The Challenges of Bringing Cryptography From Research Papers to Products

Results From an Interview Study with Experts
USENIX Security 2024

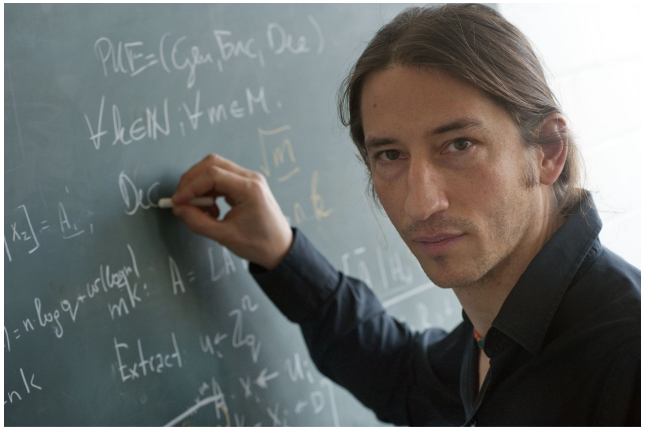
Konstantin Fischer - Ruhr University Bochum
Ivana Trummová - Czech Technical University in Prague
Phillip Gajland - Max Planck Institute for Security and Privacy
Yasemin Acar - Paderborn University
Sascha Fahl - CISPA - Helmholtz-Center for Information Security
M. Angela Sasse - Ruhr University Bochum

“Academic incentive structures do not reward real world impact of cryptography work.”

Would you agree?

Research Goal

“Cryptography Adoption”



Theoretical Cryptography…

?

…ends up…

…in, e.g., an app on an end-users phone.

Research Goal: Investigate Cryptography Adoption

Research Goal: Investigate Cryptography Adoption

RQ1
What steps are involved in cryptography adoption, and who are the relevant stakeholders?

RQ2
What are key obstacles hindering the widespread adoption and correct use of cryptography?

RQ3
What are potential ways to overcome these obstacles?

Method

Expert Interviews

21 Interviews with Cryptography Experts (~90 minutes each)

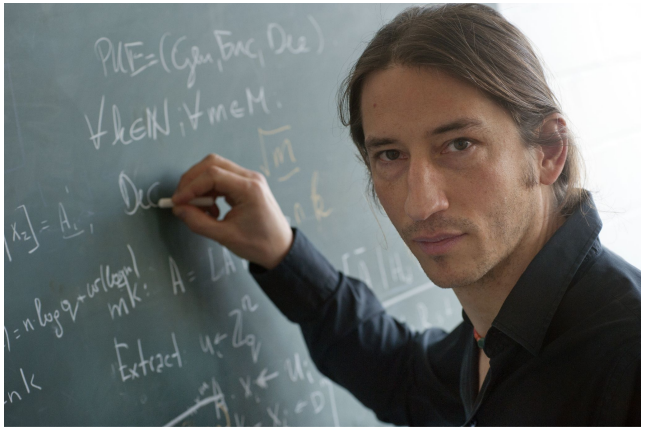
- Backgrounds:
  Academia, Industry, Non-Profit, and Governmental Organisations
- 10+ years of experience in relevant fields (average: ~23 years)
- Multi-experts with experience across multiple cryptography domains

-> Conducted thematic analysis on the interview transcripts

Results

RQ1 - What steps are involved in cryptography adoption, and who are the relevant stakeholders?

Result: RQ1 - Path of Cryptography Adoption

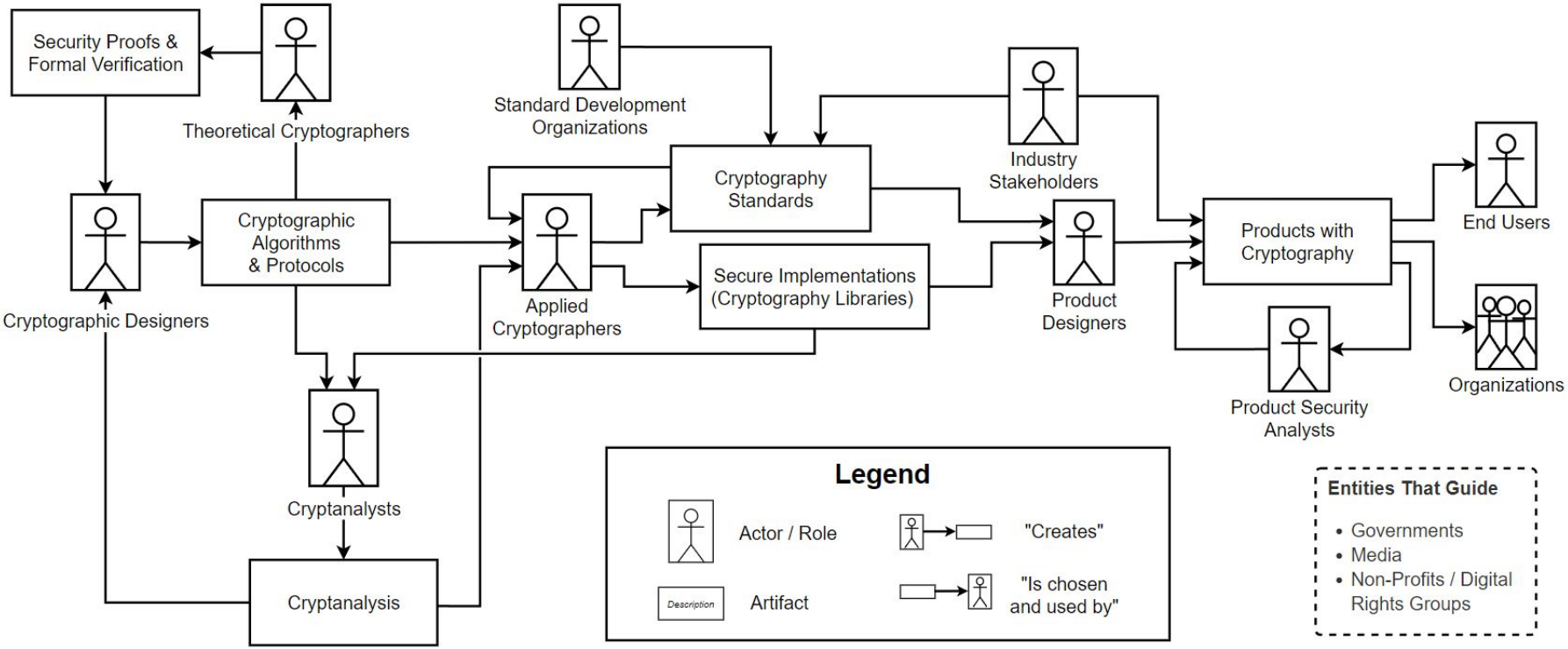


Theoretical Cryptography…

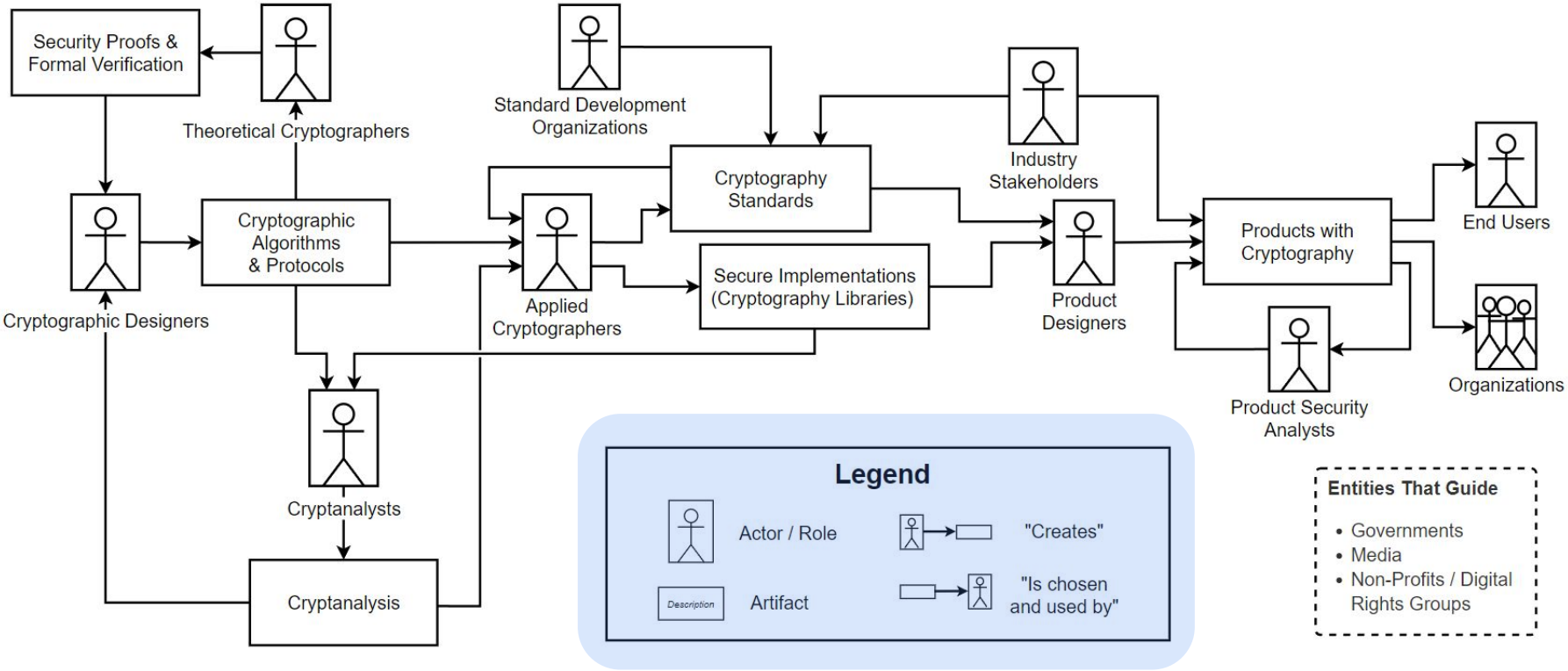
…ends up…

…in, e.g., an app on an end-users phone.

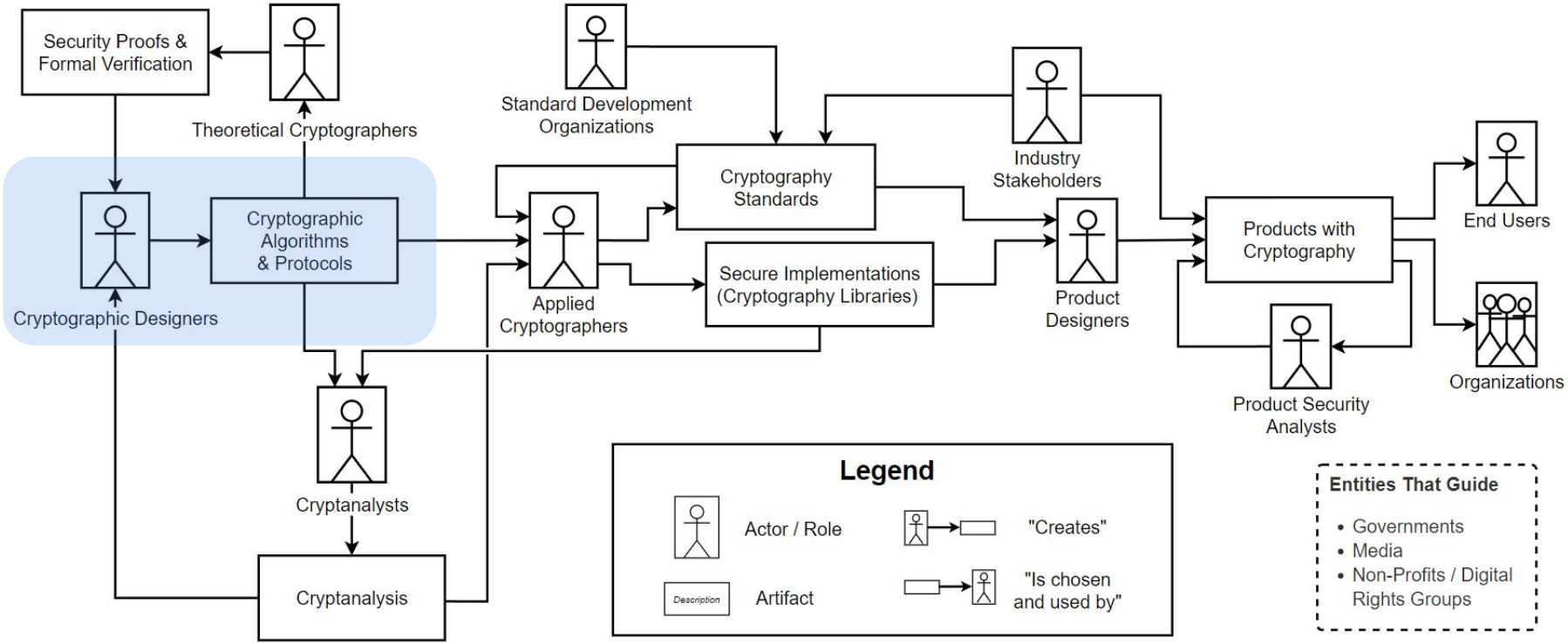
Result: RQ1 - Path of Cryptography Adoption



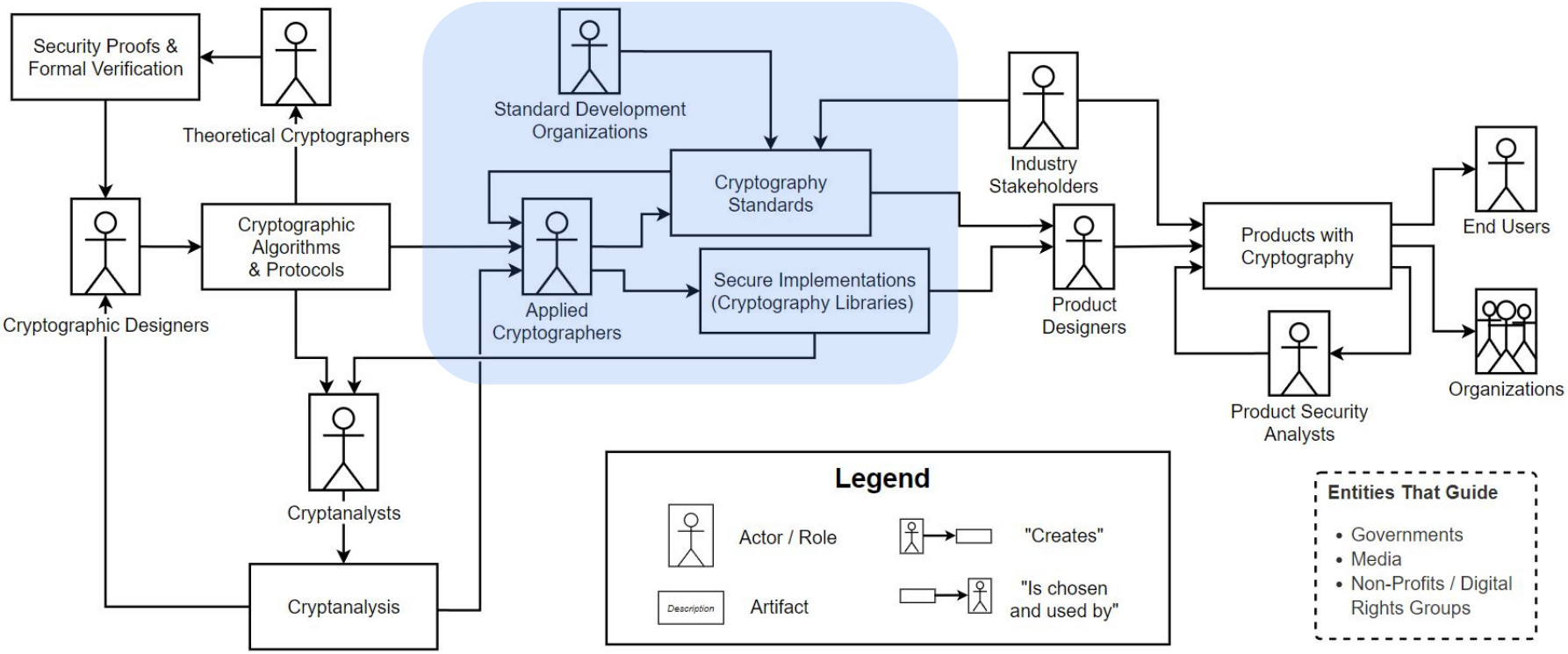
Result: RQ1 - Path of Cryptography Adoption



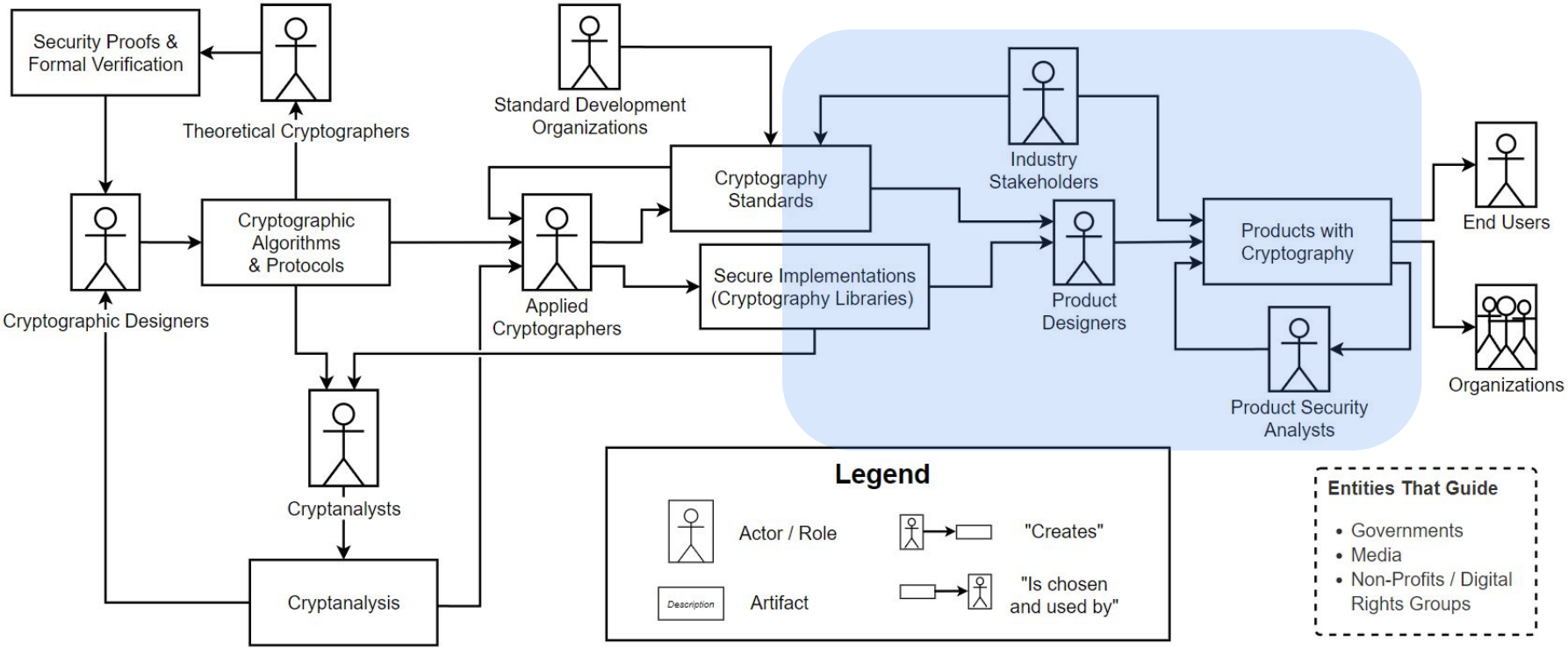
Result: RQ1 - Path of Cryptography Adoption



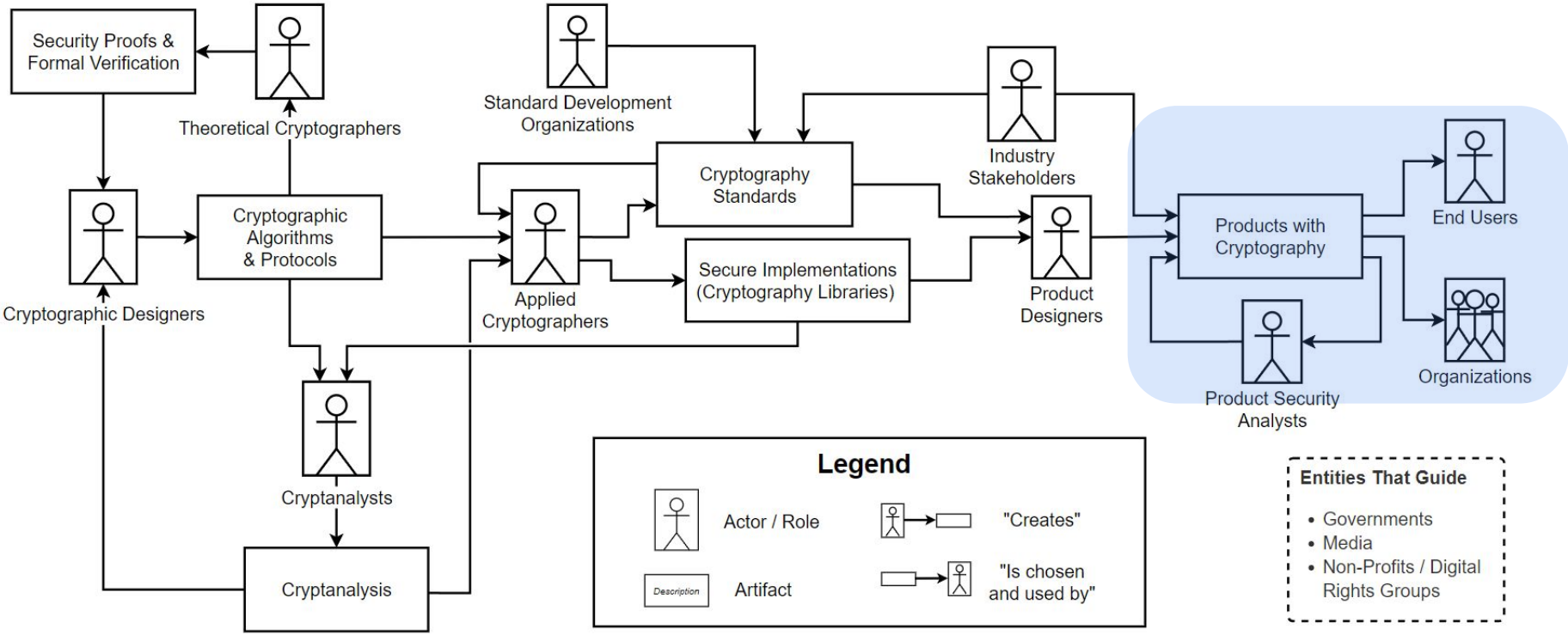
Result: RQ1 - Path of Cryptography Adoption



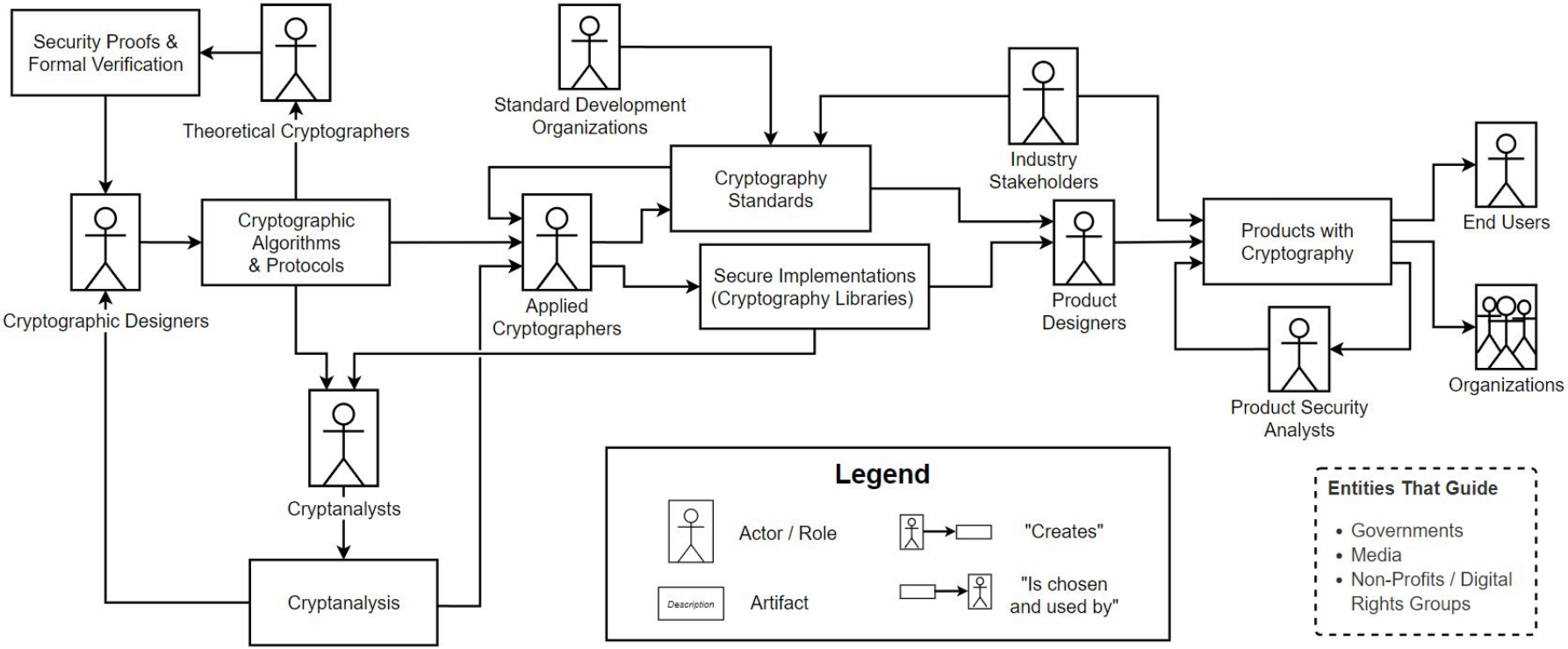
Result: RQ1 - Path of Cryptography Adoption



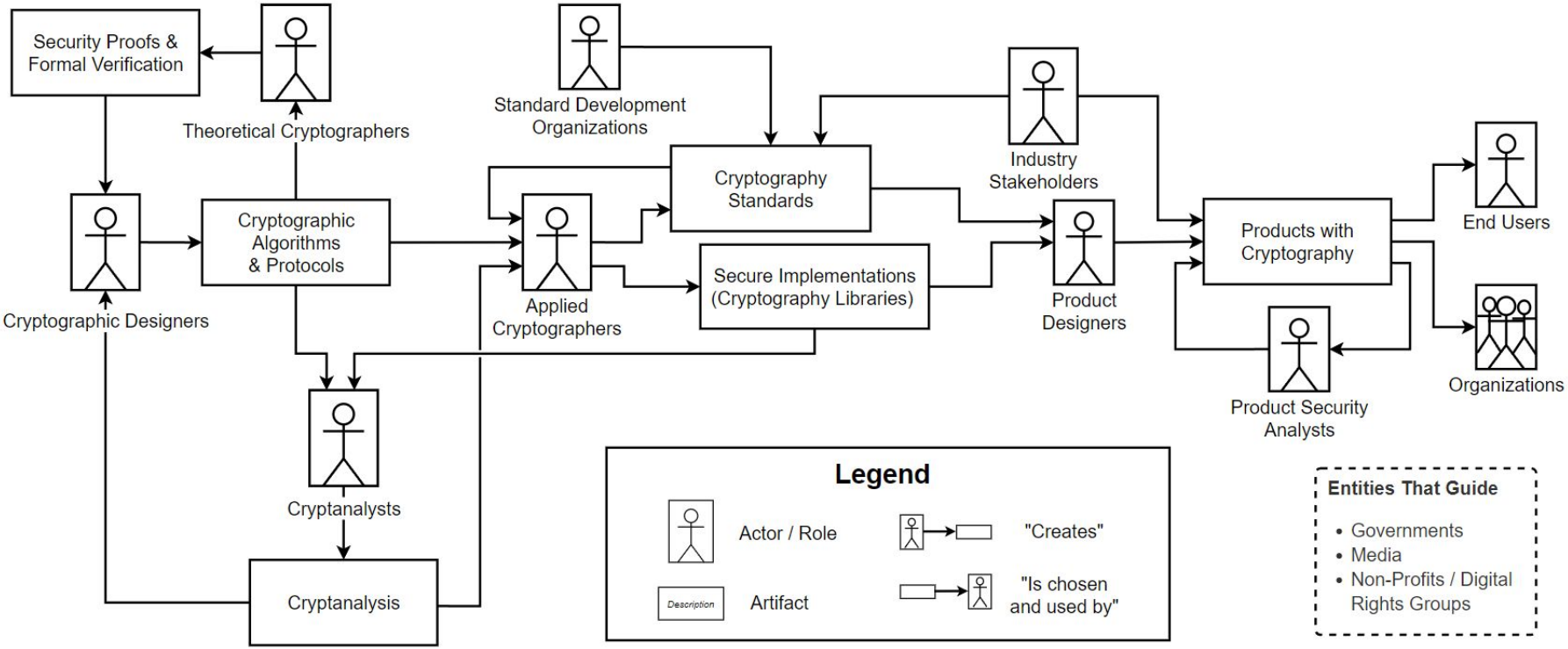
Result: RQ1 - Path of Cryptography Adoption



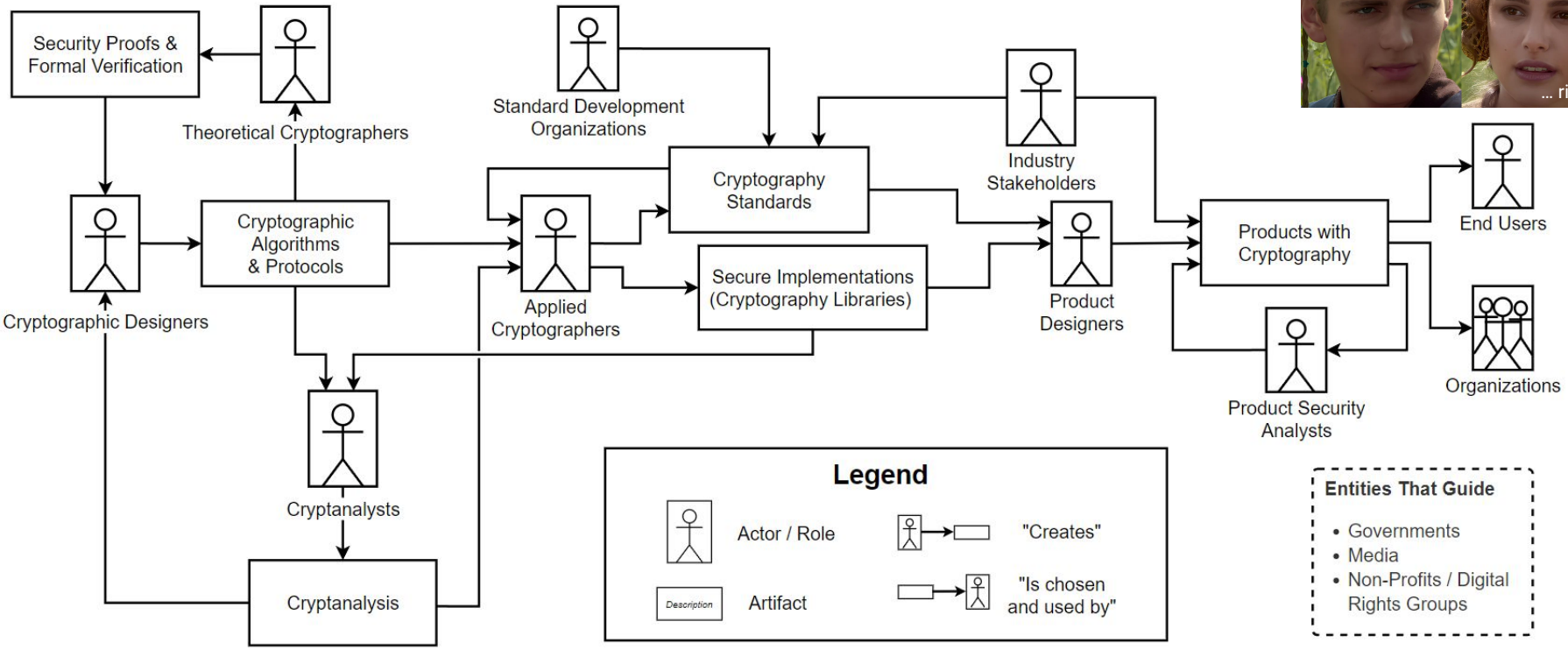
Result: RQ1 - Path of Cryptography Adoption



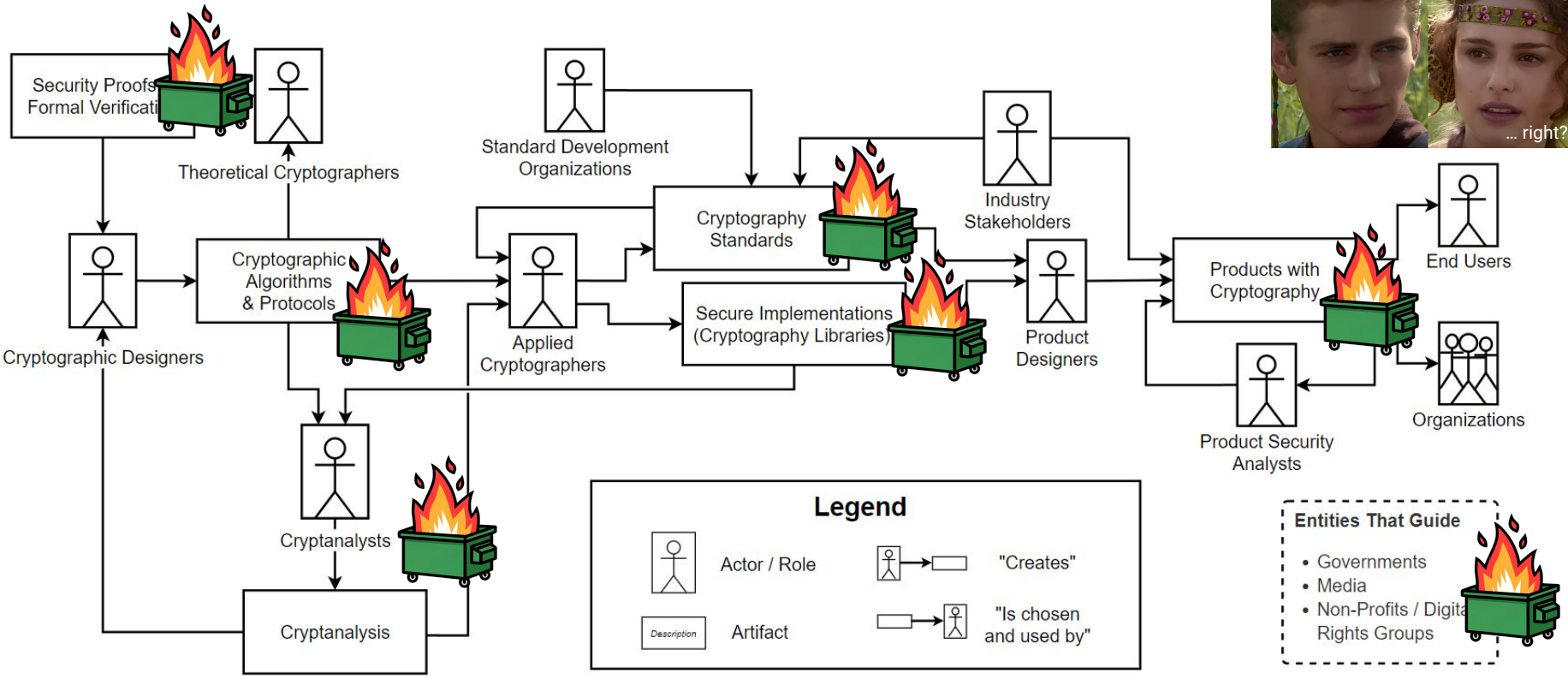
Result: RQ1 - Path of Cryptography Adoption



Result: RQ1 - Path of Cryptography Adoption



Result: RQ1 - Path of Cryptography Adoption



RQ2 - What are key obstacles hindering the widespread adoption and correct use of cryptography?

Result: RQ2 - Themes of Cryptography Adoption Blockers

Through thematic analysis, we identified 5 overarching themes across all interviews.

1. Misaligned or conflicting incentives in academia
2. Challenges in standardization
3. Troublesome or missing reference implementations
4. Communication gaps and unclear responsibilities
5. Usability Issues

Result: RQ2 - Themes of Cryptography Adoption Blockers

Through thematic analysis, we identified 5 overarching themes across all interviews.

1. Misaligned or conflicting incentives in academia
2. Challenges in standardization
3. Troublesome or missing reference implementations
4. Communication gaps and unclear responsibilities
5. Usability Issues

“Practical impact does not get you papers at CRYPTO.”

Result: RQ2 - Themes of Cryptography Adoption Blockers

Through thematic analysis, we identified 5 overarching themes across all interviews.

1. Misaligned or conflicting incentives in academia
2. Challenges in standardization
3. Troublesome or missing reference implementations
4. Communication gaps and unclear responsibilities
5. Usability Issues

“People won’t get much academic credit for spending three years flying to IETF meetings and fine-tuning a standard. So, maybe there’s an academic incentive problem.”

Result: RQ2 - Themes of Cryptography Adoption Blockers

Through thematic analysis, we identified 5 overarching themes across all interviews.

1. Misaligned or conflicting incentives in academia
2. Challenges in standardization
3. Troublesome or missing reference implementations
4. Communication gaps and unclear responsibilities
5. Usability Issues

“People won’t get much academic credit for spending three years flying to IETF meetings and fine-tuning a standard. So, maybe there’s an academic incentive problem.”

“Standardization [. . .] is very, very painful. There are academics who do that. Some in IETF, they are doing it because they feel it’s a socially important thing. . . out of some kind of social duty. But it’s difficult to find those folks!”

Result: RQ2 - Themes of Cryptography Adoption Blockers

Through thematic analysis, we identified 5 overarching themes across all interviews.

1. Misaligned or conflicting incentives in academia
2. Challenges in standardization
3. Troublesome or missing reference implementations
4. Communication gaps and unclear responsibilities
5. Usability Issues

“If you really want people to use [your crypto], you have to have code that they can use. To play with. That is what academics don’t do enough. It has to be a piece of code that is genuine enough that it can be used to do stuff, that is not just what you have said in the paper, but more general use.”

Result: RQ2 - Themes of Cryptography Adoption Blockers

Through thematic analysis, we identified 5 overarching themes across all interviews.

1. Misaligned or conflicting incentives in academia
2. Challenges in standardization
3. Troublesome or missing reference implementations
4. Communication gaps and unclear responsibilities
5. Usability Issues

“The quality [of reference implementations] is very variable because the skill set of making an implementation is different from the skill set of writing a paper that is accepted at [crypto conference].”

Result: RQ2 - Themes of Cryptography Adoption Blockers

Through thematic analysis, we identified 5 overarching themes across all interviews.

1. Misaligned or conflicting incentives in academia
2. Challenges in standardization
3. Troublesome or missing reference implementations
4. Communication gaps and unclear responsibilities
5. Usability Issues

*“I at some point tried to install Project Everest. And [researcher] told me ‘Here’s a script! You download that script. You run it. And either that just installs everything and everything works, or you’re in big, big trouble.’ – I was in big, big trouble. So I spent a whole weekend actually *not* installing Project Everest. I didn’t manage in a whole weekend.”*

RQ3 - What are potential ways to overcome these obstacles?

RQ3 - Recommendations to Foster Cryptography Adoption

Academics

Cryptographers who are interested in adoption of their output can consider

- To go the extra mile and **provide accessible (reference) implementations** of their work
- Reaching out to **experts in secure software design** and **usability**

RQ3 - Recommendations to Foster Cryptography Adoption

Academics

Cryptographers who are interested in adoption of their output can consider

- To go the extra mile and **provide accessible (reference) implementations** of their work
- Reaching out to **experts in secure software design** and **usability**

Additionally, tweak academic reward structures to account more for

- Participation in **standardization efforts**
- Secure, usable, **production-ready implementations** of cryptography

RQ3 - Recommendations to Foster Cryptography Adoption

Industry

We encourage companies and organizations to consider **investing in core infrastructure maintenance projects** like the Open Source Security Foundation (OSSF).

We encourage implementers and users of standards to **reach out upstream**, communicating problems, and needs, or actively **contribute to open standard development**, instead of developing and standardizing cryptographic solutions behind closed doors.

RQ3 - Recommendations to Foster Cryptography Adoption

Standardization Organizations

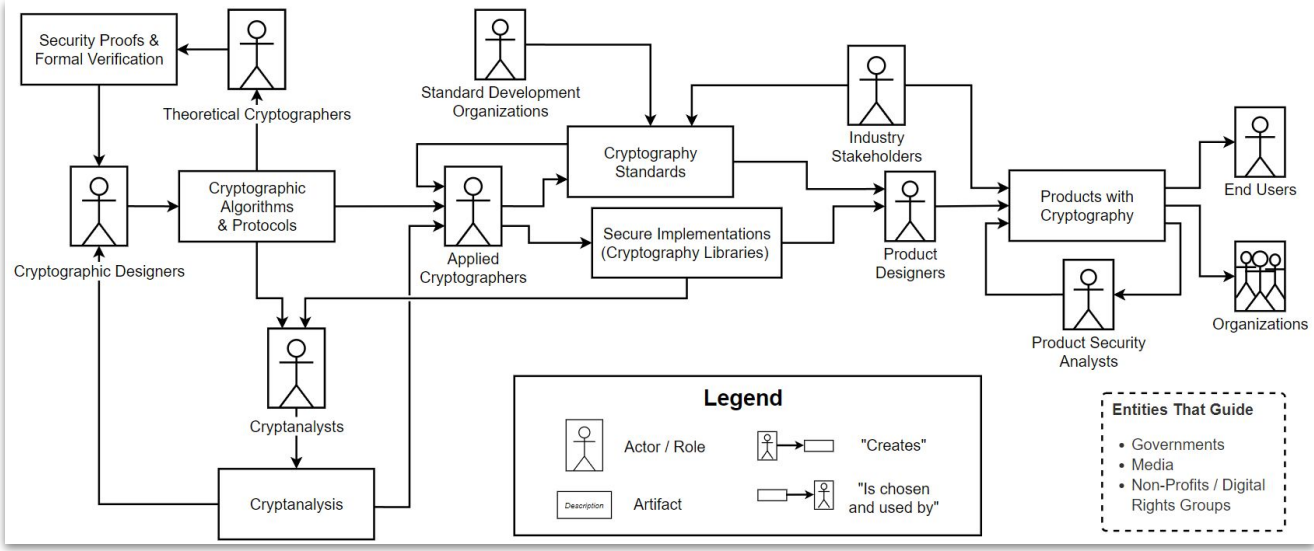
Our results imply issues with the complexity, readability, and actionability of standards. Consider employing **methods from usable security research**, like user studies, to improve standards, as well as standardization processes.

Standardization organizations should make sure they are trustworthy by further **engaging with the academic community, emphasizing open communication**, and open competitions. A “seal of approval” of a trusted standardization organization is a major driver for cryptography adoption.

Summary

Interviewed 21 cryptography experts on challenges in bringing cryptography research from papers to products.

Developed a map of the cryptography adoption path.



Identified five themes of challenges that hinder the adoption of cryptography:
Incentives in academia, Challenges in standardization, Troublesome reference implementations, Communication gaps, and Usability Issues.

Recommend working towards usable implementations, tweaking academic reward structures, fostering cross-disciplinary work and streamlining standardization processes.

Our paper describes much more challenges and recommendations to help to bring more cryptography research from papers to products—and improve end-users' security!

konstantin.fischer@rub.de