Usability and Cryptography
Part 1 and 2

Selected Areas of Cryptography Summer School 2024

Bailey Kacsmar

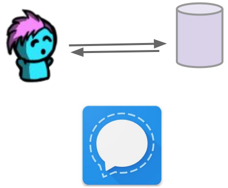
NSERC CRSNG

PUPS Research Lab

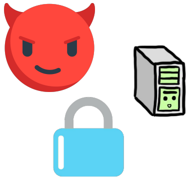
UNIVERSITY OF ALBERTA

amii

Usability

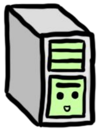


Functionality

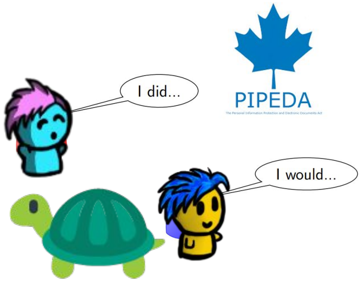


Deployability and Verifiability

“Accessibility”



“Efficiency”



Trust and Perceptions

You are probably already familiar with a “usability” based design principle

Shannon’s Maxim and Kerkhoff’s Principle Mean:

- Security shouldn’t rely on the secrecy of the method
- Do use public algorithms with secret “keys”
- The adversaries target…is the key

Core: Easier to change a “short” key than your whole system.
(e.g., Recovery)

Unconditionally Secure: One-Time Pad

Message: x_0 | x_1 | x_2 ... x_n

$$\oplus$$

Key: k_0 | k_1 | k_2 ... k_n

$$=$$

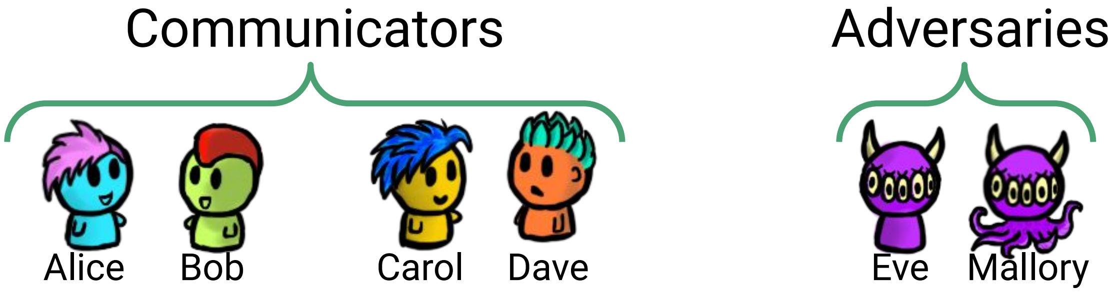
Core problem: Key as long as the message,
Only used once

Rule: $y_i = x_i + k_i \pmod{2}$

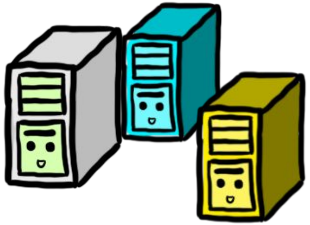
On Usability (Today)

- We need to define this term…
- Why (and how) do we “need” to consider usability?
- Usability based analysis
- Examples using analysis towards cryptography

Base Cryptography - Writing “secret” messages

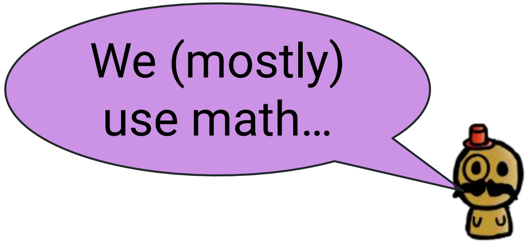


Cryptography for Security and Privacy



Someone wants to complete a task

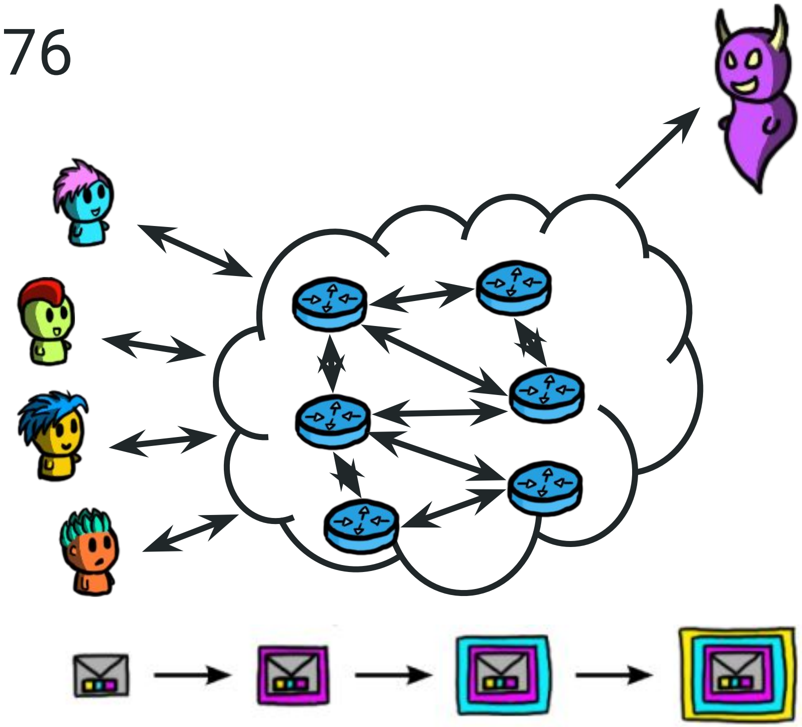
But there are privacy implications and risk from that task



Researchers develop technical solutions

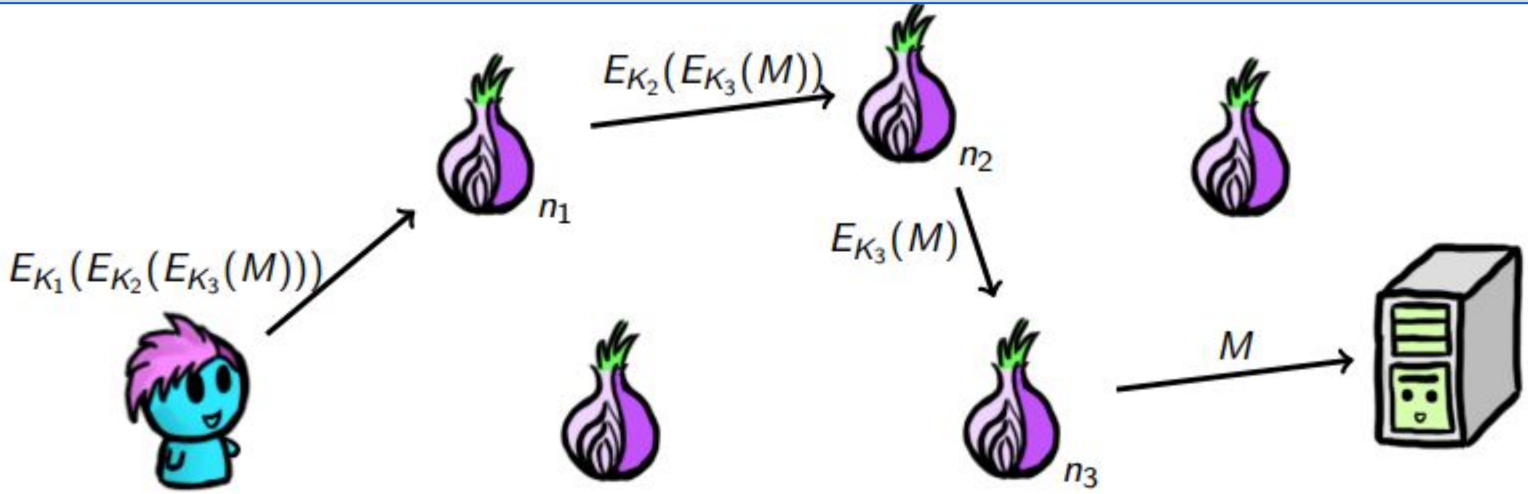
Cryptography for Communications?

- Diffie-Hellman Key Exchange, 1976
- RSA Encryption, 1977
- Shamir secret sharing, 1979
- PGP, Pretty good privacy, 1991
- ...



Application Example: Sending Messages with Tor

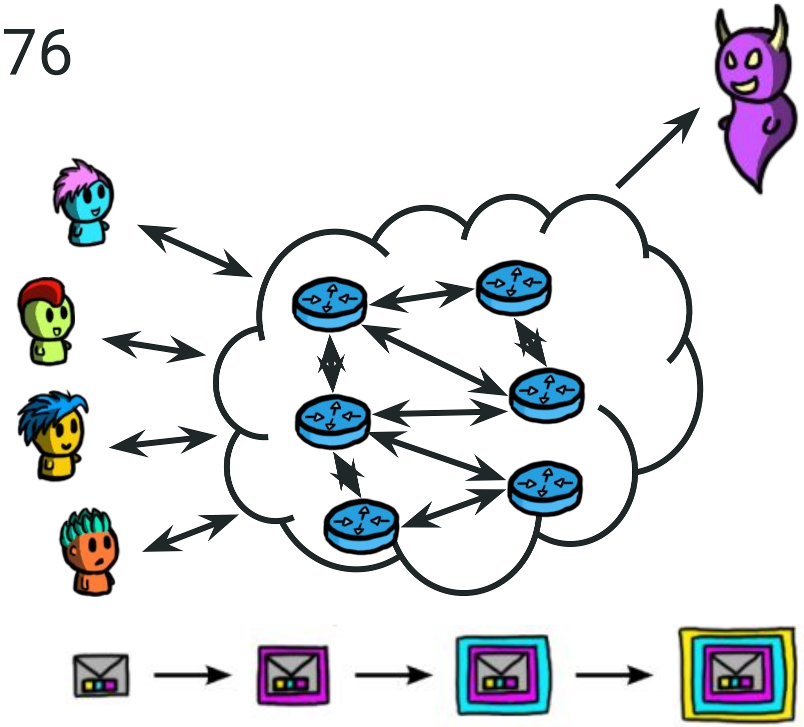
Alice (after many steps of PKC) encrypts her message “like an onion”; each node peels a layer off and forwards it to the next step



If connecting to a web server, M is encrypted (e.g., TLS)

Cryptography for **Everyday**

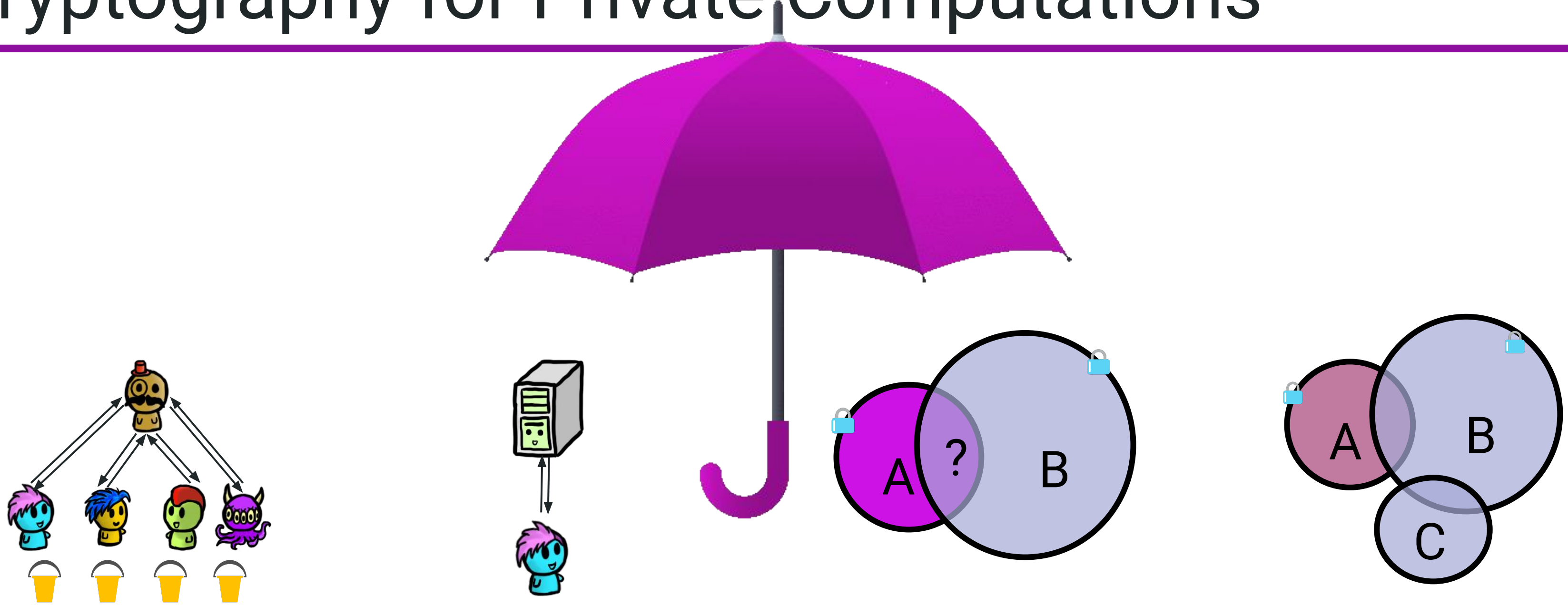
- Diffie-Hellman Key Exchange, 1976
- RSA Encryption, 1977
- Shamir secret sharing, 1979
- PGP, Pretty good privacy, 1991
- ...



Cryptography for Private Computations

Balancing Privacy and Utility

Cryptography for Private Computations



Private Machine Learning

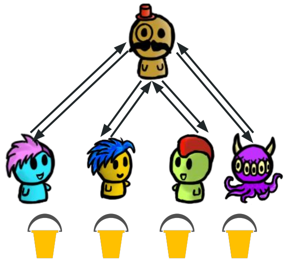
Private Query Processing

Private Set Intersection

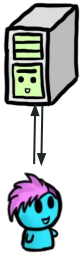
Multiparty Computations

Private Computations Class

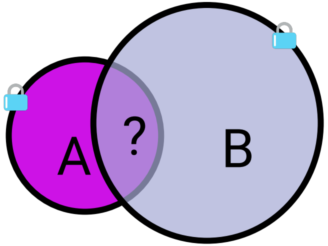
Define, **what** is being protected, from **whom**,
and under what **conditions** this protection will hold.



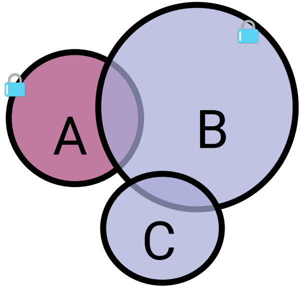
Private Machine Learning



Private Query Processing



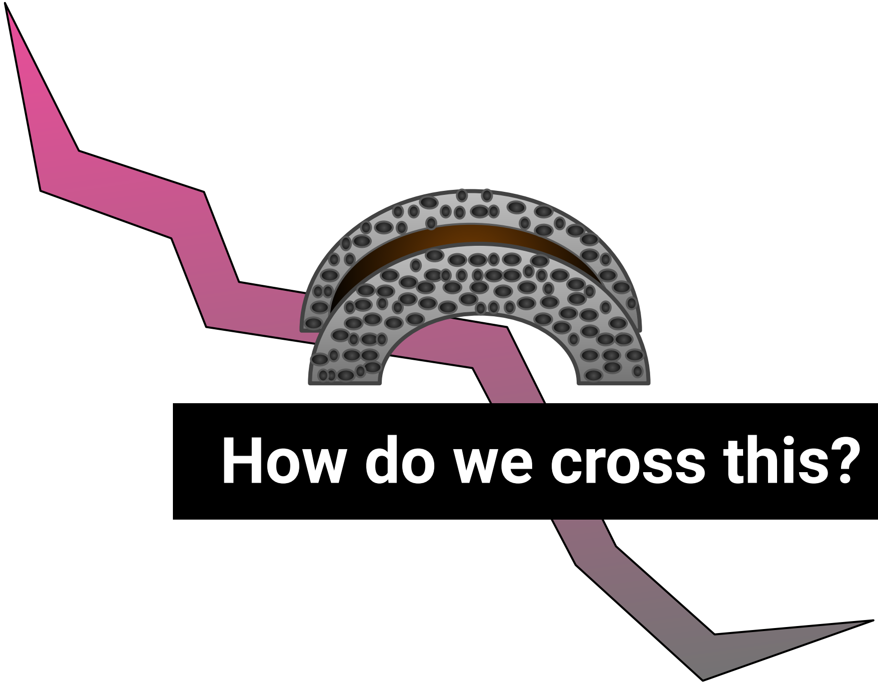
Private Set Intersection



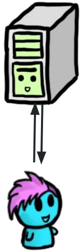
Multiparty Computations

A Tale as Old as Time…

Academic
Cryptography



How do we cross this?



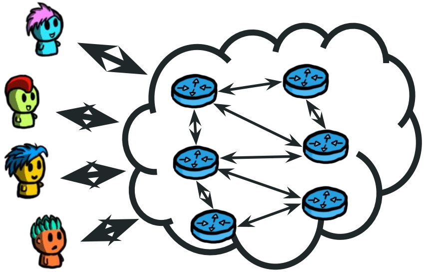
<u>Correctly</u> Deployed
Cryptography

Utility, the Usability Scapegoat

Definition: the benefit that users (and the provider) get from using the system.

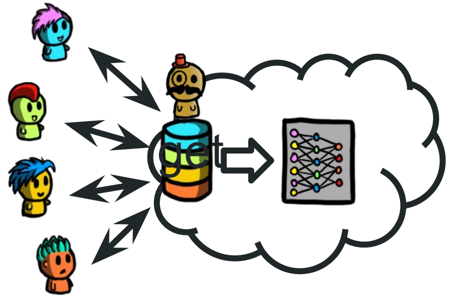
Communications system:

- For users: being able to communicate



Data Science:

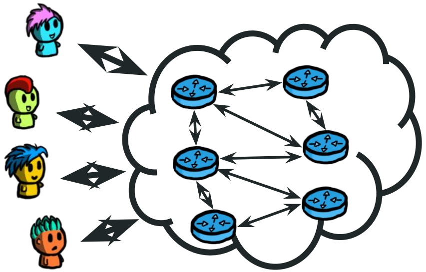
- For participants: maybe they compensation?
- For data owner: it can sell access to model/analysis for revenue
- Analysts: they pay to get benefits from the model's outputs
- General public: maybe the model outputs are good for society?



Quantifying Utility the Scapegoat

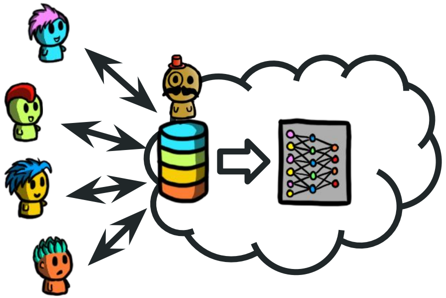
Q: How do we *quantify* utility?

Communications system:



- Low packets dropped
- High bandwidth/throughput
- Low latency/delay...

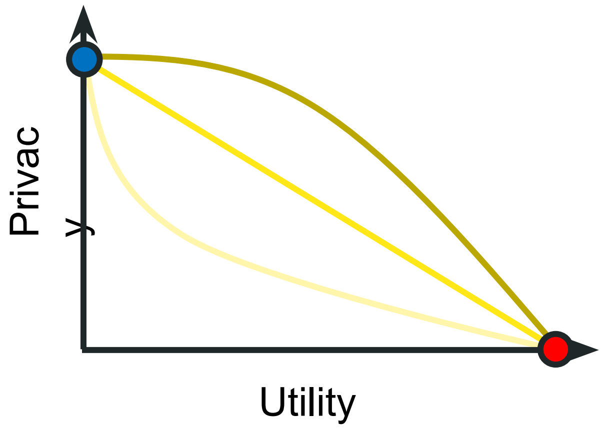
Machine learning:



- Useful model (high test accuracy)
- Unbiased model (low disparity among subpopulations)
- Low computational requirements to build the model
- Fast training algorithm...

The Privacy-Utility trade-off

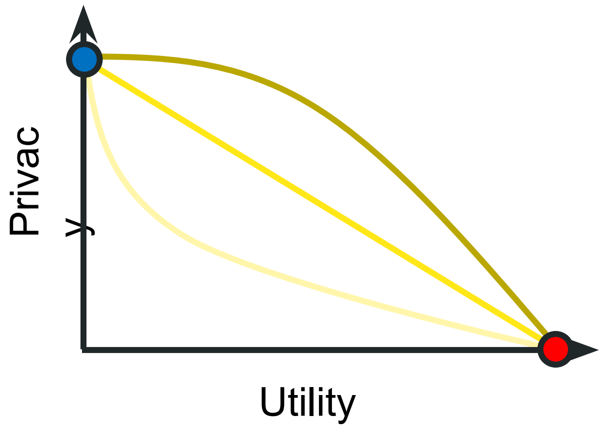
- Given any metric for privacy and for utility, they are usually at odds:



- **Q:** How do you design a system that provides maximum utility?
- **Q:** How do you design a system that provides maximum privacy?
- Designing a system that provides a good privacy-utility trade-off is hard!

The Privacy-Utility trade-off

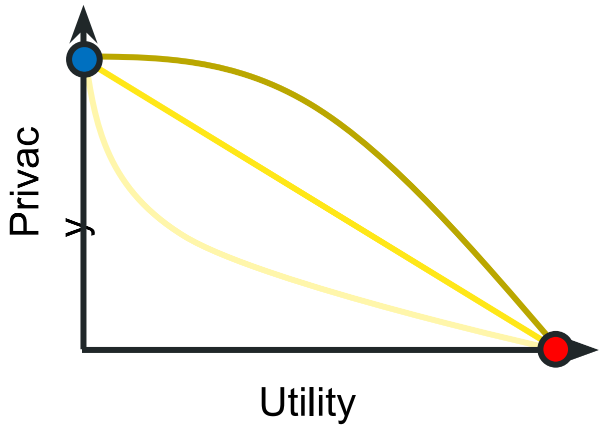
- Given any metric for privacy and for utility, they are usually at odds:



- How do you design a system that provides maximum utility?
  - You design it without privacy in mind
- How do you design a system that provides maximum privacy?
  - ..?
- Designing a system that provides a good privacy-utility trade-off is hard!

The Privacy-Utility trade-off

- Given any metric for privacy and for utility, they are usually at odds:



- How do you design a system that provides maximum utility?
  - You design it without privacy in mind
- How do you design a system that provides maximum privacy?
  - You don’t design it
- Designing a system that provides a good privacy-utility trade-off is hard!

The Entanglement, Beyond Utility Alone

SAC 2024 Special Topic:

Cryptographic tools for privacy, privacy-enhancing technologies and interactions between privacy and cryptography.

Cryptography for privacy or even security is entangled **with humans**

Beyond Data the Abstraction

Google and Mastercard Cut a Secret Ad Deal to Track Retail Sales

Google found the perfect way to link online ads to store purchases: credit card data

By Mark Bergen and Jennifer Surane
August 30, 2018, 3:43 PM EDT *Updated on August 31, 2018, 12:40 PM EDT*

washingtonpost.com

Now for sale: Data on your mental health

Drew Harwell

These retailers share customer data with Facebook's owner. Customers may not have been told | CBC News

Thomas Daigle · CBC News · Posted: Feb 07, 2023 4:00 AM EST | Last

Home Depot didn't get customer consent before sharing data with Facebook's owner, privacy watchdog finds | CBC News

Catharine Tunney · CBC News · Posted: Jan 26, 2023 9:53 AM
Updated: January 27

Double-double tracking: How Tim Hortons knows where you sleep, work and vacation

James McLeod · June 15, 2020 · In : Canada Privacy · 0 · 1,169 · 11 min read

Beyond Data the Abstraction

Google and Mastercard ... Deal to Tra...

Google found the ... card data

By Mark Bergen and Jennife...
August 30, 2018, 3:43 PM ED...

Home Depot ... consent befo... Facebook's ov... finds | CBC Ne...

Catharine Tunney · CBC Ne...
Updated: January 27

...ental

...and Vacation

...e 15, 2020 In : Canada Privacy 0 1,169 11 min read

ADOBE / CREATORS / TECH

Adobe's new terms of service aren't the problem – it's the trust

/ The reaction from Adobe's customers to a small update highlights the growing lack of faith surrounding big tech companies and their AI tools.

Creatives are fearful of how Adobe's adoption of generative AI will impact their privacy and rights over their work. Illustration by Haein Jeong / The Verge

By Jess Weatherbed, a news writer focused on creative industries, computing, and internet culture. Jess started her career at TechRadar, covering news and hardware reviews.

Jun 7, 2024, 1:37 PM MDT

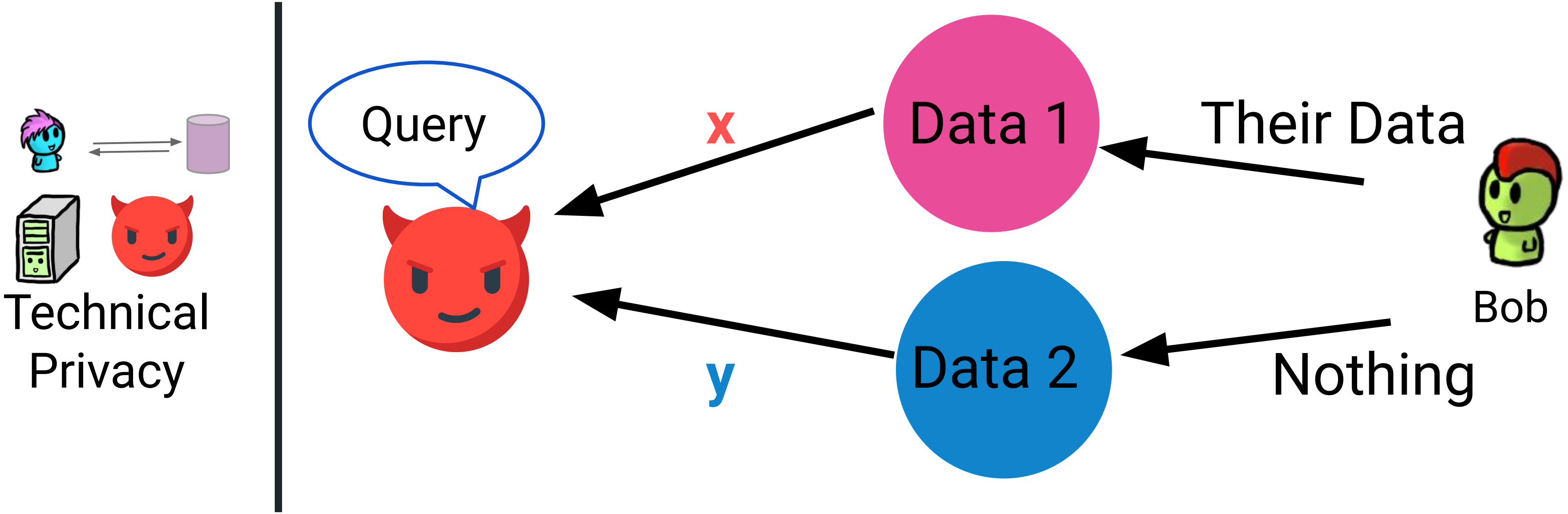
11 Comments (11 New)

If you buy something from a Verge link, Vox Media may earn a commission. ***See our ethics statement.***

Consider:

- What is differential privacy?
- How would you explain it to someone?
- Who do you need to explain it to?
- What do you need to explain to ensure that it is used correctly?
- What would you say to give the general intuition of it to <insert curious family member’s name here>

Intuition Example: Differential Privacy Intuition



Define, **what** is being protected, from **who**, and under what **conditions** this protection will hold.

Utility?

Communication?

Accessibility?

Usability?

Computation?

Hardware?

Intuition?

What does usability mean for cryptography???

This Security Trope…

People are the **weakest link** in the chain

Reject this Security Trope

People are the **weakest link** in the chain

– but it is **not that simple**, nor is that fair

Why Johnny Can’t Encrypt - 1999

Set the stage:

- We have crypto…
- We have crypto tools…
-

Whitten and Tygar. "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0." USENIX Security Symposium. 1999.

Why Johnny Can’t Encrypt - 1999

Set the stage:

- We have crypto…
- We have crypto tools…
- BUT, they’re **not really being used**…
  (by non-cryptographers)

Whitten and Tygar. "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0." USENIX Security Symposium. 1999.

Why Johnny Can't Encrypt - 1999

Set the stage:

- We have crypto…
- We have crypto tools…
- BUT, they're **not really being used**…
  (by non-cryptographers)

[PS] Why **Johnny Can't Encrypt**: A Usability Evaluation of PGP 5.0.

A Whitten, JD Tygar - USENIX security symposium, 1999 - usenix.org

User errors cause or contribute to most computer security failures, yet user interfaces for security still tend to be clumsy, confusing, or near-nonexistent. Is this simply due to a failure to …

☆ Save 99 Cite Cited by 2009 Related articles All 56 versions »

Whitten and T

Why Johnny Can't Encrypt - 1999

Set the stage:

- We have crypto…
- We have crypto tools…
- BUT, they're not really being used…(by non-cryptographers)

Only a handful of related work…

Whitten and Tygar. "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0." USENIX Security Symposium. 1999.

Why Johnny Can't Encrypt - 1999

Set the stage:

- We have crypto…
- We have crypto tools…
- BUT, they're not really being used…(by non-cryptographers)

Only a handful of related work…

Only one notion of usability across them…

Whitten and Tygar. "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0." USENIX Security Symposium. 1999.

Why Johnny Can't Encrypt - 1999

Set the stage:

- We have crypto…
- We have crypto tools…
- BUT, they're not really being used…(by non-cryptographers)

Only a handful of related work…

Only one notion of usability across them…

"Usability necessarily has different meanings in different contexts"

Whitten and Tygar. "W

Usability - 1999

“Usability necessarily has different meanings in different contexts”

“For some, **efficiency may be a priority**, for others, learnability, for still others, flexibility. In a security context, our priorities must be whatever is needed in order for the security to be used effectively.”

Whitten and Tygar. "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0." USENIX Security Symposium. 1999.

Usability - 1999

“Usability necessarily has different meanings in different contexts”

“For some, efficiency may be a priority, for others, **learnability**, for still others, flexibility. In a security context, our priorities must be whatever is needed in order for the security to be used effectively.”

Whitten and Tygar. "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0." USENIX Security Symposium. 1999.

Usability - 1999

“Usability necessarily has different meanings in different contexts”

“For some, efficiency may be a priority, for others, learnability, for still others, **flexibility**. In a security context, our priorities must be whatever is needed in order for the security to be used effectively.”

Whitten and Tygar. "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0." USENIX Security Symposium. 1999.

Usability - 1999

“Usability necessarily has different meanings in different contexts”

“For some, efficiency may be a priority, for others, learnability, for still others, flexibility. **In** a **security** context, our priorities must be **whatever is needed in order for the security to be used effectively.**”

Whitten and Tygar. "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0." USENIX Security Symposium. 1999.

Definition (1999)

Security software is usable if the people who are expected to use it:

- are reliably made aware of the security tasks they need to perform
- are able to figure out how to successfully perform those tasks
- don’t make dangerous errors are sufficiently comfortable with the interface to continue using it

Whitten and Tygar. "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0." USENIX Security Symposium. 1999.

Definition (1999)

Security software is usable if the people who are expected to use it:

- are reliably made aware of the security tasks they need to perform
- are able to figure out how to successfully perform those tasks
- don't make dangerous errors are sufficiently comfortable with the interface to continue using it

How can we improve this?

Whitten and Tygar. "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0." USENIX Security Symposium. 1999.

Challenges (1999)

Claim: Security has some inherent properties that make it a difficult problem domain for user interface design.

Whitten and Tygar. "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0." USENIX Security Symposium. 1999.

Challenges (1999)

Claim: Security has some inherent properties that make it a difficult problem domain for user interface design.

What do you think they are (were)?

Whitten and Tygar. "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0." USENIX Security Symposium. 1999.

Challenges (1999)

Claim: Security has some inherent properties that make it a difficult problem domain for user interface design.

- The unmotivated user property
- The abstraction property
- The lack of feedback property
- The barn door property
- The weakest link property

Whitten and Tygar. "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0." USENIX Security Symposium. 1999.

Challenges (1999)

Claim: Security has some inherent properties that make it a difficult problem domain for user interface design.

- The unmotivated user property
- The abstraction property
- The lack of feedback property
- The barn door property
- The weakest link property

Task: make computer security usable for people who are not already knowledgeable in that area

Whitten

(Many) Descendents and Branches after Johnny

Finally johnny can encrypt: But does this make him feel more secure?
N Gerber, V Zimmermann, B Henhapl… - Proceedings of the 13th …, 2018 - dl.acm.org
… of E2E **encryption** by non-experts in the email context. An oftenquoted example is the paper '… **Johnny can't encrypt**' [33] as well as subsequent studies on the usability of E2E **encryption** …
☆ Save 99 Cite Cited by 34 Related articles All 4 versions

Teaching Johnny not to fall for phish
P Kumaraguru, S Sheng, A Acquisti, LF Cranor… - ACM Transactions on …, 2010 - dl.acm.org
Phishing attacks, in which criminals lure Internet users to Web sites that spoof legitimate Web sites, are occurring with increasing frequency and are causing considerable harm to victims…
☆ Save 99 Cite Cited by 563 Related ar

Leading Johnny to water: Designing for usability and trust
E Atwater, C Bocovich, U Hengartner, E Lank… - … Symposium On Usable …, 2015 - usenix.org
Although the means and the motivation for securing private messages and emails with strong end-to-end encryption exist, we have yet to see the widespread adoption of existing …
☆ Save 99 Cite Cited by 76 Related articles All 3 versions »

Branches Following Engineering Style Challenges

“PGP 5.0 alerts its users to this compatibility issue…it uses different icons to depict the different key types…”

- NIST (and other) standardization processes
- Tools, libraries, etc…
- Improving intuition of icons (browsers, mobile…)

L. Cranor, Potty Talk at PEPR 2021, https://youtu.be/s4cS5Tqnemo

Branches Following the Visual Metaphors

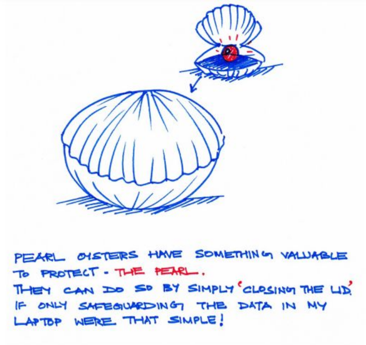


Fig. 62. "Pearl oysters have something valuable to protect - the pearl. They can do so by simply 'closing the lid.' If only safeguarding the data in my laptop were that simple!" By Sharon, age 25.

Fig. 33. "Privacy means that the thoughts in my brain are locked away. What I know does not have to go into the world, which I put an X over." By Thomas, age 19

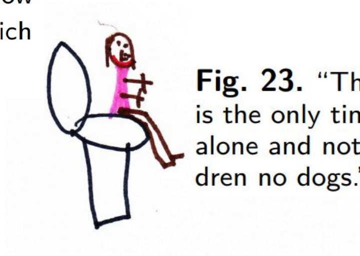


Fig. 23. "This is me enjoying my privacy. This is the only time during the day, were I am truly alone and nothing bothers me. No man no children no dogs." By Cindy, age 54

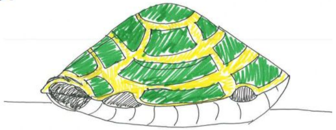


Fig. 24. "No one come in when I am in the bathroom!" By Sydney, age 7

M. Oates, et al. Turtles, locks, and bathrooms: Understanding mental models of privacy through illustration." Proceedings on Privacy Enhancing Technologies 2018.

The Branches Towards Usable Cryptography

- Ceremony analysis
- (Novel and Nuanced) threat models
- Human Computer Interaction (HCI) studies
- Software engineering (tooling)

The Principle of Psychological Acceptability

" It is essential that the human interface be **designed for ease of use**, so that users routinely and automatically **apply the protection mechanisms correctly**."

- Jerome Saltzer and Michael Schroeder

J. Saltzer and Michael Schroeder. "The Protection of Information in Computer Systems", Proceedings of the IEEE 63:0. 1975

Important

Theoretical Cryptography?

Applied Cryptography?

Deployable Cryptography?

Question the Assumptions of the Motivation

Private set intersection as “good” for:

- Ad conversion
- Security incident information sharing
- Contact discovery

Pattern of the claims made:

- Just send it (bad)
- Just hash it (bad)
- Just PSI this (good)

We can do better

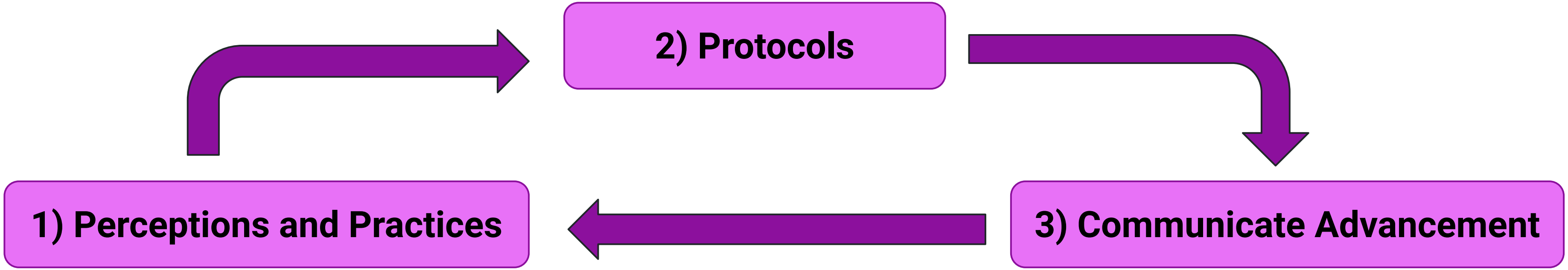
Core ideas for the remainder if today

- Humans (ceremony analysis) towards ensuring the cryptographic guarantees are preserved

- Human-centered design – to ensure we design the right cryptography

For developing cryptography.

Human-Centered Design



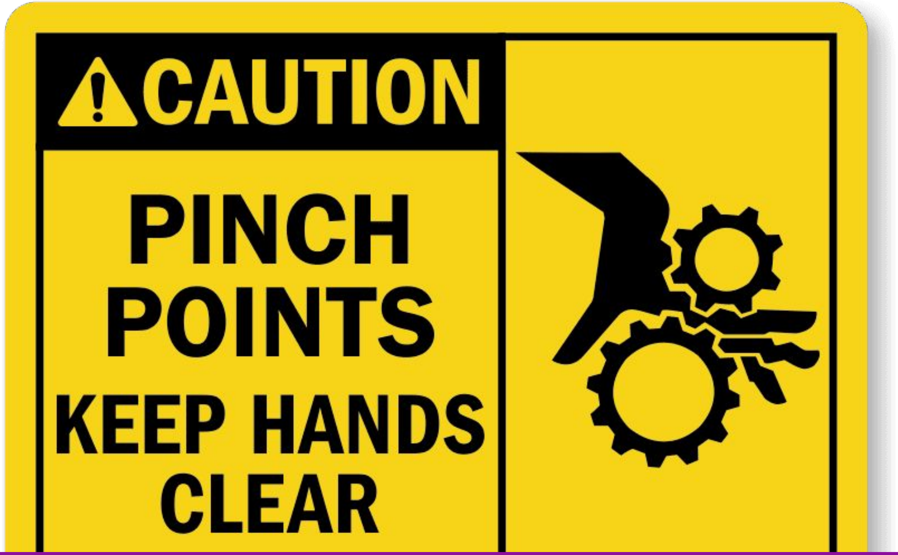
"...that aims to make systems usable and useful by **focusing on the users, their needs and requirements**, ... counteracts possible adverse effects of use..." - ISO 9241-210:2019(E)

Our First Example: Finding Pinch Points

Ceremony Analysis and Secret Sharing

B. Kacsmar, C. H. Komlo, F. Kerschbaum, and I. Goldberg. "Mind the Gap: Ceremonies for Applied Secret Sharing." Proc. Privacy Enhancing Technologies (PoPETs). 2020.

Pinch Points?



Def: When objects come together and there is a possibility that a person could be caught or injured

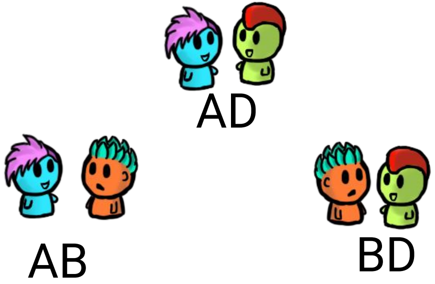
Image source: https://www.constructionsafety.co.za/ems/pinch-points/

Common Causes of Pinch Points?

- Lack of attention…
- Mobility (of equipment)
- Poor maintenance
- Lack of proper safe work procedures
- Reaching into moving points…

Secret Sharing: (t, n) - Threshold Schemes

Document



(2, 3) - Threshold Scheme

Secret s

Size n group

Threshold t

A. Shamir. (1979). How to share a secret. Communications of the ACM, 22(11), 612-613.

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

Ceremony Analysis

- The concept of **ceremony** is introduced as **an extension** of the concept **of network protocols**
- **Human nodes** alongside computer nodes
- The communication links include **UI**, **human-to-human communication,** and **transfers of physical objects** that carry data

C. Ellison. (2007). Ceremony design and analysis. Cryptology EPrint Archive.

(A Version) of TLS Protocol Flow

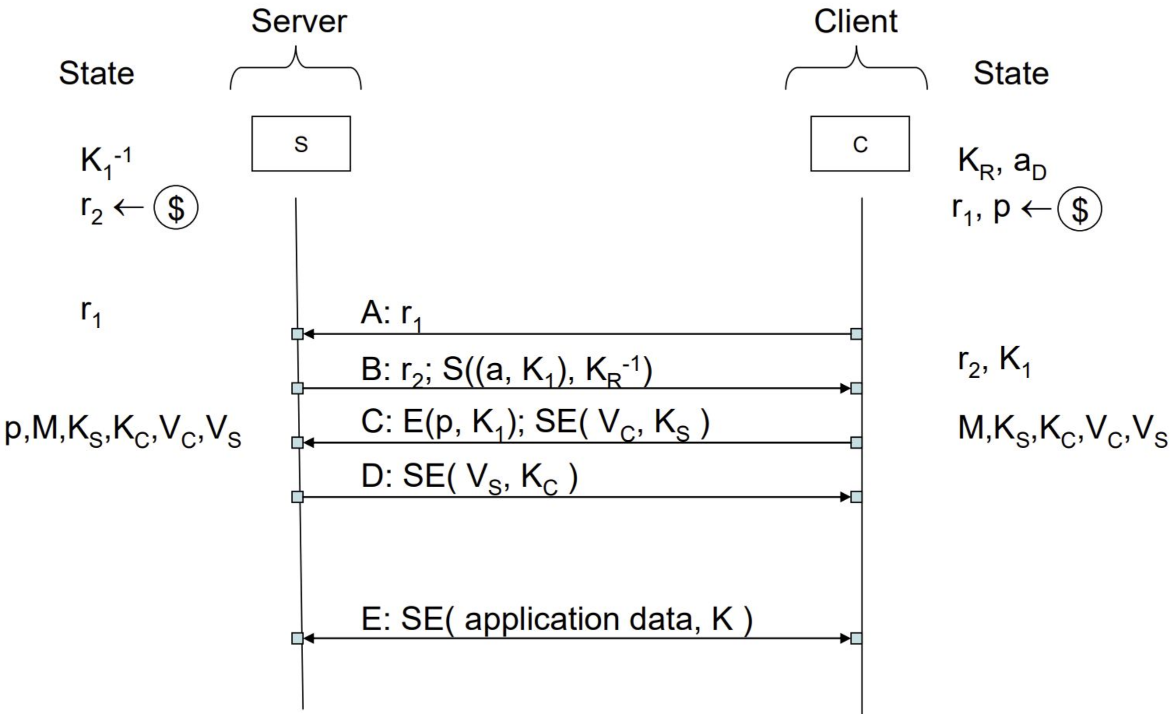


Figure 1 from C. Ellison. (2007). Ceremony design and analysis. Cryptology EPrint Archive.

(A Version) of HTTPS Ceremony

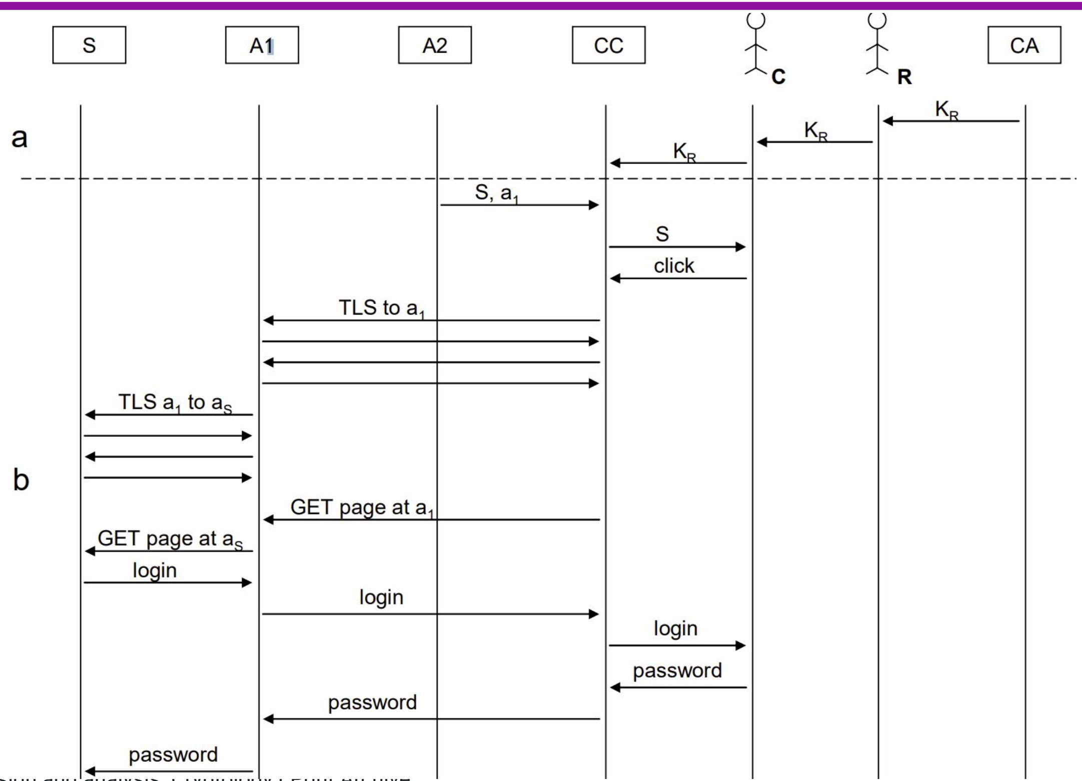
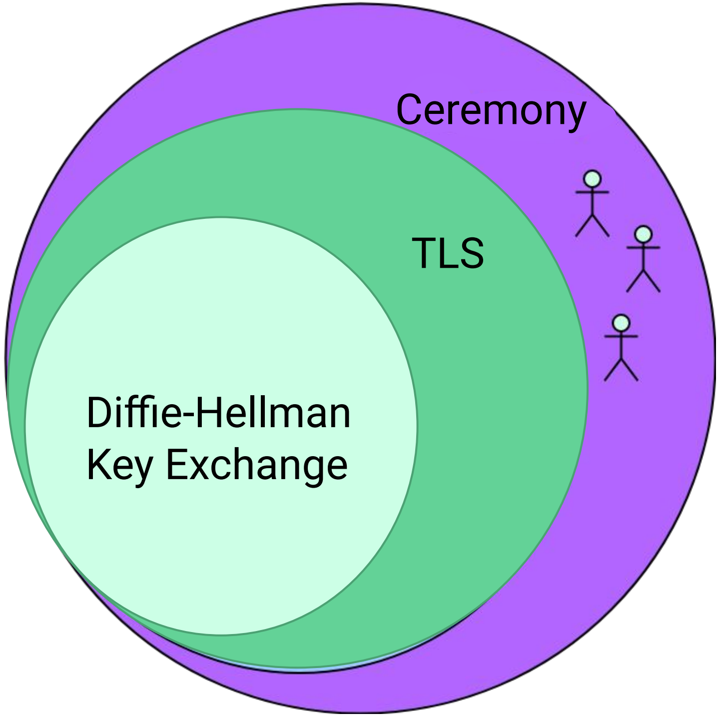


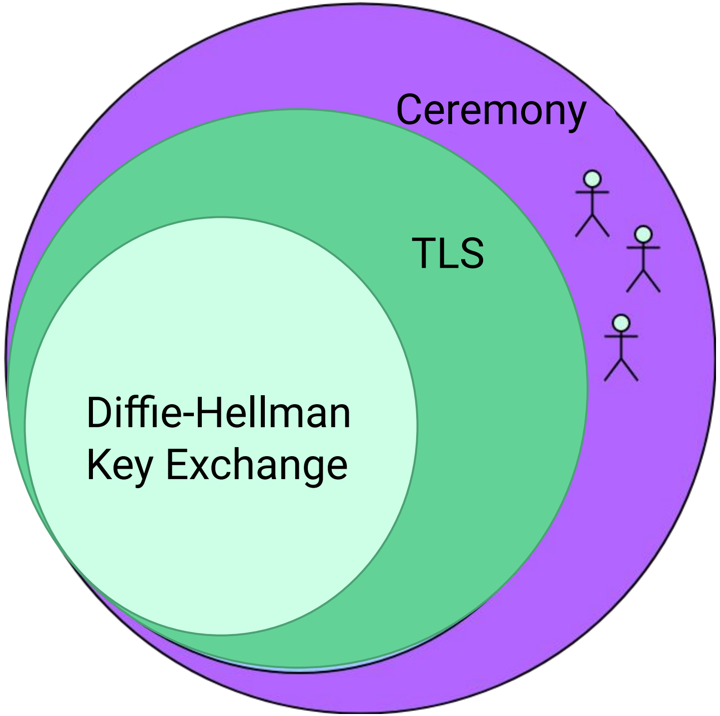
Figure 2 from C. Ellison. (2007). Ceremony design and analysis. Cryptology EPrint Archive.

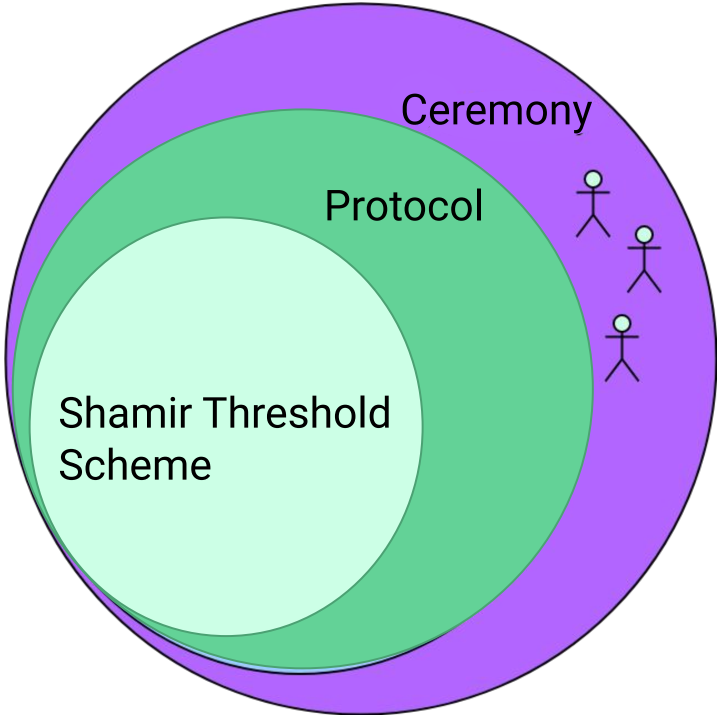
Ceremonies and Secret Sharing



C. Ellison. (2007). Ceremony design and analysis. Cryptology EPrint Archive.

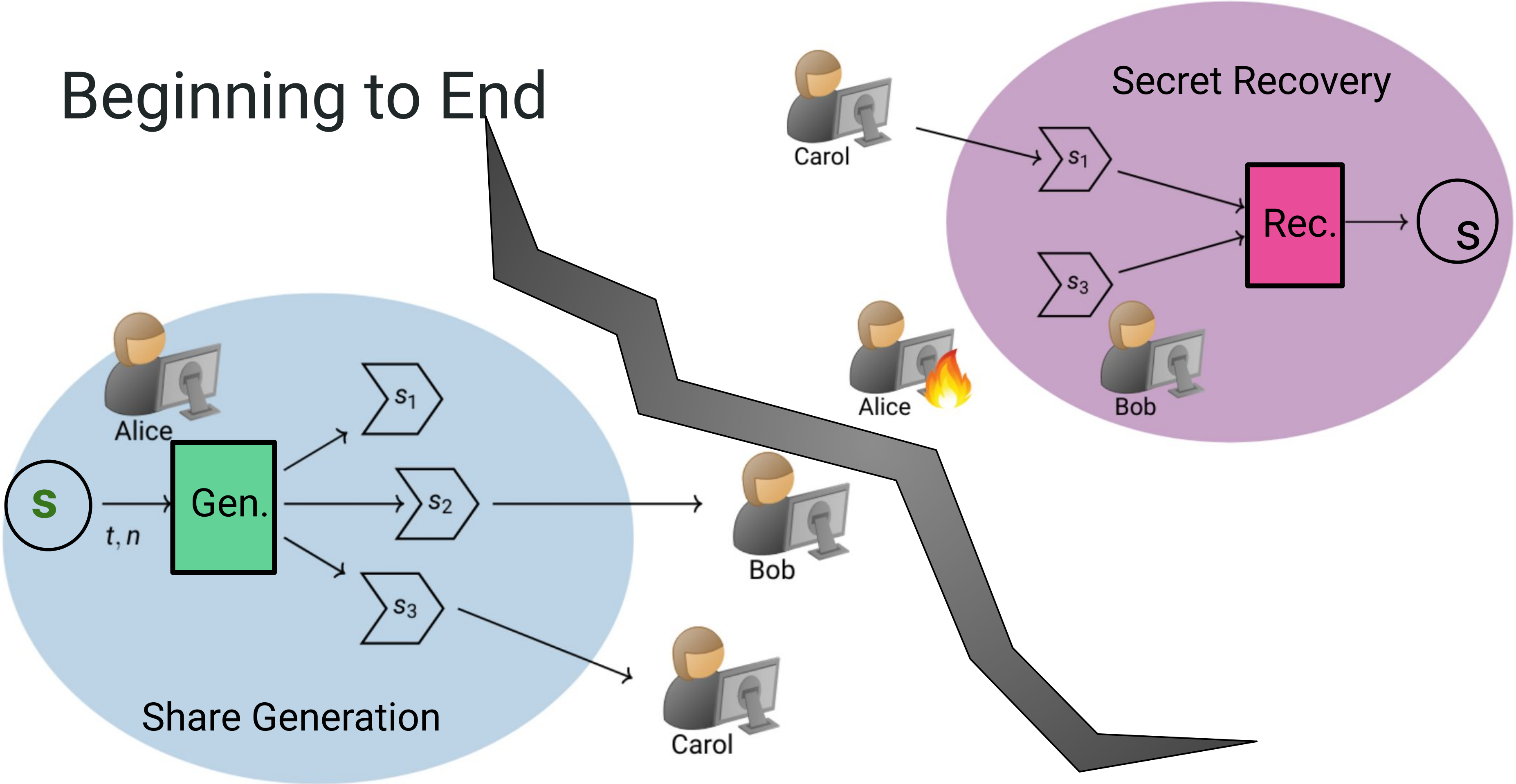
Ceremonies and Secret Sharing





C. Ellison. (2007). Ceremony design and analysis. Cryptology EPrint Archive.

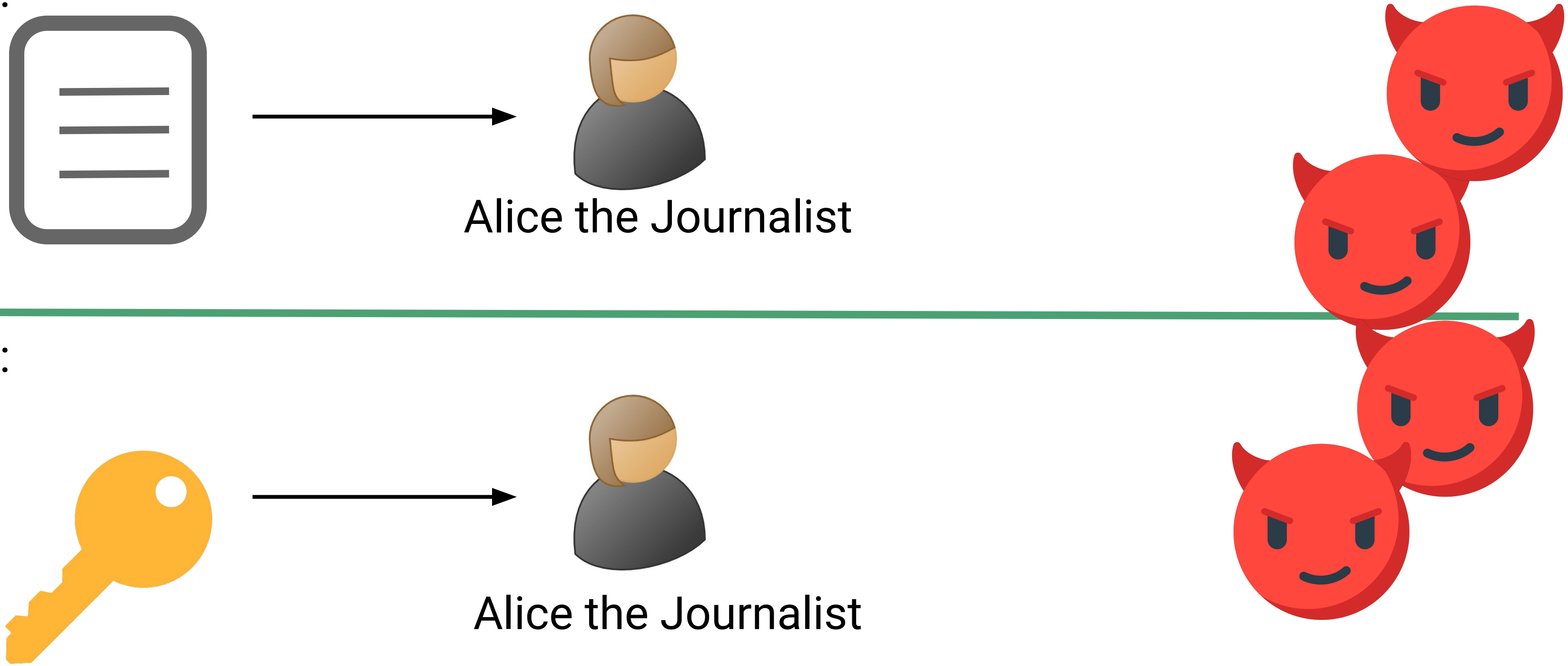
Beginning to End



Before the Beginning

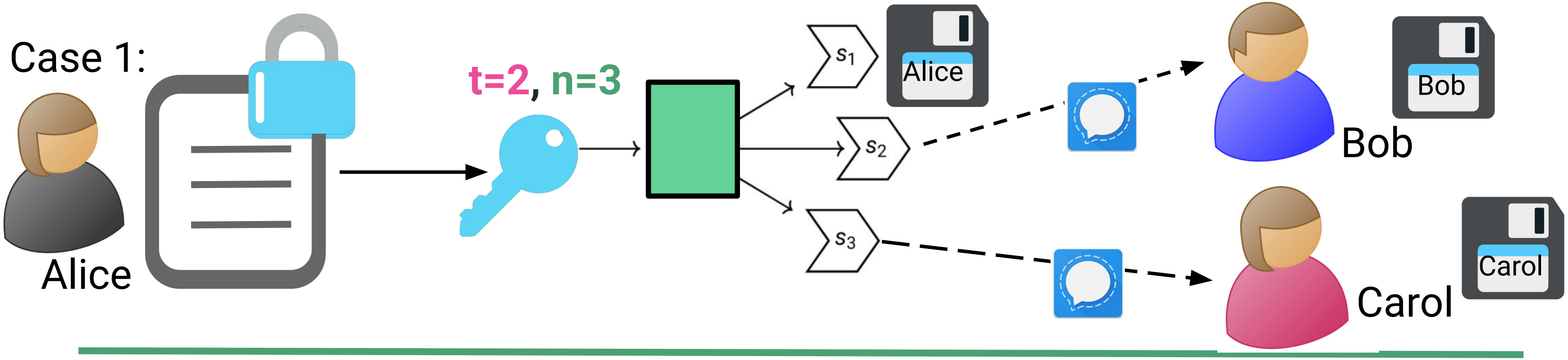
Case 1:

Case 2:



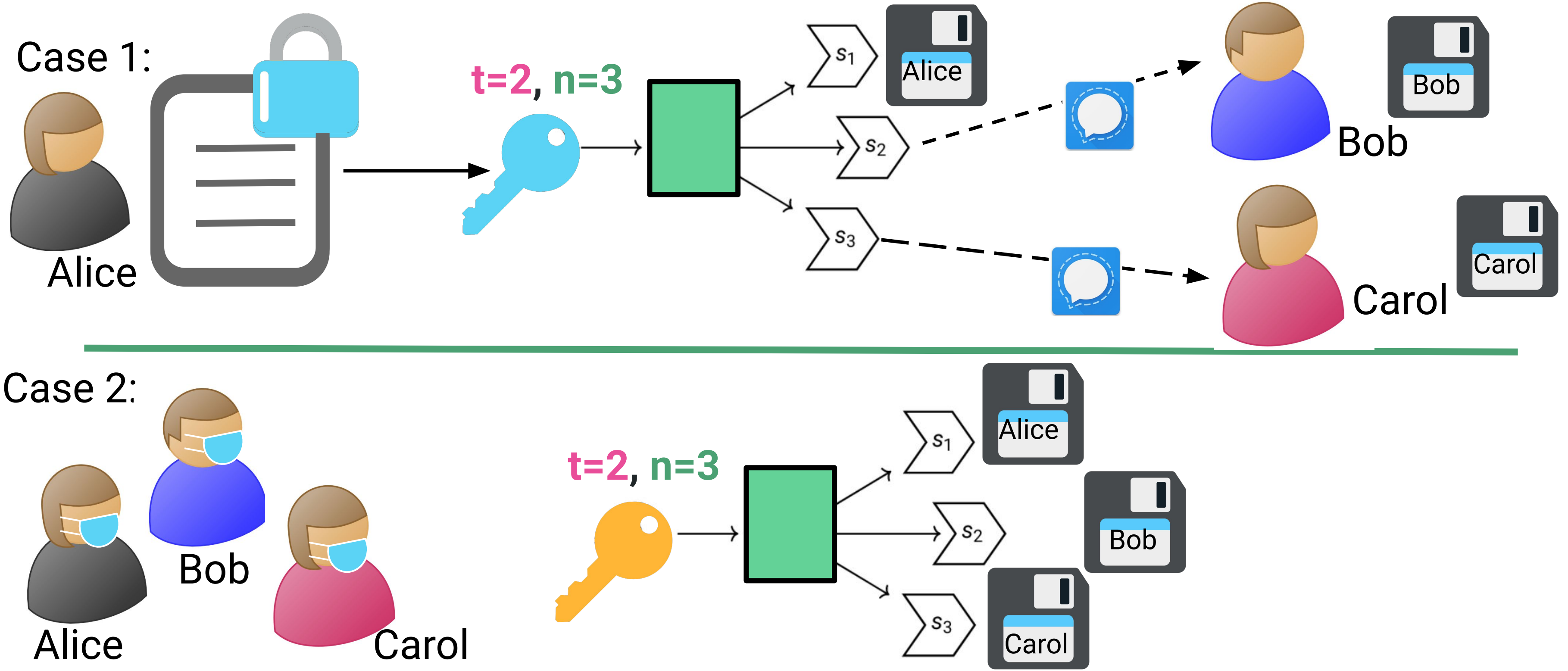
Share Generation

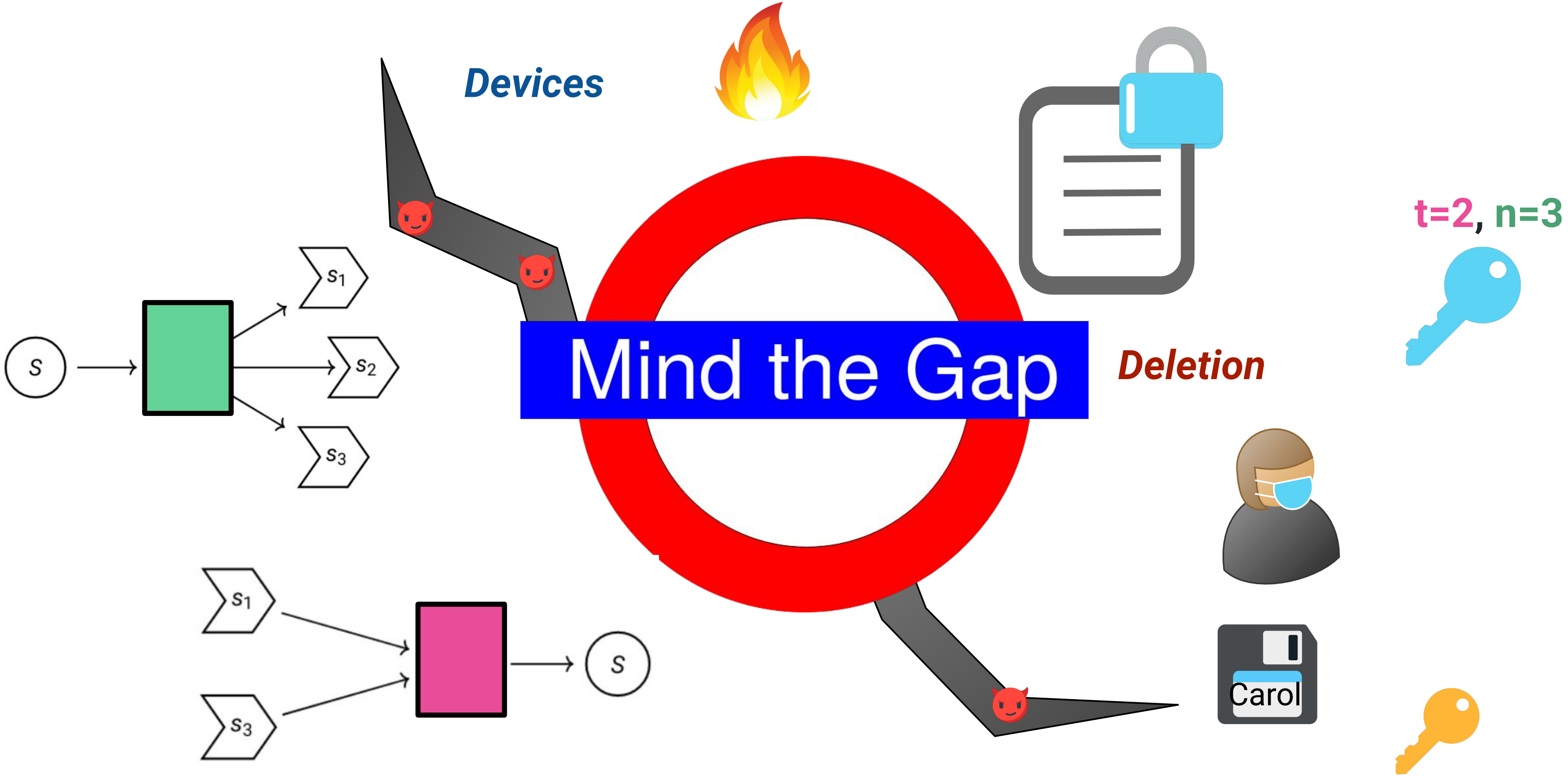
Case 1:



Case 2:

Share Generation




Devices
s
s_1
s_2
s_3
s_1
s_3
s
Mind the Gap
Deletion
t=2, n=3
Carol

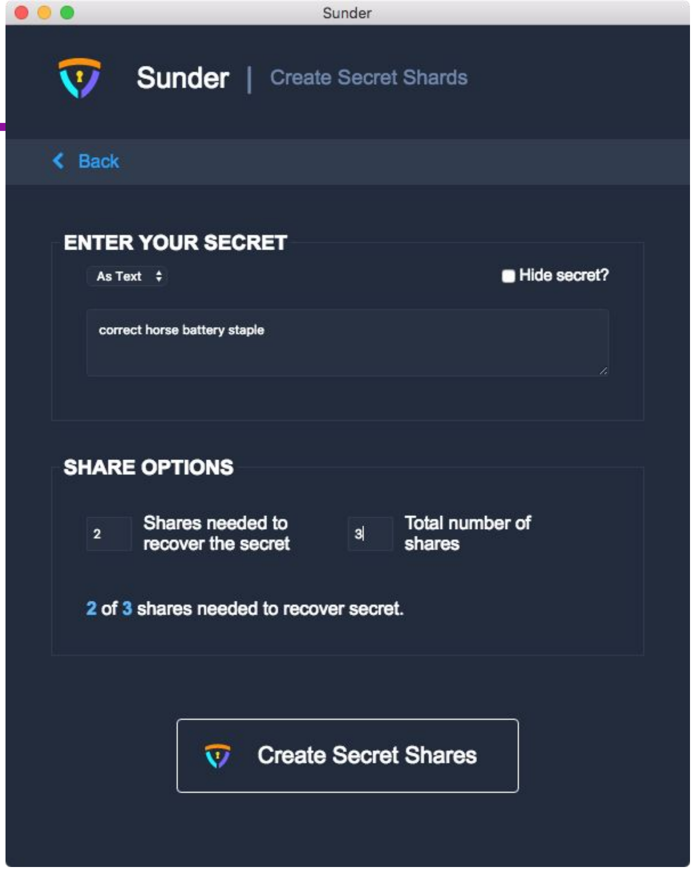
Secret Sharing Ceremony Analysis Framework

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

B. Kacsmar, C. H. Komlo, F. Kerschbaum, and I. Goldberg. "Mind the Gap: Ceremonies for Applied Secret Sharing." Proc. Privacy Enhancing Technologies (PoPETs). 2020.

Case Study: Sunder

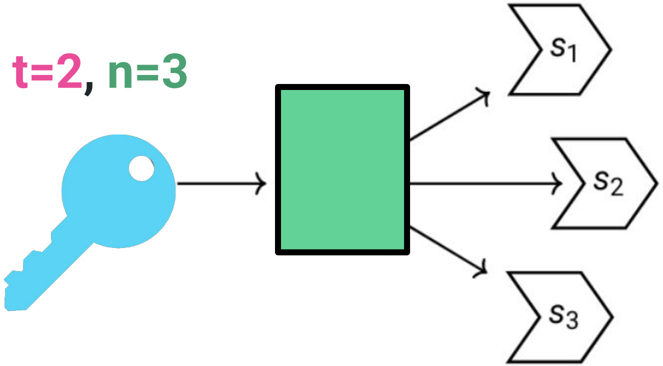
- A tool from Freedom of the Press for journalists
- Implements Shamir secret sharing
- Support for share integrity
- (Some) support for Base and Extended modes

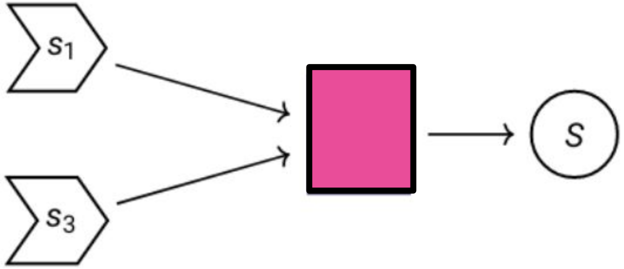


B. Kacsmar, C. H. Komlo, F. Kerschbaum, and I. Goldberg. "Mind the Gap: Ceremonies for Applied Secret Sharing." Proc. Privacy Enhancing Technologies (PoPETs). 2020.

Sunder Stages and Modes

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

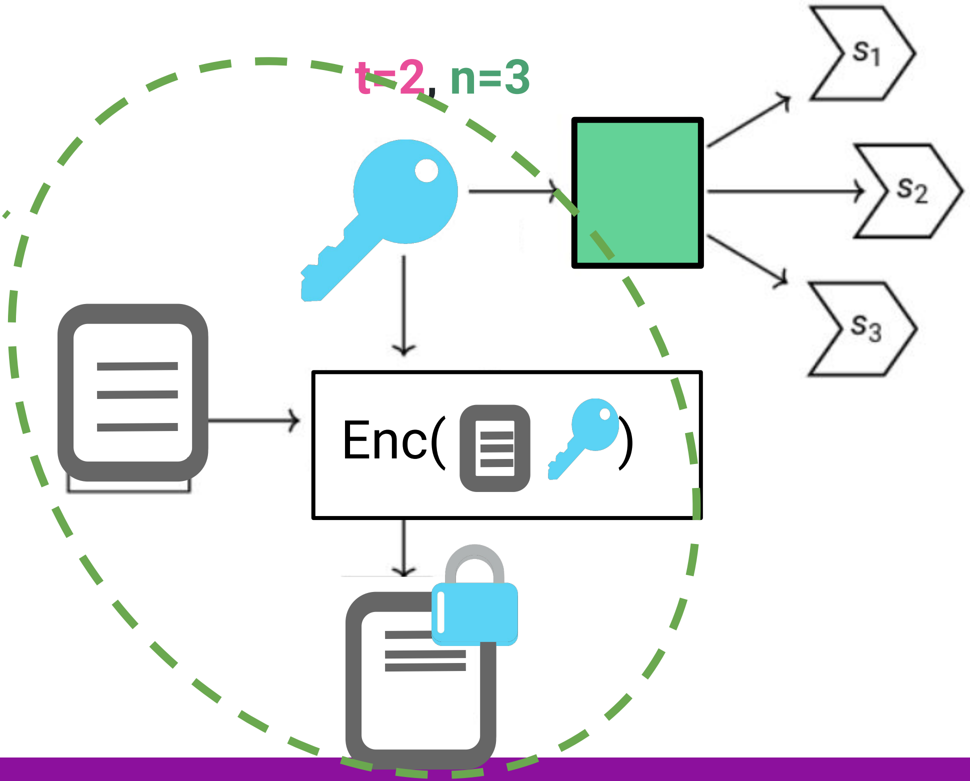




B. Kacsmar, C. H. Komlo, F. Kerschbaum, and I. Goldberg. "Mind the Gap: Ceremonies for Applied Secret Sharing." Proc. Privacy Enhancing Technologies (PoPETs). 2020.

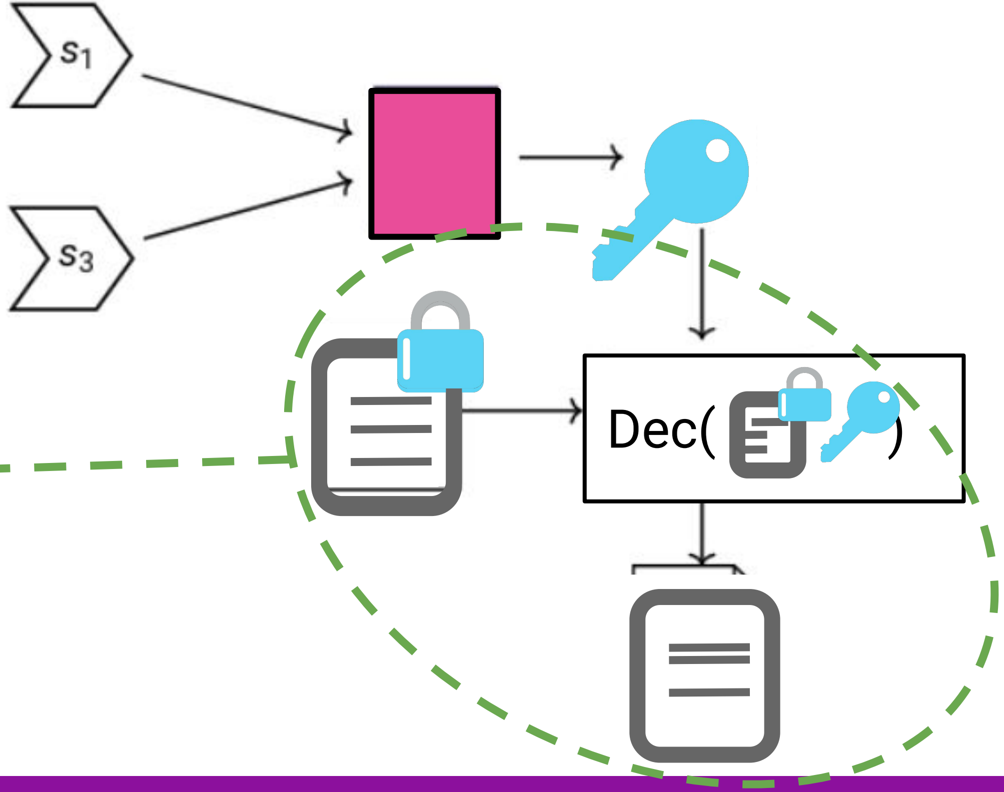
Sunder Stages and Modes

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

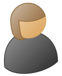


Sunder Stages and Modes

- → 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

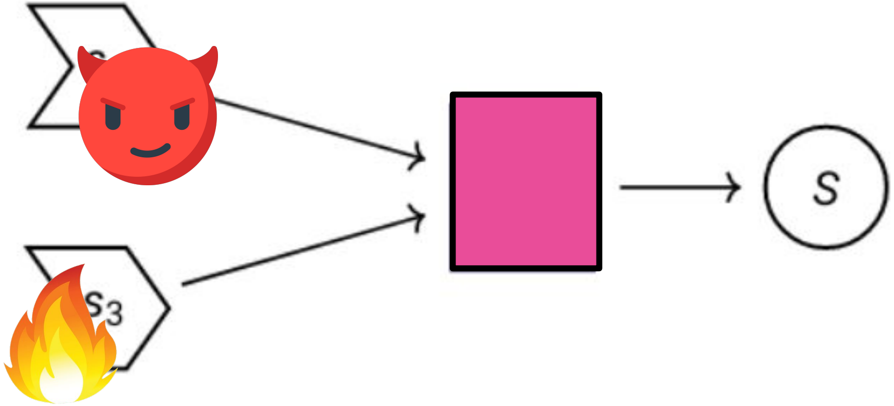
Sunder Ceremony Evaluation

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

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

Threats to Secret Reconstruction

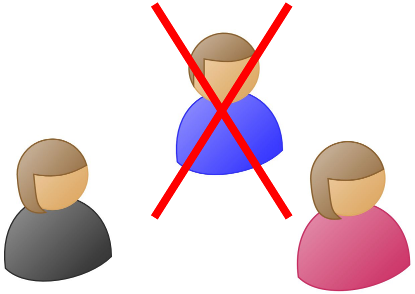
1. Alice leaving the organization
2. A share being damaged
3. A share being stolen
4. The device storing the encrypted files is destroyed



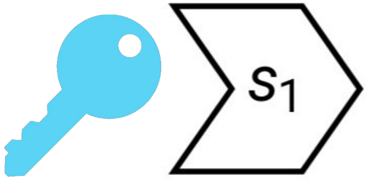
Idea!! Lightweight Proactive VSS

Adds three new stages:

- → Share Update
- → Share Validate
- → Generate Commitment



Access Revocation via Updates



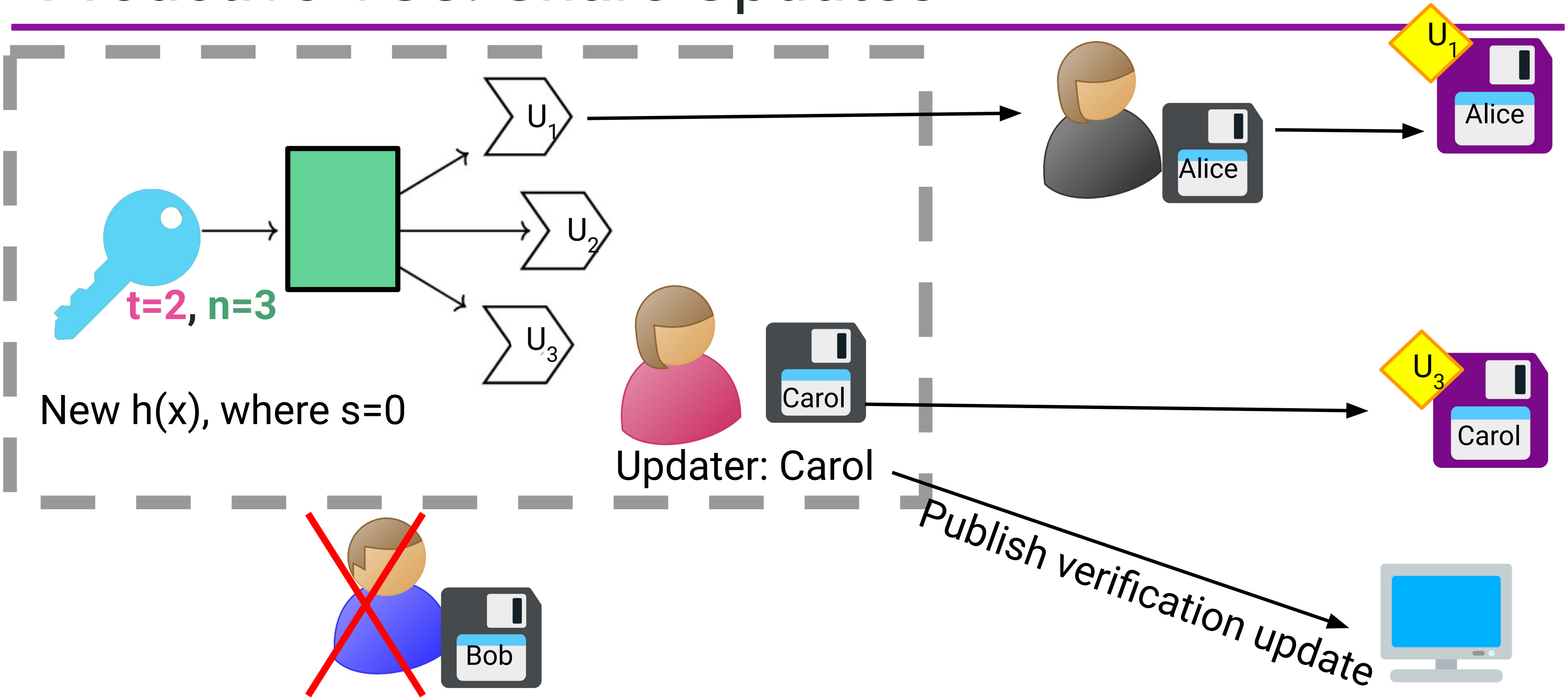
Verification of Share Integrity and File Integrity

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

B. Kacsmar, C. H. Komlo, F. Kerschbaum, and I. Goldberg. "Mind the Gap: Ceremonies for Applied Secret Sharing." Proc. Privacy Enhancing Technologies (PoPETs). 2020.

Proactive VSS: Share Updates



Lightweight Improvements Comparison

	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	○	○	○	○	●	●	●	●

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

Take this Home

- Variations in the ceremony can lead to changes in the fundamental security properties provided to end users
- Ceremonies 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

Our Second Example: Finding Design Failures

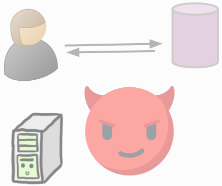
HCI and PSI

Kacsmar, Duddu, Tilbury, Ur, and Kerschbaum. Comprehension from Chaos: Towards Informed Consent for Private Computation. *2023 ACM SIGSAC Conference on Computer and Communications Security* (CCS).

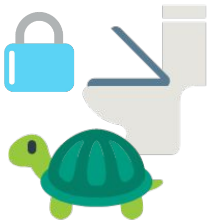
Some more risks of failing usability for cryptography?

What about usability for <u>your</u> cryptography?

A Wider View of Technical Privacy

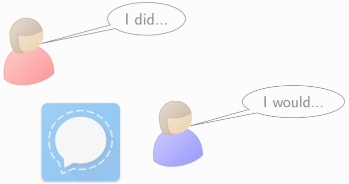


Technical Privacy



Conceptual Privacy

Legal Privacy



Usable Privacy

Understanding privacy notions and behaviours, **right to privacy**, and privacy expectations

M. Oates, et al. Turtles, locks, and bathrooms: Understanding mental models of privacy through illustration." Proceedings on Privacy Enhancing Technologies 2018.

Cryptography from Research Papers to Products

- What **steps** are involved in adopting cryptography, and who are the **relevant stakeholders**?
- What are the **key obstacles** hindering the widespread **adoption** and **correct use** of cryptography?
- What are potential ways to **overcome** these obstacles?

K. Fischer, I. Trummová, P. Gajland, Y. Acar, S. Fahl, & A. Sasse. “The Challenges of Bringing Cryptography from Research Papers to Products: Results from an Interview Study with Experts”. Usenix Security Symposium 2024

A Path from Research Papers to Products

1. Algorithm and Protocol Development
2. Standardization
3. Secure Implementation (Cryptography Libraries)
4. Product Development
5. Adoption and Use of Cryptographic Products

K. Fischer, I. Trummová, P. Gajland, Y. Acar, S. Fahl, & A. Sasse. “The Challenges of Bringing Cryptography from Research Papers to Products: Results from an Interview Study with Experts”. Usenix Security Symposium 2024

A Visualization of the Cryptography Ecosystem

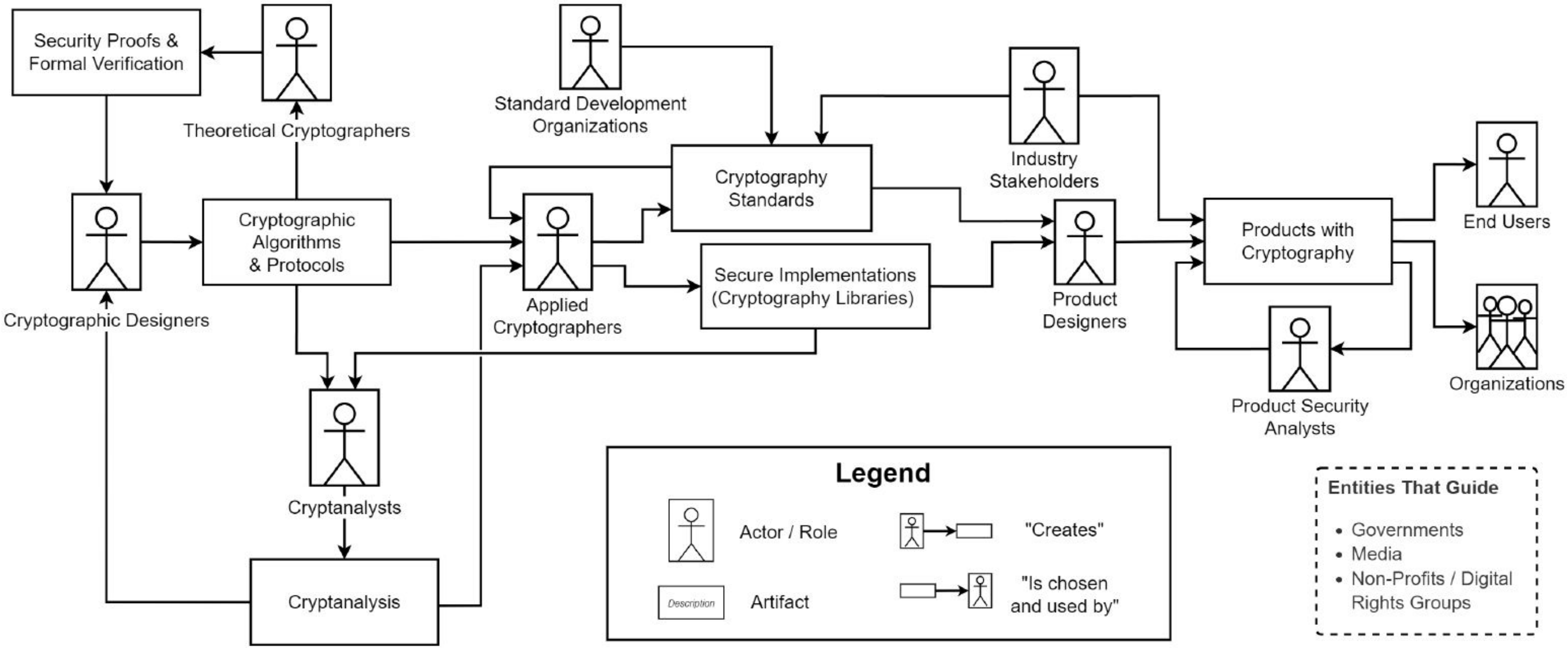


Figure 2 from: K. Fischer, I. Trummová, P. Gajland, Y. Acar, S. Fahl, & A. Sasse. “The Challenges of Bringing Cryptography from Research Papers to Products: Results from an Interview Study with Experts”. Usenix Security Symposium 2024

A Visualization of the Cryptography Ecosystem

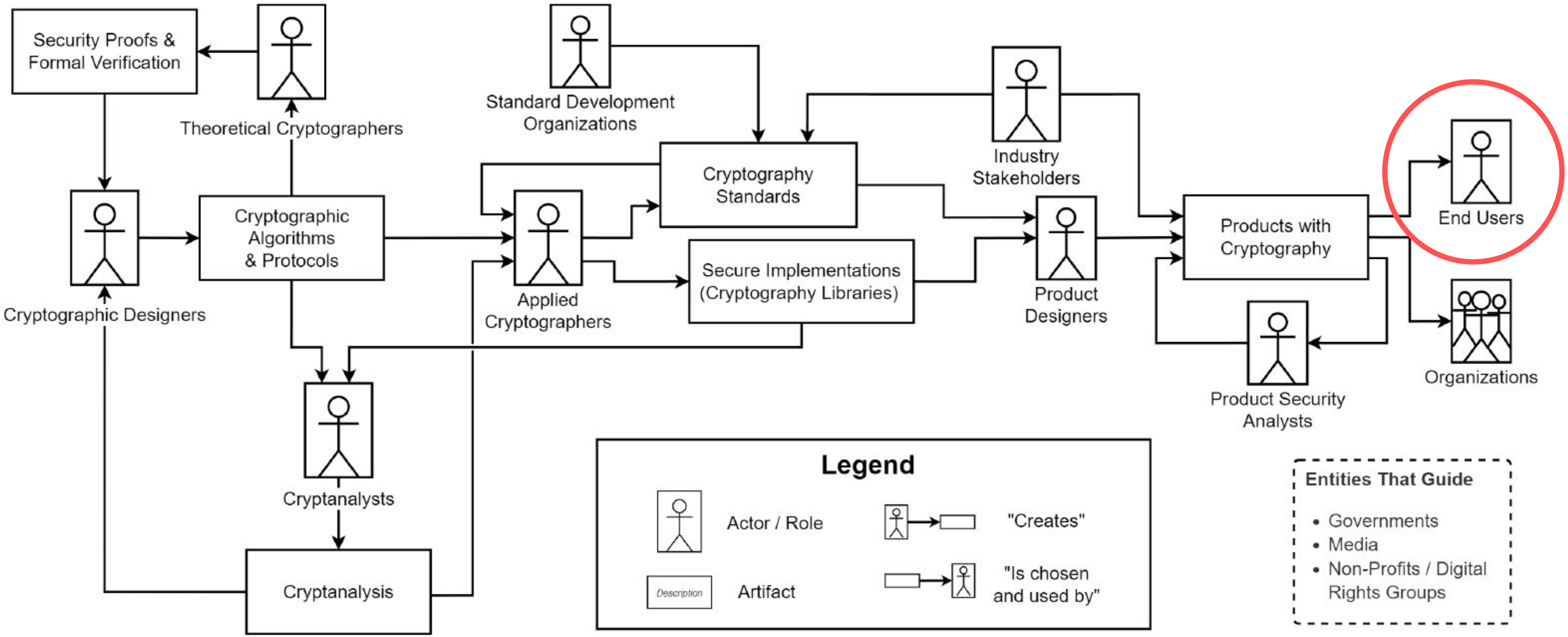


Figure 2 from: K. Fischer, I. Trummová, P. Gajland, Y. Acar, S. Fahl, & A. Sasse. "The Challenges of Bringing Cryptography from Research Papers to Products: Results from an Interview Study with Experts". Usenix Security Symposium 2024

A Visualization of the Cryptography Ecosystem

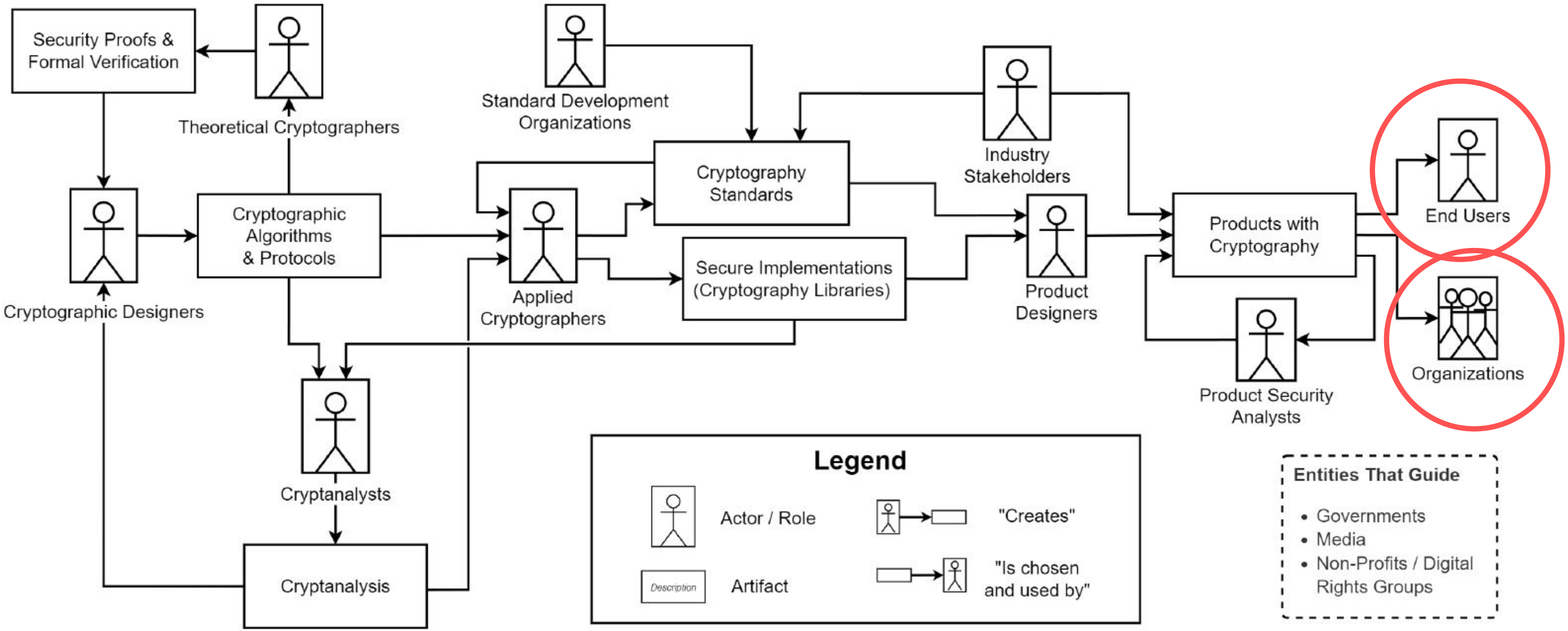


Figure 2 from: K. Fischer, I. Trummová, P. Gajland, Y. Acar, S. Fahl, & A. Sasse. “The Challenges of Bringing Cryptography from Research Papers to Products: Results from an Interview Study with Experts”. Usenix Security Symposium 2024

A Visualization of the Cryptography Ecosystem

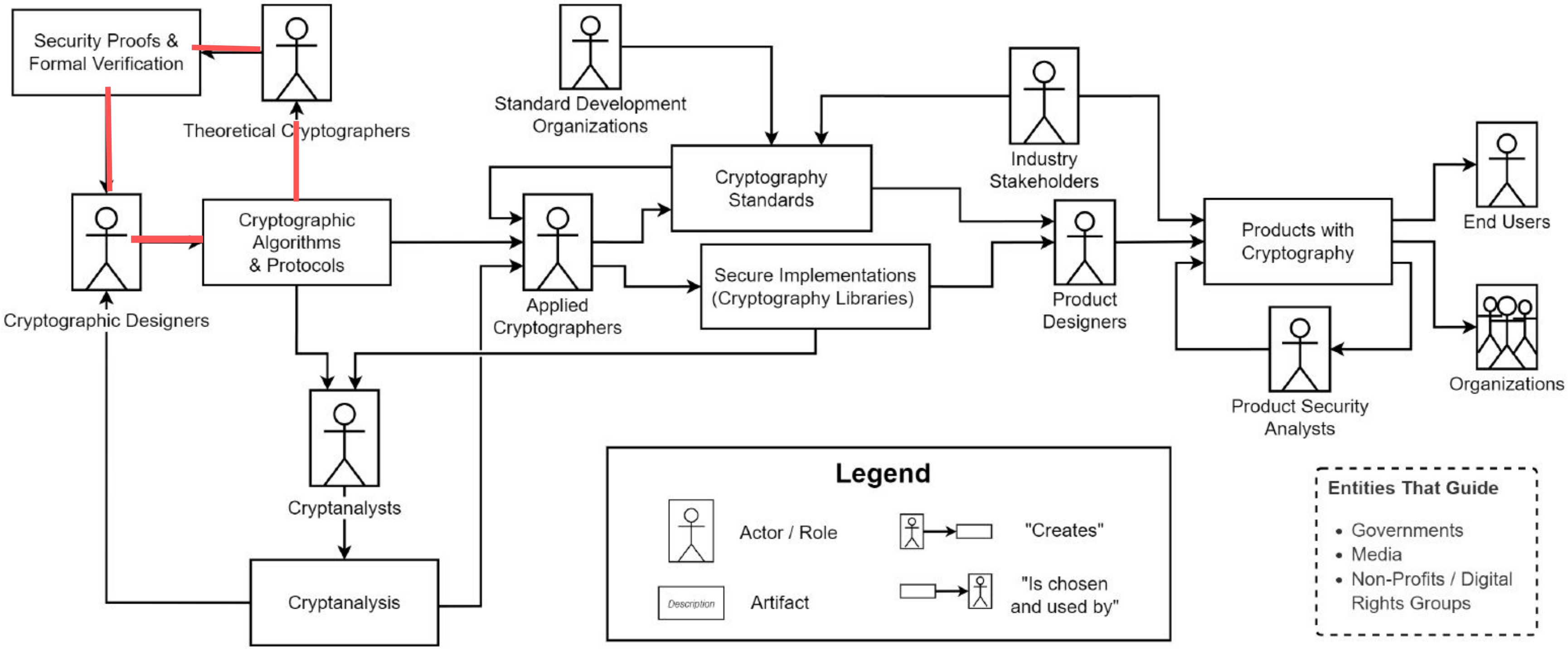


Figure 2 from: K. Fischer, I. Trummová, P. Gajland, Y. Acar, S. Fahl, & A. Sasse. “The Challenges of Bringing Cryptography from Research Papers to Products: Results from an Interview Study with Experts”. Usenix Security Symposium 2024

A Visualization of the Cryptography Ecosystem

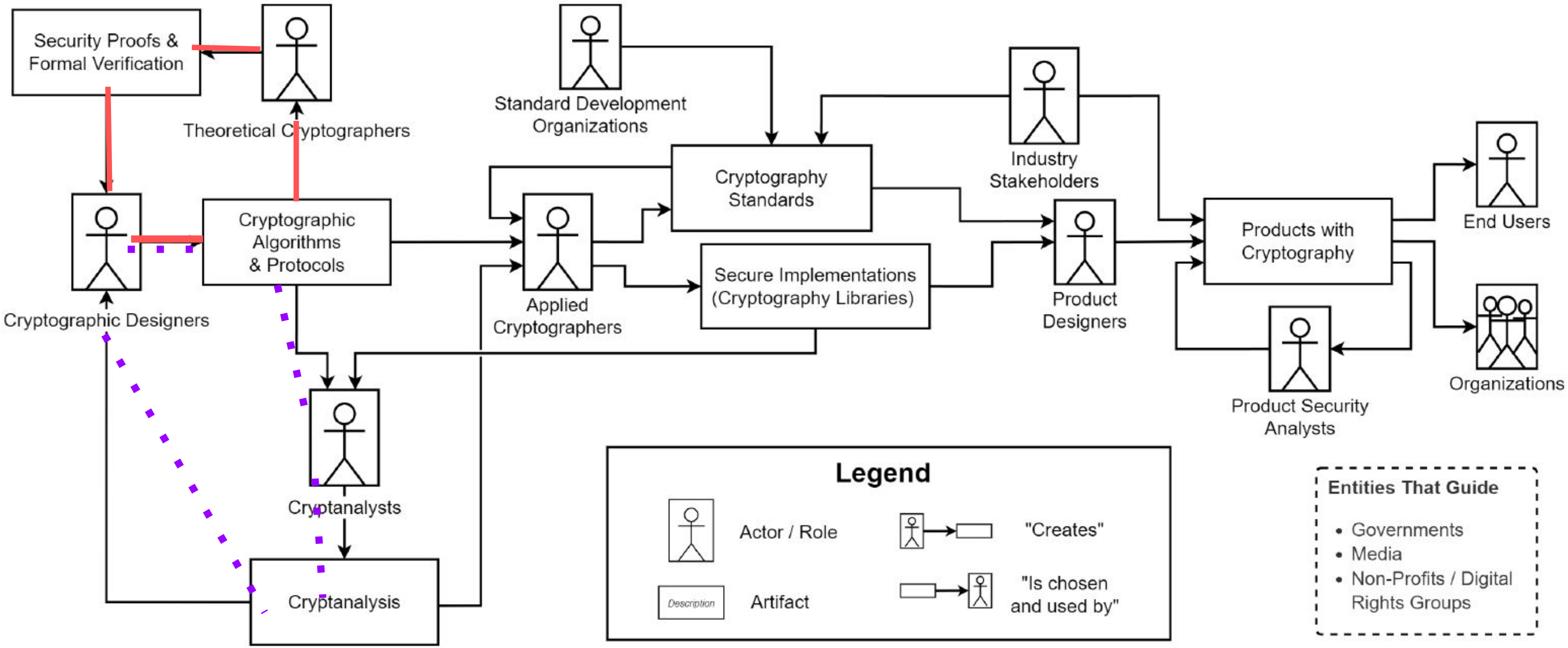


Figure 2 from: K. Fischer, I. Trummová, P. Gajland, Y. Acar, S. Fahl, & A. Sasse. "The Challenges of Bringing Cryptography from Research Papers to Products: Results from an Interview Study with Experts". Usenix Security Symposium 2024

A Visualization of the Cryptography Ecosystem

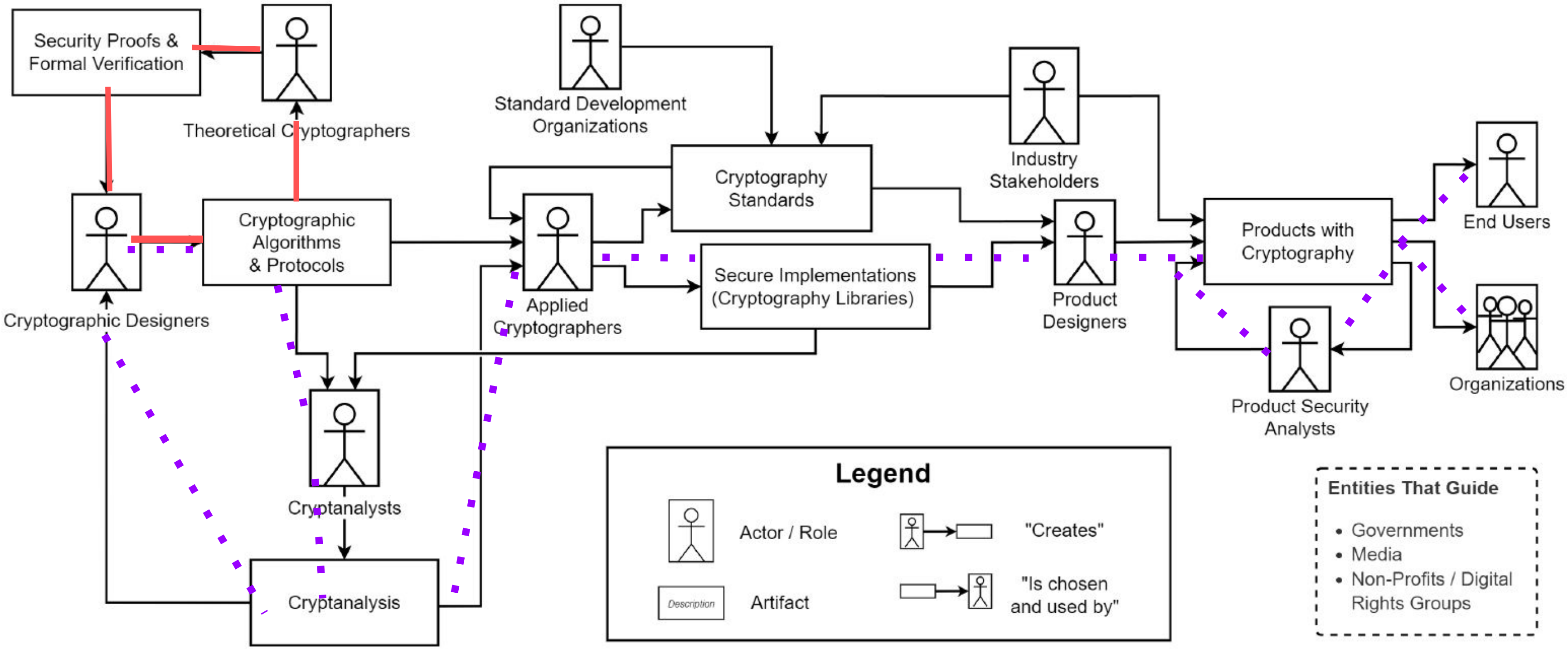
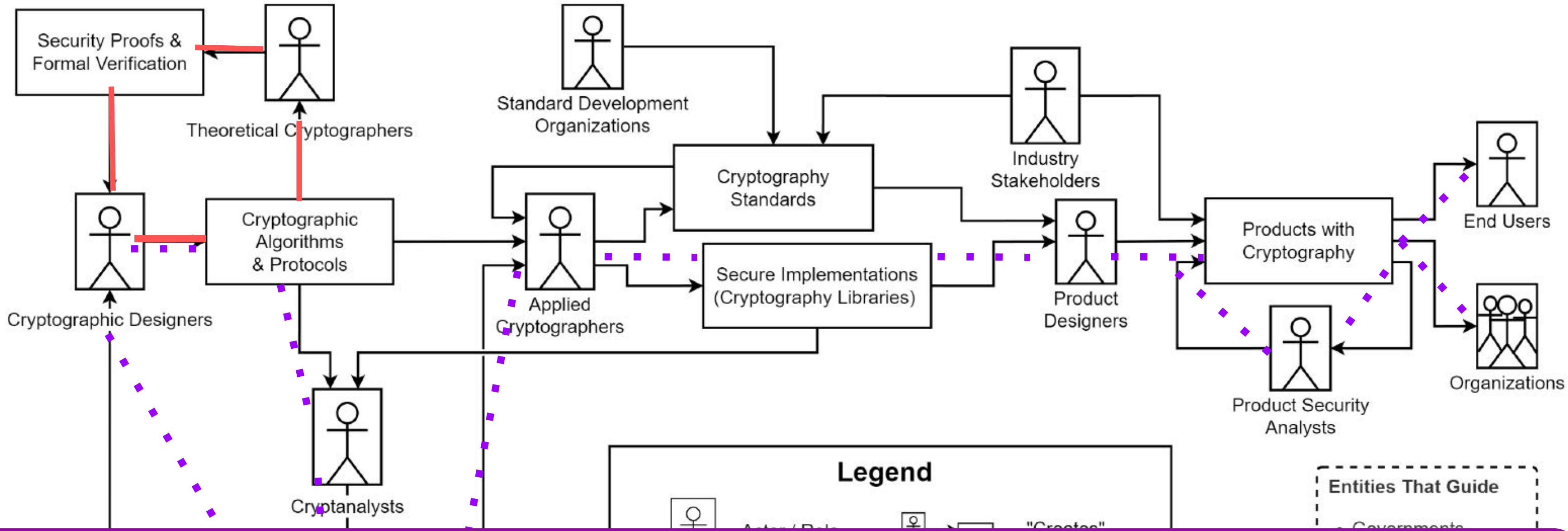


Figure 2 from: K. Fischer, I. Trummová, P. Gajland, Y. Acar, S. Fahl, & A. Sasse. "The Challenges of Bringing Cryptography from Research Papers to Products: Results from an Interview Study with Experts". Usenix Security Symposium 2024

A Visualization of the Cryptography Ecosystem



Question: Can we agree this is a problem?

Figure 2 from: K. Fischer, I. Trummova, P. Gajland, Y. Acar, S. Fahl, & A. Sasse. "The Challenges of Bringing Cryptography from Research Papers to Products: Results from an Interview Study with Experts". Usenix Security Symposium 2024

Diverging (Expert) Views

K. Fischer, I. Trummová, P. Gajland, Y. Acar, S. Fahl, & A. Sasse. “The Challenges of Bringing Cryptography from Research Papers to Products: Results from an Interview Study with Experts”. Usenix Security Symposium 2024

Diverging (Expert) Views

"[RWC] is actually a wonderful place where **industry and academia come together**. [. . .] The community is growing and a lot of papers that analyse a crypto standard will now actually appear at the security conferences." (P3)

K. Fischer, I. Trummová, P. Gajland, Y. Acar, S. Fahl, & A. Sasse. "The Challenges of Bringing Cryptography from Research Papers to Products: Results from an Interview Study with Experts". Usenix Security Symposium 2024

Diverging (Expert) Views

"[RWC] is actually a wonderful place where **industry and academia come together**. [. . .] The community is growing and a lot of papers that analyse a crypto standard will now actually appear at the security conferences." (P3)

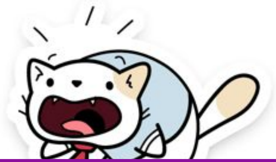
"RWC, even by it's name, it conveys what the message is: '**Don't bring your theoretical nonsense here**. We don't want to hear about it!'" (P13).

K. Fischer, I. Trummová, P. Gajland, Y. Acar, S. Fahl, & A. Sasse. "The Challenges of Bringing Cryptography from Research Papers to Products: Results from an Interview Study with Experts". Usenix Security Symposium 2024

Diverging (Expert) Views

"[RWC] is actually a wonderful place where **industry and academia come together**. [. . .] The community is growing and a lot of papers that analyse a crypto standard will now actually appear at the security conferences." (P3)

"RWC, even by it's name, it conveys what the message is: '**Don't bring your theoretical nonsense**



Posits: Motivators/Rewards are the issue

K. Fischer, I. Trummova, P. Gajland, Y. Acar, S. Fahl, & A. Sasse. "The Challenges of Bringing Cryptography from Research Papers to Products: Results from an Interview Study with Experts". Usenix Security Symposium 2024

More Diverging (Expert) Views

K. Fischer, I. Trummová, P. Gajland, Y. Acar, S. Fahl, & A. Sasse. “The Challenges of Bringing Cryptography from Research Papers to Products: Results from an Interview Study with Experts”. Usenix Security Symposium 2024

More Diverging (Expert) Views

“[Engineers] have a system and they want to make it secure. And so you indeed have to **translate** your scheme and explain them what you want to do, what you want to achieve and **why these properties are important**.” (P7)

K. Fischer, I. Trummová, P. Gajland, Y. Acar, S. Fahl, & A. Sasse. “The Challenges of Bringing Cryptography from Research Papers to Products: Results from an Interview Study with Experts”. Usenix Security Symposium 2024

More Diverging (Expert) Views

"[Engineers] have a system and they want to make it secure. And so you indeed have to **translate** your scheme and explain them what you want to do, what you want to achieve and **why these properties are important**." (P7)

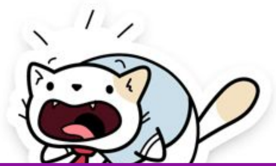
"No! I don't want to understand the problem with the application. That's your job! **My job is just the design and mathematics**!" (P10)

K. Fischer, I. Trummová, P. Gajland, Y. Acar, S. Fahl, & A. Sasse. "The Challenges of Bringing Cryptography from Research Papers to Products: Results from an Interview Study with Experts". Usenix Security Symposium 2024

More Diverging (Expert) Views

"[Engineers] have a system and they want to make it secure. And so you indeed have to **translate** your scheme and explain them what you want to do, what you want to achieve and **why these properties are important**." (P7)

"No! I don't want to understand the problem with the application. That's your job! **My job is just the**



Posits: Lack of translators is the issue

K. Fischer, I. Trummova, P. Gajland, Y. Acar, S. Fahl, & A. Sasse. "The Challenges of Bringing Cryptography from Research Papers to Products: Results from an Interview Study with Experts". Usenix Security Symposium 2024

All together now

"Of course, **not everyone needs to be an expert in multiple areas**. However, our interviews have shown that the role of a translator, "a crypto plumber", or a person in the middle is often poorly rewarded and insufficiently incentivized. Our results suggest that there is certainly a need for people to step into this role." - Fischer et al. 2024

K. Fischer, I. Trummová, P. Gajland, Y. Acar, S. Fahl, & A. Sasse. "The Challenges of Bringing Cryptography from Research Papers to Products: Results from an Interview Study with Experts". Usenix Security Symposium 2024

All together now

“Of course, not everyone needs to be an expert in multiple areas. **However**, our interviews have shown that the role of **a translator, “a crypto plumber”, or a person in the middle** is **often poorly rewarded and insufficiently incentivized**. Our results suggest that there is certainly a need for people to step into this role.” - Fischer et al. 2024

K. Fischer, I. Trummová, P. Gajland, Y. Acar, S. Fahl, & A. Sasse. “The Challenges of Bringing Cryptography from Research Papers to Products: Results from an Interview Study with Experts”. Usenix Security Symposium 2024

All together now

"Of course, not everyone needs to be an expert in multiple areas. However, our interviews have shown that the role of **a translator, "a crypto plumber", or a person in the middle** is often poorly rewarded and insufficiently incentivized. Our results suggest **that there is certainly a need for people to step into this role**." - Fischer et al. 2024

K. Fischer, I. Trummová, P. Gajland, Y. Acar, S. Fahl, & A. Sasse. "The Challenges of Bringing Cryptography from Research Papers to Products: Results from an Interview Study with Experts". Usenix Security Symposium 2024

“So what?” - The Audience

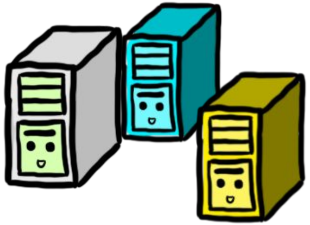
“In general users don’t care very much: I mean good cryptography is cryptography that users don’t see, right?” (P7).

Then what do we need to tell them? Do we need to?

What cryptography do we need to make? How do we know?

K. Fischer, I. Trummova, P. Gajland, Y. Acar, S. Fahl, & A. Sasse. "The Challenges of Bringing Cryptography from Research Papers to Products: Results from an Interview Study with Experts". Usenix Security Symposium 2024

Return: Why Private Computation?



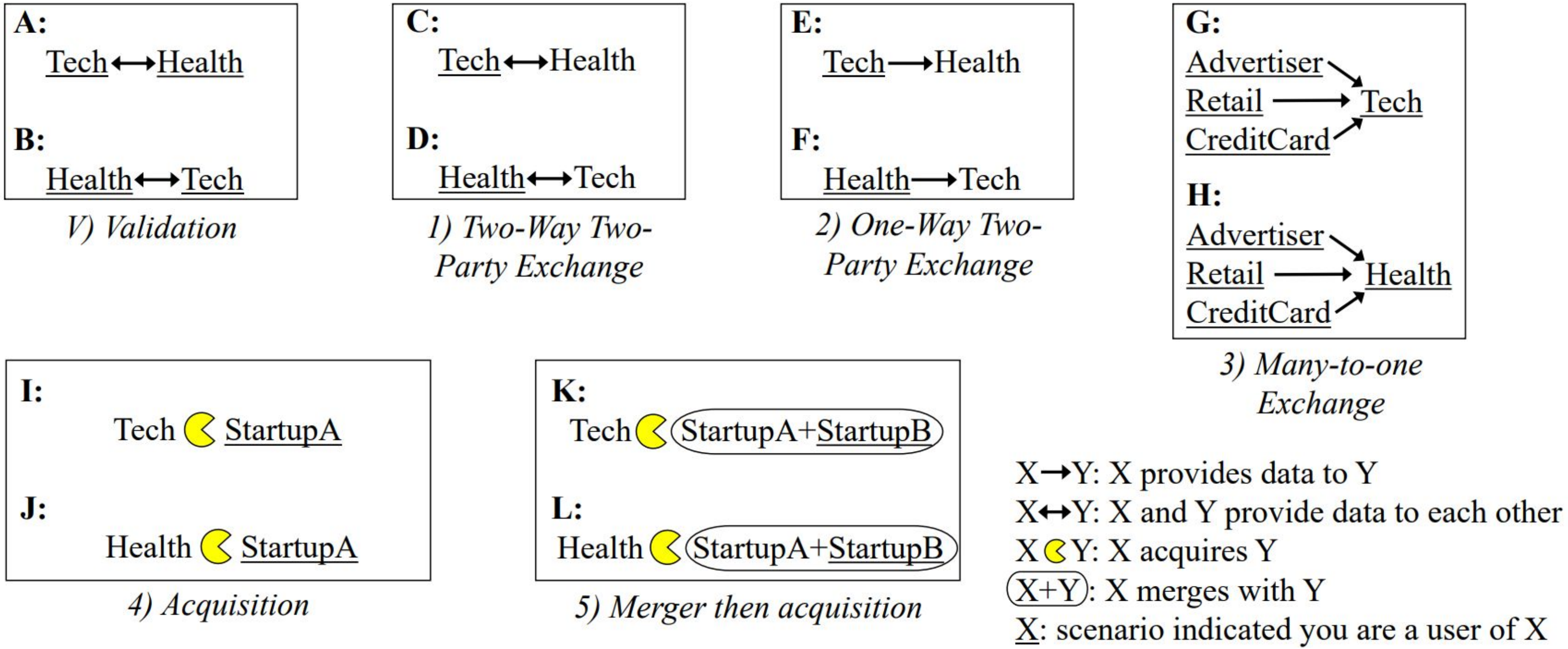
A company wants to analyze data

But the data has privacy implications for the data subjects

Researchers develop technical solutions

In what ways does private computation matter to people?

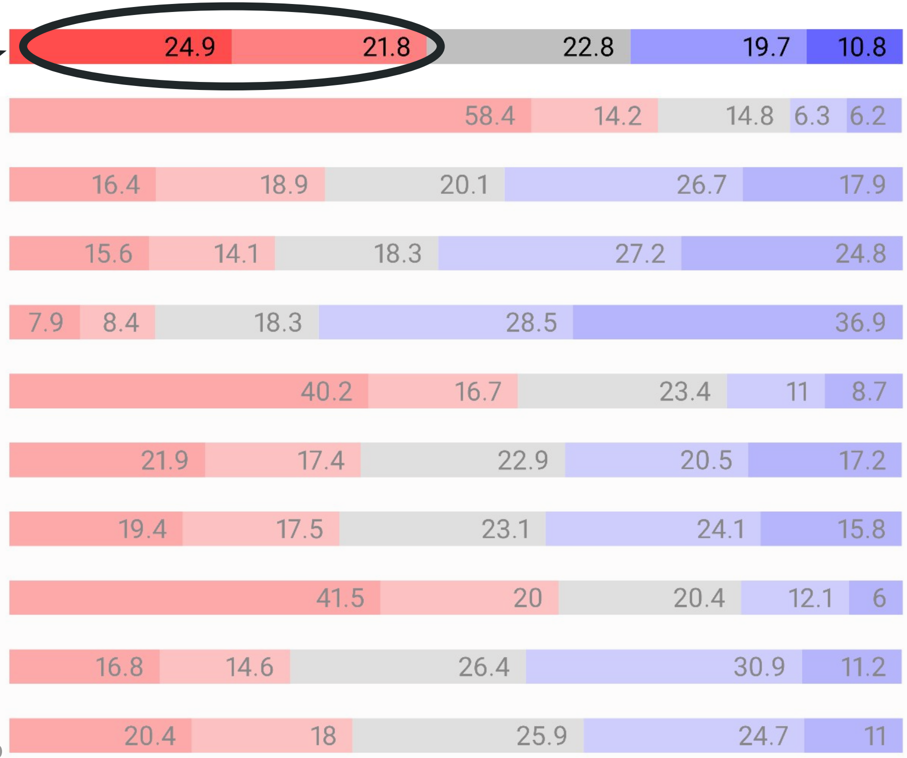
Types of Multiparty Data Sharing



Kacsmar, Tilbury, Mazmudar, Kerschbaum. Caring about Sharing: User Perceptions of Multiparty Data Sharing. *USENIX Security 2022*

Overall Acceptability Across Scenarios

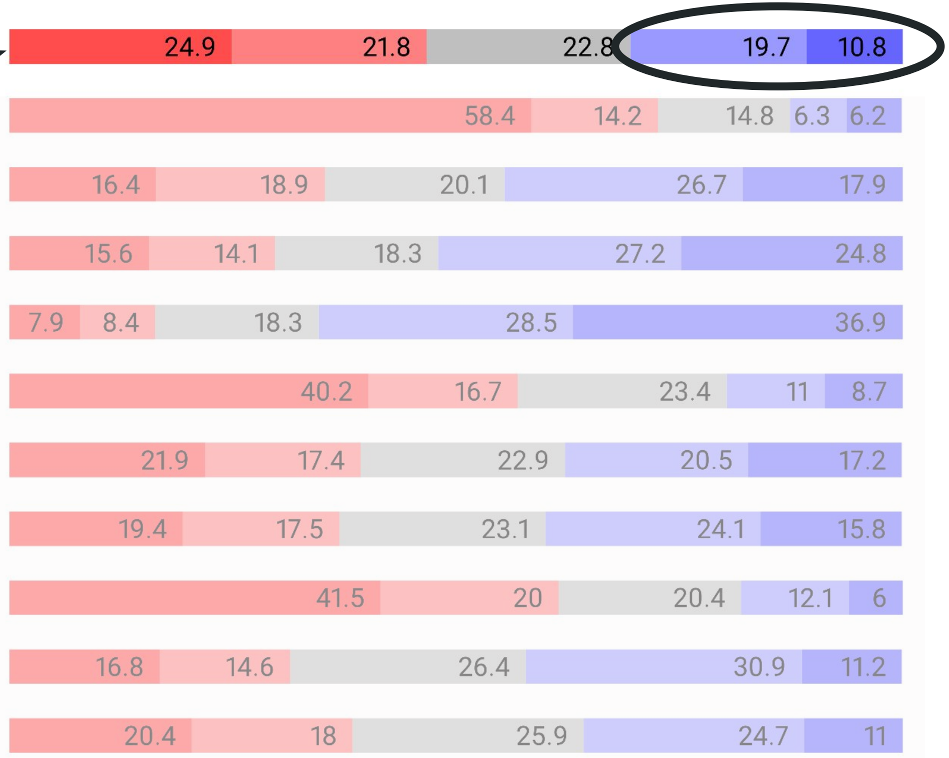
General Scenario Acceptability?



Kacsmar, Tilbury, Mazmudar, Kerschbaum. Caring about Sharing: User Percep

Overall Acceptability Across Scenarios

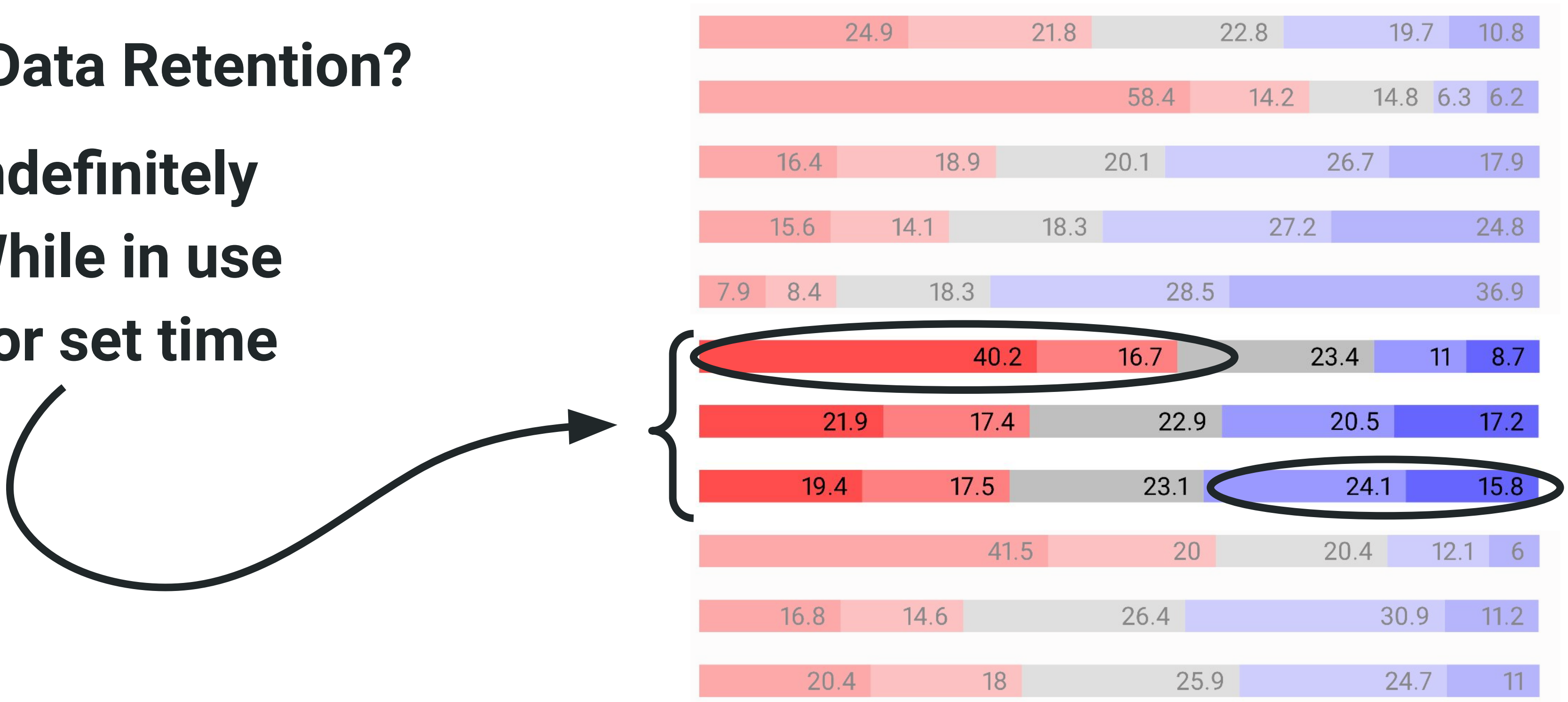
General Scenario Acceptability?



Retention: Acceptability Across All Scenarios

Data Retention?

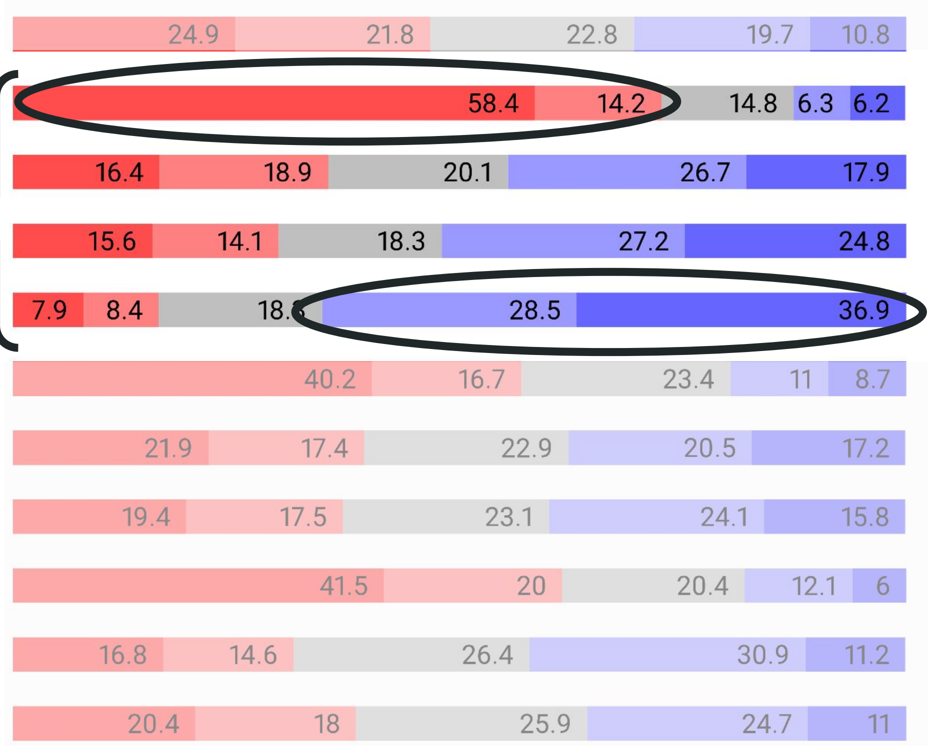
- **Indefinitely**
- **While in use**
- **For set time**



Consent: Acceptability Across All Scenarios

Informed Consent?

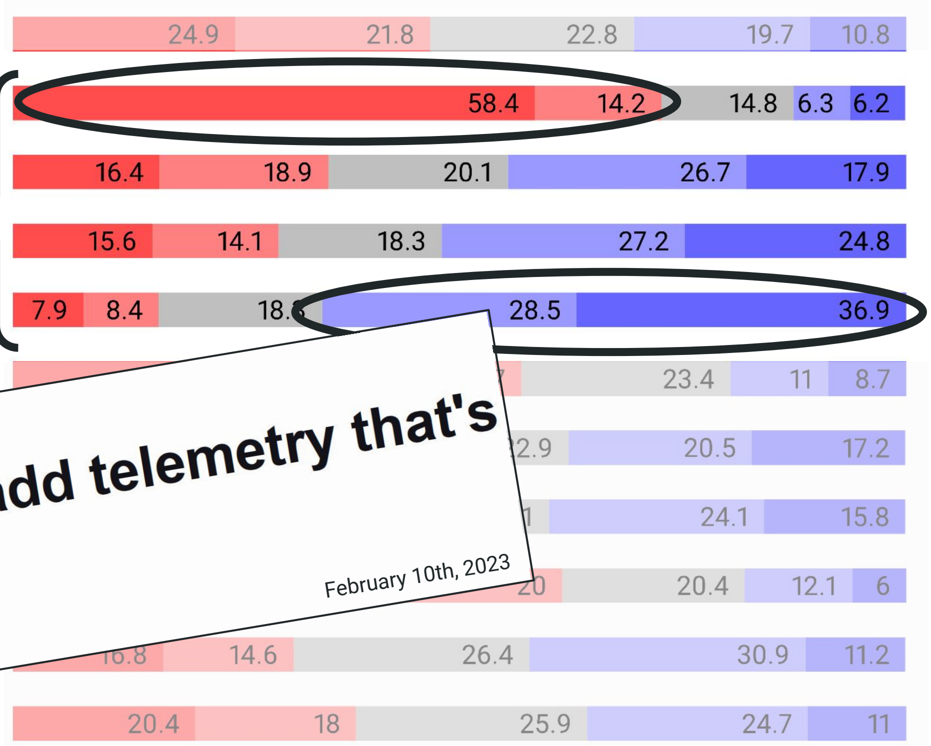
- Concealed 
- Assumed
- Opt-out
- Opt-in 



Consent: Acceptability Across All Scenarios

Informed Consent?

- Concealed 
- Assumed
- Opt-out
- Opt-in 



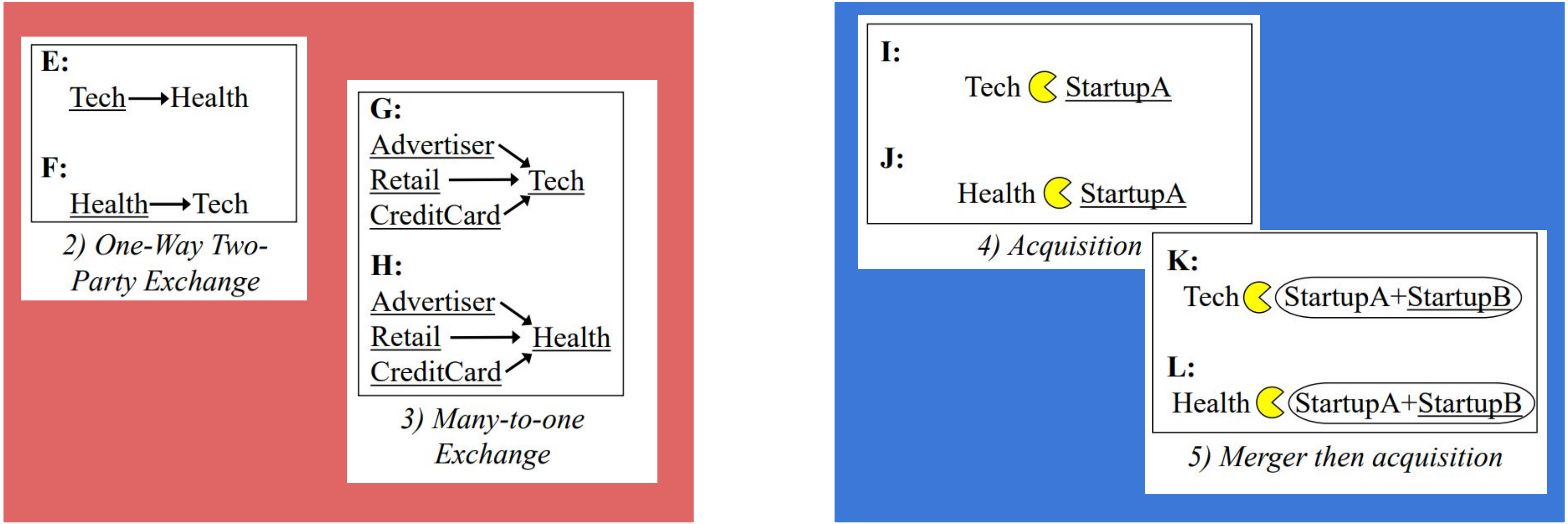
theregister.com

Google's Go may add telemetry that's on by default

Thomas Claburn

February 10th, 2023

Sharing Type Impact on Overall Acceptability



General acceptability is statistically different between types.

Kacsmar, Tilbury, Mazmudar, Kerschbaum. Caring about Sharing: User Perceptions of Multiparty Data Sharing. *USENIX Security 2022*

Throw some privacy at it.

A Private Computation? Cryptography!

I want to learn
$Z = X \cap Y$

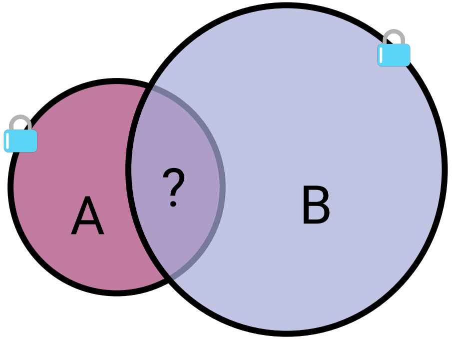
$X = \{x_1, x_2, \ldots, x_n\}$

$Y = \{y_1, y_2, \ldots, y_m\}$

Private Set Intersection (PSI)

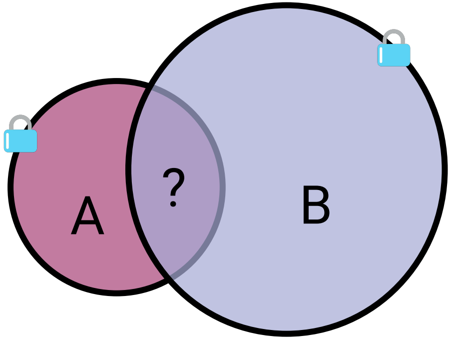
- Alice has set $X = \{x_1, x_2, x_3, \ldots, x_n\}$
- Bob has set $Y = \{y_1, y_2, y_3, \ldots, y_m\}$
- They want to compute $Z = X \cap Y$ (but reveal nothing else)
- This is an instance of a two-party computation of a specific function

Private Set Intersections



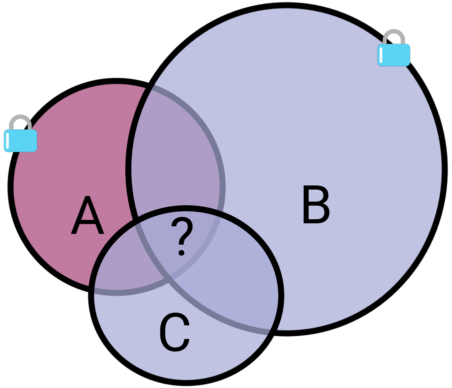
2-Party, One-Way PSI

A → B



2-Party, Two-Way PSI

A ↔ B



n-Party PSI

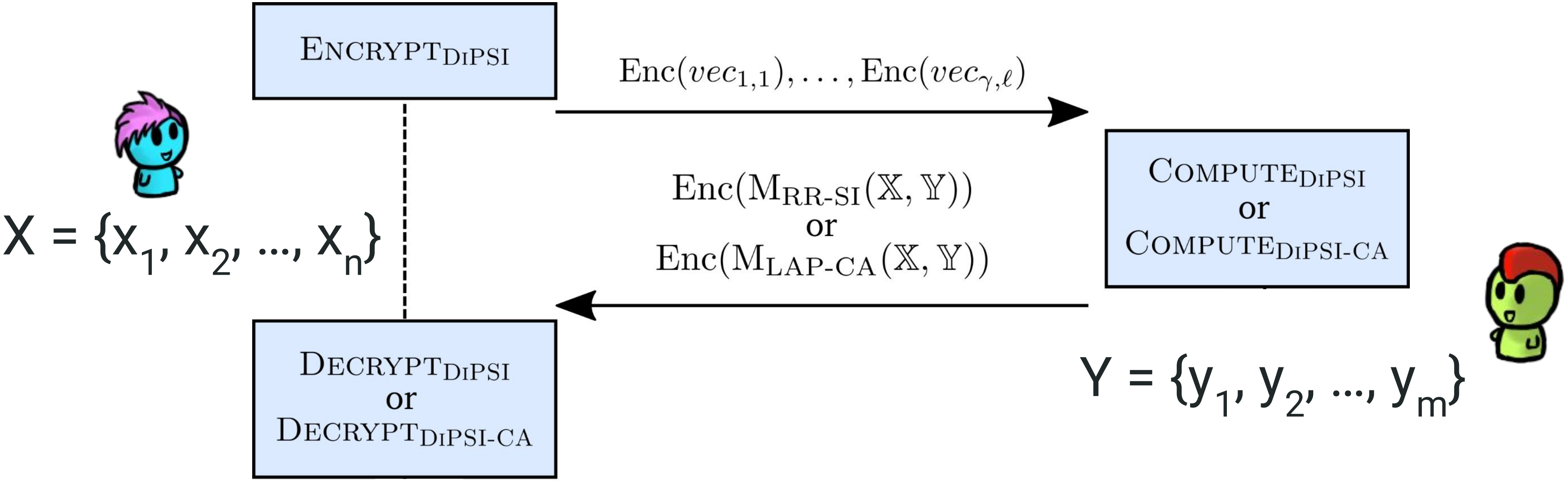
Directionality | **Reducing Information** | **Multi-party** | **Varying Guarantees**

PSI: Strawman Protocol

- Alice permutes her set X, Bob permutes his set Y
- For each $x \in X$
  - For each $y \in Y$
    - Compute x =? y
- Protocol for comparison x =? y
  - Alice → Bob: $E_A(x)$
  - Bob: Choose r. $c = (E_A(x) * E_A(-y))^r$
  - Bob → Alice: c
  - Alice: Output $x = y$, if $D_A(c) = 0$, else $x \neq y$

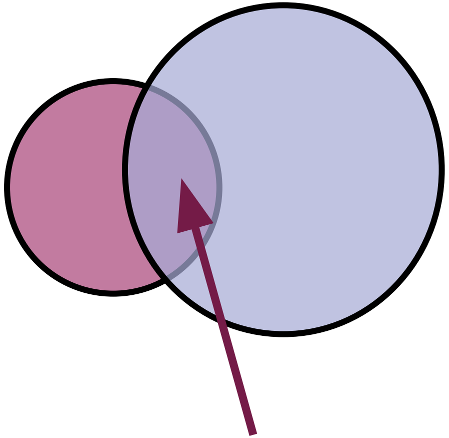
Throw some differential privacy at it.

Private Set Intersection



Kacsmar Khurram, Lukas, Norton, et al. "Differentially private two-party set operations." In 2020 IEEE European Symposium on Security and Privacy (EuroS&P), pp. 390-404. IEEE, 2020.

Why Differentially Private Set Intersection?



Individuals with transactions at **R** who saw ads for **R**

1. Let **s** be the sum of matched credit card transactions
2. Ads for **R** are very specific, if only one individual is at the match, **s** reveals purchase history for them
3. The goal of a DP-sum for this intersection is to prevent such revelations.

B. Kacsmar, B. Khurram, N. Lukas, A. Norton, et al. "Differentially private two-party set operations." In 2020 IEEE European Symposium on Security and Privacy (EuroS&P), pp. 390-404. IEEE, 2020.

Perceptions and Expectations

- What do data subjects understand?
- How is a data subject's willingness to share impacted?
- How do data subjects perceive the risks?

What they "want"

What they "need"

Build towards those attributes

Kacsmar, Duddu, Tilbury, Ur, and Kerschbaum. Comprehension from Chaos: Towards Informed Consent for Private Computation. *2023 ACM SIGSAC Conference on Computer and Communications Security* (CCS).

The Scenarios

Wage Equity	**Census Analysis**
Ad Conversion	**Contact Discovery**

Kacsmar, Duddu, Tilbury, Ur, and Kerschbaum. Comprehension from Chaos: Towards Informed Consent for Private Computation. 2*023 ACM SIGSAC Conference on Computer and Communications Security* (CCS).

Contact Discovery Conceptual Example

The app wants to **determine the common contacts** between the new user and the existing users via…

1. …the new user shares all their contact information with the social media app.
2. … the new user shares **a modified version** of their contact information…**such that** the social media app does not learn non-users…thus, **this means**…

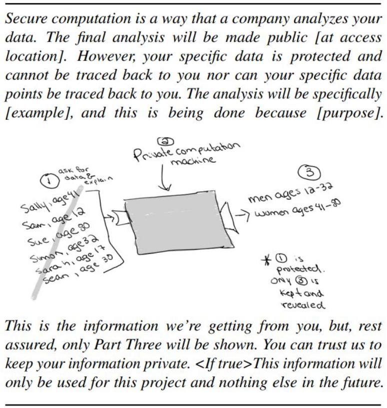
Kacsmar, Duddu, Tilbury, Ur, and Kerschbaum. Comprehension from Chaos: Towards Informed Consent for Private Computation. *2023 ACM SIGSAC Conference on Computer and Communications Security* (CCS).

The Interview

Expectations and Term Awareness → Initial Definition and Baseline → Scenario Assessment → Inference Attack Perceptions → General Perceptions → Collective Explanation Activity

Kacsmar, Duddu, Tilbury, Ur, and Kerschbaum. Comprehension from Chaos: Towards Informed Consent for Private Computation. *2023 ACM SIGSAC Conference on Computer and Communications Security* (CCS).

Participant Comprehension and Expectations



Secure computation is a way that a company analyzes your data. The final analysis will be made public [at access location]. However, your specific data is protected and cannot be traced back to you nor can your specific data points be traced back to you. The analysis will be specifically [example], and this is being done because [purpose].

This is the information we're getting from you, but, rest assured, only Part Three will be shown. You can trust us to keep your information private. <If true>This information will only be used for this project and nothing else in the future.

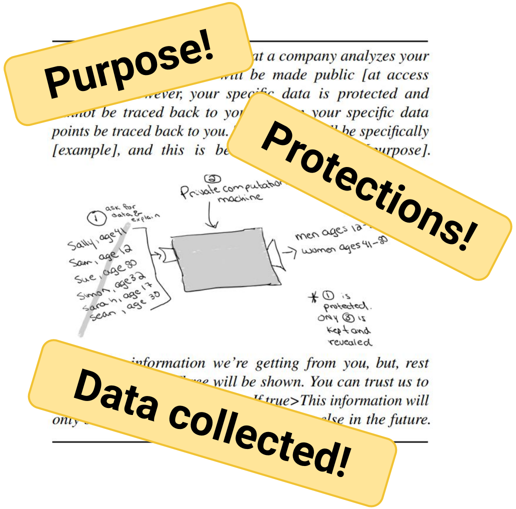
First Attempt **Second Attempt** **Final Consensus**

Kacsmar, Duddu, Tilbury, Ur, and Kerschbaum. Comprehension from Chaos: Towards Informed Consent for Private Computation. *2023 ACM SIGSAC Conference on Computer and Communications Security* (CCS).

Participant Comprehension and Expectations

First Attempt

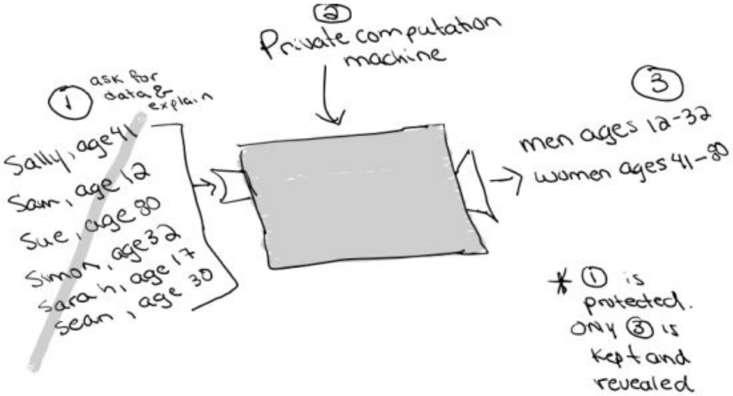
Second Attempt



Final Explanation

Unconcerned with details of the mechanism, **impact** matters

Secure computation is a way that a company analyzes your data. The final analysis will be made public [at access location]. However, your specific data is protected and cannot be traced back to you nor can your specific data points be traced back to you. The analysis will be specifically [example], and this is being done because [purpose].



This is the information we're getting from you, but, rest assured, only Part Three will be shown. You can trust us to keep your information private. <If true>This information will only be used for this project and nothing else in the future.

Kacsmar, Duddu, Tilbury, Ur, and Kerschbaum. Comprehension from Chaos: Towards Informed Consent for Private Computation. *2023 ACM SIGSAC Conference on Computer and Communications Security* (CCS).

Impact of Private Computation

"...they're trying to make it sound a little bit better" (P19).

"...it feels a little bit more protected that way" (P12)

Kacsmar, Duddu, Tilbury, Ur, and Kerschbaum. Comprehension from Chaos: Towards Informed Consent for Private Computation. *2023 ACM SIGSAC Conference on Computer and Communications Security* (CCS).

Bounded Impact of Private Computation

Intentions Matter

Divulge the Details

Regulate the Restrictions

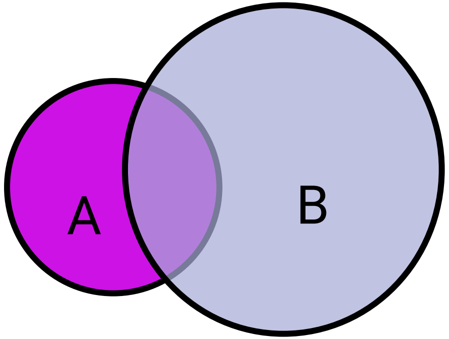
Consent Above All

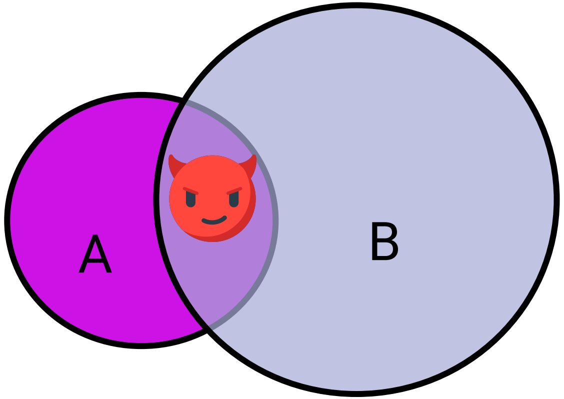
"At the end of the day,
they're still like learning specific things about me" (P7)

-So what - in cryptographic terms

Awareness of Unique Threat Models

Alice





Joins Social App

Contact Discovery

Real Identity Connected

There exist, and will continue to exist risks that cannot be regulated by technology

How can we modify PSI for Alice?

Do we understand the problem?

Not just consent, what is the attack?

Not just consent, what is the attack?

Consider:

- Alice joins the app and signs up with her phone number and “E(contact list)”, not shared with other users
- The app, uses contact discovery, but does so with PSI

Not just consent, what is the attack?

Consider:

- Alice joins the app and signs up with her phone number and “E(contact list)”, not shared with other users
- The app, uses contact discovery, but does so with PSI
- **Mallory**, joins the app

Not just consent, what is the attack?

Consider:

- Alice joins the app and signs up with her phone number and "E(contact list)", not shared with other users
- The app, uses contact discovery, but does so with PSI
- **Mallory**, joins the app
- **Mallory**, has Alice's number in her contact list

Not just consent, what is the attack?

Consider:

- Alice joins the app and signs up with her phone number and "E(contact list)", not shared with other users
- The app, uses contact discovery, but does so with PSI
- **Mallory**, joins the app
- **Mallory**, has Alice's number in her contact list
- The app connects **Mallory** and Alice

Not just consent, what is the attack?

Consider:

- Alice joins the app and signs up with her phone number and “E(contact list)”, not shared with other users
- The app, uses contact discovery, but does so with PSI
- <u>**Mallory**</u>, joins the app

Easy fix you say?

Alice should just get a new number you say?

Variant: Not just consent, what is the attack?

Consider **Alice got a new number**:

- Alice joins the app and signs up with her phone number and "E(contact list)", not shared with other users
- The app, uses contact discovery, but does so with PSI
- **Mallory**, joins the app

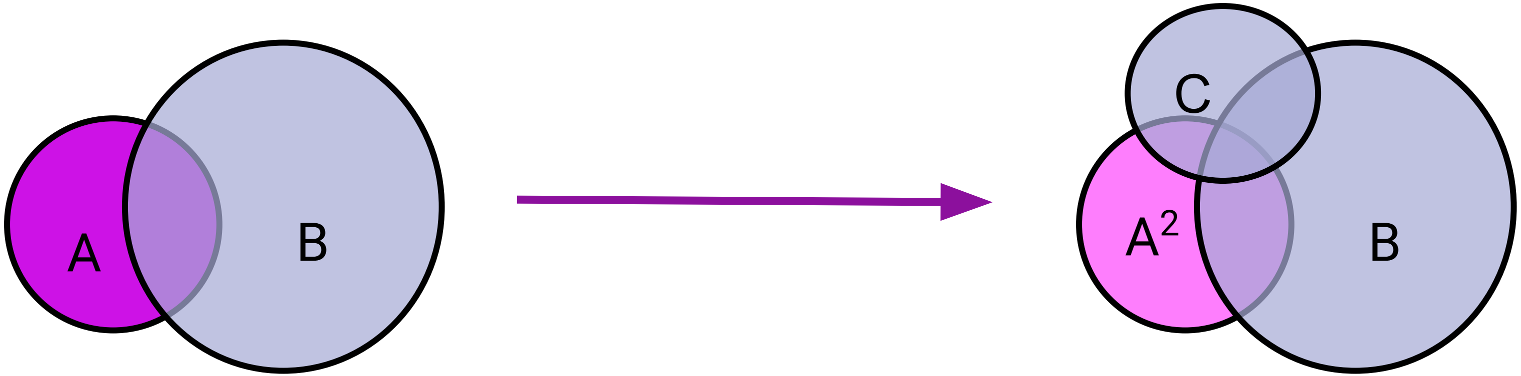
Variant: Not just consent, what is the attack?

Consider:

- Alice joins the app and signs up with her phone number and “E(contact list)”, not shared with other users
- The app, uses contact discovery, but does so with PSI
- **Mallory**, joins the app
- **Mallory**, tries a set of numbers for Alice’s area code, excluding known non-Alice’s as her contact list
- The app connects **Mallory** and Alice

How can we modify PSI for Alice?

Attempt Fix 1



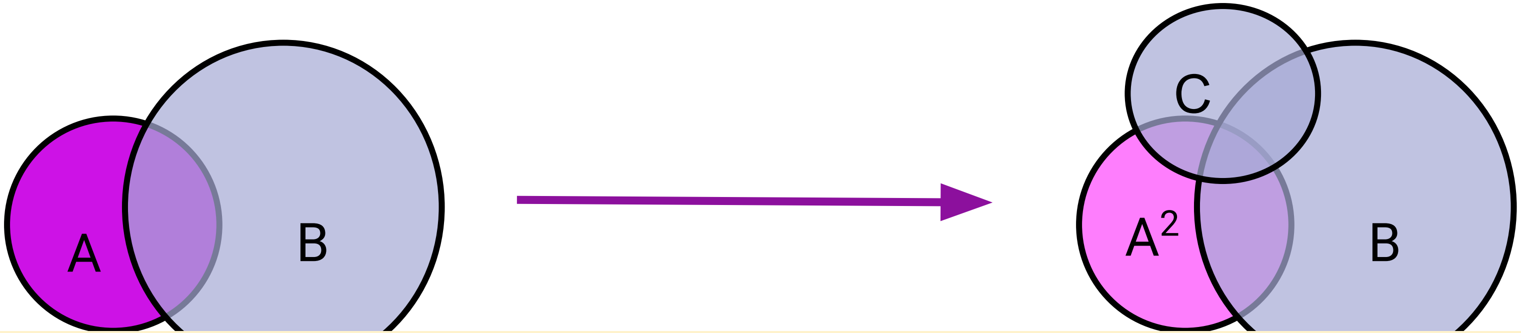
Alice's #'s ∩ App users

$A^2 \subseteq$ A #'s ∩ App users

And

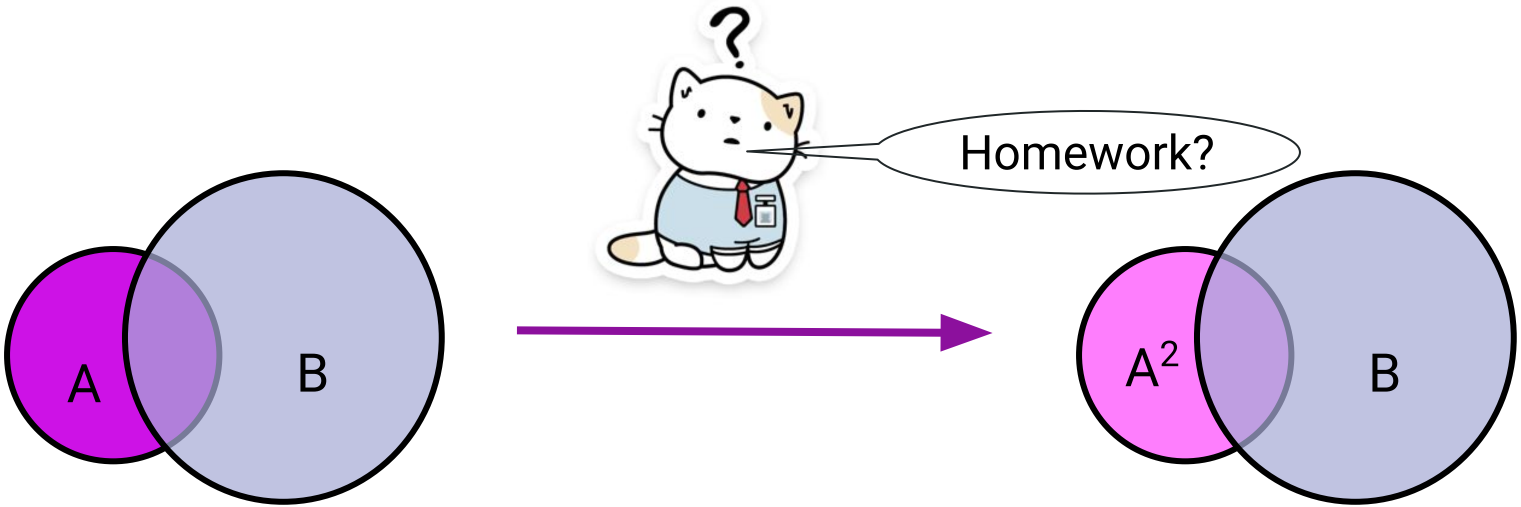
Match iff $A^2 \cap B \cap C$

Attempt Fix 1



Problem: 3 Party PSI where server will need to find the third party for every element in the primary client set.

Attempt Fix 2

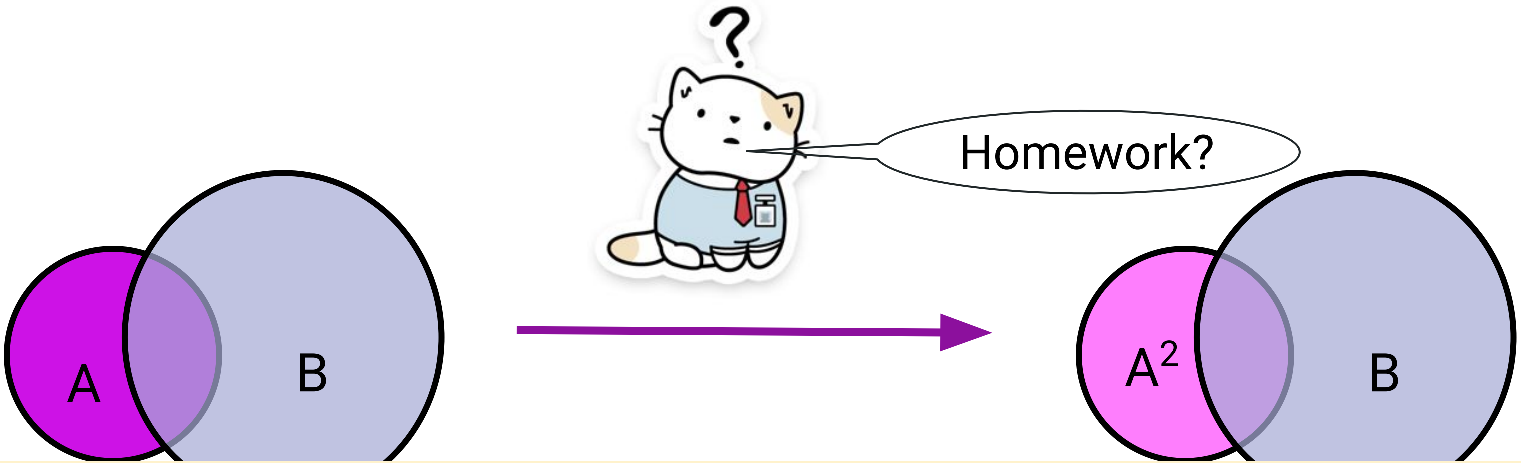


Alice's #'s ∩ App users

For all $a \in A^2$, $a \leftarrow a + A\#$

$A^2 \subseteq A$ #'s ∩ App users

Attempt Fix 2



Problem: better, might work, increased communication cost (size not count), increased size of strings to be processed, need to verify number ownership in some way…

Assorted Neat Cryptography with a Usability Vec.

Individualized PATE: Differentially Private Machine Learning with Individual Privacy Guarantees.
Boenisch et al. (PoPETs '23)

Callisto: A Cryptographic Approach to Detecting Serial Perpetrators of Sexual Misconduct
Rajan et al. (COMPASS '18)

A Gentle Tutorial for Lattice-Based Cryptanalysis
Surin and Cohney (eprint.iacr.org/2023/032)

Shatter Secrets: Using Secret Sharing to Cross Borders with Encrypted Devices.
Atwater and Goldberg (Security Protocols 2018. LNCS, vol 11286)

Take this: Usability is Critical for Cryptography

We need usability to support:

- **Accessibility** of secure systems for organizations big and small, used by individuals and populations
- **Enforceability** from legaslaters
- **Verifiability** for those implementing and deploying
- **Meaningful privacy** from applied cryptography for privacy

How will you develop cryptography that does this?

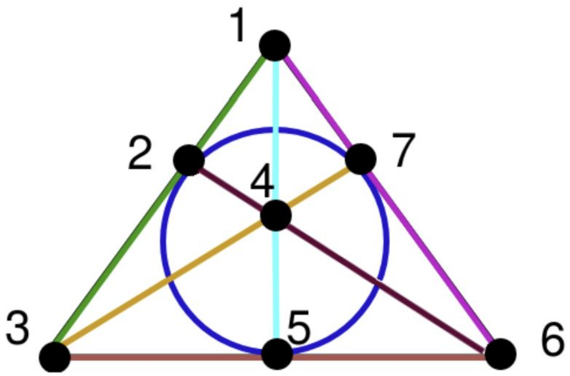
There are many other variants of properties

For instance, **repairability** and **access control**

Balanced Incomplete Block Designs (BIBD)

Let v, k, λ be integers, $v > k \geq \lambda$. A $(\mathbf{v}, \mathbf{k}, \lambda)-$**BIBD** is a design such that:

1. $|X| = v$, number of elements in the set X is v
2. each block contains exactly k points, and
3. every pair of distinct points is contained in exactly λ blocks.



$(7, 3, 1)-$BIBD

A Useful Property

Definition

Every point in a (v, k, λ)-BIBD occurs in exactly

$$r = \frac{\lambda(v-1)}{k-1}$$

blocks. The value r is termed the *replication number*.

Constructing a Repairable (2,7)-TS

Base Scheme

Construct a $(5,7)$-threshold scheme. The shares from the base scheme are $S_1, S_2 \ldots, S_7$.

Distribution Design

Assign the blocks of the $(7,3,1)$-BIBD as follows:

$P_1 \leftrightarrow 123$ $P_3 \leftrightarrow 167$ $P_5 \leftrightarrow 257$ $P_7 \leftrightarrow 356$

$P_2 \leftrightarrow 145$ $P_4 \leftrightarrow 246$ $P_6 \leftrightarrow 347$

Expanded Scheme

Distribute each S_i to players with point i from the block design.

P_1's expanded share S_1, S_2, S_3.
P_2's expanded share S_1, S_4, S_5.
P_3's expanded share S_1, S_6, S_7.
P_4's expanded share S_2, S_4, S_6.
P_5's expanded share S_2, S_5, S_7.
P_6's expanded share S_3, S_4, S_7.
P_7's expanded share S_3, S_5, S_6.

From 2-Designs to t-Designs

Definition

A $t-(v,k,\lambda)$ *design* is a design where:

1. $|X| = v$,
2. Each block is of size k,
3. Every set of t points from the set X occurs in exactly λ blocks.

Definition

A $3-(v,4,1)$ design is a *Steiner quadruple system* of order v, denoted $SQS(v)$. For all $SQS(v)$, $v \equiv 2,4 \pmod 6$.

2-Designs and 3-Designs

Example

A $2-(13,4,1)$ design with the set $X = \{0,1,2,3,4,5,6,7,8,9,a,b,c\}$

0139	028c
0457	06ab
124a	1568
17bc	235b
2679	346c
378a	489b
598a	

Example

A $3-(8,4,1)$ design with the set $X = \{1,2,3,4,5,6,7,8\}$

1234	5678
1256	3478
1278	3456
1357	2468
1368	2457
1458	2367
1467	2358