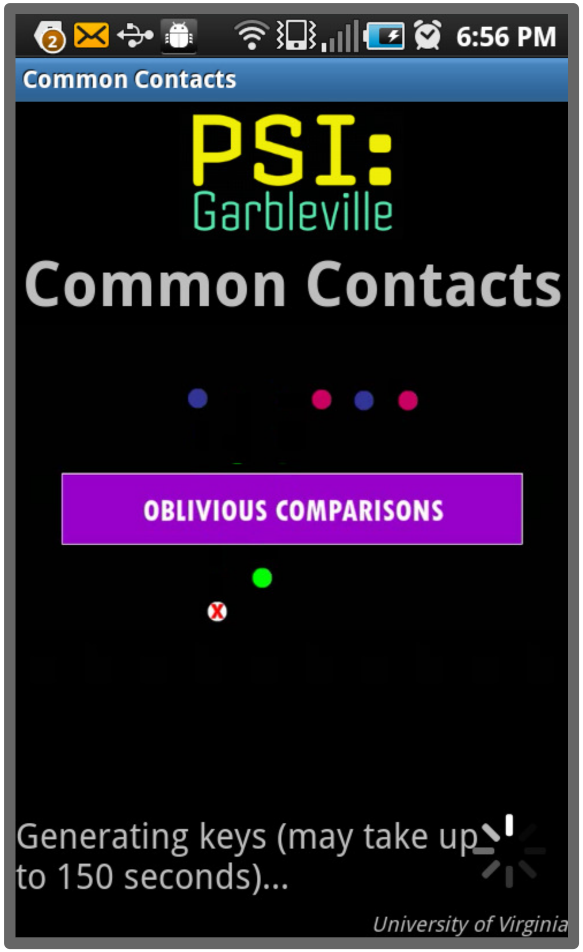
Privacy-Preserving Applications on Smartphones



6:56 PM

Common Contacts

PSI: Garbleville

Common Contacts

OBLIVIOUS COMPARISONS

Generating keys (may take up to 150 seconds)...

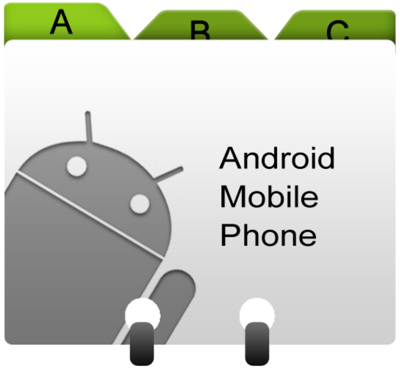
University of Virginia

Yan Huang
Peter Chapman
David Evans
University of Virginia
http://www.MightBeEvil.com

HotSec '11
August 9, 2011

What's on your phone?

Contacts



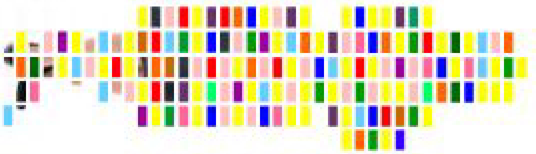
Location History

Pictures

Email

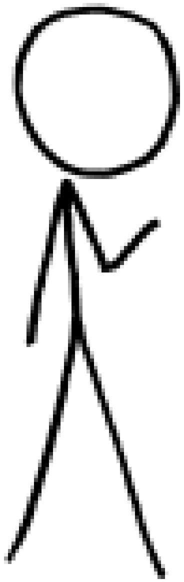
Genome

(maybe next year)

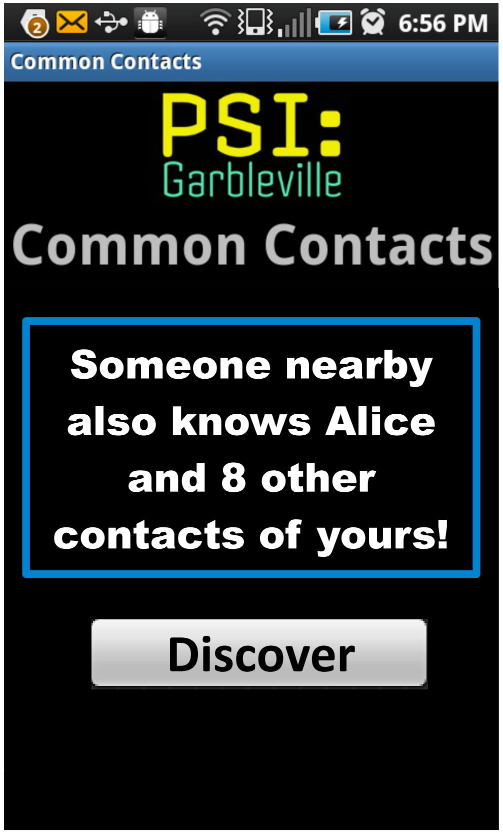


Banking & Payment

Mutual Contact Discovery

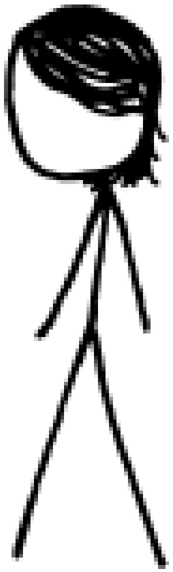


Bob



Common Contacts

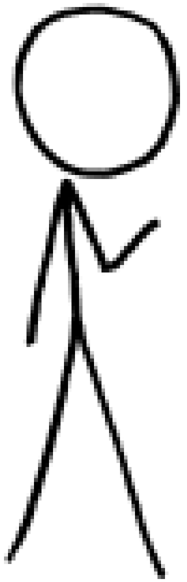
Someone nearby also knows Alice and 8 other contacts of yours!



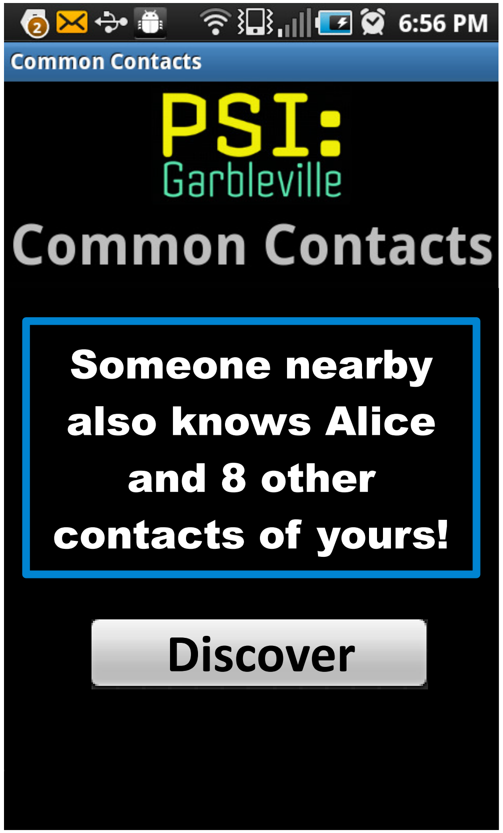
Alice

Transfer entire (hashed) contact list between devices?

Mutual Contact Discovery



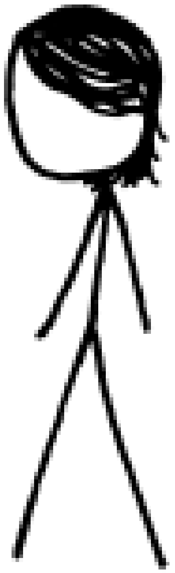
Bob



Common Contacts

Someone nearby also knows Alice and 8 other contacts of yours!

Sharing contact list with a stranger is unacceptable



Alice

The Dilemma

Can we interact with others *and* control our data?

Trust a Third Party?

SEGA

June 2011
1.3 Million

SONY

April 2011
70 Million

citi

June 2011
200,000

epsilon.

April 2011
2,500 Corporate Clients

Dropbox

June 2011
25 Million

Secure Two-Party Computation

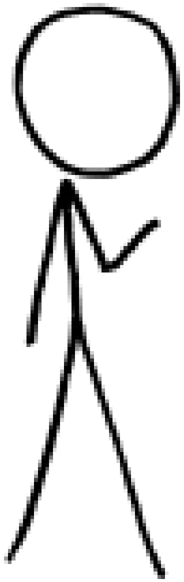
Bob (circuit evaluator)

Private Data: *a*

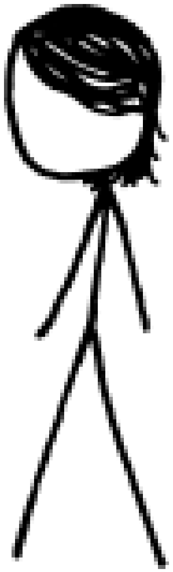
Agree on $f(a,b) \rightarrow x$

Alice (circuit generator)

Private Data: *b*



Garbled Circuit Protocol



Outputs $x = f(a,b)$ without revealing a to Bob or b to Alice.

Semi-honest threat model

Andrew Yao, 1982/1986

Potential Applications

Two Party

Common Contacts

Favorite Workshop Papers

Hyper-Targeted Advertising

Multi-Party

Voting, Auctions & more!

Collaborative Scheduling

Potential Applications

User-Initiated (Explicit)

Voting, Auctions & more!

Favorite Workshop Papers

Collaborative Scheduling

Automatic (Background)

CommonContacts

Hyper-Targeted Advertising

Implementing Privacy-Preserving Applications

Secure-Computation Framework

Java-Based
Garbled Circuit
Framework

Pipelined Circuit Execution
Free XOR
Circuit-Level Optimizations

See our talk in the **Friday, 5 PM Applied Cryptography** USENIX Security technical session:

Faster Secure Two-Party Computation Using Garbled Circuits
Yan Huang, David Evans, Jonathan Katz, & Lior Malka

Available now:
http://mightbeevil.org/framework/

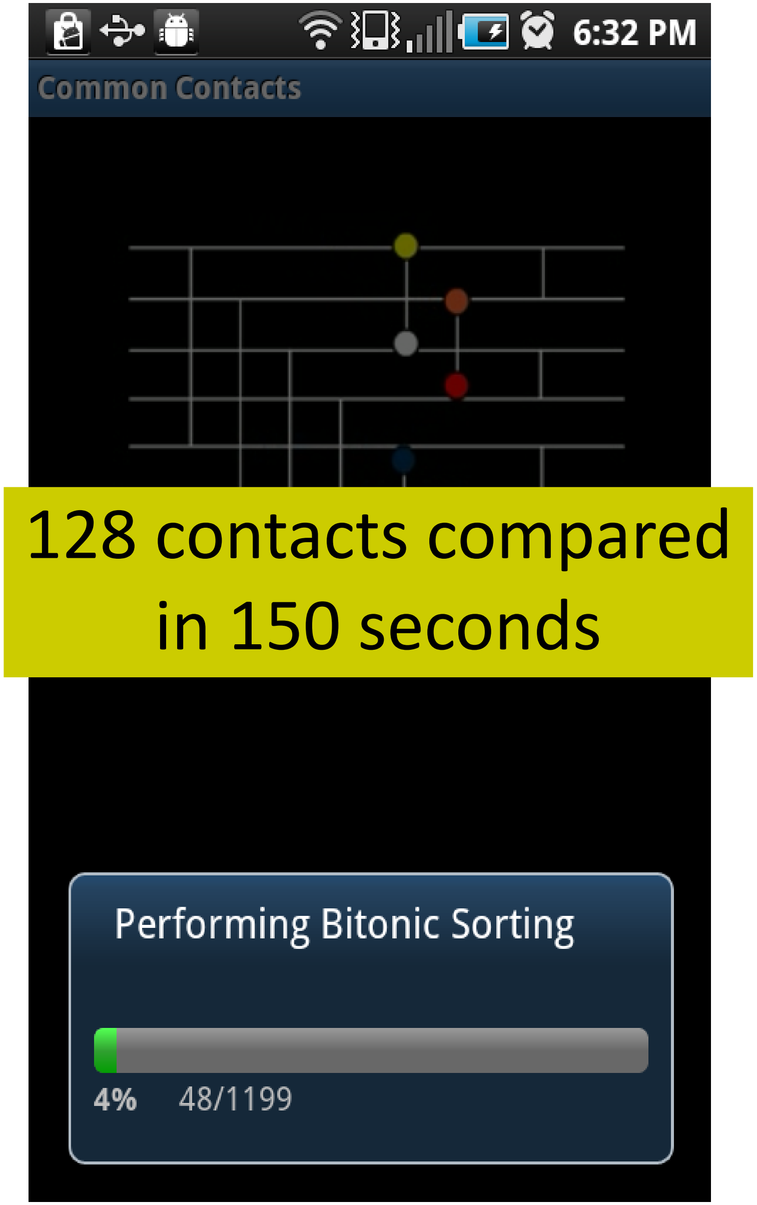
Porting the Framework

100 non-free gates per second:
1000 times slower than desktop!

No cryptographic hardware modules.

We thank Google for the Nexus One phones!

Common Contacts


6:32 PM

Common Contacts

Performing Bitonic Sorting

4% 48/1199

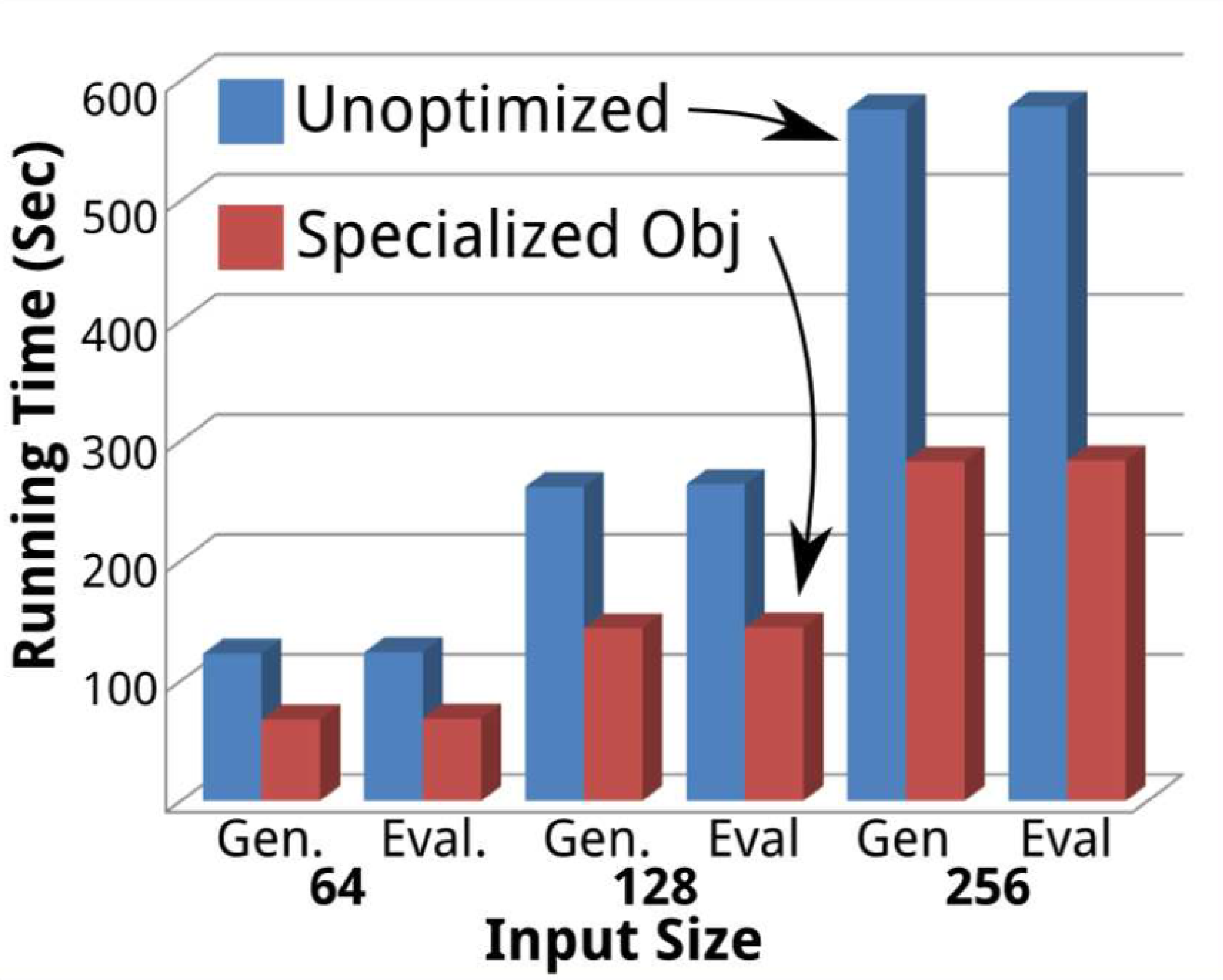
128 contacts compared in 150 seconds

Search for mutually shared contacts, without leaking others.

24-bit Hashes of Email and Phone Numbers

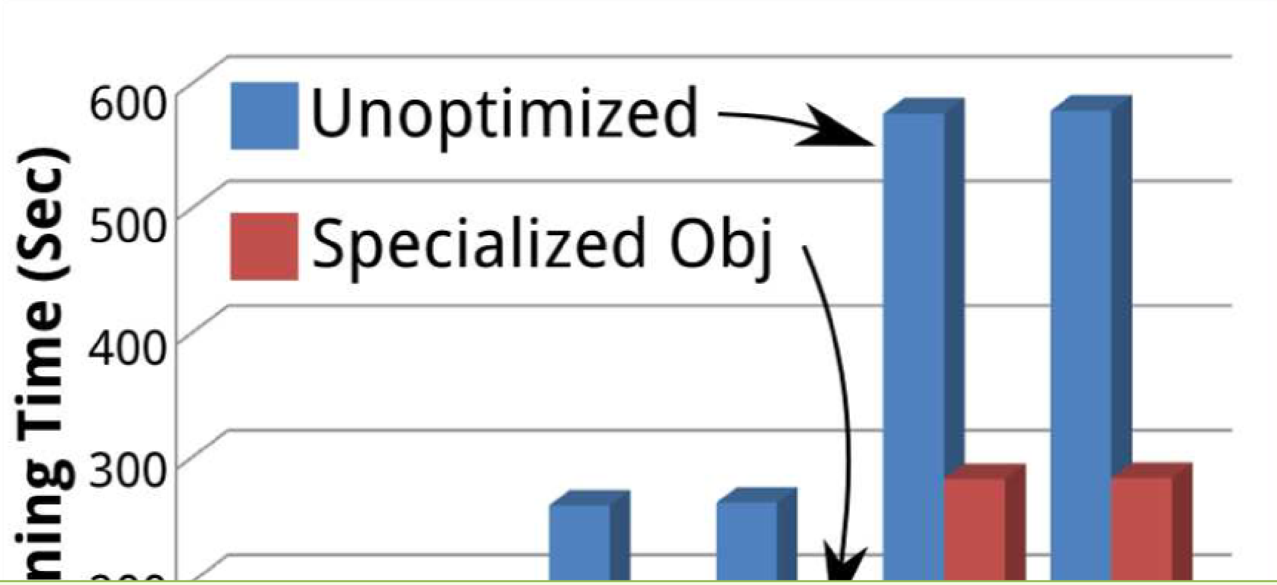
Sort-Compare-Shuffle to do private set intersection in $O(n \log n)$

Improving Mobile Performance



Java's *immutable* BigInteger causes 1/2 of time to be spent on GC

Improving Mobile Performance



Poster and Demo: *More Efficient Secure Computation on Smartphones*

Sang Koo, Yan Huang, Peter Chapman, and David Evans

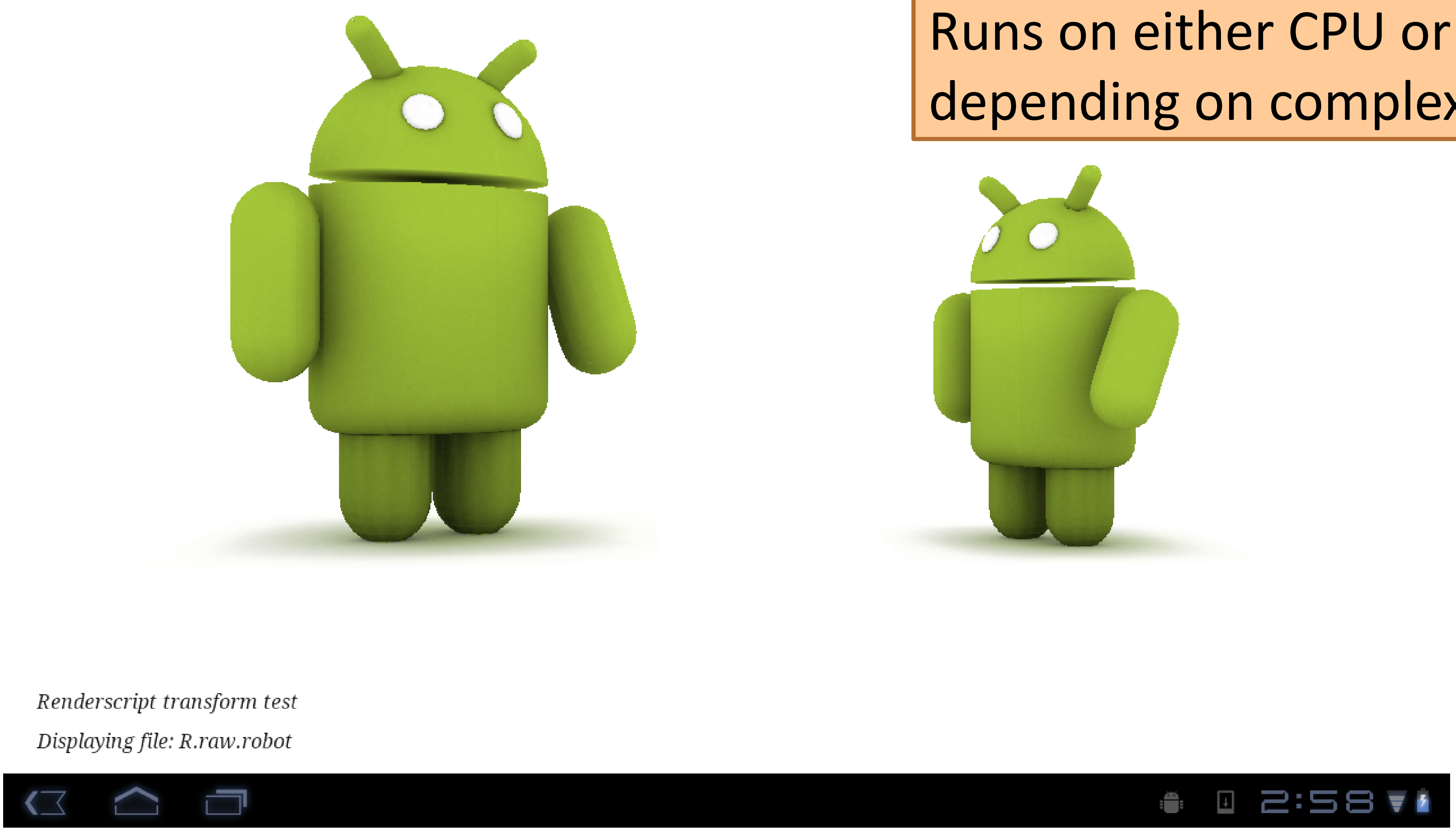
(Thursday, 6PM California East/West)

Java's *immutable* BigInteger causes 1/2 of time to be spent on GC

Future Optimization: RenderScript

C99 with extensions

Runs on either CPU or GPU depending on complexity



Renderscript transform test

Displaying file: R.raw.robot

Future Directions

Stronger Adversaries

Semi-Honest (*Honest But Curious*) **Adversary**

Adversary follows the protocol as specified (**!**)

Curious adversary tries to learn more from protocol execution transcript.

Stronger Adversaries

Semi-Honest (*Honest But Curious*) **Adversary**

Adversary follows the protocol as specified (**!**)

Curious adversary tries to learn more from protocol execution transcript.

Semi-Honest Good Enough?

Stronger Adversaries

Semi-Honest (*Honest But Curious*) **Adversary**

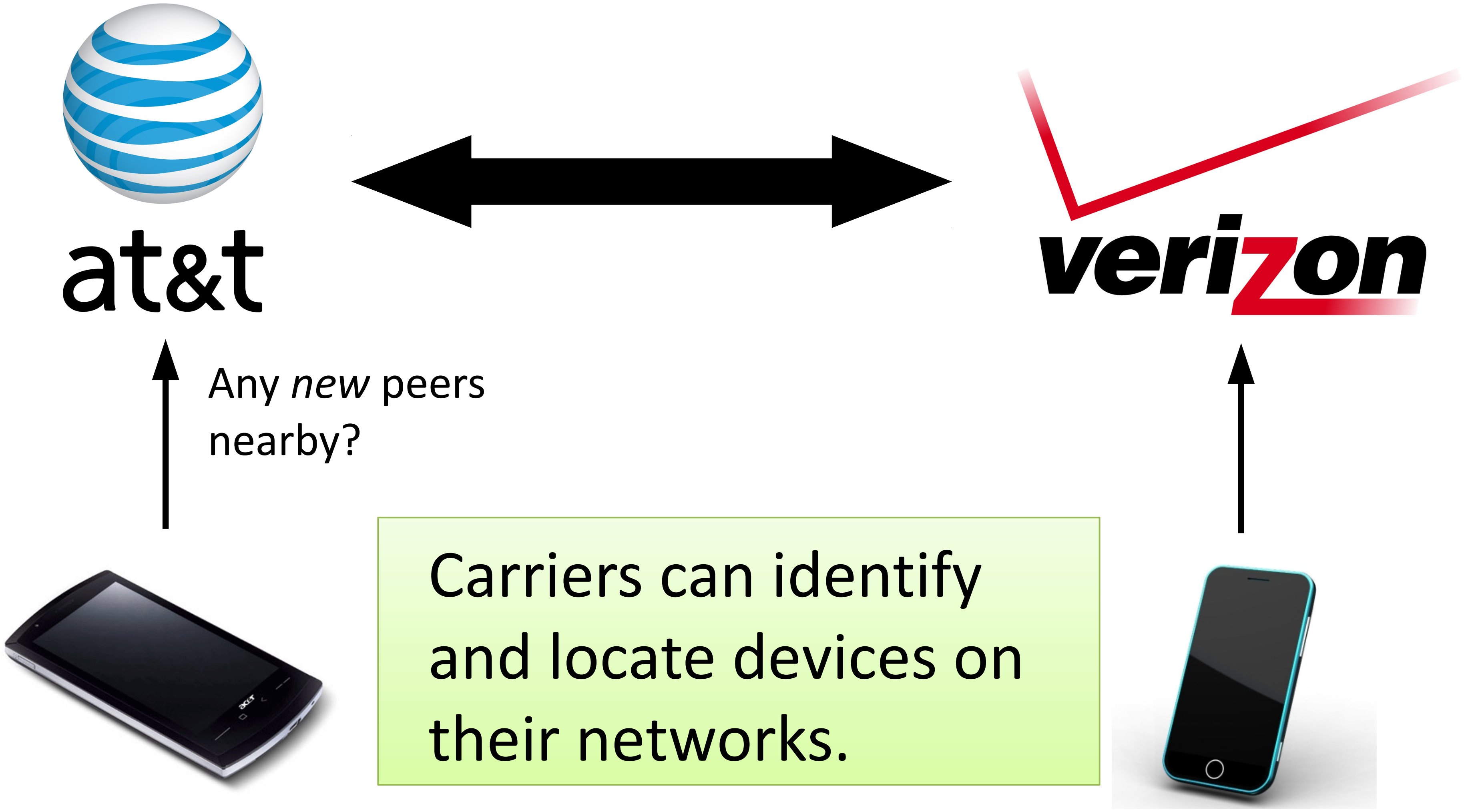
Adversary follows the protocol as specified (**!**)

Curious adversary tries to learn more from protocol execution transcript.

Semi-Honest Good Enough?

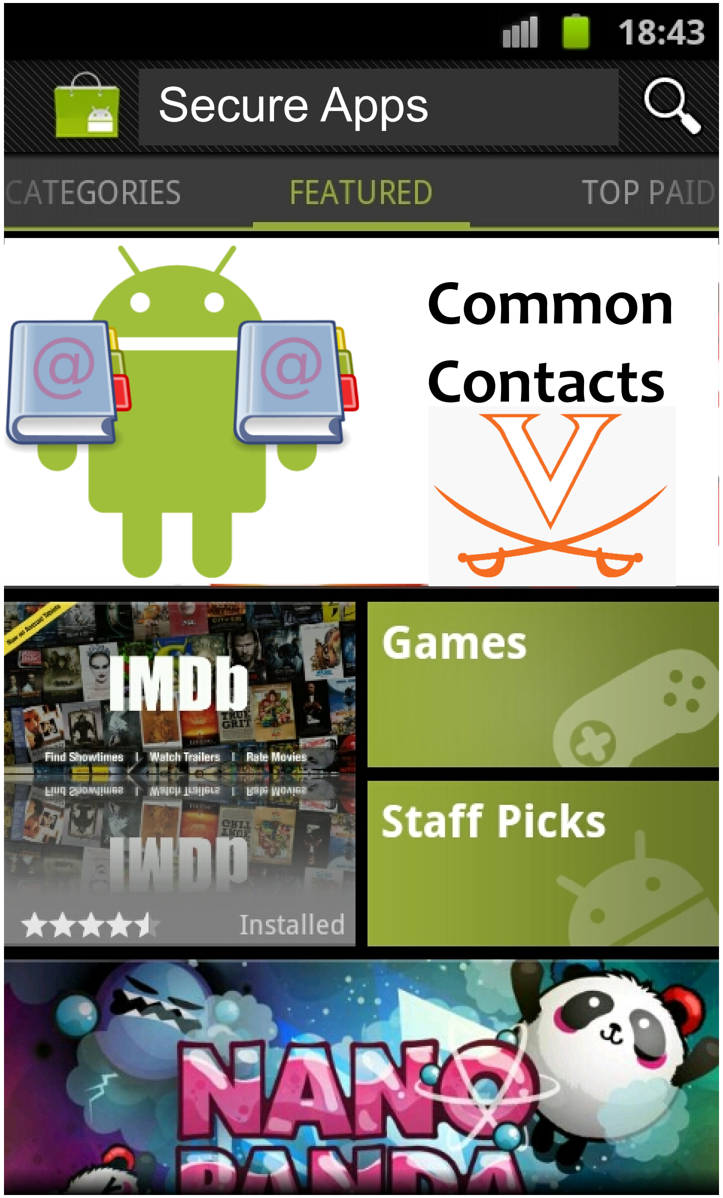
Software Based Attestation?

Leveraging the Carrier



Carriers can identify and locate devices on their networks.

OS Support for Secure Computation

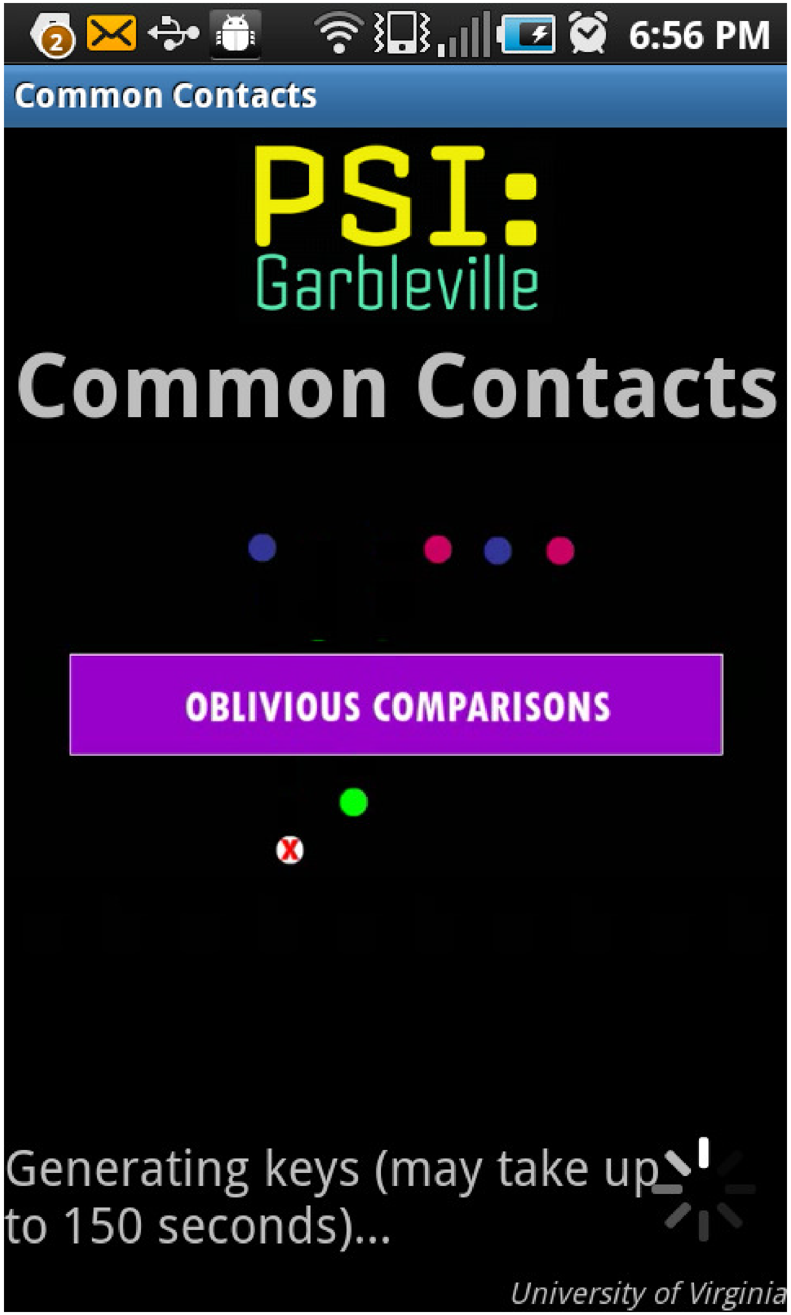


OS/Standardized Displays

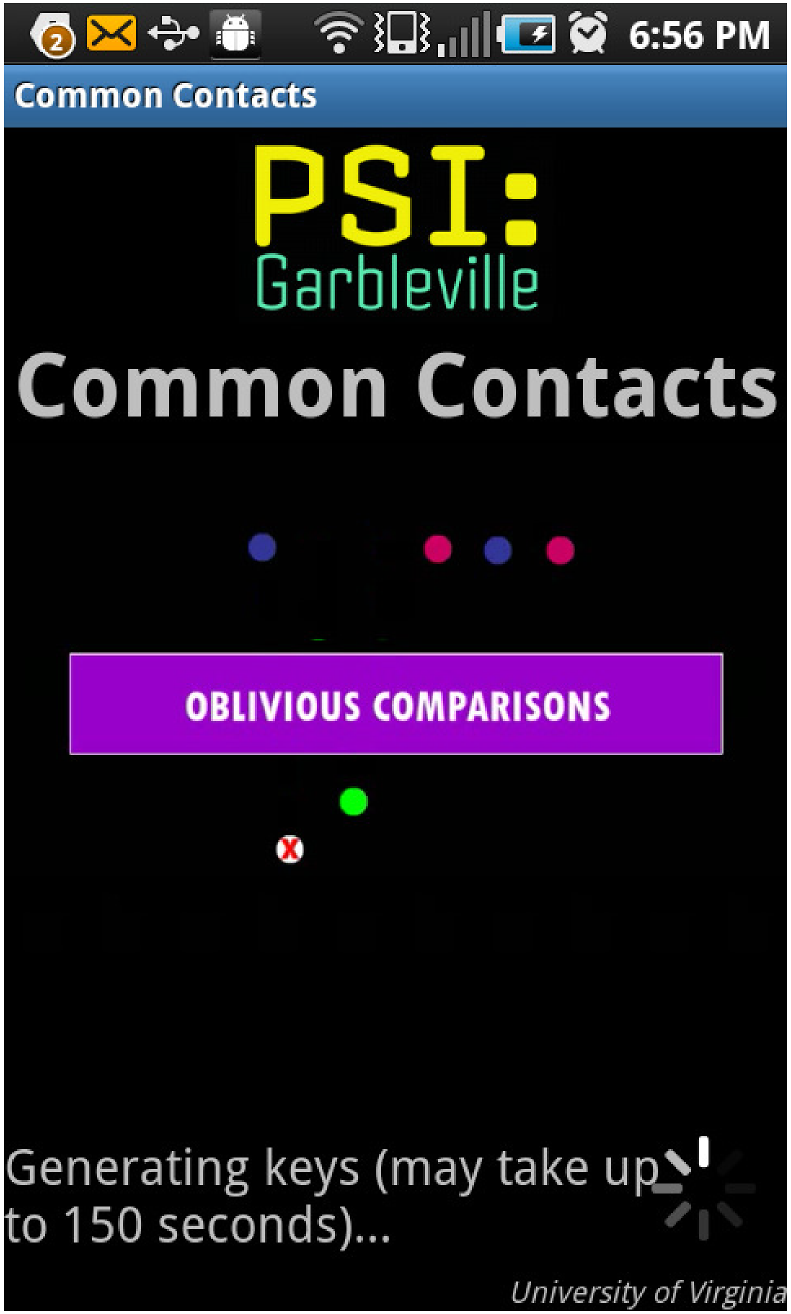
Private data restricted to secure computation by OS

Summary

- Useful applications that are “social” and cryptographically protect privacy.
- Performance challenges, open research questions, and deployment hurdles remain.



Generating keys (may take up to 150 seconds)...



Common Contacts

Common Contacts

Generating keys (may take up to 150 seconds)...

University of Virginia

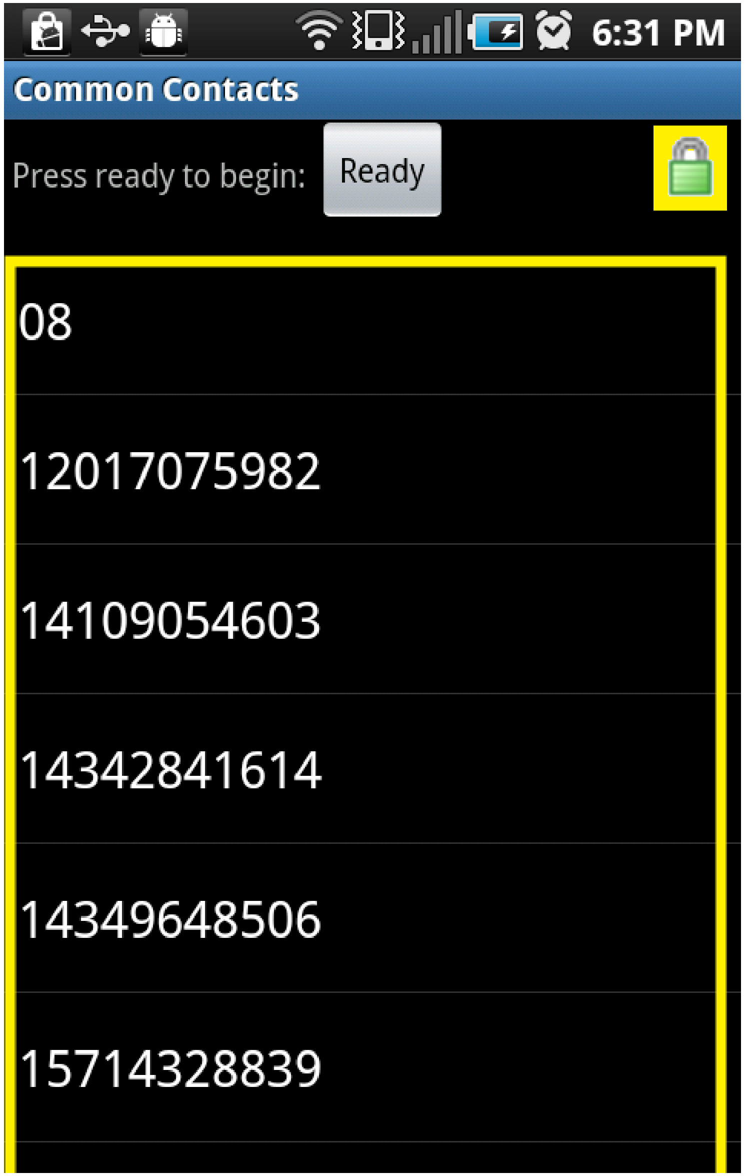
http://MightBeEvil.com/mobile/

User-Friendly Secure Computation

User Education

OS/Standardized Displays

Private data restricted to secure computation by OS



08

12017075982

14109054603

14342841614

14349648506

15714328839

Application Development

Now: Privacy-Preserving computations as a concept must break out of academia

Proper education about data leakage and threat mode

+2 Years: Secure Computation Library Development

Share Sub-circuits & Components

+5 Years: Automatic Source Conversion with Privacy-Preserving Functionality

Heterozygous Recessive Risk

Alice

Bob

	A	a
A	AA	Aa
a	aA	aa

cystic fibrosis

Noncarrier: 25%

Just Carrier: 50%

Disease: 25%

Goal: Compute overall risk across a range of diseases

Background Secure Computations

Do we go to the same bars?

Do we share the same interests?

I just watched all of Arrested Development on Hulu, got any deals?

Must cap repeated executions