A Workshop in Celebration of
Professor Jack Stankovic's 70th birthday
and his Achievements in Cyber-Physical Systems

Quality-Time-Advantage-based Key Establishment Protocols for Securing Wireless CPS

John A. Stankovic –> Wei Zhao –> Yong Guan

Yong Guan
Department of Electrical and Computer Engineering
Iowa State University

Our Research Foci

- Cyber Attacks and Crimes:A painful side-effect of the innovations of Computer, Internet and CPS technologies
  - Almost all physical crimes involve digital evidence, but low percentage of cases reported to law enforcement
- Our Research Foci in Digital Forensics and Security:
  - Accountability & Incident Response
  - Security Monitoring & Impact Analysis
  - Human-centric Security
  - Time-advantage based Security Protocols
- **NIST CoE in Forensic Sciences - CSAFE, 2015-2020.**

NSF

U.S. Army
Research Office

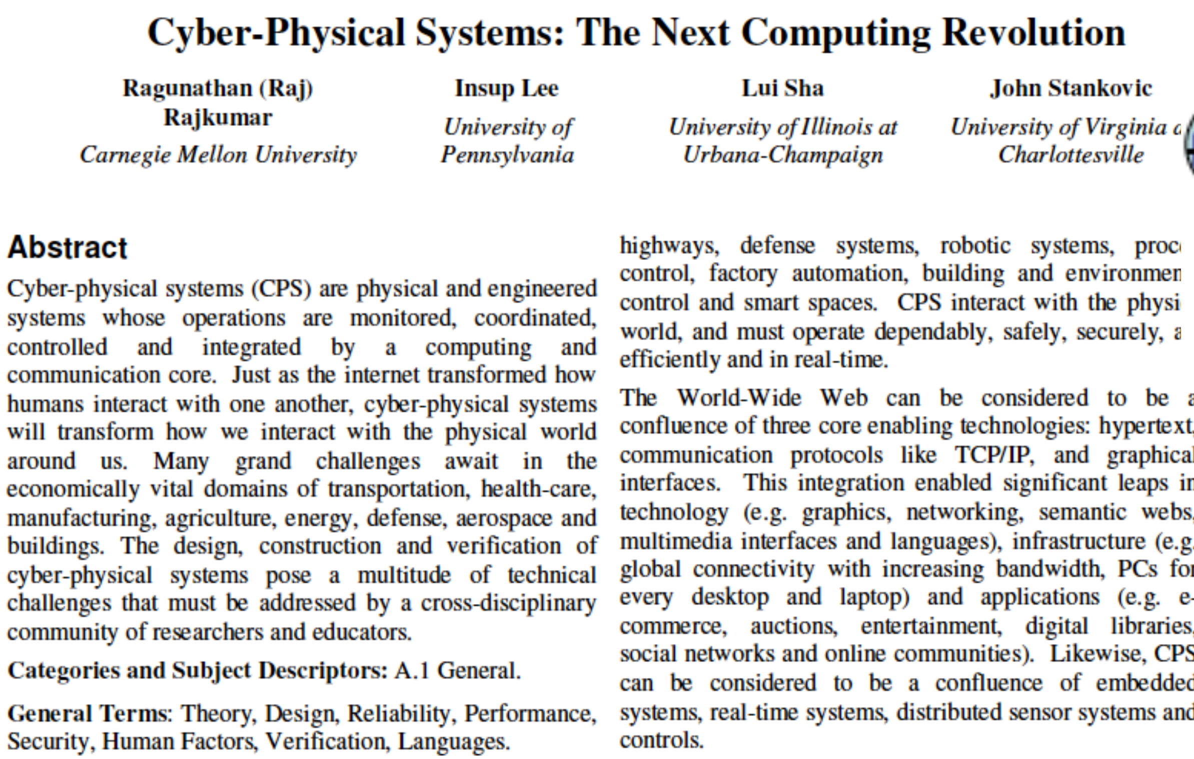
IARPA

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

UNIVERSITY of VIRGINIA

IOWA STATE UNIVERSITY

CPS @ DAC 2010 - **Jack with Raj, Insup, Lui**



Cyber-Physical Systems: The Next Computing Revolution

Ragunathan (Raj) Rajkumar
Carnegie Mellon University

Insup Lee
University of Pennsylvania

Lui Sha
University of Illinois at Urbana-Champaign

John Stankovic
University of Virginia a Charlottesville

Abstract

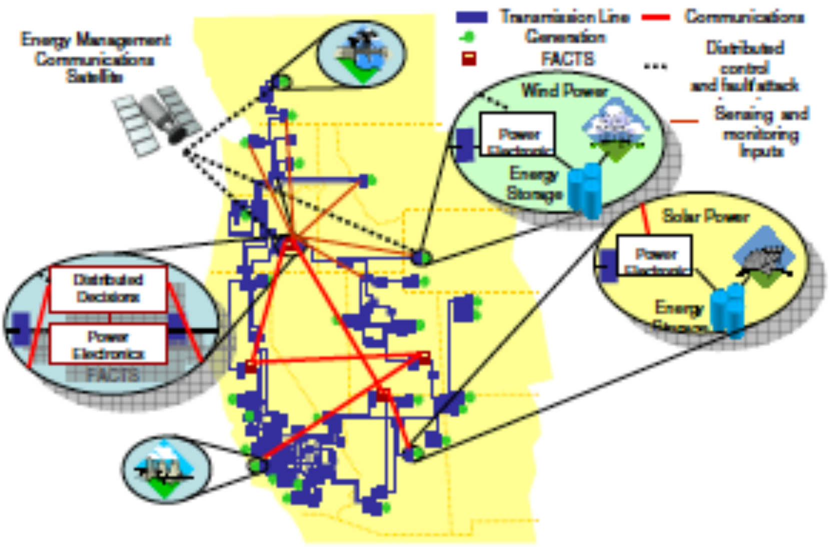
Cyber-physical systems (CPS) are physical and engineered systems whose operations are monitored, coordinated, controlled and integrated by a computing and communication core. Just as the internet transformed how humans interact with one another, cyber-physical systems will transform how we interact with the physical world around us. Many grand challenges await in the economically vital domains of transportation, health-care, manufacturing, agriculture, energy, defense, aerospace and buildings. The design, construction and verification of cyber-physical systems pose a multitude of technical challenges that must be addressed by a cross-disciplinary community of researchers and educators.

Categories and Subject Descriptors: A.1 General.

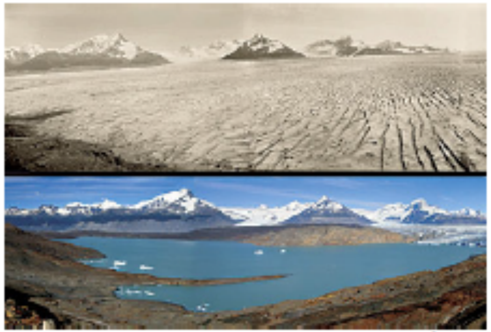
General Terms: Theory, Design, Reliability, Performance, Security, Human Factors, Verification, Languages.

highways, defense systems, robotic systems, proc control, factory automation, building and environmen control and smart spaces. CPS interact with the physi world, and must operate dependably, safely, securely, a efficiently and in real-time.

The World-Wide Web can be considered to be a confluence of three core enabling technologies: hypertext, communication protocols like TCP/IP, and graphical interfaces. This integration enabled significant leaps in technology (e.g. graphics, networking, semantic webs, multimedia interfaces and languages), infrastructure (e.g. global connectivity with increasing bandwidth, PCs for every desktop and laptop) and applications (e.g. e-commerce, auctions, entertainment, digital libraries, social networks and online communities). Likewise, CPS can be considered to be a confluence of embedded systems, real-time systems, distributed sensor systems and controls.



2.2 Symbiotic Cyber-Physical Networks at Scale: New Paradigms for Scientific Discovery



Natural resources in our environment are some of our most fundamental national assets that must be cared for sustained economic prosperity. Urbanization, deforestation, and common agricultural practices (exemplified, for instance, in the Midwestern landscape) severely diminish natural ecological diversity, introducing accumulative side-effects that are not sustainable in the long term. To give one example of unsustainable trends, observations show that global warming has resulted in the

The Problem of Key Establishment

Several procedures for key establishment:

- Public-key infrastructure (using certificates)
- Centralized systems/ key distribution centers (based on symmetric key encryption/ authentication)
- Out-of-band channels
- Superior-quality channels (the "eavesdropper channel"/wiretapping)
- Sources of common randomness (noisy signal from a satellite, network metadata, etc.)

Secure Pairing Using Time Advantage:

From "Adopted Pet (AP)" to Algebraic Protocol (WiSec'18)

- We introduced the AP pairing protocol, suited for supporting zero-configuration systems, in RFIDSec'11.
- AP protocol is automatic, and based on two principles:
  - Legitimate reader has the advantage of time;
  - Cipher weaknesses can be used constructively.

The Adopted Pet protocol was a first step towards a paradigm where authentication and security is based on the legitimate parties mounting successful attacks on each-other's cryptographic protocols, and where the work of anonymous attackers and hackers can serve as the basis for faster authentication and legitimate decryption.

A New Time-based Paradigm for Pairing

The two legitimate parties' advantage over the potential eavesdropper:

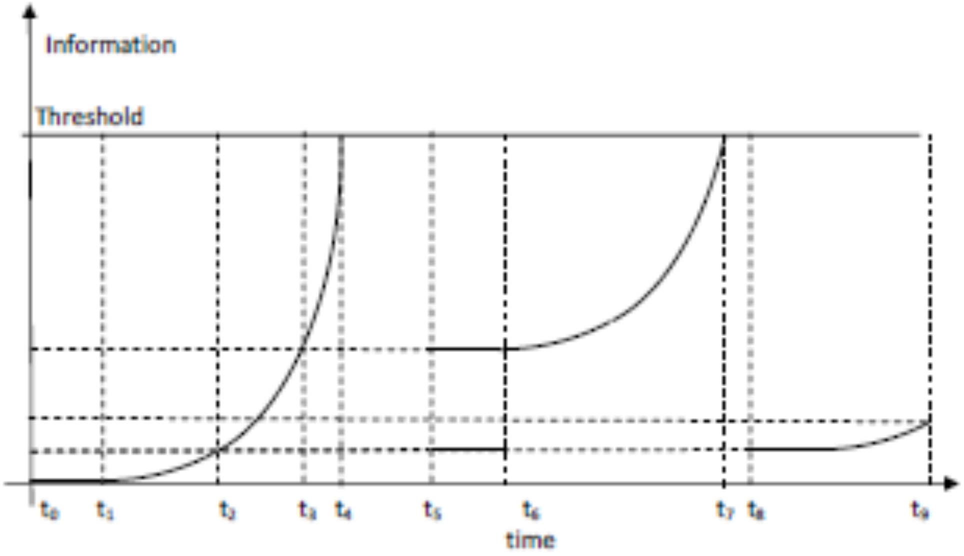
- They can spend long, uninterrupted periods of time ("quality time") with each-other

This type of advantage has some benefits:

1. very natural – this is how animals establish trust;
2. appropriate for certain lightweight applications:
   - RFID readers spend quality time with tags in the home, retailer's and manufacturer's storage, etc.;
   - Military lightweight wireless sensors spend quality time with each other before deployment;
   - Home/body-area-network devices spend most of their lives with each other;
3. requires no infrastructure or key pre-distribution;
4. requires no external source of common randomness.

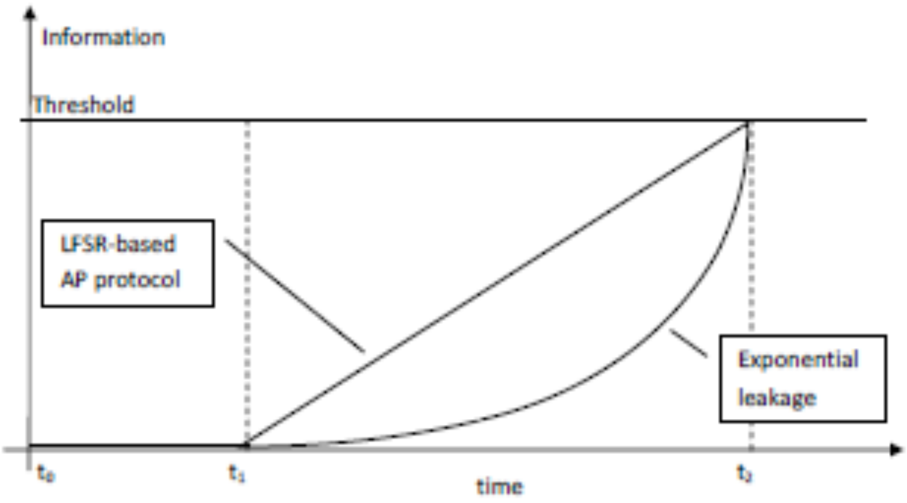
An Ideal Solution - RIFD Tags/Readers

- Tag contains inner secret;
- For every query from untrusted reader, tag responds with *clue*.
- Consecutive clues leak information about tag's secret exponentially over time (but only after time threshold $t1 - t0$).
- If reader and the tag become desynchronized, rate of gathering information returns to its initial value, and starts increasing from there (however, previous information not lost).



A Practical Solution

- Tag contains internal LFSR of length *L* and secret characteristic polynomial.
- A *clue*: LFSR is clocked and transmits one bit.
- After 2*L* consecutive clues, internal LFSR structure is known.
- No information leaks before *L* + 1 clue
- Information leaks at a linear rate (first-order approximation of ideal exponential leakage system).



Implementation Challenges

- Decent performance requires tags to respond to queries at least once per second.
- To learn the secret in not less than 10 hours, we need *L* = 18, 000 (also ensures attacker cannot formulate one equation in less than 5 hours).
- A linear complexity of *L* = 18, 000 is too large to implement as LFSR on passive RFID tag.
- We need other types of finite state machines (FSMs):
  - less memory (registers of cumulative length less than 150);
  - larger linear complexity (around 18,000).
- More complex FSMs become subject to correlation attacks.

Implementation Solutions

- We proposed and analyzed several types of implementations:
  - The bare LFSR (linear complexity too small);
  - Nonlinear Combination Generator (recommended);
  - Nonlinear Filter Generator (recommended);
  - Shrinking Generator (linear complexity too large).

Quality-Time-Advantage: A Revisit (WiSec'18)

How should we implement this?

- We chose to implement it as a puzzle – one of the parties (the challenger/ authenticator) keeps transmitting clues that the other party (the prover/ supplicant) gathers to learn the first party's secret (the puzzle solution).

What do we want from the QTAB-KEP?

1. completely automatic,
2. independent of other security protocols,
3. should rely on a single session and be independent of the protocol's starting time (to prevent DoS),
4. should allow a ***customizable information transfer function*** versus the length of uninterrupted time spent listening to clues (to enable graceful degradation or time-based authorization policies),
5. robust to interference causing a few missed clues, or a few erroneous clues.

QTAB-KEP design

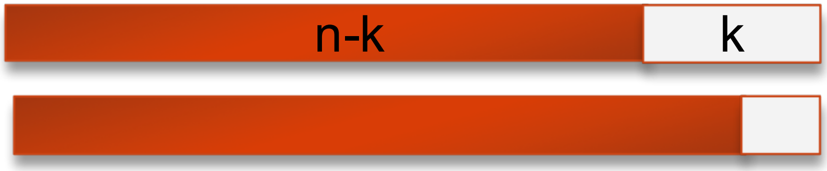
Design implications:

- 1 (completely automatic) and 2 (independent of other protocols) imply that the protocol has to be absolute-time and place independent.
- 3 (single session, independent of starting time) implies an evolving secret.
- 5 (robustness) implies some form of redundancy – error-correction coding. Note: this can also deal with (some) maliciously-injected clues.

Formalizing QTAB-KEP

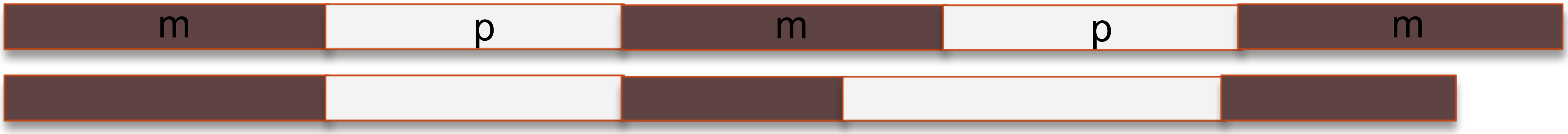
Definition 1 – Robustness

- A QTAB-KEP is said to be (n,k)- robust if a legitimate party who listens to at least n consecutive clues, out of which it can miss at most k clues, can recover the secret key with probability 1.



Definition 2 – Security:

- A QTAB-KEP is called (m,p)-secure if an attacker who can listen to at most m consecutive clues, after which she must miss at least p consecutive clues, has no more information about the secret than she had before listening to the first clue.



Basic QTAB-KEP instantiation

Slightly-modified Shamir's secret sharing scheme:

- Take a finite field F = Z/pZ, with large prime p.
- Publish n fixed points $(a_1, a_2 \ldots a_n) \in$ F.
- Choose n − k − 1 random shares $c_{i-n+1,i} = f_{1,i}$, $c_{i-n+2,i} = f_{2,1}$,..., $c_{i-k-1,i}=f_{n-k-1,i}$ from F.
- Set $a_0=0$ and $f_{0,i}=s_i$, and now, with access to n − k fixed points, we compute the unique polynomial

  $f_i(z)$ of degree n − k − 1, that goes through all these points, i.e. $f_i(a_j)=f_{j,i}$ for j=0,1,2,...,n−k−1.This is done using Lagrange interpolation.

- The remaining k+1 shares are produced as follows: $c_{i-k+1,i} = f_i(a_{n-k})$,..., $c_{i,i} = f_i(a_n)$

Basic QTAB-KEP instantiation with error correction

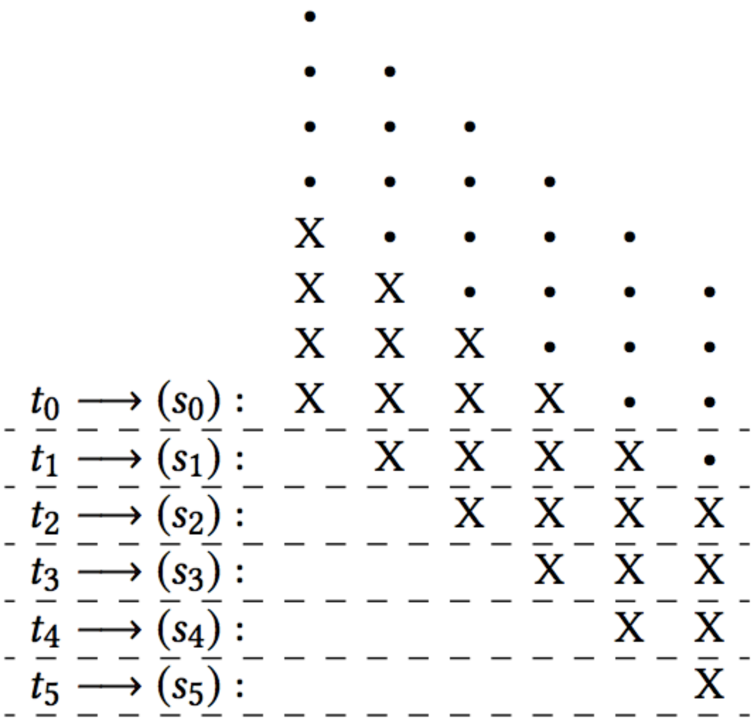
Slightly-modified Shamir's secret sharing scheme in Reed-Solomon (canonical) code form:

- Choose $n-k-1$ random coefficients $f_{1,i},\ldots f_{n-k-1,i}$ from F.
- Pick and publish a random element $a_0 \in$ F and assign the secret to be $s_i = f_i(a_0)$.
- Compute $f_i(z)=f_{n-k-1,i}z^{n-k-1}+ \ldots +f_{1,i}z+f_{0,i}$, where $f_{0,i} = s_i-(f_{n-k-1,i}a_0^{n-k-1}+ \ldots +f_{1,i}a_0)$.
- Now $f_i(a_0)=s_i$, and any subset of $n-k-1$ coefficients of $f_i(z)$ leaks no information about s_i .
- Pick and publish a random primitive element b of the field F, and construct the generator polynomial $g(z) = (z - b)(z - b^2) \ldots (z - b^k)$ of degree k.
- The first $n - k$ shares of the secret are the coefficients of $f_i(z)$, and the following k shares are the coefficients of the remainder polynomial obtained by dividing $z^k f(z)$ by $g(z)$.

Achieving start-time independence

A multiplexed QTAB scheme.

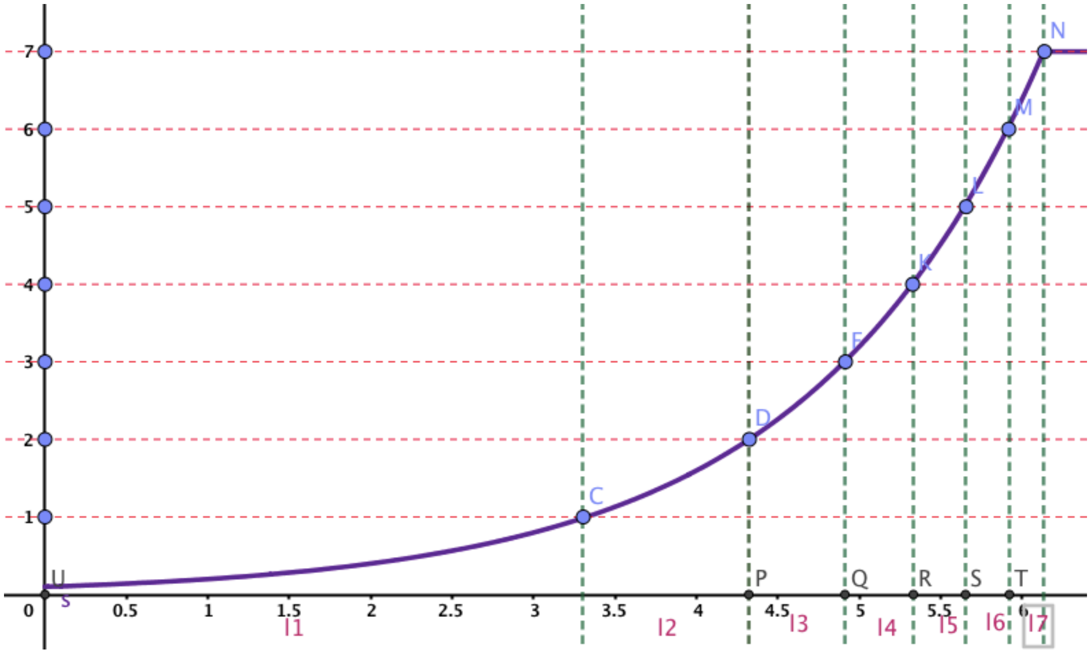
- Since first (n-k-1) clues are random, we can batch them.
- The width of the multiplexed scheme is now (k+1) instead of n.

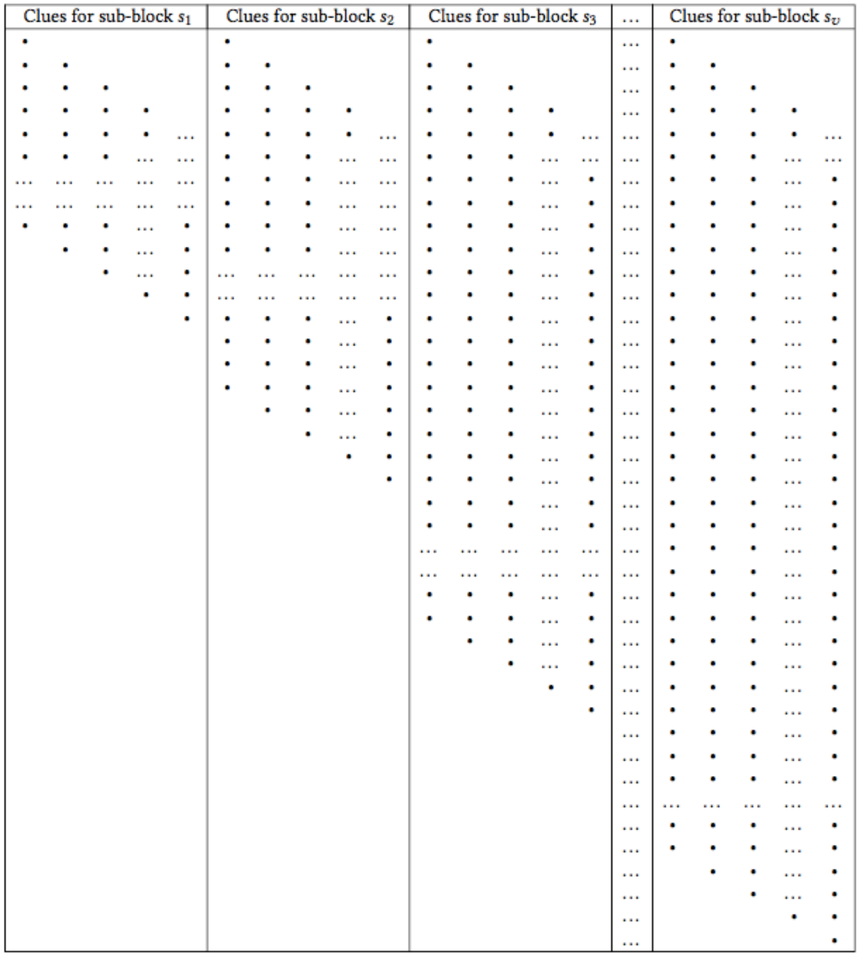


	•					
	•	•				
	•	•	•			
	•	•	•	•		
	X	•	•	•	•	
	X	X	•	•	•	•
	X	X	X	•	•	•
$t_0 \longrightarrow (s_0)$:	X	X	X	X	•	•
$t_1 \longrightarrow (s_1)$:		X	X	X	X	•
$t_2 \longrightarrow (s_2)$:			X	X	X	X
$t_3 \longrightarrow (s_3)$:				X	X	X
$t_4 \longrightarrow (s_4)$:					X	X
$t_5 \longrightarrow (s_5)$:						X

Controlling information transfer

The **extended** QTAB-KEP.





Clues for sub-block s_1
Clues for sub-block s_2
Clues for sub-block s_3
…
Clues for sub-block s_v

Security and Functionality Analysis: Research Problems

- Can the attacker synchronize encounters with tag to capture consecutive bits?
- Can an attacker verify tag's presence in a certain place (tag tracking) based on incomplete information about tag's secret?
- How does legitimate reader find secret characteristic polynomial?
- What if legitimate reader misses a small number *k* of bits in the middle?
- Can the attacker follow the same strategies for correcting de-synchronizations?

Summary and Future Work

- We introduced the AP pairing protocol and Algebraic QTAB-KEP, suited for supporting zero-configuration systems.
- Time-advantage key establishment protocol is automatic, and based on two principles:
  - legitimate reader has the advantage of time;
  - cipher weaknesses can be used constructively.

The Adopted Pet protocol is a first step towards a paradigm where authentication and security is based on the legitimate parties mounting successful attacks on each-other's cryptographic protocols, and where the work of anonymous attackers and hackers can serve as the basis for faster authentication and legitimate decryption.

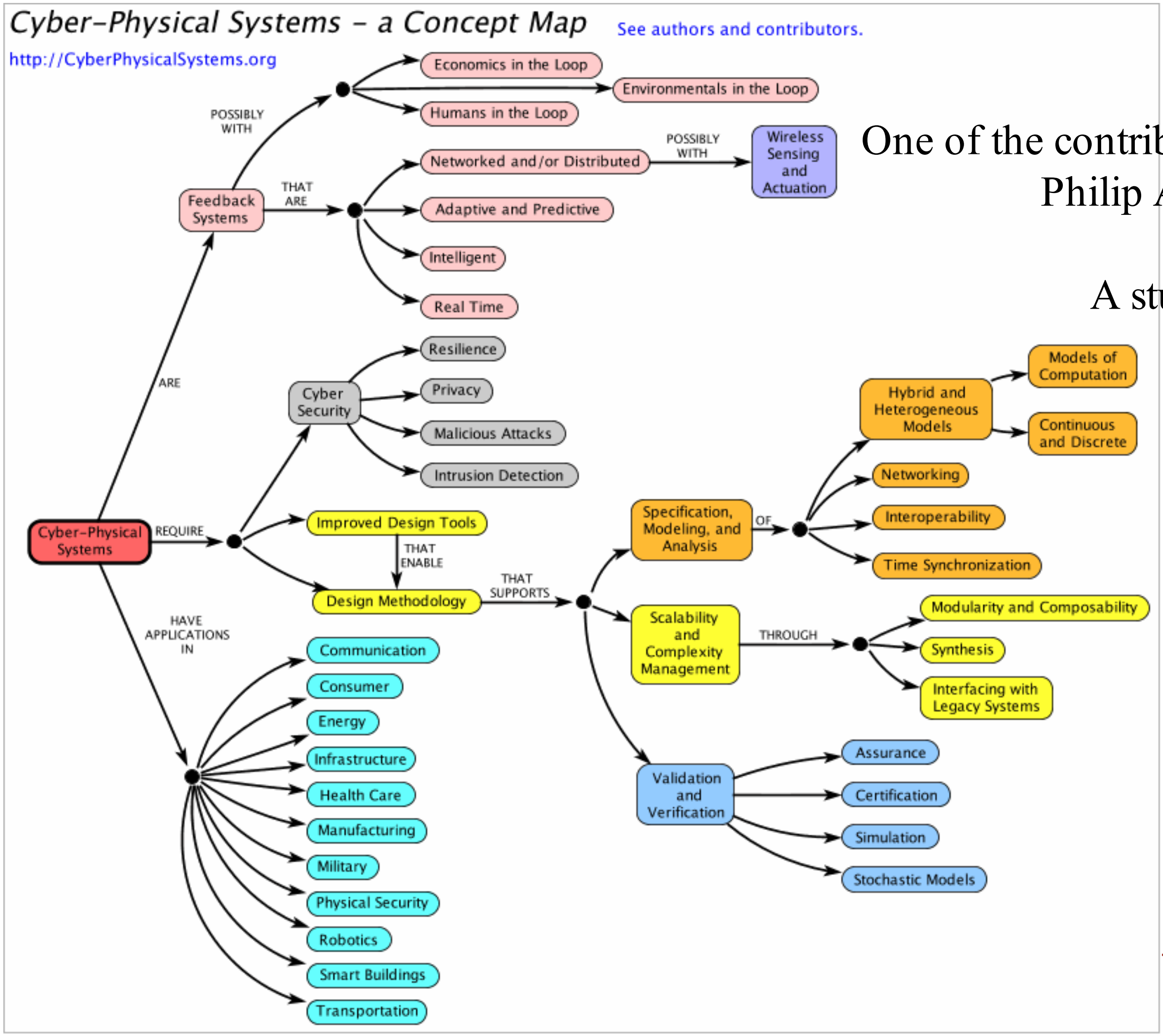
Thanks

Q&A

Yong Guan
guan@iastate.edu

Iowa State University

CPS – A Concept Map from Edward A. Lee



One of the contributors for this Concept Map:
Philip Asare, University of Virginia

A student of Jack and Prof. Lach