = \frac{1-r^{k+1}}{1-r}$ $(r \neq 1)$

$$= \frac{1-e^{\frac{2\pi i t y}{t}}}{1-e^{\frac{2\pi i y}{t}}} = \frac{1-e^{2\pi i y}}{1-e^{2\pi i y/t}} = 0$$

- $$\sum_{k=0}^{t-1} a_k \left(\sum_{j=0}^{t-1} b_j |j\rangle \right)$$

$\Downarrow$ Distribute

amplitude of state $|j\rangle$

$$\sum_{k=0}^{t-1} \sum_{j=0}^{t-1} a_k b_j |j\rangle \underset{\text{Swap order}}{\Longrightarrow} \sum_{j=0}^{t-1} \left(\sum_{k=0}^{t-1} a_k b_j \right) |j\rangle$$

S.KIMMEL

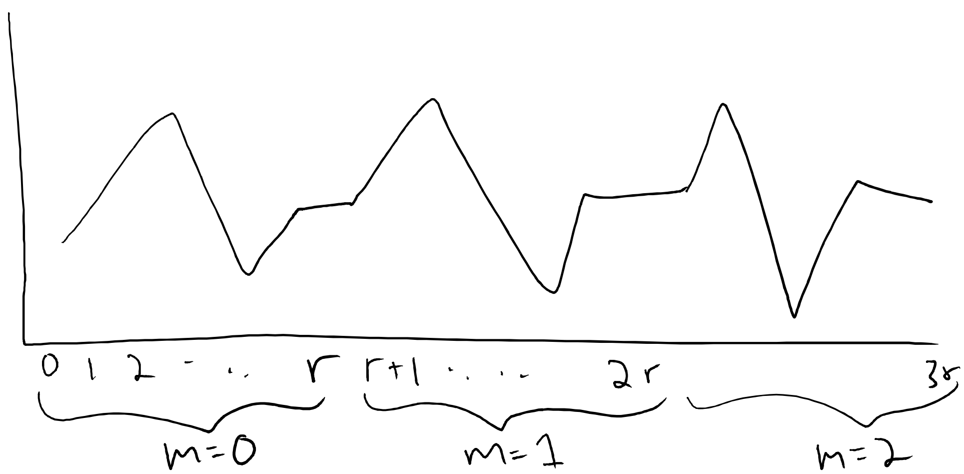
1. $|\psi_1\rangle = \left(QFT\,|0\rangle\right)|0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle_A |0\rangle_B$

2. $|\psi_2\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} U_f |x\rangle|0\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} |x\rangle|f(x)\rangle$

Recall: $f(x)$ is periodic. Let's write $x = m\underset{\uparrow \text{period}}{r} + b$

Q: What is $f(mr+b)$ equal to?

A) $f(r)$ B) $f(m)$ $\boxed{\text{C) } f(b)}$ D) $f(mr)$



$b \in [r]$

$m \in \left[\frac{N}{r}\right]$

$m=i$, $b=j$ corresponds to j^{th} element of i^{th} block of r

Rewrite x as $x = mr+b$. $\sum_x$ becomes $\sum_m \sum_b$