# An Inconvenient Trust

## User Attitudes toward Security and Usability Tradeoffs for Key-Directory Encryption Systems

**Patrick Gage Kelley**

@patrickgage

Assistant Professor, Computer Science

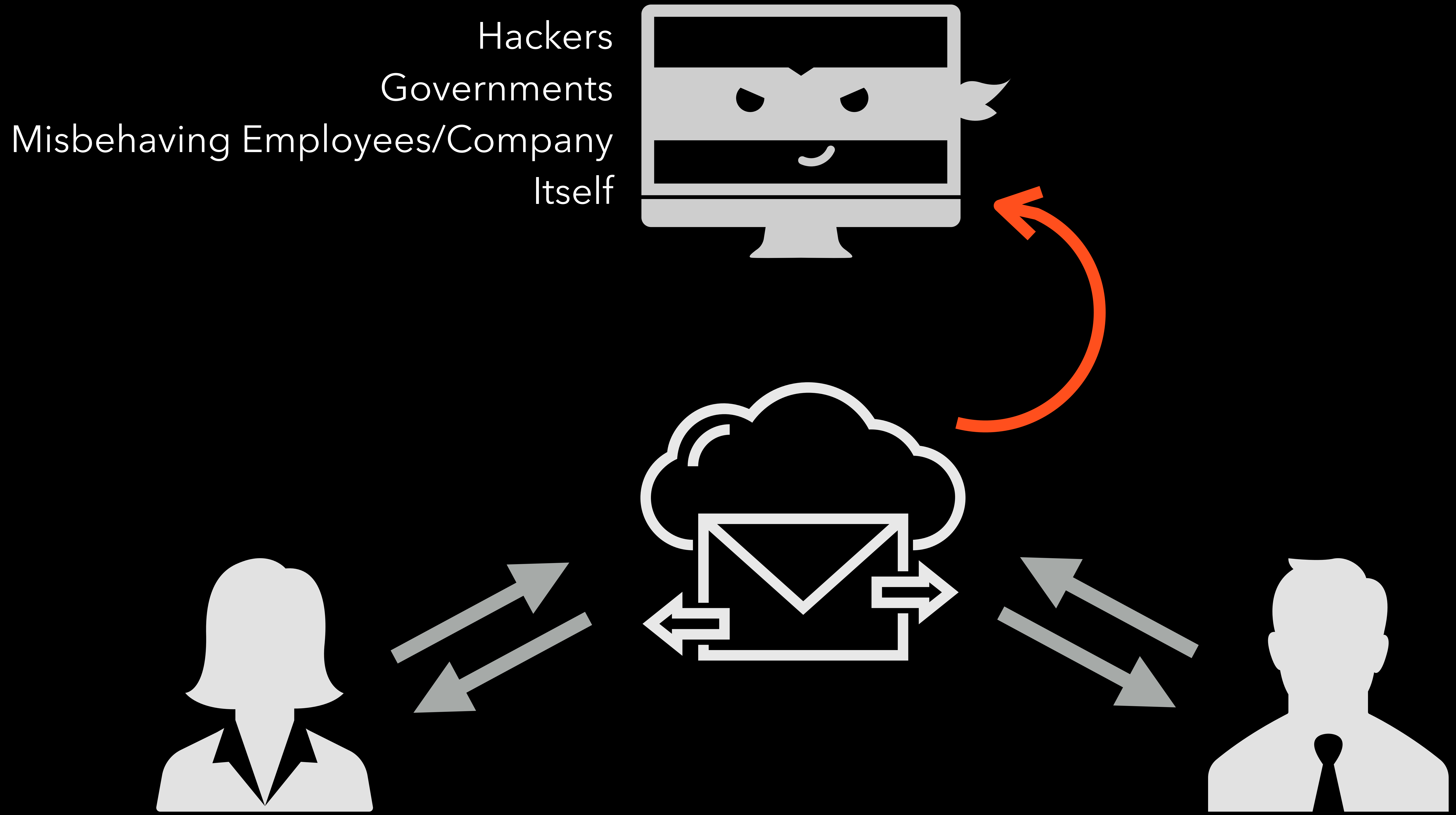
THE UNIVERSITY *of* NEW MEXICO

joint work with researchers at University of Maryland:
Wei Bai, Doowon Kim, Moses Namara, Yichen Qian,
and Dr. Michelle L. Mazurek

first published in June at the
Symposium on Usable Privacy and Security **SOUPS**

# What is End-to-End Encryption?

# What is End-to-End Encryption?



# PARTICIPANTS

**80%
Between
Ages of
18-34**

**Gender:
Male 60%
Female 40%**

**Occupation:
40% reported jobs or majors in computing, math and engineering**

# PARTICIPANTS

**Security Expertise**[1]

Only 2 out of 52 scored 3 or higher (out of 5.5)

[1] L. J. Camp, T. Kelley, and P. Rajivan. Instrument for measuring computing and security expertise. Technical Report TR715, Indiana University, Feb. 2015.

# PARTICIPANTS

**Security Expertise**[1]
Only 2 out of 52 scored 3 or higher (out of 5.5)

Have your ever **registered a domain name?**

Have your ever **created a database?**

Have you ever **used SSH?**

Have you ever **configured a firewall?**

[1] L. J. Camp, T. Kelley, and P. Rajivan. Instrument for measuring computing and security expertise. Technical Report TR715, Indiana University, Feb. 2015.

# PARTICIPANTS

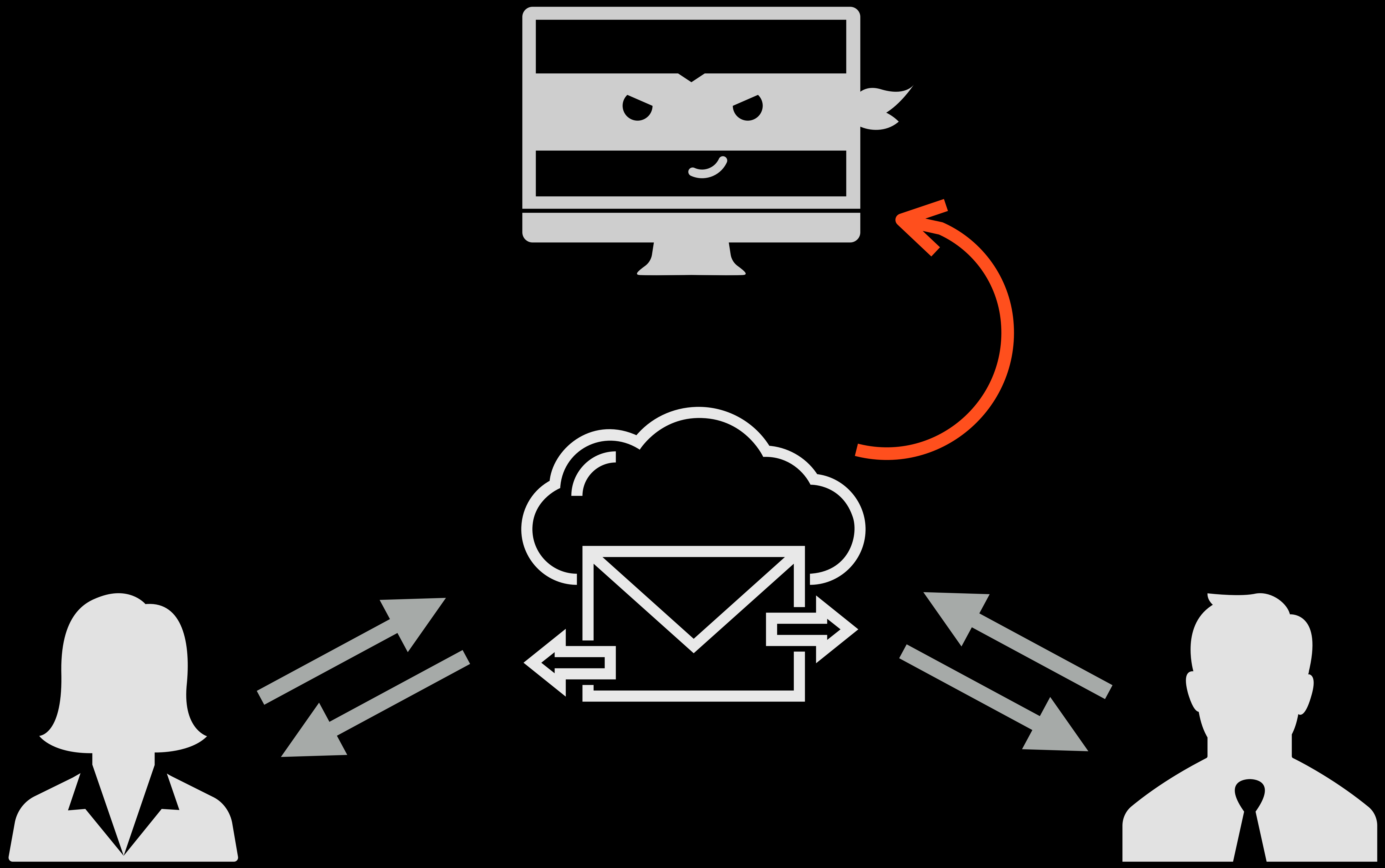
**Security Expertise**[1]

Only 2 out of 52 scored 3 or higher (out of 5.5)

If you know, please describe what a "**security certificate**" is in the context of the Internet, otherwise write "Don't know."

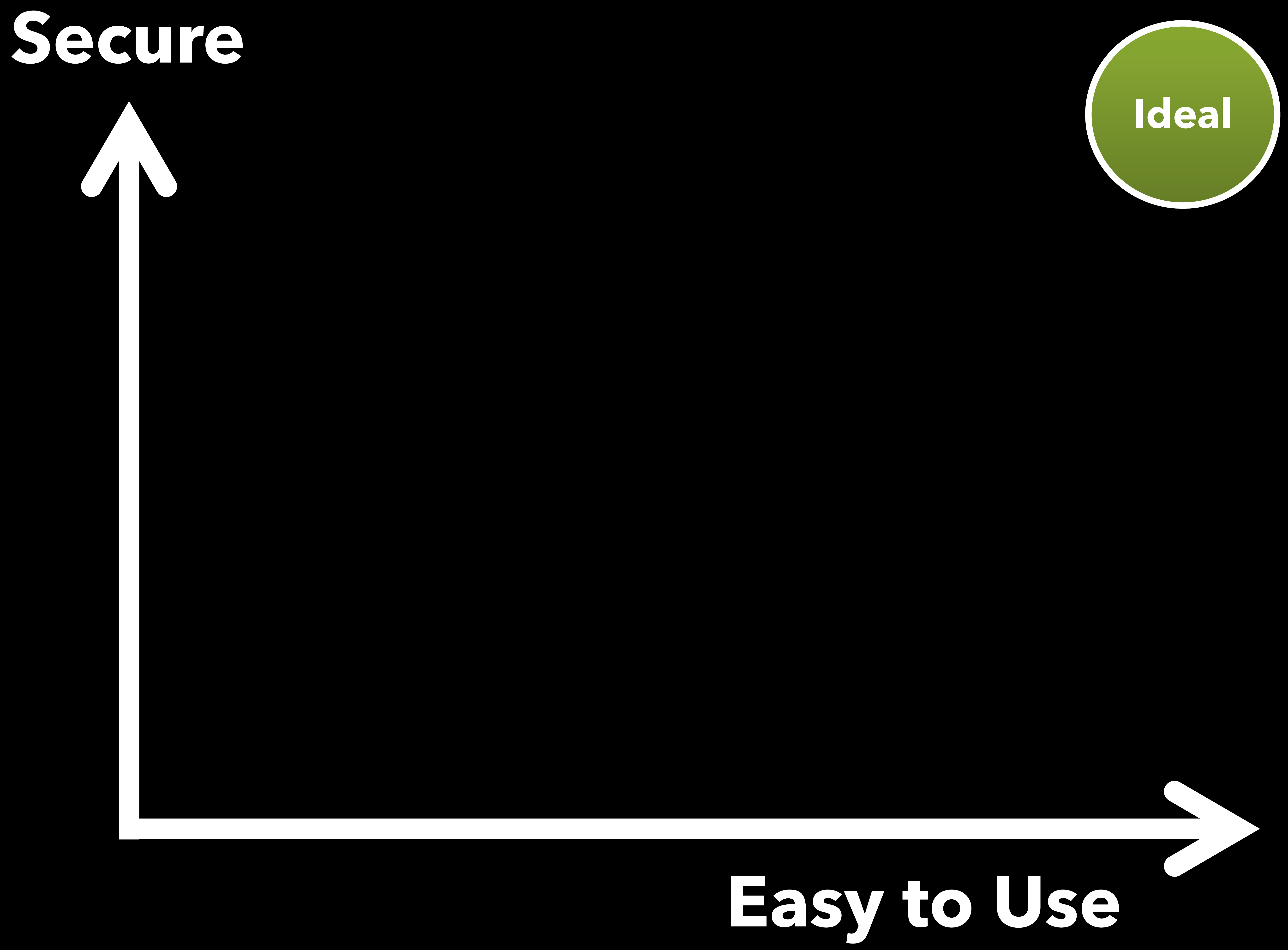
If you know, please describe what is meant by "**phishing**'' otherwise write "Don't know"

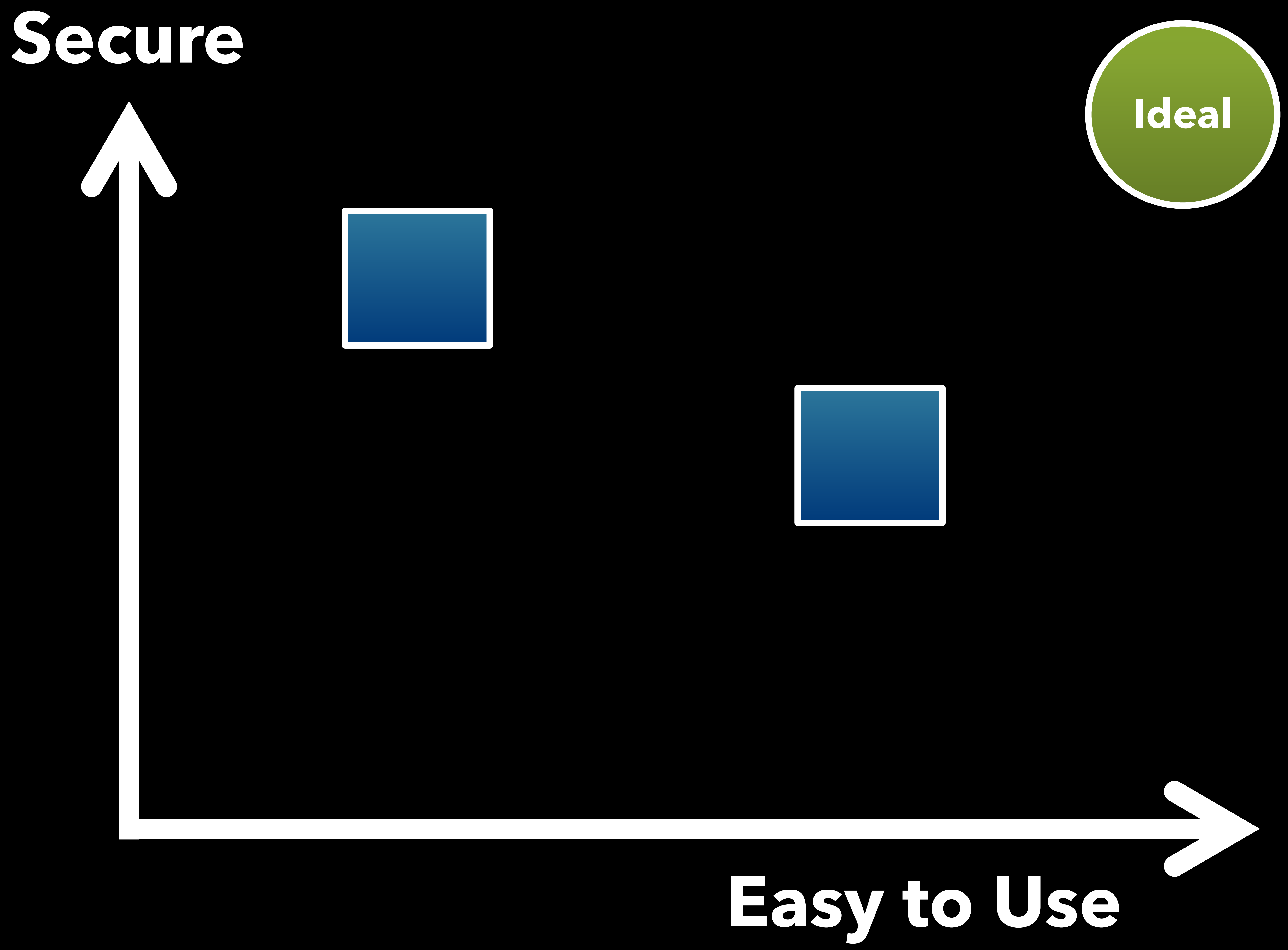
[1] L. J. Camp, T. Kelley, and P. Rajivan. Instrument for measuring computing and security expertise. Technical Report TR715, Indiana University, Feb. 2015.

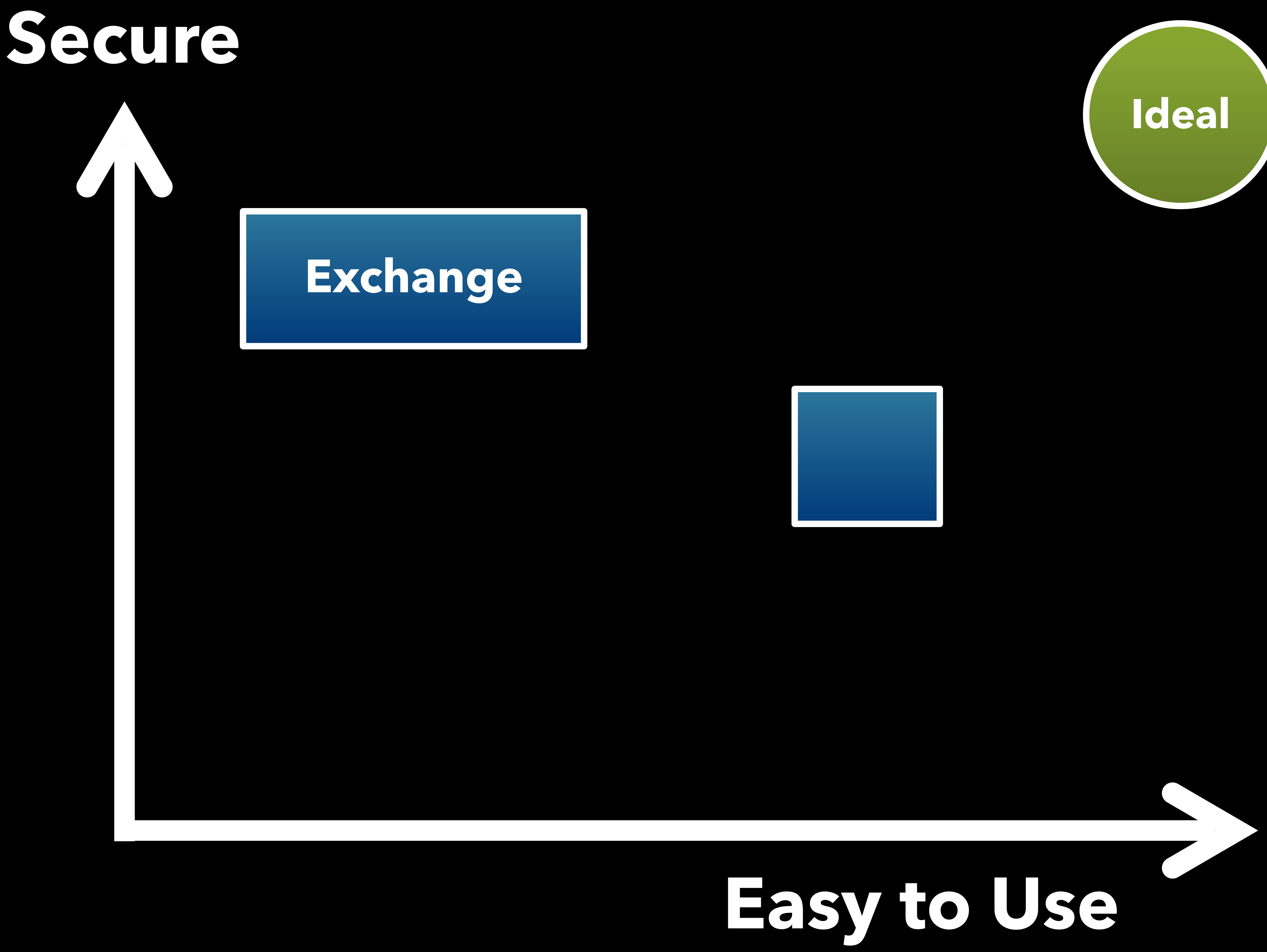


Secure

Easy to Use

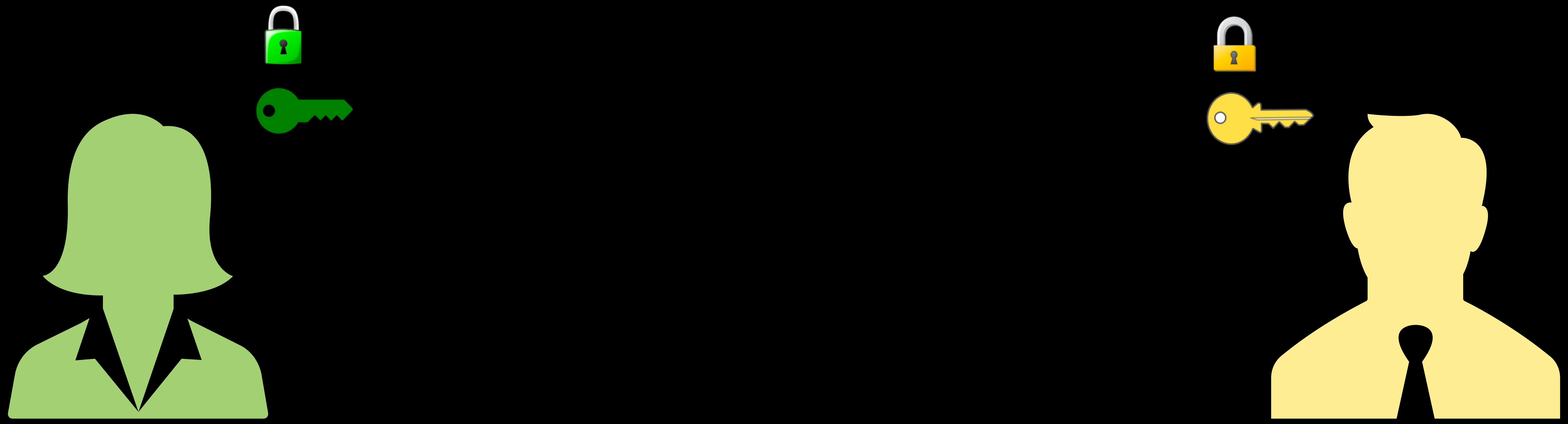

Secure
Ideal
Easy to Use


Secure
Ideal
Easy to Use

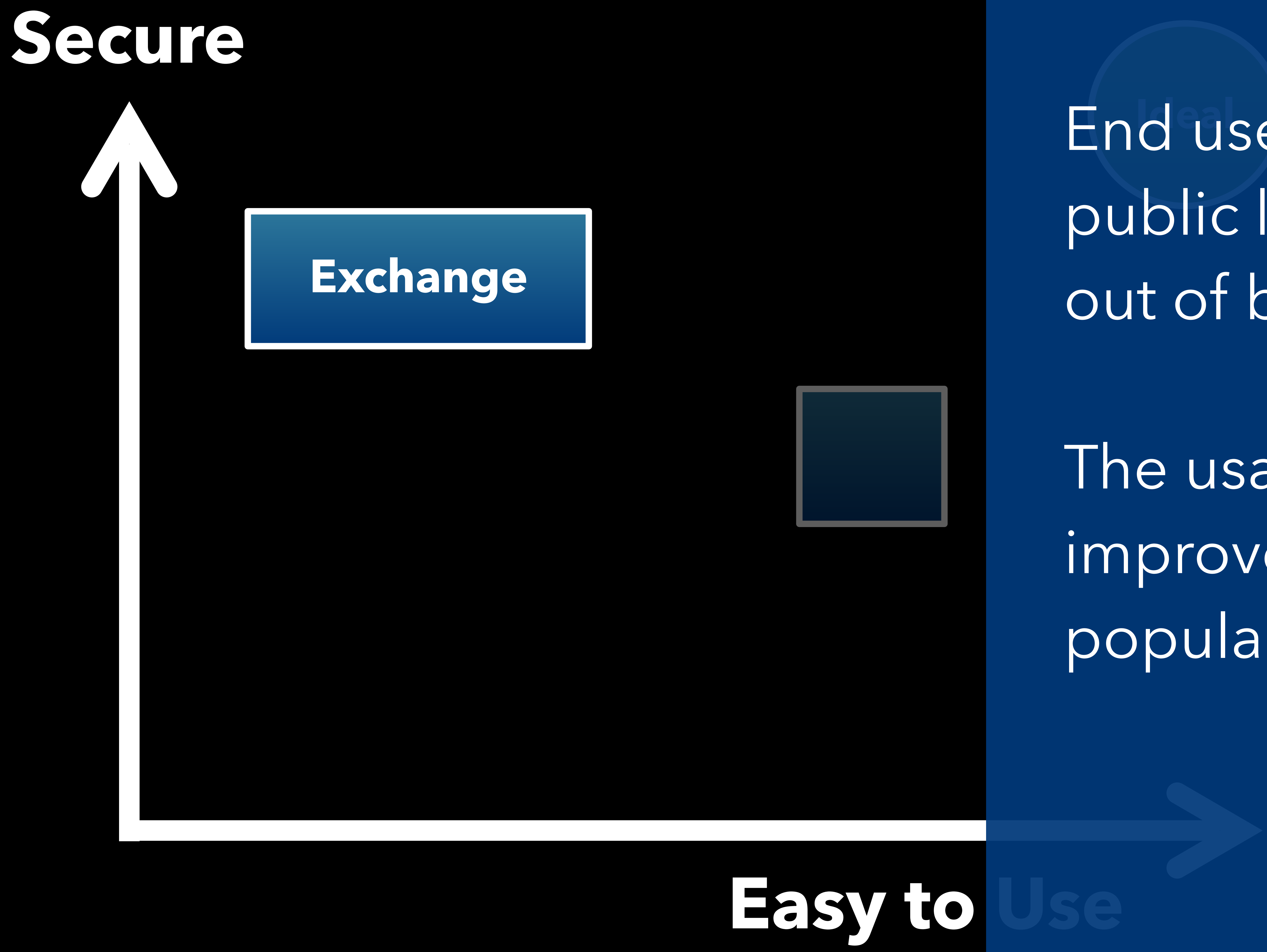

Secure
Ideal
Exchange
Easy to Use

# Exchange Model

exchanging public locks[1] manually out of band



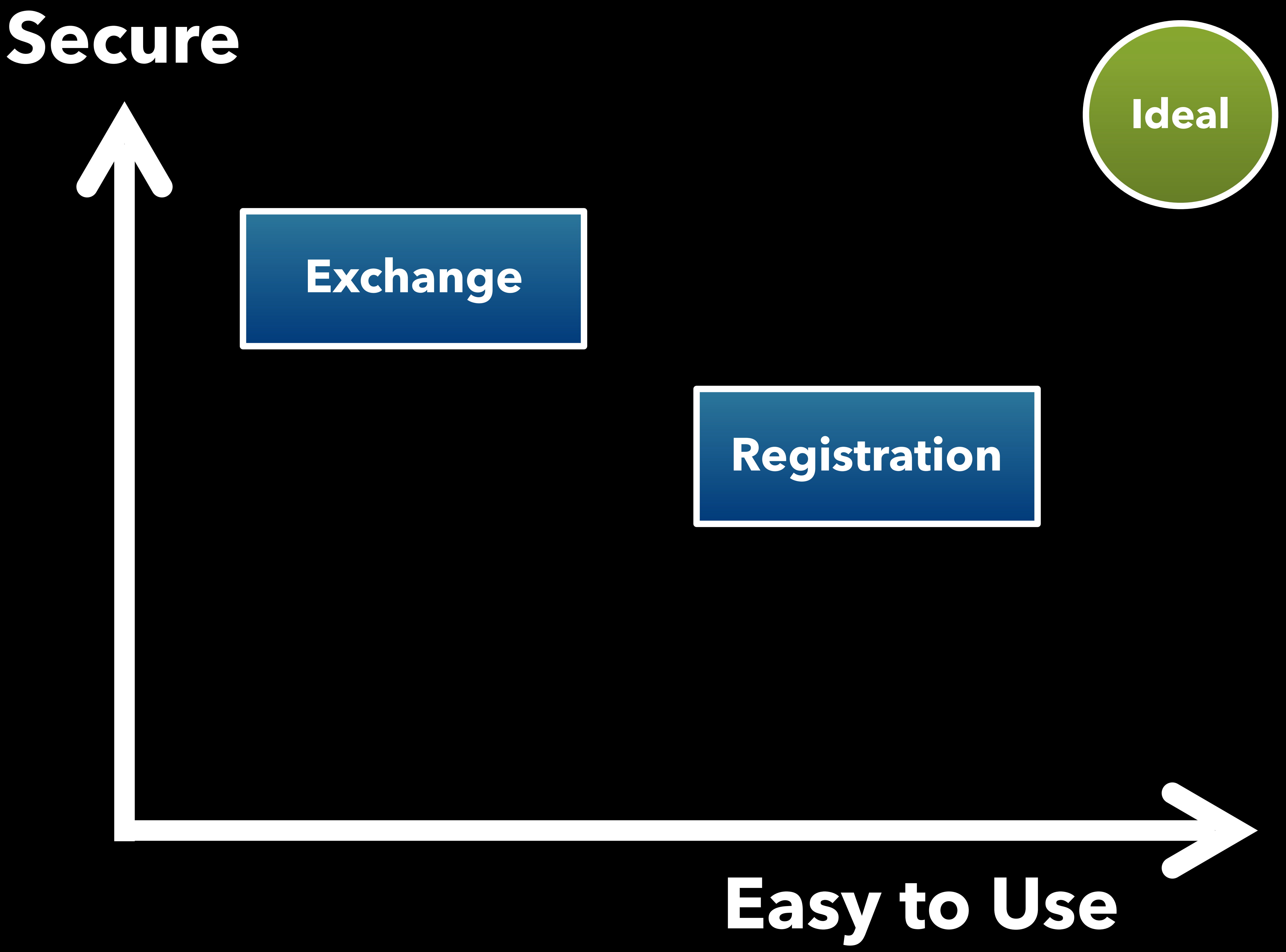
[1] W. Tong, S. Gold, S. Gichohi, M. Roman, and J. Frankle. Why King George III can encrypt. 2014



## Exchange (PGP-like) Model

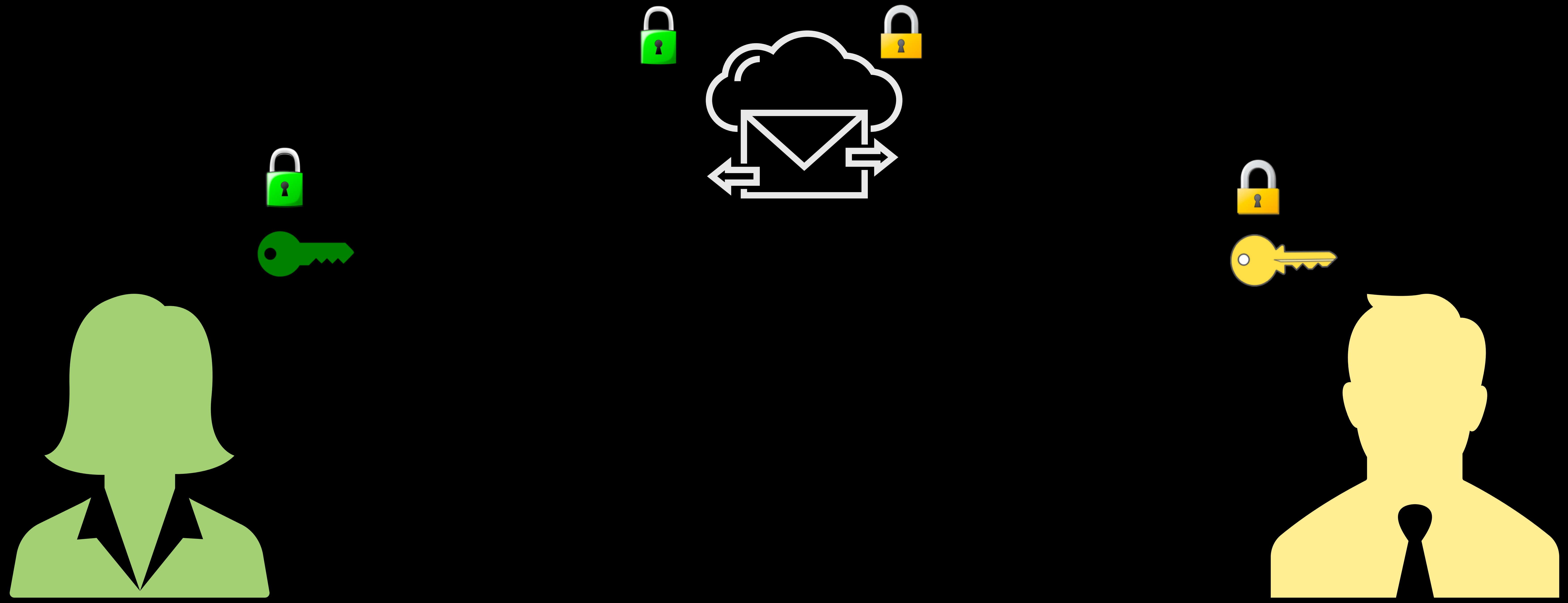
End users exchange public locks manually out of band.

The usability has been improved, but still not popular.


Secure
Ideal
Exchange
Registration
Easy to Use

# Registration Model

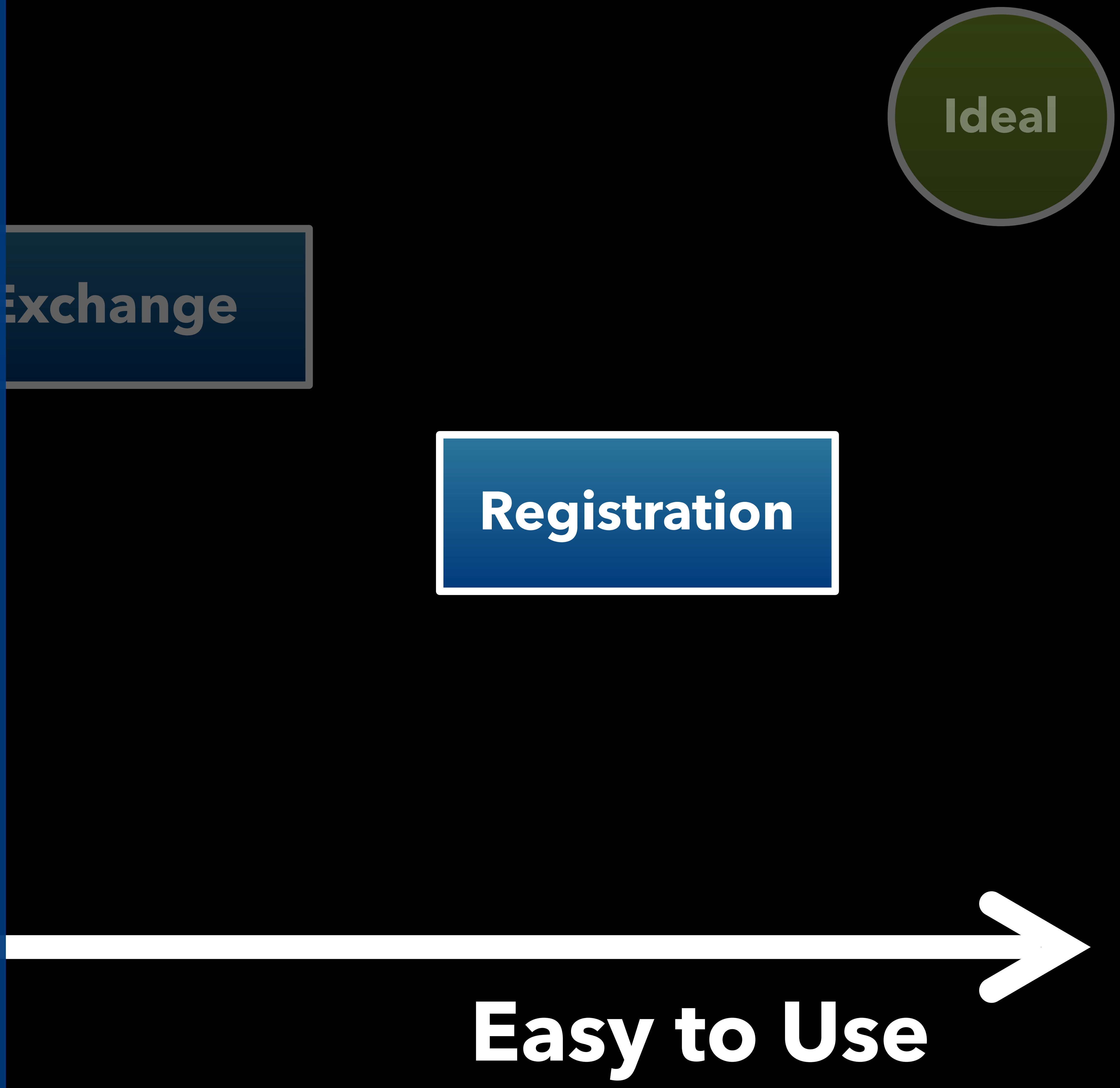
central server stores public locks



# Registration Model

A central server will be responsible for distributing public locks.

Alarms some security experts because of the trust (and government leverage) over that central server



How do
**general users consider the security and usability tradeoffs**
between exchange and registration models?

METHODOLOGY

## Participants

Email list-servs

Online platforms, e.g. Craigslist

Flyers

within-subjects design:

# METHODOLOGY

## Participants

Email list-servs

Online platforms, e.g. Craigslist

Flyers

within-subjects design:

## First Model

High-level concepts

Complete email tasks

Learn about security

Feedback

## Second Model

High-level concepts

Complete email tasks

Learn about security

Feedback

# METHODOLOGY

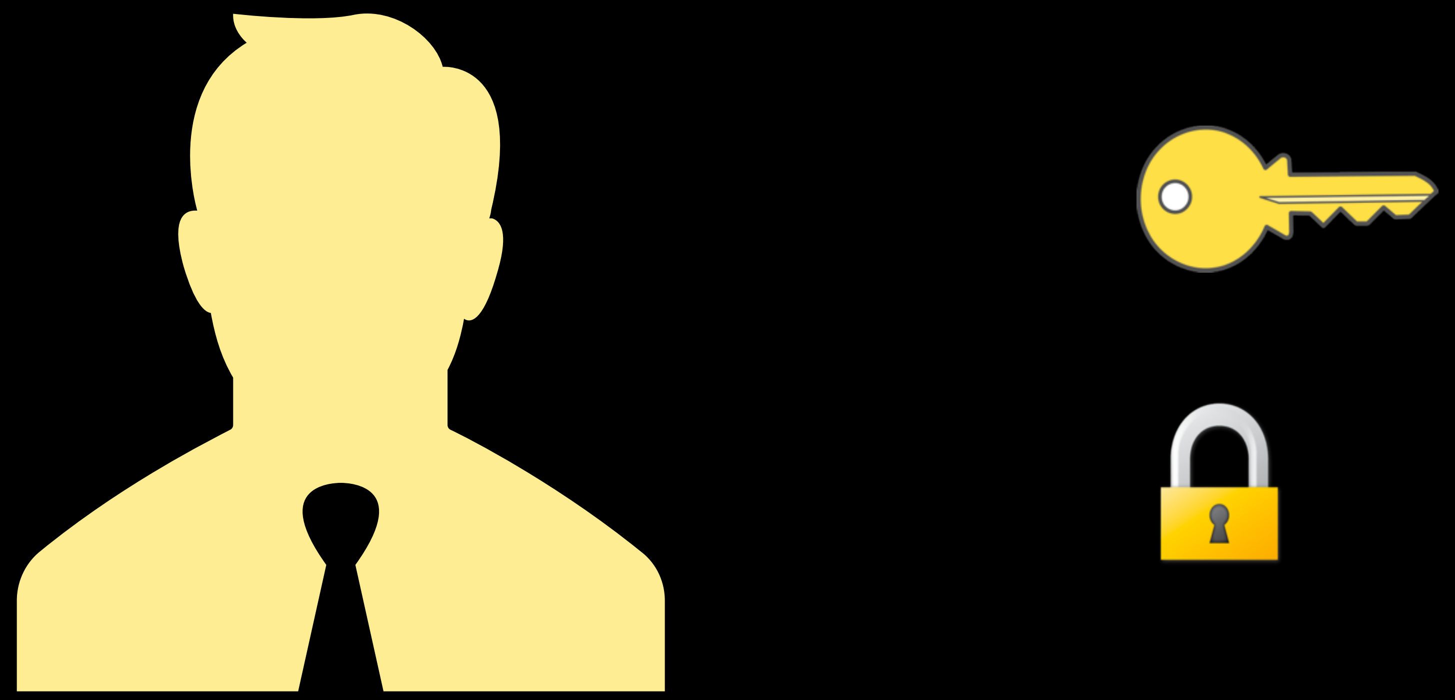
Exchange Model

Registration Model

Mailvelope

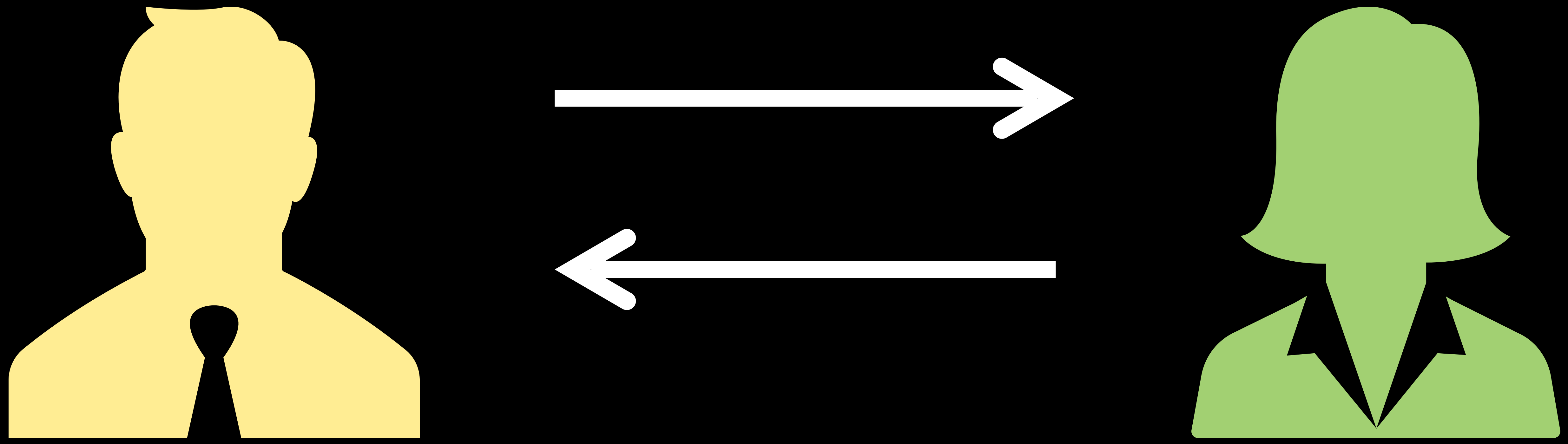
# Email Tasks for Introducing Concepts

## 1. Generate/Register public lock/private key pair



# Email Tasks for Introducing Concepts

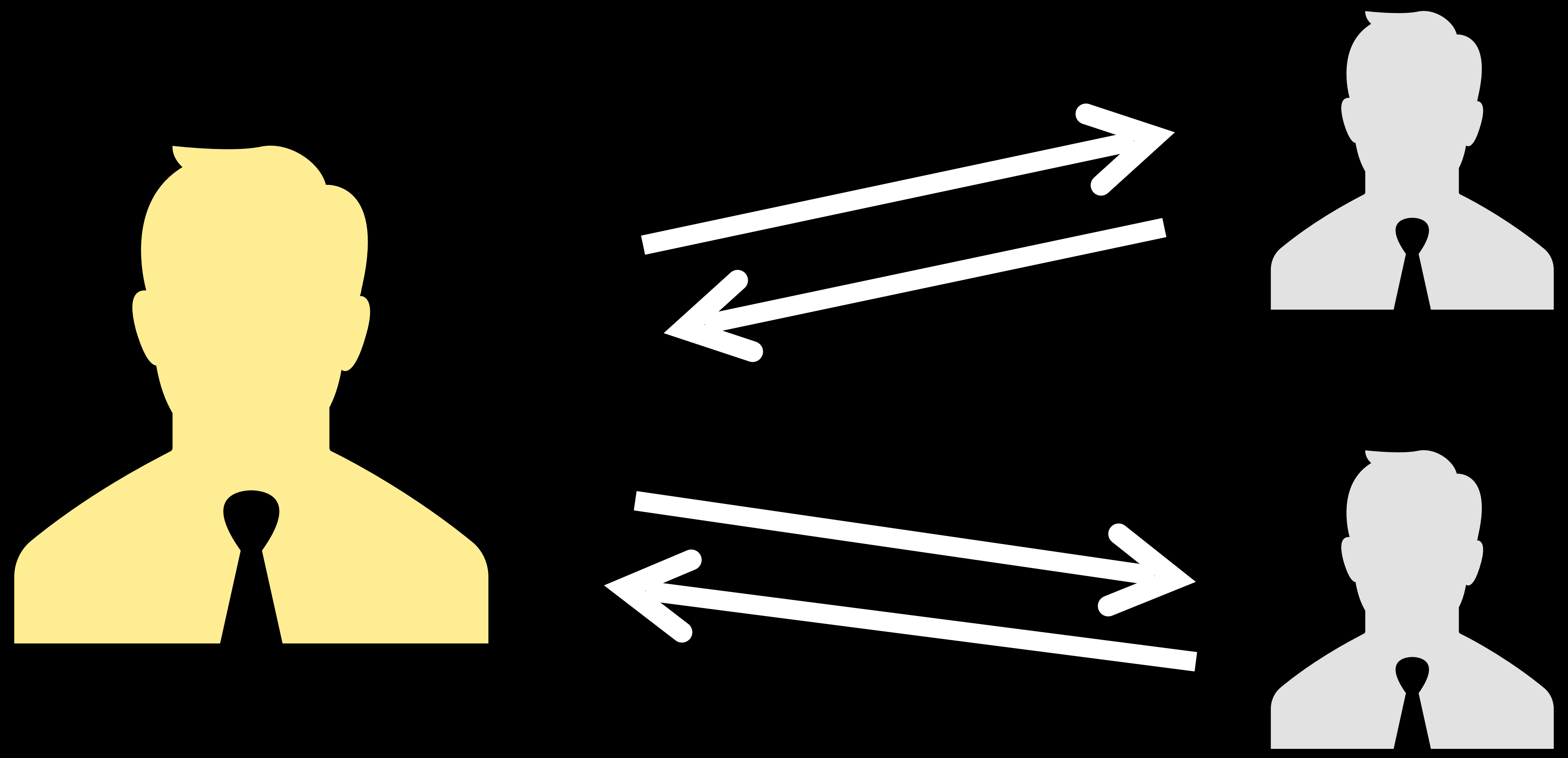
## 2. Exchange email with Alice



*Participants don't need to exchange public locks in the *registration model*

# Email Tasks for Introducing Concepts

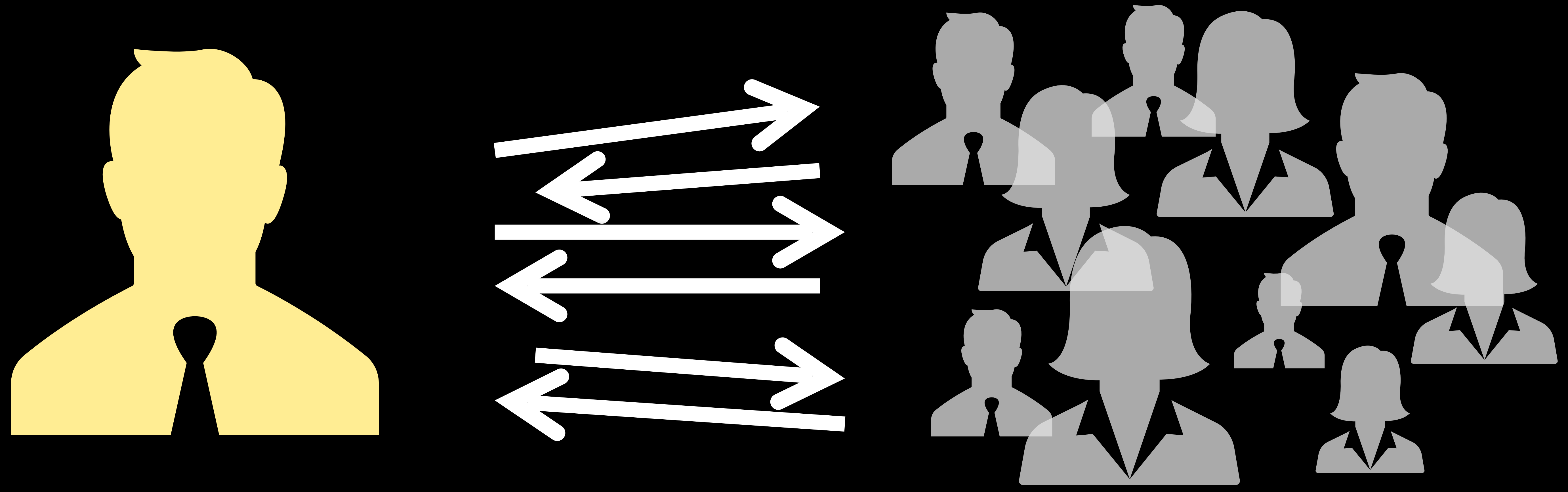
## 3. Exchange email with Bob and Carl



*Participants don't need to exchange public locks in the *registration model*

# Email Tasks for Introducing Concepts

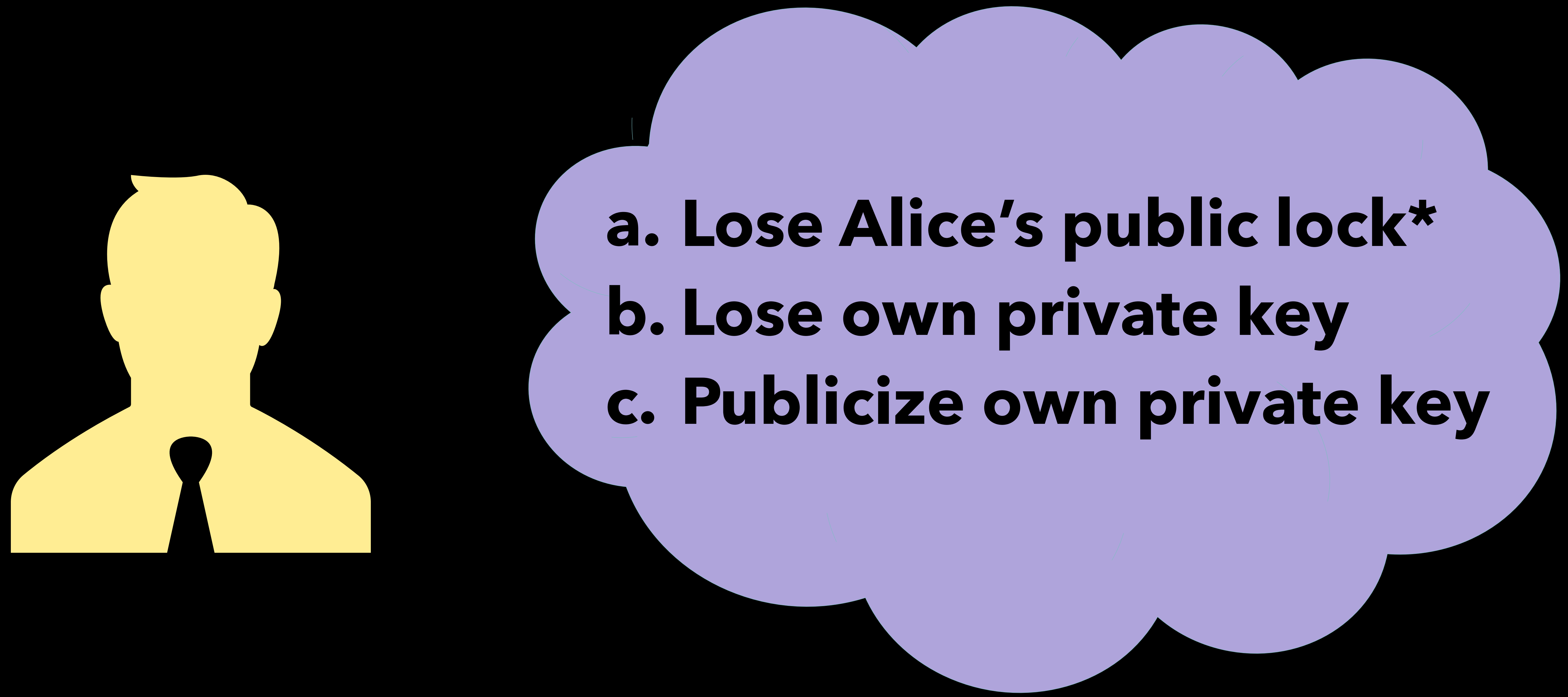
**4. Imagine exchanging email with ten people**



*Participants don't need to exchange public locks in the *registration model*

# Email Tasks for Introducing Concepts

## 5. Think about misconfigurations



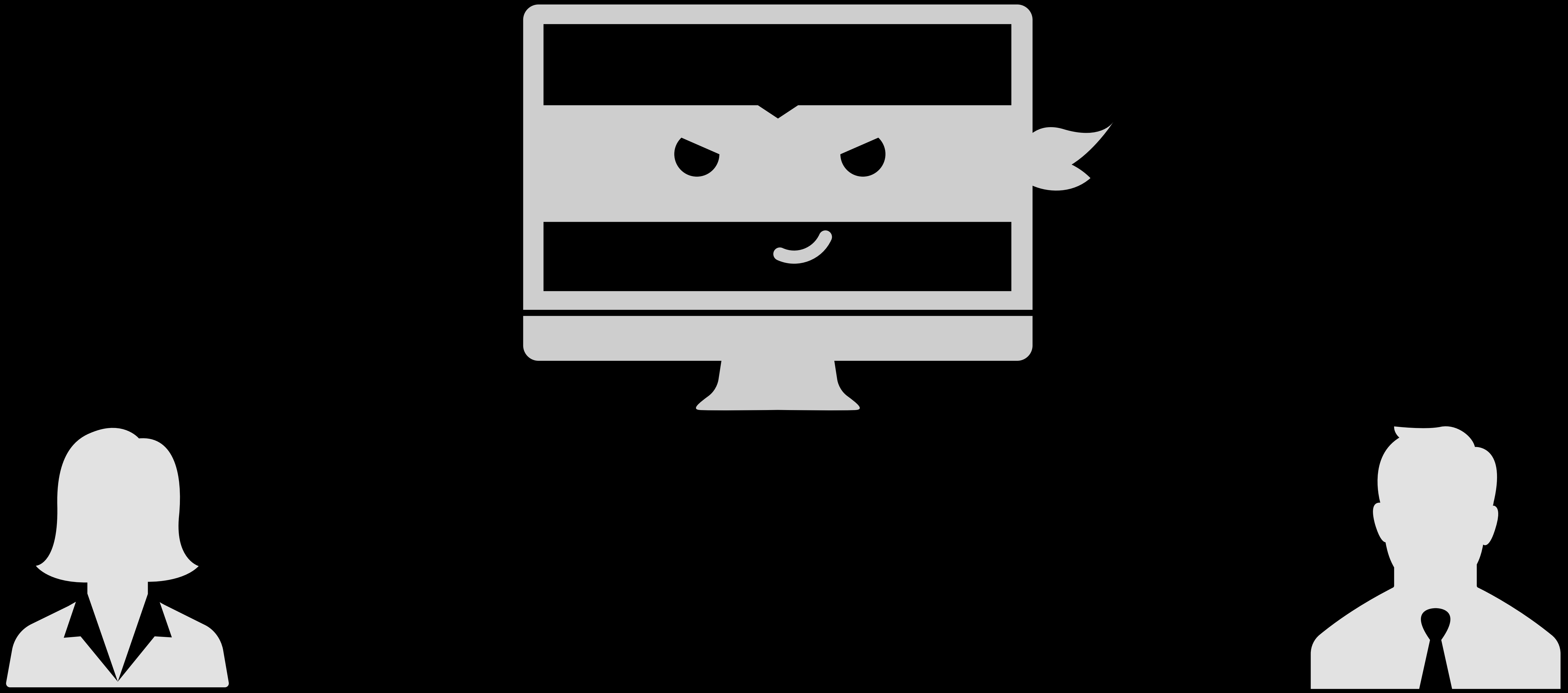
a. **Lose Alice’s public lock***

b. **Lose own private key**

c. **Publicize own private key**

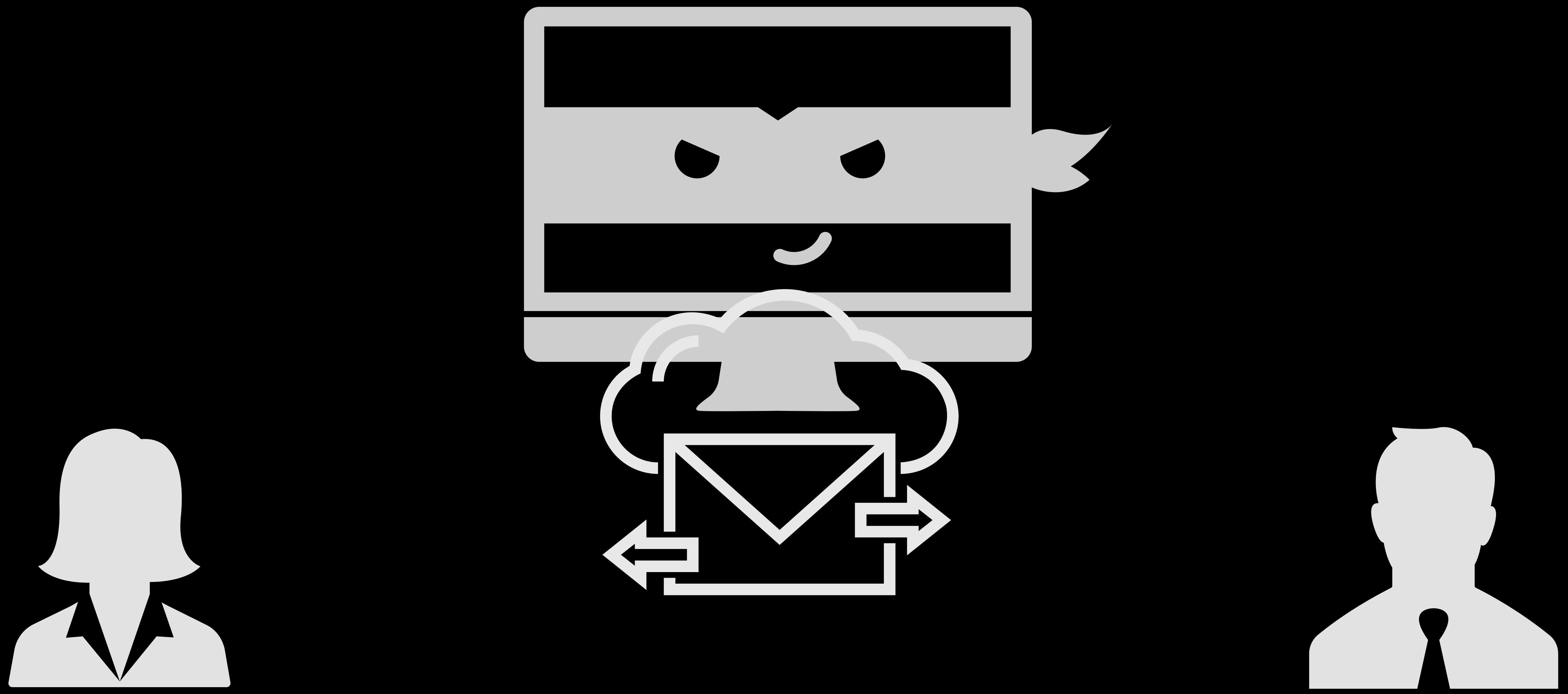
*There is no such task in *registration model*

## Security Learning: **Exchange Model**



“This threat doesn’t happen usually, because it requires Mallet to have much power and resources to achieve this.”

# Security Learning: **Registration Model**



“[In primary registration model] you need to trust the email provider”

# Security Learning: **Registration Model CaaS**[1]

“[In CaaS model] you need to trust the two parties don’t collaborate.”

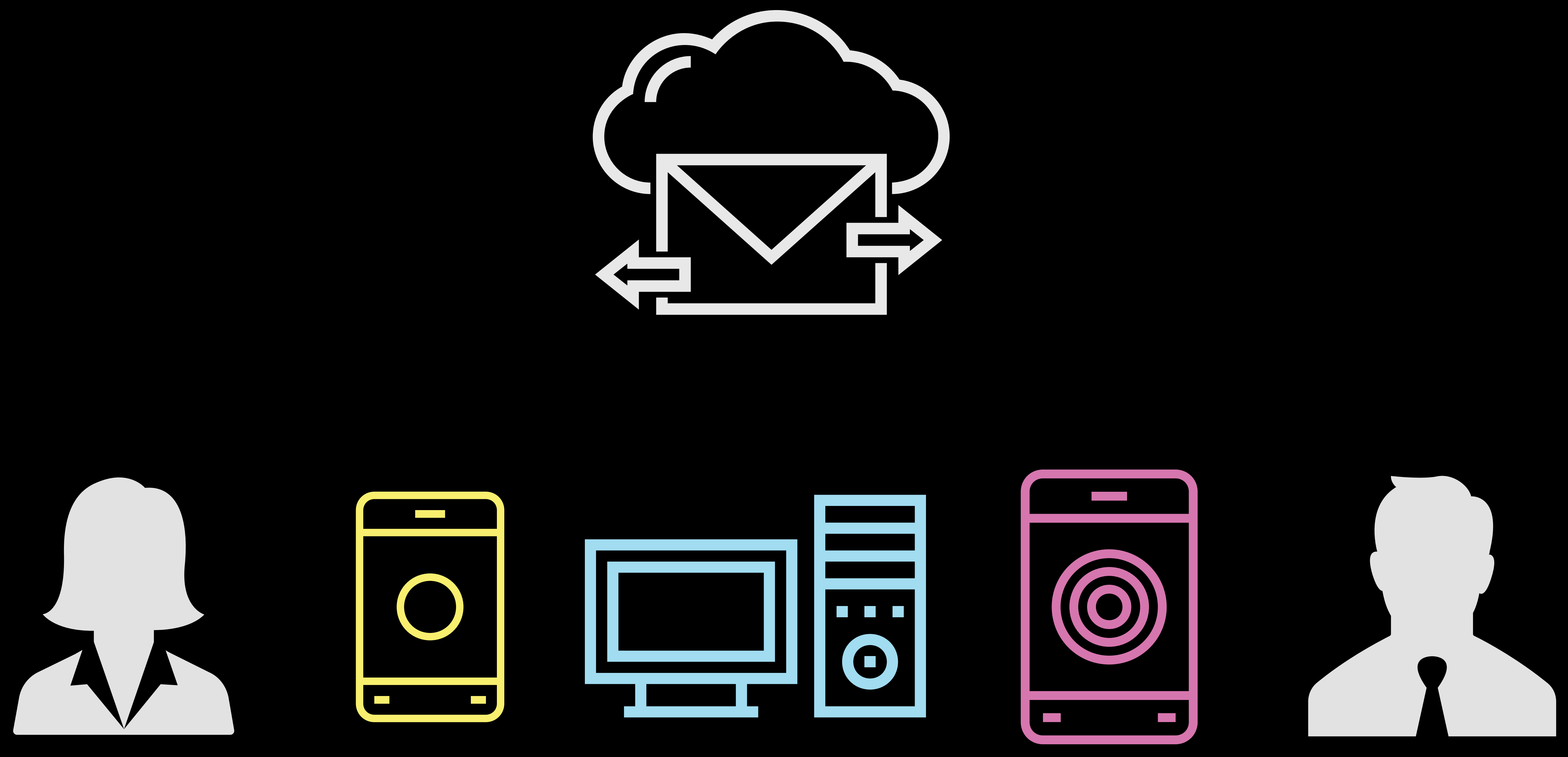
[1] S. Fahl, M. Harbach, T. Muders, and M. Smith. Confidentiality as a Service – usable security for the cloud. In Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on, pages 153–162, June 2012.

# Security Learning: **Registration Model CaaS**[1]

"[In CaaS model] you need to trust the two parties don't collaborate."

[1] S. Fahl, M. Harbach, T. Muders, and M. Smith. Confidentiality as a Service – usable security for the cloud. In Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on, pages 153–162, June 2012.

# Security Learning: **Registration Model Auditing**[1]



“[In auditing model] you need to trust the auditors and/or the software on your devices.”

[1] M. S. Melara, A. Blankstein, J. Bonneau, E. W. Felten, and M. J. Freedman. CONIKS: Bringing key transparency to end users. In 24th USENIX Security Symposium (USENIX Security 15), pages 383–398. USENIX Association, Aug. 2015.

# PARTICIPANTS

**80%
Between
Ages of
18-34**

**Gender:
Male 60%
Female 40%**

**Occupation:
40% reported
jobs or majors
in computing,
math and
engineering**

**Security Expertise**[1]
Only 2 out of 52
scored 3 or higher
(out of 5.5)

# Analysis

**Quantitative Analysis**

5-point Likert scale responses

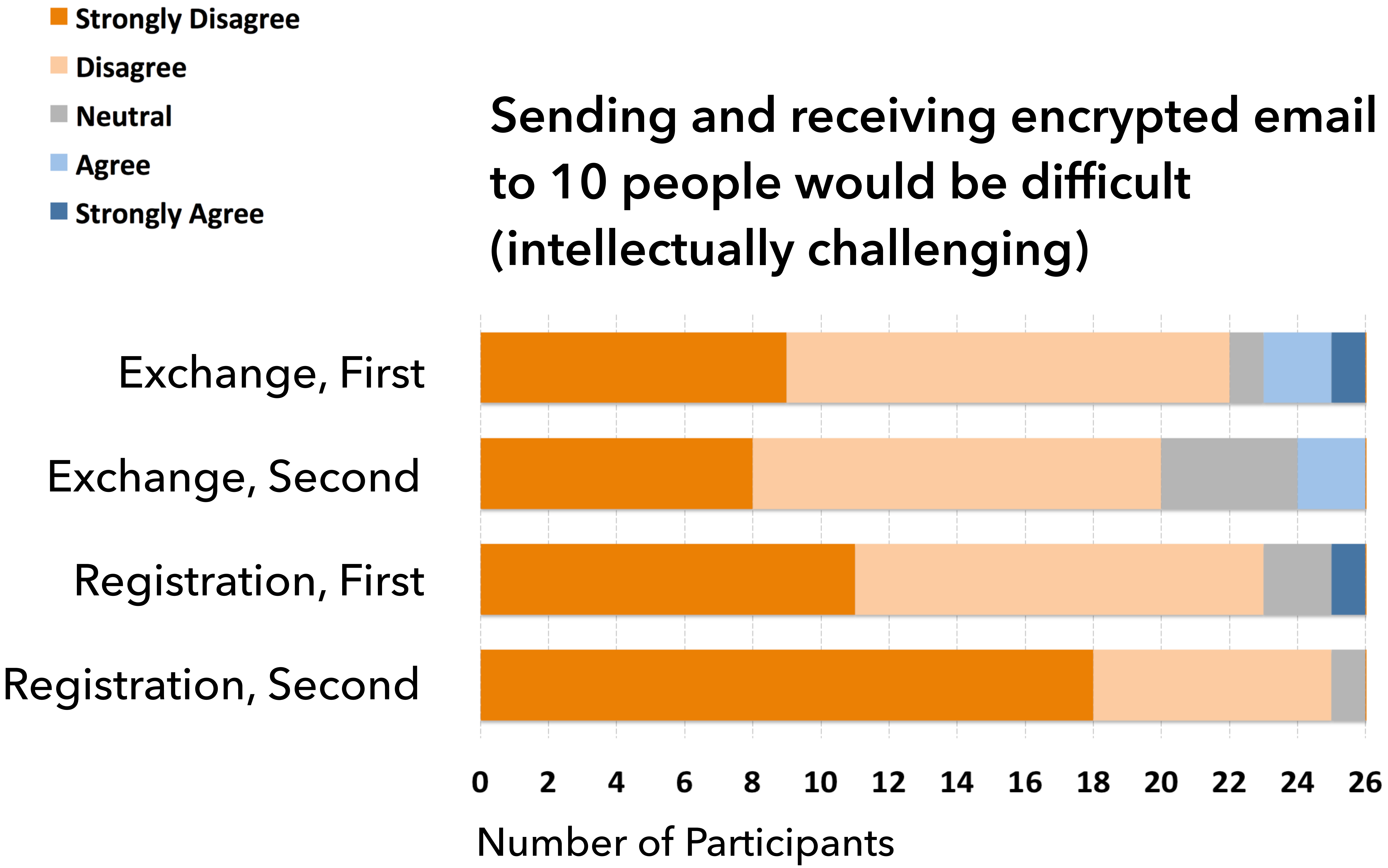
Cumulative-link mixed regression model (CLMM)

**Qualitative Analysis**

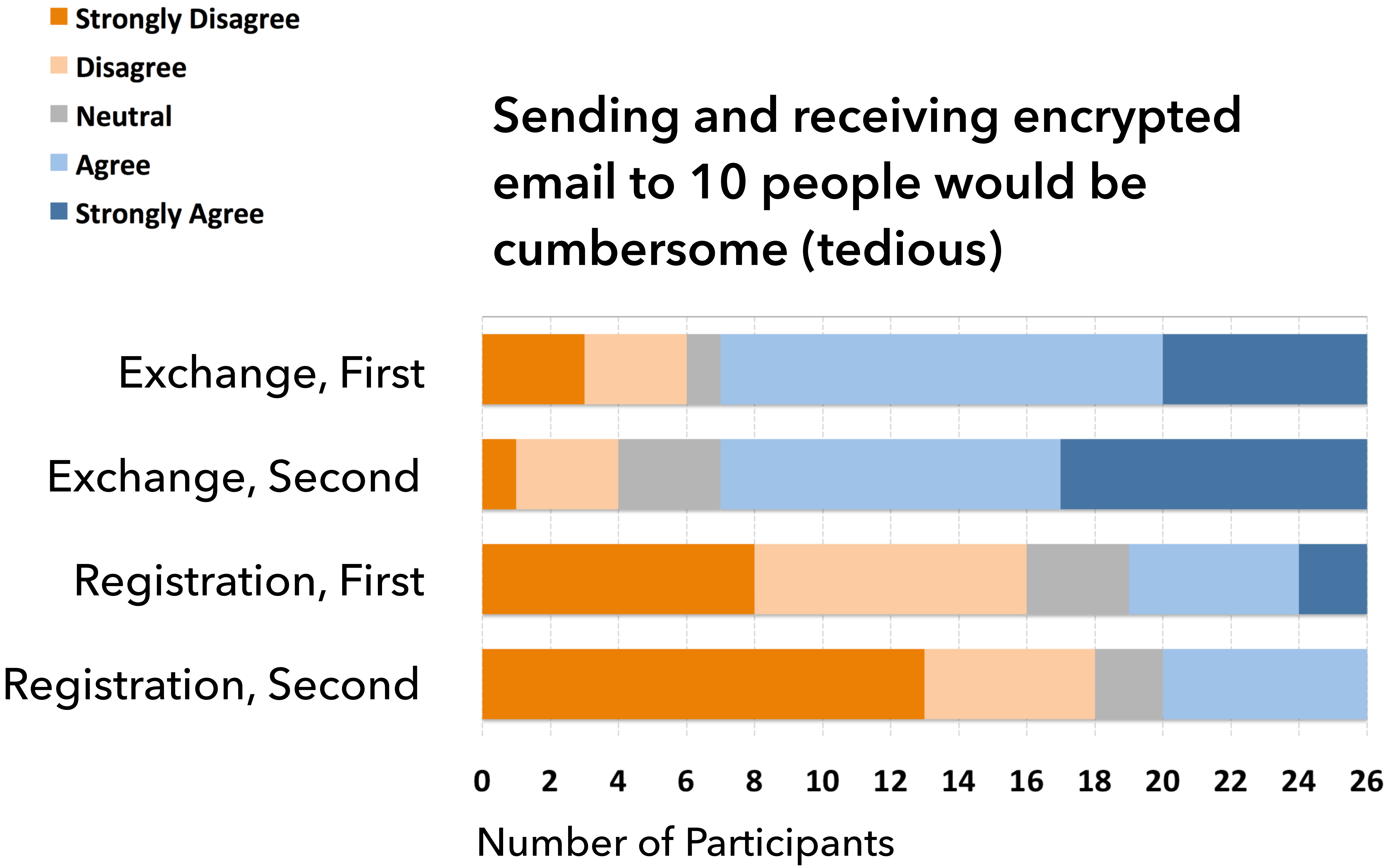
Open coding independently by two researchers

Met to resolve all differences

# RESULTS



Sending and receiving encrypted email to 10 people would be difficult (intellectually challenging)



## Sending and receiving encrypted email to 10 people would be cumbersome (tedious)

RESULTS

***Exchange model*** **was dramatically more cumbersome and somewhat more difficult.**

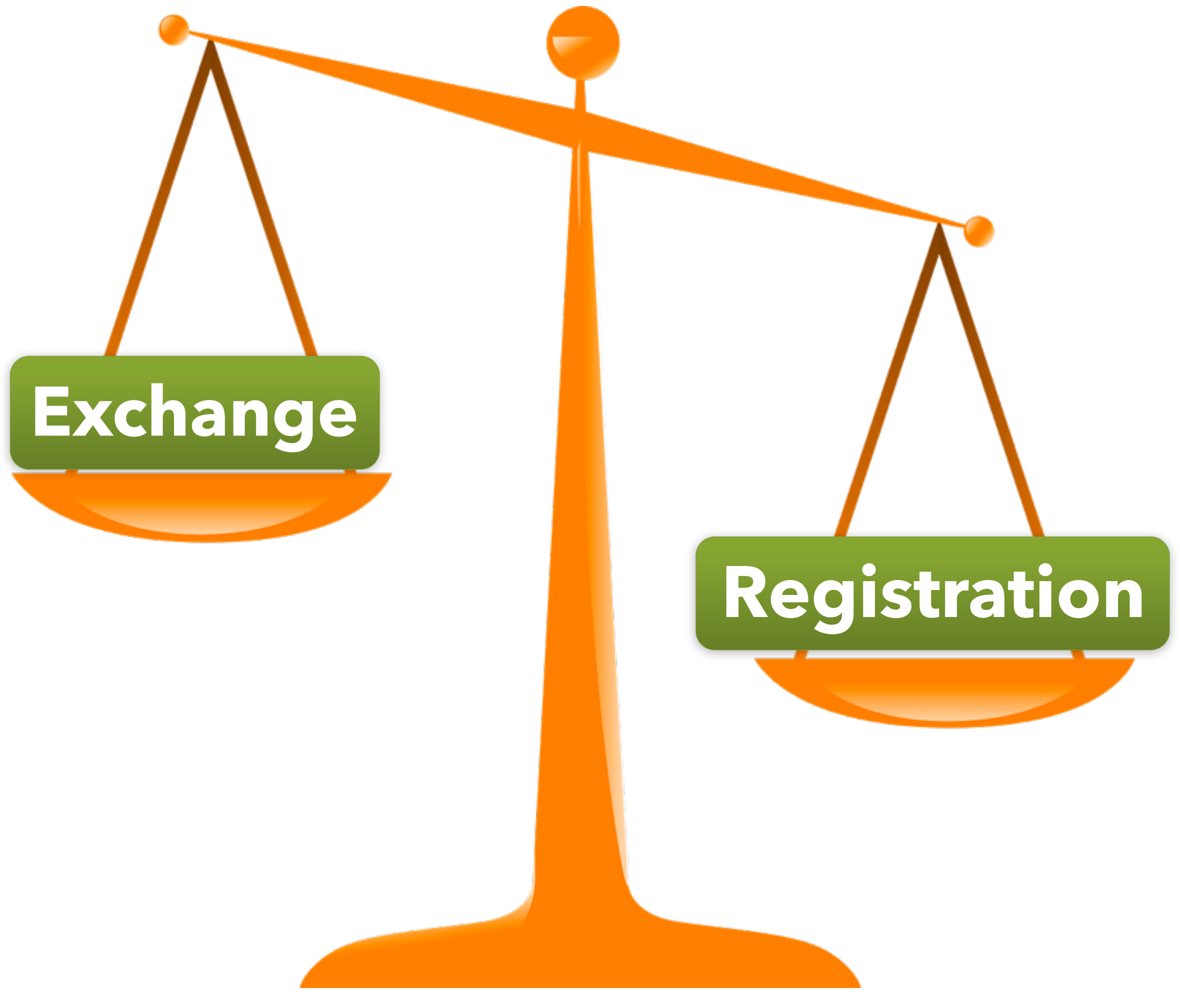
**“(The exchange model is) time consuming, especially sending urgent emails. I have no choice but to wait for (the correspondent’s public lock).”**

*– ES9*

# Security Comparison

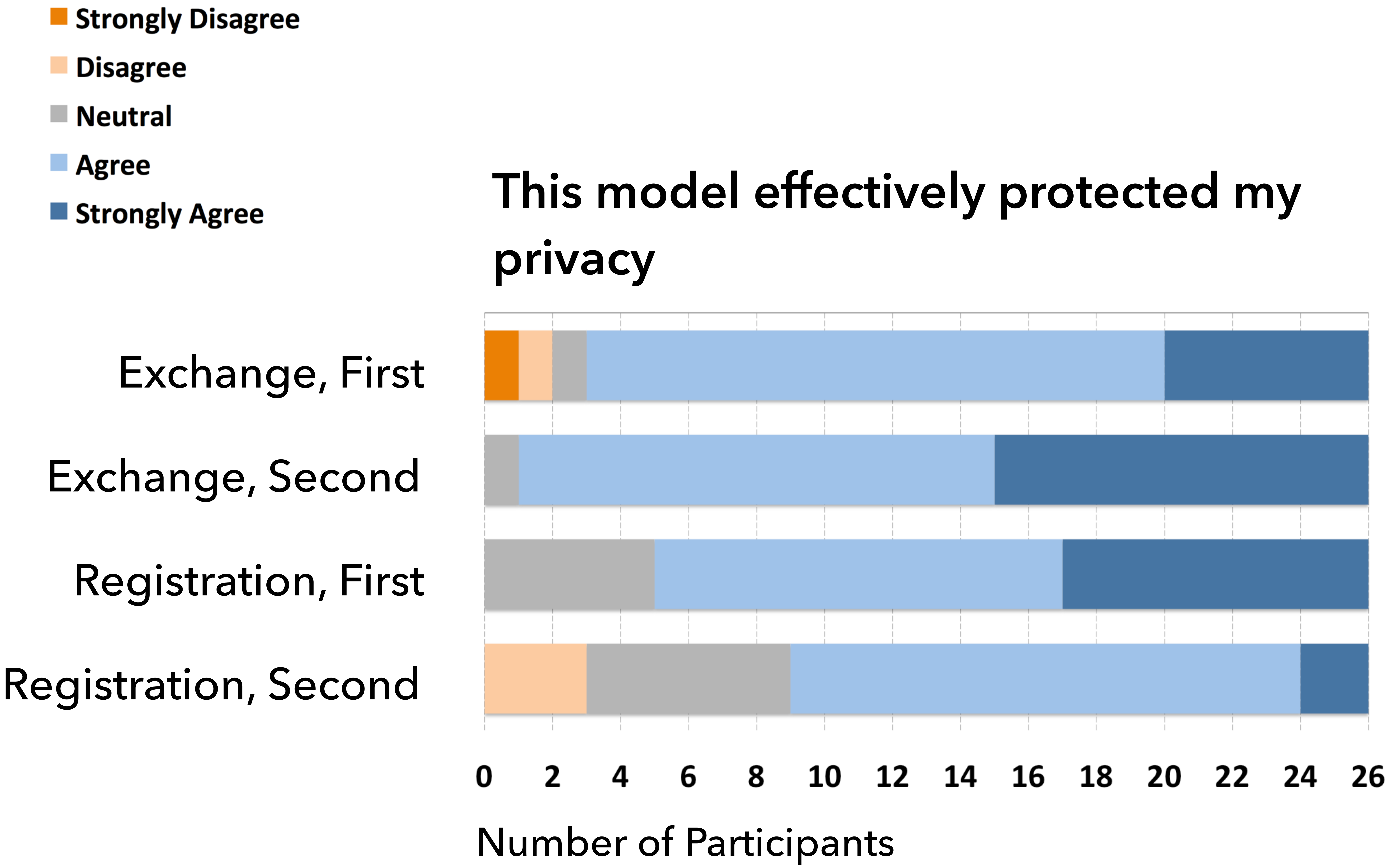
## The Perceived Security Gap **Is Small**

**Manual effort may lead to vulnerability**



**Some concern but generally trusted**

# RESULTS


Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree
This model effectively protected my privacy
Exchange, First
Exchange, Second
Registration, First
Registration, Second
0
2
4
6
8
10
12
14
16
18
20
22
24
26
Number of Participants

## RESULTS

**48 (out of 52) trusted the exchange model.**

**38 trusted the registration model.**

**The order participants saw each model played a significant role:**

> **participants who saw registration model first were more comfortable with it.**

## Exchange model: manual effort may lead to vulnerability

More than half were concerned about the security of the medium used to exchange locks.

“There are too many exchanges between different people. Exchanging [locks] to many people may go wrong.”

– RT7

## (Primary) Registration model: some concern but generally trusted

10 participants trusted their own email provider.

7 participants were specific about which kind of providers they would trust:

> “(Big companies like) Google and Yahoo! don’t do such things [violate users’ privacy], unless the government forces them to do so. In general, it’s secure."
>
> – *RT10*

## CaaS and auditing models: some additional perceived security for registration

“(In CaaS Model) If one party is screwed up, you have another one to protect [your email]. You are still safe.”

*–ES8*

“(In Auditing Model) Obviously it’s extra secure. Other parties are verifying it."

*–ET13*

## CaaS and auditing models: still some concerns

"(In CaaS Model) Involving more systems may complicate the system, so it is less trustful."

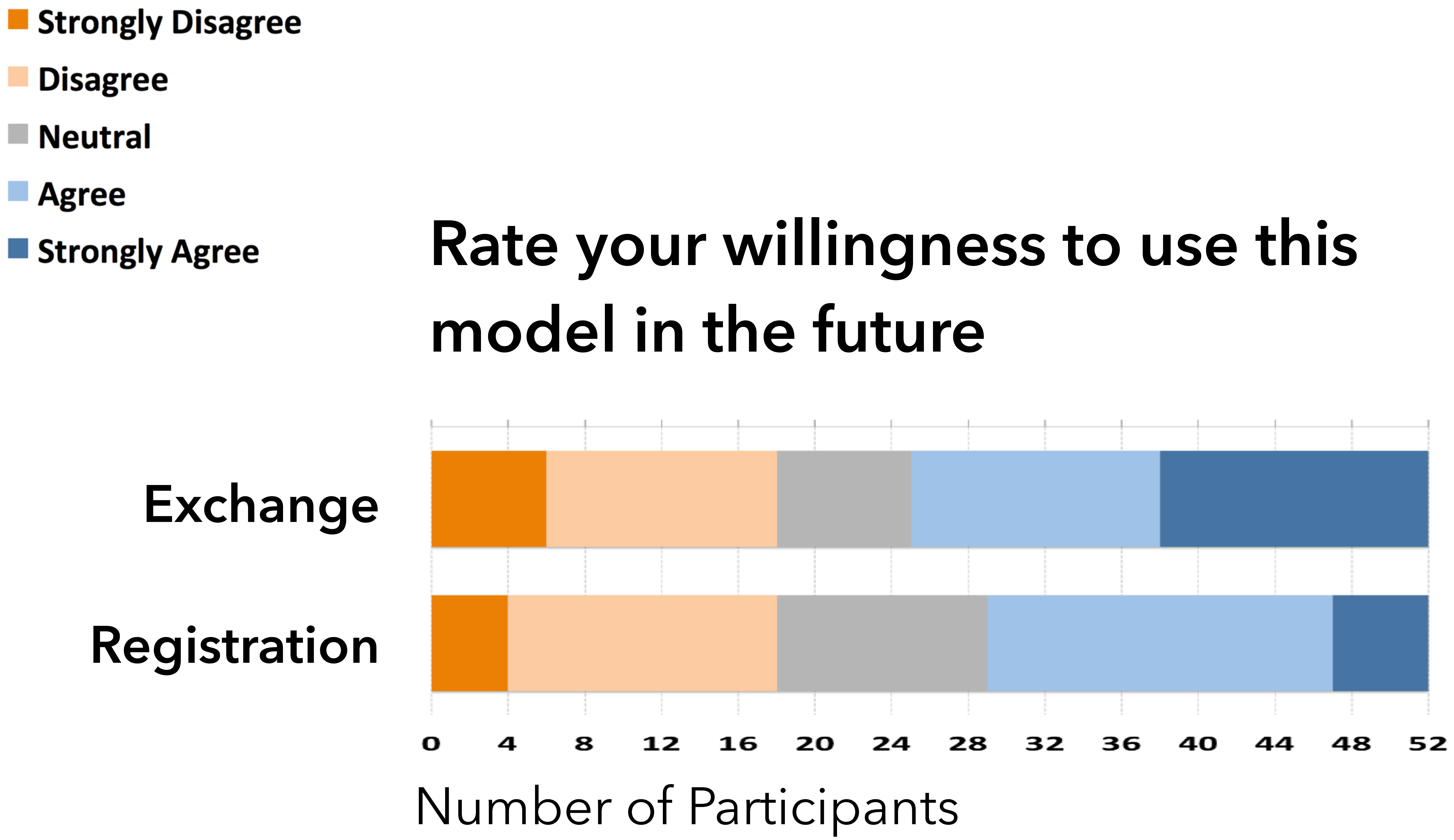
*– RS1*

"(In Auditing Model) I want to know who these auditors are, . . . Their reputations, and whether they are truly independent."

*– RS9*

# RESULTS

## Rate your willingness to use this model in the future



**No significant difference between two models for personal use.**

# When they would use the models

## Registration model

more broad use

15 would use in general email or large scale

## Exchange model

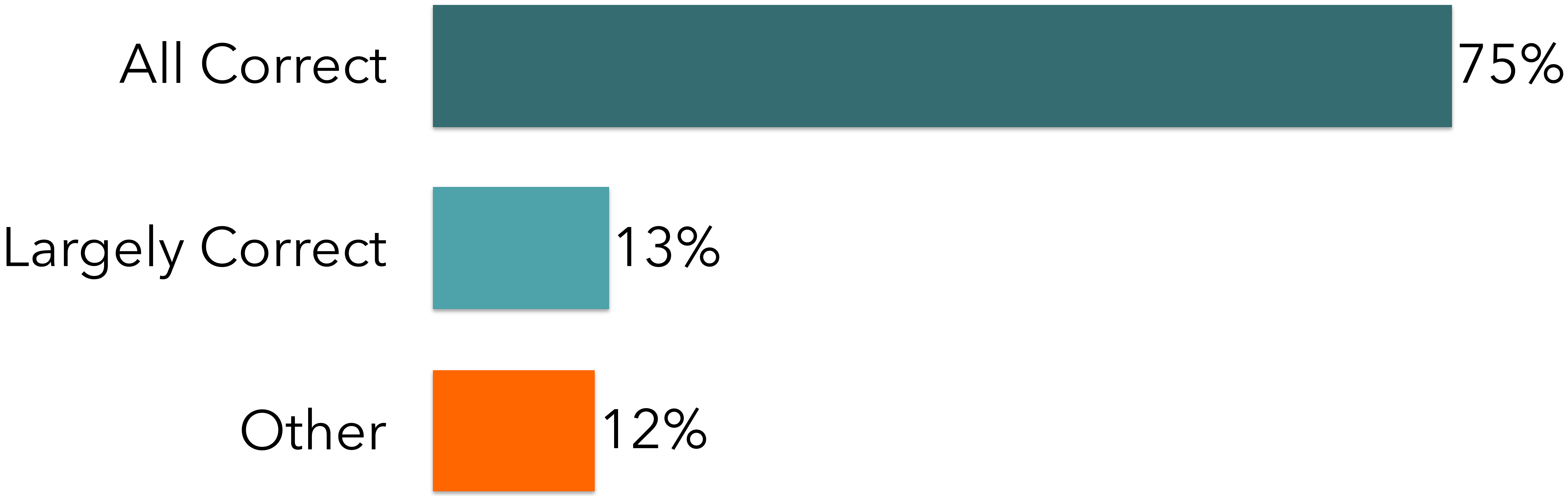
high-security info only

at a small scale only

1 would use in general email

0 large scale

# Handling Misconfigurations



# Handling Misconfigurations

## Losing private key?

One participant mentioned recovering keys from a backup (such as a USB drive) rather than generating a new key pair.

"I will send my email to a third person I trust, and ask that person to encrypt the email for me and send to my recipients. Similarly, he will decrypt the [response] email for me and forward it to me."

# Participants explicitly made tradeoffs among security and usability features.

RT13, who said he would not use the exchange model, commented that “The negotiating process maybe gives me safer feelings, more protection. But on the other hand . . . the disadvantage is it is time consuming, cumbersome, tedious, more complicated, and this is the price I have to pay for more protection."

It is **possible to explain** the high level concepts and risks of encryption to users.

Place users in the context, and trust their decisions.

They **can** think about tradeoffs effectively.

The *registration model* is **more convenient** than the *exchange model,* BUT the **perceived security gap** between them is **small**.

We used a near-best-case method for explaining encryption.

It is **possible to explain** the high level concepts and risks of encryption.

Place users in the context, and **trust their decisions**.

They **can** think about tradeoffs effectively.

The *registration model* is **more convenient** than the *exchange model,* BUT the **perceived security gap** between them is **small**.

# An Inconvenient Trust

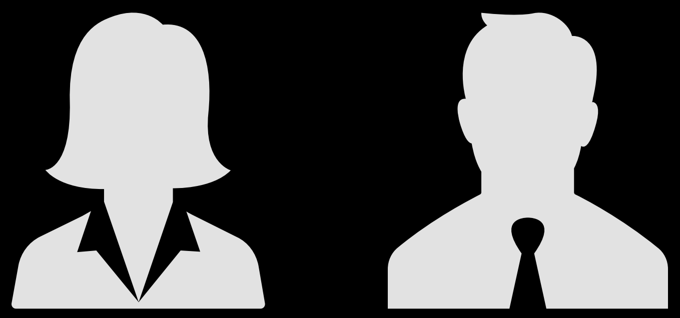
User Attitudes toward Security and Usability Tradeoffs for Key-Directory Encryption Systems

*with Wei Bai, Doowon Kim, Moses Namara, Yichen Qian, and Dr. Michelle L. Mazurek*

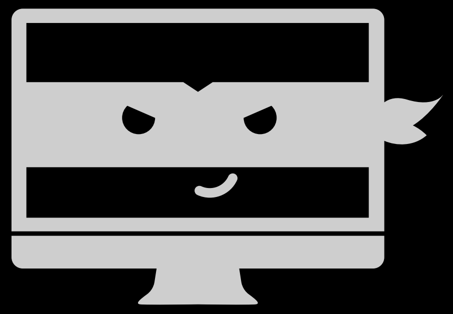
**Patrick Gage Kelley**

@patrickgage

## Icon credits



Gregor Črešnar



Adriana Danaila

Icon Fair

# An Inconvenient Trust

User Attitudes toward Security and Usability Tradeoffs for Key-Directory Encryption Systems

*with Wei Bai, Doowon Kim, Moses Namara, Yichen Qian, and Dr. Michelle L. Mazurek*

**Patrick Gage Kelley**

@patrickgage