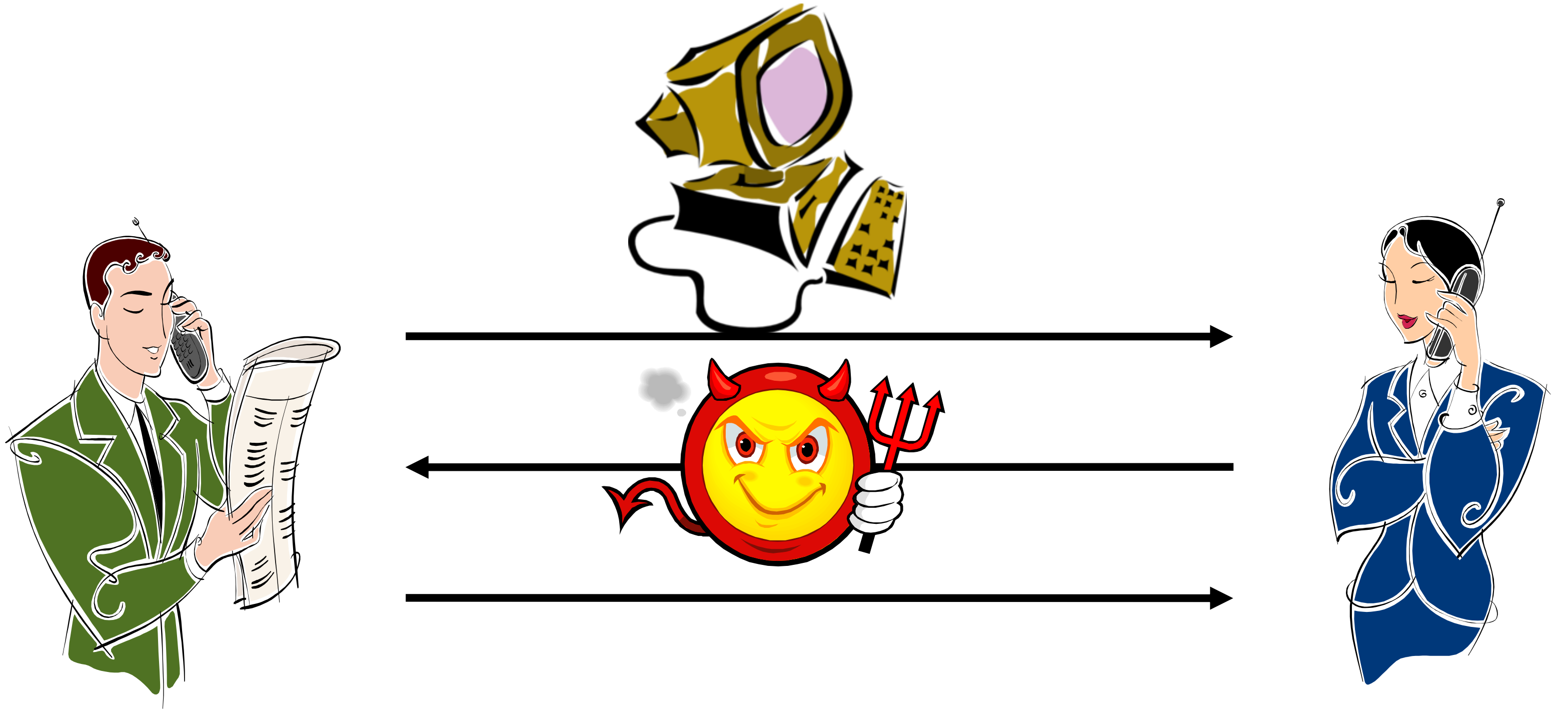
Lattice Cryptography (1. Public Key Encryption)

Vadim Lyubashevsky

IBM Research Europe, Zurich

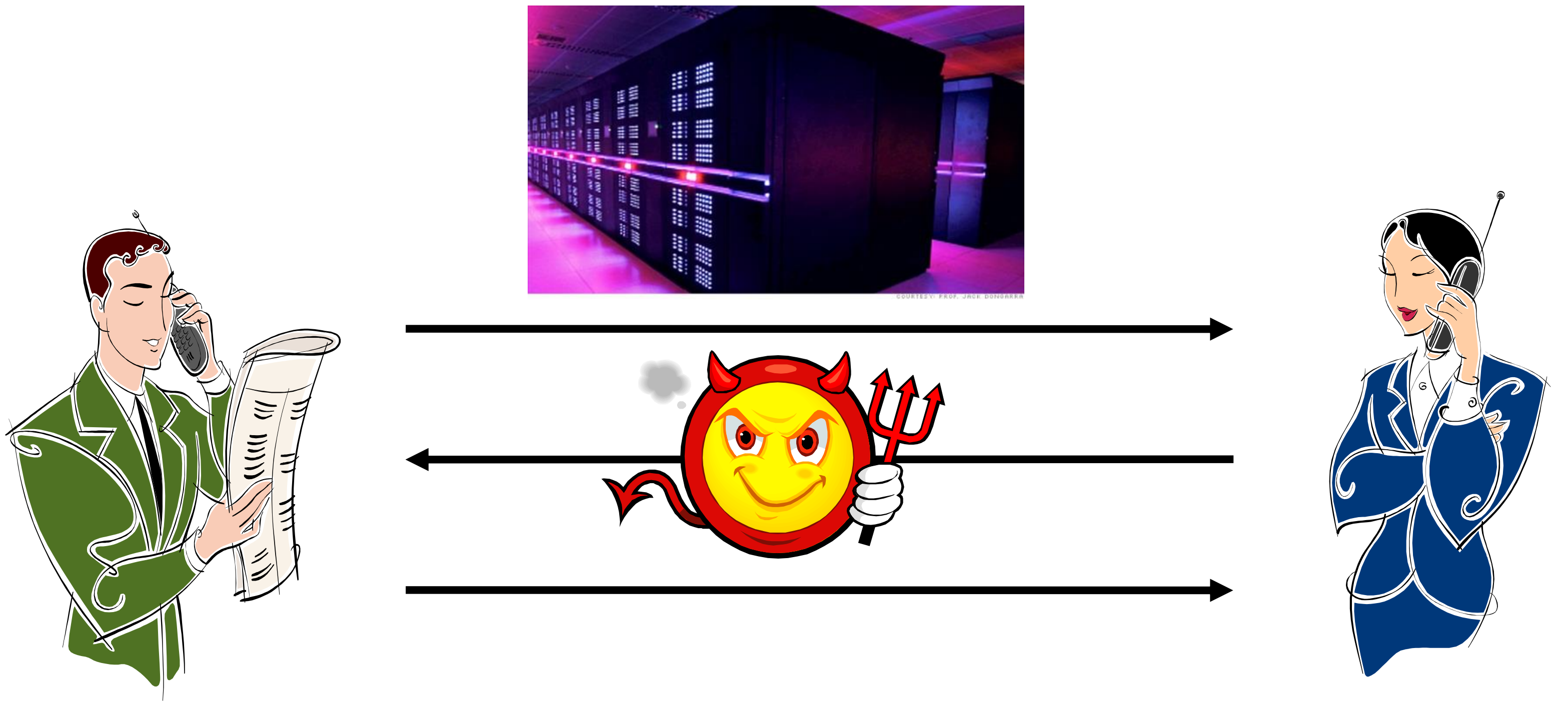
Cryptography

Allows for secure communication in the presence of malicious parties



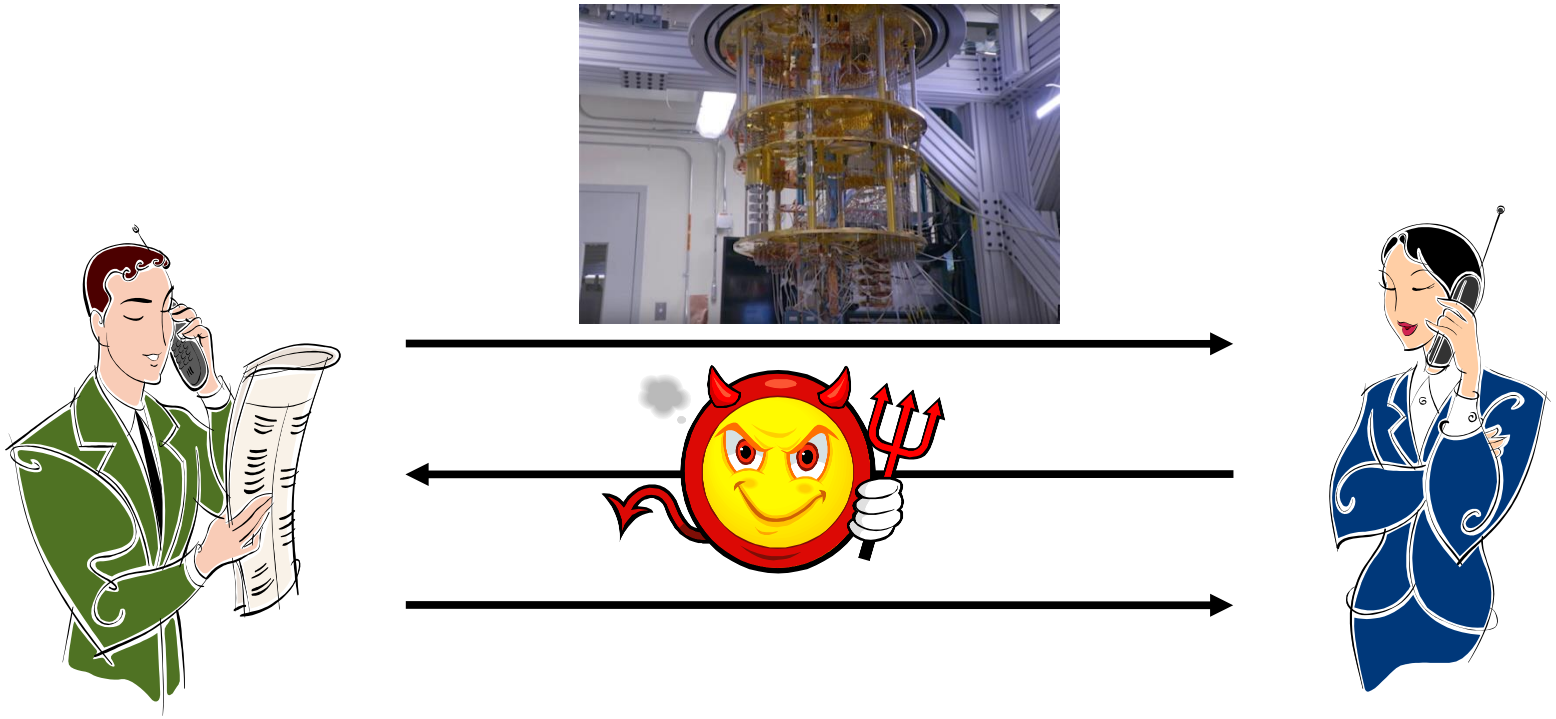
Cryptography

Large increase in the adversary's computing power requires only a small increase in the key size



Cryptography

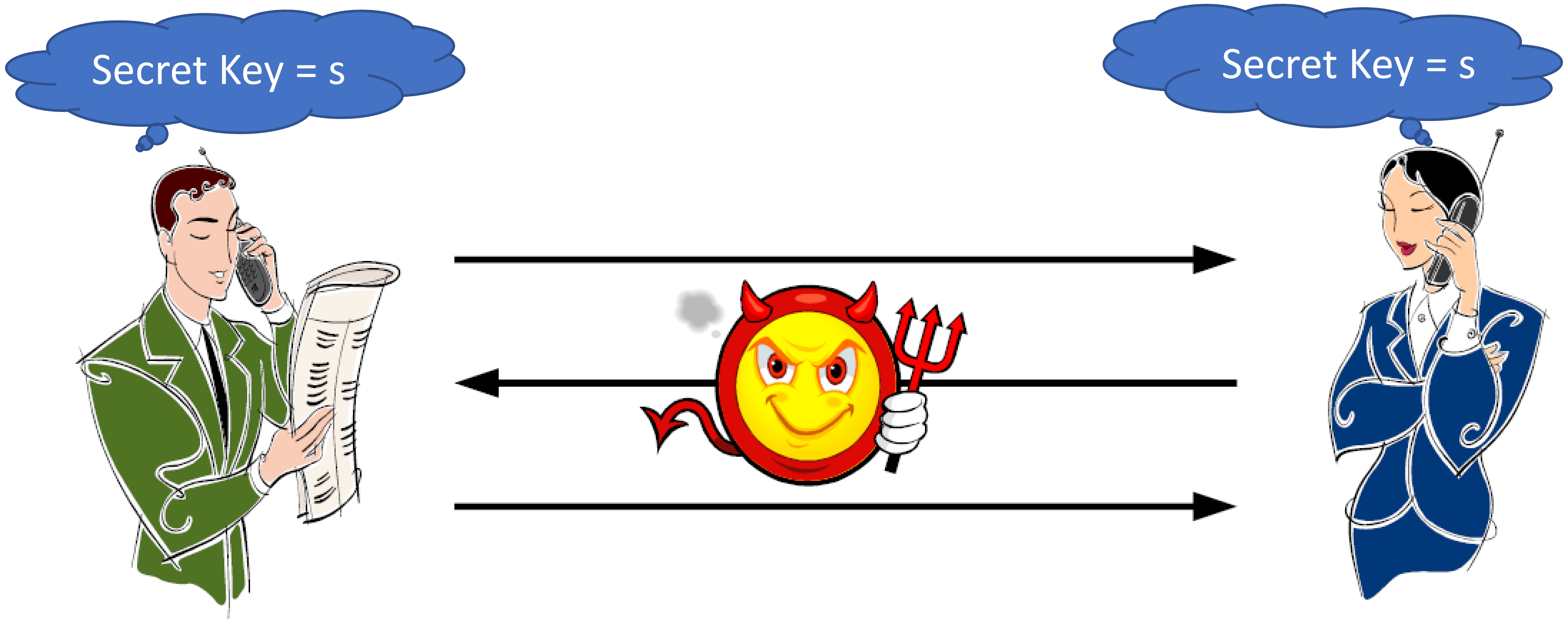
A quantum computer is outside the standard model of computation for efficiency purposes



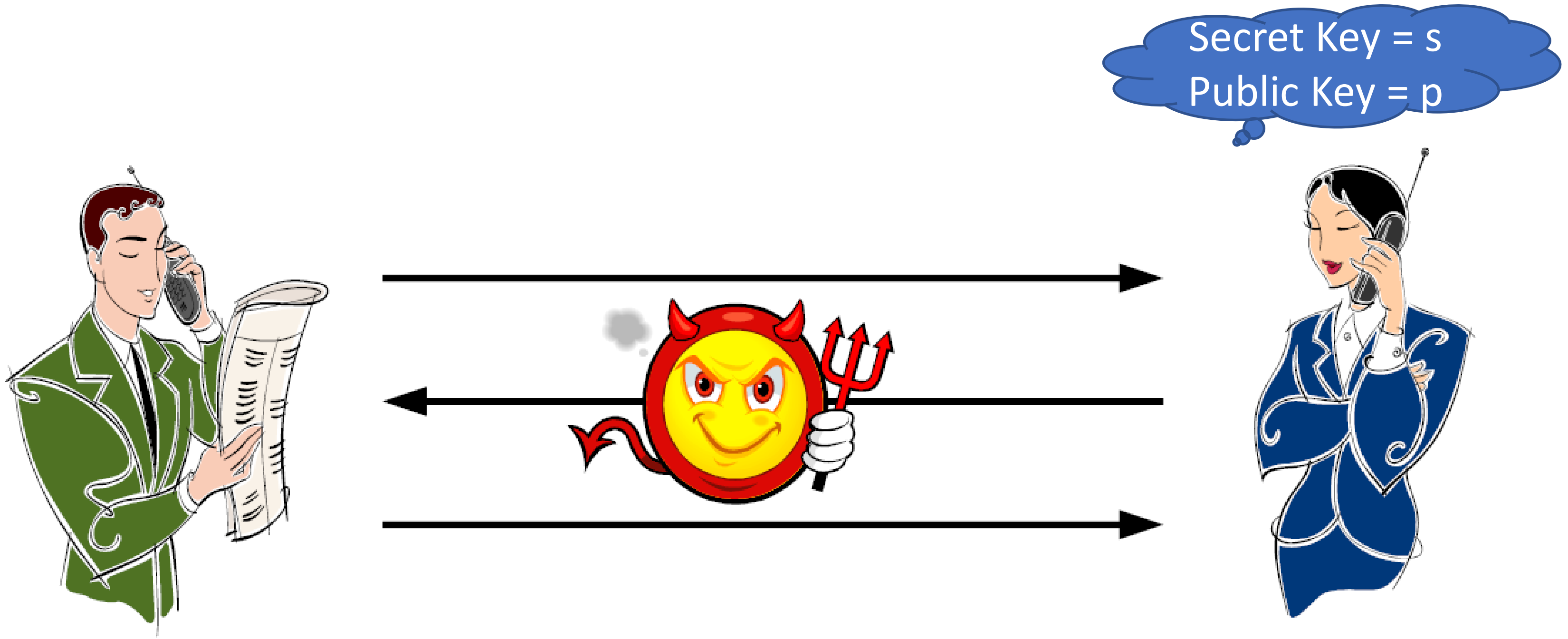
Symmetric-Key Cryptography

Symmetric-Key Cryptography

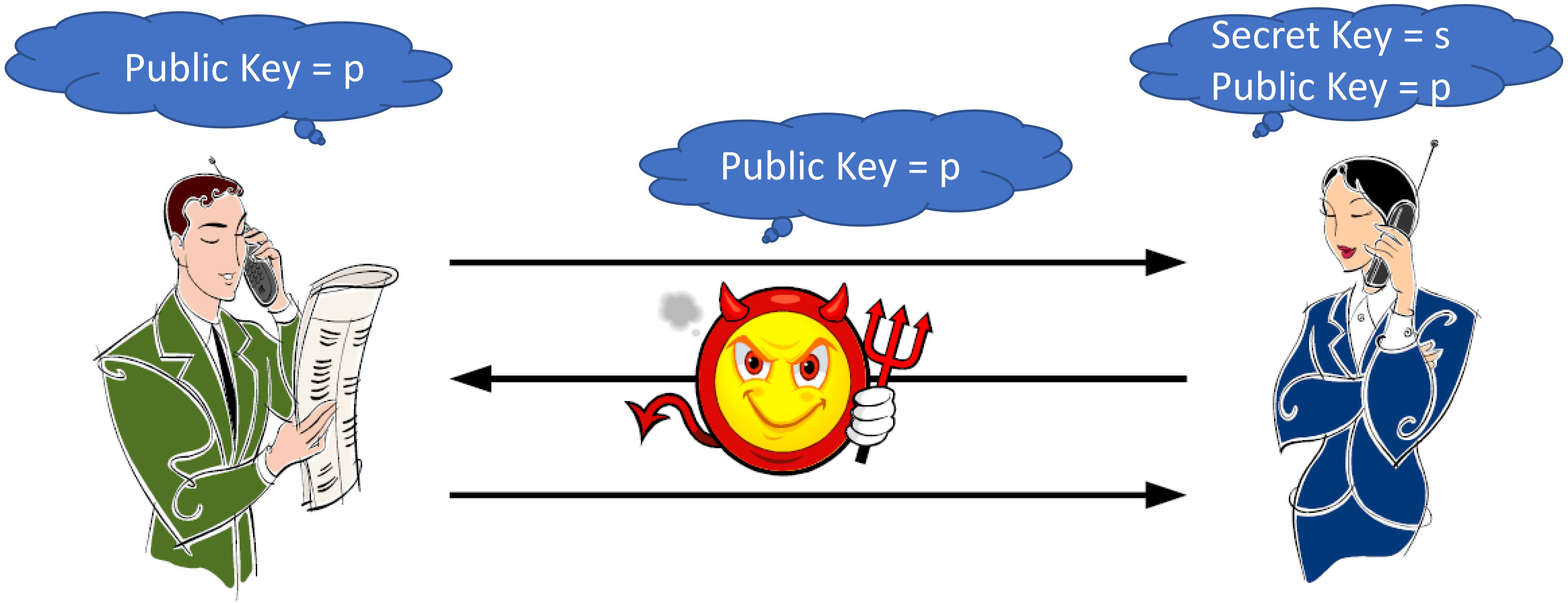
Will still exist if quantum computers are built



Public-Key Cryptography



Public-Key Cryptography



Mathematical Assumptions for Public-Key Cryptography

~~Factoring is hard~~

~~$N=pq$~~

~~Computing discrete logs is hard~~

~~$g^x=y \bmod p$~~

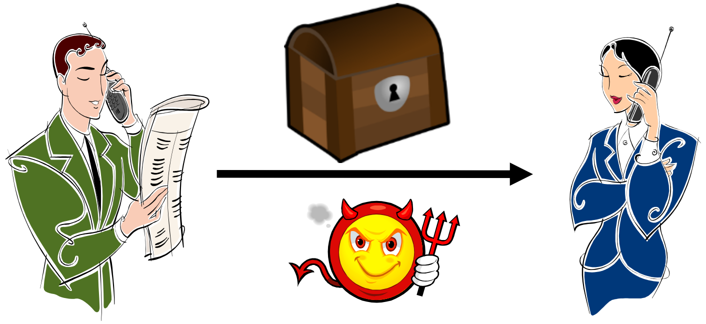
Mostly problems from number theory

All broken once a quantum computer is built

Consequence of quantum computing

Current public key schemes will be broken

Quantum computers will recover all of **today’s** secrets



Do not need quantum to defend against quantum

Quantum computers are not all-powerful.

They simply solve some problems faster.

Base cryptography on problems they don't solve.

How do we know that (quantum) computers don't solve a problem?

We don't … all we can say is that researchers tried to solve the problem for X decades and failed.

Effect of quantum computers

- Symmetric Cryptography
  - Mostly fine
- Public-Key Cryptography
  - Everything used today – broken!

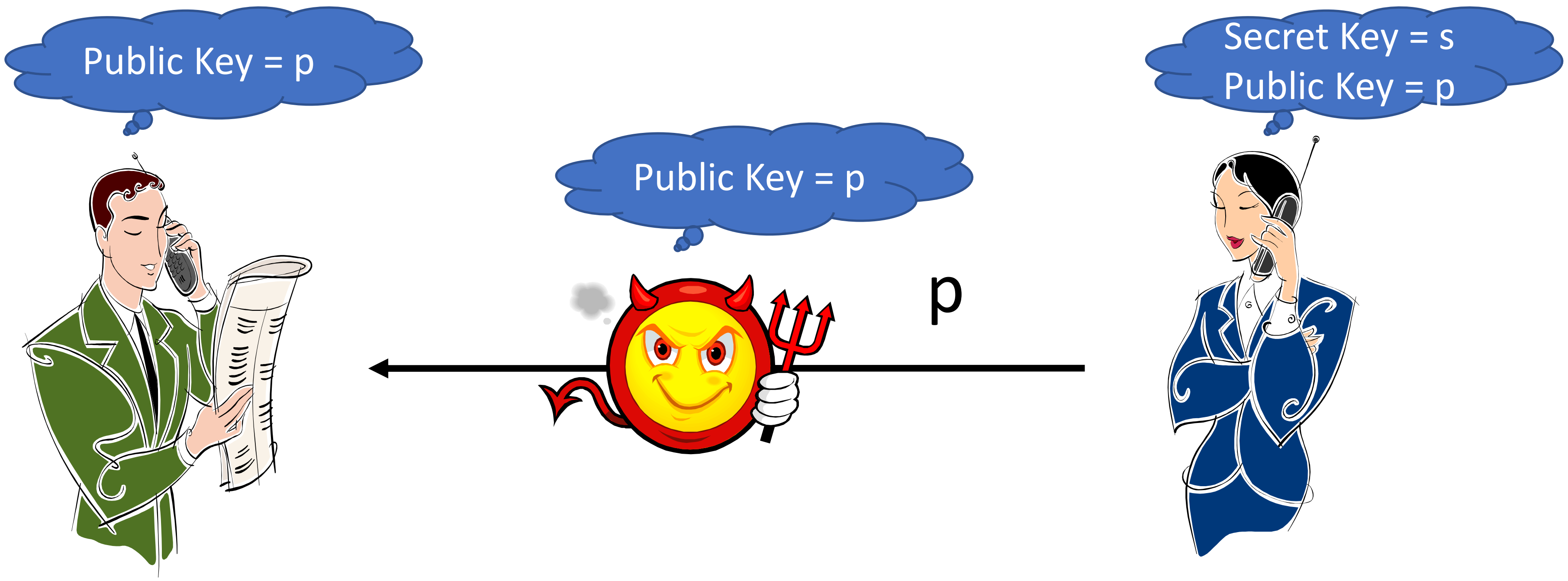
Timeline for change to Quantum-Safe (post-quantum) Crypto:

Algorithm Selection: 2017 – 2022

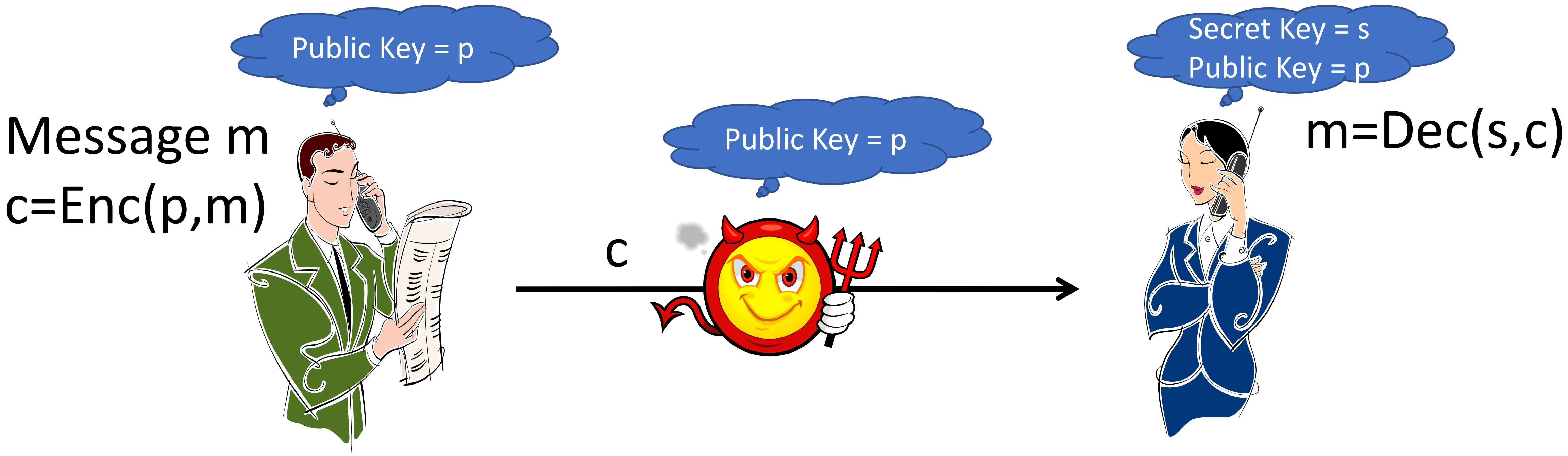
Writing Standards: 2022 – 2024

Transition should be complete (NSA): 2030-2035

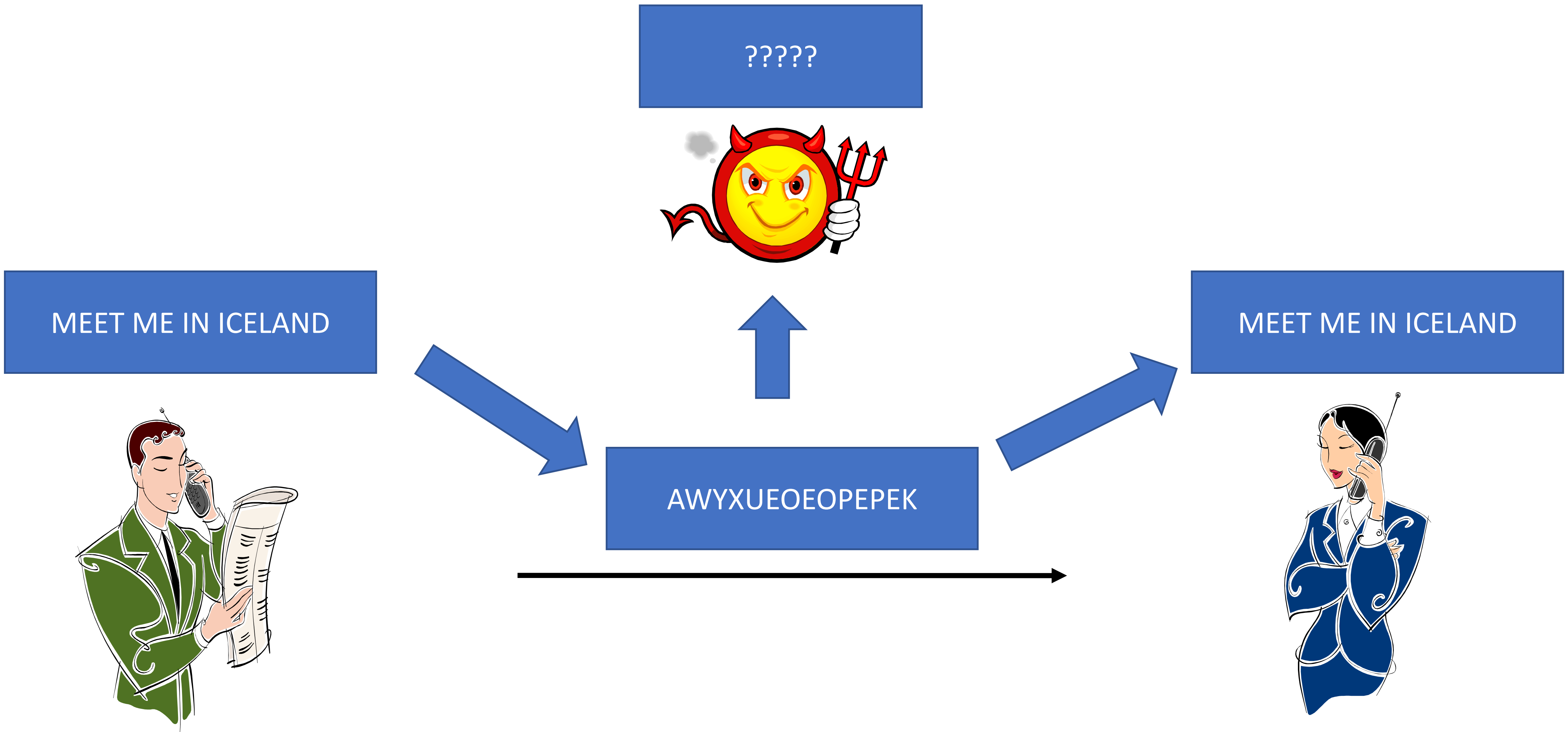
Public-Key Encryption



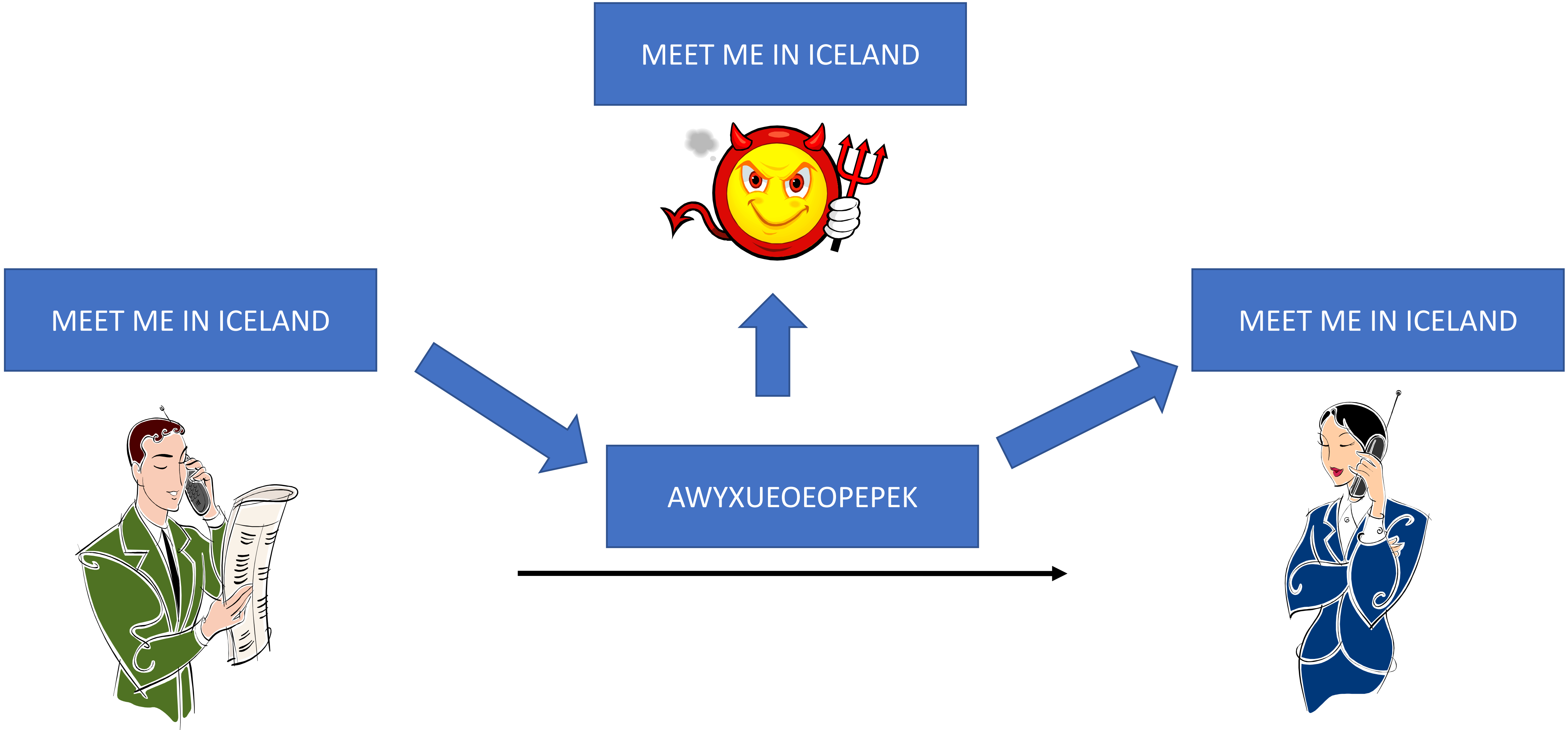
Public-Key Encryption



What is Secure Encryption?



Public Key Cryptography



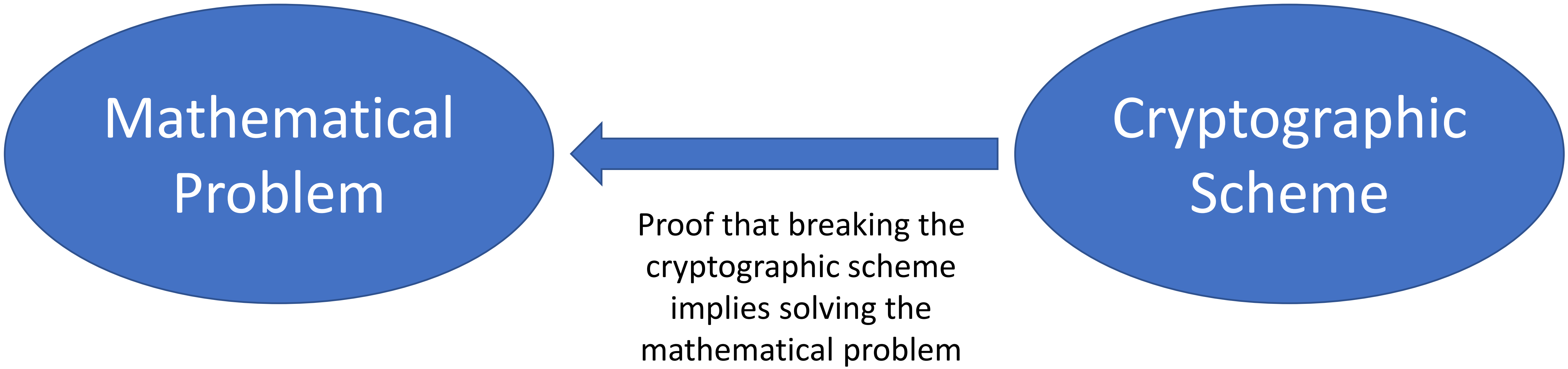
Formal Definition

For any two messages m_1 and m_2 of the adversary's choosing, he cannot **distinguish** between

- $c_1 = Enc(m_1)$
- $c_2 = Enc(m_2)$

Encryption needs to be randomized

Building Cryptography



Lattice Cryptography

- NIST had a competition to create new quantum-safe cryptographic standards
- RSA / Discrete Log / Elliptic Curve cryptography will be phased out by 2033 (at least in the US government)
- Main 2 standards - encryption and digital signature - selected are lattice-based

  (CRYSTALS-Kyber, CRYSTALS-Dilithium)

Learning with Errors Problem

Hard Problem Intuition

$$\begin{pmatrix} & & \\ & \mathbf{A} & \\ & & \end{pmatrix} \begin{bmatrix} \\ \mathbf{y} \\ \\ \end{bmatrix} = \begin{bmatrix} \mathbf{z} \\ \\ \\ \end{bmatrix} \mod p$$

Given (**A**,**z**), find **y**

Easy! Just invert **A** and multiply by **z**

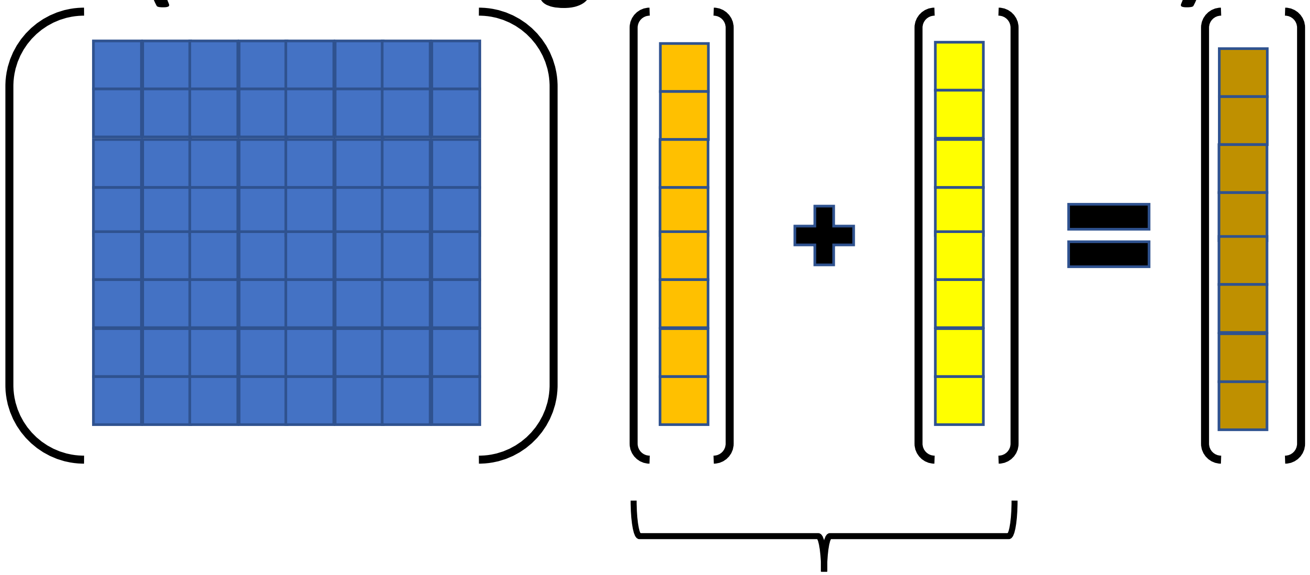
Hard Problem Intuition

$$\begin{pmatrix} & & \\ & \mathbf{A} & \\ & & \end{pmatrix} \underbrace{\begin{bmatrix} \\ \mathbf{y} \\ \\ \end{bmatrix} + \begin{bmatrix} \\ \mathbf{e} \\ \\ \end{bmatrix}}_{\text{Small coefficients}} = \begin{bmatrix} \\ \mathbf{z} \\ \\ \end{bmatrix} \mod p$$

Given (**A**,**z**), find (**y**,**e**)

Seems hard.

Hard Problem Intuition
(**Learning With Errors**)



mod p

Small coefficients to enforce uniqueness

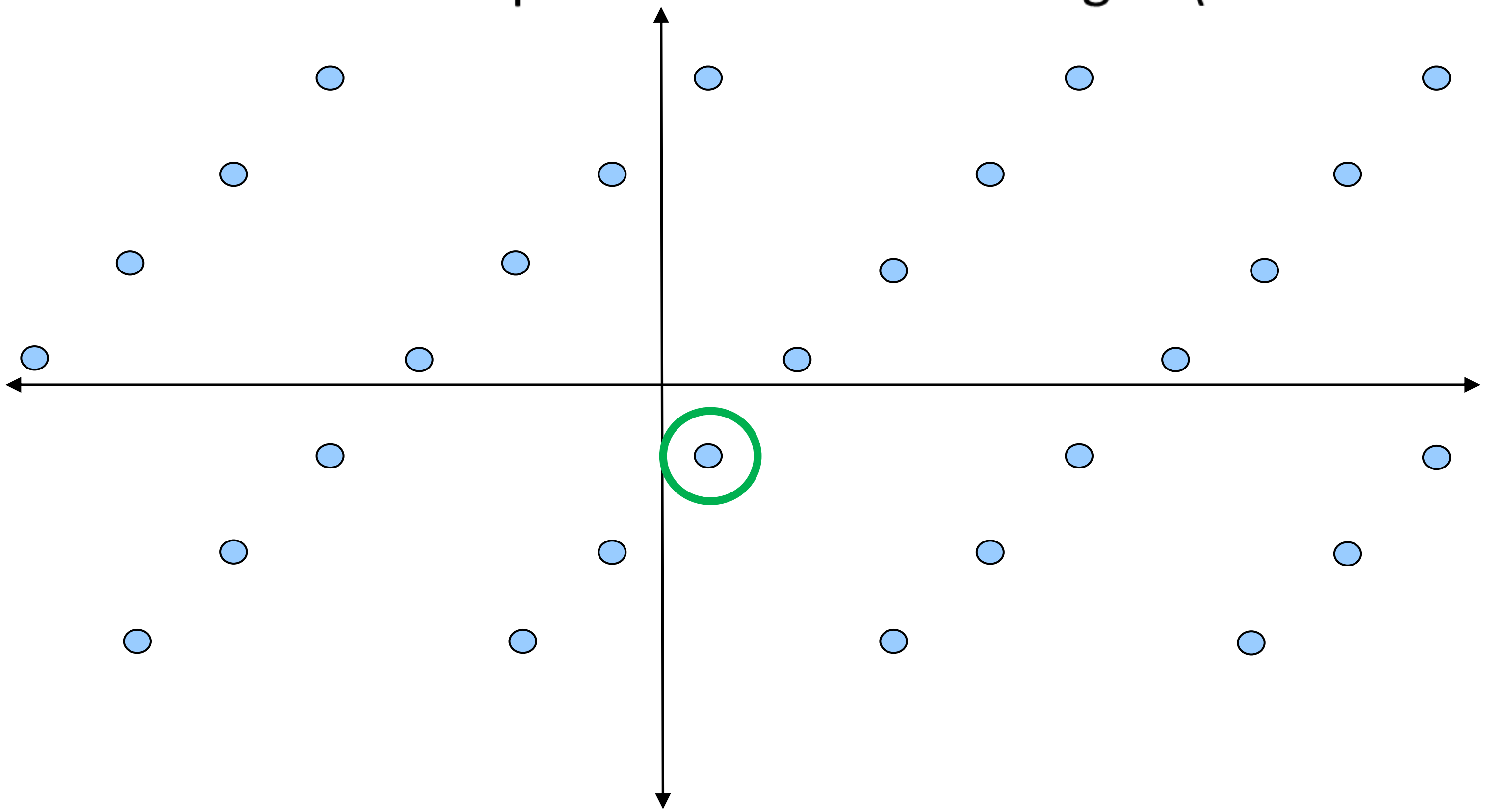
Given (**A**,**z**), find (**y**,**e**)

Seems hard.

Why is this "Lattice" Crypto?

All solutions $\binom{y}{e}$ to **Ay**+**e**=**z** mod p form a "shifted" lattice.

We want to find the point closest to the origin (BDD Problem).



Distinguishing from Random is also Hard

Search LWE Problem: Given (A,t=As+e mod p), find s

Decision LWE Problem: Given either (A, t=As+e mod p) or (A,u), where u is random mod p, figure out which tuple you have

$$\begin{pmatrix} \;\; A \;\; \end{pmatrix} \begin{bmatrix} y \end{bmatrix} + \begin{bmatrix} e \end{bmatrix} = \begin{bmatrix} z \end{bmatrix} \mod p$$

Looks Random mod p

Public Key Encryption from LWE

“Column” LWE is Pseudorandom

$$\begin{bmatrix} 4 & 6 & 7 & 9 \\ 3 & 9 & 0 & 7 \\ 8 & 4 & 6 & 5 \\ 1 & 6 & 4 & 3 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 9 \\ 8 \\ 0 \end{bmatrix}$$

“Row” LWE is also Pseudorandom

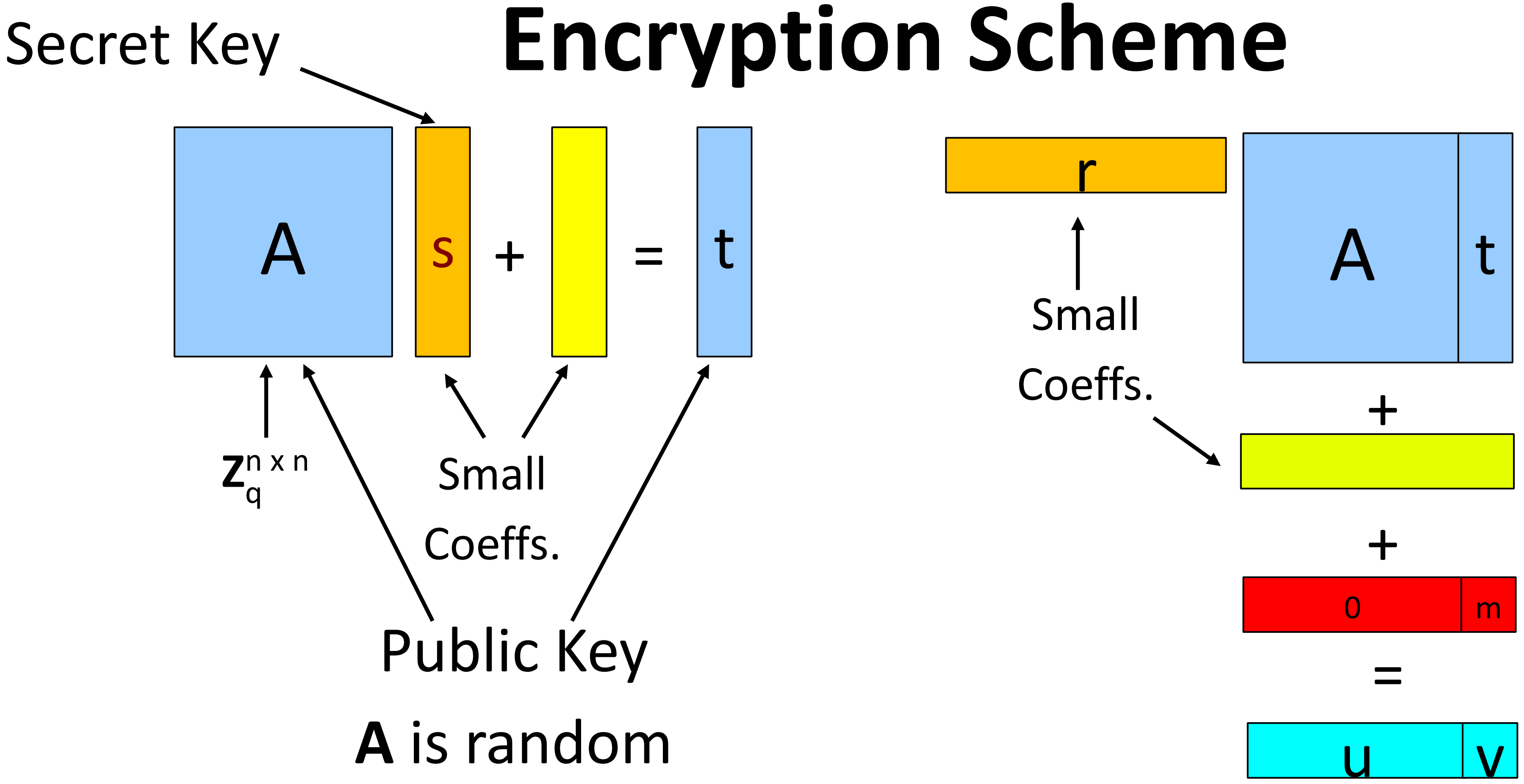
$$\begin{bmatrix}1&0&0&1\end{bmatrix}\begin{bmatrix}4&6&7&9&0\\3&9&0&7&9\\8&4&6&5&8\\1&6&4&3&0\end{bmatrix}$$

$$+\begin{bmatrix}1&1&1&0&0\end{bmatrix}$$

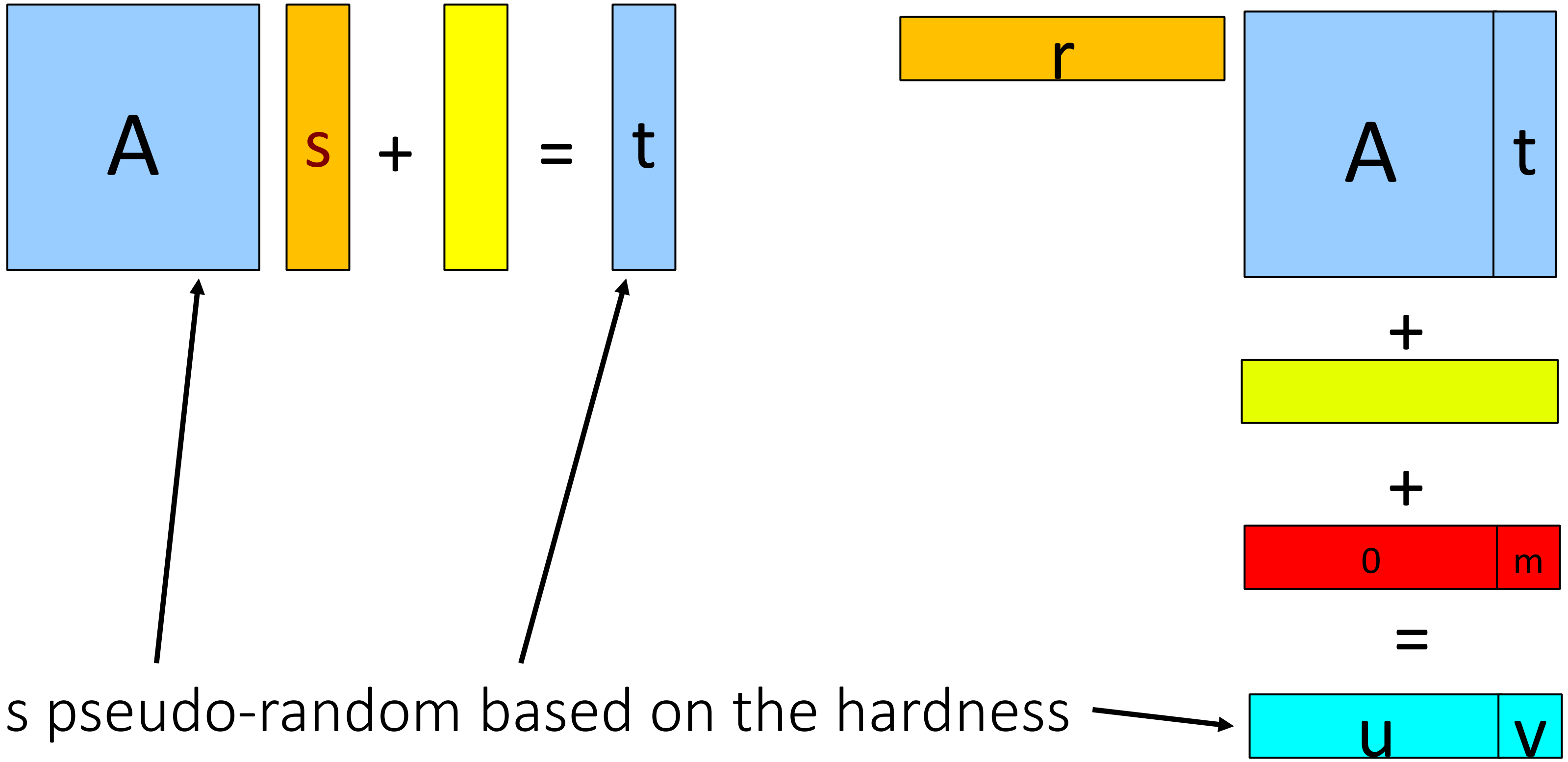
$$=\begin{bmatrix}6&3&2&2&0\end{bmatrix}$$

pseudorandom

Encryption Scheme

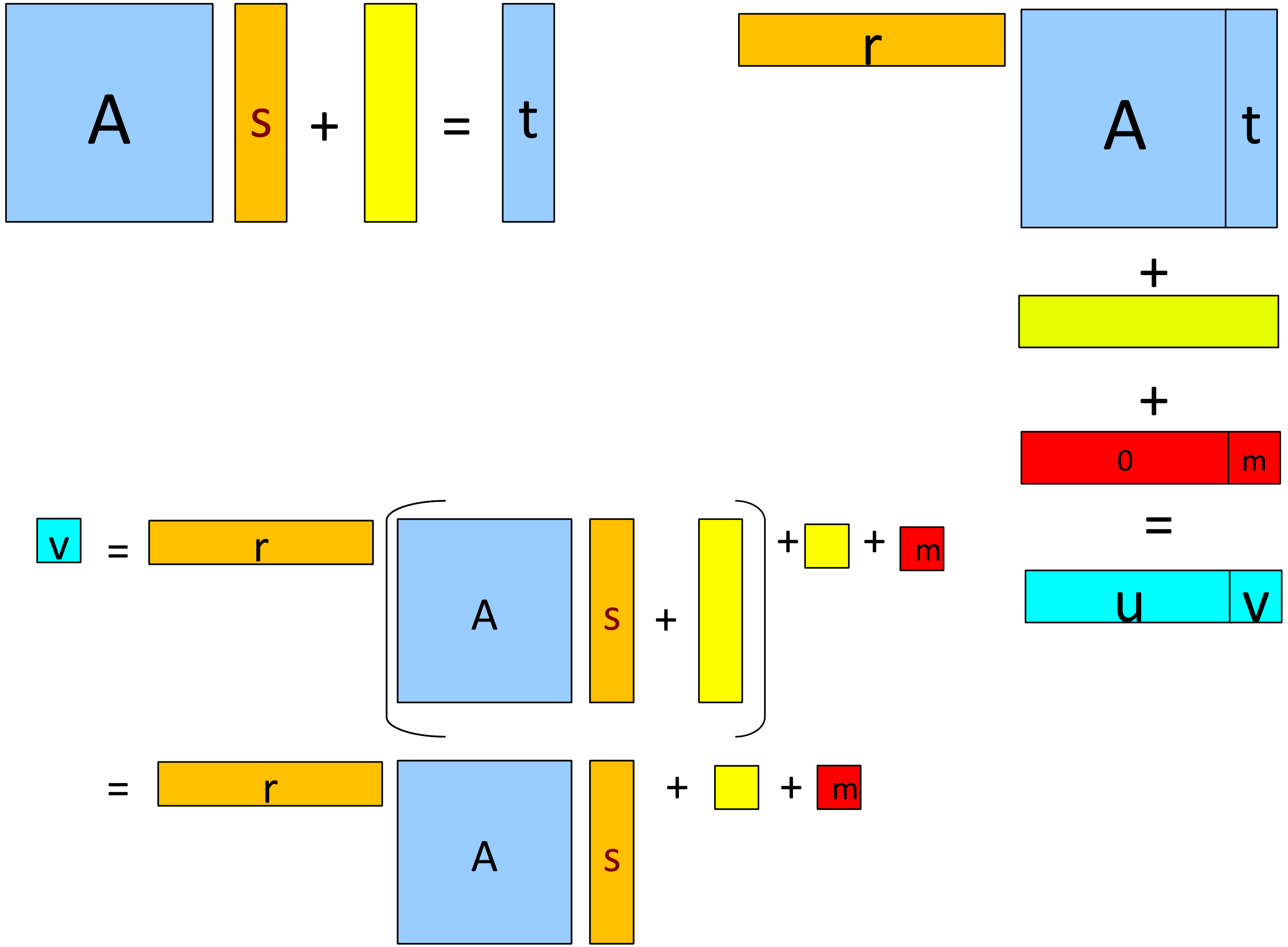


Encryption Scheme

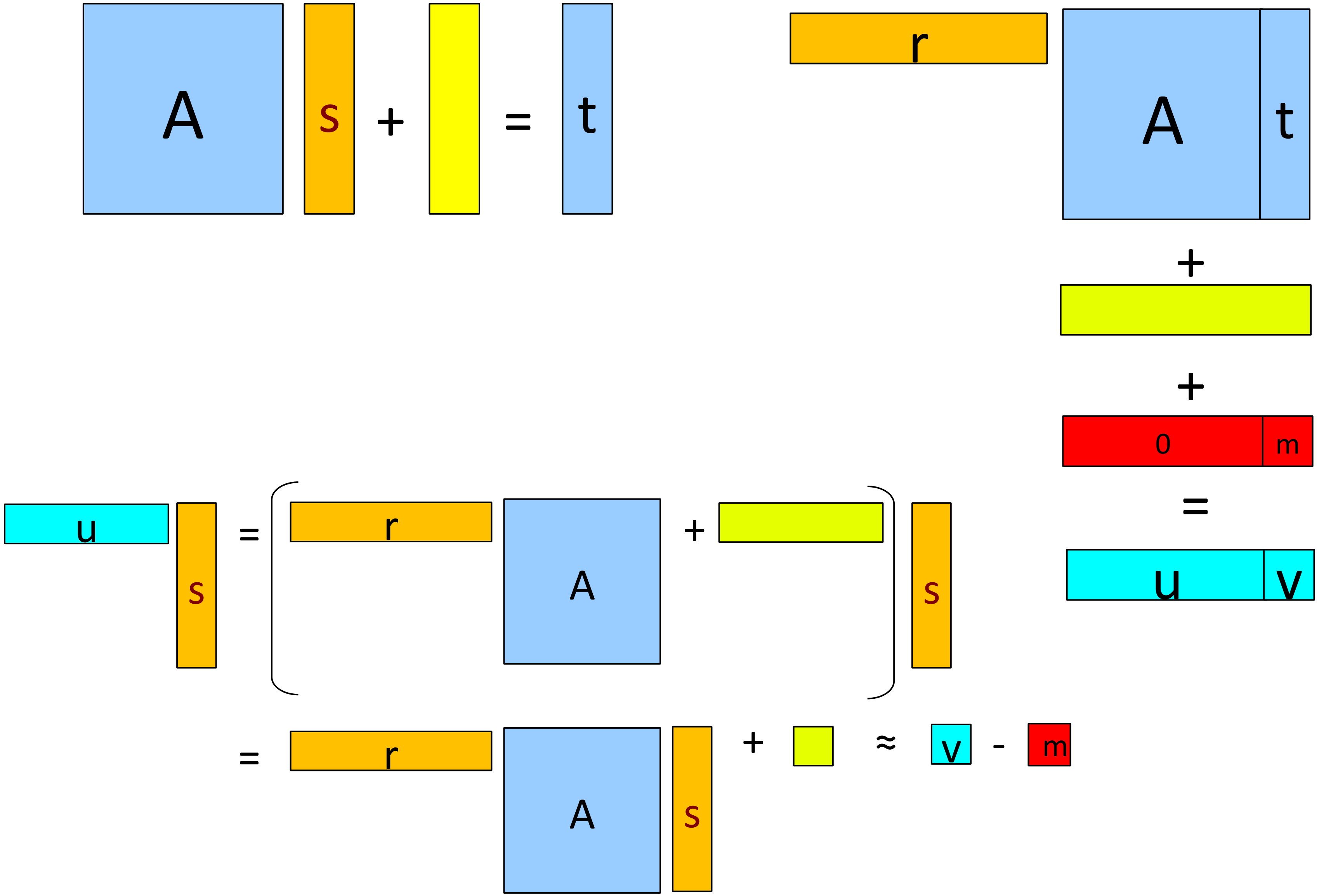


Is pseudo-random based on the hardness of the Learning with Errors Problem

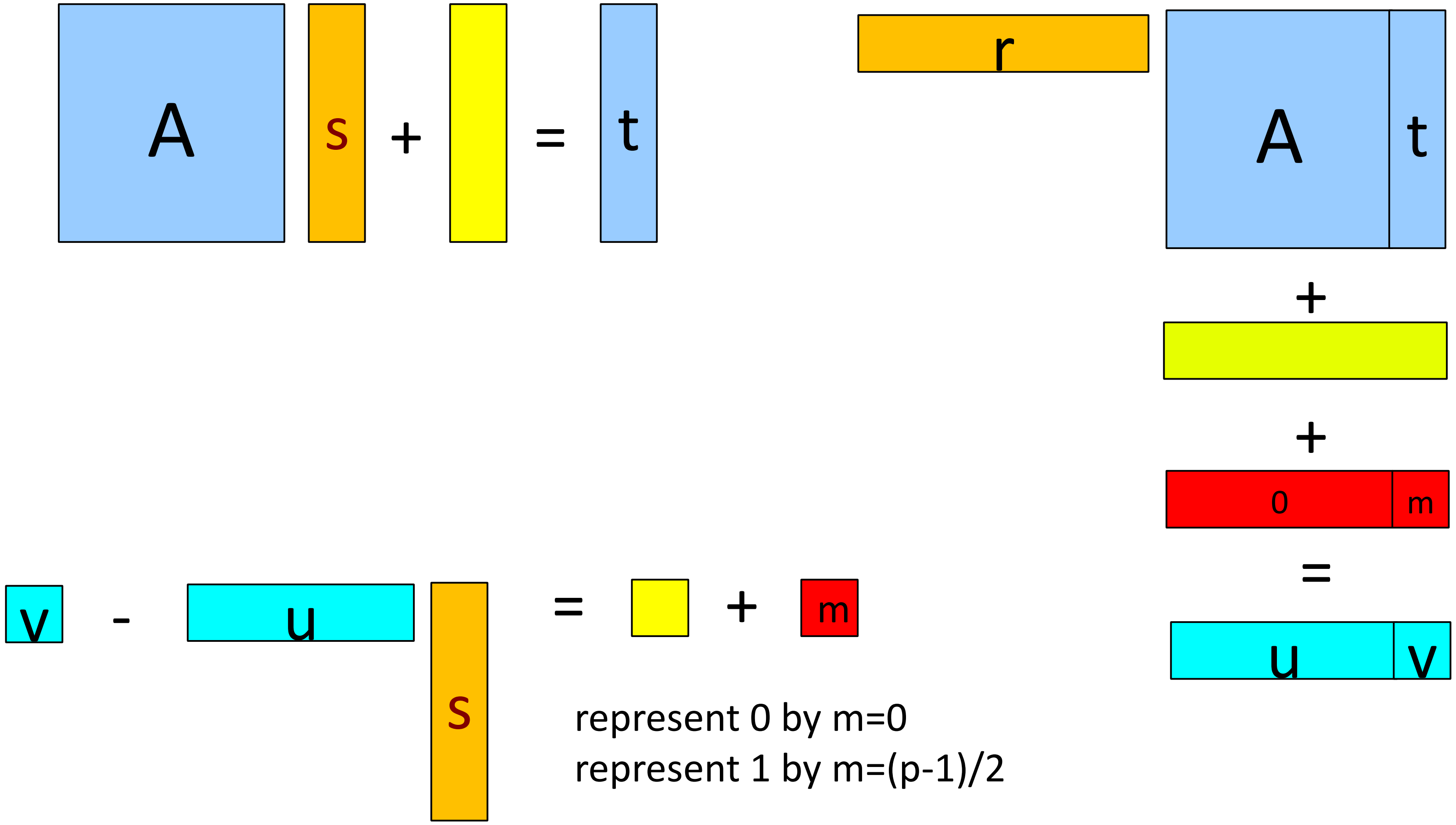
Encryption Scheme



Encryption Scheme



Encryption Scheme



Encrypts only 1 bit – large ciphertext expansion

1 bit requires n elements in Z_p

Decryption Error

Public Key: A, $t = As+e$

Ciphertext: $u = rA+e_1$, $v= rt + e_2 + m(p/2)$

Decryption: $v - us \ = r(As+e) + e_2 + m(p/2) – (rA+e_1)s$

$= re + e_2 + m(p/2) - e_1s$

Need the total error $re +e_2 - e_1s$ to be $< p/4$

(let's ignore e_2, since it's just an integer)

Say each coefficient of s, r, e, e_1, e_2 is uniformly random in {-1,0,1},

how do you make sure that the inequality is satisfied?

Decryption Error

- Can set p large enough so that re - e_1s to be < p/4 - 1
  - If the length of the vectors is n, then the maximum value is 2n
  - But intuitively, we expect the value to be around $\sqrt{n}$
  - So we will set p unnecessarily large

- Can use various inequalities (e.g. Chernoff, Hoeffding) and get closer to $\sqrt{n}$

- But we can do this much easier and more precisely

Decryption Error via Convolution

- Let's look at re = $\sum r_i \, e_i$ as the sum of n *independent* random variables
- What's the distribution of $r_i e_i$?
  - Pr[-1] = 2/9
  - Pr[0] = 5/9
  - Pr[1] = 2/9
- Write it as the polynomial $p(X)=(2/9)\ X^{-1} + (5/9)X^0 + (2/9)X^1$
- What's the distribution of $r_i e_i + r_j e_j$?
- Compute the product P(X)*P(X) and read off the coefficients!
- $\Pr[r_i e_i + r_j e_j = c]$ = the coefficient of X^c in P(X)*P(X)
- So $\Pr[re - e_1 s = c]$ = the coefficient of X^c in $P(X)^{2n}$

Problem Session

1. Implement the Encryption scheme:

    - p=257
    - Dimensions of A = 64 x 64
    - distribution of s,e,r,e_1,e_2 is Binomial: i.e. each coefficient is $b_0 + b_1 – b_2 – b_3$ (b_i are bits)

2. Write a script to compute the decryption error

Plan for the Week

1. Improve efficiency by working with polynomial rings
2. Number Theory Transform (like FFT)
3. Intro to Zero-Knowledge Proofs
4. Digital Signatures
5. Connection of these Constructions to Geometric Lattices

Supplementary Reading

https://github.com/VadimLyubash/LatticeTutorial/

(Today covered pages 1- 8)