Protecting Cryptography against Compelled Self-Incrimination

Sarah Scheffler and Mayank Varia (Boston University)
ia.cr/2020/862
USENIX Security 2021

IN THE

Supreme Court of the United States

Does the Self-Incrimination Clause of the Fifth Amendment protect an individual from being compelled to recall and truthfully enter a memorized passcode, where communicating the passcode may lead to the discovery of incriminating evidence to be used against him in a criminal prosecution?

ROBERT ANDREWS,
—v.—
STATE OF NEW JERSEY,

Date: January 7, 2021

https://www.scotusblog.com/case-files/cases/andrews-v-new-jersey/

Testimony: “disclose the contents of [your] own mind”

Testimony protected under 5th Amendment =

Pure testimony
Written + oral statements

+

(Implicit testimony
“Compliance with the subpoena tacitly concedes [one’s belief]”

–

Foregone conclusion)
“Adds little or nothing to the sum total of the government’s information”

Is the testimony in an action a foregone conclusion?

Compelled action C

Respondent

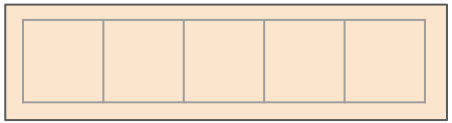
Performing this action reveals the content of my mind beyond what the government knows!

Who is right?

Government

I already know the testimony inherent in the compelled action!

Main idea: Formalize “learn nothing” using simulation



Nature: Everything except respondent’s mind

R’s mind

Compelled action C: Queries N and R

Simulator: Queries only N

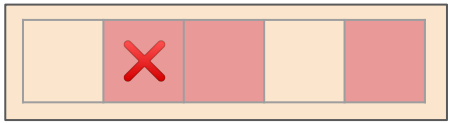
Respondent

Government

Compelled action C is a ***foregone conclusion*** wrt Sim and E if (and only if):

$\forall$ R,N allowed by E: $\mathbf{C^{N,R} \approx Sim^{N}}$

Government must simulate all “worlds” …



Nature: Everything except respondent’s mind

R’s mind

I don’t have a gun

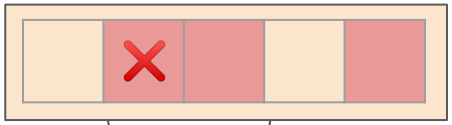
Respondent

Government

Compelled action C is a ***foregone conclusion*** wrt Sim and E if (and only if):

∀ R,N allowed by E: $C^{N,R} \approx Sim^{N}$

Government must simulate all “worlds” consistent with the evidence



2 known banks

Nature: Everything except respondent’s mind

R’s mind

I don’t have a gun

Not truthful!

Evidence E:
🙋‍♂️ testifies that
🤦‍♀️ has a gun

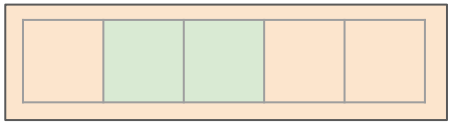
Respondent

Government

Compelled action C is a ***foregone conclusion*** wrt Sim and E if (and only if):

$\forall$ R,N **allowed by E:** $C^{N,R} \approx Sim^{N}$

Foregone conclusion definition



Nature: Everything except respondent's mind

R's mind

Compelled action C: Queries N and R

Simulator: Queries only N

Evidence E: Restricts allowable R,N

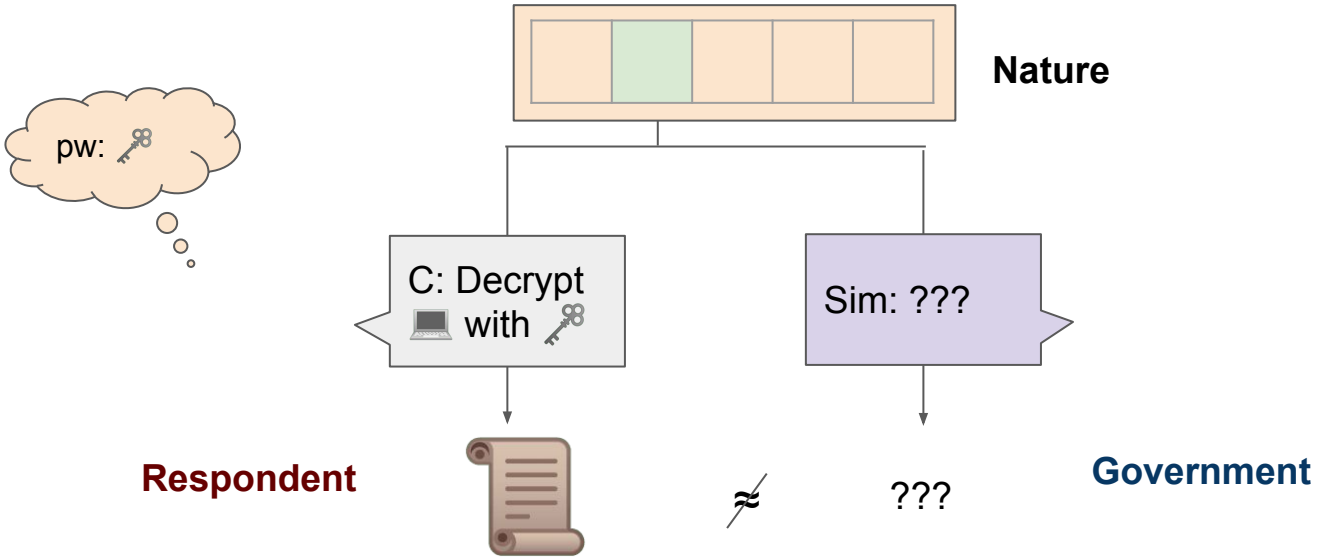
Respondent

Government

Compelled action C is a ***foregone conclusion*** wrt Sim and E if (and only if):

$\forall$ R,N allowed by E: $C^{N,R} \approx Sim^{N}$

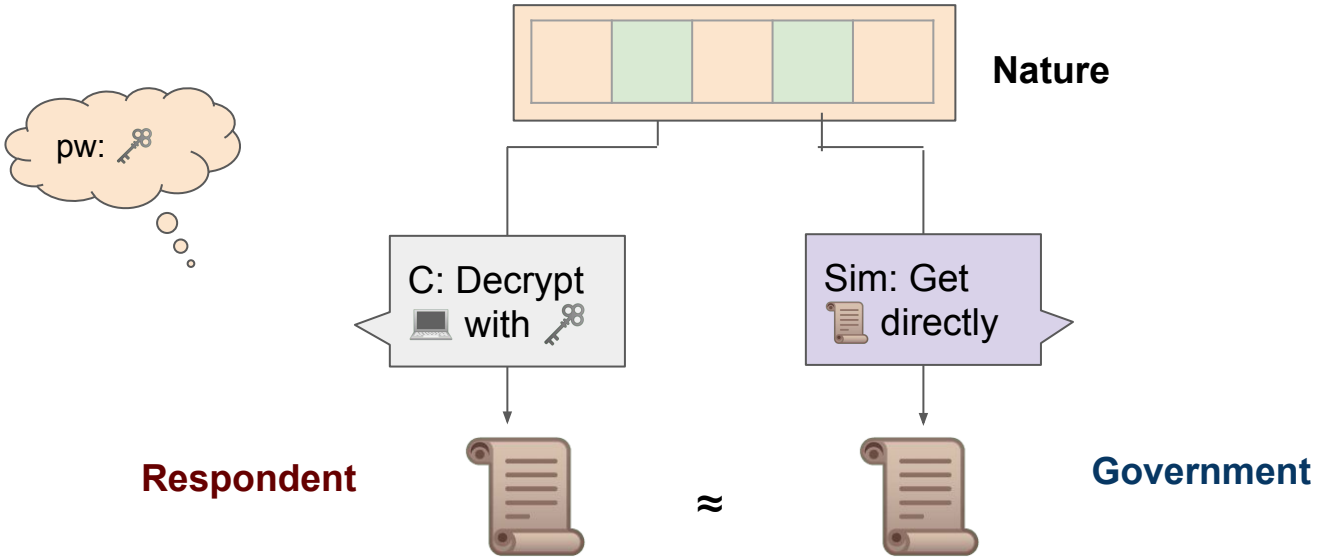
Decryption generally not compellable without help



Same reasoning applies to:

- Decryption
- Decommitments
- Hash preimages
- etc.

Some security-bolstering measures make one more vulnerable!



- HSMs
- Biometrics
- Threshold encryption
- MPC
- Cloud backup
- **Law enforcement key**

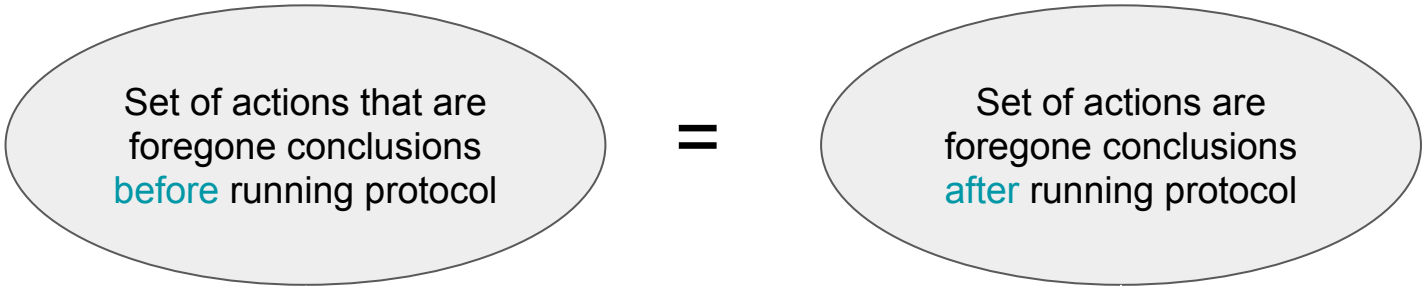
FC-resilience: Protection against **future** compelled requests

"FC" -- is **current** compelled action compellable based on past actions?

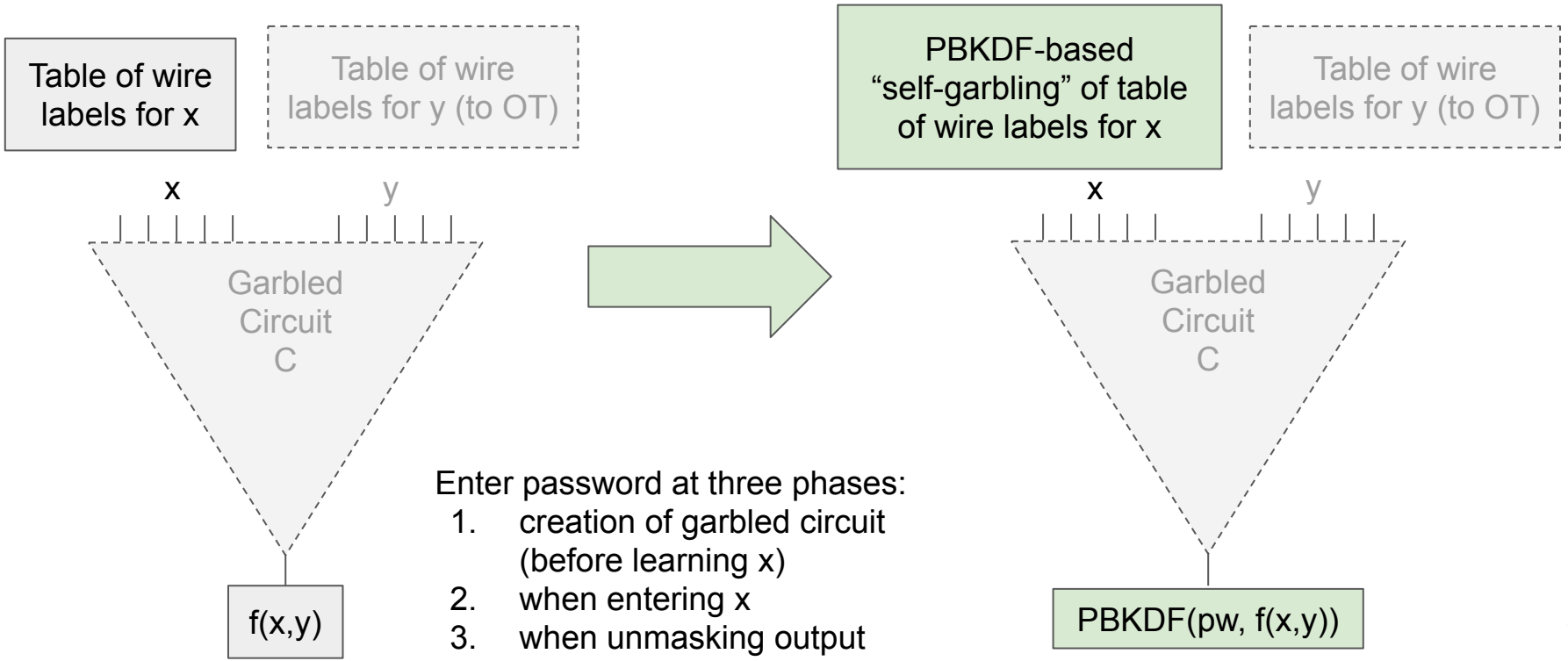
"***FC-resilient***" -- will unrelated protocol open me up to **future** compelled requests?

FC-resilience

A protocol is ***FC-resilient*** if it does not create “new” compellable foregone conclusions.



2PC with FC-resilience for the garbler



Enter password at three phases:

1. creation of garbled circuit (before learning x)
2. when entering x
3. when unmasking output

Feel free to email questions

1. Cryptographic definition of a “foregone conclusion”
2. Foregone conclusion status of crypto primitives and tools
   - ➢ Some tools that bolster security overall (hardware tokens, MPC, etc) make you vulnerable to be compelled
3. FC-resilience: Can we build protocols where the secrets cannot be compelled?
   - ➢ Construction of efficient FC-resilient MPC

Feedback is encouraged! sscheff@bu.edu eprint.iacr.org/2020/862