Towards a unifying view of block cipher cryptanalysis

David Wagner

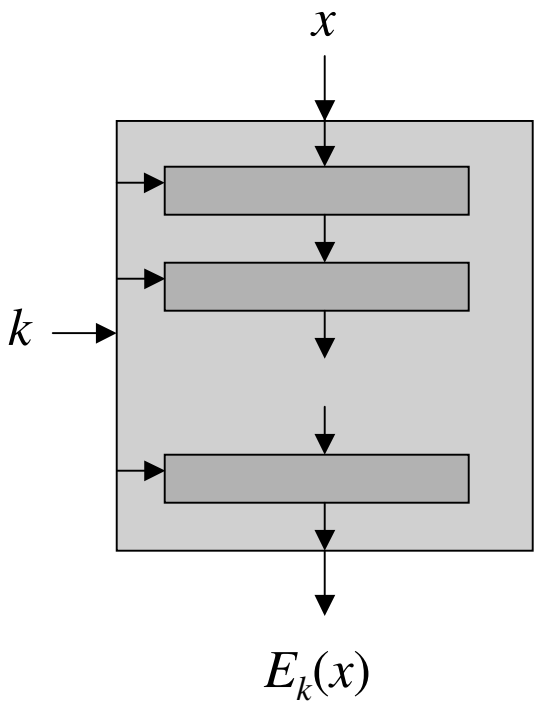
University of California, Berkeley

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

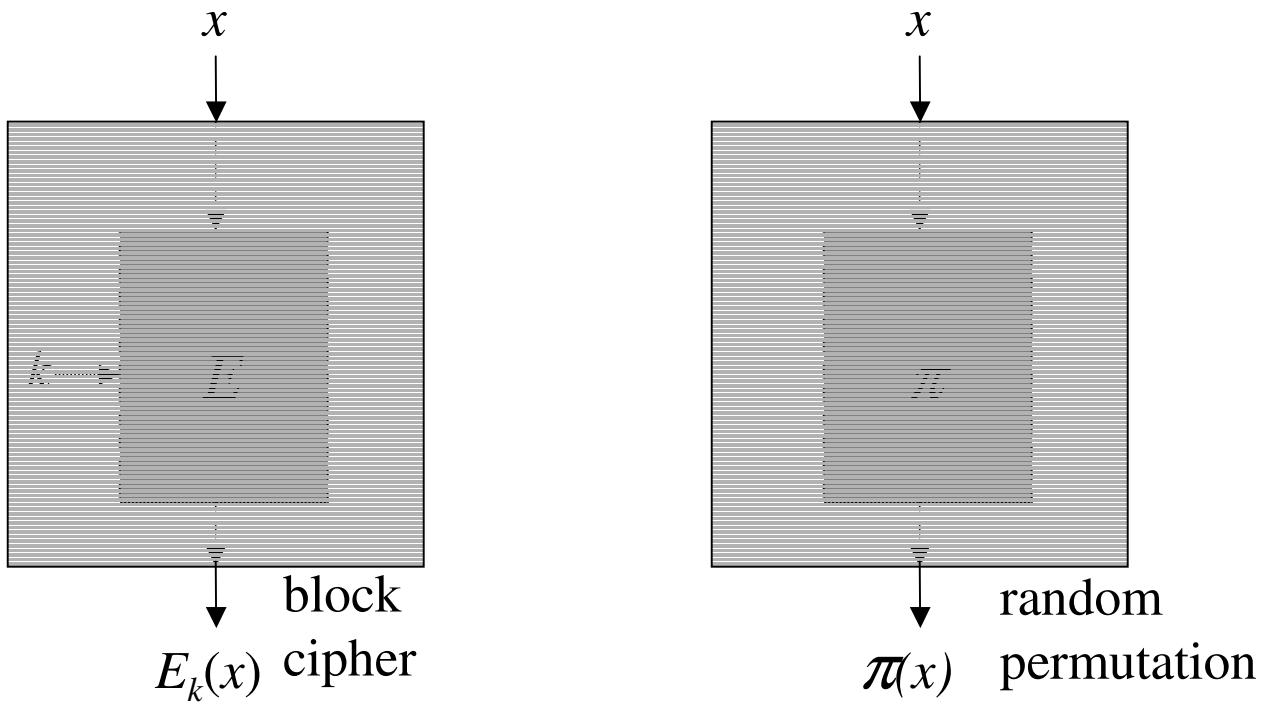
What's a block cipher?



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

When is a block cipher secure?

Answer: when these two black boxes are indistinguishable.



So many cryptanalytic attacks…

prob. rational interpol.

higher-order d.c.

probabilistic interpol.

yo-yo

rational interpol.

boomerang

integrals

MITM interpolation

interpolation attacks

sliding

truncated d.c.

How do we unify them?

l.c. with multiple approximations

differential crypt.

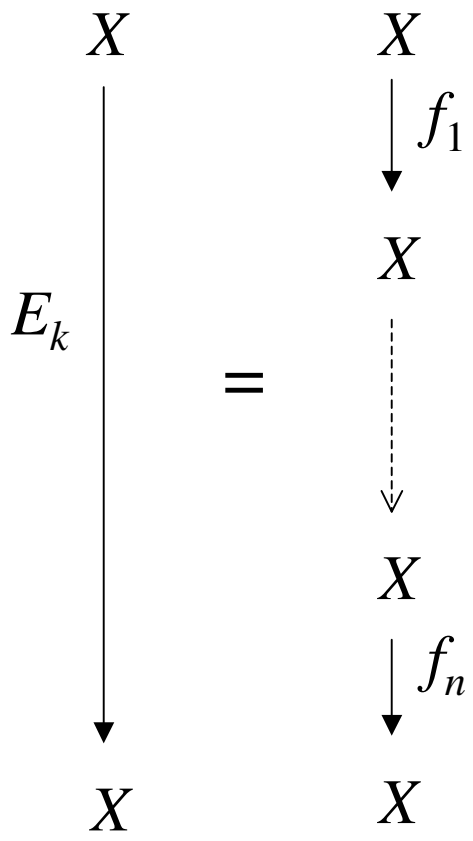
impossible d.c.

linear crypt.

complementation props.

linear factors

How to attack a product cipher

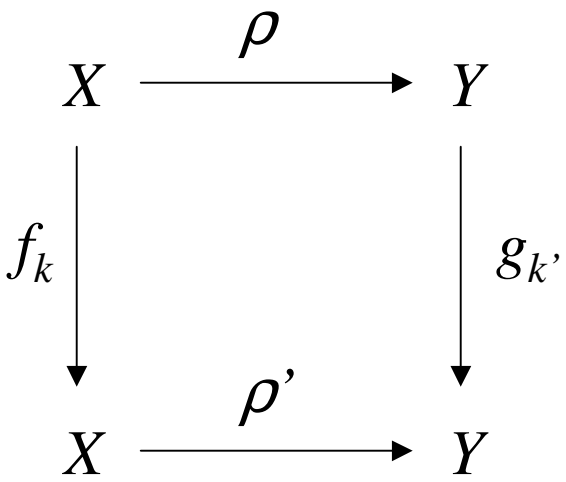


1. Identify local properties of its round functions

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

Motif #1: projection

Identify local properties using *commutative diagrams:*



where:

f_k = original round function

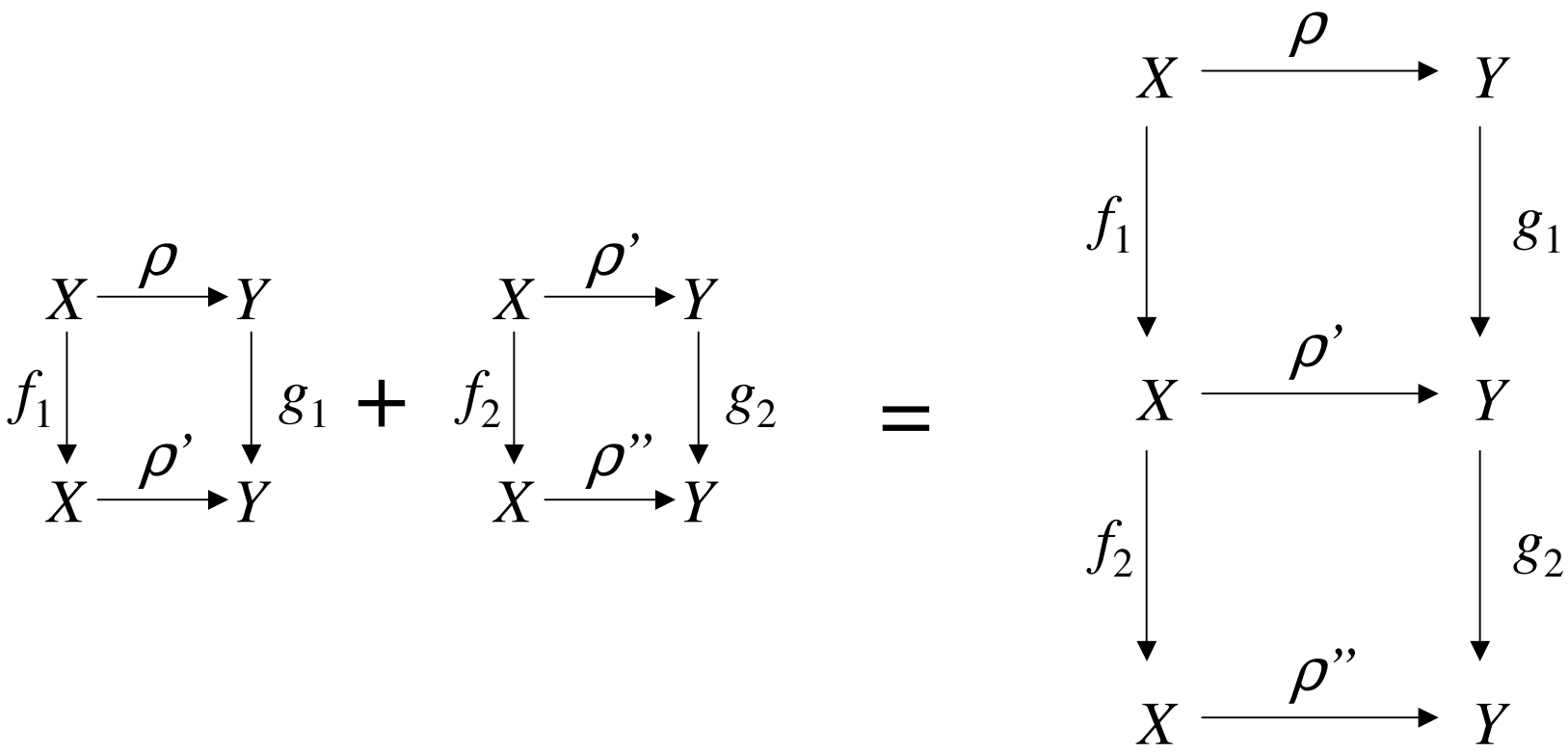
$g_{k'}$ = reduced round function

and:

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

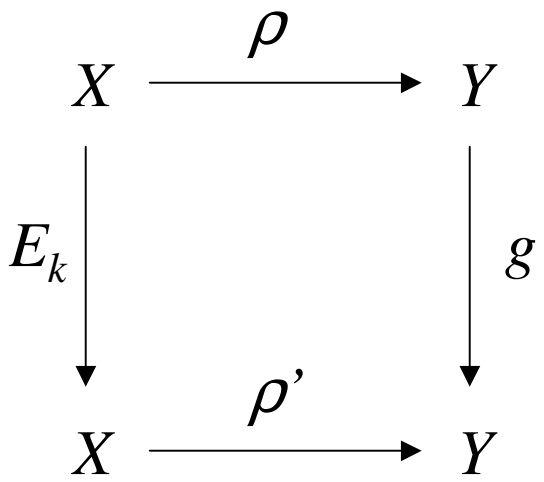
Composing local properties

Build global commutative diagrams out of local ones:



Exploiting global properties

Use global properties to build a known-text attack:

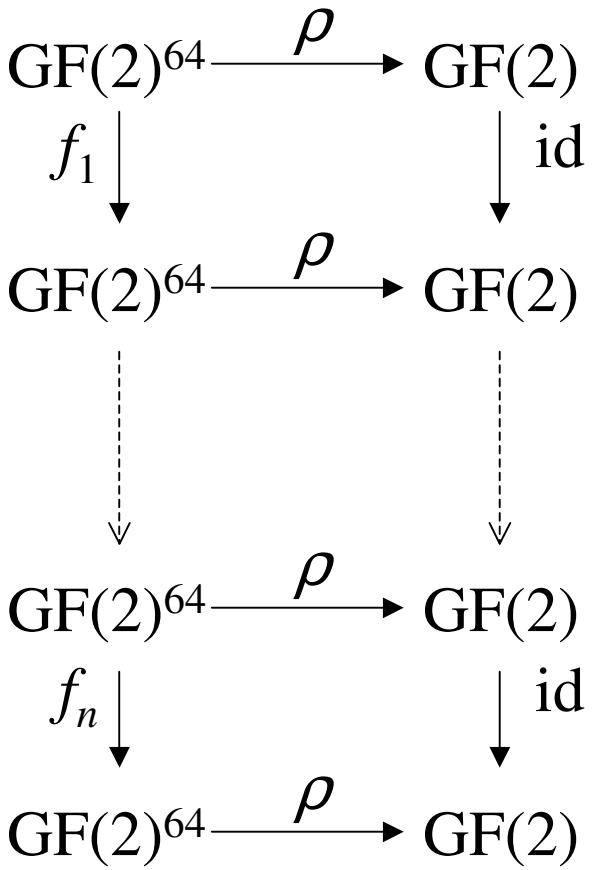


The distinguisher:

- 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

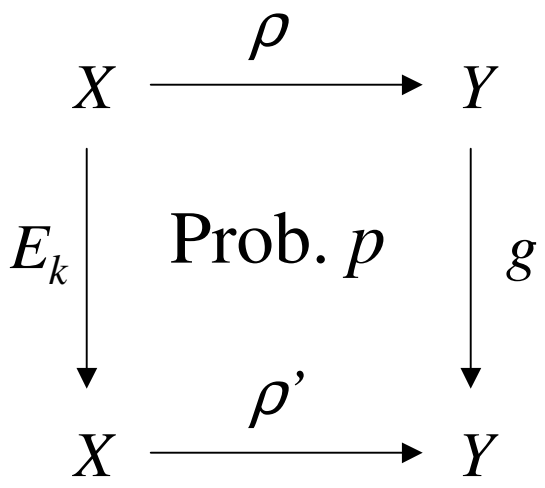
Example: linearity in Madryga

- 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
- A first attempt: probabilistic commutative diagrams?
  - Turns out to be too weak

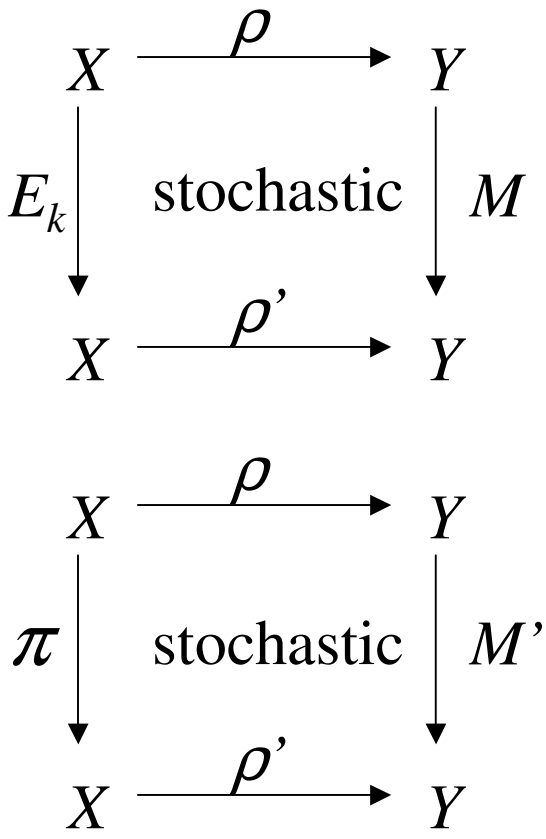


where $p = \Pr[\rho(E_k(x)) = g(\rho(x))]$

A more general formulation: Markov processes

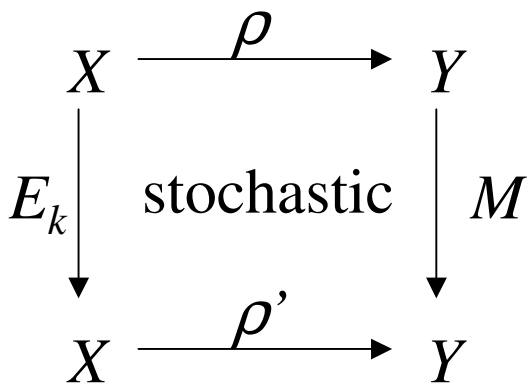
Stochastic commutative diagrams:

- E_k , ρ, ρ' induce a Markov process M, $M(i,j) = \Pr[\rho'(E_k(x)) = j \mid \rho(x) = i]$
- π, ρ, ρ' induce M'
- Pick a distance measure, e.g., $d(M, M') = \|M - M'\|_\infty$
- Best distinguisher of E_k from π has advantage $0.5\ \|M - M'\|_\infty$ [Vaudenay]
- Also, ~ $1/(\|M - M'\|_\infty)^2$ known texts suffice for a distinguishing attack



Example: Linear cryptanalysis

- Matsui's linear cryptanalysis
  - Set $X = \mathrm{GF}(2)^{64}$, $Y = \mathrm{GF}(2)$
  - Cryptanalyst chooses linear maps ρ, ρ' cleverly to make $\|M - M'\|_\infty$ as large as possible
  - Note: M is a 2×2 matrix of the form shown to the right, and $1/\varepsilon^2$ known texts break the cipher

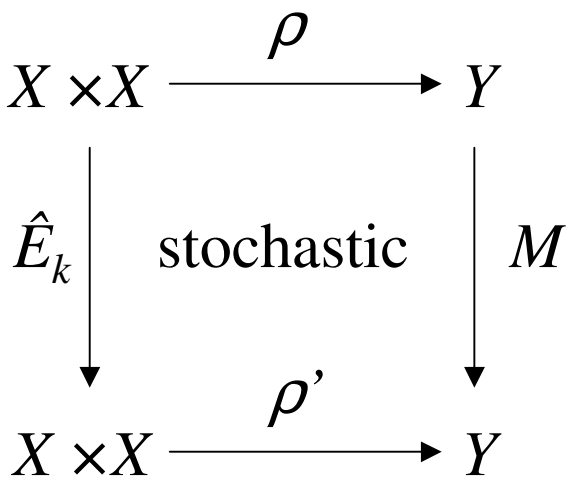


$$M = \begin{bmatrix} \tfrac{1}{2}+\varepsilon & \tfrac{1}{2}-\varepsilon \\ \tfrac{1}{2}-\varepsilon & \tfrac{1}{2}+\varepsilon \end{bmatrix}$$

and $\|M - M'\|_\infty = 2\varepsilon$

Motif #3: higher-order attacks

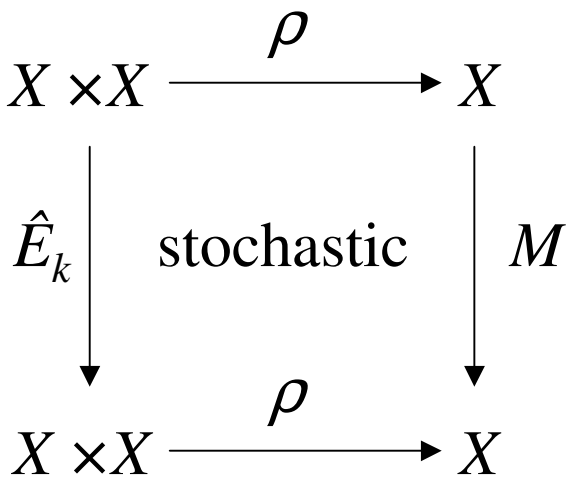
Use many encryptions to find better properties:



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

Example: Complementation

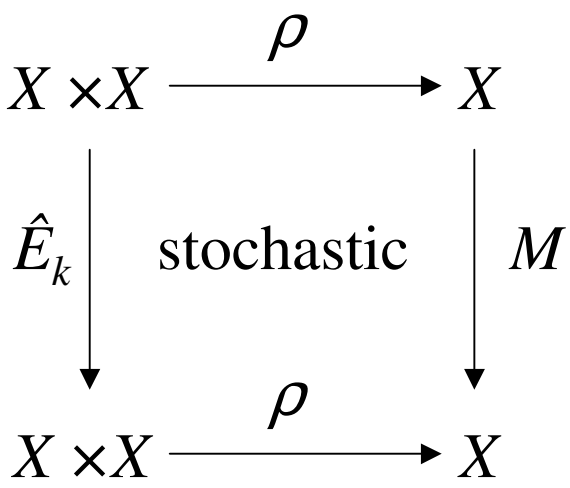
Complementation properties are a simple example:



- Take $\rho(x,x') = x' - x$
- Suppose $M(\Delta,\Delta) = 1$ for some cleverly chosen Δ
- Then we obtain a complementation property
- We can distinguish with just 2 chosen texts, since $\|M - M'\|_\infty \approx 1$

Example: Differential cryptanalysis

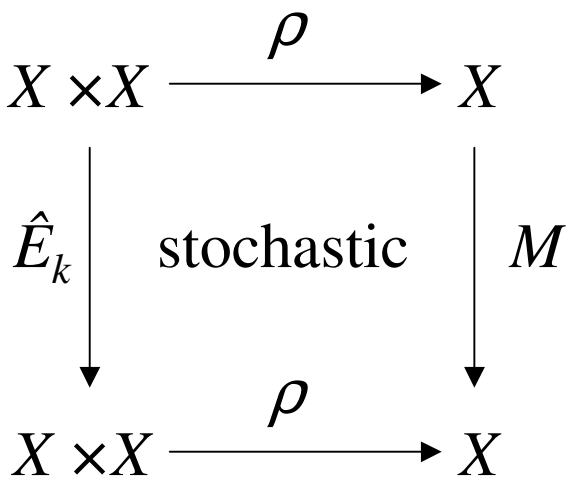
Differential cryptanalysis:



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

Example: Impossible differentials

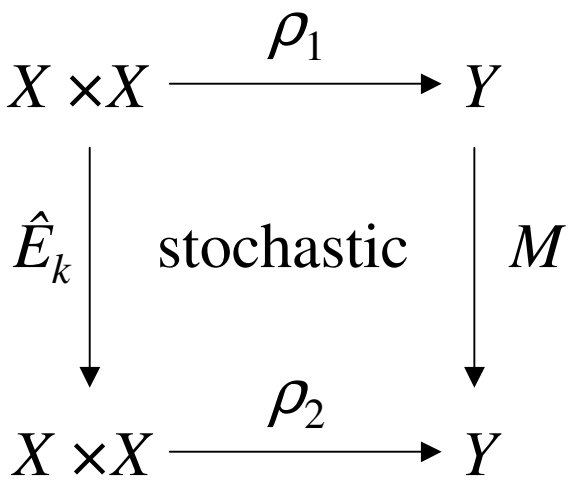
Impossible differential cryptanalysis:



- 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', we can distinguish with 2^n chosen texts

Example: Truncated diff. crypt.

Truncated differential cryptanalysis:

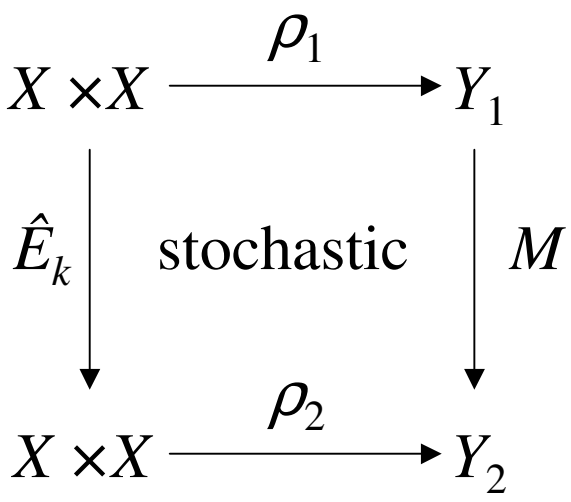


- Set $X = \mathrm{GF}(2)^n$, $Y = \mathrm{GF}(2)^m$, cleverly choose linear maps $\varphi_1, \varphi_2 : X \to Y$, and take $\rho_i(x,x') = \varphi_i(x' - x)$

- If $M(\Delta,\Delta) >> 2^{-m}$ for some clever choice of Δ, Δ', we can distinguish

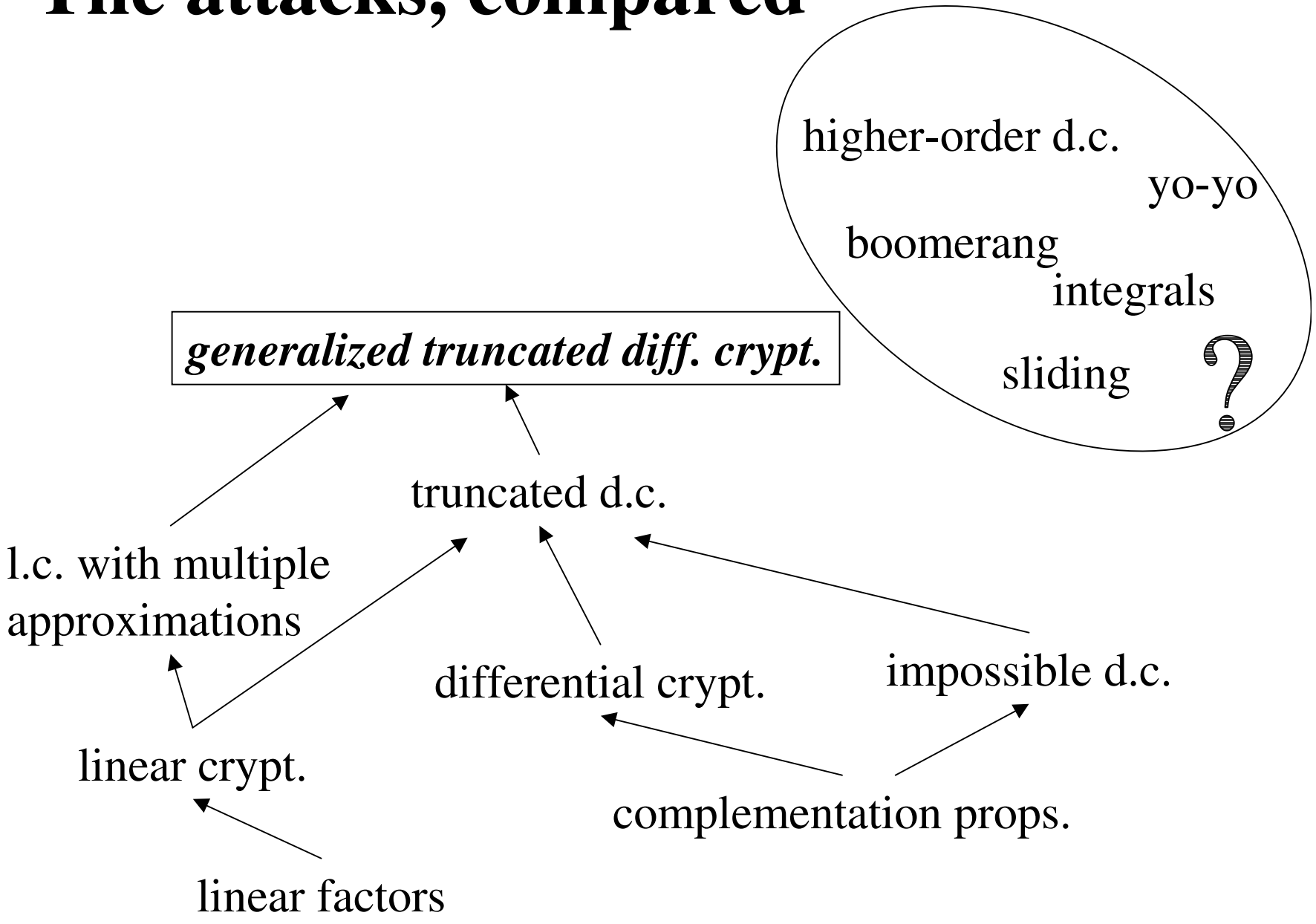
Generalized truncated d.c.

Generalized truncated differential cryptanalysis:



- Take X, Y_i, ρ_i as before; then $\|M - M'\|_\infty$ measures the distinguishing advantage of the attack
- Generalizes d.c., trunc d.c., l.c., diff-linear crypt., ...

The attacks, compared



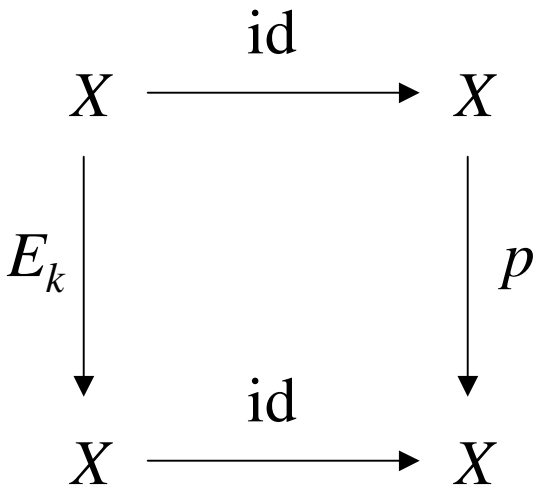
Summary (1)

- 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 $\mathrm{GL}(Y, Y) \subset \mathrm{Perm}(X)$
  - 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

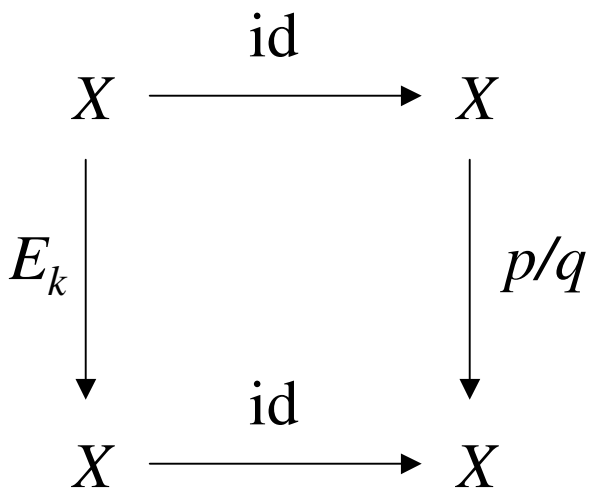
Express cipher as a polynomial in the message & key:



- Write $E_k(x) = p(x)$, then interpolate from known texts
- Generalization: MITM interpolation: $p'(E_k(x)) = p(x)$
- Generalization: probabilistic interpolation attacks
  - They use noisy polynomial reconstruction, decoding Reed-Solomon codes

Example: Rational inter. attacks

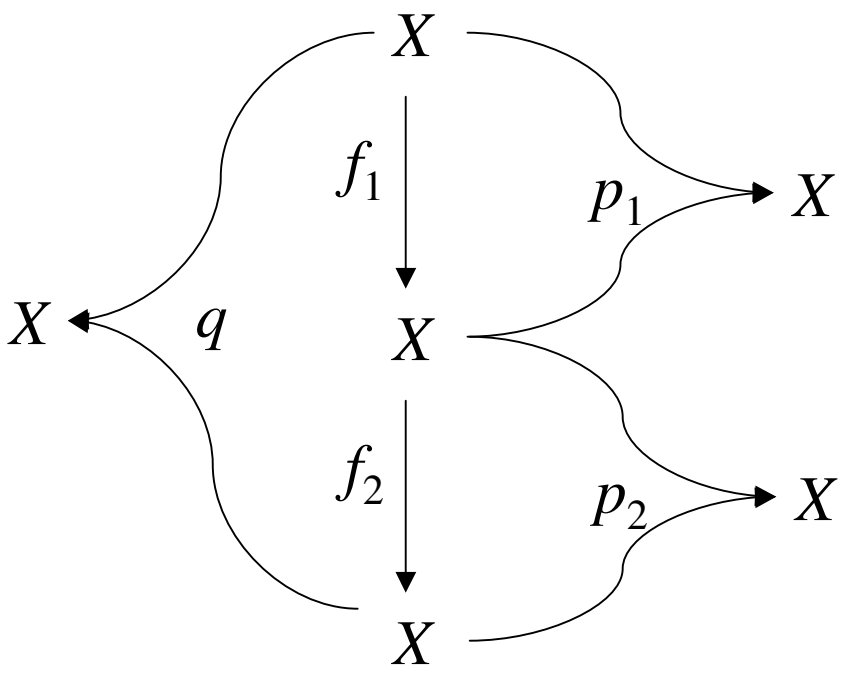
Express the cipher as a rational polynomial:



- 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
- Q: Are probabilistic rational interpolation attacks feasible?

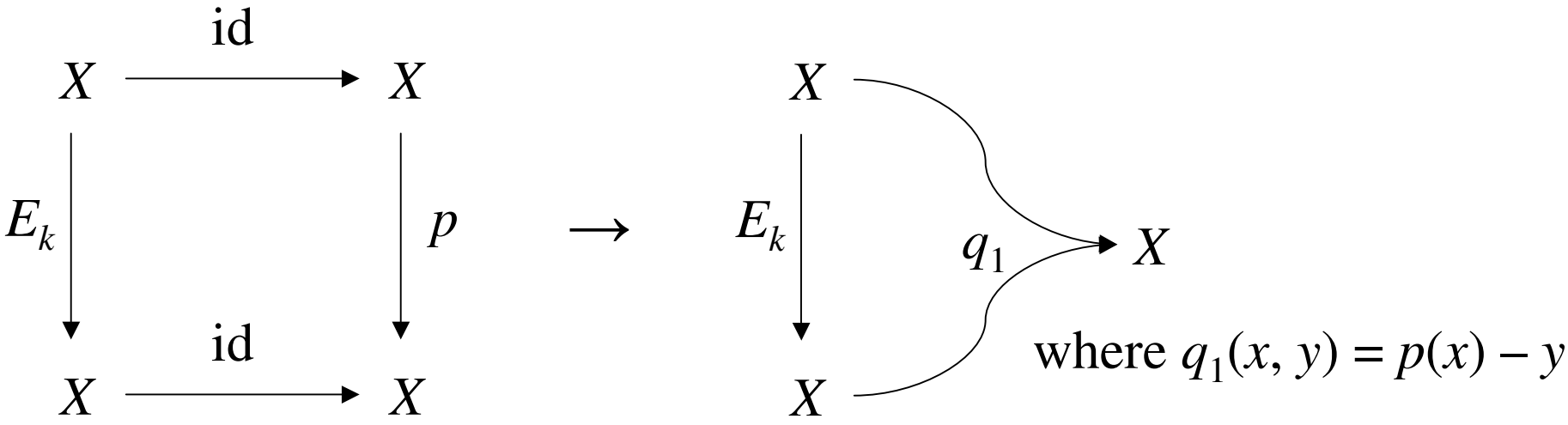
A generalization: resultants

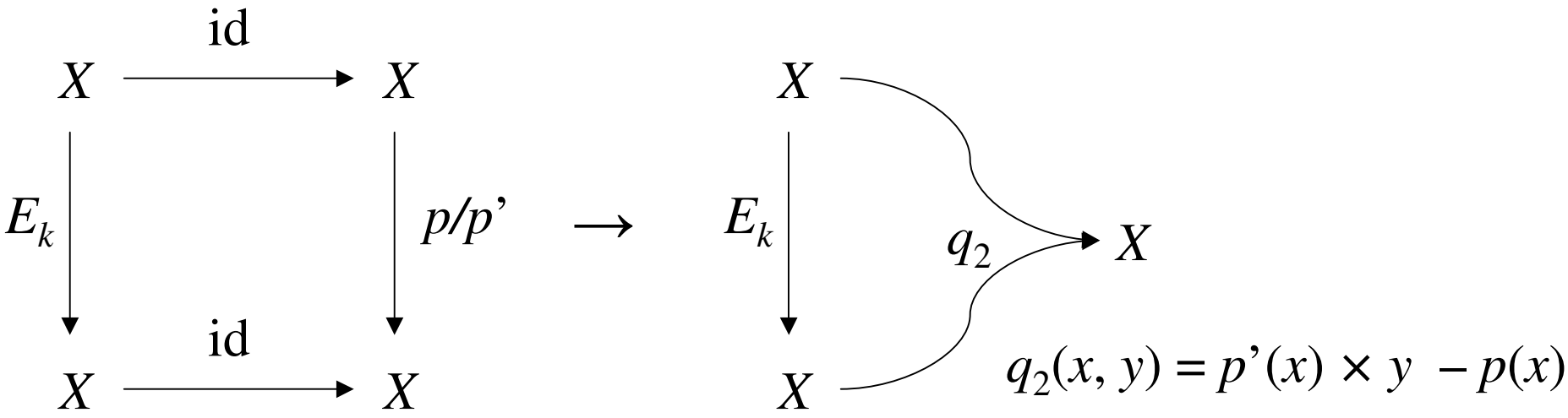
A possible direction: bivariate polynomials:



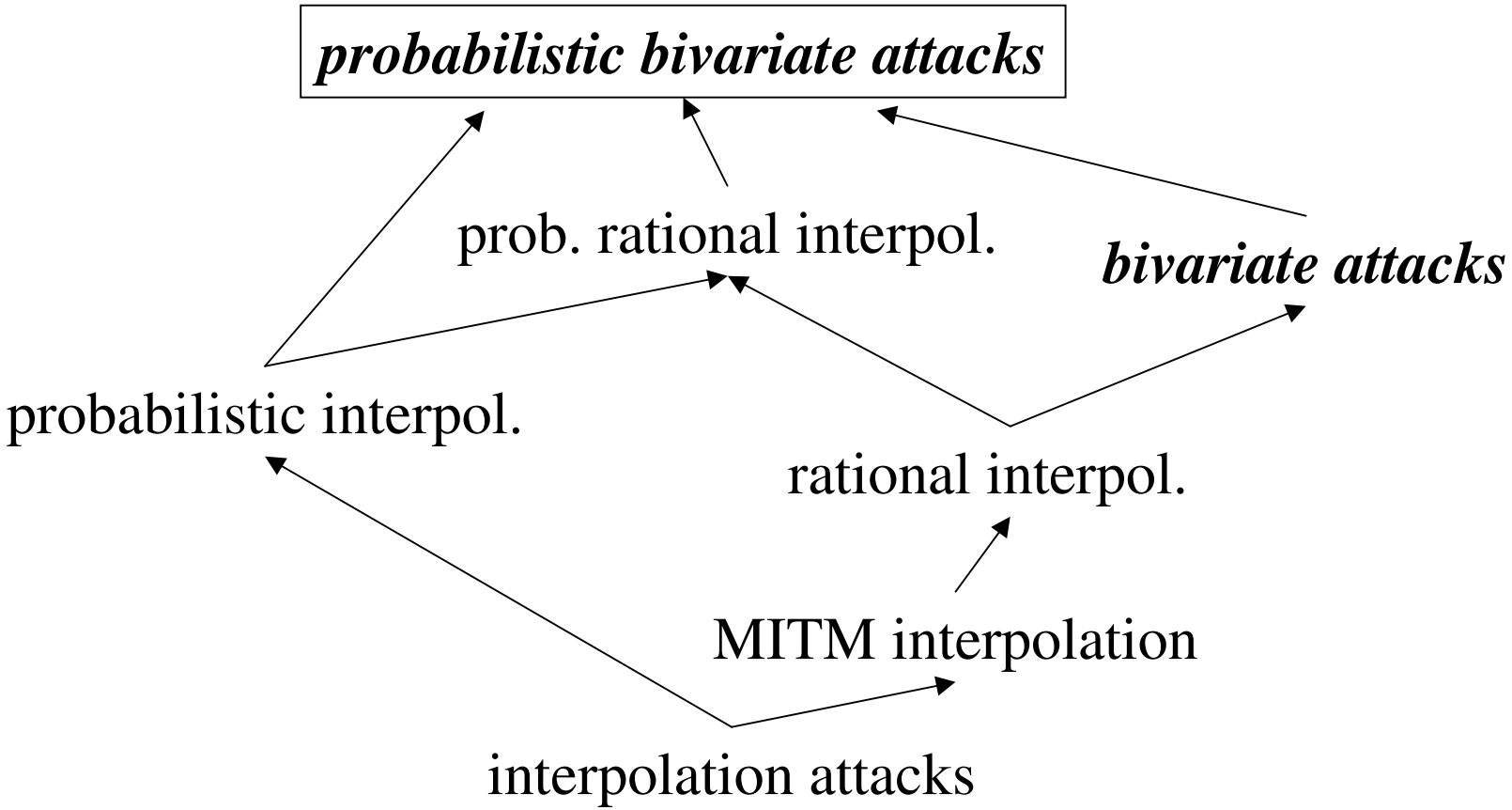
- The small diagrams commute if $p_i(x, f_i(x)) = 0$ for all x
- The small diagrams can be composed, yielding a large diagram $q(.,.) = 0$
- Let $q(x, z) = \mathrm{Res}_y(p_1(x, y), p_2(y, z))$; then we have $q(x, f_2(f_1(x))) = 0$, i.e., the large diagram commutes

Bivariate attacks generalize polynomial & rational interpolation





Algebraic attacks, compared



Summary (2)

- Many cryptanalytic methods can be understood, and compared, by expressing them as a combination of only a few basic ideas
- Commutative diagrams are a powerful way to think about cryptanalysis
- Questions?