Security Conference

Covercrypt: Efficient Quantum-Safe Hybrid Key Exchanges with Hidden Access Policies

Presented by: Chloé Hébant, cryptographer

cosmian

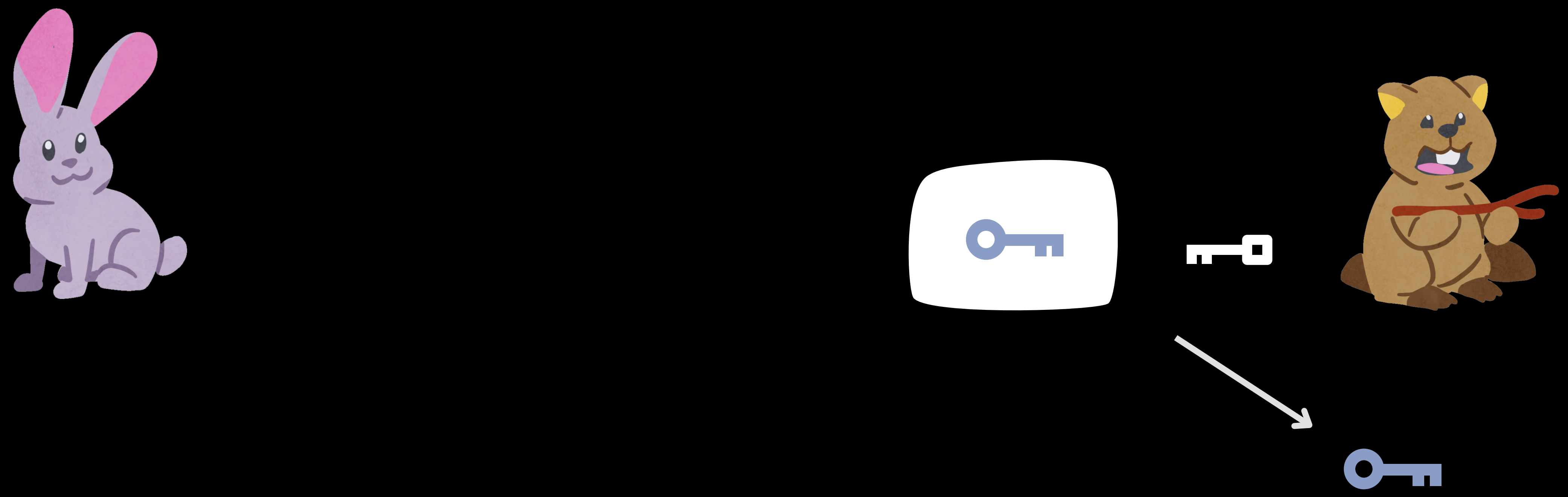
October, 17th, 2023.

KEY ENCAPSULATION MECHANISMS (KEM)

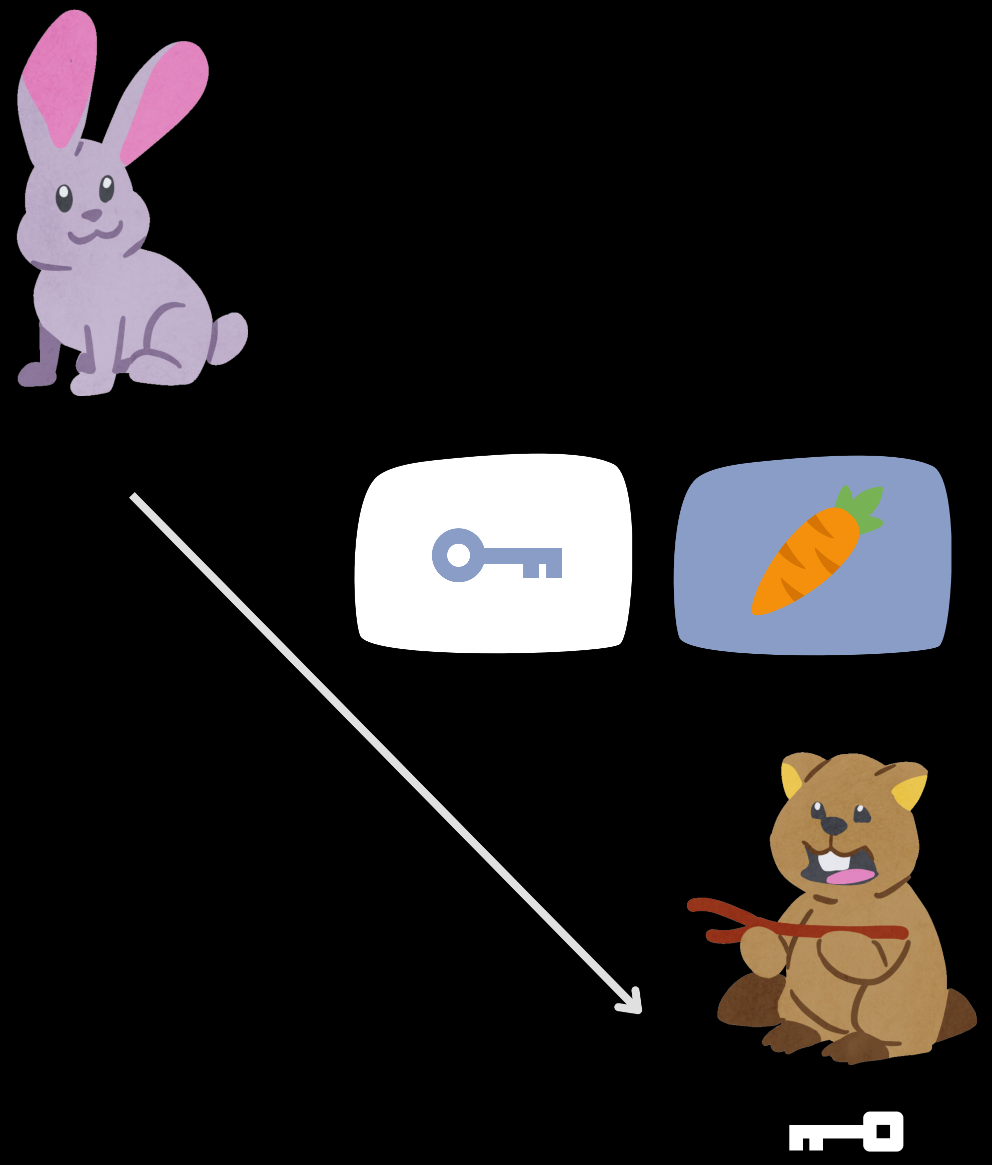
WHY DO WE NEED IT?

BASIC KEM

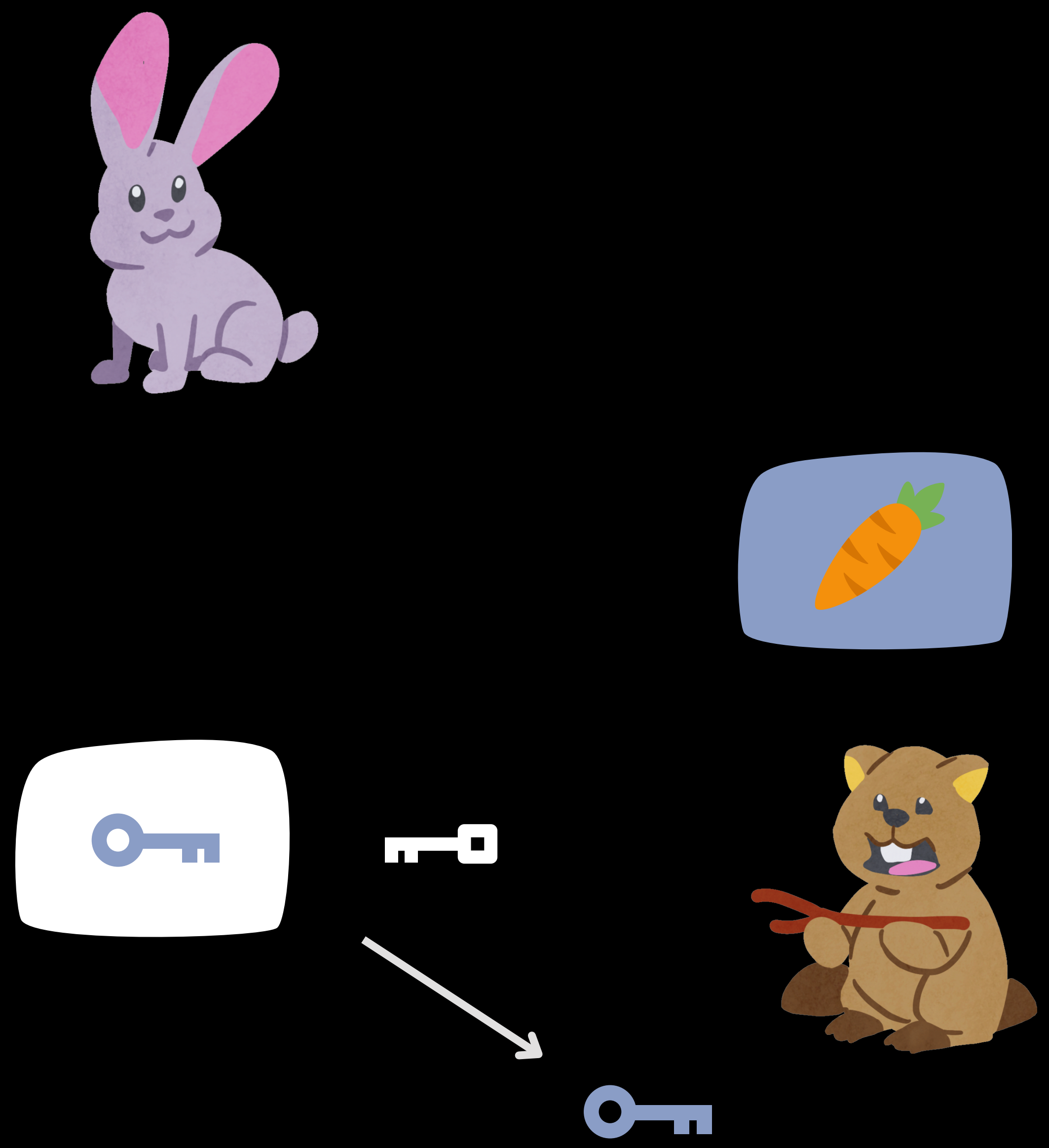
BASIC KEM



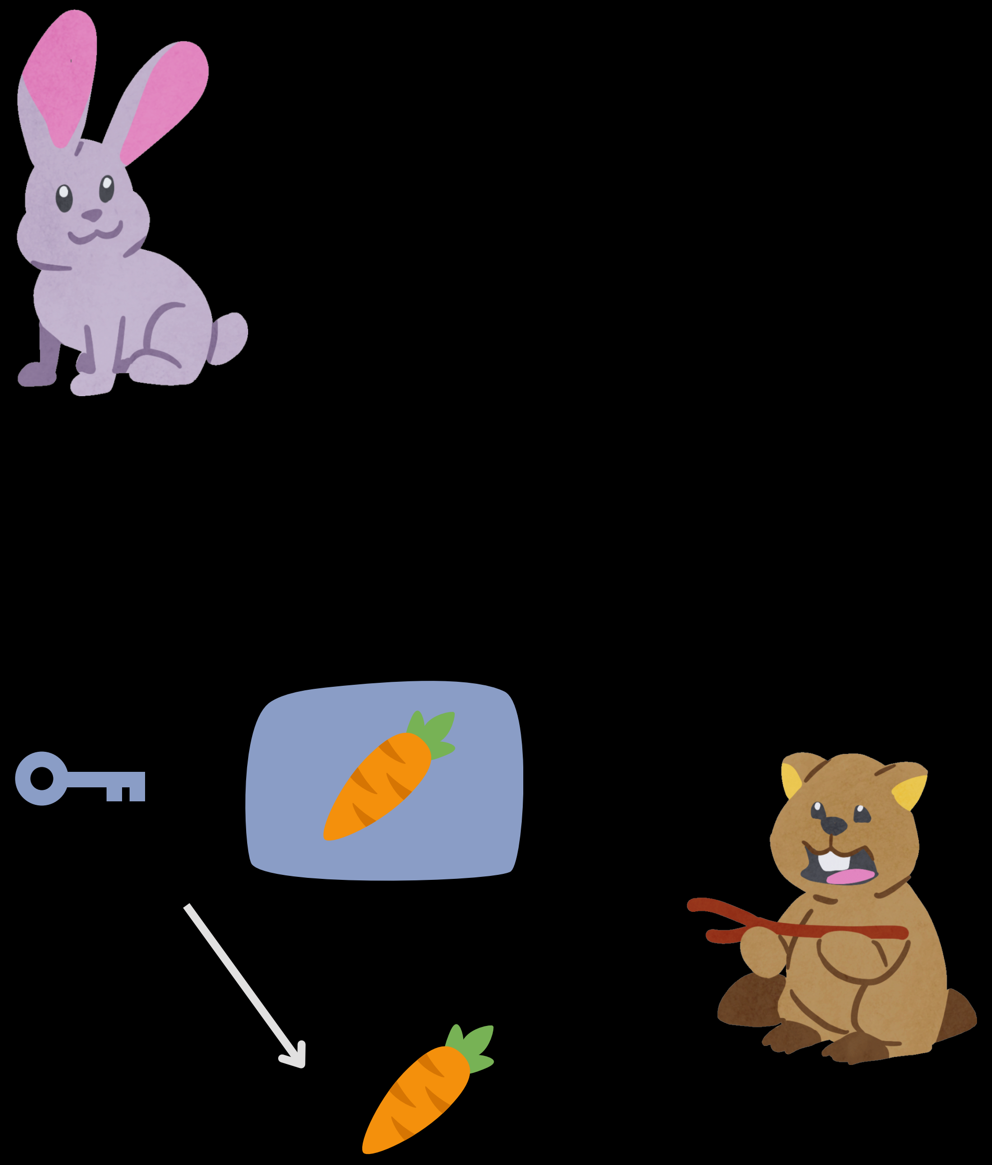
KEM USES: KEM+DEM



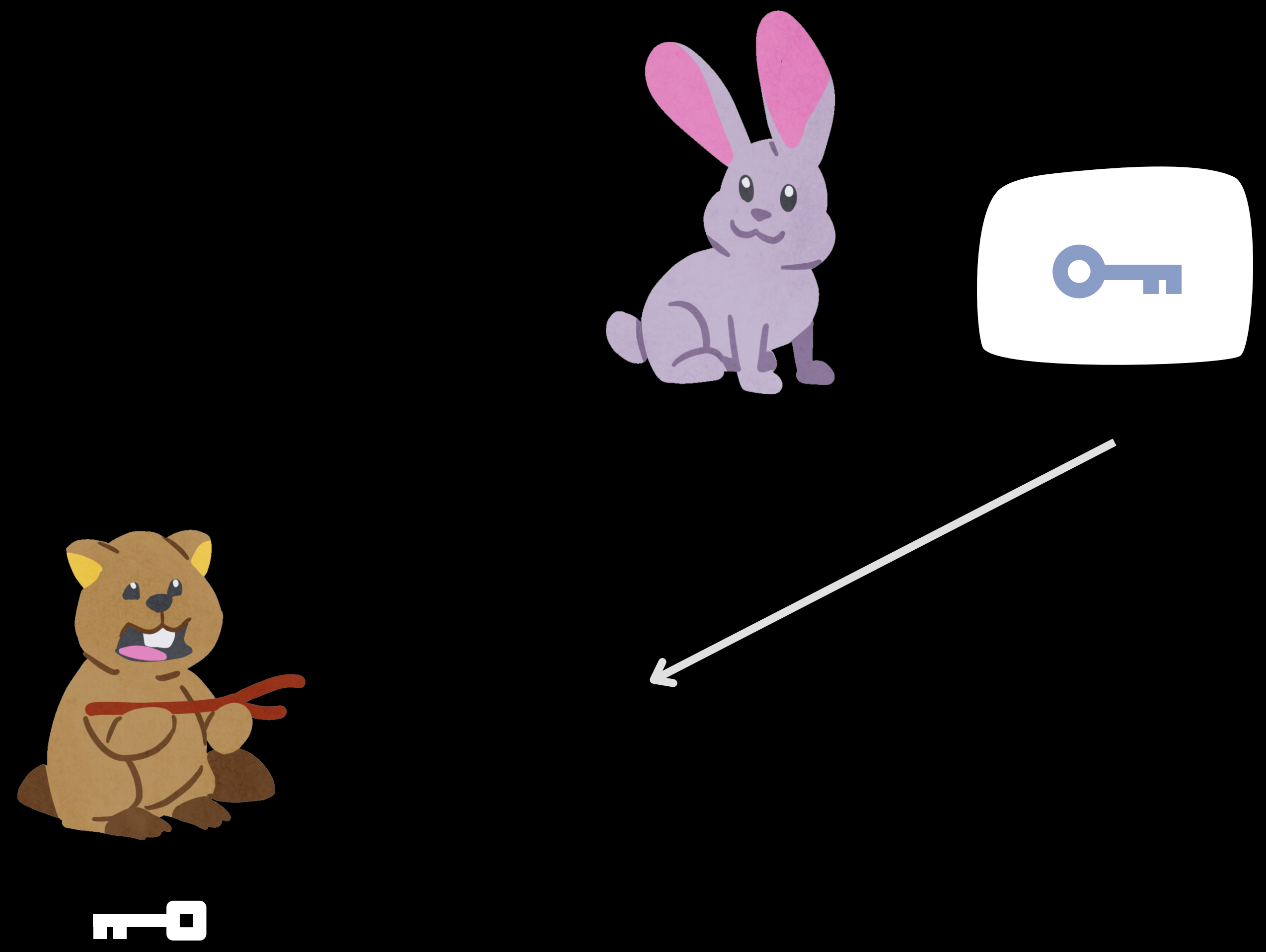
KEM USES: KEM+DEM



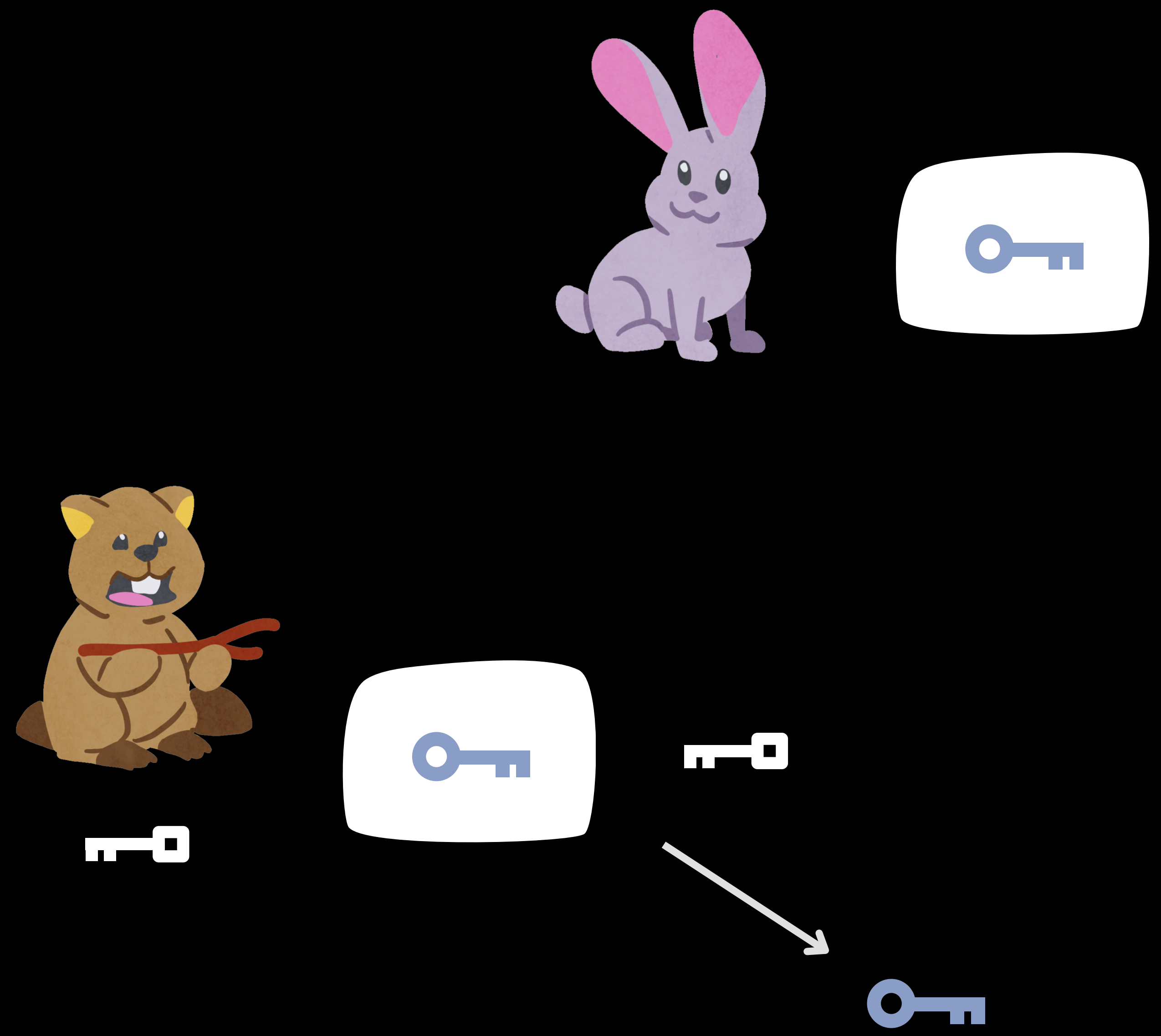
KEM USES: KEM+DEM



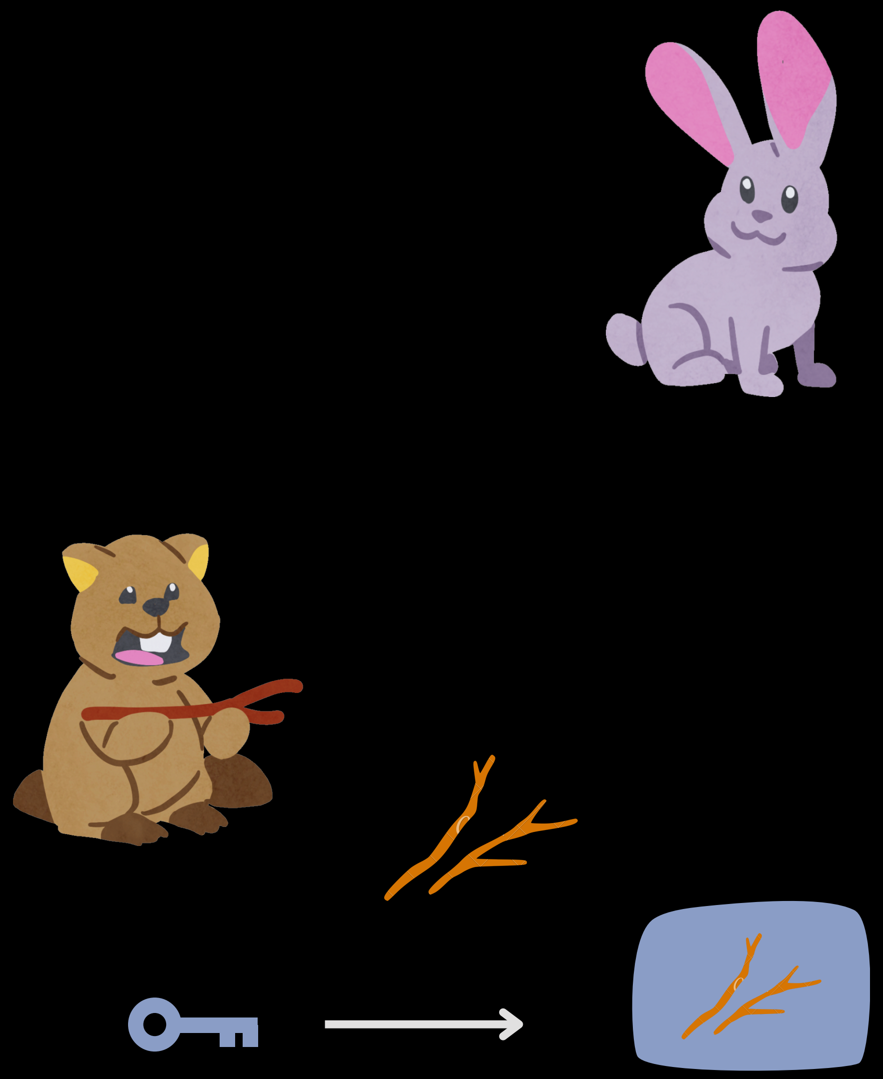
KEM USES: AUTHENTICATION



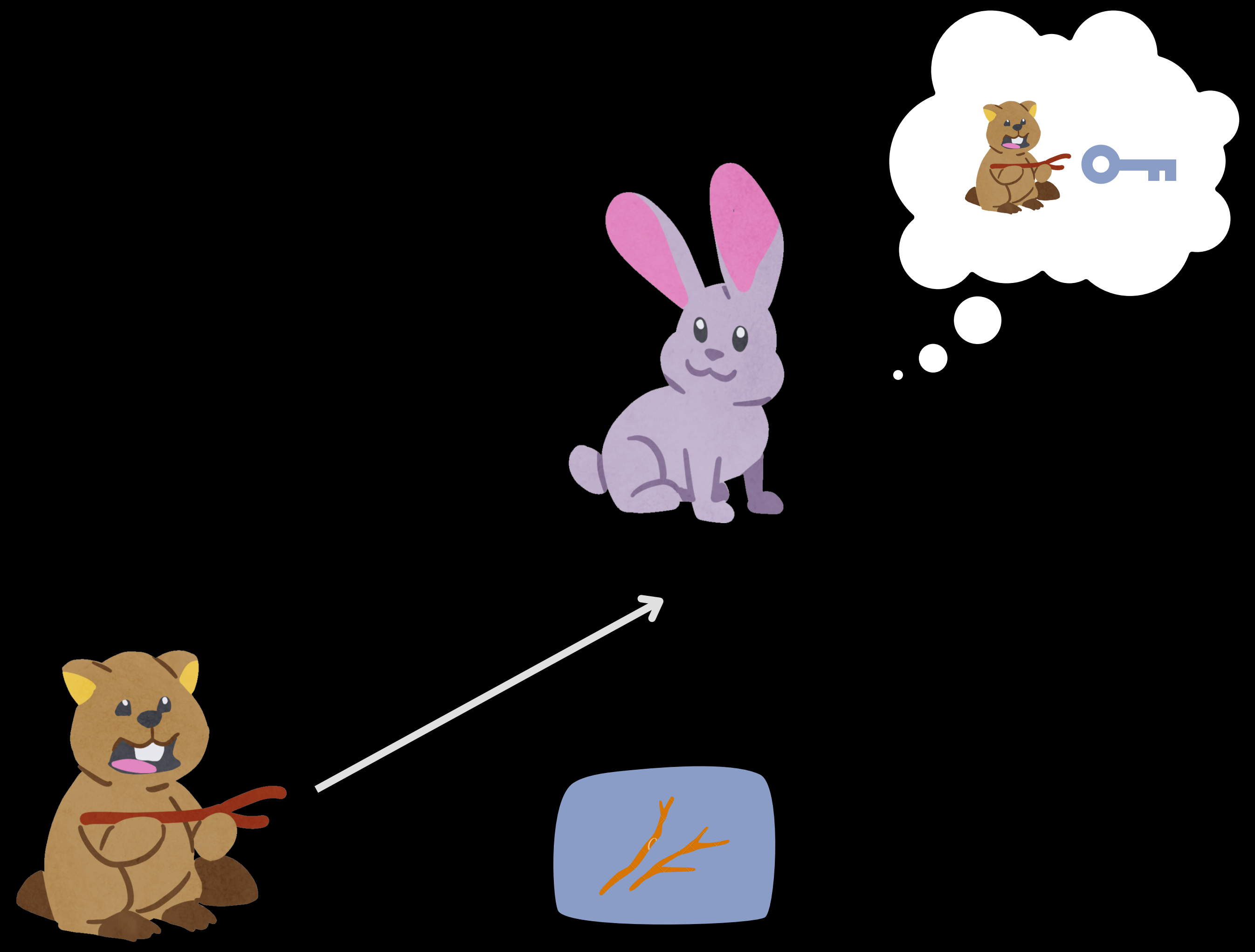
KEM USES: AUTHENTICATION



KEM USES: AUTHENTICATION



KEM USES: AUTHENTICATION



INTERESTING PROPERTIES

WHAT CAN THE BEST STATE-OF-THE-ART PROVIDE IN PRACTICE?

POST- *AND PRE*-QUANTUM RESISTANCE

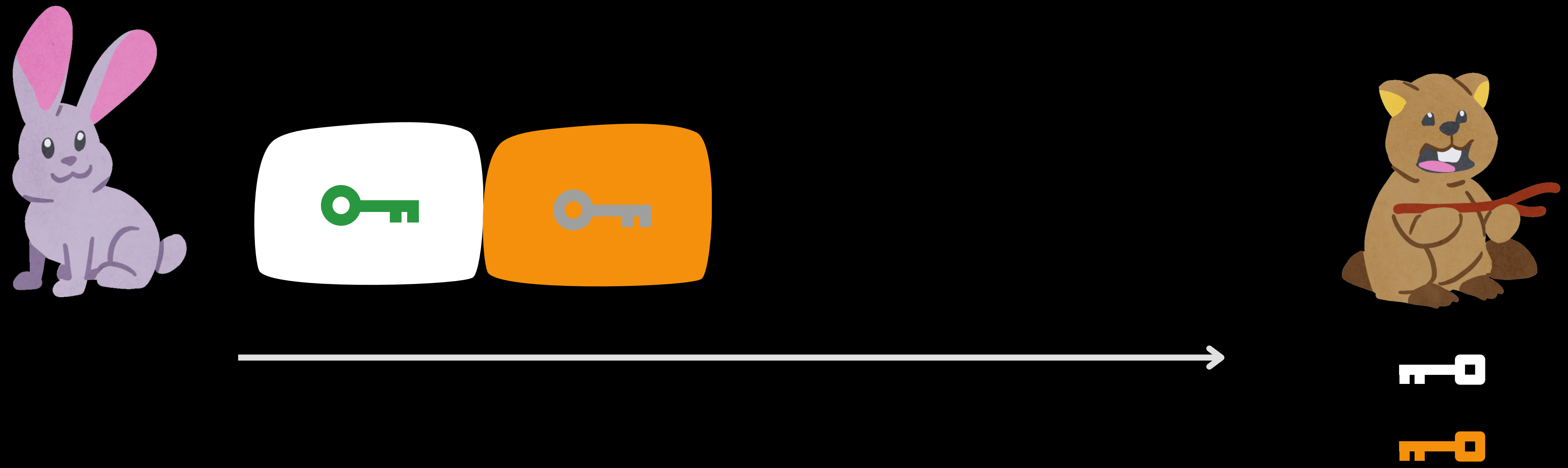
HYBRIDIZING TWO KEM SCHEMES, THE PRIVACY OF ENCAPSULATED KEYS RELIES ON THE BEST OF BOTH SECURITIES

Good recommendation to be secure against post-quantum attacks while relying on older schemes whose security has been more thoroughly tested than new post-quantum ones.

From security agencies like ANSSI for instance, and standards organizations like ETSI.

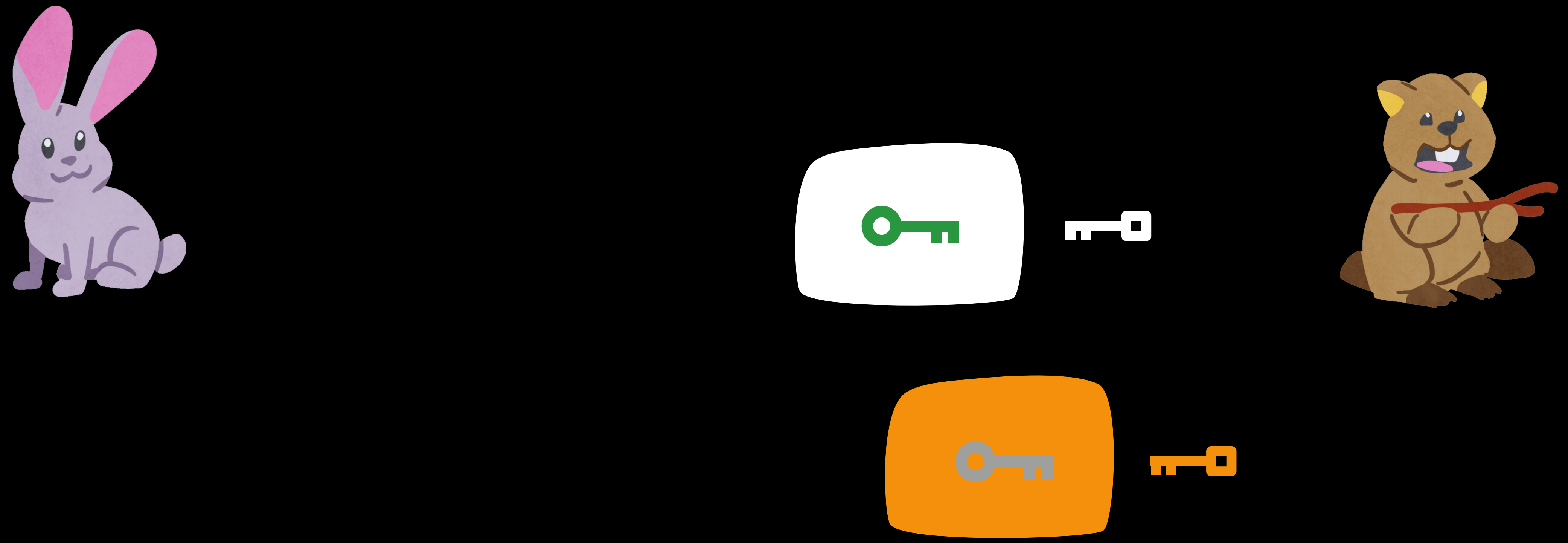
POST- *AND PRE*-QUANTUM RESISTANCE

HYBRIDIZING TWO KEM SCHEMES, THE PRIVACY OF ENCAPSULATED KEYS RELIES ON THE BEST OF BOTH SECURITIES



POST- *AND PRE*-QUANTUM RESISTANCE

HYBRIDIZING TWO KEM SCHEMES, THE PRIVACY OF ENCAPSULATED KEYS RELIES ON THE BEST OF BOTH SECURITIES

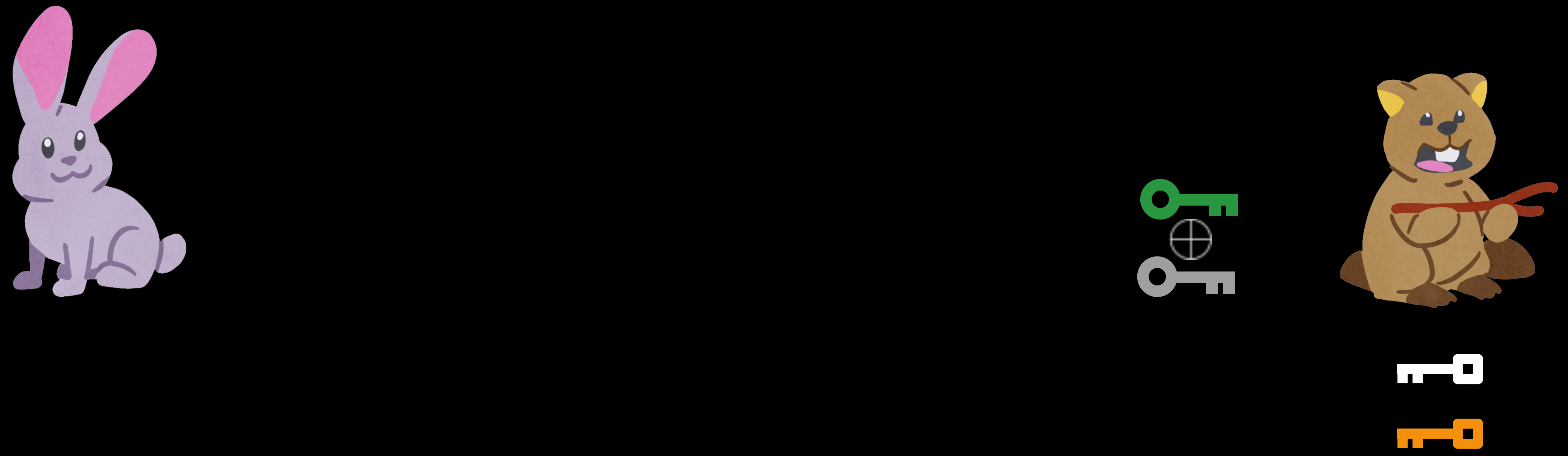


POST- *AND PRE*-QUANTUM RESISTANCE

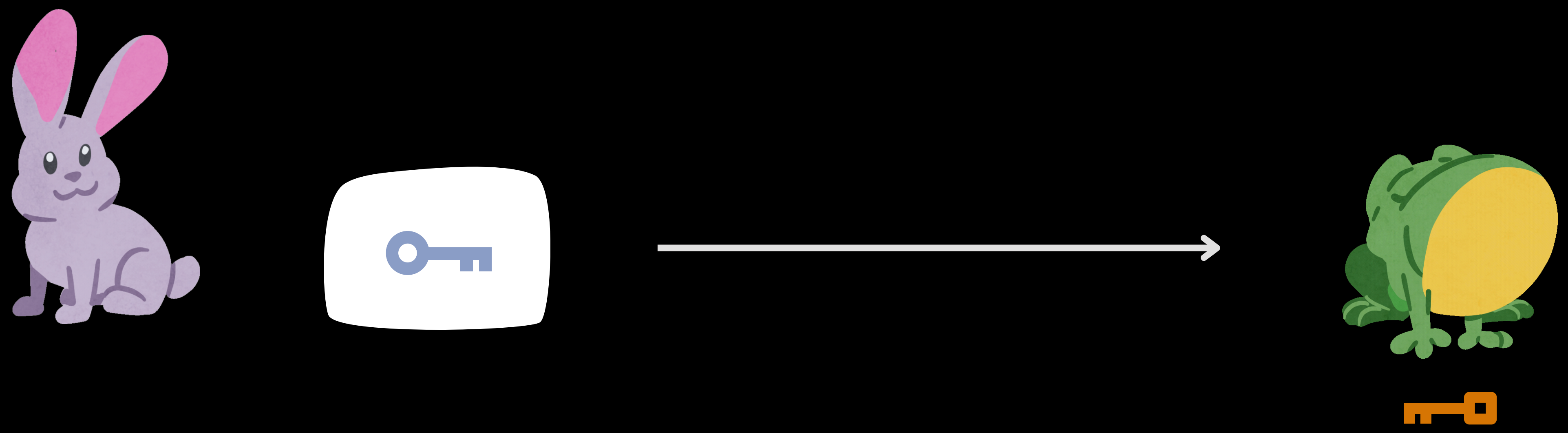
HYBRIDIZING TWO KEM SCHEMES, THE PRIVACY OF ENCAPSULATED KEYS RELIES ON THE BEST OF BOTH SECURITIES

POST- *AND PRE*-QUANTUM RESISTANCE

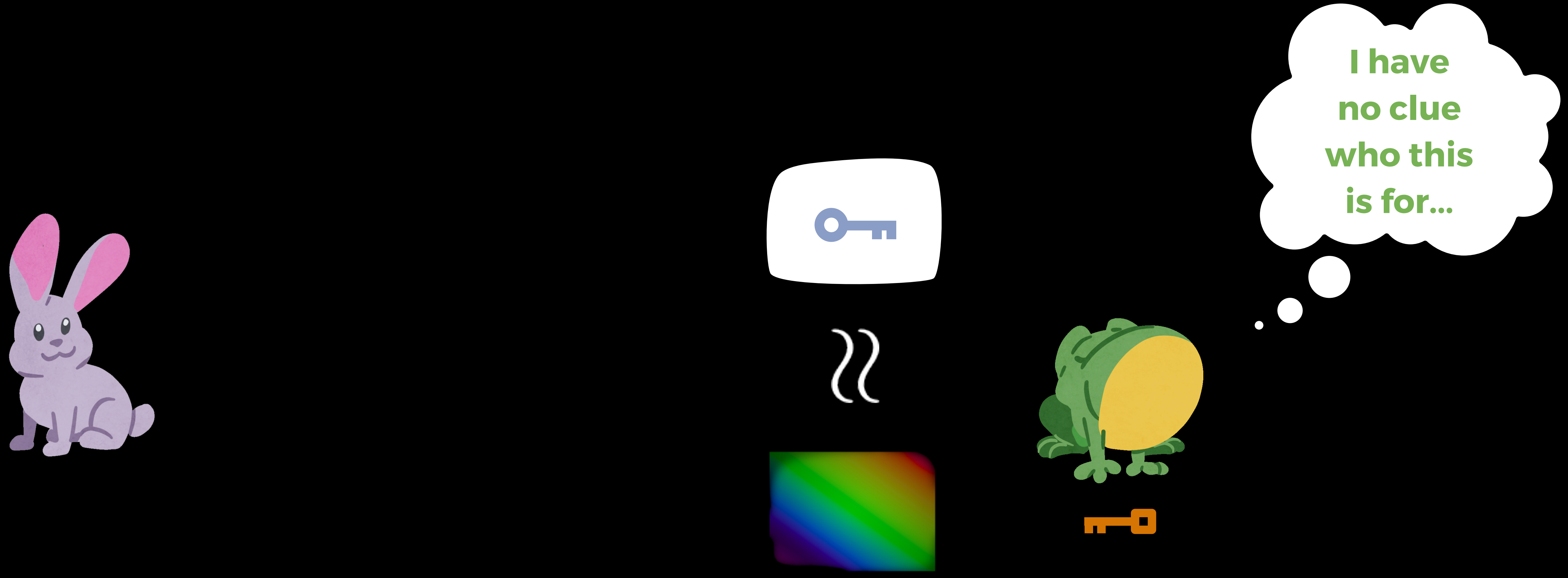
HYBRIDIZING TWO KEM SCHEMES, THE PRIVACY OF ENCAPSULATED KEYS RELIES ON THE BEST OF BOTH SECURITIES



ANONYMITY



ANONYMITY



an encapsulation under any other pk

ENCAPSULATING FOR SUBSET COVERS

ENCAPSULATING FOR SUBSET COVERS

IN MANY USE-CASES,
ONE DOES NOT WANT
TO PROVIDE ENCAPSULATIONS
FOR EVERY SINGLE TARGET IDENTITY...

ENCAPSULATING FOR SUBSET COVERS

Users will have attributes,
and encapsulations will work
for logical (and, or, not) policies
on these attributes.

ENCAPSULATING FOR SUBSET COVERS

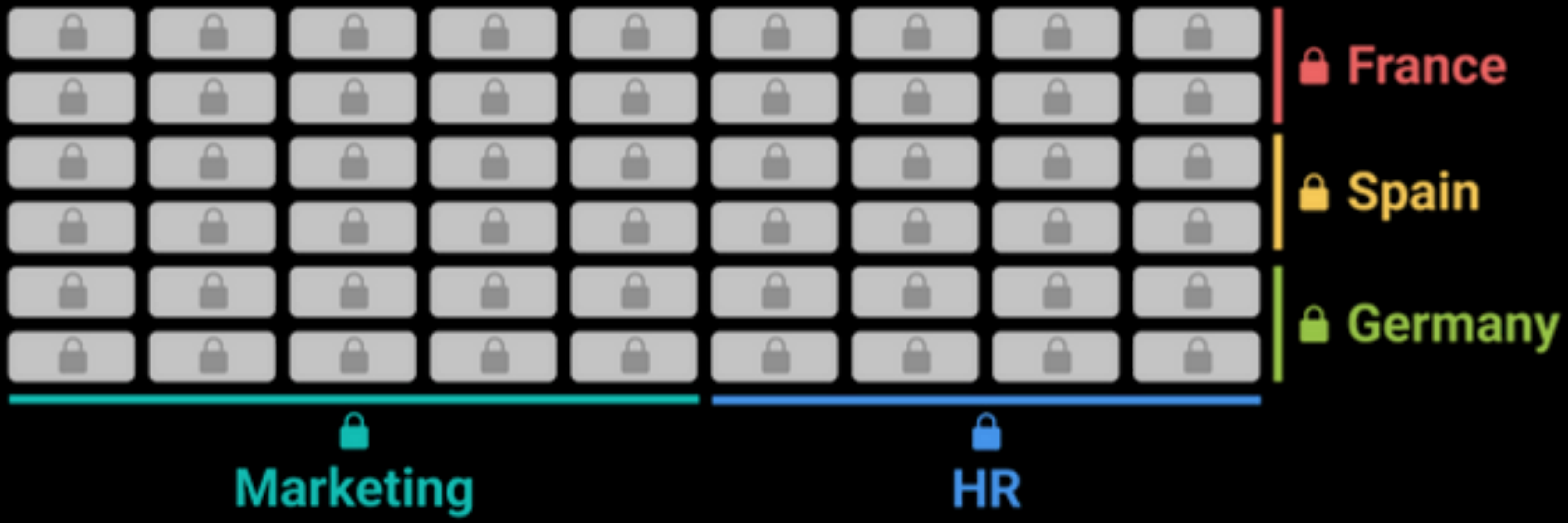
COULD ONE USE ATTRIBUTE-BASED ENCRYPTION (ABE)?

These powerful schemes would have all the features wanted with respect to attribute policies.

ENCAPSULATING FOR SUBSET COVERS

COULD ONE USE
ATTRIBUTE-BASED ENCRYPTION (ABE)?
These powerful schemes would have all the features wanted with respect to attribute policies.
But way more features
than those we actually need,
And much more efficient solutions exist
using subset-cover paradigms.

ENCAPSULATING FOR SUBSET COVERS



ENCAPSULATING FOR SUBSET COVERS

AN EXAMPLE:

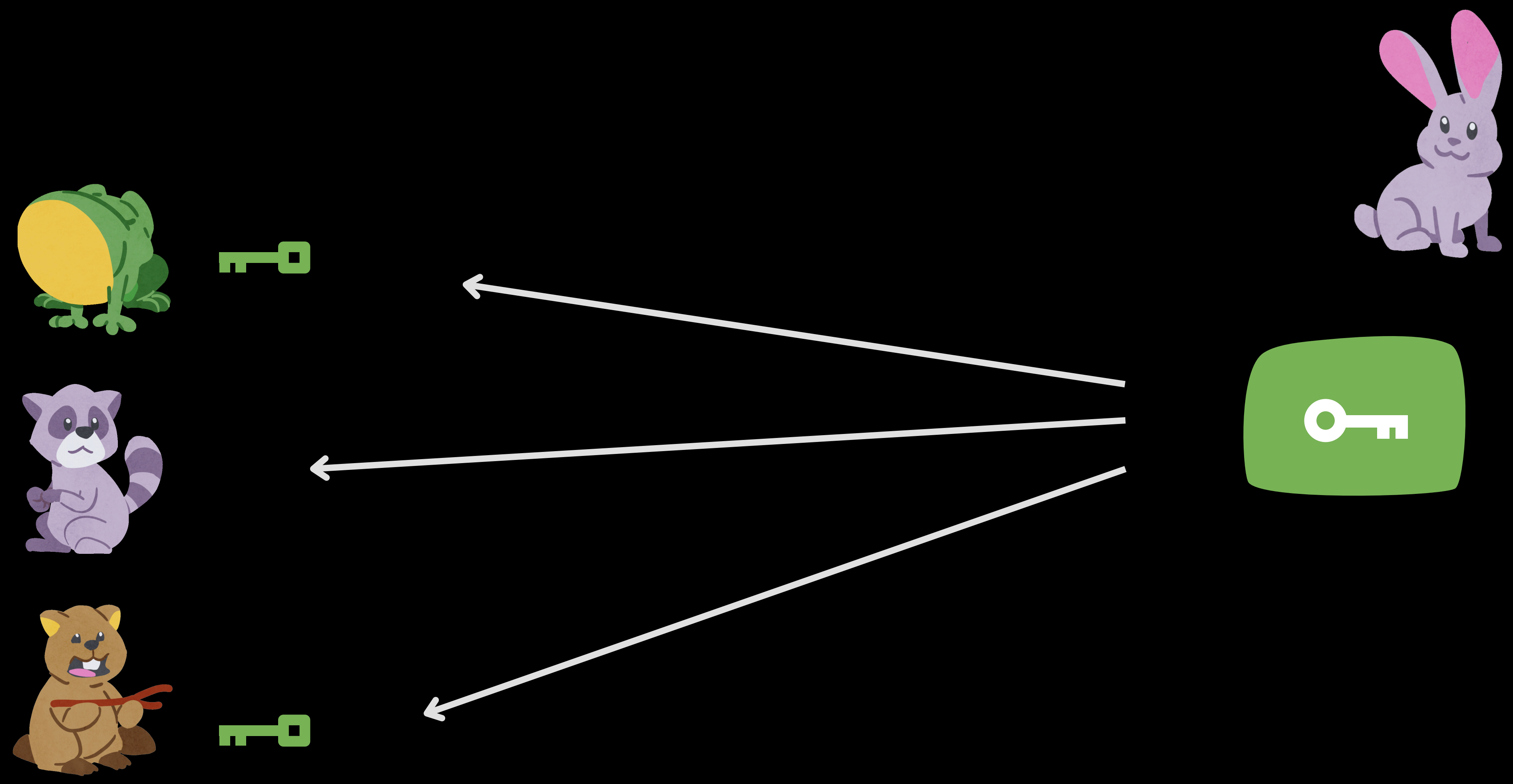
breathes in air and water,
aquatic

breathes in air,
eats from human trash

breathes in air,
aquatic

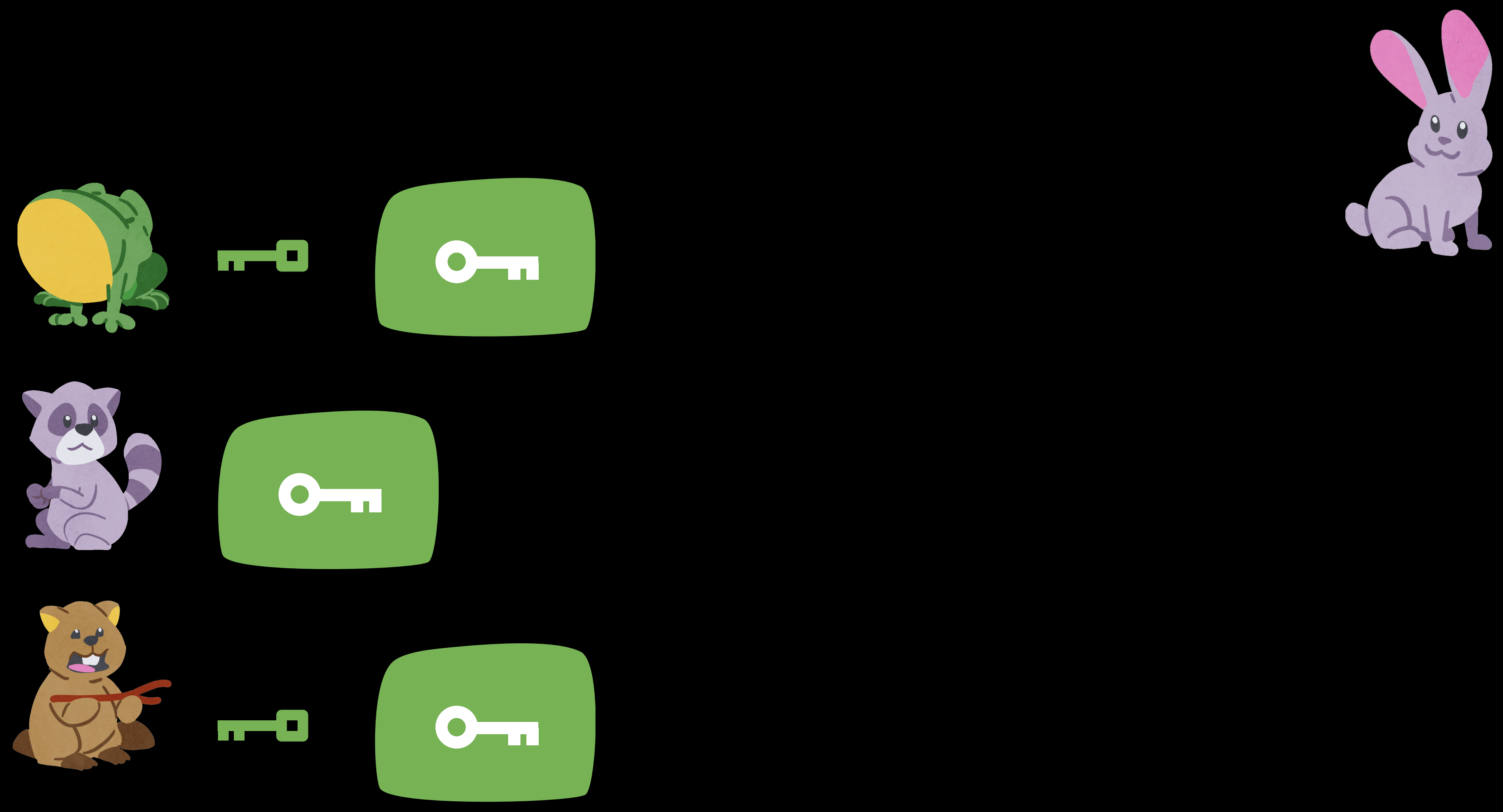
ENCAPSULATING FOR SUBSET COVERS

AN EXAMPLE:



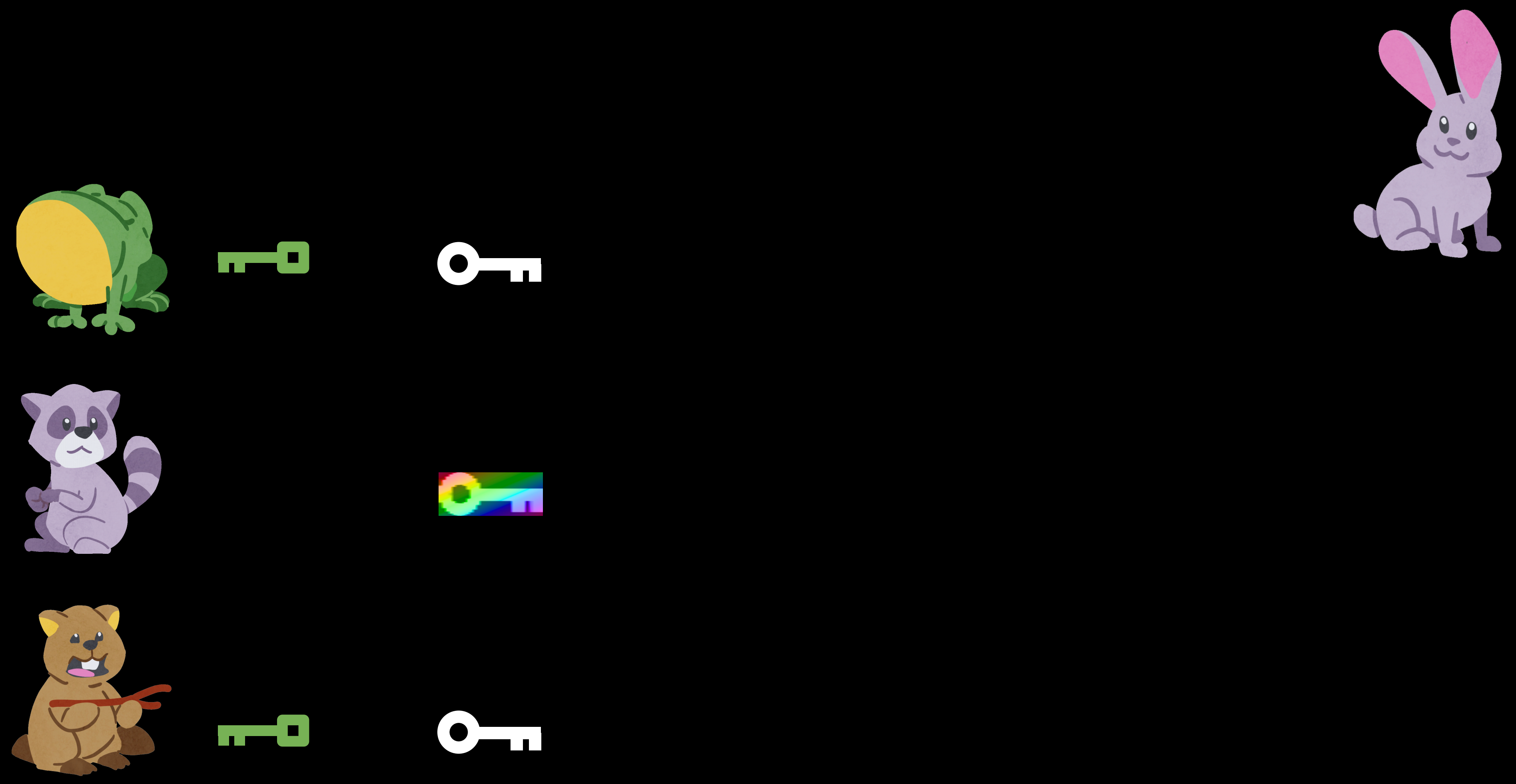
ENCAPSULATING FOR SUBSET COVERS

AN EXAMPLE:



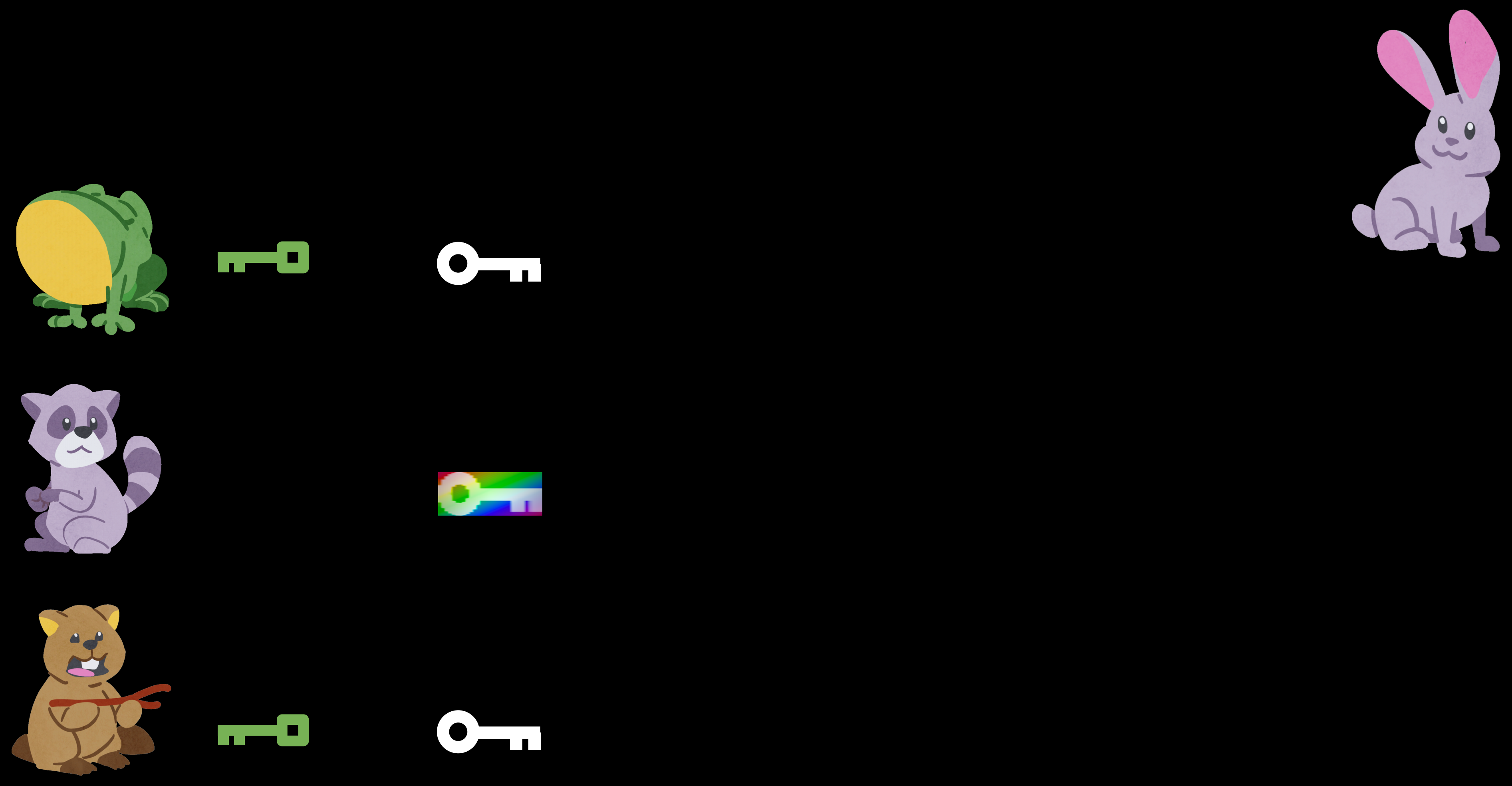
ENCAPSULATING FOR SUBSET COVERS

AN EXAMPLE:



AUTHENTICATION

HOW CAN RACCOON KNOW THAT WHAT SHE DECAPSULATED IS SOMETHING RANDOM AND NOT A REAL KEY?

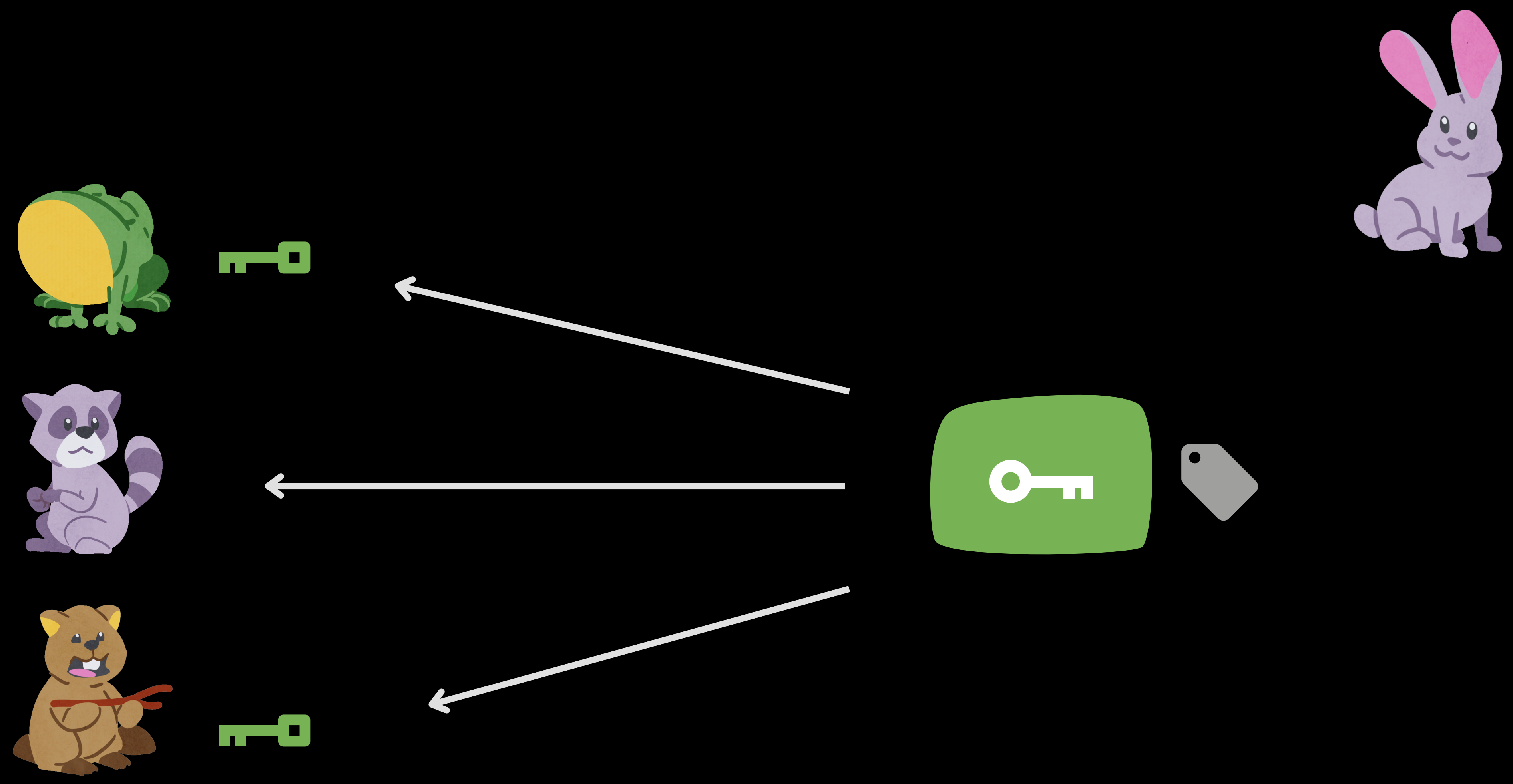


AUTHENTICATION

HOW CAN RACCOON KNOW THAT WHAT SHE DECAPSULATED IS SOMETHING RANDOM AND NOT A REAL KEY?

AUTHENTICATION

HOW CAN RACCOON KNOW
THAT WHAT SHE DECAPSULATED
IS SOMETHING RANDOM
AND NOT A REAL KEY?

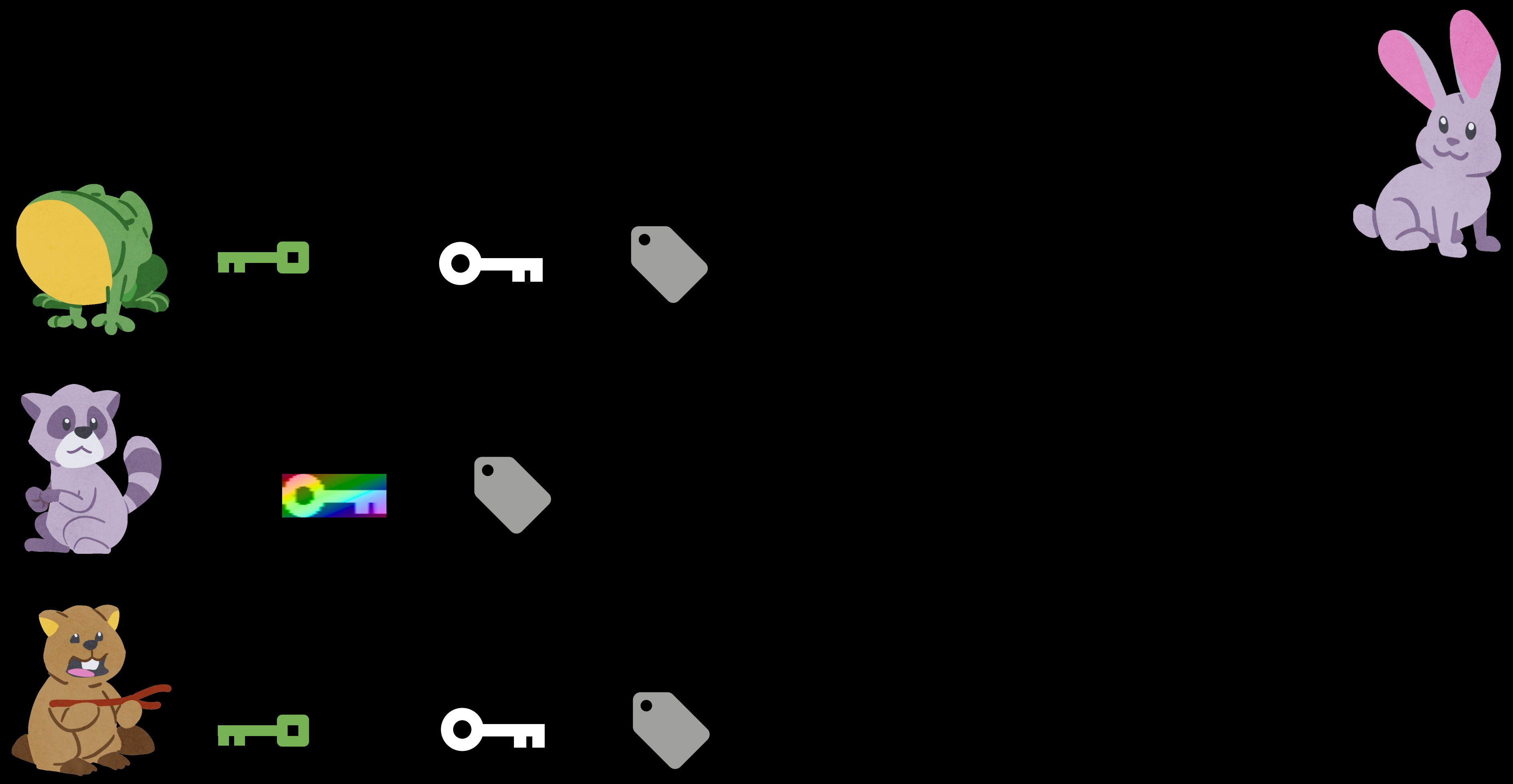


AUTHENTICATION

HOW CAN RACCOON KNOW
THAT WHAT SHE DECAPSULATED
IS SOMETHING RANDOM
AND NOT A REAL KEY?

AUTHENTICATION

HOW CAN RACCOON KNOW
THAT WHAT SHE DECAPSULATED
IS SOMETHING RANDOM
AND NOT A REAL KEY?

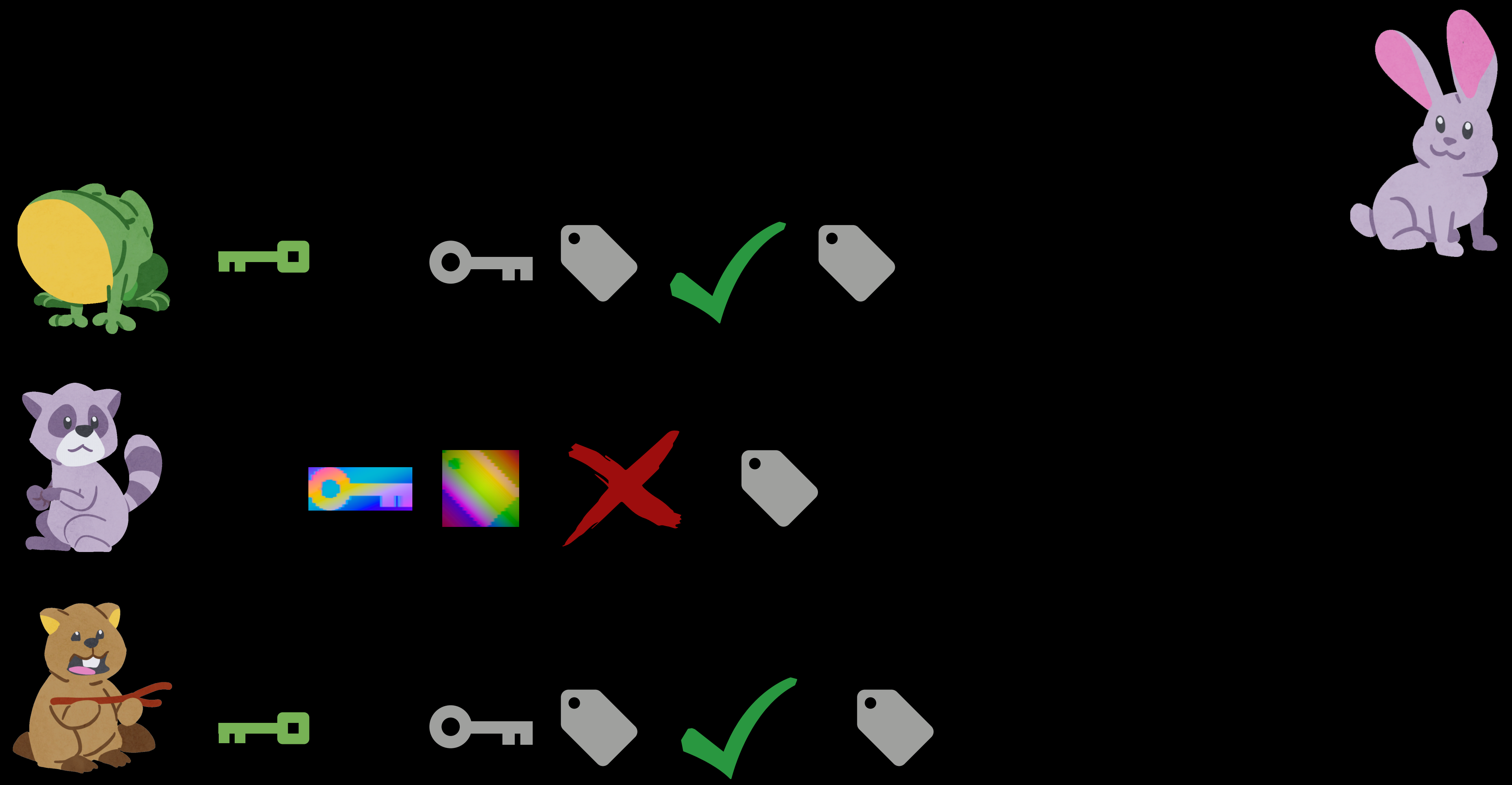


AUTHENTICATION

HOW CAN RACCOON KNOW THAT WHAT SHE DECAPSULATED IS SOMETHING RANDOM AND NOT A REAL KEY?

AUTHENTICATION

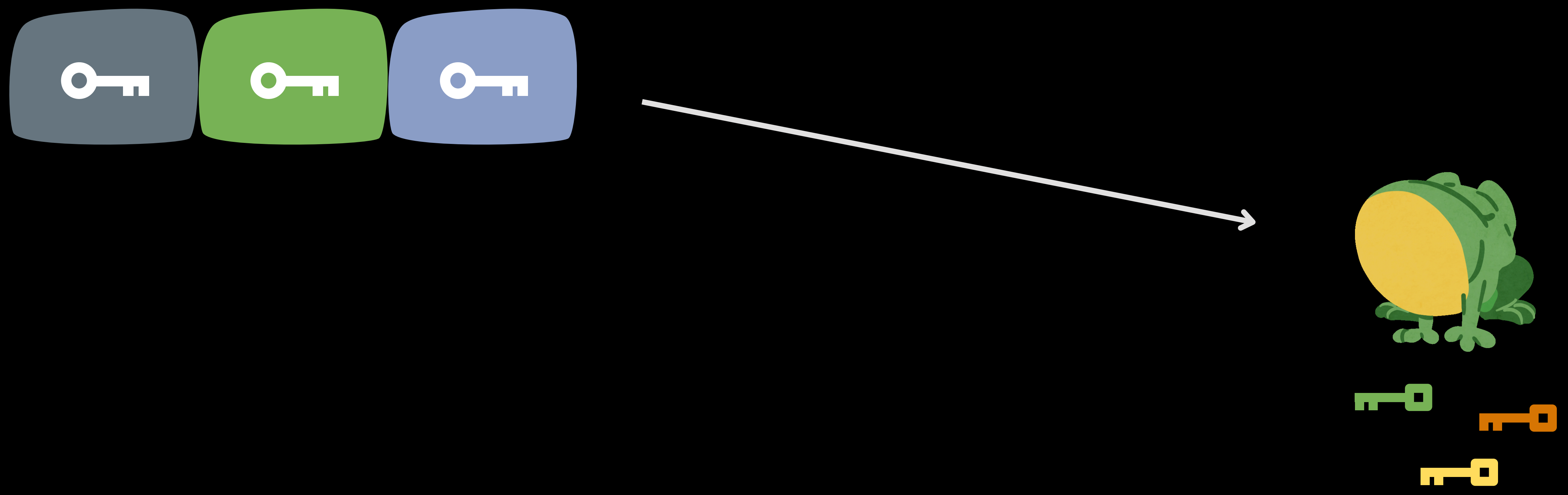
HOW CAN RACCOON KNOW
THAT WHAT SHE DECAPSULATED
IS SOMETHING RANDOM
AND NOT A REAL KEY?



BOOSTING EFFICIENCY WITH AUTHENTICATION

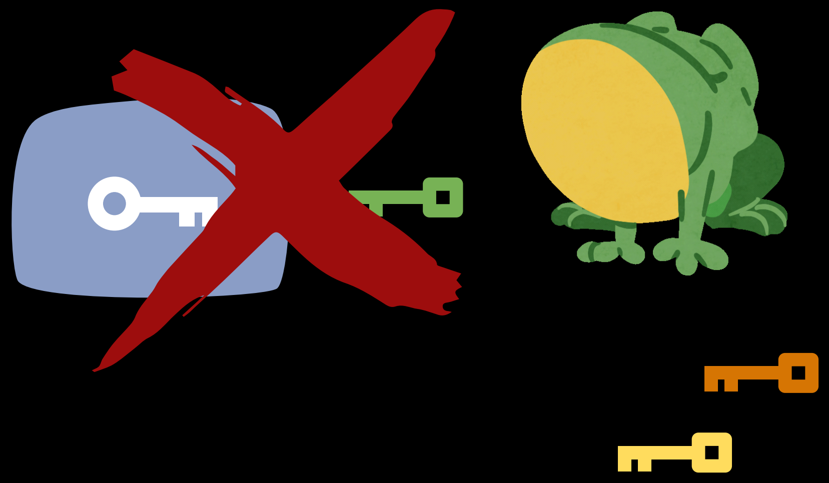
AN EARLY-ABORTS PARADIGM

USING A KEM WITH AUTHENTICATION TAGS



AN EARLY-ABORTS PARADIGM

USING A KEM WITH AUTHENTICATION TAGS

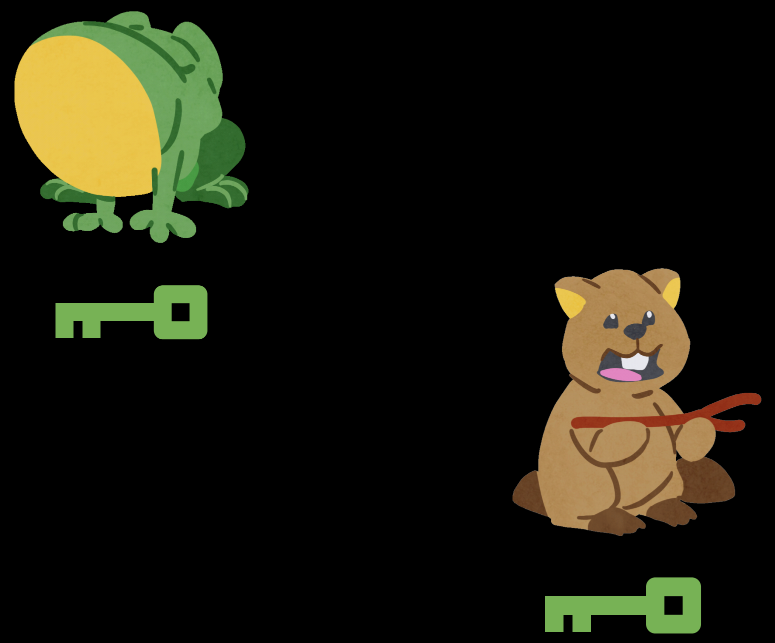


AN EARLY-ABORTS PARADIGM

USING A KEM WITH AUTHENTICATION TAGS

BUT...

SHOULD USERS HAVE THE SAME KEYS?



GENERALLY NOT GOOD PRACTICE: HOW DO WE HOLD USERS ACCOUNTABLE?

SOLUTION:
USERS HAVE ATTRIBUTE KEYS
+ A UNIQUE USER KEY

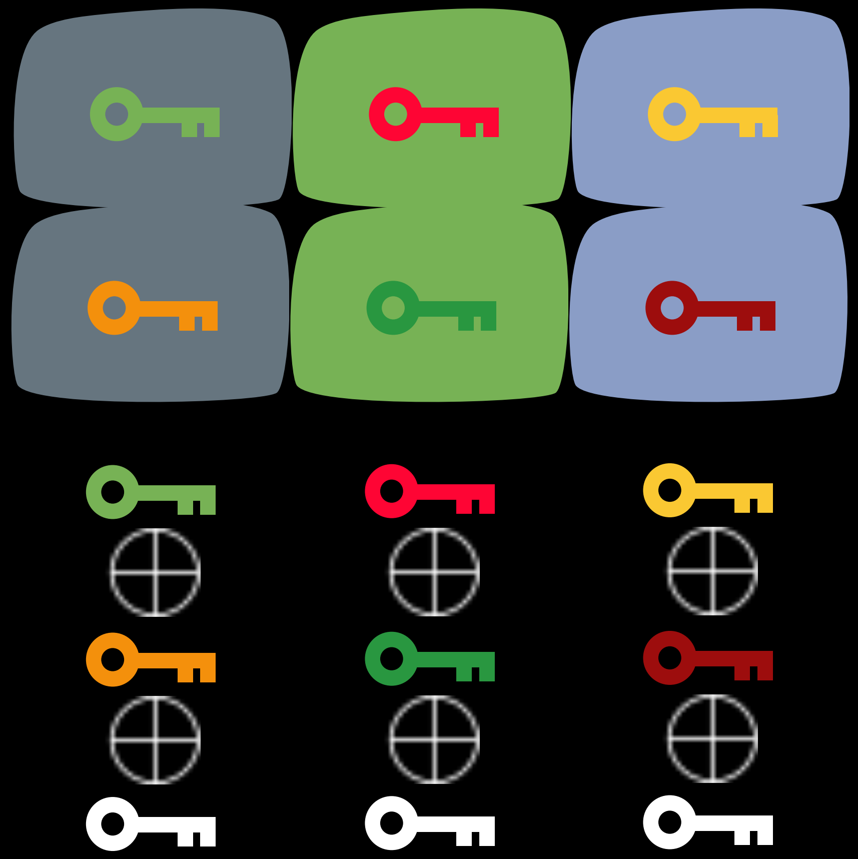
THIS UNIQUE USER KEY IS ALSO USED IN DECAPSULATION.

as an (optional) additional feature,
this user key can be used to trace users
when the tracing authority is in tracing mode.
Meaning that if some users leak their keys
-> ACCOUNTABILITY

USING PKE SCHEME PROPERTIES IN THE HYBRIDIZATION

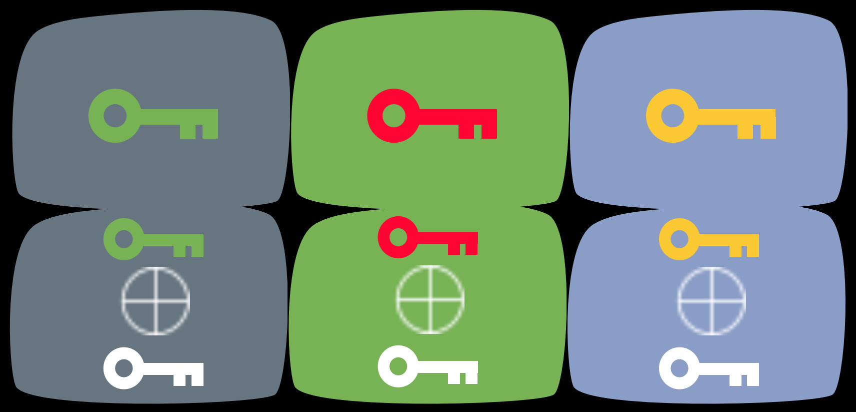
IF ONE OF THE KEMS COMES FROM A PKE SCHEME, WE CAN SAVE ON ENCAPSULATION SIZE

GENERIC APPROACH TO ENCAPSULATE 🔑 :



USING PKE SCHEME PROPERTIES IN THE HYBRIDIZATION

IF ONE OF THE KEMS COMES FROM A PKE SCHEME, WE CAN SAVE ON ENCAPSULATION SIZE



ENCAPSULATING 🔑 WITH A PKE:

The session key
XORed with the first KEM's masking key
can be used in the KEM built
from a Public Key Encryption scheme.

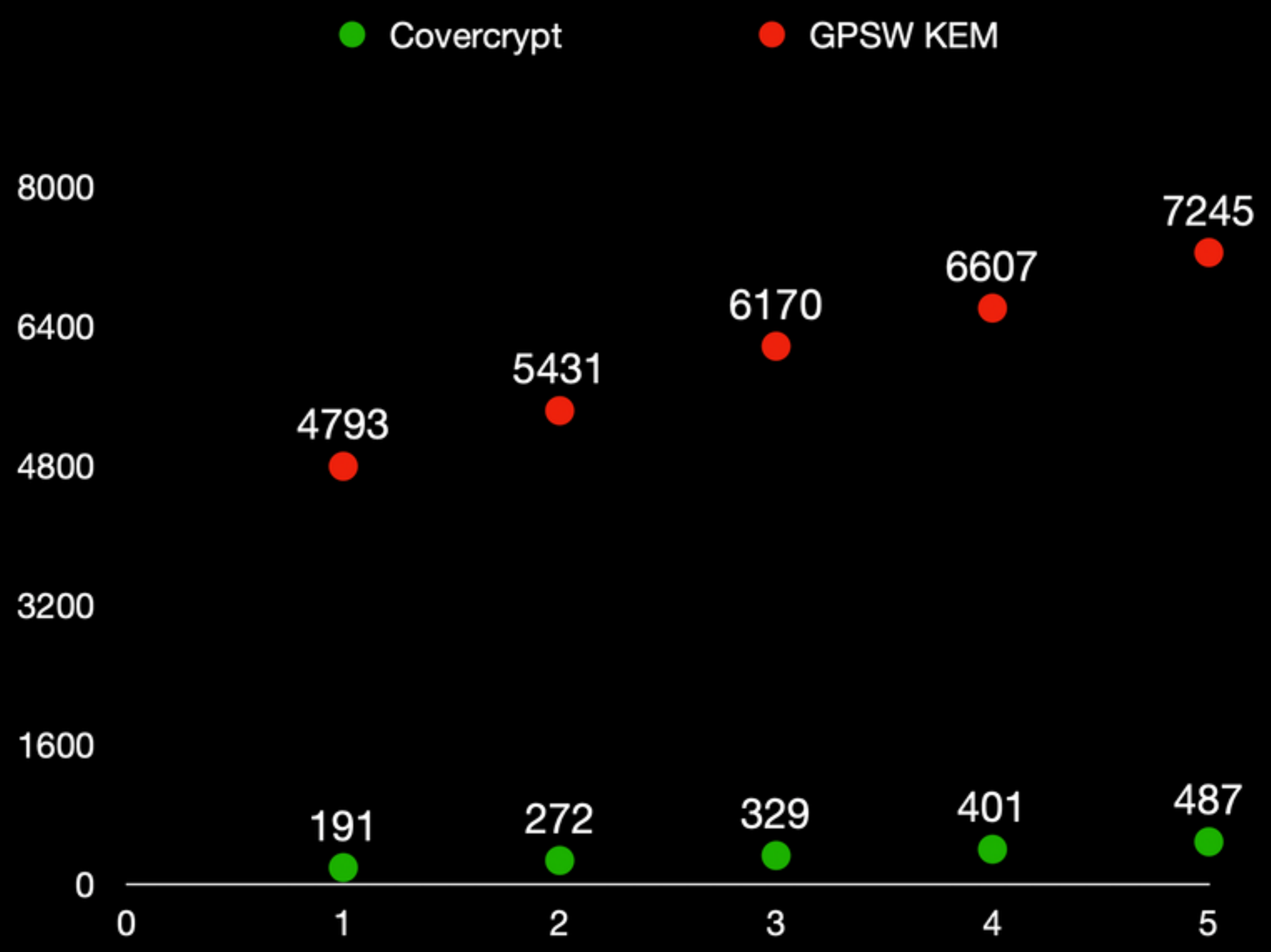
Remark:
with ElGamal, the top
encapsulations can
be reduced to one

PERFORMANCE

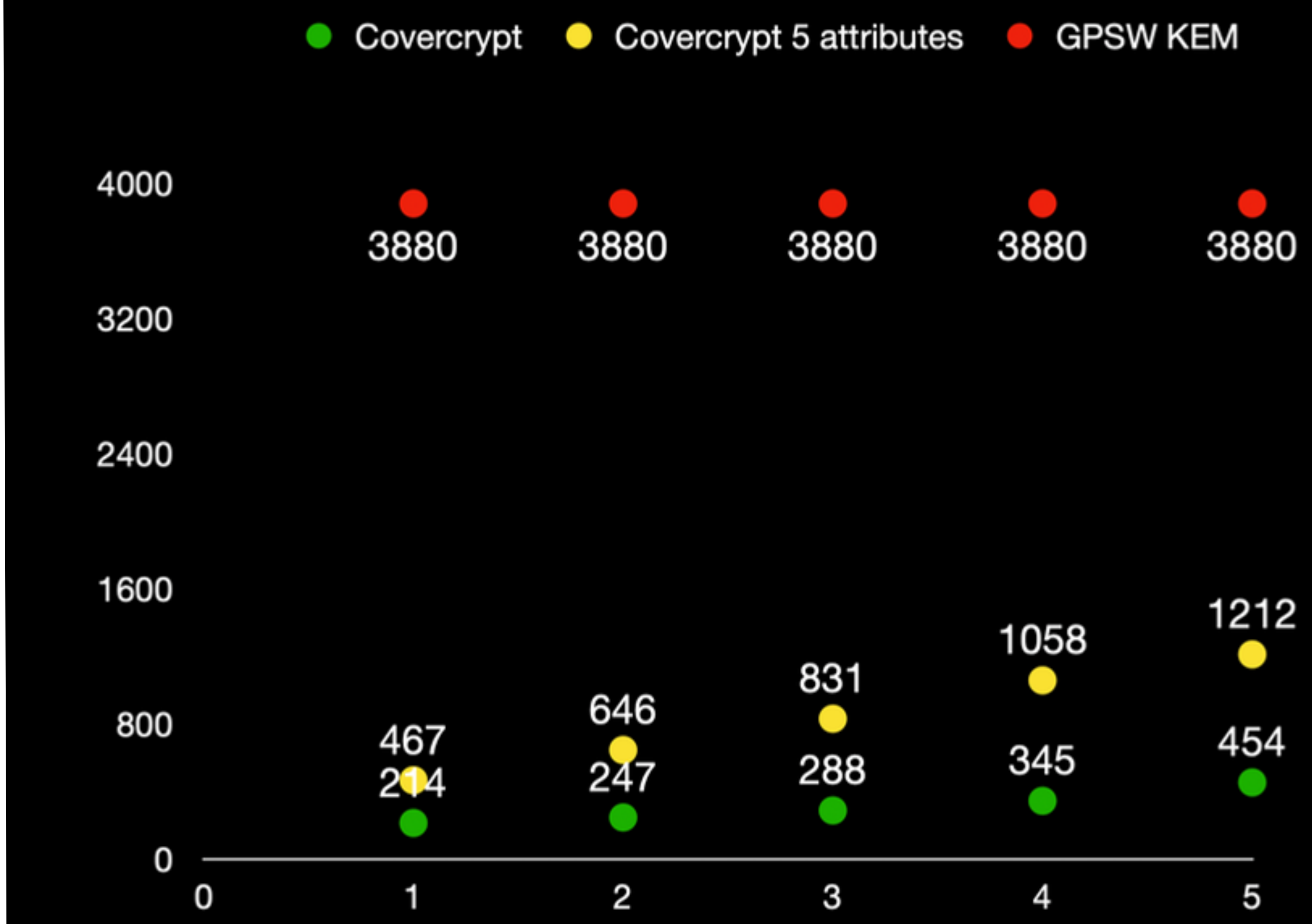
WHEN IMPLEMENTING SUCH A KEM

COVERCRYPT vs GPSW KEM

Encapsulation time (in µs)



Decapsulation time (in µs)



CONCLUSION

A KEM for KEM-DEM, authentication, and more

Hybridization for post- and pre-quantum resistance

Anonymity

Subset-covers of user-**attributes**

Very **efficient**: no ABE, authentication and early-aborts

Unique user-keys, tracing is possible

THANK YOU

WORK BY THÉOPHILE BRÉZOT [1], PAOLA DE PERTHUIS [1, 2] & DAVID POINTCHEVAL[2]

FULL VERSION: HTTPS://EPRINT.IACR.ORG/2023/836
PUBLISHED AT ESORICS 2023

SPEAKER: CHLOÉ HÉBANT [1], SLIDES: PAOLA DE PERTHUIS

1: cosmian

2: 1794 ENS ÉCOLE NORMALE SUPÉRIEURE

MEET US AT OUR DEMO STAND

WORK BY THÉOPHILE BRÉZOT [1], PAOLA DE PERTHUIS [1, 2] & DAVID POINTCHEVAL[2]

FULL VERSION: HTTPS://EPRINT.IACR.ORG/2023/836

PUBLISHED AT ESORICS 2023

SPEAKER: CHLOÉ HÉBANT [1], SLIDES: PAOLA DE PERTHUIS

1: cosmian

2: 1794 ENS ÉCOLE NORMALE SUPÉRIEURE