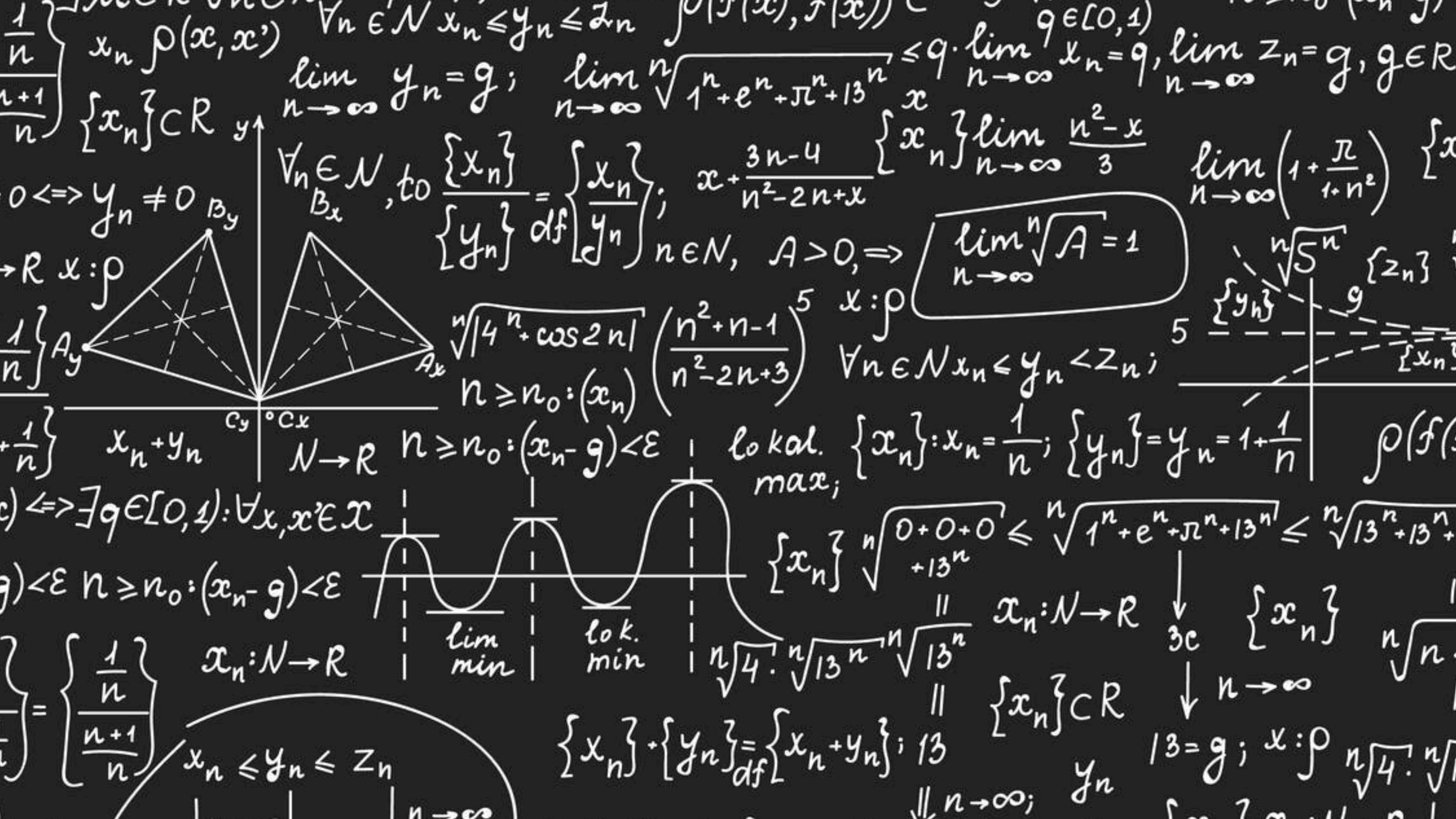
Crypto for the People

Seny Kamara

BROWN

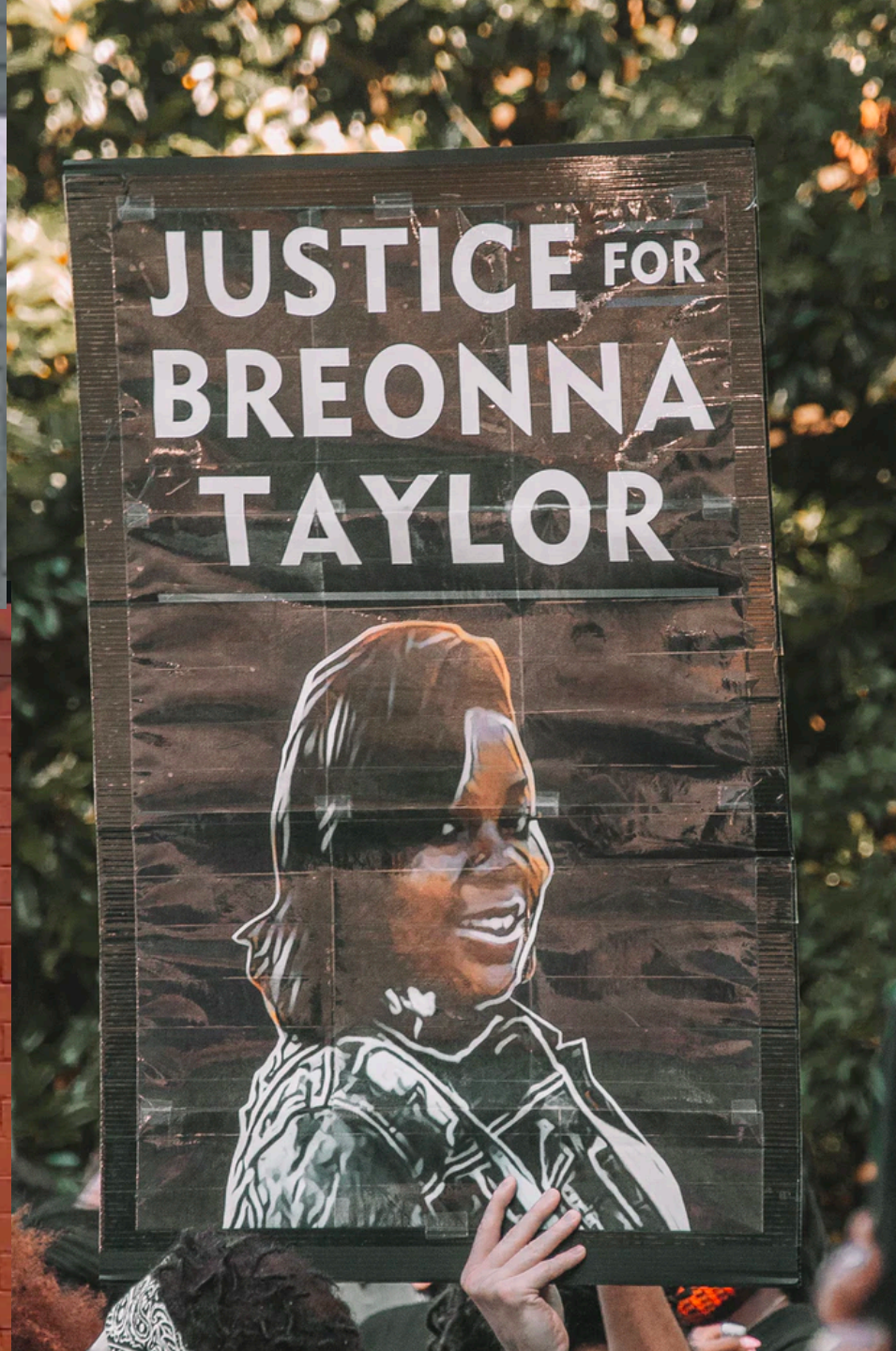
ENCRYPTED SYSTEMS LAB



∀n ∈ N xn ≤ yn ≤ zn
lim yn = g; n→∞
lim ⁿ√(1ⁿ+eⁿ+πⁿ+13ⁿ) ≤ q · lim xn = q, lim zn = g, g ∈ R
q ∈ [0,1)
{xn} ⊂ R
∀n ∈ N, to {xn}/{yn} =df {xn/yn};
x + (3n−4)/(n²−2n+x)
{xn} lim (n²−x)/3
lim (1 + π/(1+n²))
yn ≠ 0
By
Bx
Ay
Ax
Cy
Cx
x : ρ
n ∈ N, A > 0, ⇒ lim ⁿ√A = 1
ⁿ√5ⁿ
{zn}
{yn}
{xn}
ⁿ√|4ⁿ + cos2n|
((n²+n−1)/(n²−2n+3))⁵
∀n ∈ N xn ≤ yn < zn;
n ≥ n0 : (xn)
xn + yn
N → R
n ≥ n0 : (xn − g) < ε
lokal. max;
{xn} : xn = 1/n; {yn} = yn = 1 + 1/n
∃q ∈ [0,1) : ∀x, x' ∈ X
lim min
lok. min
{xn} ⁿ√(0+0+0+13ⁿ) ≤ ⁿ√(1ⁿ+eⁿ+πⁿ+13ⁿ) ≤ ⁿ√(13ⁿ+13ⁿ
xn : N → R
{xn} ⊂ R
n → ∞
13 = g; x : ρ
{xn} + {yn} =df {xn + yn}; 13
xn ≤ yn ≤ zn


STAY
ALIVE


FOREVER BREATHING
IN OUR HEARTS

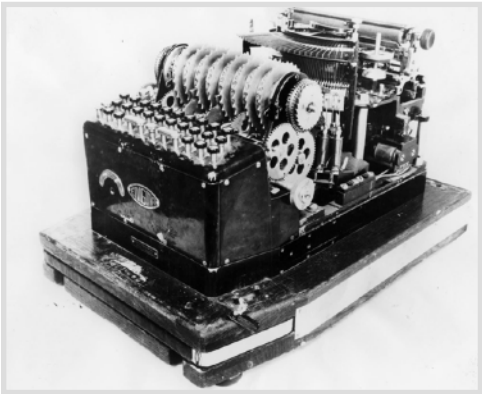

JUSTICE FOR
BREONNA
TAYLOR

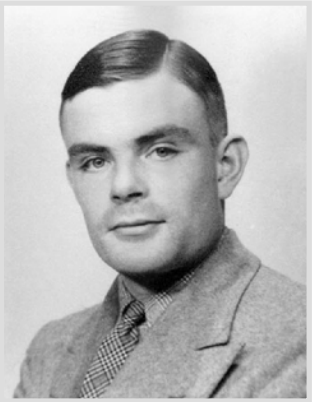
Perspective

- as a Black person
- as an immigrant
- as an applied cryptographer
- as an *outsider*


1001100101 10
10100101 0001
1000011001 1
10101 1100100
1111011100 111
10110111 001

The Impact of Cryptography



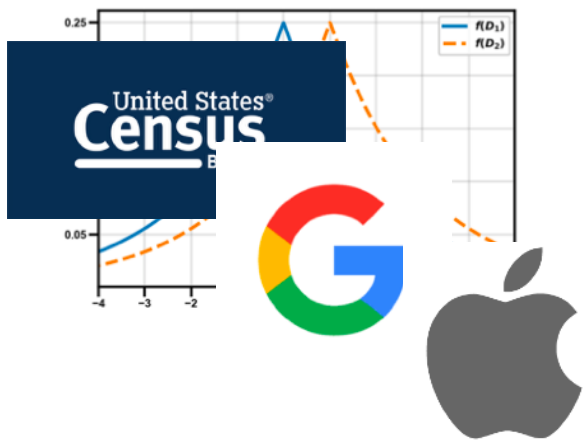


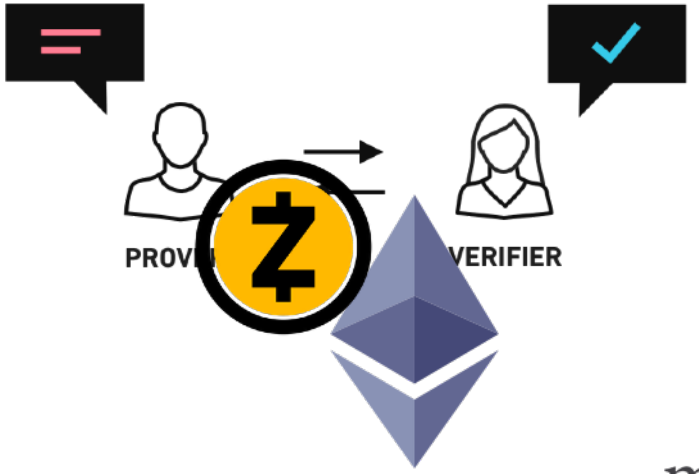
- Cryptanalysis (Bletchley Park)
  - shortened WWII by 2 years
  - saved 14 million lives
- Crypto is fundamental to
  - e-commerce
  - banking ($40T)
  - data security & privacy
- AES alone has contributed $250B to the US economy

Modern Cryptography

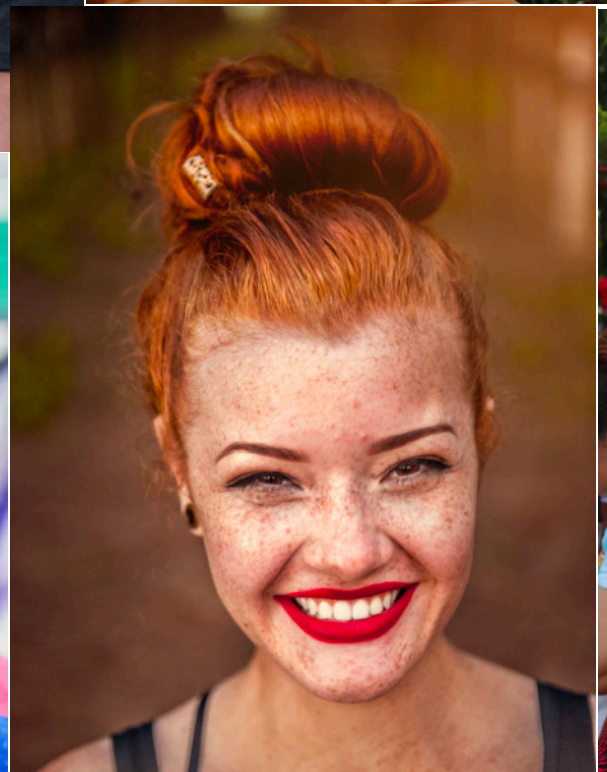
Anonymous Credentials	Private Set Intersection	Multi-Party Computation	Differential Privacy	Blockchains
Zero-Knowledge Proofs	FHE	Oblivious RAM	Functional Encryption	Structured Encryption
Block Ciphers	Hash Functions	Public-Key Encryption	Signatures	PRFs & PRGs

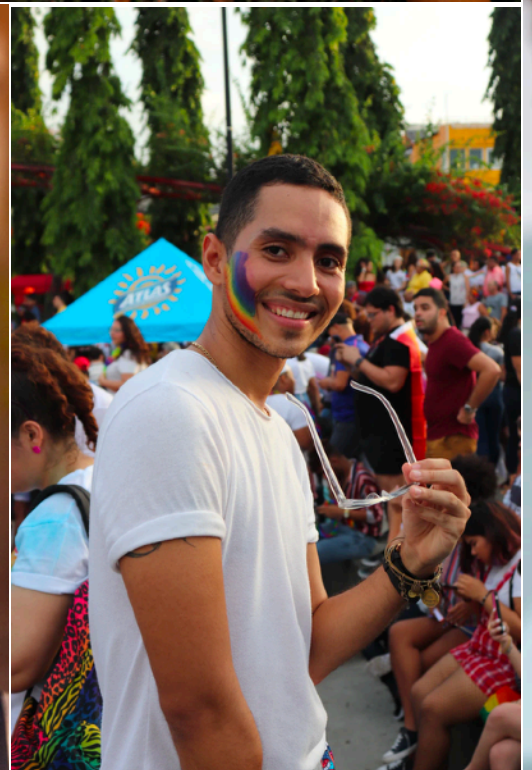
The Impact of Modern Cryptography





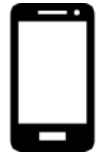
Who Benefits from Cryptography?

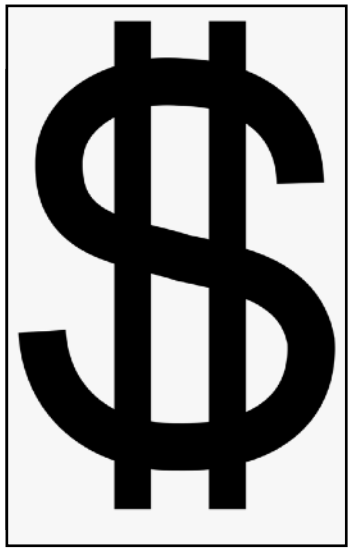


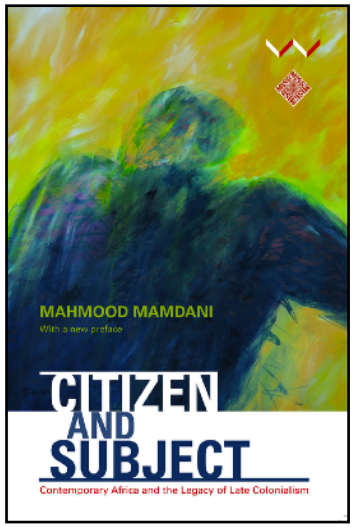


But it's a Pipeline!

But it's a Pipeline!







The Pipeline Argument

SKETCHY

- Big Tech
  - poor track record on user privacy & security
  - users ≠ customers
  - users are not monolithic…
  - …and Big Tech doesn't cater equally to all users

- Government
  - NSA, ICE & FBI spend money & political capital to erode privacy

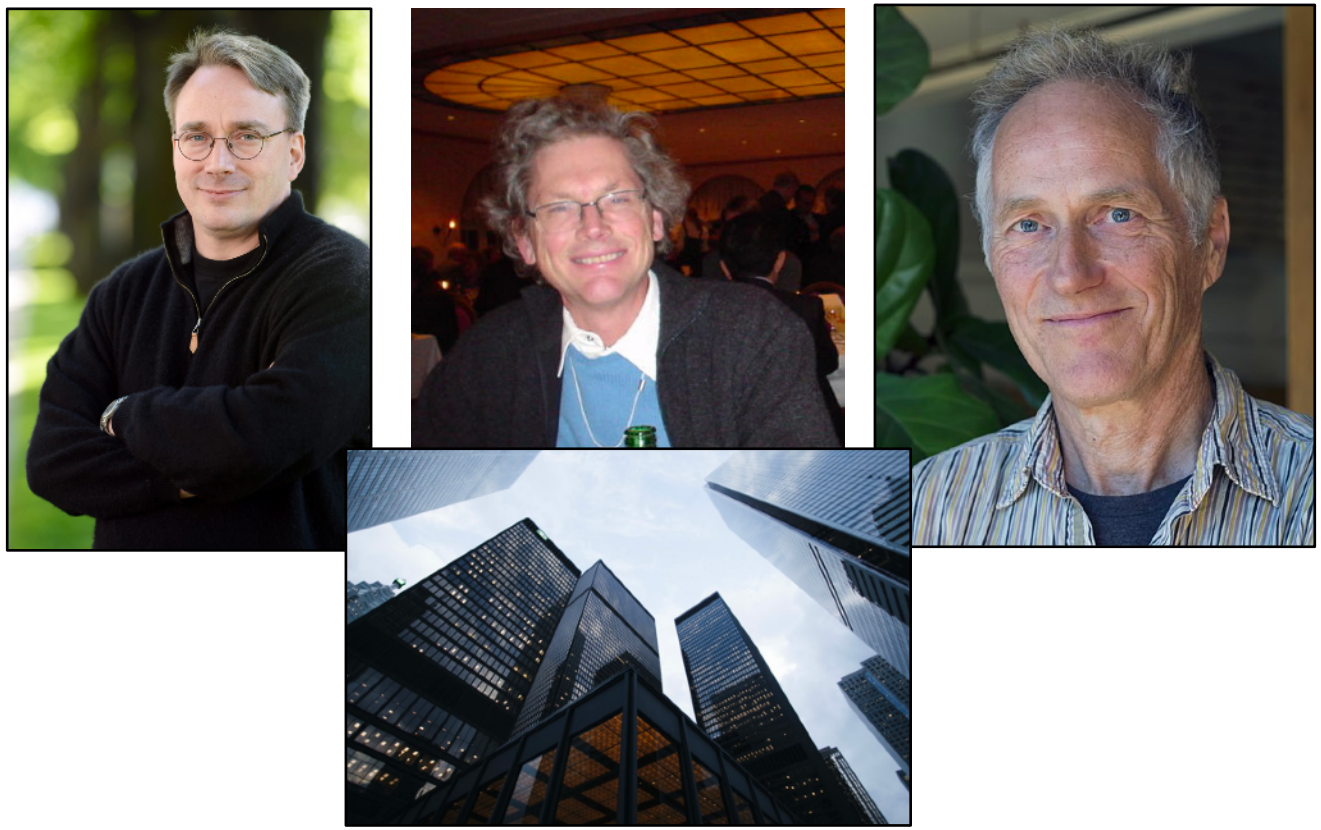
Academia

- We're *trained* to do *corporate* research
  - my 8 years at Microsoft Research ≈ my 6+4 years in Academia
- How do we motivate our research?
  - My protocol has practical value!
- Having your work used by a startup or a big company is a big deal!
  - demonstrates real-world impact
  - increases chances of getting funding
  - increases chances of getting tenure

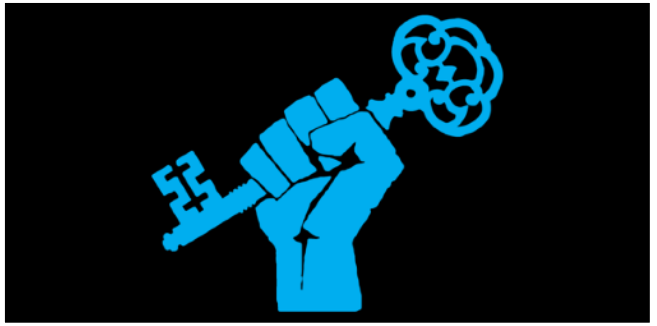
Academia

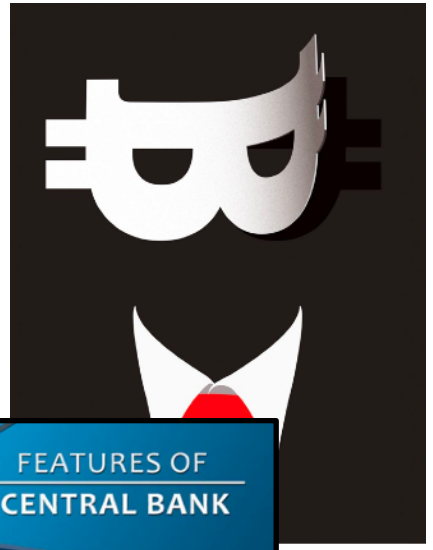
The University of X Office of Technology Transfer is responsible for bringing inventions arising from U of X research to *society*.

Open Source Movement

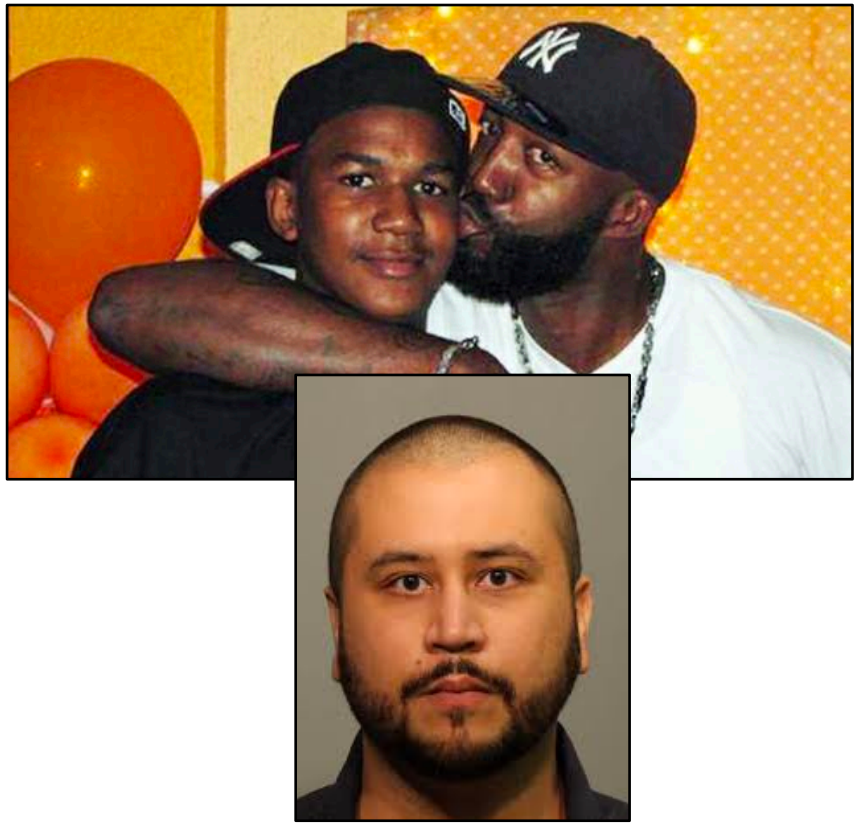


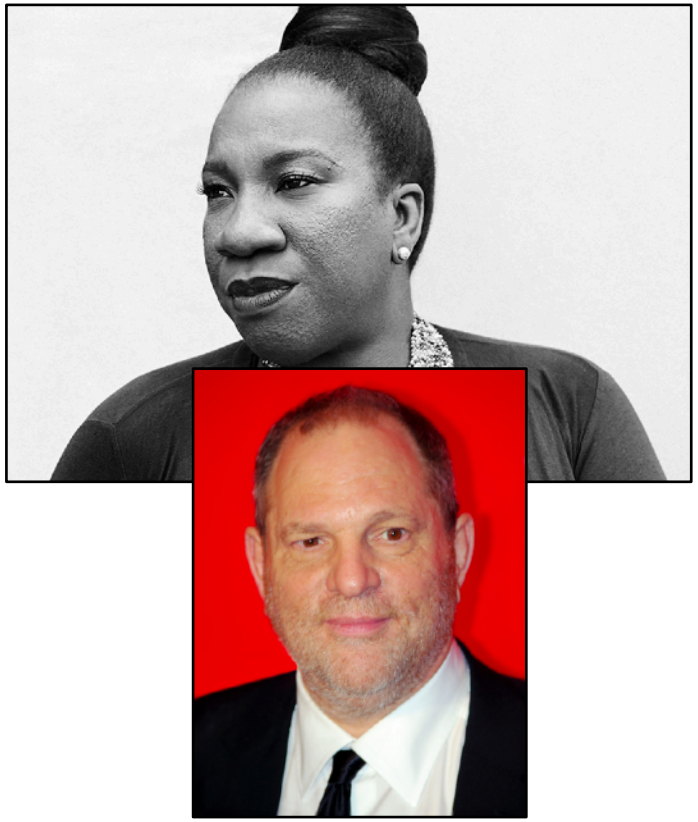
Cypherpunk Movement





What About the Rest of ***Us***?





What About the Rest of Us?

Q: Who’s going to make crypto for the marginalized?

Crypto for the People

- Academia ≈ (free) corporate research lab

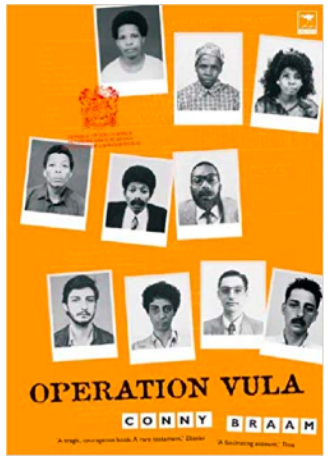
- Cypherpunks are concerned with *personal* freedoms
  - with respect to Governments & Intelligence Agencies
  - very libertarian perspective

- *Crypto for the People* is concerned with fighting *oppression* & *violence*
  - from Law Enforcement (Police, FBI, ICE)
  - from social hierarchies and norms
  - from domestic terrorists
    - Neo Nazis, the Alt-right, White supremacists, religious fanatics

I just design algorithms & protocols

Agency

- As scientists & as researchers, we have agency
- Academic freedom & tenure allows us to take risks




TUNISIA
MOROCCO
ALGERIA
LIBYA
EGYPT
SAHARA
MAURITANIA
MALI
NIGER
CHAD
SUDAN
DJIBOUTI
SENEGAL
GAMBIA
GUINEA BISSAU
GUINEA
BURKINA FASO
NIGERIA
TOGO
BENIN
ETHIOPIA
SOMALIA
SIERRA LEONE
LIBERIA
COTE D'IVOIRE
GHANA
CAMEROON
CENTRAL AFRICAN REPUBLIC
UGANDA
KENYA
EQUATORIAL GUINEA
GABON
CONGO
RWANDA
BURUNDI
ZAIRE
TANZANIA
COMORES
MALAWI
ANGOLA
ZAMBIA
MOZAMBIQUE
MADAGASCAR
ZIMBABWE
NAMIBIA
BOTSWANA
SWAZILAND
SOUTH AFRICA
LESOTHO

South Africa

- Population of 57 million
  - Black 80%
  - Coloured 8.8%
  - White 8.4%
  - Indian/Asian 2.5%

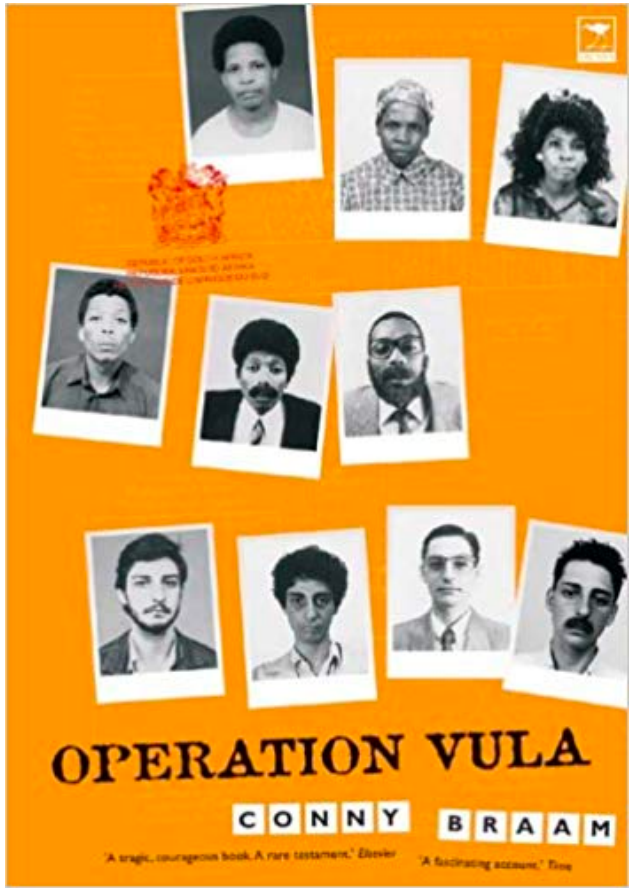
Apartheid 1948-1990's

- System of institutionalized racial segregation
- Petty apartheid
  - facilities, events, …
- Grand apartheid
  - housing, employment, …

African National Congress

- Founded in 1912
- Non-violent until Sharpeville Massacre in 1960
  - South African police opened fire on protestors
- ANC banned in 1960
  - starts to operate internationally

Vula

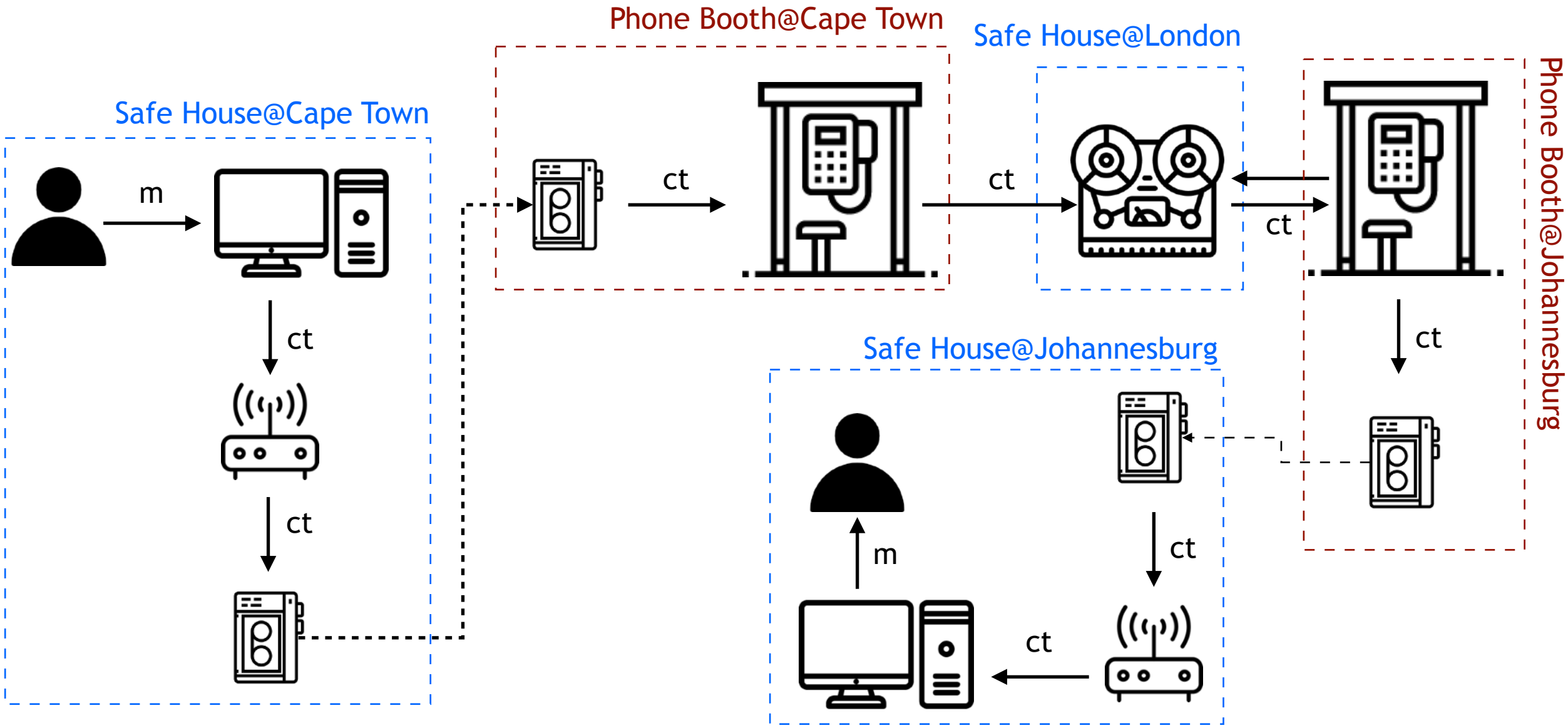


- Due to ban
  - secure communications are critical to operations
  - exiled generals and covert operatives in SA
- Secret inks & book codes
  - hard to use, low-bandwidth & tedious
- In mid-80's ANC develops a communication system
  - between London, Zambia, Netherlands & South Africa

Vula

- Asynchronous
  - parties can’t be online at the same time
- Covert
  - use of encryption & computers was suspicious at the time
- Distance
  - lots of errors introduced in communications from Lusaka to London
- Public
  - users may not have phone lines at home

Vula


Phone Booth@Cape Town
Safe House@London
Safe House@Cape Town
Phone Booth@Johannesburg
Safe House@Johannesburg
m
ct
ct
ct
ct
ct
ct
ct
m

Vula

- Encryption scheme
  - Enc(K, m) = PRG(K) ⊕ m, with custom-designed PRG
  - keys were seeds from books
  - used seeds were marked with invisible ink
  - mention of error-correction

- System ran without detection until early 1990's
  - heavily used by ANC
  - used to communicate w/ Nelson Mandela in jail

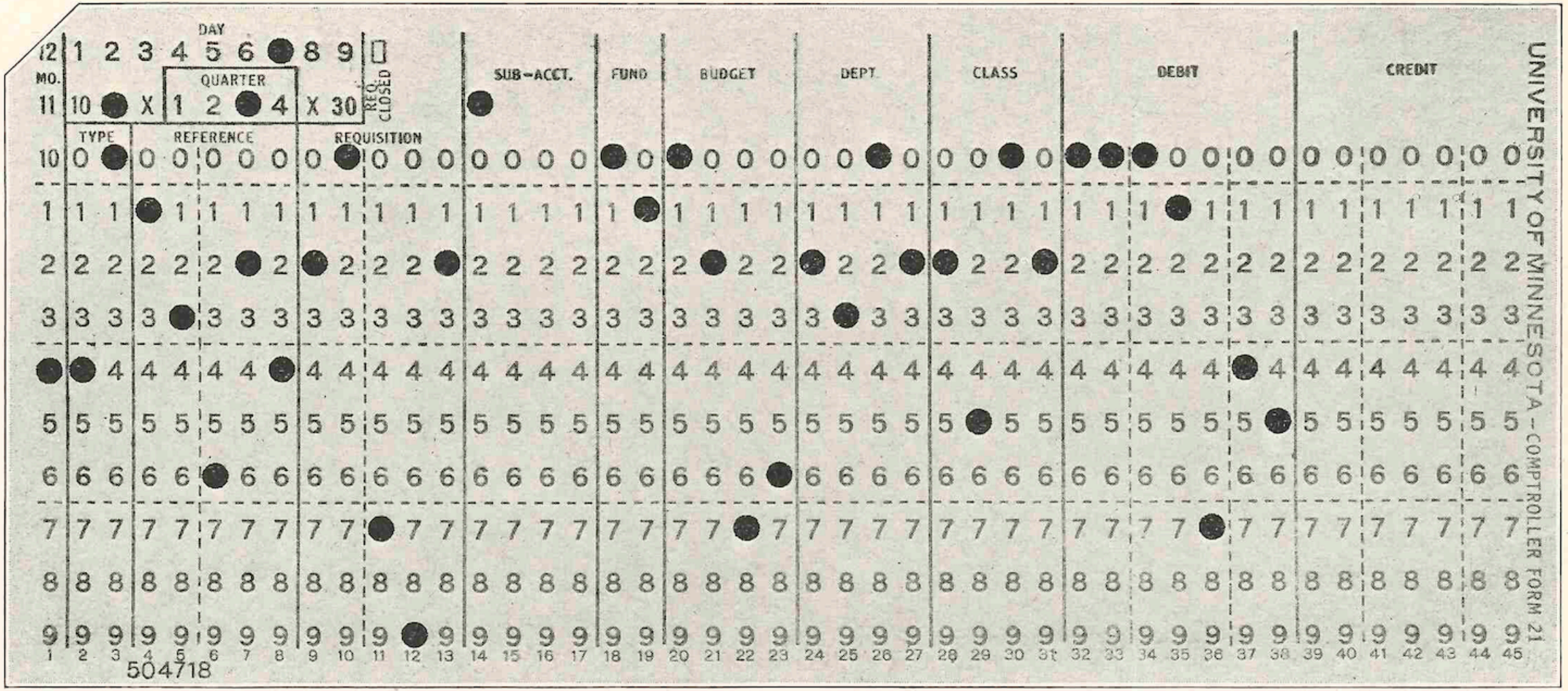
Vula

- Vula designers consulted crypto literature but…

> "…all I discovered was that cryptology was an arcane science for bored mathematicians, not for underground activists.
>
> However I discovered a few tricks and used these to develop a system to meet our needs."
>
> —- Tim Jenkin

- Q: Should activists & protestors be solving their own crypto problems?

Databases Power *Everything*



HOLLERITH TABULATING CARD

Date—April 27, 1927
Quarter—Third
Type—40 Invoice
Reference—Invoice No. 13624

Requisition No. 20792 (Open)
Sub-Acct.—None
Fund—01 Support Fund
Budget—276 Bacteriology Supplies

Department—2302 Medical School—Bacteriology
Classification—2502 Chemicals
Amount—Debit $17.45

Historical use of “Proto”-Databases

- 1933
  - Hitler elected Chancellor of Germany
  - German government conducts a census
  - Uses Dehomag/IBM tabulation machines to identify Jews
  - Estimates of 400,000 Jews increases to 2 million

- Every Nazi concentration camp had one of these machines

CalGang

- CA police database used to track gang members

- 88,000 people in CalGang
  - 85% Black and Latino men

- Criteria for inclusion
  - admission, association, tattoos, hanging out in gang areas
  - gang dress, hand signs, informants

- Consequences of being in gang database
  - increased police harassment & attention
  - denial of bail, housing, employment

CalGang Audit (2015)

- Many errors
  - 42 entries were less than 1 years old…

- Reviewed 100 individuals with a total of 563 “evidence points”
  - found 13 individuals who should not have been included
  - 131/563 “evidence points” were not supported

- Juveniles & their parents supposed to be notified
  - 2 agencies did not notify 70% of the 129 juveniles records *reviewed*

ICEGangs

- Immigration Customs Enforcement (ICE) gang DB
  - inspired by CalGang

- Both built by company called CSRA (acq. by General Dynamics)

- Consequences of being in ICEGangs
  - increased priority for deportation
  - can be denied DACA status

TAP Databases

[Amjad-Dai-K.-Pu-Qin'20]

- Databases have a huge impact on marginalized people

- What if we could design a database that
  - erases itself even if someone actively tries to preserve it
  - only preserve records past expiration with authorization from Judge
  - allows contents to be checked and audited privately

- Flip the power dynamics
  - currently need to trust Law Enforcement to erase data
  - to keep record, Law Enforcement has to get permission from Judge

TAP Databases
[Amjad-Dai-K.-Pu-Qin'20]

- Preliminary results show this is possible
  - still slow and incomplete

- Would Law Enforcement ever use this?
  - Not voluntarily but…

- Handschuh Agreement (1985)
  - Class action lawsuit vs. New York City & NYPD for spying on…
  - …Black Panthers, Anti-war & Gay Rights activists, and others
  - resulted in decree that set guidelines on how NYPD gathers intelligence

Not Crypto for the People

- My new blockchain will
  - serve rural communities in Africa
  - "solve long-standing developmental issues & unlock much-needed economic growth"

- Doing it wrong
  - using marginalized groups to motivate your existing research or product

- Doing it right
  - new research/tech to address problems experienced by marginalized groups
  - *in consultation with experts*

I Am *Not* Suggesting…

- …that cryptographers do useless work
- …that cryptographers don't care about people
- …that every cryptographer should work on this kind of problem
- …or even that *you* should work on this kind of problem

I *Am* Suggesting…

- …that the Crypto *community*
  - …has had little impact on marginalized people
  - …is barely aware of the problems of marginalized groups
  - …suffers from a serious lack of diversity

The Impact of Cryptography ?

- Cryptography is critical to
  - Government, Diplomacy, War, Intelligence,
  - Banking, e-Commerce, Privacy

- Modern cryptography is in the process of impacting
  - Finance, data storage & processing, advertising, analytics, ML, …

Q: Can cryptography impact “the People”



It's Up to the Community

- New research agendas
  - research problems motivated by experiences of marginalized groups
  - value potential impact rather than "technical depth"

- New incentives & rewards
  - publication venues, workshops, lecture series

- New sources of funding
  - Big Tech and DoD won't care. Will the NSF fund this? Will *you* rate it on panels?

- Efforts to diversify the community
  - demographically but also intellectually

Towards Diversifying Cryptography

- Diversity doesn't "just happen"

- Diversity requires
  - effort, resources, strategy
  - changes in culture

- More open & welcoming culture
  - open invitations instead of "invitation only"
  - create diverse recruiting pipelines
  - value more diverse research agendas