State-Level Secrets

When Theory Meets Practice for Journalists Working with Encrypted Documents

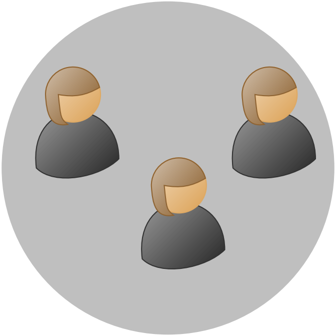
Bailey Kacsmar and Chelsea H. Komlo

CrySP
Cryptography, Security, and Privacy
Research Group

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

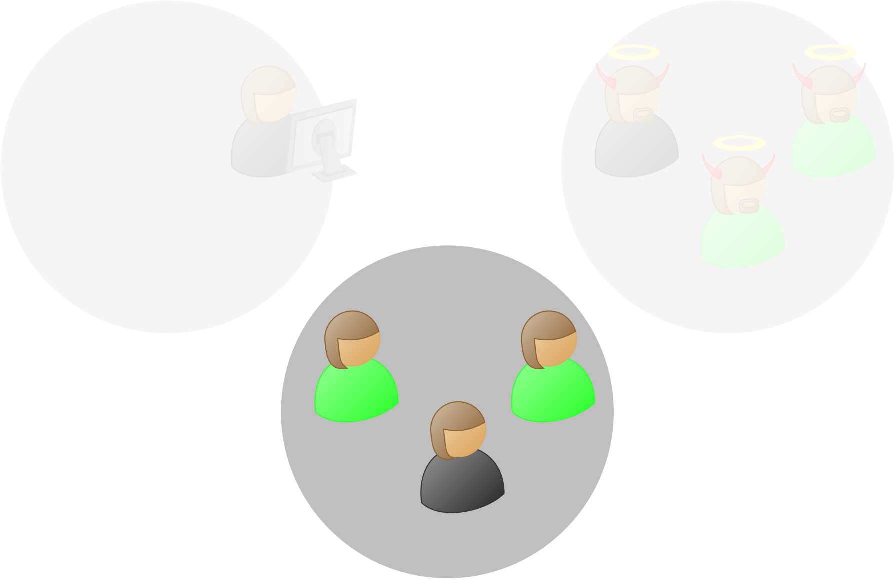
(t, n)-Threshold Schemes and Journalism

$(2, 3)$-Threshold Scheme Example



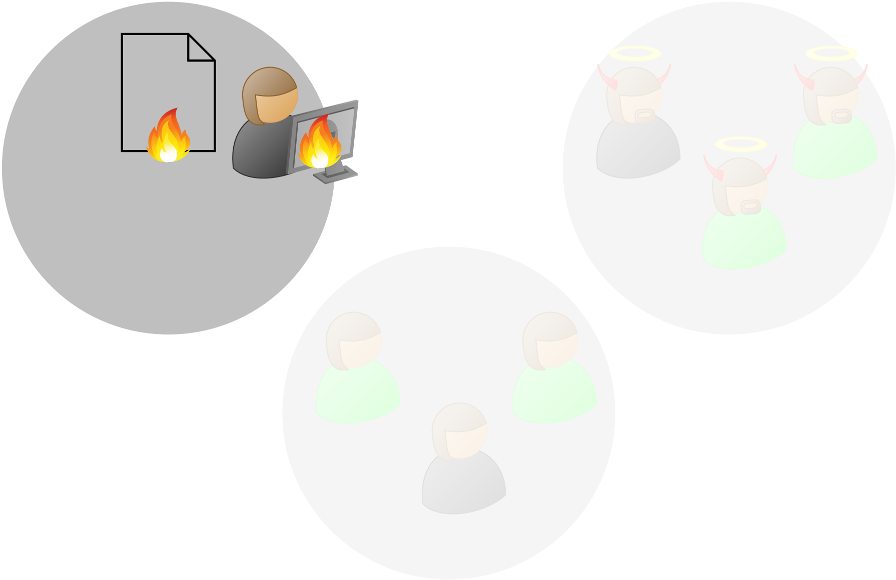
(t, n)-Threshold Schemes and Journalism

$(2, 3)$-Threshold Scheme Example



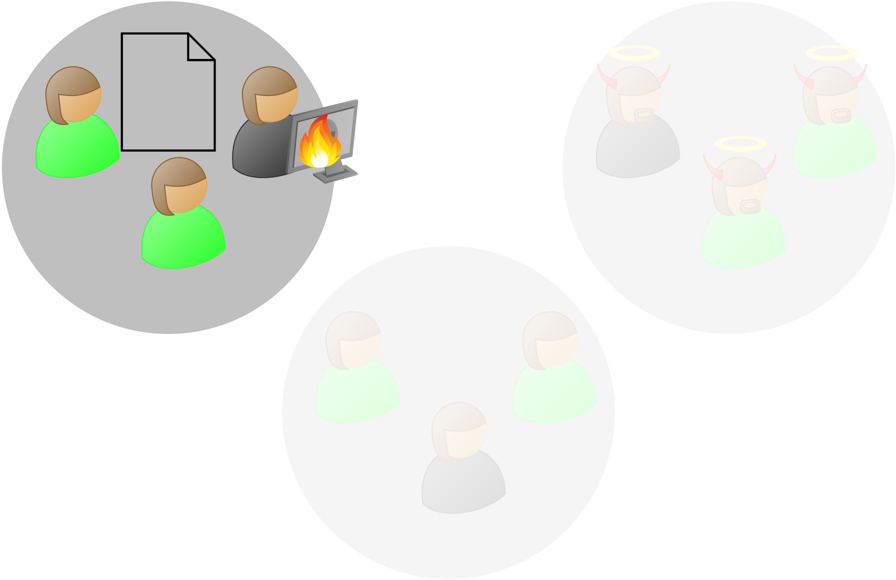
(t, n)-Threshold Schemes and Journalism

$(2, 3)$-Threshold Scheme Example



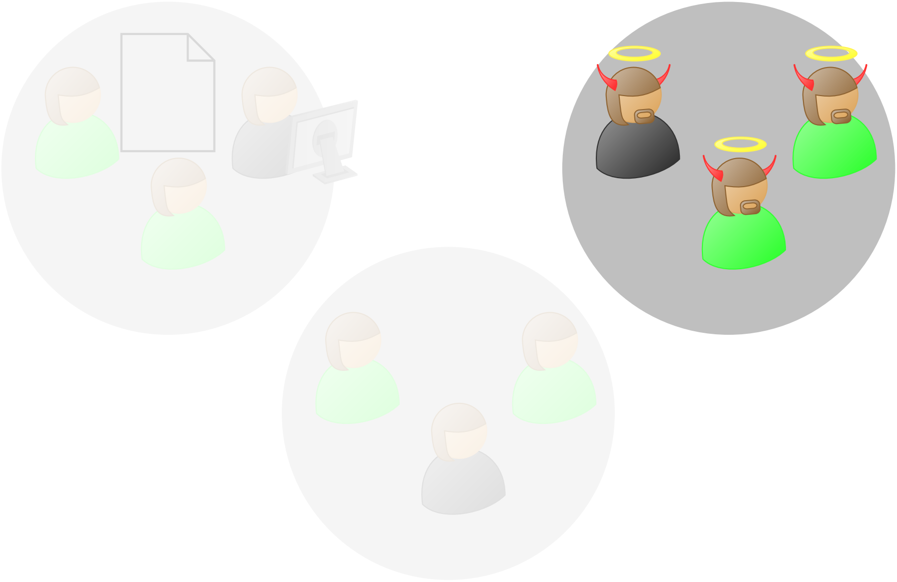
(t, n)-Threshold Schemes and Journalism

$(2, 3)$-Threshold Scheme Example

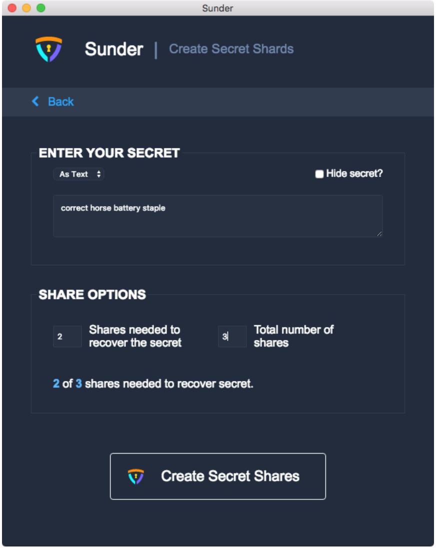


(t, n)-Threshold Schemes and Journalism

$(2, 3)$-Threshold Scheme Example



Freedom of the Press Foundation and Sunder



ENTER YOUR SECRET

As Text

□ Hide secret?

correct horse battery staple

SHARE OPTIONS

2 Shares needed to recover the secret

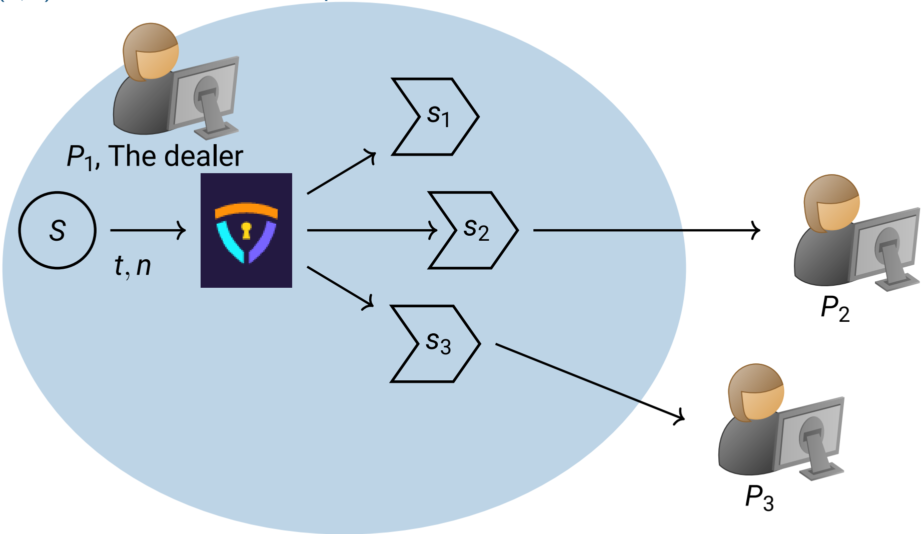
3 Total number of shares

2 of 3 shares needed to recover secret.

github.com/freedomofpress/sunder

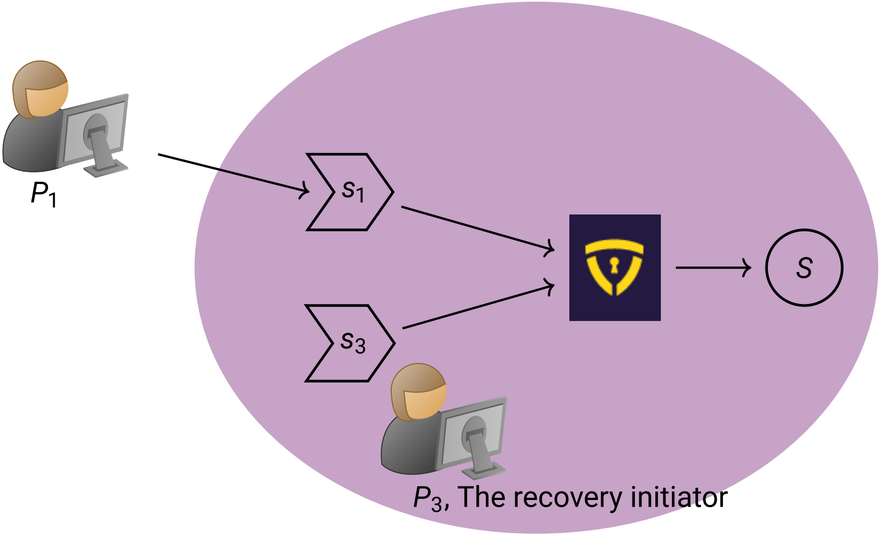
Basic Secret Sharing as a Protocol: Generation and Distribution

$(2, 3)$-Threshold Scheme Example



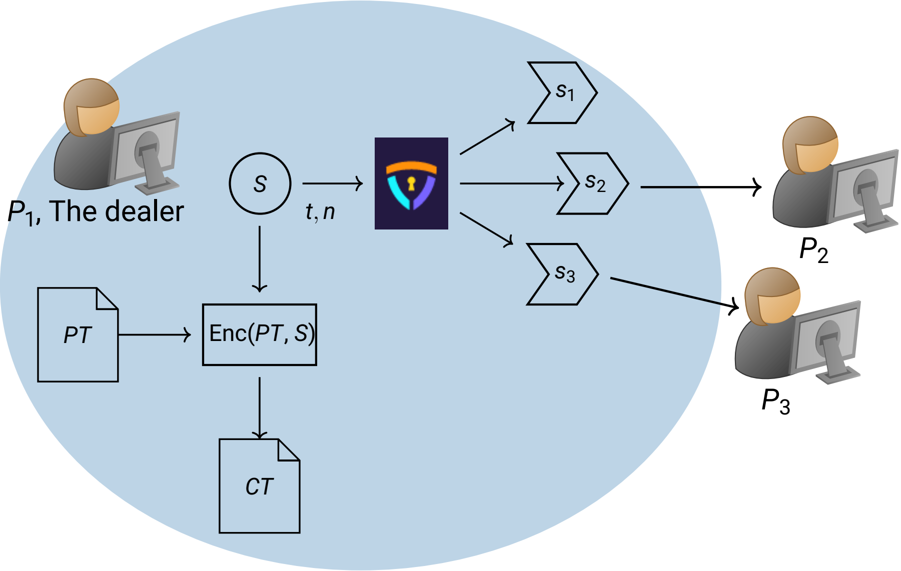
Basic Secret Sharing: Reconstruction

(2, 3)-Threshold Scheme Example



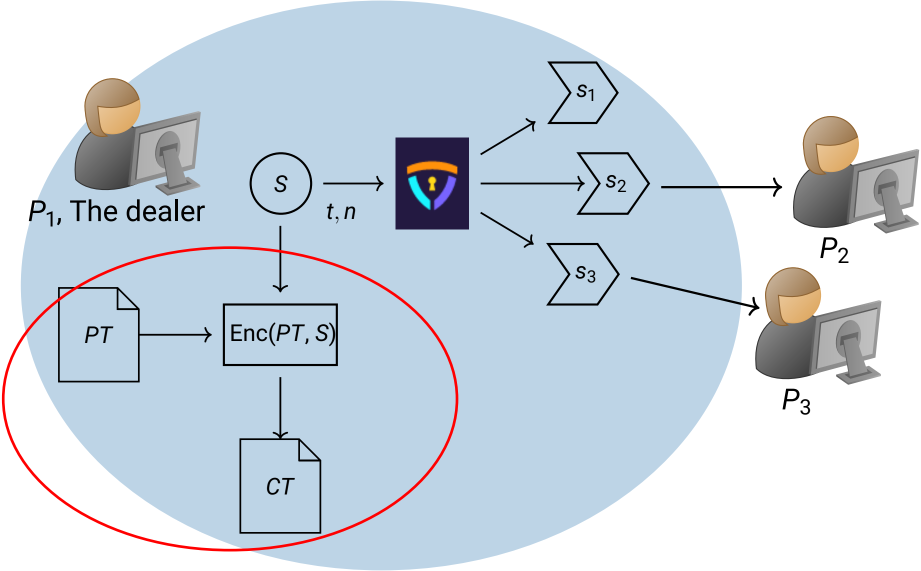
Expanded Secret Sharing: Generation and Distribution

$(2,3)$-Threshold Scheme Example



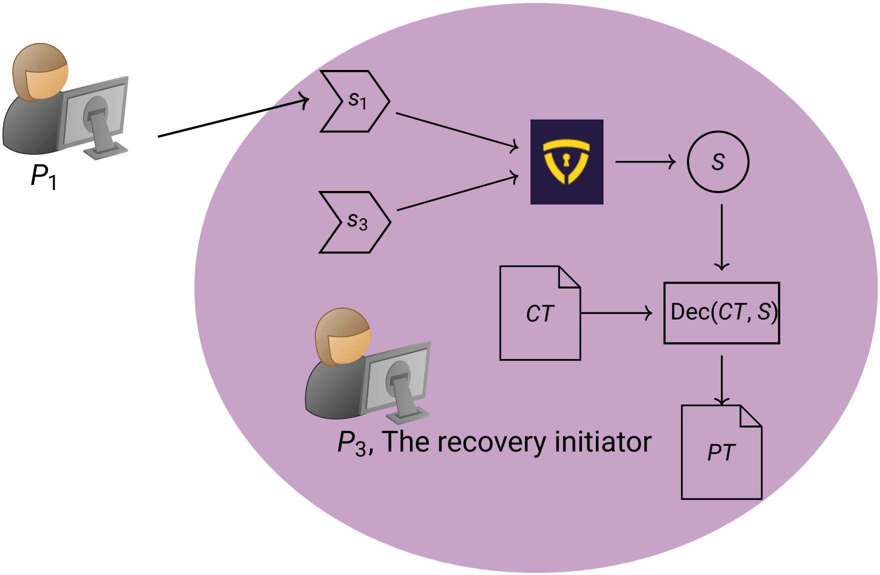
Expanded Secret Sharing: Generation and Distribution

$(2, 3)$-Threshold Scheme Example



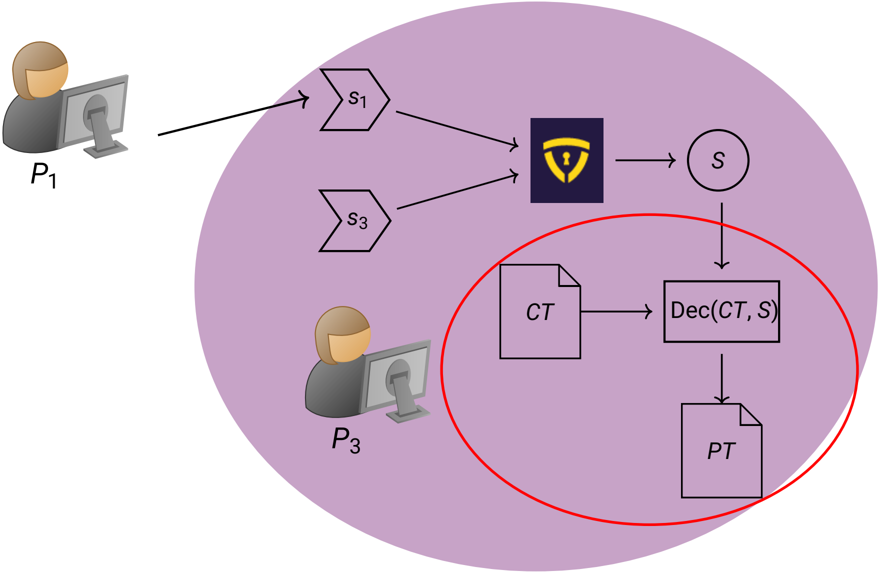
Expanded Secret Sharing: Reconstruction

$(2, 3)$-Threshold Scheme Example



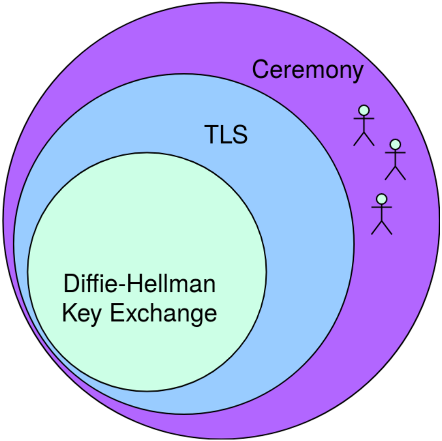
Expanded Secret Sharing: Reconstruction

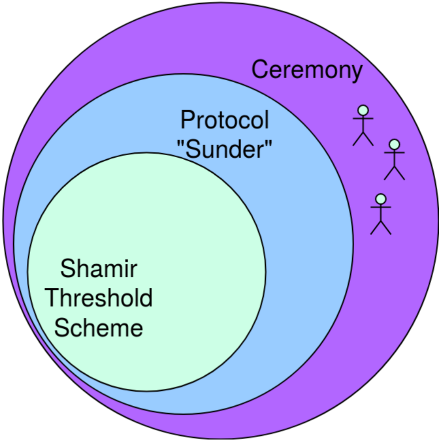
$(2, 3)$-Threshold Scheme Example



Ceremonies and Security

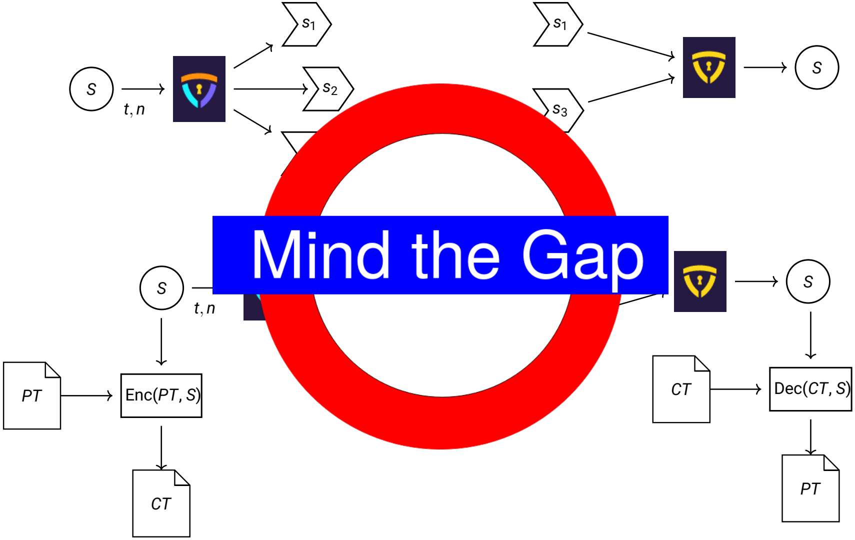
Layers of Security Analysis





C. Ellison, Ceremony Design and Analysis, 2007.

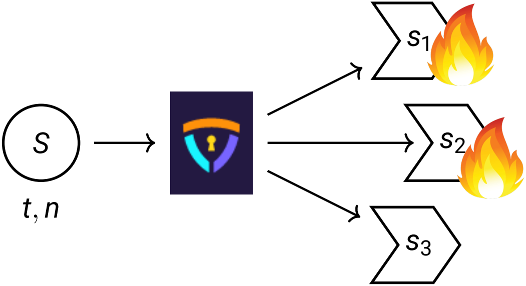
Protocol and Ceremony Security



Gaps and Improvements: Base

Share Loss: Gaps

Protocol

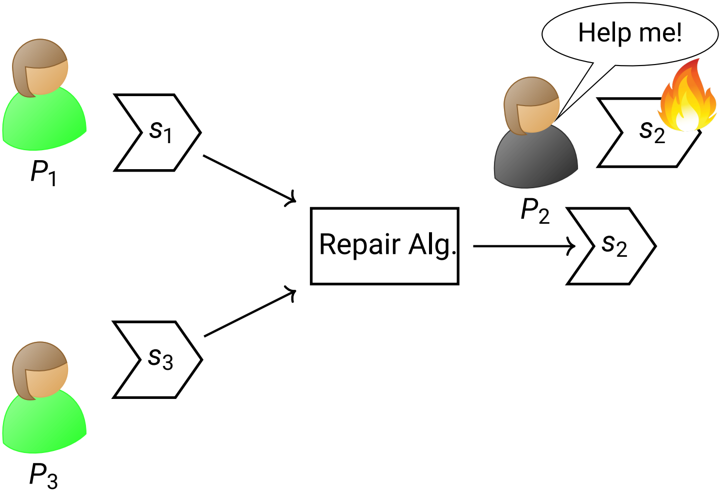


Loss of $n - t - 1$ shares renders the secret unrecoverable.

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

Share Loss: Improvements

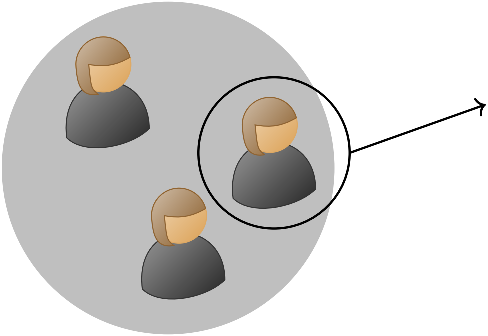
Protocol: (2,3)-Threshold Scheme Example



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

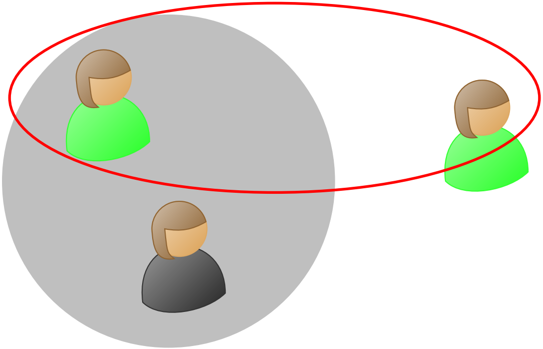
Organizational Turnover: Gaps

Protocol



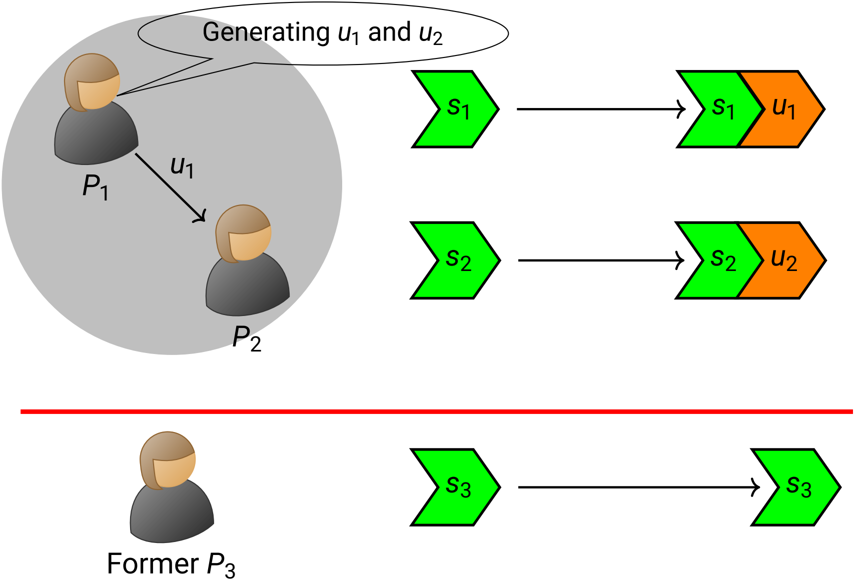
Organizational Turnover: Gaps

Protocol



Organizational Turnover: Improvements

Protocol



Generating u_1 and u_2

P_1

u_1

P_2

s_1 → s_1 u_1

s_2 → s_2 u_2

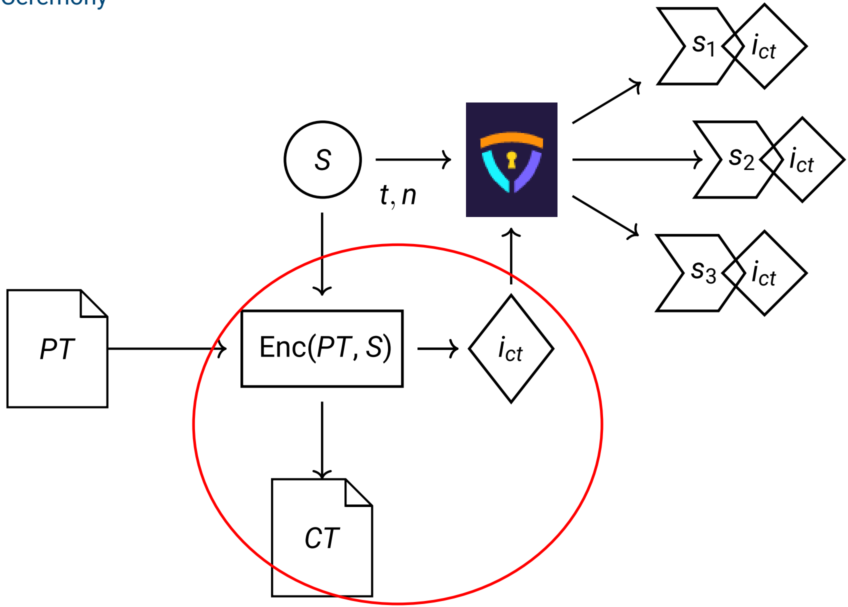
Former P_3

s_3 → s_3

Gaps and Improvements: Extended

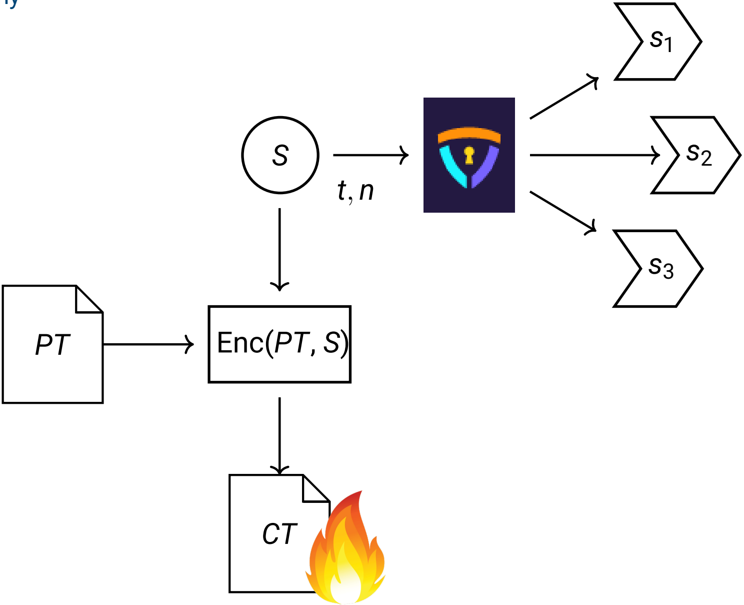
Integrity for Ciphertext: Gaps and Improvements

Ceremony



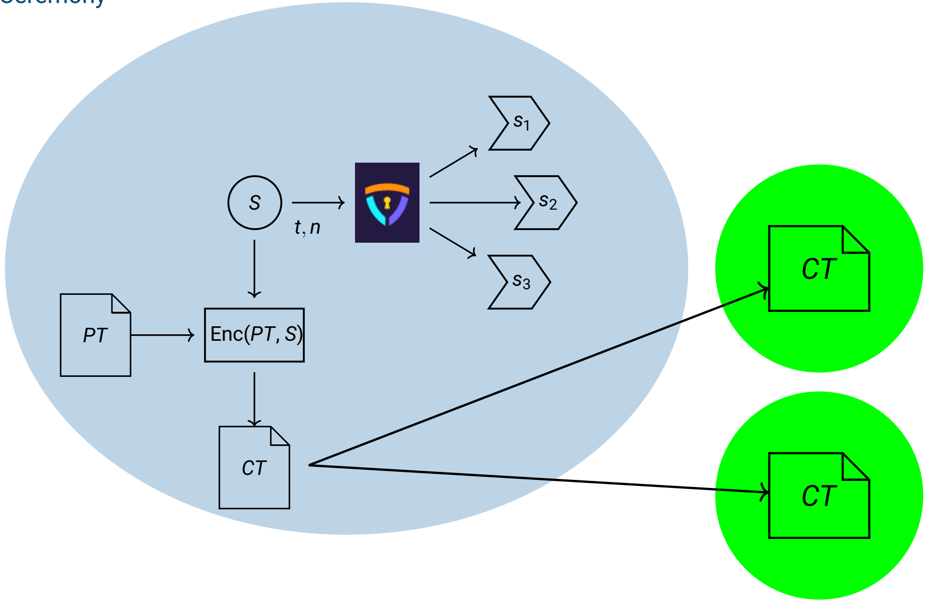
Redundancy for Ciphertext: Gaps

Ceremony



Redundancy for Ciphertext: Improvements

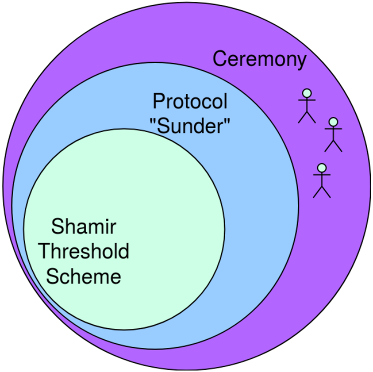
Ceremony



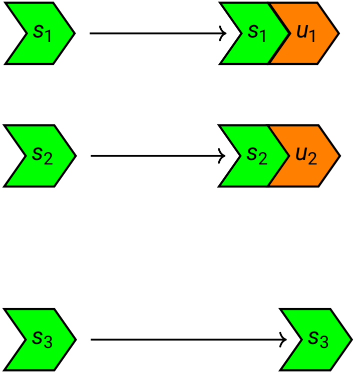
Ongoing and Future Work

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 crysp.uwaterloo.ca