

# State-Level Secrets

## When Theory Meets Practice for Journalists Working with Encrypted Documents

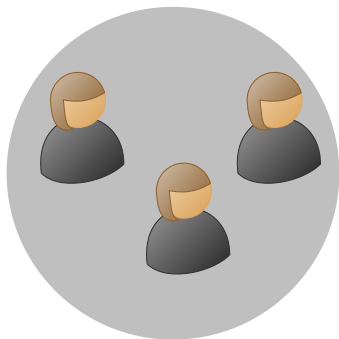
Bailey Kacsmar and Chelsea H. Komlo



**UNIVERSITY OF WATERLOO**  
FACULTY OF MATHEMATICS  
David R. Cheriton School  
of Computer Science

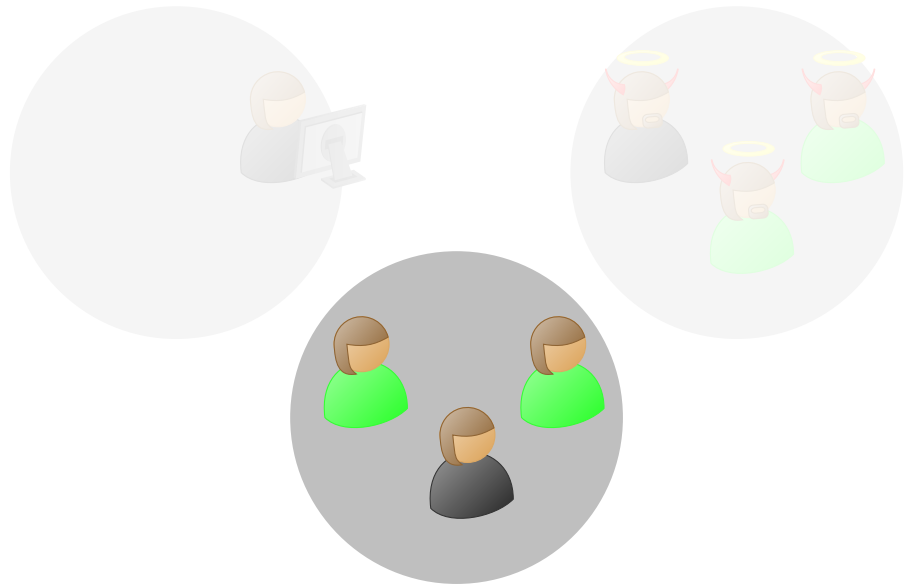
# $(t, n)$ -Threshold Schemes and Journalism

## $(2, 3)$ -Threshold Scheme Example



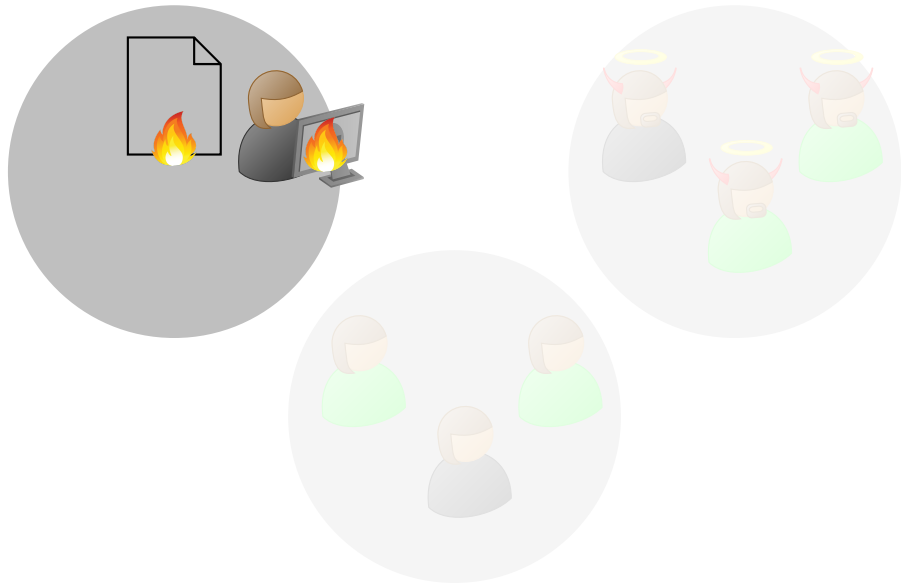
# $(t, n)$ -Threshold Schemes and Journalism

## $(2, 3)$ -Threshold Scheme Example



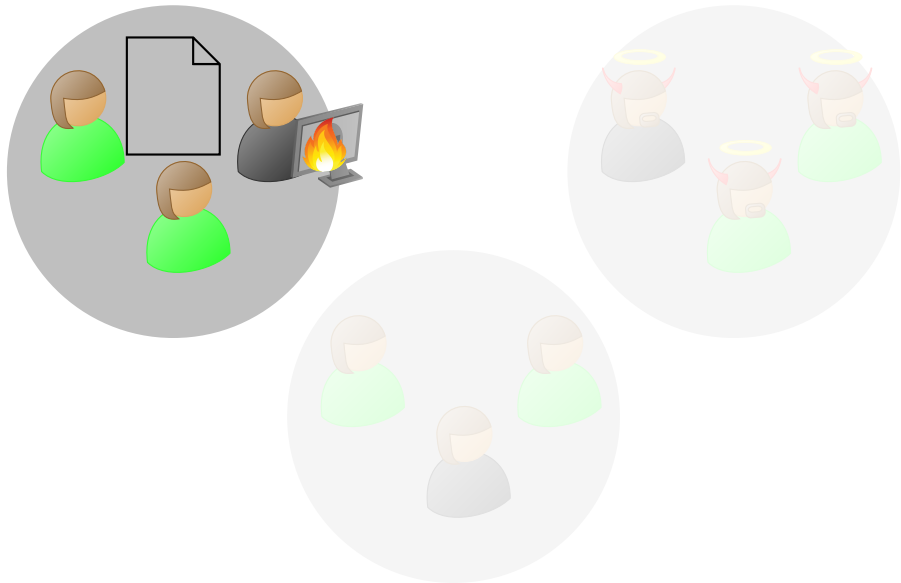
# $(t, n)$ -Threshold Schemes and Journalism

## (2, 3)-Threshold Scheme Example



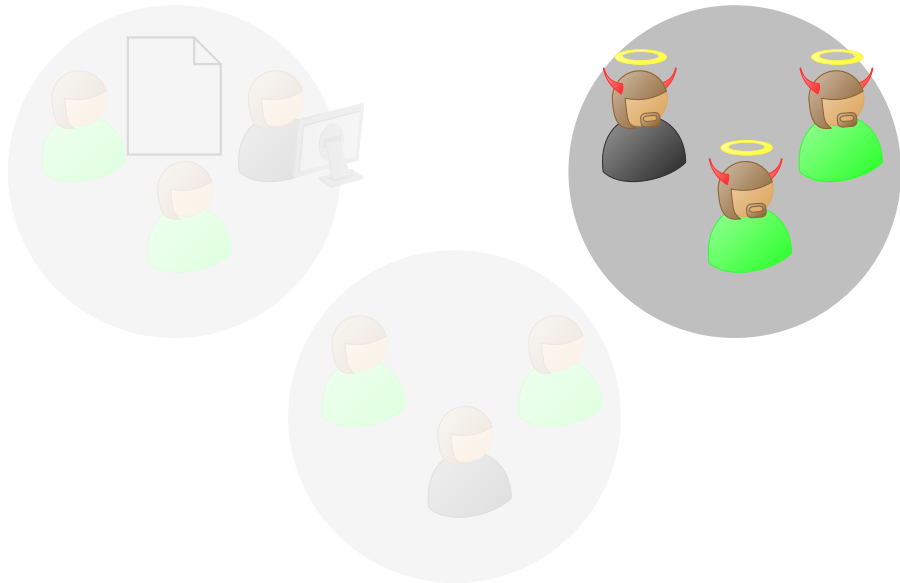
# $(t, n)$ -Threshold Schemes and Journalism

## (2, 3)-Threshold Scheme Example

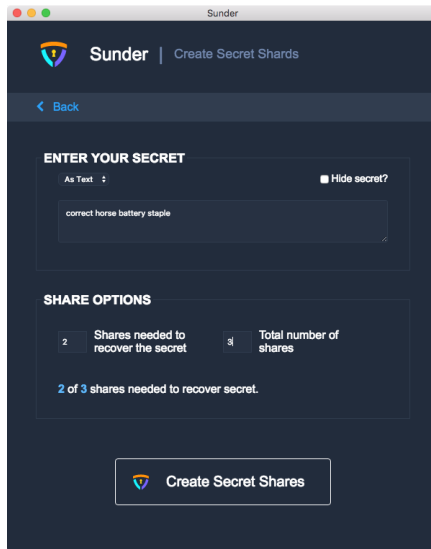


# $(t, n)$ -Threshold Schemes and Journalism

## (2, 3)-Threshold Scheme Example



# Freedom of the Press Foundation and Sunder



The screenshot shows the Sunder web application interface. At the top, there's a header with the Sunder logo and the text "Sunder | Create Secret Shards". Below the header is a navigation bar with a "Back" button. The main content area is divided into two sections: "ENTER YOUR SECRET" and "SHARE OPTIONS".

**ENTER YOUR SECRET**

As Text  Hide secret? ☐

correct horse battery staple

**SHARE OPTIONS**

2 Shares needed to recover the secret 3 Total number of shares

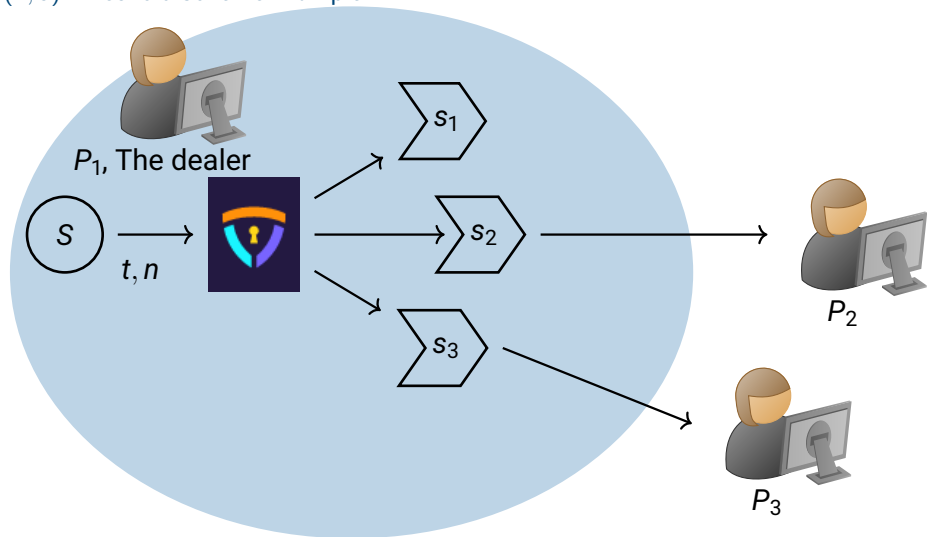
2 of 3 shares needed to recover secret.

Create Secret Shares

[github.com/freedomofpress/sunder](https://github.com/freedomofpress/sunder)

# Basic Secret Sharing as a Protocol: Generation and Distribution

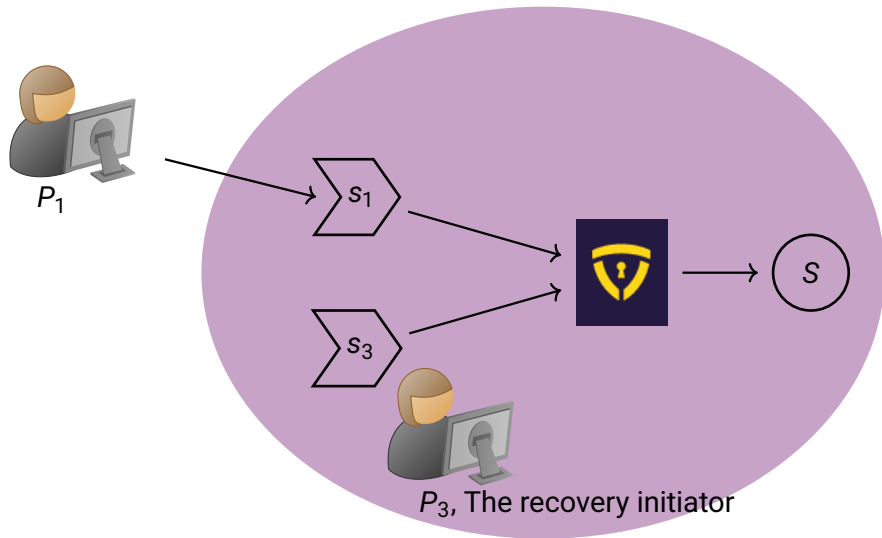
## (2, 3)-Threshold Scheme Example





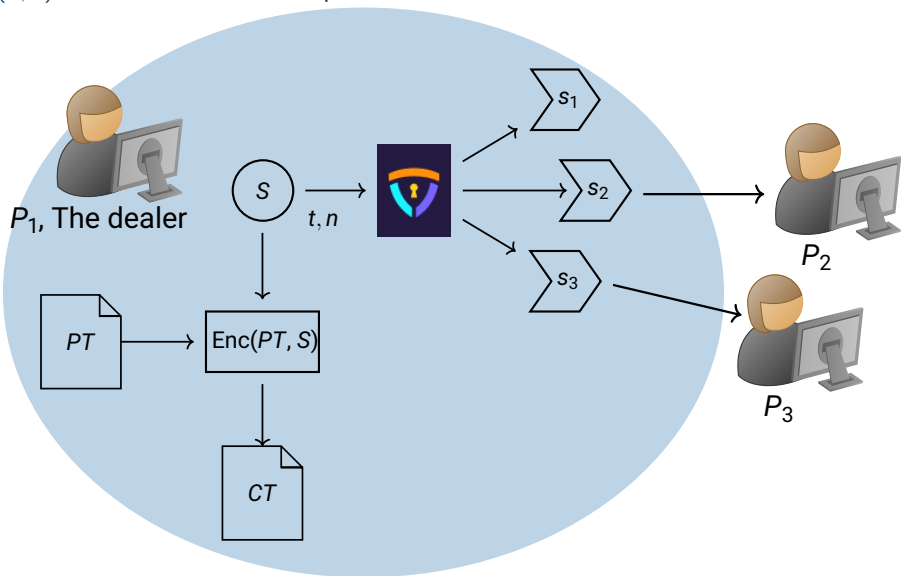
# Basic Secret Sharing: Reconstruction

## (2, 3)-Threshold Scheme Example



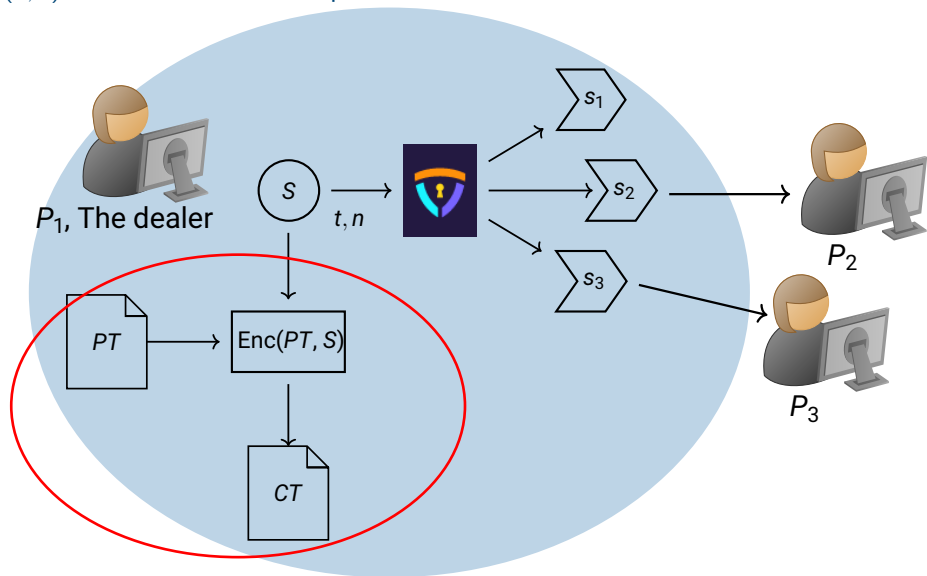
# Expanded Secret Sharing: Generation and Distribution

## (2, 3)-Threshold Scheme Example



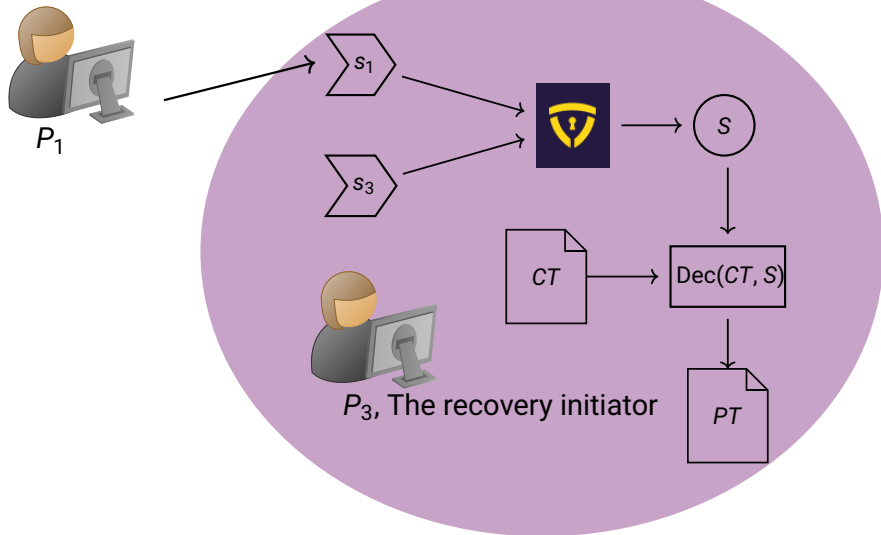
# Expanded Secret Sharing: Generation and Distribution

## (2, 3)-Threshold Scheme Example



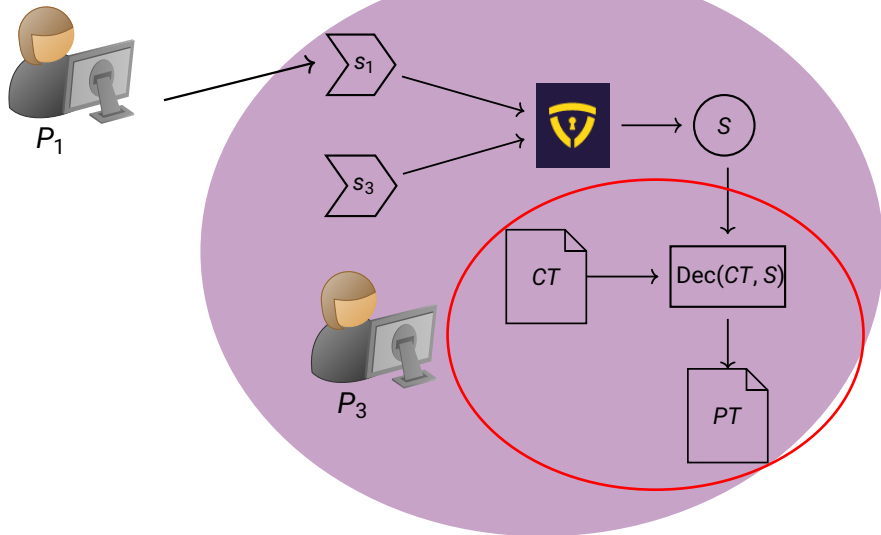
# Expanded Secret Sharing: Reconstruction

## (2, 3)-Threshold Scheme Example



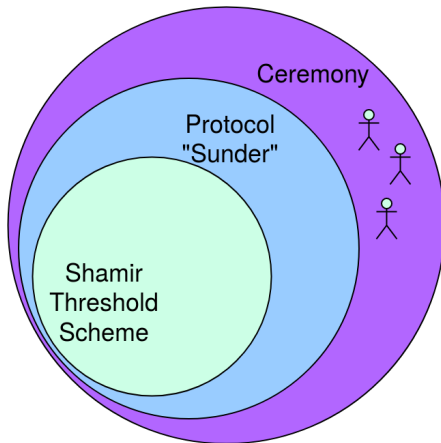
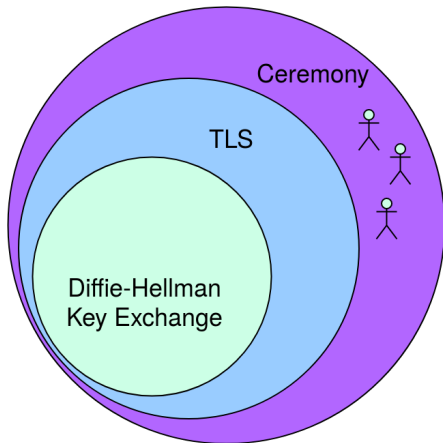
# Expanded Secret Sharing: Reconstruction

## (2, 3)-Threshold Scheme Example



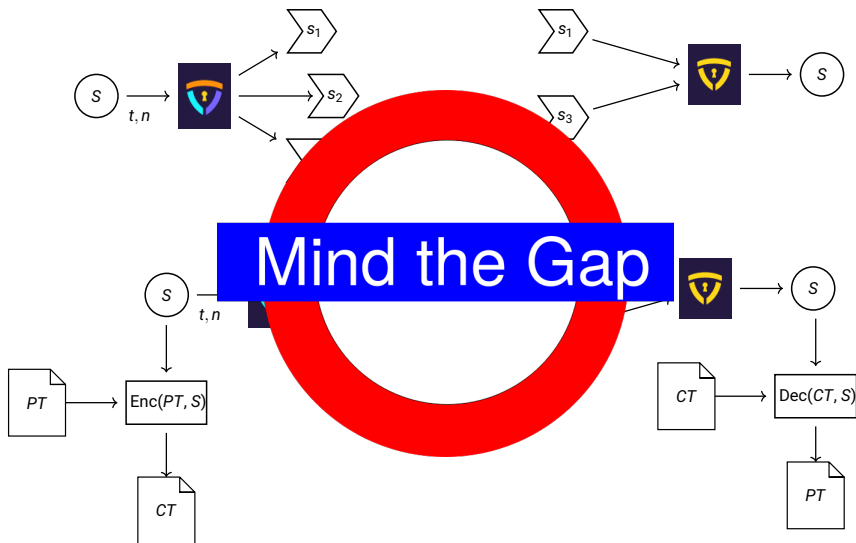
# Ceremonies and Security

## Layers of Security Analysis



C. Ellison, Ceremony Design and Analysis, 2007.

# Protocol and Ceremony Security

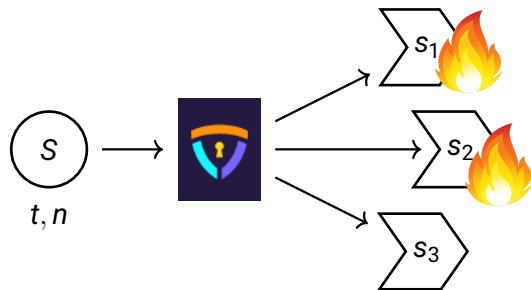


# Gaps and Improvements: Base



# Share Loss: Gaps

## Protocol

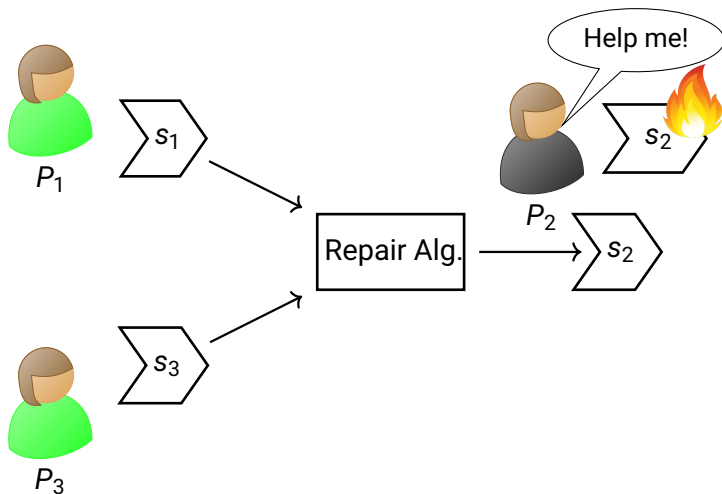


Loss of  $n - t - 1$  shares renders the secret unrecoverable.

Attackers can destroy or perform a denial of service attack against shares.

# Share Loss: Improvements

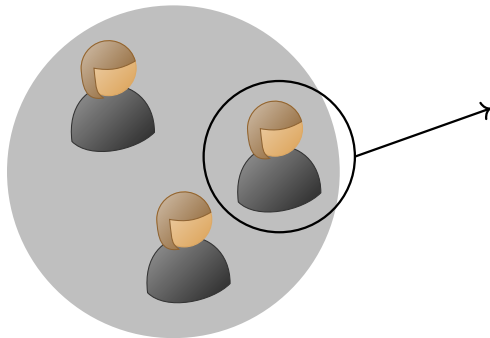
Protocol: (2,3)-Threshold Scheme Example



Laing, Stinson, A Survey and Refinement of Repairable Threshold Schemes, 2018.

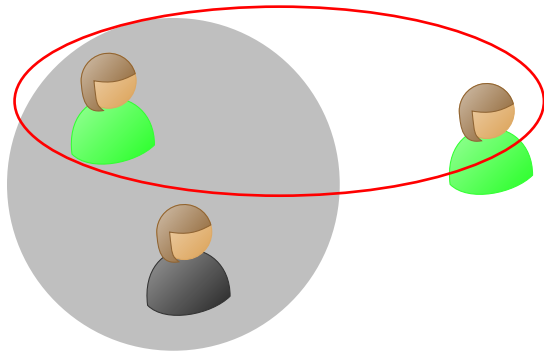
# Organizational Turnover: Gaps

## Protocol



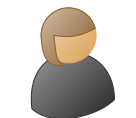
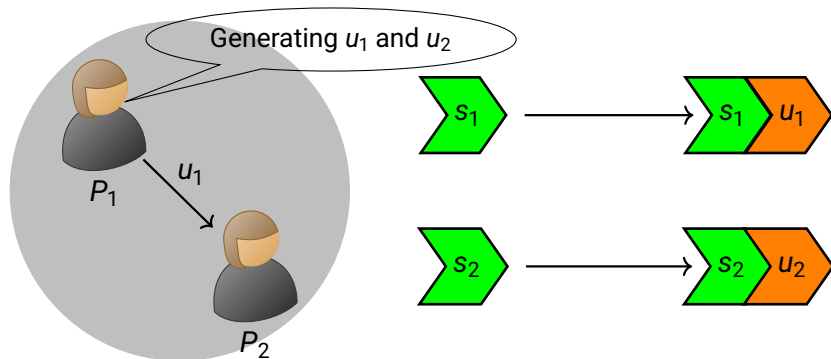
# Organizational Turnover: Gaps

## Protocol

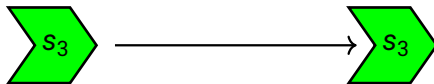


# Organizational Turnover: Improvements

## Protocol



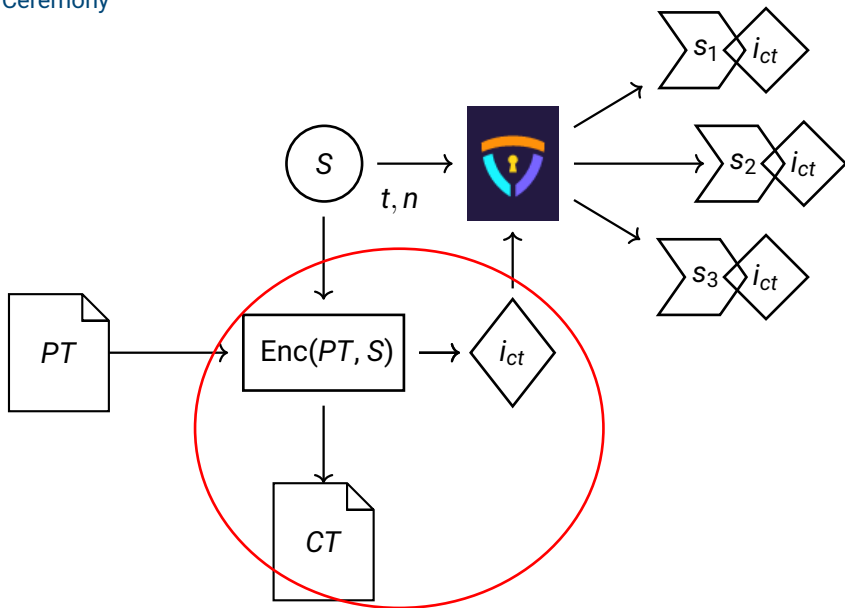
Former  $P_3$



# Gaps and Improvements: Extended

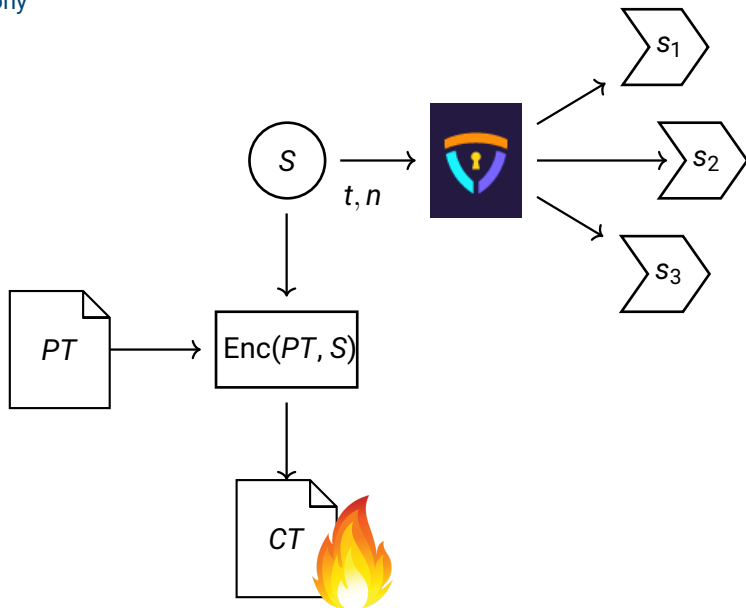
# Integrity for Ciphertext: Gaps and Improvements

Ceremony



# Redundancy for Ciphertext: Gaps

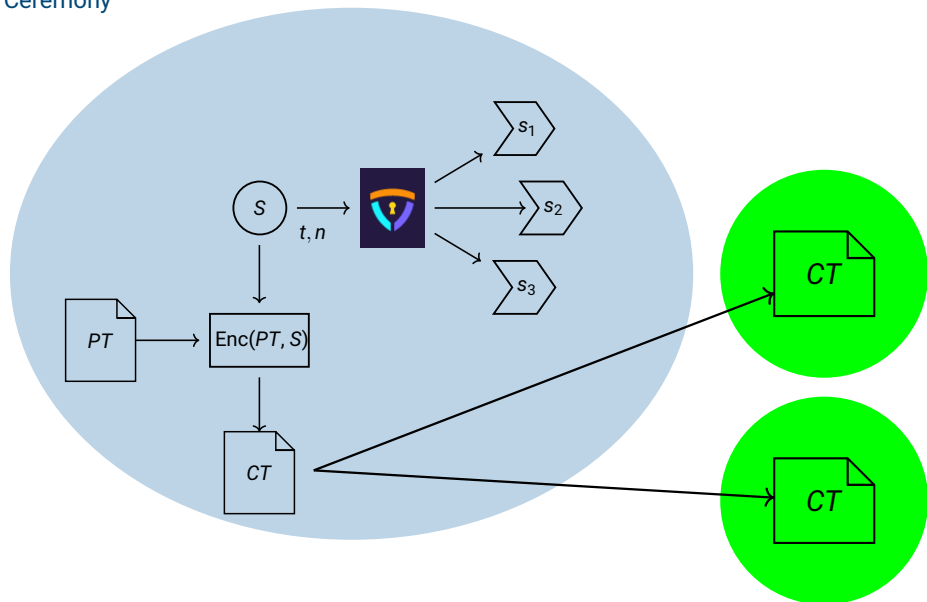
Ceremony





# Redundancy for Ciphertext: Improvements

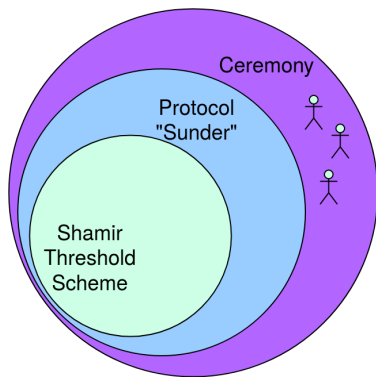
Ceremony



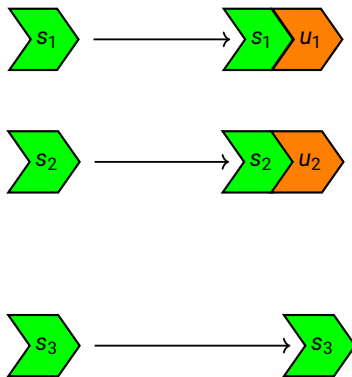
# Ongoing and Future Work

# Current Work

## Complete Ceremony Analysis



## Updating Shares Functionality



# Future Work

- Adding implementations of repairing algorithms for lost shares
- Designing schemes to limit dealer trust

# Takeaways

- Secret sharing schemes are not suitable for real-world use as-is
- Actionable improvements for gaps found in integrity, confidentiality, authenticity, and availability
- Ceremony analysis identifies gaps between user responsibility and security expectations

Thank You!

---

Watch for our paper at [crisp.uwaterloo.ca](https://crisp.uwaterloo.ca)