Cryptography, Trust and Privacy: It's complicated

Ero Balsa (Cornell Tech)
Helen Nissenbaum (Cornell Tech)
Sunoo Park (Cornell Tech → Columbia)

CNIL Privacy Research Day -- June 14, 2023

Cryptography, Trust and Privacy: It's Complicated

Ero Balsa
Cornell Tech
USA
ero.balsa@cornell.edu

Helen Nissenbaum
Cornell Tech
USA
helen.nissenbaum@cornell.edu

Sunoo Park
Cornell Tech
USA
sep243@cornell.edu

ABSTRACT

Privacy technologies support the provision of online services while protecting user privacy. Cryptography lies at the heart of many such technologies, creating remarkable possibilities in terms of functionality while offering robust guarantees of data confidentiality. The cryptography literature and discourse often represent that these technologies *eliminate the need to trust* service providers, i.e., they enable users to protect their privacy even against untrusted service providers. Despite their apparent promise, privacy technologies have seen limited adoption in practice, and the most successful ones have been implemented by the very service providers these technologies purportedly protect users from.

The adoption of privacy technologies by supposedly adversarial service providers highlights a mismatch between traditional models of trust in cryptography and the trust relationships that underlie deployed technologies in practice. Yet this mismatch, while well known to the cryptography and privacy communities, remains relatively poorly documented and examined in the academic literature—let alone broader media. This paper aims to fill that gap.

Firstly, we review how the deployment of cryptographic technologies relies on a chain of trust relationships embedded in the modern computing ecosystem, from the development of software to the provision of online services, that is not fully captured by traditional models of trust in cryptography. Secondly, we turn to two case studies—web search and encrypted messaging—to illustrate how, rather than *removing* trust in service providers, cryptographic privacy technologies *shift* trust to a broader community of security and privacy experts and others, which in turn enables service providers to implicitly build and reinforce their trust relationship with users. Finally, concluding that the trust models inherent in the traditional cryptographic paradigm elide certain key trust relationships underlying deployed cryptographic systems, we highlight the need for organizational, policy, and legal safeguards to address that mismatch, and suggest some directions for future work.

ACM Reference Format:
Ero Balsa, Helen Nissenbaum, and Sunoo Park. 2022. Cryptography, Trust and Privacy: It's Complicated. In *Proceedings of the 2022 Symposium on Computer Science and Law (CSLAW '22), November 1–2, 2022, Washington, DC, USA.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3511265.3550443

CSLAW '22, November 1–2, 2022, Washington, DC, USA

ACM ISBN 978-1-4503-9234-1/22/11…$15.00
https://doi.org/10.1145/3511265.3550443

1 INTRODUCTION

Modern cryptography enables remarkably versatile uses of information while simultaneously maintaining (partial) secrecy of that information. In addition to good old encryption, modern techniques such as secure multiparty computation and homomorphic encryption have opened a new realm of possibilities in privacy technologies, enabling the design and development of previously impossible—and sometimes seemingly paradoxical—combinations of functionality and confidentiality. Examples include, among others, anonymous credentials, which can enable verification without requiring identification [14, 17]; homomorphic encryption, which can enable cloud services that conceal user content from cloud providers [58]; and private information retrieval, which keeps user consumption of digital information (e.g., web search, media streaming) confidential from the provider [29, 40].

Being at the heart of modern privacy technologies, cryptography has pushed the limits of what is possible in terms of *data minimization*, a core principle in privacy engineering and *privacy by design* [31]. Cryptography is instrumental to the realization of data minimization strategies such as minimum data collection and minimum data exposure, which in turn result in minimization of the *need for trust* [32]. In theory, by shielding data flows from unauthorized access and prying eyes *by design*, implemented through code, rather than contractual agreements or privacy policies, cryptography enables privacy-preserving systems that do not rely on the goodwill or good behavior of the service provider or system administrators, thus minimizing the need to trust them with the protection of users' privacy.

Yet in spite of the powerful privacy properties that cryptographic privacy technologies promise, few of these technologies have seen adoption in practice. Whereas cryptography for security has been largely successful, holding the key (no pun intended) to secure transactions online, cryptography for privacy has not shared the same fate [41]. Cryptography for security may address important privacy concerns (e.g., HTTPS); however, few organizations have adopted the kind of privacy technologies that protect their customers or users against the organization itself, in theory ridding users of the need to rely on service providers to protect their privacy [23, 30]. In the same vein, despite the fact that outcries about privacy invasions and state and corporate surveillance have become a mainstay in contemporary media, few users have taken matters into their own hands and adopted these technologies to protect their privacy.[1]

Reasons for this lack of adoption have long puzzled and drawn the interest of the academic community. Assumptions and hypotheses about poor usability, user and organizational unawareness, economic incentives and inefficiency are regarded as a complex

[1] Notably, some cryptographic privacy technologies cannot be unilaterally adopted by users, as they require service providers to deploy them (e.g., privacy technologies based on private information retrieval).

Appeared at CSLaw 2022

In a nutshell…

Departing premise:

Cryptography "removes trust in service provider"

Main contributions:

01. Document misalignment between trust models

02. Illustrate <u>shift</u> rather than <u>removal</u> of trust

03. Explore technical, organizational and legal strategies to realign trust

CORNELL TECH
HOME OF THE JACOBS INSTITUTE

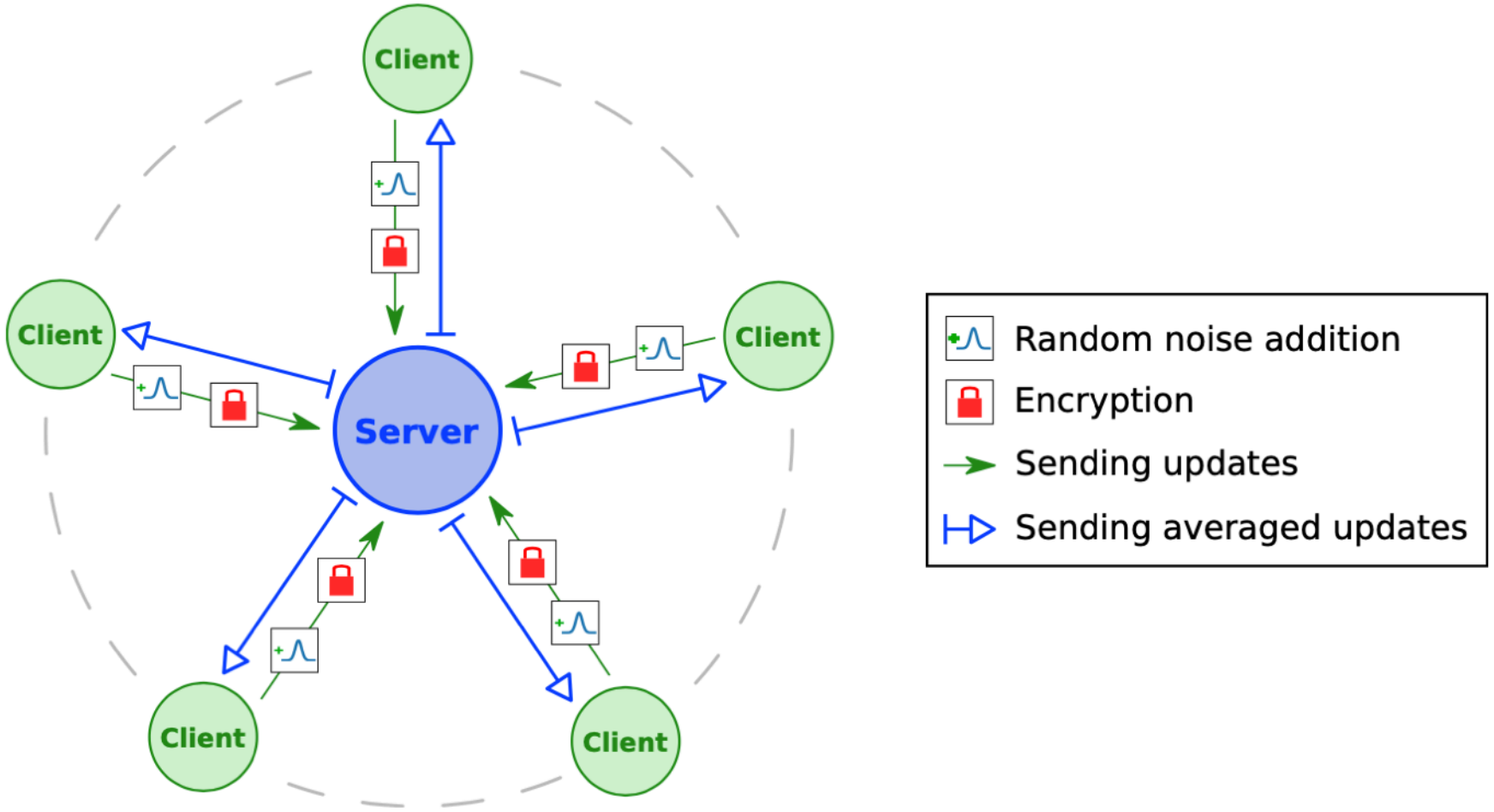


Fig. 1. Our secure federated learning architecture.

Image taken from **Sébert, A. G., Sirdey, R., Stan, O., & Gouy-Pailler, C. (2022):**
"Protecting data from all parties: Combining FHE and DP in federated learning"

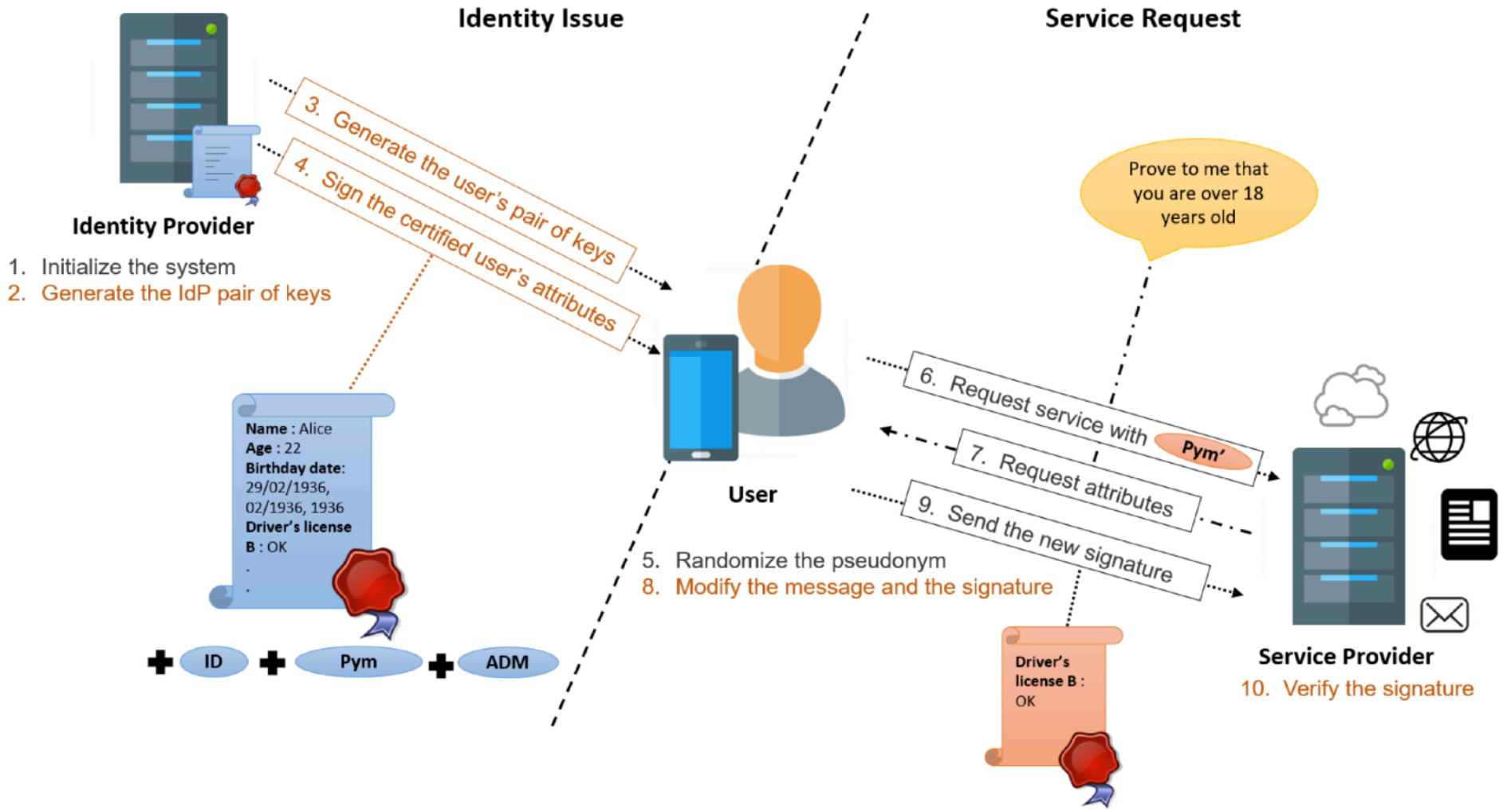


Image taken from **Souha Masmoudi, Maryline Laurent, Nesrine Kaaniche:** *PIMA: a privacy-preserving identity management system based on an unlinkable MAlleable signature. Journal of Network and Computer Applications (JNCA), 2022, 208 (103517), pp.1-35.*

Privacy-by-design

"Data security is undergoing a significant evolution. Initially, security sought to protect data at the perimeter of the organisation. It is now moving to a new "zero trust" paradigm where the bad actors are already assumed to be inside the organisation."

"[PETs] provide more control to data subjects and enhance trust in the processing of data (compare with section above on zero trust). OECD research has long championed 'privacy by design'."

Taken from: "Emerging privacy enhancing technologies. Current regulatory and policy approaches". OECD Digital Economy Papers. March 2023, No. 351

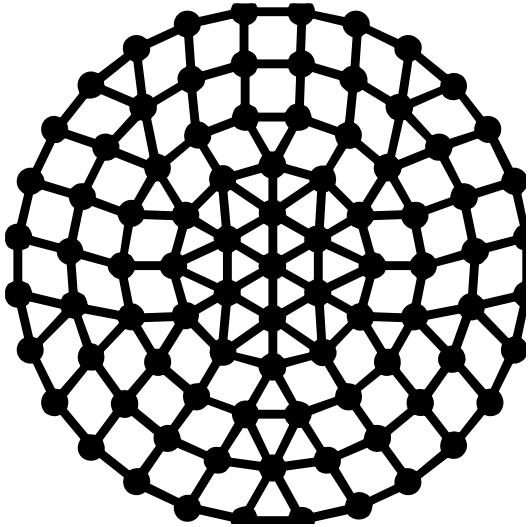
Key points

1. Cryptography does not "remove trust"
   - Misalignment between trust models
   - Shift and distribution rather than removal of trust

2. Need for technical, organizational and legal strategies to close trust gap

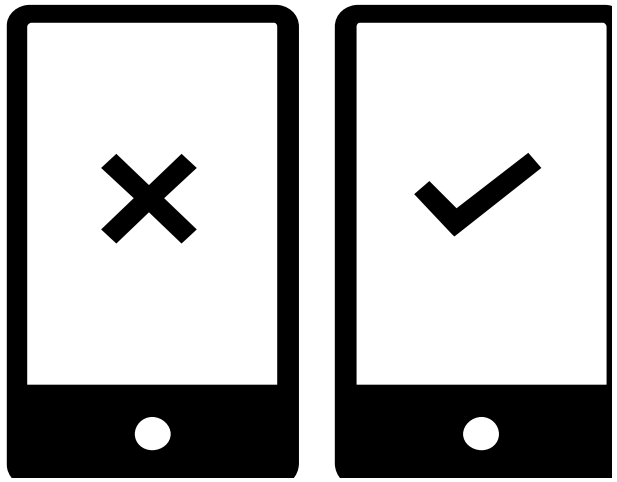
CORNELL TECH
HOME OF THE JACOBS INSTITUTE

In our paper: two concrete examples



1. Private web search

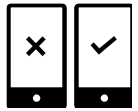
More hypothetical



2. Instant messaging

Deployed applications

Instant messaging



We compare

- "TrustIM" (promise-based)
- WhatsApp (end-to-end encrypted)
- Signal (end-to-end encrypted)

(Some) observations:

- Control of the client and updates
- Signal open source!

Trust as a *societal* phenomenon

Extraordinarily rich concept, covers a variety of relationships

Trust (philosophy & social science):

- interaction history
- reputation
- known personal characteristics
- mutuality and reciprocity
- contextual norms and roles (familiar, professional, …)
- …

Trust (cryptography):

- Narrowly defined, term of art: *adherence to specified behavior*
- Obscures certain nuances: "*Bob is trusted*"
  - 'Bob' stands as a *monolith* for Bob himself, his client, his device.
  - Bob may be untrustworthy (outside of the cryptographic model)

Lessons

Cryptography (may) distribute, shift trust

Does not eliminate but reinforces trust on provider!

Need sociotechnical arrangements (publish code, audits by experts)

Bridging the (trust) gap

What legal, organizational, technical, or other measures could support cryptographic privacy technologies where traditional modeling assumptions are in doubt?

Technical & organizational

- Publish specifications
- Publish source code
- Signed code, binary transparency, reproducible builds
- …

Private law

- Make contractual commitments to technical/ organizational measures for privacy
- Commit to clear penalties and consequences in case of violation
- ...

Public law

- Obligatory third-party audits for tech companies meeting some conditions
- Mandatory disclosure of audit results to govt agencies or public
- Heightened duty of care for certain companies
- ...

CORNELL TECH
HOME OF THE JACOBS INSTITUTE

Thank you!

Paper: Ero Balsa, Helen Nissenbaum, and Sunoo Park. "*Cryptography, Trust and Privacy: It's Complicated*" Proceedings of the 2022 Symposium on Computer Science and Law. 2022.

Contact: <ero.balsa@cornell.edu>