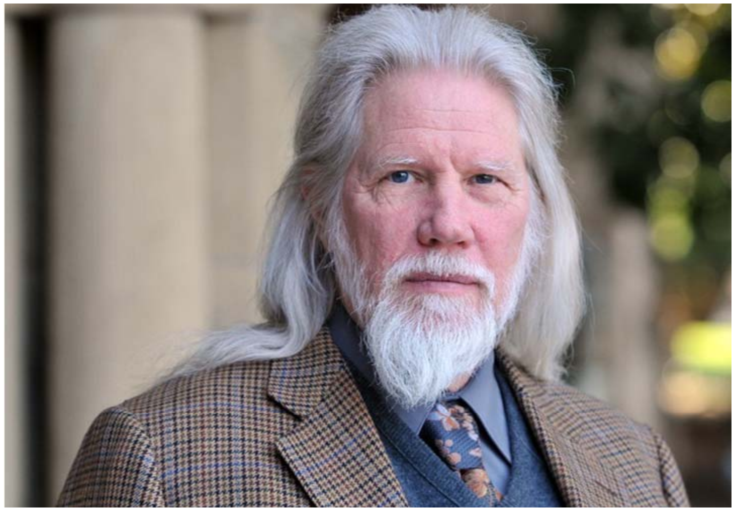
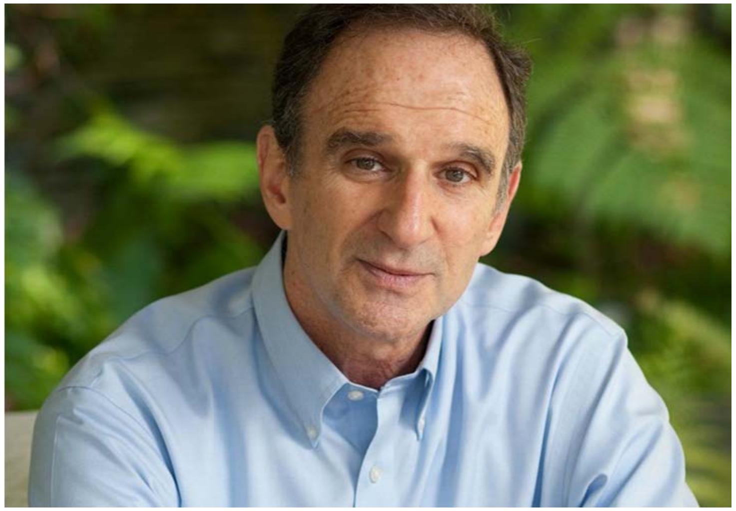
Cryptography and Blockchains: Building the Bedrock of Information Society

Ueli Maurer

ETH Zürich

Univ. of Copenhagen, June 24, 2019, Copenhagen.





Whitfield Diffie (*1944)

Martin Hellman (*1945)

Inventors of public-key cryptography

James Massey (1934 USA – 1913 Copenhagen)

Founder of the IACR
(International Association for Cryptologic Research)

Peter Landrock (born 1948)

Eminent Danish cryptographer

physical objects $\rightarrow$ **digital objects**

physical objects → digital objects

physical objects → digital objects



physical objects → digital objects

0110101101001011111101011

physical objects → digital objects



0110101101001011111101011

Effect of digital objects in the real world:

physical objects → digital objects



0110101101001011111101011

Effect of digital objects in the real world:

- execution of a program on a computer

physical objects → digital objects



01101011010010111111101011

Effect of digital objects in the real world:

- execution of a program on a computer
- transfer my entire account balance to account XY

physical objects → digital objects



01101011010010111111101011

Effect of digital objects in the real world:

- execution of a program on a computer
- transfer my entire account balance to account XY
- presentation using a virtual-reality interface

physical objects → digital objects



0110101101001011111101011

Effect of digital objects in the real world:

- execution of a program on a computer
- transfer my entire account balance to account XY
- presentation using a virtual-reality interface
- launch a nuclear missile

physical objects → digital objects

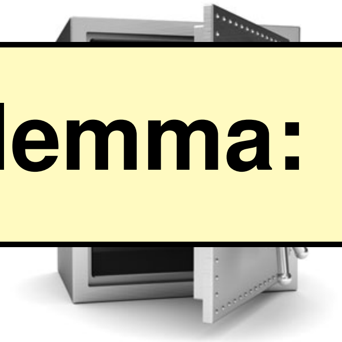


01101011010010111111101011

Effect of digital objects in the real world:

- execution of a program on a computer
- transfer my entire account balance to account XY
- presentation using a virtual-reality interface
- launch a nuclear missile
- trigger the end of humanity ....

physical objects → digital objects



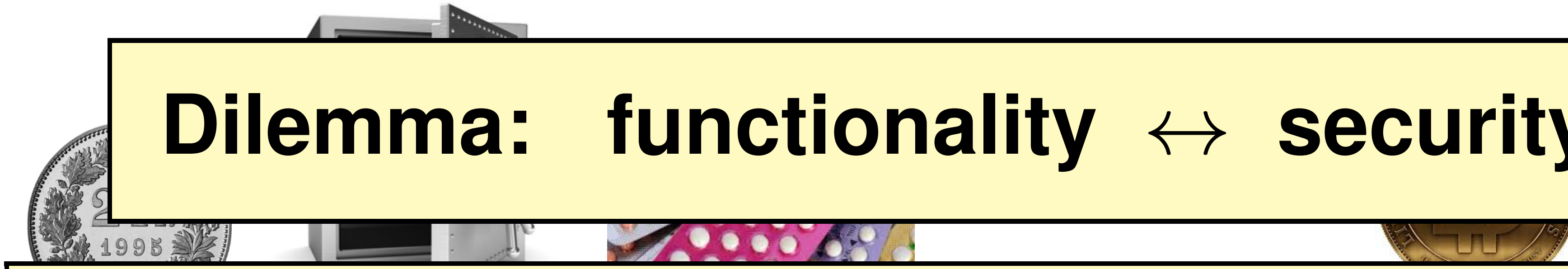
Dilemma: functionality ↔ security

01101011010010111111101011

Effect of digital objects in the real world:

- execution of a program on a computer
- transfer my entire account balance to account XY
- presentation using a virtual-reality interface
- launch a nuclear missile
- trigger the end of humanity ....

physical objects $\rightarrow$ **digital objects**



Dilemma: functionality $\leftrightarrow$ security

Functionality: One can efficiently decrypt using the key.

0110101101001011111101011

Effect of digital objects in the real world:

- execution of a program on a computer
- transfer my entire account balance to account XY
- presentation using a virtual-reality interface
- launch a nuclear missile
- trigger the end of humanity ....

physical objects → digital objects

Dilemma: functionality ↔ security

Functionality: One can efficiently decrypt using the key.

Security: One can **not** efficiently decrypt without the key.

- execution of a program on a computer
- transfer my entire account balance to account XY
- presentation using a virtual-reality interface
- launch a nuclear missile
- trigger the end of humanity ....

physical objects → digital objects




Dilemma: functionality ↔ security

Functionality: One can efficiently decrypt using the key.

Security: One can **not** efficiently decrypt without the key.

⇒ One cannot test or measure security.
One can only prove it (mathematically).

- launch a nuclear missile
- trigger the end of humanity ....

Information security: 2 types

1. **“Protective” security**

Information security: 2 types

1. **"Protective" security**
   - defensive view
   - protect against system flaws and attacks
   - mission of software design/ formal methods

Information security: 2 types

1. **"Protective" security**

   – defensive view
   – protect against system flaws and attacks
   – mission of software design/ formal methods

3 dilemmata:

- Functionality/security tradeoff dilemma
- Specification complexity dilemma
- Implementation impossibility dilemma

Information security: 2 types

1. **“Protective” security**
   - defensive view
   - protect against system flaws and attacks
   - mission of software design/ formal methods

Information security: 2 types

1. **“Protective” security**

   – defensive view

   – protect against system flaws and attacks

   – mission of software design/ formal methods

2. **Construction of virtual trusted systems**

Information security: 2 types

1. **“Protective” security**
   - defensive view
   - protect against system flaws and attacks
   - mission of software design/ formal methods

2. **Construction of virtual trusted systems**
   - mission of **cryptography**

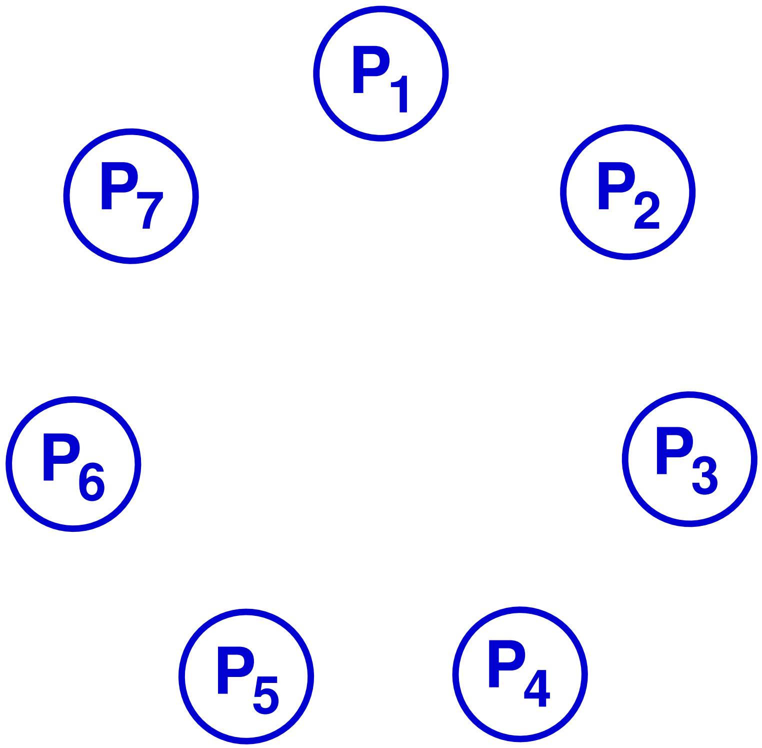
Information security: 2 types

1. **"Protective" security**
   - defensive view
   - protect against system flaws and attacks
   - mission of software design/ formal methods

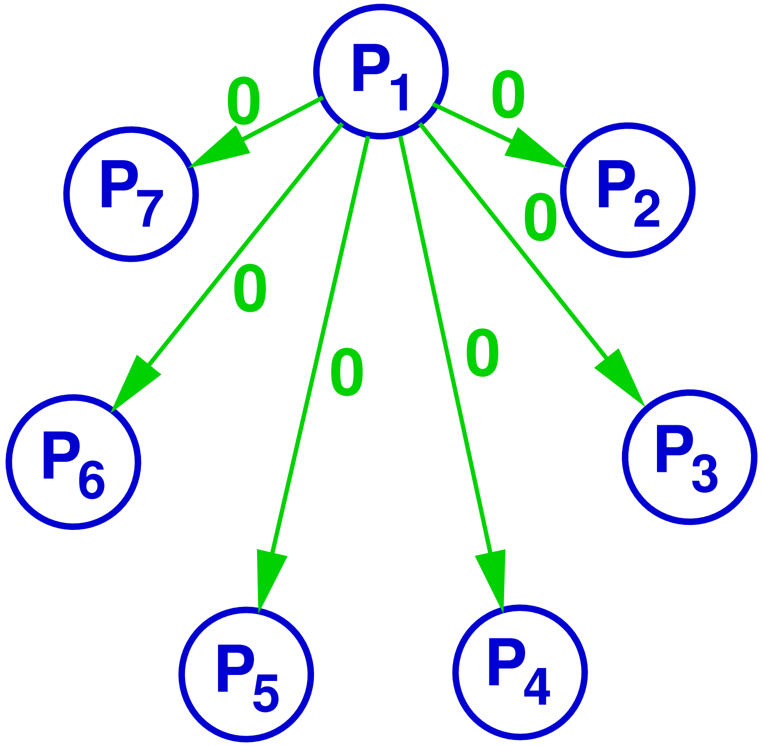
2. **Construction of virtual trusted systems**
   - mission of **cryptography**
   - virtual systems are also **economic systems**

Virtual Trusted Systems

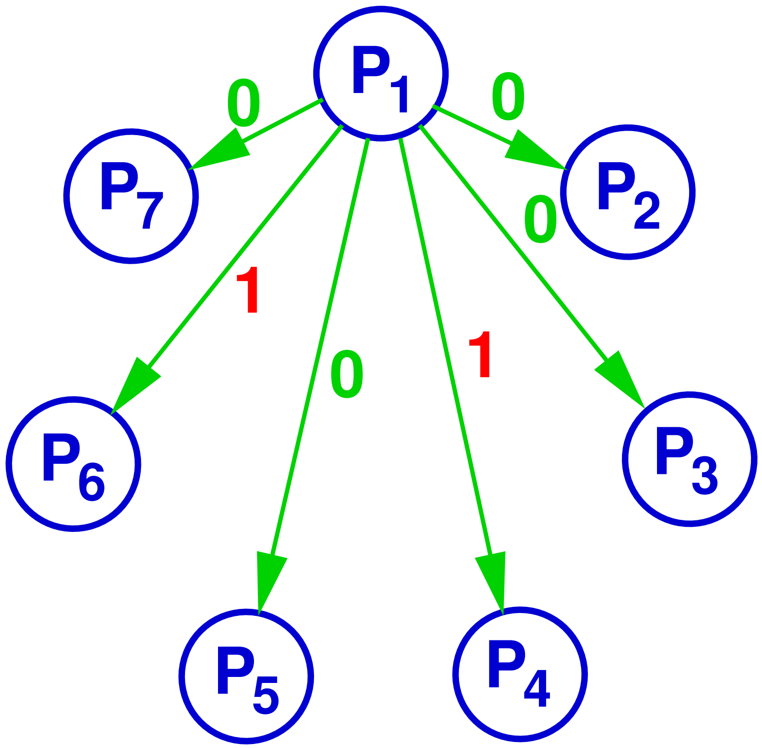
Virtual Trusted Systems



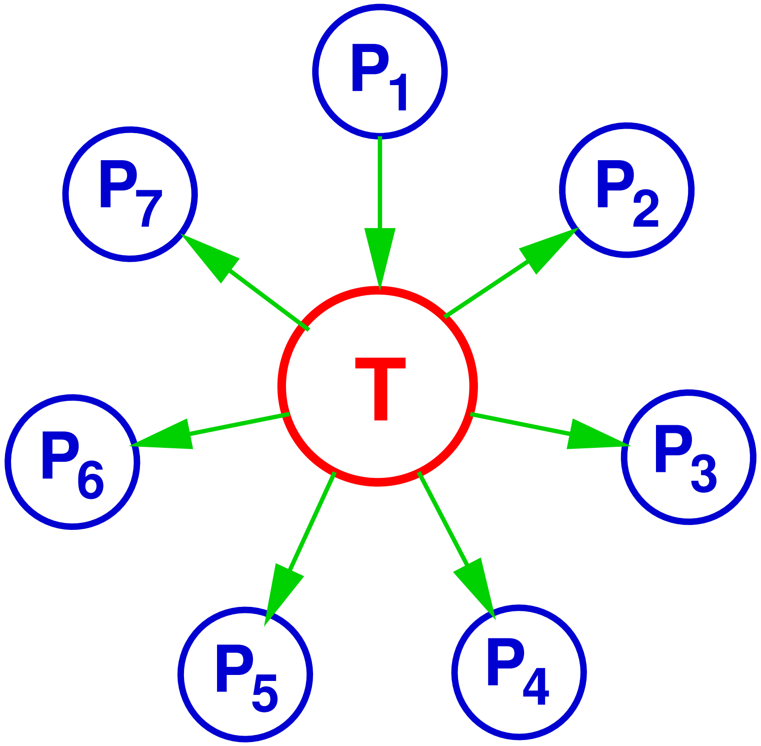
Virtual Trusted Systems



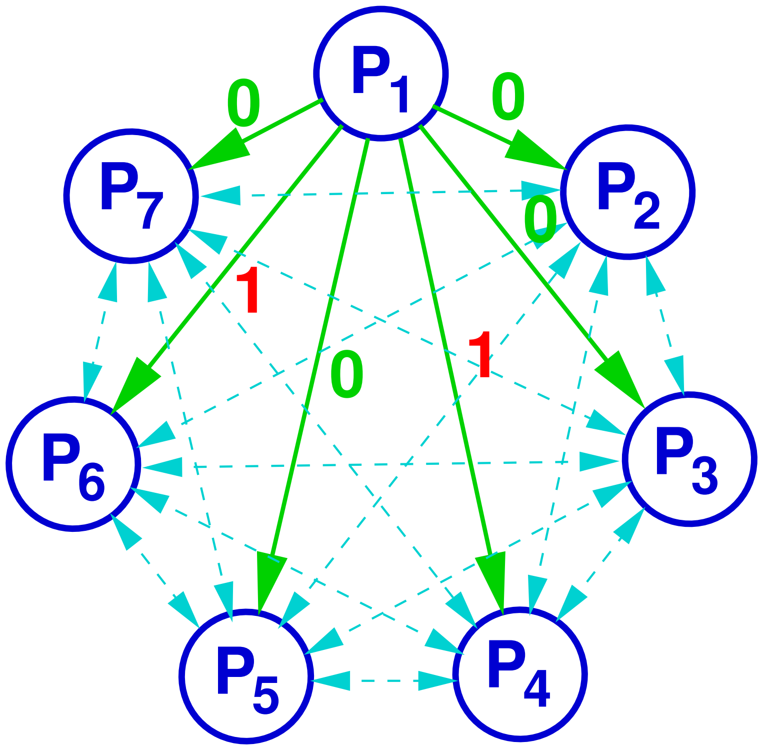
Virtual Trusted Systems



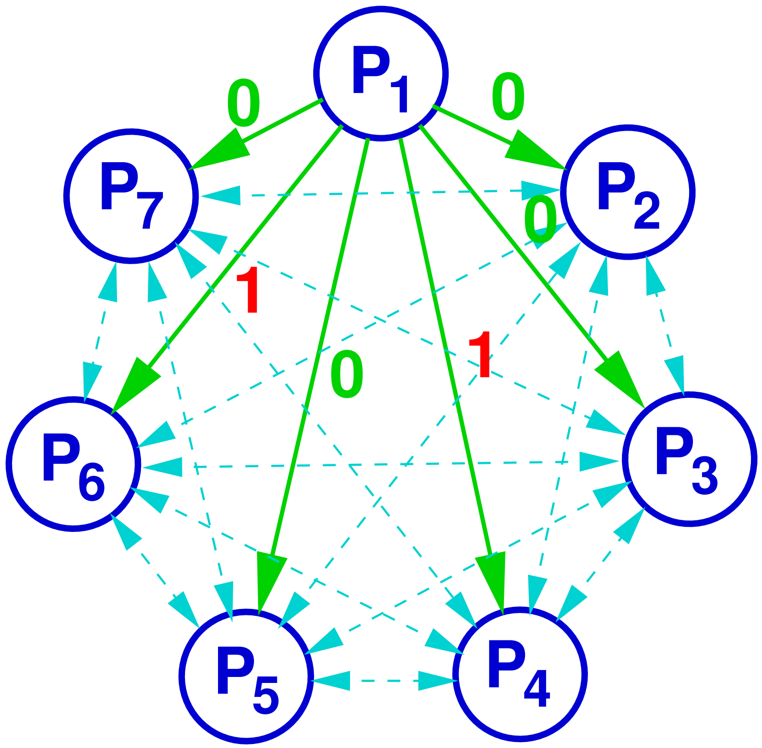
Virtual Trusted Systems



Virtual Trusted Systems

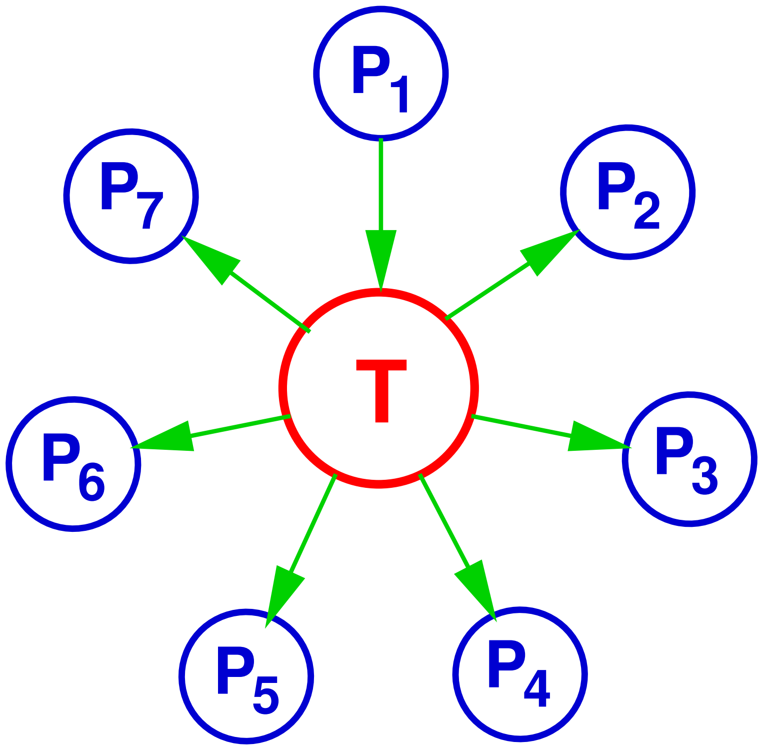


Virtual Trusted Systems



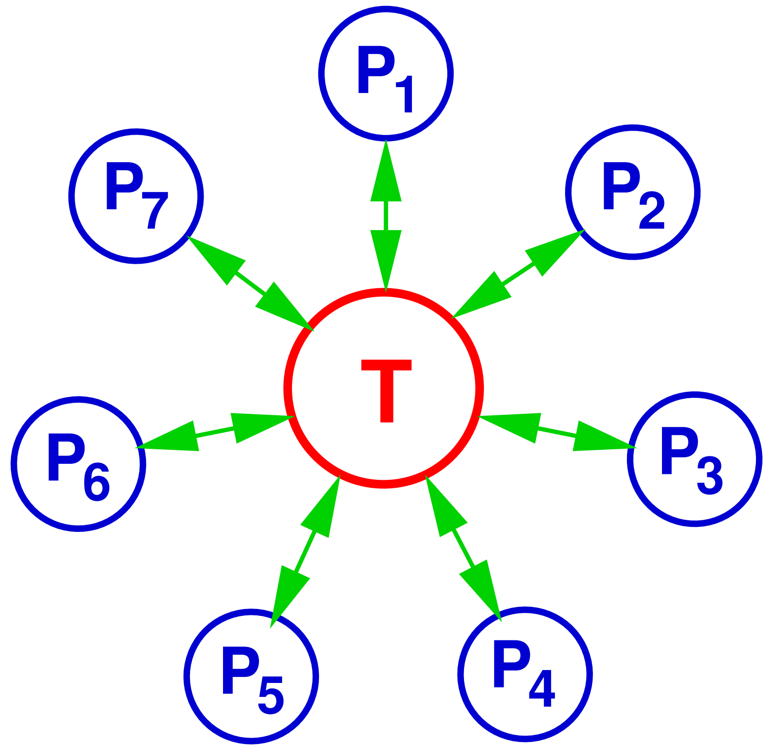
Theorem [LSP80]: This is possible if and only if less than 1/3 of the parties are corrupted.

Virtual Trusted Systems



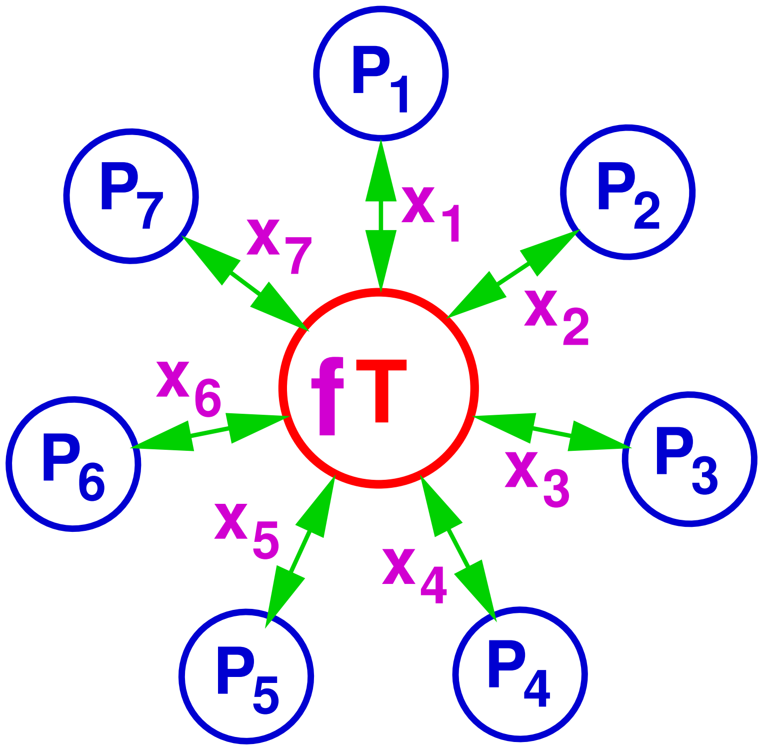
Theorem [LSP80]: This is possible if and only if less than 1/3 of the parties are corrupted.

Virtual Trusted Systems



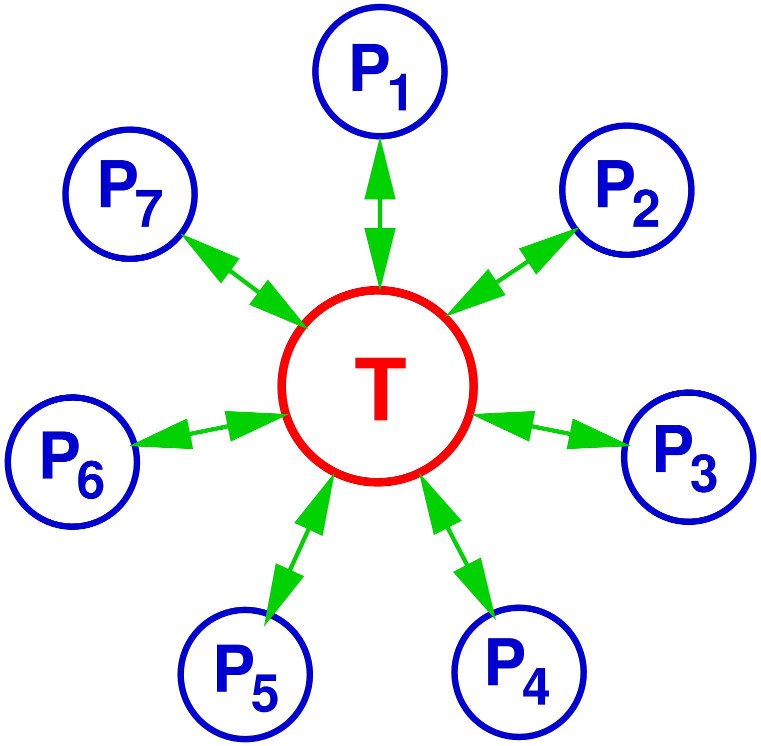
Theorem [LSP80]: This is possible if and only if less than 1/3 of the parties are corrupted.

Virtual Trusted Systems



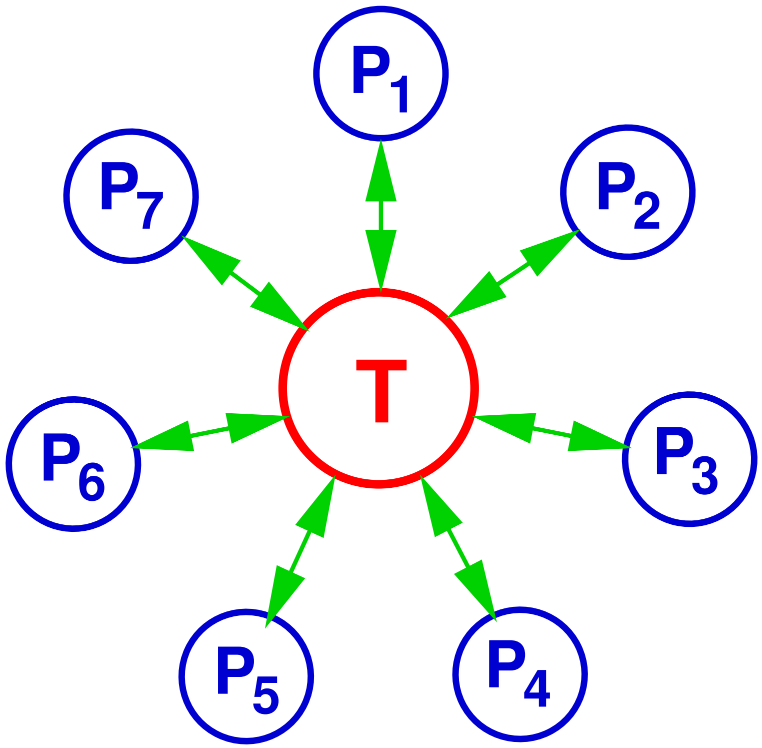
Theorem [LSP80]: This is possible if and only if less than 1/3 of the parties are corrupted.

Virtual Trusted Systems



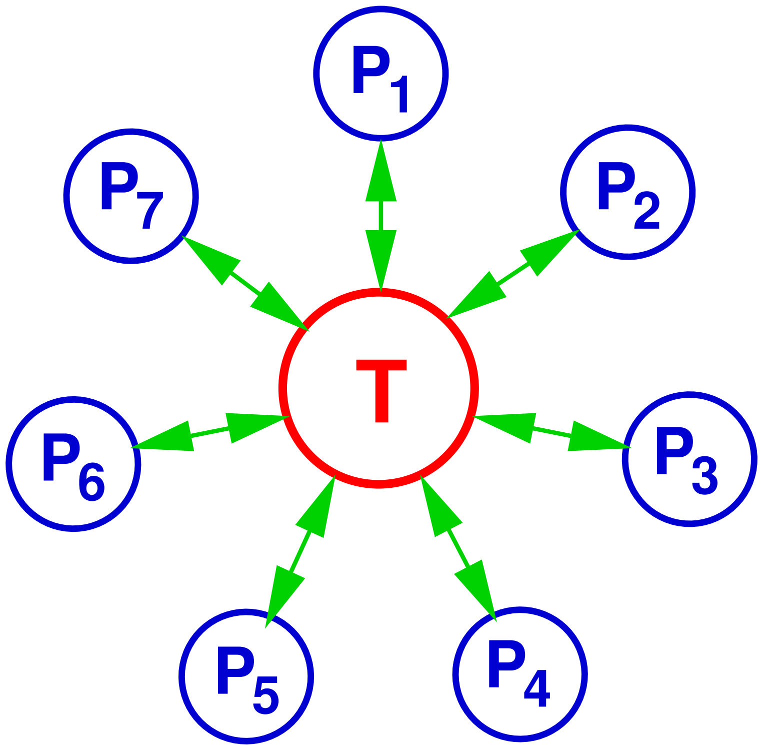
Theorem [LSP80]: This is possible if and only if less than 1/3 of the parties are corrupted.

Virtual Trusted Systems



Examples: T can be a

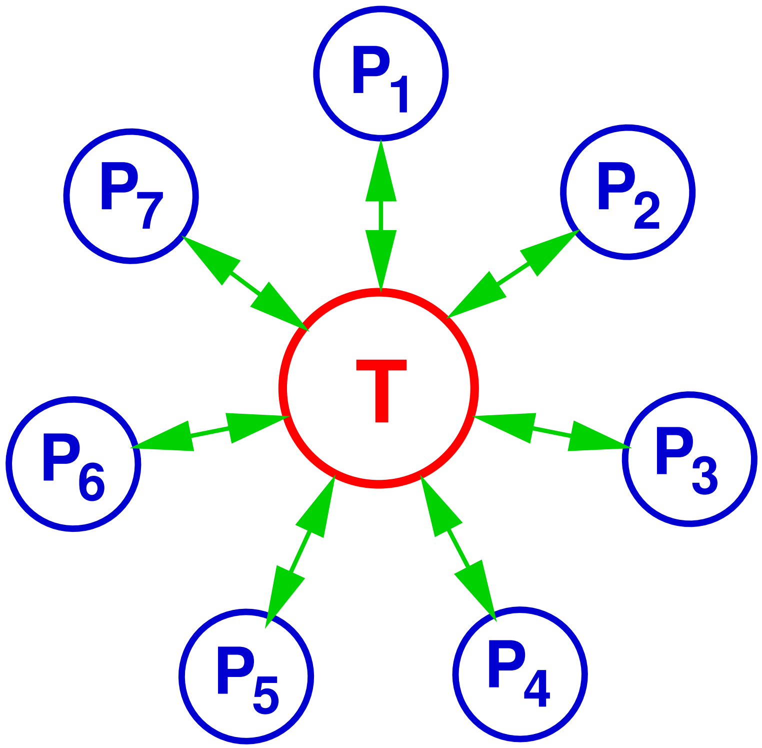
Virtual Trusted Systems



Examples: T can be a

- a secure channel between 2 entities

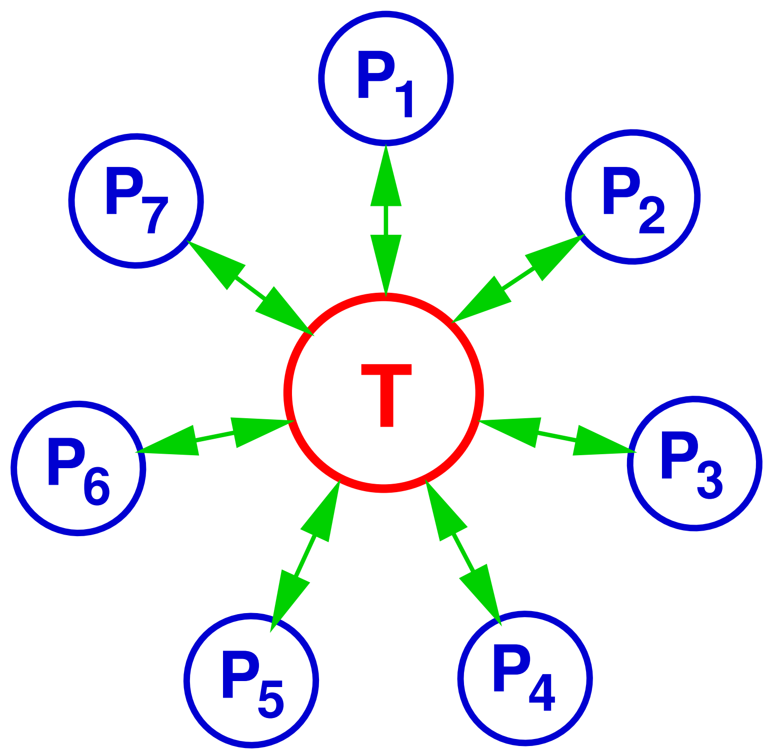
Virtual Trusted Systems



Examples: T can be a

- a secure channel between 2 entities
- voting system

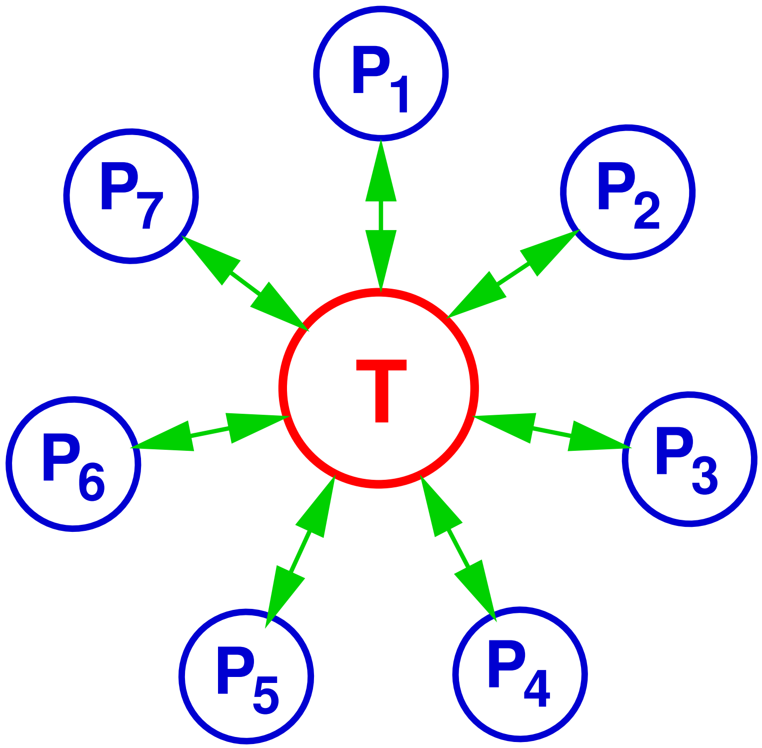
Virtual Trusted Systems



Examples: T can be a

- a secure channel between 2 entities
- voting system
- virtual central bank

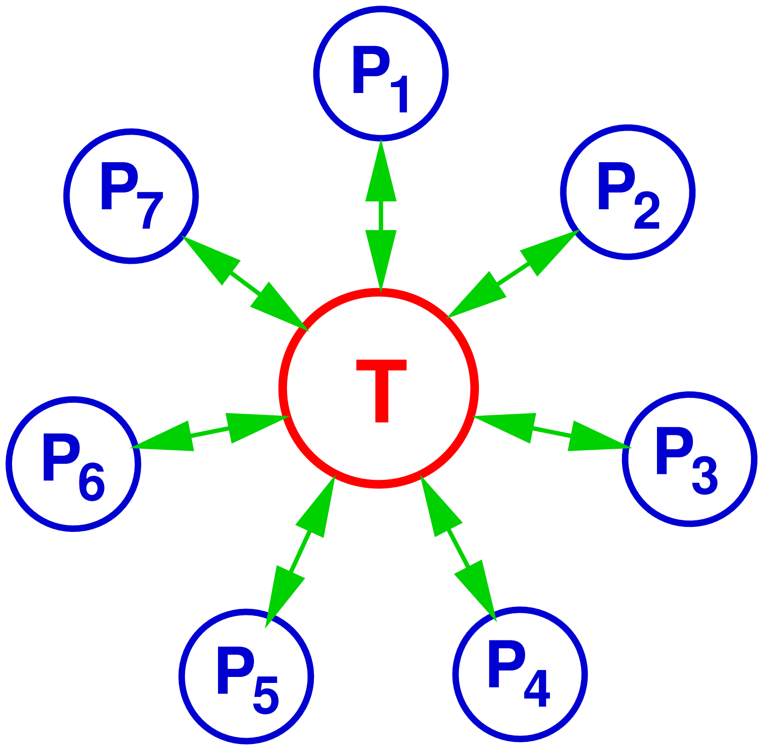
Virtual Trusted Systems



Examples: T can be a

- a secure channel between 2 entities
- voting system
- virtual central bank
- programmable transaction system

Virtual Trusted Systems



Scientific techniques:

- Consensus and Byzantine agreement protocols
- Secure multi-party computation (MPC)
- Blockchain protocols

Final remarks

Final remarks

- Cryptography as the core enabling science of constructing virtual systems

Final remarks

- Cryptography as the core enabling science
  of constructing virtual systems

- Economic science of virtual system construction

Final remarks

- Cryptography as the core enabling science
  of constructing virtual systems
- Economic science of virtual system construction
- We have only (or not even) seen the tip of the iceberg.

Final remarks

- Cryptography as the core enabling science
  of constructing virtual systems
- Economic science of virtual system construction
- We have only (or not even) seen the tip of the iceberg.
- Versatile transaction systems

Final remarks

- Cryptography as the core enabling science
  of constructing virtual systems
- Economic science of virtual system construction
- We have only (or not even) seen the tip of the iceberg.
- Versatile transaction systems
- Autonomous digital objects

Final remarks

- Cryptography as the core enabling science
  of constructing virtual systems
- Economic science of virtual system construction
- We have only (or not even) seen the tip of the iceberg.
- Versatile transaction systems
- Autonomous digital objects
- Pro-control vs. anti-control dispute

Final remarks

- Cryptography as the core enabling science
  of constructing virtual systems
- Economic science of virtual system construction
- We have only (or not even) seen the tip of the iceberg.
- Versatile transaction systems
- Autonomous digital objects
- Pro-control vs. anti-control dispute
- Denmark and Switzerland are leading nations in this space.

Thank you!