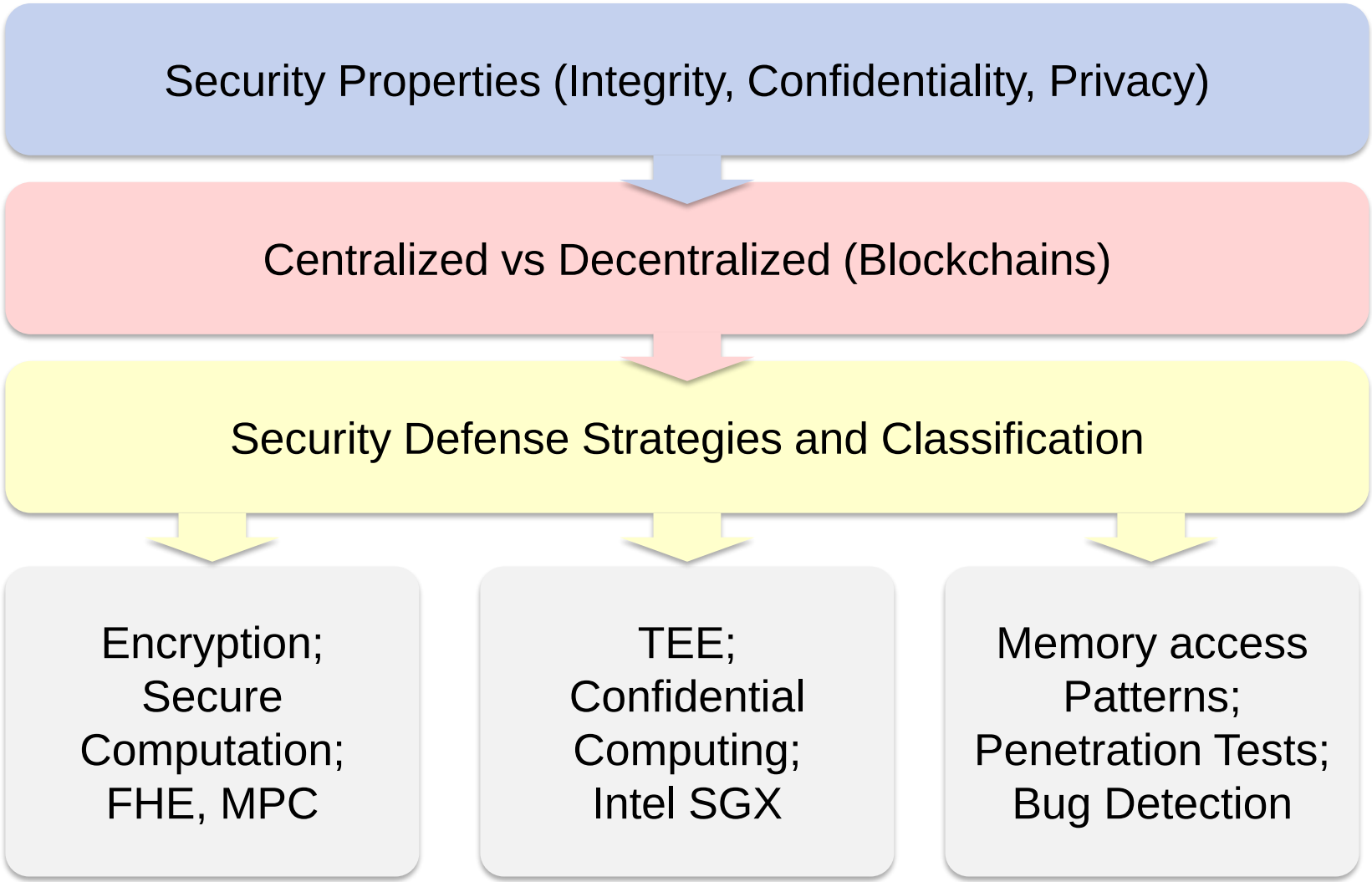
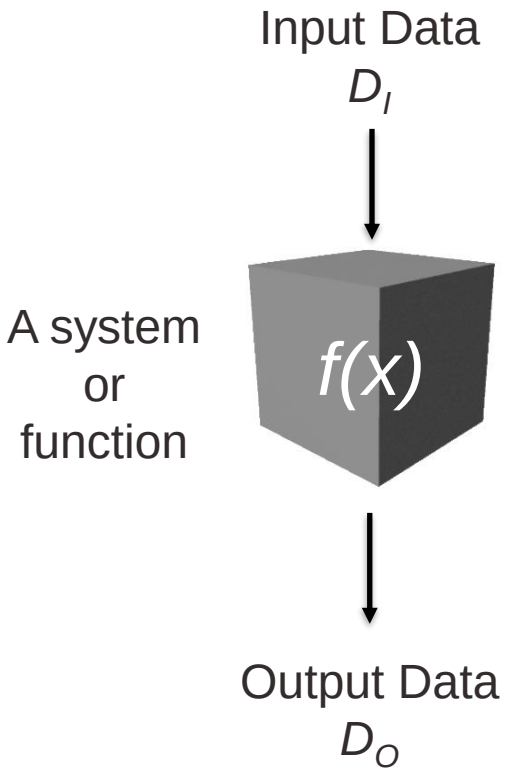
OSDI'21 and ATC'21 Session Preview: "Security & Privacy" "Blockchains & Security"

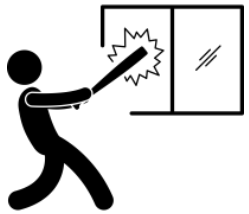
Chia-Che Tsai
Assistant Professor, Texas A&M

Outline


Security Properties (Integrity, Confidentiality, Privacy)
Centralized vs Decentralized (Blockchains)
Security Defense Strategies and Classification
Encryption; Secure Computation; FHE, MPC
TEE; Confidential Computing; Intel SGX
Memory access Patterns; Penetration Tests; Bug Detection

Security? How Do You Define It?





Integrity:
Protection of the data or system states from illegal modification

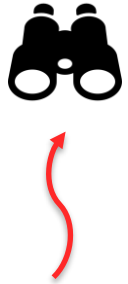
Confidentiality:
Protection of the data or system states from illegal observation

Other properties (e.g., availability)

Confidentiality vs Privacy

Confidentiality:
Protection of the **data** or **system states** from illegal observation

Privacy:
Protection of the users' **identities** or **personal states** from illegal observation of **data** or **metadata**

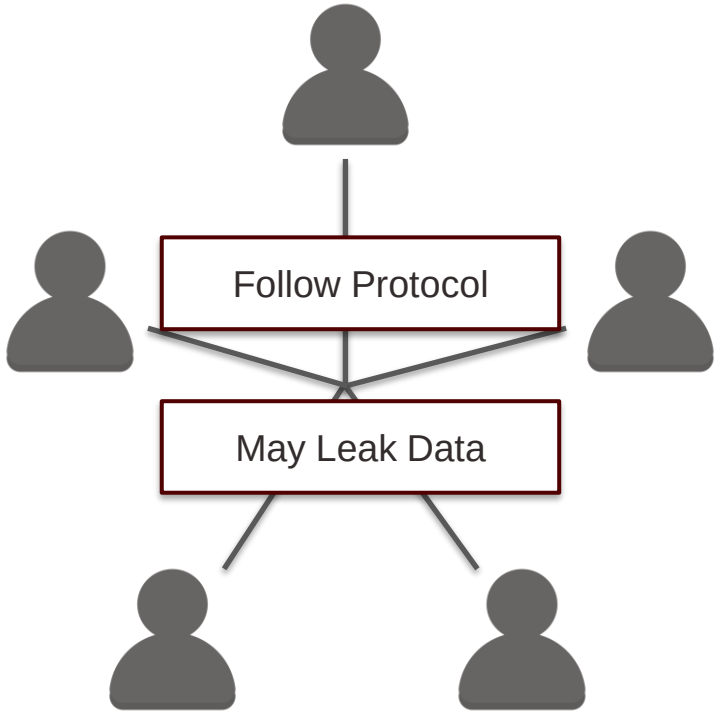


Metadata:
Who is sending message?
How big is the message?
When is the message sent?
… etc

Model Your Threats

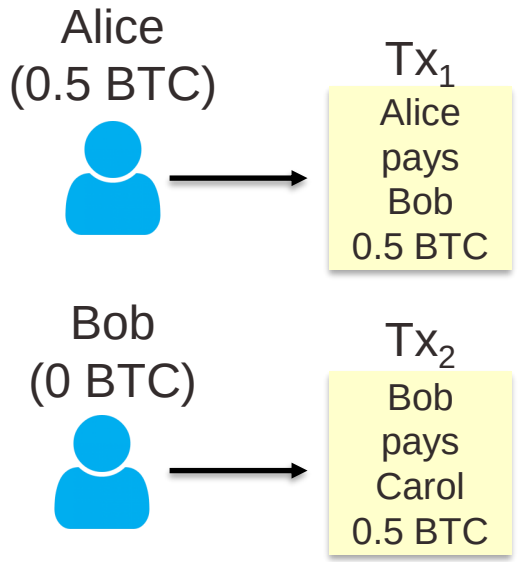
1. Single-Party; Centralized Trust

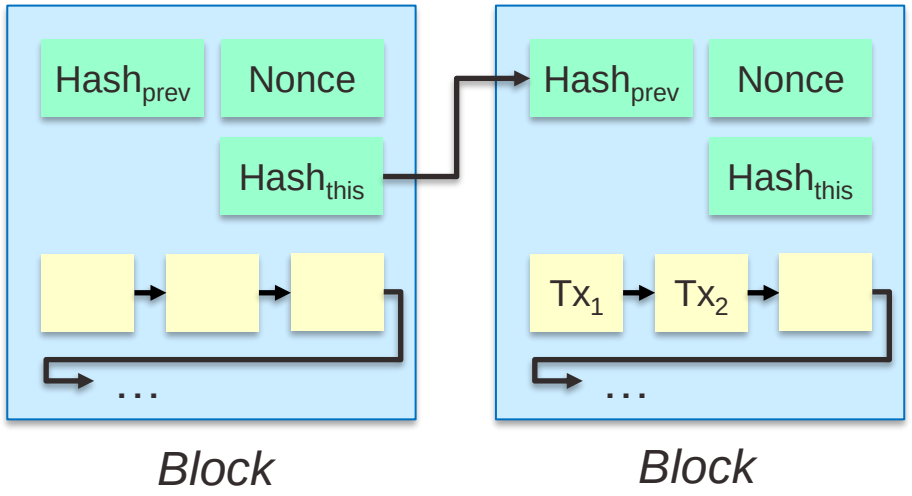
2. Multi-Party; Decentralized Trust



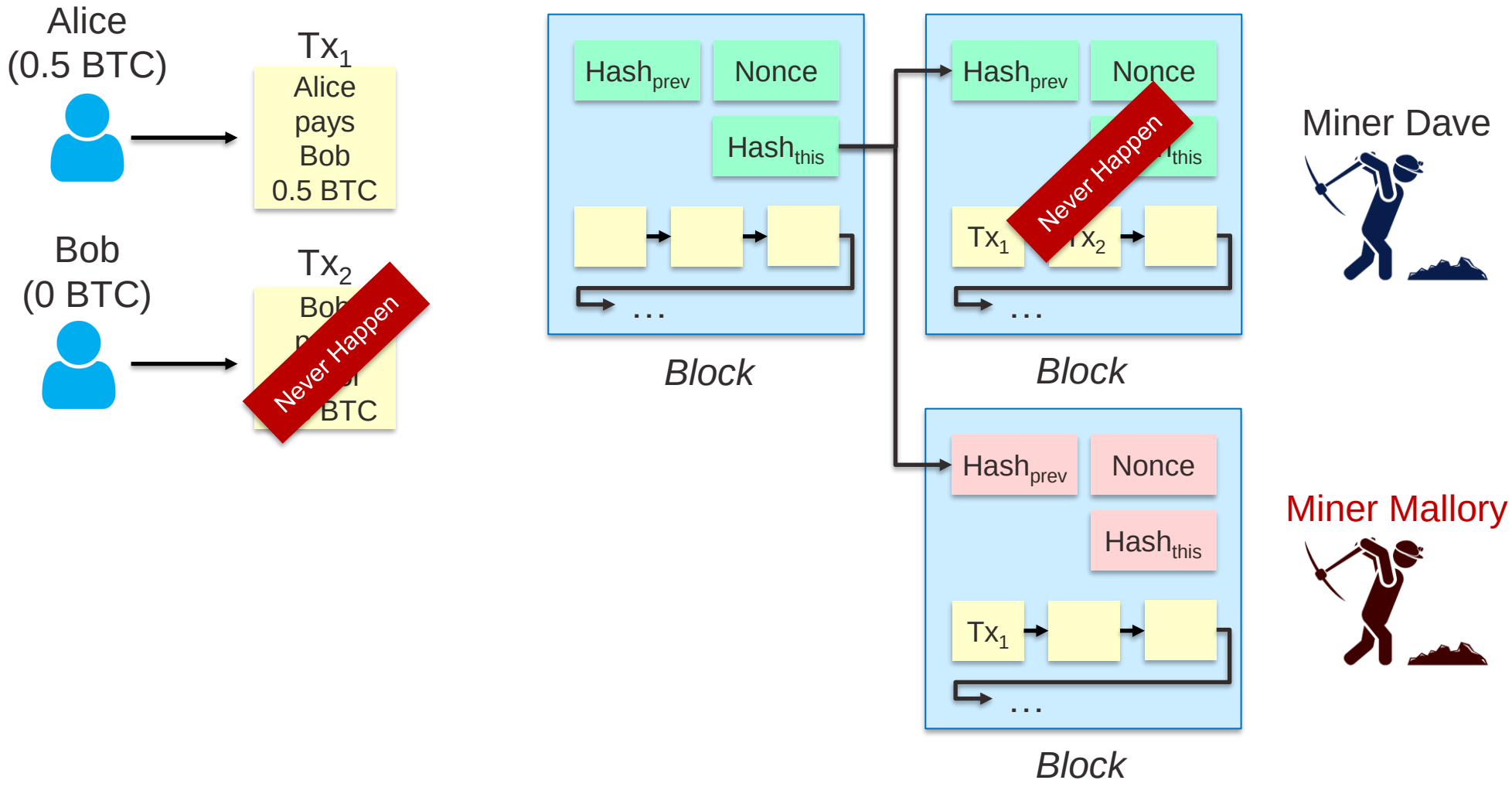
3. Multi-Party; Semi-Honest (Honest-but-curious)

Decentralization with Blockchains

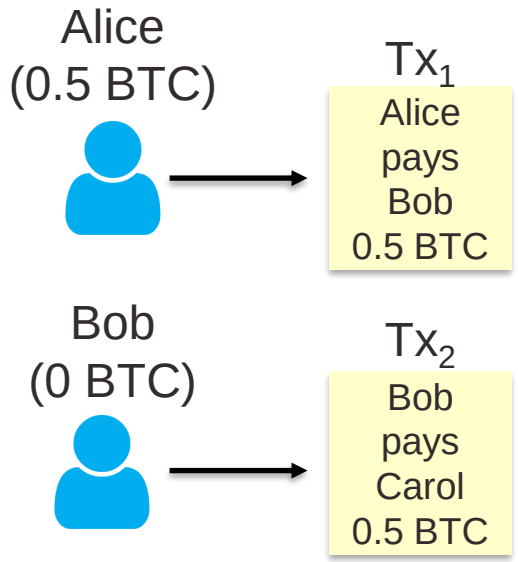


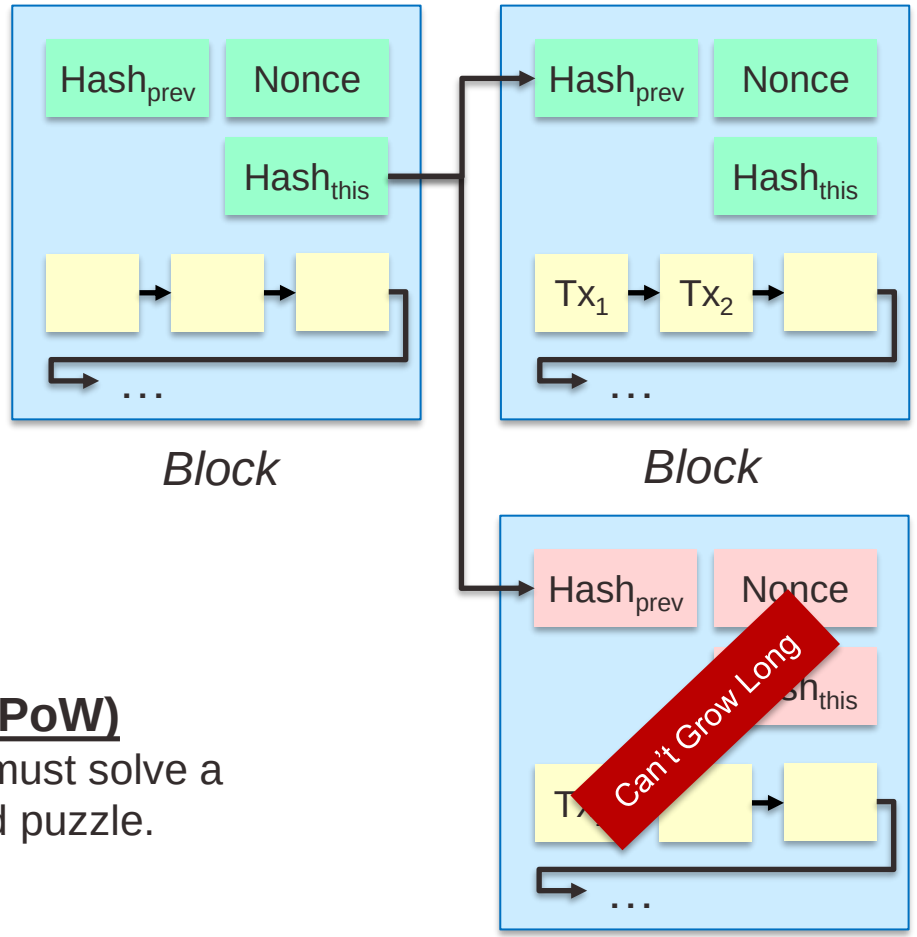


Decentralization with Blockchains



Decentralization with Blockchains





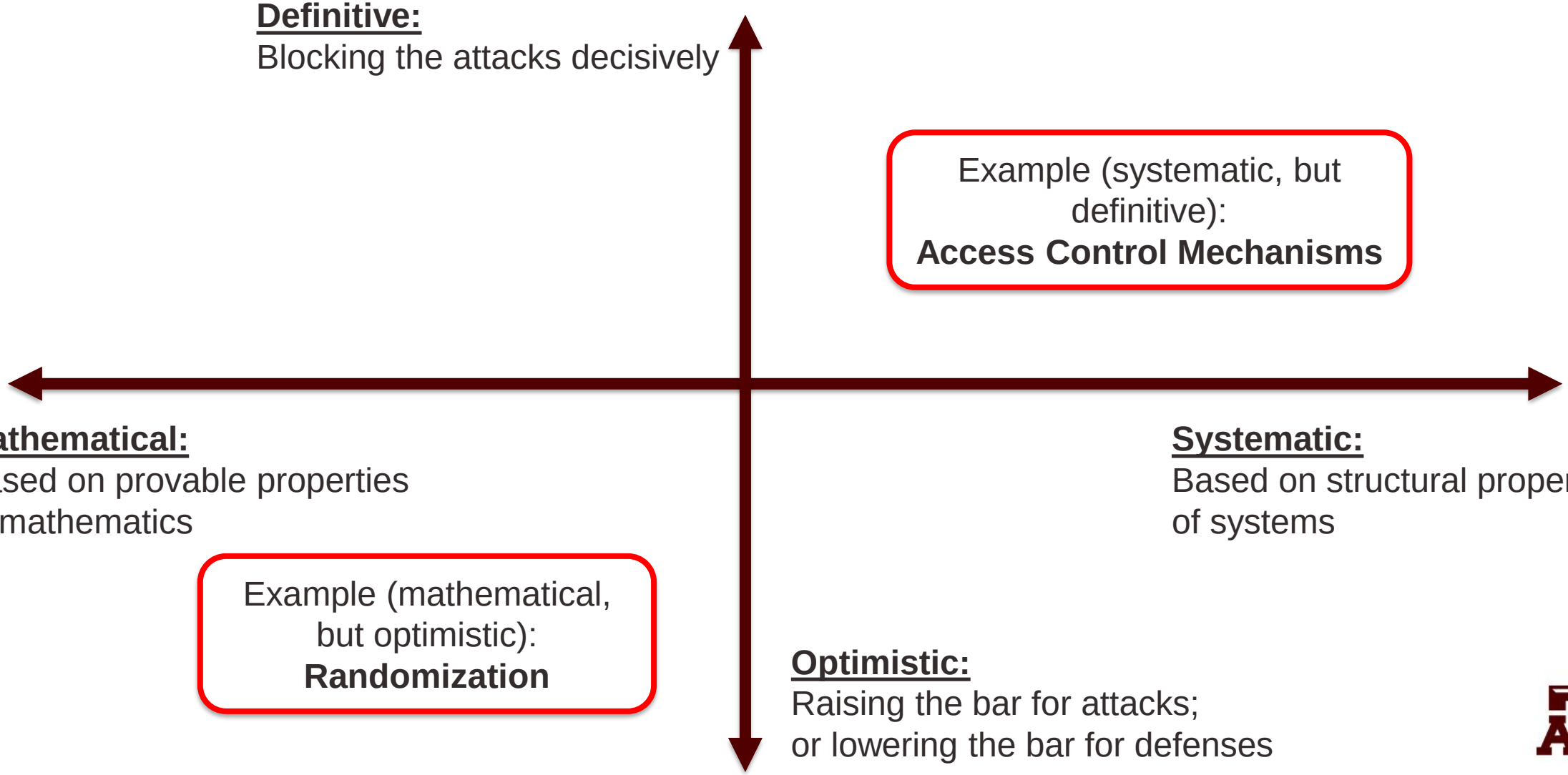
The "good" majority are incentivized.

Miner Mallory

Proof of Work (PoW)

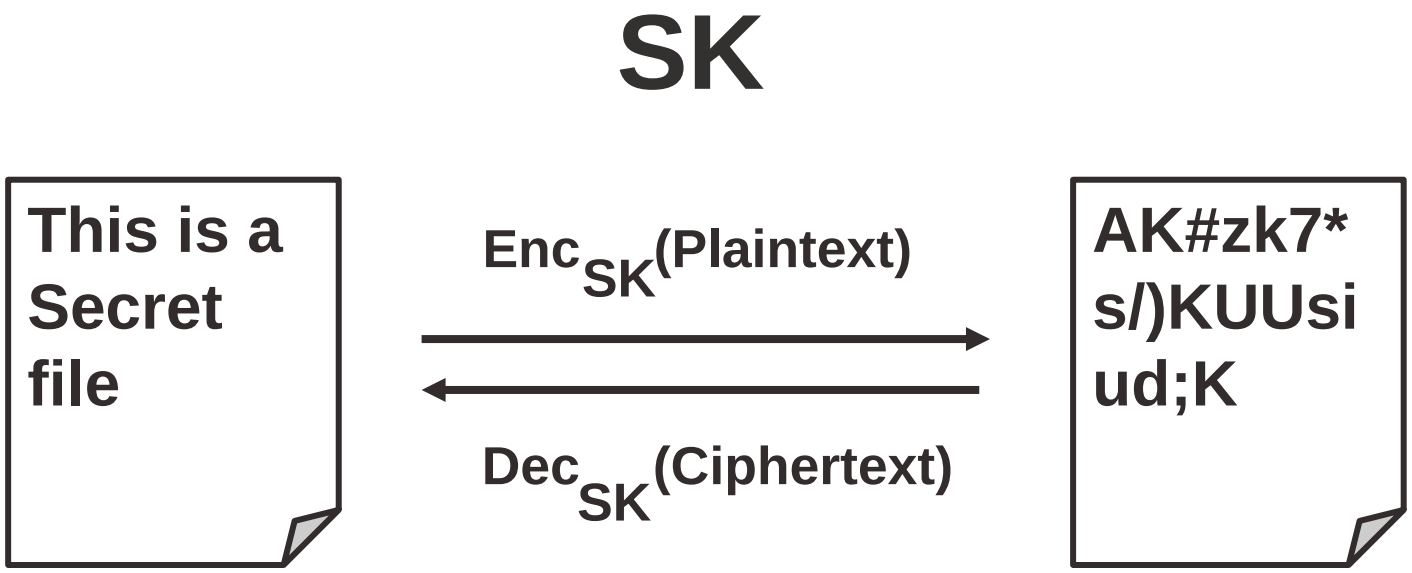
Before adding a block, must solve a computationally hard puzzle.

Defense Strategies Diagram



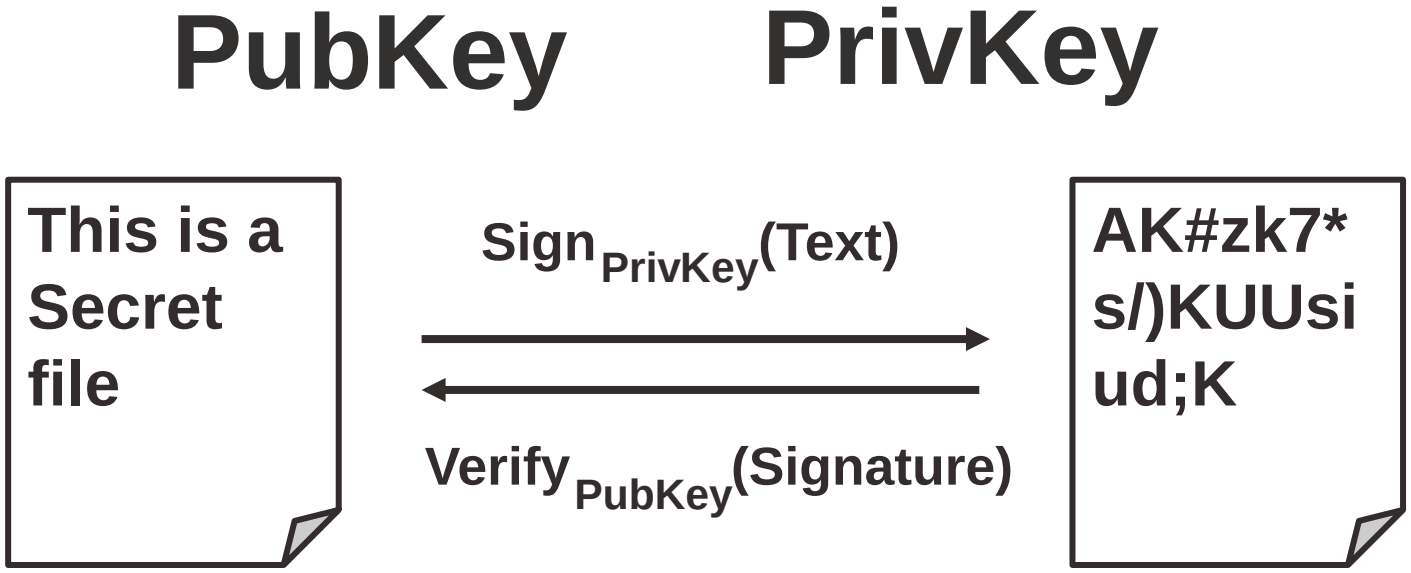
Encryption (1/2)

- Symmetric (Secret Key) Encryption



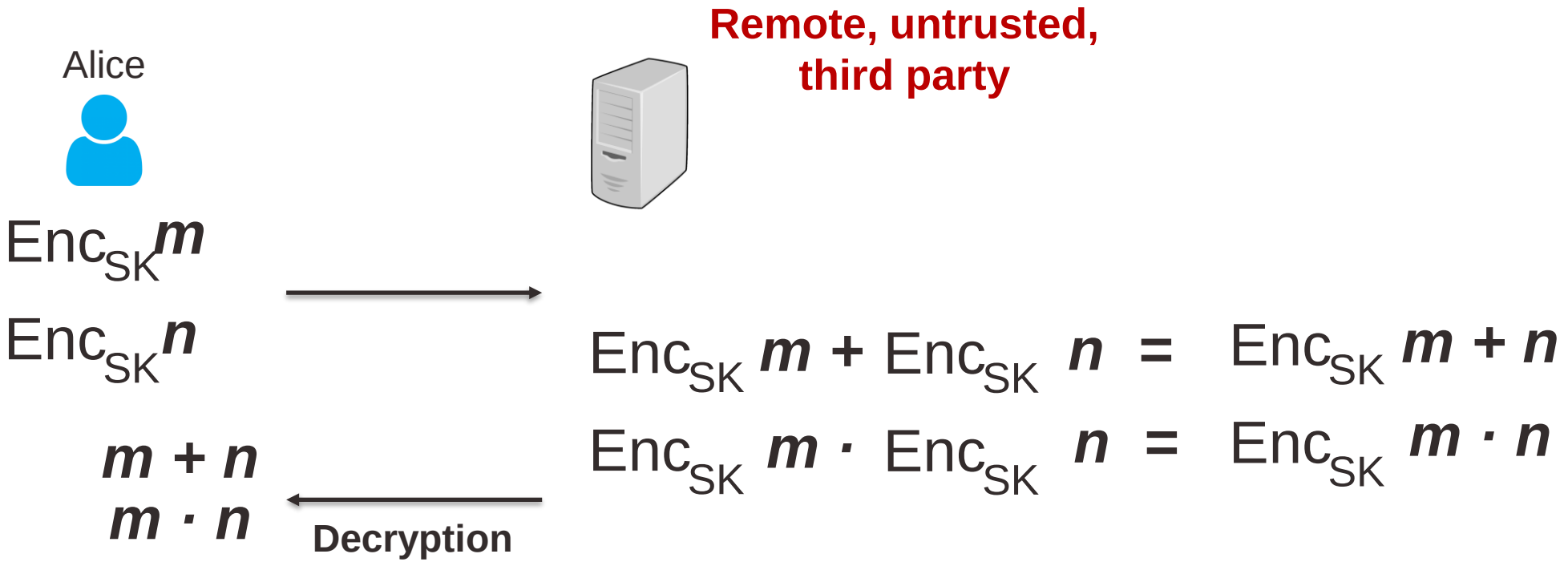
Encryption (2/2)

- Asymmetric (Public Key) Encryption



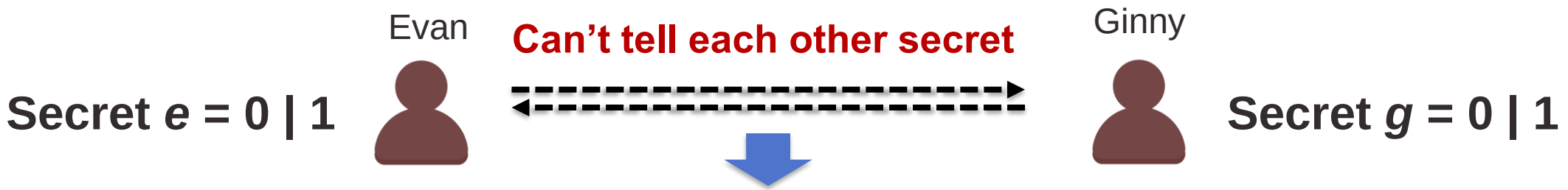
Secure Computation (1/2)

- Fully Homomorphic Encryption (FHE)



Secure Computation (2/2)

- Garbled Circuits [Yao86] – MPC



Example:
$f(e, g) = e \wedge g$

e	g	e ∧ g
0	0	0
1	0	0
0	1	0
1	1	1

Garble

e	g	e ∧ g
0	0	Enc(H($W_{e=0}$, $W_{g=0}$), 0)
1	0	Enc(H($W_{e=1}$, $W_{g=0}$), 0)
0	1	Enc(H($W_{e=0}$, $W_{g=1}$), 0)
1	1	Enc(H($W_{e=1}$, $W_{g=1}$), 1)

Shuffle

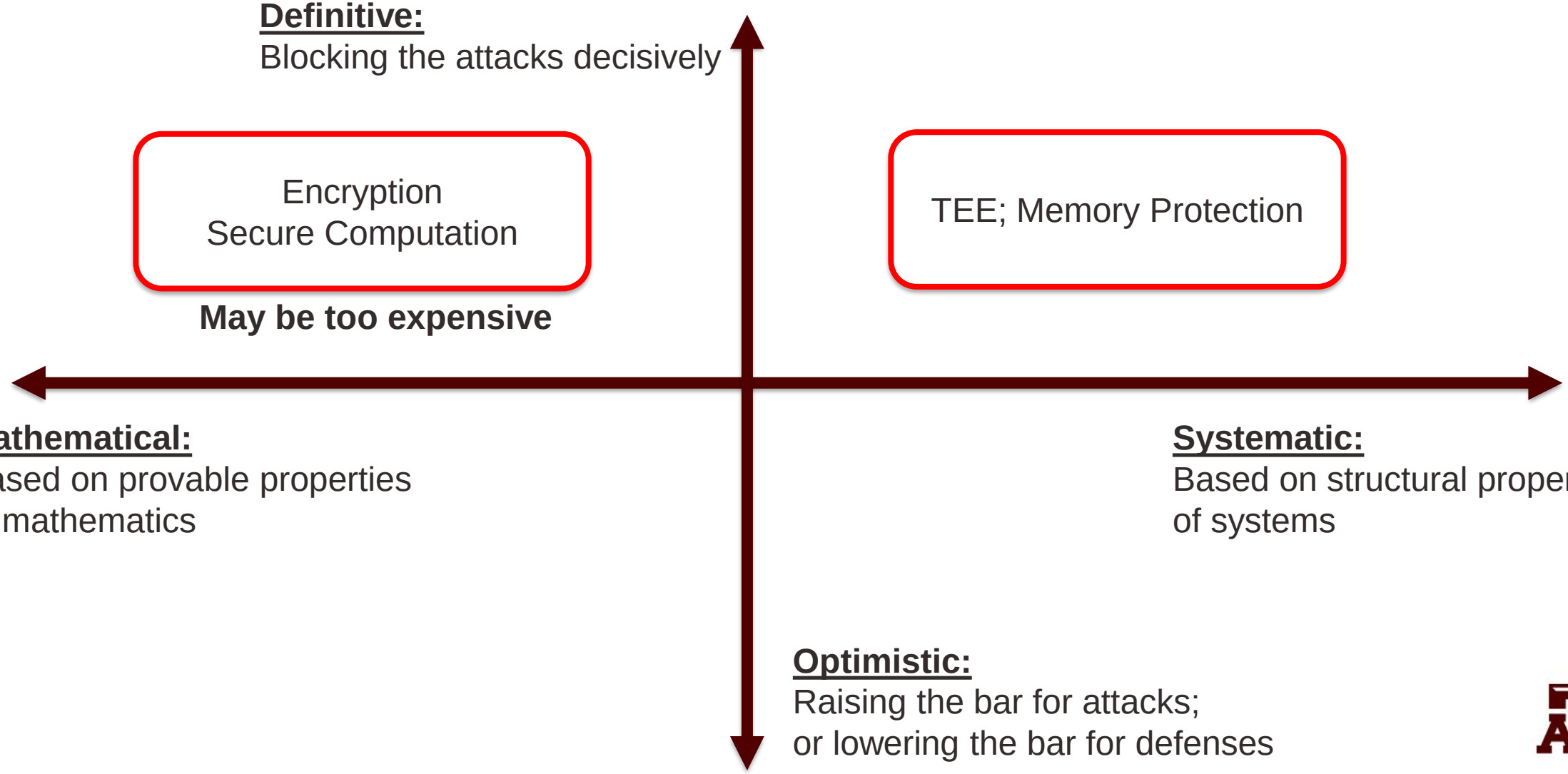
e	g	e ∧ g
0	0	Enc(H($W_{e=0}$, $W_{g=0}$), 0)
1	0	Enc(H($W_{e=1}$, $W_{g=1}$), 1)
0	1	Enc(H($W_{e=0}$, $W_{g=1}$), 0)
1	1	Enc(H($W_{e=1}$, $W_{g=0}$), 0)

Get H(W_e, W_g)

Decrypting outputs

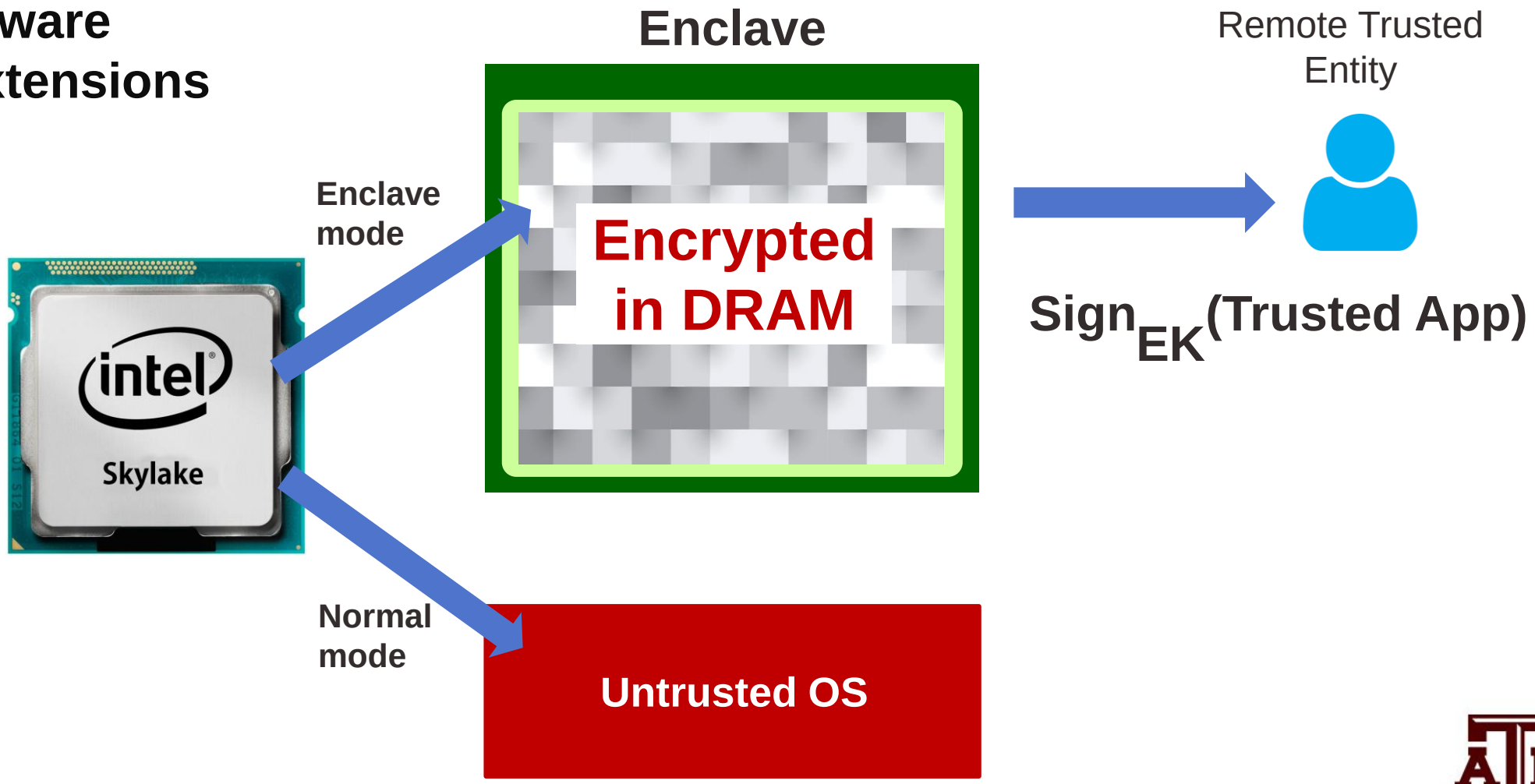
Example borrowed from "A Gentle Introduction to Yao's Garbled Circuits" by Sophia Yakoubov

Defense Strategies Diagram



TEE; Memory Protection

Intel Software Guard Extensions (SGX)



Memory Access Patterns

- Data-dependent memory access

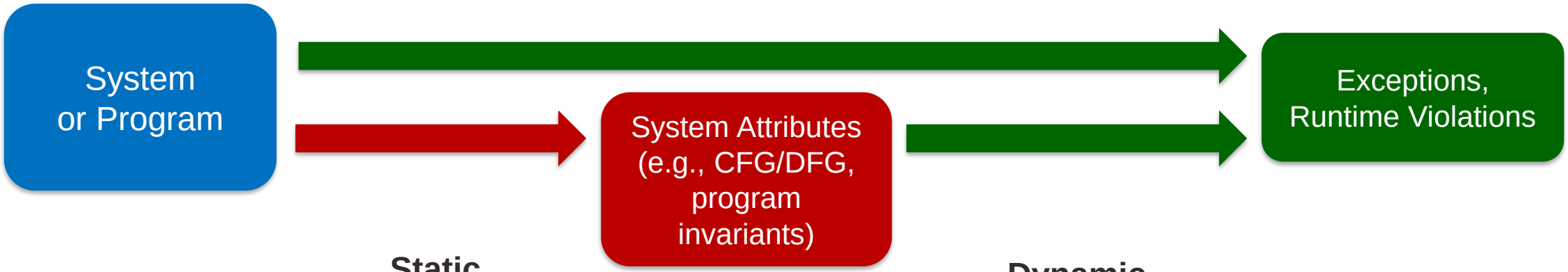
(From RSA's ElGamal Algorithm)

Modular Exponentiation (x, e, N):

```
y ← 1
for e_i = every bit in e:
    y ← Square(y)
    y ← Reduce(y, N)
    if  e_i = 1 then
        y ← Multiply(y, x)
        y ← Reduce(y, N)
```

1. **Differential timing attacks**
2. **contention attacks in system states** like cache or TLB.

Penetration Testing & Bug Detection



Static
Program analysis,
model checking,
formal verification

Dynamic
System tracing,
runtime detection

- Time-consuming
- Conservative
- Deep learning curves

- Hard to guarantee coverage (fuzzing, symbolic execution)
- Runtime overheads

Lineup

- Secure computation & cryptographic enforcement
  - **MAGE: Nearly Zero-Cost Virtual Memory for Secure Computation**
    Sam Kumar, David E. Culler, and Raluca Ada Popa
  - **Zeph: Cryptographic Enforcement of End-to-End Data Privacy**
    Lukas Burkhalter, Nicolas Küchler, Alexander Viand, Hossein Shafagh, Anwar Hithnawi
- Metadata Privacy
  - **Addra: Metadata-private voice communication over fully untrusted infrastructure**
    Ishtiyaque Ahmad, Yuntian Yang, Divyakant Agrawal, Amr El Abbadi, and Trinabh Gupta

Lineup

- Decentralization and blockchain efficiency and testing
  - **Bringing Decentralized Search to Decentralized Services**
    Youngseok Yang, Taesoo Kim, Byung-Gon Chun
  - **An Off-The-Chain Execution Environment for Scalable Testing and Profiling of Smart Contracts**
    Yeonsoo Kim, Seongho Jeong, Kamil Jezek, Bernd Burgstaller, and Bernhard Scholz
  - **RainBlock: Faster Transaction Processing in Public Blockchains**
    Soujanya Ponnapalli, Aashaka Shah, Souvik Banerjee, Dahlia Malkhi, Amy Tai, Vijay Chidambaram, and Michael Wei

Lineup

- TEE; confidential computing
  - **Avocado: A Secure In-Memory Distributed Storage System**
    Maurice Bailleu, Dimitra Giantsidi, Vasilis Gavrielatos, Do Le Quoc, Vijay Nagarajan, Pramod Bhatotia
  - **Accelerating Encrypted Deduplication via SGX**
    Yanjing Ren, Jingwei Li, Zuoru Yang, Patrick P. C. Lee, and Xiaosong Zhang
- Bug detection & penetration testing
  - **Finding Consensus Bugs in Ethereum via Multi-transaction Differential Fuzzing**
    Youngseok Yang, Taesoo Kim, Byung-Gon Chun
  - **ICARUS: Attacking low Earth orbit satellite networks**
    Giacomo Giuliari, Tommaso Ciussani, Adrian Perrig, Ankit Singla

Thank you!

Any Question or Feedback: chiache@tamu.edu