



Four Fundamental

Future Facets of Information Security

Kannan Srinathan

IIT-H



The Awesome Foursome ...

A Brief Discussion



Four Famous Proverbs

- **Well begun is half done!**
- **Seek out the seed of triumph in every adversity!**
- **It is better to know some of the questions than all of the answers!**
- **All's well that ends well!**



Well begun is half done!

Exemplary samples include:

- Aryabhata's Zero
- Church-Turing Hypothesis
- Shannon Information and Digitalization
- Von Neumann Architecture
- Trans-disciplinary links and Reductions
- Kerckhoffs's principle
- Provable Security



Our First Future Facet of Information Security

Quantum Complexity and One-Way Functions

Quantum Start to Crypto!



Amazing Anomalous Advantages of Adversity!

Exemplary samples include:

- Randomization
- Computational Difficulty
- Quantum Uncertainty and No-Cloning
- Game Theory and Byzantium
- Secure Communication in Noisy Channels



Our Second Future Facet of Information Security

Utilizing Uncertainties For Improved Security

More Adversity is Better!

Faults and failures

Asynchrony and delays

Mobility and churn

Bugs and more bugs

Dishonesty and malice

Noise and natural diffusions

Quantum collapse and decoherence

Congestion and clutter

Chaos and sensitivity

Disorder and dynamics

...



Clash of Philosophies!

Exemplary samples include:

- What is a proof?
 - Mathematics versus Computing
- What is time, and space?
 - Physics versus Algorithms
- What is efficiency?
 - Concrete versus Asymptotic
- What is the best solution?
 - Resource precedence versus re-usability



Our Third Future Facet of Information Security

Whole is greater than sum-of-parts

Is Security Emergent?

What is a fault?

Who is honest?

What is foreground/background?

**Can a cluster of insecure systems-
simulate security?**

What is a security policy?

...

...



All's Well That Ends Well!

Exemplary samples include:

- RGB Color Encoding
- Computational Indistinguishability and pseudorandomness
- Proactivization
- Super-resolution



Our Fourth Future Facet of Information Security

No-Overhead Security

Security and Performance Can Co-Exist!

Why remember *passwords*?

Intelligent Security Systems

Fault-tolerance as a function of time

Space for Improvement:

Faster

Lighter

Friendlier

Simpler

Finer

Fitter

Smarter

More Economical

...



THANK YOU !

Any Questions?