PETS 2017
The 17th Privacy Enhancing Technologies Symposium
July 18–21, 2017
Minneapolis, MN, USA

VirginiaTech
Invent the Future

Provably Secure Anonymous-yet-Accountable Crowdsensing with Scalable Sublinear Revocation

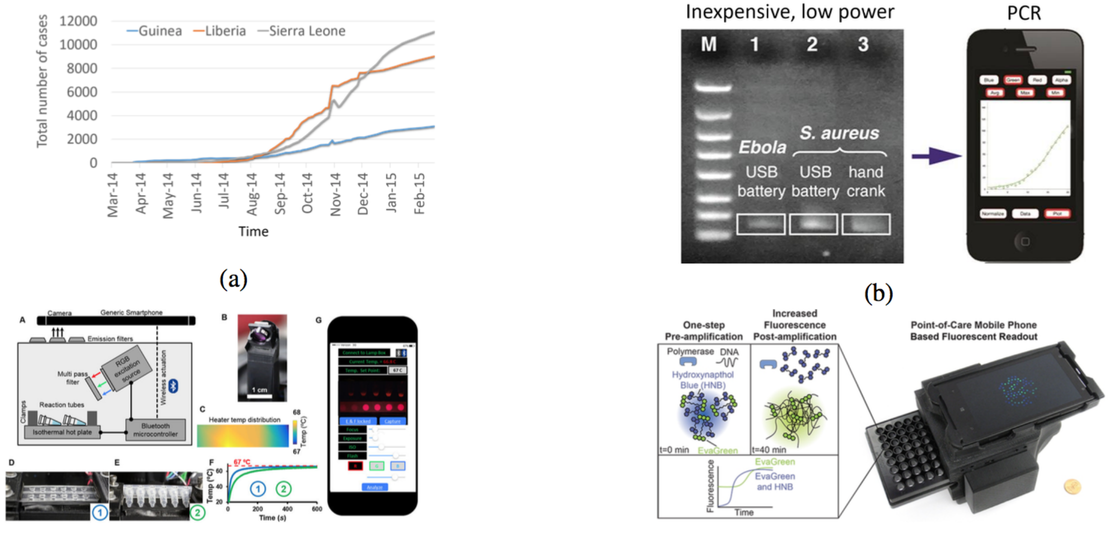
Sazzadur Rahaman[1], Long Cheng[1], Danfeng (Daphne) Yao[1], He Li[2], Jung-Min (Jerry) Park[2]

Computer Science[1], Electrical & Computer Engineering[2]

Virginia Tech

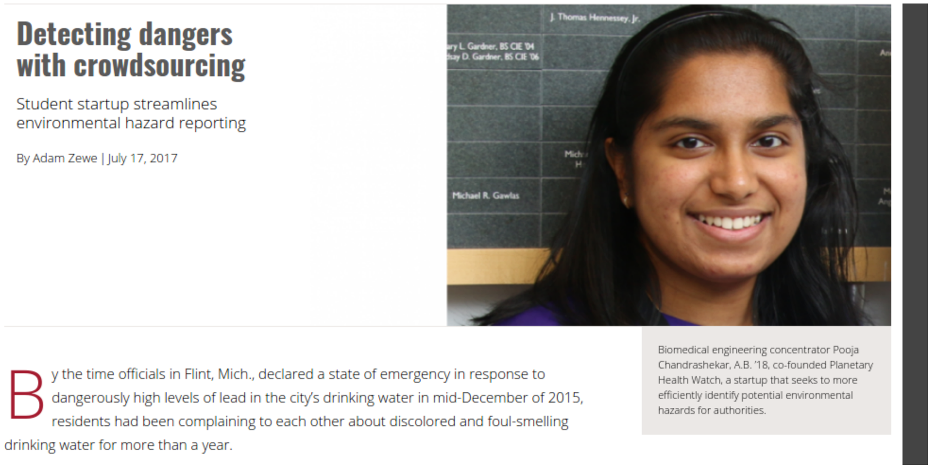
{sazzad14, chengl, danfeng}@cs.vt.edu, {heli, jungmin}@ece.vt.edu

Mobile Computing Opportunities



(a) (b)

(c) (d)



Detecting dangers with crowdsourcing

Student startup streamlines environmental hazard reporting

By Adam Zewe | July 17, 2017

By the time officials in Flint, Mich., declared a state of emergency in response to dangerously high levels of lead in the city's drinking water in mid-December of 2015, residents had been complaining to each other about discolored and foul-smelling drinking water for more than a year.

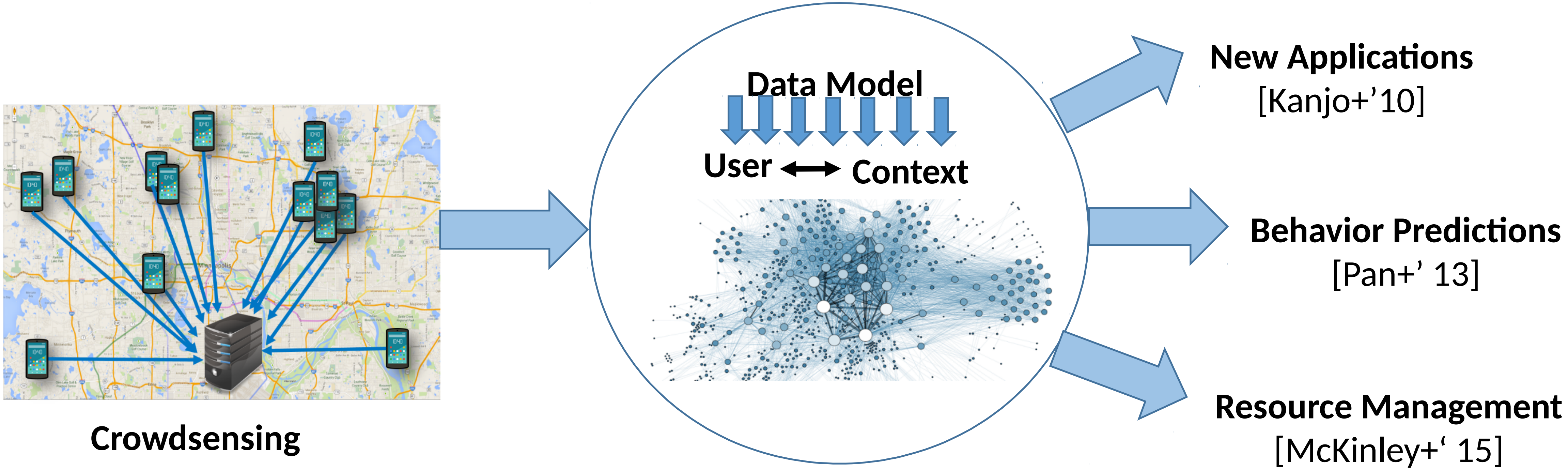
Biomedical engineering concentrator Pooja Chandrashekar, A.B. '18, co-founded Planetary Health Watch, a startup that seeks to more efficiently identify potential environmental hazards for authorities.

Detecting dangers with crowdsourcing[1]

Bioanalysis using portable PCR built on mobile phones

[1] https://www.seas.harvard.edu/news/2017/07/detecting-dangers-with-crowdsourcing

Crowdsensing and Citizen Science



Data Model

User ⟷ Context

New Applications
[Kanjo+'10]

Behavior Predictions
[Pan+' 13]

Resource Management
[McKinley+' 15]

Crowdsensing

Machine learning

Pros:

Cost effective, easy to deploy

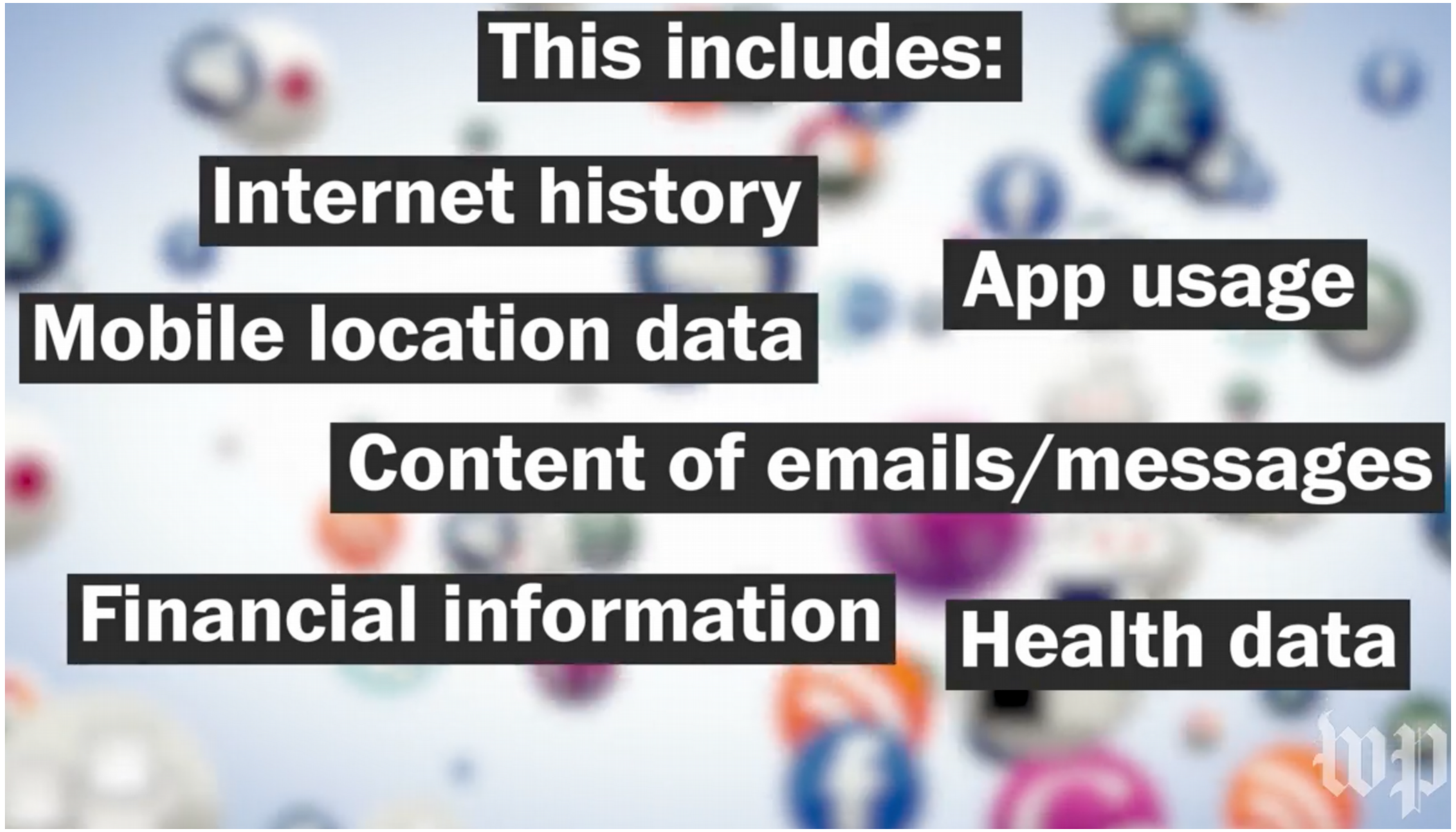
Users are in control!

Cons:

New possibilities to track users!

Is Privacy a Lost Battle?

March 28, 2017 – Congress sent proposed legislation to the White House that wipes away landmark online privacy protections.



This includes:

Internet history

App usage

Mobile location data

Content of emails/messages

Financial information

Health data

[Washington Post, March 28, 2017]

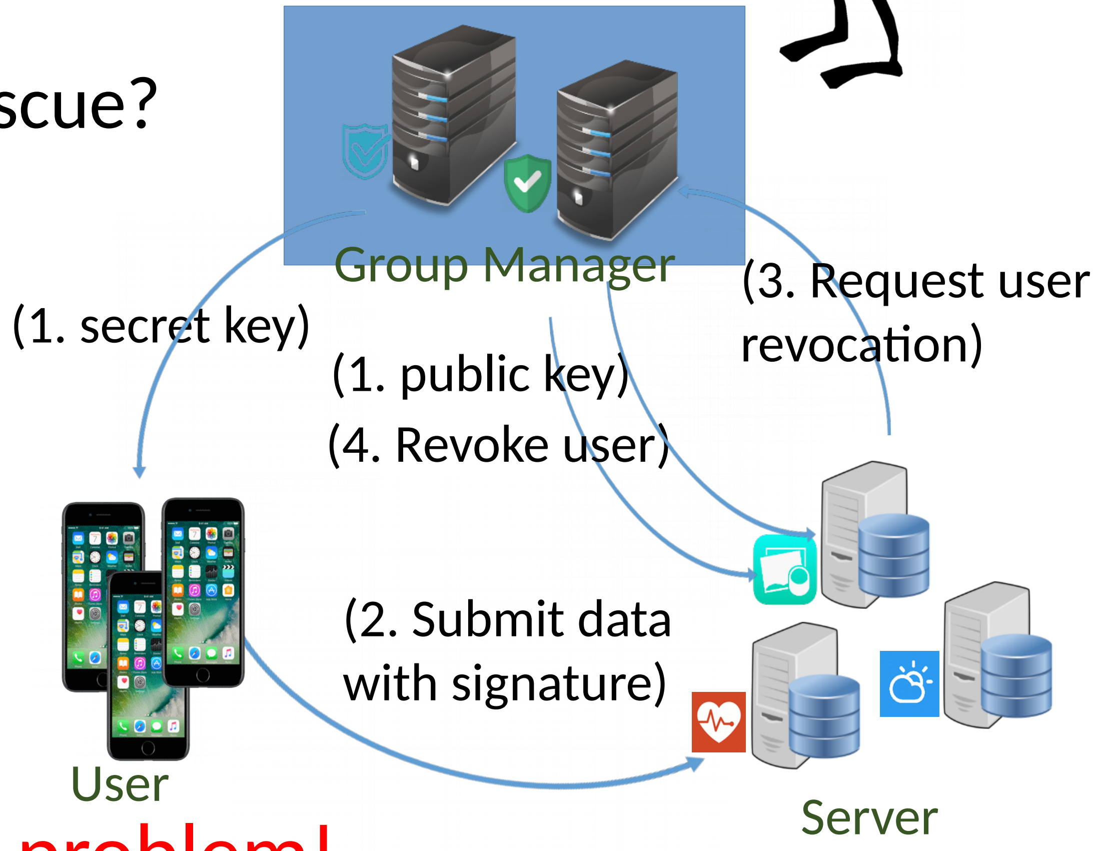
Privacy in crowdsensing

Are we ready to offer privacy preserving crowdsensing infrastructure?

Privacy Preserving Authentication to the rescue?

Privacy Preserving Authentication (PPA):

The mechanism of authenticating a user without knowing her identity.



Group Manager

(1. secret key)

(1. public key)

(4. Revoke user)

(3. Request user revocation)

(2. Submit data with signature)

User

Server

State-of-the art PPA cannot solve this problem!

Challenges for Existing PPA

Pseudonym-based: [SPPEAR: Gisdakis+' 14]

Actual IDs are replaced with short-lived pseudonyms.

Cons:

- Public Key certification overhead
- Signatures under the same secret key are linkable

Group Signature-based: [AnonySense: Cornelius+' 08]

One public key for all users and No two signatures are linkable under same signing key

Cons:

- The revocation check is of O(R)

It can give you server timeout 100s of Revoked Users!

Finding sublinear revocation for VLR-based GS is open for 13+ years! [Boneh+'04]

Our Contribution

A new computationally scalable GS Scheme (SRBE)

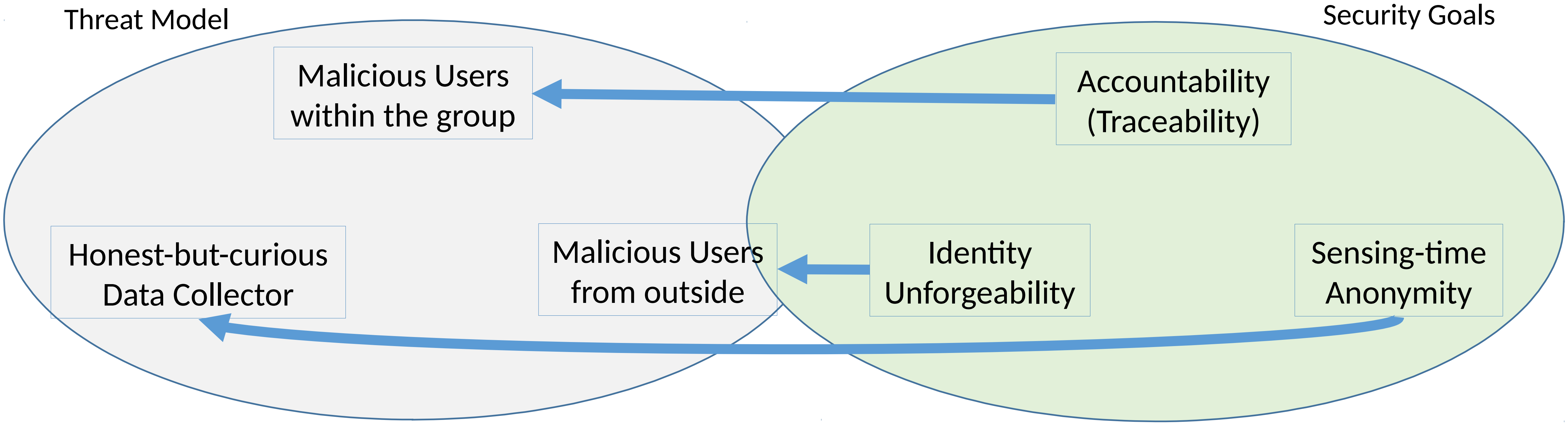
Features:

- Security properties: Backward Unlinkable Anonymity, Traceability and Exculpability.
- Sublinear Revocation check – Extremely scalable!
- It uses pseudonyms but achieves Constant revocation token size

A new scalable Crowdsensing Framework (GroupSense) with prototype implementation.

Threat Model and Security Goals

Assumption: Group Manager forms a group, anyone can join/leave at anytime!


Threat Model
Security Goals
Malicious Users within the group
Accountability (Traceability)
Honest-but-curious Data Collector
Malicious Users from outside
Identity Unforgeability
Sensing-time Anonymity

Goal: A practical anonymous-yet-accountable privacy preserving infrastructure

Our Contribution

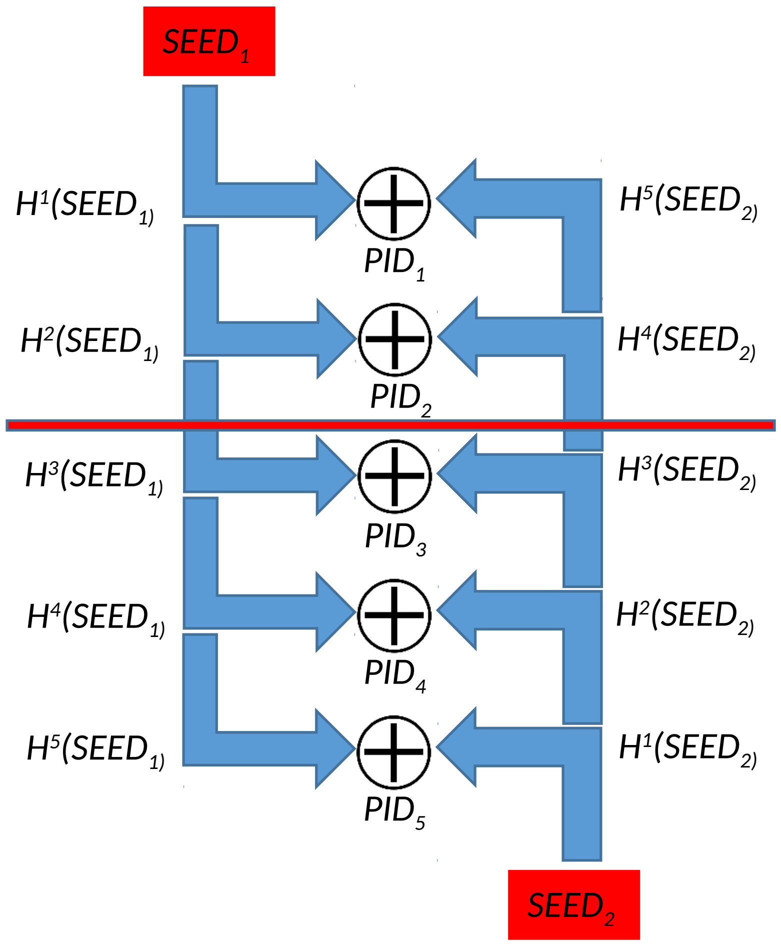
A new computationally scalable GS Scheme (SRBE)

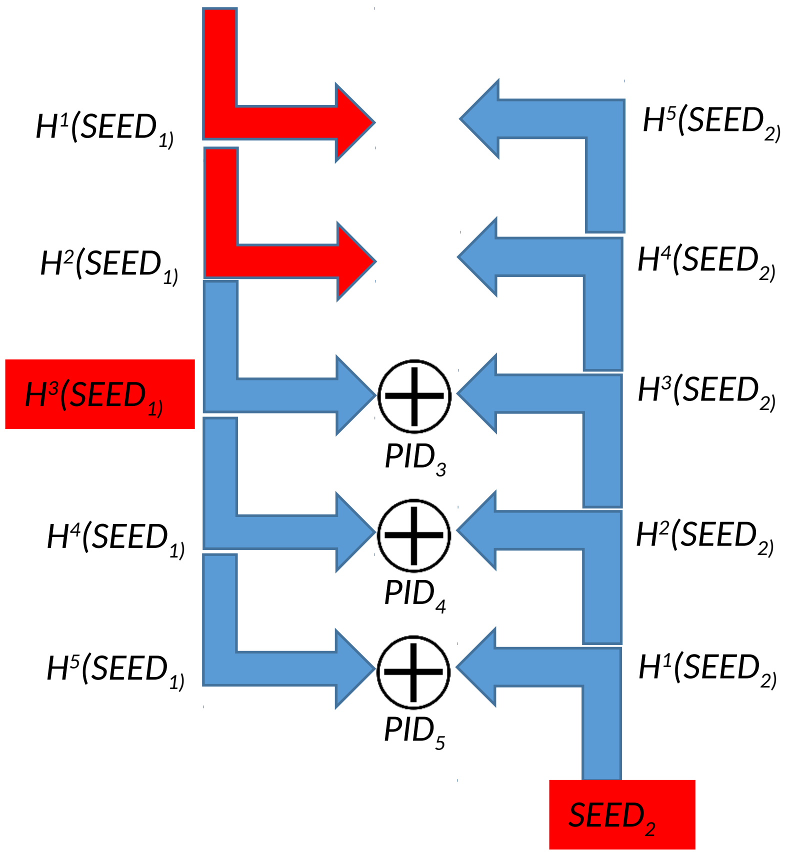
Features:

- Security properties: Backward Unlinkable Anonymity, Traceability and Exculpability.
- Sublinear Revocation check – Extremely scalable!
- It uses pseudonyms but achieves Constant revocation token size

A new scalable Crowdsensing Framework (GroupSense) with prototype implementation.

SRBE – Constant Revocation token Size

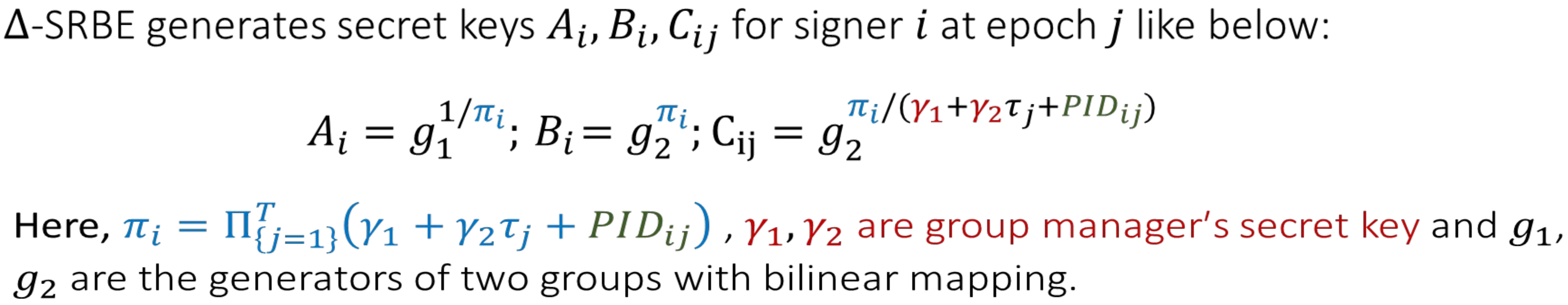




Embedding Pseudonyms in Signature

Security Properties:

- Signers are restricted to use issued pseudoIDs only.
- Signer *i* is restricted to use PID_{ij} for time period *j*.
- Even if one knows PID_{ij} , she cannot forge signatures.



Δ-SRBE generates secret keys A_i, B_i, C_{ij} for signer i at epoch j like below:

$$A_i = g_1^{1/\pi_i};\ B_i = g_2^{\pi_i};\ \mathrm{C_{ij}} = g_2^{\pi_i/(\gamma_1+\gamma_2\tau_j+PID_{ij})}$$

Here, $\pi_i = \Pi_{\{j=1\}}^{T}(\gamma_1 + \gamma_2\tau_j + PID_{ij})$, γ_1, γ_2 are group manager's secret key and g_1, g_2 are the generators of two groups with bilinear mapping.

Security Analysis

We prove the security of Δ-SRBE in the Random Oracle Model

Backward Unlinkable Anonymity: DLIN Assumption [Boneh+, 2004]

The anonymity of a valid signer is preserved (holds for revoked users too).

Limitation: Signatures from the same signer in the same time interval are linkable.

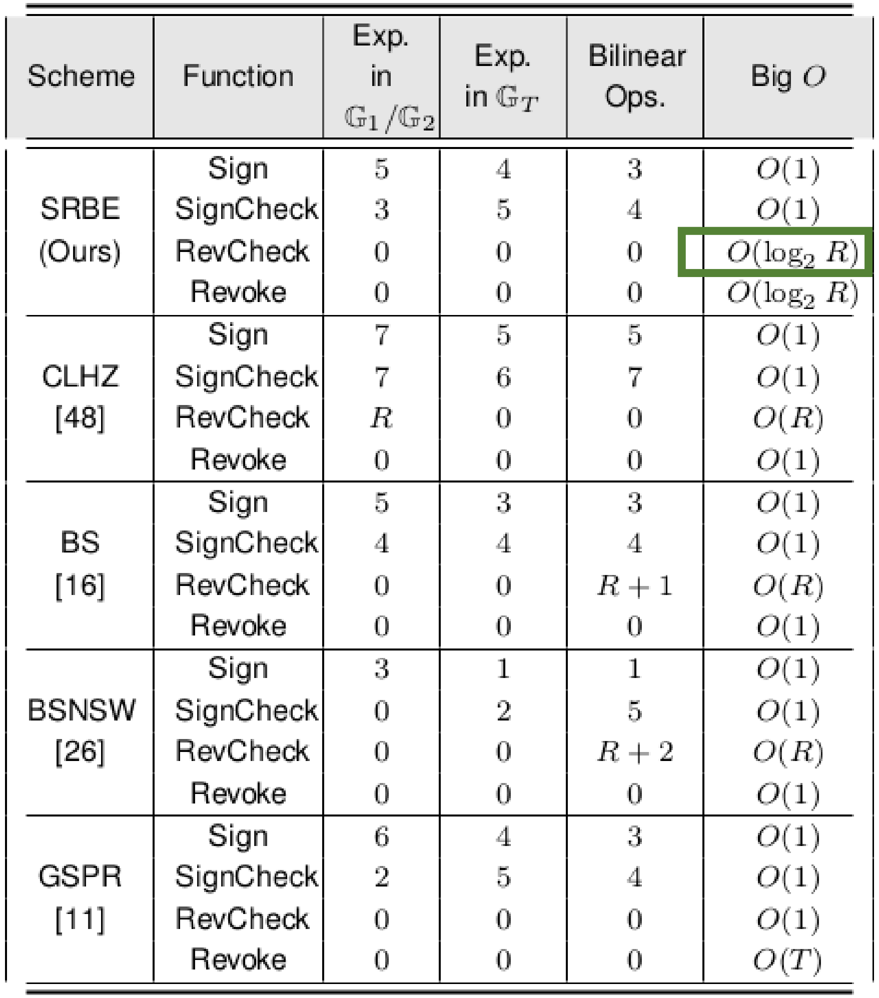
Traceability: q-BSDH Assumption [Boneh+, 2004]

Any valid signature is traceable to an honest signer.

Exculpability: DL Assumption [Kiayias+, 2004]

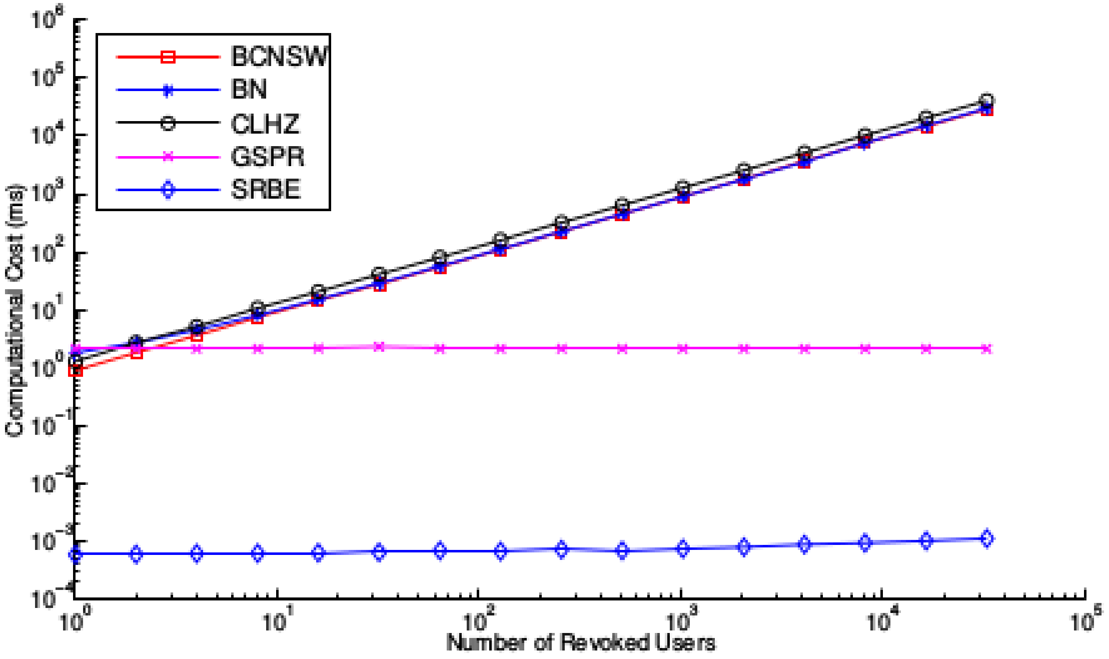
Even the group manager cannot frame an honest signer

Performance



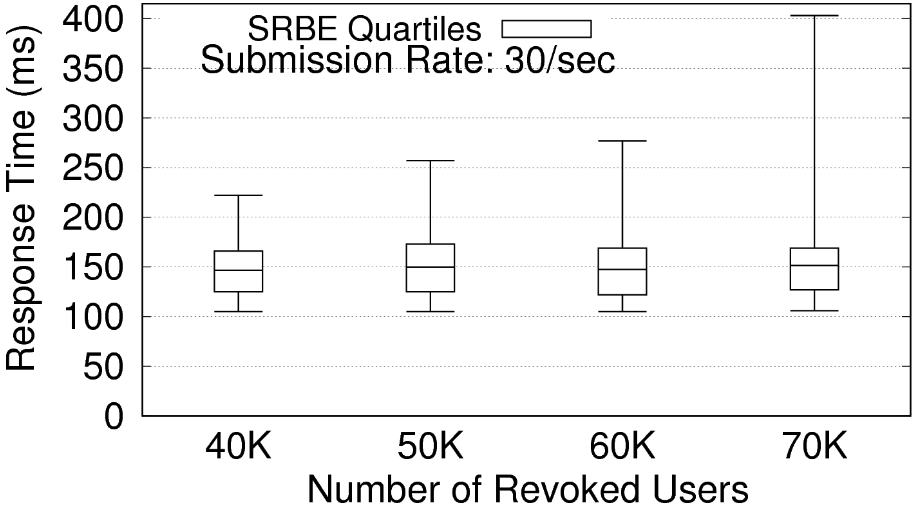
Scheme	Function	Exp. in $\mathbb{G}_1/\mathbb{G}_2$	Exp. in $\mathbb{G}_T$	Bilinear Ops.	Big O
SRBE (Ours)	Sign	5	4	3	$O(1)$
	SignCheck	3	5	4	$O(1)$
	RevCheck	0	0	0	$O(\log_2 R)$
	Revoke	0	0	0	$O(\log_2 R)$
CLHZ [48]	Sign	7	5	5	$O(1)$
	SignCheck	7	6	7	$O(1)$
	RevCheck	R	0	0	$O(R)$
	Revoke	0	0	0	$O(1)$
BS [16]	Sign	5	3	3	$O(1)$
	SignCheck	4	4	4	$O(1)$
	RevCheck	0	0	$R+1$	$O(R)$
	Revoke	0	0	0	$O(1)$
BSNSW [26]	Sign	3	1	1	$O(1)$
	SignCheck	0	2	5	$O(1)$
	RevCheck	0	0	$R+2$	$O(R)$
	Revoke	0	0	0	$O(1)$
GSPR [11]	Sign	6	4	3	$O(1)$
	SignCheck	2	5	4	$O(1)$
	RevCheck	0	0	0	$O(1)$
	Revoke	0	0	0	$O(T)$

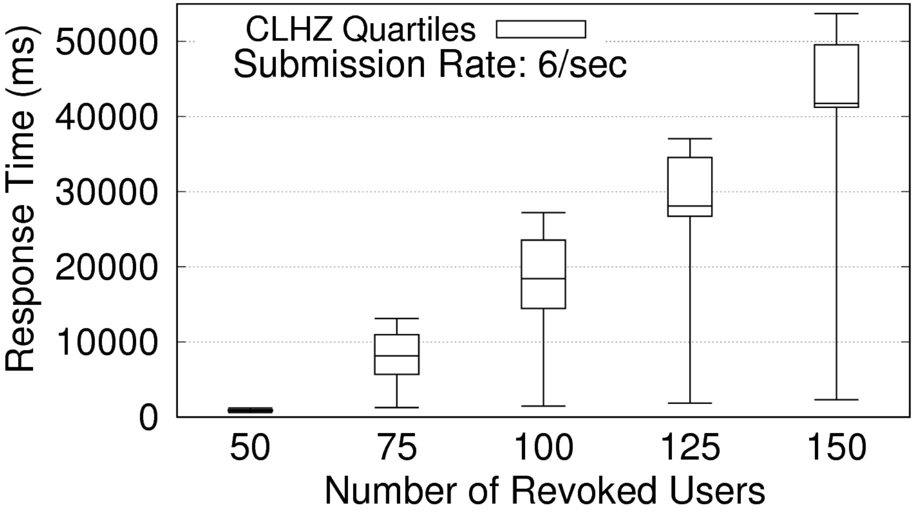
Overall computational complexity



Performance of RevocationCheck

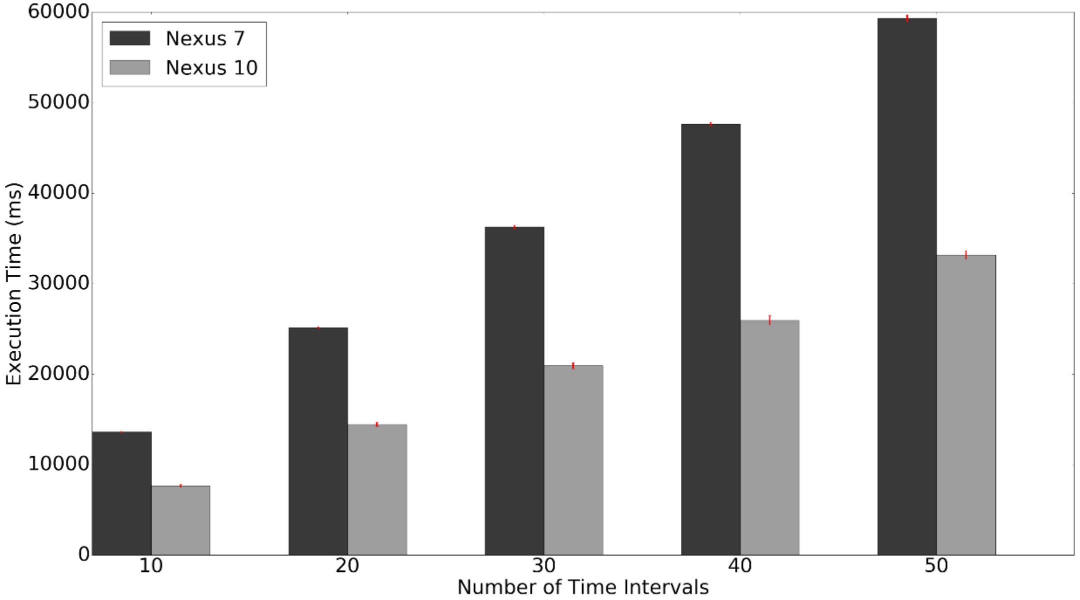
GroupSense Performance - Server



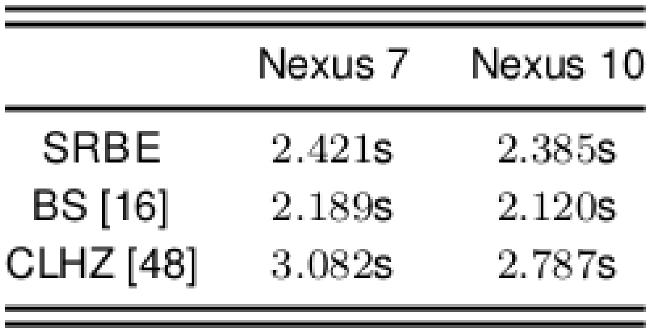


GroupSense performance during data submission

GroupSense Performance - Android



Join Algorithm performance



	Nexus 7	Nexus 10
SRBE	2.421s	2.385s
BS [16]	2.189s	2.120s
CLHZ [48]	3.082s	2.787s

Sign Algorithm performance

Future Work

Privacy preserving authentication (PPA) is only a piece of a bigger puzzle!

Correlation Based Attacks

- Correlation using Meta-Data (e.g., Device Info, IP)
- Correlation using Data itself (e.g., GPS location, Special habits)

There are lots of studies addressing these problem in general.

Unfortunately most of them do not consider data collector's app in phone!
Which is inconsistent with crowdsensing settings. [Christin+' 16]

Unified platform for anonymous-yet-accountable crowdsensing is necessary!

[Key Takeways…]

Sublinear revocation is feasible…

Universal crowdsensing-platform is necessary for:

- Mass adoption
- interdisciplinary collaborations to solve daunting humanity problems…

Questions?

Thanks!