ISABELLA: Improving Structures of Attribute-Based Encryption Leveraging Linear Algebra

Doreen Riepel[1] **Marloes Venema**[2] Tanya Verma[3]

University of California San Diego, La Jolla, USA

University of Wuppertal, Wuppertal, Germany

Tinfoil, San Francisco, USA

ACM CCS 2024

BERGISCHE UNIVERSITÄT WUPPERTAL

Motivation and contribution

- Attribute-based encryption (ABE) offers secure access control on data
- Building secure schemes with advanced features for practice is difficult



Motivation and contribution

- Attribute-based encryption (ABE) offers secure access control on data
- Building secure schemes with advanced features for practice is difficult



- ISABELLA: a framework for pairing-based ABE
  - design of new schemes **with practical features**
  - **automated security analysis support**
  - intrinsic support for **highly adaptive** nature of advanced practical features



Motivation and contribution

- Attribute-based encryption (ABE) offers secure access control on data
- Building secure schemes with advanced features for practice is difficult



- ISABELLA: a framework for pairing-based ABE
  - design of new schemes **with practical features**
  - **automated security analysis support**
  - intrinsic support for **highly adaptive** nature of advanced practical features



Direct result: improved and new efficient schemes with advanced features



High-level overview

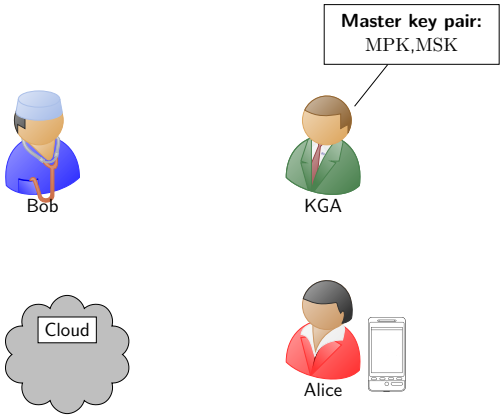
1. Introduction to ABE
2. Pairing-based ABE and pair encodings
3. ISABELLA
4. Wrapping up

High-level overview

1. Introduction to ABE
2. Pairing-based ABE and pair encodings
3. ISABELLA
4. Wrapping up

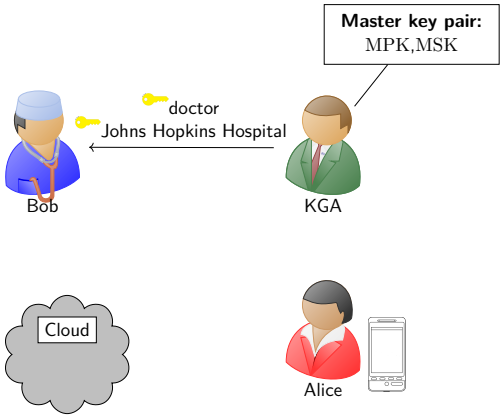
Example: Ciphertext-policy attribute-based encryption (CP-ABE)

Setup:



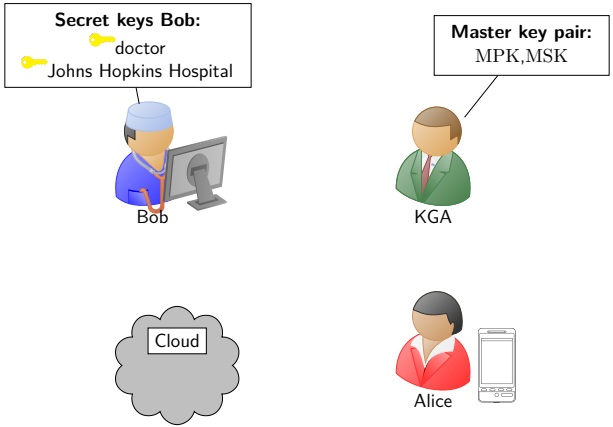
Example: Ciphertext-policy attribute-based encryption (CP-ABE)

Key generation:



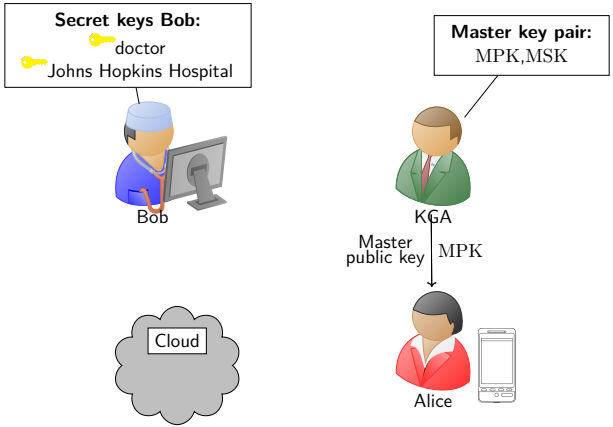
Example: Ciphertext-policy attribute-based encryption (CP-ABE)

Key generation:



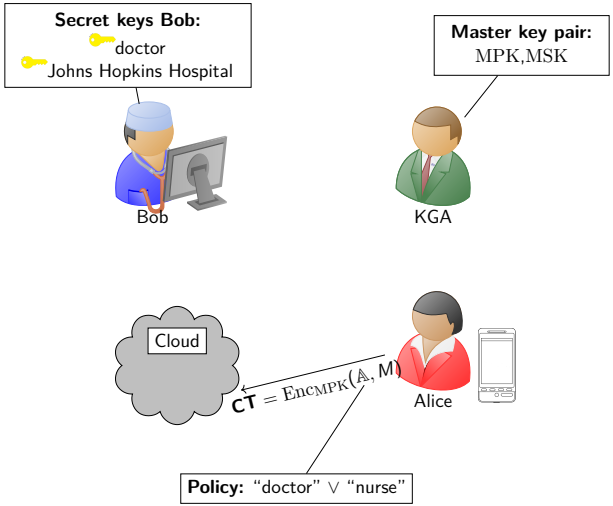
Example: Ciphertext-policy attribute-based encryption (CP-ABE)

Encryption:

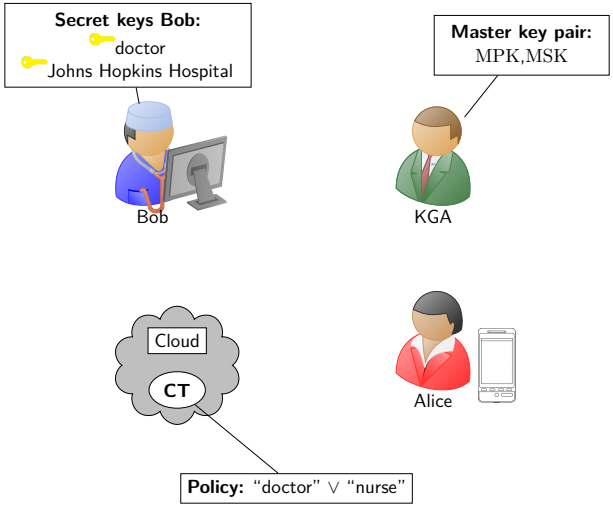


Example: Ciphertext-policy attribute-based encryption (CP-ABE)

Encryption:

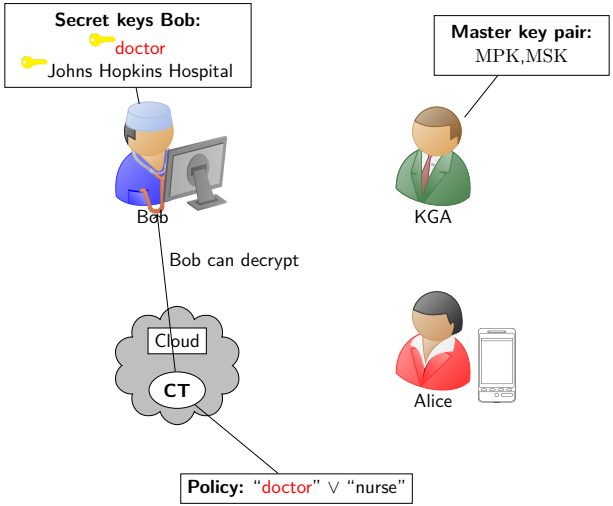


Example: Ciphertext-policy attribute-based encryption (CP-ABE)

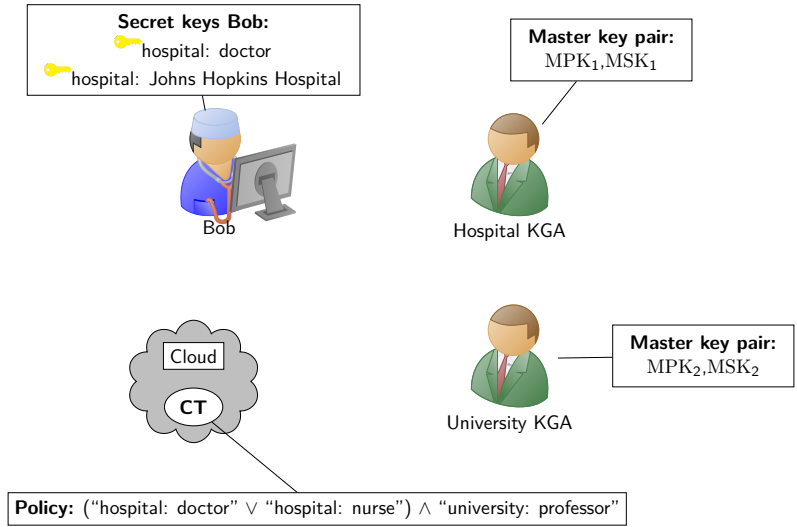


Example: Ciphertext-policy attribute-based encryption (CP-ABE)

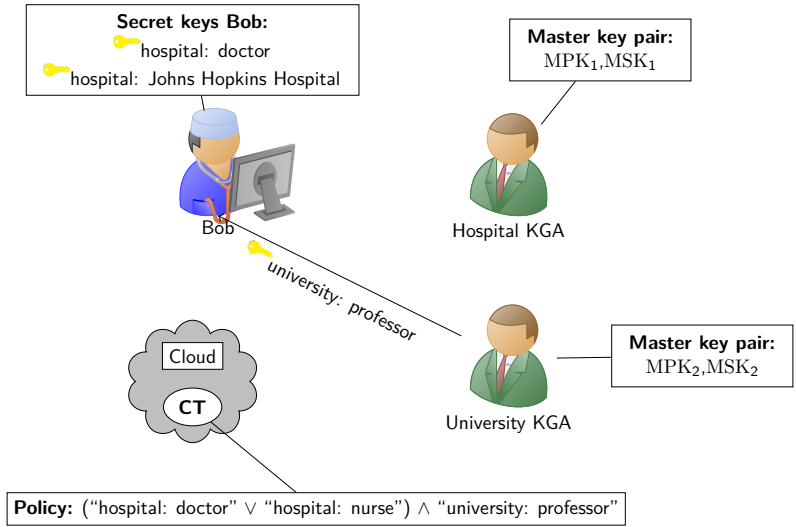
Decryption:



Multi-authority CP-ABE



Multi-authority CP-ABE



High-level overview

1 Introduction to ABE

2 Pairing-based ABE and pair encodings

3 ISABELLA

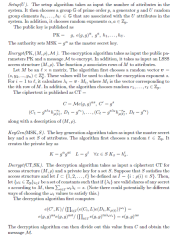
4 Wrapping up

Pairing-based ABE and pair encodings

- Pairing-based ABE is established: many desirable practical properties, high security guarantees, and efficiency

Pairing-based ABE and pair encodings

- Pairing-based ABE is established: many desirable practical properties, high security guarantees, and efficiency
- Pair encodings: **abstraction** of many practical ABE schemes [Att14, Wee14, AC17]

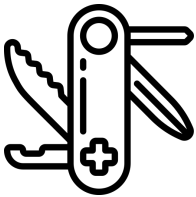


$$\Rightarrow$$

$$\mathbf{k}(\alpha, r, \mathbf{b}, \mathcal{S}) = (\alpha + rb, r, \{rb_i\}_{i\in\mathcal{S}})$$
$$\mathbf{c}(s, s'_i, \mathbf{b}, \mathbb{A}) = (s, \{\lambda_i b + s'_i b_i, s'_i\}_{i\in\mathbb{A}})$$

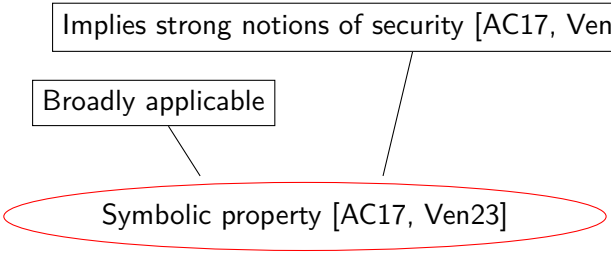
Pair encodings and the symbolic property

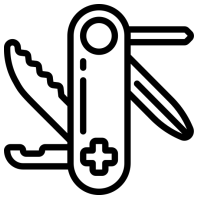
Symbolic property [AC17, Ven23]



The symbolic property is a powerful tool to simplify design of schemes.

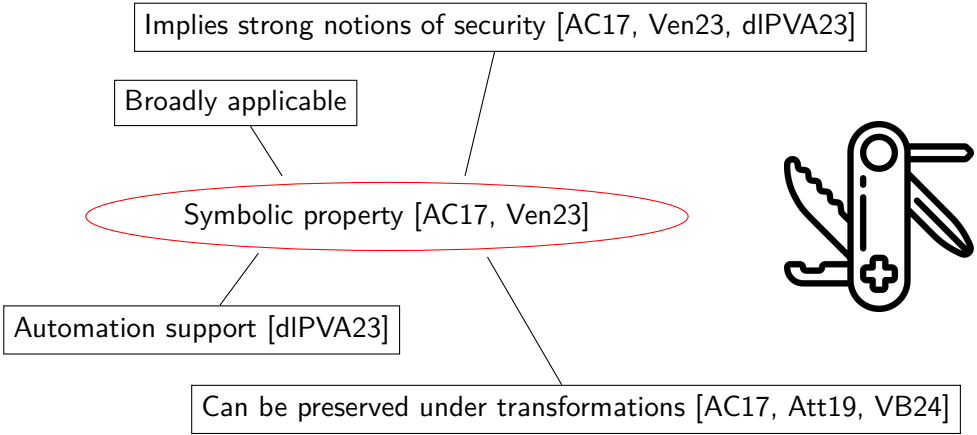
Pair encodings and the symbolic property





The symbolic property is a powerful tool to simplify design of schemes.

Pair encodings and the symbolic property



The symbolic property is a powerful tool to simplify design of schemes.

High-level overview

1 Introduction to ABE

2 Pairing-based ABE and pair encodings

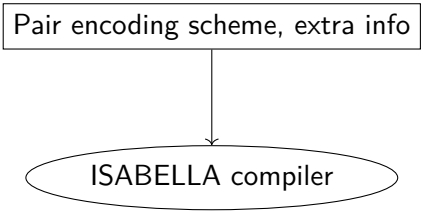
3 ISABELLA

4 Wrapping up

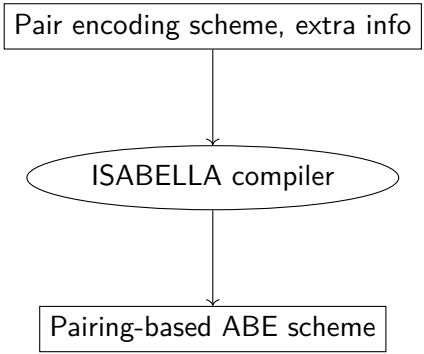
The ISABELLA compiler

Pair encoding scheme, extra info

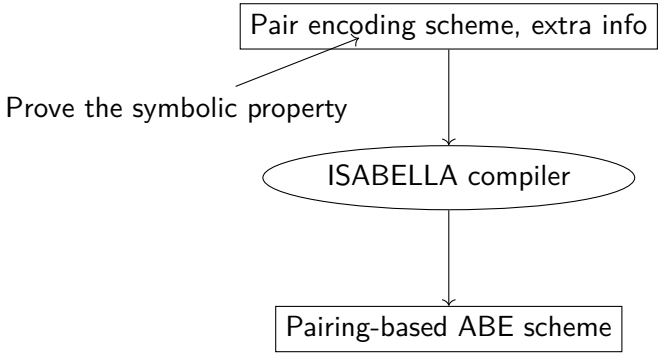
The ISABELLA compiler



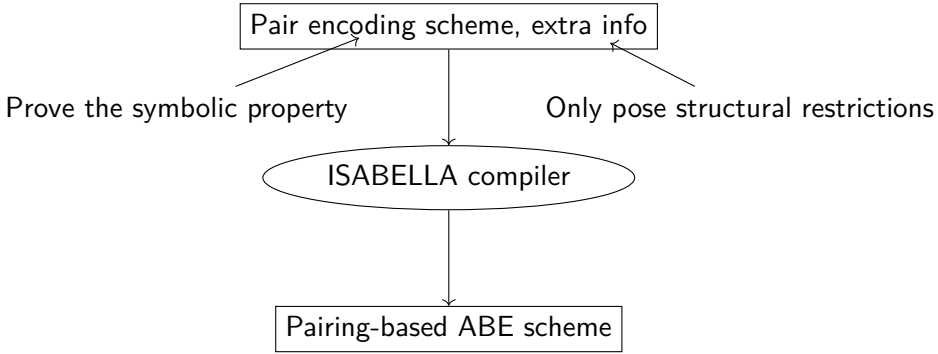
The ISABELLA compiler



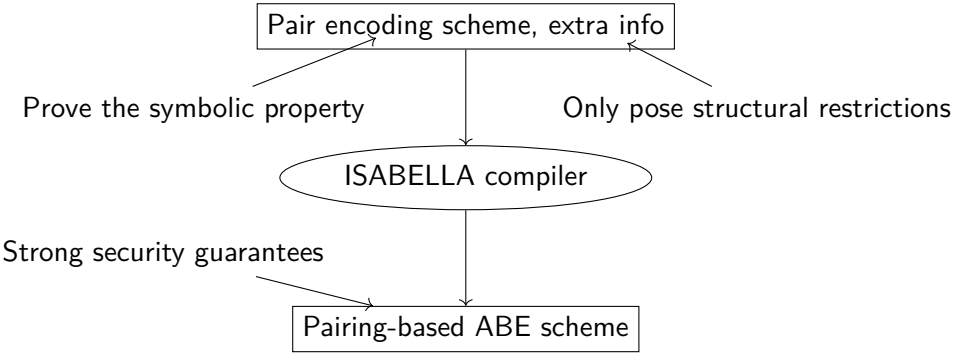
The ISABELLA compiler



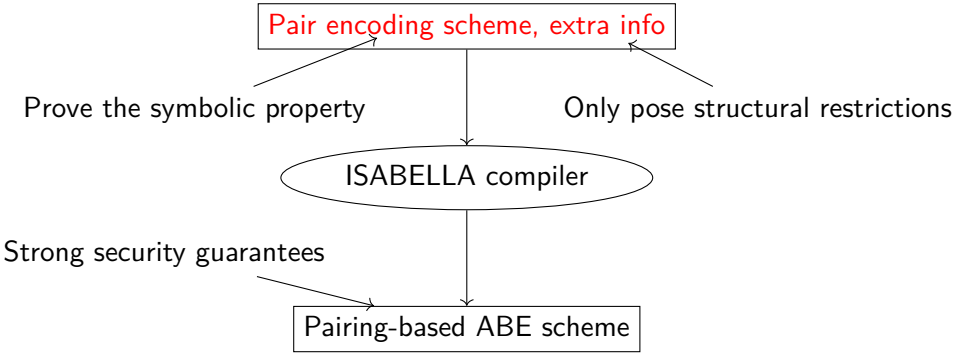
The ISABELLA compiler



The ISABELLA compiler



The ISABELLA compiler

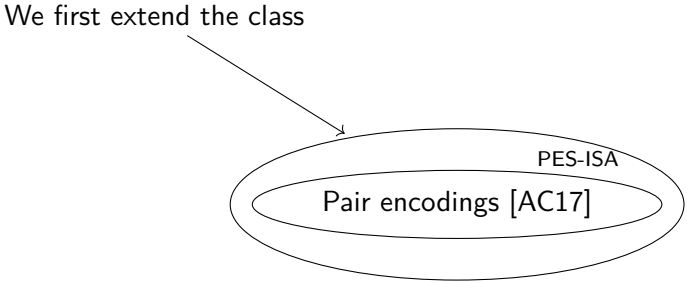


The improvements compared to other compilers are the most notable in the input

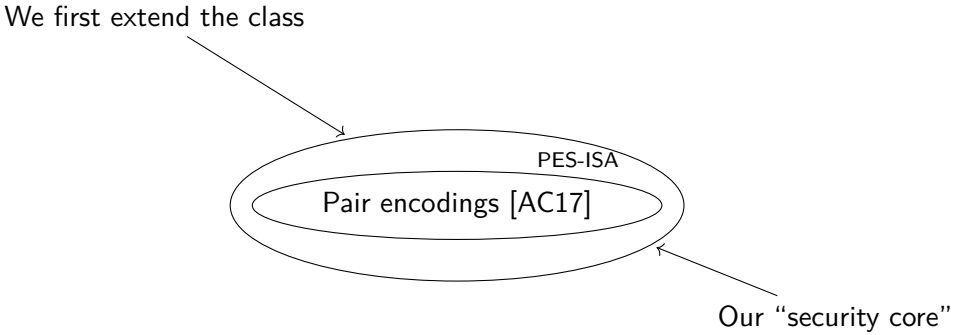
Overview of ISABELLA input



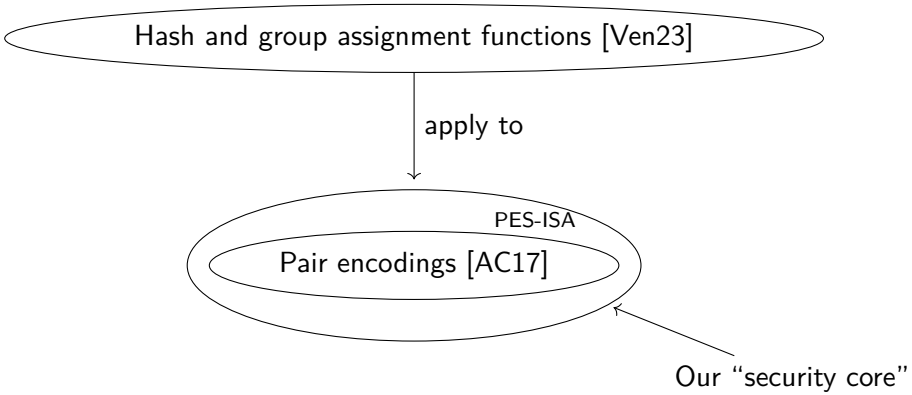
Overview of ISABELLA input



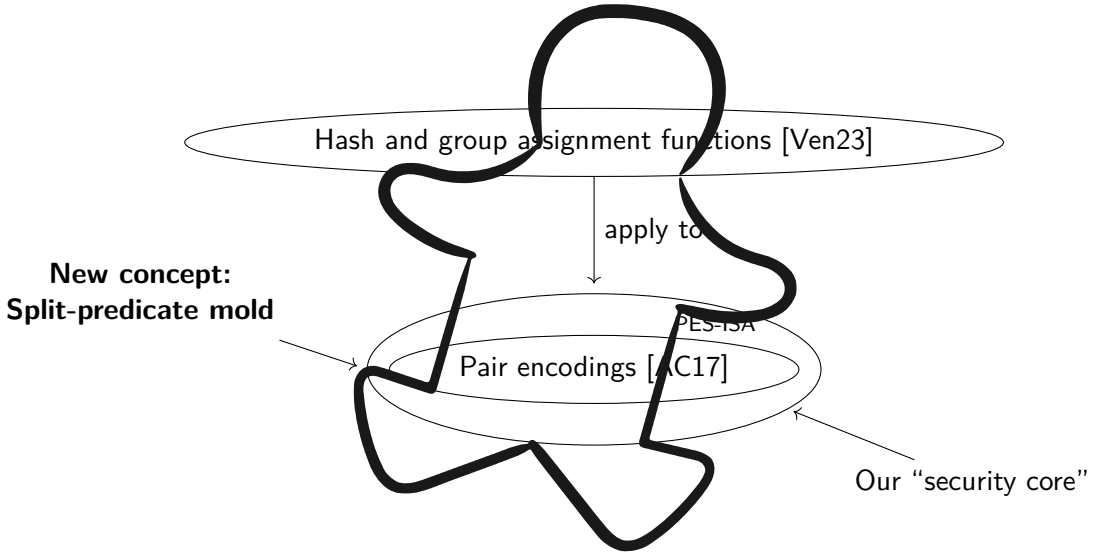
Overview of ISABELLA input



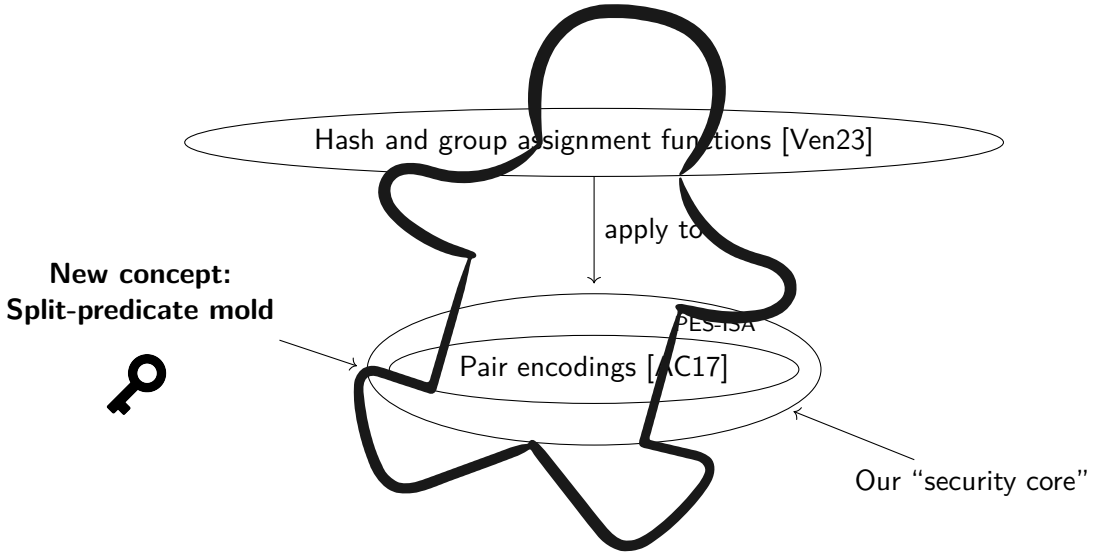
Overview of ISABELLA input



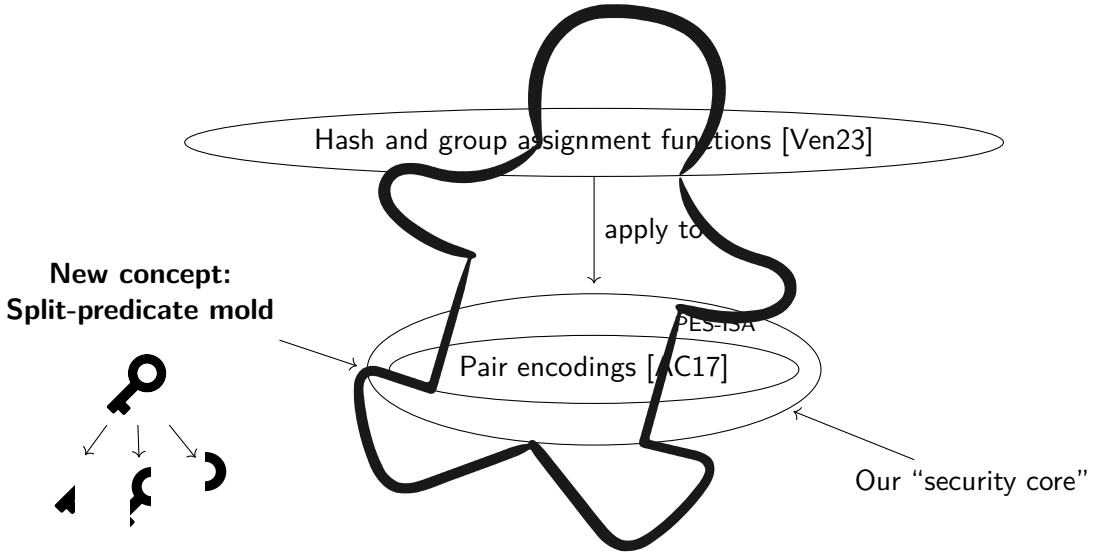
Overview of ISABELLA input



Overview of ISABELLA input



Overview of ISABELLA input



Split-predicate molds for functional adaptivity

- Functional adaptivity: adaptive nature of the key generation
- User can query key generation multiple times

Split-predicate molds for functional adaptivity

- Functional adaptivity: adaptive nature of the key generation
- User can query key generation multiple times
- Examples:



High-level overview

1. Introduction to ABE
2. Pairing-based ABE and pair encodings
3. ISABELLA
4. Wrapping up

Wrapping up

ISABELLA: a framework for pairing-based ABE

- design of new schemes **with practical features**
- **automated security analysis support**
- intrinsic support for **highly adaptive** nature of advanced practical features



Wrapping up

ISABELLA: a framework for pairing-based ABE

- design of new schemes **with practical features**
- **automated security analysis support**
- intrinsic support for **highly adaptive** nature of advanced practical features

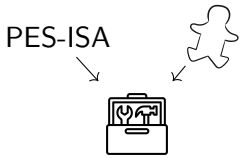
PES-ISA



Wrapping up

ISABELLA: a framework for pairing-based ABE

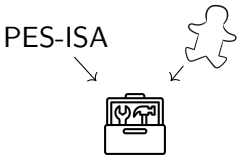
- design of new schemes **with practical features**
- **automated security analysis support**
- intrinsic support for **highly adaptive** nature of advanced practical features



Wrapping up

ISABELLA: a framework for pairing-based ABE

- design of new schemes **with practical features**
- **automated security analysis support**
- intrinsic support for **highly adaptive** nature of advanced practical features



Links:

- Our paper: `https://eprint.iacr.org/2024/1352`
- Our code: `https://github.com/lincolncryptools/ISABELLA`



References I

[AC17] S. Agrawal and M. Chase.
Simplifying design and analysis of complex predicate encryption schemes.
In J.-S. Coron and J. B. Nielsen, editors, *EUROCRYPT*, volume 10210 of *LNCS*, pages 627–656. Springer, 2017.

[Att14] N. Attrapadung.
Dual system encryption via doubly selective security: Framework, fully secure functional encryption for regular languages, and more.
In P. Q. Nguyen and E. Oswald, editors, *EUROCRYPT*, volume 8441 of *LNCS*, pages 557–577. Springer, 2014.

[Att19] N. Attrapadung.
Unbounded dynamic predicate compositions in attribute-based encryption.
In Y. Ishai and V. Rijmen, editors, *EUROCRYPT*, volume 11476 of *LNCS*, pages 34–67. Springer, 2019.

[dlPVA23] A. de la Piedra, M. Venema, and G. Alpár.
ACABELLA: automated (crypt)analysis of attribute-based encryption leveraging linear algebra.
To appear at CCS, 2023.

[VB24] M. Venema and L. Botros.
Using predicate extension for predicate encryption to generically obtain chosen-ciphertext security and signatures.
IACR Communications in Cryptology, 1(1), 2024.

[Ven23] M. Venema.
A practical compiler for attribute-based encryption: New decentralized constructions and more.
In M. Rosulek, editor, *CT-RSA*, volume 13871 of *LNCS*, pages 132–159. Springer, 2023.

[Wee14] H. Wee.
Dual system encryption via predicate encodings.
In Y. Lindell, editor, *TCC*, volume 8349 of *LNCS*, pages 616–637. Springer, 2014.

Some of the figures in these slides are from `flaticon.com`