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

Usable and Secure Password Management

Competing Goals:
Security  Usability

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

REQUIRES IDEAS FROM:
- COGNITIVE PSYCHOLOGY
- COMBINATORICS
- CRYPTOGRAPHY
- GAME THEORY
- ...

Assistant Professor
of Computer Science
jblocki@purdue.edu

**RESEARCH GOAL:** Tools for private data analysis

- Differentially Private Analysis of Social Networks
- Differentially Private Passwords

**Assistant Professor of Computer Science**

- Jeremiah Blocki
- jblocki@purdue.edu

**Research Goal:** Cryptographic tools to protect low entropy secrets (e.g., passwords) against attackers.

- Memory Hard Functions
- Stackelberg Game Theory

**Offline Dictionary Attack**

<table>
<thead>
<tr>
<th>Username</th>
<th>Hashed Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>jblocki</td>
<td>7c4a8d09ca3762af61e59520943dc26494f8941b</td>
</tr>
</tbody>
</table>

Researchers devise method to safely share password data


Purdue Computer Science
BENJAMIN DELAWARE

ASSISTANT PROFESSOR

BENDY@PURDUE.EDU
Certified

Binary Encoders + Decoders

OK!

Encode

00101

Decode

00101

5mph

Certification

Specification

NETWORK

- **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
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
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.

\[
\begin{bmatrix} A \\ \end{bmatrix} \cdot \begin{bmatrix} B \\ \end{bmatrix} \approx \begin{bmatrix} C \\ \end{bmatrix} \cdot \begin{bmatrix} R \\ \end{bmatrix}
\]

• 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 of Computer Science
byoungyoung@purdue.edu

Research Interests
System Security, Software Security
- Vulnerability detection and elimination
- Trusted computing platforms
- Web privacy and security

Application Domains
- Secure operating systems
- Secure web browsers
- Secure cloud platforms

CaVer - a type casting verification tool
Byoungyoung Lee

Research Impacts

- Discovered +100 security vulnerabilities in commodity 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 DARPA Cyber Grand Challenge (CGC) Finalist
Secure Systems for Commodify Software

Apps
- DangNull [NDSS 15]
- Expector [WWW 15]
- TrackMeOrNot [WWW 16]
- CaVer [Security 15]
- ASLR-Guard [CCS 15]
- HtLeak [BlackHat 14]

OS
- Juxta [SO SP 15]
- Kenali [NDSS 16]
- KUP [ATC 16]
- Morula [Oakland 14]

HW
- Jail-iOS [BlackHat 14]
- HDFI [Oakland 16]
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
Insight is Lost in Islands of Data

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

Adverse drug reaction costs over $136 billion dollars in US annually
Drug Safety: Challenges of Real-time Fusion & Exploration of Open Data

Why capture the semantic/context? Semantic is essential to connect the dots.
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

Application Domains
Concurrent systems software
Real-time, probabilistic systems
Education
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*

\[
\begin{align*}
b_1 &= b_1 \\
b_1 &= b_1 + 10 \\
b_1 &= b_1 + 10
\end{align*}
\]

\[
\begin{align*}
b_2 &= b_2 \\
b_2 &= b_2 + 20 \\
b_2 &= b_2 + 20
\end{align*}
\]

bal = b1

bal = b2

\[
\begin{align*}
\text{lock}(l) \\
\text{unlock}(l)
\end{align*}
\]

bal_new ≡ bal + 30
Simplify Programming Reliable Systems for Novices

- Simulate personalized feedback given in traditional classrooms

*Automated feedback engines for programming assignments*

```c
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

```c
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
UnLoc: Unsupervised Indoor Localization

Indoor environments rich in landmarks

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.