Alternating Product Ciphers: A Case for Provable Security Comparisons

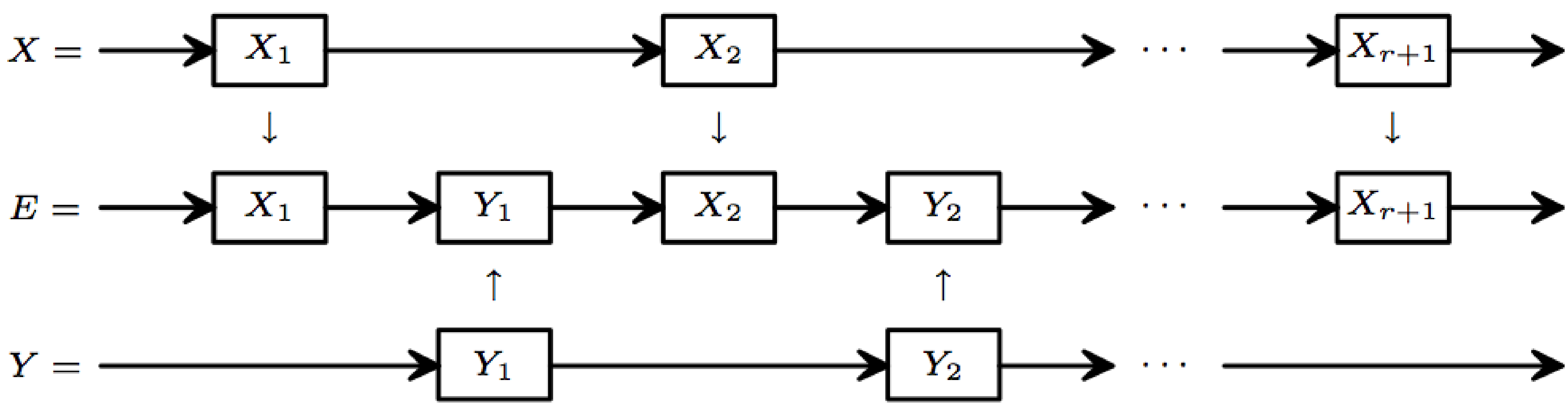
Indocrypt 2013

John Pliam
Johns Hopkins University

Introduction

Definitions: Deciphering the Title

Def. Alternating Product



Def. Provable Security Comparisons

- (provable security) comparisons
  - Inequalities like **Adv**(Z) < **Adv**(Y)
- provable (security comparisons)
  - Other security metrics H_a, W, G_a

$$\begin{tikzcd} z \arrow[r, dotted, no head, "\preceq"] \arrow[d] & y \arrow[d] \\ H(Z) \arrow[r, dotted, no head, "\geq"'] & H(Y) \end{tikzcd} \qquad \begin{tikzcd} z \arrow[r, dotted, no head, "\preceq_q"] \arrow[d] & y \arrow[d] \\ \mathbf{Adv}_Z(q) \arrow[r, dotted, no head, "\leq"'] & \mathbf{Adv}_Y(q) \end{tikzcd} \qquad \begin{tikzcd} z \arrow[r, dotted, no head, "\preceq_q"] \arrow[d] & y \arrow[d] \\ W(Z|C,p) \arrow[r, dotted, no head, "\geq"'] & W(Y|C,p) \end{tikzcd}$$

Indeed ...

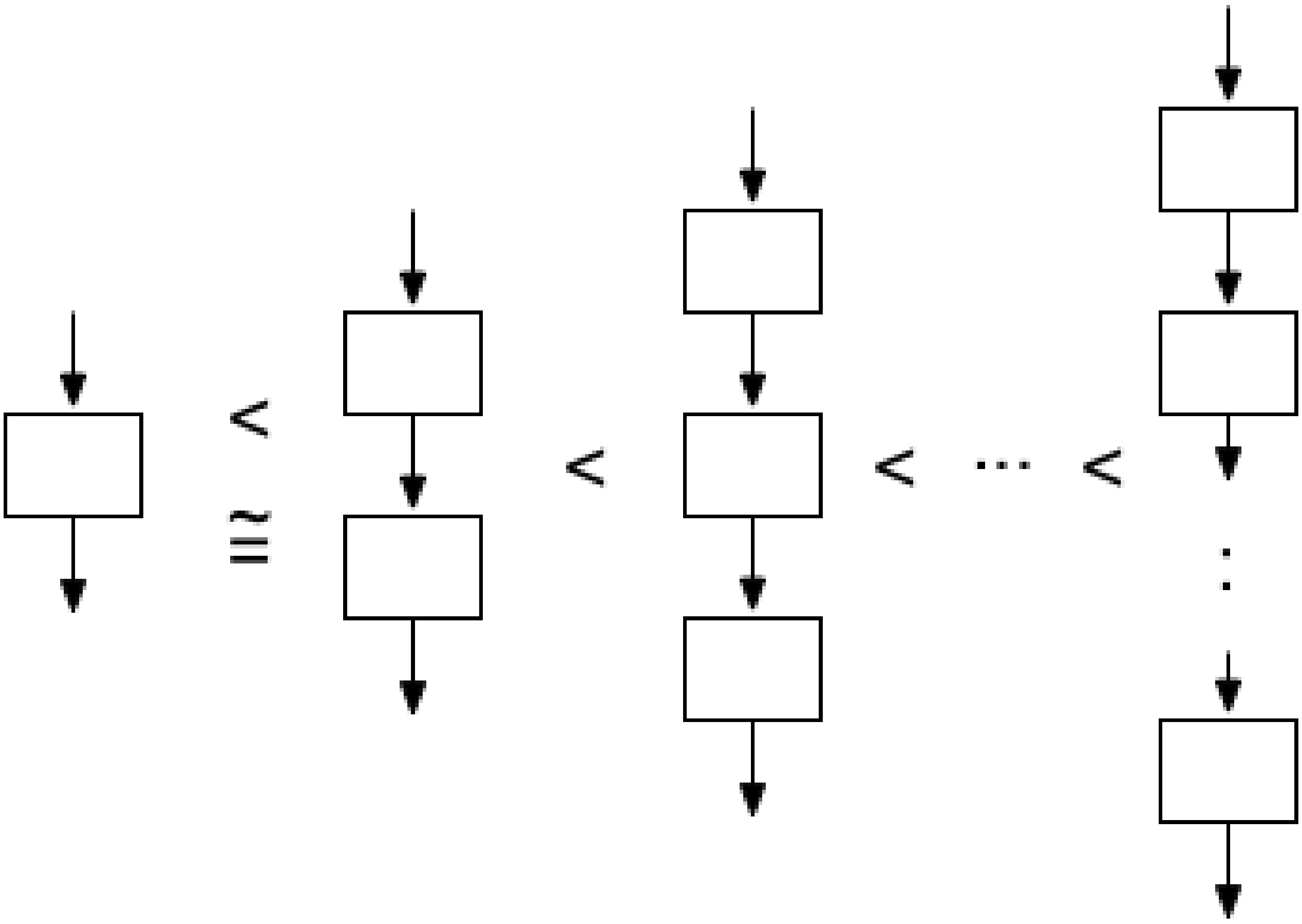
$$\begin{tikzcd} z \arrow[r, dash, dotted, "\preceq"] \arrow[d] & y \arrow[d] \\ H(Z) \arrow[r, dash, dotted, "\geq"] & H(Y) \end{tikzcd} \qquad \begin{tikzcd} z \arrow[r, dash, dotted, "\preceq"] \arrow[d] & y \arrow[d] \\ H_\infty(Z) \arrow[r, dash, dotted, "\geq"] & H_\infty(Y) \end{tikzcd} \qquad \begin{tikzcd} z \arrow[r, dash, dotted, "\preceq"] \arrow[d] & y \arrow[d] \\ H_\alpha(Z) \arrow[r, dash, dotted, "\geq"] & H_\alpha(Y) \end{tikzcd} \qquad \begin{tikzcd} z \arrow[r, dash, dotted, "\preceq_q"] \arrow[d] & y \arrow[d] \\ \mathbf{Adv}_Z(q) \arrow[r, dash, dotted, "\leq"] & \mathbf{Adv}_Y(q) \end{tikzcd}$$

$$\begin{tikzcd} z \arrow[r, dash, dotted, "\preceq"] \arrow[d] & y \arrow[d] \\ G_0(Z) \arrow[r, dash, dotted, "\geq"] & G_0(Y) \end{tikzcd} \qquad \begin{tikzcd} z \arrow[r, dash, dotted, "\preceq"] \arrow[d] & y \arrow[d] \\ G_1(Z) \arrow[r, dash, dotted, "\geq"] & G_1(Y) \end{tikzcd} \qquad \begin{tikzcd} z \arrow[r, dash, dotted, "\preceq"] \arrow[d] & y \arrow[d] \\ G_\alpha(Z) \arrow[r, dash, dotted, "\geq"] & G_\alpha(Y) \end{tikzcd} \qquad \begin{tikzcd} z \arrow[r, dash, dotted, "\preceq_q"] \arrow[d] & y \arrow[d] \\ W(Z|C,p) \arrow[r, dash, dotted, "\geq"] & W(Y|C,p) \end{tikzcd}$$

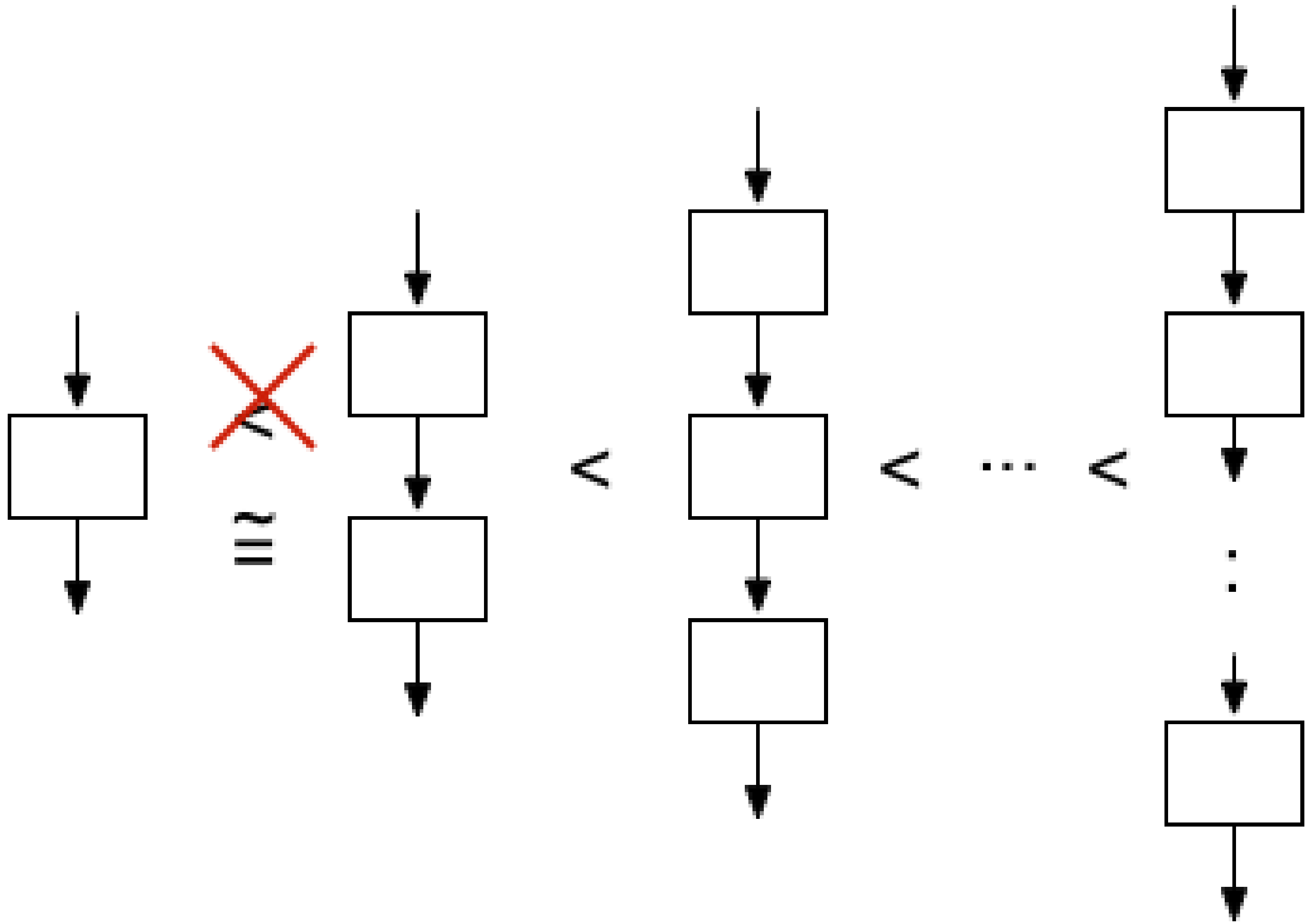
$$\begin{tikzcd} z \arrow[r, dash, dotted, "\preceq"] \arrow[d] & y \arrow[d] \\ w_\alpha(Z) \arrow[r, dash, dotted, "\geq"] & w_\alpha(Y) \end{tikzcd} \qquad \begin{tikzcd} z \arrow[r, dash, dotted, "\preceq_q"] \arrow[d] & y \arrow[d] \\ \mathbf{Adv}_1(Z) \arrow[r, dash, dotted, "\leq"] & \mathbf{Adv}_1(Y) \end{tikzcd} \qquad \begin{tikzcd} z \arrow[r, dash, dotted, "\preceq_q"] \arrow[d] & y \arrow[d] \\ \mathbf{Adv}_2(Z) \arrow[r, dash, dotted, "\leq"] & \mathbf{Adv}_2(Y) \end{tikzcd} \qquad \begin{tikzcd} z \arrow[r, dash, dotted, "\preceq_q"] \arrow[d] & y \arrow[d] \\ \mathbf{Adv}_3(Z) \arrow[r, dash, dotted, "\leq"] & \mathbf{Adv}_3(Y) \end{tikzcd}$$

Part I
Alternating Product Ciphers

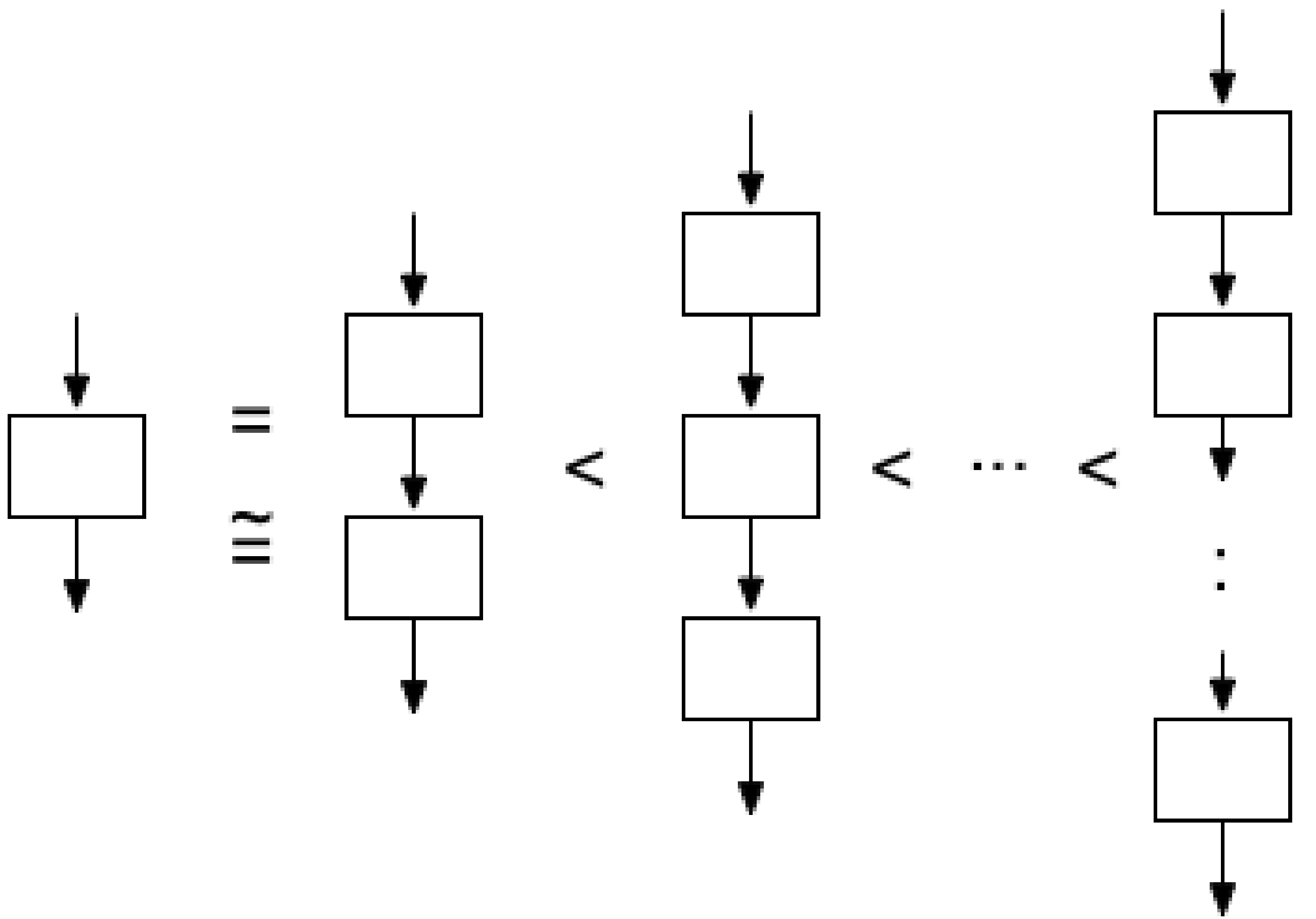
Under “Random” Cipher Approx



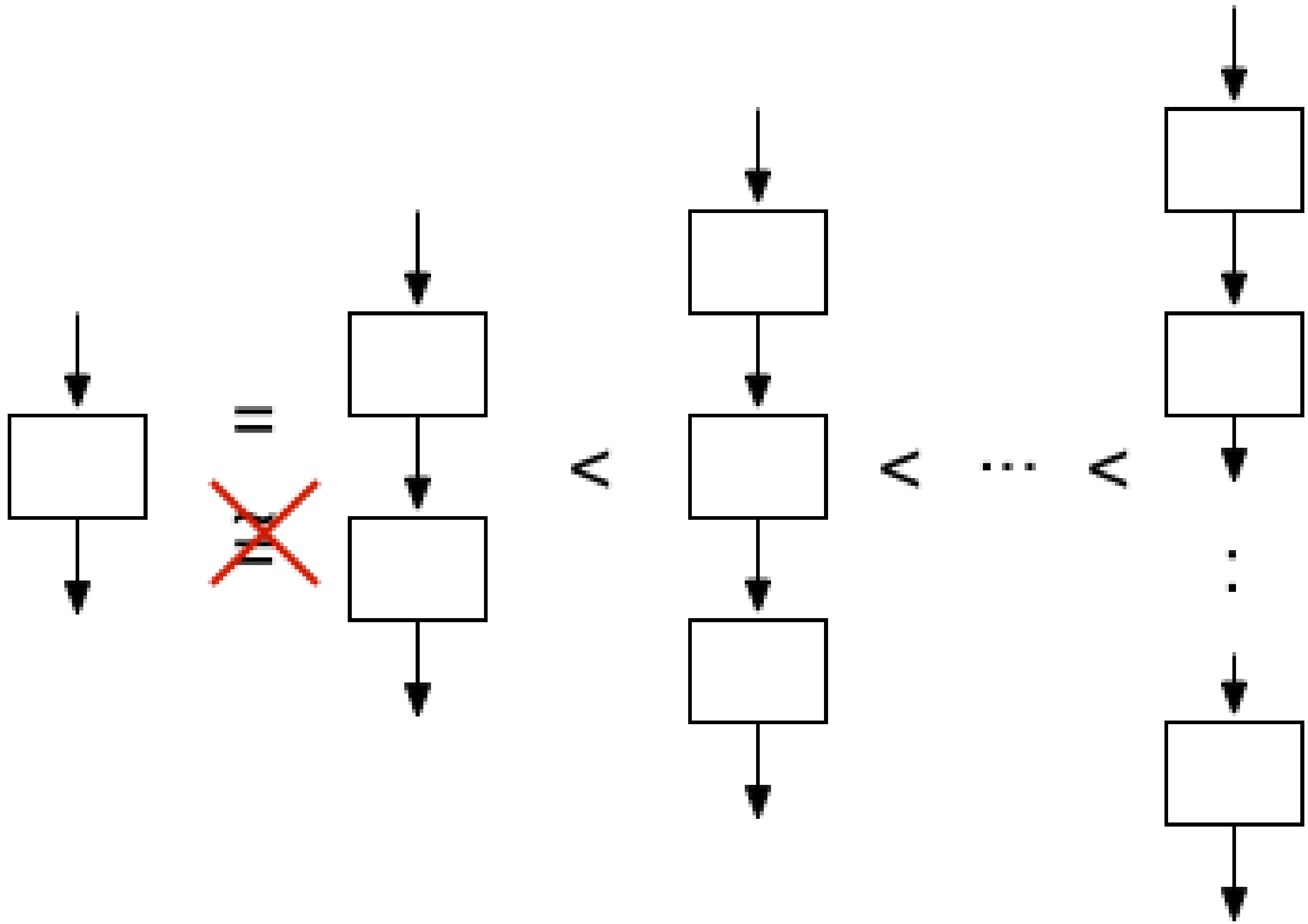
Cipher “is Group”



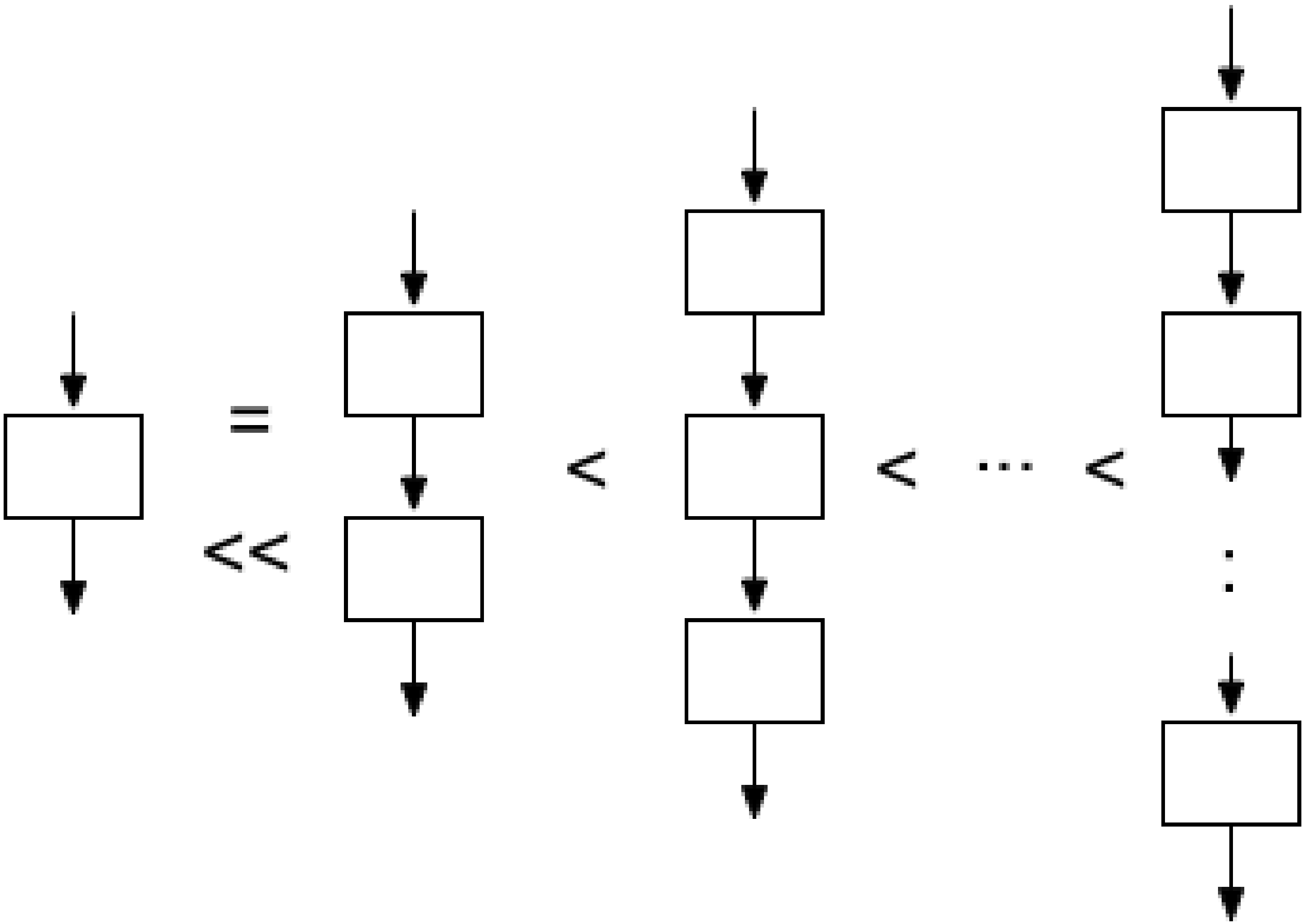
Could be =



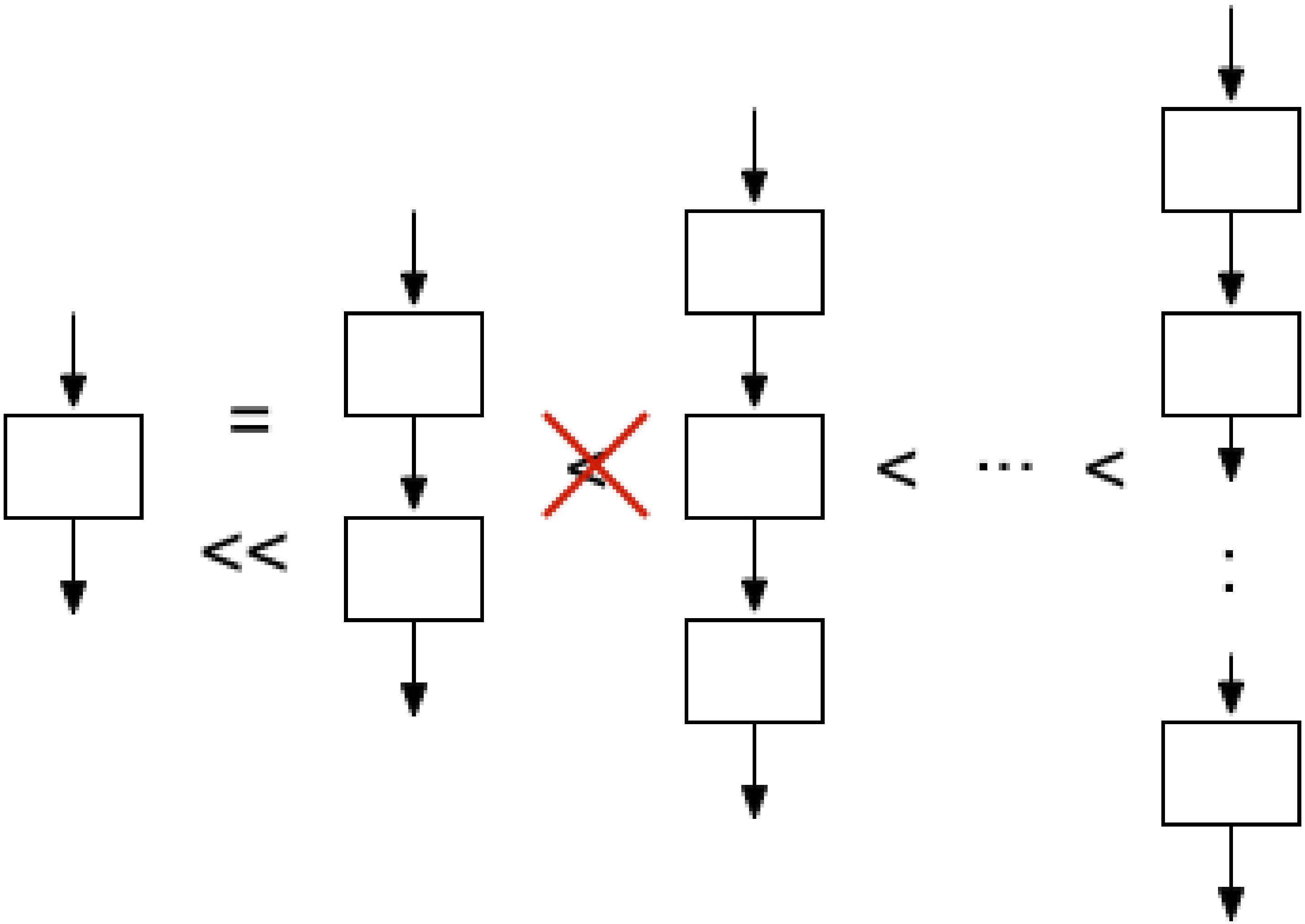
MITM *uses* ideal approx



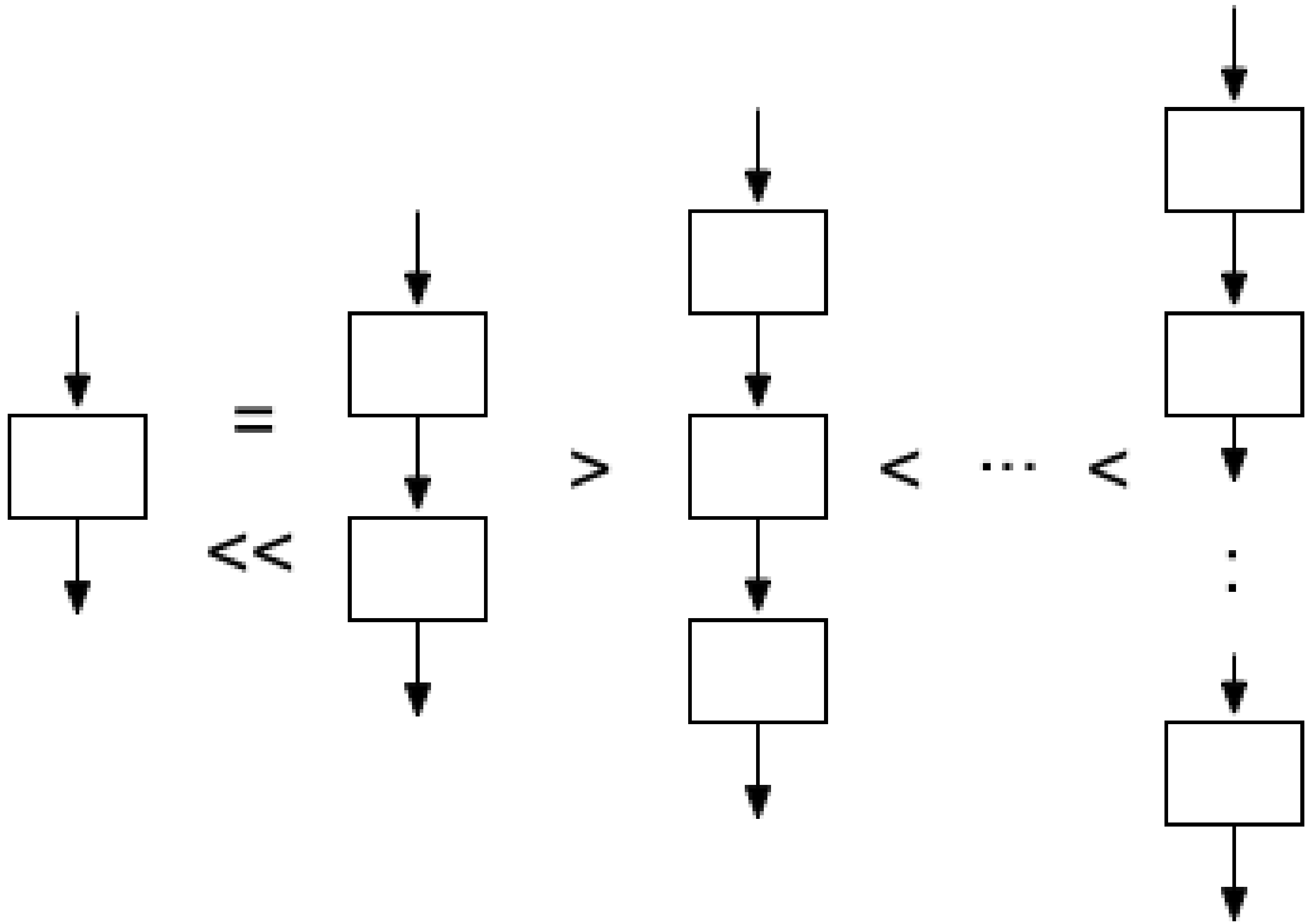
Pliam, 1998-99



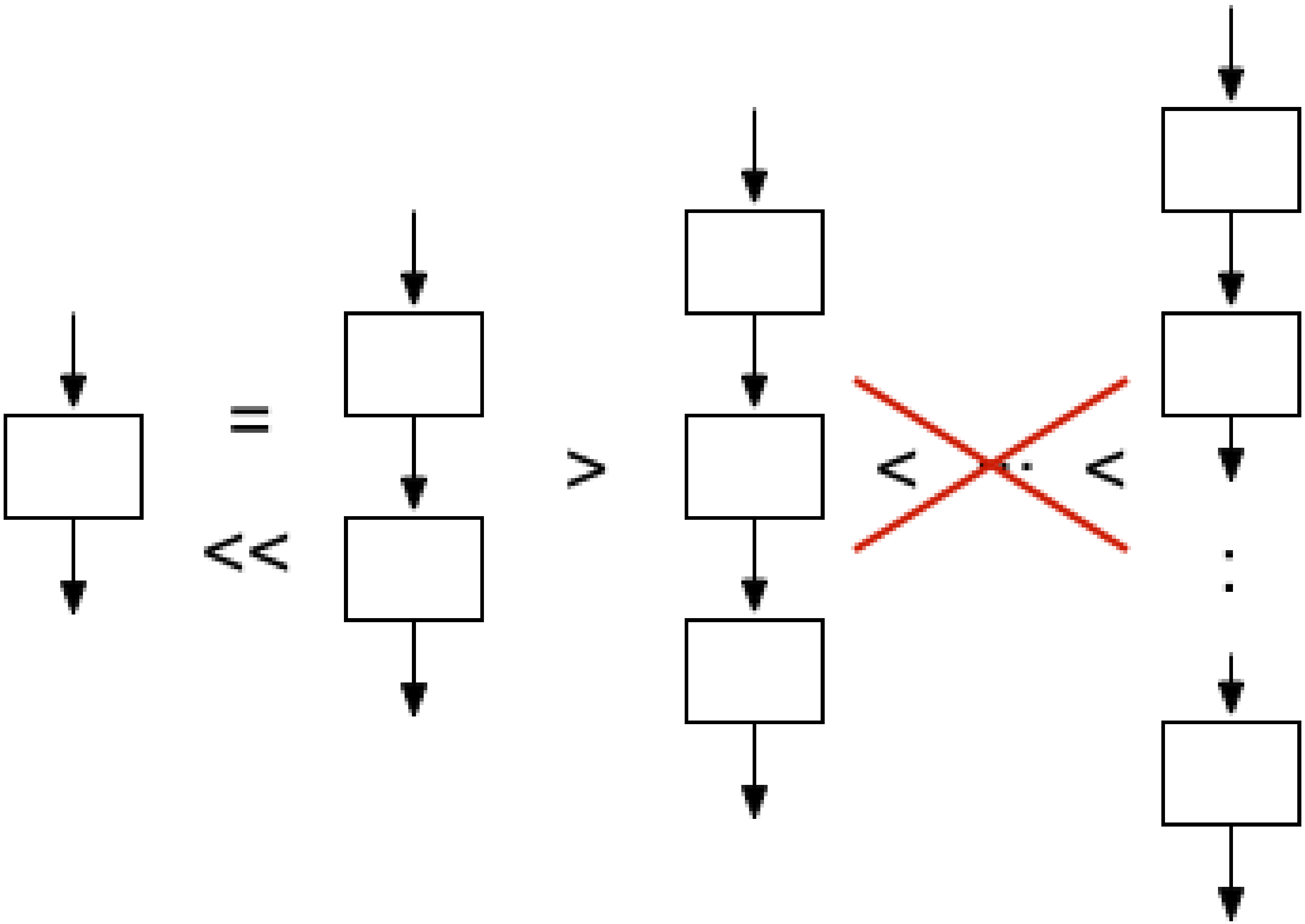
This Paper



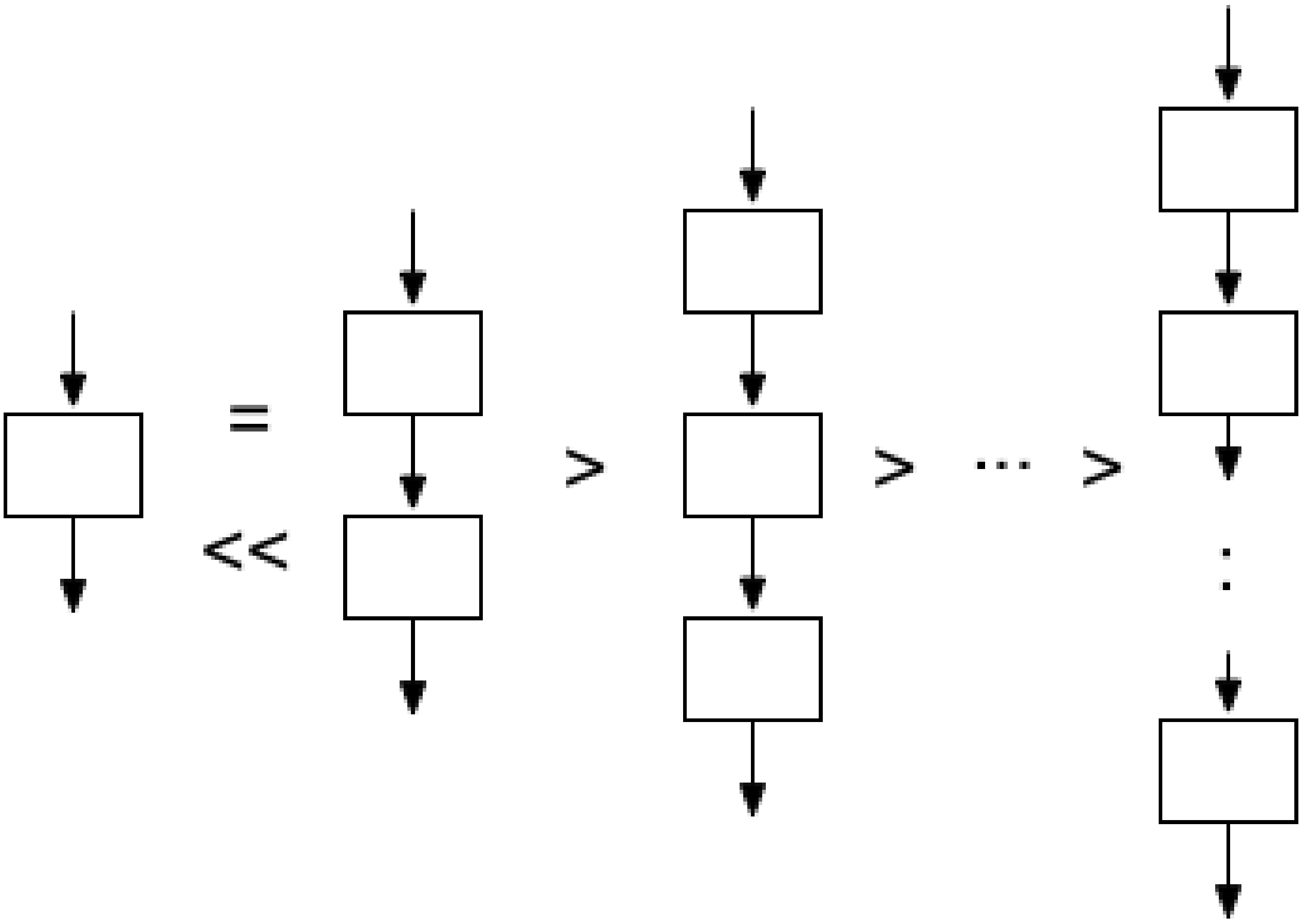
3-Fold Collapse



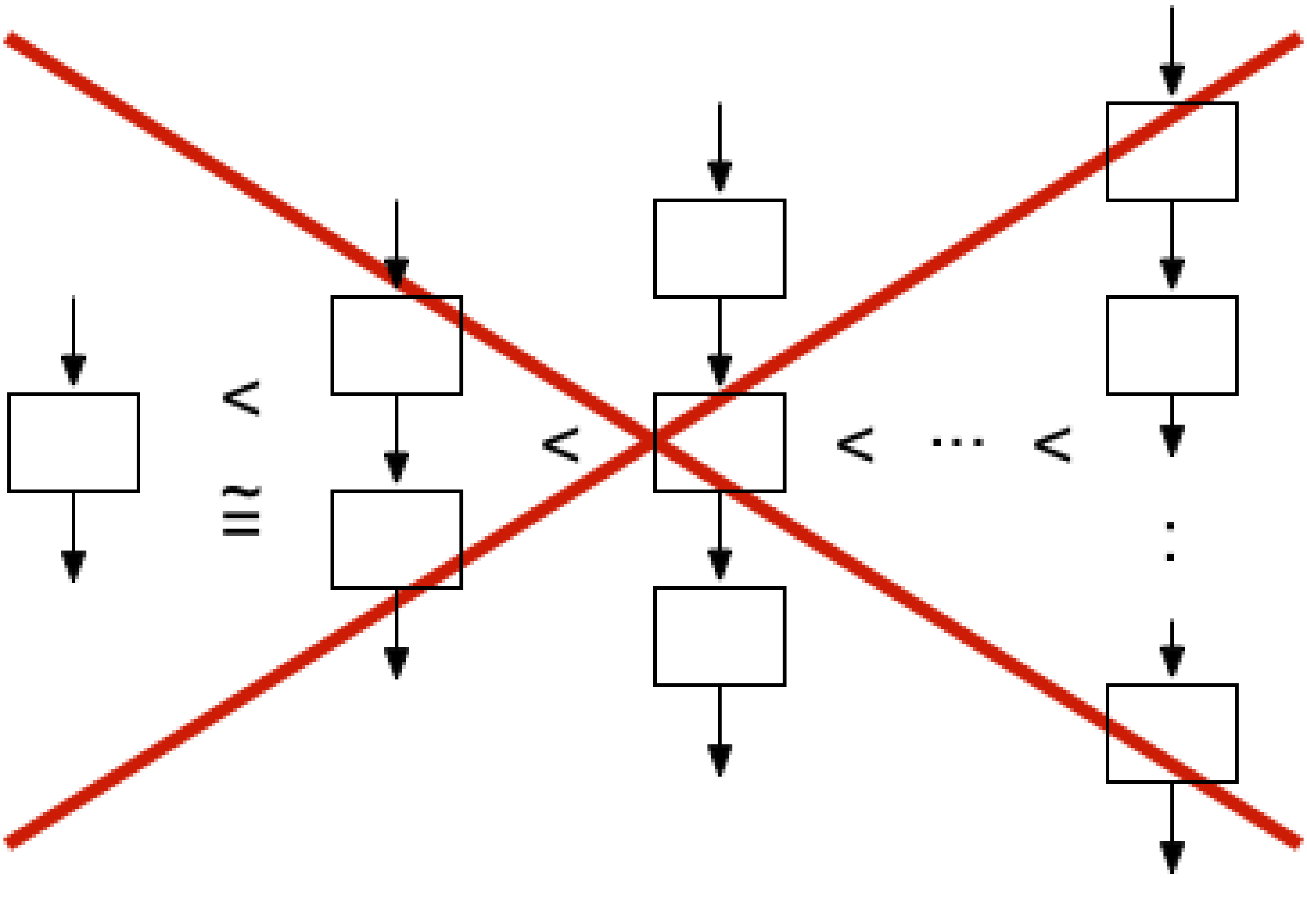
By Extension



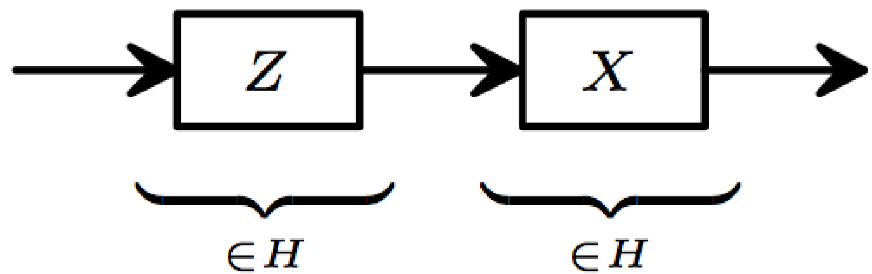
General Collapse

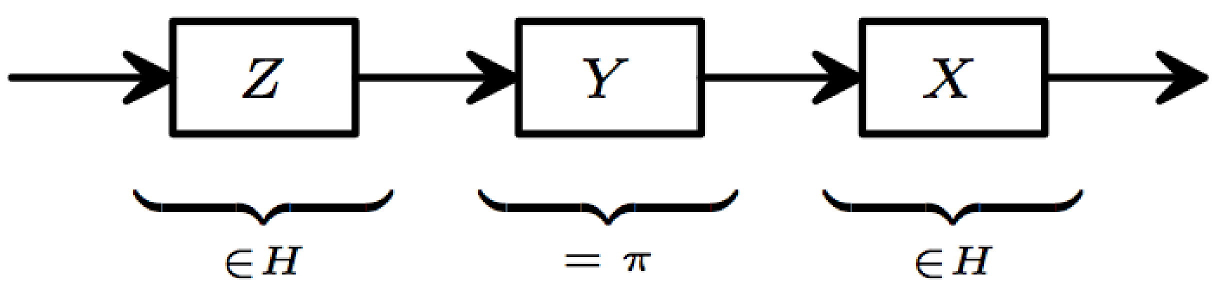


Report Card: F



3-Fold Expansion





support: $|H| \dashrightarrow |H \pi H|$

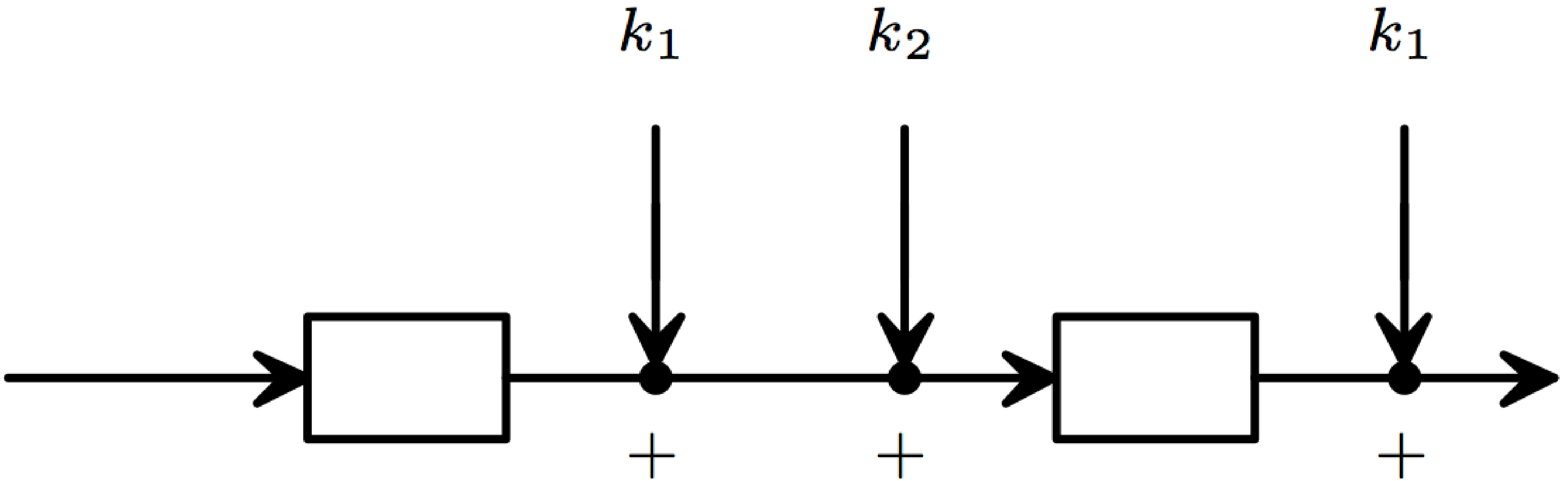
3-Fold Collapse

$$\longrightarrow \underbrace{\boxed{Z}}_{\in \pi H} \longrightarrow \underbrace{\boxed{X}}_{\in \pi H} \longrightarrow$$

$$\longrightarrow \underbrace{\boxed{Z}}_{\in \pi H} \longrightarrow \underbrace{\boxed{Y}}_{= \sigma} \longrightarrow \underbrace{\boxed{X}}_{\in \pi H} \longrightarrow$$

when $\sigma \in H\pi^{-1}$, support: $\quad |H\pi H| \dashrightarrow |H|$

Simplest Counterexample

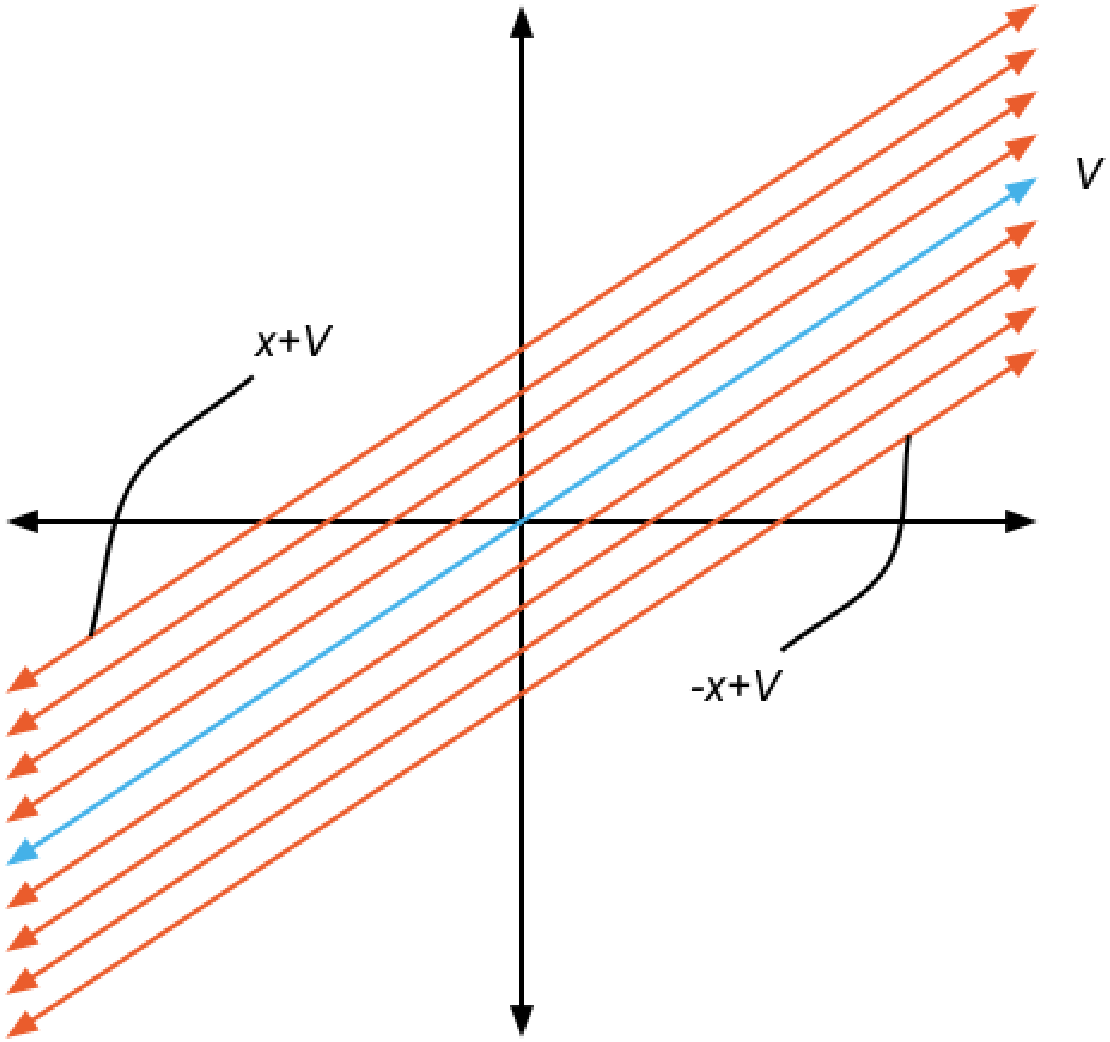


when $k_1 = k_2$, support collapses

Cosets

- **Fact**: the set of all permutations taking plaintext *p* to ciphertext *c*
  - Is *coset gH*,
  - Where *H* is subgroup, Stab(*p*)

Structure of Cosets



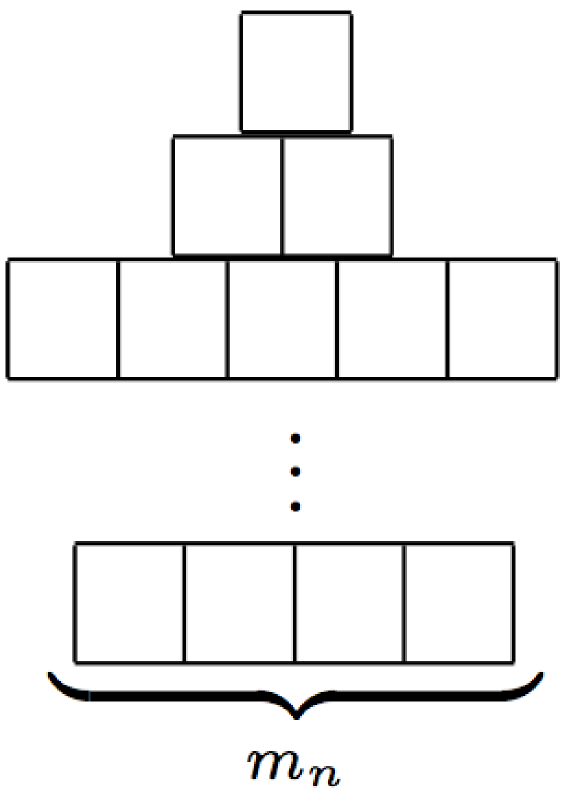
Extends to Nonabelian Case

	abelian	***nonabelian***
cosets	$x + V$	gH
Lagrange	$W = \bigcup x + V$	$G = \bigcup gH$
action	$\mathrm{y+(x+V) = (y+x)+V}$	$\mathrm{k(gH) = (kg)H}$
stabilizer	V	H

Orbit-Stabilizer Theorem

- **Thm**. Any (transitive) group action is equivalent to a coset action.

Double Cosets



HK

Hg_1K

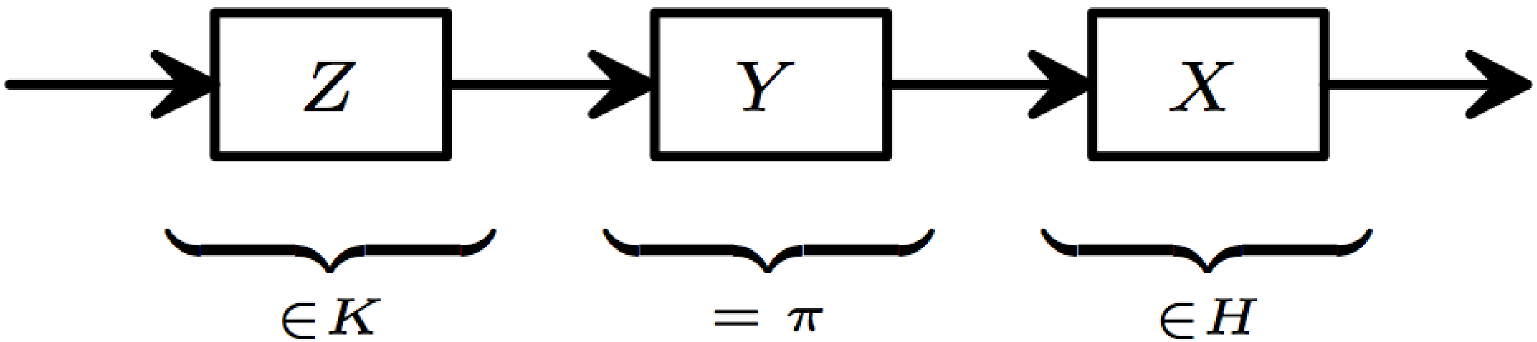
Hg_2K

$\vdots$

Hg_nK

$$m_i = [H : H \cap {}^{g_i}K]$$

Theorem 2

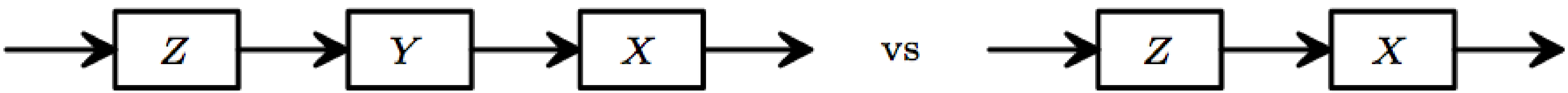


Thm. $T = XYZ$, $t = x * y * z$ is a convex direct sum

$$t = \bigoplus_{i=1}^{m} \alpha_i z_i,$$

where $m = [H{:}H \cap {}^{\pi}K]$ and $z_i \preceq z$.

Corollaries



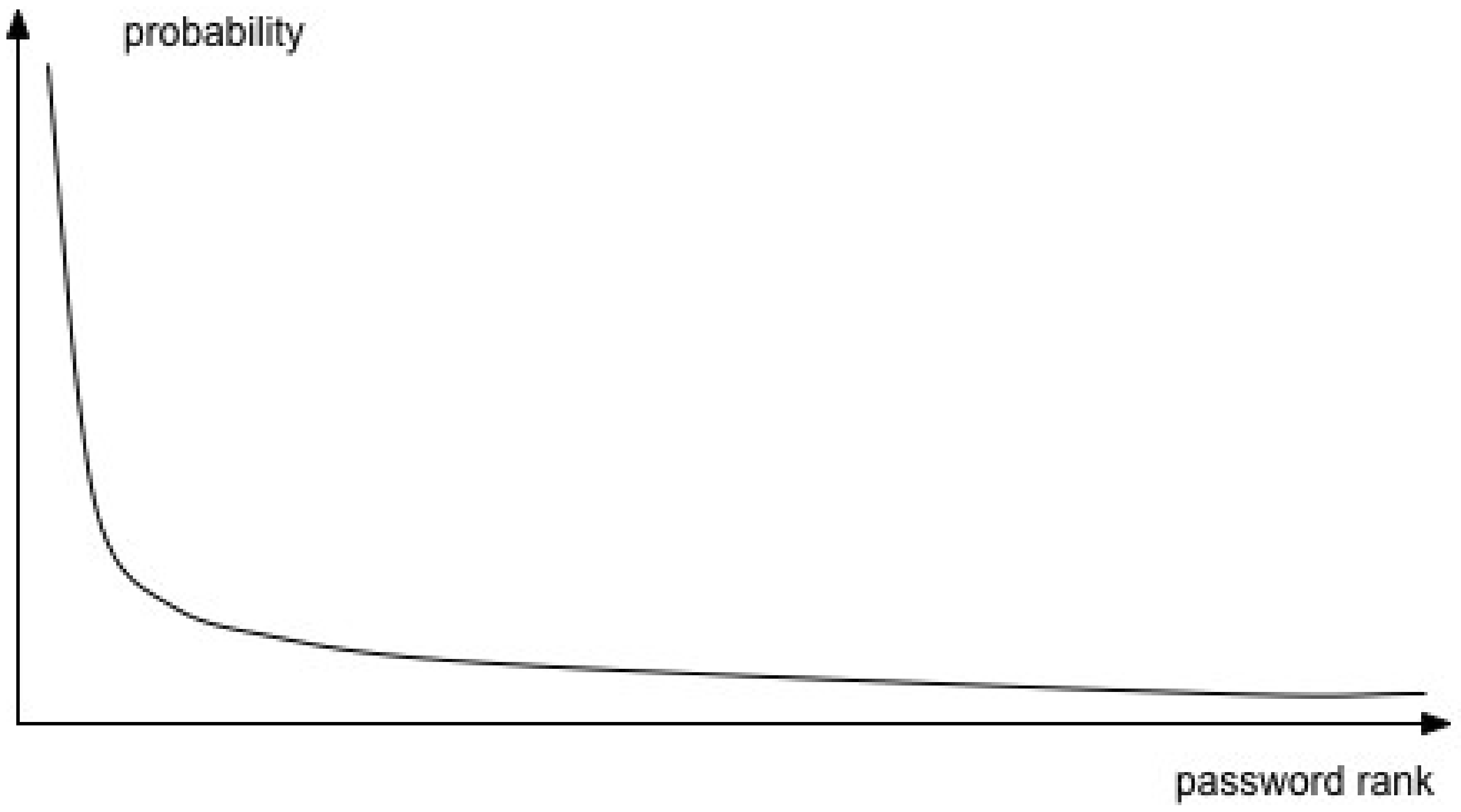
$$T = XYZ \text{ and } D = XZ$$

case1: $T = \Lambda D$

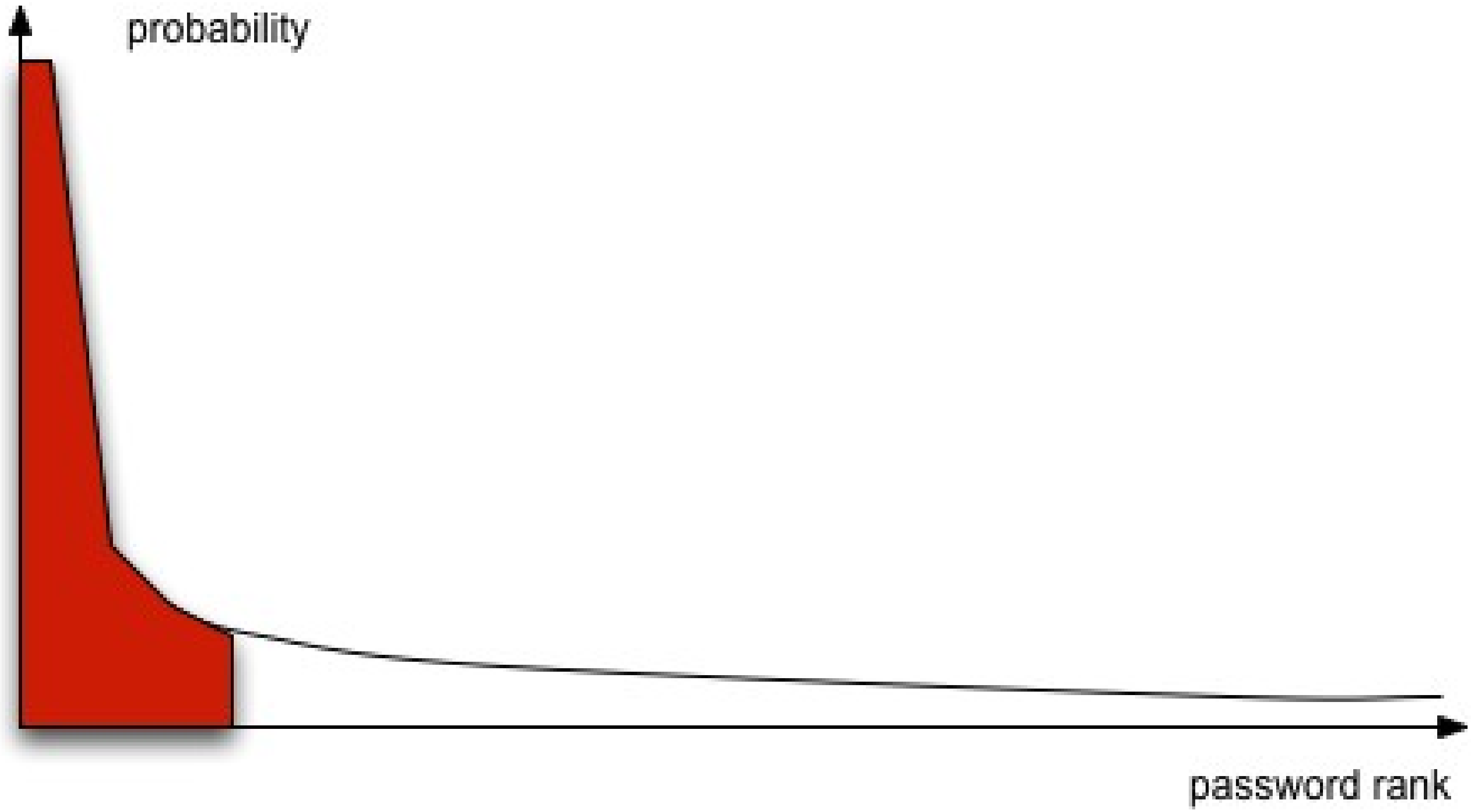
case2: $D = \Lambda' T$

Part II
Provable Security Comparisons

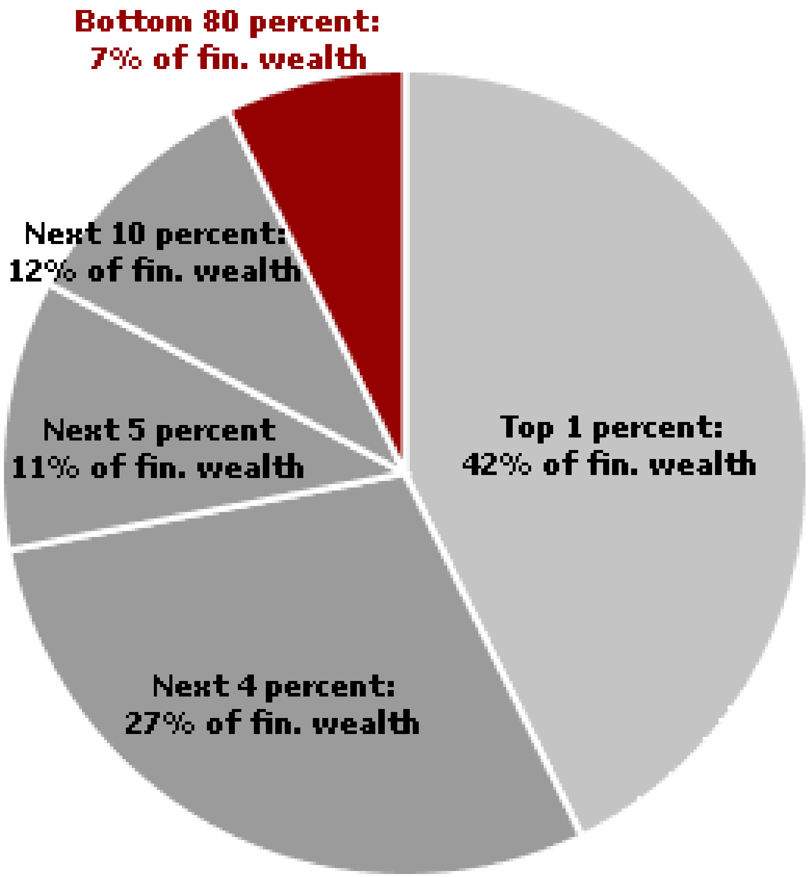
Passwords by Non-Increasing Likelihood



Cumulative Probability

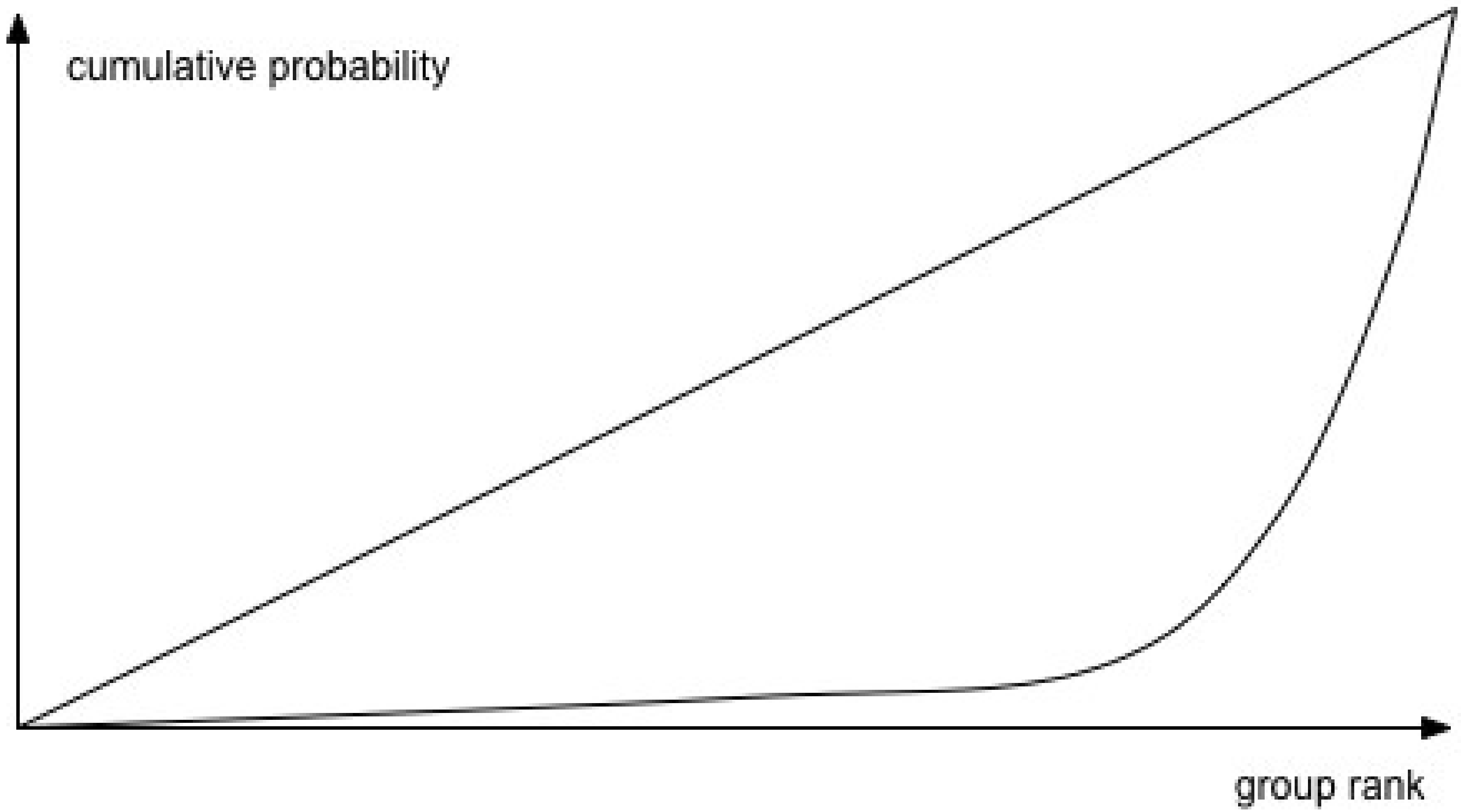


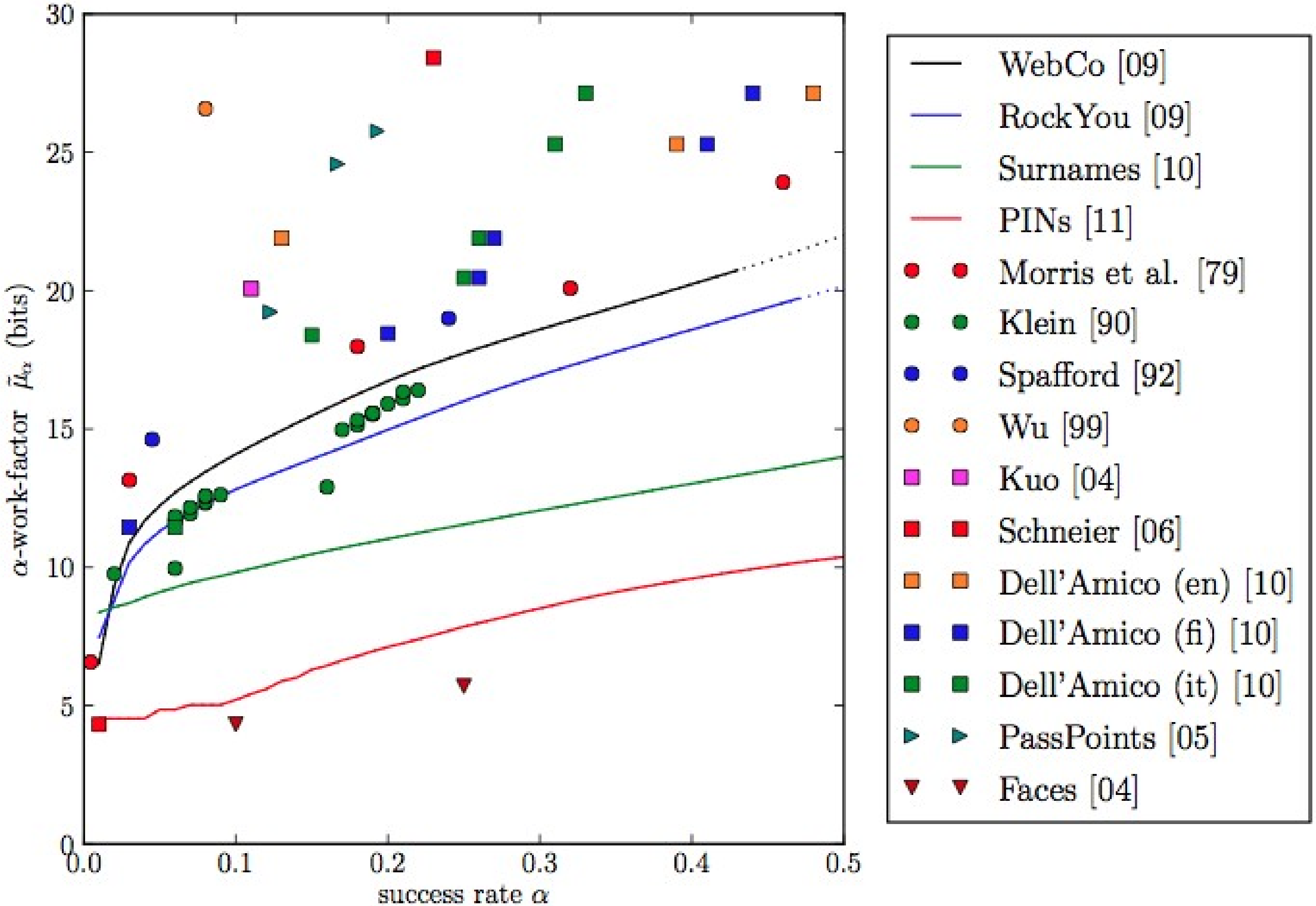
Sounds Familiar? “99%”



Financial wealth
distribution, 2007

Lorenz Curve c. 1910



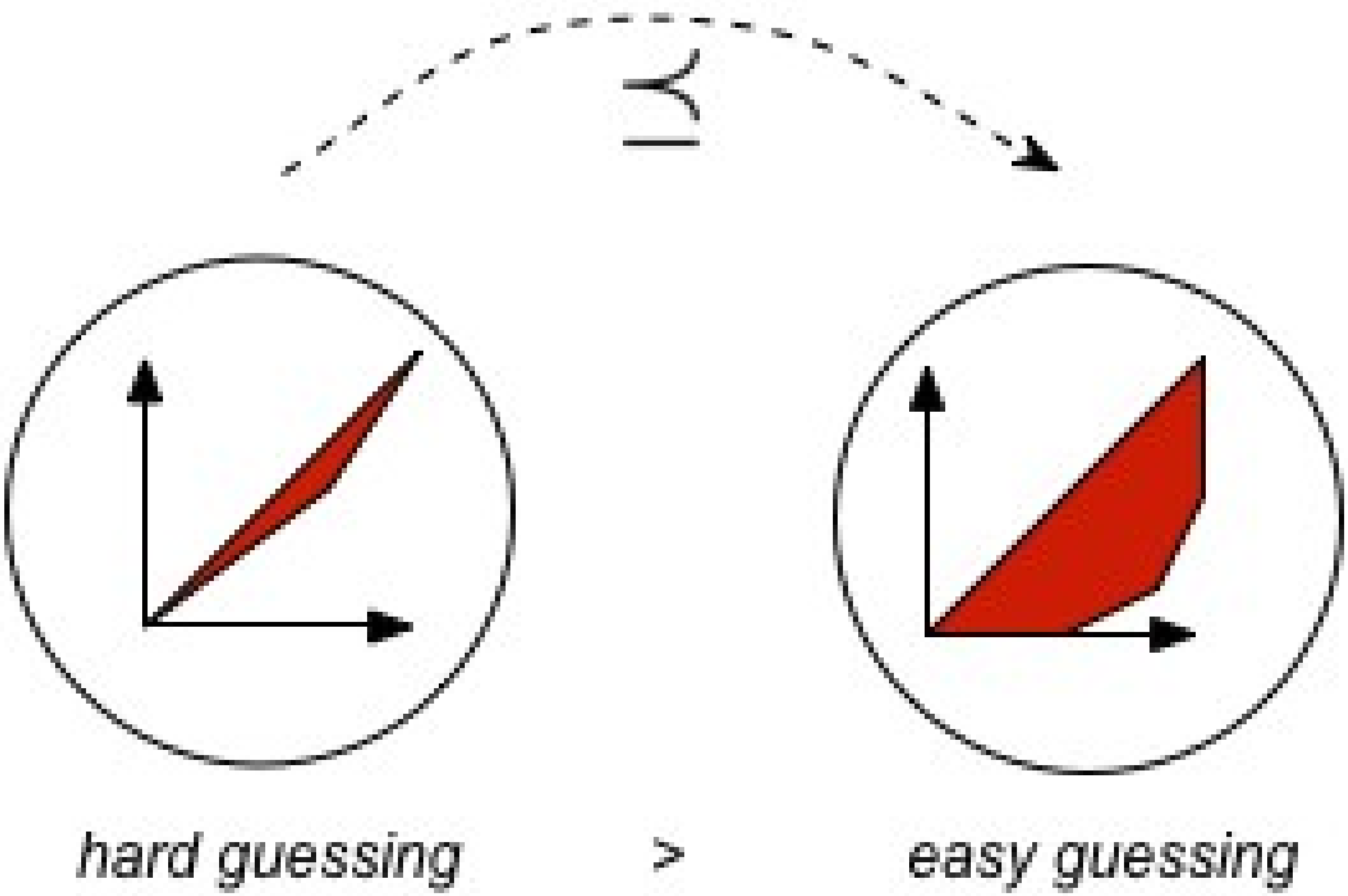


30
25
20
15
10
5
0
0.0
0.1
0.2
0.3
0.4
0.5
success rate α
α-work-factor $\tilde{\mu}_\alpha$ (bits)
WebCo [09]
RockYou [09]
Surnames [10]
PINs [11]
Morris et al. [79]
Klein [90]
Spafford [92]
Wu [99]
Kuo [04]
Schneier [06]
Dell'Amico (en) [10]
Dell'Amico (fi) [10]
Dell'Amico (it) [10]
PassPoints [05]
Faces [04]

Theory of Inequalities

- Schur, 1923
- Hardy, Littlewood & Polya, 1929
- Birkhoff, von Neumann ca. 1950

Majorization, Schur Convexity



Higher-Dim Diagrams ...

$$\begin{tikzcd} z \arrow[r, dotted, no head, "\preceq"] \arrow[d] & y \arrow[d] \\ H(Z) \arrow[r, dotted, no head, "\geq"] & H(Y) \end{tikzcd}
\quad
\begin{tikzcd} z \arrow[r, dotted, no head, "\preceq"] \arrow[d] & y \arrow[d] \\ H_\infty(Z) \arrow[r, dotted, no head, "\geq"] & H_\infty(Y) \end{tikzcd}
\quad
\begin{tikzcd} z \arrow[r, dotted, no head, "\preceq"] \arrow[d] & y \arrow[d] \\ H_\alpha(Z) \arrow[r, dotted, no head, "\geq"] & H_\alpha(Y) \end{tikzcd}
\quad
\begin{tikzcd} z \arrow[r, dotted, no head, "\preceq_q"] \arrow[d] & y \arrow[d] \\ \mathbf{Adv}_Z(q) \arrow[r, dotted, no head, "\leq"] & \mathbf{Adv}_Y(q) \end{tikzcd}$$

$$\begin{tikzcd} z \arrow[r, dotted, no head, "\preceq"] \arrow[d] & y \arrow[d] \\ G_0(Z) \arrow[r, dotted, no head, "\geq"] & G_0(Y) \end{tikzcd}
\quad
\begin{tikzcd} z \arrow[r, dotted, no head, "\preceq"] \arrow[d] & y \arrow[d] \\ G_1(Z) \arrow[r, dotted, no head, "\geq"] & G_1(Y) \end{tikzcd}
\quad
\begin{tikzcd} z \arrow[r, dotted, no head, "\preceq"] \arrow[d] & y \arrow[d] \\ G_\alpha(Z) \arrow[r, dotted, no head, "\geq"] & G_\alpha(Y) \end{tikzcd}
\quad
\begin{tikzcd} z \arrow[r, dotted, no head, "\preceq_q"] \arrow[d] & y \arrow[d] \\ W(Z|C,p) \arrow[r, dotted, no head, "\geq"] & W(Y|C,p) \end{tikzcd}$$

$$\begin{tikzcd} z \arrow[r, dotted, no head, "\preceq"] \arrow[d] & y \arrow[d] \\ w_\alpha(Z) \arrow[r, dotted, no head, "\geq"] & w_\alpha(Y) \end{tikzcd}
\quad
\begin{tikzcd} z \arrow[r, dotted, no head, "\preceq_q"] \arrow[d] & y \arrow[d] \\ \mathbf{Adv}_1(Z) \arrow[r, dotted, no head, "\leq"] & \mathbf{Adv}_1(Y) \end{tikzcd}
\quad
\begin{tikzcd} z \arrow[r, dotted, no head, "\preceq_q"] \arrow[d] & y \arrow[d] \\ \mathbf{Adv}_2(Z) \arrow[r, dotted, no head, "\leq"] & \mathbf{Adv}_2(Y) \end{tikzcd}
\quad
\begin{tikzcd} z \arrow[r, dotted, no head, "\preceq_q"] \arrow[d] & y \arrow[d] \\ \mathbf{Adv}_3(Z) \arrow[r, dotted, no head, "\leq"] & \mathbf{Adv}_3(Y) \end{tikzcd}$$

Higher Data Complexity?

$$\begin{tikzcd}
z \arrow[r, dotted, no head, "\preceq_q"] \arrow[d] & y \arrow[d] & \\
\hat{z} \arrow[r, dotted, no head, "\preceq"] \arrow[d] & \hat{y} \arrow[d] & \in \mathbb{R}\uparrow_H^G \\
\mathbf{Adv}_Z(q) \arrow[r, dotted, no head, "\leq"'] & \mathbf{Adv}_Y(q) &
\end{tikzcd}$$

$$\begin{tikzcd}
z \arrow[r, dotted, no head, "\preceq_q"] \arrow[d] & y \arrow[d] & \in \mathbb{R}H\uparrow_H^G \\
\hat{z} \arrow[r, dotted, no head, "\preceq"] \arrow[d] & \hat{y} \arrow[d] & \\
W(Z|C,p) \arrow[r, dotted, no head, "\geq"'] & W(Y|C,p) &
\end{tikzcd}$$

Kronecker-Like Formula

When $z \preceq y$ with $z = Dy$ and D "like" $Z = XY$,

$$z_{\downarrow}^{(i)} = \sum_{i=1}^{[G:H]} \omega_{ij} D_{ij} y_{\downarrow}^{(i)},$$

where $[\omega_{ij}]$ and each D_{ij} are doubly stochastic.

Diagram Chase ...

$$
\begin{tikzcd}
z \arrow[r, dash, dotted, "\preceq_q"] \arrow[d] & y \arrow[d, "y \mapsto {[y(g_i H)]}"] & \\
\hat{z} \arrow[r, dash, dotted, "\preceq"] \arrow[d, "\|* - u\|"'] & \hat{y} \arrow[d, "\|* - u\|"] & \in \mathbb{R}\!\uparrow_H^G \\
\mathbf{Adv}_Z(q) \arrow[r, dash, dotted, "\leq"'] & \mathbf{Adv}_Y(q) &
\end{tikzcd}
$$

$$
\begin{tikzcd}
z \arrow[r, dash, dotted, "\preceq_q"] \arrow[d] & y \arrow[d, "y \mapsto \sum y_{\downarrow}^{(i)}"] & \in \mathbb{R}H\!\uparrow_H^G \\
\hat{z} \arrow[r, dash, dotted, "\preceq"] \arrow[d, "W(*)"'] & \hat{y} \arrow[d, "W(*)"] & \\
W(Z|C,p) \arrow[r, dash, dotted, "\geq"'] & W(Y|C,p) &
\end{tikzcd}
$$

Filling In Details

$$\longrightarrow \boxed{Z} \longrightarrow \boxed{Y} \longrightarrow \boxed{X} \longrightarrow \quad \text{vs} \quad \longrightarrow \boxed{Z} \longrightarrow \boxed{X} \longrightarrow$$

$T = XYZ$ and $D = XZ$

case1: $T = \Lambda D$;

$$t \preceq_q d, H(T) \geq H(D), \mathbf{Adv}(T) \leq \mathbf{Adv}(D), \ldots$$

case2: $D = \Lambda' T$;

$$d \preceq_q t, H(D) \geq H(T), \mathbf{Adv}(D) \leq \mathbf{Adv}(T), \ldots$$

Summary

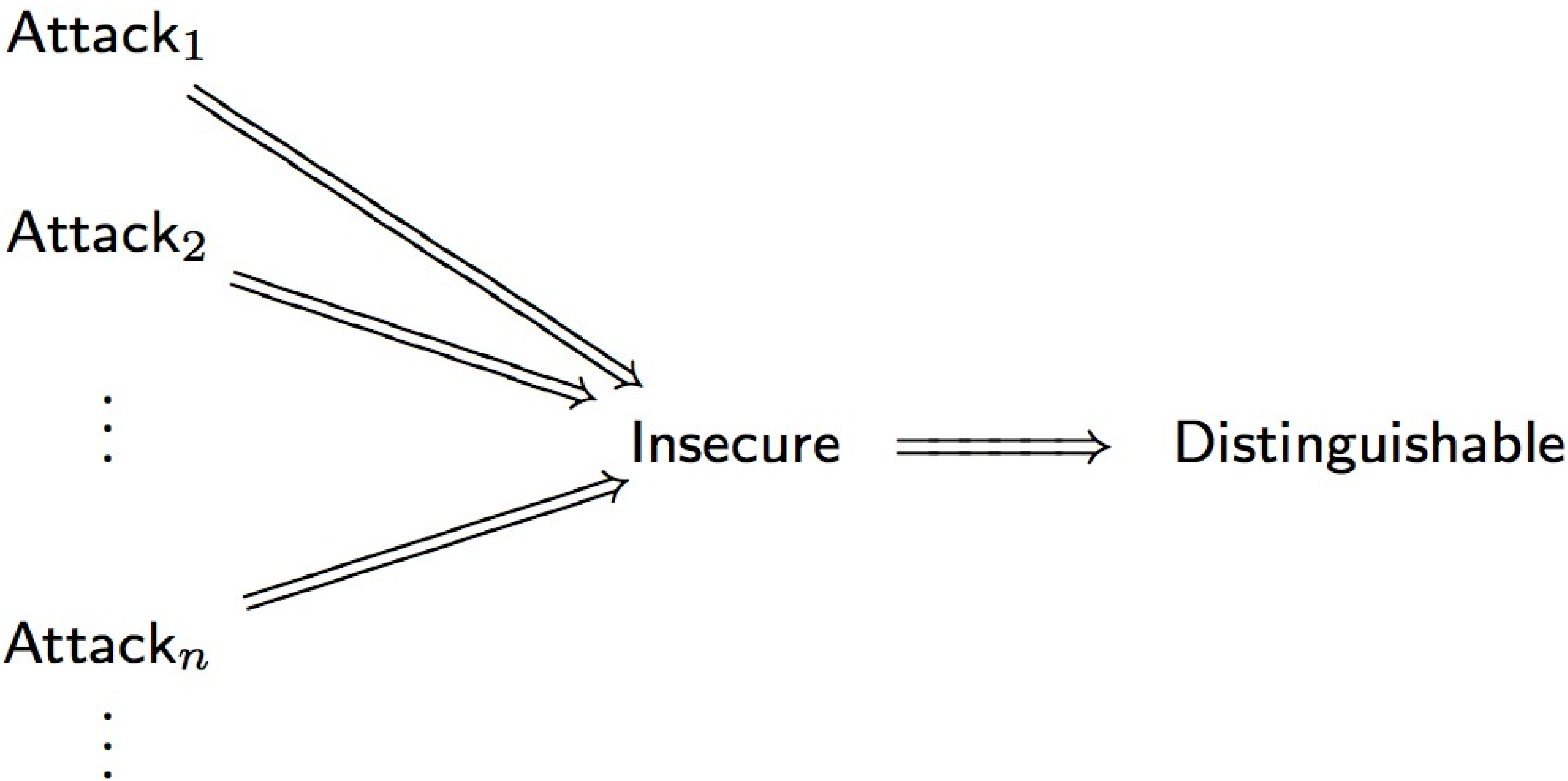
$$\longrightarrow \boxed{Z} \longrightarrow \boxed{Y} \longrightarrow \boxed{X} \longrightarrow \quad \text{vs} \quad \longrightarrow \boxed{Z} \longrightarrow \boxed{X} \longrightarrow$$

- Security ordering of alternating product *depends strongly* on internal structure.
- Expansion/Collapse along *double cosets*
- Comparing via *majorization* leads to coherence across many (*Schur-convex*) metrics

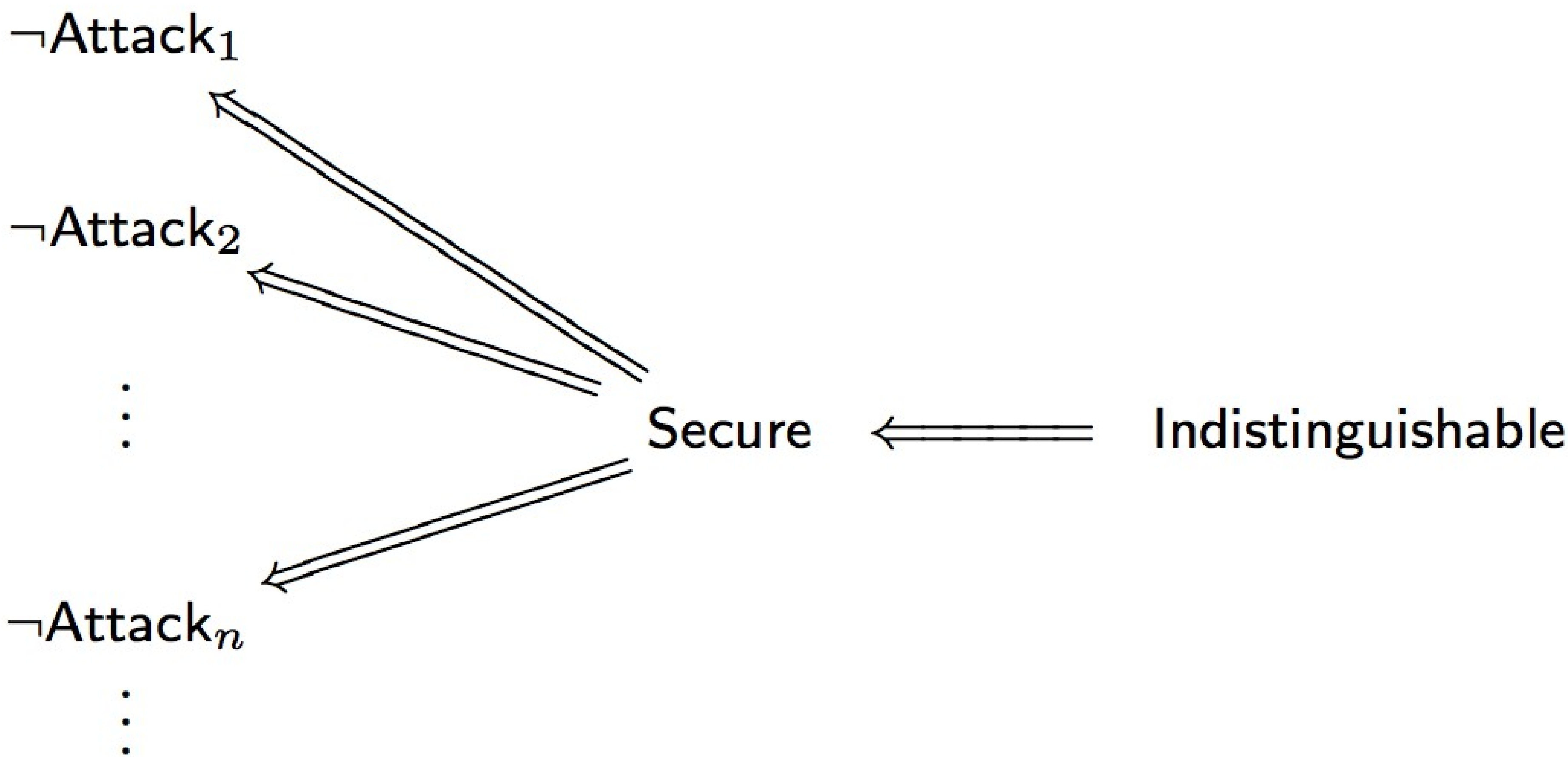
Epilogue

Provable Security Implications

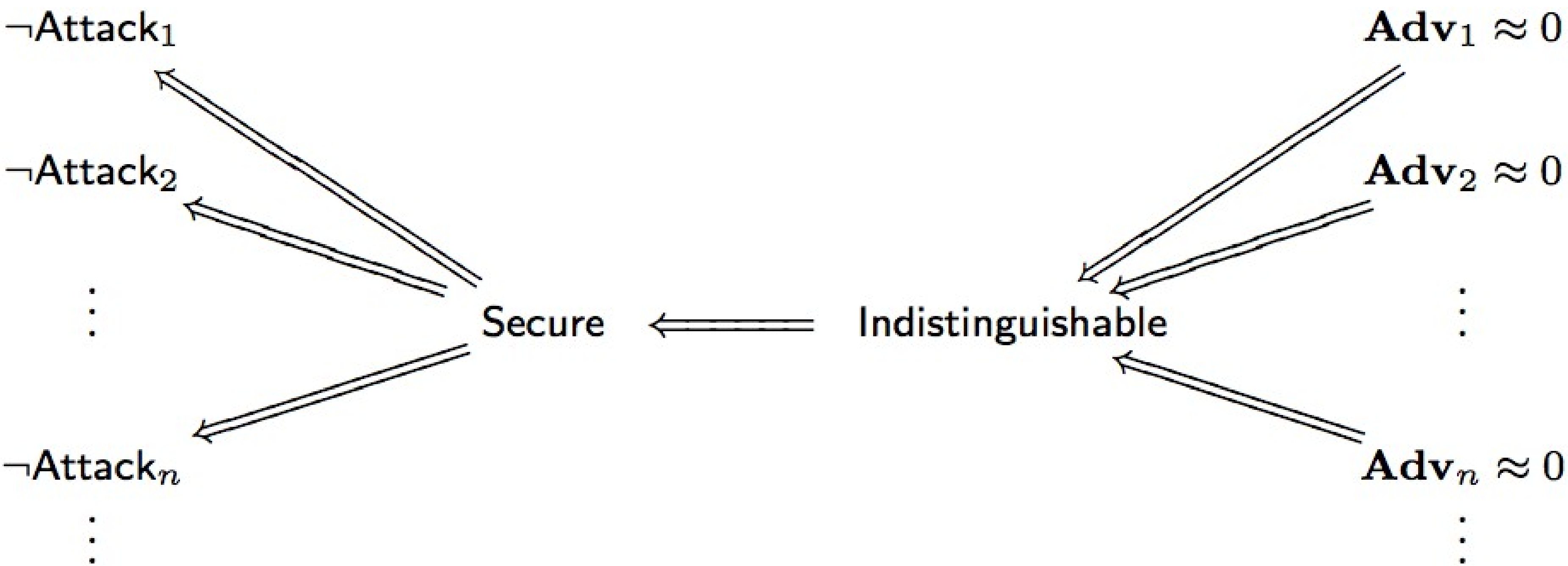
Provable Security



Indistinguishability



Advantage Proliferation



Need To Prune

- **Hypothesis**: To prune out the “bad” **Adv**'s, focus on those preserving order (*majorization*).