# Mathematical Aspects of Few Secret Sharing Schemes


## Avishek Adhikari

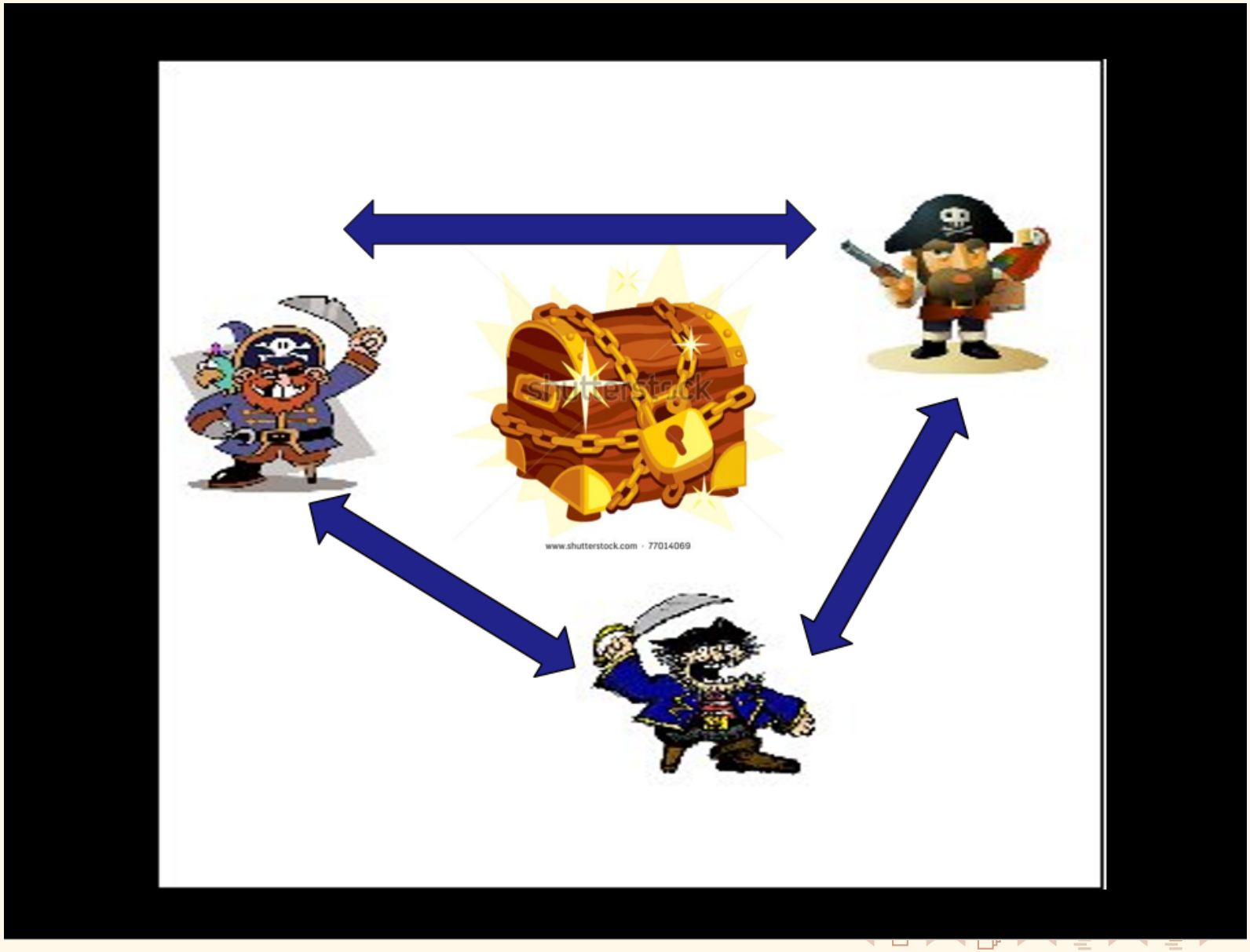
**Professor, Department of Mathematics**
**Presidency University, Kolkata.**
**Founder Secretary of IMBIC, India (Branches: Sweden, Japan)**
**Treasurer, Cryptology Research Society of India (CRSI)**

**Research Team Members**
**Jyotirmoy Pramanik, Md. Kutubuddin Sardar**
**Subarsha Banerjee, Sandip Kumar Mondal**
**Chandan Goswami and Dr Prakash Dey**

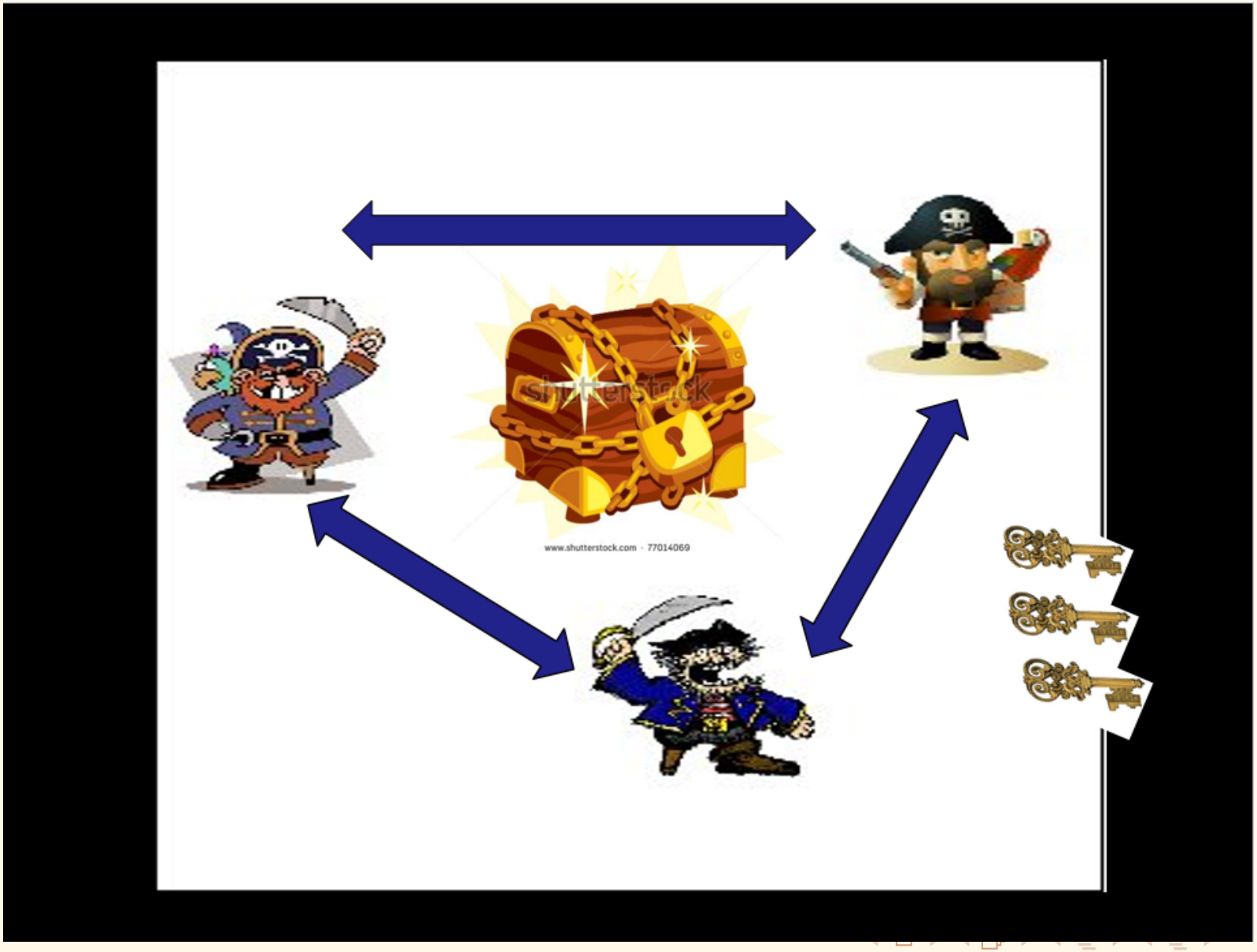
# What is Secret Sharing?

# What is Secret Sharing?

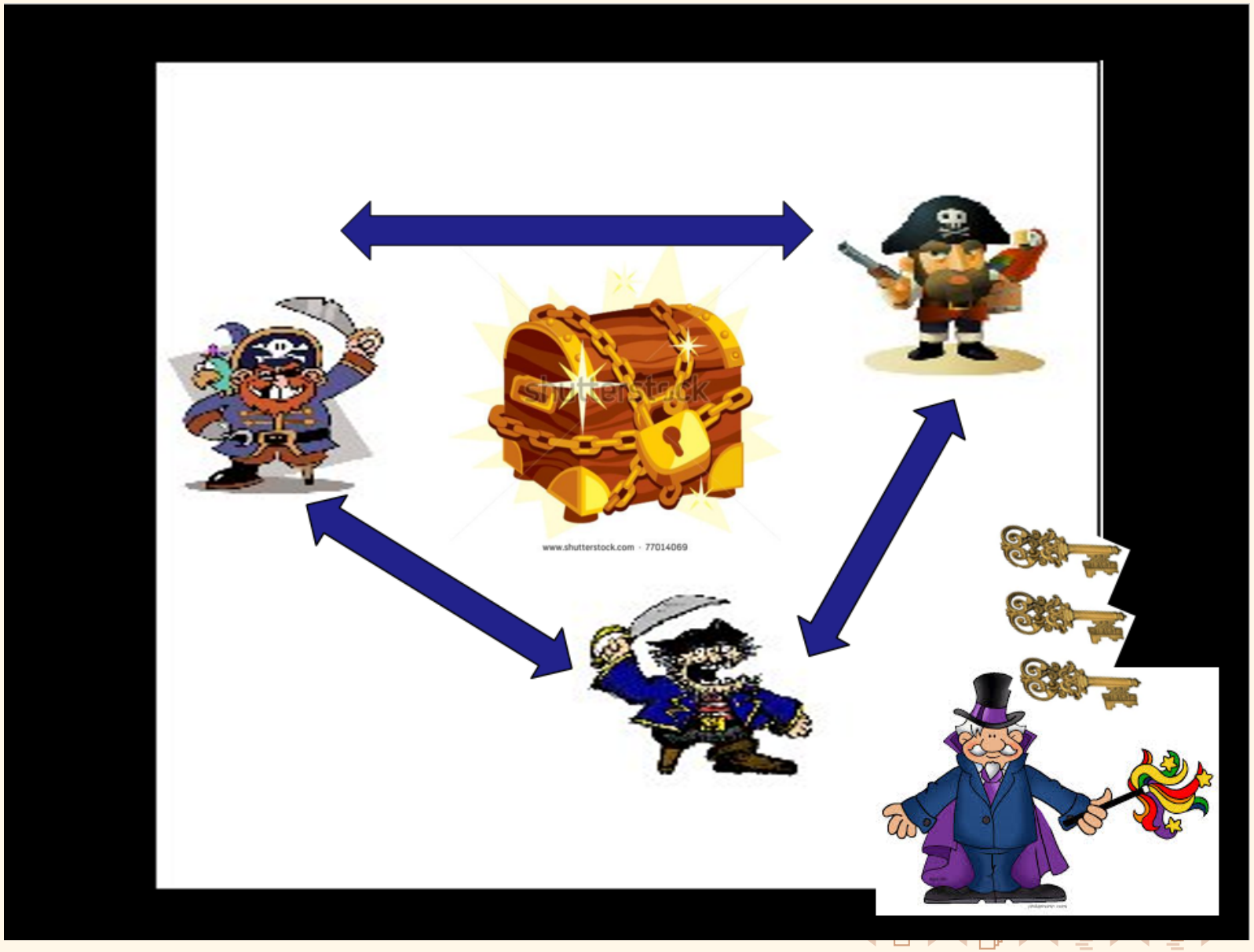
# What is Secret Sharing?



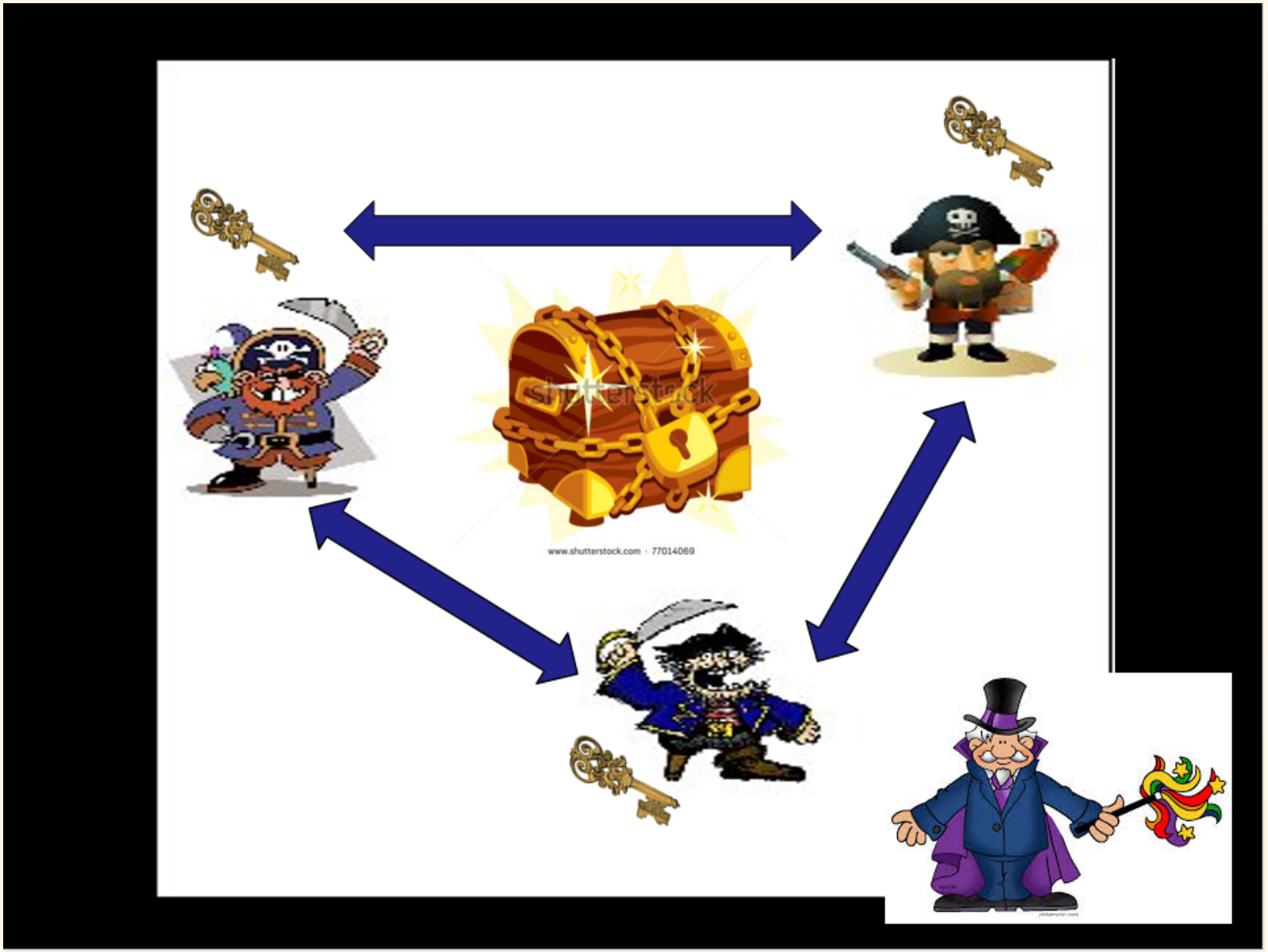
# What is Secret Sharing?



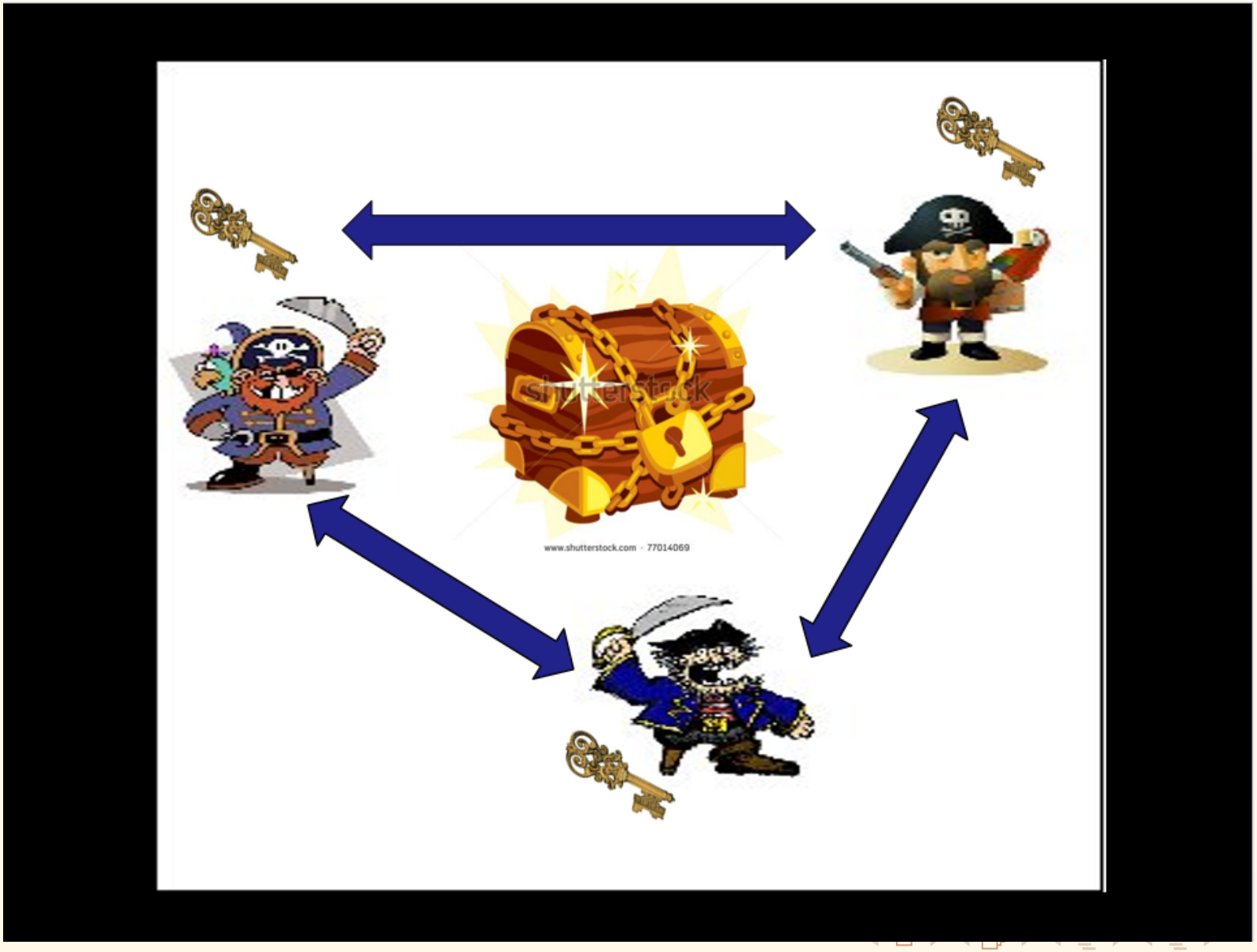
# What is Secret Sharing?



# What is Secret Sharing?



# What is Secret Sharing?

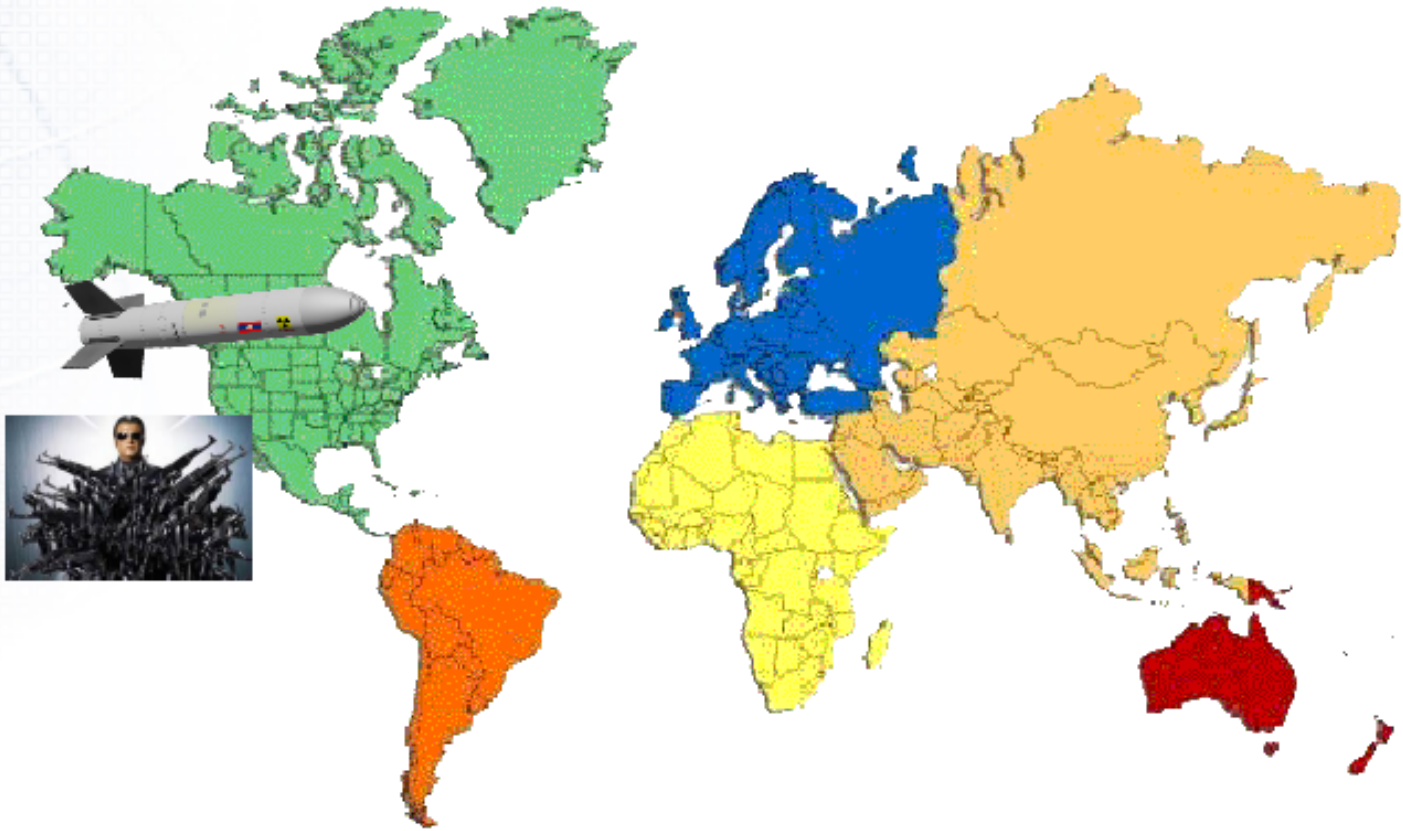


# $(t, w)$ threshold scheme

Let $t$ and $w$ be two positive integers, such that $t \leq w$. A $(t, w)$ *threshold scheme* is a method of sharing a scheme key $k$ among a set of $w$ participants in such a way that any $t$ participants can compute the value of $k$, but no group of $(t-1)$ participants can do so.

# Real Life Example of Secret Sharing

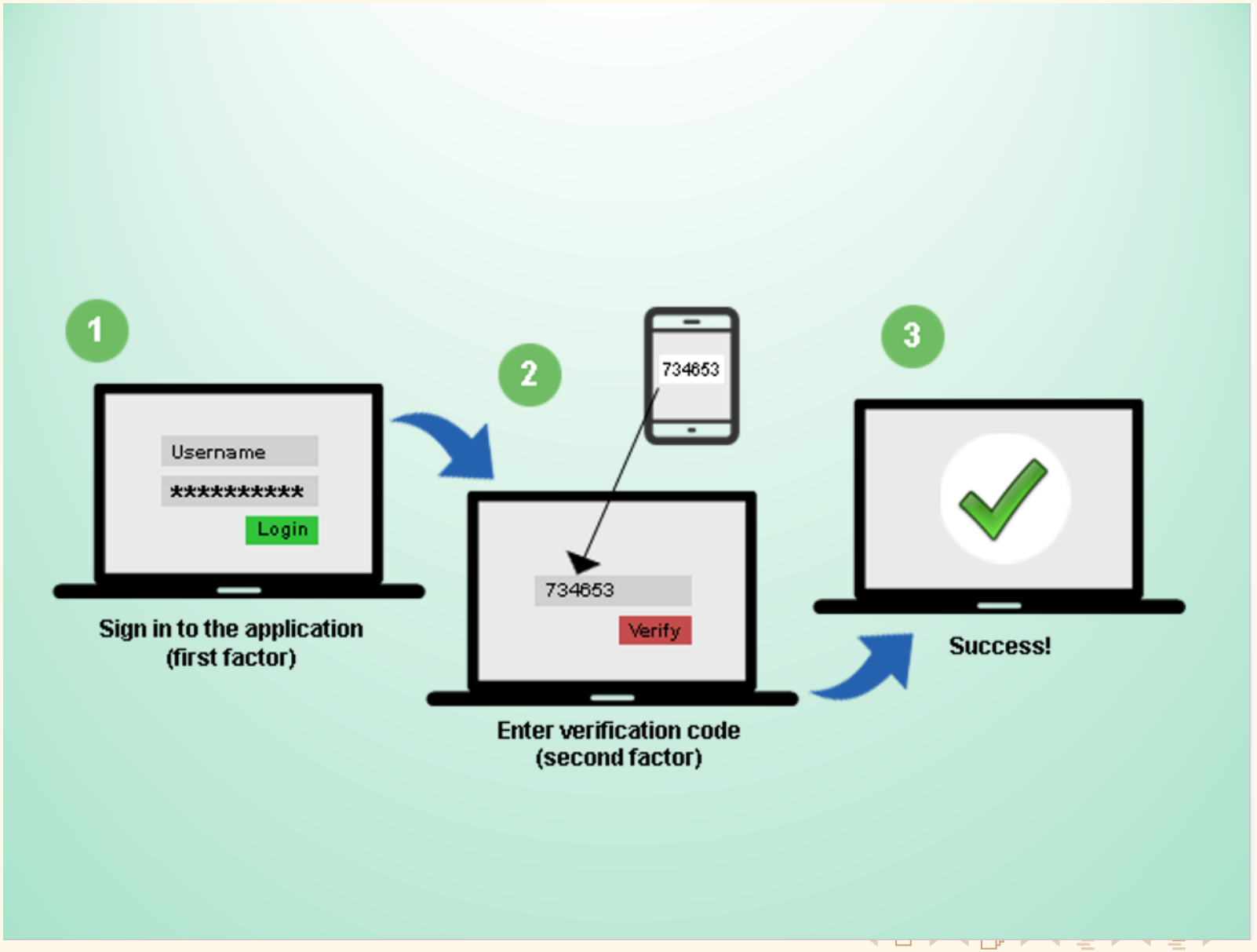
# Real Life Example of Secret Sharing



# Credit Card and its Pin

# Credit Card and its Pin


# Multi-Level Authentications



# Data Usages in India

hindustantimes

## India's internet consumption up during Covid-19 lockdown, shows data

Data from the department of telecommunications showed that between March 22 and March 28, Indians consumed an average of 307,963 TB or 307 petabytes (PB) of data.

INDIA Updated: Apr 21, 2020 21:38 IST

Data from the department of telecommunications showed that between March 22 and March 28, Indians consumed an average of 307,963 TB or 307 petabytes (PB) of data.

The daily average consumption in this period was 9% higher than 282PB data used on March 21 (the day the janta curfew was announced) and 13% more than March 19, when consumption was 270 PB. 1 PB=$10^6$ GB

# Data Usages in India

hindustantimes

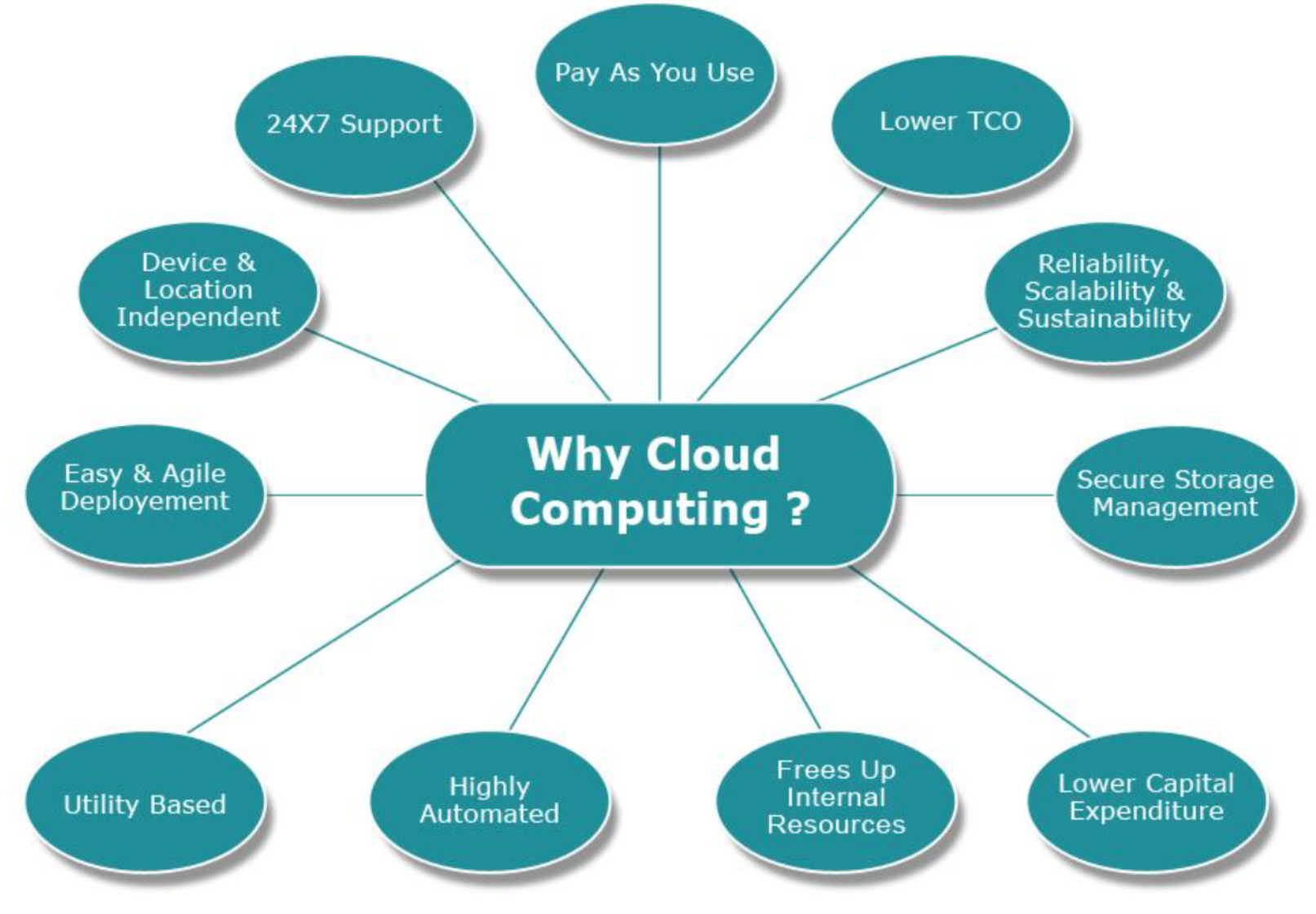
The consumption, DoT figures show, peaked on two days - March 22 and March 27 - when 312 PB of data was used. On March 26, 311 PB of data was consumed. The lockdown, announced on March 24, began on March 25. On March 22, India was put under a voluntary, one-day curfew.

Another Source: https://datareportal.com/reports/digital-2020-india

There were 400.0 million social media users in India in January 2020. The number of social media users in India increased by 130 million (+48%) between April 2019 and January 2020. [3]

# Application of Secret Sharing in Digital World

# Application of Secret Sharing in Digital World



# Application of Secret Sharing in Digital World

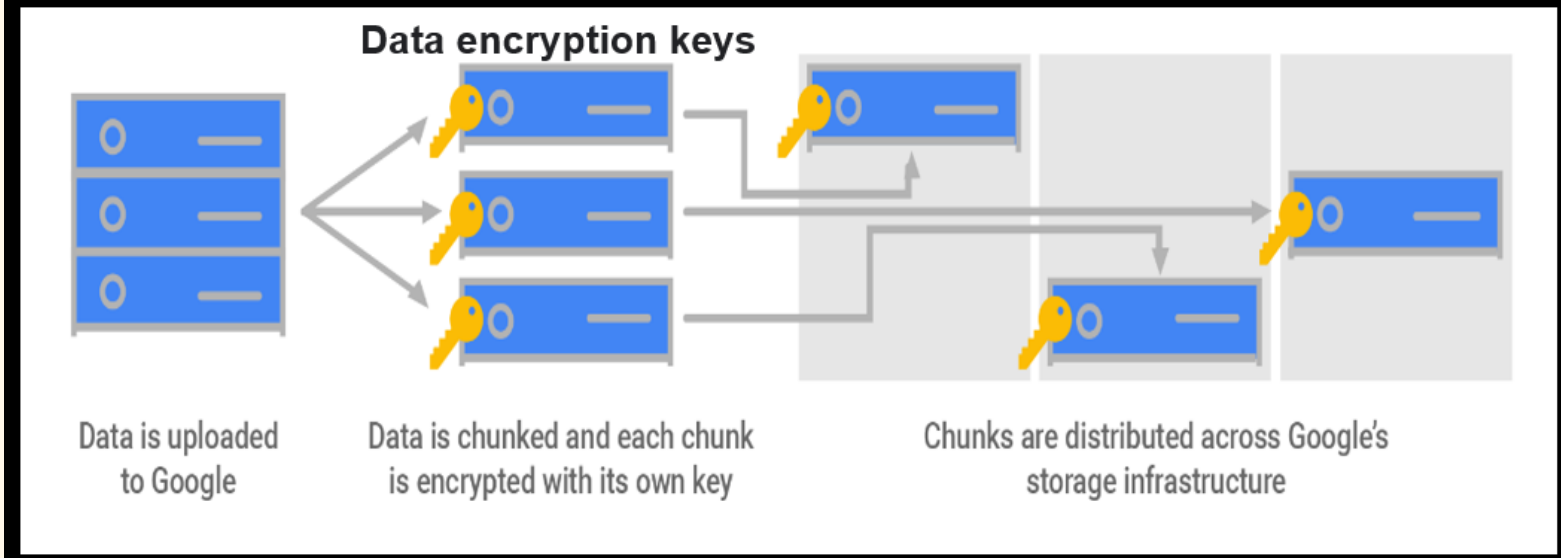
# Application of Secret Sharing in Digital World

# Application of Secret Sharing in Digital World

# Internet in Day-to-Day Life: Various Online Activities

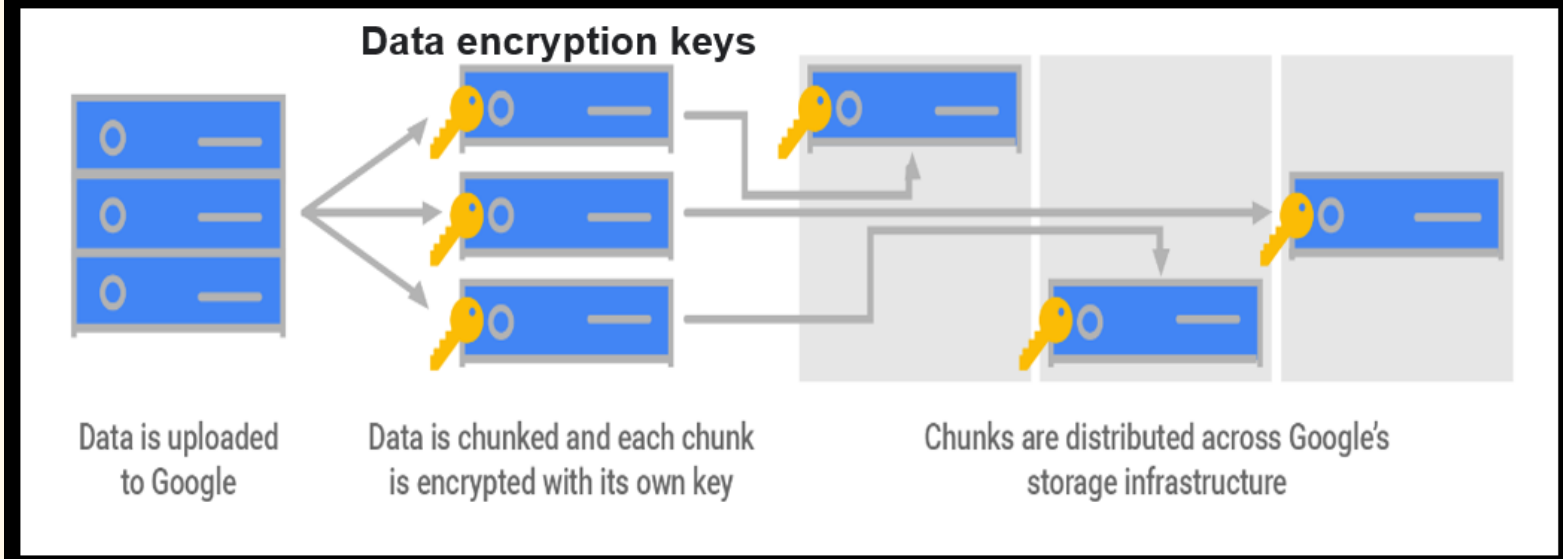
# All Have Secrets in Life

# How Google Cloud Stores Data at Rest




Each chunk is encrypted at the storage level with an individual encryption key: two chunks will not have the same encryption key, even if they are part of the same Cloud Storage object, owned by the same customer, or stored on the same machine.

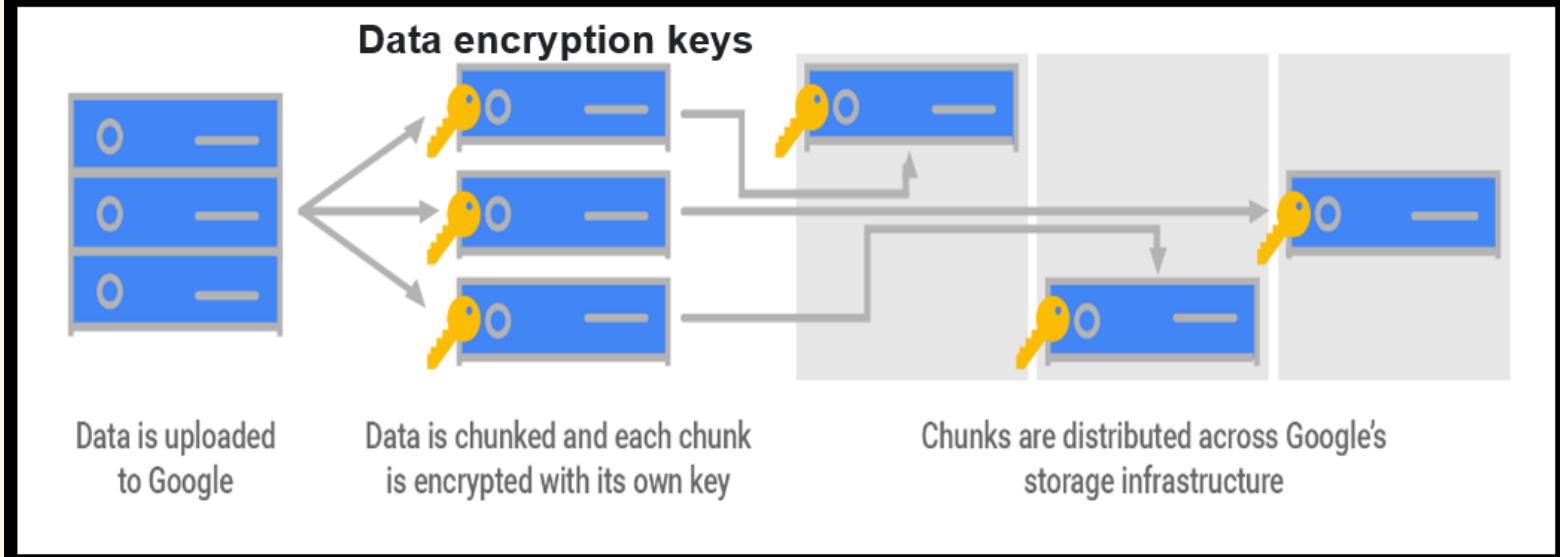
# Application of Secret Sharing in Digital World




The DEKs are encrypted with (or "wrapped" by) a *key encryption key (KEK)*. One or more KEKs exist for each Google Cloud service.

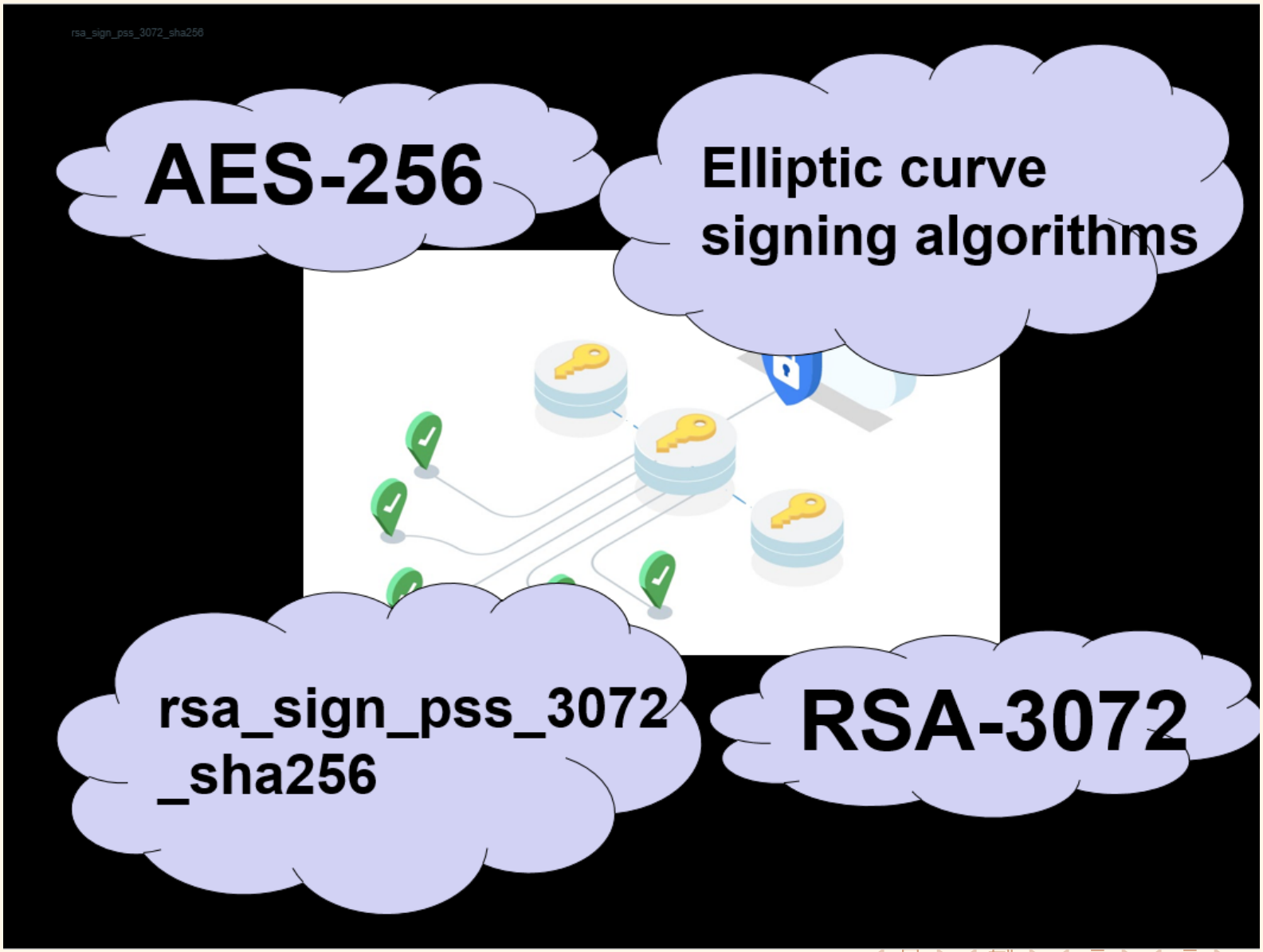
These KEKs are stored centrally in Google's *Key Management Service (KMS)*, a repository built specifically for storing keys.

# How Google Cloud Stores Data at Rest




When a storage system needs to retrieve encrypted data, it retrieves the wrapped DEK and passes it to KMS. KMS then verifies that this service is authorized to use the KEK, and if so, unwraps and returns the plaintext DEK to the service. The service then uses the DEK to decrypt the data chunk into plaintext and verify its integrity.

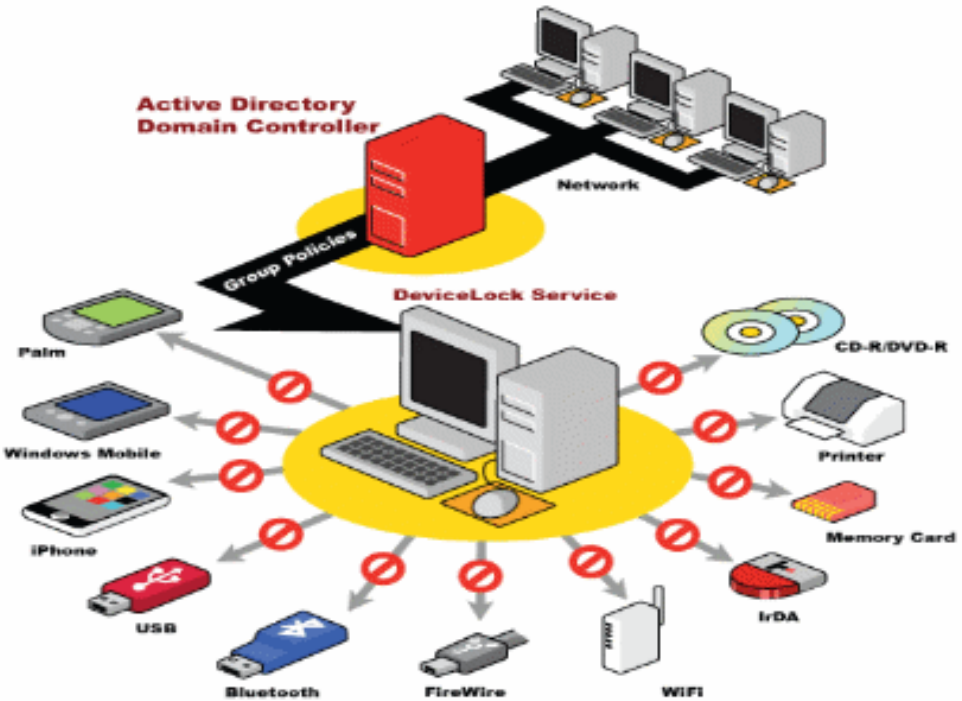
# Key Management Services: Cryptographic Tools Used



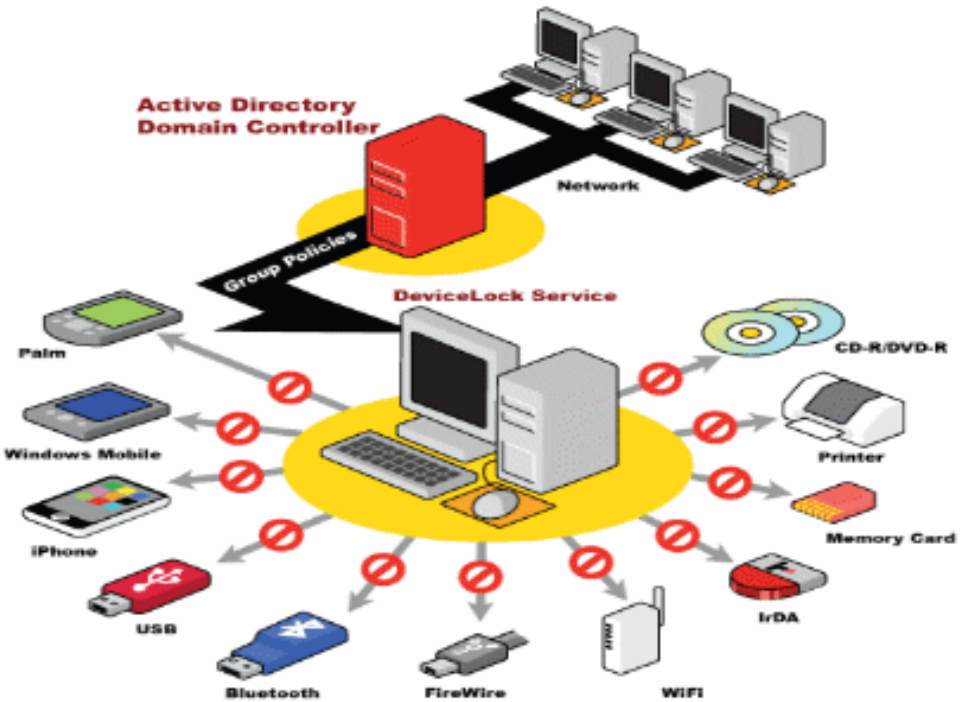
# Prime Numbers in our day to day life (904 digits)

1230231922161117176931558813276752514640713895736833
7157661180291600588006146729487753600678385934595824
2964925405180490851288418089823682358508248206534833
1234959350355845017413023320111360666922624728239756
8804164344783156936750134130907572086903767932966588
1066294182449348845172650530371291600534674790862370
2673480919353936813105736620402352744776903840477883
6511003224093019834883638029305404824879097634840982
5394072868513204440886373475427121259247177864394948
6688511721051561970432780747454823776808464180697103
0838618121843485655227401957966826222055118455120805
5201031005025580158934964592800113374547422071501368
3413907542779063759833876101354235184245096670042160
7206294115815023712480084304471848420986103205804179
9220666224732872212208851364368390767036020916265367
0641130936997002170500675501374723998766005827579300
7232534748906122501351718891748990799112915123997738
72178519018229993369

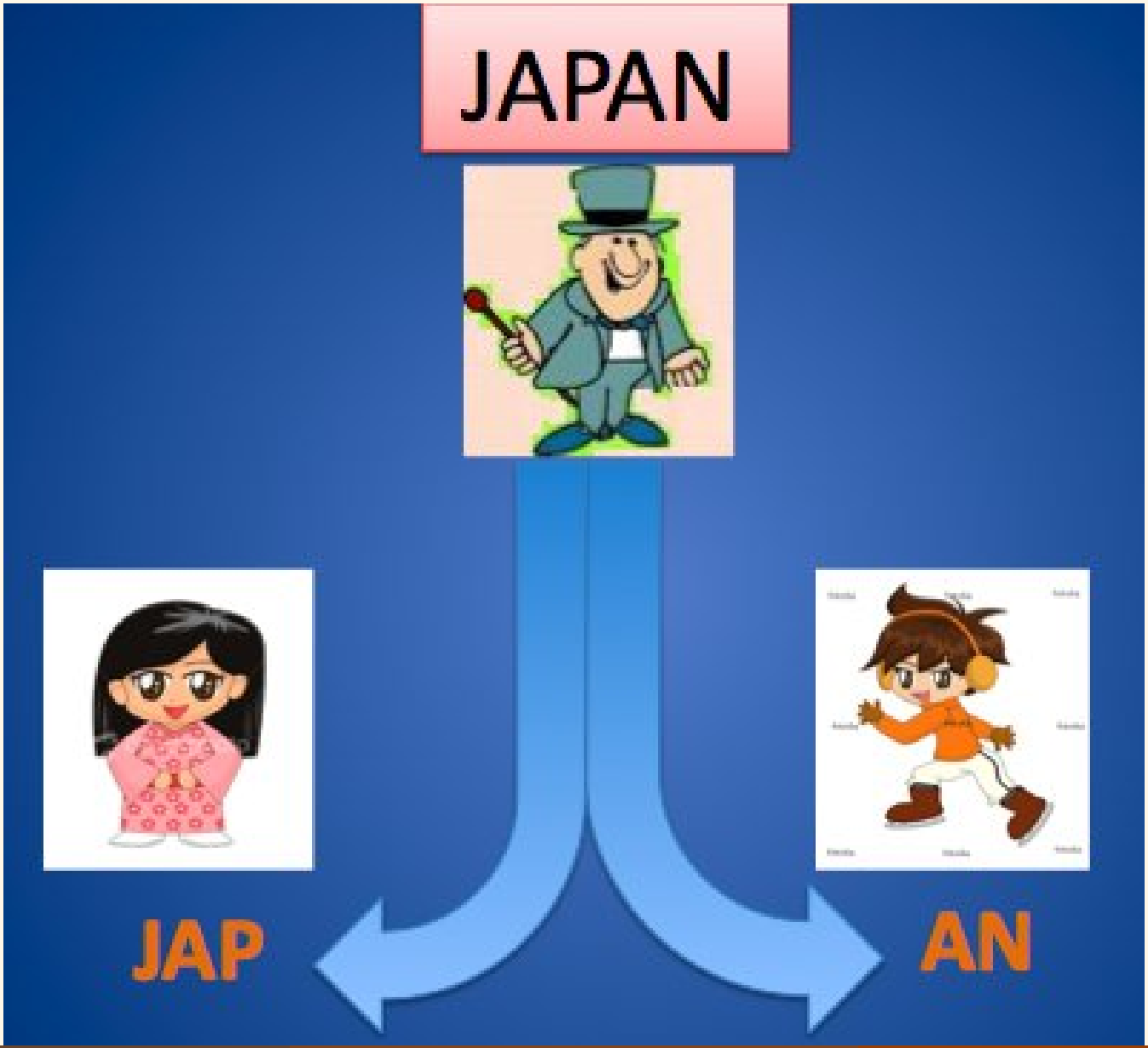
# Storing Secrets in Different Places

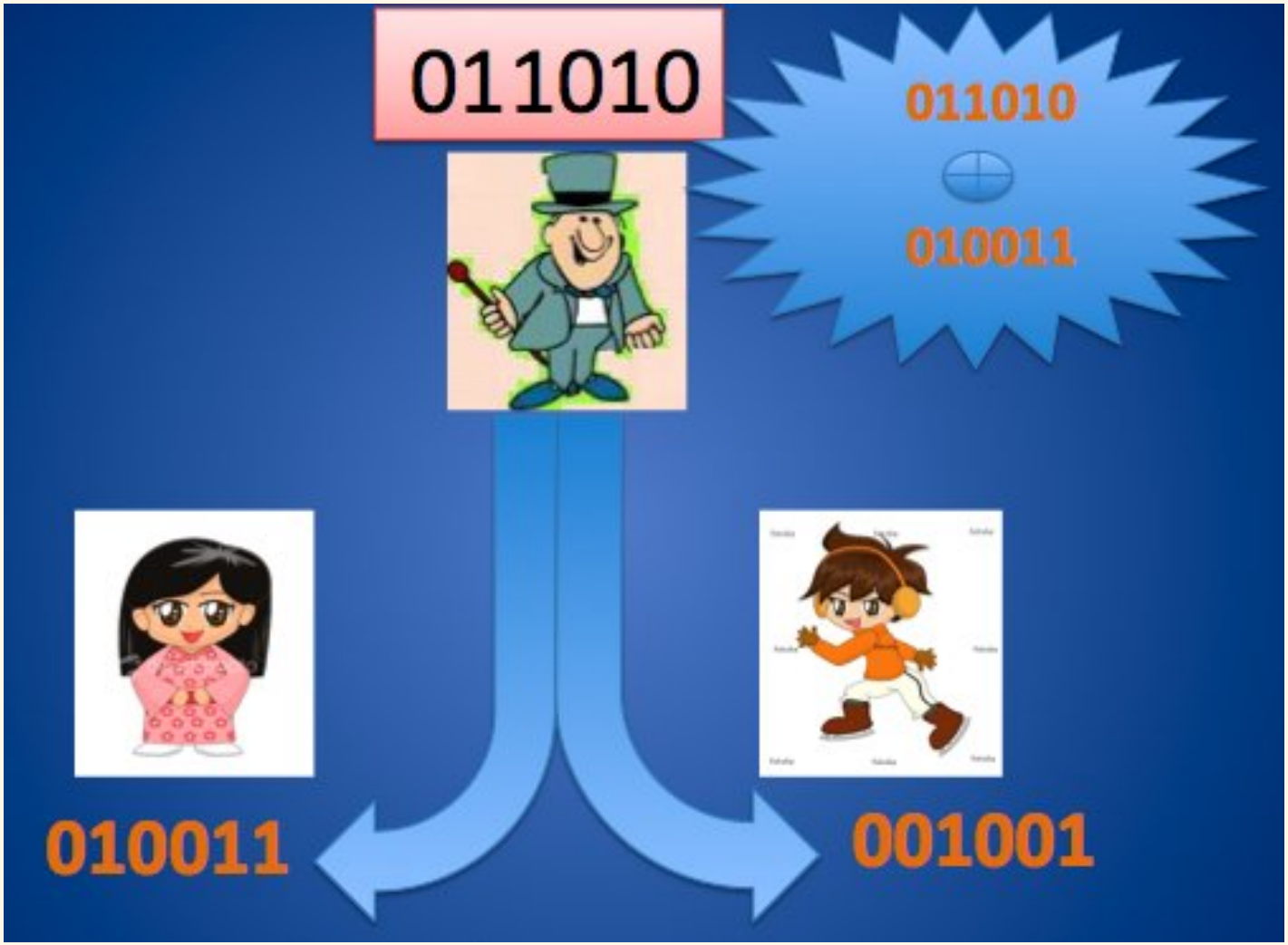
# Storing Secrets in Different Places

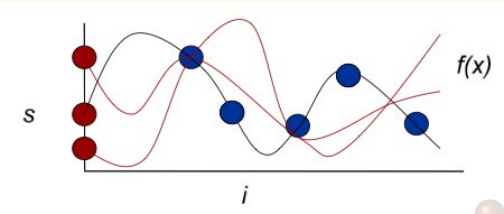

# Simple Way!



# Perfectly Secure (2,2)-SSS

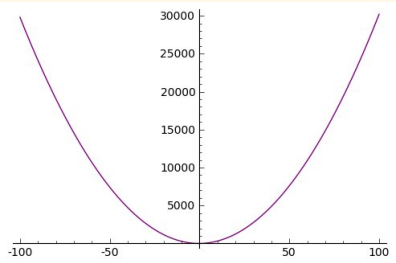


# Shamir's $(k, n)$-Secret Sharing Scheme



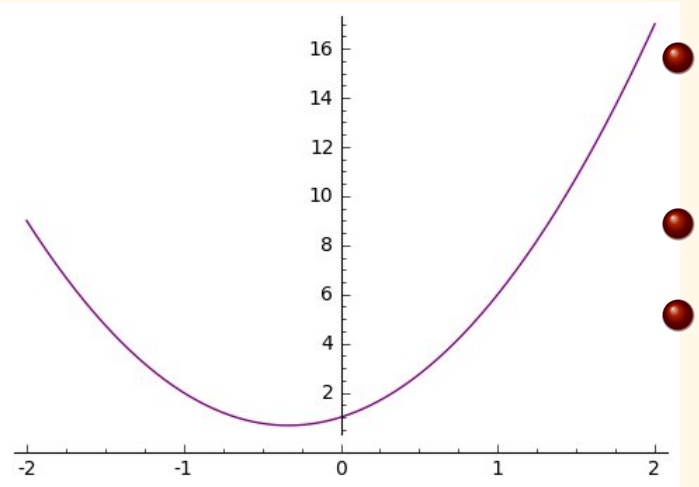

- It takes two points to define a straight line, three points to fully define a quadratic, four points to define a cubic, and so on.
- One can fit a unique polynomial of degree $(k-1)$ to any set of $k$ points that lie on the polynomial.

# Shamir's $(k, n)$-Secret Sharing Scheme




- It takes two points to define a straight line, three points to fully define a quadratic, four points to define a cubic, and so on.
- One can fit a unique polynomial of degree $(k-1)$ to any set of $k$ points that lie on the polynomial.

# Shamir's (3, 4) threshold scheme




- Let $\mathcal{P}=\{P_1, P_2, P_3, P_4\}$ be a set of 4 participants.
- The key set, $\mathcal{K}=\mathbb{Z}_p$, where $p = 5$ is a prime & $p > n$. Let the secret be 1.
- The set of all possible shares, $\mathcal{S}=\mathbb{Z}_5$.
- The dealer constructs a random polynomial $f(x) \in \mathbb{Z}_5[x]$ of degree $t - 1 = 3 - 1 = 2$, in which the constant term is the secret $K = 1$.

$$f(x) = 1 + 2x + 3x^2$$

# Shamir's (3, 4) threshold scheme

- Every participant $P_i$ obtains a point $(x_i, y_i)$ on this polynomial, where $y_i = f(x_i)$ and distinct $x_i \in \mathbb{Z}_p$.
- $P_1$ gets (1,a(1)=6=1), ($P_2$) gets (2,2), $P_3$ gets $(3, 4)$ and $P_4$ gets (4,2).

## Recovery of Secret

- Suppose a subset B of $t = 3$ participants wants to recollect the secret.
- Let the participants $P_1, P_2, P_3$ want to determine $K = 1$.
- They know that $1 = f(1)$, $2 = f(2)$ and $4 = f(3)$.
- They will assume the form of the secret polynomial as $y = f(x) = a_0 + a_1 x + a_2 x^2$, where $a_0, a_1$ and $a_2$ are unknown and belong to $\mathbb{Z}$.
- Thus, these participants can obtain 3 linear equations in the 3 unknowns $a_0, a_1, a_2$.

# Shamir's (t, n) threshold scheme

- $$\begin{bmatrix} 1 & 1 & 1^2 \\ 1 & 2 & 2^2 \\ 1 & 3 & 3^2 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \end{bmatrix} = \begin{bmatrix} f(1) \\ f(2) \\ f(3) \end{bmatrix}$$
  - Now, the coefficient matrix $A$ is the so called Vandermonde's matrix.

$$detA = \prod_{1 \le j < k \le t} (x_{i_k} - x_{i_j}) \mod p = (1-2)(2-3)(3-1) = 4*4*2 = 2 \neq 0$$

Thus multiplying both sides by the inverse of A, we can find the $a_0 = 1$.

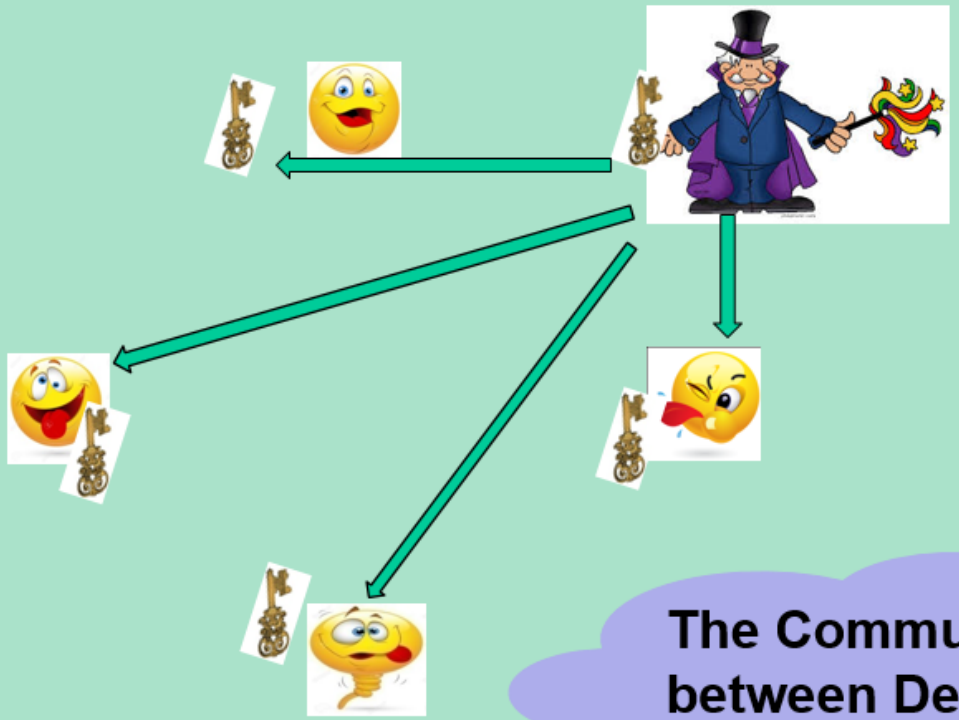
# Shamir's (t, n) threshold scheme

- $$\begin{bmatrix} 1 & 1 & 1^2 \\ 1 & 2 & 2^2 \\ 1 & 3 & 3^2 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \end{bmatrix} = \begin{bmatrix} f(1) \\ f(2) \\ f(3) \end{bmatrix}$$
- Now, the coefficient matrix $A$ is the so called Vandermonde's matrix.

$$detA = \prod_{1 \le j < k \le t} (x_{i_k} - x_{i_j}) \mod p = (1-2)(2-3)(3-1) = 4*4*2 = 2 \neq 0$$

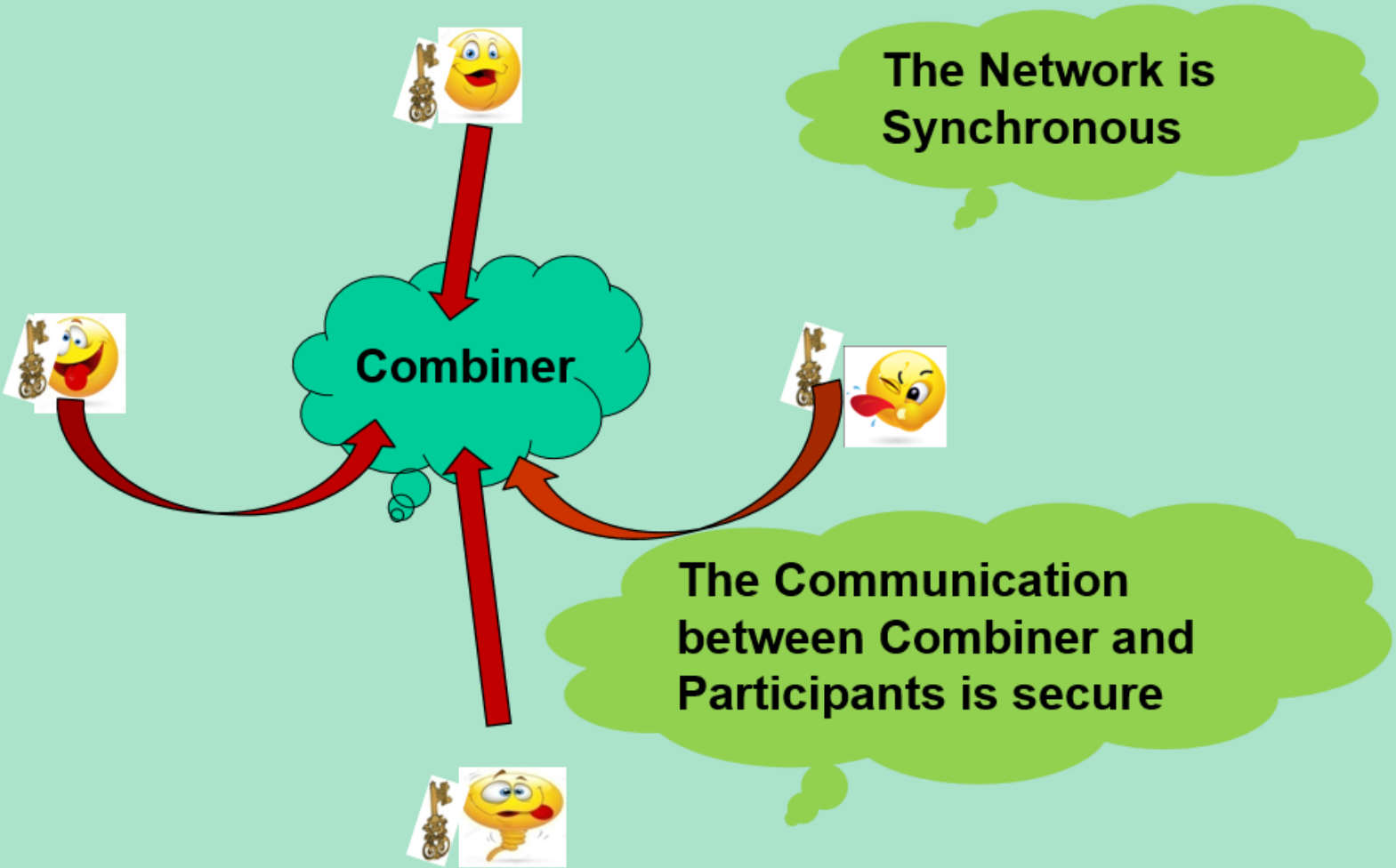
Thus multiplying both sides by the inverse of A, we can find the $a_0 = 1$.

# Communication Model in SSS

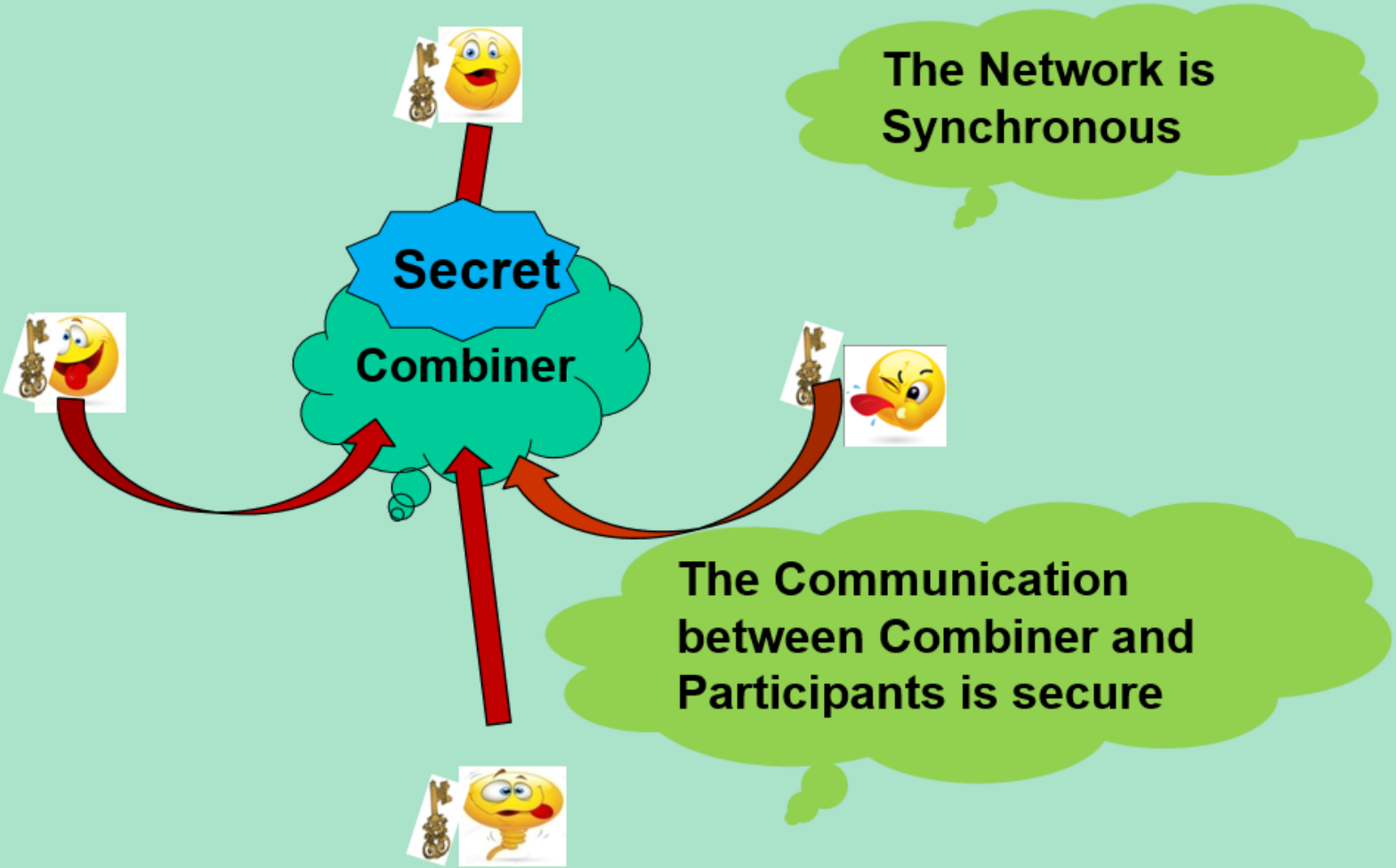


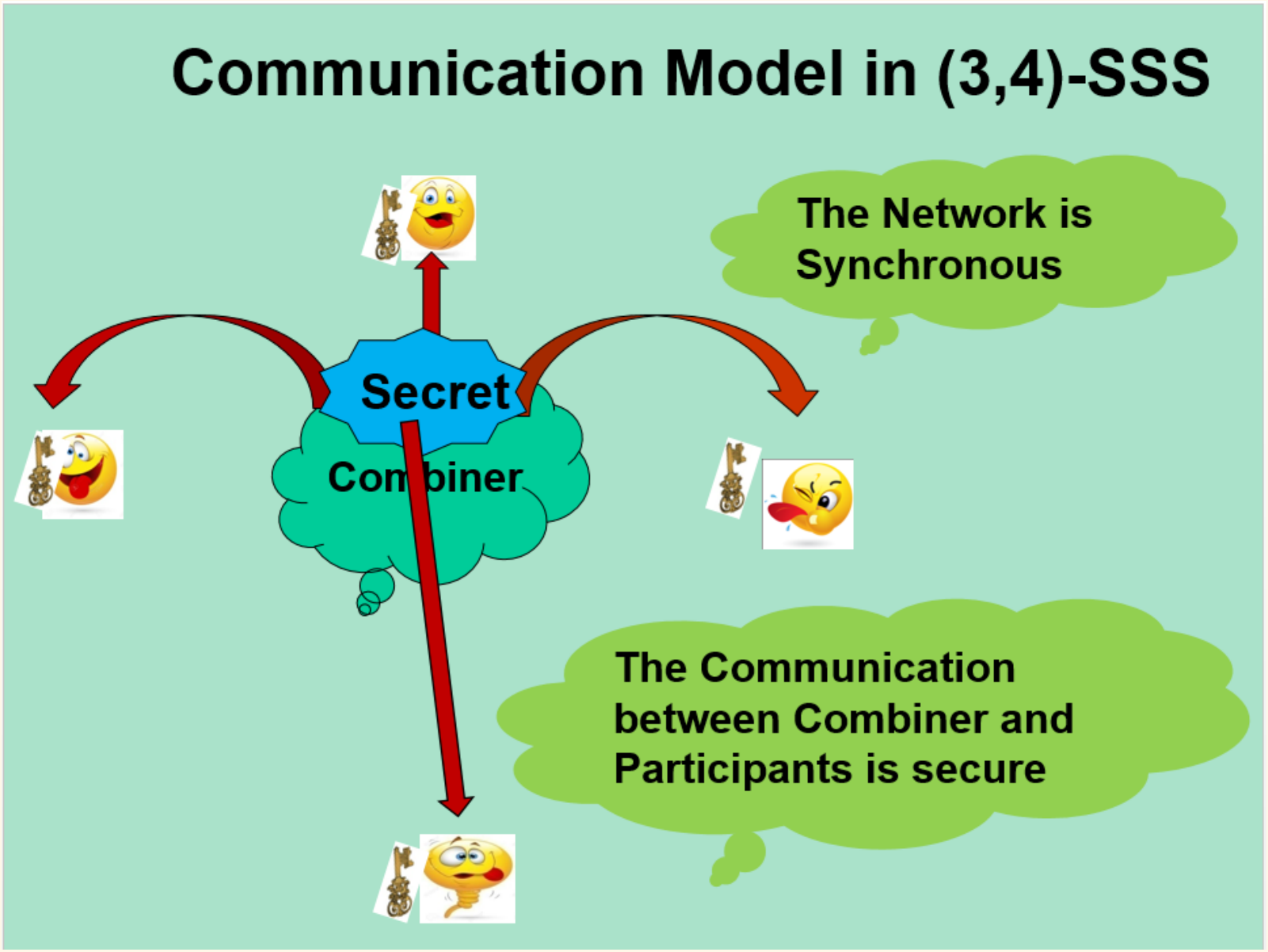
The Communication between Dealer and Participants is secure

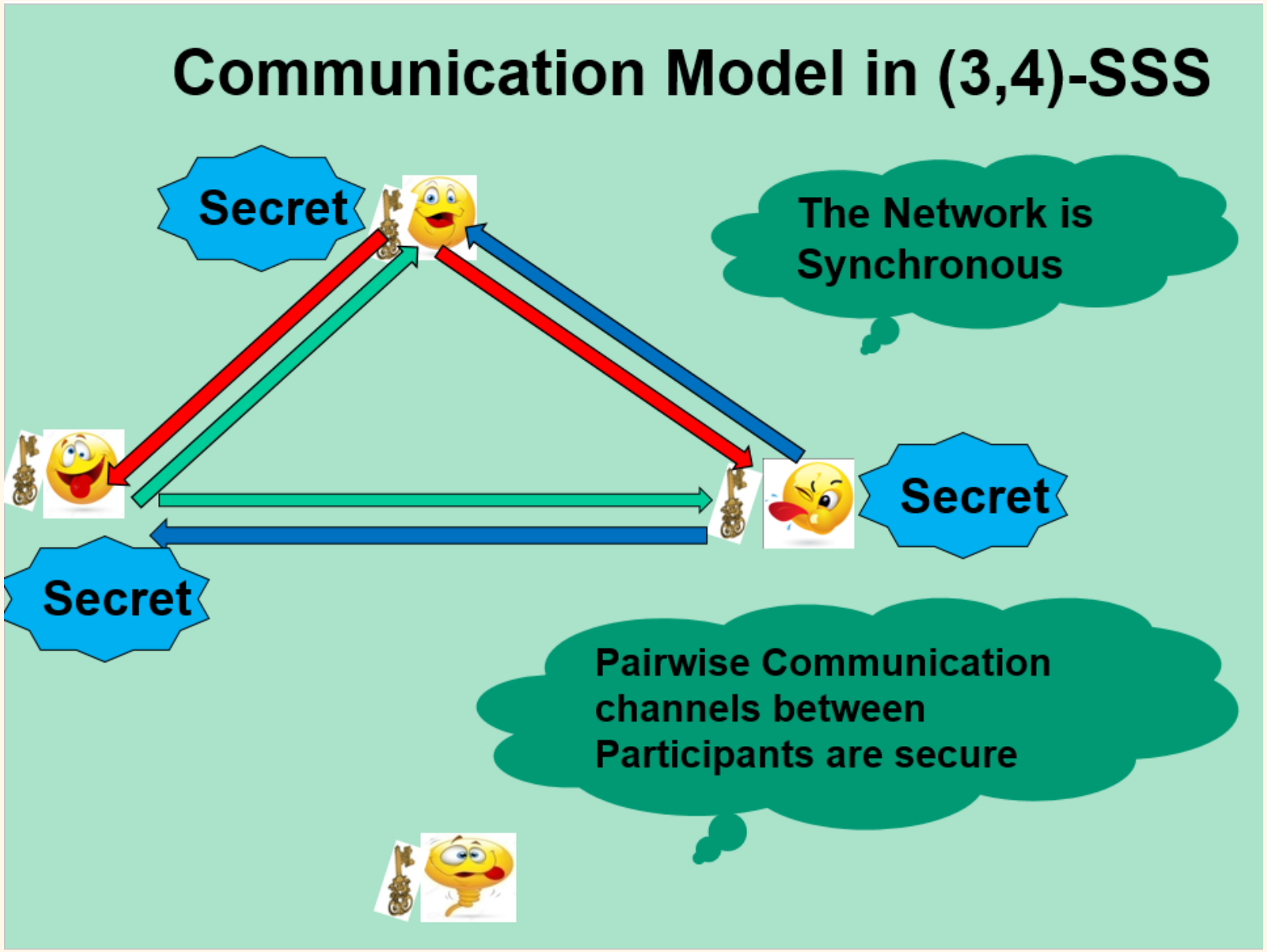
# Communication Model in (3,4)-SSS



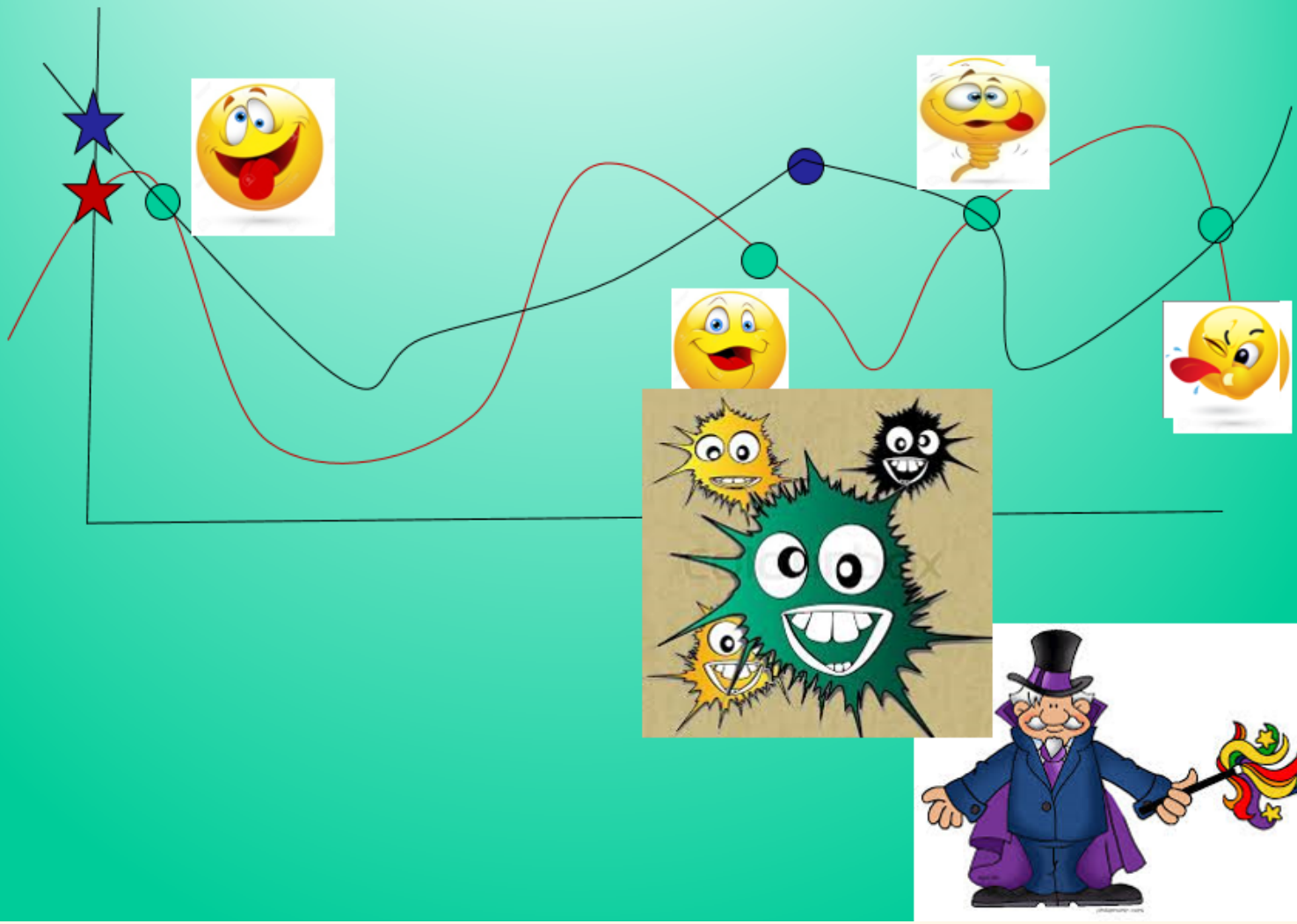
# Communication Model in (3,4)-SSS




Communication Model in (3,4)-SSS
The Network is Synchronous
Secret
Combiner
The Communication between Combiner and Participants is secure

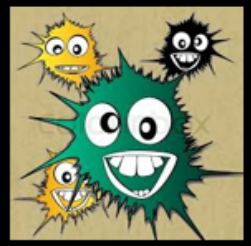

Communication Model in (3,4)-SSS
Secret
The Network is Synchronous
Secret
Secret
Pairwise Communication channels between Participants are secure

# Twist in the Story!



# Characterization of Adversarial Activities

Adversary



Honest but Curious

Malicious

Non-Rushing

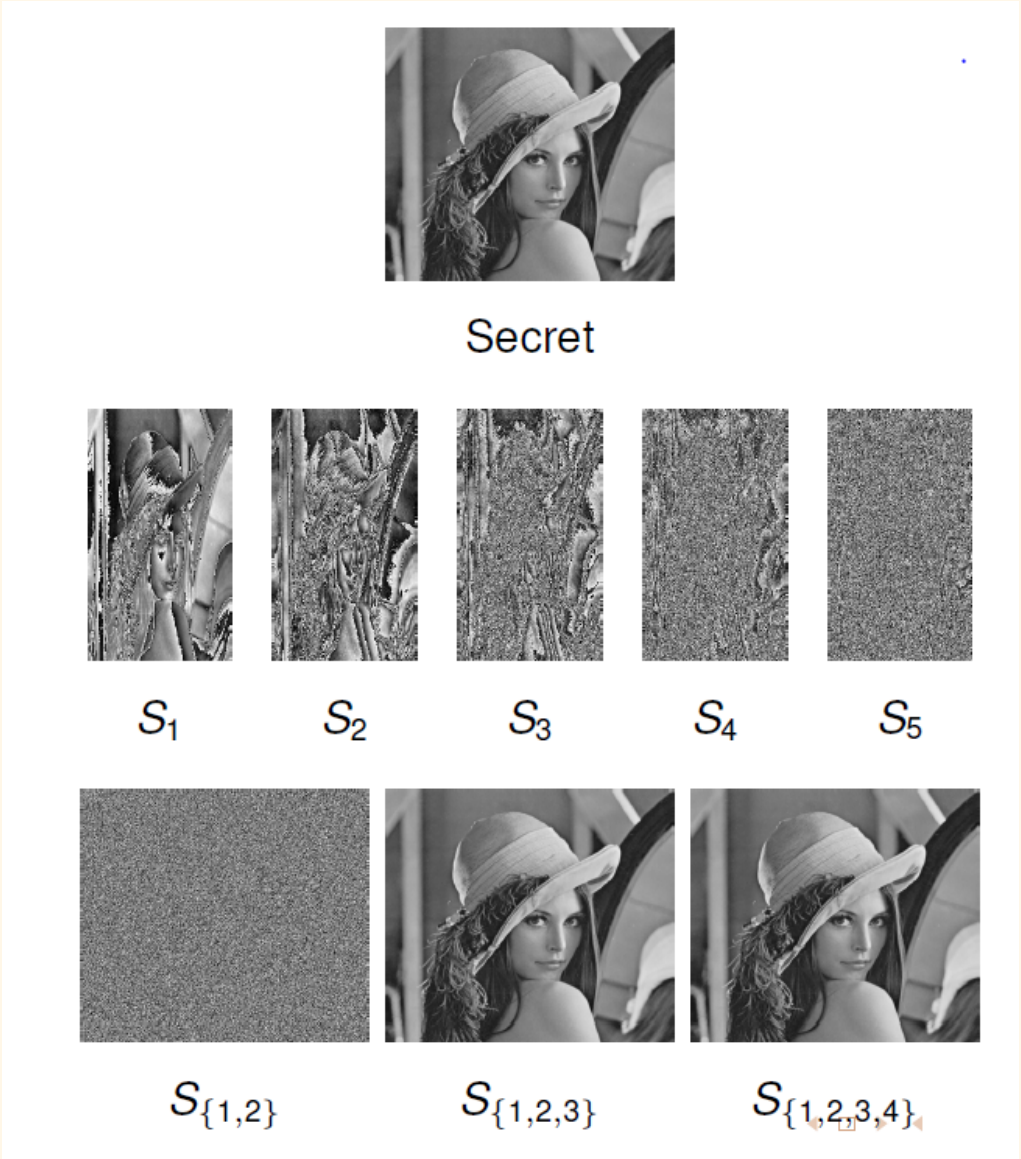
Rushing

# Different Types of Secret Sharing

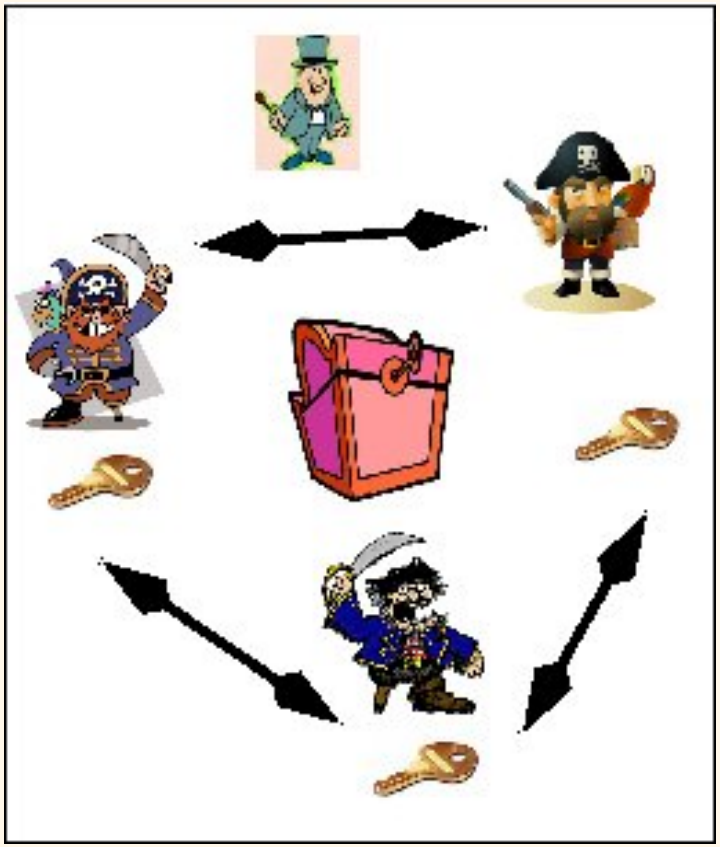
Secret Sharing Scheme (SSS)

- SSS in Presence of Semi-honest Adv.
- SSS in Presence of Malicious Adv.(Rushing/Non-rushing)
  - Cheating Detectable SSS
  - Cheating Identifiable SSS
  - Robust SSS
  - Verifiable SSS


# $(k, n)$-Image Sharing Scheme (Thien and Lin, '02)



# *t*-(k,n)-Secret Sharing Scheme



# *t*-(k,n)-Secret Sharing Scheme

# *t*-(k,n)-Secret Sharing Scheme

# $t$-$(k, n)$-Secret Image Sharing Scheme

# $t$-$(k, n)$-Secret Image Sharing Scheme

ARTICLE IN PRESS

Signal Processing: Image Communication xxx (xxxx) xxx

Contents lists available at ScienceDirect

Signal Processing: Image Communication

journal homepage: www.elsevier.com/locate/image


## Essential secret image sharing scheme with small and equal sized shadows

Md Kutubuddin Sardar [a], Avishek Adhikari [b,*]

[a] Department of Pure Mathematics, University of Calcutta, India
[b] Department of Mathematics, Presidency University, India

ARTICLE INFO

*Keywords:*
Grayscale image
Finite field
$(t, k, n)$-threshold secret sharing scheme

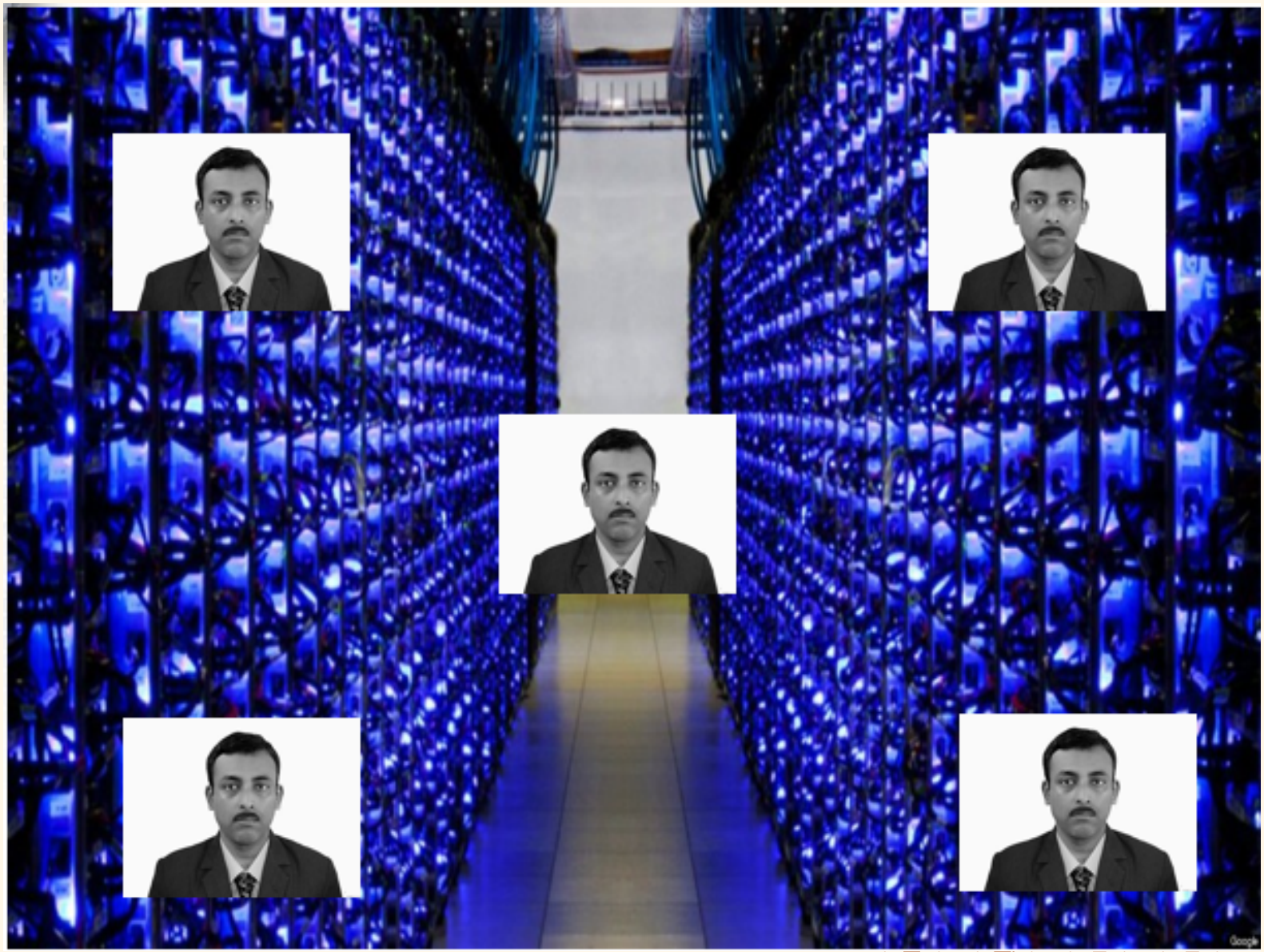
ABSTRACT

In the literature of secret sharing, the property of essential secret sharing scheme ensures that no set of participants, missing at least one essential participant, should be able to get any information regarding the secret. However, there are essential secret image sharing schemes available in the literature in which we have shown mathematically as well as through experiments that any $k$ or more non-essential participants together can get information about the secret image. It is true that in most of these schemes, preprocessing steps such as random permutations or chaotic maps are used on the secret image to avoid this problem. But that will surely introduce an overhead to the schemes. Moreover, the security of these schemes mainly depends on the preprocessing step and not on the secret sharing schemes. However, our proposed $(t, k, n)$-ESIS scheme for grayscale images over the finite field GF($p^m$) does not require any preprocessing step to secure the scheme. Though, the proposed scheme over GF($p^m$) with $p^m > 2^8$ is little lossy, it has the advantage over most of the ESIS schemes in the sense that the scheme works fine, even if the number of participants is more than 255. Most importantly, our proposed scheme over GF($2^8$) is completely lossless. Moreover, our proposed scheme, does not have the limitations such as different size of shadows, concatenation of sub-shadows, use of derivative polynomials etc. Finally, our scheme has reduced share size and work fine without any preprocessing steps on secret image, making our scheme efficient.

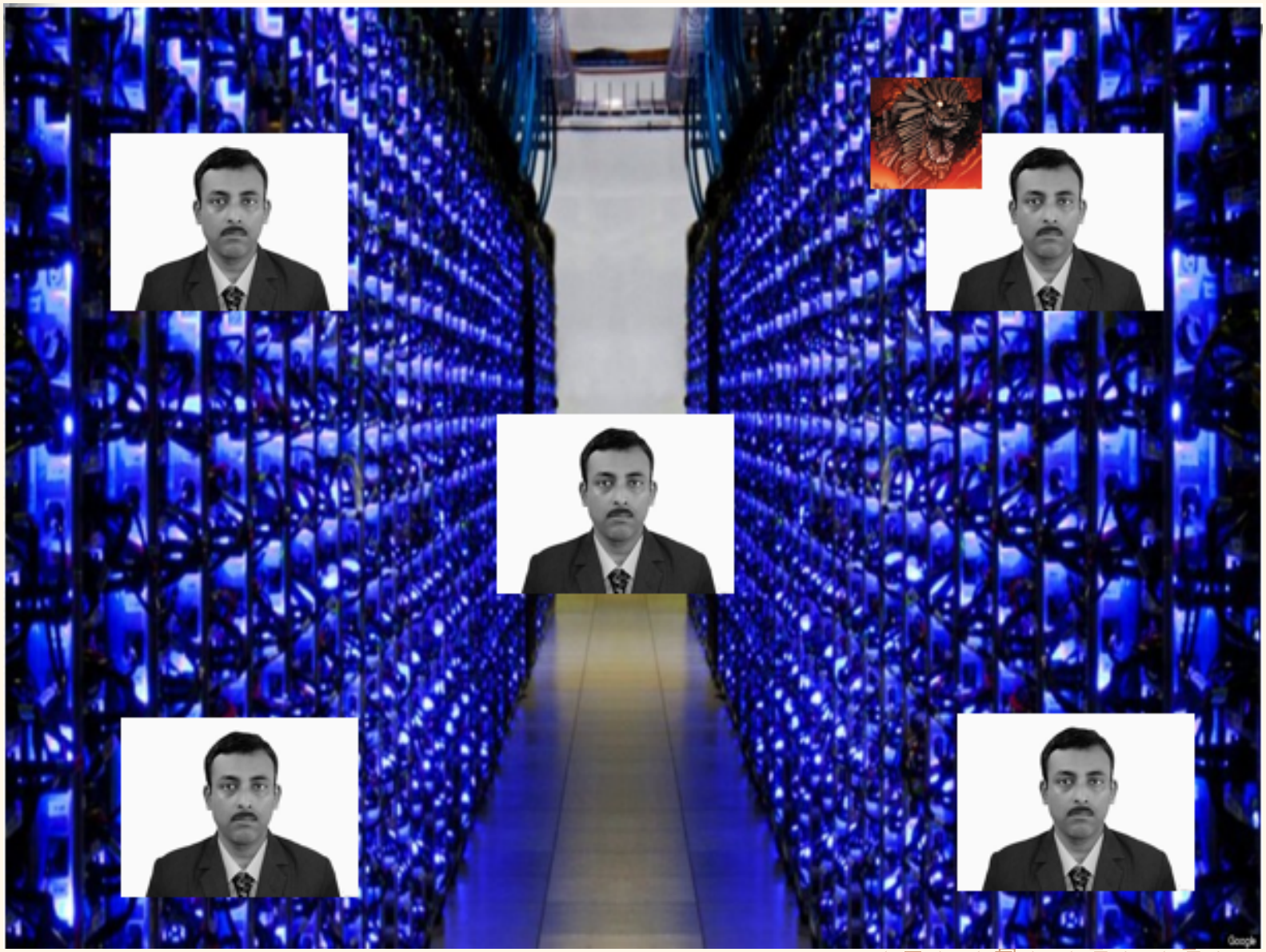
# Attacks on $(k, n)$-SISS

# Attacks on $(k, n)$-SISS

# Attacks on $(k, n)$-SISS



# Attacks on $(k, n)$-SISS



# Attacks on $(k, n)$-SISS

# Attacks on $(k, n)$-SISS

# Attacks on $(k, n)$-SISS

# Attacks on $(k, n)$-SISS

# Attacks on $(k, n)$-SISS

# Attacks on $(k, n)$-SISS

# Attacks on $(k, n)$-SISS

# Evolving Secret Sharing Scheme

## The Inifite PhD Scholars Problem

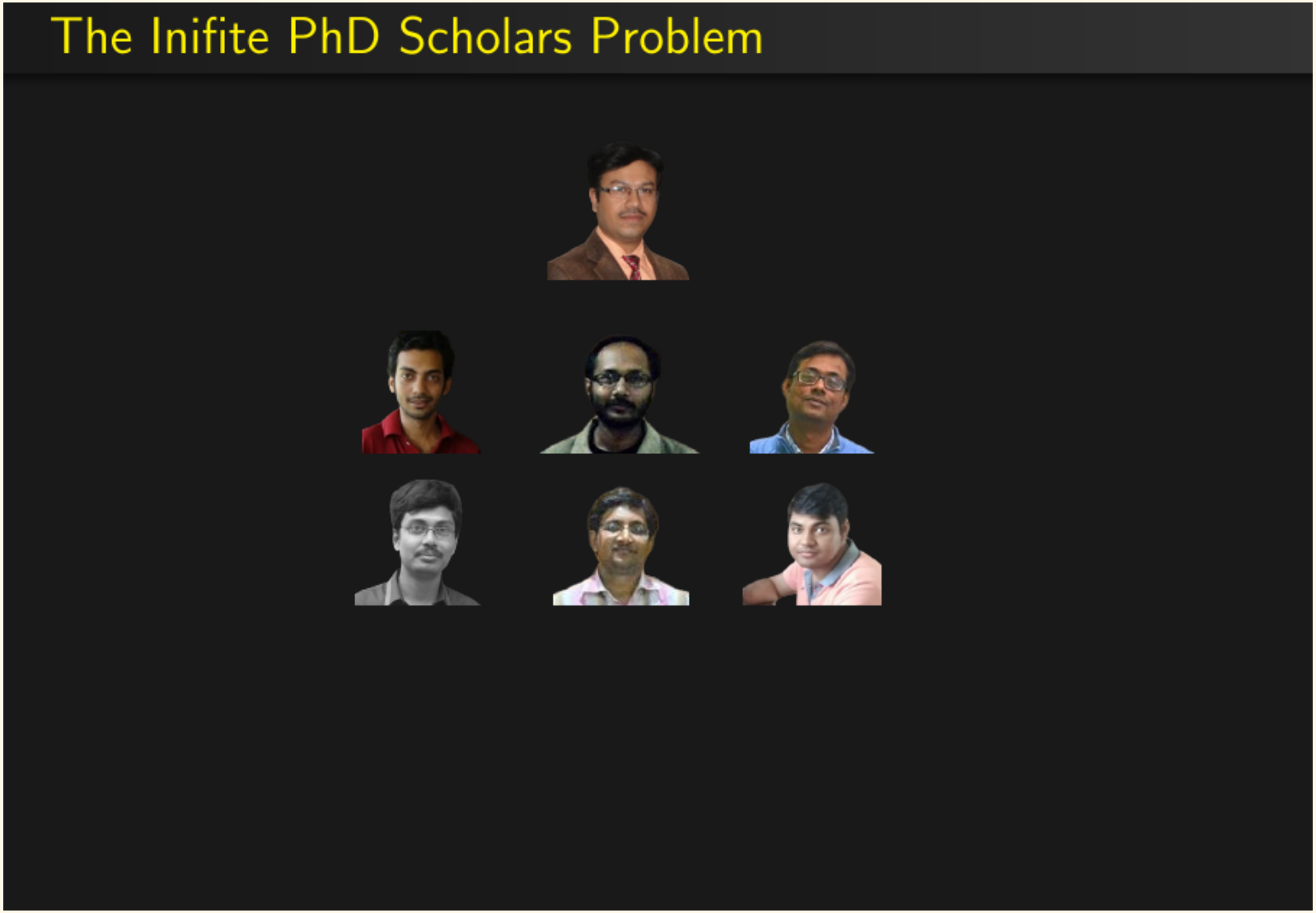
# Evolving Secret Sharing Scheme

## The Inifite PhD Scholars Problem

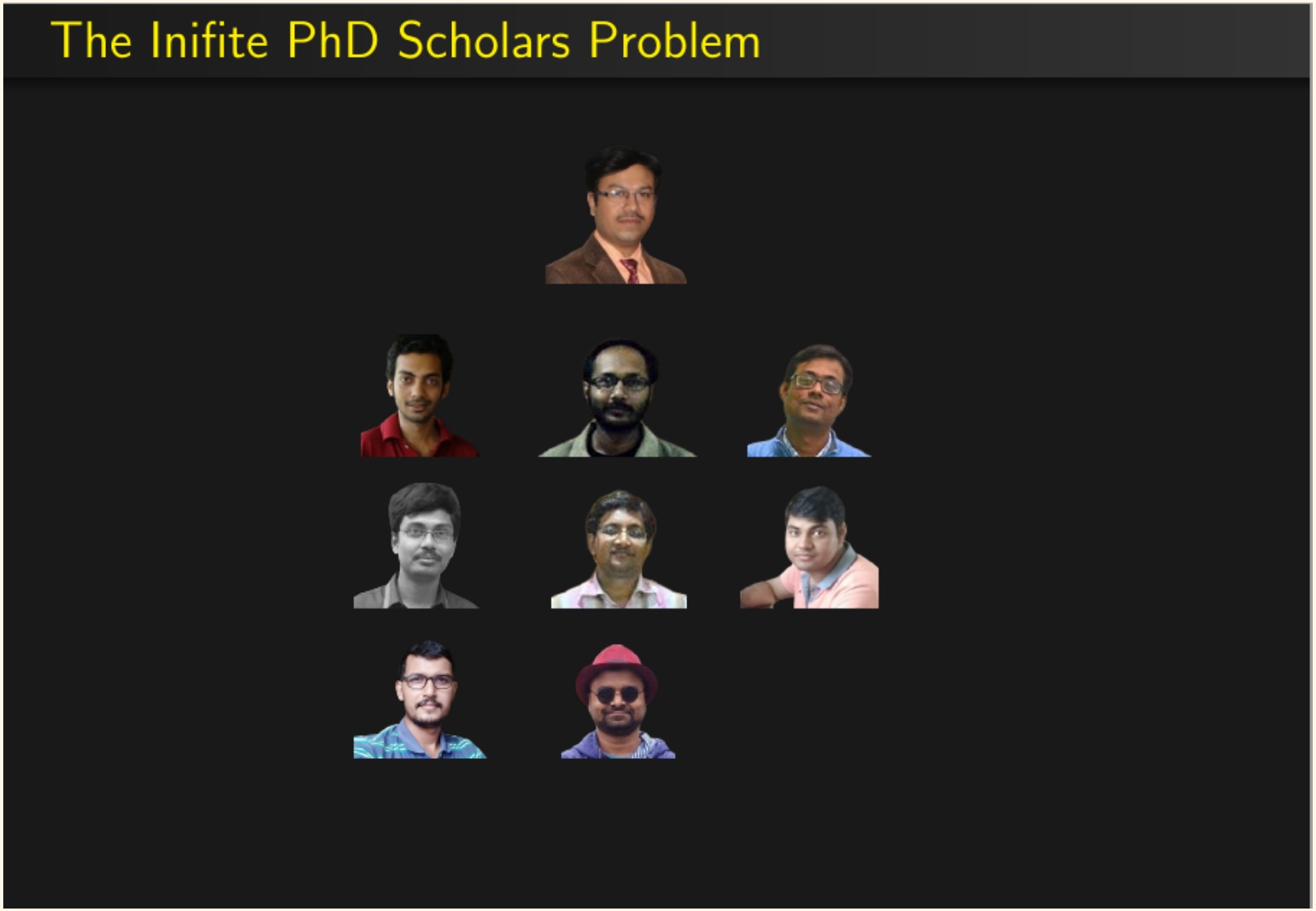
# Evolving Secret Sharing Scheme

## The Inifite PhD Scholars Problem

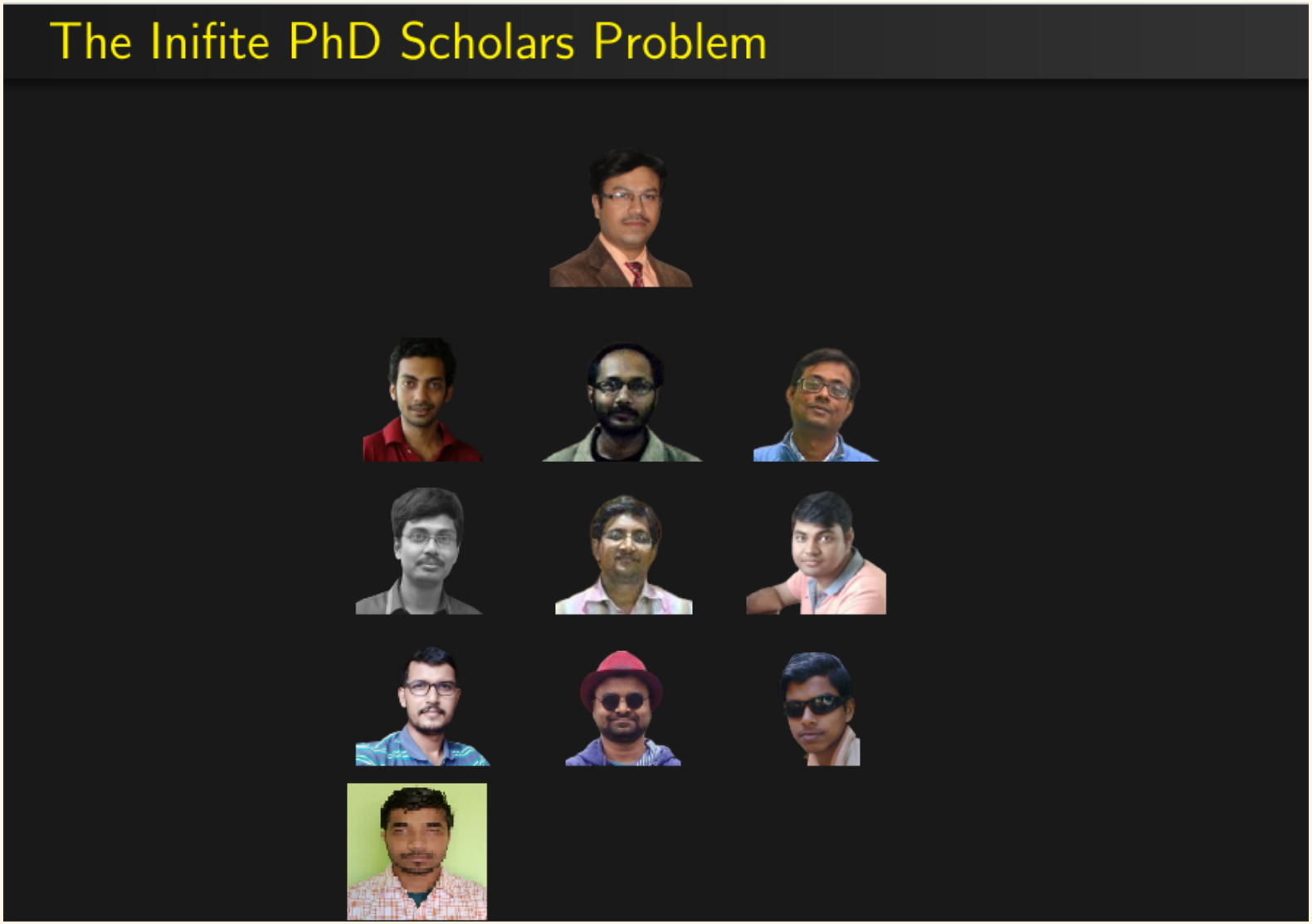
# Evolving Secret Sharing Scheme



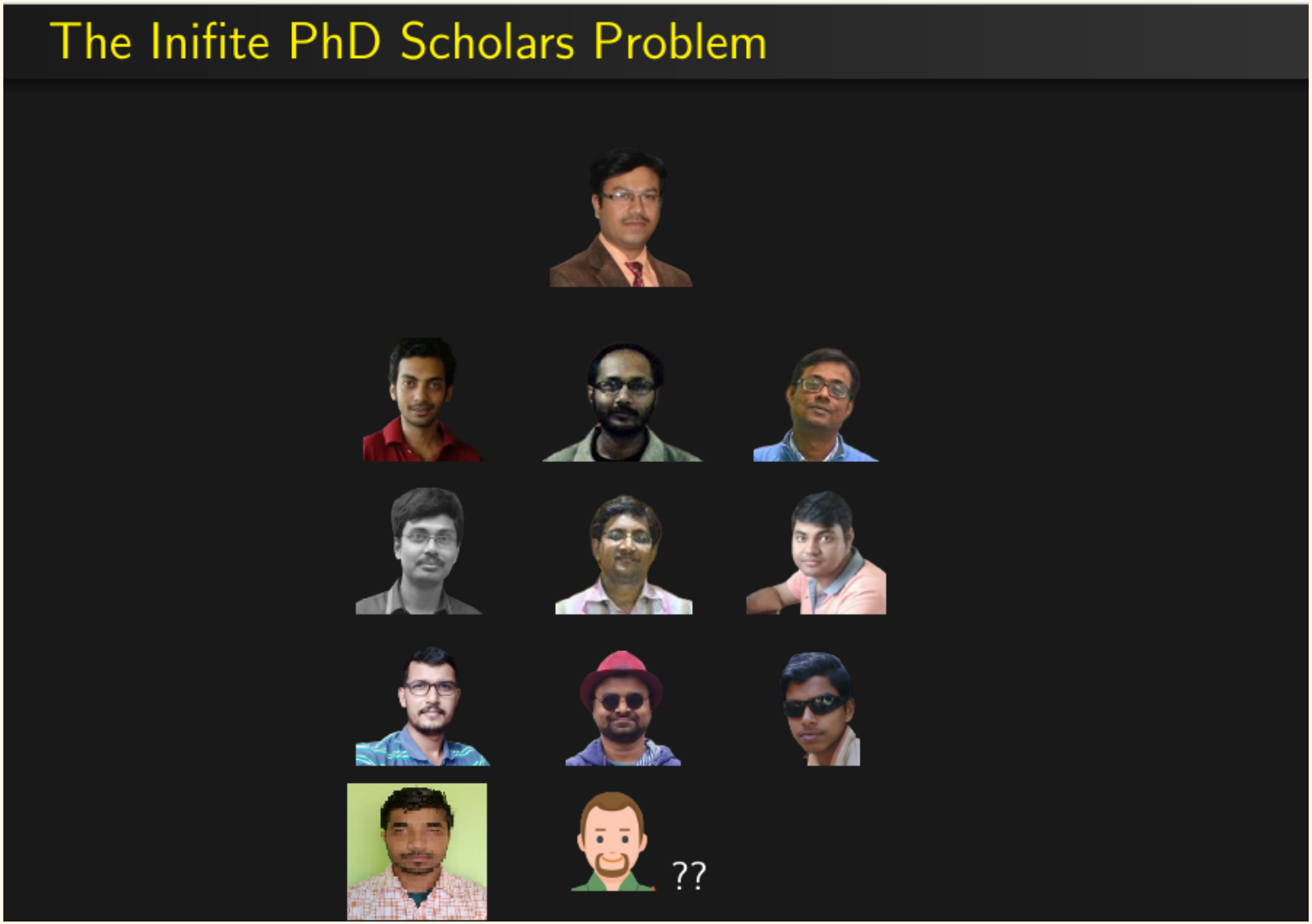
# Evolving Secret Sharing Scheme



# Evolving Secret Sharing Scheme



# Evolving Secret Sharing Scheme



# Bioliography


- Avishek Adhikari, M R Adhikari, **Basic Modern Algebra with Applications**, **Springer Book**, 2014.
- Avishek Adhikari, *Linear Algebraic Techniques to Construct black and white Visual Cryptographic Schemes for General Access Structure and its Applications to Color Images*, **Design, Codes and Cryptography, Springer Journal**, December 2014, Volume 73, Issue 3, pp 865-895.
- Sabyasachi Dutta, Raghvendra Singh Rohit and Avishek Adhikari, *Constructions and Analysis of Some Efficient t-$(k, n)^*$-Visual Cryptographic Schemes Using Linear Algebraic Techniques*, **Design, Codes and Cryptography, Springer Journal**, 2015, DOI 10.1007/s10623-015-0075-5.
- Shamir, A.: How to share a secret. Commun. ACM 22(11), 612?613 (1979)

# Bioliography


Komargodski, I., Naor, M., Yogev, E.: How to share a secret, infinitely. In: Hirt, M., Smith, A. (eds.) TCC 2016. LNCS, vol. 9986, pp. 485?514. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53644-5 19

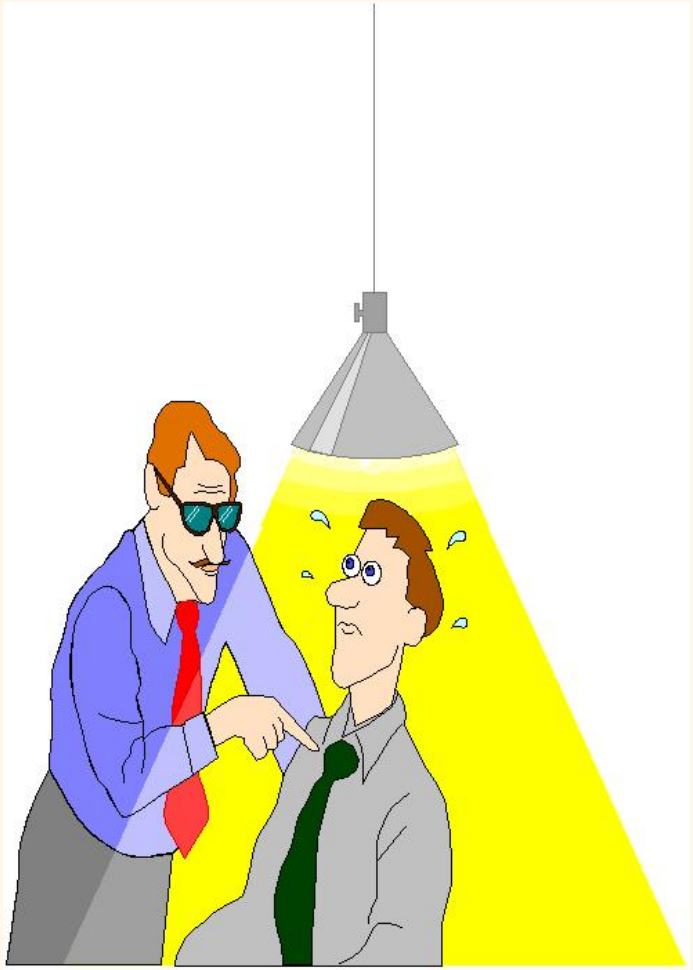
Komargodski, I., Paskin-Cherniavsky, A.: Evolving secret sharing: dynamic thresholds and robustness. In: Kalai, Y., Reyzin, L. (eds.) TCC 2017. LNCS, vol. 10678, pp. 379?393. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-70503- 3 12

# Acknowledgment and Bibliography


- Thankful to **Google** for helping in finding important information and necessary images.

- I am thankful to my PhD Scholars Jyotirmoy Pramanik, Md Kutubuddin Sardar and my student Anisha Dutta for helping me in making the slide.
- Thanks to **Department of Information Technology, Government of India, DRDO and WESEE (Ministry of Defense), DST-SERB, DST-MATRICS, DST-FIST, NBHM, JSPS and JST, Government of Japan** for providing me financial support towards my research.

# Questions or Comments!



**avishek.adh@gmail.com**


Thank
You