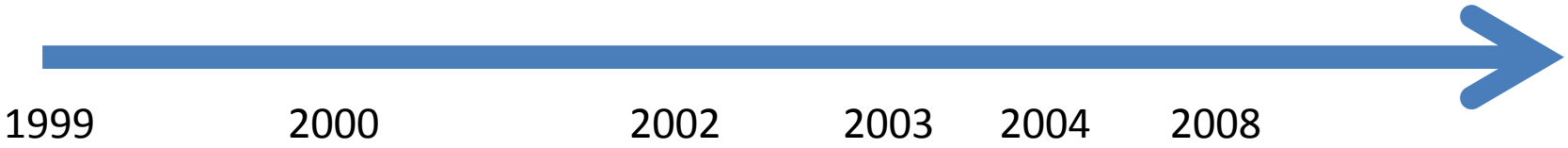
A note on the comparison of distinguishers

Oscar Reparaz, Benedikt Gierlichs,
Ingrid Verbauwhede

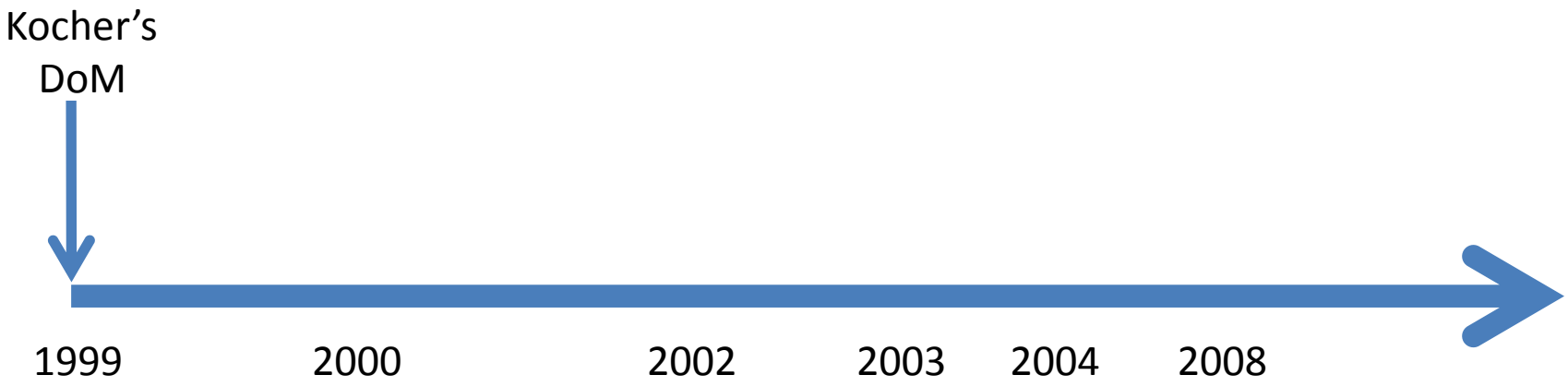
COSIC/KU Leuven

COSADE 2014, Paris

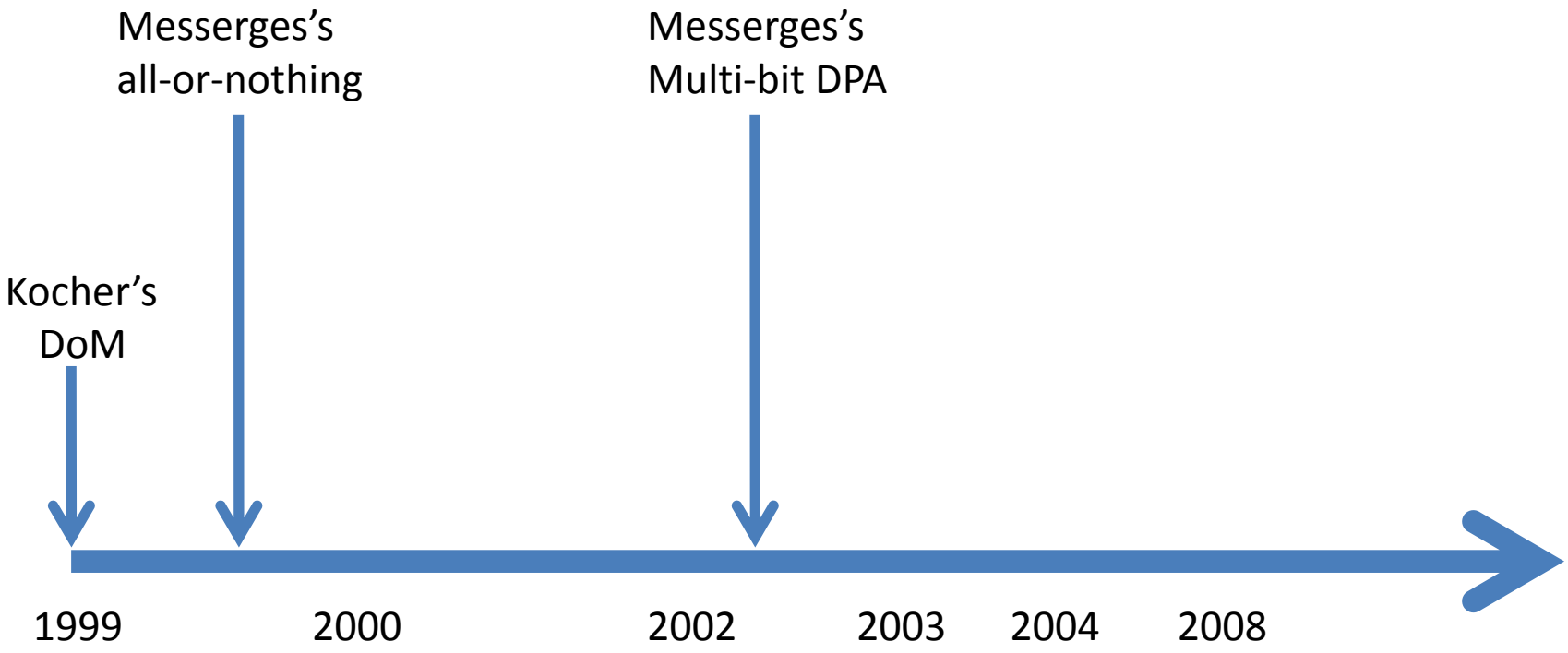
A jungle of distinguishers



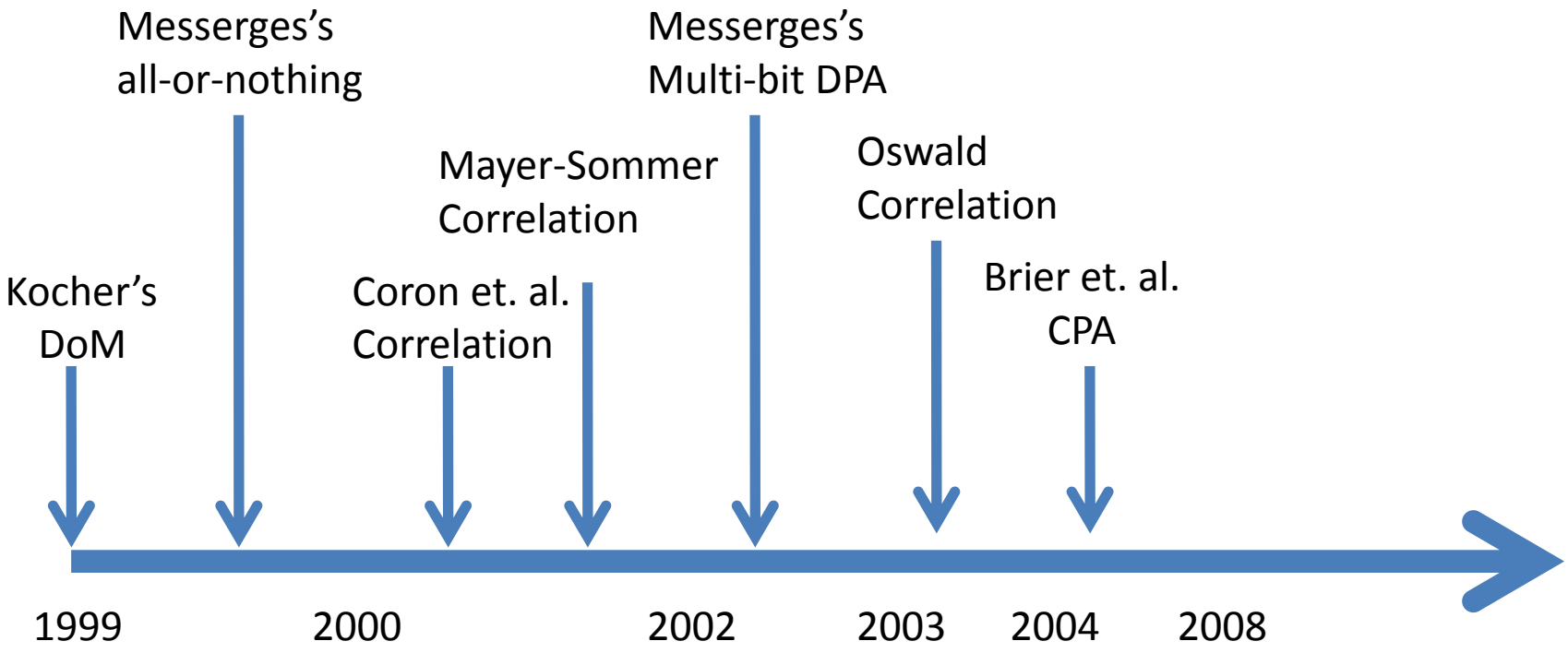
A jungle of distinguishers



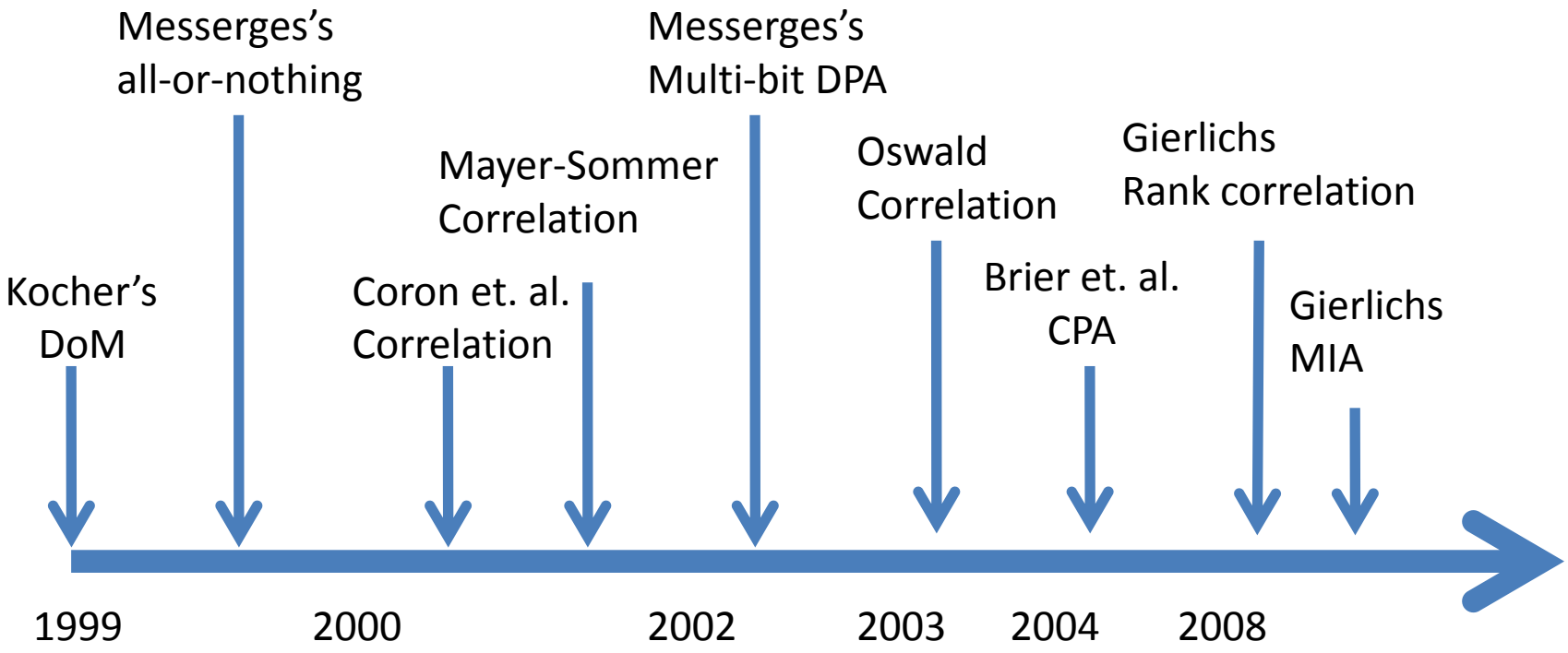
A jungle of distinguishers



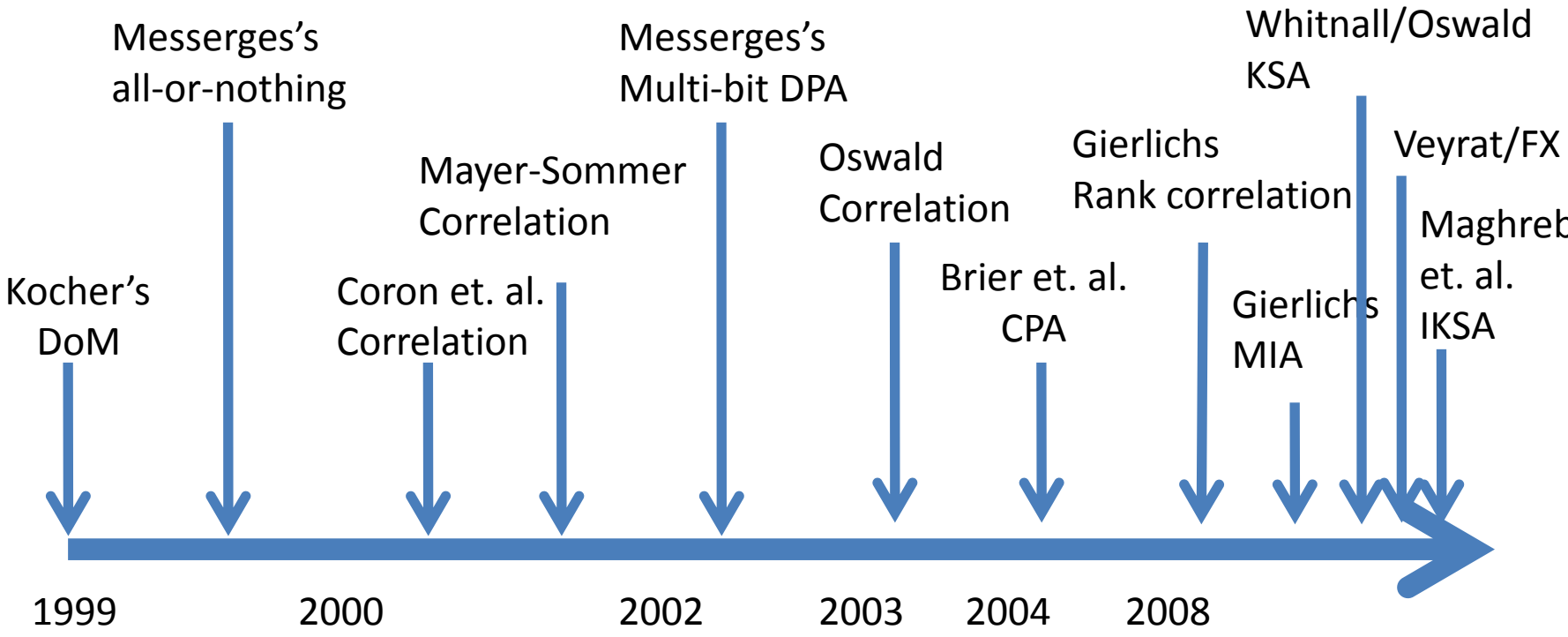
A jungle of distinguishers



A jungle of distinguishers



A jungle of distinguishers



One for All - All for One: Unifying Standard DPA Attacks

Stefan Mangard[1], Elisabeth Oswald[2], François-Xavier Standaert[3⋆]

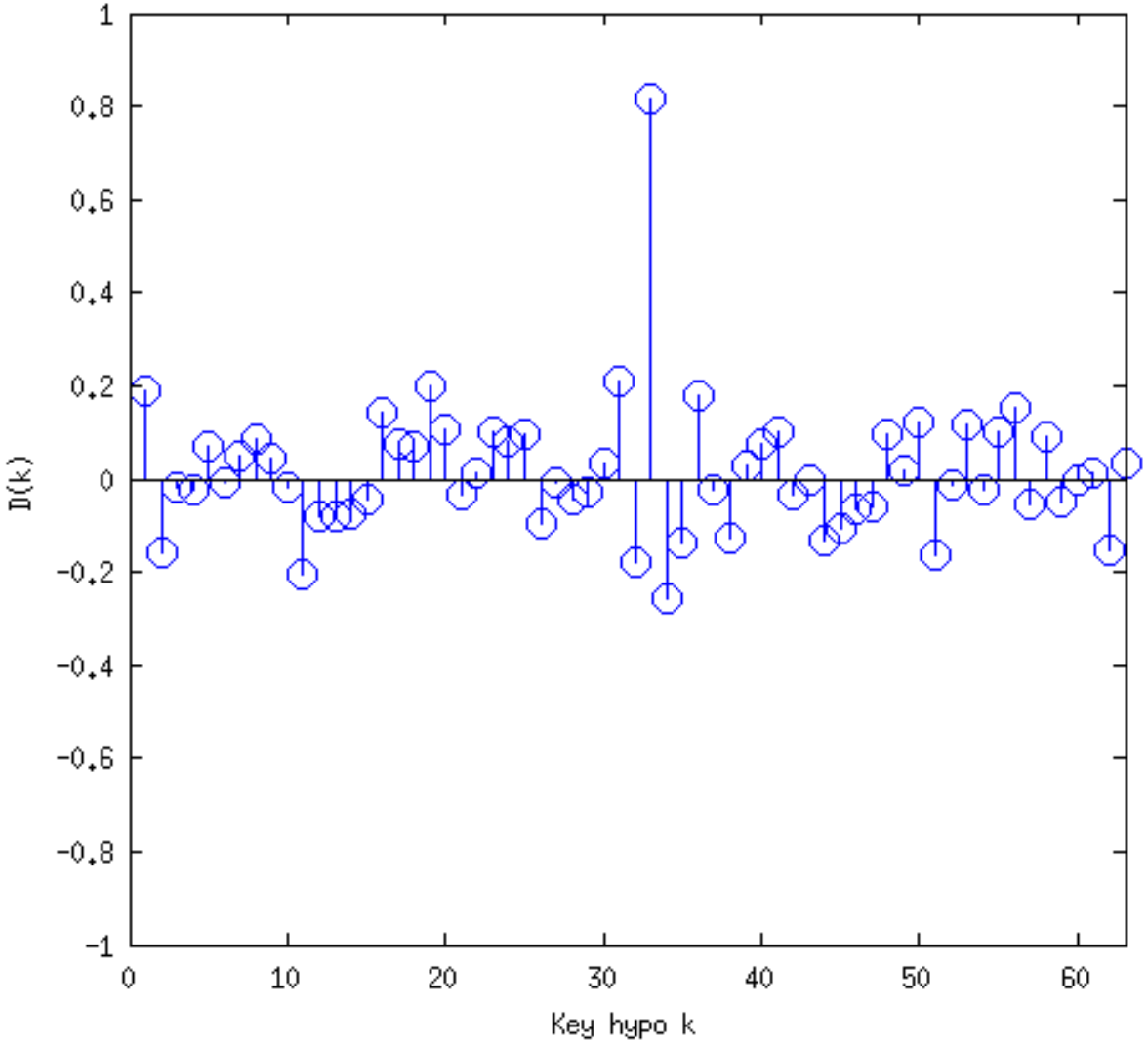
- Success rates

A fair evaluation framework for comparing side-channel distinguishers

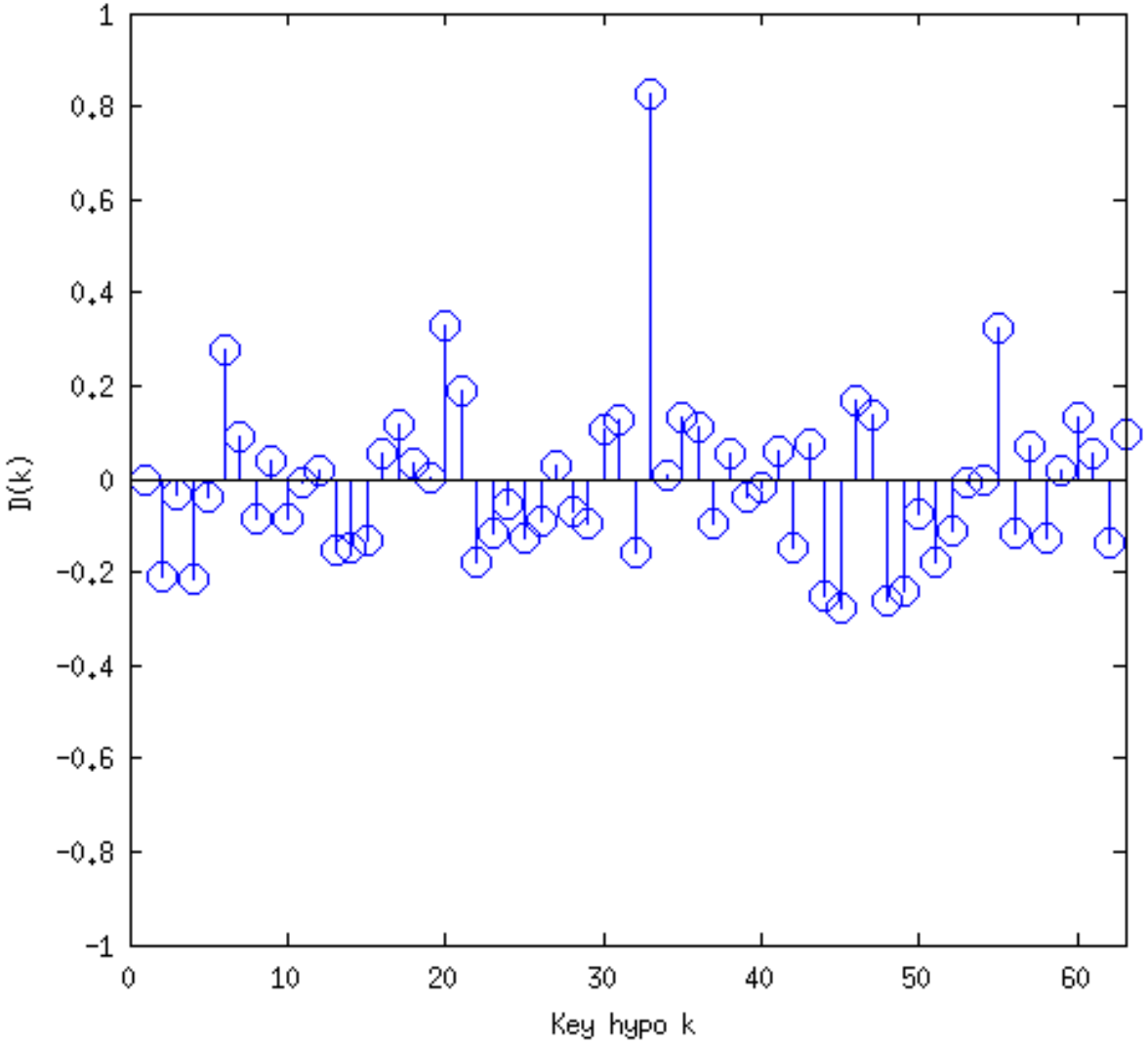
Carolyn Whitnall · Elisabeth Oswald

- Introduces (theoretical) distinguishing margins

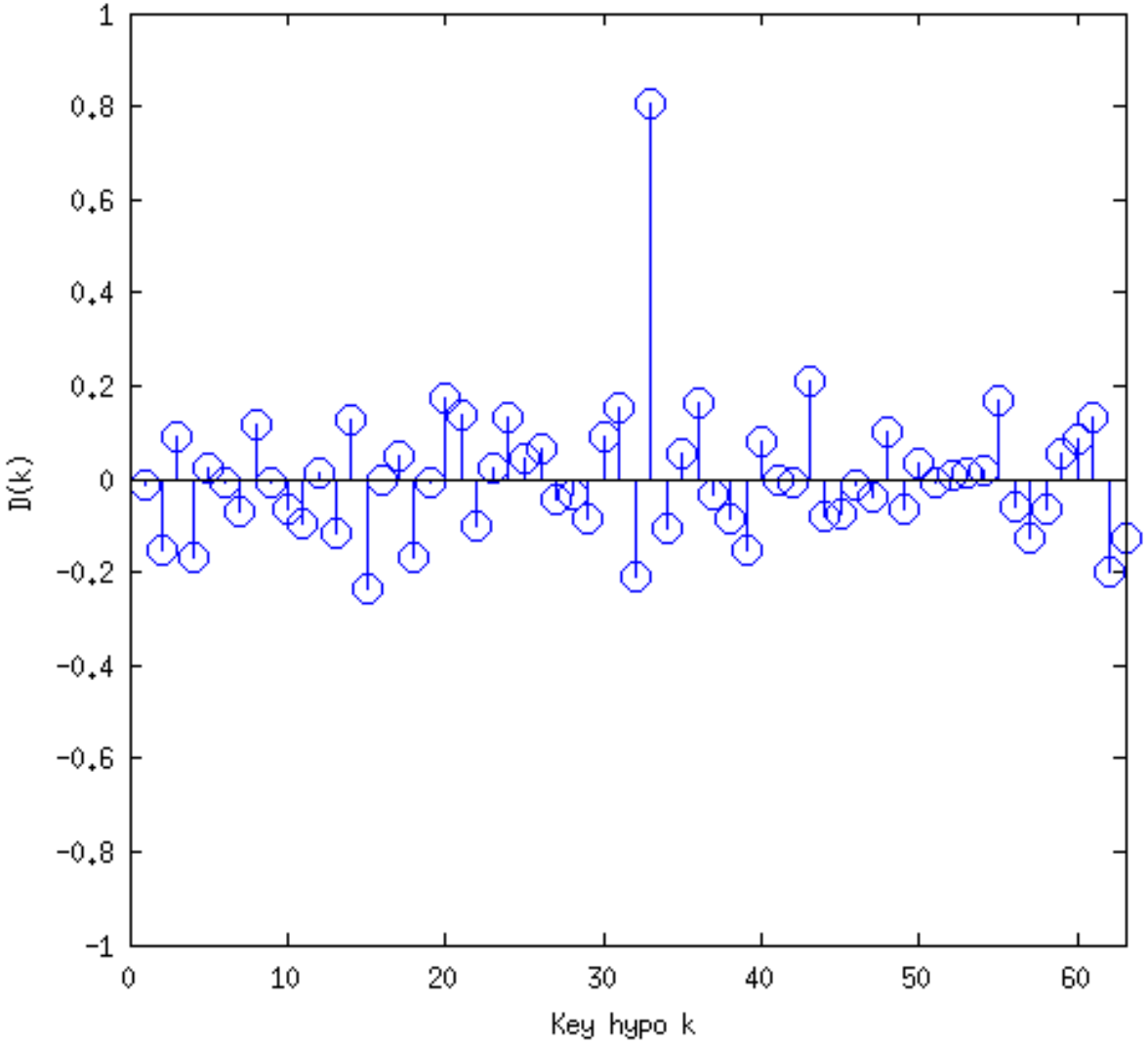
Definitions: distinguishing vector



Definitions: distinguishing vector



Definitions: distinguishing vector



Definitions: success rate, relative margins

Definitions: success rate, relative margins

- Success rates
  - Repeat the experiment, count how many successful

Definitions: success rate, relative margins

- Success rates
  - Repeat the experiment, count how many successful
- Distinguishing margins
  - Normalized “distance” between correct key hypo and nearest rival

$$\mathrm{RelMargin}(D) = \frac{D(k^*) - \max\left[D(k)|k \neq k^*\right]}{\mathrm{std}(D)}$$

Comparision success rates vs. distinguishing margins

Comparision success rates vs. distinguishing margins

Success rates

Comparision success rates vs. distinguishing margins

Success rates

- + Can be empirically computed quite easily
- + Easy interpretation

Comparision success rates vs. distinguishing margins

Success rates

- + Can be empirically computed quite easily
- + Easy interpretation
- - Not so easy to compute for certain distinguishers

Comparision success rates vs. distinguishing margins

Success rates

- + Can be empirically computed quite easily
- + Easy interpretation
- - Not so easy to compute for certain distinguishers

Distinguishing margins

Comparision success rates vs. distinguishing margins

Success rates

- + Can be empirically computed quite easily
- + Easy interpretation
- - Not so easy to compute for certain distinguishers

Distinguishing margins

- + Can be (easily) computed in a theoretic way for many distinguishers (thereby circumventing estimation issues)

Comparision success rates vs. distinguishing margins

Success rates

- + Can be empirically computed quite easily
- + Easy interpretation
- - Not so easy to compute for certain distinguishers

Distinguishing margins

- + Can be (easily) computed in a theoretic way for many distinguishers (thereby circumventing estimation issues)
- - should not be taken as the sole metric

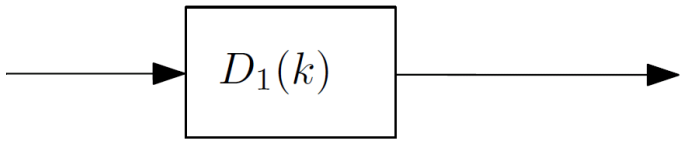
Distinguisher 1

- Absolute value of DoM

Distinguisher 1

- Absolute value of DoM

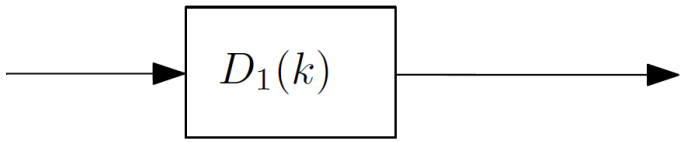
$$D_1(k) = \left| \widehat{\mathbf{E}}(T|L(Z_k) = 1) - \widehat{\mathbf{E}}(T|L(Z_k) = 0) \right|$$



Distinguisher 1

- Absolute value of DoM

$$D_1(k) = \left| \widehat{\mathbf{E}}(T|L(Z_k) = 1) - \widehat{\mathbf{E}}(T|L(Z_k) = 0) \right|$$



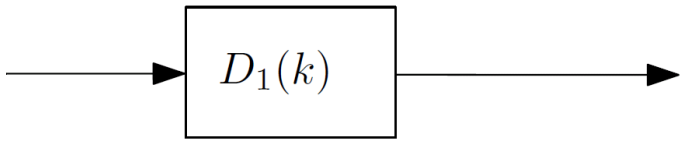
Distinguisher 2

- Absolute value of DoM, squared

Distinguisher 1

- Absolute value of DoM

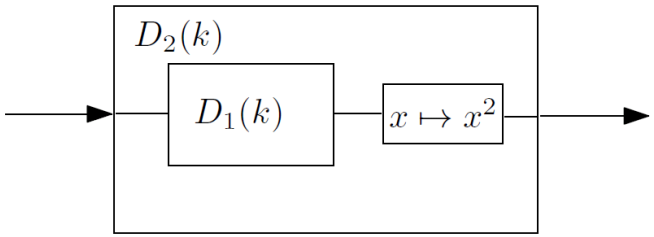
$$D_1(k) = \left| \widehat{\mathbf{E}}(T|L(Z_k) = 1) - \widehat{\mathbf{E}}(T|L(Z_k) = 0) \right|$$



Distinguisher 2

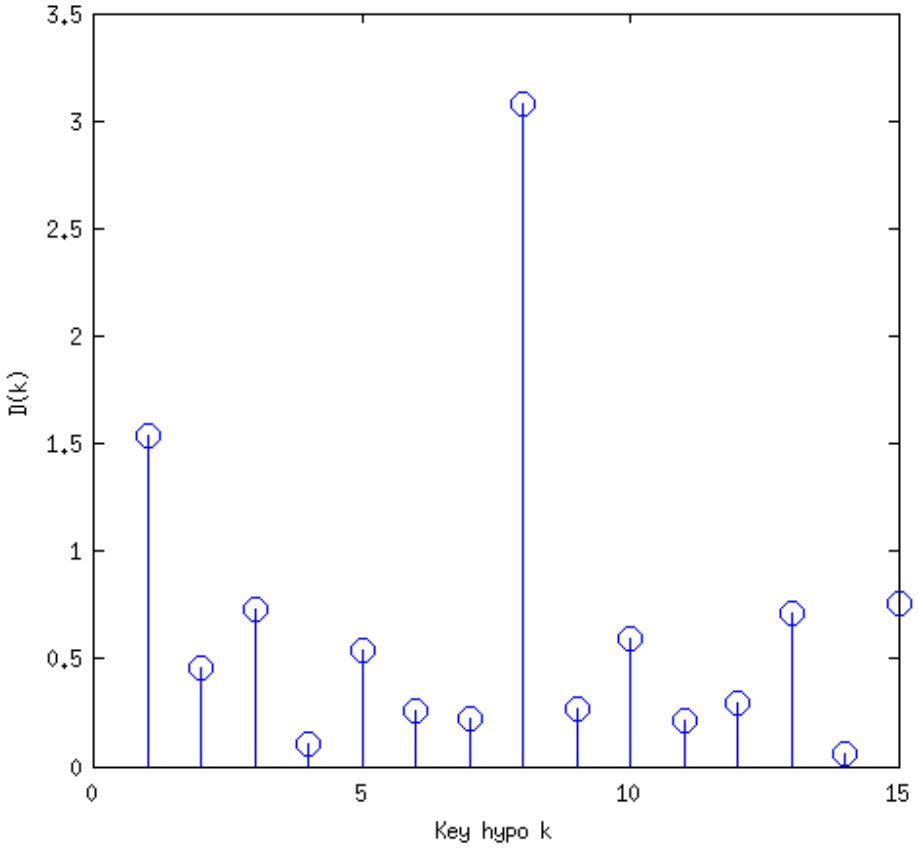
- Absolute value of DoM, squared

$$D_2(k) = [D_1(k)]^2 = \left| \widehat{\mathbf{E}}(T|L(Z_k) = 1) - \widehat{\mathbf{E}}(T|L(Z_k) = 0) \right|^2$$

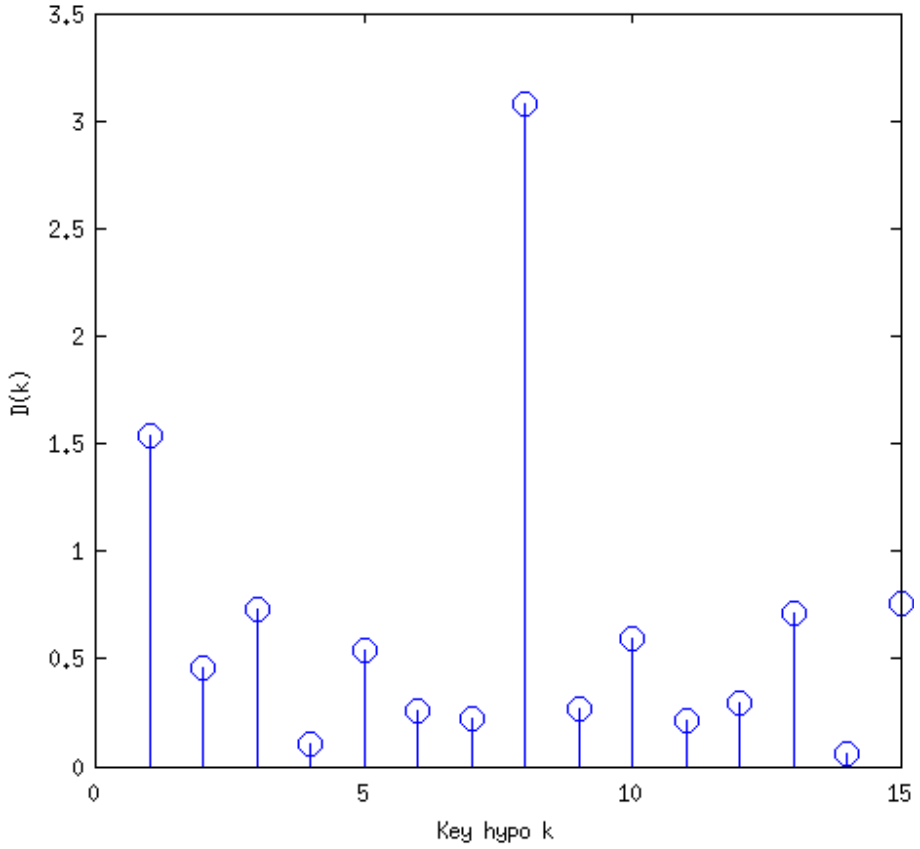


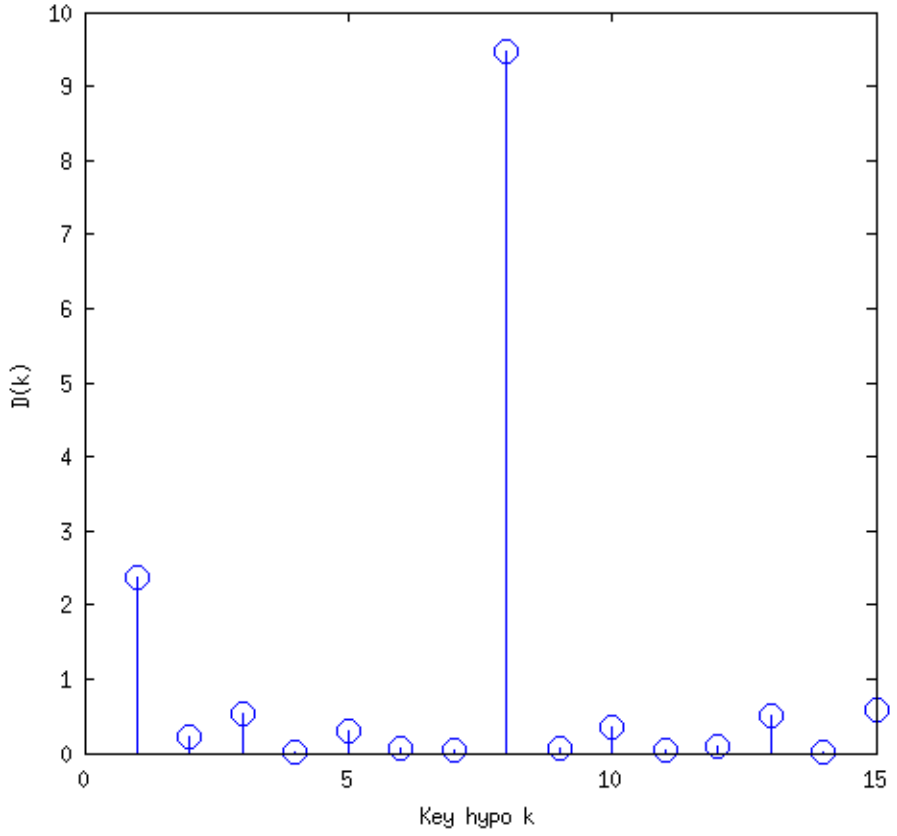
Distinguishing vectors for distinguisher 1 and 2

Distinguishing vectors for distinguisher 1 and 2

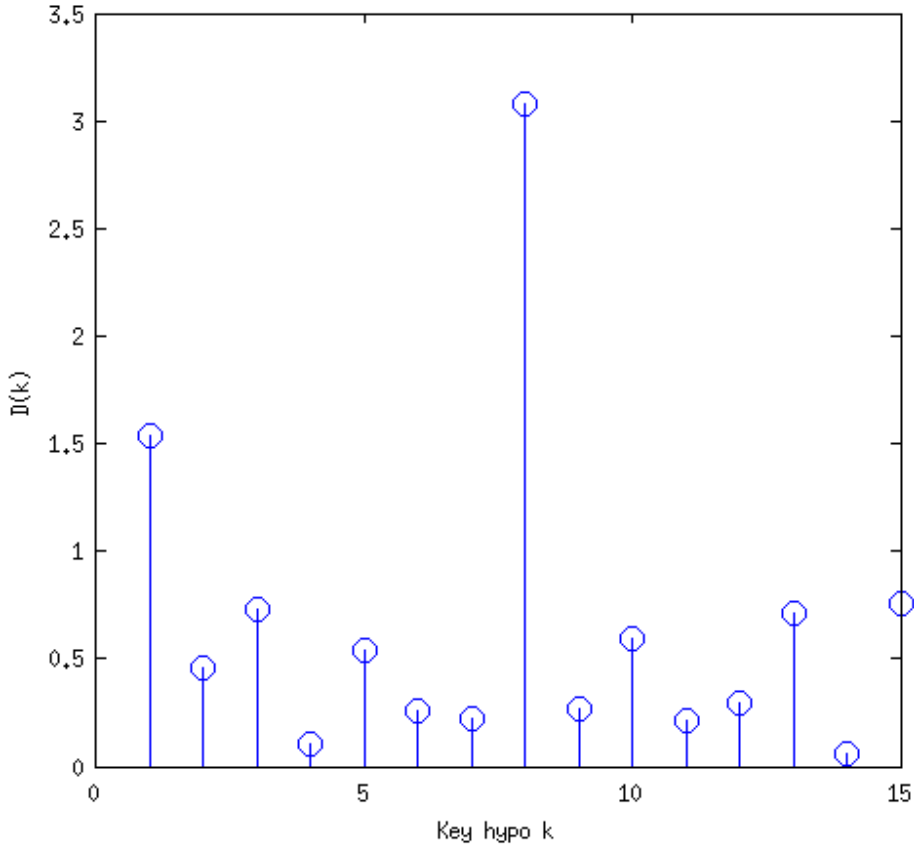


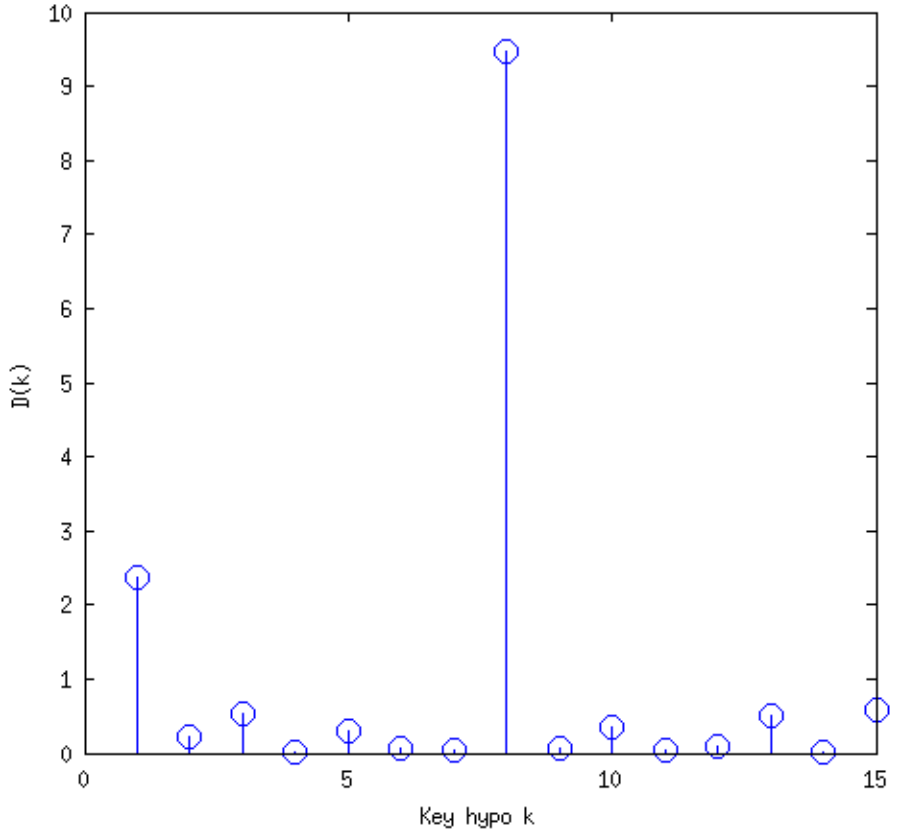
Distinguishing vectors for distinguisher 1 and 2





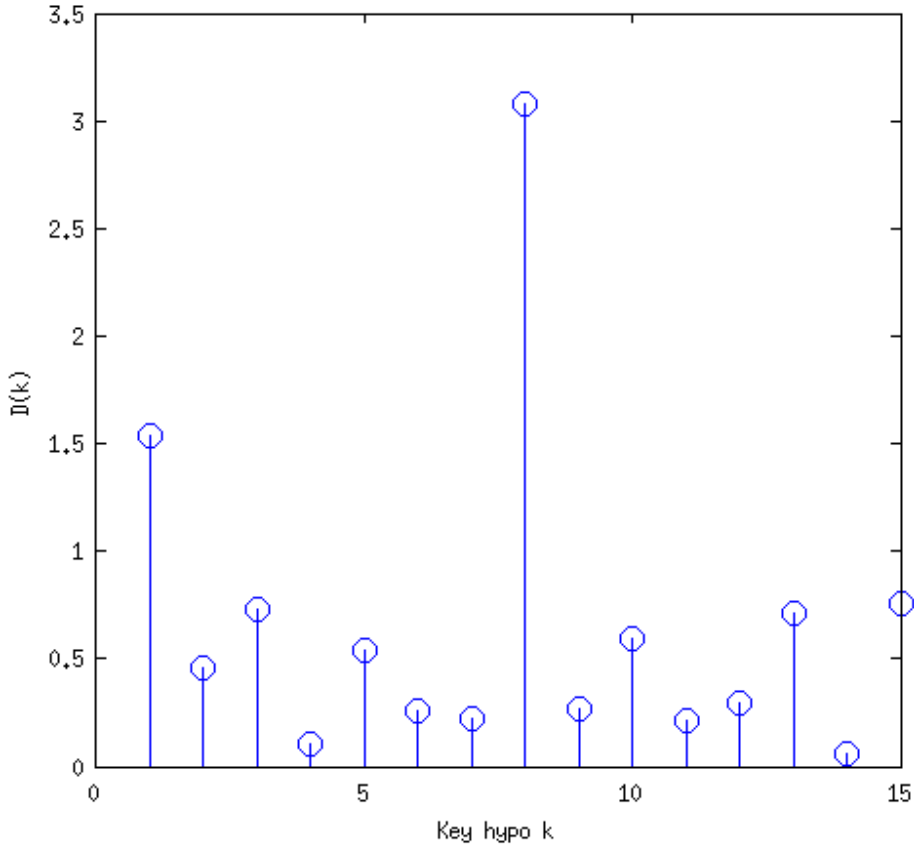
Distinguishing vectors for distinguisher 1 and 2

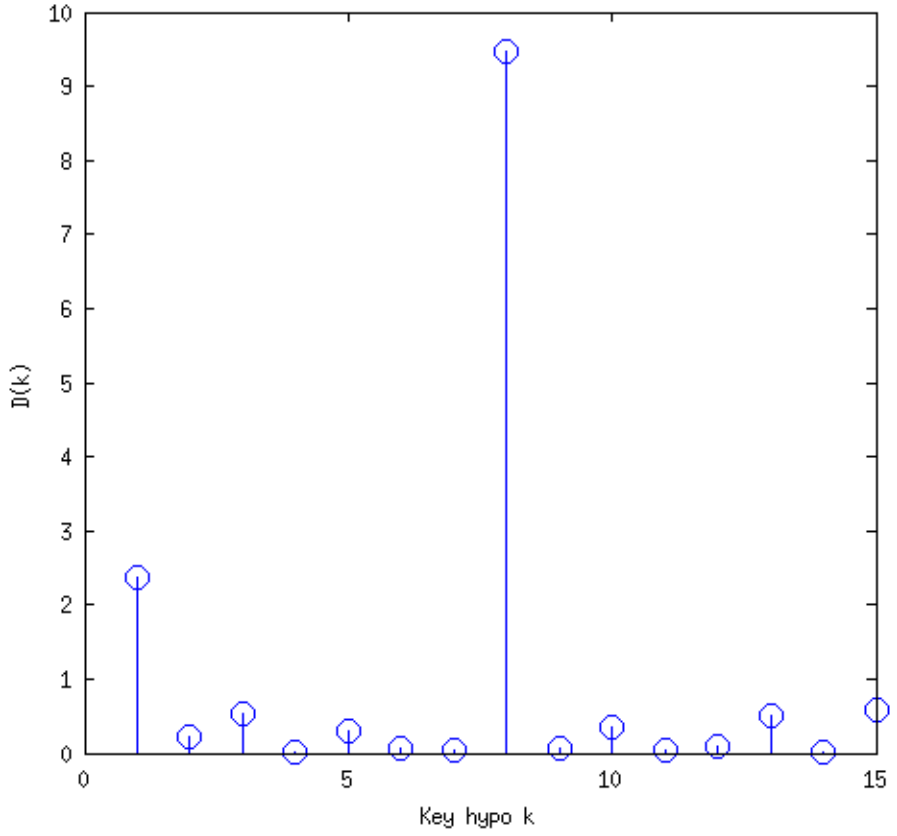




Order preserved → same success rate

Distinguishing vectors for distinguisher 1 and 2



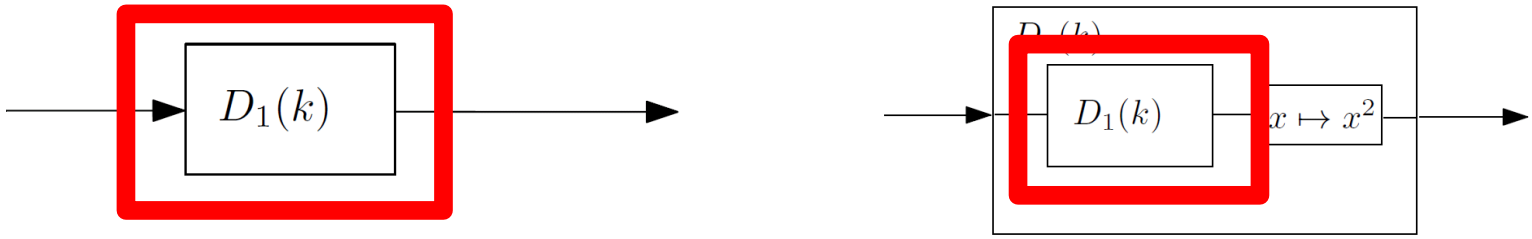


RelMargin(D1) = 0.25 ≠ RelMargin(D2) = 0.51

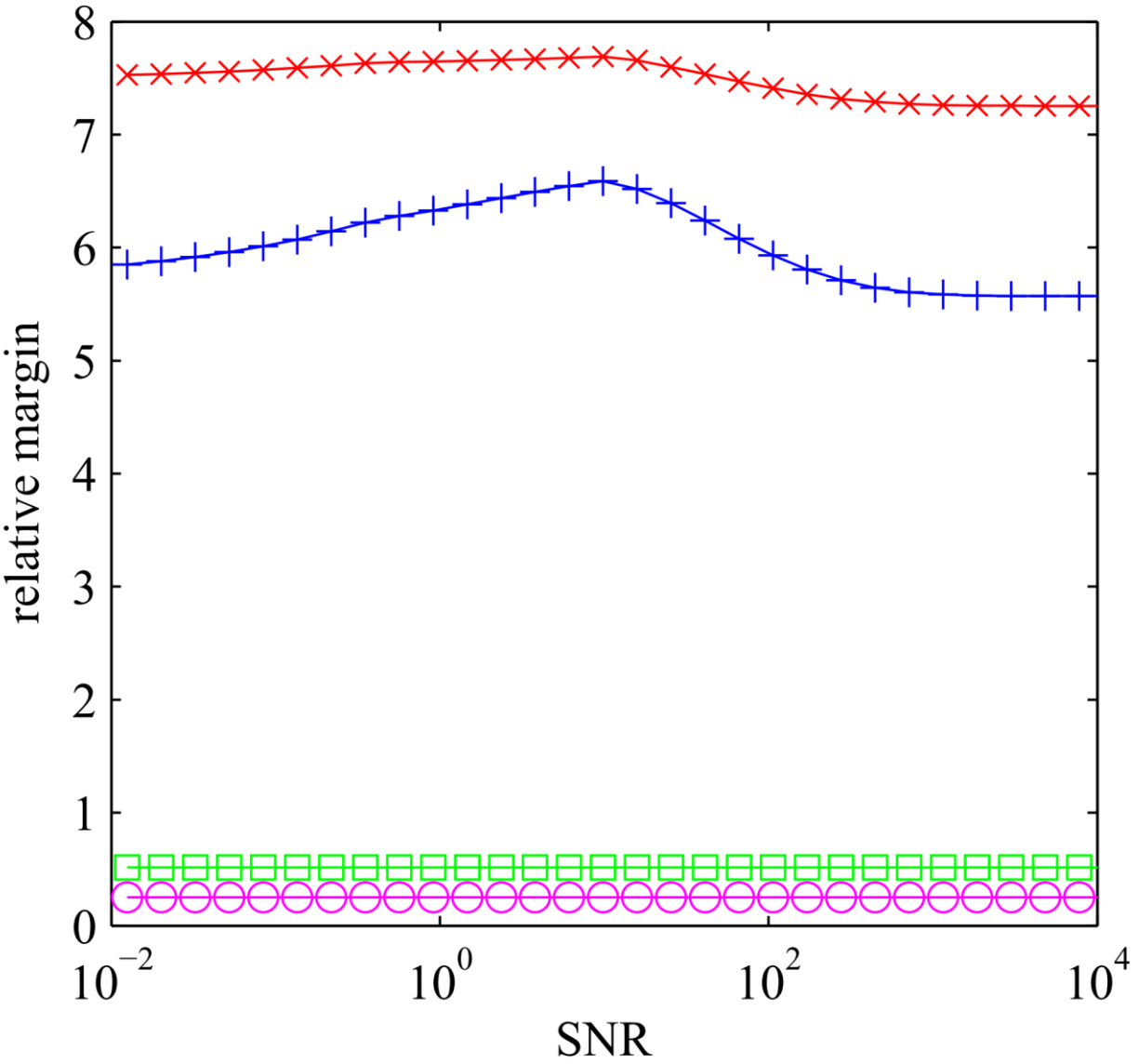
A different D1 box

A different D1 box

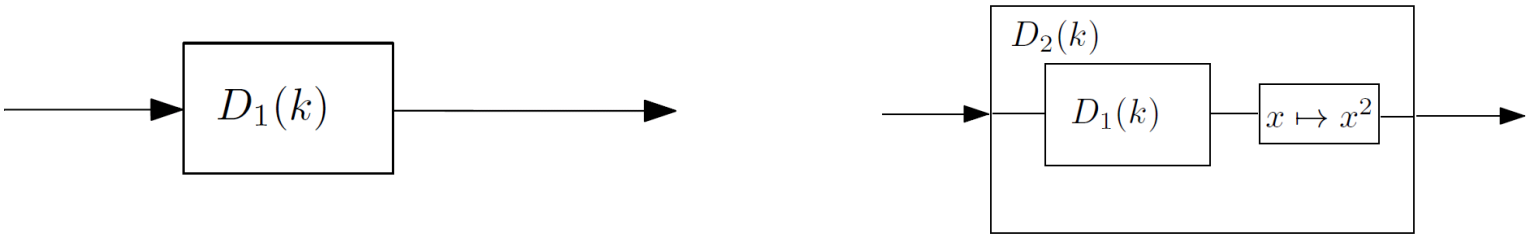
A different D1 box



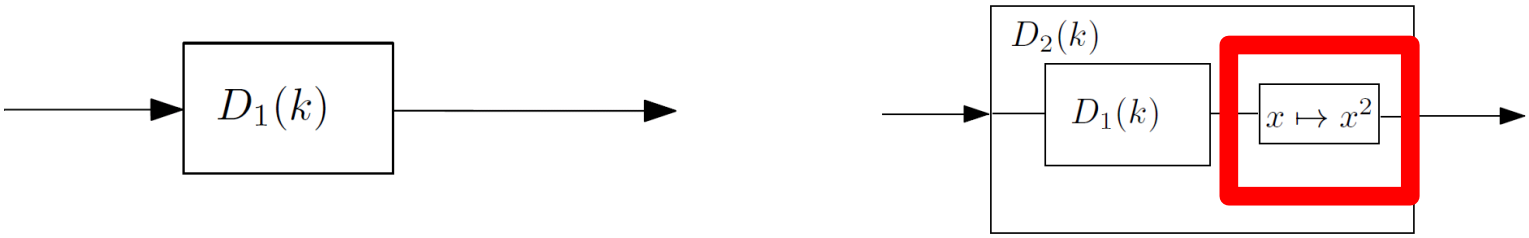
A different D1 box



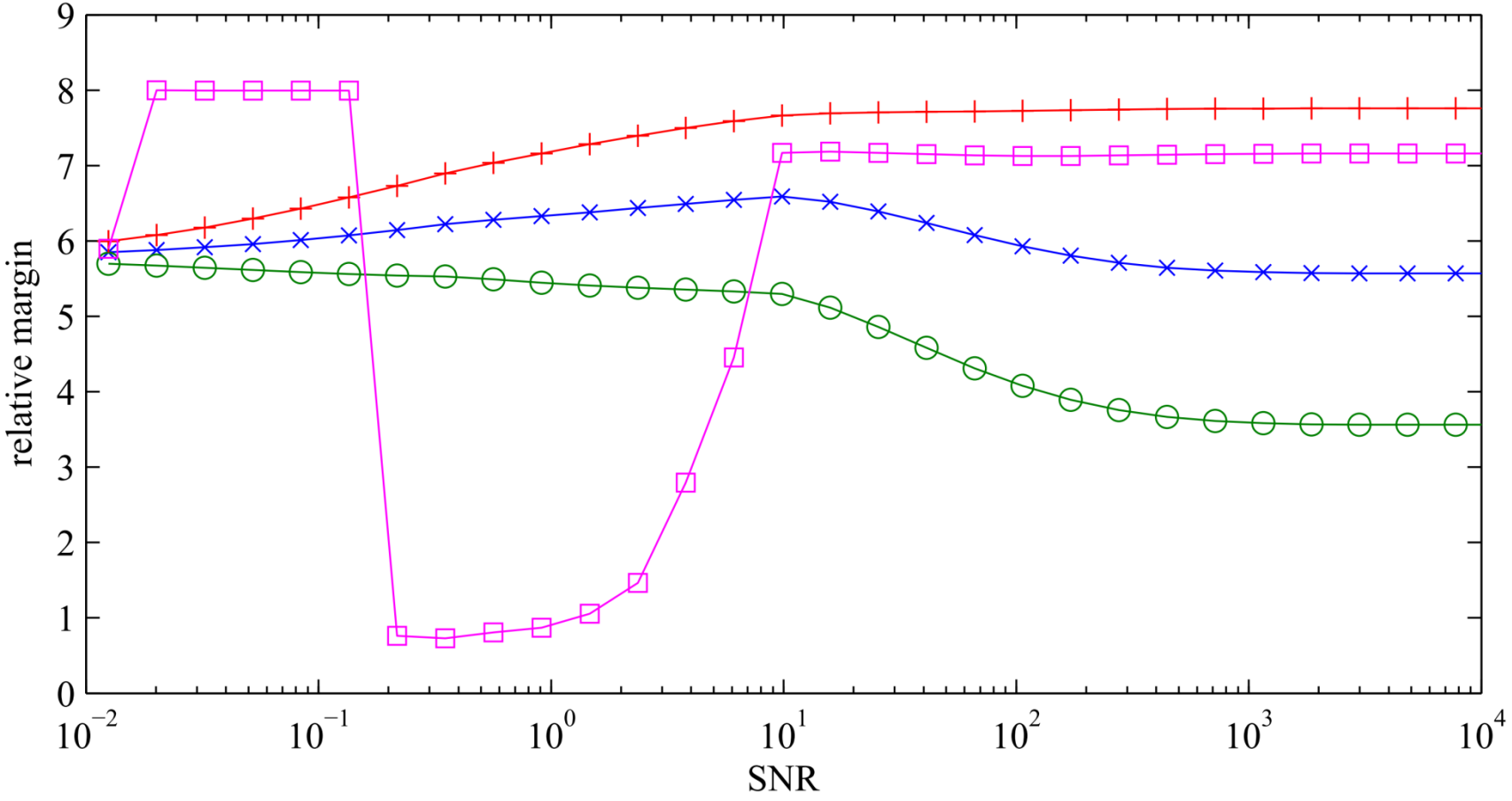
Different transformation functions



Different transformation functions



Different transformation functions



Conclusion

- No one-fits-all solution
- Nice theoretical properties, but sometimes *too* theoretical