popets-2024-0115
eprint/2023/1070

KU LEUVEN

FACULTY OF ENGINEERING SCIENCE

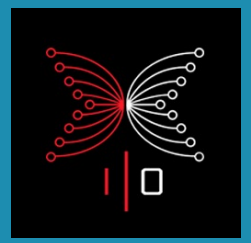
COSIC

# Unlinkable Policy-Compliant Signatures for Compliant and Decentralized Anonymous Payments

Christian Badertscher
Input Output

**Mahdi Sedaghat**
COSIC, KU Leuven

Hendrik Waldner
Univ. of Maryland



KU LEUVEN


PETS'24, Bristol, UK – July 9th

# Digital Signatures: An Equivalence of Written Signature

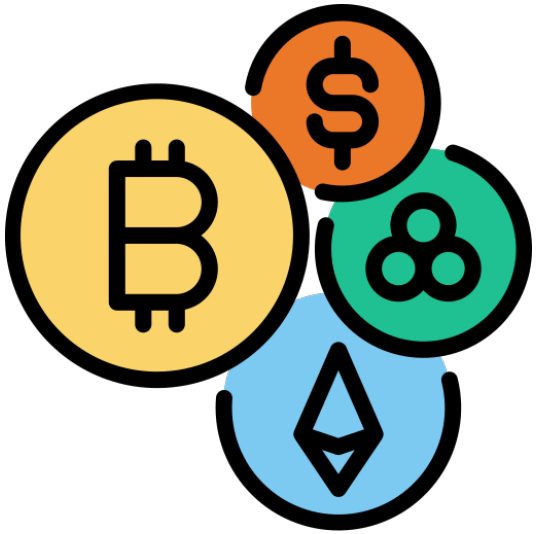

**Authentication**

**Integrity**

**Non-Repudiation**

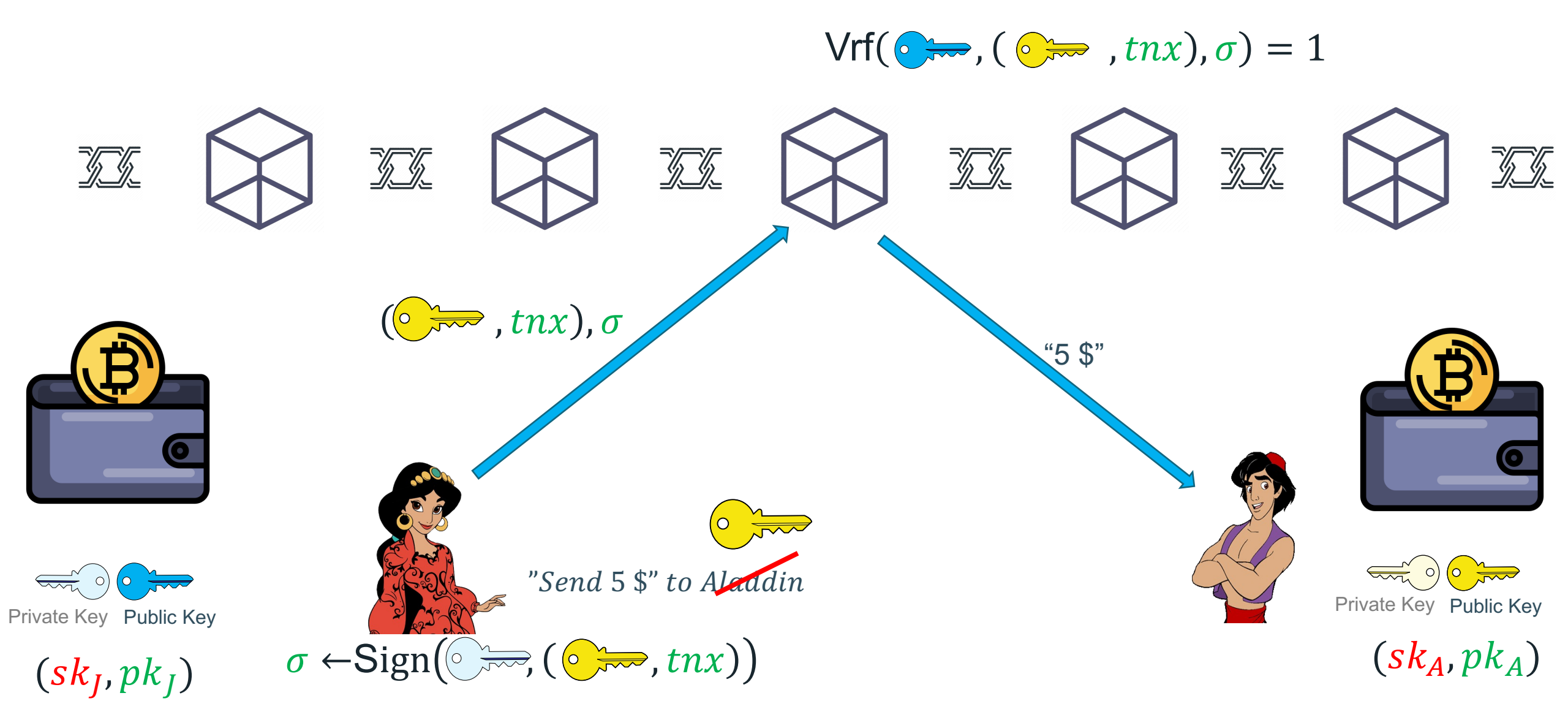
The main Goal: To bind a message to its author.

Digital Signatures are everywhere on the internet.

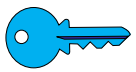


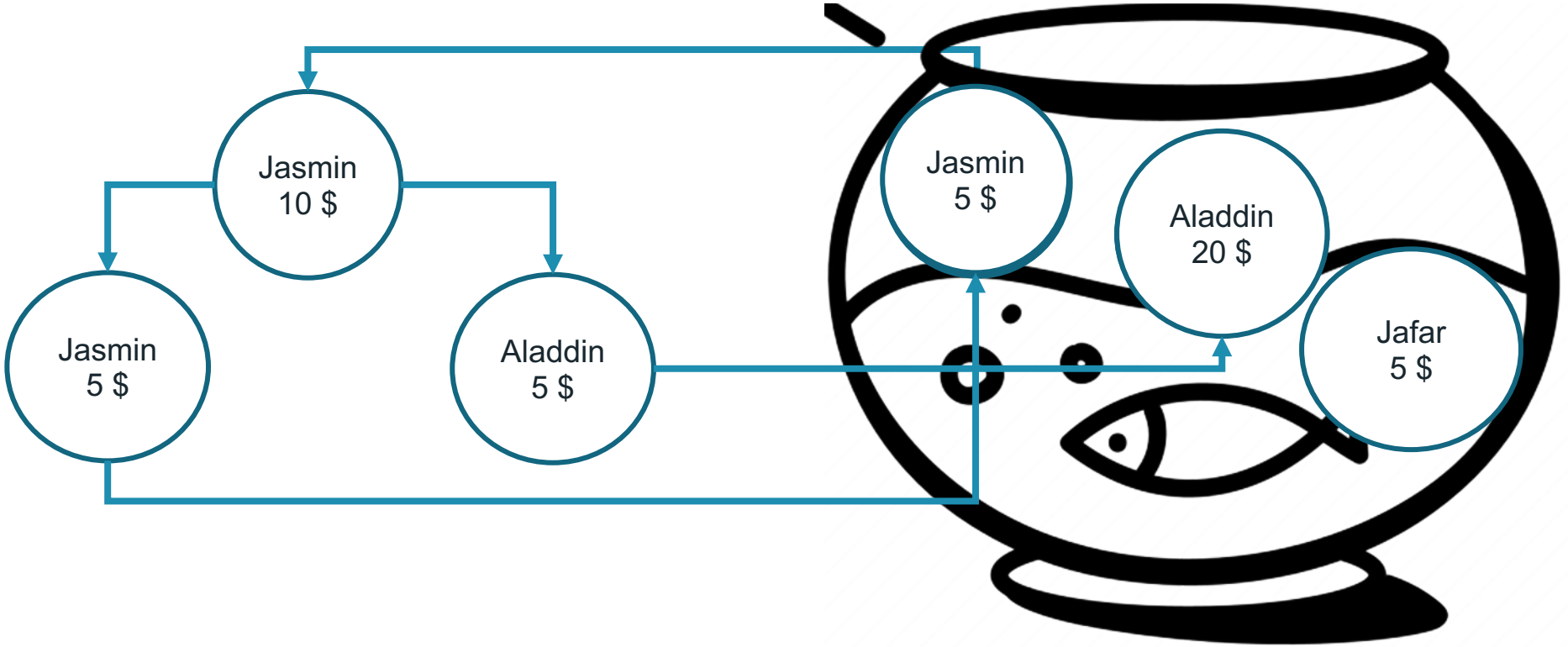
Especial focus on financial transactions.

# **Motivation:** UTxO-based cryptocurrencies



# **Motivation:** UTxO-based cryptocurrencies

Vrf(  , (  , $tnx$), $\sigma$) = 1



# Pseudonymity ≠ Anonymity

The PID of the **payee** and **payer** and the **value** in Bitcoin are publicly available!!

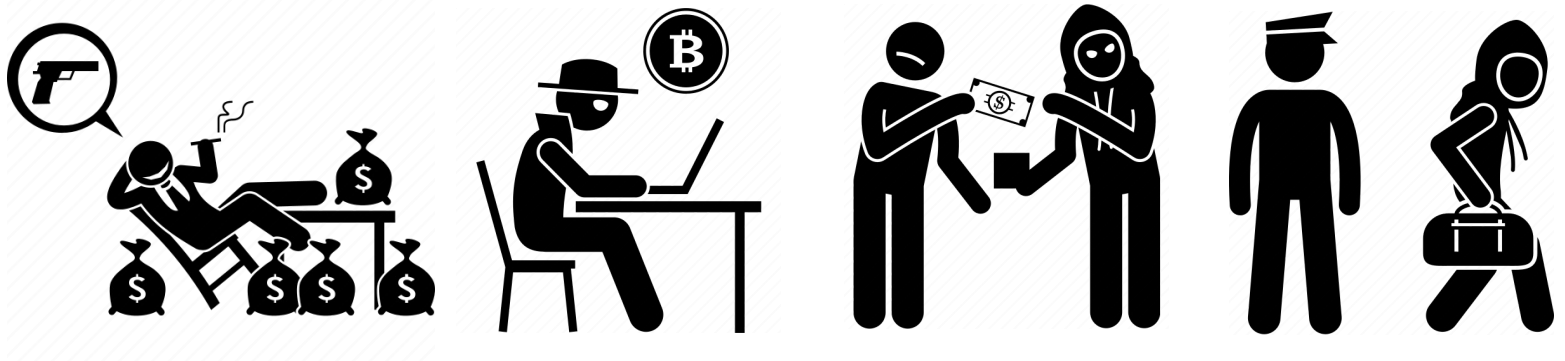
If your employer pays employee in Bitcoin?! All salaries are visible

Distributed anonymous payments (DAP).

The identity and the values are hidden.

Such cryptocurrencies can be used in an illegal context

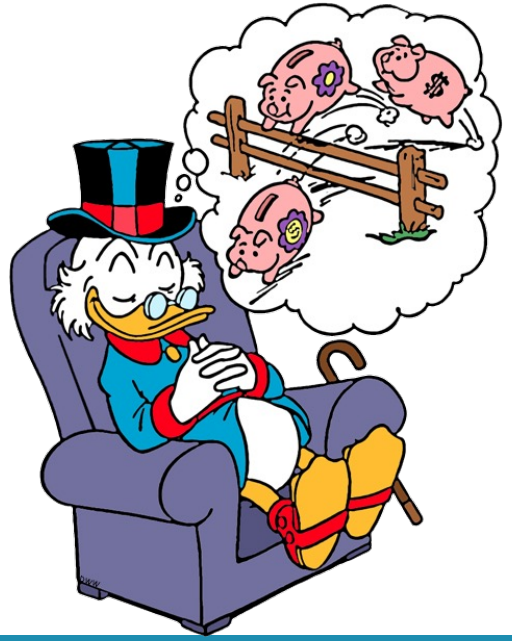
- Tax evasion
- Ransomware
- Drug trafficking
- Terrorist funding
- etc.

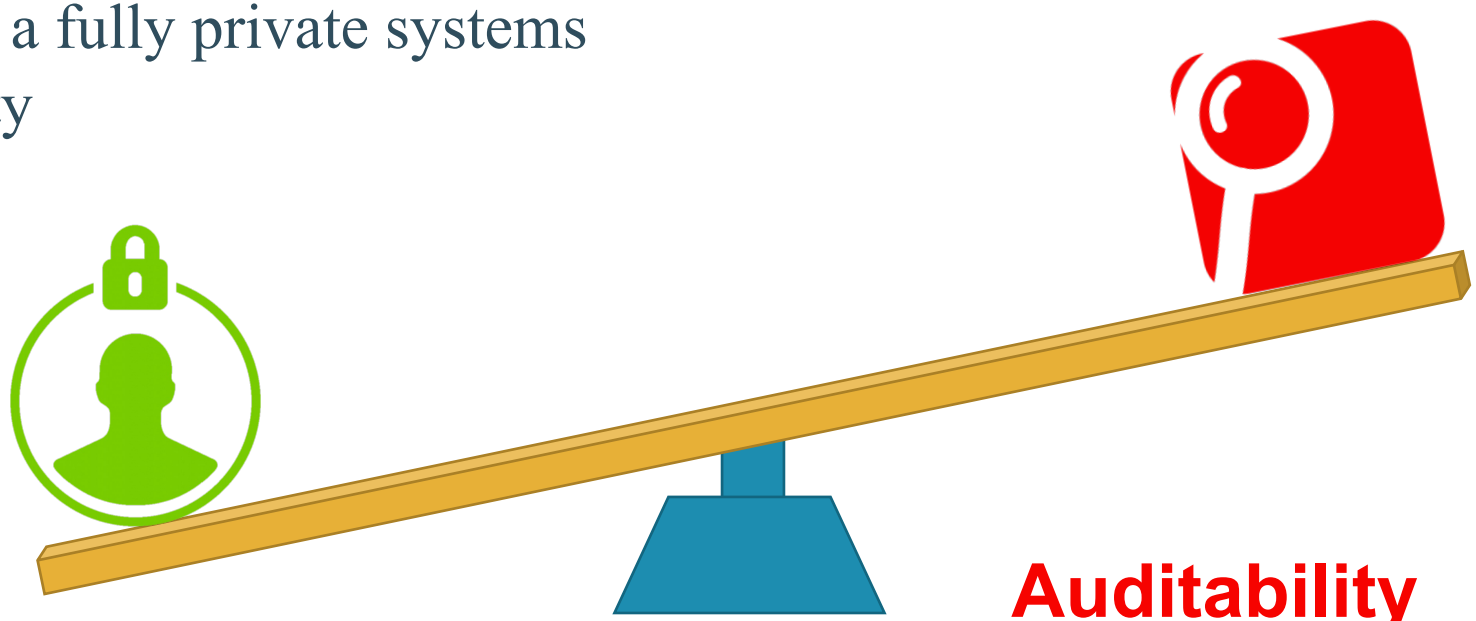


# Privacy vs. Accountability: In theory

## Privacy

- Users willing a fully private systems
- No traceability
- Unlinkability






## Auditability

- To prevent possible illicit activities
- To trace the suspicious actions

# Some Existing Solutions: Accountable Privacy

1. Public Key Encryption:

2. Threshold Encryption:

1- Prevention is better than cure!

2- How an auditor can be suspicious to a fully anonymous tnx?!

# Prevention vs. Detection:


**We are interested on:**
**Joint policy**

# Possible solution for UTxO-based systems:

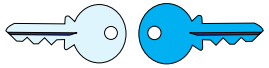
Policy

$((\text{key}, tnx), \sigma$

1 $\text{Vrf}(\text{key}, (\text{key}, tnx), \sigma) = 1$

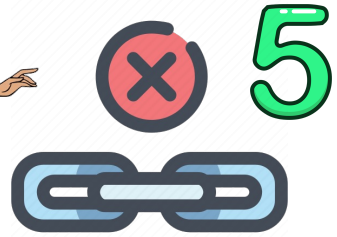
2 3 If $\text{Policy}(x_J, x_A) = 1$

4

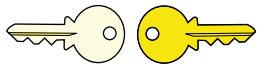


Private Key Public Key

$(sk_J, pk_J, x_J)$



5



Private Key Public Key

$(sk_A, pk_A, x_A)$

# Some Possible Solutions: Related Cryptographic Primitives

| | 1<br>Unforgeability | 2<br>P/A-based | 3<br>Joint policy | 4<br>S/R privacy | 5<br>Unlinkability |
|---|---|---|---|---|---|
| **Digital Signatures** | + | − | ⊘ | ⊘ | ⊘ |
| **Attribute-based Signatures** | + | + | − | ⊘ | ⊘ |
| **Policy-based Signatures** | + | + | + | − | ⊘ |
| **Policy-Compliant Signatures** | + | + | + | + | − |

# Unlinkable Policy-Compliant Signatures:

It improves PCS [BMW21] from TCC'21.

Setup

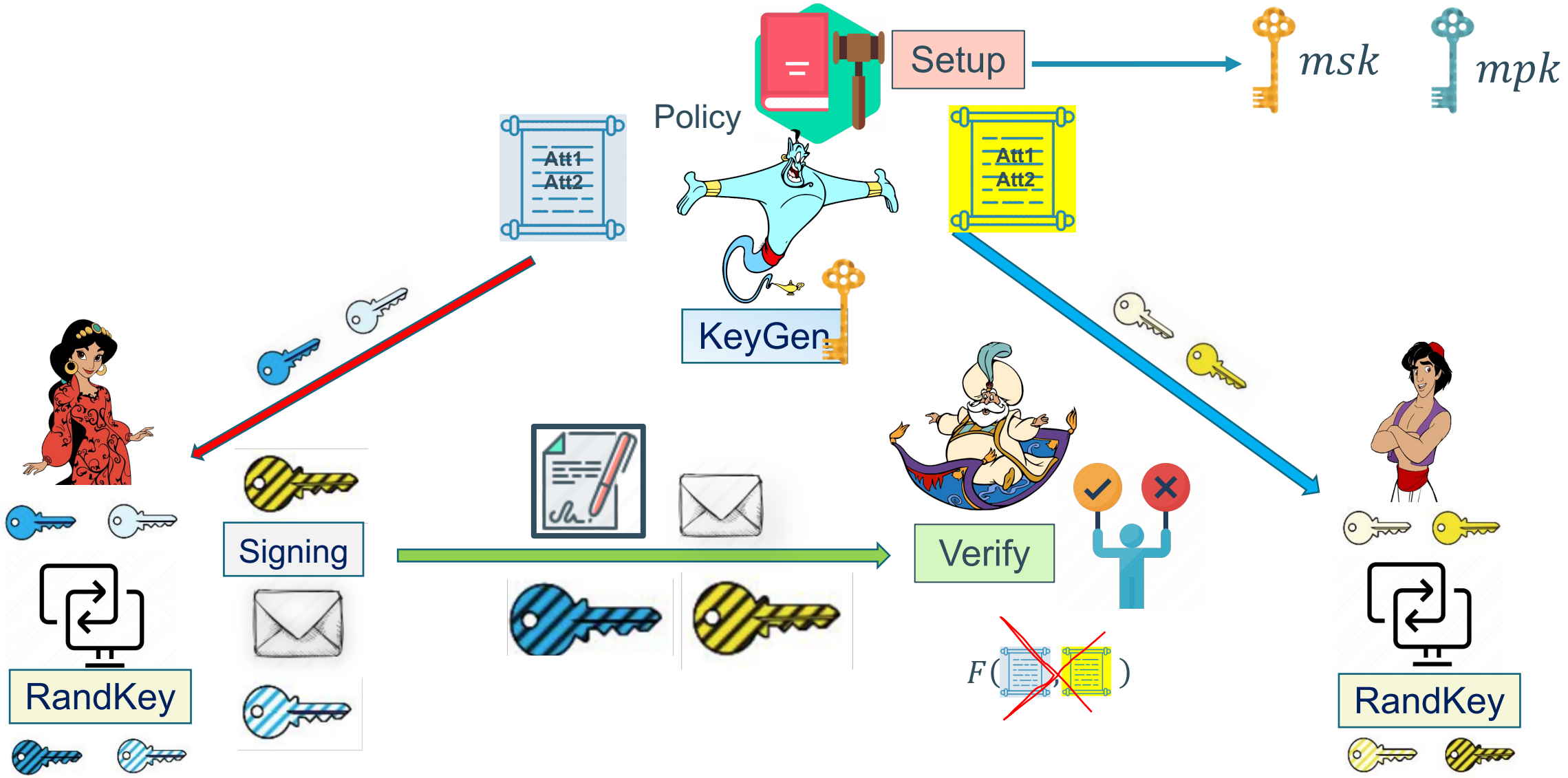
KeyGen

RandKey

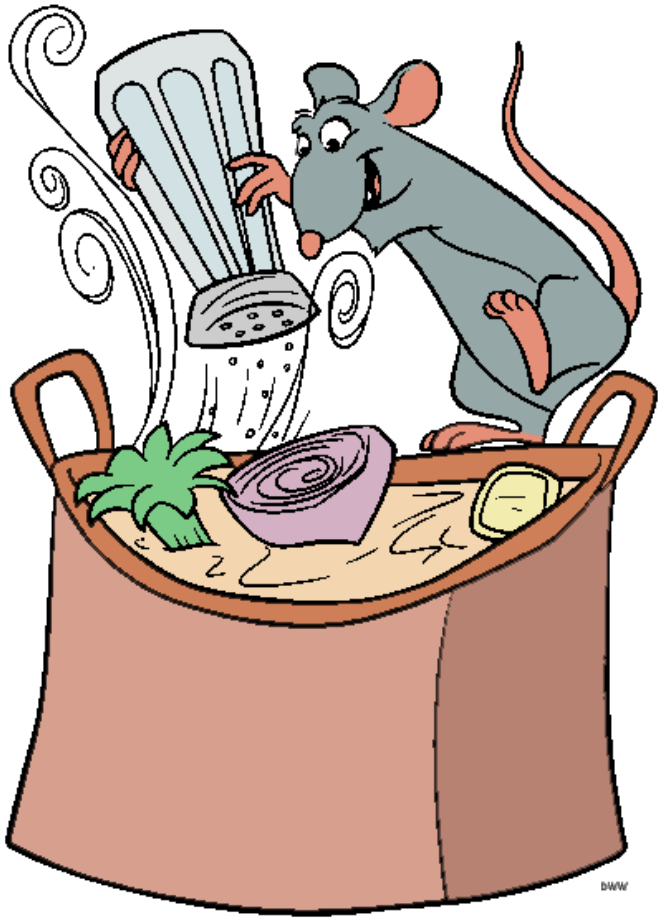
Signing

Verify

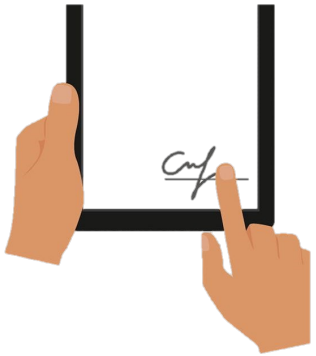
# Unlinkable Policy-Compliant Signatures:



# Main Ingredients:



Digital Signatures



Predicate-Only
Predicate Encryptions

Pseudo-Random Functions

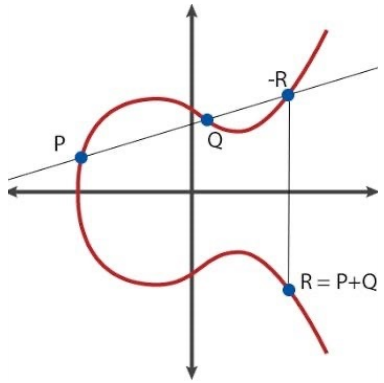
Zero-Knowledge proofs

# An Instantiation of Generic construction:

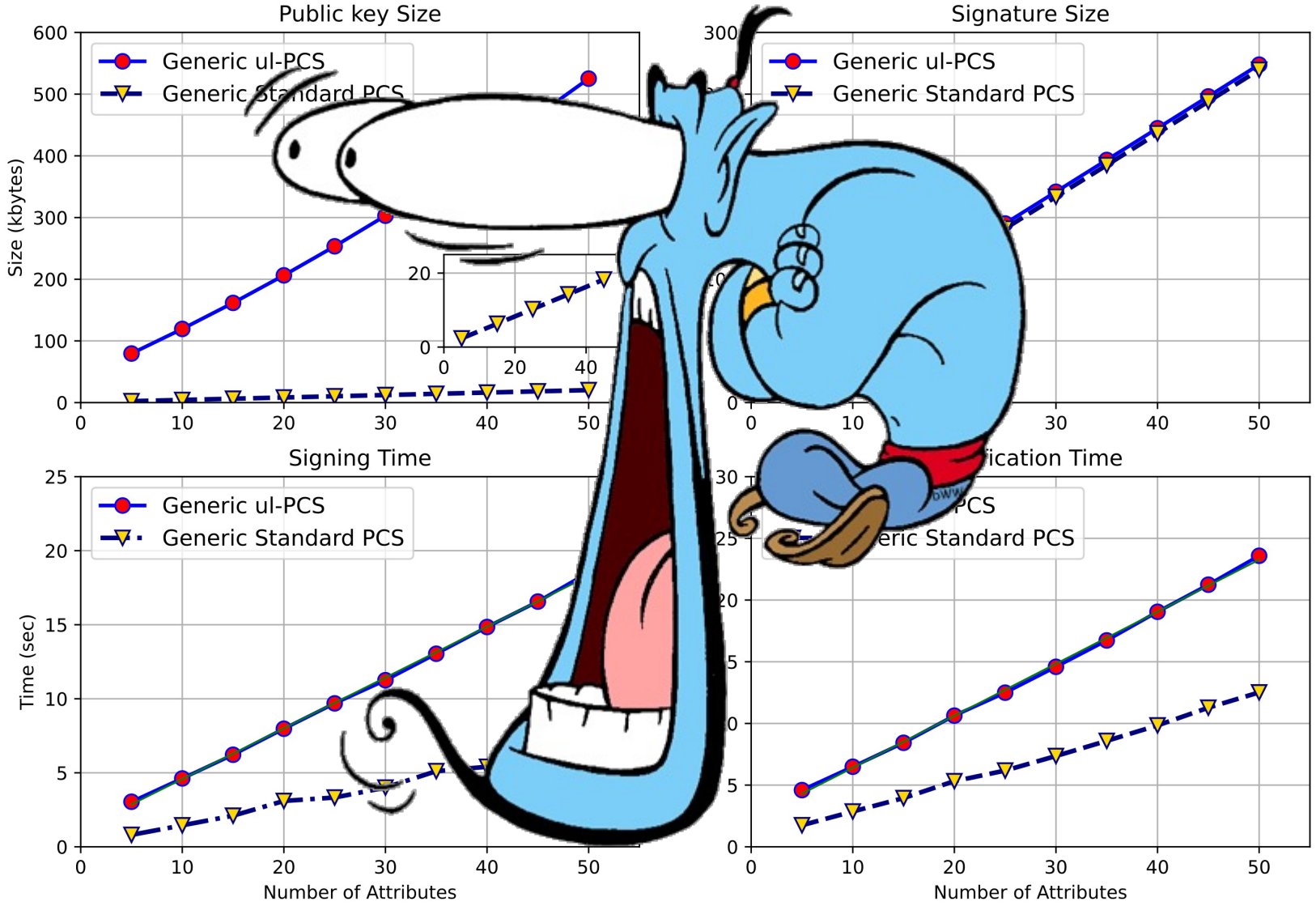
1. **Digital Signatures**
   - BLS signatures [BLS04] when message and signatures are public, else
     - Selectively Randomizable SPS and SPS-EQ in [FHS19]
     - Constant signature size (3 base group elements)
     - Groth-Sahai [GS08] proof system friendly
2. **Predicate-Only Predicate Encryptions**
   - Okamoto-Takashima [OT12]
     - Policy: Inner-products predicate functionalities
3. **Pseudo-Random functions**
   - Dodis-Yampolsky PRF [DY05]
4. **NIZK**
   - Sigma protocols [Sch89]: when the scalar is known
   - Groth-Sahai [GS08] proof systems: when all witnesses are group elements (batched version from ACM CCS'2017 [HHKRR17])
   - Bulletproof range-proofs [BBPWM18]

# Privacy is expensive?!

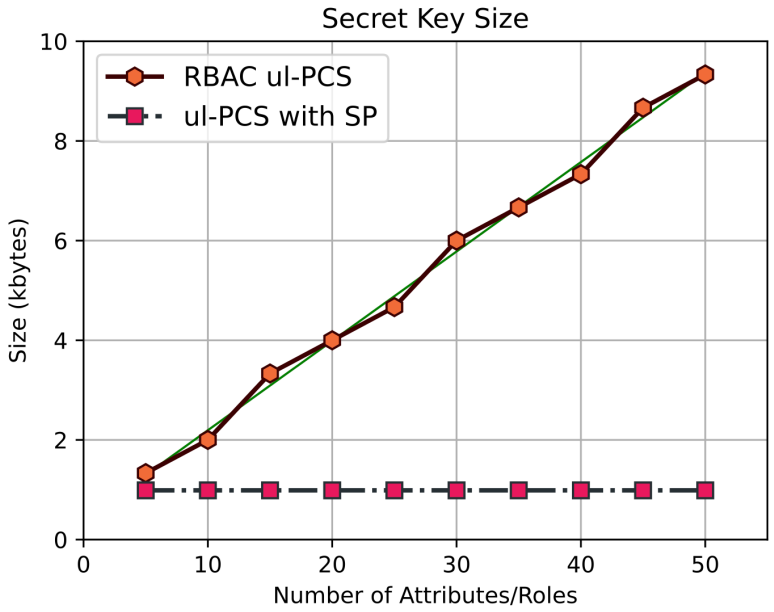
Ubuntu 20.04.2 LTS
an Intel Core i7-9850H CPU @ 2.60 GHz
with 16 GB of memory

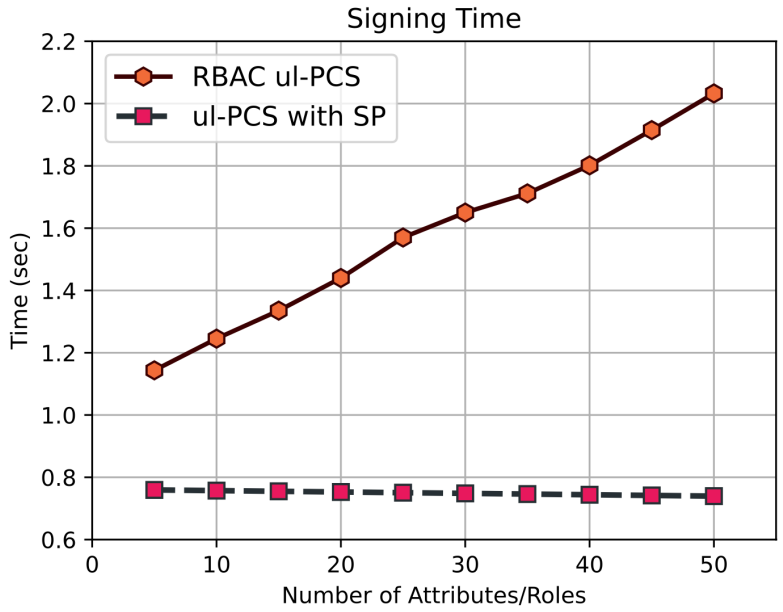



Charm-Crypto framework
BN254



# **Benchmarks:** Role-based and Separate Policies




| **Scheme** | KeyGen time (ms) | RandKey time (ms) | Verify time (ms) | pk size (kbytes) | $\sigma$ size (kbytes) |
|---|---|---|---|---|---|
| ul-PCS, role-based | 750 | 550 | 1 630 | 28 | 16 |
| ul-PCS, separable policies | 490 | 480 | 1 020 | 28 | 14.5 |

# Conclusion: What we didn't cover

popets-2024-0115
eprint/2023/1070

We formally define/prove 4 different security properties:

- Correctness
- Unforgeability
- Attribute-Hiding
- Unlinkablity

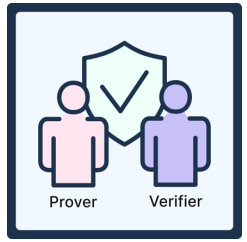
Details about more efficient alternatives:

- Role-based policies
- Separable policies

Detailed ZK instantiation for all proposed schemes.

Application to DAPs. Regulated One-Time Account.

- More applications.




# Potential Future Work:

- Minimize the needed trust to the central issuer.

- Design more efficient PO-PE → more efficient generic construction.

- Take a different approach with the same security properties. (Implement it using zk-SNARKs)

# References:


- [Schnorr89] Schnorr, Claus-Peter. "Efficient identification and signatures for smart cards." In Conference on the Theory and Application of Cryptology, pp. 239-252. Springer, New York, NY, 1990.
- [GMR89] Goldwasser, Shafi, Silvio Micali, and Chales Rackoff. "The knowledge complexity of interactive proof-systems." In *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*, pp. 203-225. 2019.
- [GS08] Jens Groth and Amit Sahai. Efficient non-interactive proof systems for bilinear groups. In Nigel P. Smart, editor, EUROCRYPT 2008, volume 4965 of LNCS, pages 415–432. Springer, Heidelberg, April 2008
- [Shamir79] A. Shamir. How to Share a Secret. In Commun. ACM 22(11), pp. 612–613, 1979.
- [OT12] Okamoto, T., Takashima, K.: Adaptively attribute-hiding (hierarchical) inner product encryption. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 591–608. Springer, Heidelberg (Apr 2012).
- [BMW21] Badertscher, C., Matt, C., Waldner, H.: Policy-compliant signatures. In: Nissim, K., Waters, B. (eds.) TCC 2021, Part III. LNCS, vol. 13044, pp. 350–381. Springer, Heidelberg (Nov 2021).
- [BBPWM18] B¨unz, B., Bootle, J., Boneh, D., Poelstra, A., Wuille, P., Maxwell, G.: Bulletproofs: Short proofs for confidential transactions and more. In: 2018 IEEE Symposium on Security and Privacy. pp. 315–334
- [DY05] Dodis, Y., Yampolskiy, A.: A verifiable random function with short proofs and keys. In: Vaudenay, S. (ed.) PKC 2005. LNCS, vol. 3386, pp. 416–431. Springer, Heidelberg (Jan 2005).
- [EKKV22] Engelmann, F., Kerber, T., Kohlweiss, M., Volkhov, M.: Zswap: zk-snark based non-interactive multi-asset swaps. Proc. Priv. Enhancing Technol. 2022(4), 507–527 (2022).
- [FHS19] Fuchsbauer, G., Hanser, C., Slamanig, D.: Structure-preserving signatures on equivalence classes and constant-size anonymous credentials. Journal of Cryptology 32(2), 498–546 (Apr 2019).
- [BLS04] Boneh, D., Lynn, B., Shacham, H.: Short signatures from the Weil pairing. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 514–532. Springer, Heidelberg (Dec 2001).

KU LEUVEN

# Thank You!

ssedagha@esat.kuleuven.be

The illustrations are credited to Disneyclips.