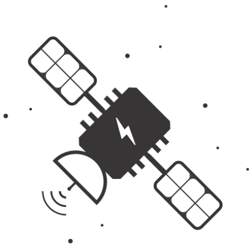
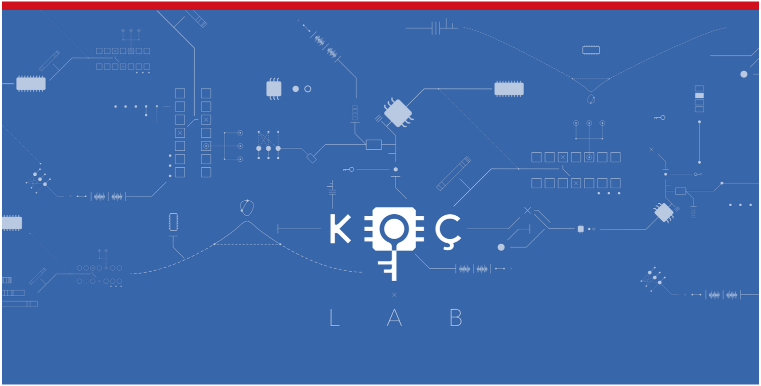
Continuous-Time Aspects of Cyber-Physical Security

Çetin Kaya Koç

University of California Santa Barbara



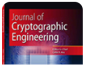
KOÇ LAB



News

Apr 2016 - Kahn Festschrift

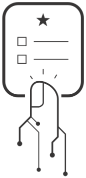
The paper "Bitsliced high-performance AES-ECB on GPUs", authored by Lim, Petzold and Koç, appears in the book *The New Codebreakers* published by Springer. PDF



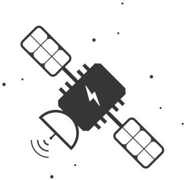
Apr 2016 - Cryptographic Engineering 6/1

The only comprehensive source of high-quality scientific articles on methods, techniques, tools, implementations, and applications of research in cryptographic

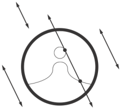
Koç Lab Research Areas



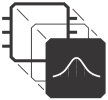
Electronic Voting



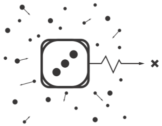
Cyber-Physical Security



Cryptographic Hardware and Embedded Systems



Deterministic, Hybrid and True Random Number Generators



Elliptic Curve Cryptography and Finite Fields

Acknowledgments

This research of
Sam Green, İhsan Çiçek, and Çetin Kaya Koç
is supported by the National Science Foundation.

Ukrainian Power Grid Attacked

- In December 2015, Ukraine experienced widespread power outages.
- The outages have been attributed to a cyber attack.
- This is the first reported cyber attack to a power grid.

There have been many other cyber attacks on the energy sector, industrial control systems, water distribution, medical devices, transportation, and defense systems.

Defining Cyber-Physical Systems

- **Cyber-physical systems** (CPS) are at the intersection of computation, networking, and physical components.
- They control much of the critical infrastructure.
- CPS also perform smaller-scale tasks like home automation, steering in autonomous vehicles, and medical instruments.
- Known, predictable, and secure behavior of CPS is necessary to ensure the safety of the people whom these systems serve.
- However, every computing system is vulnerable to cyber attack.
- Vulnerability is compounded when the physical environment and digital controls are tightly coupled, making reliable operational guarantees difficult outside of nominal conditions.

Outline

- Introduction
- **Cyber-Physical Safety and Security**
- Complicating Factors in CPS Design and Analysis
- Analog Computing for CPS

Why are CPS Difficult to Design and Defend?

- The design of **safe** and **secure** CPS is more difficult than building hack-proof software (which may not be possible itself).
- At the root is a need to understand how physics and logic interact in the system of interest.
- Physical interactions and effects have historically been the domain of physics, mechanical, chemical, industrial, and electrical engineering.
- Logical interactions have historically been analyzed by computer scientists and mathematicians.
- Advances in IC programming abstraction (e.g. PLCs and microcontrollers) significantly lowers the barrier to entry for building advanced CPS.
- "Advanced" CPS implies neither secure nor safe CPS.

Outline

- Introduction
- Cyber-Physical Safety and Security
- **Complicating Factors in CPS Design and Analysis**
- Analog Computing for CPS

CPS are Hybrid Systems

- Understanding the hybrid physical-digital characteristics of CPS is still an immature discipline.
- The physical = analog" = continuous-time aspects of CPS are often most appropriately modeled as systems of differential equations.
- The afety and security analysis of CPS is not “merely” software vulnerability analysis.
- CPS analysis must include both discrete-time and continuous-time perspectives — and often these are coupled.

CPS Design Requires Hybrid Theory

Discrete Theory + Continuous Theory = Hybrid Theory

- "Discrete-Time" here (for simplicity) refers to logic, models, and algorithms suitable for execution on a microprocessor.
- "Continuous-Time" describes state transitions of many physical systems whose current state can be modeled as a (system of) differential equation(s), e.g.

$$\frac{\mathrm{d}\phi_t(x)}{\mathrm{d}t} = f(\phi_t(x)), \quad \phi_t(0) = x_0, \quad (t \in \mathbb{R}).$$

- Hybrid CT/DT theory is unexplored when compared to pure discrete or continuous-time theory.

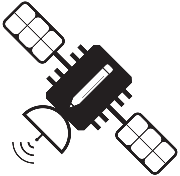
CPS Design and Analysis

The fact that CPS are hybrid discrete-continuous time has interesting implications

- Analysis models, programming languages, and tools must be matured — more critical now, with the advent and low barrier-to-entry enabled by the IoT development infrastructure.
- CPS engineering education must have interdisciplinary components — current computer science, mechanical and chemical engineering curriculum have minimal overlap.
- Fields of importance in CPS design and analysis include: discrete dynamical systems, continuous dynamical systems, state machine theory, scheduling algorithms, temporal logic, various modeling techniques, and data authentication, integrity, and confidentiality.

New National Science Foundation Workshop

Objectives of CPS Ed Workshop



- Encourage development of new books, labs, and curricula.
- Prepare students for careers in CPS practice and research.
- Visit and examine CPS sites that incorporate security countermeasures.
- Expose and encourage future collaboration between the world's researchers and educators.

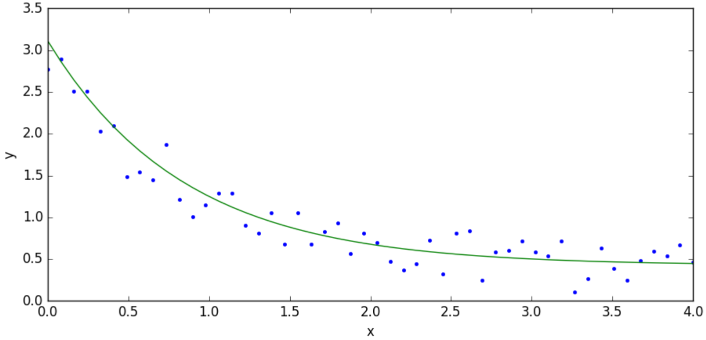
For details, visit `http://CPSed.org`

Outline

- Introduction
- Cyber-Physical Safety and Security
- Complicating Factors in CPS Design and Analysis
- **Analog Computing for CPS**

Implication of Maturing Hybrid Theory

The necessary inclusion of continuous-time analysis in the CPS design process hints towards another opportunity: using analog computing for *faster and more energy efficient* results than digital computing for real-time CPS applications tolerating approximate solutions.



Traditional Analog Computing Applications

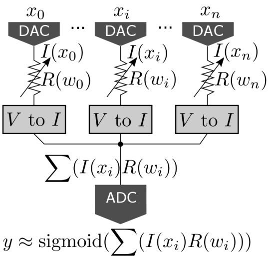
Geology: Hydraulic models, seismology
Economics: Market simulation
Power engineering: Network simulation, power plant development
Electronics: Circuit simulation, filter design, frequency responses
Automation: Data processing, correlation analysis, closed loop control, servo systems, embedded systems
Process control: Mixing tanks, heat exchangers, evaporators, distillation columns
Transport systems: Steering systems, automatic gear boxes, traffic-flow simulation, ship simulation
Aeronautical engineering: Landing gears, jet engines, rotor blades, flight simulation, guidance and control
Rocketry: Rocket motor simulation, craft maneuvers, craft simulation

Modern Analog Computing

Analog computing was never abandoned. Popular applications currently include:

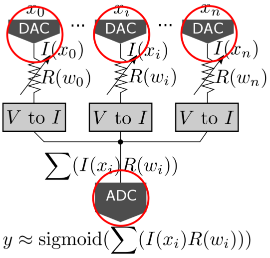
- Mixed-Signal Integrated Circuits: extensively used for signal processing in integrated circuits.
- True Random Number Generators: free-running oscillators, ring oscillators.
- Neuromorphic Computing: emulation of biological computing mechanisms (which are inherently analog).
- Statistical Computing: takes advantage of the strengths, and mitigates the weaknesses, of analog circuits.
- General Purpose Analog Computing: theoretical; explores computing with ordinary differential equations.

General-Purpose Code Acceleration with Limited-Precision Analog Computation (ISCA 2014)



- Obtained 3.7× speedup using 6.3× less power than digital equivalent in the following benchmarks:
  - Financial market modeling
  - Signal processing
  - Robotics
  - Compression
  - Machine learning
  - Image processing

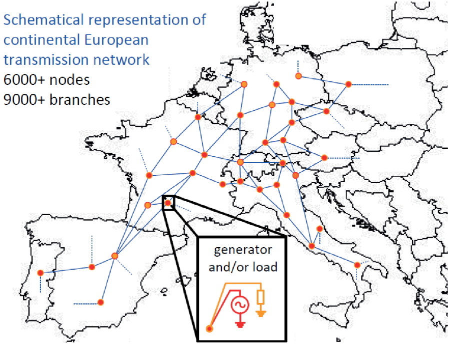
General-Purpose Code Acceleration with Limited-Precision Analog Computation (ISCA 2014)



- Obtained 3.7× speedup using 6.3× less power than digital equivalent in the following benchmarks:
  - Financial market modeling
  - Signal processing
  - Robotics
  - Compression
  - Machine learning
  - Image processing

High Speed Application of Analog Computing to CPS

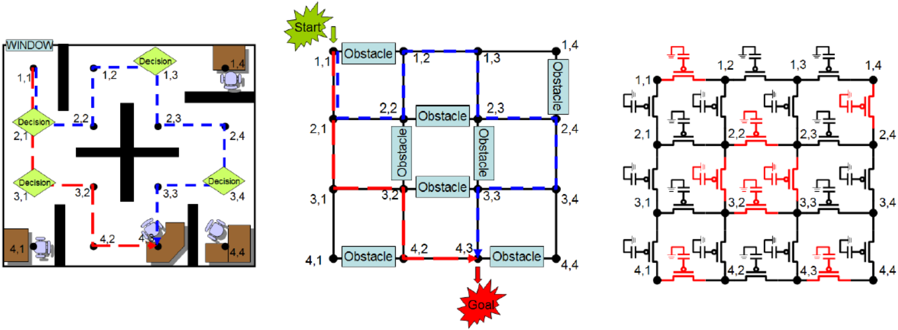
Analog Microelectronic Emulation for Dynamic Power System, 2013 dissertation.



Develops analog computing emulator for power grid with the objective to overcome speed limitations of commonly used numerical simulators.

Low Power Application of Analog Computing to CPS

Reconfigurable Analog Circuits for Autonomous Vehicles, 2013 dissertation.



"Low-power hybrid analog-digital solutions will provide longer operation times and increased computing capability when compared to a resource-constrained all-digital approach."

Using Analog Computing for Anomaly Detection in CPS

Secure Control Systems: A Control-Theoretic Approach to Cyber-Physical Security, 2012 dissertation.

- Creates a CPS security framework, using anomaly detection and estimation to protect against intrusion, deception, and denial of service attacks.
- Works at the physical infrastructure and communication layers.
- Uses both estimation and graph theory to formalize a decoding algorithm to achieve detection of corrupted output measurements.
- Centralized control and distributed computing is used to monitor for attacks.

Analog computing solutions for CPS safety and security algorithms are a good fit — CPS input and output are often already analog.

Many Barriers to Analog Computing

- *Very brittle*: A change in one part of an analog design may require changes to all other parts.
- *Noisy*: Precision limited to $\approx 10^{-4}$.
- *Difficult to build*: Simulation of complex analog circuit is not reliable; must build, test, and tune.
- *Large*: In VLSI, high-performance analog components consume larger area than digital. Analog VLSI technology doubles in components per area every 8 years versus 2 for digital.
- *Drift*: Temperature will cause analog behavior (and therefore mathematical outputs) to change.

Use analog only for what it is very good at.

Conclusions and Future Directions

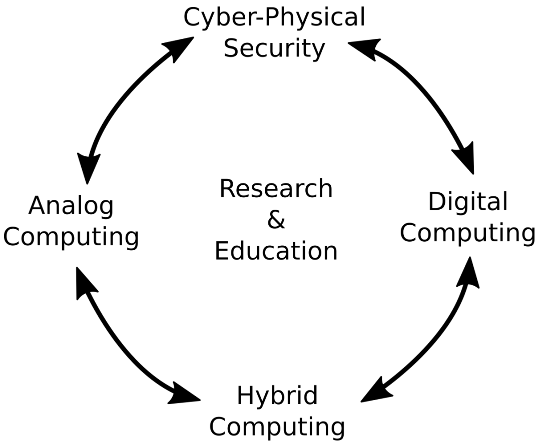
CPS Design and Analysis

- Cyber-physical systems are inherently mixed discrete-continuous.
- Engineering education must be updated to account for the nuances of CPS design. Examples: continuous-time systems $\rightarrow$ computer science, building secure software $\rightarrow$ mechanical engineering.

Analog Computing for CPS

- More work to be done using analog computing for monitoring and assisting in CPS safety and security.
- Excellent for some real-time, low-power problems where approximate answers are suitable.
- To best leverage strengths and weaknesses, practical implementations will most likely be hybrid digital-analog.

Questions?


Cyber-Physical
Security
Analog
Computing
Research
&
Education
Digital
Computing
Hybrid
Computing