Subtle Authenticated Encryption

Guy Barwell Martijn Stam Daniel Page

Subtitled
~~Subtle~~ Authenticated Encryption

Guy Barwell Martijn Stam Daniel Page

Now with closed-caption sub-titles! Thanks to Eve for scribing an early version of this talk.

Authentication/encryption notions

There are many different Authenticated Encryption notions, each striving to model a different aspect of security or real world behaviour.

Authentication/encryption notions

Authentication

There are many different Authenticated Encryption notions, each striving to model a different aspect of security or real world behaviour.

Authentication/encryption notions

Authentication

Encryption

There are many different Authenticated Encryption notions, each striving to model a different aspect of security or real world behaviour.

Authentication/encryption notions

Authentication

Authenticated Encryption

Encryption

There are many different Authenticated Encryption notions, each striving to model a different aspect of security or real world behaviour.

Authentication/encryption notions

Authentication

Authenticated Encryption

Encryption

Probabilistic

There are many different Authenticated Encryption notions, each striving to model a different aspect of security or real world behaviour.

Authentication/encryption notions

Deterministic

Authentication

Authenticated Encryption

Encryption

Probabilistic

There are many different Authenticated Encryption notions, each striving to model a different aspect of security or real world behaviour.

Authentication/encryption notions

Deterministic

Nonce

Authentication

Authenticated Encryption

Encryption

Probabilistic

There are many different Authenticated Encryption notions, each striving to model a different aspect of security or real world behaviour.

Authentication/encryption notions

Deterministic

Nonce

IV based

Probabilistic

Authentication

Encryption

Authenticated Encryption

There are many different Authenticated Encryption notions, each striving to model a different aspect of security or real world behaviour.

Authentication/encryption notions

Deterministic

Nonce

Nonce-based but actually mean random-IV based

IV based

Probabilistic

Authentication

Authenticated Encryption

Encryption

There are many different Authenticated Encryption notions, each striving to model a different aspect of security or real world behaviour.

Authentication/encryption notions

Deterministic

Nonce

Nonce-based but actually mean random-IV based

IV based

Probabilistic

Stateless

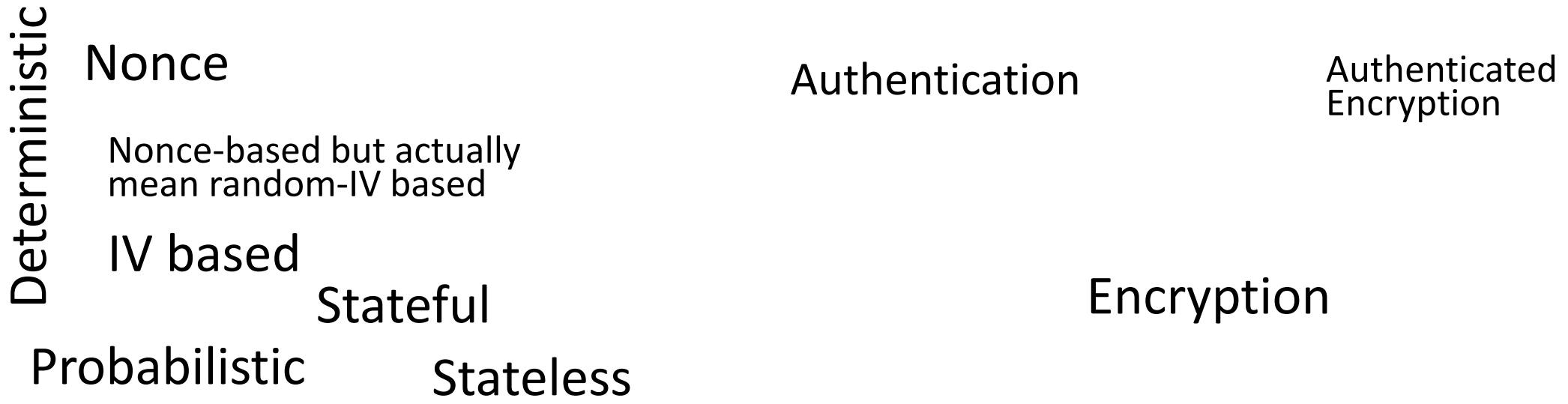
Authentication

Authenticated Encryption

Encryption

There are many different Authenticated Encryption notions, each striving to model a different aspect of security or real world behaviour.

Authentication/encryption notions



There are many different Authenticated Encryption notions, each striving to model a different aspect of security or real world behaviour.

Authentication/encryption notions

Deterministic

Nonce

Nonce-based but actually mean random-IV based

IV based

Stateful

Probabilistic

Stateless

Authentication

Authenticated Encryption

Encryption

IND-CPA

Oh look, now he's got them flying in – that explains why this wasn't in Beamer.

Authentication/encryption notions

Deterministic

Nonce

Nonce-based but actually mean random-IV based

IV based

Stateful

Probabilistic

Stateless

Authentication

INT-CTXT

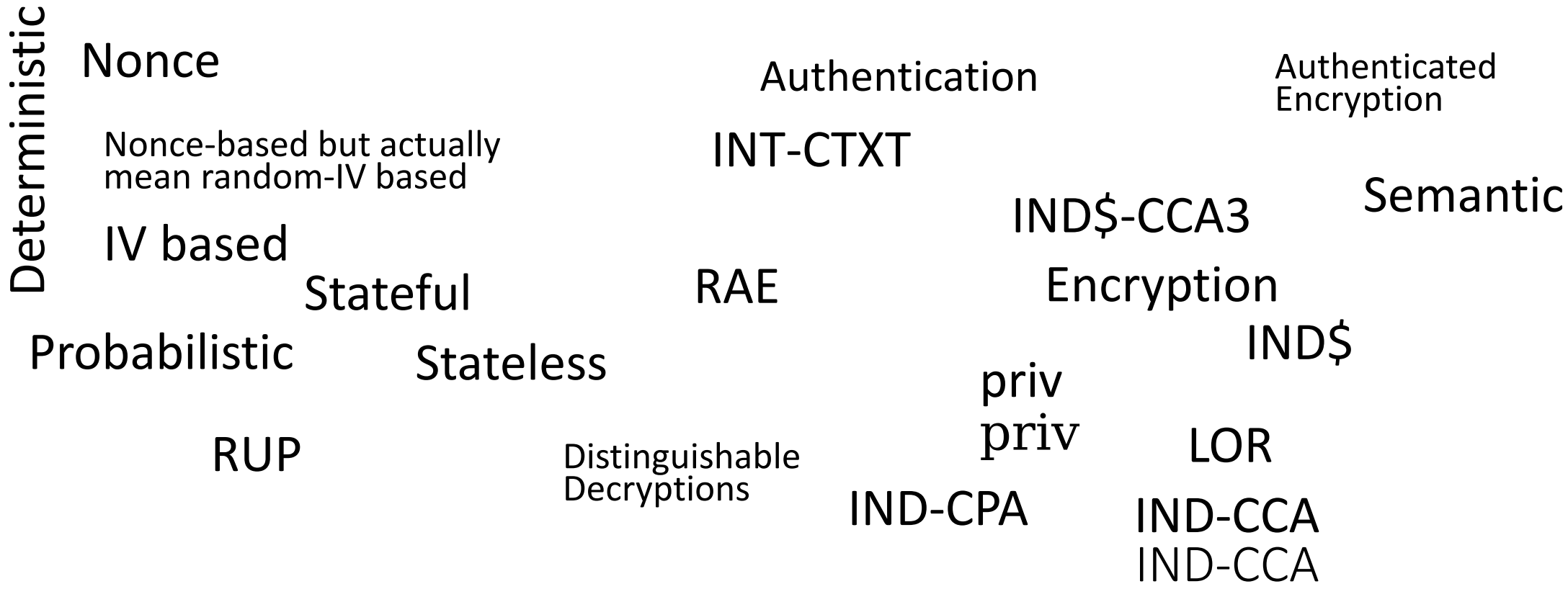
Authenticated Encryption

Encryption

IND-CPA

Oh look, now he's got them flying in – that explains why this wasn't in Beamer.
Or at least, it would if the presentation hadn't been compiled to PDF – bet he feels really silly now!

Authentication/encryption notions



Oh look, now he's got them flying in – that explains why this wasn't in Beamer.
Or at least, it would if the presentation hadn't been compiled to PDF – bet he feels really silly now!

Authentication/encryption notions

Deterministic

Ei-Ei-Oh Secure
(Old McDonald model)

Post-Quantum

Nonce

Authentication

Authenticated Encryption

Nonce-based but actually mean random-IV based

INT-CTXT

Secure for all adversaries making $q \leq 2^{-n}$ queries

Semantic

IND$-CCA3

IV based

Stateful

RAE

Encryption

Probabilistic

Kid-brother-proof

IND$

Stateless

priv

priv

I couldn't break it so its probably secure

RUP

Distinguishable Decryptions

LOR

IND-CPA

IND-CCA

IND-CCA

One-way passive security

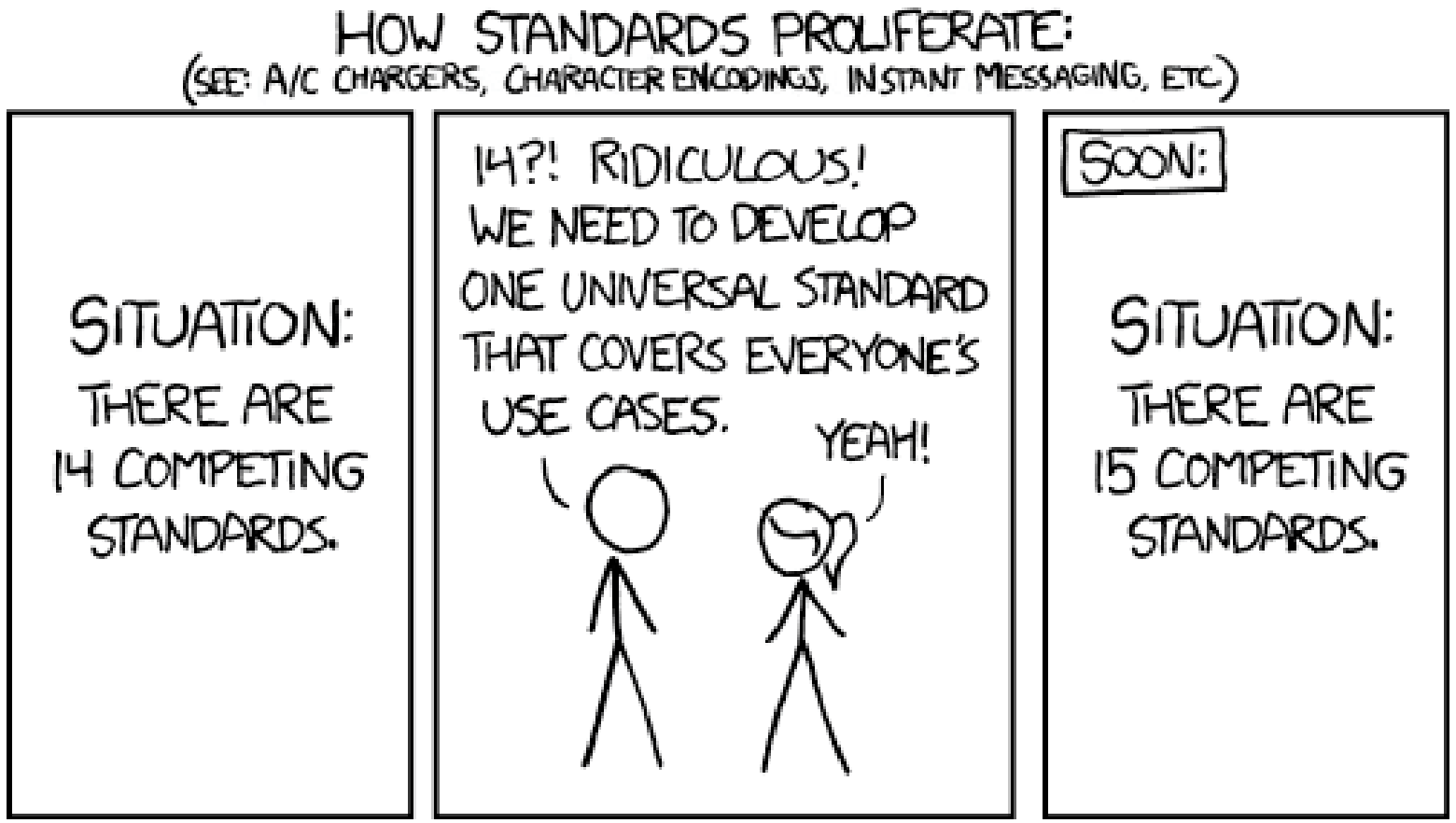
May contain traces of nuts

Oh look, now he's got them flying in – that explains why this wasn't in Beamer.
Or at least, it would if the presentation hadn't been compiled to PDF – bet he feels really silly now!

There are too many different formalisations!

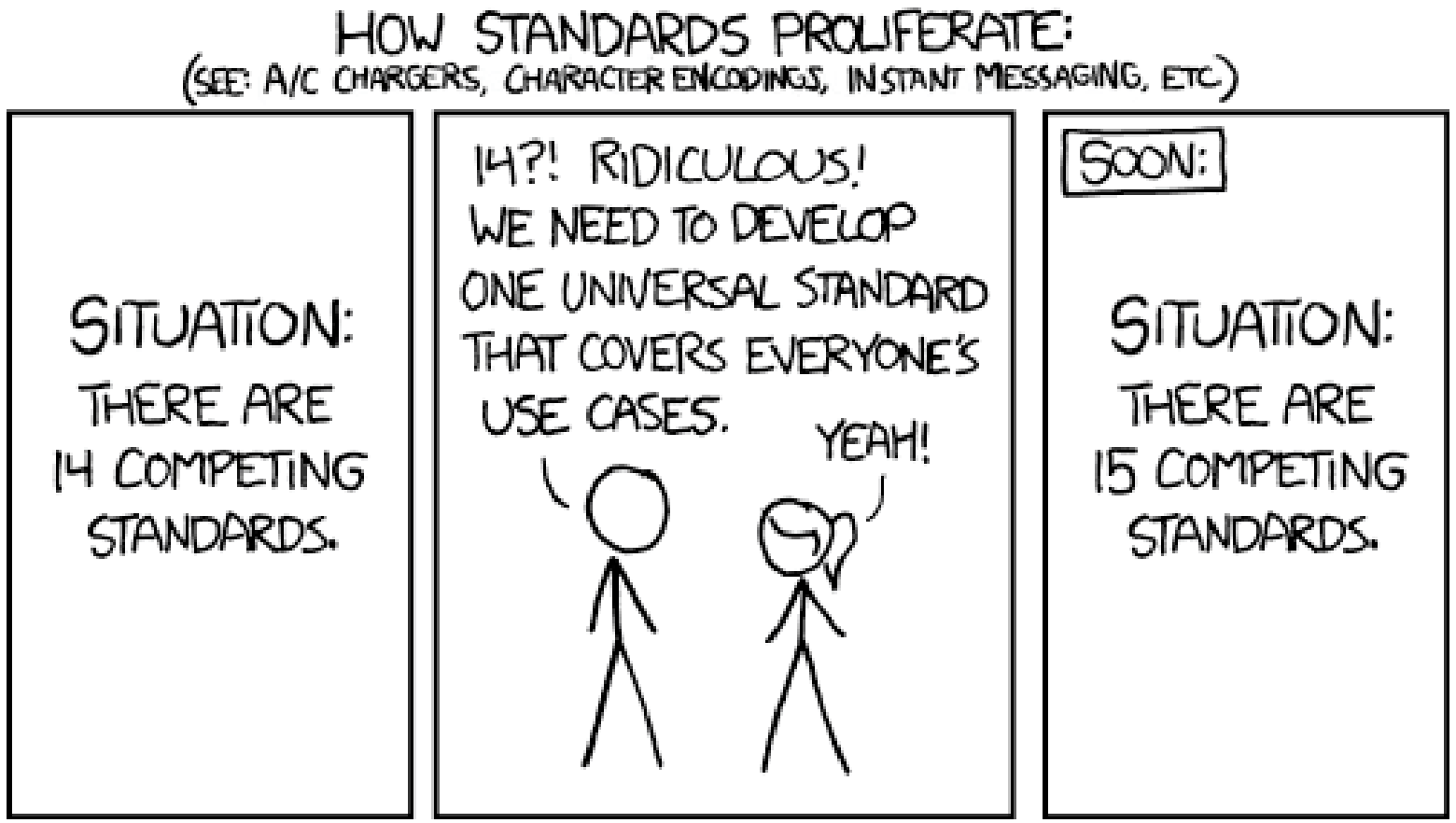
“Too many formalisations” – He’s blatantly going to show that old XKCD cartoon…

There are too many different formalisations!



"Too many formalisations" – He's blatantly going to show that old XKCD cartoon…

There are too many different formalisations!



"Too many formalisations" – He's blatantly going to show that old XKCD cartoon

Told you! That's not at all derivative…

Subtle Authenticated Encryption Framework:

$$
\begin{aligned}
\mathrm{Enc}, \mathcal{E} &: \mathsf{K} \times \mathsf{N} \times \mathsf{A} \times \mathsf{M} \rightarrow \mathsf{C} \\
\mathrm{Dec}, \mathcal{D} &: \mathsf{K} \times \mathsf{N} \times \mathsf{A} \times \mathsf{C} \rightarrow \mathsf{M} \cup \{\perp\} \\
\Lambda &: \mathsf{K} \times \mathsf{N} \times \mathsf{A} \times \mathsf{C} \rightarrow \{\top\} \cup \mathsf{L}
\end{aligned}
$$

Definitional choices:

- Nonce Based (deterministic)

We require schemes be nonce-based, correct and tidy.

Subtle Authenticated Encryption Framework:

$$
\begin{aligned}
\mathrm{Enc}, \mathcal{E} &: \mathsf{K} \times \mathsf{N} \times \mathsf{A} \times \mathsf{M} \rightarrow \mathsf{C} \\
\mathrm{Dec}, \mathcal{D} &: \mathsf{K} \times \mathsf{N} \times \mathsf{A} \times \mathsf{C} \rightarrow \mathsf{M} \cup \{\bot\} \\
\Lambda &: \mathsf{K} \times \mathsf{N} \times \mathsf{A} \times \mathsf{C} \rightarrow \{\top\} \cup \mathsf{L}
\end{aligned}
$$

Definitional choices:

- Nonce Based (deterministic)
- Tidy & Correct

We require schemes be nonce-based, correct and tidy.
This means the scheme is wholly specified by $\mathcal{E}$, and the implementation leakage by Λ

Subtle Authenticated Encryption Framework:

$$
\begin{array}{rlcll}
\mathrm{Enc}, \mathcal{E} & : \mathsf{K} \times \mathsf{N} \times \mathsf{A} \times \mathsf{M} & \rightarrow & \mathsf{C} & \\
\mathrm{Dec}, \mathcal{D} & : \mathsf{K} \times \mathsf{N} \times \mathsf{A} \times \mathsf{C} & \rightarrow & \mathsf{M} & \cup \{\perp\} \\
\Lambda & : \mathsf{K} \times \mathsf{N} \times \mathsf{A} \times \mathsf{C} & \rightarrow & \{\top\} & \cup \mathsf{L}
\end{array}
$$

Definitional choices:

- Nonce Based (deterministic)
- Tidy & Correct
- Real World vs Ideal World

Sorry, he's just reading the slides out now (such a bad habit)

Subtle Authenticated Encryption Framework:

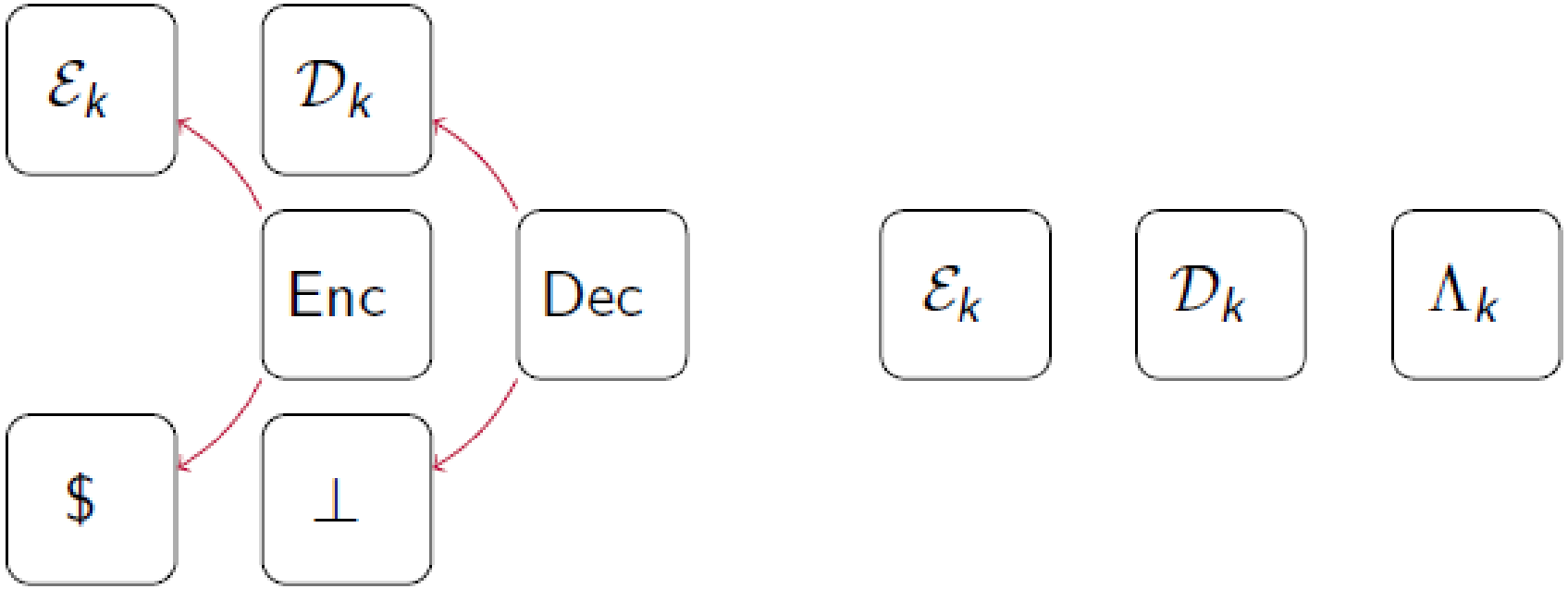
$$
\begin{aligned}
\mathrm{Enc}, \mathcal{E} &: \mathsf{K} \times \mathsf{N} \times \mathsf{A} \times \mathsf{M} \rightarrow \mathsf{C} \\
\mathrm{Dec}, \mathcal{D} &: \mathsf{K} \times \mathsf{N} \times \mathsf{A} \times \mathsf{C} \rightarrow \mathsf{M} \cup \{\perp\} \\
\Lambda &: \mathsf{K} \times \mathsf{N} \times \mathsf{A} \times \mathsf{C} \rightarrow \{\top\} \cup \mathsf{L}
\end{aligned}
$$

Definitional choices:

- Nonce Based (deterministic)
- Tidy & Correct
- Real World vs Ideal World
- Separate out Leakage from D

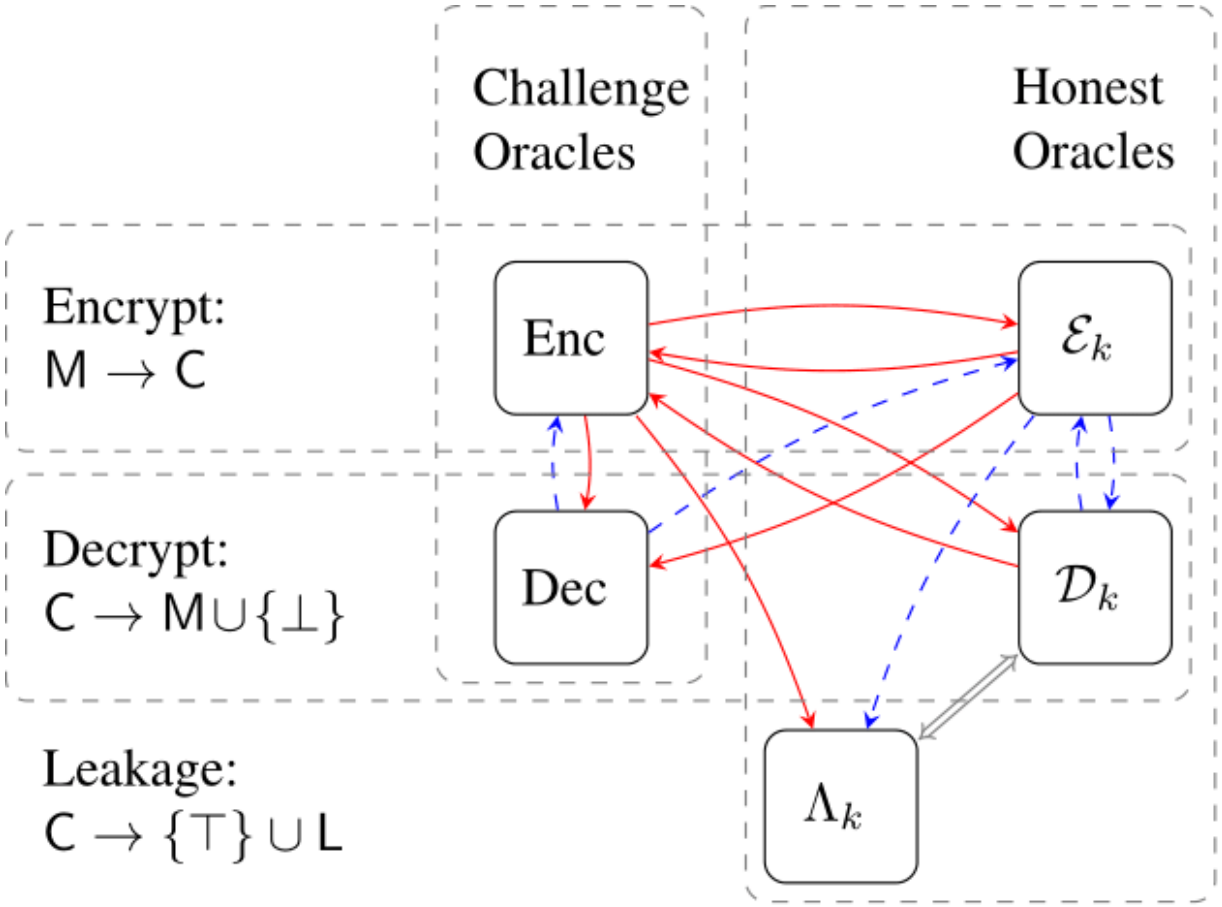
Sorry, he's just reading the slides out now (such a bad habit)

Oracles look like this:



The adversary is provided with some subset of these 5 oracles, and tasked with distinguishing which world the challenge oracles are taken from.

And interact like this:



Key:

Prohibited Queries

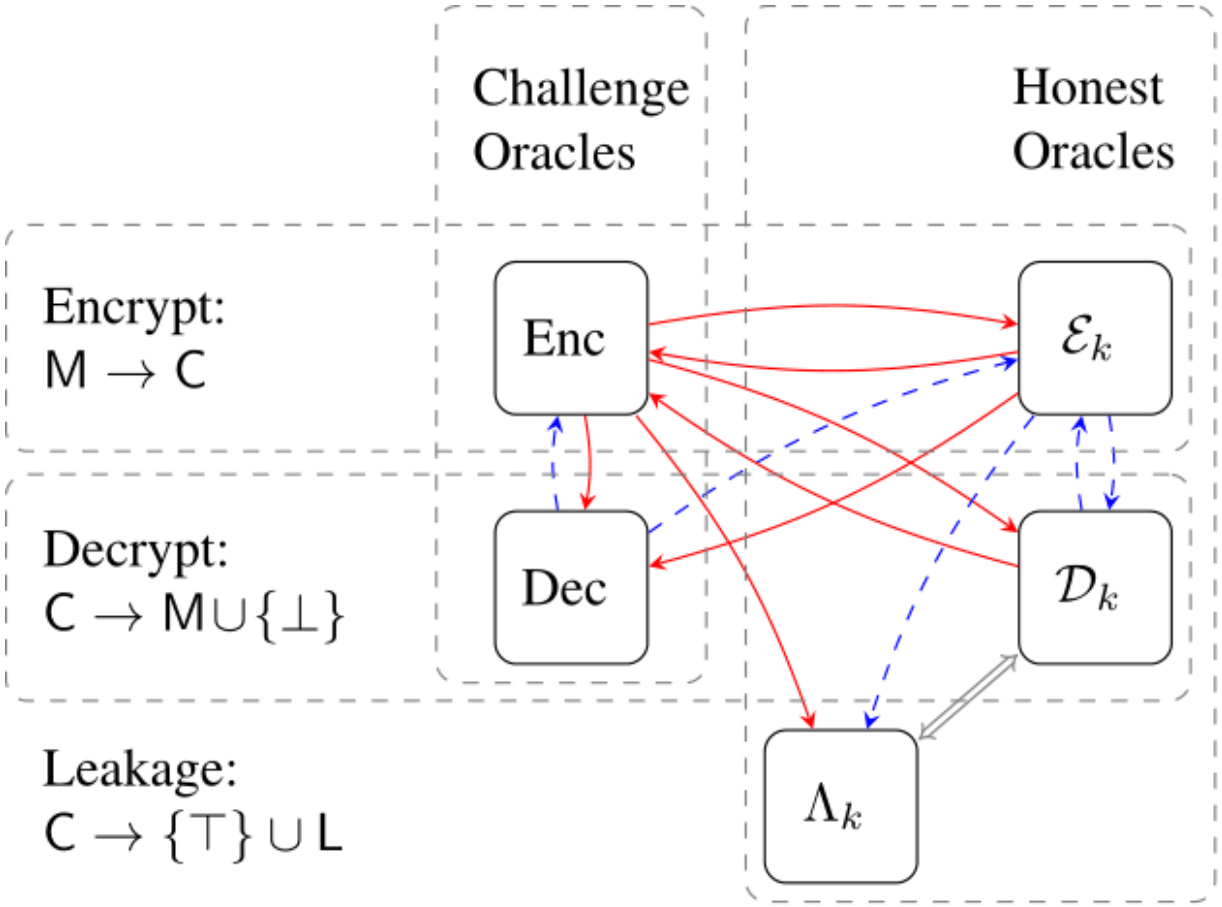
Pointless Queries

Entangled Oracles

An arrow $A \rightarrow B$ means that queries made to A restrict queries to B. Arrows within the same row mean inputs cannot be repeated, those from one row to another mean the output of A cannot later be used as input to B.

There are a large number of queries that must be forbidden to prevent trivial wins, and several others that are pointless.

And interact like this:



Key:

Prohibited Queries

Pointless Queries

Entangled Oracles

An arrow $A \rightarrow B$ means that queries made to A restrict queries to B. Arrows within the same row mean inputs cannot be repeated, those from one row to another mean the output of A cannot later be used as input to B.

There are a large number of queries that must be forbidden to prevent trivial wins, and several others that are pointless.

Blah blah, formal stuffs - this is getting a bit dull isn't it? Tell you what, I'll add a funny picture before the next slide…

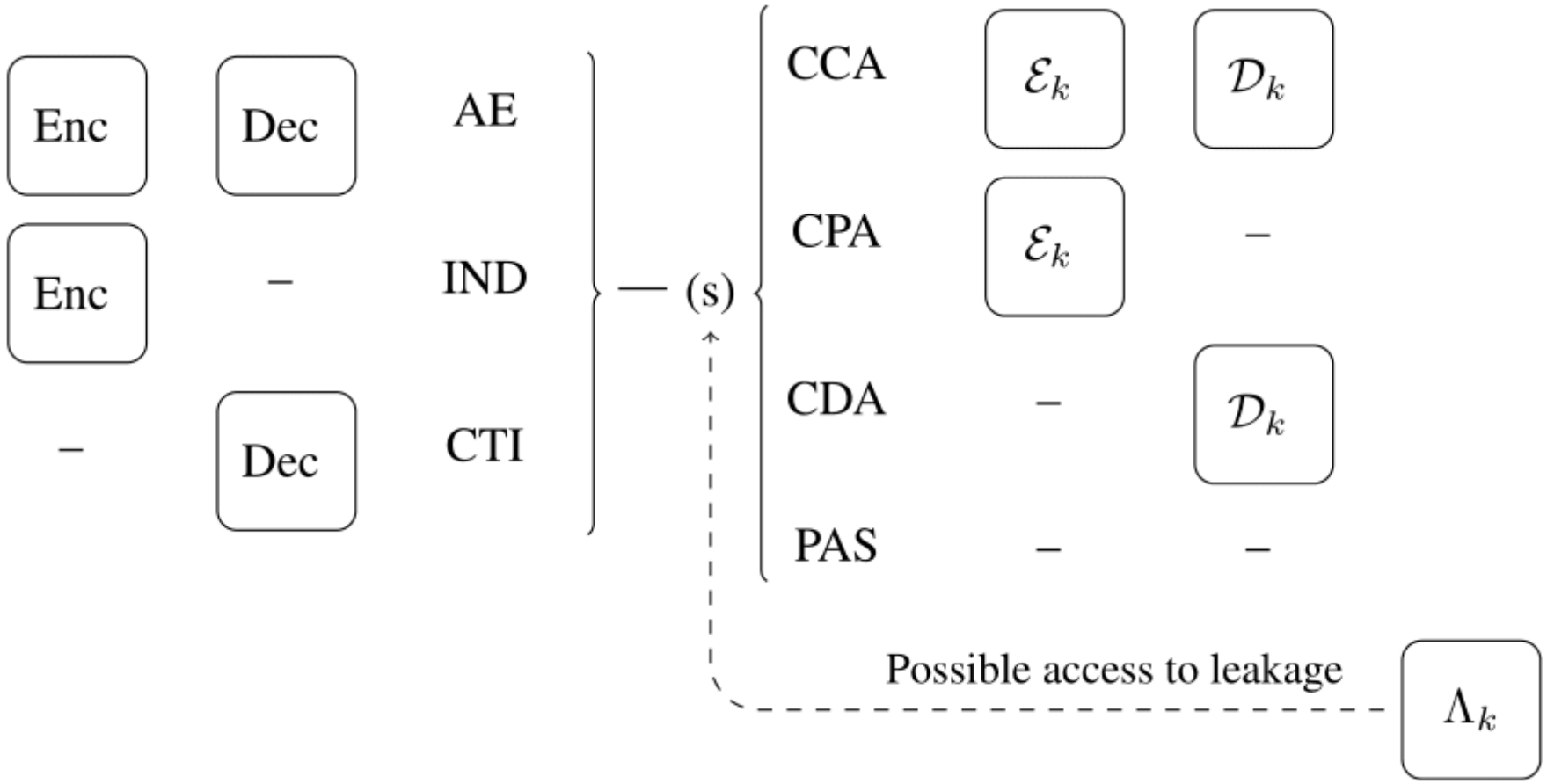
"The trouble with quotes on the Internet is that you can never know if they are genuine."

Abraham Lincoln

Source: https://goo.gl/JHs7QL

You're welcome

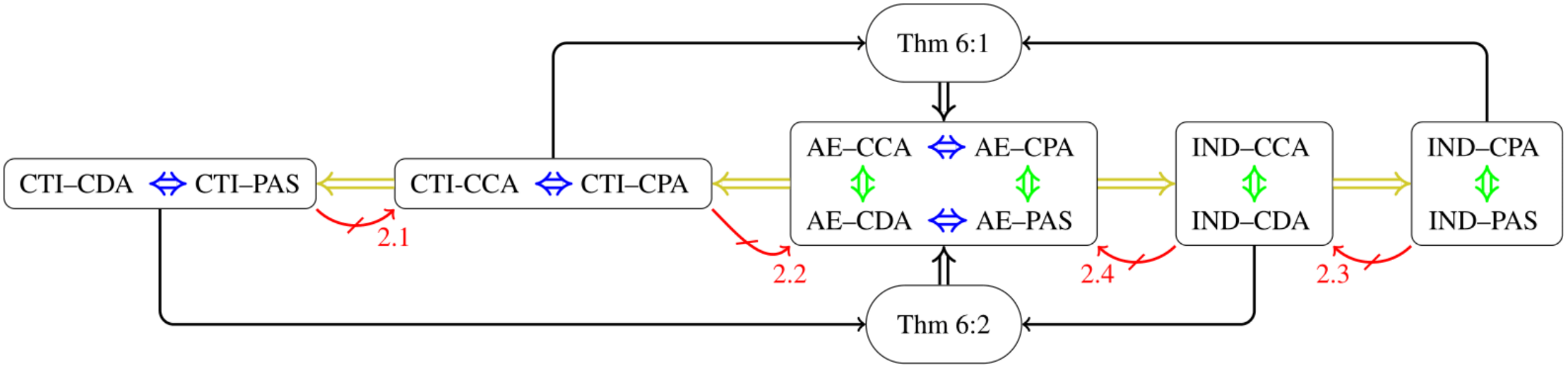
We define security games like this:



Schemes are named in such a way that reflects clearly which oracles the adversary has access to.

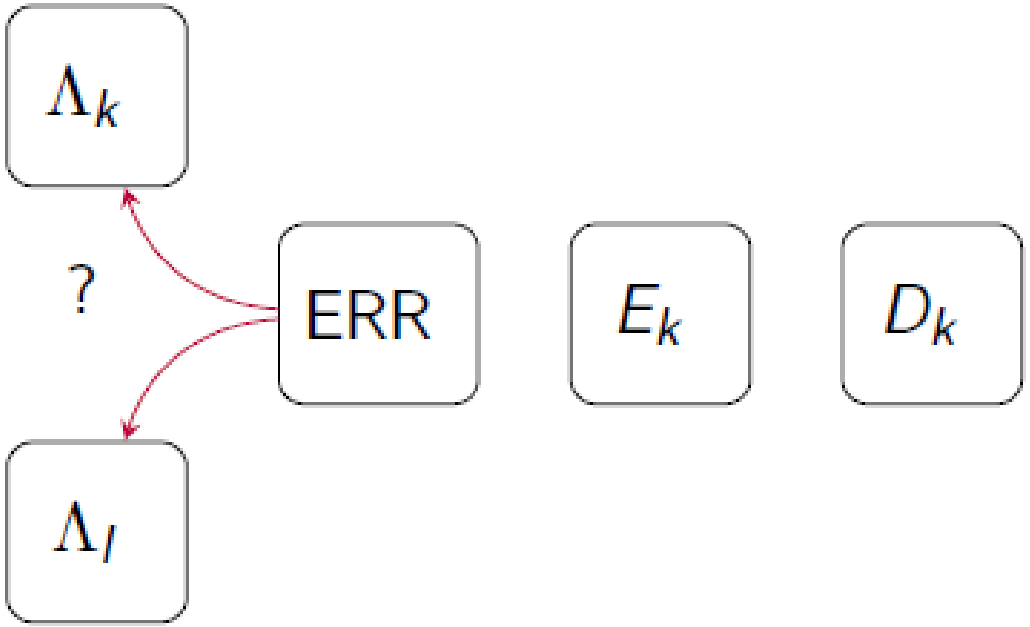
This leads to lots of games, but luckily many of them are equivalent

Which are related like this:



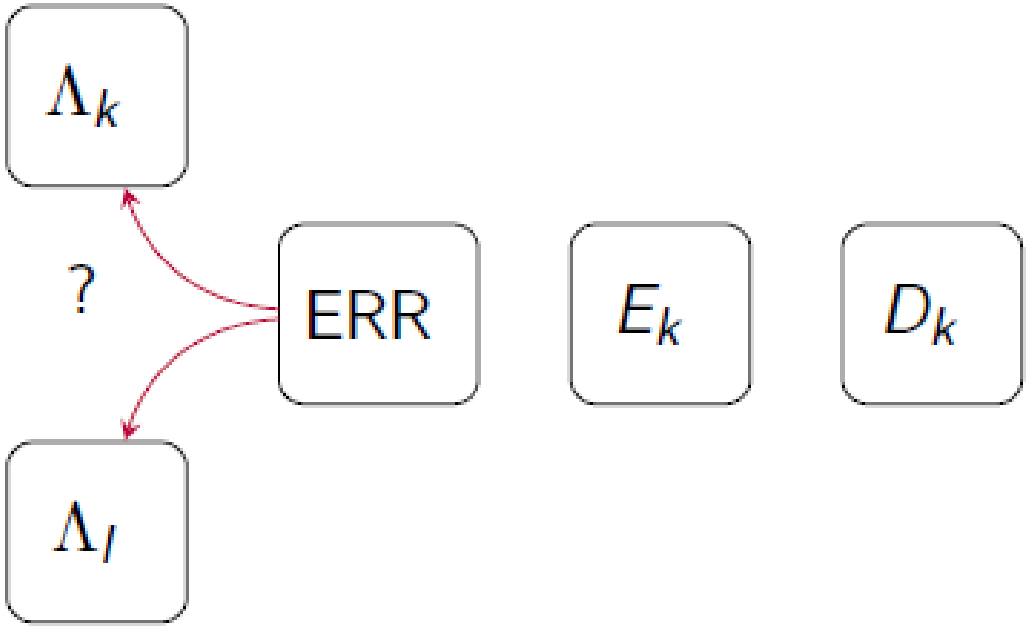
The same relations between the subtle cases, which are completely separated from the leakage-free case

We also introduce Error Invariance:



Inspired by the INV-ERR notion of BDPS and the DI notion of RUP, we introduce Error Invariance, or ERR— , to measure "how bad" errors are. It can be paired with any 'power' oracles: Guy has drawn ERR—CCA.

We also introduce Error Invariance:



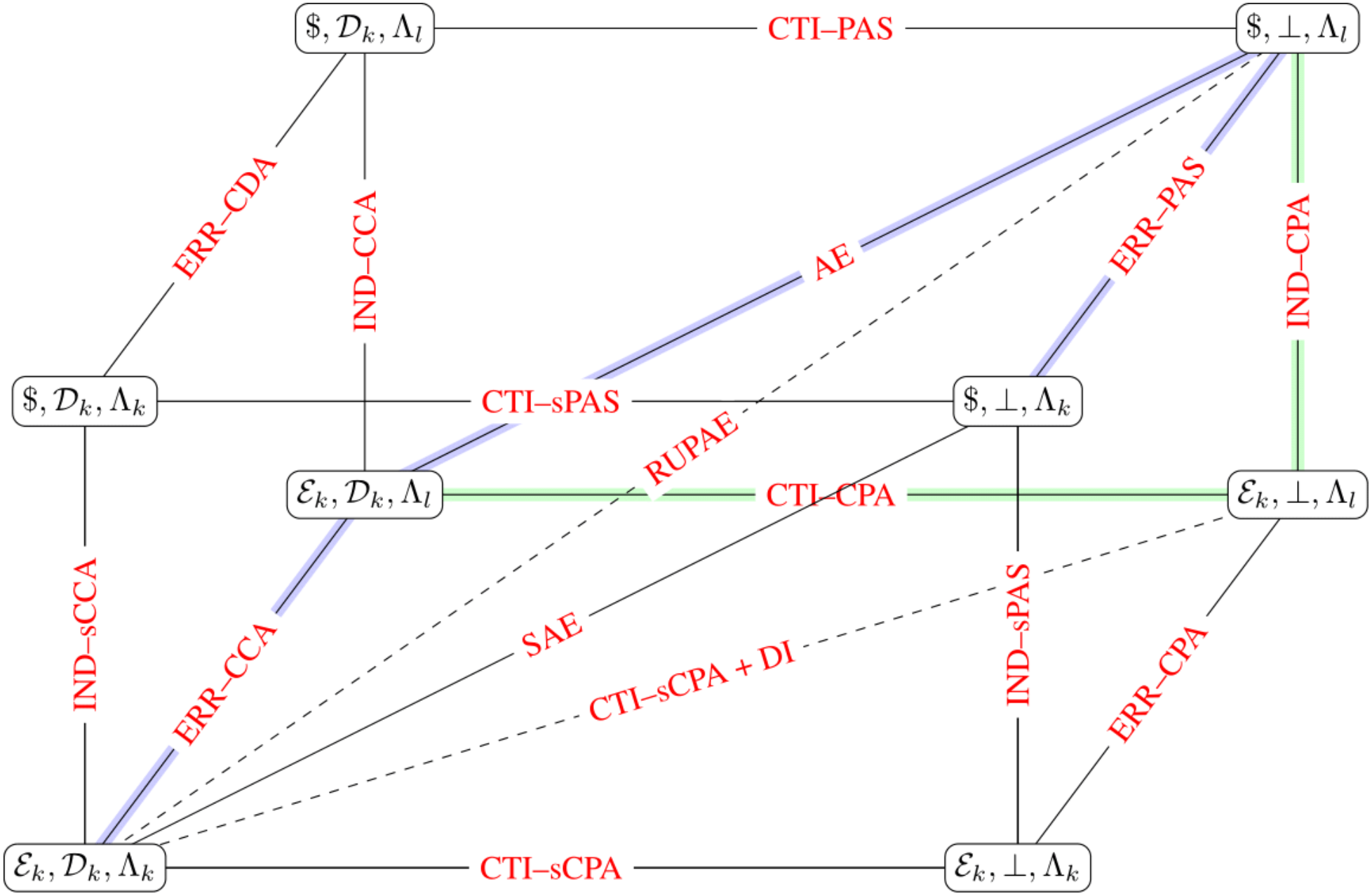
Note use of a separately drawn key rather than a different simulator: a scheme is fully specified by ($\mathcal{E}$, Λ)

Dog + Wig

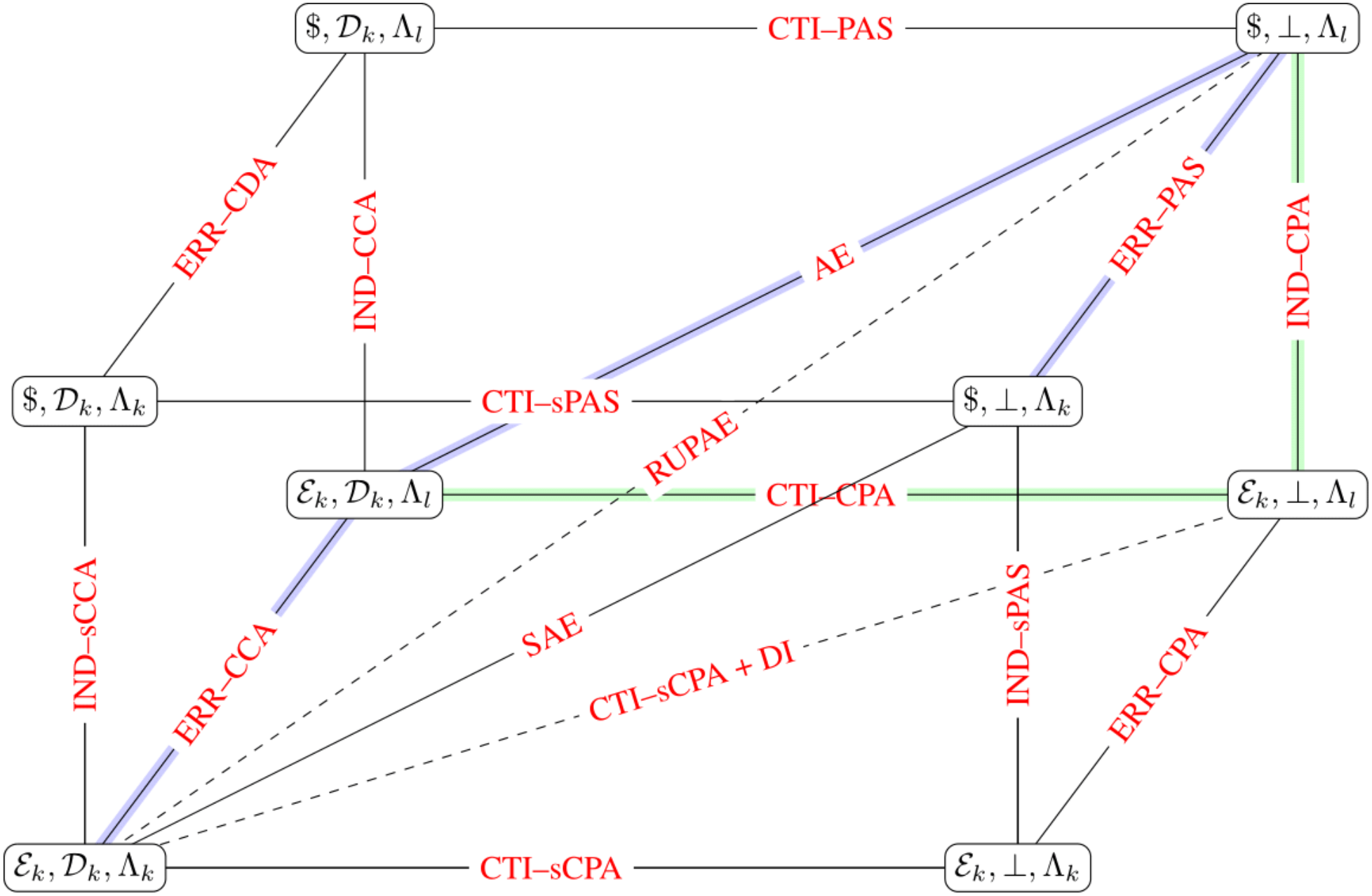
⇓

Terrified Postman

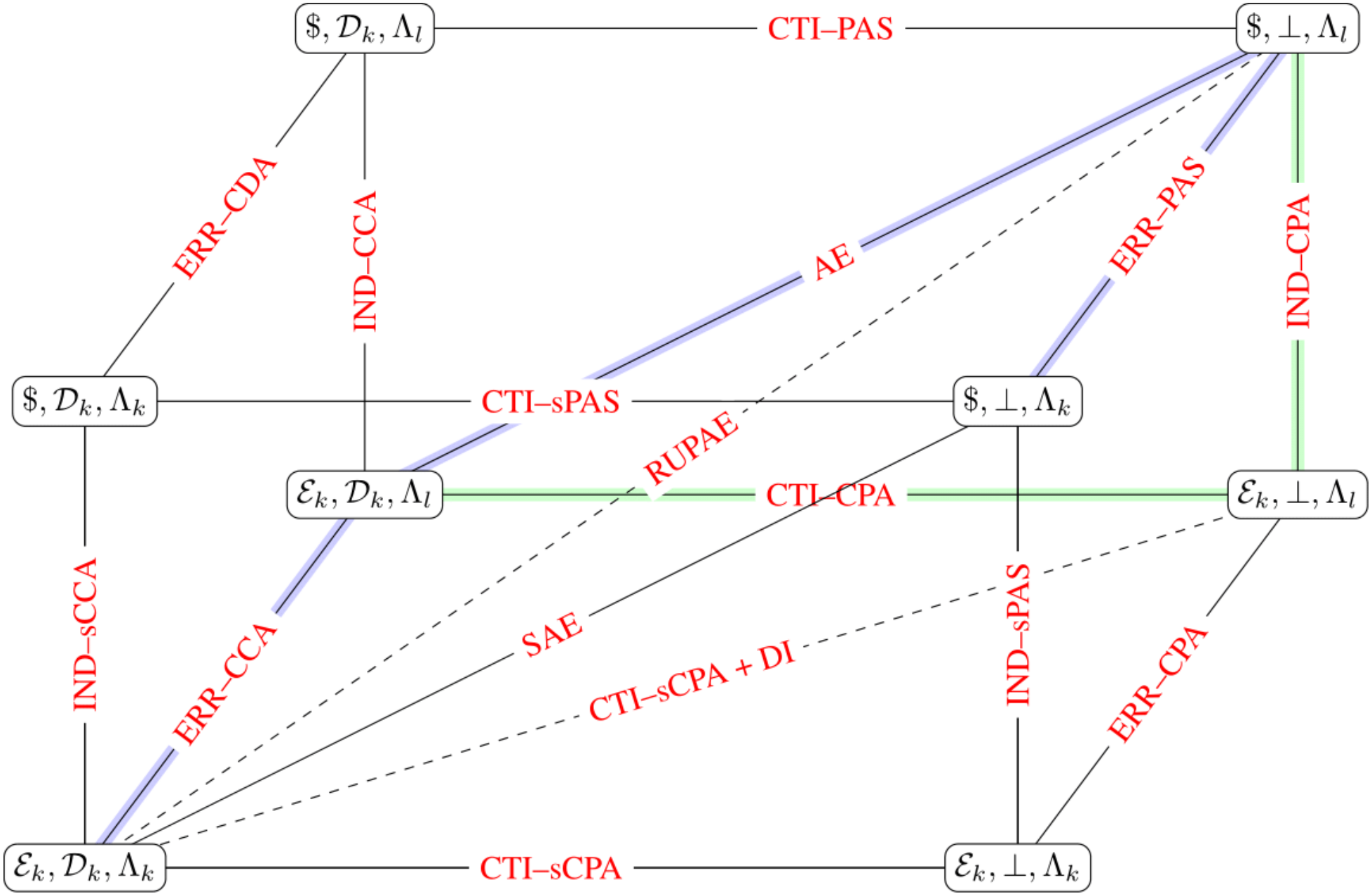
Sorry about that, got a bit heavy – have another fun picture
(source http://imgur.com/gallery/ouO6lj4)



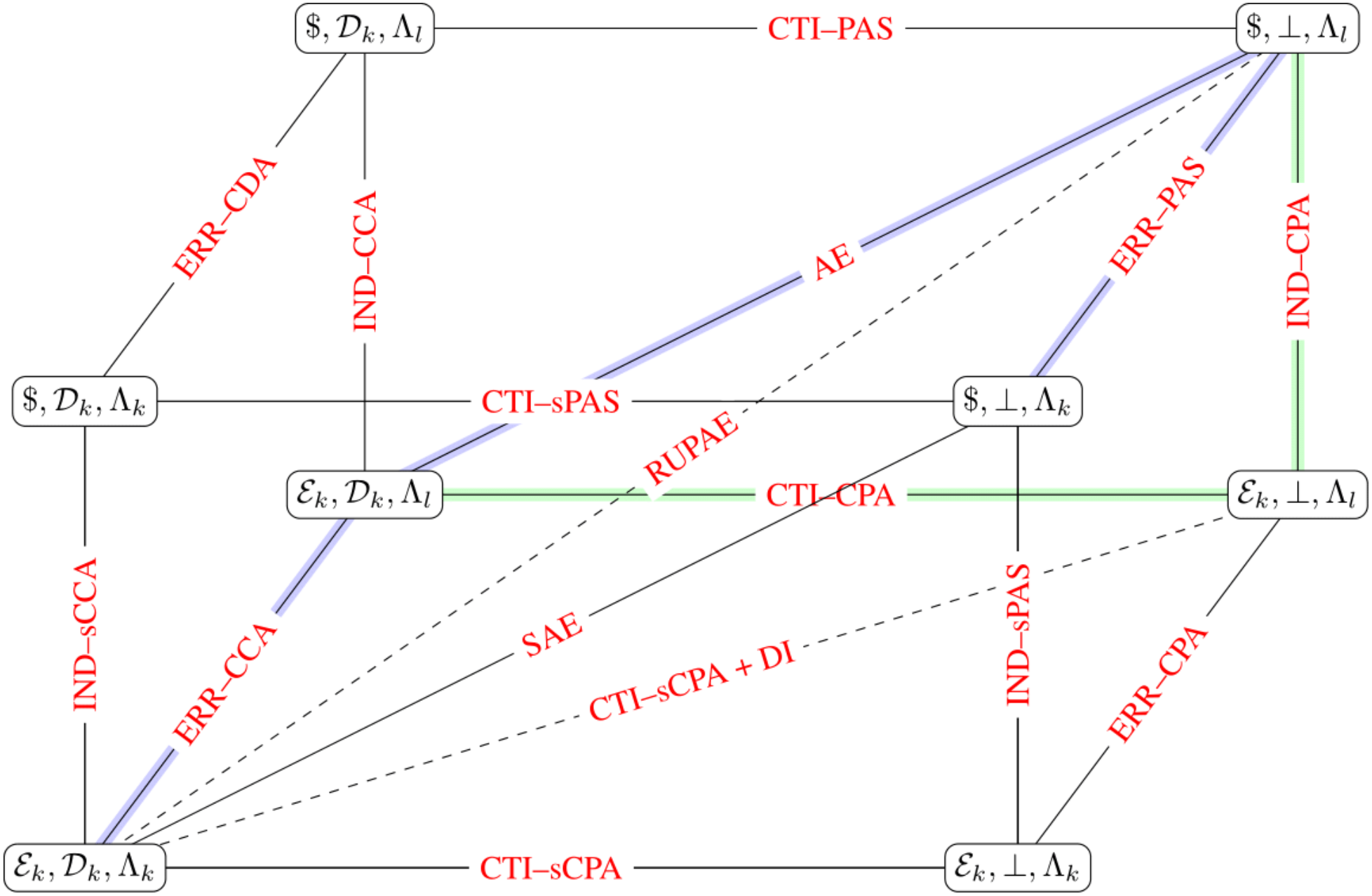
The cube above “acts nicely”. So, the composition results implied hold, giving us useful decompositions for SAE and AE



Finally then, a decent a decent Tikz image, although it's a bit blurry in these slides.



Finally then, a decent a decent Tikz image, although it's a bit blurry in these slides.
Presumably the full paper has a nice vector version though, probably worth a look...



Thank you for your time.

http://eprint.iacr.org/2015/895