Attribute-Based Encryption and its connection to Communication Disclosure of Secrets

ARPE Romain Gay – ENS Cachan

1st internship: advised by Eike Kiltz

2nd internship: advised by Luca Trevisan

Motivation

Attribute-based encryption(ABE)[SW'05] is a new paradigm for public-key encryption that enables fine-grained access control for encrypted data. In ABE, ciphertexts are associated with descriptive values x in addition to a plaintext, secret keys are associated with values y, and a secret key decrypts the ciphertext if and only if P(x,y) = 1 for some boolean predicate P . Here, y together with P may express an arbitrarily complex access policy, which is in stark contrast to traditional public-key encryption, where access is all or nothing.

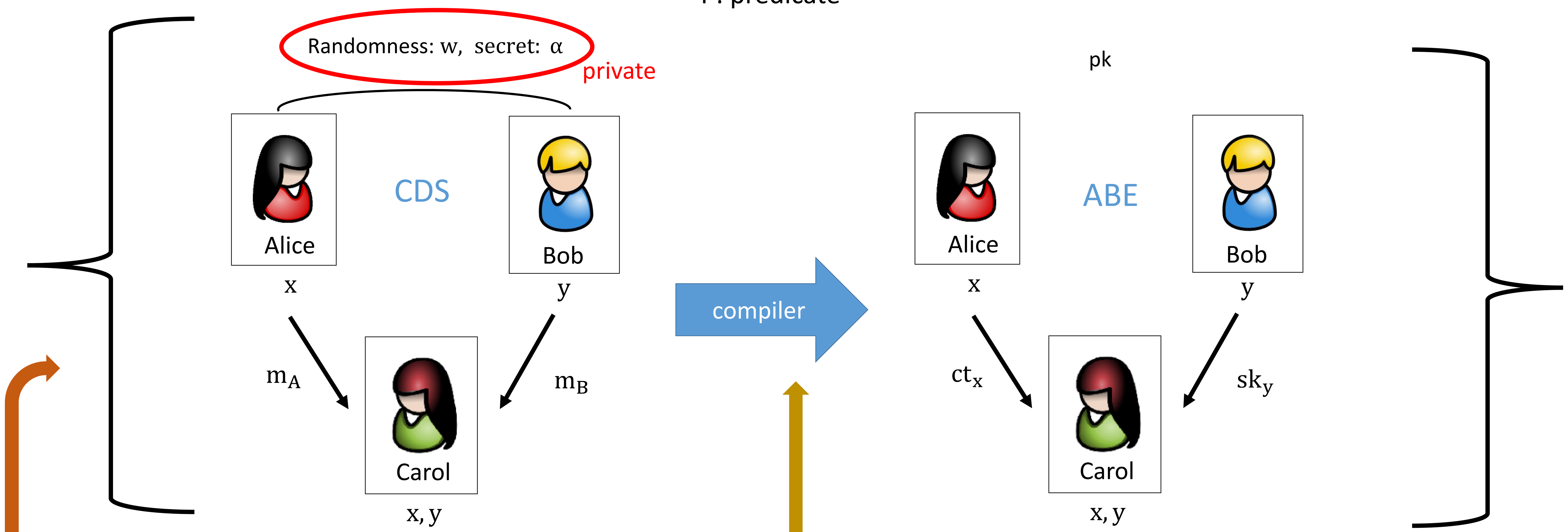
Open problems

1st internship: the compiler of [Wee'14] as well as ours relies on bilinear maps. It would be interesting to extend the scope of these compilers, for instance to the case of lattice-based ABE.

2n internship: the lower bounds are not tight for all sets of parameters. Also, in our work, we only focus on the case of a single bit secret. It is not known how to perform a CDS for a multi-bit secret, otherwise than doing a CDS for each bit of the secret independently.

P: predicate

- One-time secure
- Statistically secure
- Private key



- Many-time secure
- Computationally secure
- Public key

- **Correctness**: if P(x,y)=1, Carol recovers α
- **Privacy**: if P(x,y)=0, m_A, m_B statically hides α

- **Correctness**: if P(x,y)=1, sk_y decrypts ct_x
- **Security**: an adversary that requests adaptively keys $sk_{y_1}, sk_{y_2}, \ldots$ such that $P(x,y_i) = 0$ can't decrypt ct_x

2nd internship, results:

We initiate a systematic treatment of the communication complexity of conditional disclosure of secrets (CDS) [GIKM'00], where two parties want to disclose a secret to a third party if and only if their respective inputs satisfy some predicate. We present a general upper bound and the first non-trivial lower bounds on the size of m_A and m_B for conditional disclosure of secrets. This implies lower bounds for ABE.

1st internship, results:

We present a modular framework for the design of efficient adaptively secure attribute-based encryption (ABE) schemes for a large class of predicates under standard assumptions in prime-order groups, improving upon [Wee'14].
We compile a one-time, statistically secure, private-key primitive (CDS) into a many-time, computationally secure, public-key primitive (ABE).

References:
[SW'05]: A. Sahai and B. Waters, Fuzzy identity-based encryption, Eurocrypt 2005
[Wee'14]: H. Wee, Dual system encryption via predicate encodings, TCC 2014
[GIKM'00]: Y. Gertner, Y. Ishai, E. Kushilevitz, and T. Malkin, Protecting data privacy in private information retrieval schemes, J. Comput. Syst. Sci., 2000.