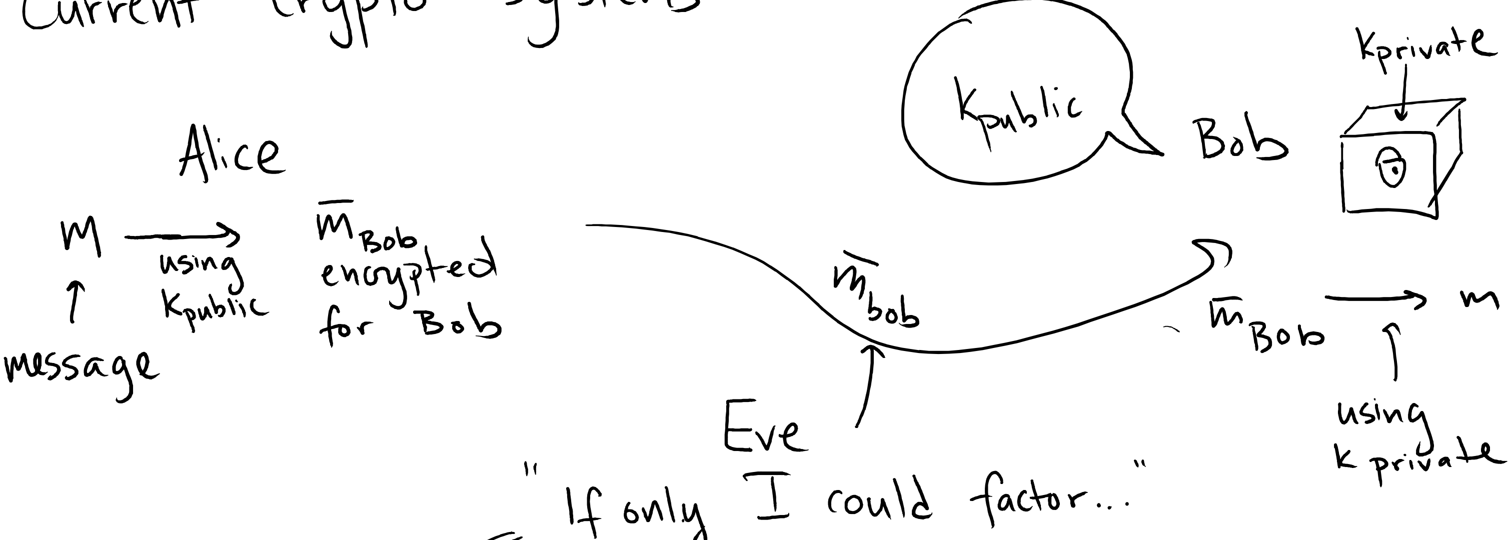
S.KIMMEL

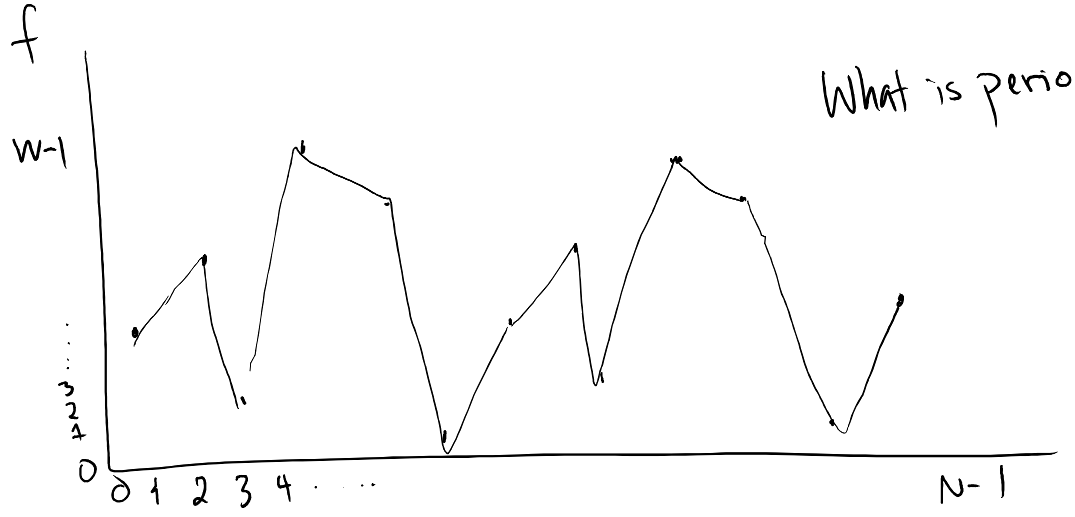
Current Crypto Systems


Alice
$m \xrightarrow[\text{using } K_{public}]{} \bar{m}_{Bob}$
message
encrypted for Bob
K_{public}
Bob
$K_{private}$
$\bar{m}_{bob}$
Eve
$\bar{m}_{Bob} \longrightarrow m$
using $k_{private}$
"If only I could factor..."

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: $[N] = \{0,1,2,\dots N-1\}$
- 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

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

* Changing standard basis labels:

$$\begin{array}{ccccccc}
 & \text{Old Label} & & \text{Vector} & & \text{New Label} & \\
 & |00\rangle & = & \begin{pmatrix}1\\0\\0\\0\end{pmatrix} & = & |0\rangle & \\
\text{Binary Rep} \Rightarrow & |01\rangle & = & \begin{pmatrix}0\\1\\0\\0\end{pmatrix} & = & |1\rangle & \Leftarrow \text{Base 10 Rep} \\
 & |10\rangle & = & \begin{pmatrix}0\\0\\1\\0\end{pmatrix} & = & |2\rangle &
\end{array}$$

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

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

✲ Changing standard basis labels:

$$\begin{array}{ccccccc}
 & & \text{Old Label} & \text{Vector} & & \text{New Label} & \\
 & & |00\rangle = & \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} & = & |0\rangle & \\
\text{Binary Rep} & \Rightarrow & |01\rangle = & \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} & = & |1\rangle & \Leftarrow \ \text{Base 10 Rep} \\
 & & |10\rangle = & \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} & = & |2\rangle &
\end{array}$$

$$f: \underset{\substack{\uparrow \\ \text{domain}}}{[100]} \to \underset{\substack{\uparrow \\ \text{range}}}{[50]}$$

Suppose $f(5) = 23$

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

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

$$= \underset{\text{length } 100 \,\rightarrow}{} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ \vdots \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ \vdots \end{pmatrix} \leftarrow \text{length } 50$$