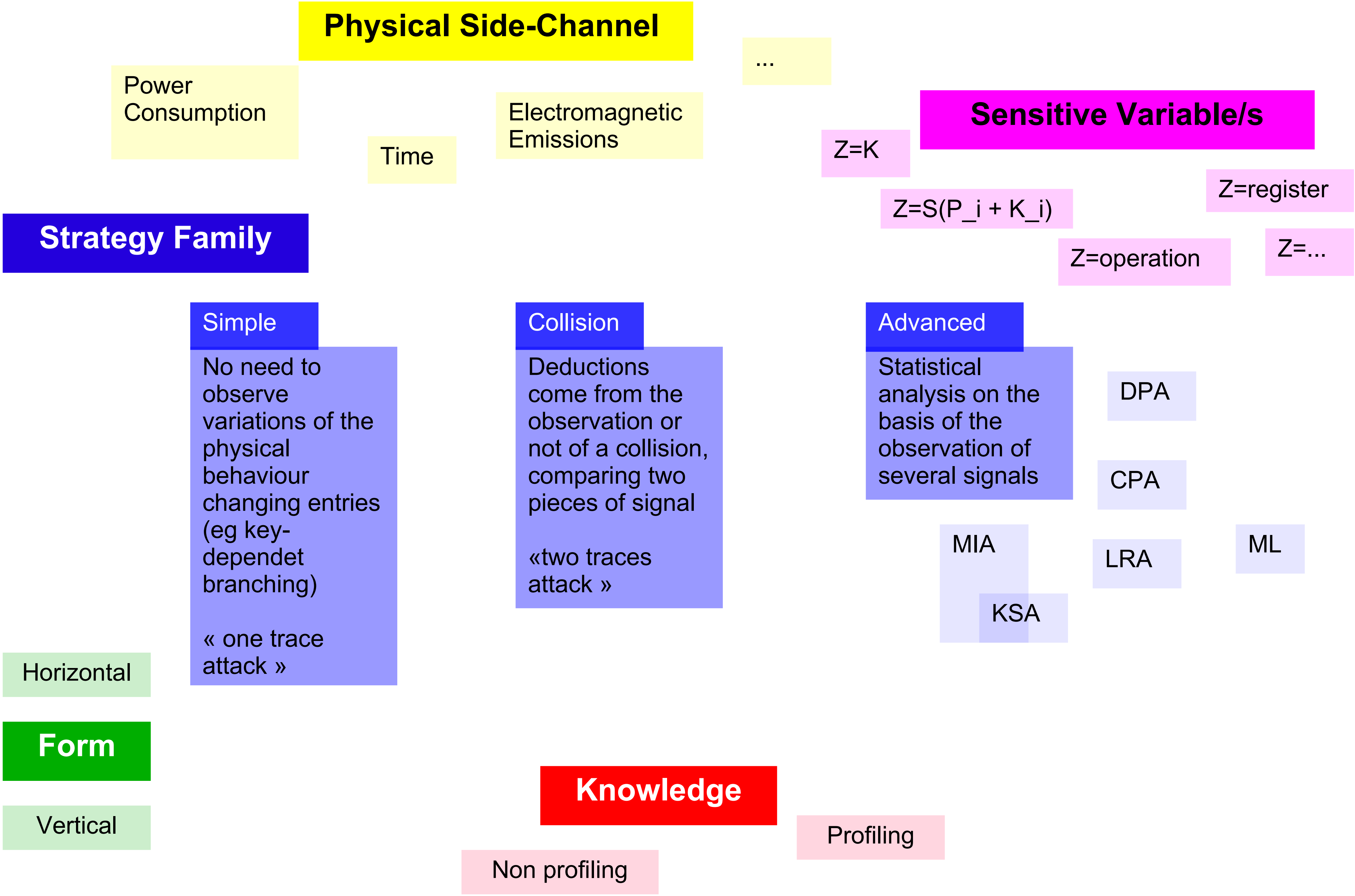


Physical Side-Channel

Power Consumption

Time

Electromagnetic Emissions

...

Sensitive Variable/s

Z=K

Z=S(P_i + K_i)

Z=register

Z=operation

Z=...

Strategy Family

Simple

No need to observe variations of the physical behaviour changing entries (eg key-dependet branching)

« one trace attack »

Collision

Deductions come from the observation or not of a collision, comparing two pieces of signal

«two traces attack »

Advanced

Statistical analysis on the basis of the observation of several signals

DPA

CPA

MIA

LRA

ML

KSA

Horizontal

Form

Vertical

Knowledge

Non profiling

Profiling

Physical Side-Channel

Power Consumption

Time

Electromagnetic Emissions

...

Sensitive Variable/s

Z=K

Z=S(P_i + K_i)

Z=register

Z=operation

Z=...

Strategy Family

Simple

No need to observe variations of the physical behaviour changing entries

« one trace attack »

Collision

Deductions come from the observation or not of a collision, comparing two pieces of signal

«two traces attack »

Advanced

Statistical analysis on the basis of the observation of several signals

DPA

CPA

MIA

LRA

ML

KSA

- Leakage model m(Z)
- key hypotheses
- compute Z under hypotheses
- predict physical observation via m(Z)
- compare predictions and acquisitions via a « distinuguisher »

Form

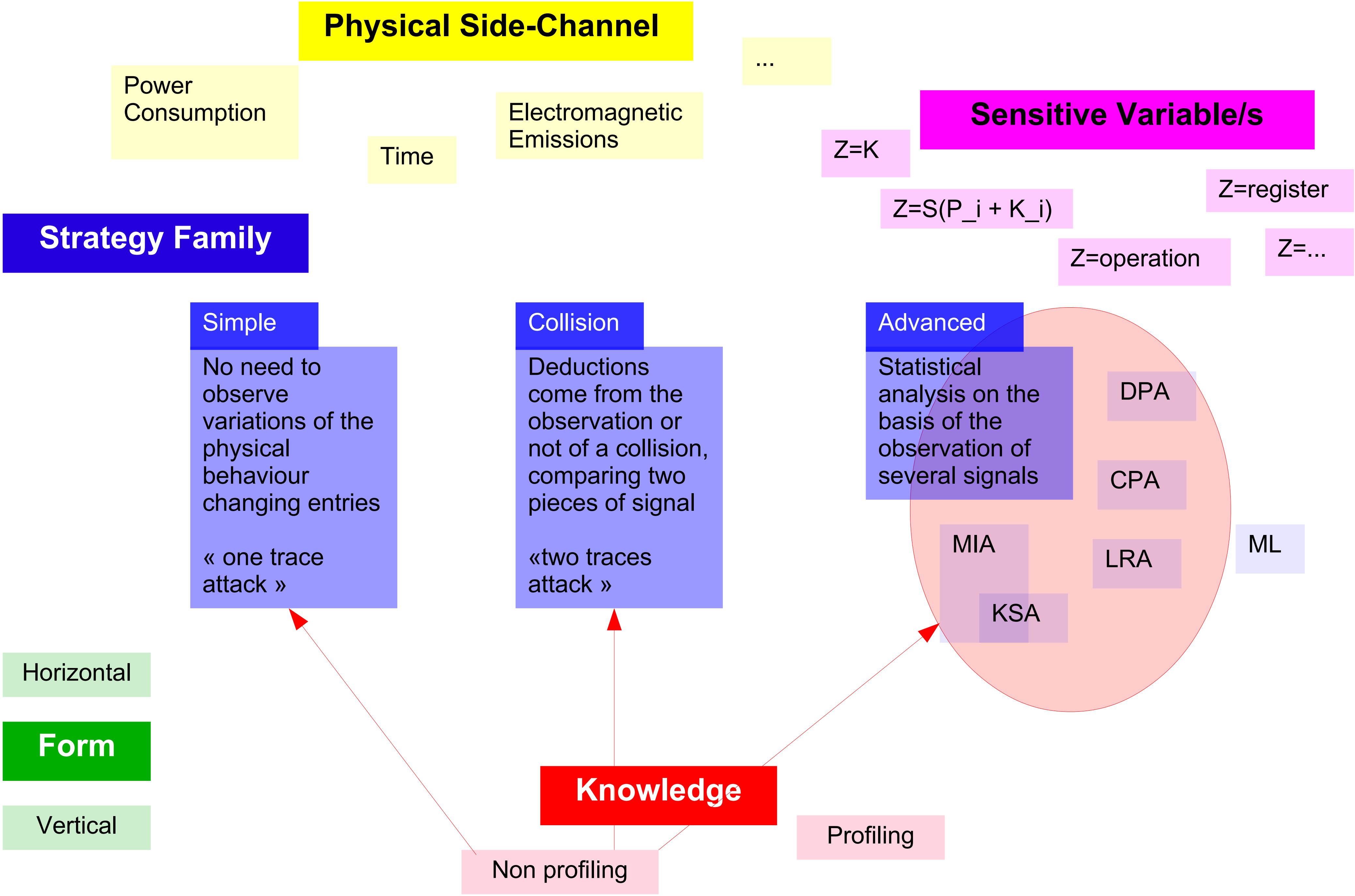
Horizontal

Vertical

Knowledge

Non profiling

Profiling



Physical Side-Channel

Power Consumption

Time

Electromagnetic Emissions

...

Sensitive Variable/s

Z=K

Z=S(P_i + K_i)

Z=register

Z=operation

Z=...

Strategy Family

Simple

No need to observe variations of the physical behaviour changing entries

« one trace attack »

Collision

Deductions come from the observation or not of a collision, comparing two pieces of signal

«two traces attack »

Advanced

Statistical analysis on the basis of the observation of several signals

Horizontal

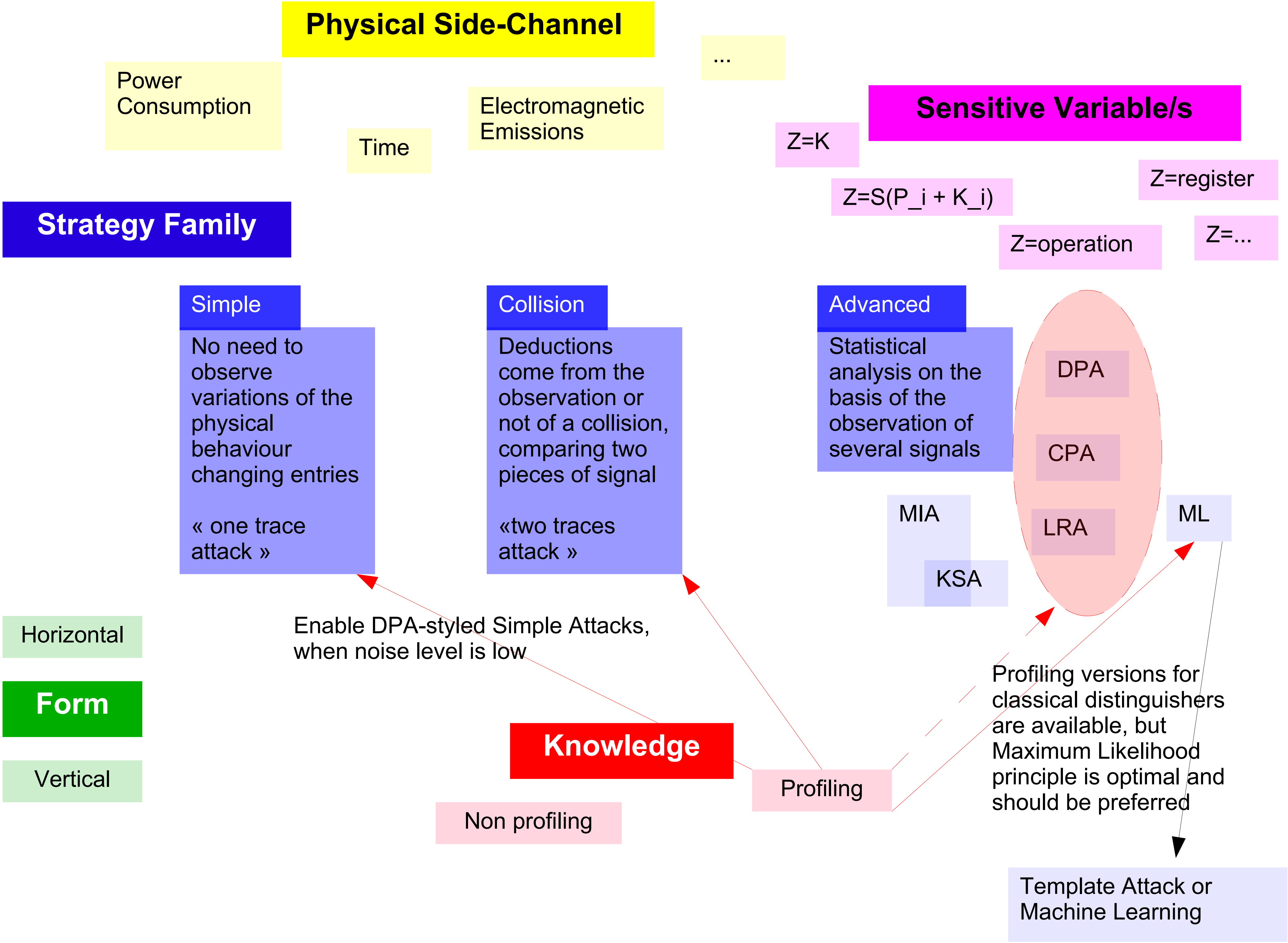
Form

Vertical

Knowledge

Non profiling

Profiling



Physical Side-Channel

Power Consumption

Time

Electromagnetic Emissions

...

Sensitive Variable/s

Z=K

Z=S(P_i + K_i)

Z=register

Z=operation

Z=...

Strategy Family

Simple

No need to observe variations of the physical behaviour changing entries

« one trace attack »

Collision

Deductions come from the observation or not of a collision, comparing two pieces of signal

«two traces attack »

Advanced

Statistical analysis on the basis of the observation of several signals

DPA

CPA

LRA

MIA

KSA

ML

Horizontal

Form

Vertical

Enable DPA-styled Simple Attacks, when noise level is low

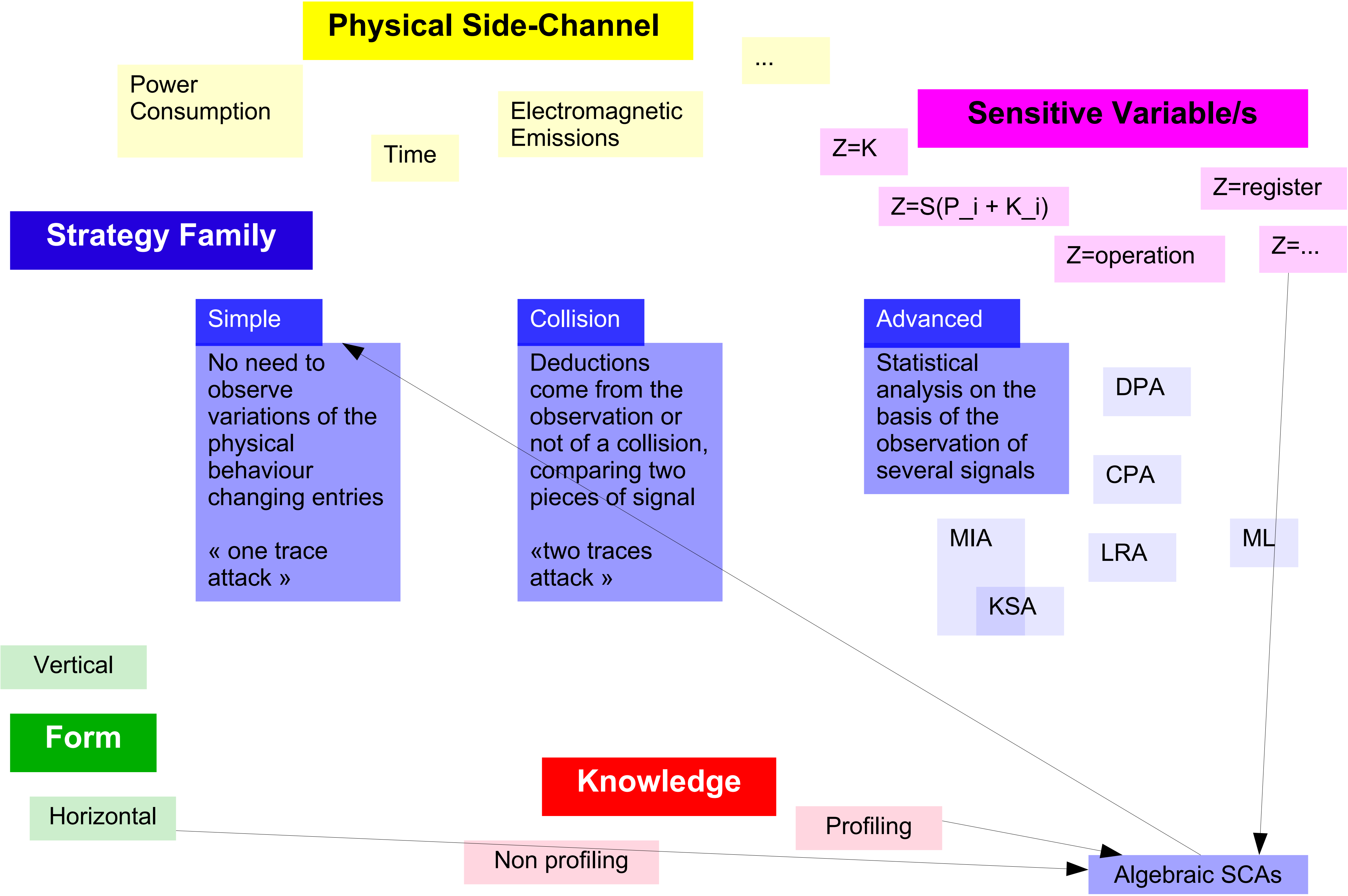
Knowledge

Profiling

Non profiling

Profiling versions for classical distinguishers are available, but Maximum Likelihood principle is optimal and should be preferred

Template Attack or Machine Learning



Physical Side-Channel

Power Consumption

Time

Electromagnetic Emissions

...

Sensitive Variable/s

Z=K

Z=S(P_i + K_i)

Z=register

Z=operation

Z=...

Strategy Family

Simple

No need to observe variations of the physical behaviour changing entries

« one trace attack »

Collision

Deductions come from the observation or not of a collision, comparing two pieces of signal

«two traces attack »

Advanced

Statistical analysis on the basis of the observation of several signals

DPA

CPA

MIA

LRA

ML

KSA

Vertical

Form

Horizontal

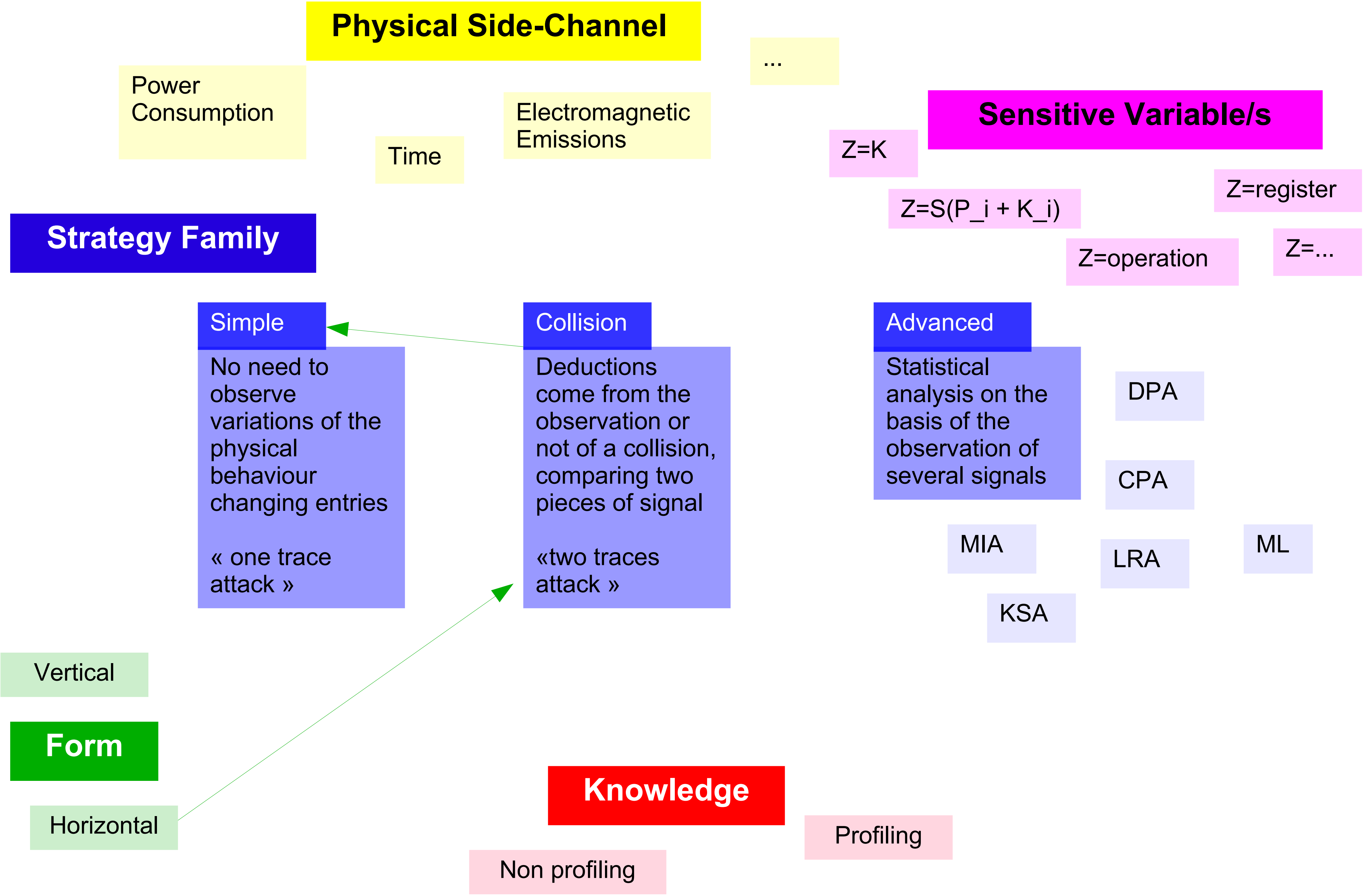
Knowledge

Profiling

Non profiling

Algebraic SCAs

No divide-and-conquer
Z \in ALL intermediate variables



Physical Side-Channel

Power Consumption

Time

Electromagnetic Emissions

...

Sensitive Variable/s

Z=K

Z=S(P_i + K_i)

Z=register

Z=operation

Z=...

Strategy Family

Simple

No need to observe variations of the physical behaviour changing entries

« one trace attack »

Collision

Deductions come from the observation or not of a collision, comparing two pieces of signal

«two traces attack »

Advanced

Statistical analysis on the basis of the observation of several signals

DPA

CPA

MIA

LRA

ML

KSA

Form

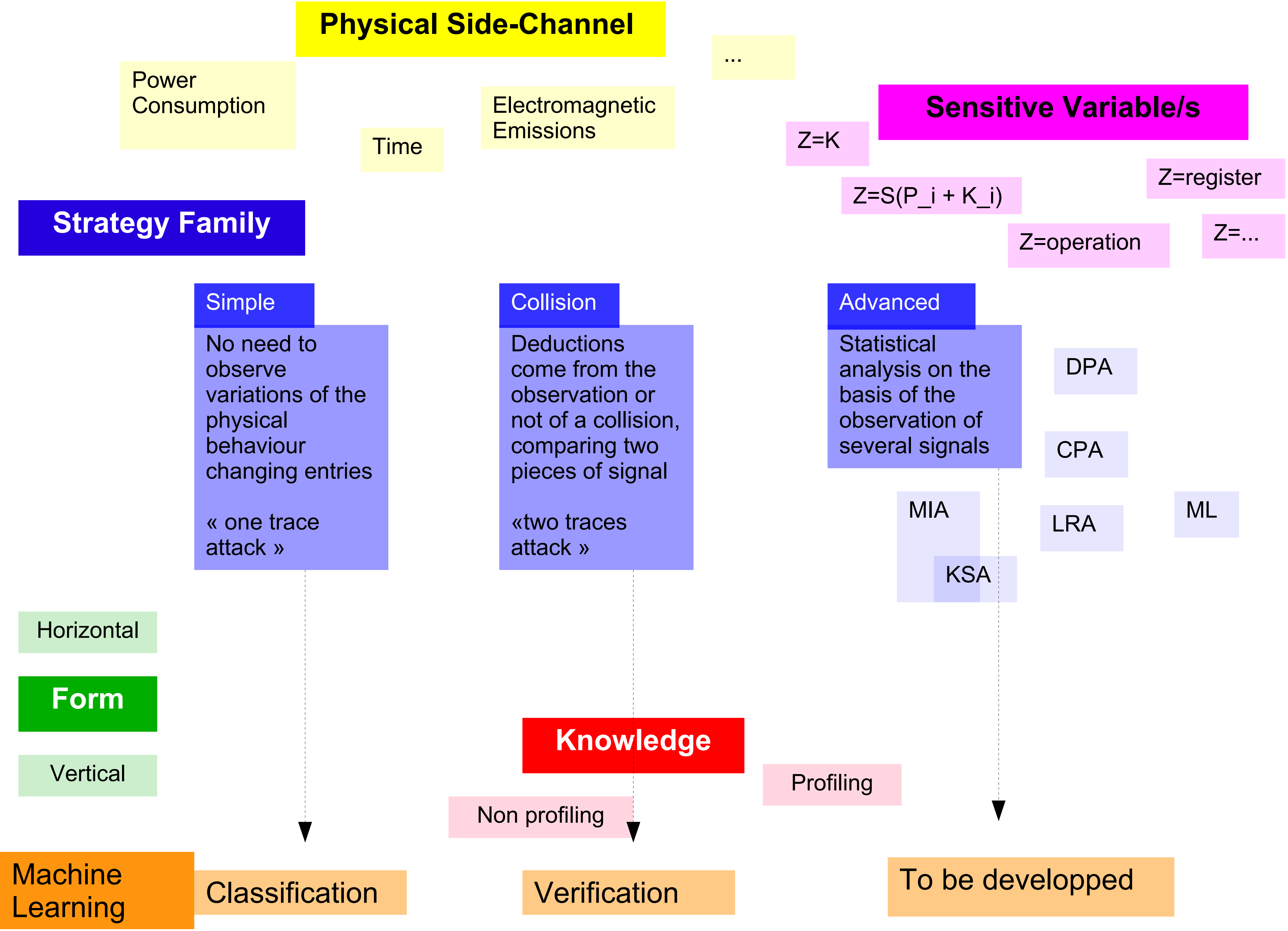
Vertical

Horizontal

Knowledge

Non profiling

Profiling



Physical Side-Channel

Power Consumption

Time

Electromagnetic Emissions

...

Sensitive Variable/s

Z=K

Z=S(P_i + K_i)

Z=register

Z=operation

Z=...

Strategy Family

Simple

No need to observe variations of the physical behaviour changing entries

« one trace attack »

Collision

Deductions come from the observation or not of a collision, comparing two pieces of signal

«two traces attack »

Advanced

Statistical analysis on the basis of the observation of several signals

DPA

CPA

MIA

LRA

ML

KSA

Horizontal

Form

Vertical

Knowledge

Non profiling

Profiling

Machine Learning

Classification

Verification

To be developped