

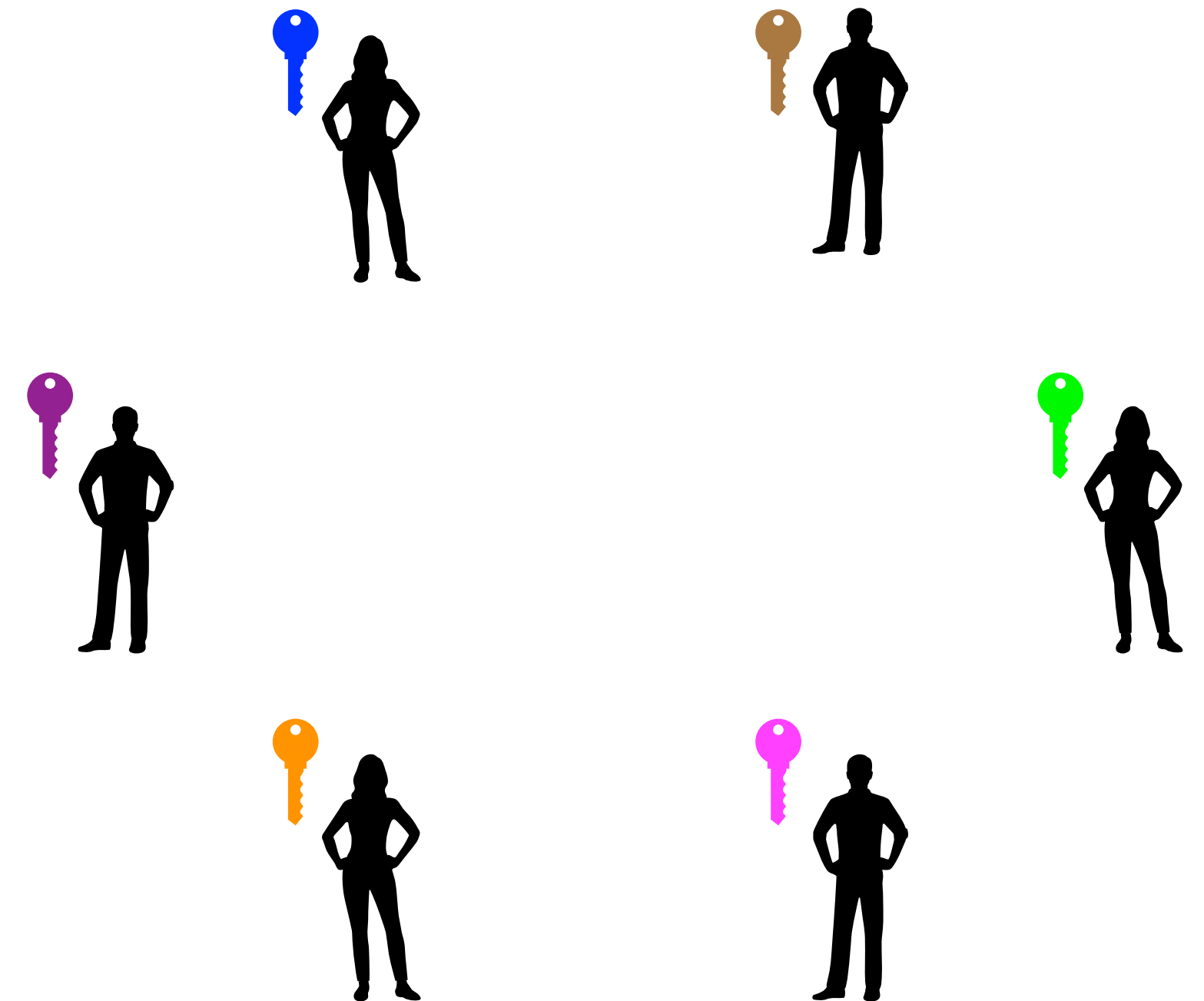
How to share lattice trapdoors

Literally

Based on the ongoing work with Martin Albrecht, Russell Lai and Ivy Woo.

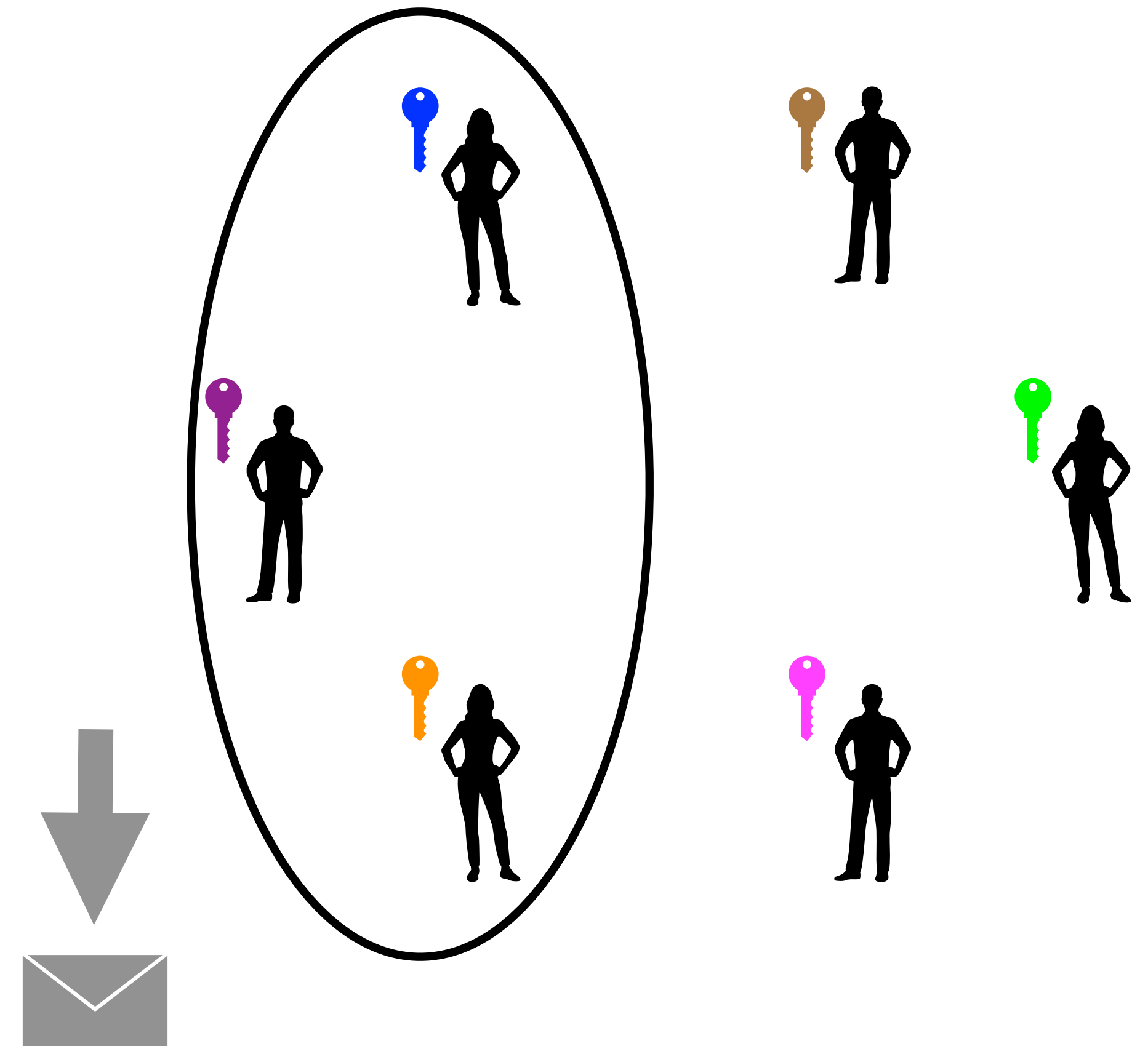
Threshold Cryptography

Goal: Distribute Trust
E.g. Threshold Signatures



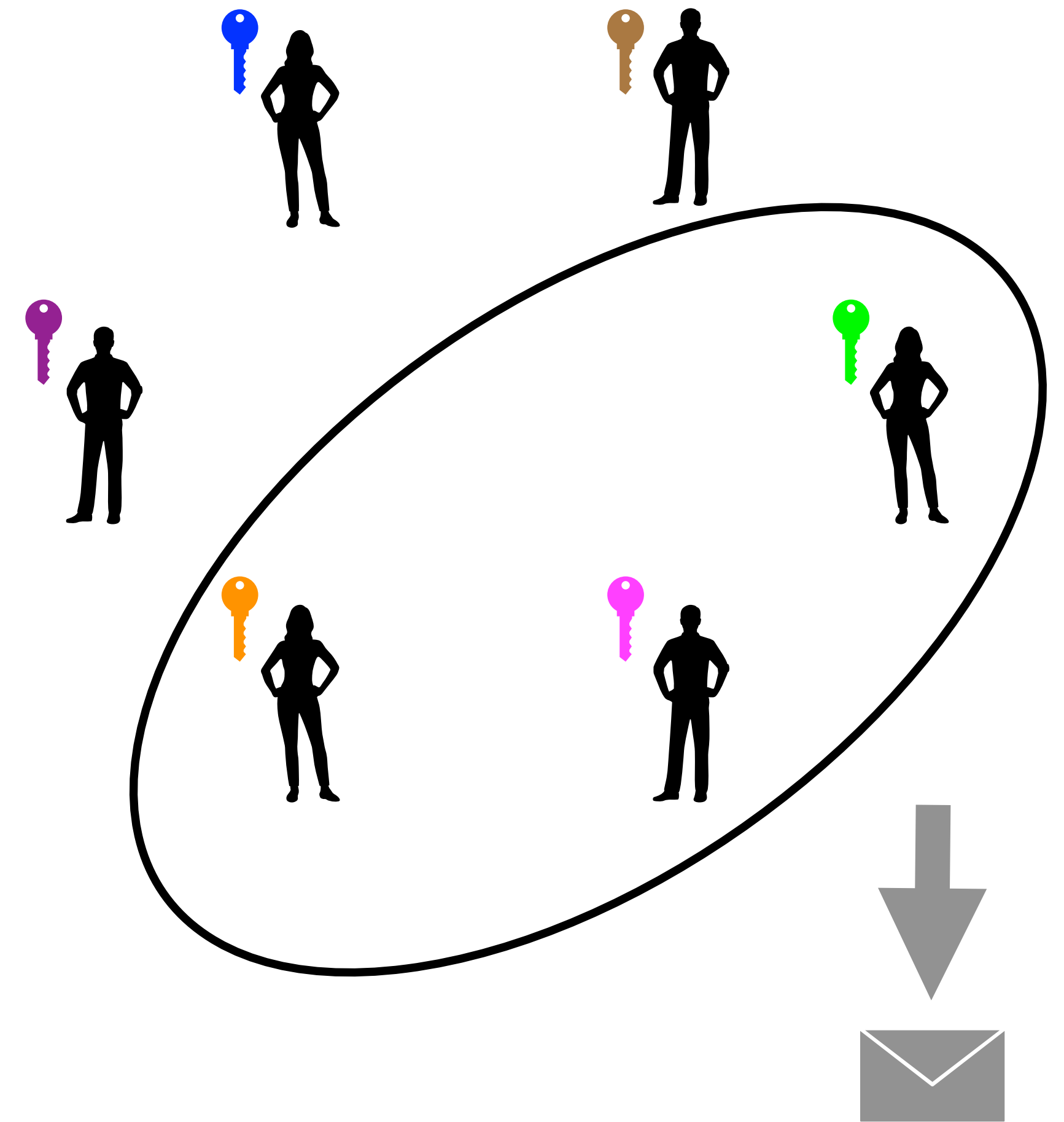
Threshold Cryptography

Goal: Distribute Trust
E.g. Threshold Signatures



Threshold Cryptography

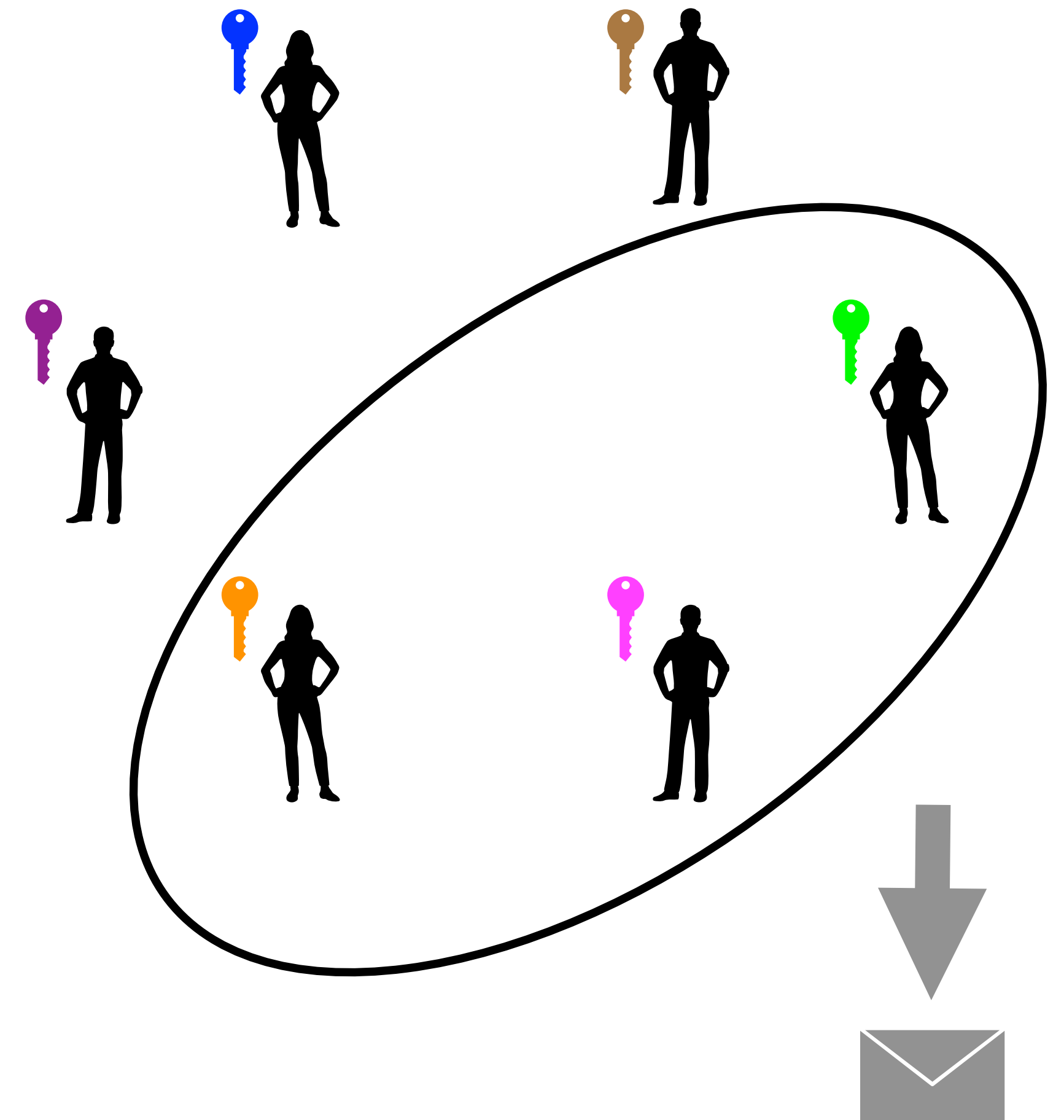
Goal: Distribute Trust
E.g. Threshold Signatures



Total number of k users
Any group t can sign

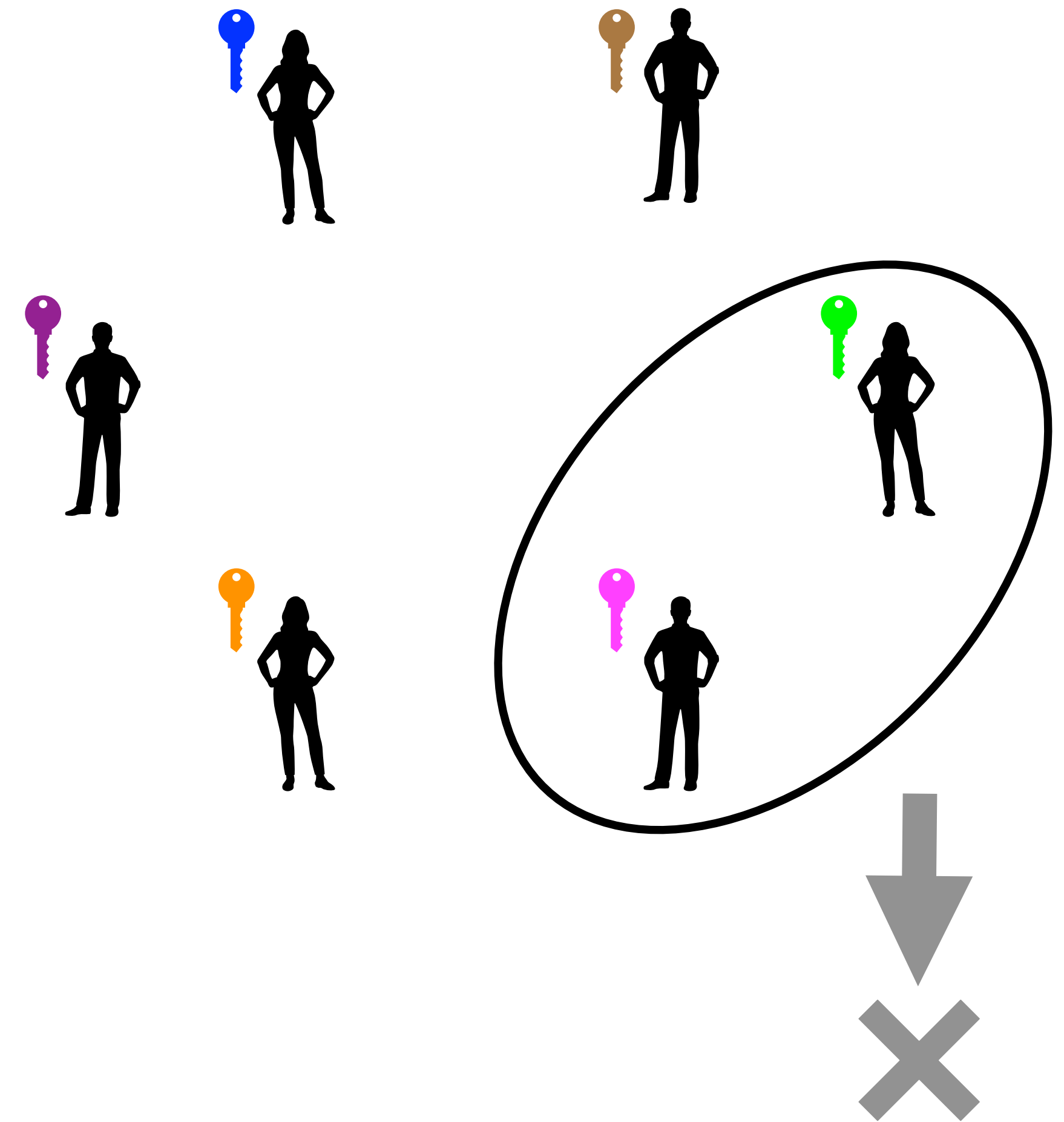
Threshold Cryptography

Goal: Distribute Trust
E.g. Threshold Signatures



Threshold Cryptography

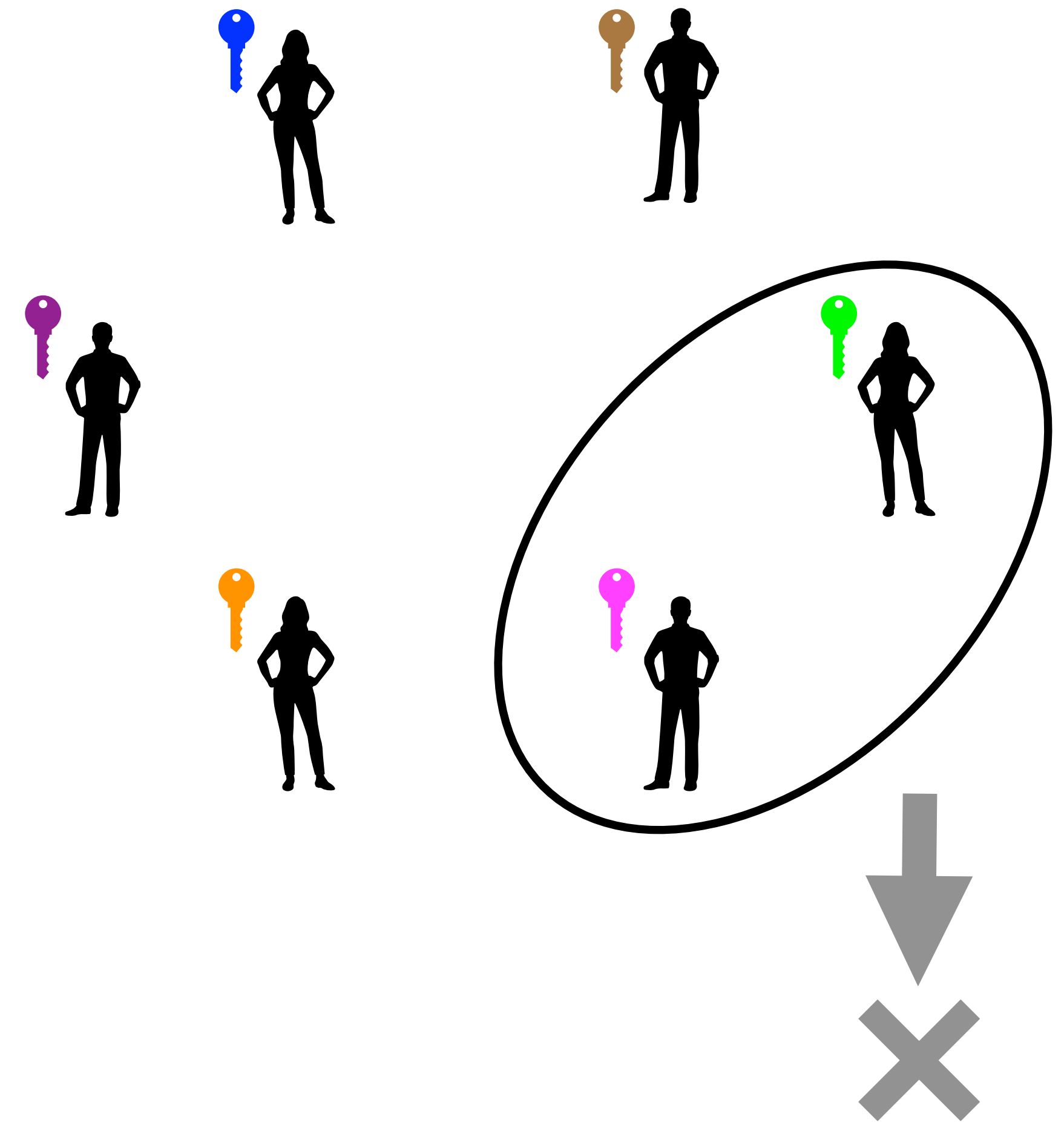
Goal: Distribute Trust
E.g. Threshold Signatures



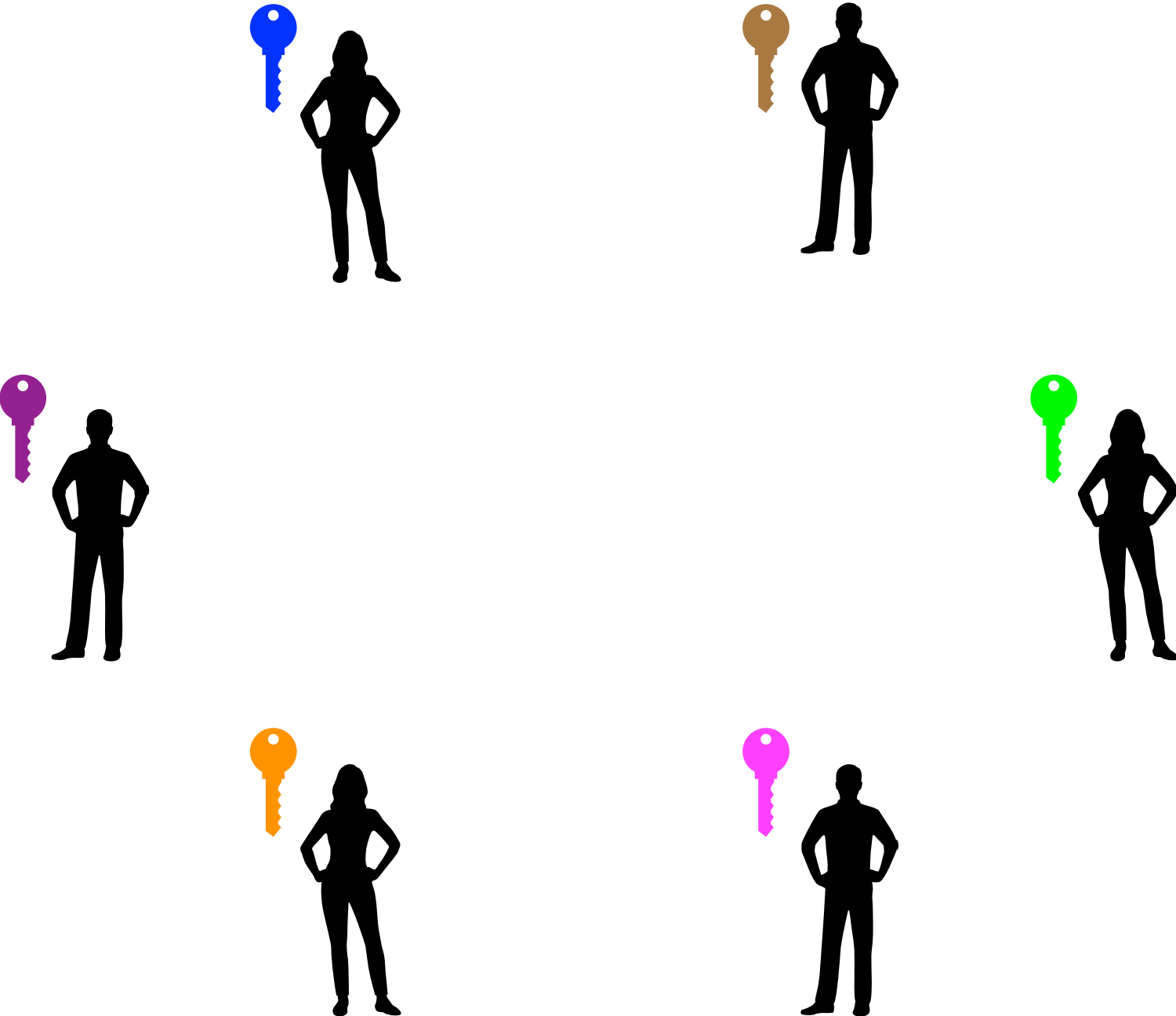
Threshold Cryptography

**Was: Fundamental CS
Question**

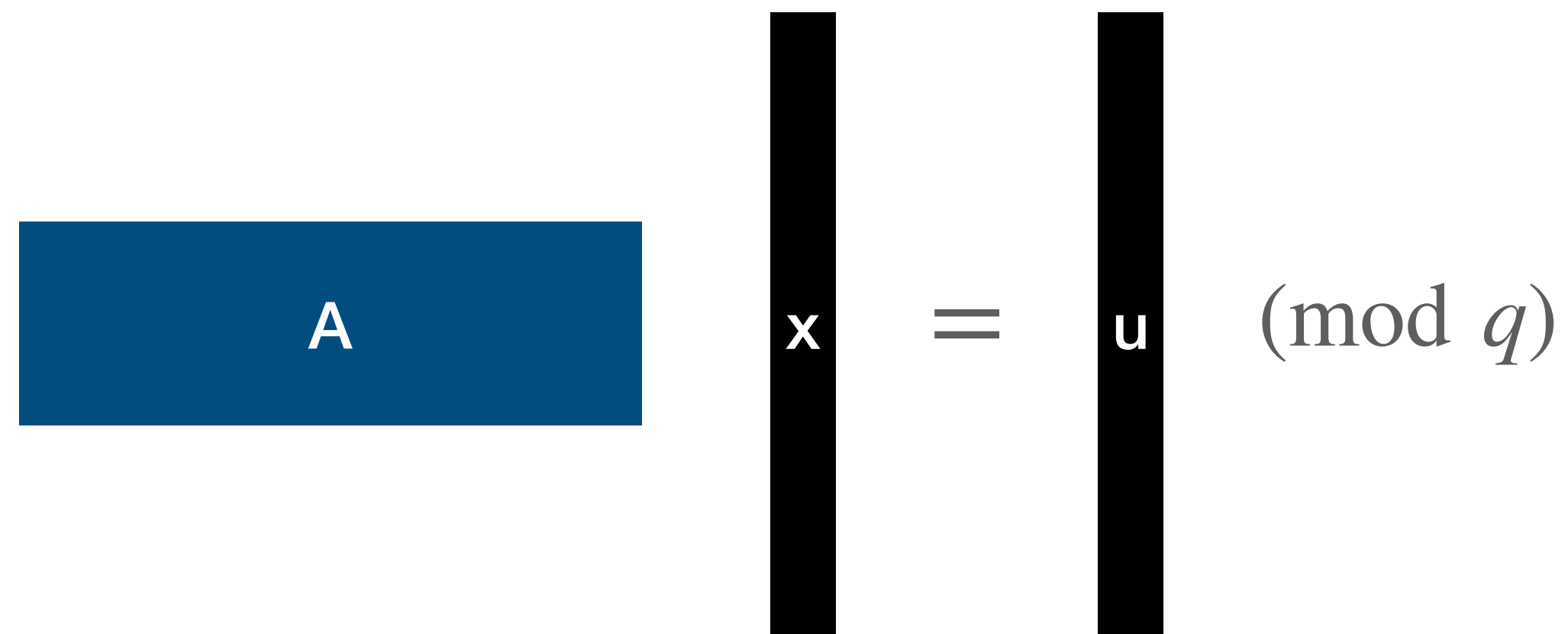
**Now: NIST Call 2023
+ post-quantum***



Lattice Trapdoors



Lattice Trapdoors


$$\boxed{A} \begin{array}{|c|} \hline x \\ \hline \end{array} = \begin{array}{|c|} \hline u \\ \hline \end{array} \pmod{q}$$

x - sufficiently short vector.

Lattice Trapdoors

A

x

=

u

(mod q)

x - short vector.

A

T

=

0

0

\ddots

0

0

(mod q)

T - matrix of short vectors

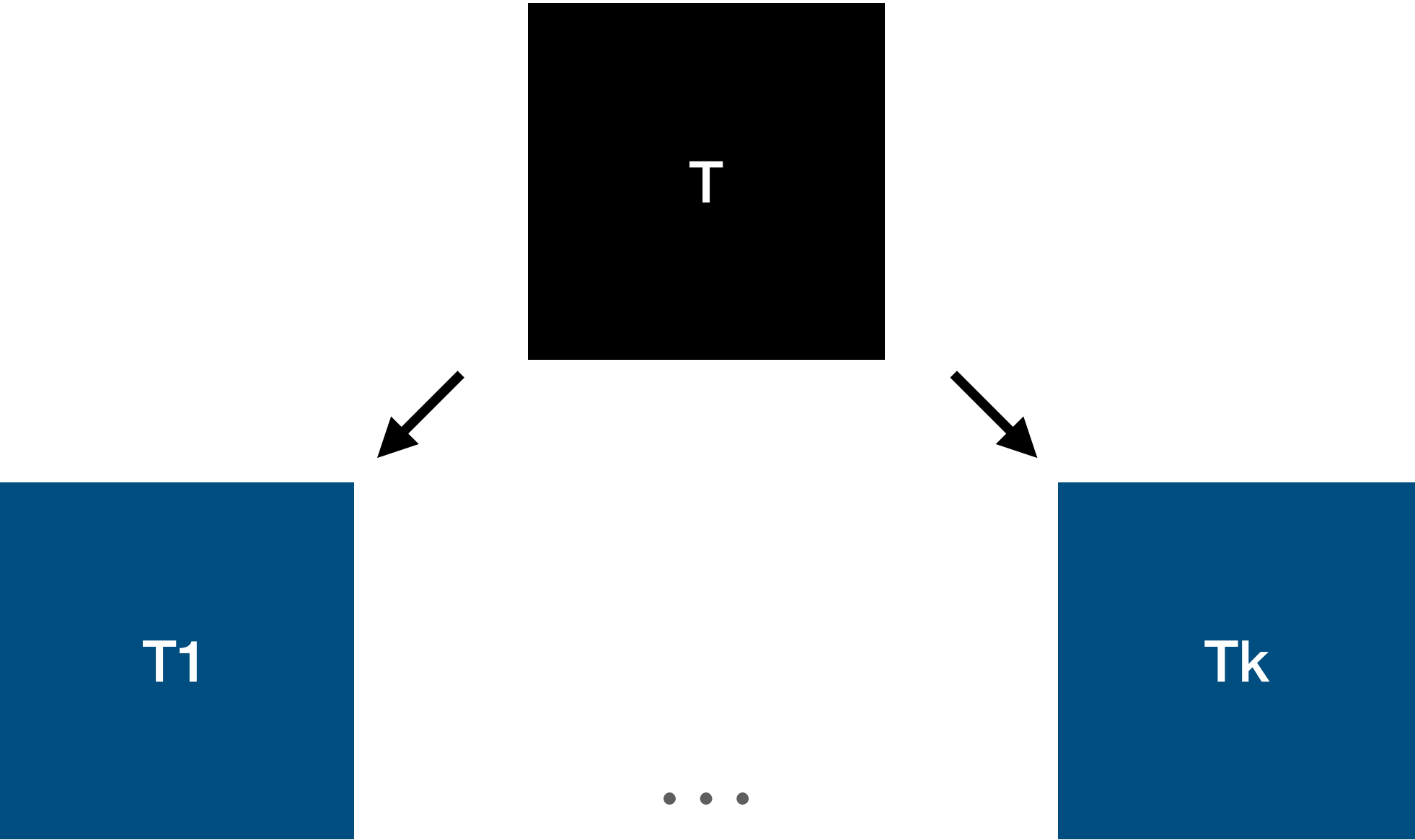
How to share T?

- **Fancy Crypto**
 - Homomorphic encryption
 - Multi-party computation
- **Natively**
 - ???????

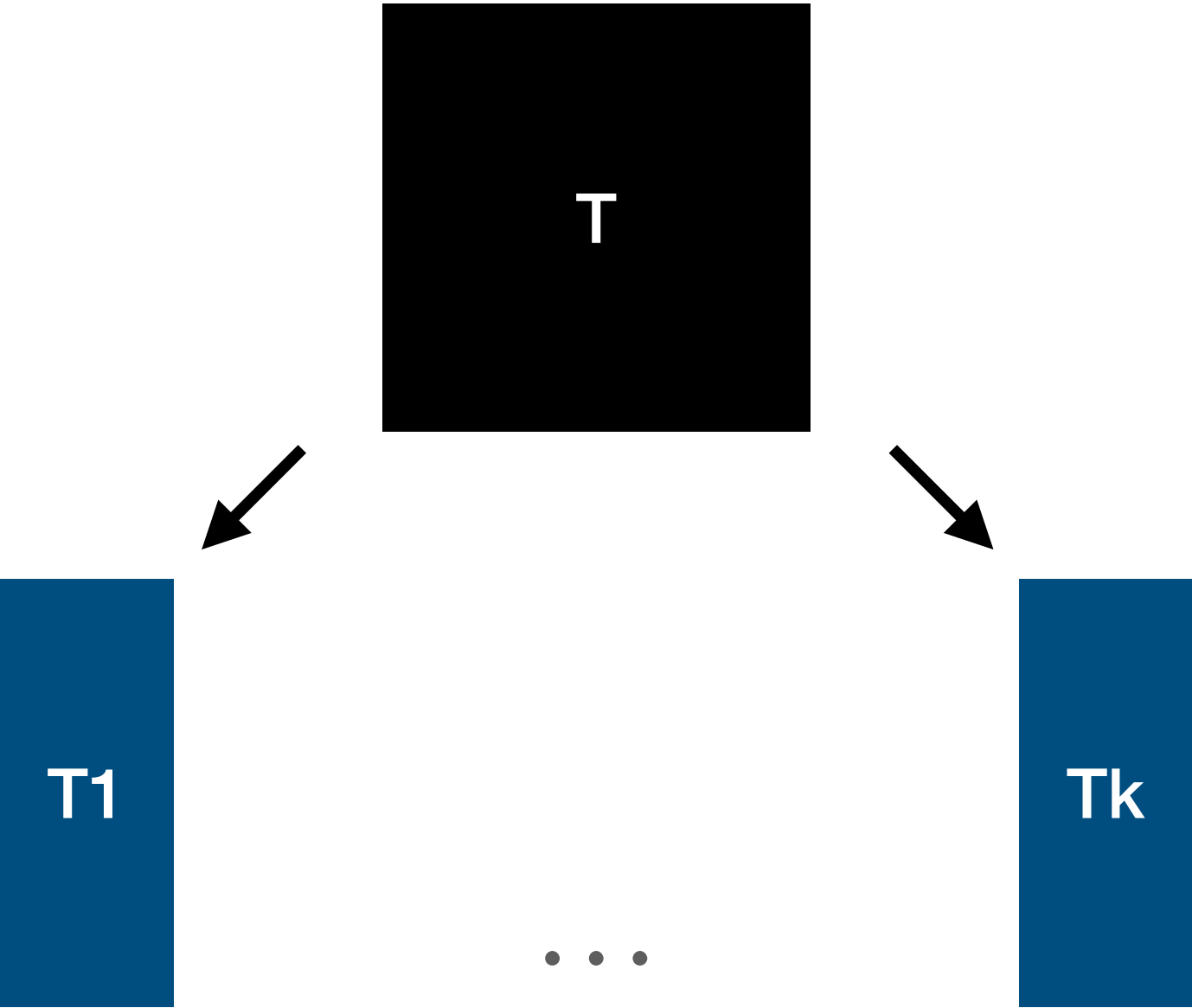
$$\boxed{\begin{array}{c} \text{A} \end{array} \begin{array}{c} \text{T} \end{array} = \begin{array}{cc} 0 & 0 \\ & \ddots \\ 0 & 0 \end{array} \pmod{q}}$$

Bad Ideas

Give T - insecure

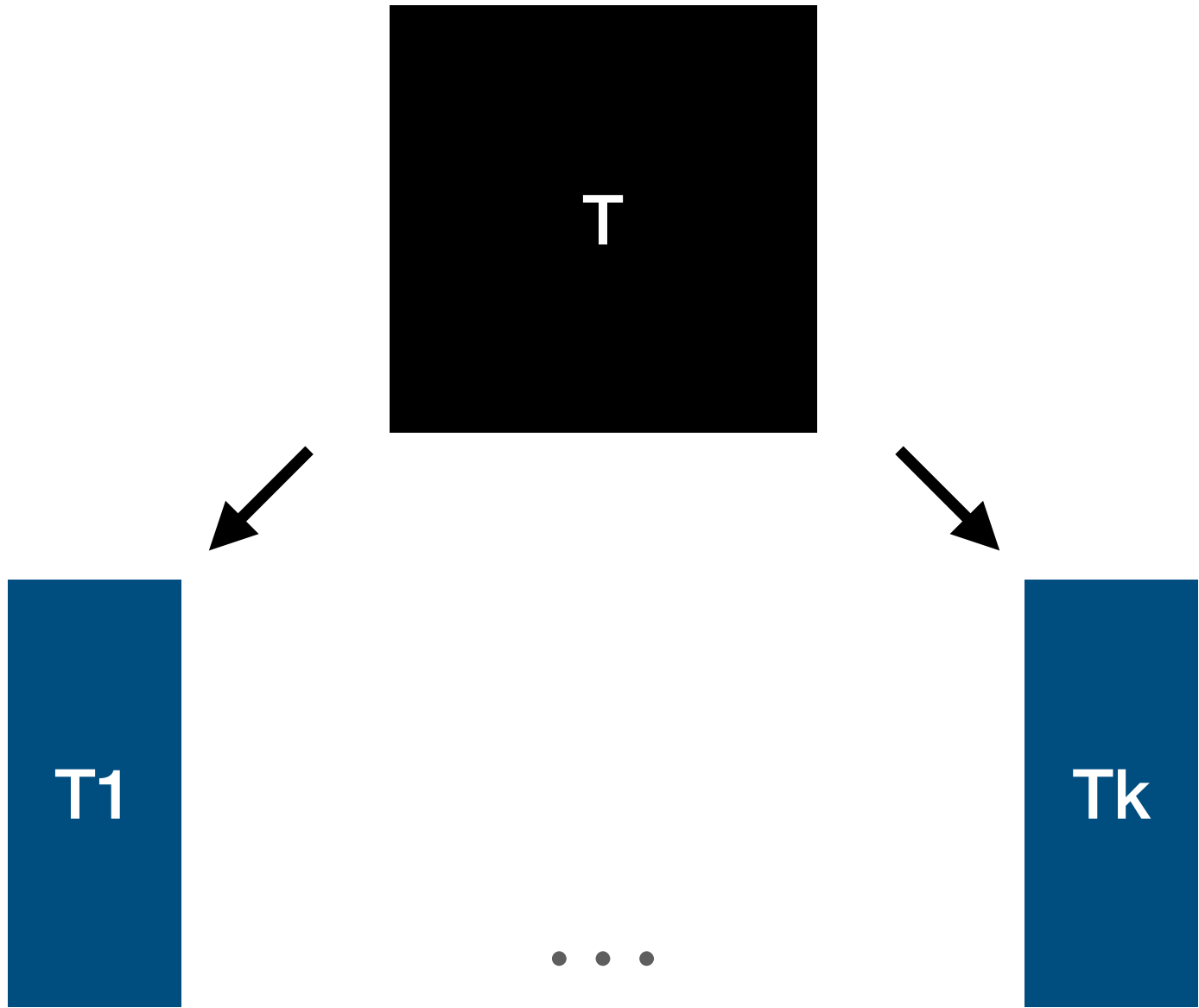


Split T - incorrect



Our Idea

Split T + Split the image space.



Given vectors v_1, \dots, v_k such that any combination of t of them forms an invertible matrix.

An equation showing the relationship between a matrix A , a transformation $T1$, and a matrix of vectors modulo q . On the left is a blue rectangle labeled A . To its right is a blue rectangle labeled $T1$. To the right of $T1$ is an equals sign. To the right of the equals sign is a blue rectangle containing a matrix of vectors: the first row has $|$, $|$, and \dots ; the second row has v_1 , $2v_1$, and \dots ; the third row has $|$, $|$, and \dots . To the right of this matrix is the text $(\text{mod } q)$.

Our Idea

To compute a preimage of u with parties $1, \dots, t$

1. Set $V = (v_1 \mid \dots \mid v_t)$.
2. Compute $z = V^{-1}u$ then we have: $Vz = u$.
3. Party i computes $x_i : Ax_i = v_i z_i$
4. The signature is the sum:

$$A \Sigma x_i = \Sigma v_i z_i = Vz = u$$

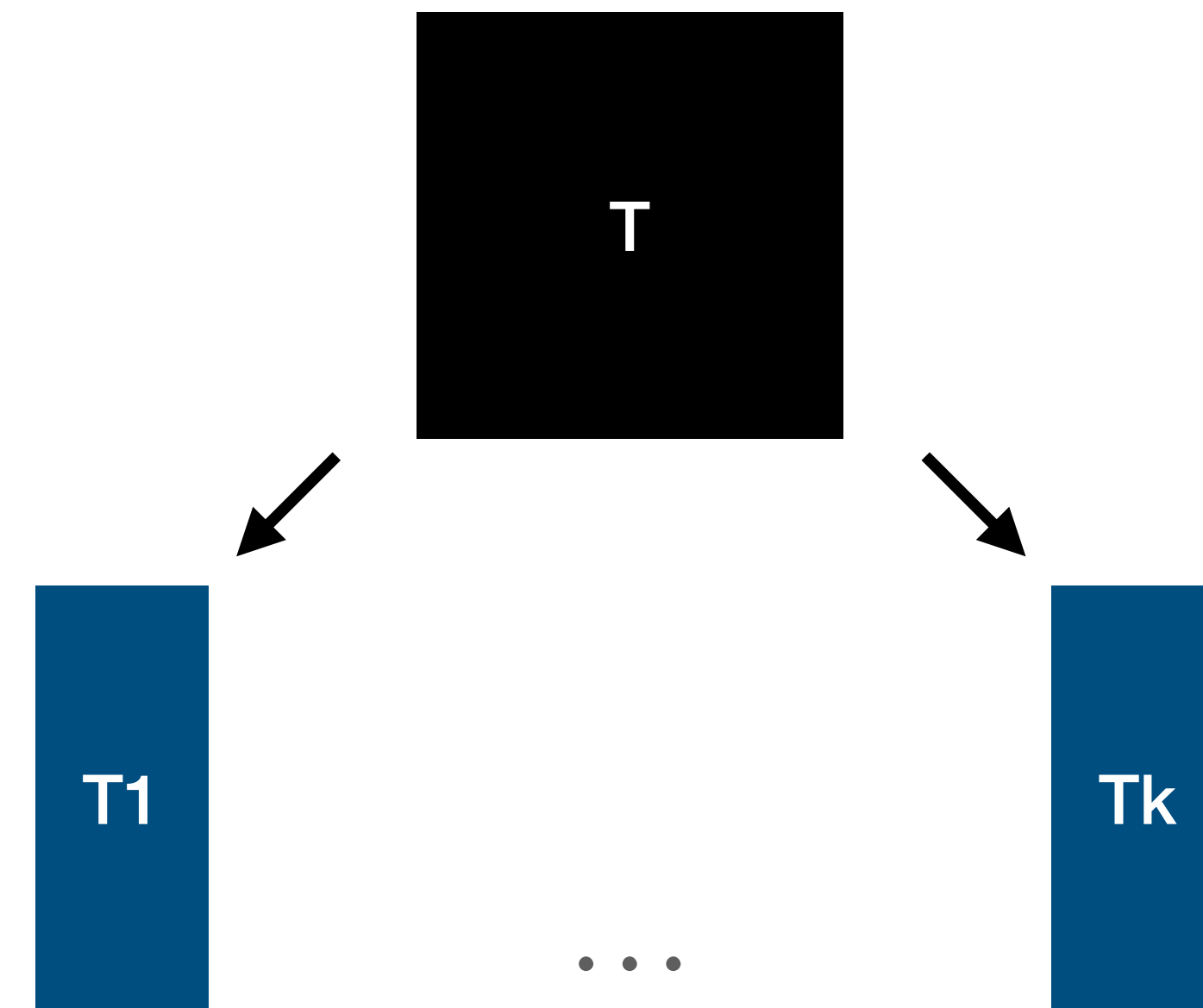
$$A \begin{matrix} T1 \end{matrix} = \begin{bmatrix} | & | & \dots \\ v_1 & 2v_1 & \dots \\ | & | & \dots \end{bmatrix} \pmod{q}$$

Challenges

Theory of Partial Trapdoors

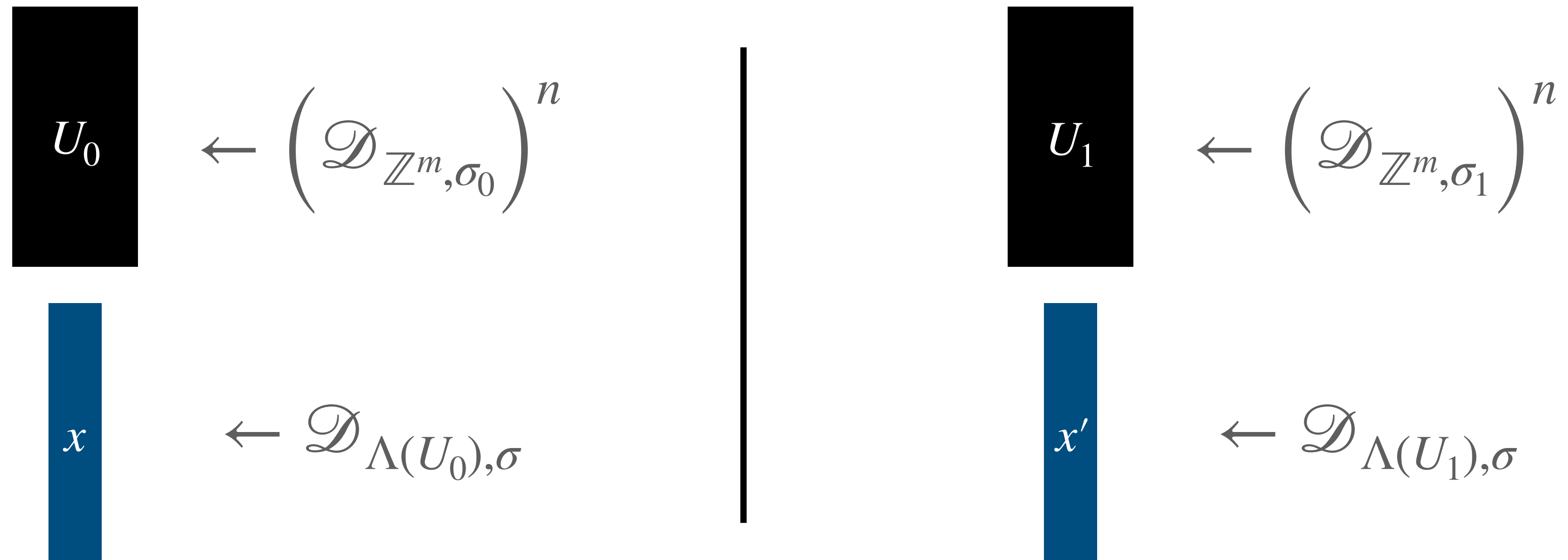
New Distributions

Distributions of Lattices



The Distribution Conjecture

Let $m > n$, and $\sigma/m > \sigma_1 > \sigma_0$.



Then $x \approx x'$.

Open directions

Anonymity

Set of Collaborators

Robust Security

Efficiency



Thank you!

Contact me on: sasha.lapiha.2021@live.rhul.ac.uk