# Cryptography from Roots to Fruits

# Criptografía desde las Raíces hasta los Frutos

Seny Kamara
Leah Namisa Rosenbloom*
Crypto Reading Group
Brown University

*speaker
*orador

# Grounding Questions — Preguntas Fundamentales

What is the "root" of cryptography? Where does it come from?

¿Cuál es la "raíz" de la criptografía? ¿De dónde viene?

Why do we care? What "fruit" are we trying to produce?

¿Por qué nos importa? ¿Qué "fruto" estamos tratando de producir?

# The Many-Tree Metaphor

## La metáfora de los muchos árboles

"Cryptographers are not a monolith" means...

- We all have different roots
- Our identities are multiple and complex
- The following trees are meant to capture aspects of cryptographers, not stereotype individuals

"Criptógrafes no son un monolito" significa...

- Todos tenemos raíces diferentes
- Nuestras identidades son múltiples y complejas.
- Los siguientes árboles están destinados a capturar aspectos de los criptógrafos, no a estereotipar a individuos

# Theoretical Cryptographer

## Criptógrafe Teórico

### Fruit

- Publications
- Conference talks
- Intellectual property
- Continued lineage

Fruta: Publicaciones, Conferencias, Propiedad intelectual, Linaje continuo

### Trunk

- Foundational open problems
- Objective: primitives from minimal assumptions and computation/ communication complexity

Tronco: Problemas abiertos fundamentales; Objetivo: primitivos a partir de suposiciones mínimas y complejidad de computación/comunicación

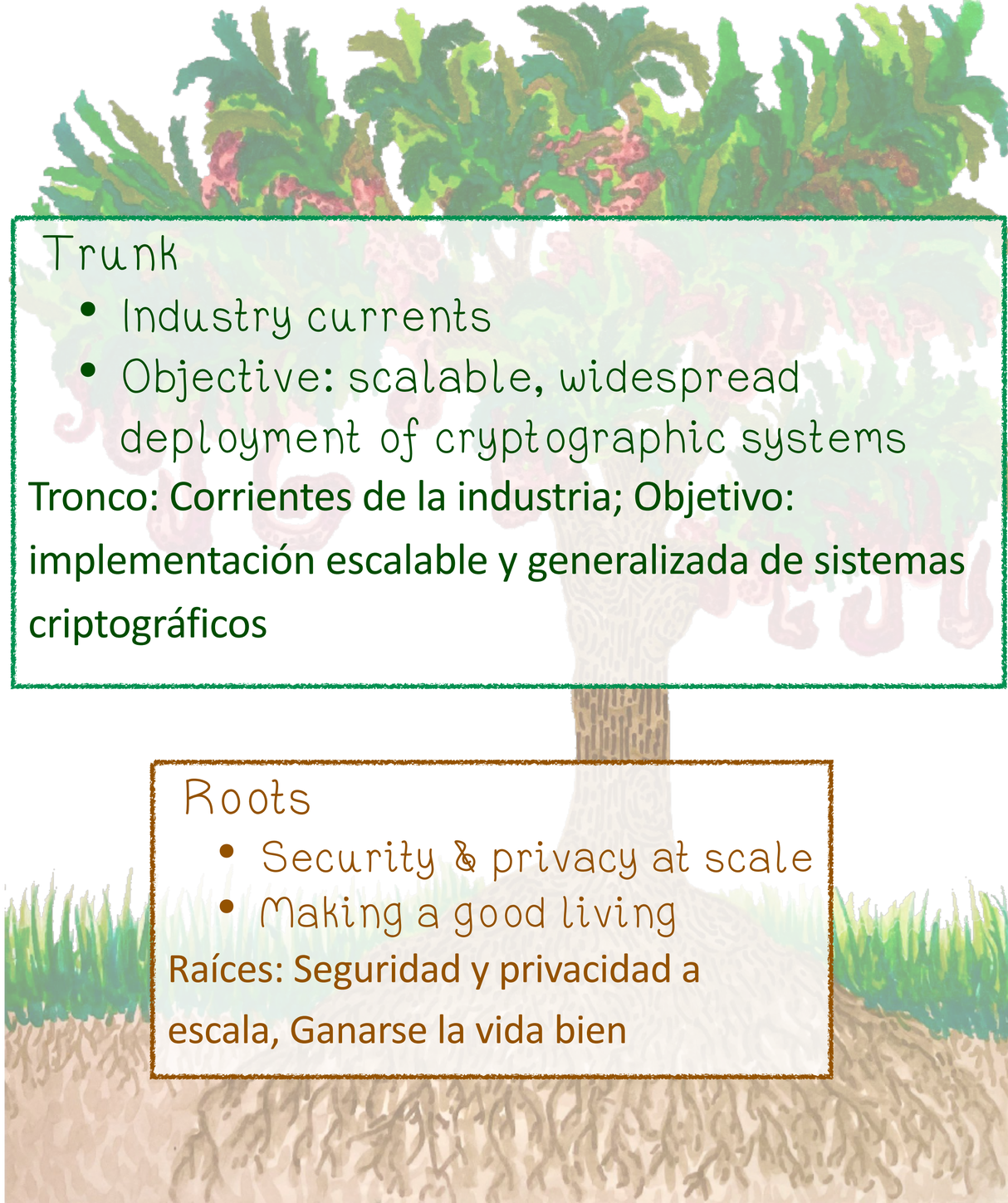
### Roots

- Mathematics/ theoretical CS
- Complexity theory
- Academic lineages

Raíces: Matemáticas/CS teórica, Teoría de la complejidad, Linajes académicos

# Industry Cryptographer

## Criptógrafe de la Industria



**Trunk**

- Industry currents
- Objective: scalable, widespread deployment of cryptographic systems

Tronco: Corrientes de la industria; Objetivo: implementación escalable y generalizada de sistemas criptográficos

**Fruit**

- Implementations
- Widespread deployment
- Making, protecting property (capital, IP)

Fruta: Implementaciones, despliegue generalizada y creación, protección de la propiedad (capital, propiedad intelectual)

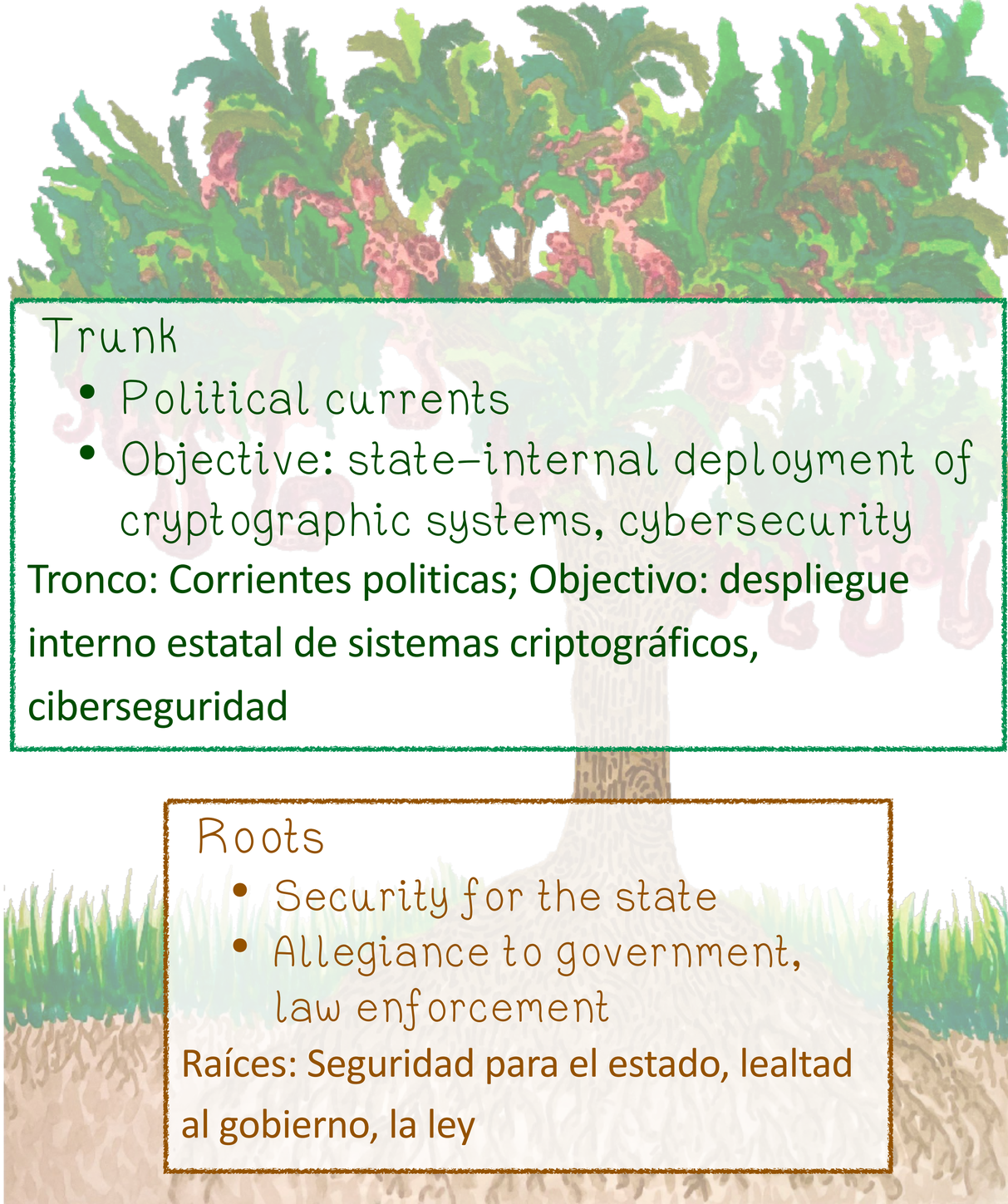
**Roots**

- Security & privacy at scale
- Making a good living

Raíces: Seguridad y privacidad a escala, Ganarse la vida bien

# State Cryptographer

## Criptógrafe Estatal



Fruit

- Implementations
- State-internal deployment
- Making, protecting state-owned property and power

Fruta: Implementaciones, Despliegue interno del Estado, Fabricación y protección de la propiedad y el poder del Estado

Trunk

- Political currents
- Objective: state-internal deployment of cryptographic systems, cybersecurity

Tronco: Corrientes politicas; Objectivo: despliegue interno estatal de sistemas criptográficos, ciberseguridad

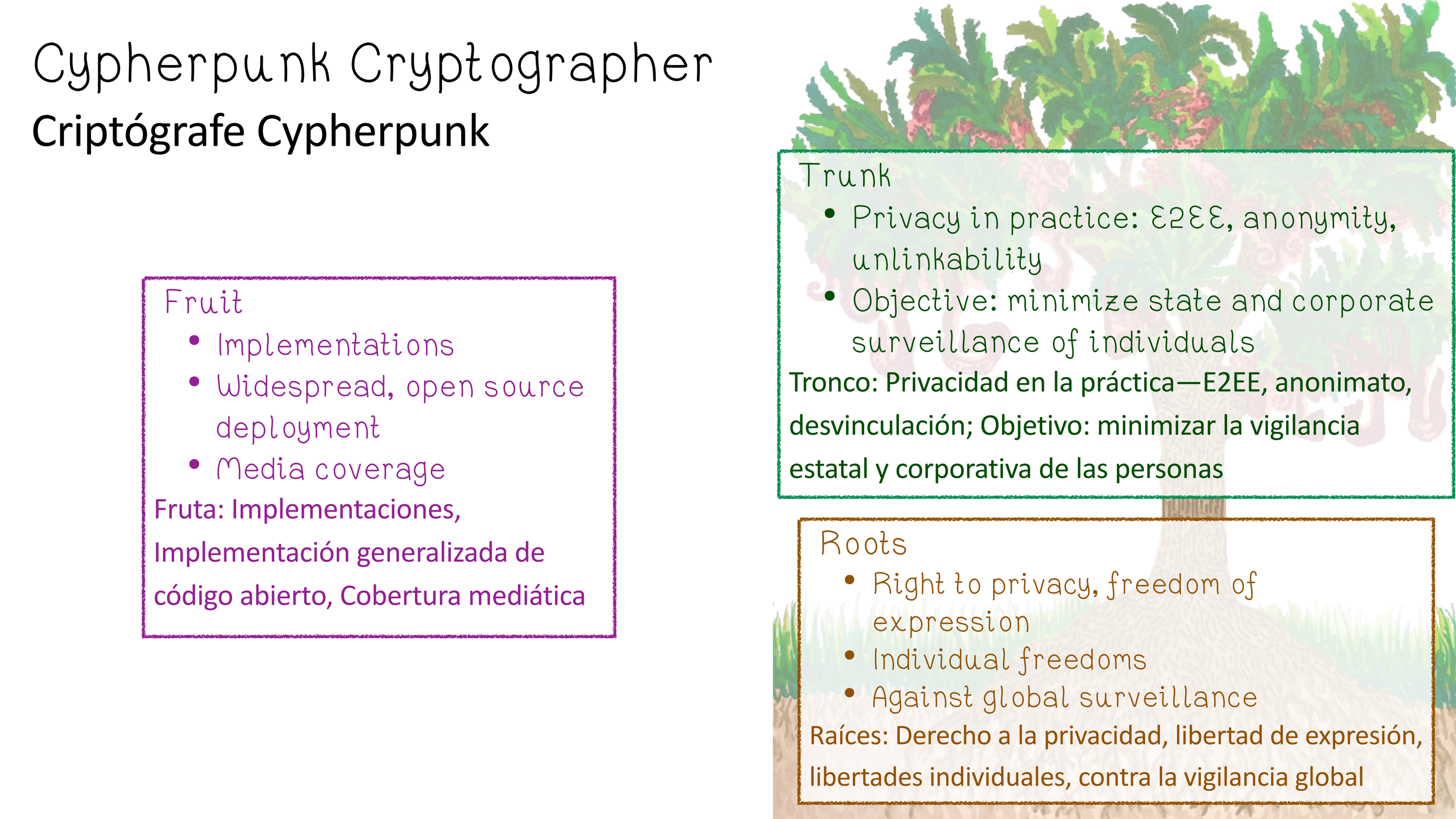
Roots

- Security for the state
- Allegiance to government, law enforcement

Raíces: Seguridad para el estado, lealtad al gobierno, la ley

# Cypherpunk Cryptographer

## Criptógrafe Cypherpunk



Fruit

- Implementations
- Widespread, open source deployment
- Media coverage

Fruta: Implementaciones, Implementación generalizada de código abierto, Cobertura mediática

Trunk

- Privacy in practice: E2EE, anonymity, unlinkability
- Objective: minimize state and corporate surveillance of individuals

Tronco: Privacidad en la práctica—E2EE, anonimato, desvinculación; Objetivo: minimizar la vigilancia estatal y corporativa de las personas

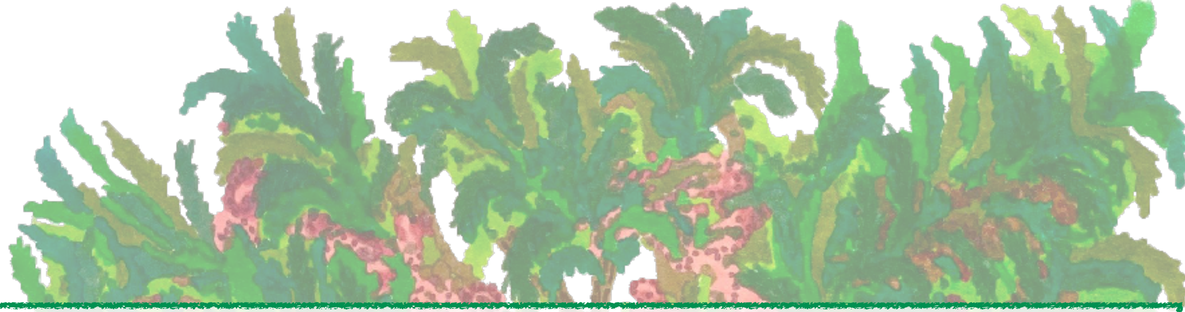
Roots

- Right to privacy, freedom of expression
- Individual freedoms
- Against global surveillance

Raíces: Derecho a la privacidad, libertad de expresión, libertades individuales, contra la vigilancia global

# Policy Cryptographer

## Criptógrafe de Políticas



### Trunk

- Political currents
- Objective: create government policies that protect right to privacy, free expression

Tronco: Corrientes politicas; Objetivo: crear políticas gubernamentales que protejan el derecho a la privacidad y la libertad de expresión.

### Fruit

- Legal policy, precedent
- Implementation
- Government

Fruta: Política jurídica, precedente, implementación, gobierno

### Roots

- Right to privacy, freedom of expression
- Individual freedoms
- Against state surveillance

Raíces: Derecho a la privacidad, libertad de expresión, libertades individuales, Contra la vigilancia estatal

# “Crypto for the People” Cryptographer

## “Criptó para la Gente” Criptógrafe

### Fruit

- New reference frame
- Implementations
- Local deployment
- New lineages

Fruta: Nuevo marco de referencia, implementaciones, espliegue local, nuevos linajes

### Trunk

- Systemic, tech-facilitated privacy and security problems of marginalized people
- Objective: work with marginalized people to understand, solve problems

Tronco: Problemas sistémicos de privacidad y seguridad de las personas marginadas facilitados por la tecnología; Objetivo: trabajar con personas marginadas para comprender y resolver problemas.

### Roots

- Right to privacy, free expression for people and communities who are marginalized and oppressed by longevic, instutionalized systems
- “Cryptography rearranges power”

Raíces: Derecho a la privacidad y libre expresión para las personas y comunidades marginadas y oprimidas por sistemas institucionalizados longevos, “La criptografía reordena el poder”

# Organizing Cryptographer

## Criptógrafe Organizador

Trunk

- Systemic, tech-facilitated privacy and security problems of marginalized people
- Objective: work with marginalized people to understand, solve problems
- Leverage cryptography to facilitate organizing against all systems of oppression

Tronco: Problemas sistémicos de privacidad y seguridad de las personas marginadas facilitados por la tecnología; Objetivo: trabajar con personas marginadas para comprender y resolver problemas, Aprovechar la criptografía para facilitar la organización contra todos los sistemas de opresión

Fruit

- New reference frame
- Implementations
- Local deployment
- New lineages
- (Hopefully) Dismantling systems of oppression, replacing them with systems of our collective imagination

Fruta: Nuevo marco de referencia, implementaciones, despliegue local, nuevos linajes, (con suerte) desmantelar los sistemas de opresión, reemplazándolos con sistemas de nuestra imaginación colectiva

Roots

- Right to privacy, free expression for people and communities who are marginalized and oppressed by longevic, instutionalized systems
- “Cryptography rearranges power”
- Cryptography should rearrange power

Raíces: Derecho a la privacidad y libre expresión para las personas y comunidades marginadas y oprimidas por sistemas institucionalizados longevos, “La criptografía reordena el poder,” La criptografía debería reorganizar el poder

# Not All Trees are Equitably Resourced

## No todos los árboles cuentan con recursos equitativos

### Sun & Nutrients

- Time
- Space
- Money
- Respect

Sol y nutrientes: Tiempo, Espacio, Dinero, Respeto

### Existing Paradigms

- Theoretical v. Applied
- Crypto-for-Security v. Crypto-for-Privacy (Narayanan 2013)
- Crypto-for-Crypto v. Crypto-for-Privacy (Rogaway 2015)
- Crypto for the People (Kamara 2020)

Paradigmas existentes: Teórico versus Aplicado, Cripto-para-seguridad contra Cripto-para-privacidad (Narayanan 2013), Cripto-para-Cripto contra Cripto-para-Privacidad (Rogaway 2015), Cripto para la gente (Kamara 2020)

### The Many-Tree Metaphor

- Honoring diverse roots, paradigms
- Let's refocus our time, space, money, and respect to center those who are (and have been) marginalized

La metáfora de los muchos árboles: Honrando diversas raíces y paradigmas, Reorientemos nuestro tiempo, espacio, dinero y respeto para centrarnos en aquellos que están (y han estado) marginados

Image Credits: Jean Robert and Gemma (2010)

# Grounding Questions — Preguntas Fundamentales

What is the "root" of cryptography? Where does it come from?

¿Cuál es la "raíz" de la criptografía? ¿De dónde viene?

Which roots and histories will we nourish moving forward?

¿Qué raíces e historias alimentaremos en el futuro?

Why do we care? What "fruit" are we trying to produce?

¿Por qué nos importa? ¿Qué "fruto" estamos tratando de producir?

How does our work reflect our histories, values, and motivations?

¿Cómo refleja nuestro trabajo nuestras historias, valores y motivaciones?

# Cryptography from Roots to Fruits — Criptografía desde las Raíces hasta los Frutos

- Grounding Questions — Preguntas Fundamentales ✓
- The Many-Tree Metaphor — La metáfora de los muchos árboles ✓
- Threat Modeling Paradigm Shift — Cambio de paradigma en el modelado de amenazas
- Cryptography & Technology for Grassroots Organizing — Criptografía y tecnología para la organización de base
- Trust Infrastructure for Grassroots Organizing — Infraestructura de confianza para la organización de base
- Activity: What is Your Tree? — Actividad: ¿Cuál es tu árbol? ←
- From Roots to Fruits, Revisited — De las raíces a los frutos, revisados

# Think-Pair-Discuss Activity

## Actividad: Pensar, Emparejar, Discutir

1. Think, Write, Draw (5 min)
   a. What does your tree look like?

   Roots: values & motivation, frames of reference, personal history
   Trunk: problems of interest, solution toolbox, work environment
   Fruit: (re)produced work, environment, values & motivation

   Piensa, escribe, dibuja: ¿Cómo es tu árbol?

   Raíces: valores y motivación, marcos de referencia, historia personal
   Tronco: problemas de interés, caja de herramientas de solución, ambiente de trabajo
   Fruta: trabajo (re)producido, entorno, valores y motivación.

2. Pair (10 min)
   a. Find a partner and introduce yourself.
   b. Share 1-2 aspects of your tree that you are the most excited about.
   c. Discuss: How are various parts of your tree represented in the wider cryptography community? Which aspects (if any) would you like to see take up more or less space?

   Emparejar: Encuentra un compañero y preséntate. Comparte 1 o 2 aspectos de tu árbol que más te entusiasmen. Discutir: ¿Cómo se representan las distintas partes de su árbol en la comunidad criptográfica más amplia? ¿Qué aspectos (si los hay) le gustaría que ocuparan más o menos espacio?

3. Group Discussion (10 min) — Discusión de grupo