

Abuse Resistant Law Enforcement Access Systems

Eurocrypt 2021

ia.cr/2021/321

*Matthew Green (JHU), **Gabriel Kaptchuk (BU)**, and Gijs Van Laer (JHU)*

Abuse Resistant Law Enforcement Access Systems

Or: “Why ‘Law Enforcement’ is in the Session Title”

Eurocrypt 2021

ia.cr/2021/321

*Matthew Green (JHU), **Gabriel Kaptchuk (BU)**, and Gijs Van Laer (JHU)*

Abuse Resistant Law Enforcement Access Systems

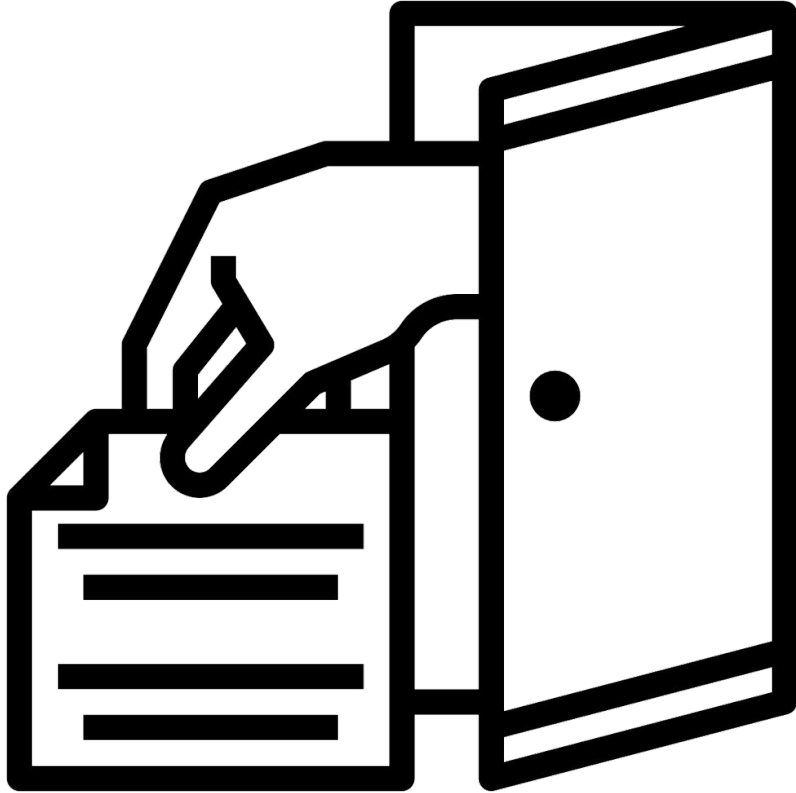
Or: “Why ‘Law Enforcement’ is in the Session Title”

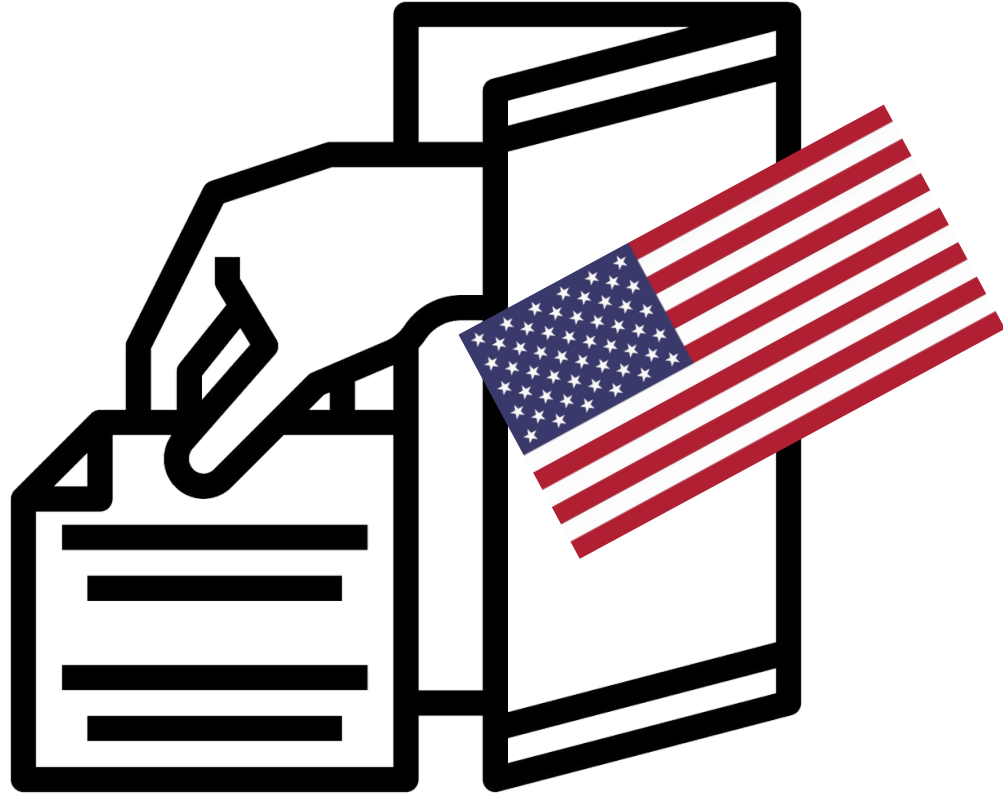
Or: “The Weirdest Paper at Eurocrypt 2021”

Eurocrypt 2021

ia.cr/2021/321

Matthew Green (JHU), Gabriel Kaptchuk (BU), and Gijs Van Laer (JHU)







The First Crypto Wars



Snowden Leaks



Apple vs FBI



EARN IT Act



**"I think you'd rather find the solution than have Congress do it for you."
-- Senator Ernst (R, Iowa). Senate Hearing Dec 2019**





The First Crypto Wars

Snowden Leaks

Apple vs FBI

EARN IT Act

**"I think you'd rather find the solution than have Congress do it for you."
-- Senator Ernst (R, Iowa). Senate Hearing Dec 2019**





The First Crypto Wars

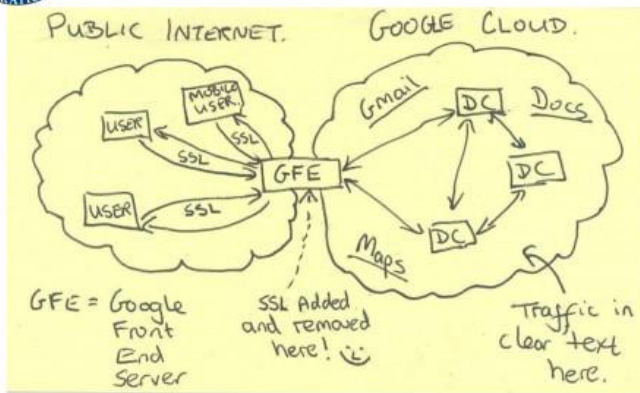


TOP SECRET//SI//NOFORN

Snowden Leaks



Current Efforts - Google



TOP SECRET//SI//NOFORN

EARN IT Act

"I think you'd rather find the solution than have Congress do it for you."
-- Senator Ernst (R, Iowa). Senate Hearing Dec 2019

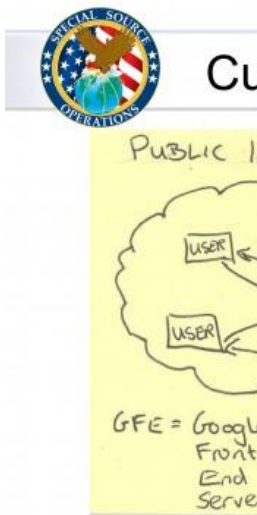




The First Crypto Wars



Snowden Leaks



Apple vs FBI

EARN IT Act



**"I think you'd rather find the solution than have Congress do it for you."
-- Senator Ernst (R, Iowa). Senate Hearing Dec 2019**



The First Crypto Wars



Snowden Leaks



Apple vs FBI



EARN IT Act



**"I think you'd rather find the solution than have Congress do it for you."
-- Senator Ernst (R, Iowa). Senate Hearing Dec 2019**





The First Crypto Wars



Snowden Leaks



Apple vs FBI

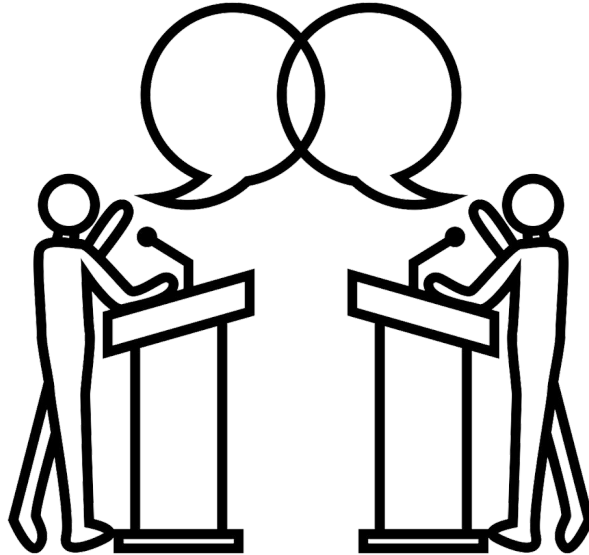


EARN IT Act



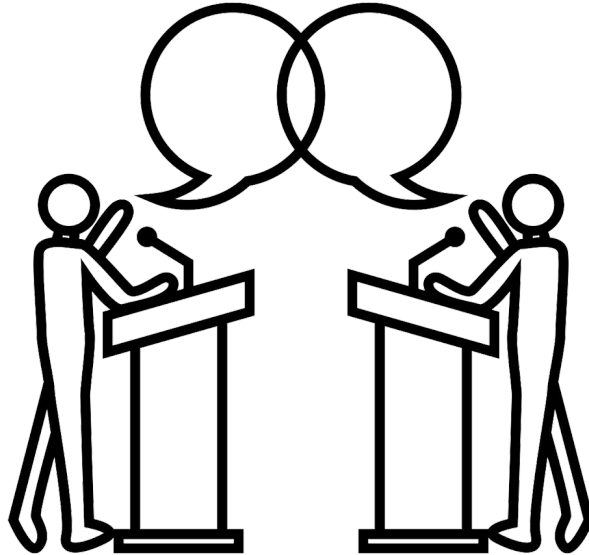
**"I think you'd rather find the solution than have Congress do it for you."
-- Senator Ernst (R, Iowa). Senate Hearing Dec 2019**







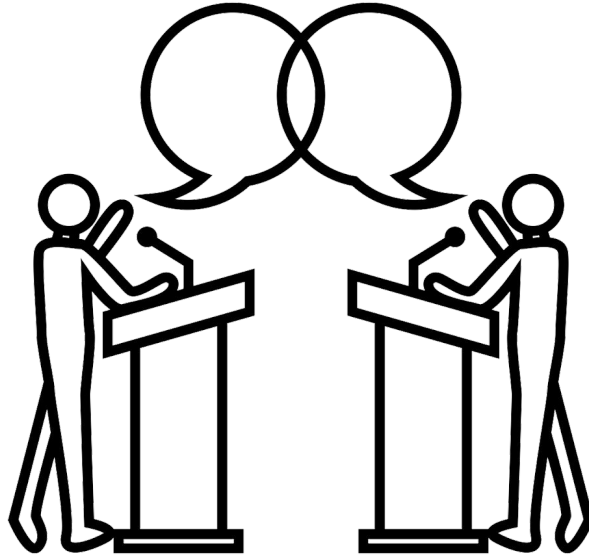
Limits Constitutionally Sanctioned Searches





Limits Constitutionally Sanctioned Searches

Tech People are Smart -- Figure it out!

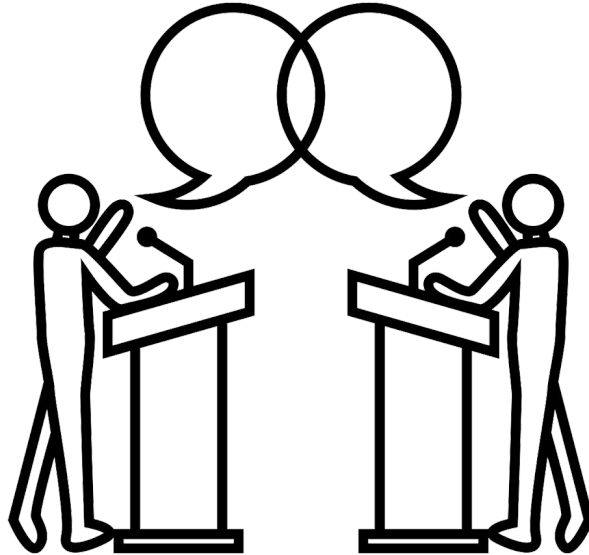




Limits Constitutionally Sanctioned Searches

Tech People are Smart -- Figure it out!

High Value Key Material Already Exists

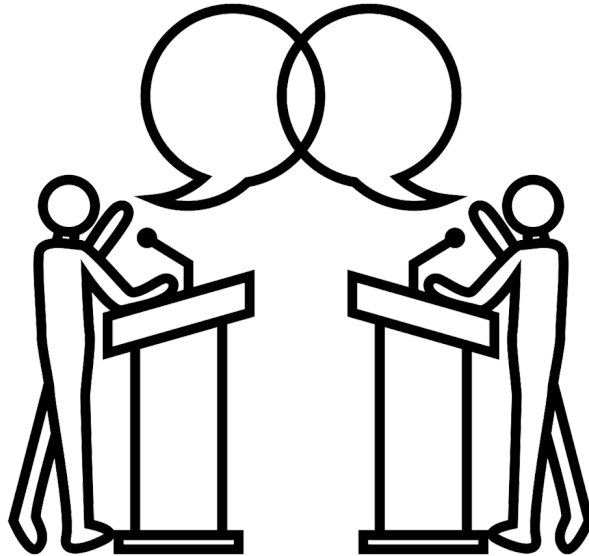




Limits Constitutionally Sanctioned Searches

Tech People are Smart -- Figure it out!

High Value Key Material Already Exists



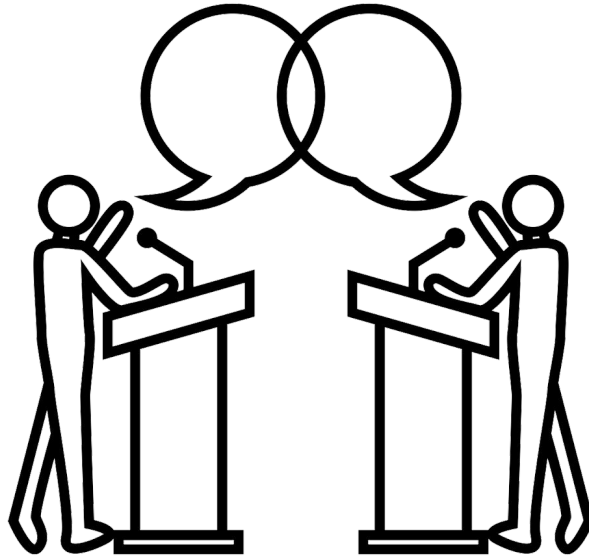
Encryption is fundamental to business and privacy



Limits Constitutionally Sanctioned Searches

Tech People are Smart -- Figure it out!

High Value Key Material Already Exists



Encryption is fundamental to business and privacy

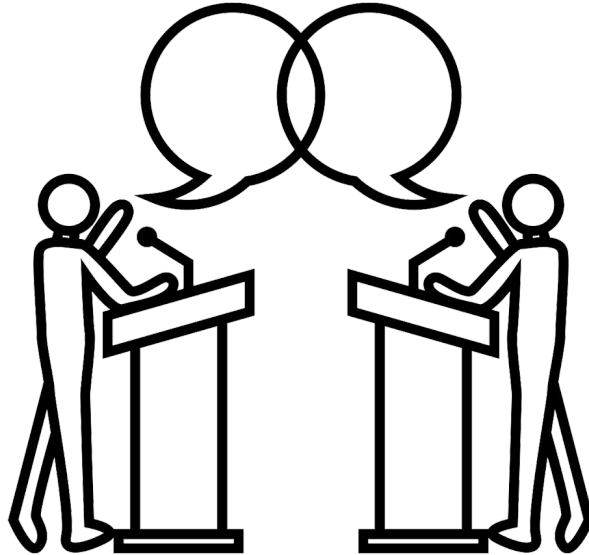
Backdoors are vulnerable to abuse and theft



Limits Constitutionally Sanctioned Searches

Tech People are Smart -- Figure it out!

High Value Key Material Already Exists



Encryption is fundamental to business and privacy

Backdoors are vulnerable to abuse and theft

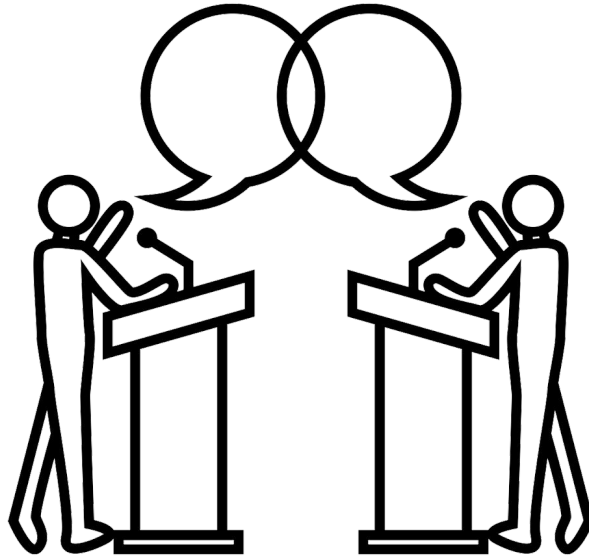
Hard to detect catastrophic failure



Limits Constitutionally Sanctioned Searches

Tech People are Smart -- Figure it out!

High Value Key Material Already Exists



Lots of rhetoric, very little dialog, no specifications!



Encryption is fundamental to business and privacy

Backdoors are vulnerable to abuse and theft

Hard to detect catastrophic failure



Limits Constitutionally Sanctioned Searches

Tech People are Smart -- Figure it out!

High Value Key Material Already Exists

Lots of rhetoric, very little dialog, no specifications!



Encryption is fundamental to business and privacy

Backdoors are vulnerable to abuse and theft

Need to detect catastrophic failure

Contributions

Put forward a new simulation-based, socially motivated definition:

Abuse Resistant Law Enforcement Access Systems

Contributions

Put forward a new simulation-based, socially motivated definition:

Abuse Resistant Law Enforcement Access Systems

Split into two flavors:

(1) Prospective ARLEAS

(2) Retrospective ARLEAS

Contributions

Put forward a new simulation-based, socially motivated definition:

Abuse Resistant Law Enforcement Access Systems

Split into two flavors:

(1) Prospective ARLEAS

(2) Retrospective ARLEAS

Constructions:

(1) Prospective ARLEAS from **NI-MPC, SS-NIZKs, and Public Ledgers**

(2) Retrospective ARLEAS from **EWE, SS-NIZKs, and Public Ledgers**

Contributions

Put forward a new simulation-based, socially motivated definition:

Abuse Resistant Law Enforcement Access Systems

Split into two flavors:

(1) Prospective ARLEAS

(2) Retrospective ARLEAS

Constructions:

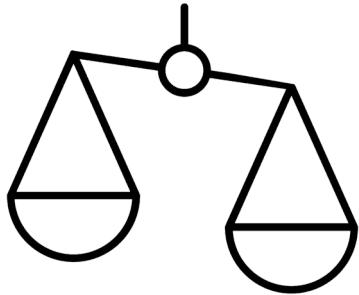
(1) Prospective ARLEAS from **NI-MPC, SS-NIZKs, and Public Ledgers**

(2) Retrospective ARLEAS from **EWE, SS-NIZKs, and Public Ledgers**

Lower Bound:

Retrospective ARLEAS \Rightarrow EWE (for related, non-trivial language)

ARLEAS Parties



Judge



Law Enforcement



User

Abuse Resistant Law Enforcement Access Systems



Global Warrant Policies



Secure Messages without Warrant



Transparency and Abuse Detectability



Cryptographic Enforcement

Parameter Examples



Global Warrant Policies



Transparency and Abuse Detectability



Cryptographic Enforcement

Parameter Examples



Global Warrant Policies



**Warrants must list individual people
(no drag nets)**



Transparency and Abuse Detectability



Cryptographic Enforcement

Parameter Examples



Global Warrant Policies



**Warrants must list individual people
(no drag nets)**



Transparency and Abuse Detectability



**# of warrants activated
differentially private statistics**



Cryptographic Enforcement

Parameter Examples



Global Warrant Policies



**Warrants must list individual people
(no drag nets)**



Transparency and Abuse Detectability



**# of warrants activated
differentially private statistics**

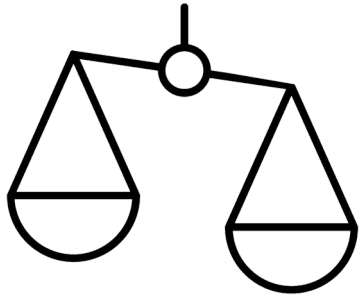


Cryptographic Enforcement



**Use of Backdoor Implies
(Computationally) Adherence**

ARLEAS Parties



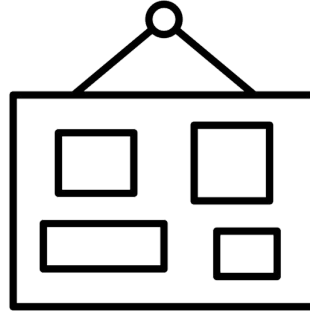
Judge



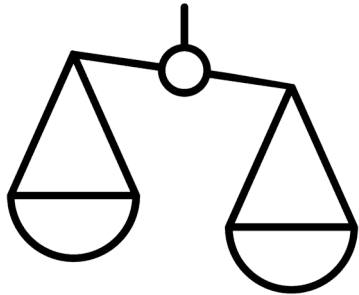
Law Enforcement



User



Bulletin Board / Public Ledger



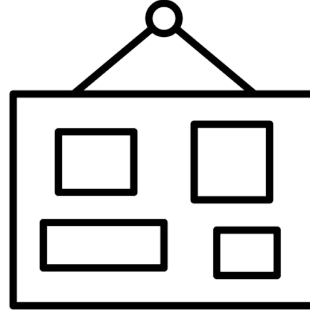
Judge



Law Enforcement

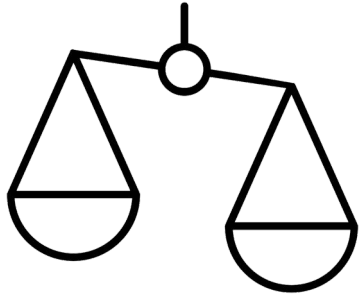


User



- No escrow secrets
- Publicly accessible
- Authenticate postings offline

Bulletin Board / Public Ledger



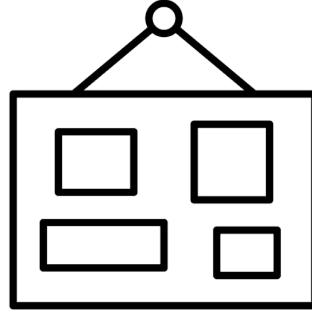
Judge



Law Enforcement

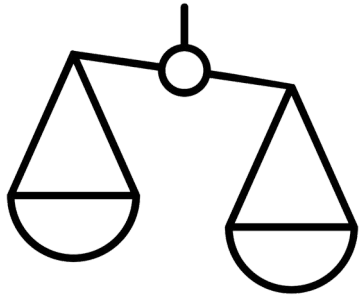


User



- No escrow secrets
- Publicly accessible
- Authenticate postings offline

Bulletin Board / Public Ledger



Judge

Corrupt



Law Enforcement

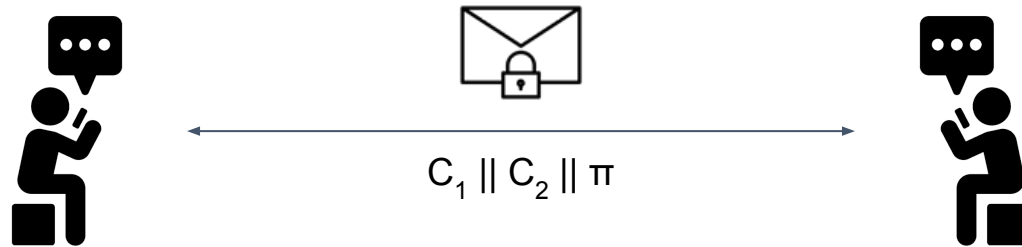


User

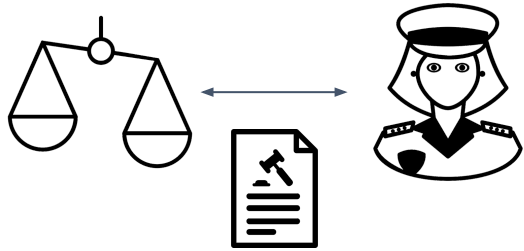
ARLEAS Paradigm



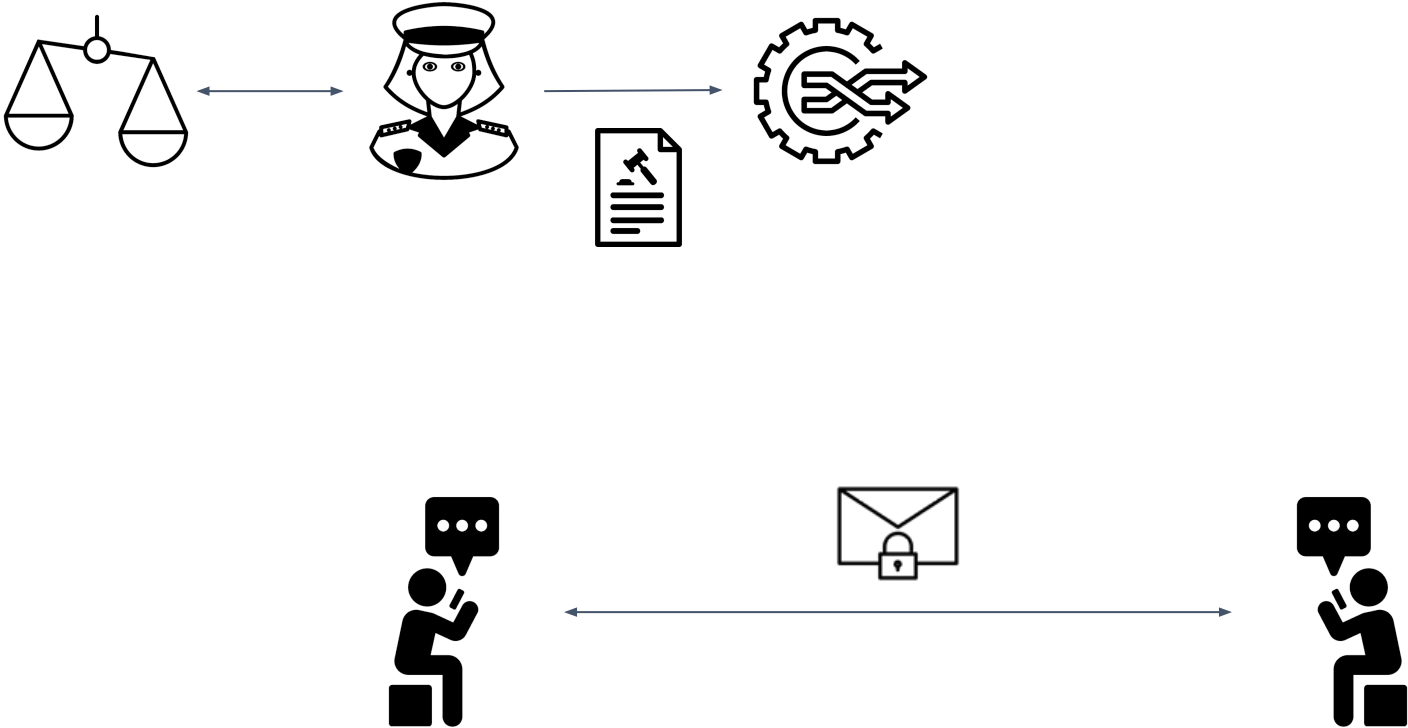
ARLEAS Paradigm



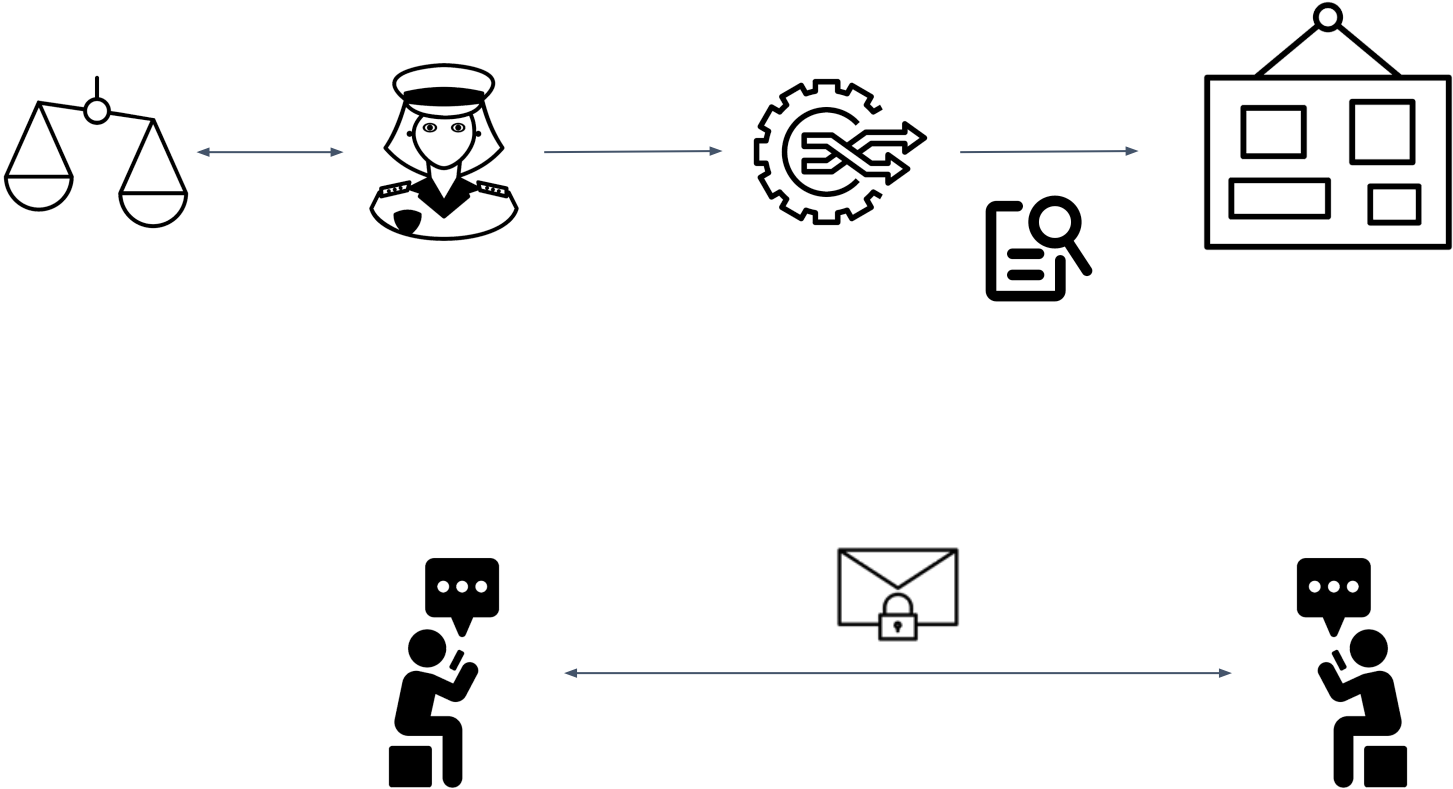
ARLEAS Paradigm



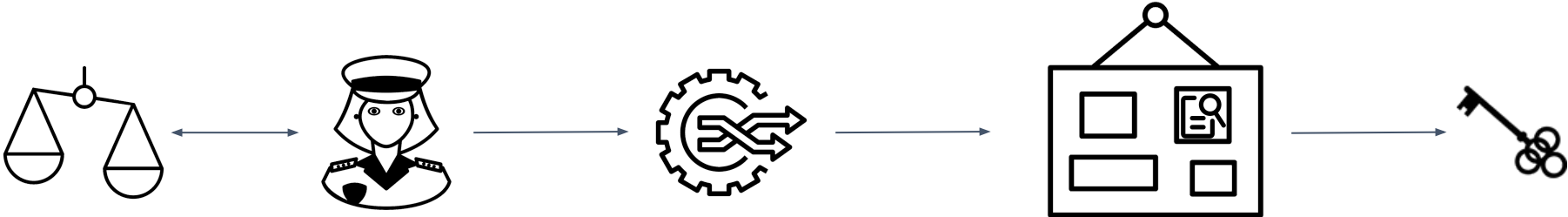
ARLEAS Paradigm



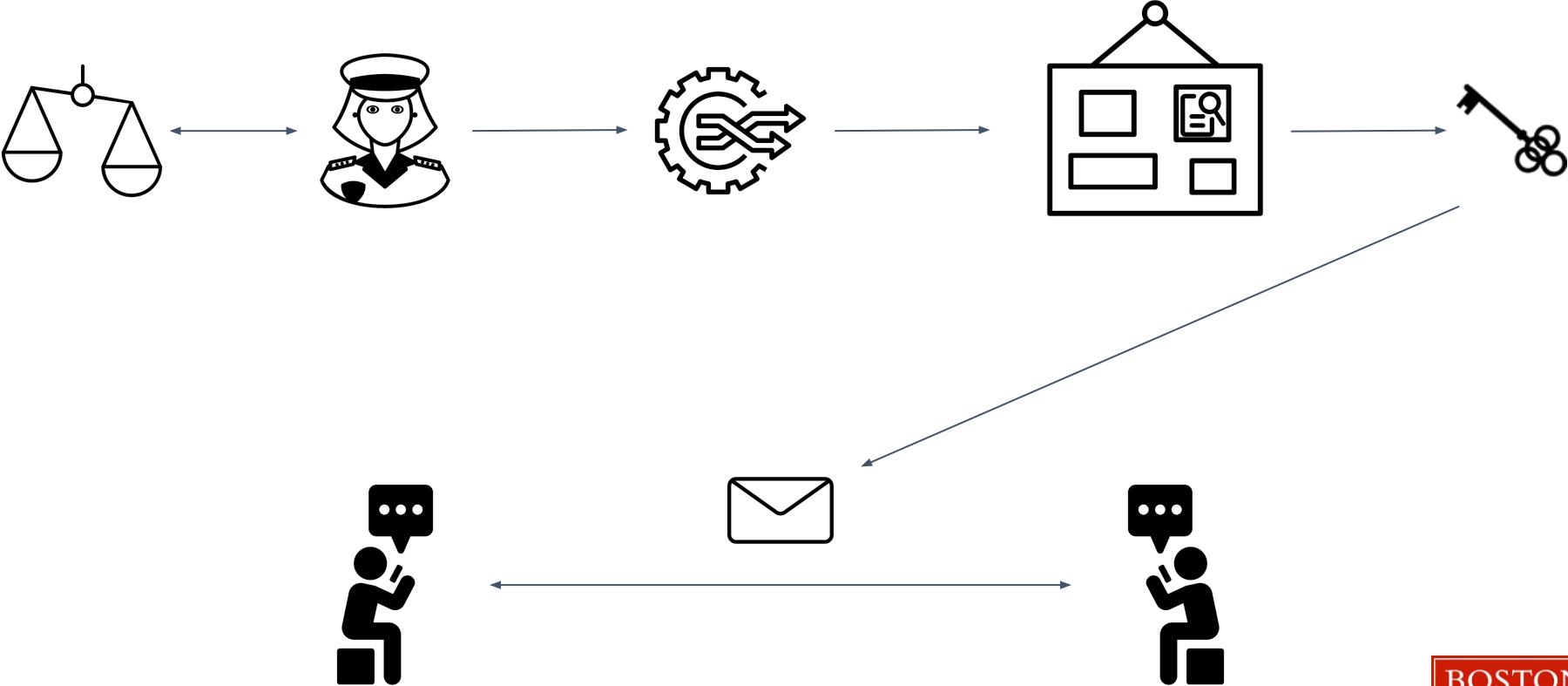
ARLEAS Paradigm



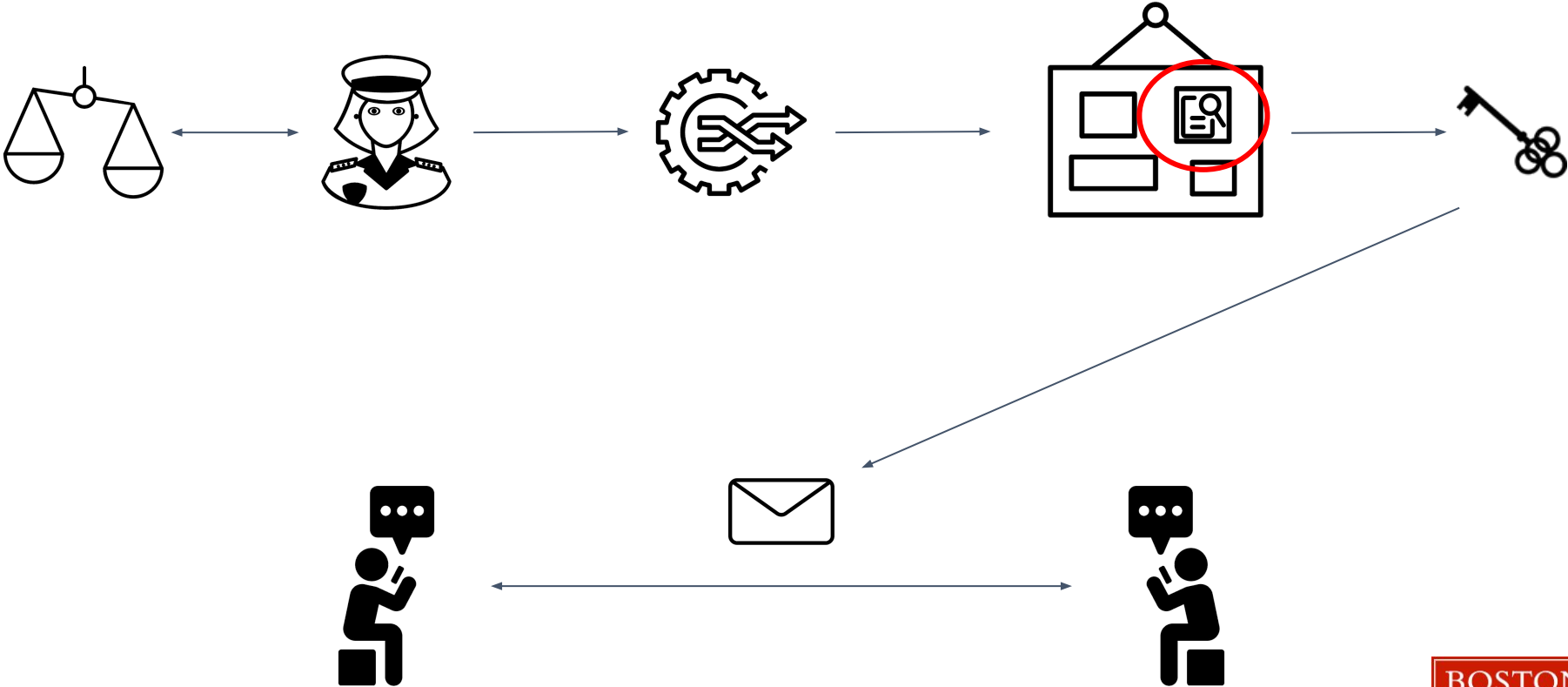
ARLEAS Paradigm



ARLEAS Paradigm



ARLEAS Paradigm





Prospective ARLEAS



Retrospective ARLEAS



Prospective ARLEAS

Warrant “activation” creates backdoor for all in-scope messages encrypted **AFTER** activation



Retrospective ARLEAS

Warrant “activation” creates backdoor for all in-scope messages encrypted **BEFORE** activation



**Moment of Warrant
Activation**



Prospective ARLEAS



**Moment of Warrant
Activation**



Retrospective ARLEAS

(orange)



Prospective ARLEAS

(purple)



**Moment of Warrant
Activation**



Retrospective ARLEAS

(orange)



EASY!

Prospective ARLEAS

(purple)



**Moment of Warrant
Activation**

Hard!



Retrospective ARLEAS

(orange)

EASY!



Prospective ARLEAS

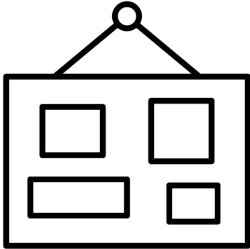
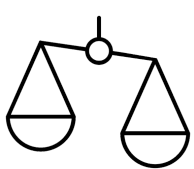
(purple)



**Moment of Warrant
Activation**



Prospective ARLEAS





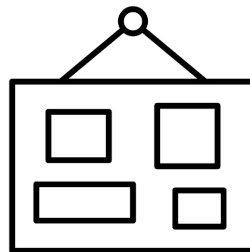
Prospective ARLEAS



Transparency Information
Simulation Sound NIZK of Correctness



First Round of NI-MPC for
“Reveal message if it is covered by warrant”





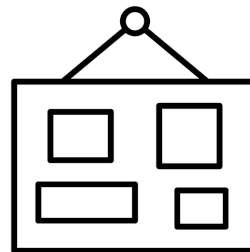
Prospective ARLEAS



Transparency Information
Simulation Sound NIZK of Correctness



First Round of NI-MPC for
"Reveal message if it is covered by warrant"





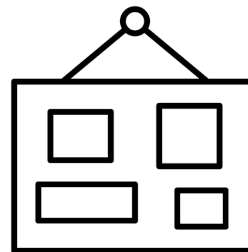
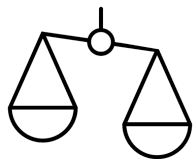
Prospective ARLEAS



Transparency Information
Simulation Sound NIZK of Correctness



First Round of NI-MPC for
"Reveal message if it is covered by warrant"




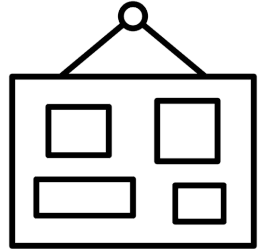
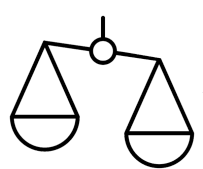
C_1 : Normal Ciphertext
 C_2 : Second Round of NI-MPC
 π : NIZK of Correctness






Retrospective ARLEAS

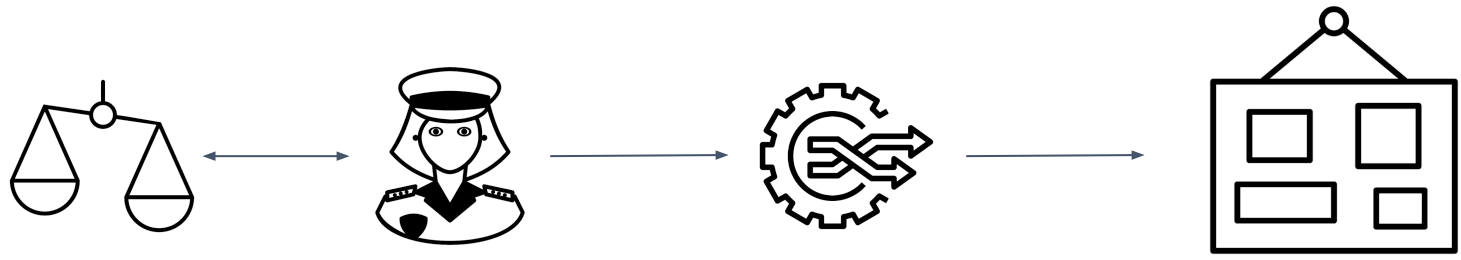
 **Transparency Information**
Simulation Sound NIZK of Correctness






Retrospective ARLEAS

 **Transparency Information**
Simulation Sound NIZK of Correctness




 C_1 : Normal Ciphertext
 C_2 : EWE of Plaintext
 Π : NIZK of Correctness

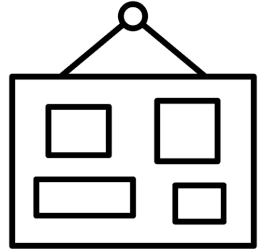
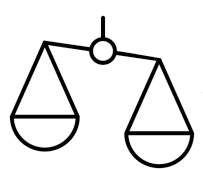




Retrospective ARLEAS

 **Transparency Information**
Simulation Sound NIZK of Correctness

 **Warrant Signed By Judge**
Proof of Publication Of Transparency Info



C_1 : Normal Ciphertext
 C_2 : EWE of Plaintext
 π : NIZK of Correctness



Contributions

Put forward a new simulation-based, socially motivated definition:

Abuse Resistant Law Enforcement Access Systems

Split into two flavors:

(1) Prospective ARLEAS

(2) Retrospective ARLEAS

Constructions:

(1) Prospective ARLEAS from **NI-MPC, SS-NIZKs, and Public Ledgers**

(2) Retrospective ARLEAS from **EWE, SS-NIZKs, and Public Ledgers**

Lower Bound:

Retrospective ARLEAS \Rightarrow EWE (for related, non-trivial language)

Thanks!

ia.cr/2021/321