Redefining the Origin of Secrecy in a Post-Quantum World

Speaker: Dr Frey Wilson, CTO @ Cavero Quantum

black hat EUROPE 2024

SECURITYWEEK
CYBERSECURITY NEWS, INSIGHTS & ANALYSIS

Malware & Threats | Security Operations | Security Architecture | Risk Management | CISO Strategy | ICS/OT | Funding/M&A

NETWORK SECURITY

Russian Telco Hijacked Internet Traffic of Major Networks – Accident or Malicious Action?

A huge BGP hijack by Russian state telecommunications provider Rostelecom diverted the traffic from more than 200 n Google, Amazon, Facebook and Cloudflare – to Russian servers on April 1. It may have been accidental, it may not.

By Kevin Townsend

The Register

Apple network traffic takes mysterious detour through Russia

Land of Putin capable of attacking routes in cyberspace as well as real world

Thomas Claburn

Wed 27 Jul 2022 // 18:56 UTC

Apple's internet traffic took an unwelcome detour through Russian networking equipment for about twelve hours between July 26 and July 27.

In a write-up for MANRS (Mutually Agreed Norms for Routing Security), a public interest group that looks after internet routing, Internet Society senior internet technology manager Aftab Siddiqui said that Russia's Rostelecom started announcing routes for part of Apple's network on Tuesday, a practice referred to as BGP (Border Gateway Protocol) hijacking.

ZDNET

belonge to those who embrace it today

trending | tech | innovation | business | security | advice | buying gu

/ tech

Home / Tech / Security

For two hours, a large chunk of European mobile traffic was rerouted through China

It was China Telecom, again. The same ISP accused last year of "hijacking the vital internet backbone of western

Reuters

World | Business | Markets | Sustainability | Legal | Breakingviews | Technology | Investigatio

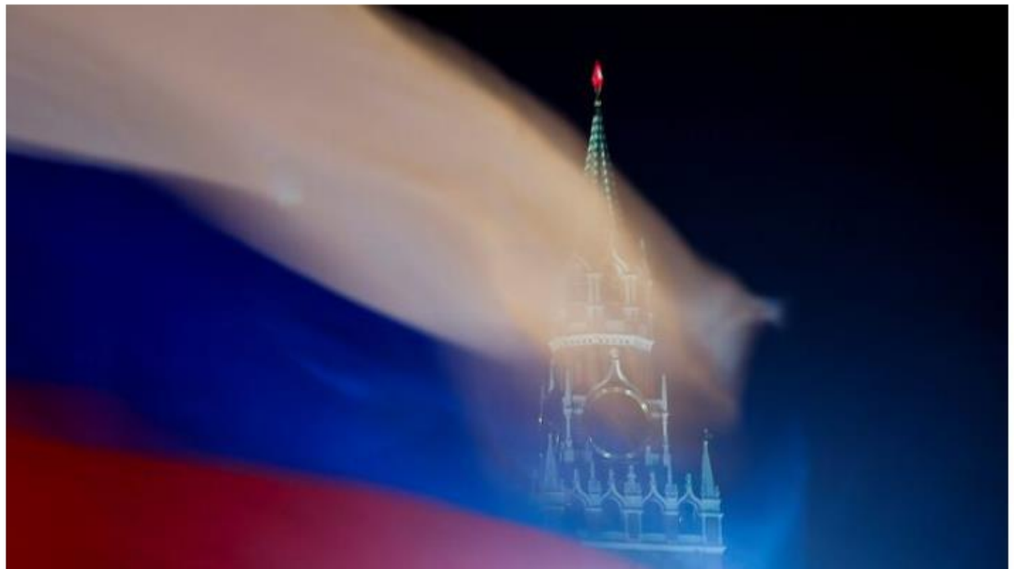
Europe

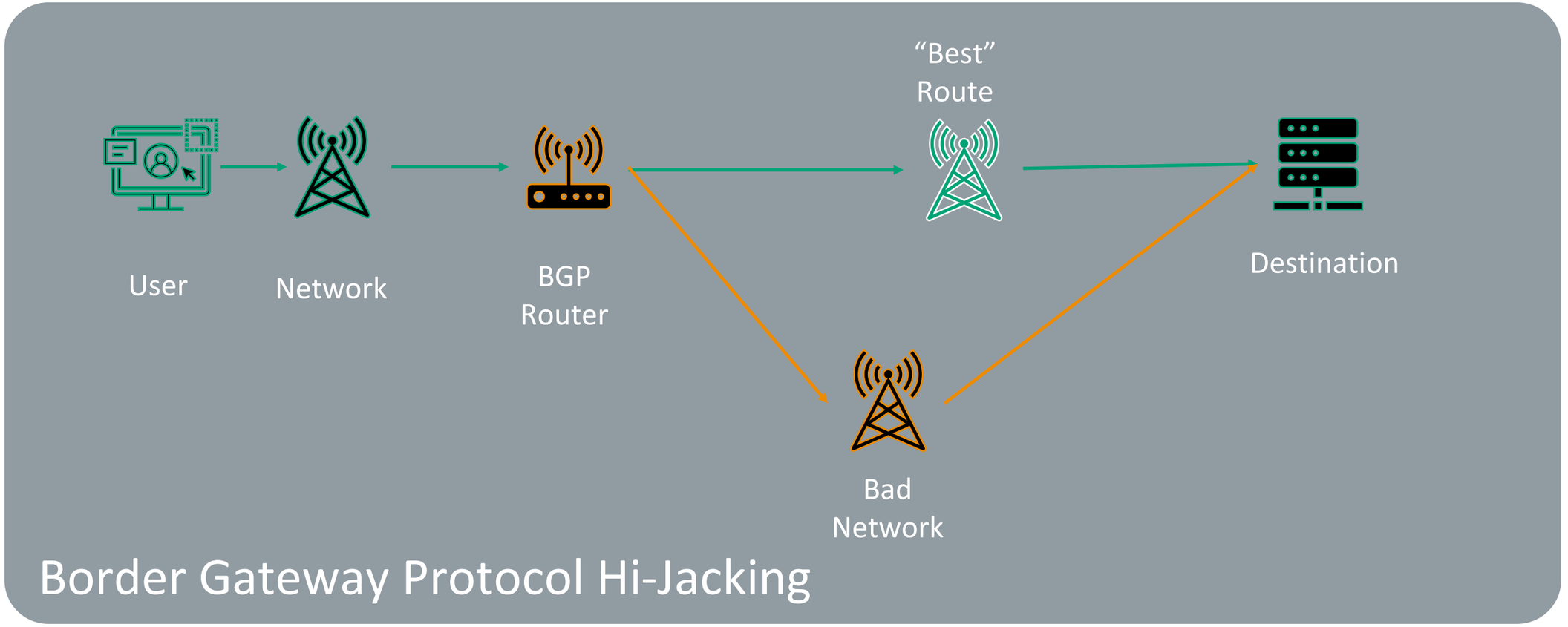
Russia reroutes internet traffic in occupied Ukraine to its infrastructure

By Reuters

May 2, 2022 10:23 PM GMT+1 · Updated 3 years ago

Aa





Border Gateway Protocol Hi-Jacking


```
hashcat (v6.2.1) starting...

CUDA API (CUDA 11.3)
====================
* Device #1: NVIDIA GeForce RTX 2080 Ti, 10137/11264 MB, 68MCU

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Optimizers applied:
* Optimized-Kernel
* Zero-Byte
* Precompute-Init
* Early-Skip
* Not-Iterated
* Prepended-Salt
* Single-Hash
* Single-Salt
* Brute-Force
* Raw-Hash

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1100 MB

e983672a03adcc9767b24584338eb378:00:hashcat

Session..........: hashcat
Status...........: Cracked
Hash.Name........: SolarWinds Serv-U
```

~~How do we encrypt our data better?~~

How do we share keys better?

```
$~: whoami
> Dr Frey Wilson
> CTO @ Cavero Quantum
> Quantum-Safe Symmetric Key Distribution
```

CAVERO QUANTUM

Ben Varcoe
Co-Founder

George Brumpton
Researcher

James Trenholme
CEO

UNIVERSITY OF LEEDS

…Many PhD Students since 2012

Random Number Generation

Asymmetric Keys

PKI

Signing

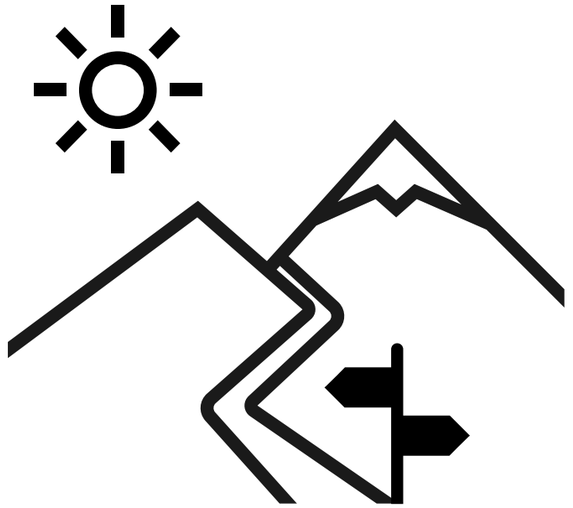
Authentication

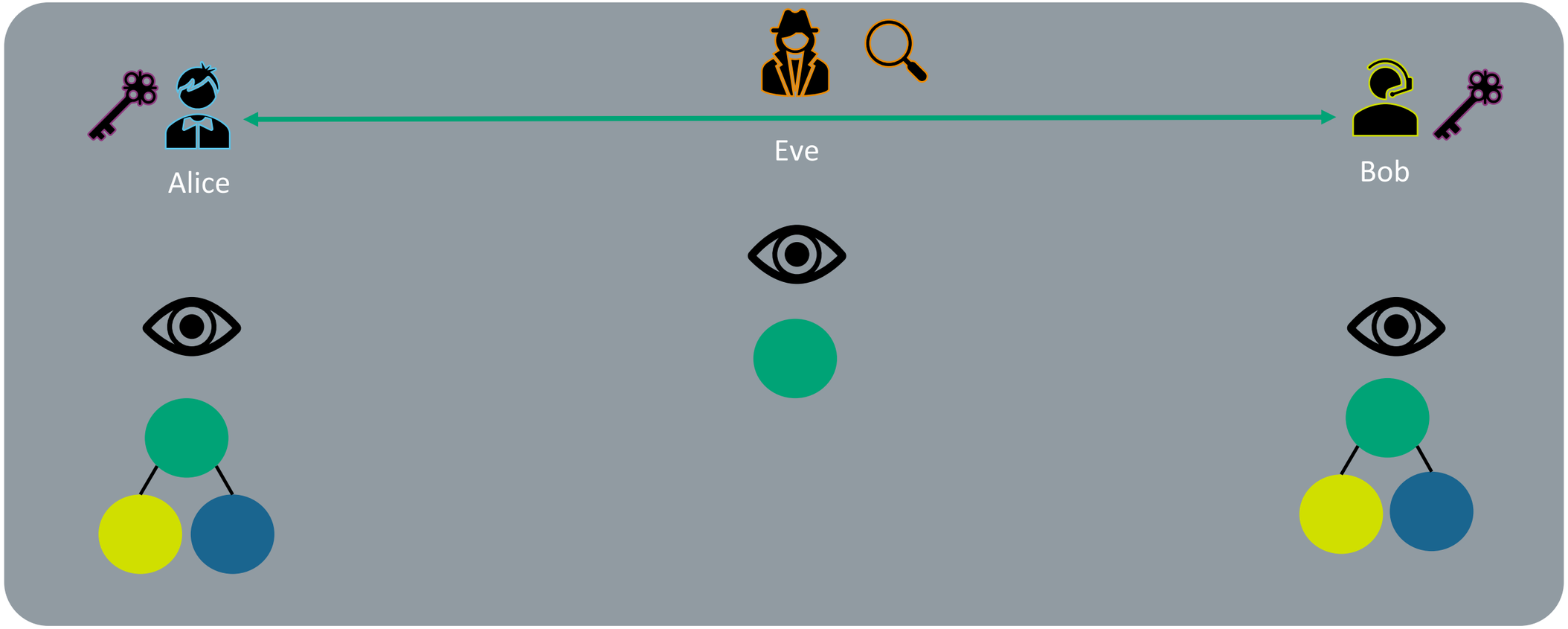
Sharing Symmetric Keys

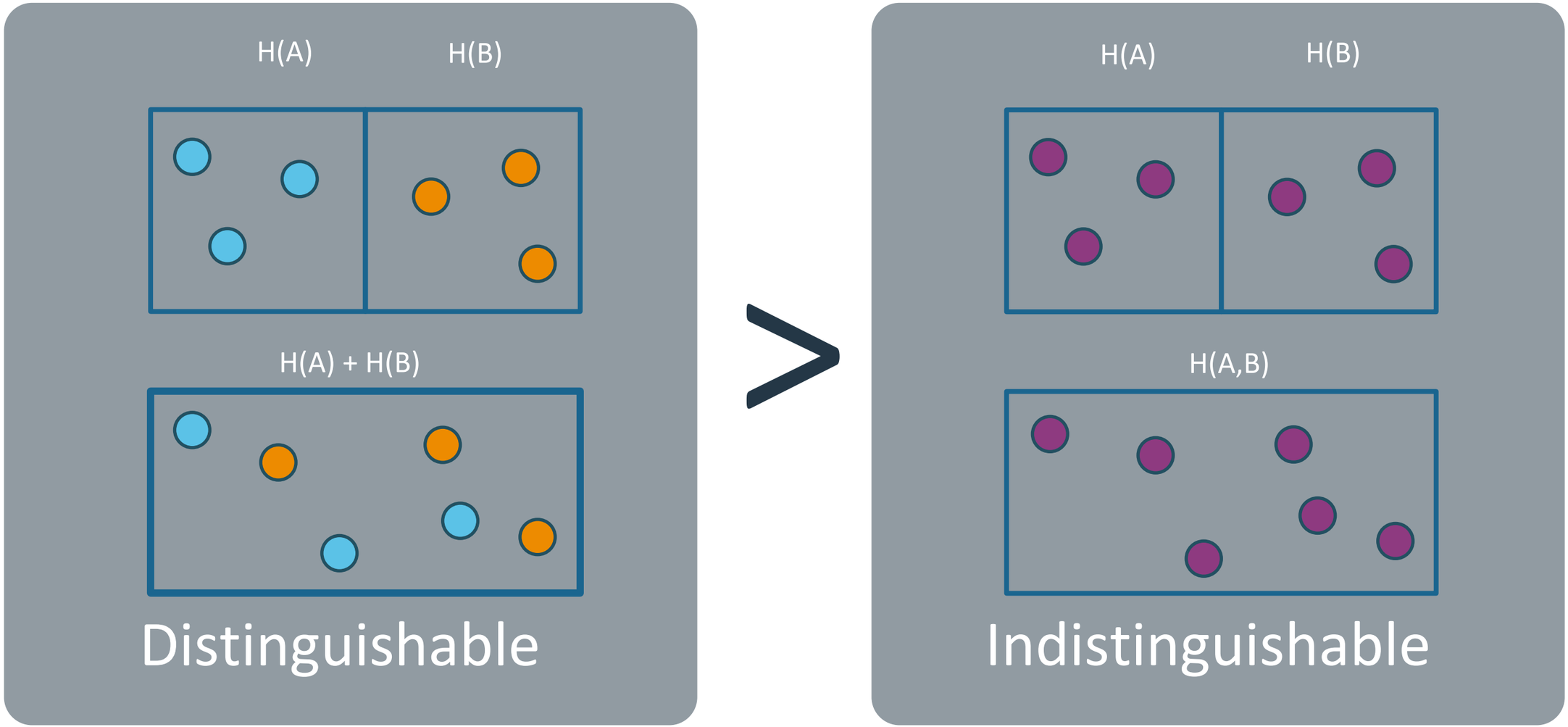
Ciphers

Roadmap

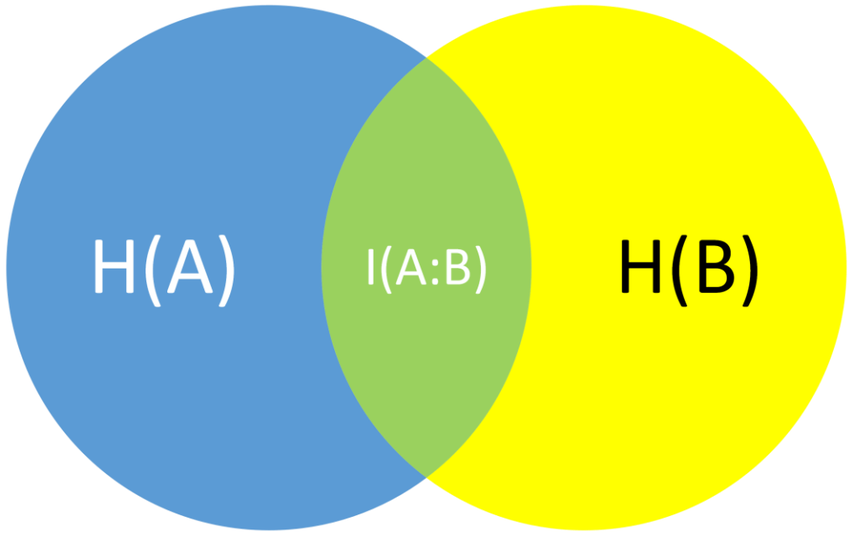
- Ingredients for Secrecy
- Existing Methods
- Implications of Quantum Computers
- Quantum Resilient Alternatives Method #1
- Quantum Resilient Alternatives Method #2
- A New Method!

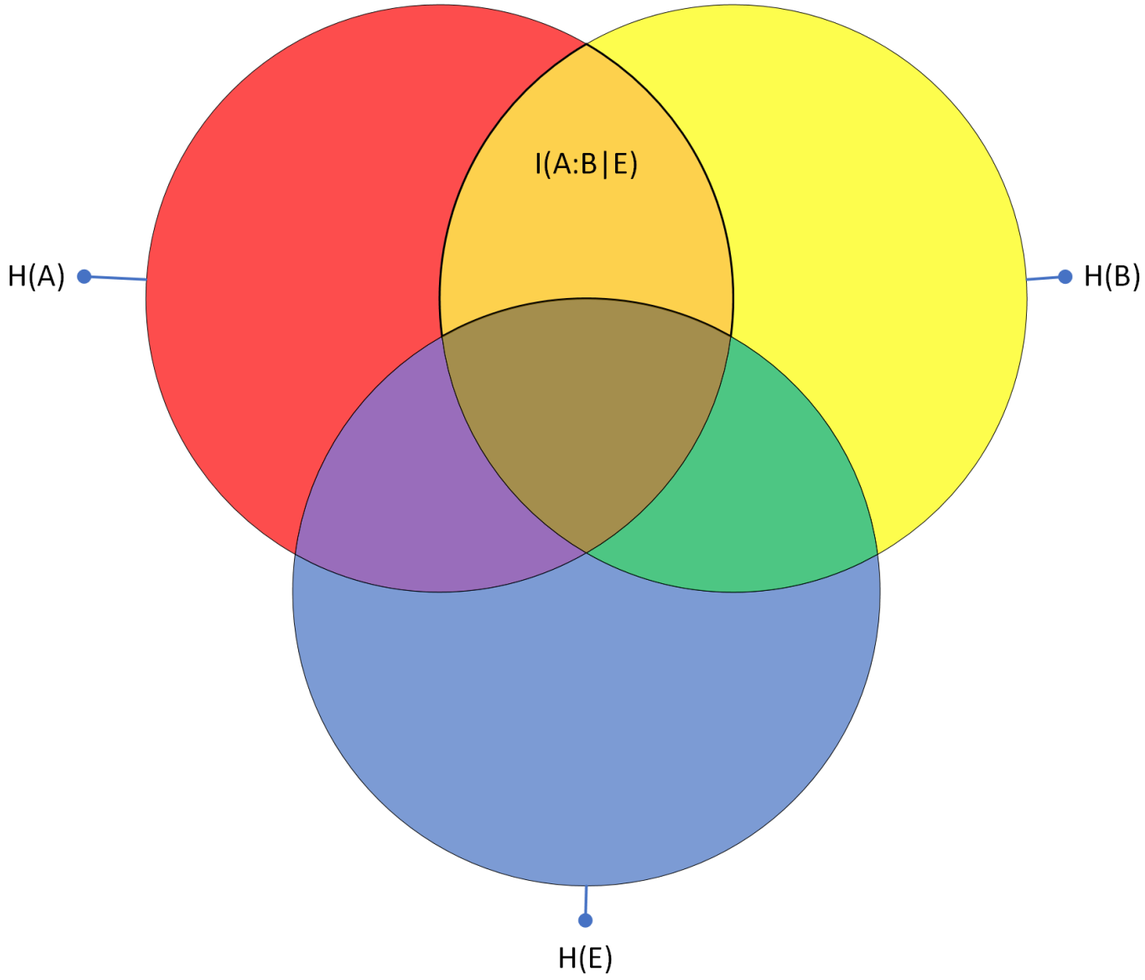




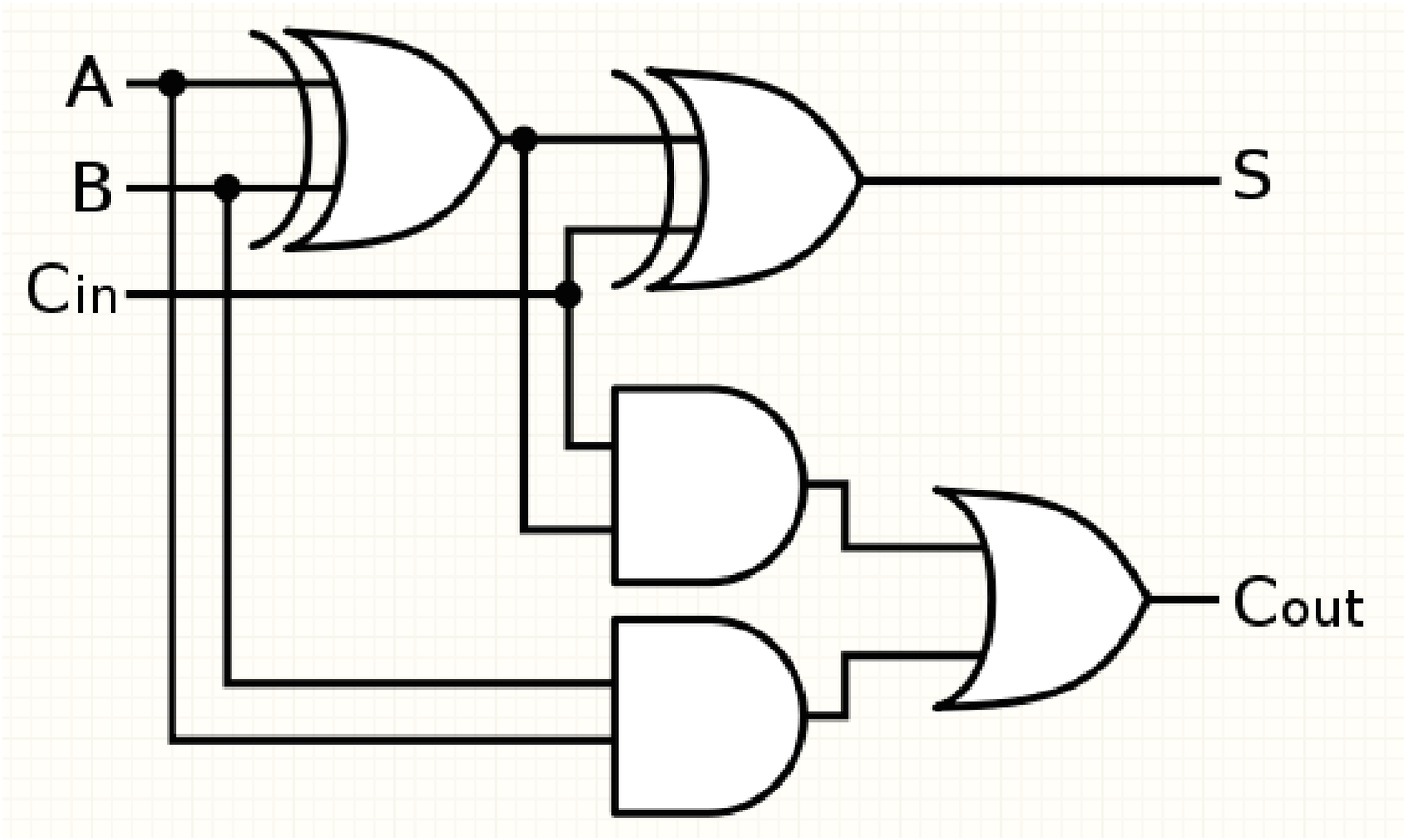

H(A)
H(B)
H(A) + H(B)
Distinguishable
>
H(A)
H(B)
H(A,B)
Indistinguishable

$$H(A) + H(B) = H(A,B) + I(A:B)$$





Information Theoretic Approach

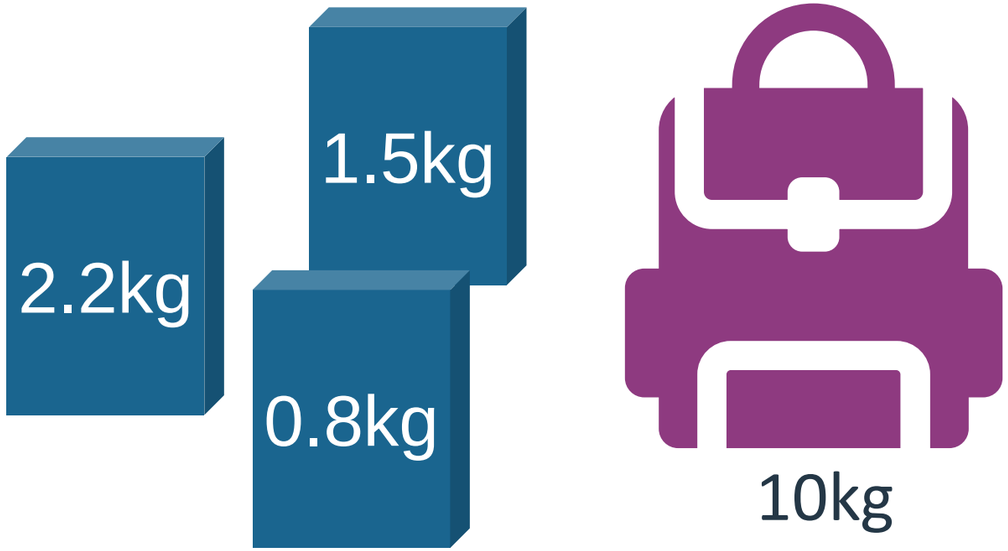


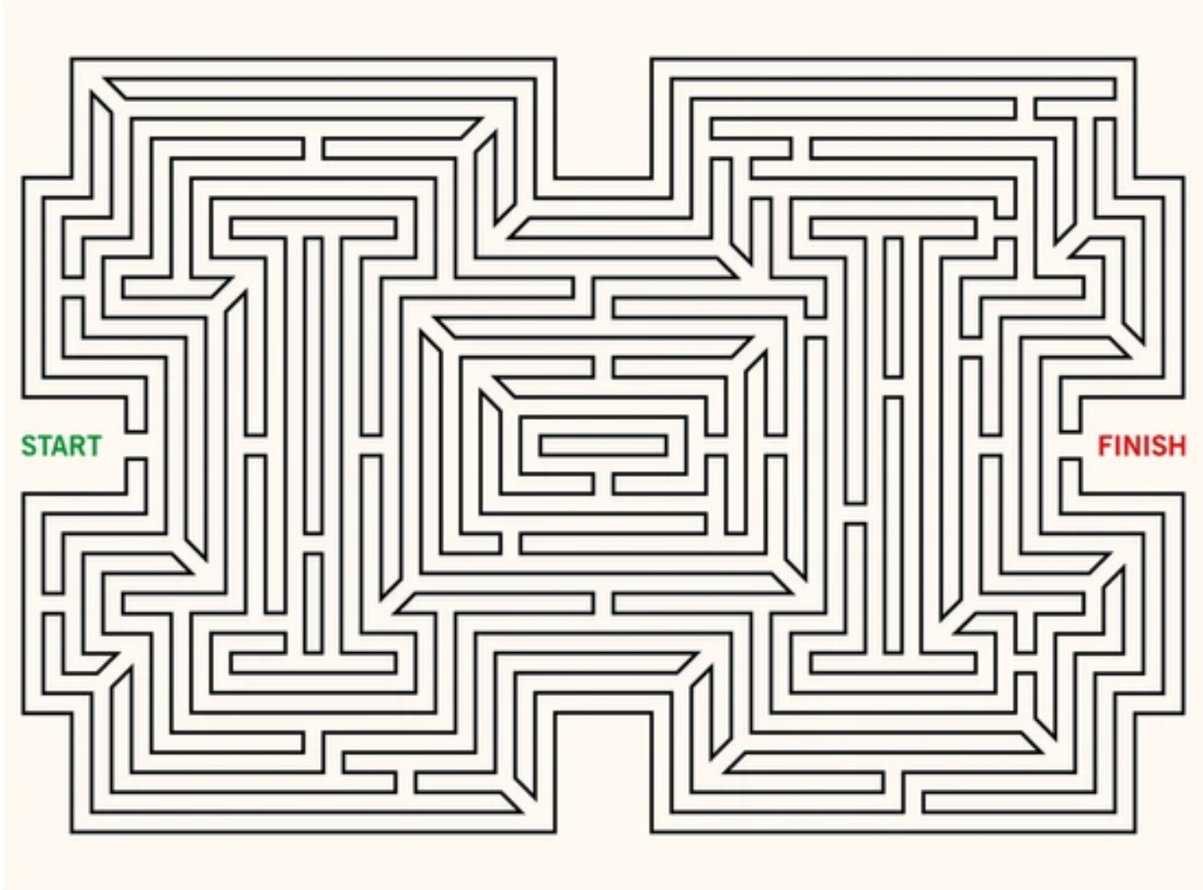

```
>>> x=[0,45,678,43,52,67,923,74,32,376]
>>> avg=sum(x)/len(x)
>>> print(x)
[0, 45, 678, 43, 52, 67, 923, 74, 32, 376]
>>> print(avg)
229.0
```

```
>>> if 45 in x: print("found")
... else:       print("not found")
...
found
```

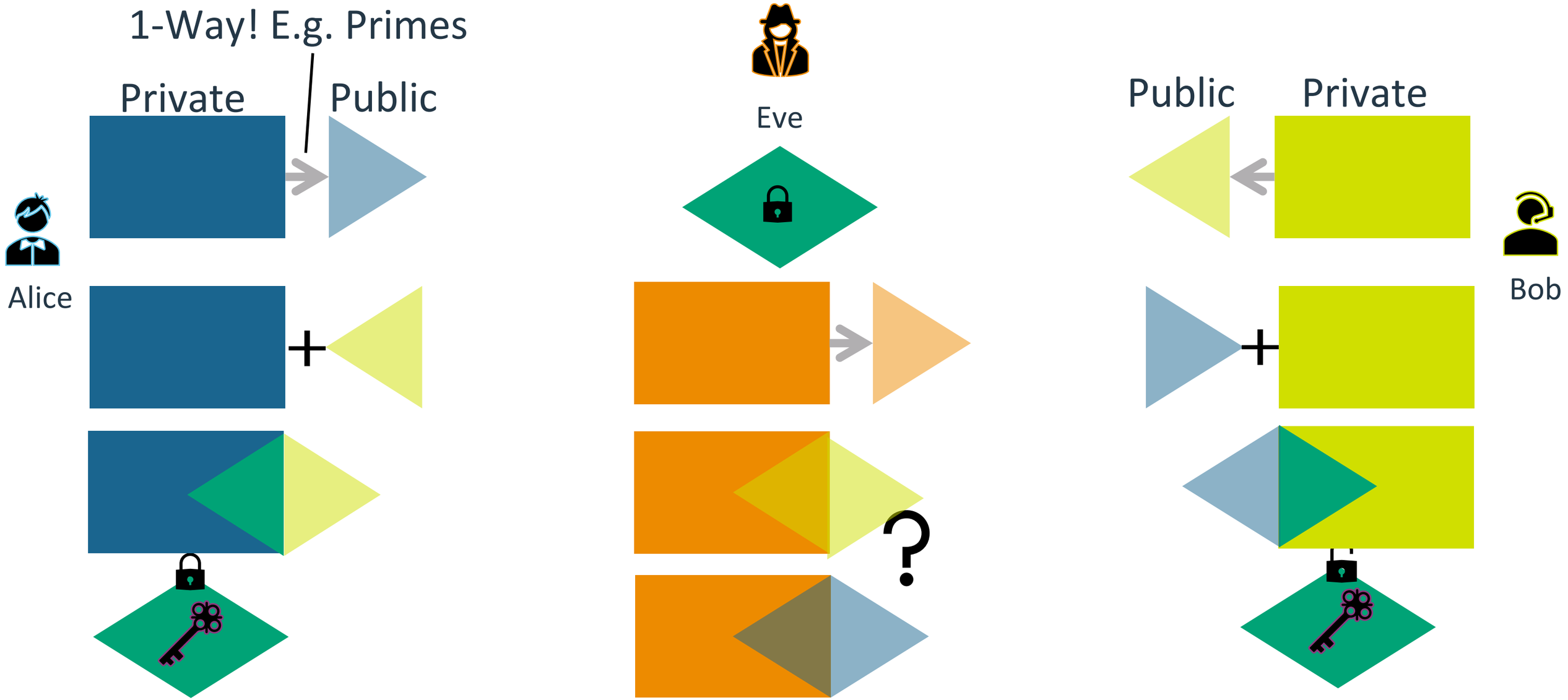
Computational Complexity Approach

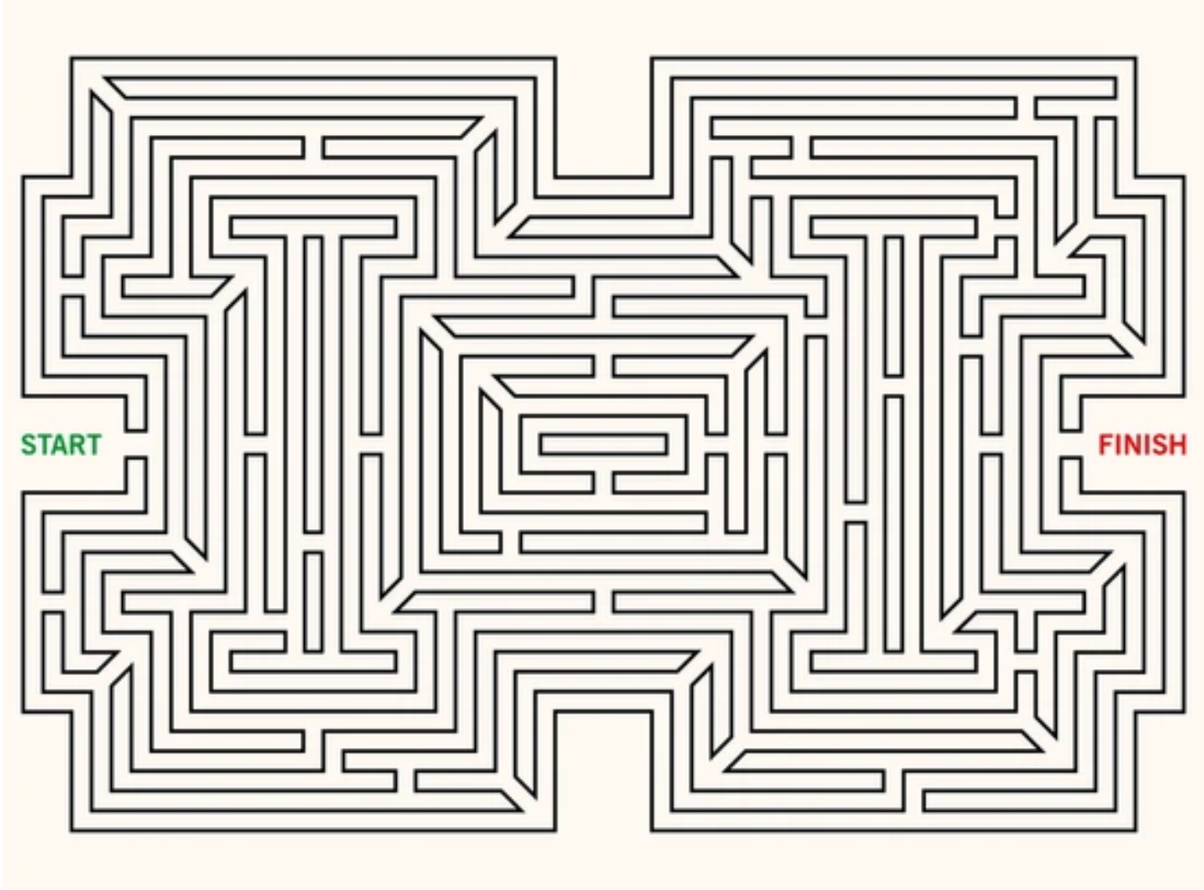
Prime factors of 616081?



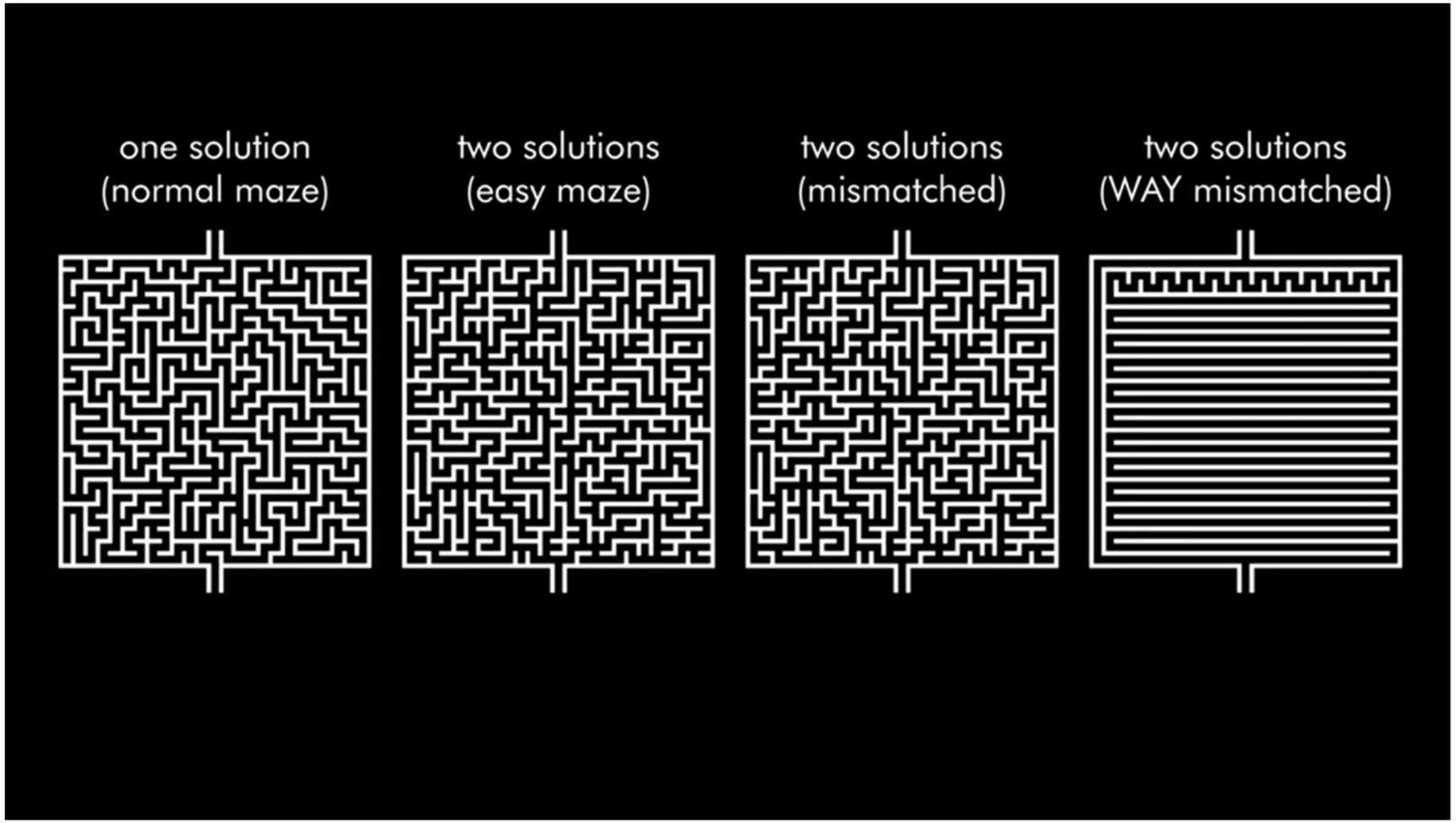


Computational Complexity Approach


1-Way! E.g. Primes
Private
Public
Alice
Eve
Public
Private
Bob

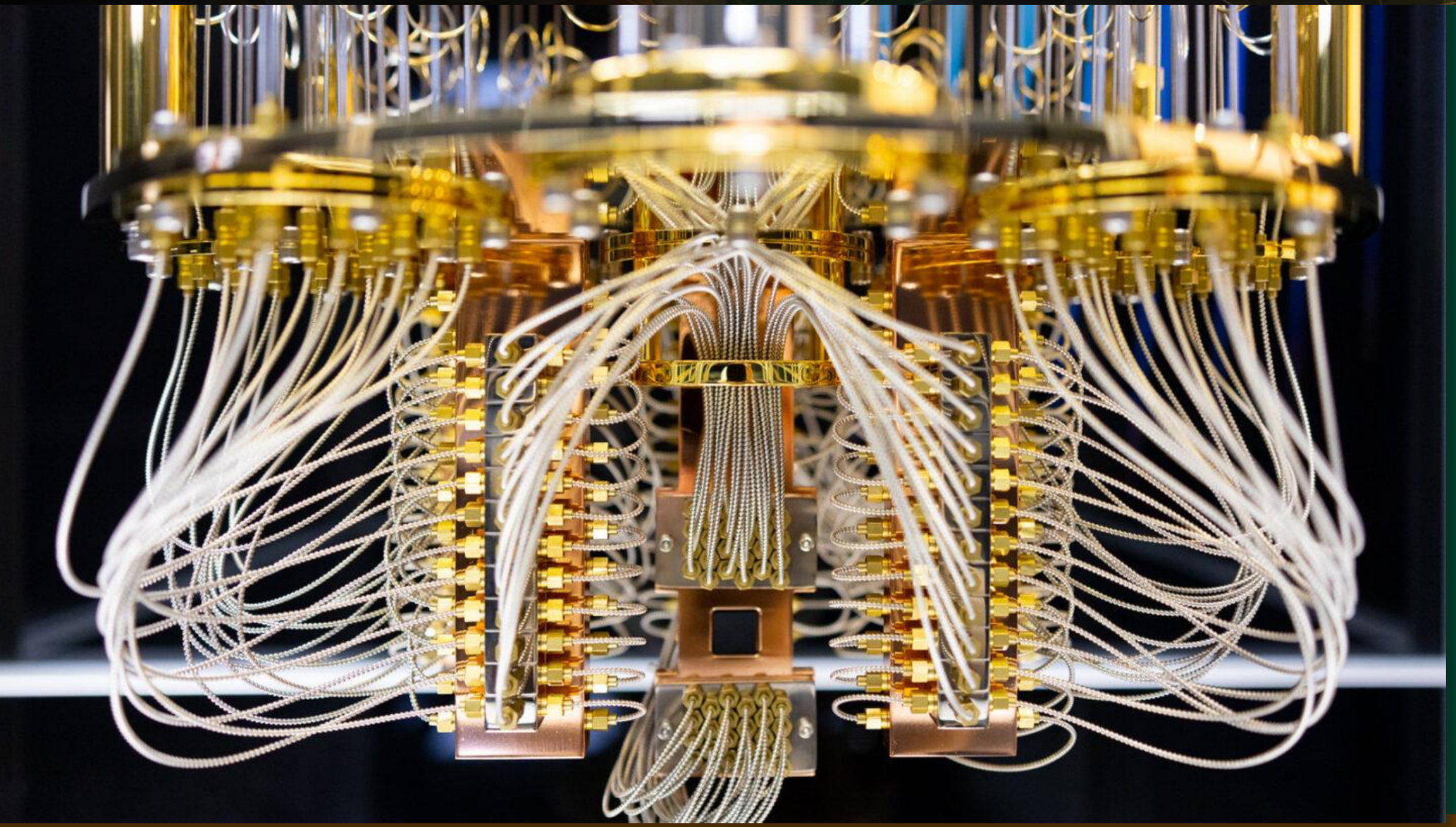


?



Local copy

How does electricity find the "Path of Least Resistance"? AlphaPhoenix, YouTube

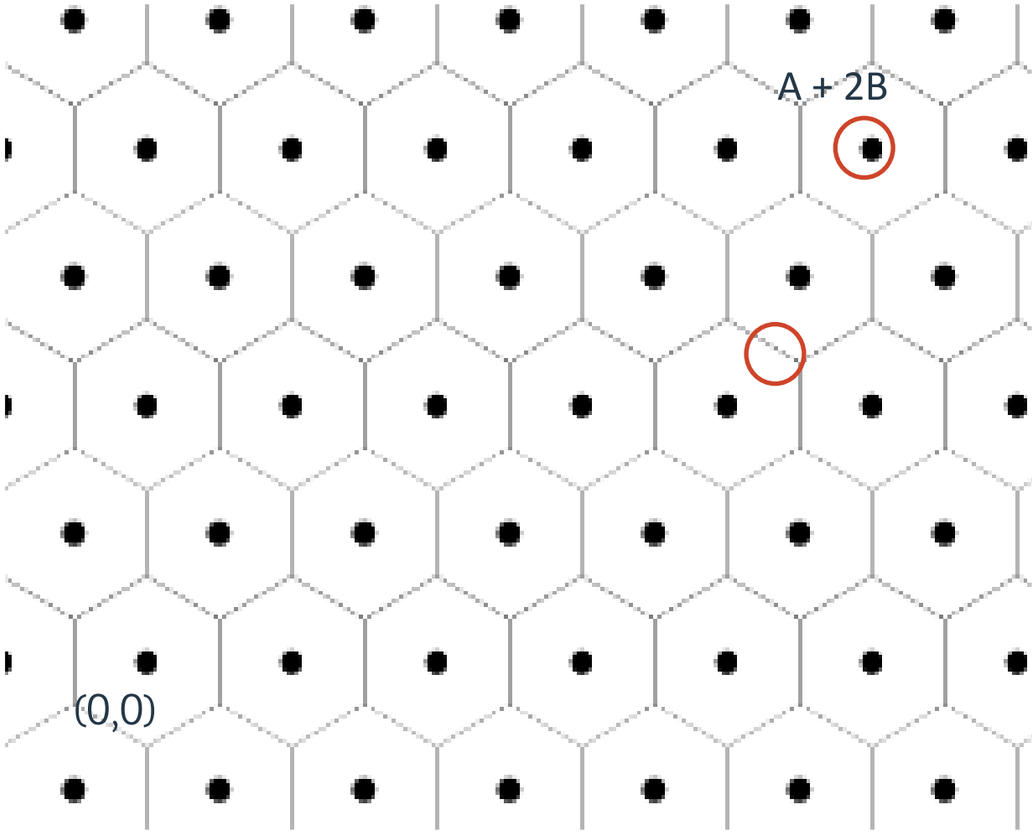


Searching problems:

Grover’s Search
Shor’s

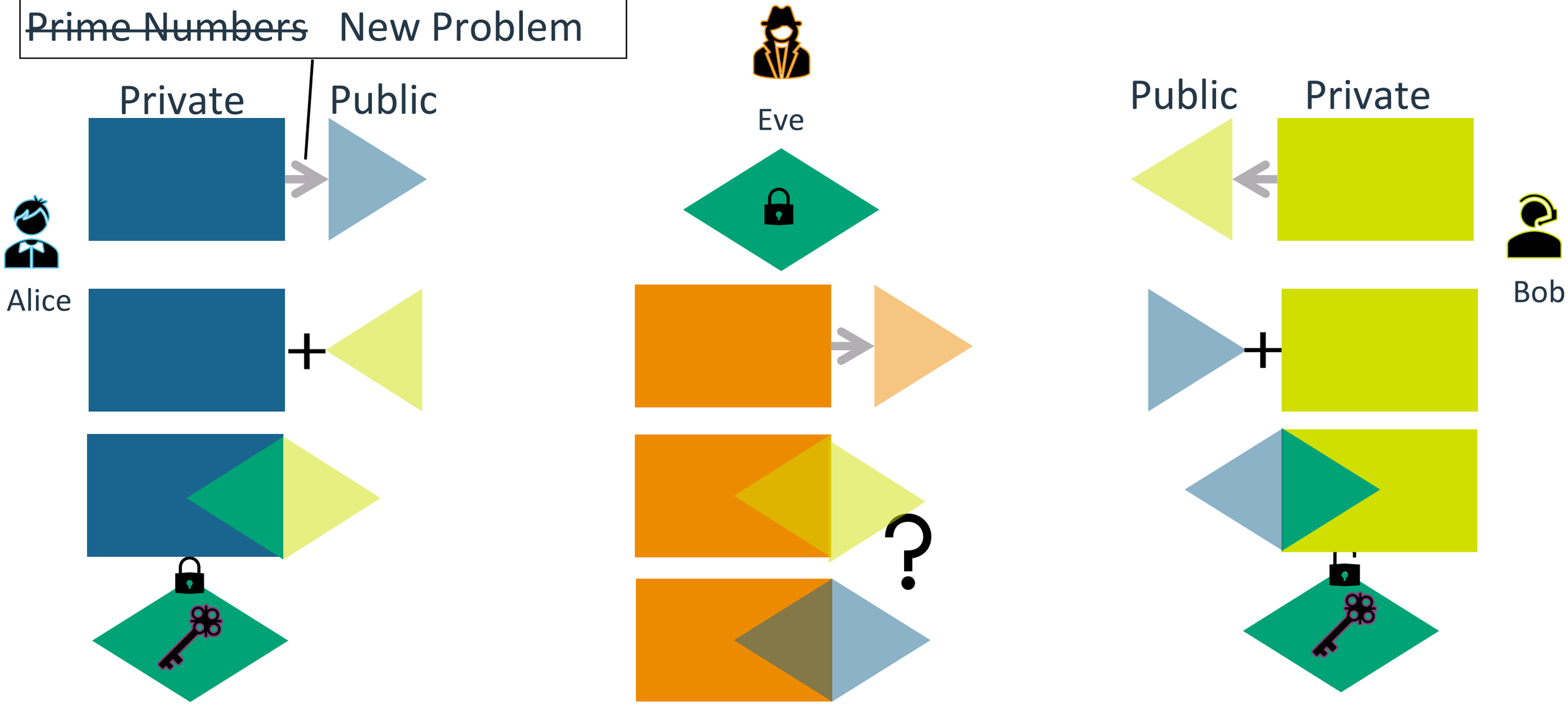
Which problems?

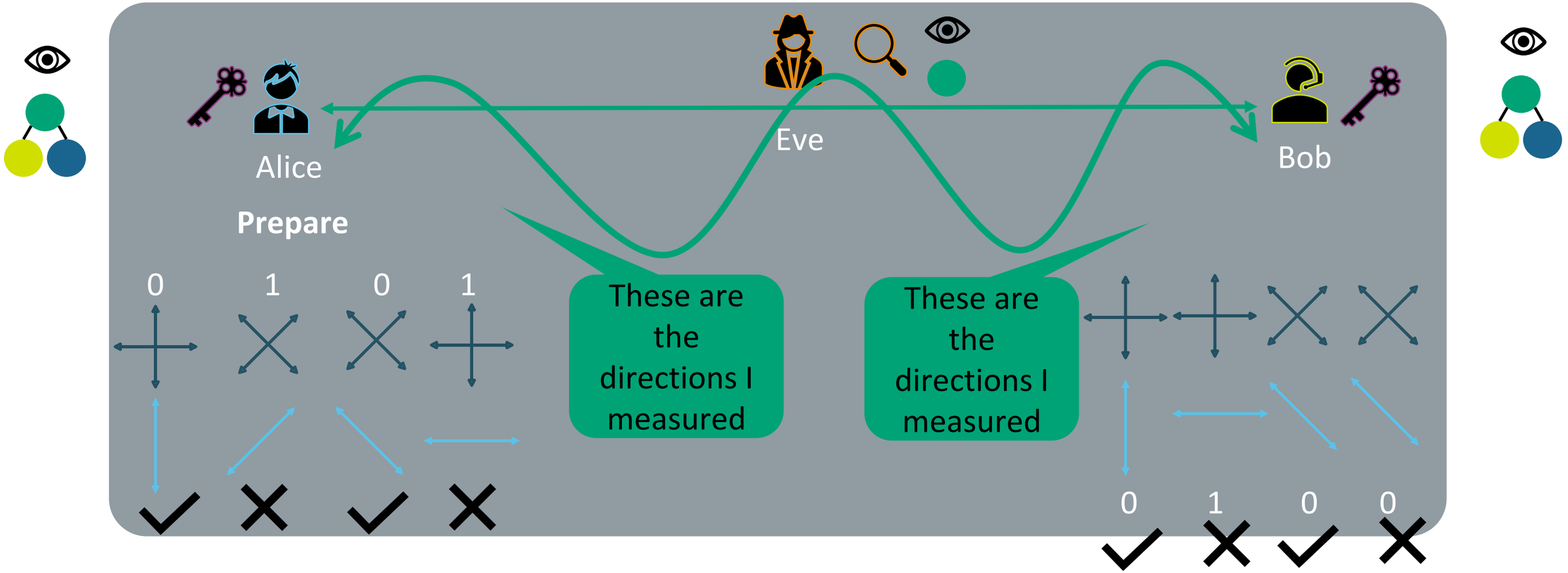
Find the closest point?



Lattice Based
Code Based
Multivariate polynomials
Based

~~Prime Numbers~~ New Problem




Alice
Eve
Bob
Prepare
0
1
0
1
These are the directions I measured
These are the directions I measured
0
1
0
0

Alice	Bob
0	0
0	0
0	1
0	0
0	0
1	1
1	0
1	1

Filter For Correllation

1) On the basis choice
2) “information reconciliation”

E => 00 or 11

O => 01 or 10

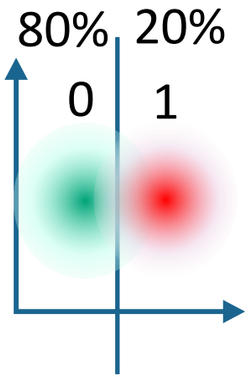
…

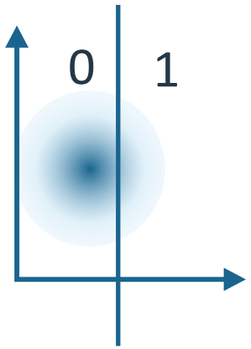
	Alice	Bob	
E	0	0	E
	0	0	
E	0	1	O
	0	0	
O	0	0	O
	1	1	
E	1	0	O
	1	1	

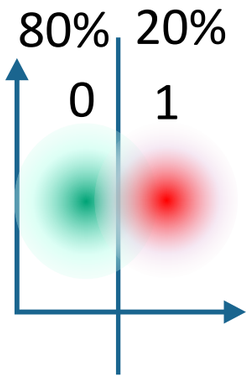
Alice	Bob	Eve		Eve
0	0	0	E ?	0x 1? 0?
0	0	1		1x 1? 0?
0	1	~~1~~		~~1~~
0	0	~~0~~		~~0~~
0	0	0	O ?	0x 1? 0?
1	1	0		0x 0? 1?
1	0	~~1~~		~~1~~
1	1	~~1~~		~~1~~

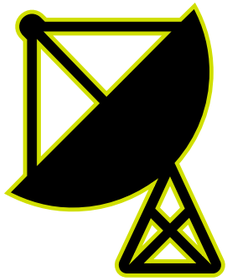
1.) 3-wayCorrelated datasets
2.) Indistinguishability for Eve

Eve's strategy = Knapsack problem!

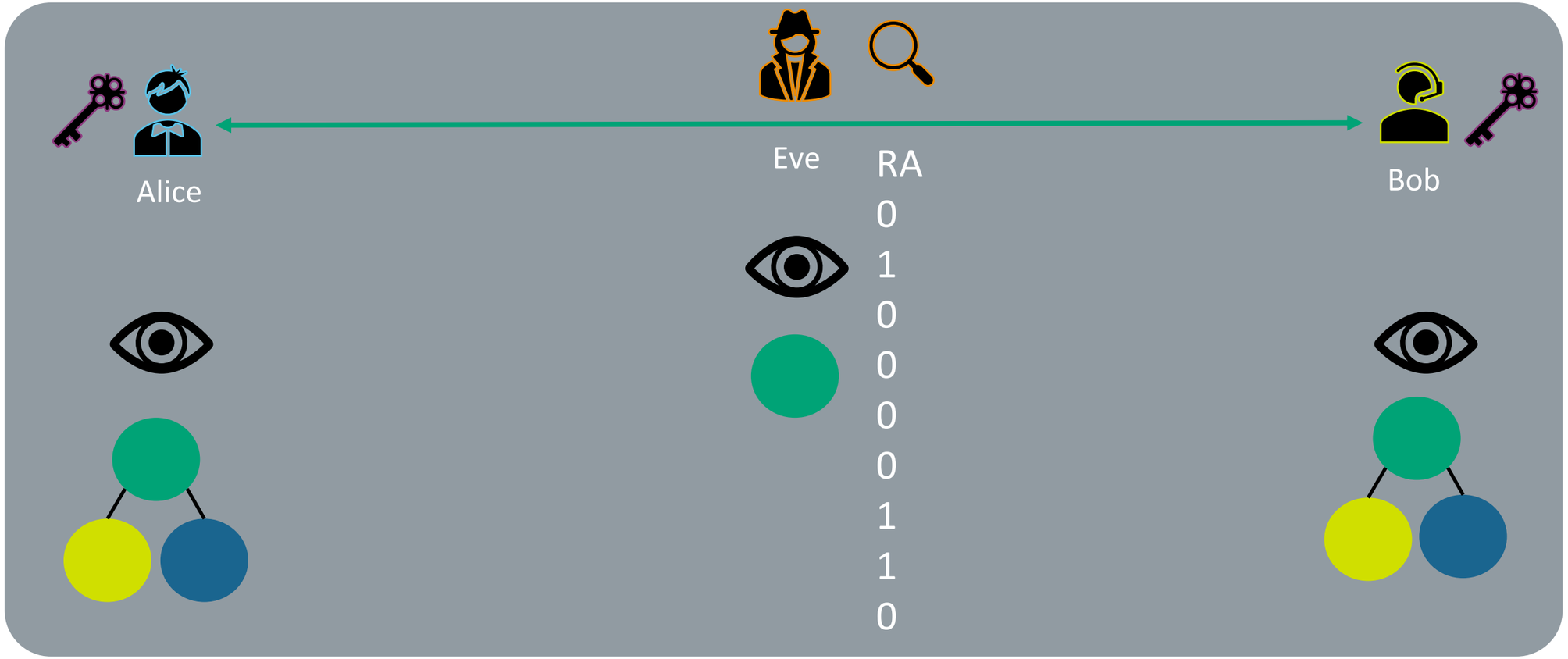








Alice	Bob	Eve	%
0	**Y**	**Y**	**80%*80%= 64%**
0	**Y**	**N**	**80%*20%= 16%**
0	N	Y	20%*80%= 16%
0	N	N	20%*20%= 4%



R	A	RA
0	0	0
1	0	1
1	1	0
0	0	0
0	0	0
1	1	0
0	1	1
1	0	1
0	0	0

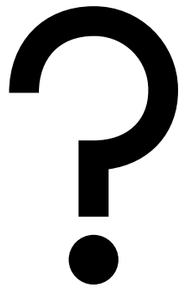
RA	B	RAB
0	0	0
1	1	0
0	1	1
0	0	0
0	1	1
0	0	0
1	1	0
1	0	1
0	0	0

H(A) + H(B) = H(A,B) + I(A:B)

P(R=0) = 0.5

P(RAB=0) = 0.5

P(R,RAB) = 0.5

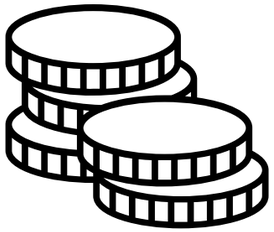


H ∝ P

I(A:B) = 0

… This only applies when length of string, L →∞

Random numbers are weird!



H, T, T, T, H, H, H, T, H, T, H, T	6 HEADS, 6 TAILS	P(H)=0.5
H, T, T, H, H, H, H, T, H, T, H, H	7 HEADS, 5 TAILS	P(H)=0.58

Both of these were generated from the same unbiased coin P(H)=0.5

For small samples, all the different possibilities have a real chance of happening!

Kolmogorov Complexity

A = 0000000000 “10x0”

B = 0110100011 “1x0, 2x1, 1x0, 1x1, 3x0, 2x1”

K(A) < K(B)

What if K(A) +K(B) > K(A,B)?

A	B	A,B
0	0	0,0
0	1	0,1
1	1	1,1
0	0	0,0
0	1	0,1
1	0	1,0
1	1	1,1
0	0	0,0
0	0	0,0

1x0, 1x1, 1x0, 1x1

2x0, 2x1

1) R, A → RA

2) B → RAB

3) Filter & keep correlation

4) Privacy amplification

R	A	RA
0	0	0
1	0	1
1	1	0
0	0	0
0	0	0
1	1	0
0	1	1
1	0	1
0	0	0

RA	B	RAB
0	0	0
1	1	0
0	1	1
0	0	0
0	1	1
0	0	0
1	1	0
1	0	1
0	0	0

- Eve has RA
- Preferential filtering for Bob = Eve retains errors
- Correlation filter has ambiguity

Authentication?

- ✓ Integrity detectable = Verifiable consistent conversation

  Key first, authenticate later = Peer-to-peer mutual authentication

- ✓ PKI integrable

Overhead:

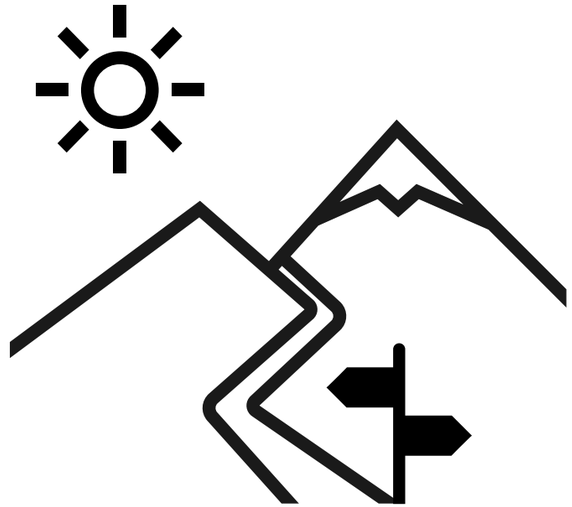
Processing vs Communication (IoT?)

Definable security

Assuming BQP ≠ NP-Complete → Quantum-safe

Roadmap

- ~~Ingredients for Secrecy~~
- ~~Existing Methods~~
- ~~Implications of Quantum Computers~~
- ~~Quantum Resilient Alternatives Method #1~~
- ~~Quantum Resilient Alternatives Method #2~~
- A New Method!



SoundBytes:

1) Secrecy is a matter of perspective

2) Random numbers have weird properties

3) RKKE – Reciprocal Kolmogorov Key Establishment – a lightweight alternative

Thank You

SoundBytes:

1) Secrecy is a matter of perspective
2) Random numbers have weird properties
3) RKKE – Reciprocal Kolmogorov Key Establishment – a lightweight alternative