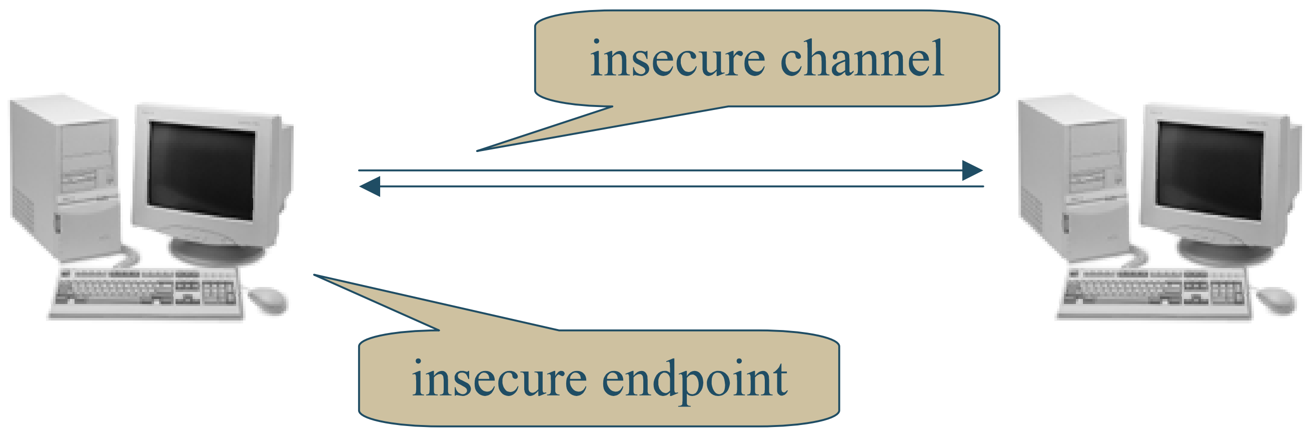
A few open problems in computer security

David Wagner
University of California, Berkeley

Overview of the field



- Communication security through *cryptography*
- Endpoint security through *systems techniques*

Background

Goals:

- Confidentiality
- Integrity
- Availability

… even in the presence of
a malicious adversary!

Problems:

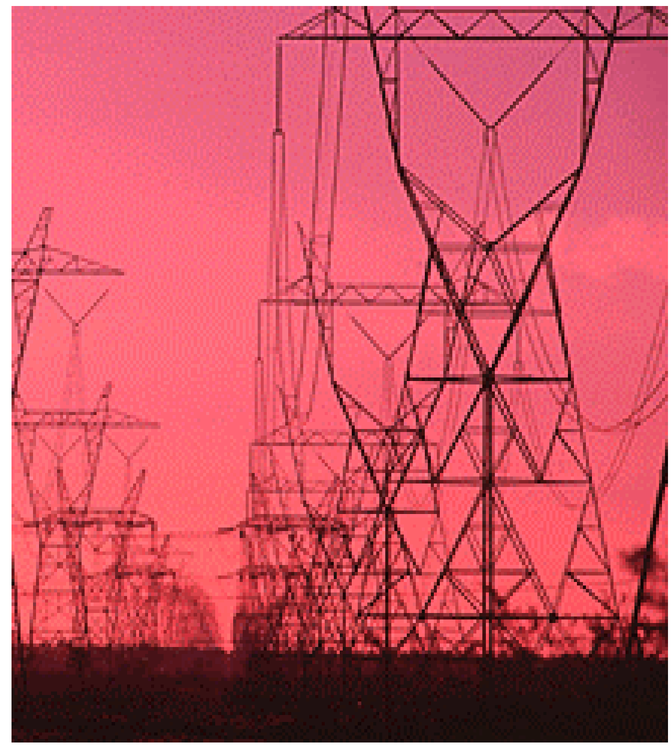
- Today’s systems often fail to meet these goals
- Security is often an afterthought

Part 1: Critical Infrastructure

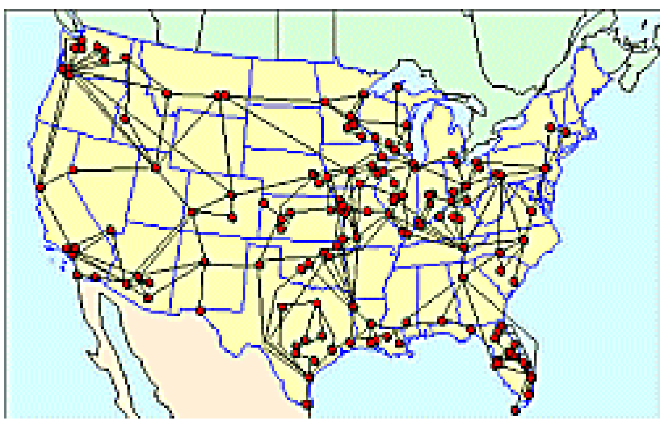
Infrastructure protection

- Critical infrastructures
  - e.g., power, water, oil, gas, telecom, banking, …
  - Evolving legacy systems
  - Increasingly reliant on I.T.
  - Very large scale
  - *Tightly interdependent*

  ⇒ Security is a challenge!

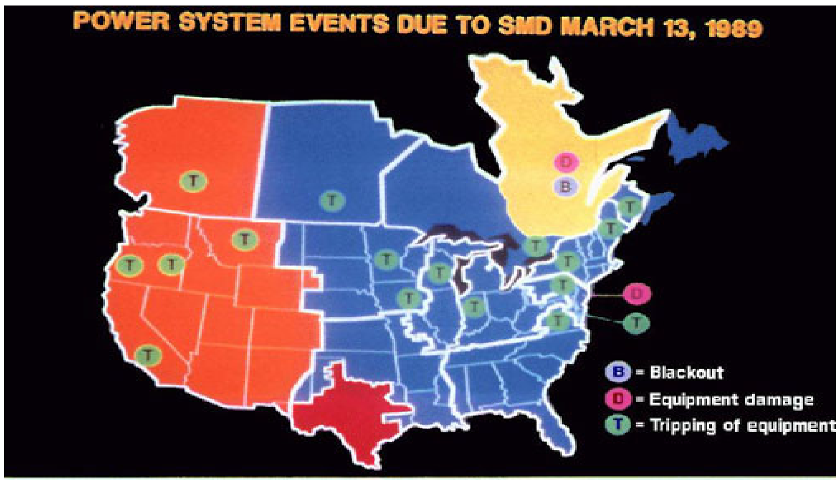


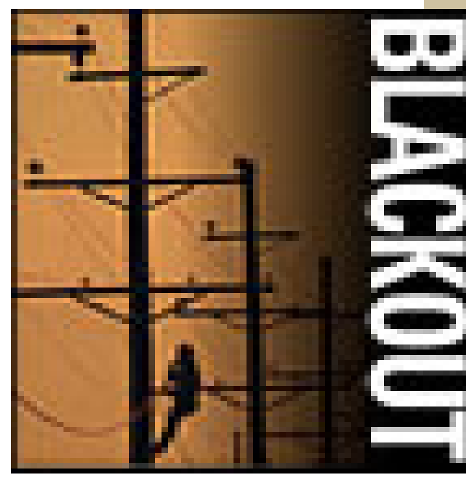
The electric power grid



- Elements
  - Loads (users)
  - Distribution (local area)
  - Transmission (long-distance)
  - Generators (adapt slowly)
  - Control centers
  - Bidding & coordination
  - Communication networks

Cascading failures



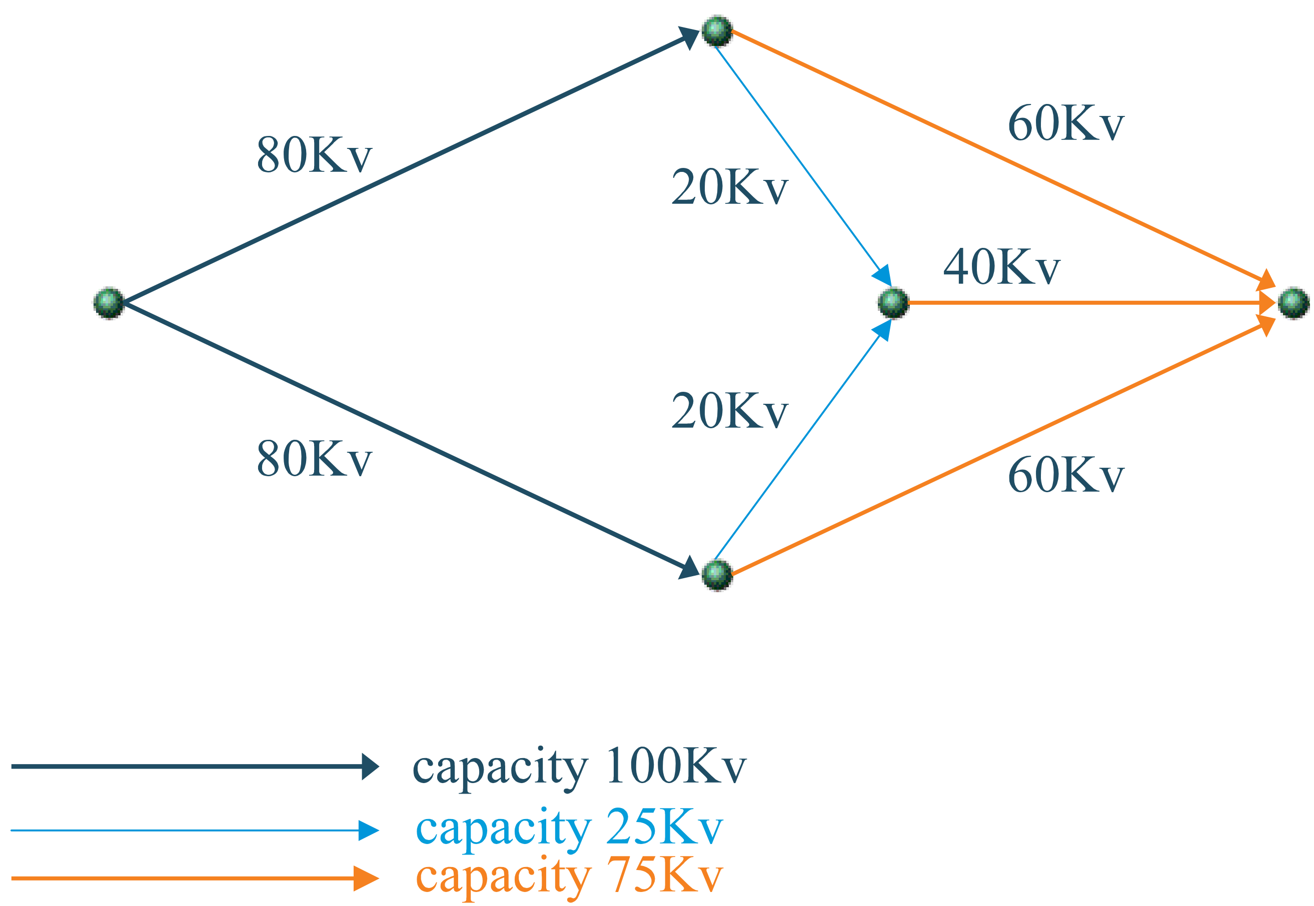


March 1989: Solar storms cause outages in Quebec, trips interlocks throughout the US

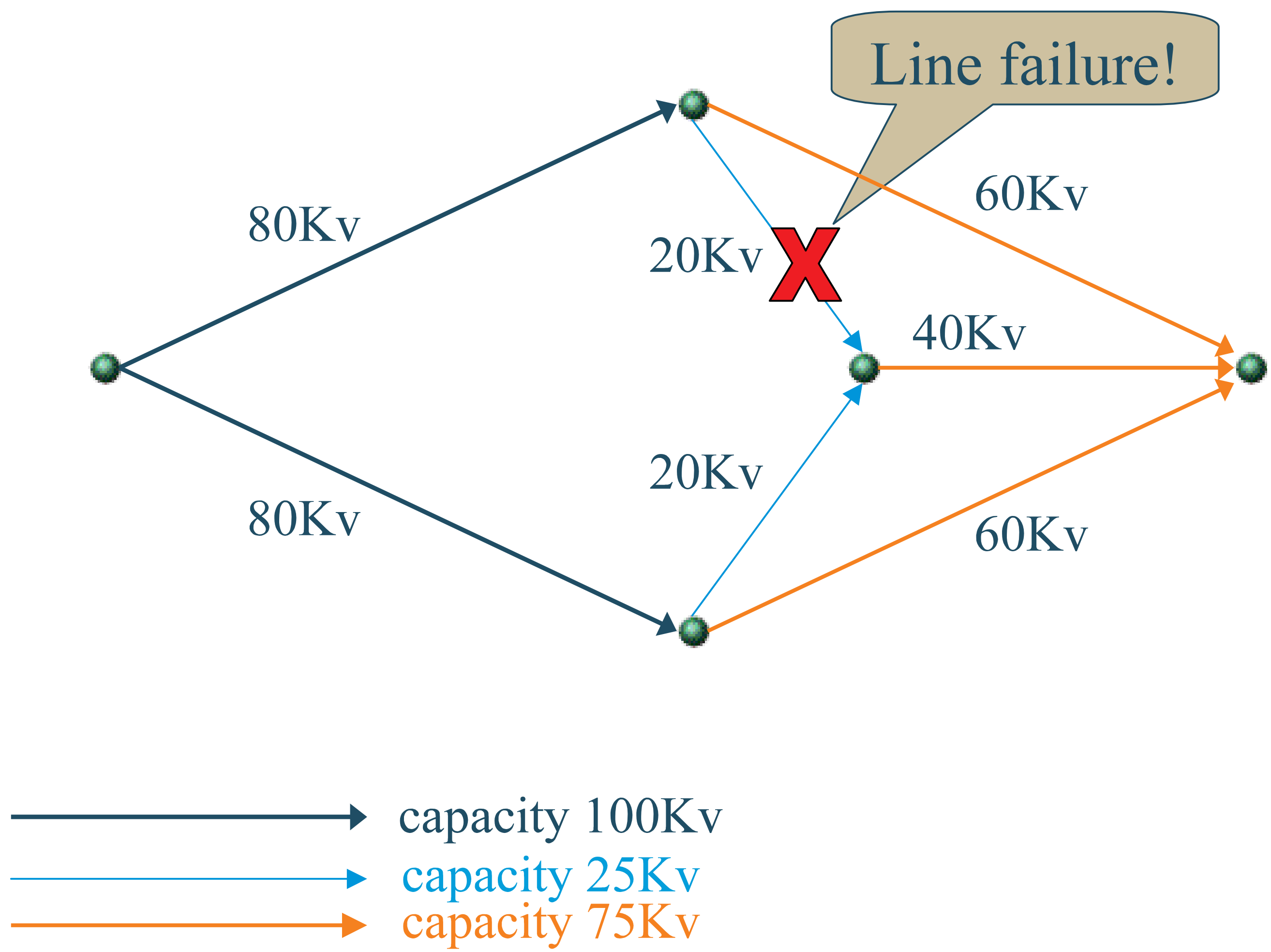
August 1996: Two faults in Oregon cause oscillations that lead to blackouts in 13 states

- Generation capacity margin at only 12% (down from 25% in 1980)
- Will get worse over next decade:
  demand grows 20%, transmission capacity grows 3% (projected)

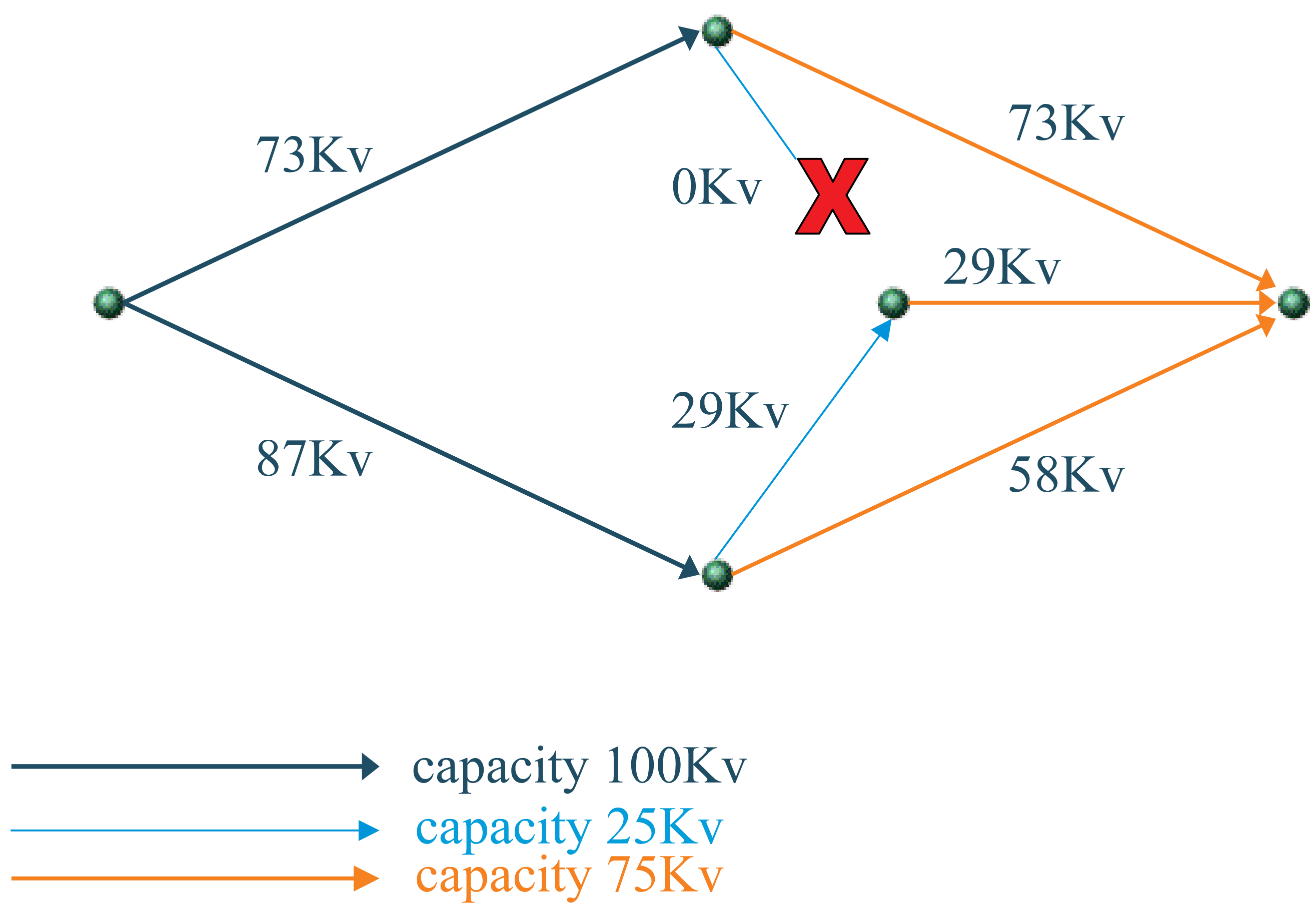
Transmission: An example?



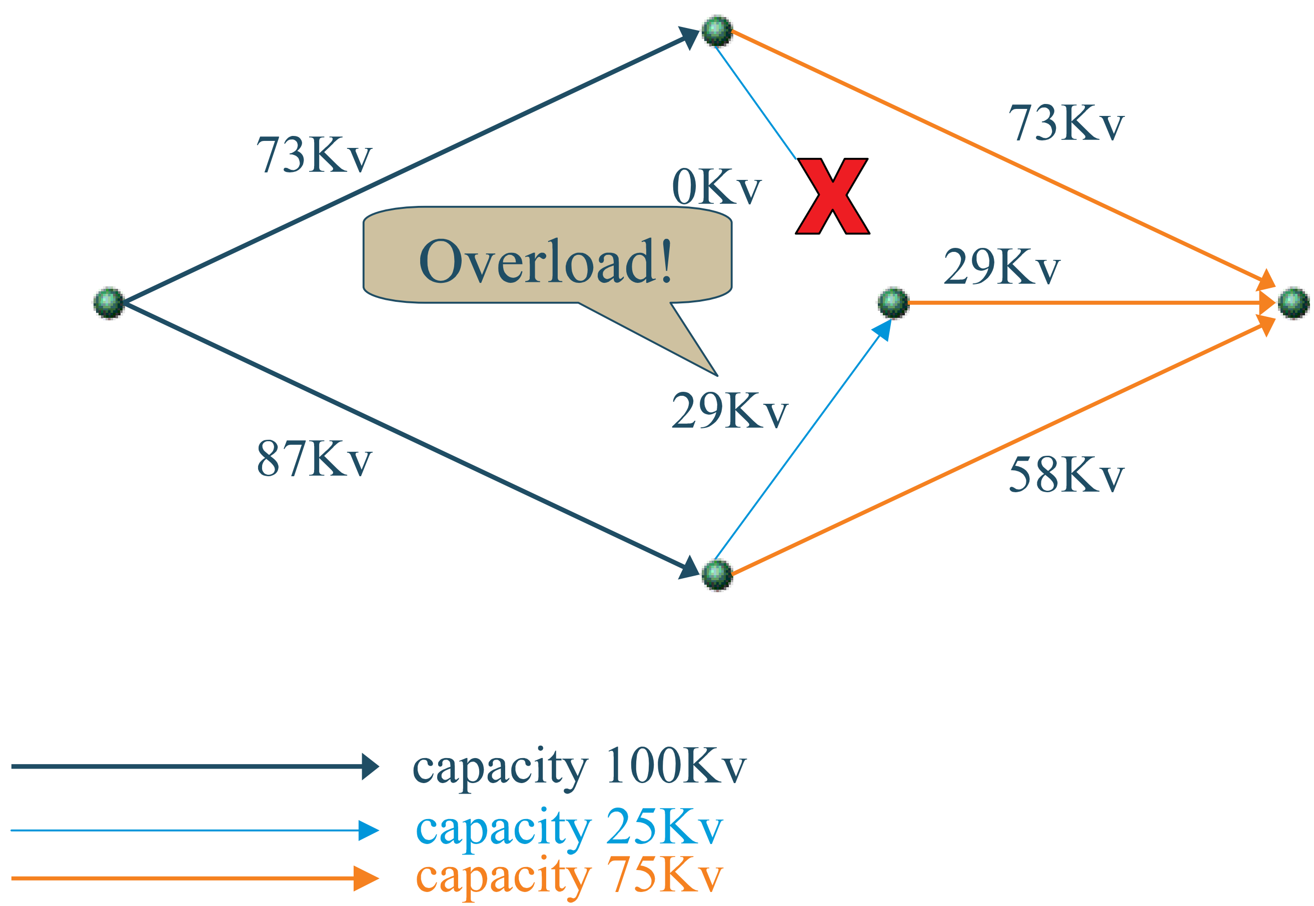
Transmission: An example?



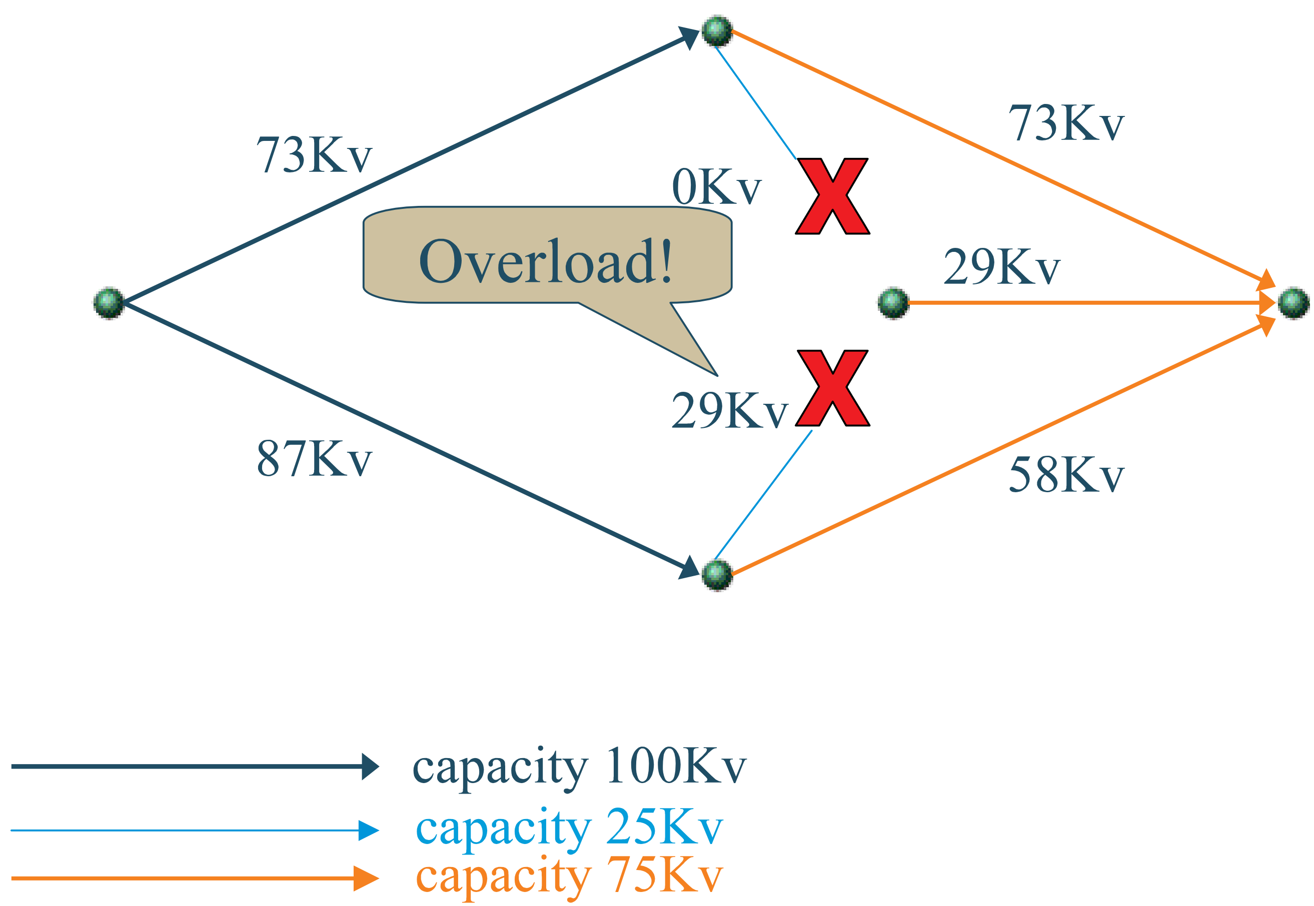
Transmission: An example?



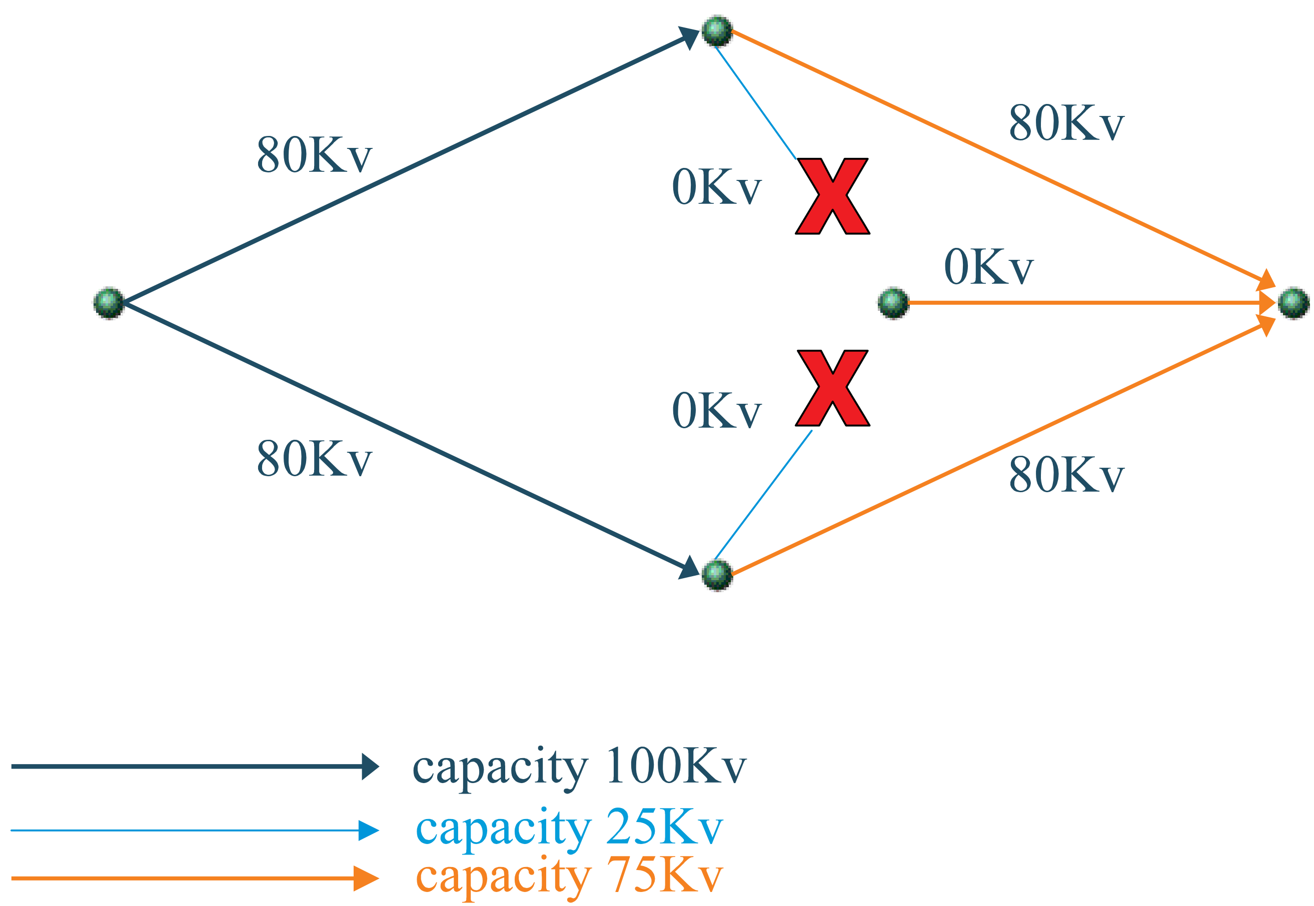
Transmission: An example?



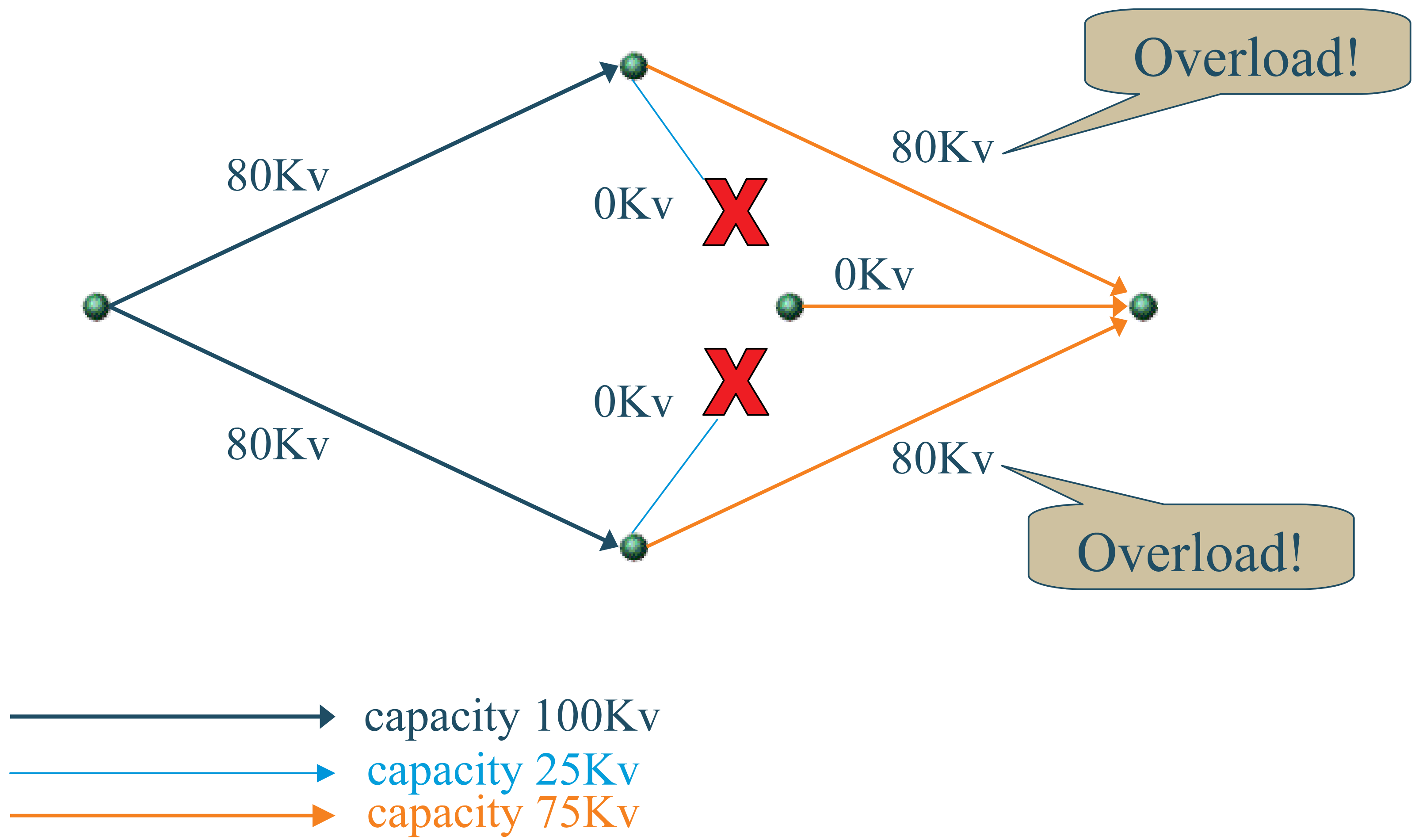
Transmission: An example?



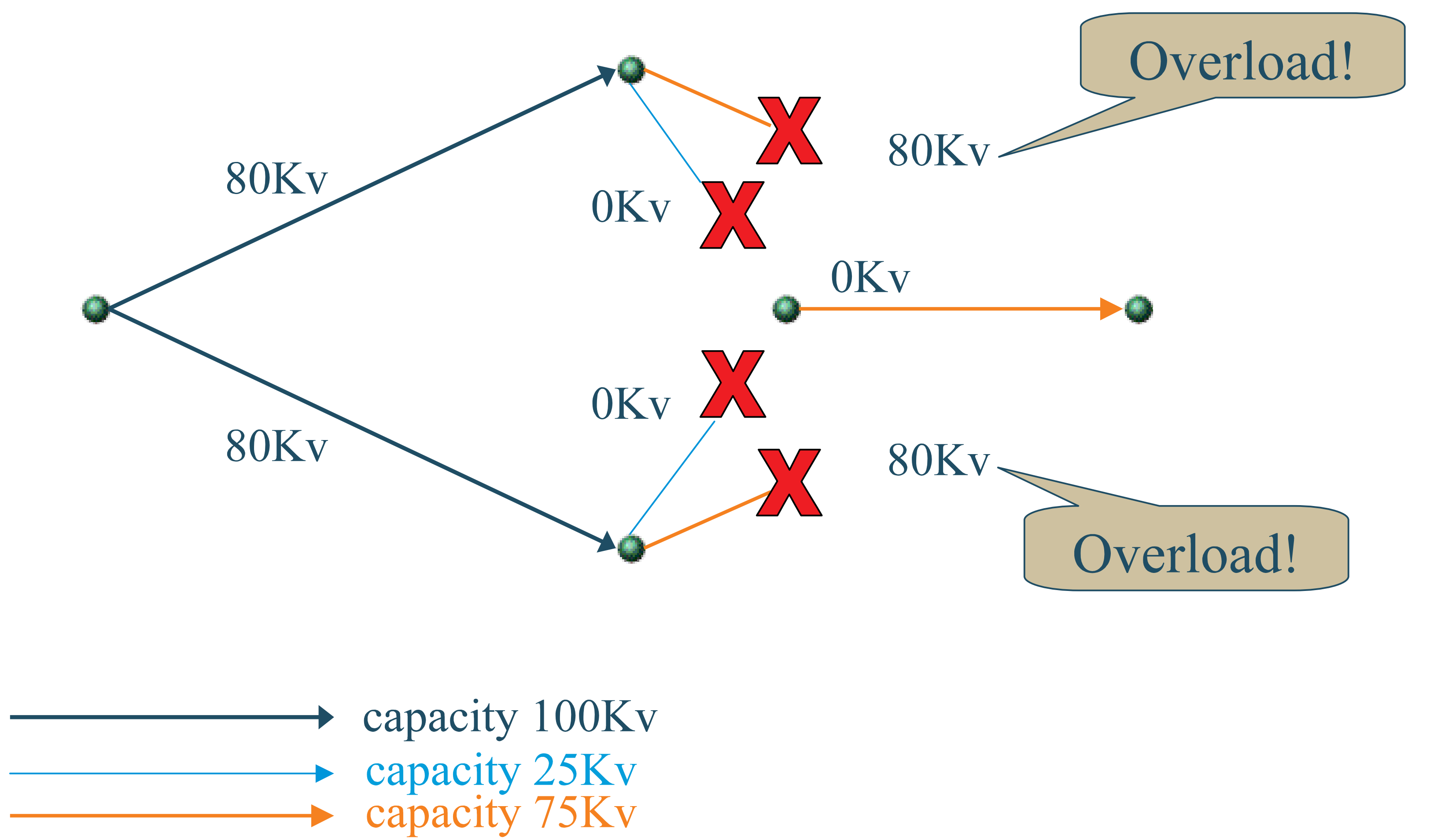
Transmission: An example?



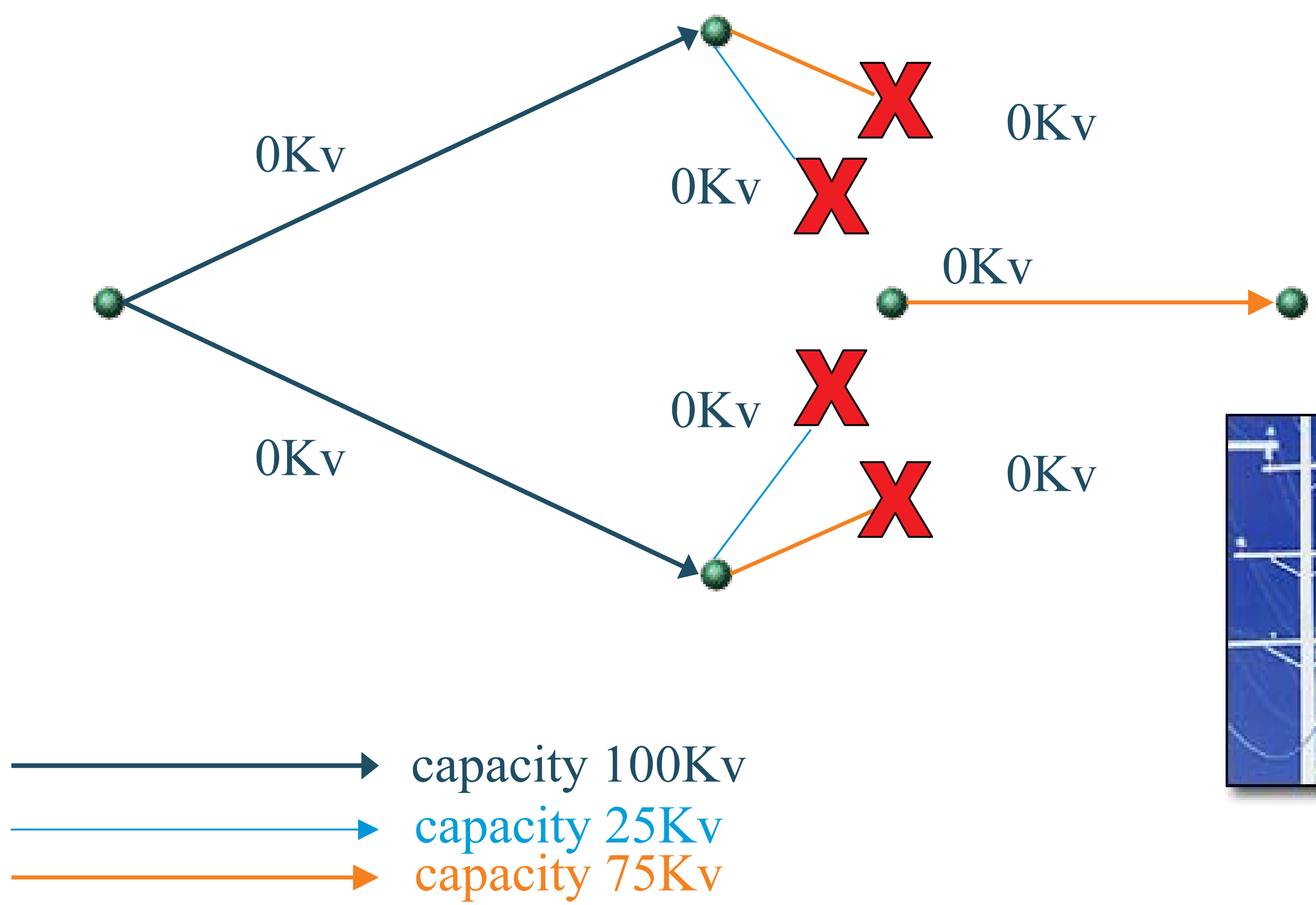
Transmission: An example?



Transmission: An example?



Transmission: An example?

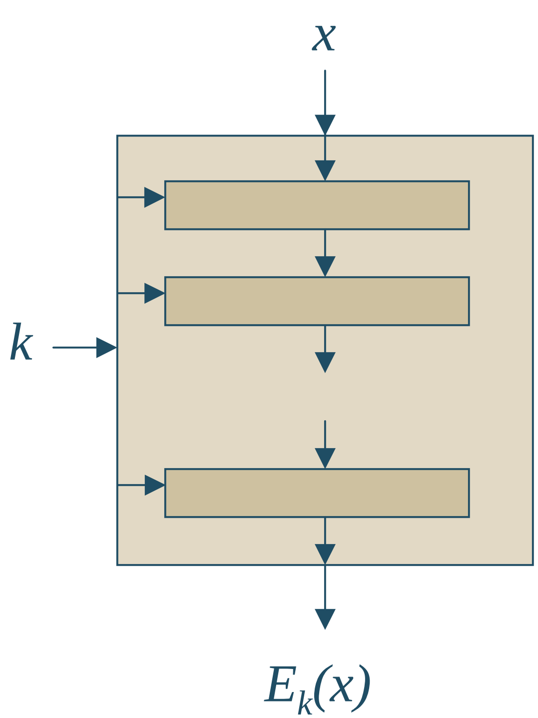


Possible research problems

- Modelling an infrastructural system
  - Can we construct a useful predictive model?
  - Given a model, can we efficiently measure its security against malicious attack?
- Structural properties of such systems
  - What key parameters determine their properties?
  - Are there local control rules that ensure global stability?
  - How can we design inherently self-stabilizing systems?

Part 2: Algebraic Crypto

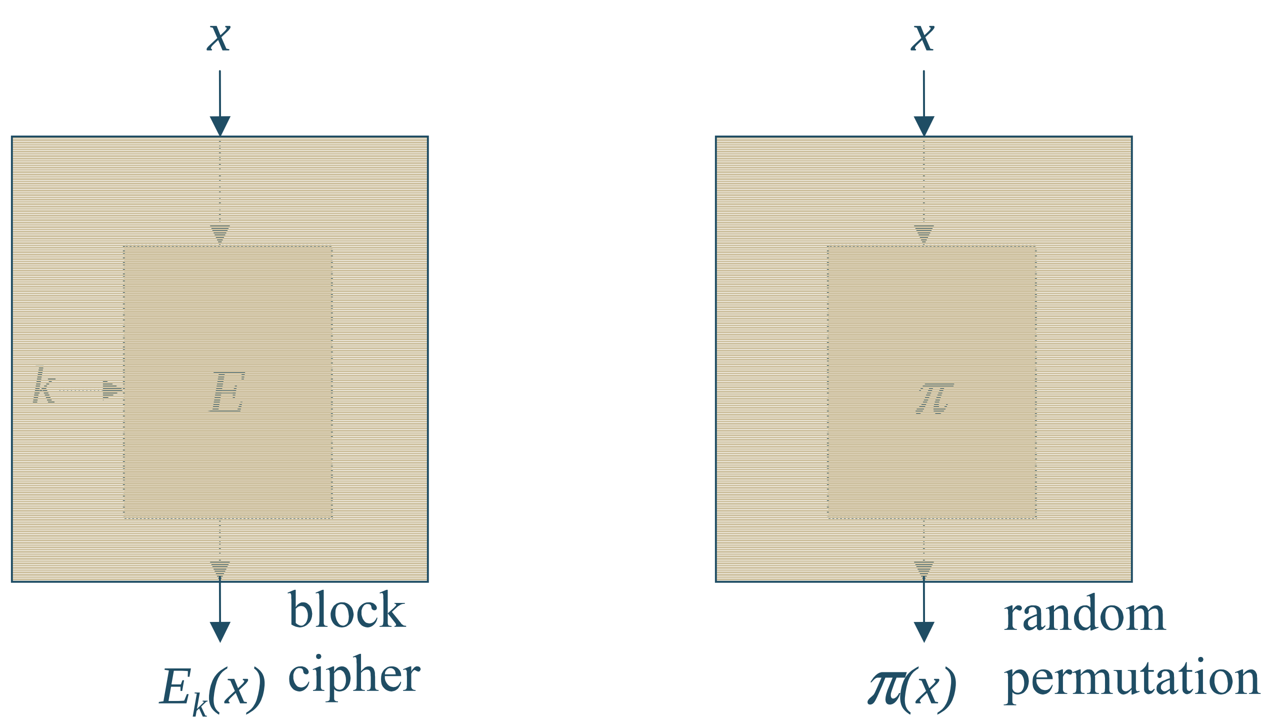
What's a block cipher?



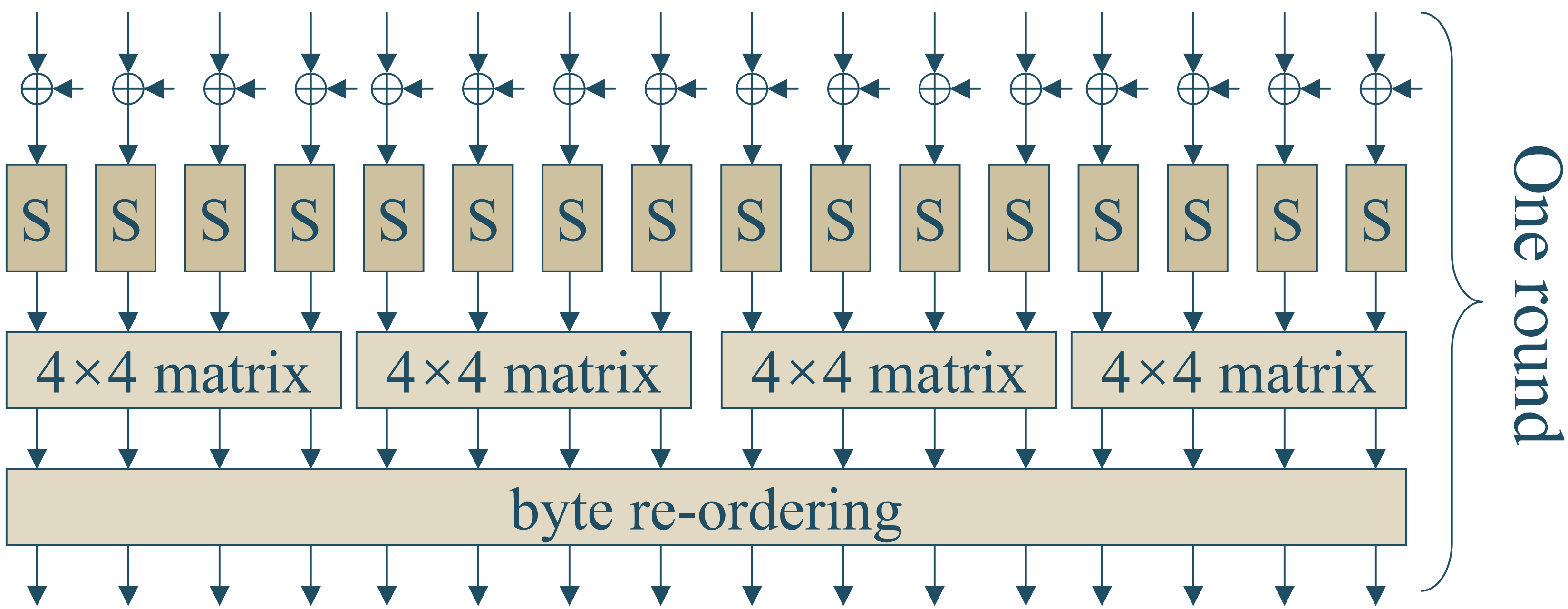
$E_k : X \rightarrow X$ bijective for all k

When is a block cipher secure?

Answer: when these two black boxes are indistinguishable.



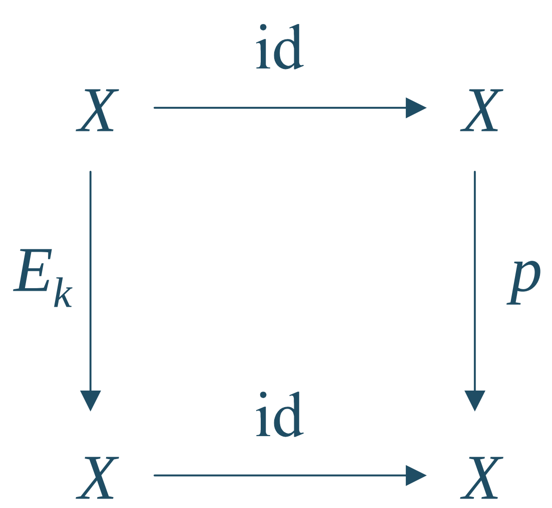
Example: The AES



$S(x) = l(x^{-1})$ in $GF(2^8)$, where l is $GF(2)$-linear
and the MDS matrix and byte re-ordering are $GF(2^8)$-linear

Interpolation attacks

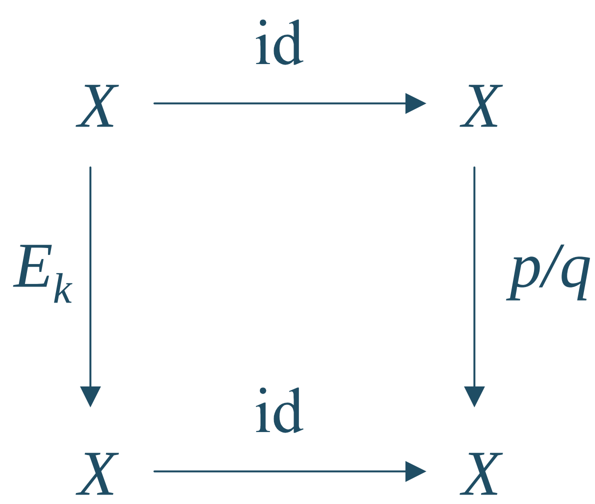
Express cipher as a polynomial in the message & key:



- Write $E_k(x) = p(x)$, then interpolate from known texts
  - Or, $p'(E_k(x)) = p(x)$
- Generalization: probabilistic interpolation attacks
  - Noisy polynomial reconstruction, decoding Reed-Muller codes

Rational interpolation attacks

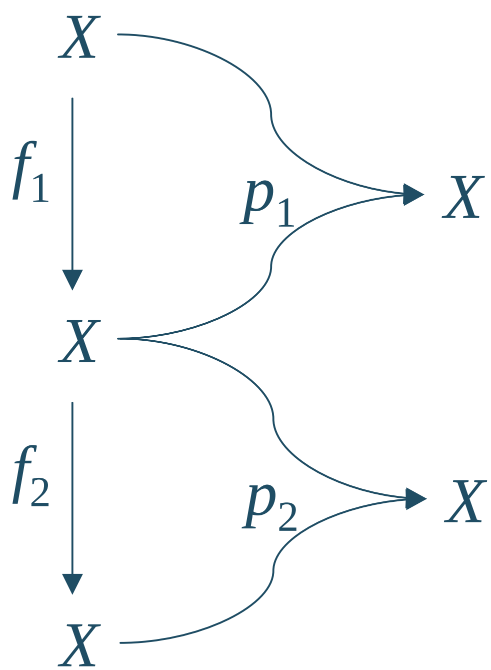
Express the cipher as a rational polynomial:



- If $E_k(x) = p(x)/q(x)$, then:
  - Write $E_k(x) \times q(x) = p(x)$, and apply linear algebra
  - Note: rational poly's are closed under composition
- Are probabilistic rational interpolation attacks feasible?

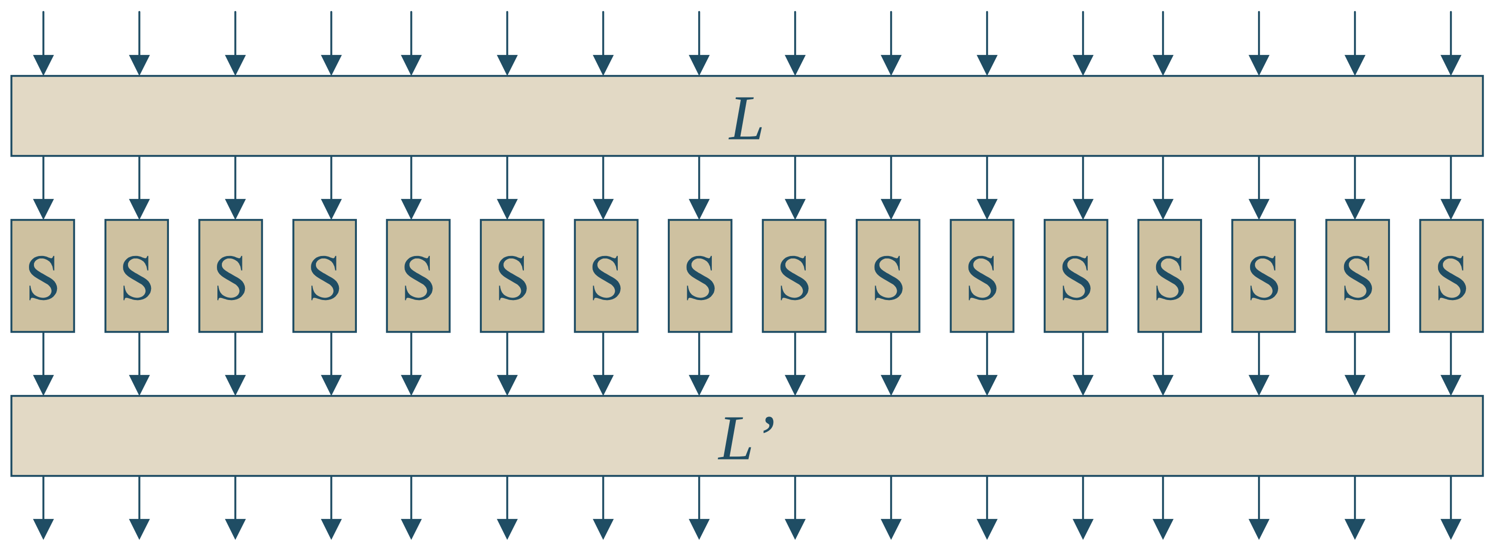
Resultants

A unifying view: bivariate polynomials:



- The small diagrams commute if $p_i(x, f_i(x)) = 0$ for all x
- Small diagrams can be composed to obtain $q(x, f_2(f_1(x))) = 0$, where $q(x,z) = \mathrm{res}_y(p_1(x,y), p_2(y,z))$
- Some details not worked out...

Public-key encryption



Let $S(x) = x^3$ in GF(2^8). Define $f = L' \circ S \circ L$.

Private key: L, L', a pair of GF(2^8)-linear maps

Public key: f, given explicitly by listing its coefficients

The MP problem

- Find semi-efficient algorithms for the following:
  - Let $f_1, \ldots, f_m$ be multivariate polynomials in n unknowns over a finite field K, and consider the system of equations
    $f_1(x_1, \ldots, x_n) = 0$
    …
    $f_m(x_1, \ldots, x_n) = 0$
  - Often: f_i are sparse, low degree, and $K = GF(2^q)$ for $q \leq 8$
  - Also, the case $m >> n$ is of special interest in crypto

What's known about MP?

- For quadratic equations (degree 2):
  - $m \geq n^2/2$: polynomial time via linearization
  - $m \geq \varepsilon n^2$: polynomial time via re-linearization, XL
  - $m \geq n^2 + c$: conjectured subexponential time via XL
  - $m = n$: hard? (NP-complete worst-case)

Why not existing Groebner base algorithms?
- exponential running time ($n >> 15$ is infeasible)
- not optimized for small fields

Summary

- Critical infrastructure protection
  - An important area, and
  - A source of intellectually satisfying problems
- Algebraic cryptosystems of growing importance
  - Collaboration between cryptographic and mathematical communities might prove fruitful here

Backup Slides

Power grid security

- Eligible Receiver (Nov 97): NSA hackers take down part of power grid, E911 in simulated attack using off-the-shelf software
- Zenith Star (Oct 99): little improvement
- Vulnerability assessments: control systems connected to Internet, dialup modems with poor passwords, using weak software