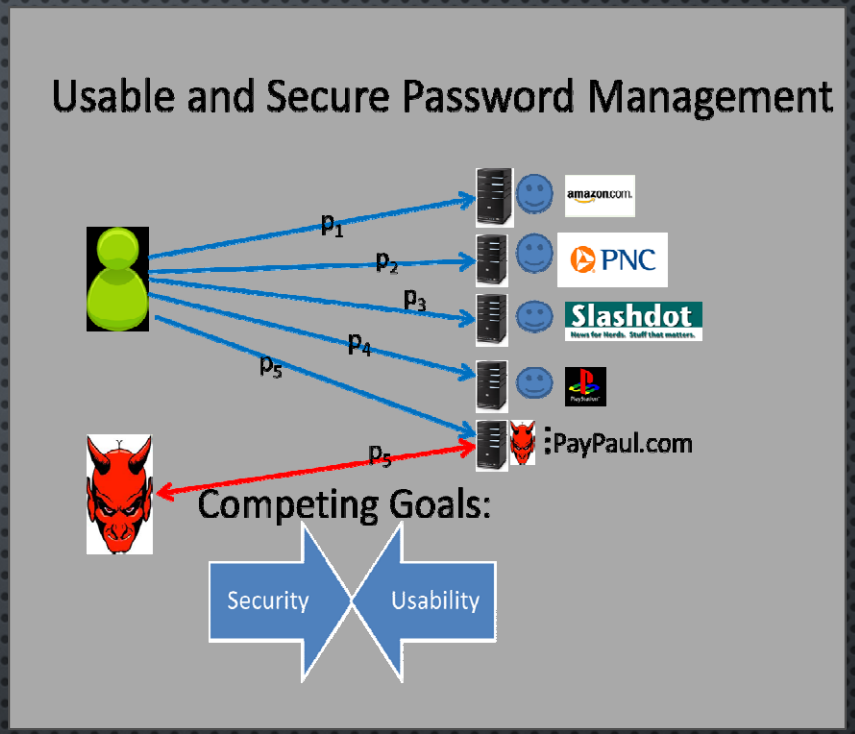
JEREMIAH BLOCKI

ASSISTANT PROFESSOR

JBLOCKI@PURDUE.EDU

Jeremiah Blocki

Assistant Professor
of Computer Science
jblocki@purdue.edu



Research Interests

Information Security, Theory & Algorithms

- Human Authentication
- Cryptography
- Game Theory and Security
- Memory Hard Functions
- Differential Privacy
- Security
- Audit Mechanisms

Application Domains

Privacy Preserving Data Analysis
Human Authentication
Password Hashing

COMPUTER SCIENCE

PURDUE SCIENCE

Jeremiah Blocki

Assistant Professor
of Computer Science
jblocki@purdue.edu

REQUIRES IDEAS FROM:

- COGNITIVE PSYCHOLOGY
- COMBINATORICS
- CRYPTOGRAPHY
- GAME THEORY
- …

RESEARCH GOAL: USABLE AND SECURE STRATEGIES FOR HUMANS TO CREATE AND REMEMBER MULTIPLE PASSWORDS.

http://www.scientificamerican.com/article/memory-trick-increases-password-security/

COMPUTER SCIENCE

PURDUE SCIENCE

Jeremiah Blocki

Assistant Professor
of Computer Science
jblocki@purdue.edu

RESEARCH GOAL: CRYPTOGRAPHIC TOOLS TO PROTECT LOW ENTROPY SECRETS (E.G., PASSWORDS) AGAINST ATTACKERS.

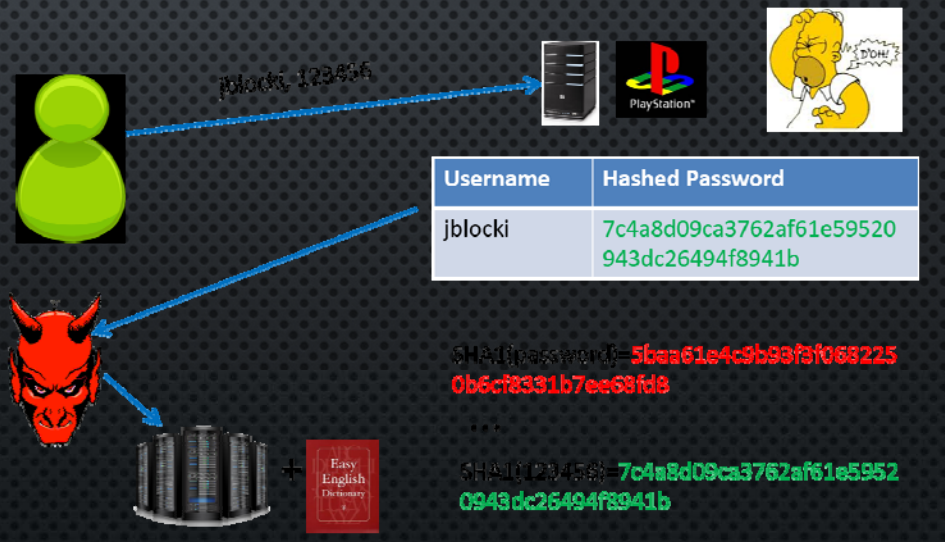
- MEMORY HARD FUNCTIONS
- STACKELBERG GAME THEORY

RESEARCH GOAL: TOOLS FOR PRIVATE DATA ANALYSIS

Differentially Private Analysis of Social Networks

Differentially Private Passwords

Offline Dictionary Attack



Username	Hashed Password
jblocki	7c4a8d09ca3762af61e59520 943dc26494f8941b

COMPUTER SCIENCE

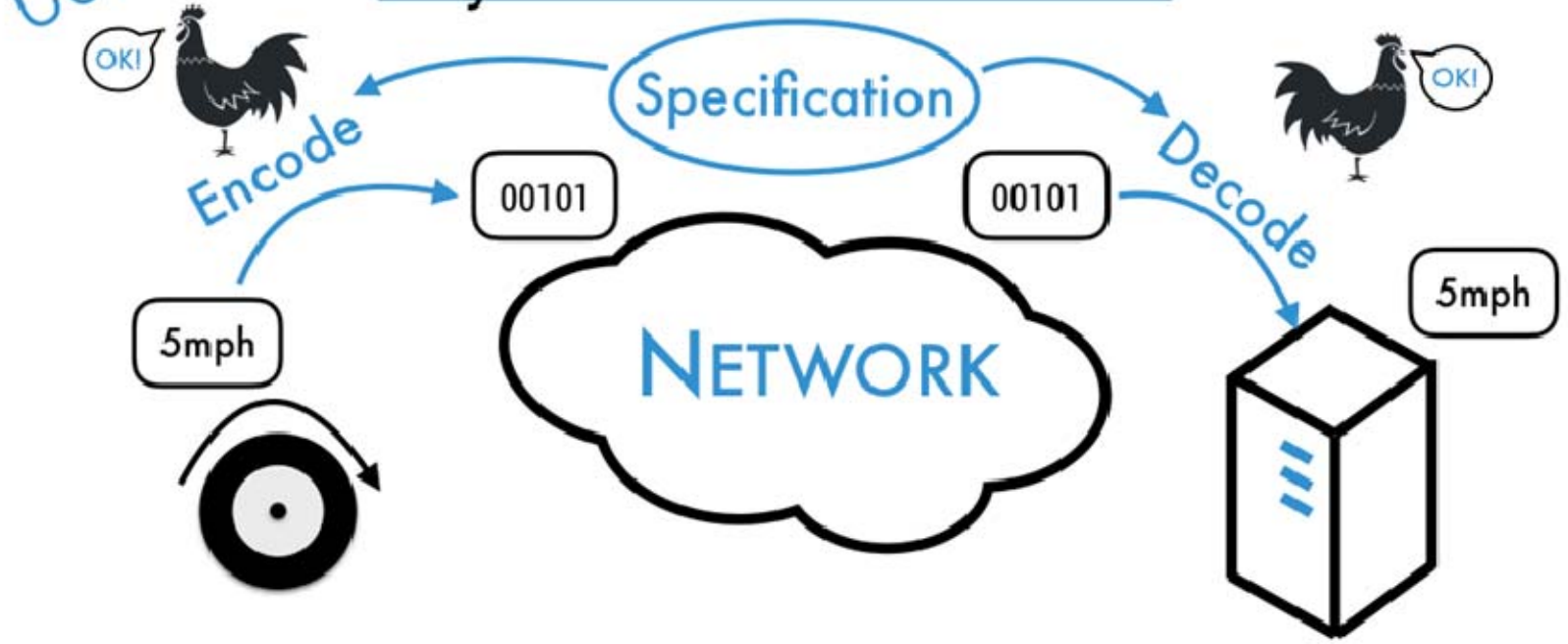
PURDUE SCIENCE

BENJAMIN DELAWARE

ASSISTANT PROFESSOR

BENDY@PURDUE.EDU

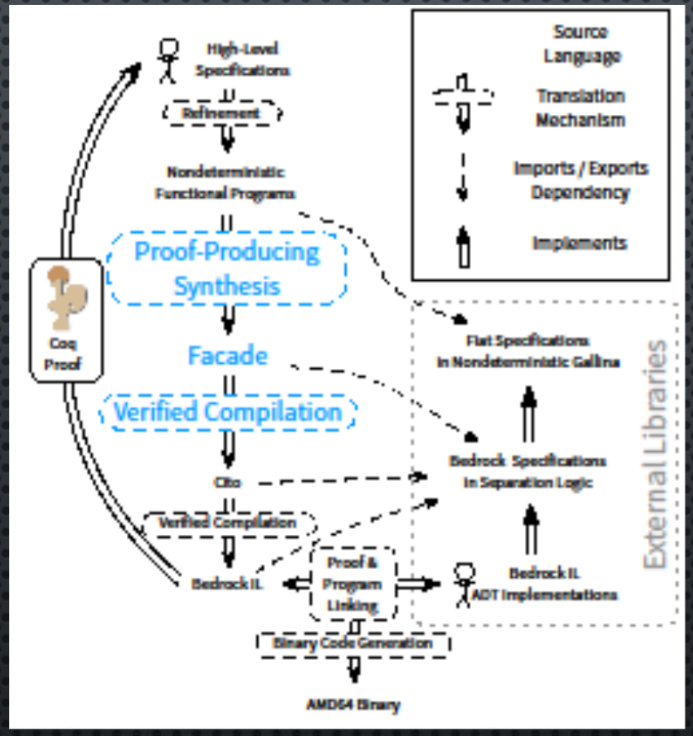
Certified Binary Encoders + Decoders



- Formal Synthesis of binary encoders + decoders from specification
- Machine-checked proof certifying relationship (+memory safety)
- User-extensible with new strategies
  - Provides compatibility with existing protocols + legacy software

applications

- Binary encoder and decoders for robotic sensors
- ROS Master server for autonomous vehicles
- Authoritative and Recursive DNS servers
- Clean-slate development of path tracking software
- Derivation of verified Haskell ByteString library


High-Level Specifications
Refinement
Nondeterministic Functional Programs
Proof-Producing Synthesis
Coq Proof
Facade
Verified Compilation
Cito
Verified Compilation
Bedrock IL
Proof & Program Linking
Binary Code Generation
AMD64 Binary
Source Language
Translation Mechanism
Imports / Exports Dependency
Implements
Flat Specifications in Nondeterministic Gallina
Bedrock Specifications in Separation Logic
Bedrock IL ADT Implementations
External Libraries

Research Interests: Programming Languages and Formal Methods
Sub-box: Program Synthesis and Verification
- Mechanized Reasoning and Decision Procedures
- Programming Language Design
- Static Analysis

Application Areas:
- Mission Critical Software
- Core Internet Infrastructure
- Autonomous Vehicles

PETROS DRINEAS

ASSOCIATE PROFESSOR

PDRINEAS@PURDUE.EDU

Petros Drineas

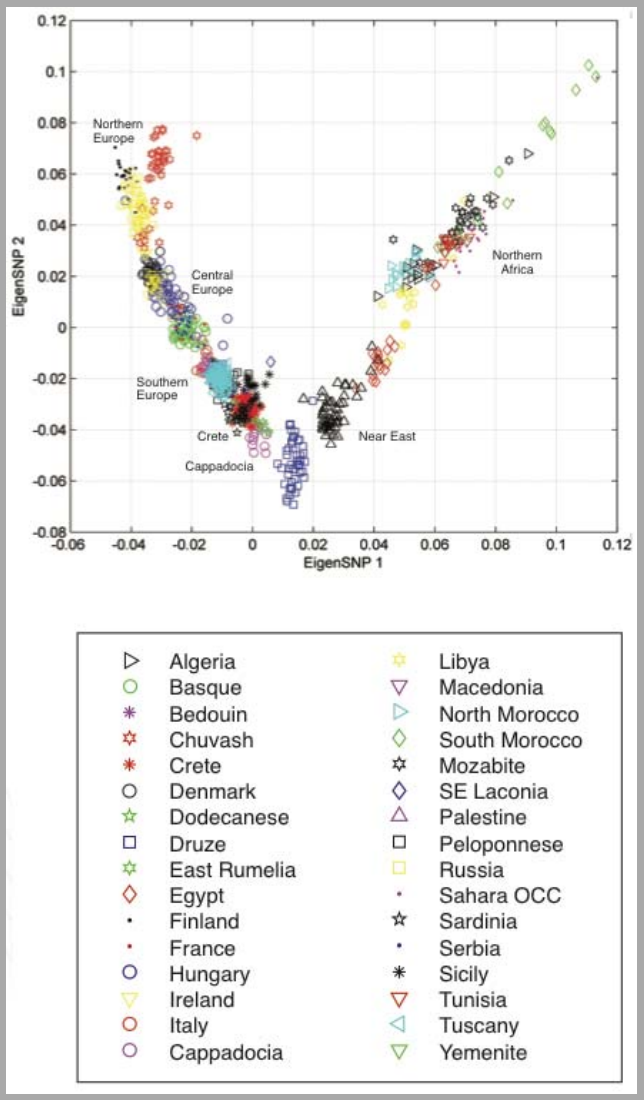
Associate Professor

pdrineas@purdue.edu
http://www.drineas.org/

Research Interests

Theory, Numerical Linear Algebra, Big Data

- Randomized Algorithms for Numerical Linear Algebra (RandNLA) problems
- Applications to machine learning and data mining problems
- Big Data analysis, with a particular emphasis on the analysis of population genetics data



COMPUTER SCIENCE

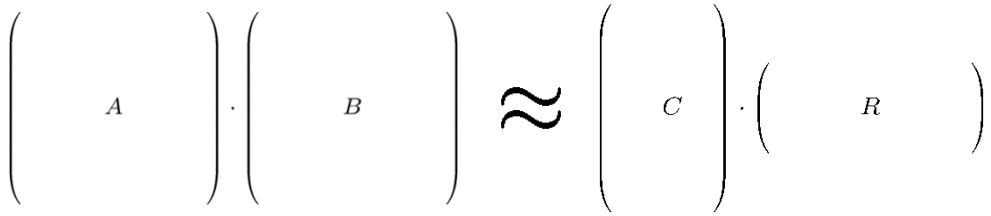
PURDUE SCIENCE

RandNLA: Randomization in Numerical Linear Algebra

Randomized algorithms

• By (carefully) sampling rows/columns of a matrix, we can construct new, smaller matrices that are close to the original matrix (w.r.t. matrix norms) with high probability.

Example: Randomized Matrix Multiplication



• By preprocessing the matrix using "random projection" matrices , we can sample rows/columns much less carefully (uniformly at random) and still get nice bounds with high probability.

Matrix perturbation theory

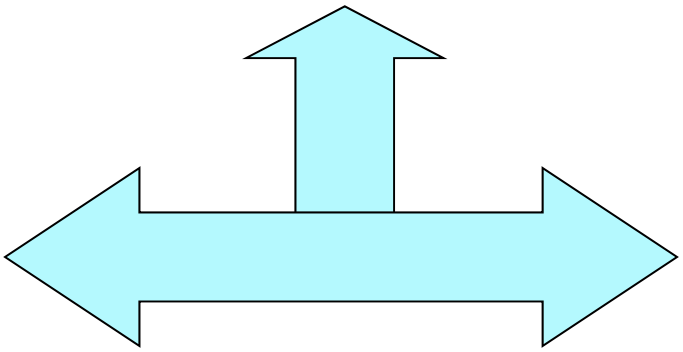
• The resulting smaller matrices behave similarly (e.g., in terms of singular values and singular vectors) to the original matrices thanks to the norm bounds.

Interplay

RandNLA allows us to design provably accurate algorithms for matrix problems that are massive, computationally expensive, or even NP-hard.

Applications in BIG DATA

(Data Mining, Information Retrieval, Machine Learning, Bioinformatics, etc.)



Theoretical Computer Science

Randomized and approximation algorithms

Applied Mathematics

Numerical Linear Algebra, Matrix Computations, Perturbation Theory, and Probability Theory

BYOUNGYOUNG LEE

ASSISTANT PROFESSOR

BYOUNGYOUNG@PURDUE.EDU

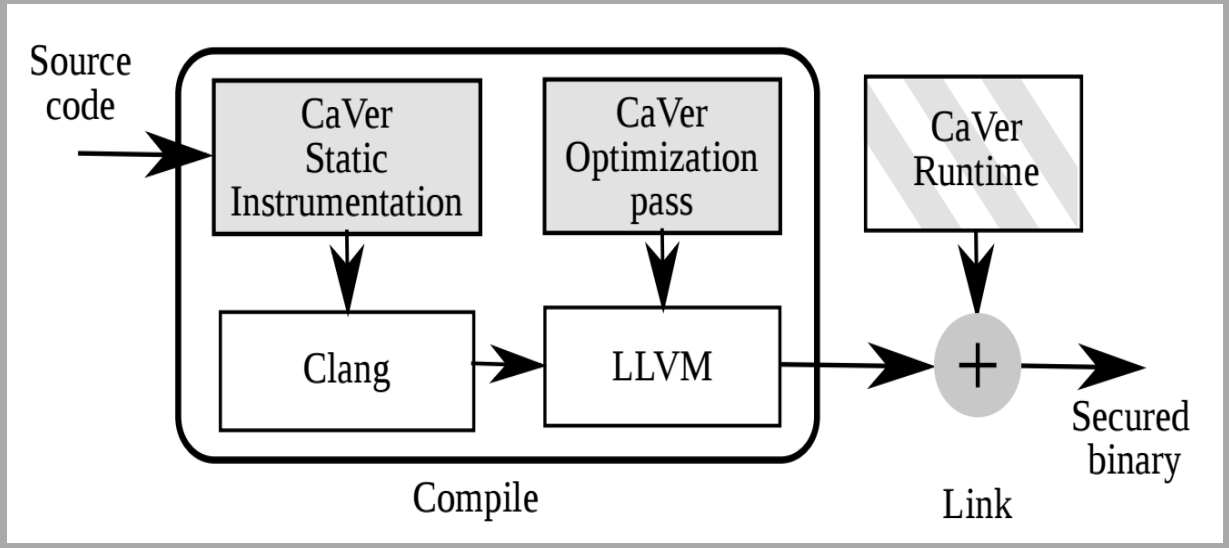
Byoungyoung Lee

Assistant Professor of Computer Science
byoungyoung@purdue.edu

Research Interests

System Security, Software Security

- Vulnerability detection and elimination
- Trusted computing platforms
- Web privacy and security



CaVer - a type casting verification tool

Application Domains

Secure operating systems,
Secure web browsers,
Secure cloud platforms

COMPUTER SCIENCE

PURDUE SCIENCE

Byoungyoung Lee

Research Impacts

- Discovered +100 security vulnerabilities in commodify systems
  - Microsoft Windows Kernel, Linux Kernel, Google Chrome, Firefox, etc.
- Technology transfer
  - Google Chrome team adopted DangNull (use-after-free detection tool)
  - Firefox team adopted CaVer (bad-casting detection tool)
- Awards
  - 2015 Internet Defense Prize by Facebook and USENIX
  - 2015 The Best Applied Security Research Paper (3rd place) by CSAW
  - 2015 DARPA Cyber Grand Challenge (CGC) Finalist

Byoungyoung Lee

Secure Systems for Commodify Software

Apps

DangNull [NDSS 15]
Expector [WWW 15]
TrackMeOrNot [WWW 16]

CaVer [Security 15]

HtLeak [BlackHat 14]

ASLR-Guard [CCS 15]

OS

Juxta [SOSP 15]
Kenali [NDSS 16]
KUP [ATC 16]

Morula [Oakland 14]

Jail-iOS [BlackHat 14]

HW

HDFI [Oakland 16]

COMPUTER SCIENCE

PURDUE SCIENCE

MOHAMMAD SADOGHI

ASSISTANT PROFESSOR

MSADOGHI@PURDUE.EDU

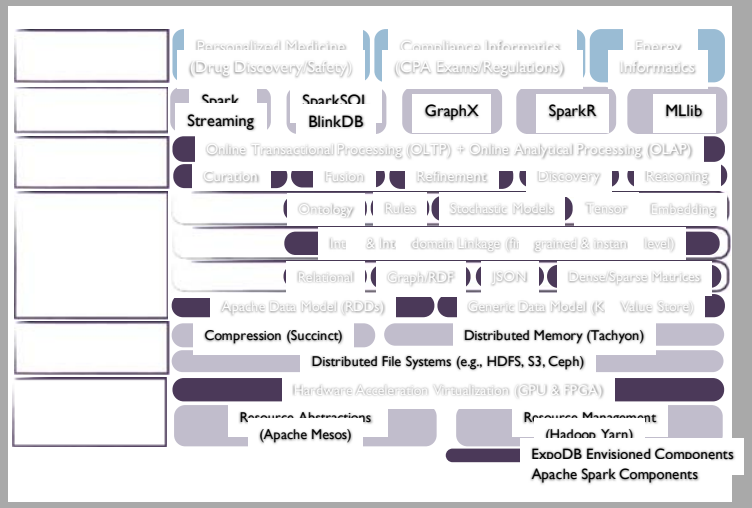
Mohammad Sadoghi

Assistant Professor
of Computer Science
msadoghi@purdue.edu

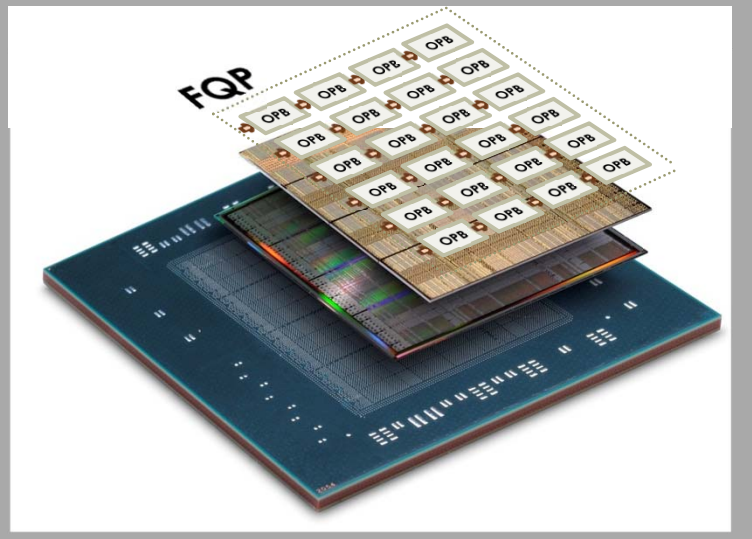
Research Interests

Databases and Machine Learning

- Real-time OLTP & OLAP Systems
- Role of (Virtualized) Modern Hardware (e.g., FPGAs, GPUs, SSDs) in Database Systems on Cloud
- Machine Learning and Data Mining to Semantically Enrich Data
- Data Quality and Enriched Data Curation/Integration
- Uncertainty and Inconsistency in Data Management



ExpoDB: An Exploratory Data Science Platform

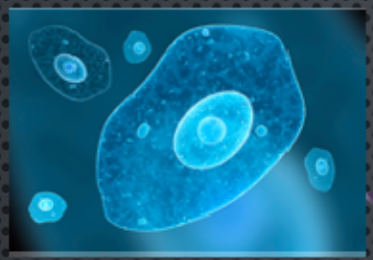


Flexible Query Processing (FQP) on a Reconfigurable Computing Fabric

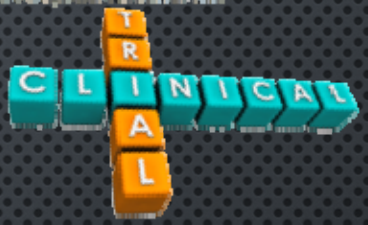
COMPUTER SCIENCE

PURDUE SCIENCE

Insight is Lost in Islands of Data



UniProt



ctd™ *Illuminating how chemicals affect human health.*
Comparative Toxicogenomics Database

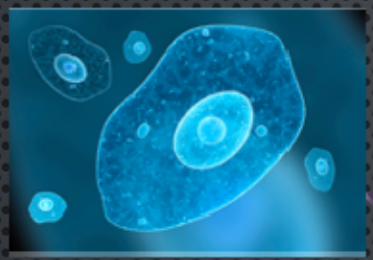
PubMed

BJC British Journal of Cancer

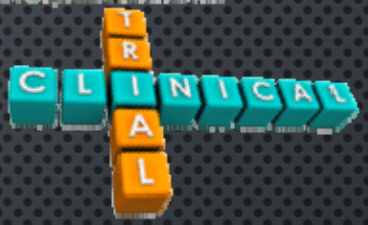
DRUGBANK

Data is spread across many islands of disconnected sources (a lack of holistic view)

Insight is Lost in Islands of Data



UniProt



ctd™ *Illuminating how chemicals affect human health.*
Comparative Toxicogenomics Database

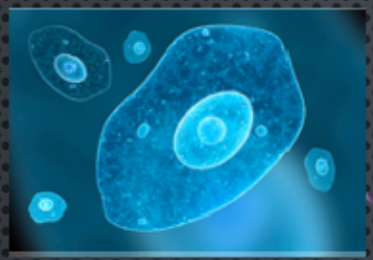
PubMed

BJC British Journal of Cancer

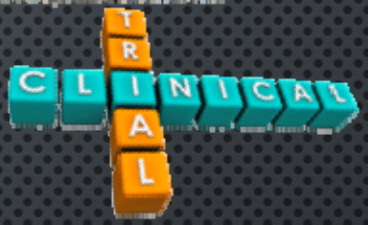
DRUGBANK

Sadly, adverse drug reactions (ADRs) is the 4th leading cause of deaths in United States, resulting in 100,000 loss of life annually

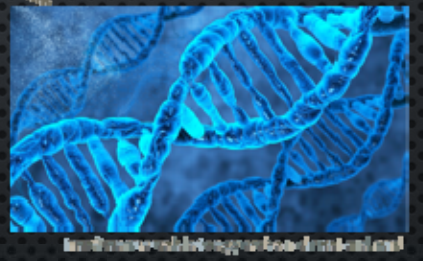
Insight is Lost in Islands of Data



UniProt



ctd™ *Illuminating how chemicals affect human health.*
Comparative Toxicogenomics Database

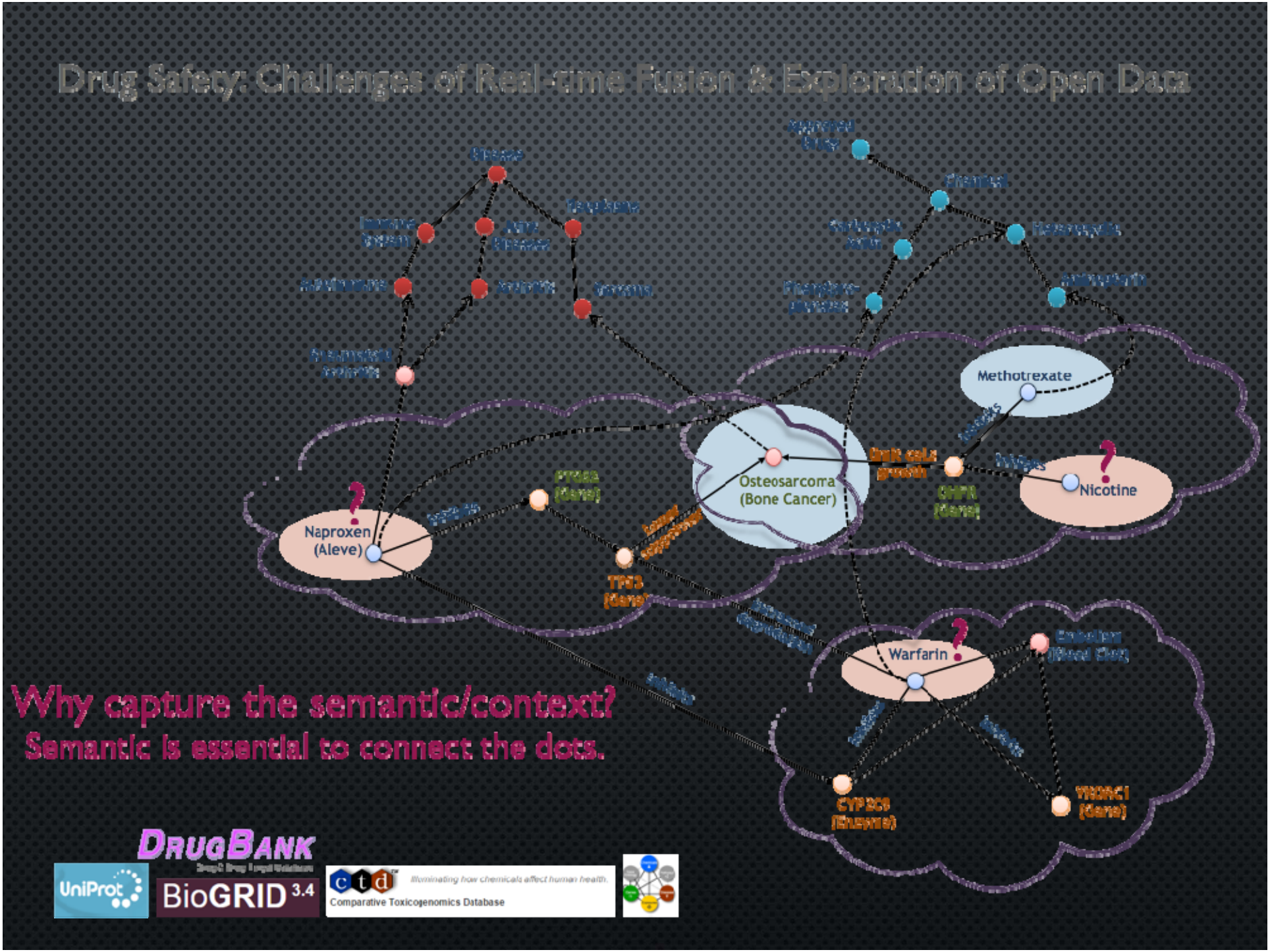


PubMed

BJC British Journal of Cancer

DRUGBANK

Adverse drug reaction costs over $136 billion dollars in US annually


Drug Safety: Challenges of Real-time Fusion & Exploration of Open Data
Methotrexate
Osteosarcoma
(Bone Cancer)
Nicotine
Naproxen
(Aleve)
Warfarin
TP53
(Gene)
CHRFR
(Gene)
CYP2C9
(Enzyme)
VKORC1
(Gene)
Why capture the semantic/context?
Semantic is essential to connect the dots.
DrugBank
UniProt
BioGRID 3.4
ctd
Illuminating how chemicals affect human health.
Comparative Toxicogenomics Database

ROOPSHA SAMANTA

ASSISTANT PROFESSOR

ROOPSHA@PURDUE.EDU

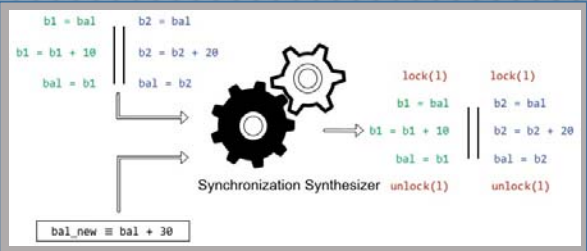
Roopsha Samanta

Assistant Professor
Computer Science
roopsha@purdue.edu

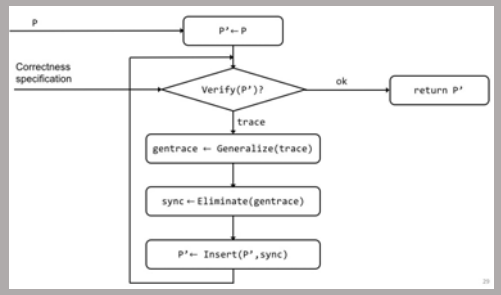
Research Interests

Formal Methods, Programming Languages

- Computer-aided concurrent programming
- Program repair and synthesis for personalized education
- Reasoning about robustness of systems



Trace-based Synchronization Synthesis



Application Domains

Concurrent systems software
Real-time, probabilistic systems
Education

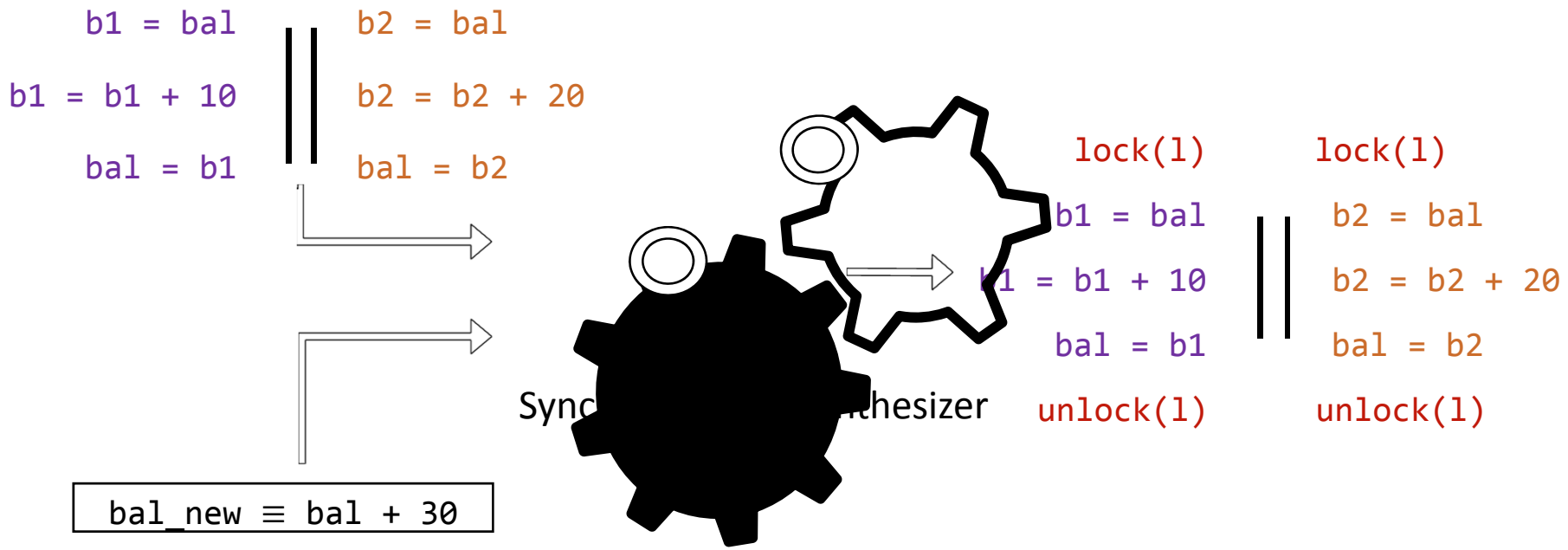
COMPUTER SCIENCE

PURDUE SCIENCE

Simplify Programming Reliable Systems for Experts

- Reduce the cognitive burden of programmers
- Automate tedious and tricky tasks

  Inference of synchronization such as locks in concurrent programs



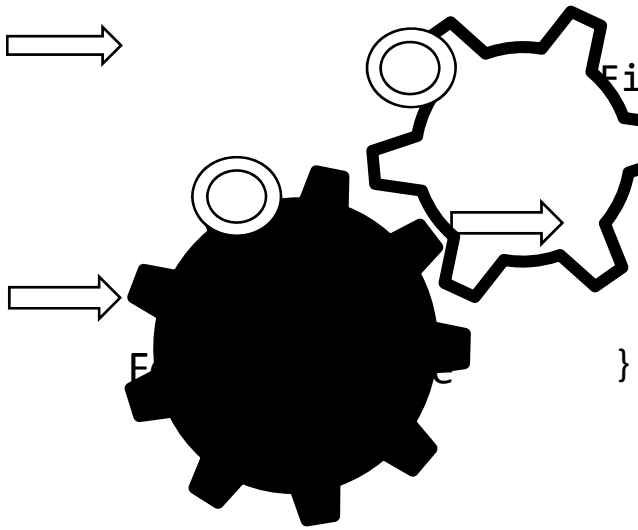
Simplify Programming Reliable Systems for Novices

- Simulate personalized feedback given in traditional classrooms

  Automated feedback engines for programming assignments

```
Find(str s, ch c, int k){
  for(int j=0;j<k;j++)
   if(s[j]==c)
      return true;
   return false;
 }
```

Return true if character c occurs in string s before position k+1



Change to j<=k

```
Find(str s, ch c, int k){
 for(int j=0;j<k;j++)
  if(s[j]==c)
     return true;
 return false;
}
```

HE WANG

ASSISTANT PROFESSOR

HW@PURDUE.EDU

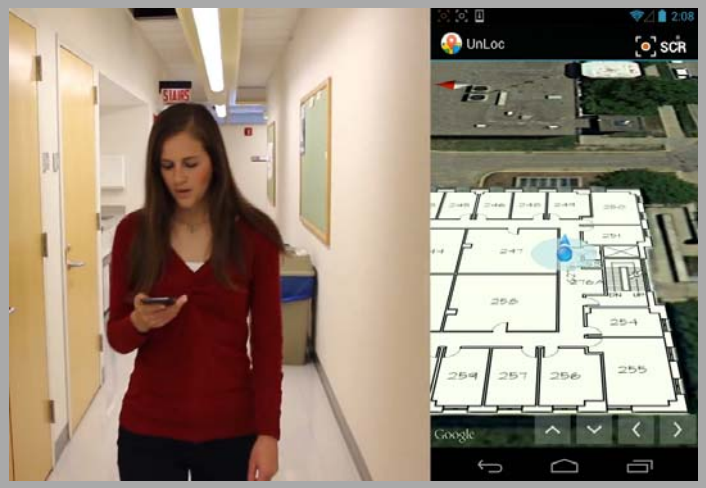
He Wang

Assistant Professor of Computer Science
hw@purdue.edu

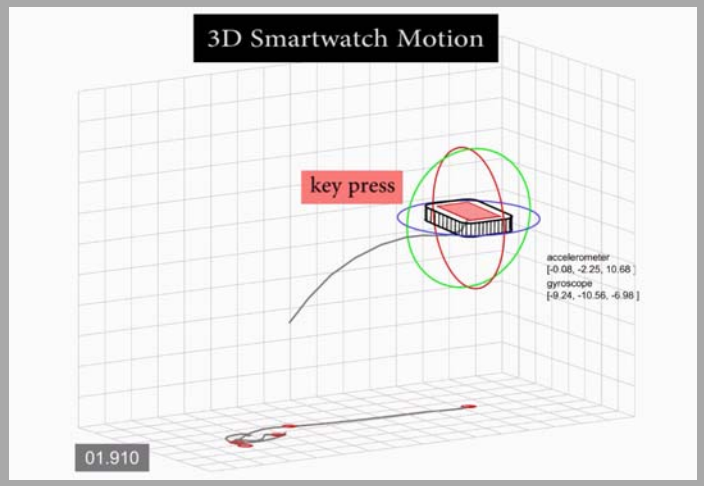
Research Interests

Mobile Sensing and Mobile Computing

- Localization
- Activity/Gesture Recognition
- Wearables
- IoT
- Data Analytics
- Security/Privacy



UnLoc: Unsupervised Indoor Localization



MoLe: Motion Leaks through Smartwatch Sensors

COMPUTER SCIENCE

PURDUE SCIENCE

UnLoc: Unsupervised Indoor Localization

1.63 m accuracy, no infrastructure cost, no calibration needed.

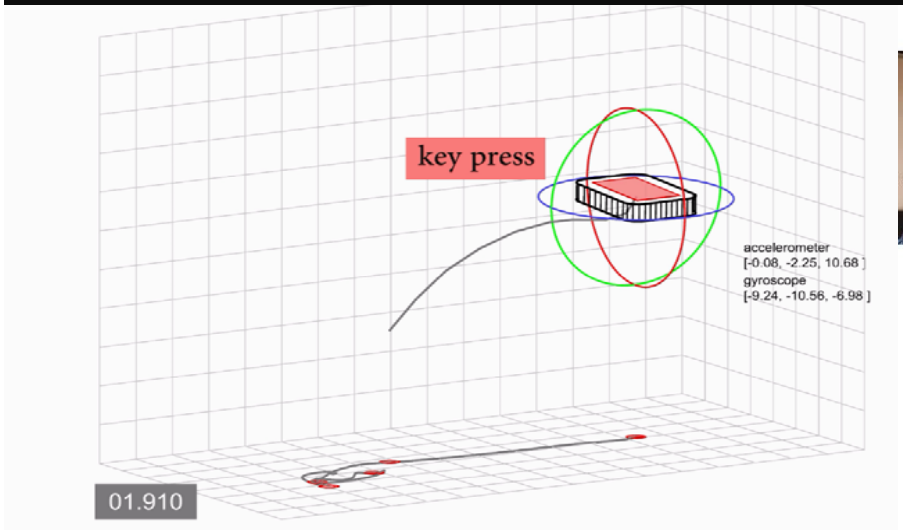
Demo at intel SAMSUNG ...

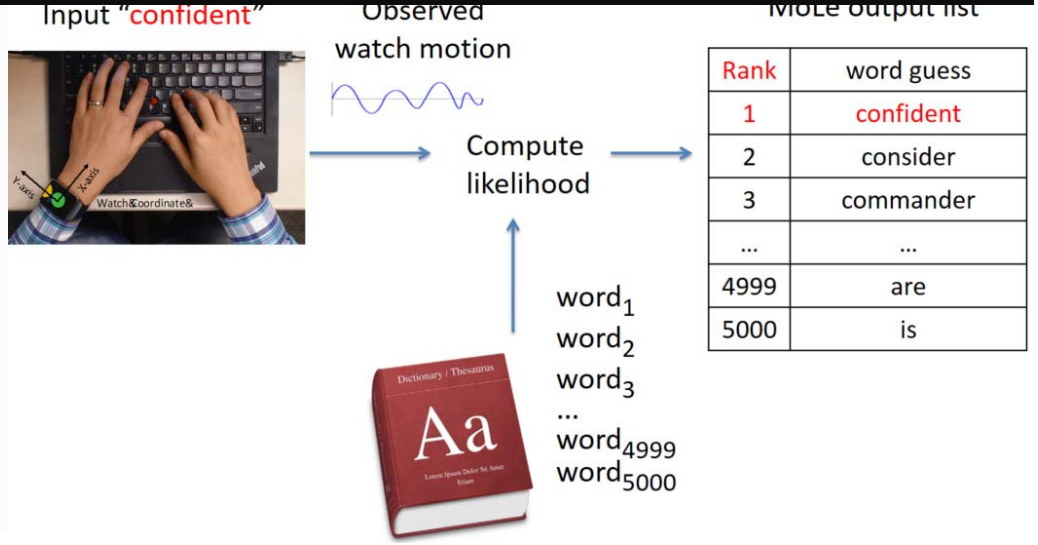
Media SCIENTIFIC AMERICAN™ THE VERGE ...

MoLe: Motion Leaks through Smartwatch Sensors

Can Smartwatch Sensors Infer What You Are Typing?

Type a word W that is longer than 6 characters,
MoLe will shortlist 10 words on average that will include W.





MoLe output list

Rank	word guess
1	confident
2	consider
3	commander
...	...
4999	are
5000	is

Daily Mail · sina · YAHOO! News · THE TIMES OF INDIA · Bangkok Post