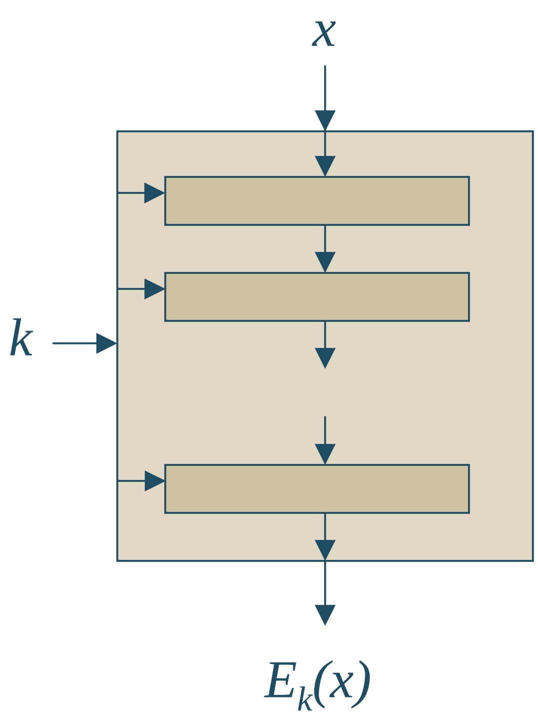
Analysis and design of symmetric ciphers

David Wagner
University of California, Berkeley

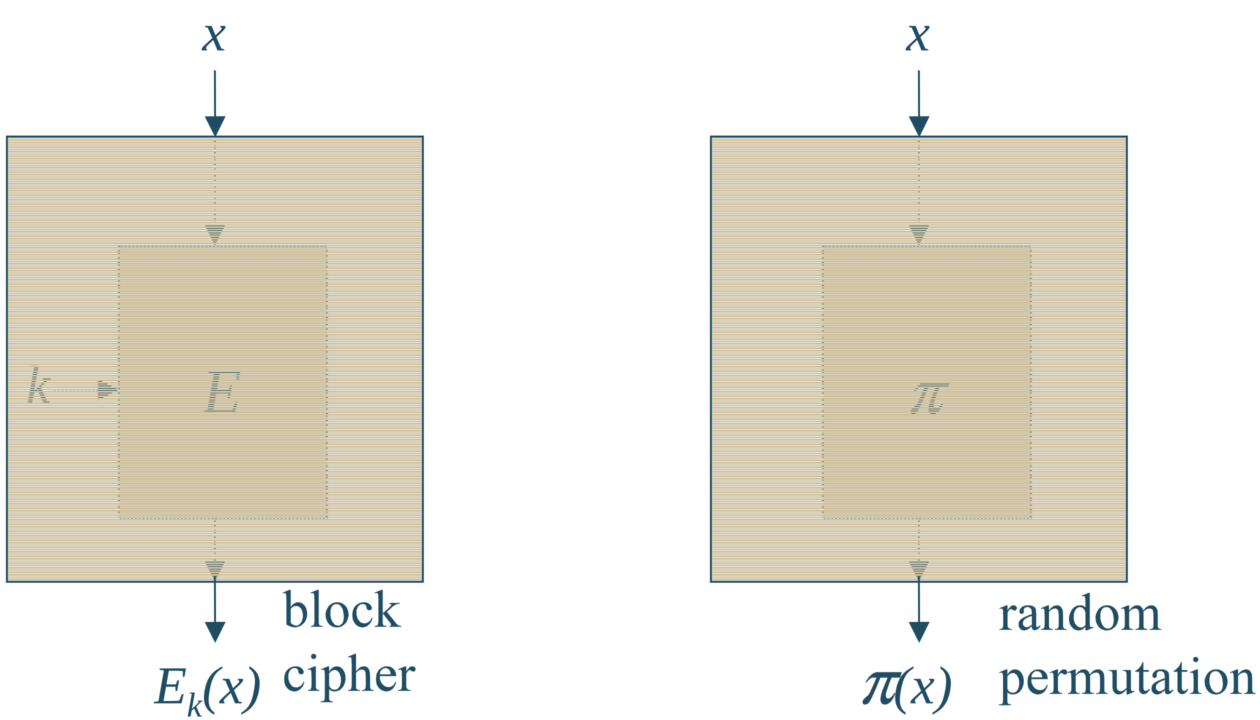
What's a block cipher?



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

When is a block cipher secure?

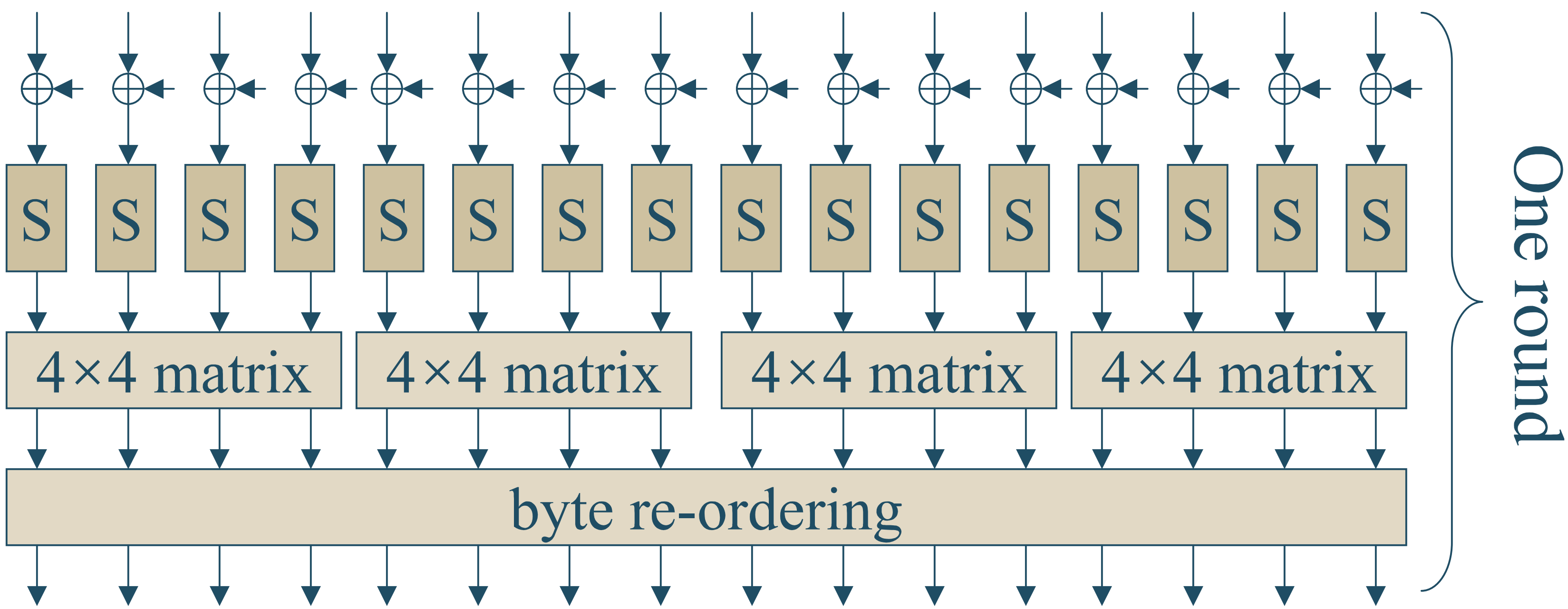
Answer: when these two black boxes are indistinguishable.



$E_k(x)$ block cipher

$\pi(x)$ random permutation

Example: The AES



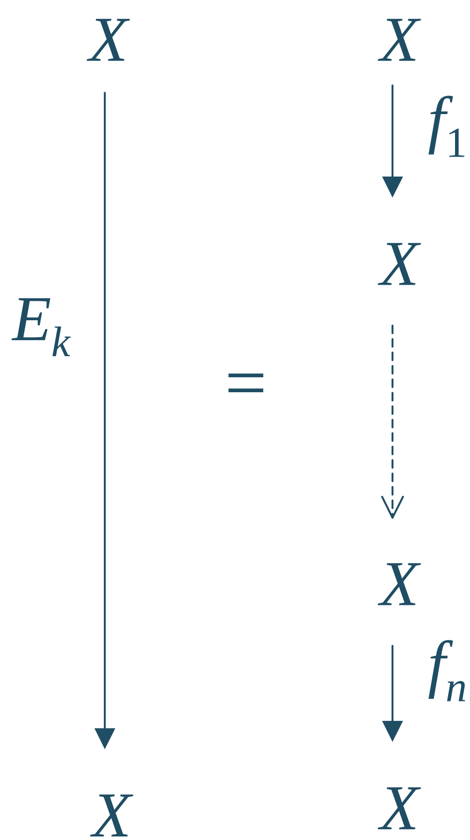
$S(x) = l(l'(x)^{-1})$ in GF(2^8), where l,l' are GF(2)-linear and the MDS matrix and byte re-ordering are GF(2^8)-linear

In this talk:

How do we tell if a block cipher is secure? How do we design good ones?

- Survey of cryptanalysis of block ciphers
- Steps towards a unifying view of this field
- Algebraic attacks

How to attack a product cipher



1. Identify local properties of its round functions

2. Piece these together into global properties of the whole cipher

Motif #1: projection

Identify local properties using *commutative diagrams:*

$$\begin{array}{ccc} X & \xrightarrow{\rho} & Y \\ \downarrow{\scriptstyle f_k} & & \downarrow{\scriptstyle g_{k'}} \\ X & \xrightarrow{\rho'} & Y \end{array}$$

where:

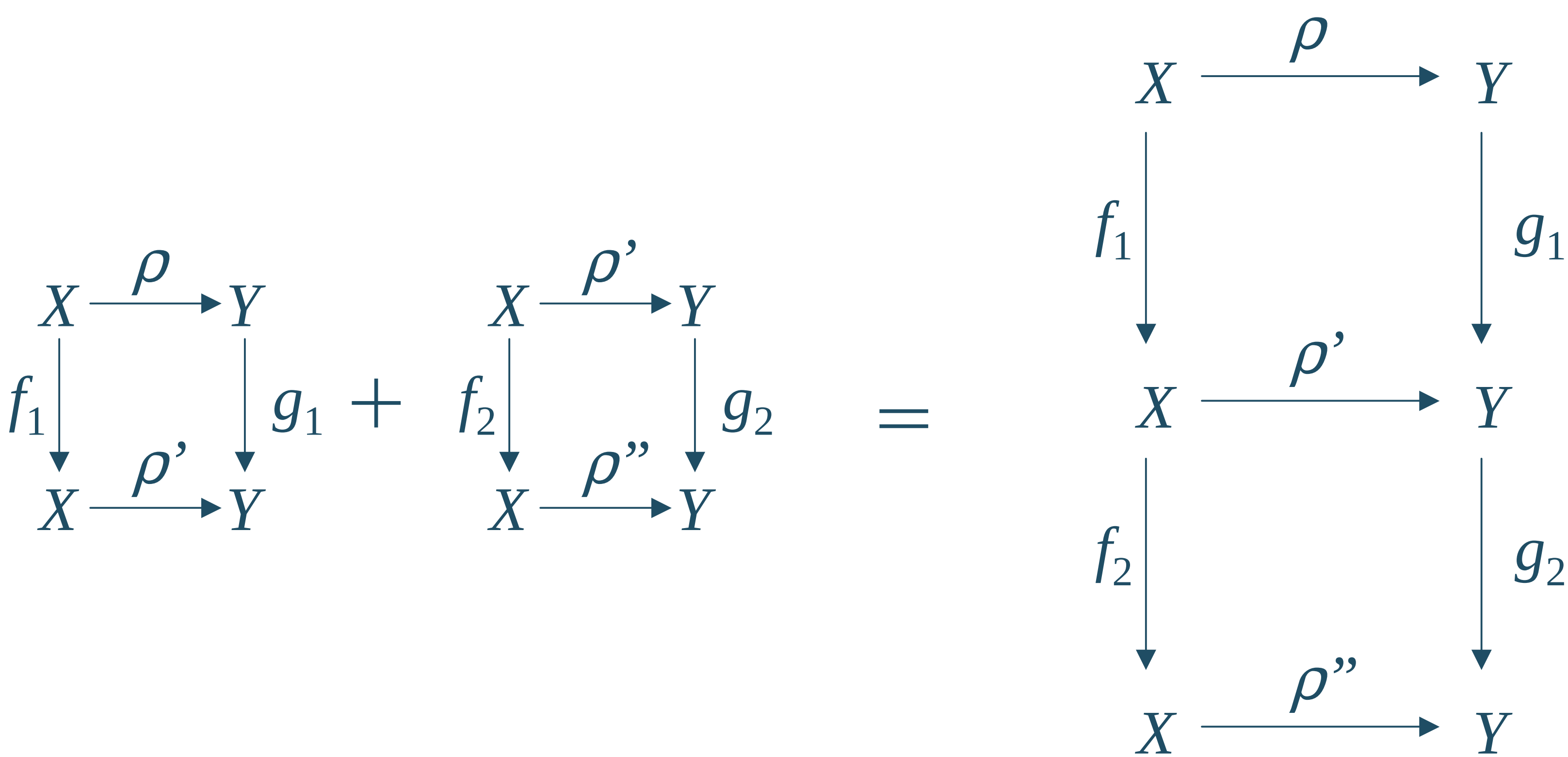
f_k = original round function
$g_{k'}$ = reduced round function

and:

$g_{k'} \circ \rho = \rho' \circ f_k$

Concatenating local properties

Build global commutative diagrams out of local ones:



Exploiting global properties

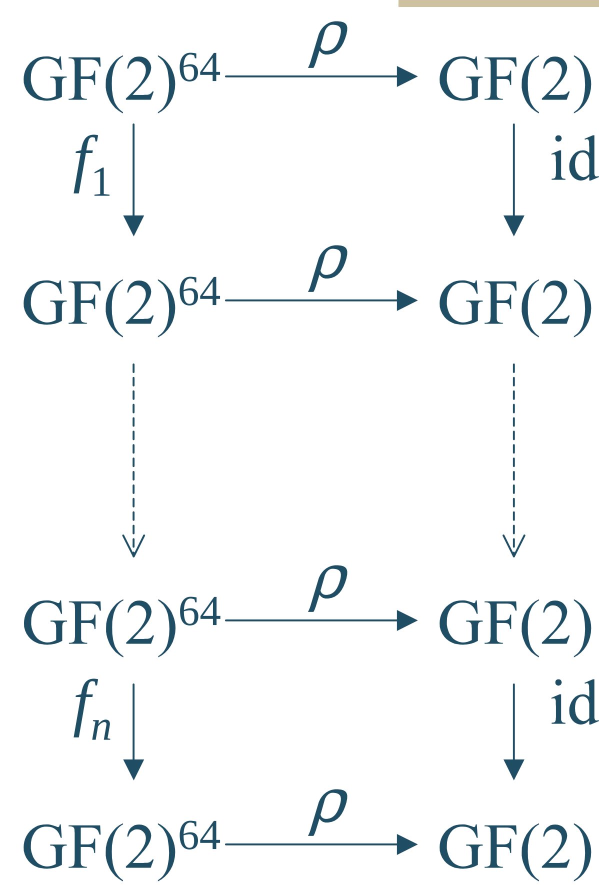
Use global properties to build a known-text attack:

$$
\begin{array}{ccc}
X & \xrightarrow{\rho} & Y \\
\downarrow{E_k} & & \downarrow{g} \\
X & \xrightarrow{\rho'} & Y
\end{array}
$$

- The distinguisher:
  - Let (x, y) be a plaintext/ciphertext pair
  - If $g(\rho(x)) = \rho'(y)$, it's probably from E_k
  - Otherwise, it's from π

Example: linearity in Madryga

- Madryga leaves parity unchanged
  - Let $\rho(x)$ = parity of x
  - We see $\rho(E_k(x)) = \rho(x)$
- This yields a distinguisher
  - $\Pr[\rho(\pi(x)) = \rho(x)] = ½$
  - $\Pr[\rho(E_k(x)) = \rho(x)] = 1$



Motif #2: statistics

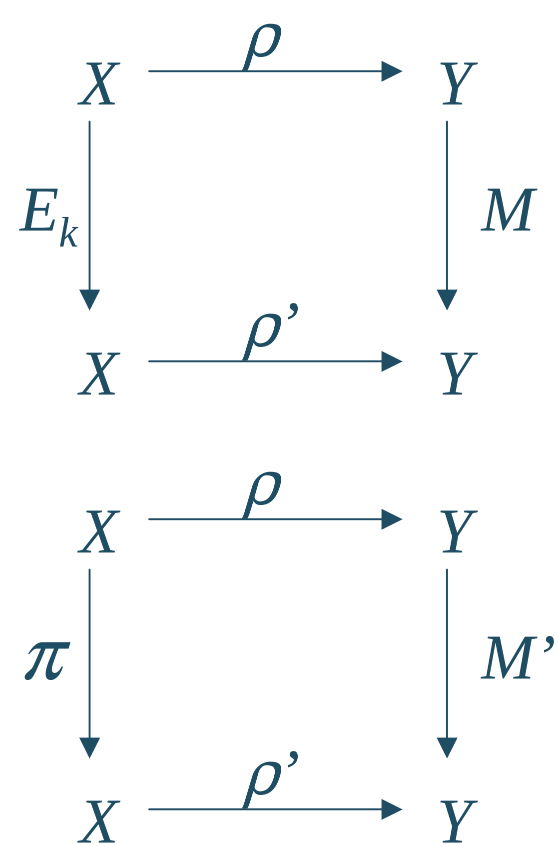
- Suffices to find a property that holds with large enough probability
- Maybe probabilistic commutative diagrams?

$$\begin{array}{ccc} X & \xrightarrow{\rho} & Y \\ {\scriptstyle E_k}\downarrow & \text{Prob. } p & \downarrow{\scriptstyle g} \\ X & \xrightarrow{\rho'} & Y \end{array}$$

where $p = \Pr[\rho'(E_k(x)) = g(\rho(x))]$

A better formulation?

- Stochastic comm. diagrams
  - E_k , ρ, ρ' induce a stochastic process M (hopefully Markov); π, ρ, ρ' yield M'
  - Pick a distance measure $d(M, M')$, say $1/||M(x) - M'(x)||^2$ where the r.v. x is uniform on X
  - Then $d(M,M')$ known texts suffice to distinguish E_k from π



Example: Linear cryptanalysis

- Matsui's linear cryptanalysis
  - Set $X = GF(2)^{64}$, $Y = GF(2)$
  - Cryptanalyst chooses linear maps ρ, ρ' cleverly to make $d(M,M')$ as small as possible
  - Then M is a 2×2 matrix of the form shown here, and $1/\varepsilon^2$ known texts break the cipher

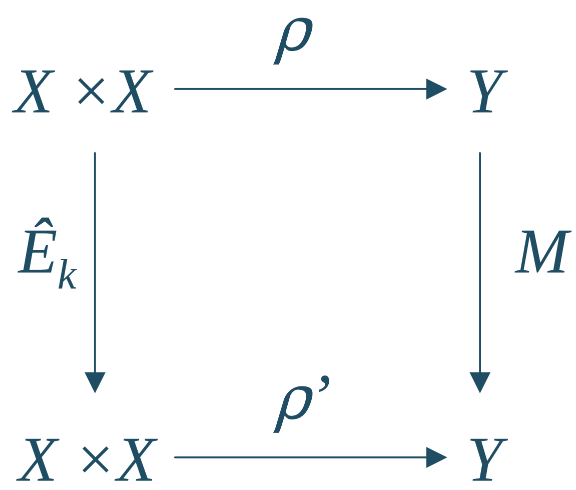
$$\begin{array}{ccc} X & \xrightarrow{\rho} & Y \\ \downarrow E_k & & \downarrow M \\ X & \xrightarrow{\rho'} & Y \end{array}$$

$$M = \begin{bmatrix} \frac{1}{2}+\varepsilon & \frac{1}{2}-\varepsilon \\ \frac{1}{2}-\varepsilon & \frac{1}{2}+\varepsilon \end{bmatrix}$$

and $d(M, M') = 1/\varepsilon^2$

Motif #3: higher-order attacks

Use many encryptions to find better properties:



- Here we've defined $\hat{E}_k(x,x') = (E_k(x), E_k(x'))$

Example: Complementation

Complementation properties are a simple example:

$$\begin{array}{ccc} X \times X & \xrightarrow{\rho} & X \\ \downarrow \hat{E}_k & & \downarrow M \\ X \times X & \xrightarrow{\rho} & X \end{array}$$

- Take $\rho(x,x') = x' - x$
- Suppose $M(\Delta,\Delta) = 1$ for some cleverly chosen Δ
- Then we obtain a complementation property
  - Exploit with chosen texts

Example: Differential crypt.

Differential cryptanalysis:

$$\begin{array}{ccc} X \times X & \xrightarrow{\rho} & X \\ \downarrow \hat{E}_k & & \downarrow M \\ X \times X & \xrightarrow{\rho} & X \end{array}$$

- Set $X = \mathrm{GF}(2)^n$, and take $\rho(x,x') = x' - x$
- If $p = M(\Delta,\Delta') \gg 0$ for some clever choice of Δ, Δ':
  - can distinguish with $2/p$ chosen plaintexts

Example: Impossible diff.'s

Impossible differential cryptanalysis:

$$\begin{array}{ccc} X \times X & \xrightarrow{\rho} & X \\ \downarrow \hat{E}_k & & \downarrow M \\ X \times X & \xrightarrow{\rho} & X \end{array}$$

- Set $X = \mathrm{GF}(2)^n$, and take $\rho(x,x') = x' - x$
- If $M(\Delta,\Delta') = 0$ for some clever choice of Δ, Δ':
  - can distinguish with $2/M'(\Delta,\Delta')$ known texts

Example: Truncated diff. crypt.

Truncated differential cryptanalysis:

$$\begin{array}{ccc} X \times X & \xrightarrow{\rho_1} & Y \\ \downarrow \hat{E}_k & & \downarrow M \\ X \times X & \xrightarrow{\rho_2} & Y \end{array}$$

- Set $X = \mathrm{GF}(2)^n$, $Y = \mathrm{GF}(2)^m$, cleverly choose linear maps $\varphi_1, \varphi_2 : X \longrightarrow Y$, and take $\rho_i(x,x') = \varphi_i(x' - x)$
- If $M(\Delta,\Delta') \gg 0$ for some clever choice of Δ, Δ', we can distinguish

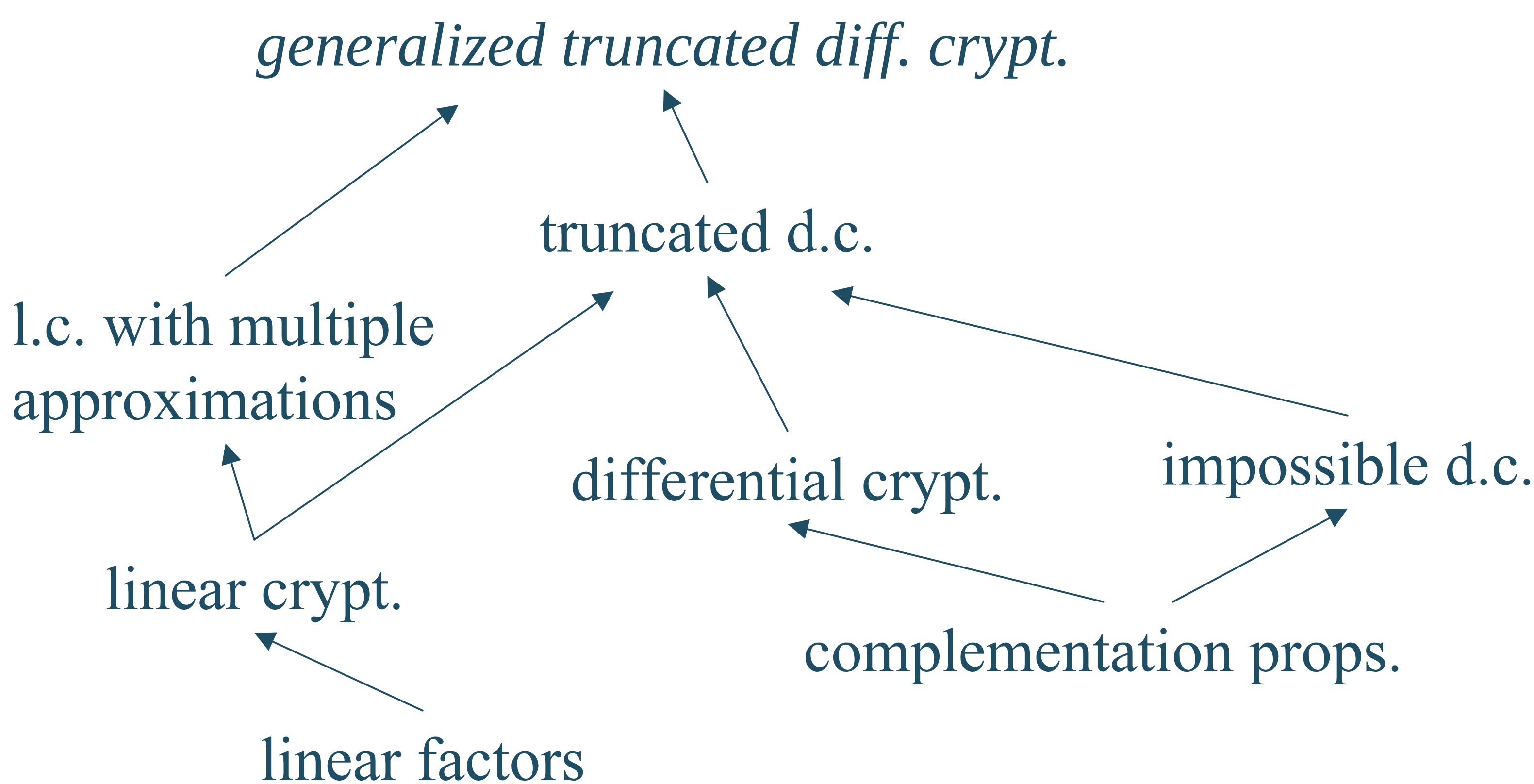
Generalized truncated d.c.

Generalized truncated differential cryptanalysis:

$$\begin{array}{ccc} X \times X & \xrightarrow{\rho_1} & Y_1 \\ \downarrow \hat{E}_k & & \downarrow M \\ X \times X & \xrightarrow{\rho_2} & Y_2 \end{array}$$

- Take X, Y_i, ρ_i as before; then $\varepsilon = \max_x \|M(x) - M'(x)\|$ measures the distinguishing power of the attack
- Generalizes the other attacks

The attacks, compared



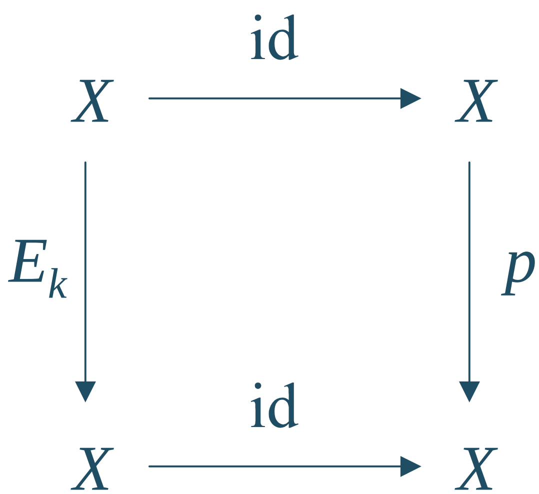
Summary (1)

- A few leitmotifs generate many known attacks
  - Many other attack methods can also be viewed this way (higher-order d.c., slide attacks, mod n attacks, d.c. over other groups, diff.-linear attacks, algebraic attacks, etc.)
  - Are there other powerful attacks in this space?
    Can we prove security against all commutative diagram attacks?
- We're primarily exploiting linearities in ciphers
  - E.g., the closure properties of $GL(Y, Y) \subset Perm(X)$
  - Are there other subgroups with useful closure properties?
    Are there interesting "non-linear" attacks?
    Can we prove security against all "linear" comm. diagram attacks?

Part 2: Algebraic attacks

Example: Interpolation attacks

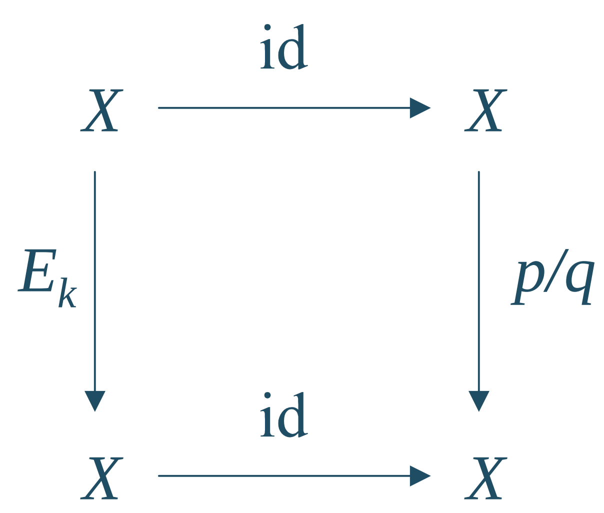
Express cipher as a polynomial in the message & key:



- 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

Example: Rational inter. attacks

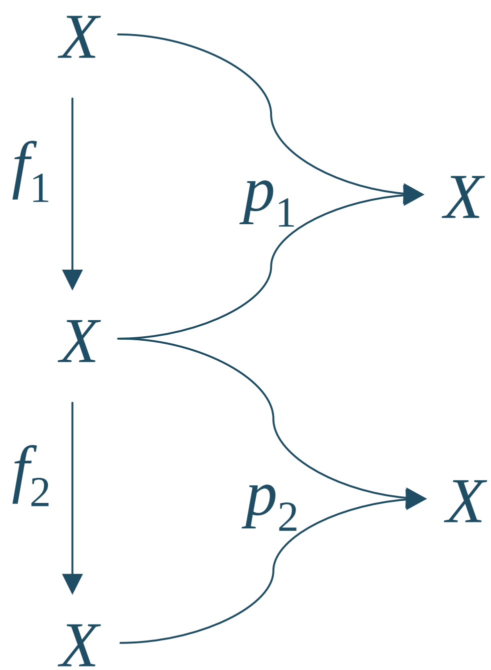
Express the cipher as a rational polynomial:



- 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?

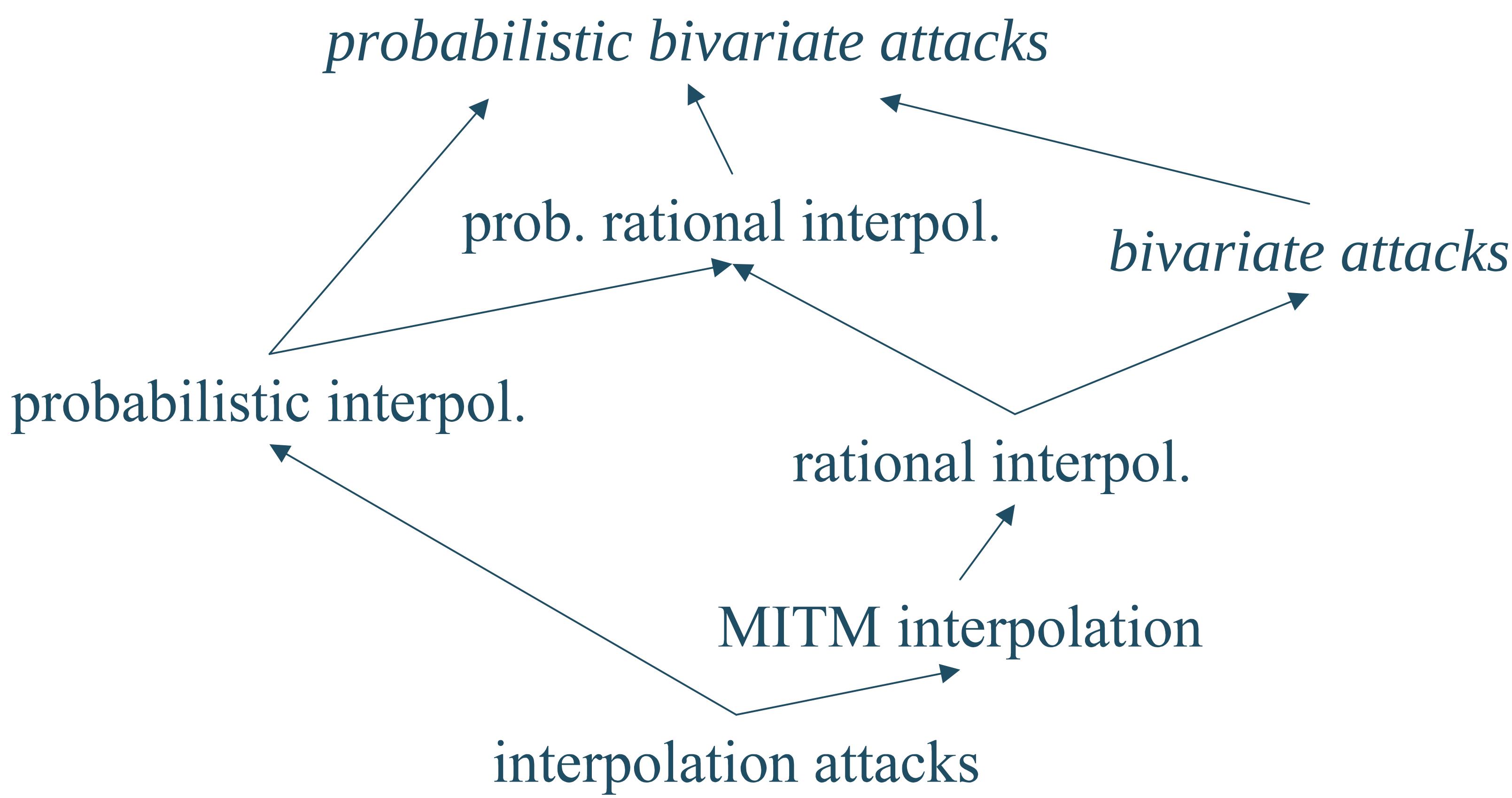
A generalization: resultants

A possible direction: 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...

Algebraic attacks, compared



Summary

- Many cryptanalytic methods can be understood using only a few basic ideas
  - Commutative diagrams as a unifying theme?
- Algebraic attacks of growing importance
  - Collaboration between cryptographic and mathematical communities might prove fruitful here