The Standards People

Cryptographic access control by attributes

Ongoing standards development at ETSI

ETSI - Cyber Security | Cyber Security Standards | Cyber Security Technology

Presented by:

Giovanni Bartolomeo (CNIT)
Paola de Perthuis (Cosmian, École normale supérieure)

giovanni.bartolomeo@uniroma2.it
paola.de.perthuis@cosmian.com

25th July 2023

Agenda

- Overview of cybersecurity activities in ETSI
- TC CYBER Introduction & ongoing work
- Attribute-Based Encryption for ABAC (ETSI TS 103 532)
- Focus on Quantum-Safe Cryptography: CYBER-QSC Ongoing Work and publications
- Efficient Quantum-Safe Hybrid KEM with Attribute Subset-Cover

Overview of cybersecurity activities in ETSI

CROSS-DOMAIN CYBERSECURITY (TC CYBER)

- Cybersecurity ecosystem
- Protection of personal data & communications
- Consumer IoT security and privacy
- Security of critical infrastructures
- Enterprise and individual cybersecurity
- Forensics
- Cybersecurity tools and guides

SECURING TECHNOLOGIES & SYSTEMS

- Mobile / wireless systems (5G, TETRA, DECT, RRS, RFID…)
- Network functions virtualization
- Intelligent Transports Systems
- Broadcasting
- Artificial Intelligence
- IoT (oneM2M)

SECURITY TOOLS & TECHNIQUES

- Lawful interception & retained data
- Digital signatures & trust services
- Permissioned distributed ledgers
- Smart cards / secure elements
- Security algorithms
- Quantum key distribution
- Quantum-safe cryptography
- Encrypted Traffic Integration

ETSI TC CYBER – Introduction

Created in 2014, ETSI Technical Committee CYBER is ETSI's Centre of Excellence and focal point for Cyber Security:

- Advising and assisting all ETSI groups with the development of Cyber Security Requirements
- Developing and maintaining the Standards, Specifications and other deliverables
- Collecting and specifying Cyber Security requirements from relevant stakeholders
- Identifying gaps where existing standards do not fulfil the requirements and providing specifications and standards to fill these gaps
- Coordinating with external groups such as ENISA
- Answering policy requests related to Cyber Security, and security in broad sense in the ICT sector

International community of ~80 participants

- From industry, government(s), research and academia, users and society
- 4 plenary meetings per year, bi-weekly regular and ad-hoc calls

ETSI TC CYBER – Ongoing Work

Cybersecurity ecosystem

Consumer IoT

Security and Privacy

Protection of personal data and communication

Network Security

Cybersecurity for Critical Infrastructures

Cybersecurity tools & guides

Direct support to EU legislation

Quantum-Safe Cryptography

https://www.etsi.org/cyber-security/tc-cyber-roadmap

Focus on the Protection of personal data and communications

ETSI is addressing the technical support to privacy legislation in the EU and beyond.

Relevant past publications include:

- Technical guide to privacy addressing and cataloguing relevant standards globally ETSI TR 103 370 V1.1.1 (2019-01)
- Attribute-Based Encryption ABE requirements ETSI TS 103 458 V1.1.1 (2018-06)
- Mechanisms for privacy assurance and verification ETSI TS 103 485 V1.1.1 (2020-08)

Ongoing work:

- A Verifiable Credentials extension using Attribute-Based Encryption
- Design practices against technology enabled coercive control

Attribute-Based Encryption: an evolution of PKC

Public Key Crypto	Identity-Based Encryption[1]	Attribute-Based Encryption[2-4]
$z=\{x\}_{pk(a)}$ $x=\{z\}^{-1}_{sk(a)}$ *Solves key-distribution problem (pk is publicly available)*	$z=\{x\}_{mpk,\text{"receiver"}}$ $x=\{z\}^{-1}_{mpk,sk(\text{"receiver"})}$ *Many randomized secrets keys for one set of MPK, MSK* *Public keys "replaced" by plain strings* *A KMS distributes MPK and generates secret keys*	$z=\{x\}_{mpk,(a\wedge b)\vee c}$ $x=\{z\}^{-1}_{mpk,sk(\{a,b\})}$ *Combines IBE with SSS [2] and monotonic span trees [3,4]* *A fine-granuled content access policy implemented in crypto!* *Many further math properties…*

1. A. Shamir. Identity-based cryptosystems and signature schemes. In Proceedings of CRYPTO 84 on Advances in cryptology, pages 47–53. Springer-Verlag New York, Inc., 1984.
2. A. Sahai and B. Waters. Fuzzy identity-based encryption. In EUROCRYPT, pages 457-473, 2005.
3. V. Goyal, O. Pandey, A. Sahai, B. Waters: "Attribute-based encryption for fine-grained access control of encrypted data", Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS '06, pages 8-98, New York, NY, USA, 2006. ACM.
4. J. Bethencourt, A. Sahai, B. Waters: "Ciphertext-policy attribute-based en-cryption", Proceedings of the 2007 IEEE Symposium on Security and Privacy, SP'07, pages 32-334. Washington, DC, USA, IEEE Computer Society.

Application Examples

Key-Policy ABE: Mail archive use case

- Each mail is labelled with attributes describing sender, receiver, time, subject, category, etc.
- Users are able to access only a subset of emails whose attributes satisfying their assigned key-policy

Ciphertext-Policy ABE: Role-based access control for medical records or industrial IoT applications: data folders encrypted with a policy

- Users are able to access only those folders whose policy is satisfied by attributes embedded in their keys
- Additional context attributes may be included

ABE: Main features (1)

Combine PK encryption and distributed, fine-grained, attribute-based access control

No need to grant right at the time of encryption

Can define almost any kind of policy and predicates (*)

Encrypt once – decrypt many: no need to encrypt per user, but per group of users (owning a similar key-policy or attributes)

Collusion prevention as main security feature

A special case of more general functional encryption (ciphertext decrypts differently according to decryption key)

ABE: Main features (2)

A three-party relationship, with public parameters by the ABE Authority

- No need for a new PKI, though an integration is possible; more suitable for federated, decentralized model

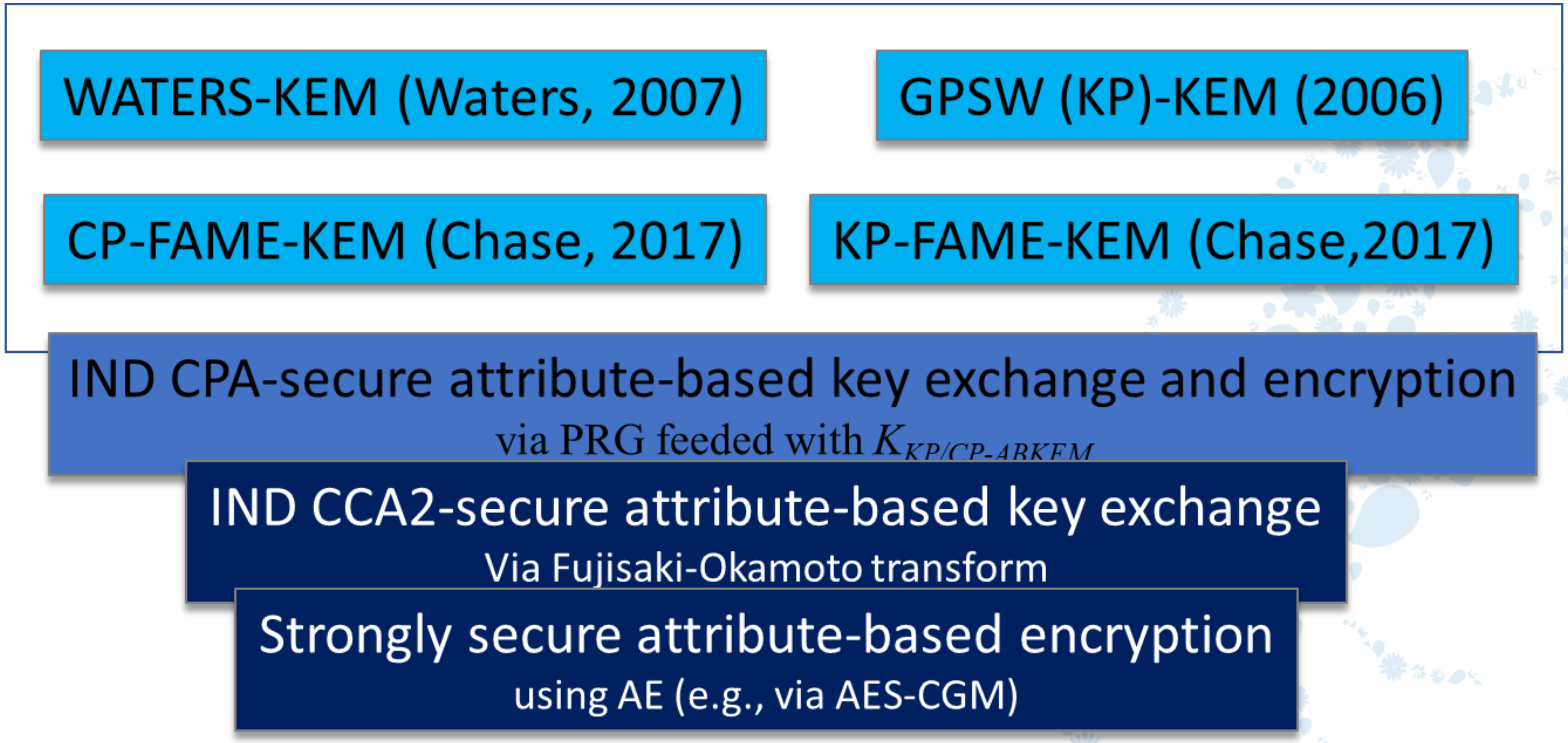
Secret key distributed to authenticated users

Combine attributes from multiple ABE authorities is possible (by a shared user ID)

- Chase, M. (2007): "Multi-authority Attribute Based Encryption", TCC (p. 515-534).
- Lewko, A. B. & Waters, B. (2011): "Decentralizing Attribute-Based Encryption", EUROCRYPT, (p. 568-588). Patent US8516244 B2 and US2012314854 A1 available under FRAND terms & conditions, since 2022 according to ETSI IPR database

Attribute-Based Encryption for ABAC
ETSI TS 103 532 V1.2.1 (2021-05) (1)

A modular toolbox architecture for standard ABE



WATERS-KEM (Waters, 2007)

GPSW (KP)-KEM (2006)

CP-FAME-KEM (Chase, 2017)

KP-FAME-KEM (Chase,2017)

IND CPA-secure attribute-based key exchange and encryption

via PRG feeded with $K_{KP/CP\text{-}ABKEM}$

IND CCA2-secure attribute-based key exchange

Via Fujisaki-Okamoto transform

Strongly secure attribute-based encryption

using AE (e.g., via AES-CGM)

Attribute-Based Encryption for ABAC ETSI TS 103 532 V1.2.1 (2021-05) (2)

TS 103 532 specifies: CP-WATERS-KEM, KP-GPSW-KEM, CP-FAME-KEM, KP-FAME-KEM as standard ABE KEM schemas

However, other CP-ABKEMs and KP-ABKEMs may be used, under compliance with the following requirements:

- Requirement 1: Correctness and indistinguishability under CPA
- Requirement 2: Sufficient security levels - shall admit values of the security parameter that provide 128, 192, 256, 384 and 512-bit security

Attribute-Based Encryption for ABAC
ETSI TS 103 532 V1.2.1 (2021-05) (3)

Revocation is implemented by key expiration

- alternatively, ciphertext (partial) re-encryption
- but "Forward" revocation is easier
  - Attribute revocation by White/Black lists
  - Combine keys with crypto accumulators

KMS for user secret key distribution: ideal for framework that already relies on one or more central authority/ies

Ciphertext length / key length vs number of used attributes

Attribute-Based Encryption for ABAC
ETSI TS 103 532 V1.2.1 (2021-05) (4)

Standard Policy language? TS 103 532 provides a first attempt…

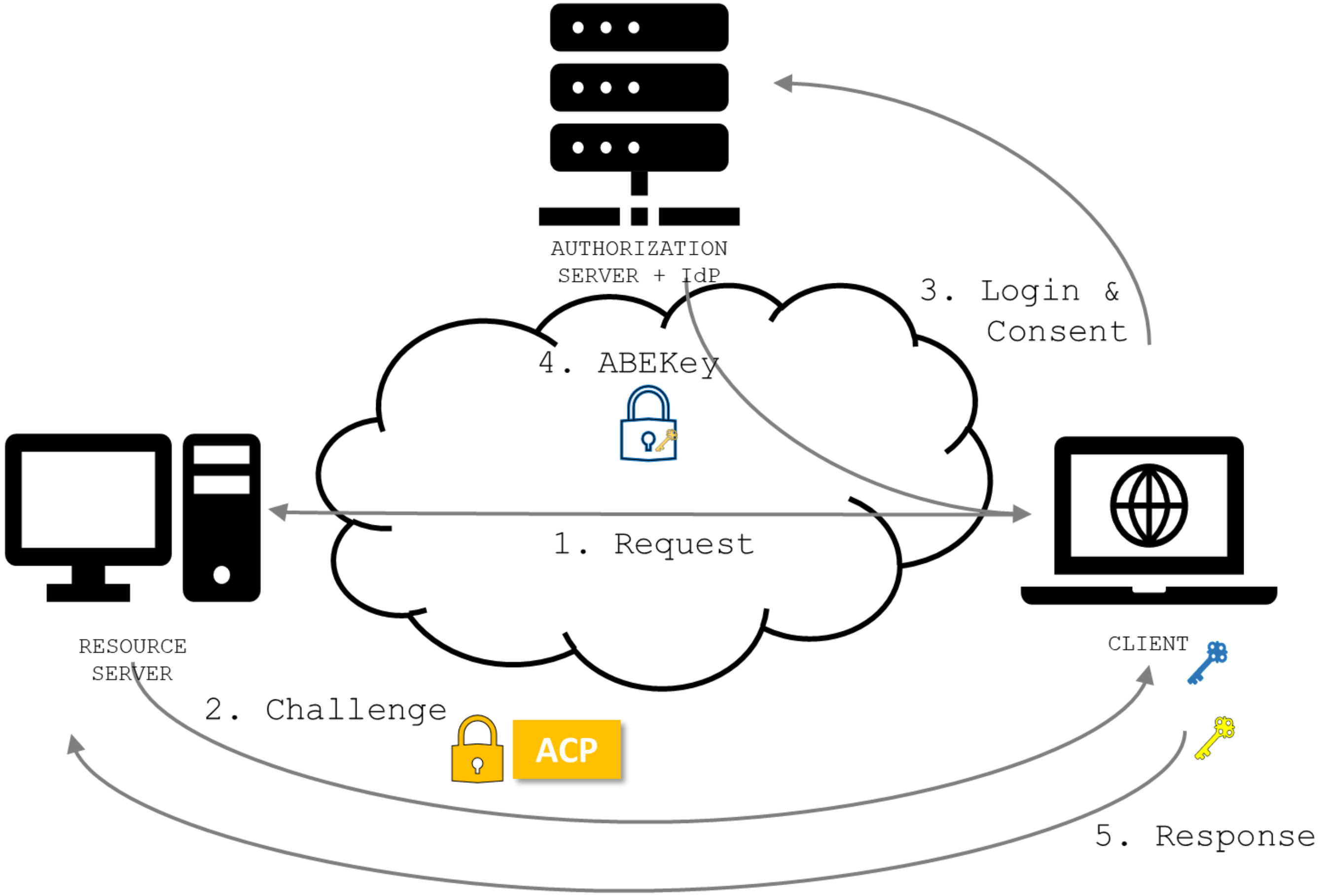
- Layer 1: exploits native capabilities, offers simple typed attributes (int, string, bool) and operators (Boolean/relational/threshold)
- Layer 2: meant for higher-level preprocessors and compilers that wish to extend ABKEM access control beyond the native capabilities of a schemes, offers rich semantics data types
- Translation of a subset of XACML

Browser support (Webcrypto?)

HF: relatively complex crypto, not always perfectly understood by developers

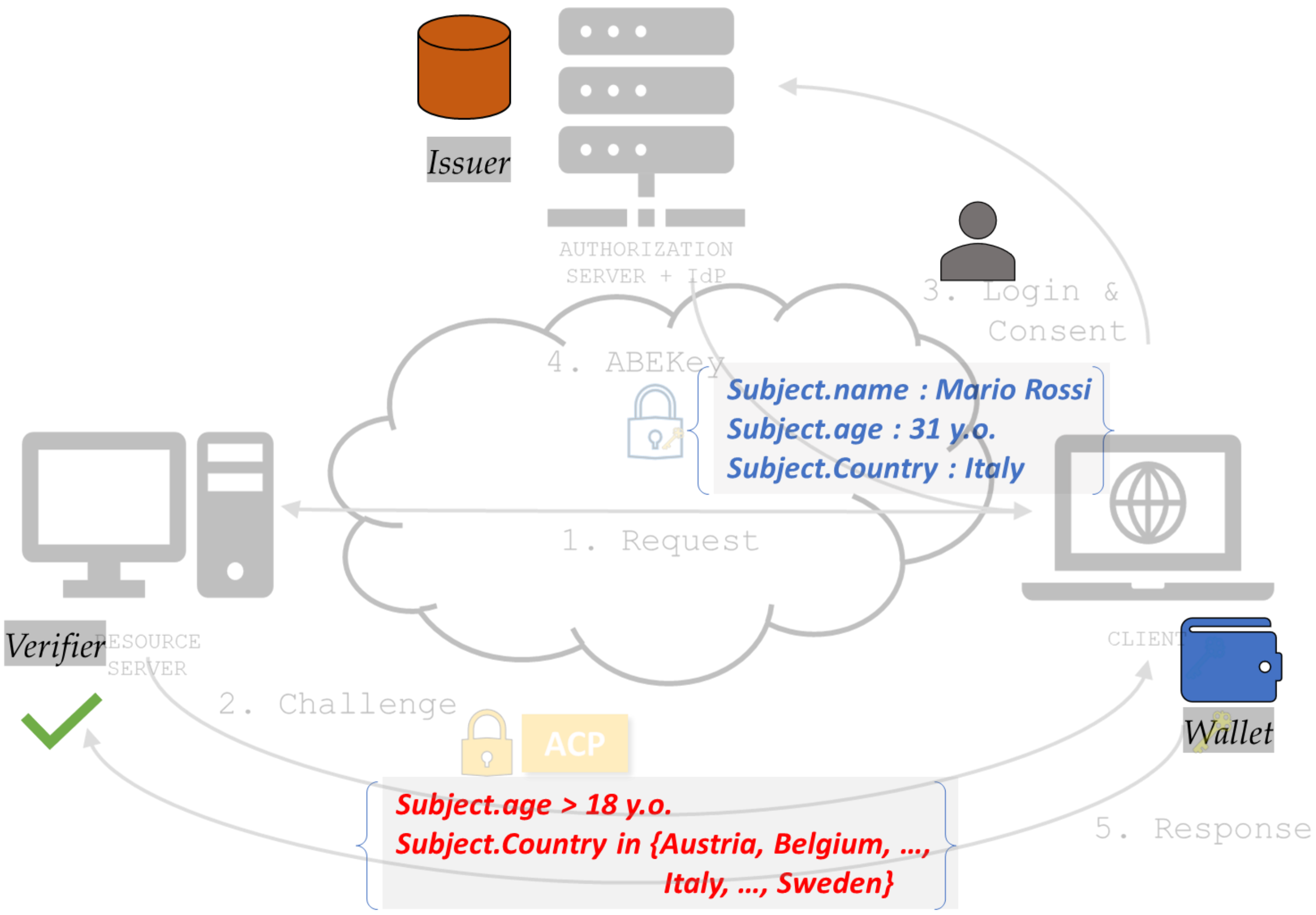
Challenge-response mechanism for delegated authentication/authorization (1)

A Verifiable Credentials extension using Attribute-Based Encryption?



Challenge-response mechanism for delegated authentication/authorization (2)

A Verifiable Credentials extension using Attribute-Based Encryption?



Focus on Quantum-Safe Cryptography (QSC)

Launched in 2013 as a Workshop and as an Industry Specification group in 2015 to **study the potential impacts of Quantum Computing** in order to make recommendations on Quantum Safe Cryptography.

QSC became a working group of TC CYBER in 2017.

Specialises in providing **practical advice to industry** on issues such as risk assessment, migration timelines, architecture and integration issues.

Realistic quantum-safe options for important real-world applications such as VPNs, code signing, transport security…

(Does not specify algorithms or key distribution techniques)

Quantum-Safe Cryptography –
Ongoing Work and publications

Current Work Items:

CYBER; Deployment Considerations for Hybrid Schemes (TR)

CYBER; Quantum-Safe Hybrid Key Exchanges (revision of TS 103 744)

Impact of Quantum Computing on Cryptographic Security Proofs (TR)

CYBER; Impact of Quantum Computing on Symmetric Cryptography (TR)

Past publications:

CYBER; Quantum-Safe Cryptography Migration for ITS and C-ITS, ETSI TR 103 949 V1.1.1 (2023-05)

CYBER; Quantum-Safe Key Exchanges, ETSI TR 103 507 V1.1.1 (2017-10)

Quantum-Safe Public Key Encryption and Key Encapsulation, ETSI TR 103 832 V1.1.2 (2021-09)

CYBER; Quantum-Safe Signatures, ETSI TR 103 616 V1.1.1 (2021-09)

CYBER; Quantum-Safe Virtual Private Networks, ETSI TR 103 617 V1.1.1 (2018-09)

CYBER; Quantum-Safe Identity-Based Encryption, ETSI TR 103 618 V1.1.1 (2019-12)

CYBER; Migration strategies for Quantum Safe schemes, ETSI TR 103 619 V1.1.1 (2020-07)

State Management for stateful authentication mechanisms, ETSI TR 103 692 V1.1.1 (2021-11)

CYBER; Quantum-safe Hybrid Key Exchanges, ETSI TS 103 744 V1.1.1 (2020-12)

Efficient Quantum-Safe Hybrid Key Exchange Mechanisms (KEM) with Attribute Subset-Cover

New initiative,

not ABE but grants its desired properties in practice, very efficiently.

https://eprint.iacr.org/2023/836

By Théophile Brézot [1], **Paola de Perthuis** [1,2] & David Pointcheval [2]

1: cosmian 2: 1794 ENS ÉCOLE NORMALE SUPÉRIEURE

Motivations

As before with Attribute-Based Encryption (ABE),

we can build a Key Encapsulation Mechanism (KEM),

to get Public-Key Encryption (PKE) in the KEM-DEM paradigm,

also in authentication contexts (encapsulating the session key).

Motivations

As before with Attribute-Based Encryption (ABE),

we can build a Key Encapsulation Mechanism (KEM),

to get Public-Key Encryption (PKE) in the KEM-DEM paradigm,

also in authentication contexts (encapsulating the session key).

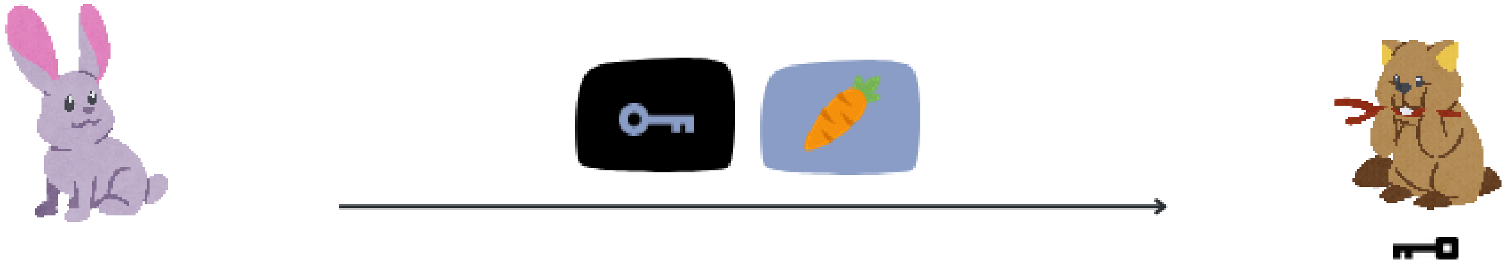
Motivations

As before with Attribute-Based Encryption (ABE),

we can build a Key Encapsulation Mechanism (KEM),

to get Public-Key Encryption (PKE) in the KEM-DEM paradigm,

also in authentication contexts (encapsulating the session key).



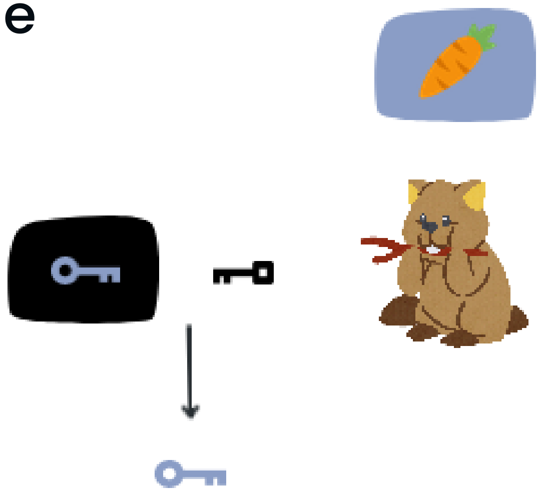
Motivations

As before with Attribute-Based Encryption (ABE),

we can build a Key Encapsulation Mechanism (KEM),

to get Public-Key Encryption (PKE) in the KEM-DEM paradigm,

also in authentication contexts (encapsulating the session key).



Motivations

As before with Attribute-Based Encryption (ABE),

we can build a Key Encapsulation Mechanism (KEM),

to get Public-Key Encryption (PKE) in the KEM-DEM paradigm,

also in authentication contexts (encapsulating the session key).

Hybridization of KEMs

Basic KEM

Hybridization of KEMs

Basic KEM

Hybridization of KEMs

Basic KEM

Hybridization of KEMs

Hybridizing KEMs to get the best of both securities

on the encapsulated key privacy.

A 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.

This is part of discussions at ETSI,

and a recommendation from several security agencies.

Hybridization of KEMs

How?

You can make the key you want to transmit the XOR of two encapsulated keys.

A KEM with respect to user attributes

Could one use Attribute-Based Encryption (ABE)?

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

But maybe way more features than those we actually often need in practice,

and much more efficient solutions exist

using subset-cover paradigms.

when not all logical combinations of attributes are needed in real systems.

A KEM with respect to user attributes

An example

breathes in air and
water
aquatic and
amphibian

breathes in air
mammal

breathes in air
aquatic and a
mammal

A KEM with respect to user attributes

An example

breathes in **air and water**

aquatic and amphibiar

breathes in **air**

mammal

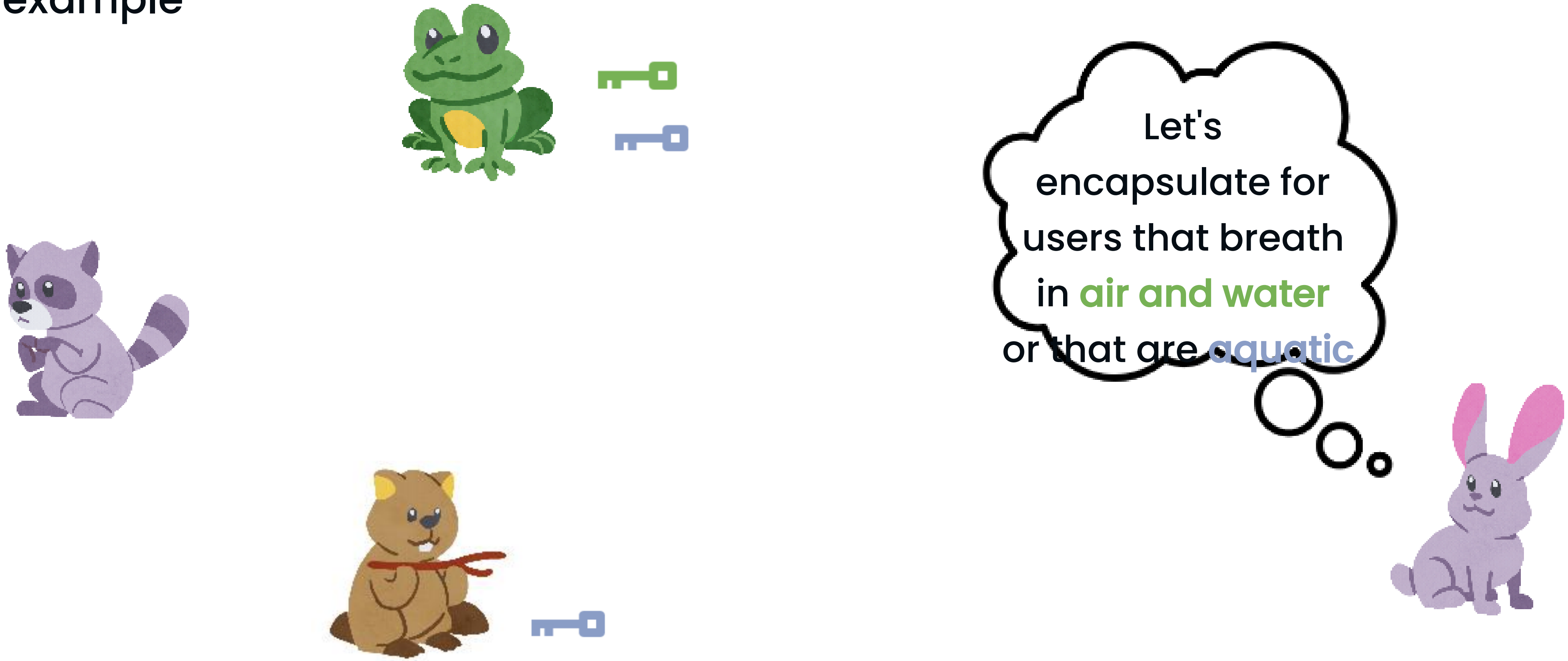
breathes in **air**

aquatic and a mammal

Let's encapsulate for users that breath in **air and water** or that are **aquatic**

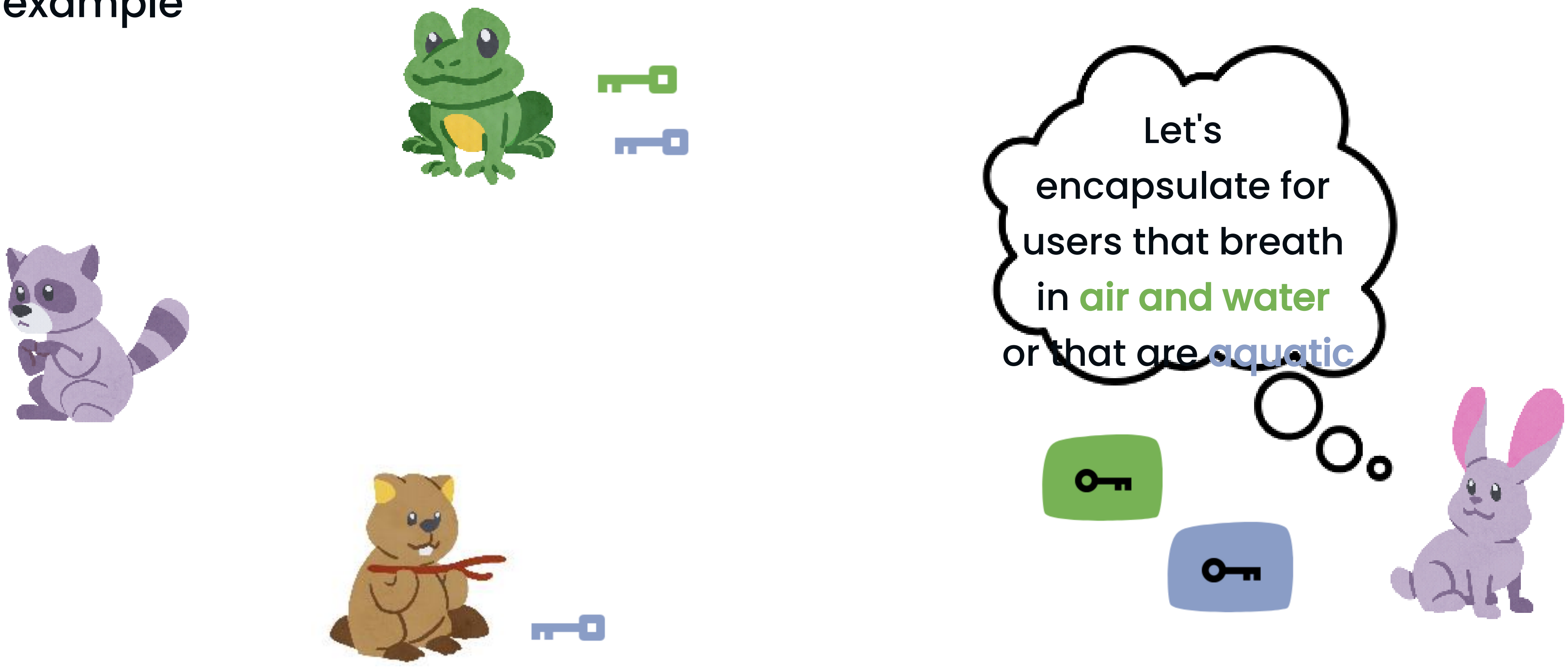
A KEM with respect to user attributes

An example


Let's encapsulate for users that breath in air and water or that are aquatic

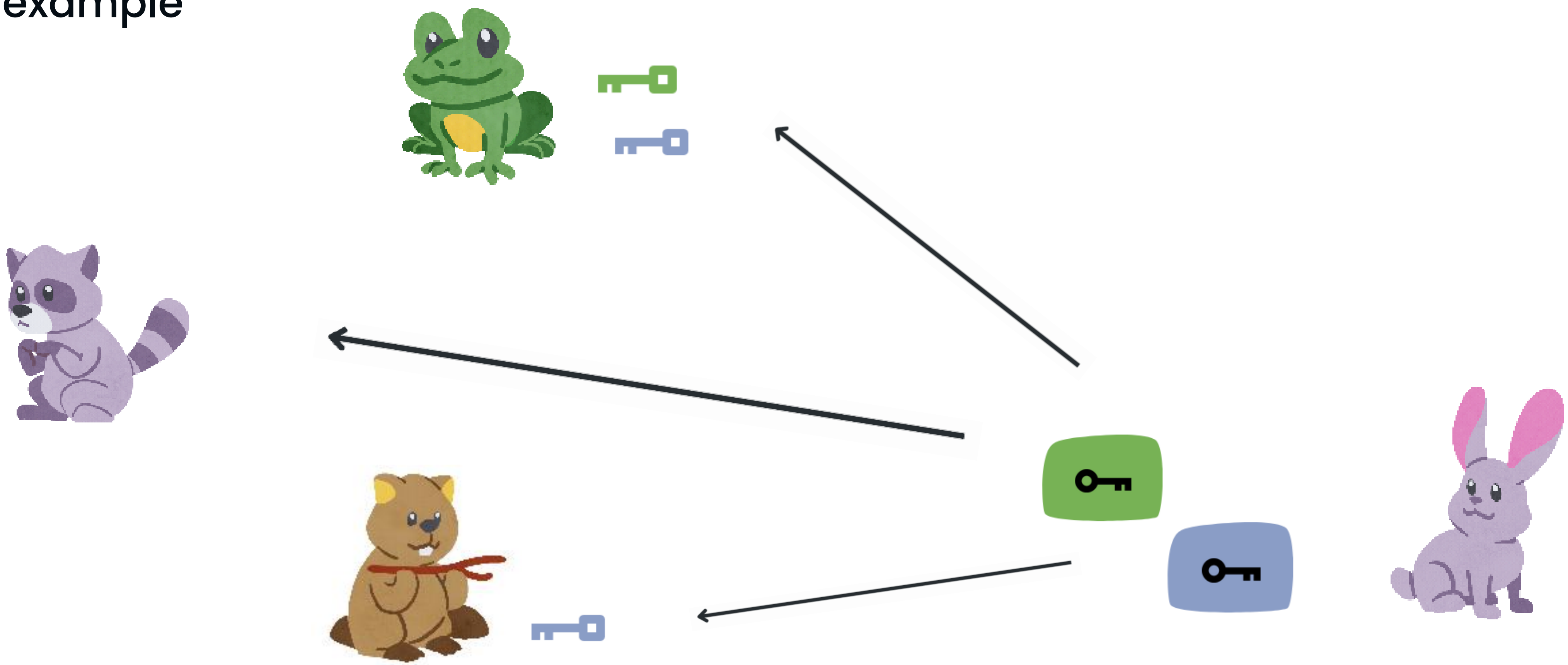
A KEM with respect to user attributes

An example


Let's encapsulate for users that breath in air and water or that are aquatic

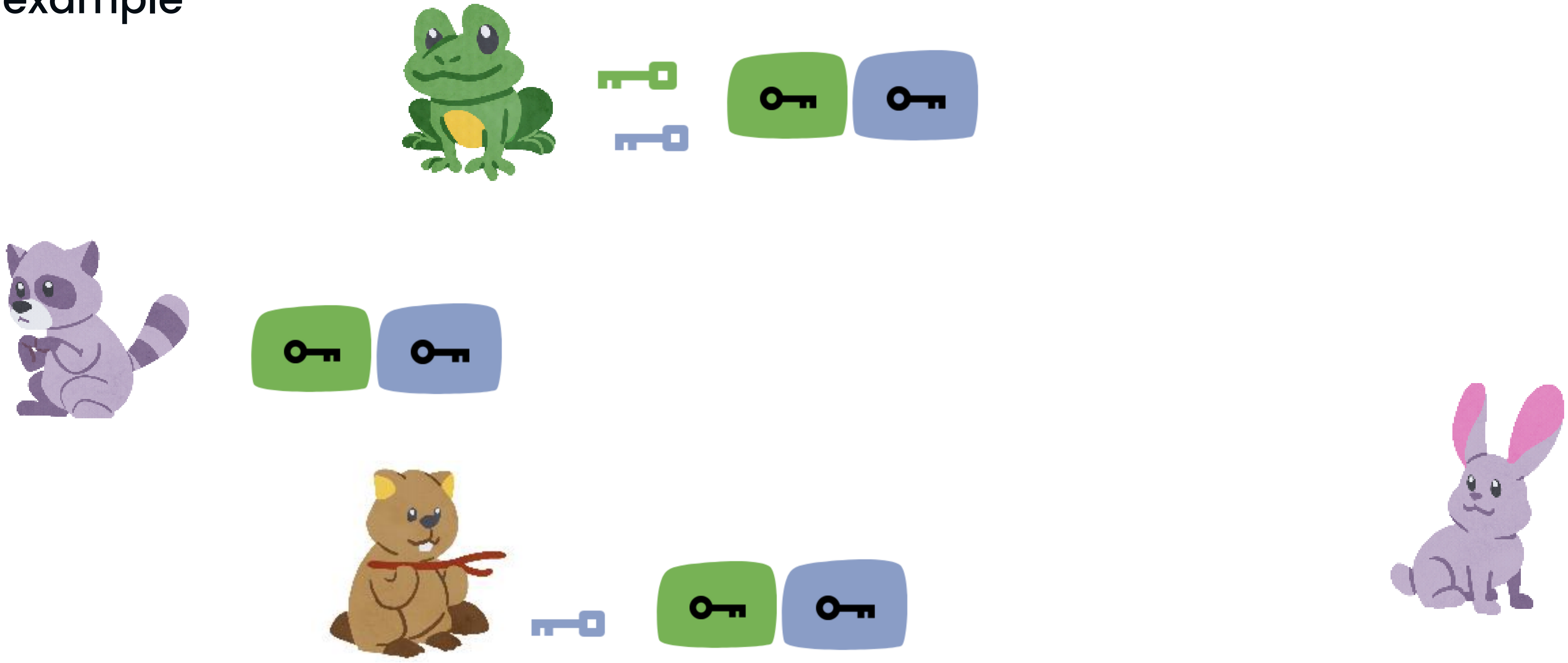
A KEM with respect to user attributes

An example



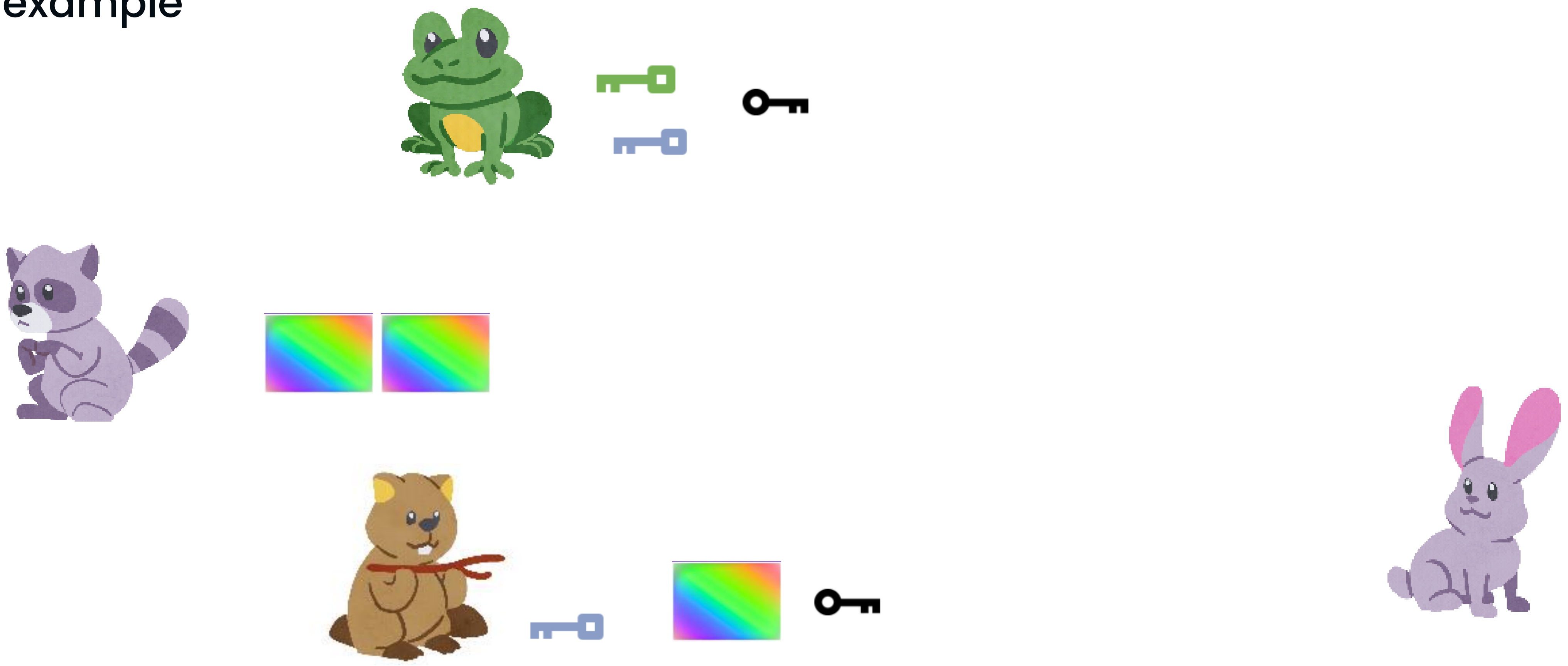
A KEM with respect to user attributes

An example



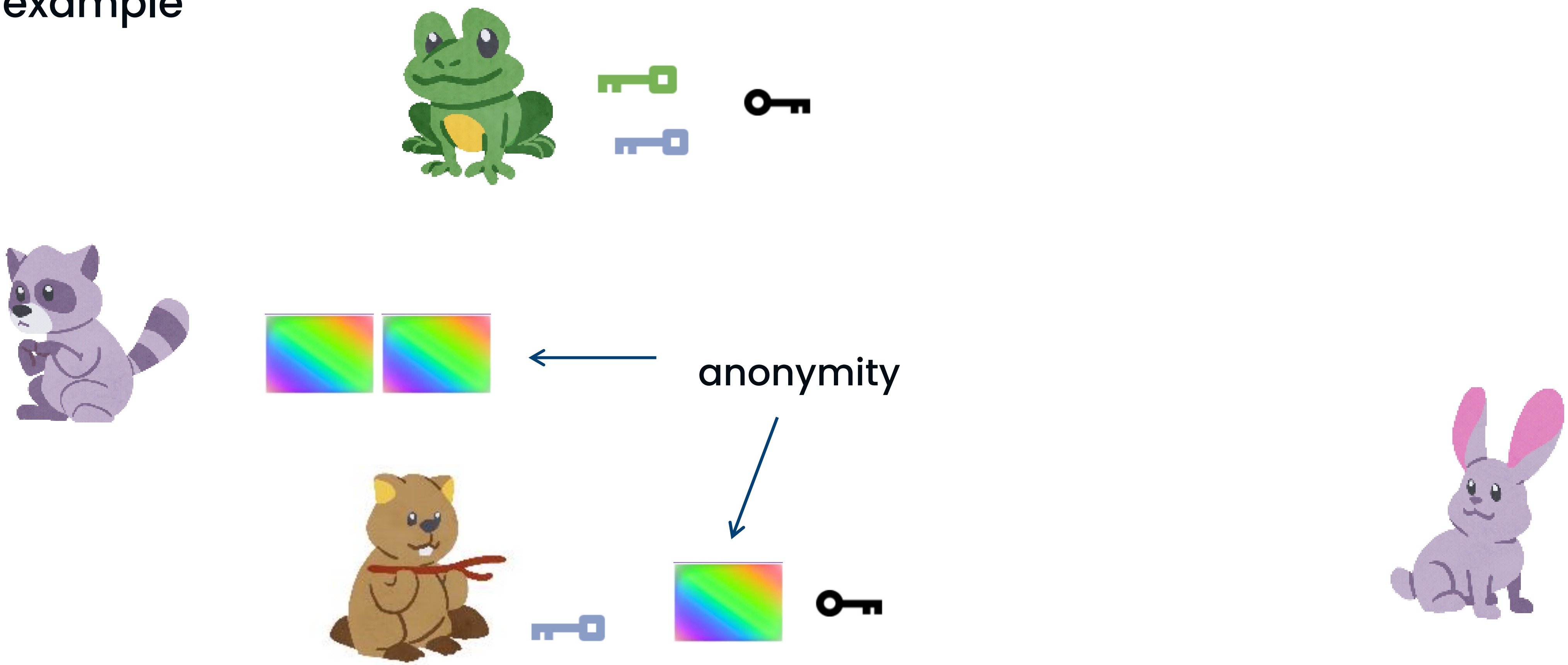
A KEM with respect to user attributes

An example



A KEM with respect to user attributes

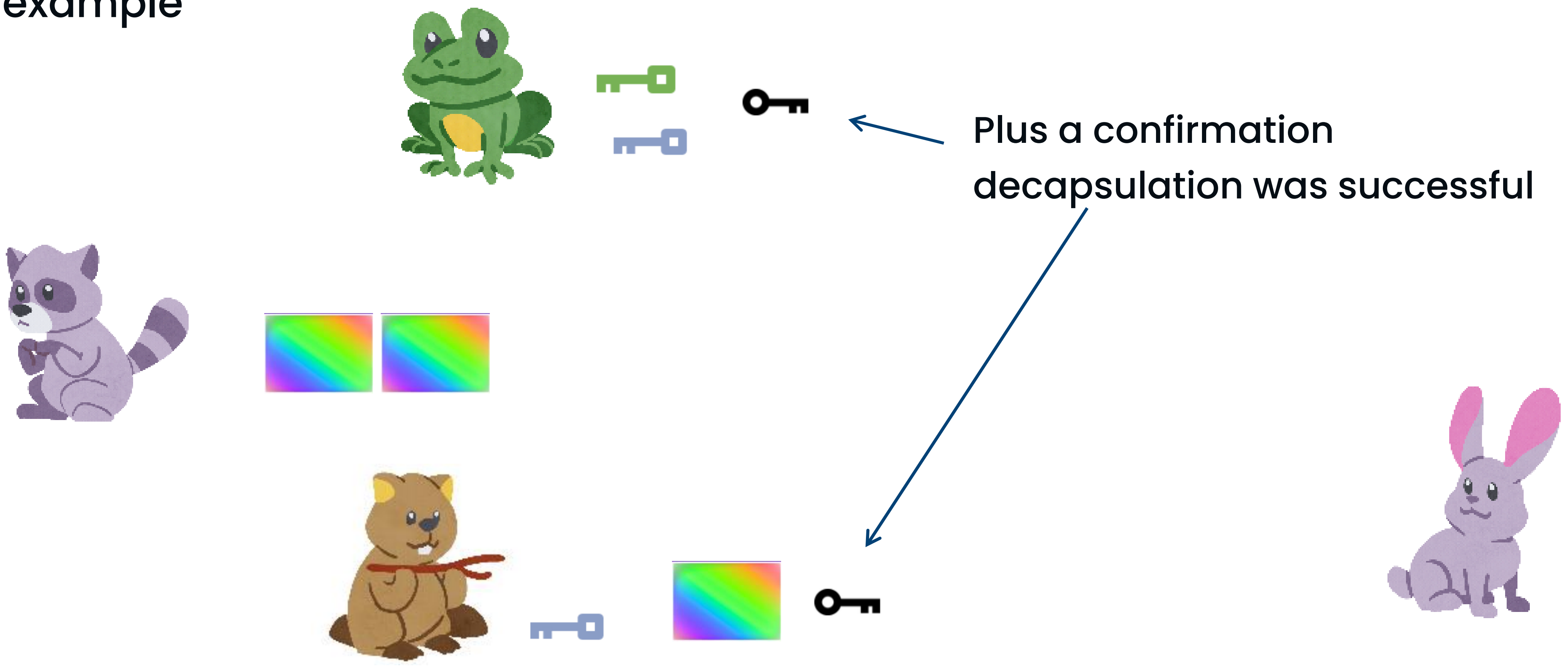
An example



anonymity

A KEM with respect to user attributes

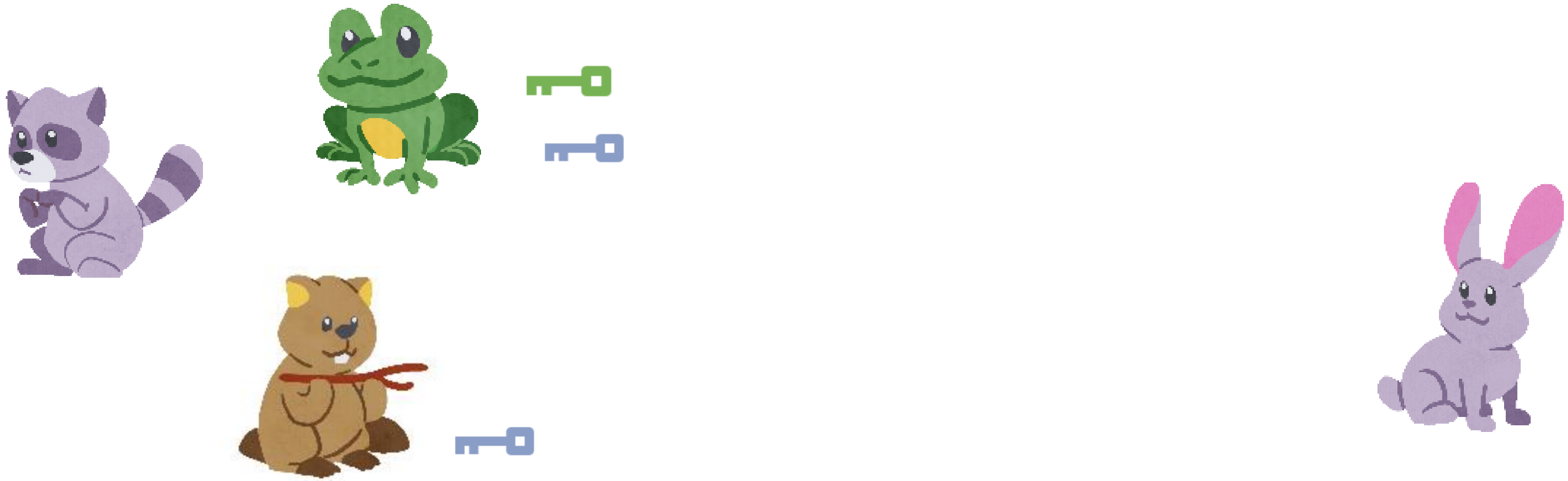
An example



Plus a confirmation decapsulation was successful

A KEM with respect to user attributes

Remark: some keys shared across users

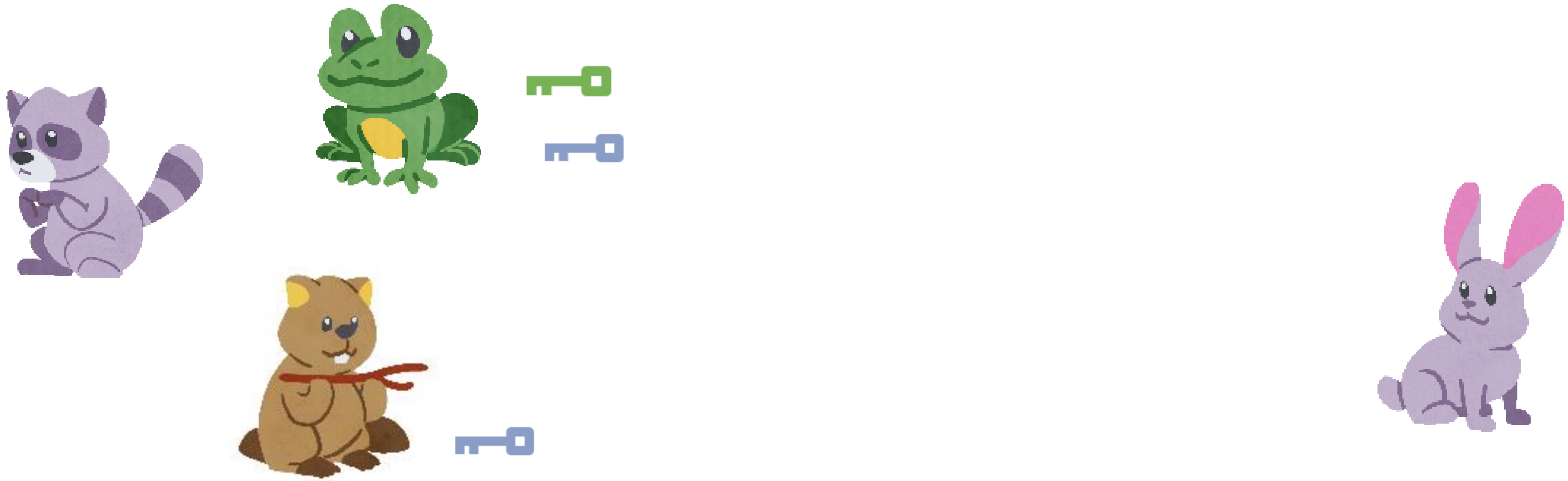


A KEM with respect to user attributes

Remark: some keys shared across users

—› scheme with additional user unique keys: better practice

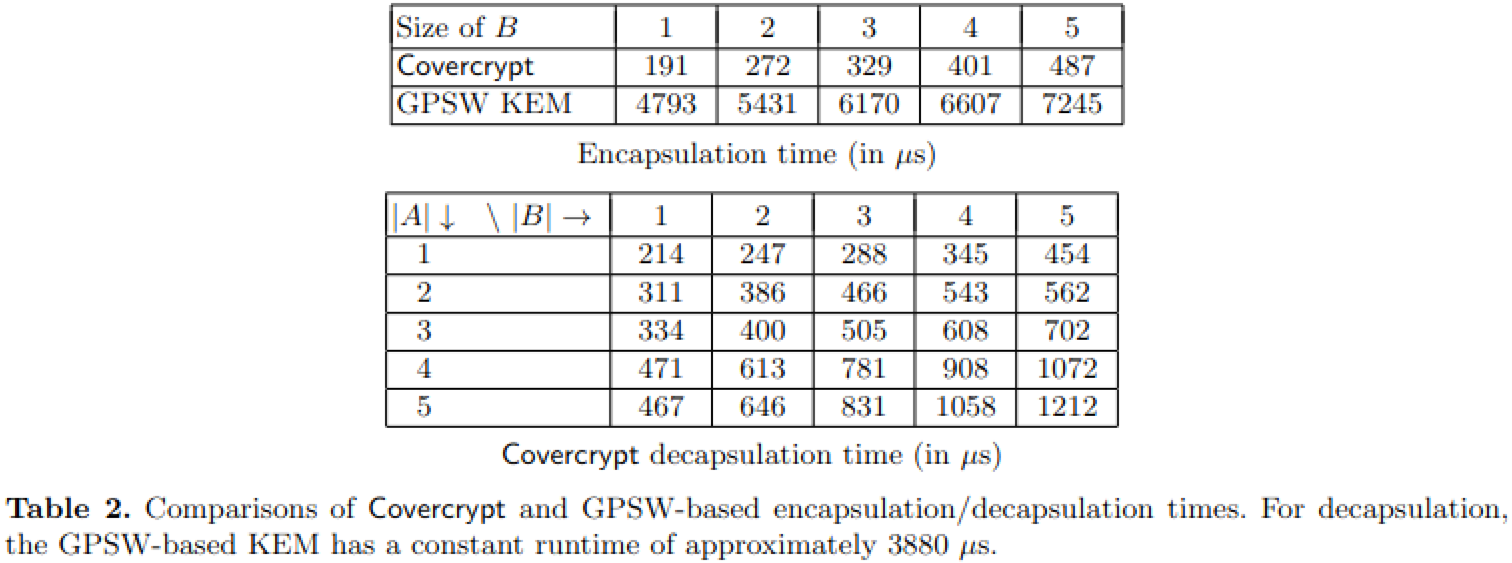
and can even be used for tracing



Performance

Comparison with a pre-quantum ABE-based KEM:

there is an order of magnitude speedup when the policies are simple



Size of B	1	2	3	4	5
Covercrypt	191	272	329	401	487
GPSW KEM	4793	5431	6170	6607	7245

Encapsulation time (in μs)

$\lvert A\rvert \downarrow \setminus \lvert B\rvert \rightarrow$	1	2	3	4	5
1	214	247	288	345	454
2	311	386	466	543	562
3	334	400	505	608	702
4	471	613	781	908	1072
5	467	646	831	1058	1212

Covercrypt decapsulation time (in μs)

Table 2. Comparisons of Covercrypt and GPSW-based encapsulation/decapsulation times. For decapsulation, the GPSW-based KEM has a constant runtime of approximately 3880 μs.

Efficient Quantum-Safe Hybrid Key Exchange Mechanisms (KEM) with Attribute Subset-Cover

New initiative,

not ABE but grants its desired properties in practice, very efficiently.

https://eprint.iacr.org/2023/836

By Théophile Brézot [1], **Paola de Perthuis** [1,2] & David Pointcheval [2]

1: cosmian

2: ENS ÉCOLE NORMALE SUPÉRIEURE

Work continues at ETSI TC CYBER and QSC…

Call for contributions

- Cryptographic level: new schemas (including PQC)
- Application level: new use cases
- Interoperability with existing standards
- Involvement of SDOs