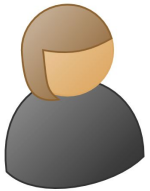
Mind the Gap: Ceremonies for Applied Secret Sharing

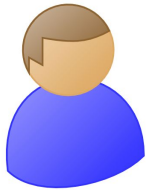
Bailey Kacsmar, Chelsea H. Komlo,
Florian Kerschbaum, and Ian Goldberg

Secret Sharing: (t, n) - Threshold Schemes

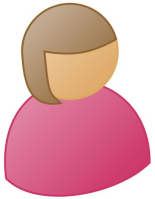
Document



Alice

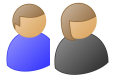


Bob

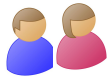


Carol

AC



AB



BC

(2, 3) - Threshold Scheme

Secret **s**

Size **n** group

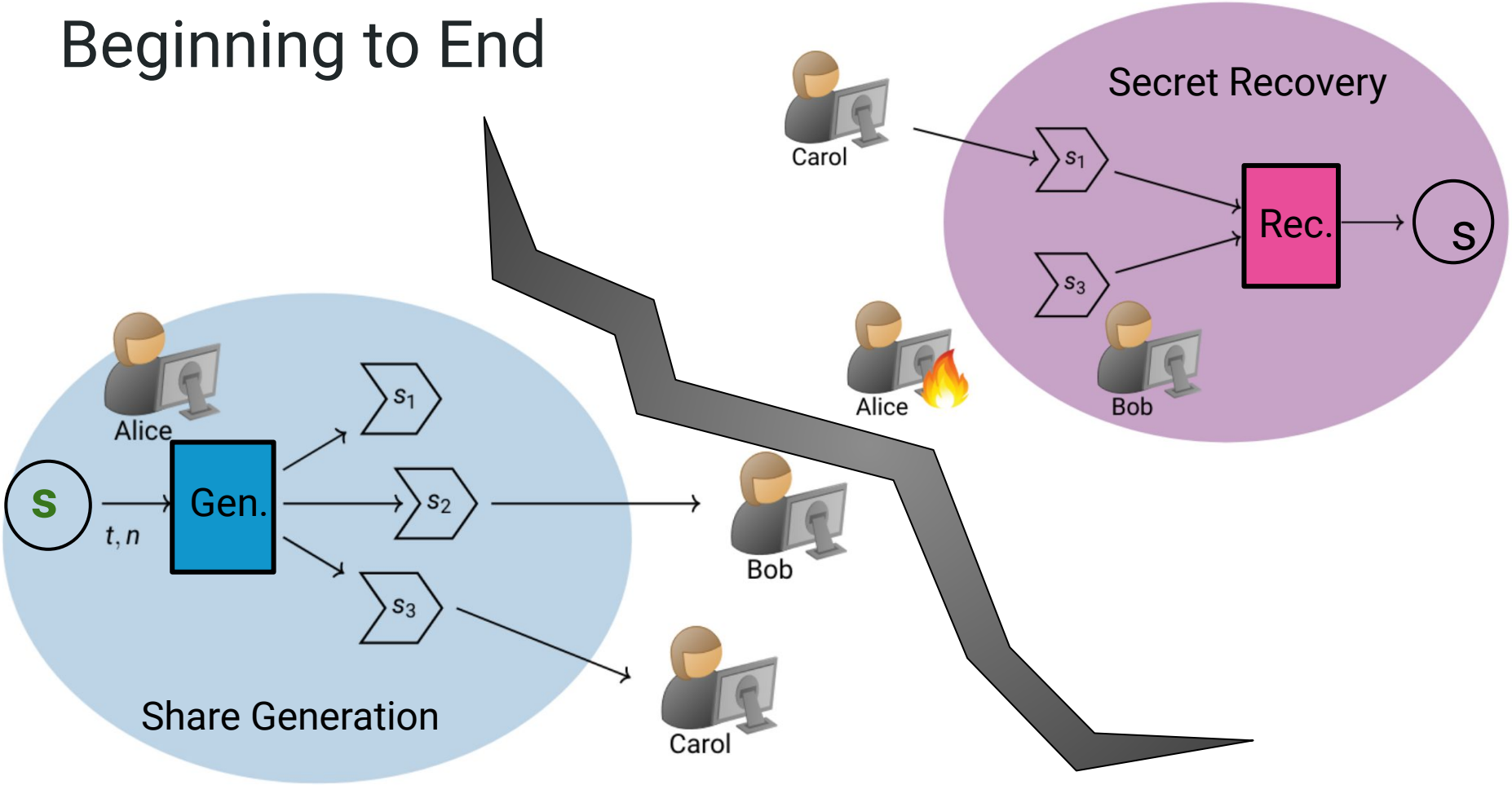
Threshold **t**

Properties of (t, n) - Threshold Scheme

- **Reconstruction:** any size t subset of the n participants can compute the secret given their t shares

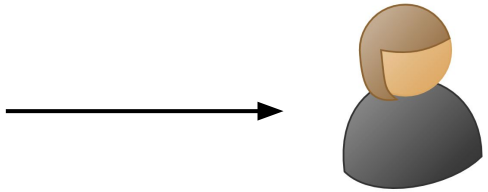
- **Secrecy:** no subset of the n participants consisting of t-1 or fewer participants is able to gain any knowledge of the secret given their combined shares

Beginning to End

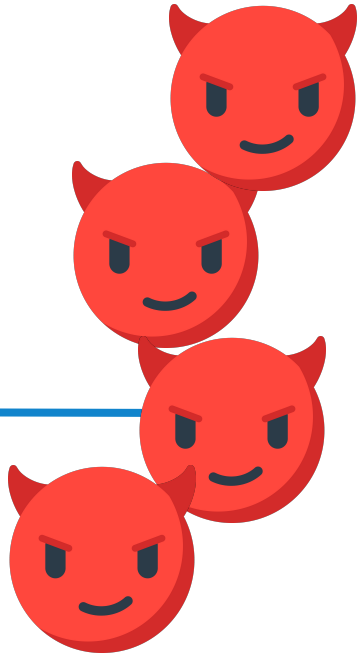


Before the Beginning

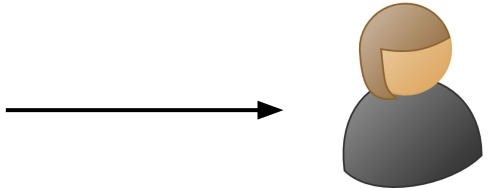
Case 1:



Alice the Journalist

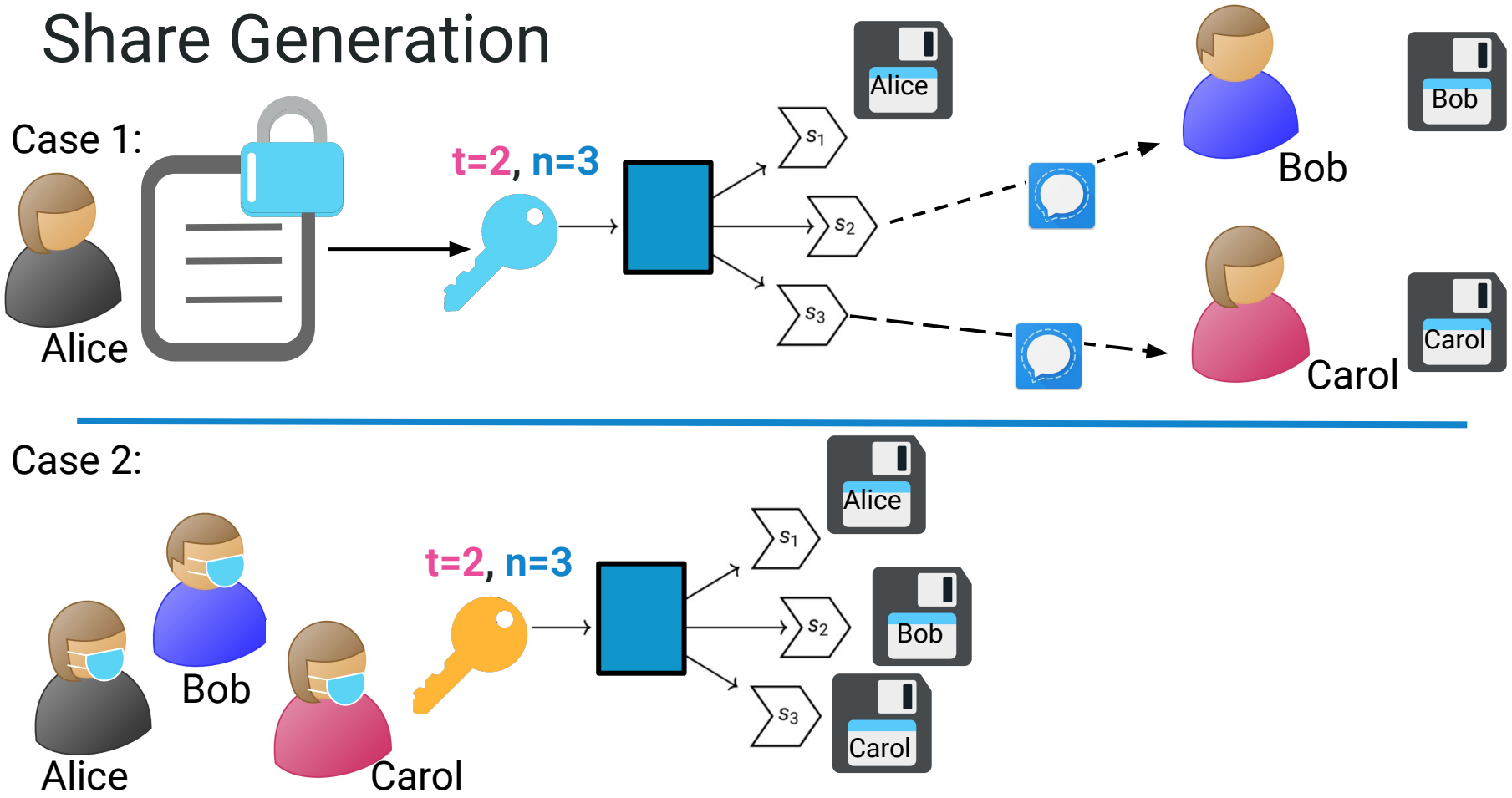


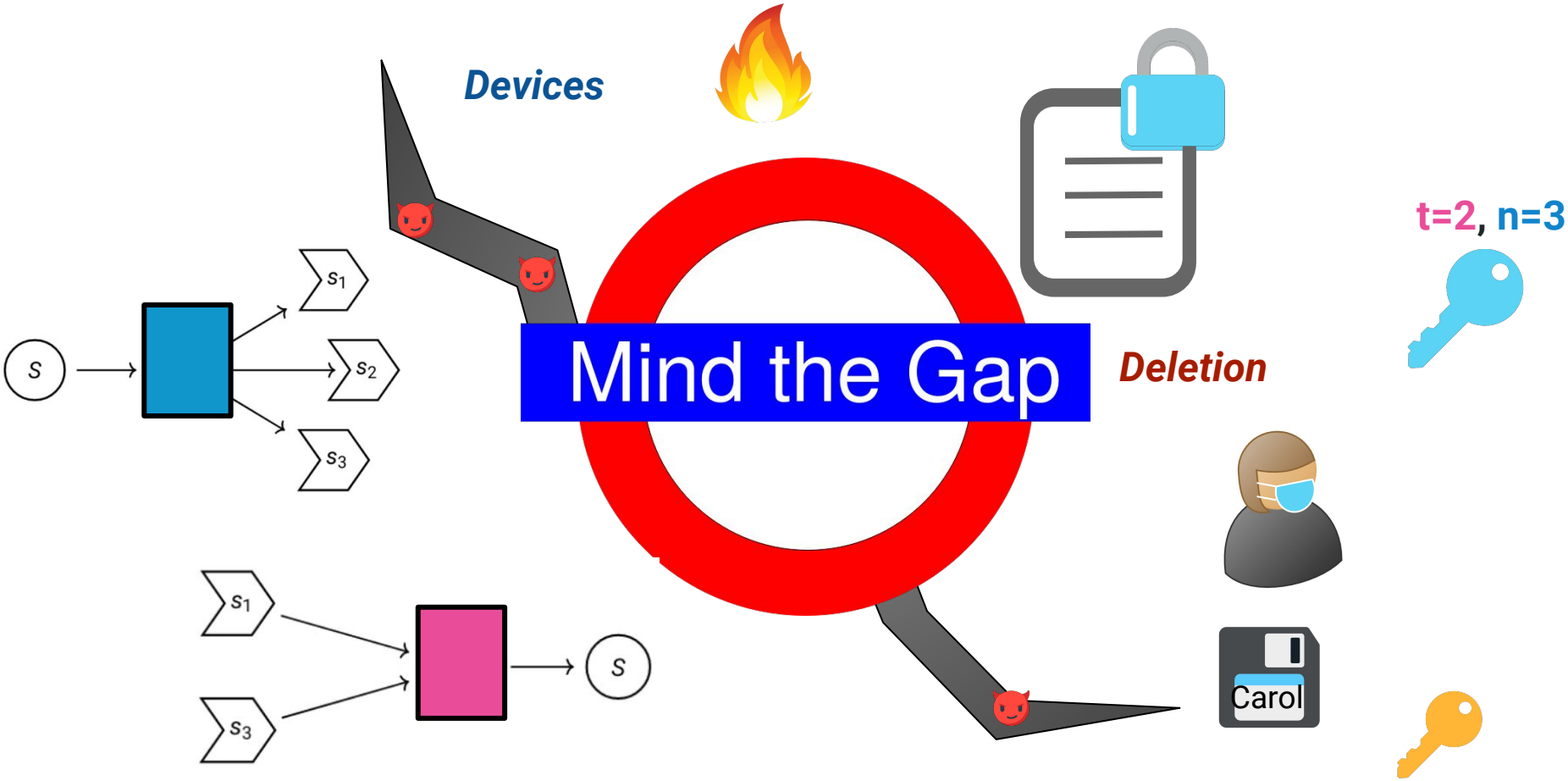
Case 2:



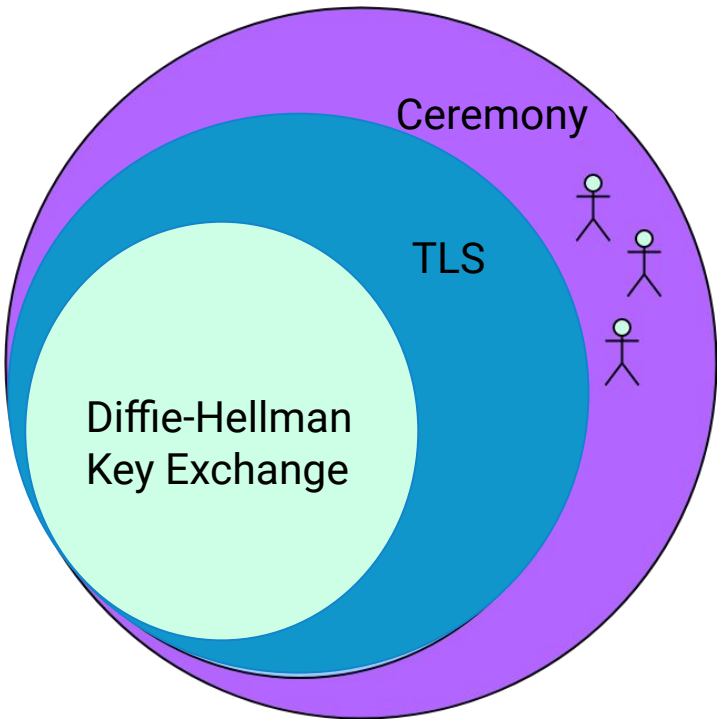
Alice the Journalist

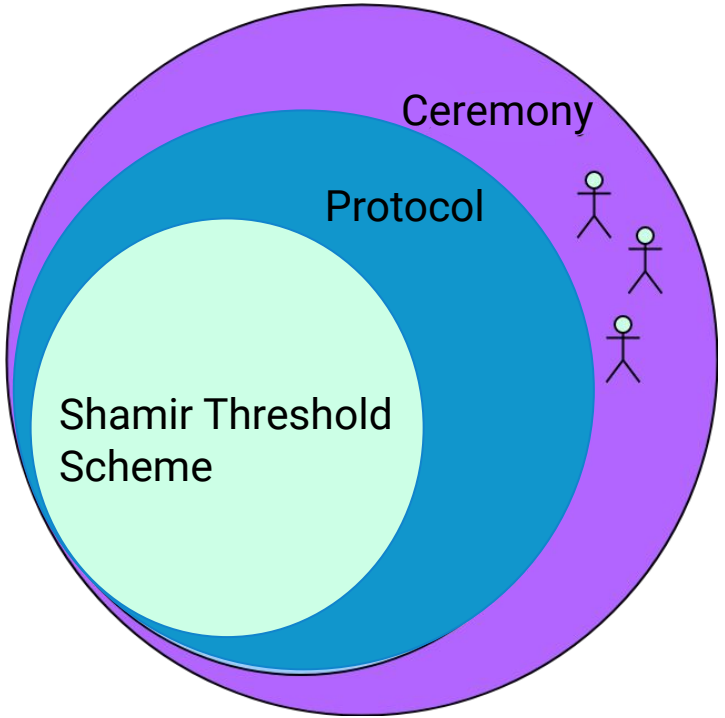
Share Generation




Devices
Mind the Gap
Deletion
t=2, n=3
s
s1
s2
s3
s1
s3
s
Carol

Ceremonies and Secret Sharing





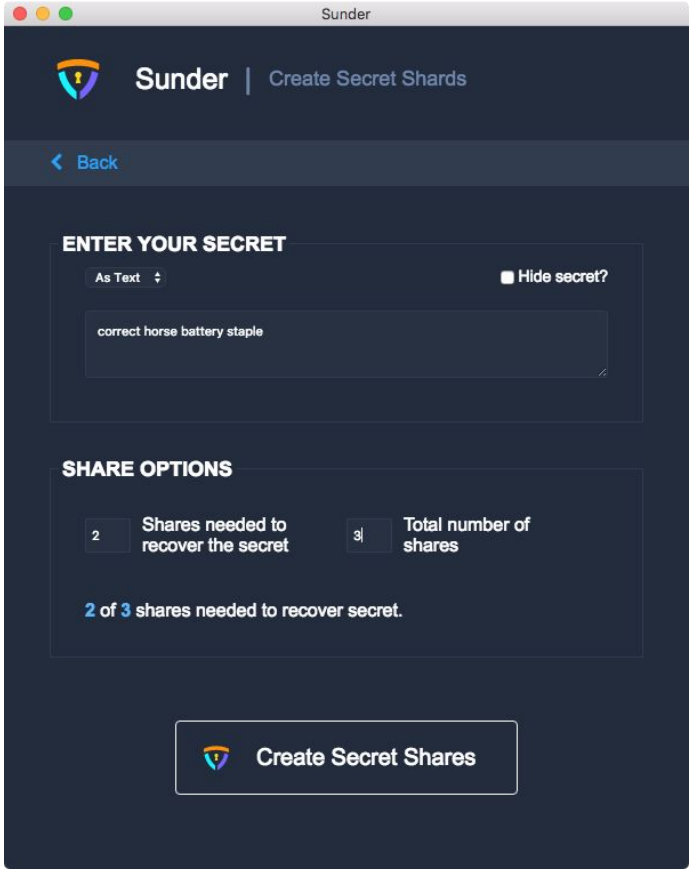
Ellison, 2007

Our Secret Sharing Ceremony Analysis Framework

1. Identify the stages of the ceremony
2. Define the threat model
3. Define the mode of operation
4. Evaluate the security goals against the adversaries

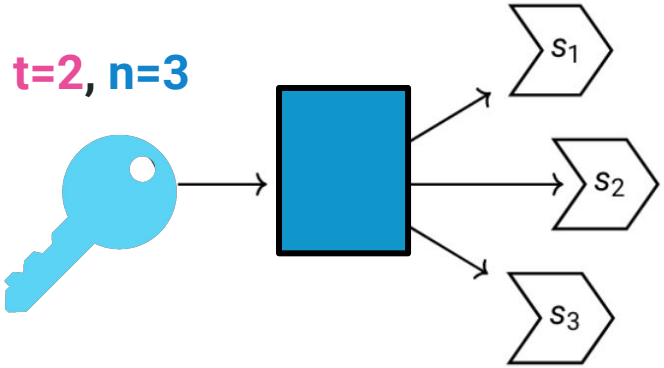
Case Study: Sunder

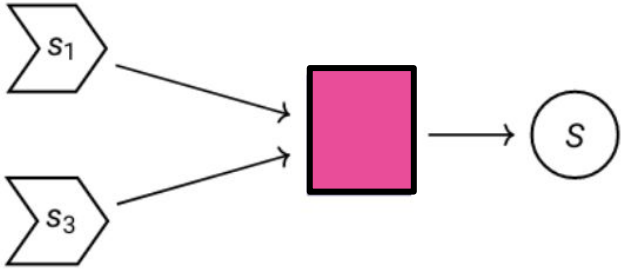
- A tool from Freedom of the Press for journalists
- Implements Shamir secret sharing
- Support for share integrity
- (Some) support for Base and Extended modes



Sunder Stages and Modes

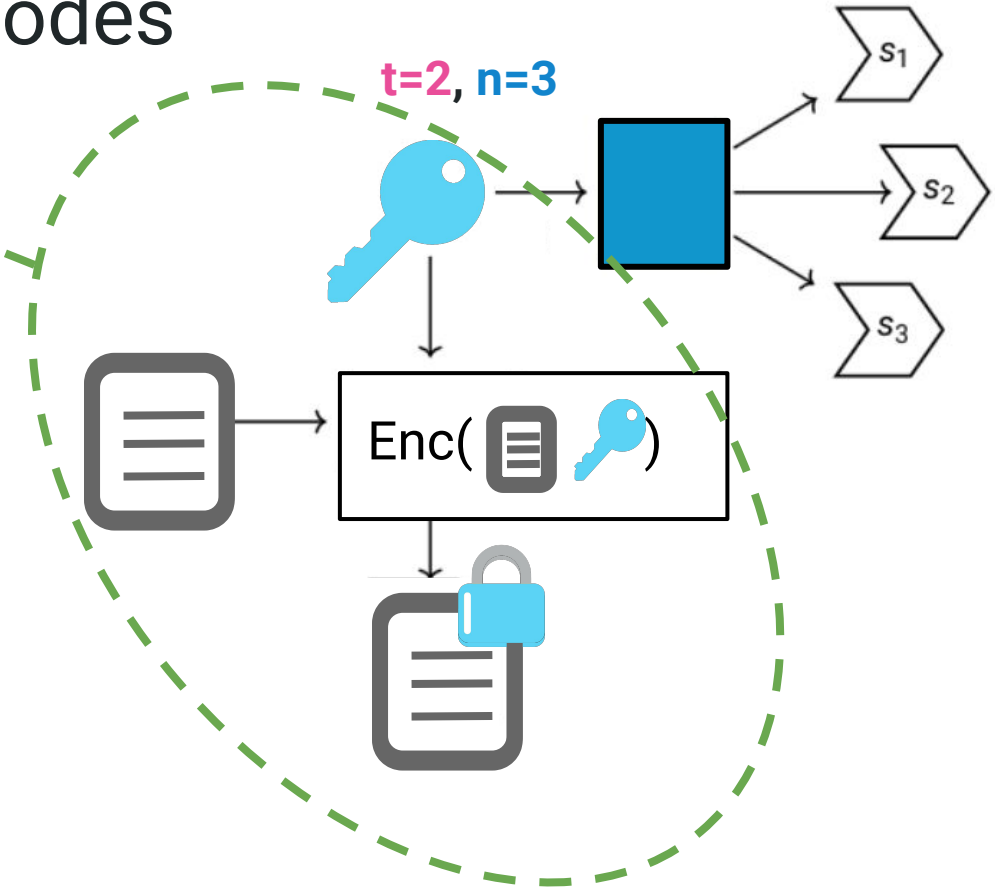
- Secret Preparation
- **Share Generation**
- **Share Distribution**
- **Secret Reconstruction**
- Extended Reconstruction





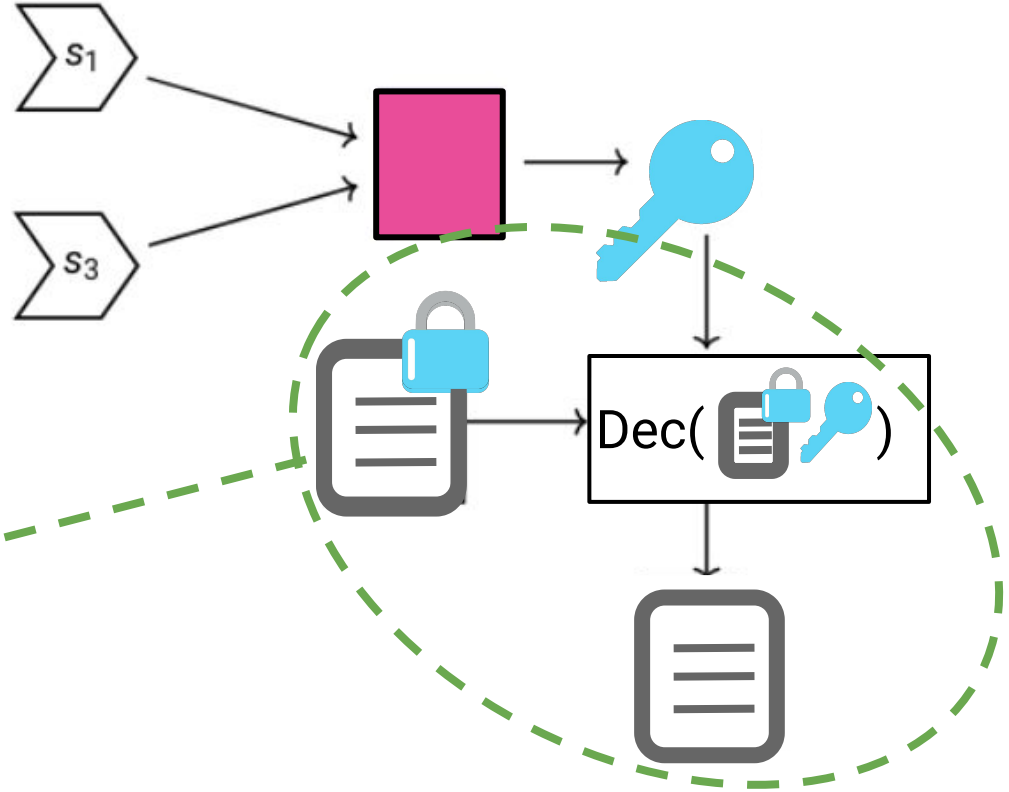
Sunder Stages and Modes

- **Secret Preparation**
- Share Generation
- Share Distribution
- Secret Reconstruction
- Extended Reconstruction



Sunder Stages and Modes

- Secret Preparation
- Share Generation
- Share Distribution
- **Secret Reconstruction**
- **Extended Reconstruction**



Sunder Stage: Share Distribution

1. Choice: Select **n** participants

Sunder Stage: Share Distribution

1. Choice: Select **n** participants
2. Choice: Select a secure communication channel  

Sunder Stage: Share Distribution

1. Choice: Select **n** participants
2. Choice: Select a secure communication channel  
3. Action: The dealer sends each participant their share and corresponding public verification key

Sunder Stage: Share Distribution

1. Choice: Select **n** participants
2. Choice: Select a secure communication channel  
3. Action: The dealer sends each participant their share and corresponding public verification key
4. Action: Delete each share from the dealer's device.

Sunder Stage: Share Distribution

1. Choice: Select **n** participants
2. Choice: Select a secure communication channel  
3. Action: The dealer sends each participant their share and corresponding public verification key
4. Action: Delete each share from the dealer's device.
5. Choice: Each participant selects an appropriate storage mechanism for their share

Sunder Stage: Share Distribution

1. Choice: Select **n** participants
2. Choice: Select a secure communication channel  
3. Action: The dealer sends each participant their share and corresponding public verification key
4. Action: Delete each share from the dealer's device.
5. Choice: Each participant selects an appropriate storage mechanism for their share
6. Action: Each participant stores their share

Sunder: Analysis Threat Model

- A **high-powered adversary** with the power and resources of a government actor
- Adversaries may be **participants or outsiders**
- We do not assume roles are static
- Adversarial **goals** may include: learning secret information, modifying secret information, preventing secret recovery, and causing harm to participants

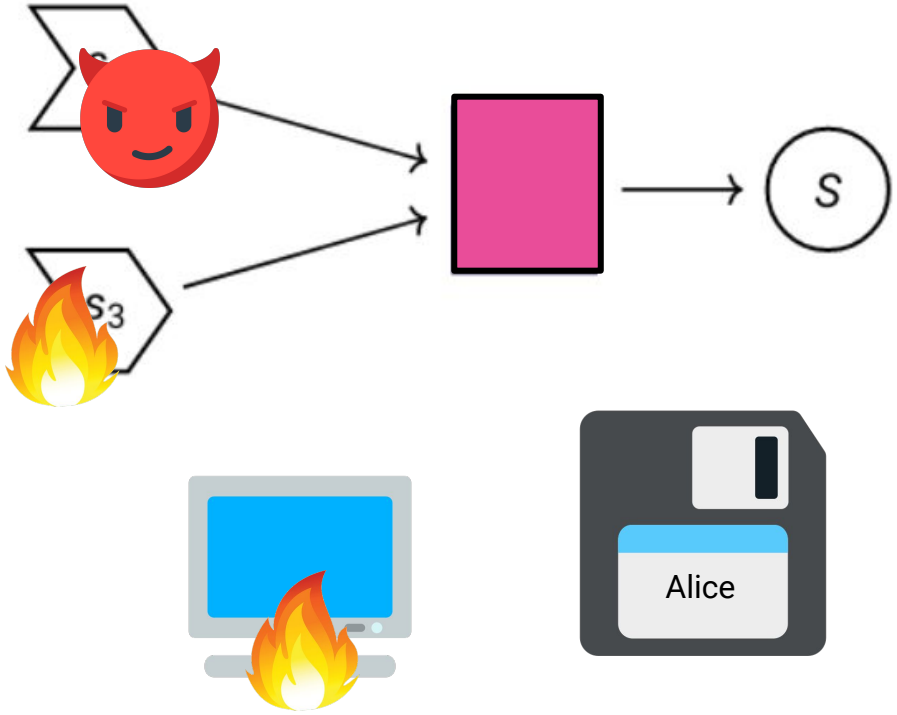
Sunder Ceremony Evaluation

●=achieved; ◐=ceremony dependent; ○=not achieved

	Classic Shamir				Sunder Ceremony			
	Base		*Ext*		*Base*		*Ext*	
	HBC	MAL	HBC	MAL	HBC	MAL	HBC	MAL
t-Sep. Priv.	●	●	●	●	●	●	●	●
Availability	●	●	○	○	●	●	◐	◐
IT Sec.	◐	◐	○	○	○	○	○	○
Conf.	◐	◐	◐	◐	◐	◐	◐	◐
Integrity	○	○	○	○	●	●	◐	◐

Threats to Secret Reconstruction

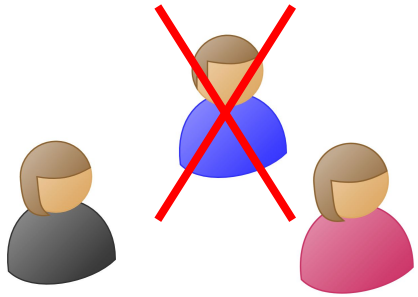
1. Alice leaving the organization
2. A share being damaged
3. A share being stolen
4. The device storing the encrypted files is destroyed



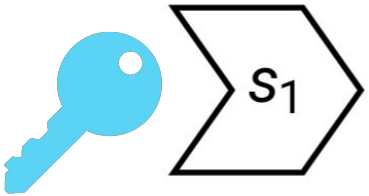
Our Lightweight Proactive VSS

Adds three new stages:

- ➔ Share Update
- ➔ Share Validate
- ➔ Generate Commitment



Access Revocation via Updates



Verification of Share Integrity and File Integrity

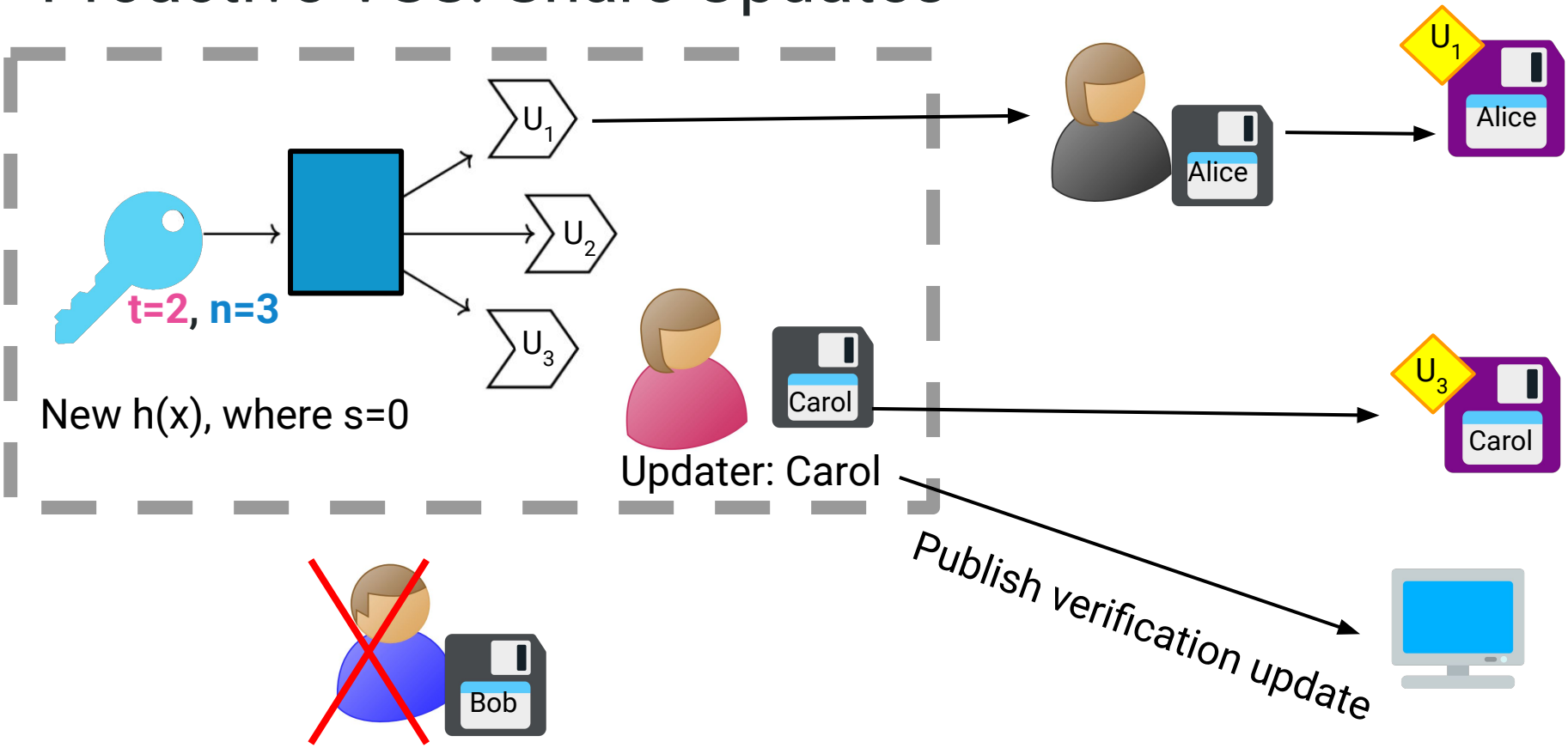
Proactive VSS: Share Validation

1. Action: The participant fetches the commitment from its trusted public location

2. Device: The participant will evaluate the validation function

3. Device: The participant verifies the correctness of her share by checking the commitment matches the validation function

Proactive VSS: Share Updates



Lightweight Improvements Comparison

●=achieved; ◐=ceremony dependent; ○=not achieved

	Classic Shamir				Our Proactive VSS			
	Base		*Ext*		*Base*		*Ext*	
	HBC	MAL	HBC	MAL	HBC	MAL	HBC	MAL
t-Sep. Priv.	●	●	●	●	●	●	●	●
Availability	●	●	○	○	●	●	●	●
IT Sec.	◐	◐	○	○	○	○	○	○
Conf.	◐	◐	◐	◐	●	●	●	●
Integrity	○	○	○	○	●	●	●	●

Takeaways

- ➔ We present a framework to facilitate the analysis of practical threshold schemes
- ➔ Variations in the ceremony can lead to changes in the fundamental security properties provided to end users
- ➔ Our framework can aid in the design and analysis of future implementations of secret sharing through its detailed ceremony definition and explicit coverage of previously undefined assumptions

Sunder Stages: Share Generation

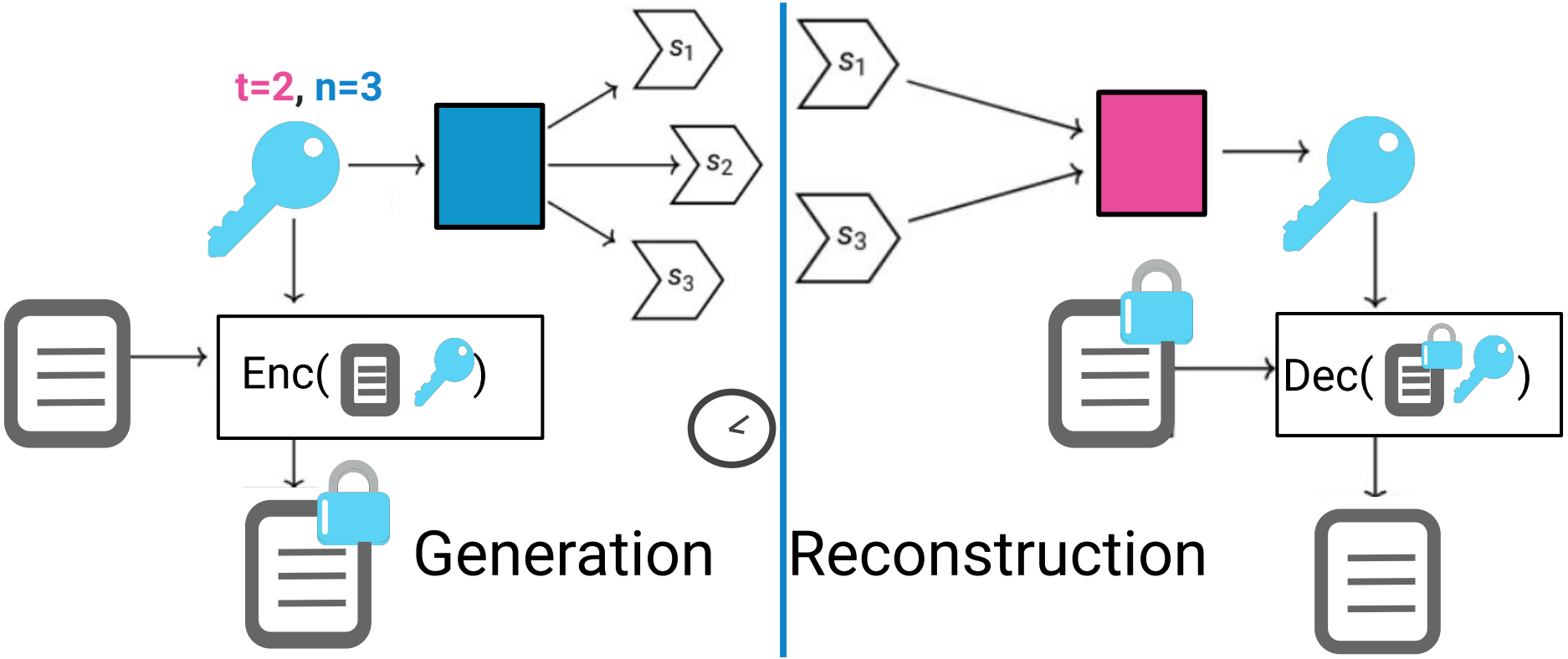
1. Choice: The dealer chooses values for **n** and **t**

2. Device: Generates a signature key pair

3. Device: Generates **n** shares

4. Action: Delete all copies of **s** and the signature key. (The device retains the public verification key.)

Extended Mode



Shatter Secrets: Evaluation

●=achieved; ◐=ceremony dependent; ○=not achieved

	Classic Shamir				Shatter Secrets	
	Base		*Ext*		*Ext*	
	HBC	MAL	HBC	MAL	HBC	MAL
t-Sep. Priv.	●	●	●	●	●	●
Availability	●	●	○	○	○	○
IT Sec.	◐	◐	○	○	○	○
Conf.	◐	◐	◐	◐	●	●
Integrity	○	○	○	○	◐	◐

Proactive VSS: Share Validation

1. Action: The participant fetches the commitment $\vec{C}$ from its trusted public location
2. Device: Using $\phi_0, \cdots, \phi_{t-1}$ which constitute $\vec{C}$, the participant will then calculate ψ by evaluating $\prod_{j=0}^{t-1} \phi_j^{{a_i}^j}$
3. Device: The participant can then validate the correctness of her share by validating ψ is equal to $g^{f(a_i)}$