CryptoGroup
Università di Catania

Dario Catalano

Group Members

Permanent members

- Dario Catalano, Prof. Associato
- Mario Di Raimondo, Ricercatore

Other members

- 1 (visiting) Ph.D. student
- 4 undergraduate students

General Research Interests

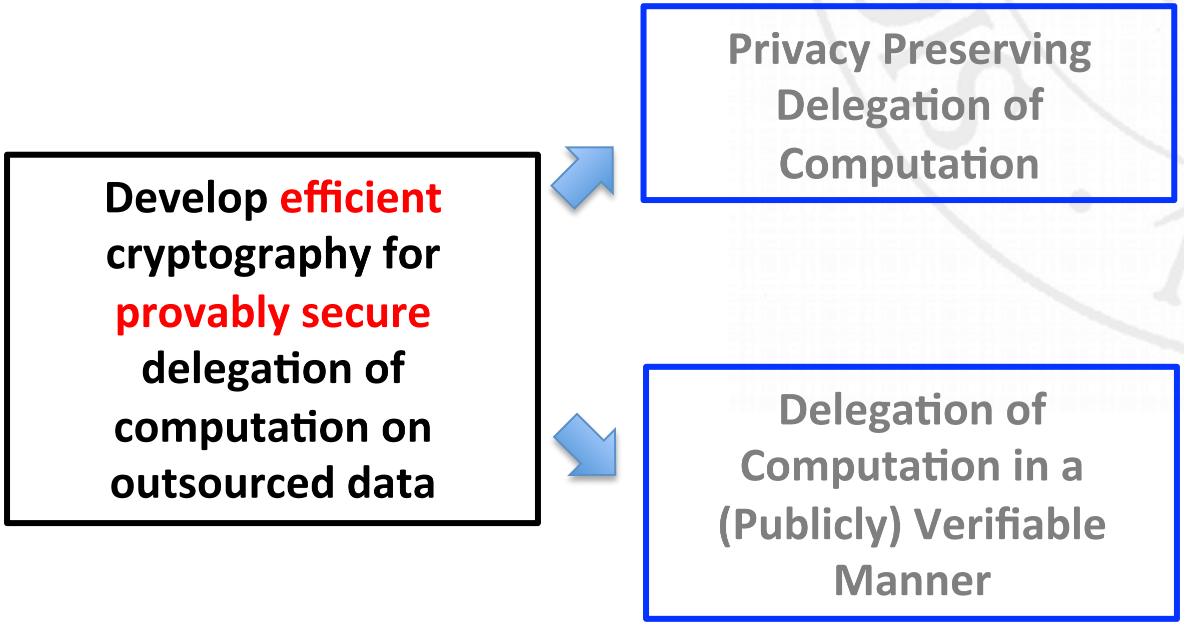
- Design and implementation of efficient and provably secure algorithmic tools to enable secure communication/computation.
  - Focus on foundational issues motivated by practical needs

New frameworks to address practically relevant threats
e.g. Coercion Resistance in Electronic Elections

Efficient Cryptography for distributed systems
e.g. Digital Signatures in distributed systems

Efficient Cryptographic primitives with special properties
e.g. Searchable Encryption, Homomorphic encryption

More specific research interests

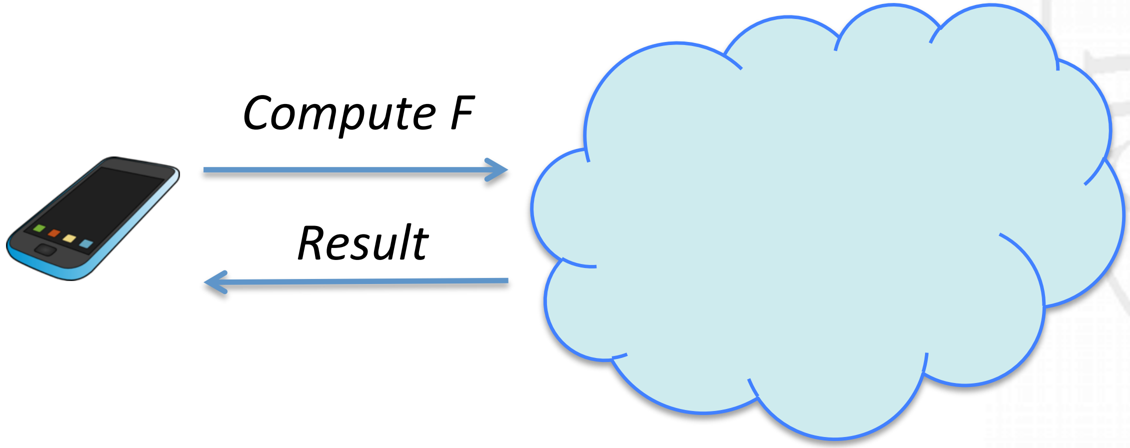


Develop efficient cryptography for provably secure delegation of computation on outsourced data

Privacy Preserving Delegation of Computation

Delegation of Computation in a (Publicly) Verifiable Manner

Privacy Preserving Delegation of Computation



Compute F

Result

Goals

Security - Confidentiality of data should be preserved (even with respect to cloud)

Efficiency - Communication should be minimized

Solution: homomorphic/functional encryption

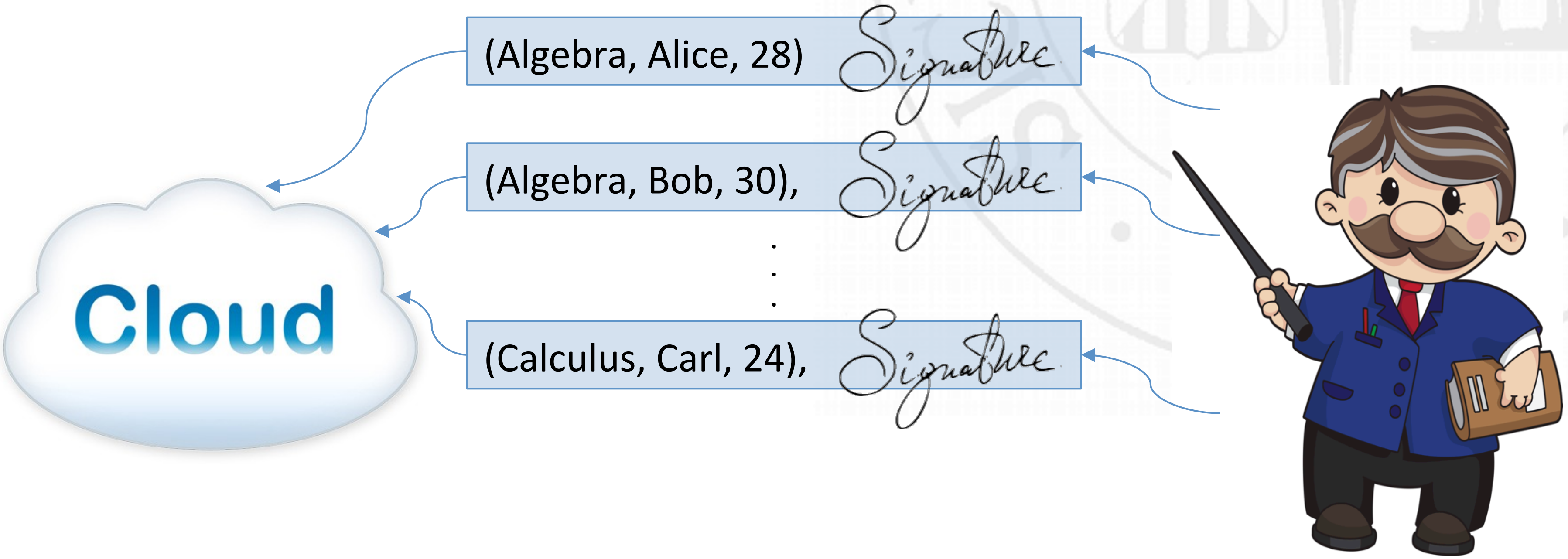
Recent Publications

[BCFG17] *Practical Functional Encryption for Quadratic Functions with Applications to Predicate Encryption* **CRYPTO 2017**

[BCF17] *Labeled Homomorphic Encryption - Scalable and Privacy-Preserving Processing of Outsourced Data* **ESORICS 2017**

[CF15] *Using Linearly-Homomorphic Encryption to Evaluate Degree-2 Functions on Encrypted Data* **ACM CCS 2015**

Delegating Computation on Outsourced Data



(Algebra, Alice, 28)

(Algebra, Bob, 30),

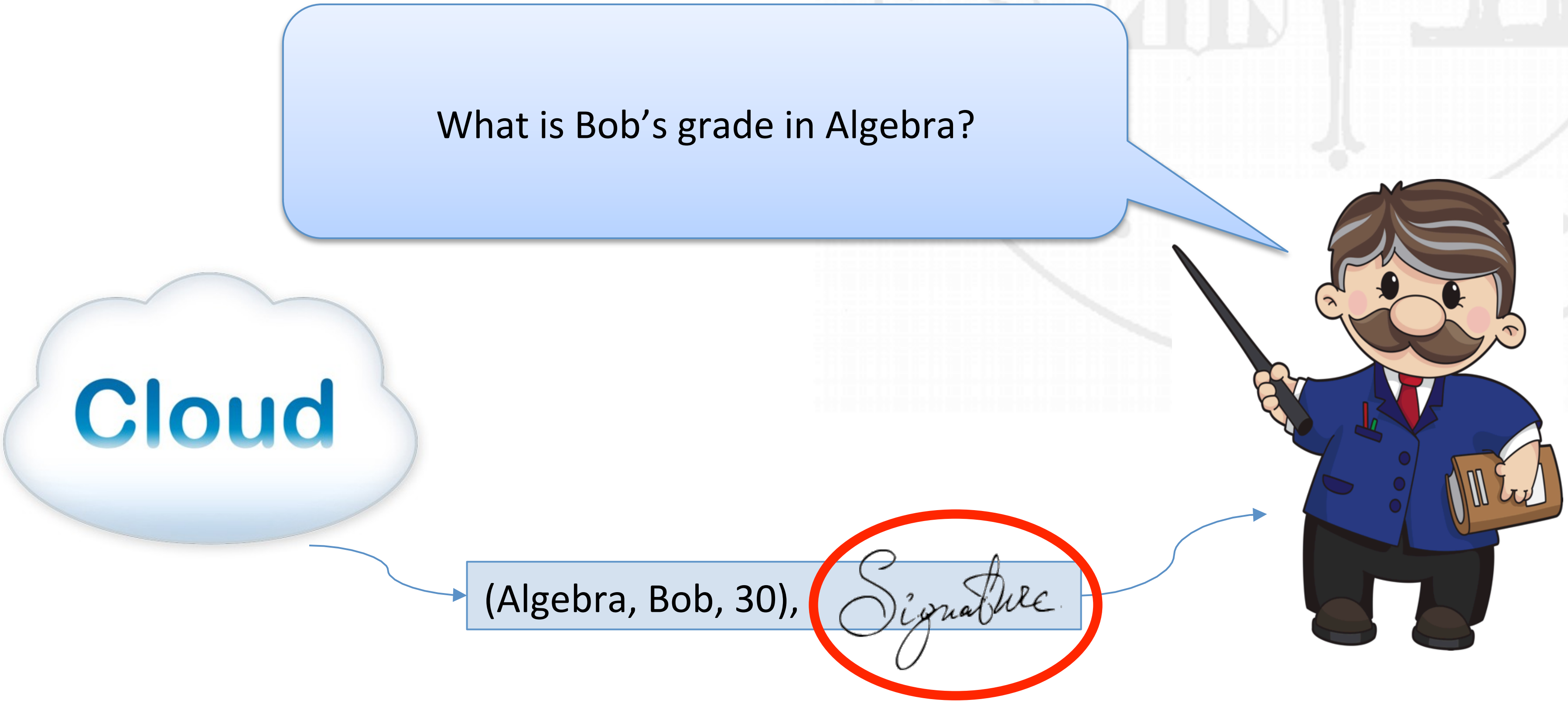
.
.
.

(Calculus, Carl, 24),

Setting

- Server provides seemingly unbounded storage
- The client has limited storage capacity (it “forgets” about its data)

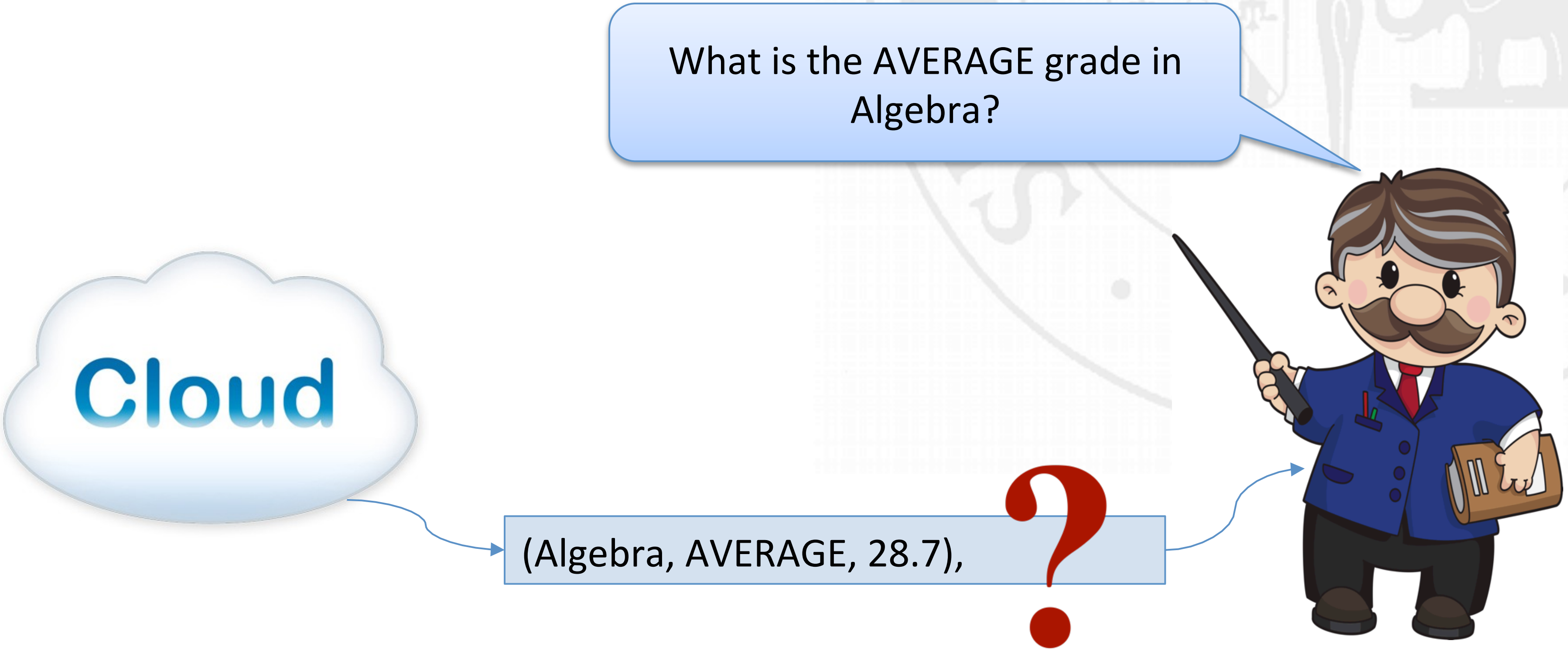
Delegating Computation on Outsourced Data



What is Bob's grade in Algebra?

(Algebra, Bob, 30), Signature

Delegating Computation on Outsourced Data



What is the AVERAGE grade in Algebra?

Cloud

(Algebra, AVERAGE, 28.7), ?

- Authentication problem… **Solution = Signatures/MACs?**
  - No! ☹ Data are going to be manipulated
- **Solution:** homomorphic signatures/MACs

Delegating Computation on Outsourced Data

Recent Publications

[CFN15] *Programmable Hash Functions Go Private: Constructions and Applications to (Homomorphic) Signatures with Shorter Public Keys.* **CRYPTO 2015**

[CMP14] *Authenticating Computation on Groups: New Homomorphic Primitives and Applications* **ASIACRYPT 2014**

[CFW14] *Homomorphic Signatures with Efficient Verification for Polynomial Functions* **CRYPTO 2014**

[CF13] *Practical Homomorphic MACs for Arithmetic Circuits* **EUROCRYPT 2013**

[CFW11] *Adaptive Pseudo-free Groups and Applications* **EUROCRYPT 2011**

Thanks!