Be More and Be Merry

Enhancing Data and User Authentication in Collaborative Settings

Ph.D. Candidate: **Elena Pagnin**

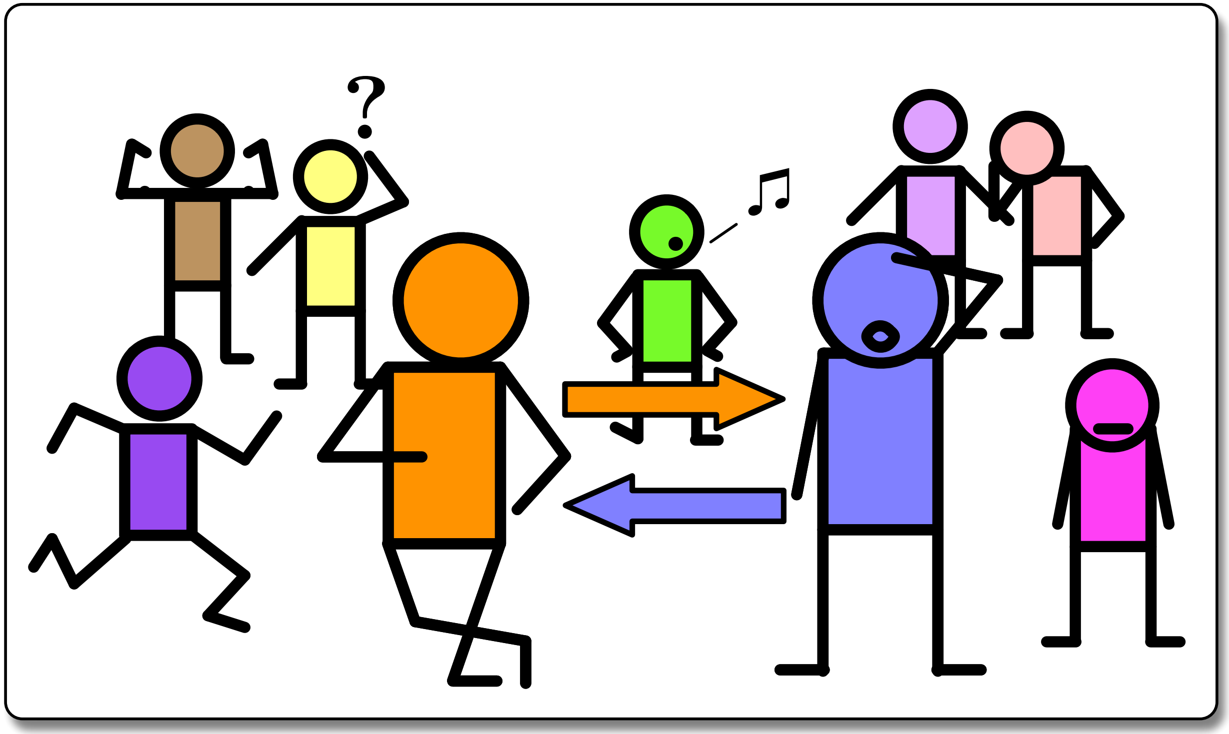
Advisors: Andrei Sabelfeld, Dario Fiore

Examiner: David Sands

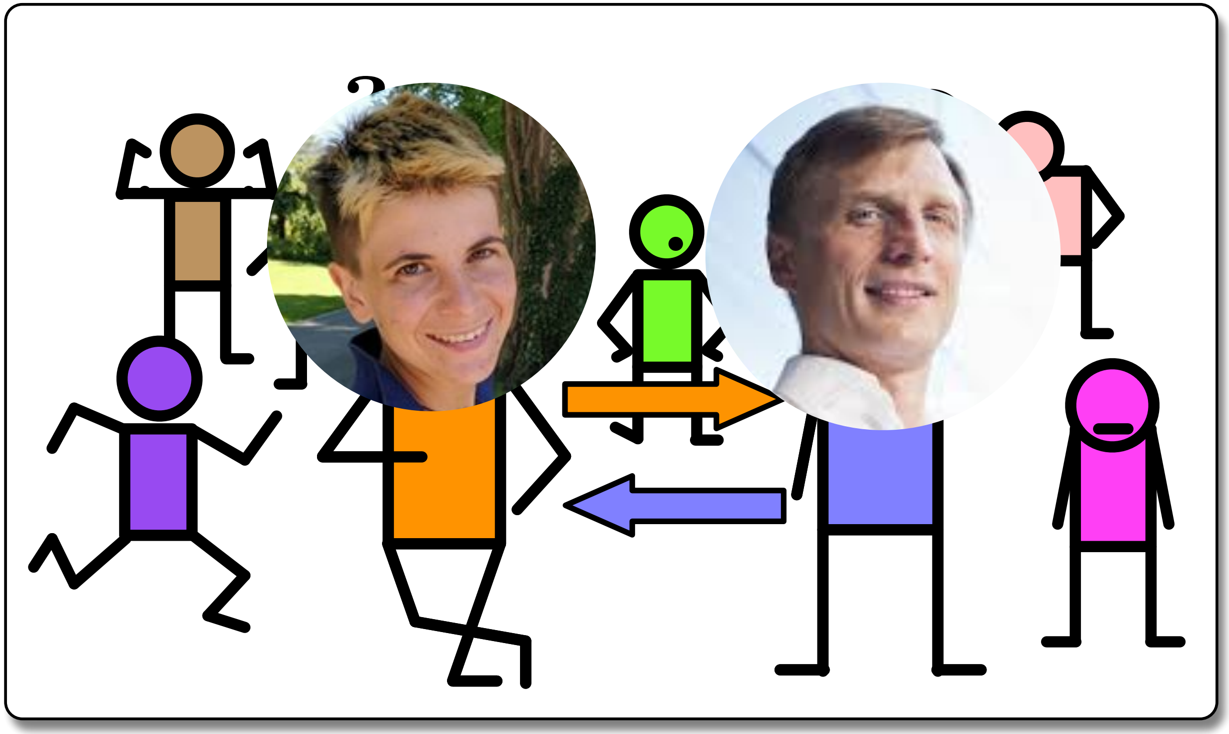
Opponent: **Bart Preneel**

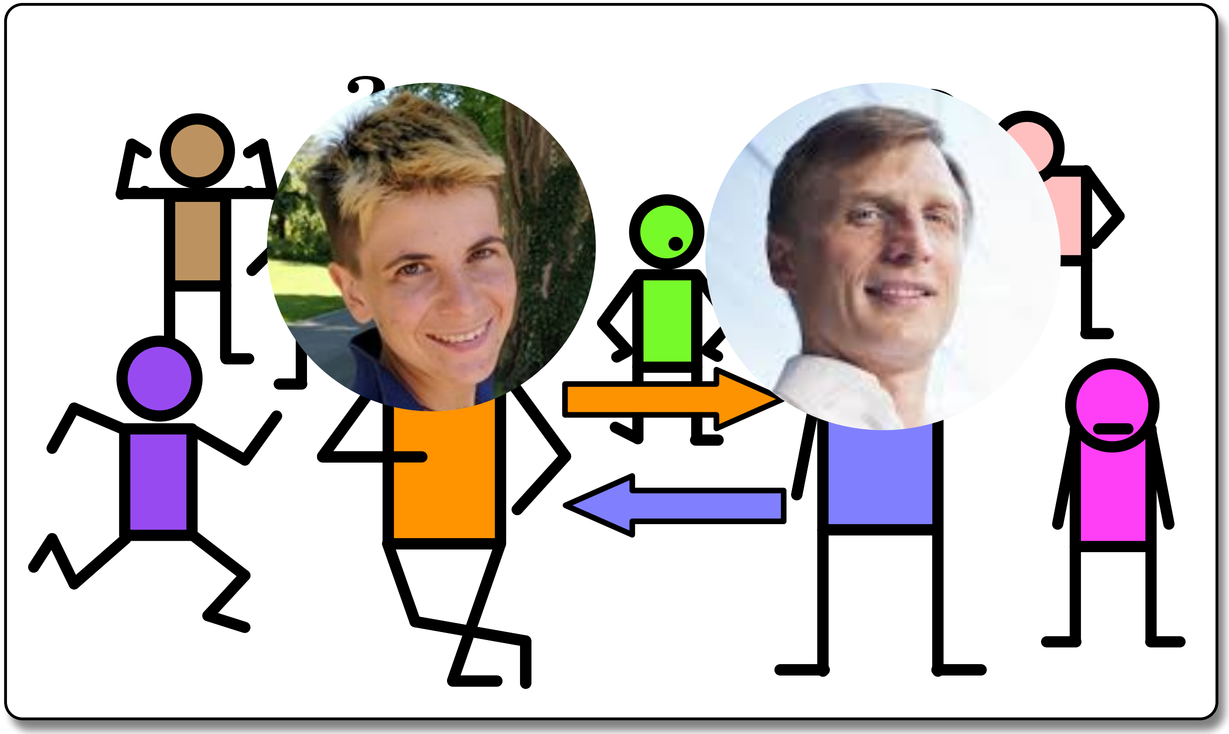
Committee: Claudio Orlandi, Damien Vergnaud, Martin Hell

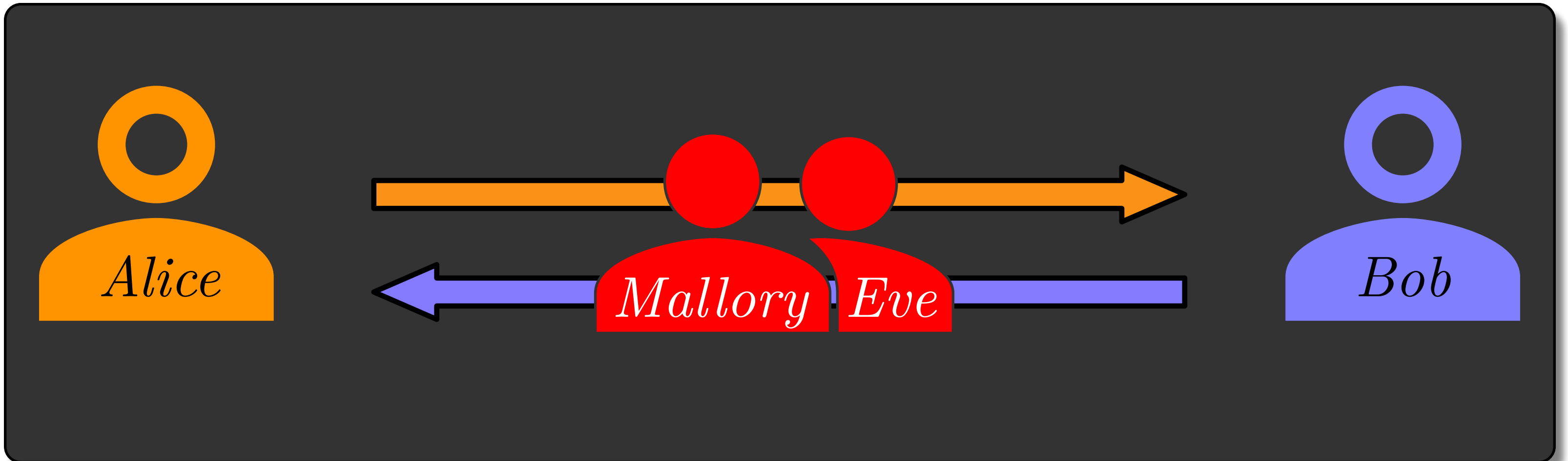
The Cryptographers' World



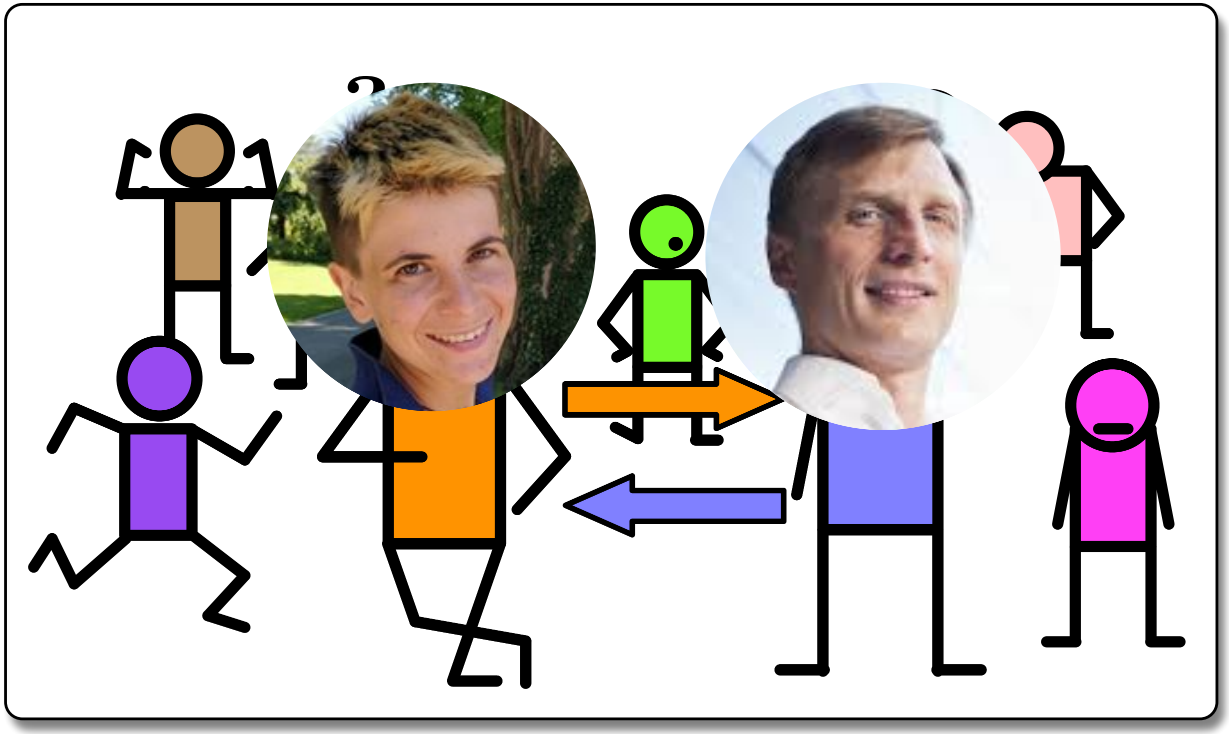
Be More and Be Merry

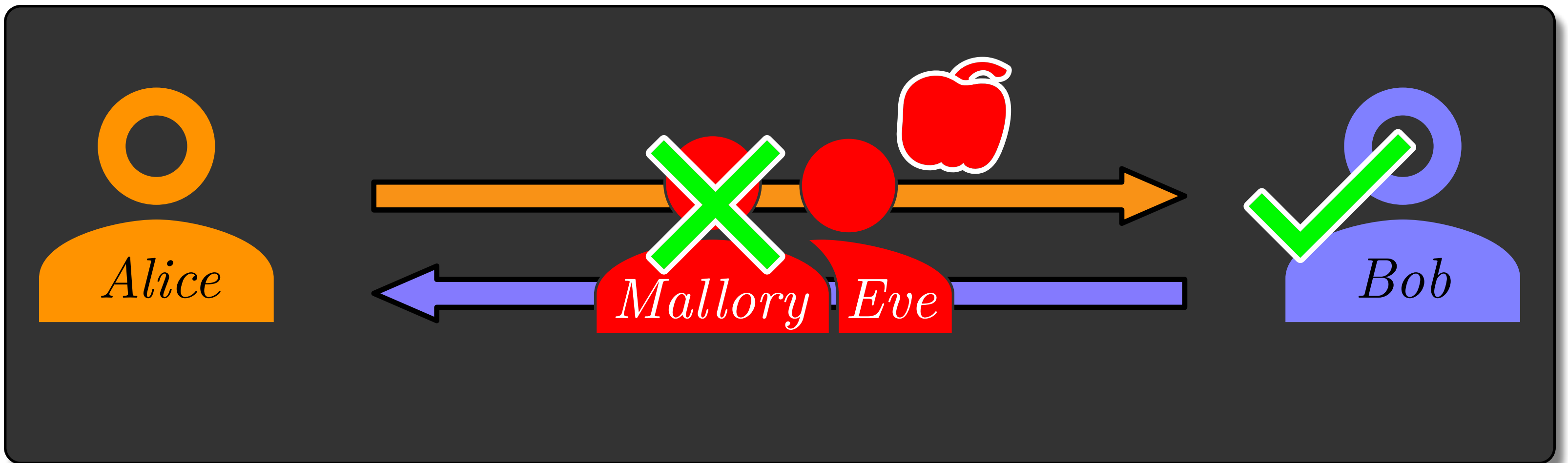





Alice
Mallory
Eve
Bob

The Cryptographers' World





Kappa (Introduction)

Kappa (Introduction)

Collection of Papers

A *Multi-Key Homomorphic Authenticators* ASIACRYPT '16

B *Matrioska: a Compiler for Multi-key Homomorphic Signatures* SCN '18

C *Anonymous Single-Round Server-Aided Verification* LATINCRYPT '17

D *Two-Hop Distance Bounding: Keep your Friends Close* IEEE TMC 2018

E *On the Leakage of Information in Biometric Authentication* INDOCRYPT '14

F *Revisiting Yasuda et al.'s Biometric. Auth. Protocol: Are you Private Enough?* CANS '17

Be More and Be Merry

Kappa (Introduction)

Collection of Papers

A *Multi-Key Homomorphic Authenticators* ASIACRYPT '16

B *Matrioska: a Compiler for Multi-key Homomorphic Signatures* SCN '18

C *Anonymous Single-Round Server-Aided Verification* LATINCRYPT '17

D *Two-Hop Distance Bounding: Keep your Friends Close* IEEE TMC 2018

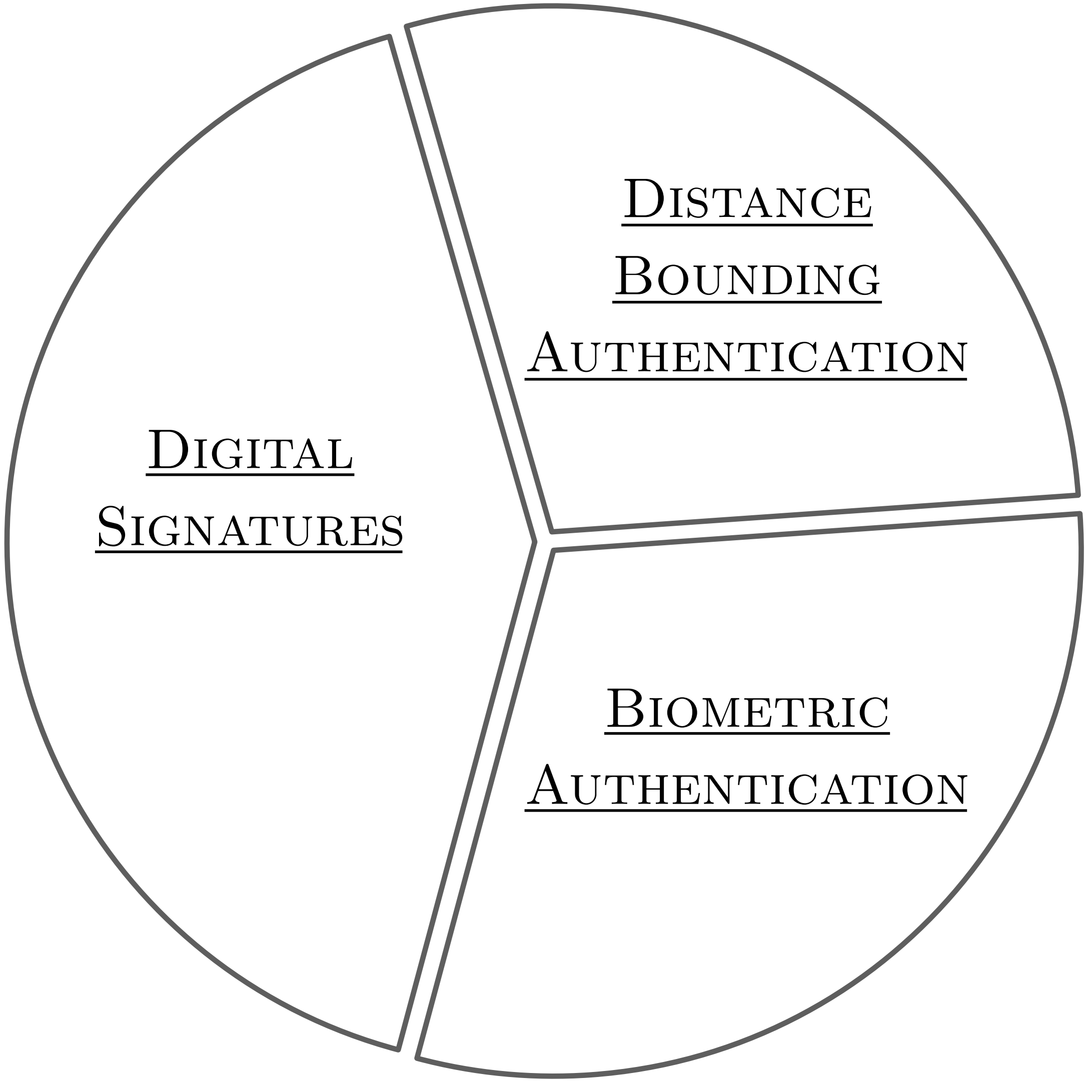
E *On the Leakage of Information in Biometric Authentication* INDOCRYPT '14

F *Revisiting Yasuda et al.'s Biometric. Auth. Protocol: Are you Private Enough?* CANS '17

Be More and Be Merry

Authentication in Collaborative Settings

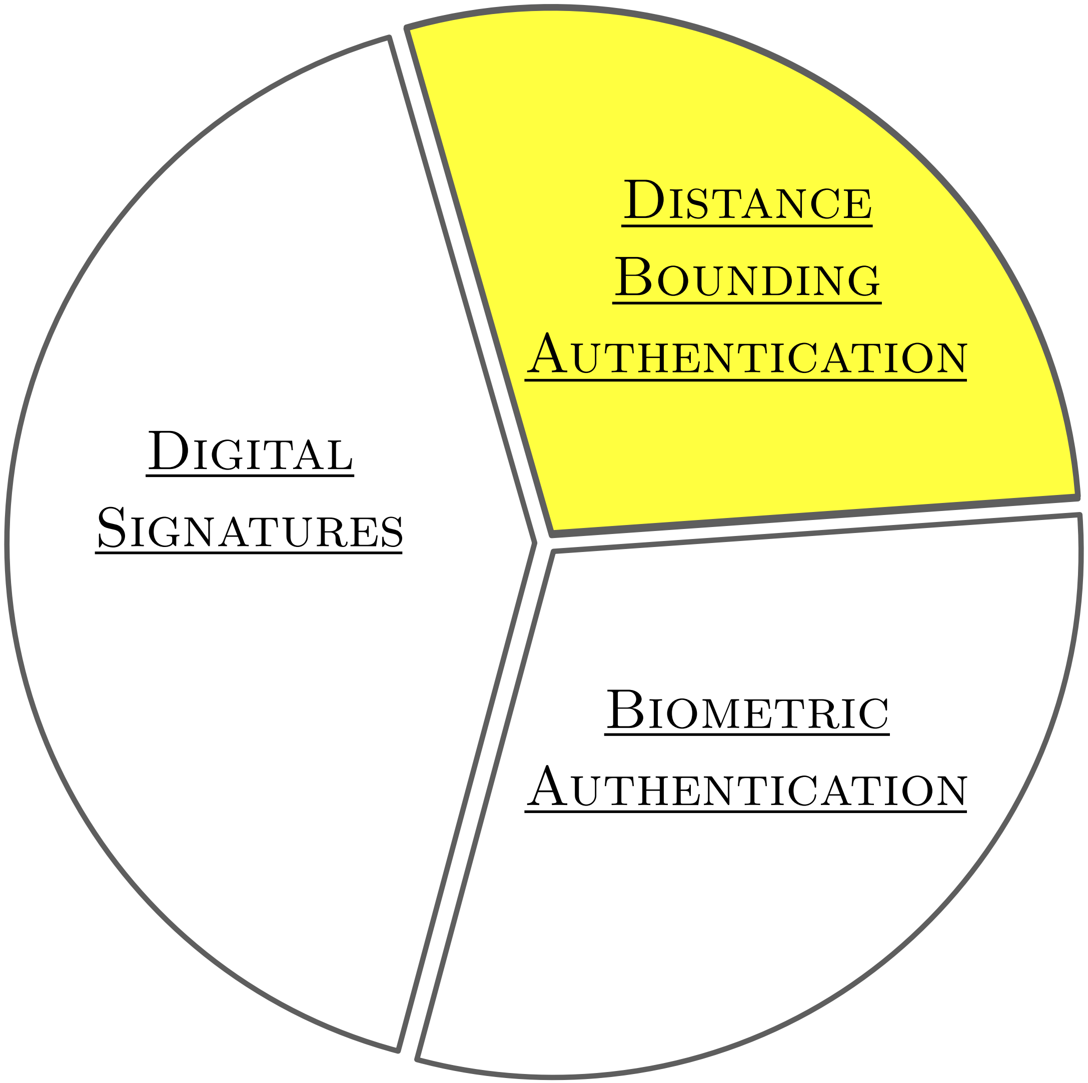
Main Research Areas covered in the Thesis



Be More and Be Merry

Contributions overview and implications

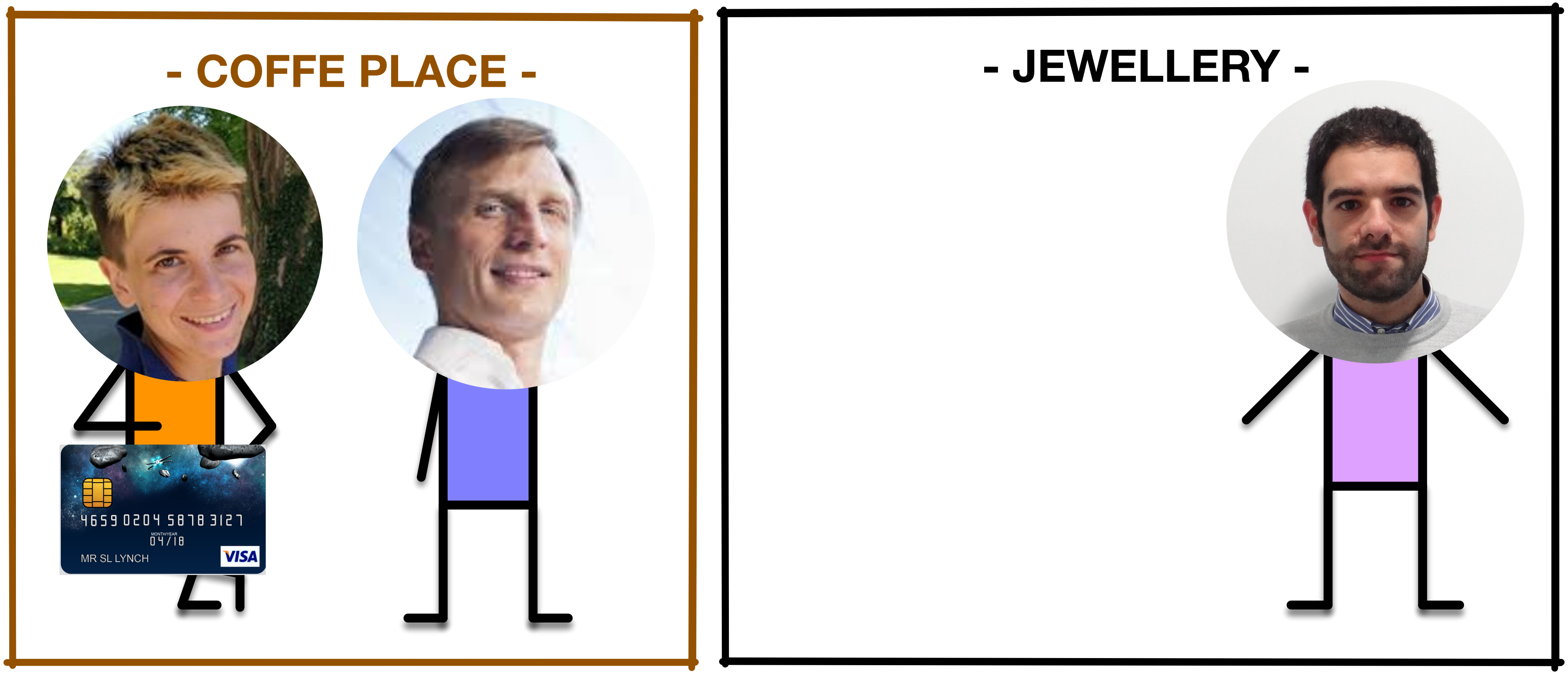
D *Two-Hop Distance Bounding: Keep your Friends Close* IEEE TMC 2018

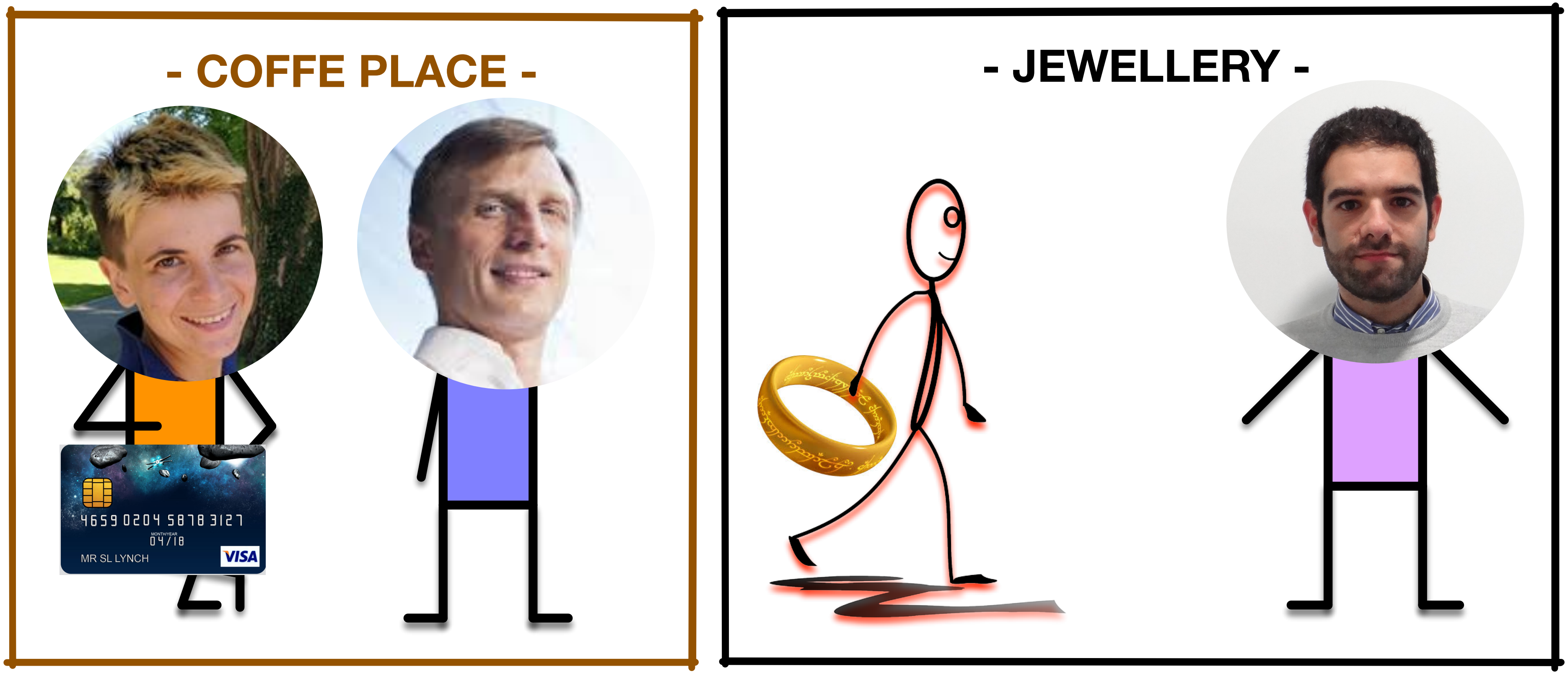


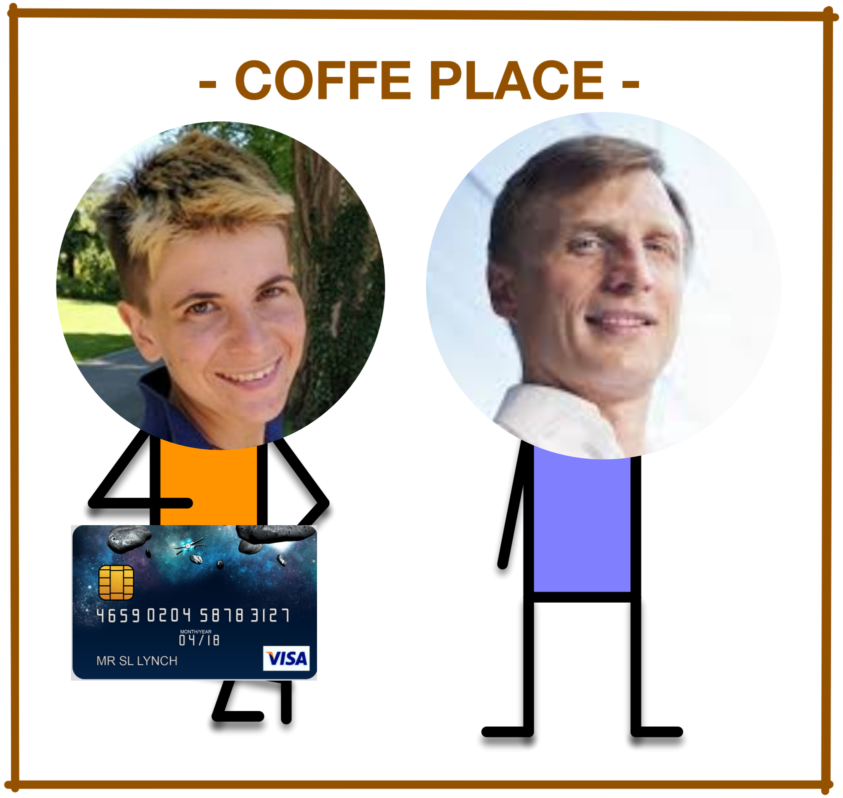
HB+DB: distance bounding meets human based authentication FGCS 2018

Using distance bounding protocols to securely verify the proximity of two-hop neighbours IEEE CL 2015

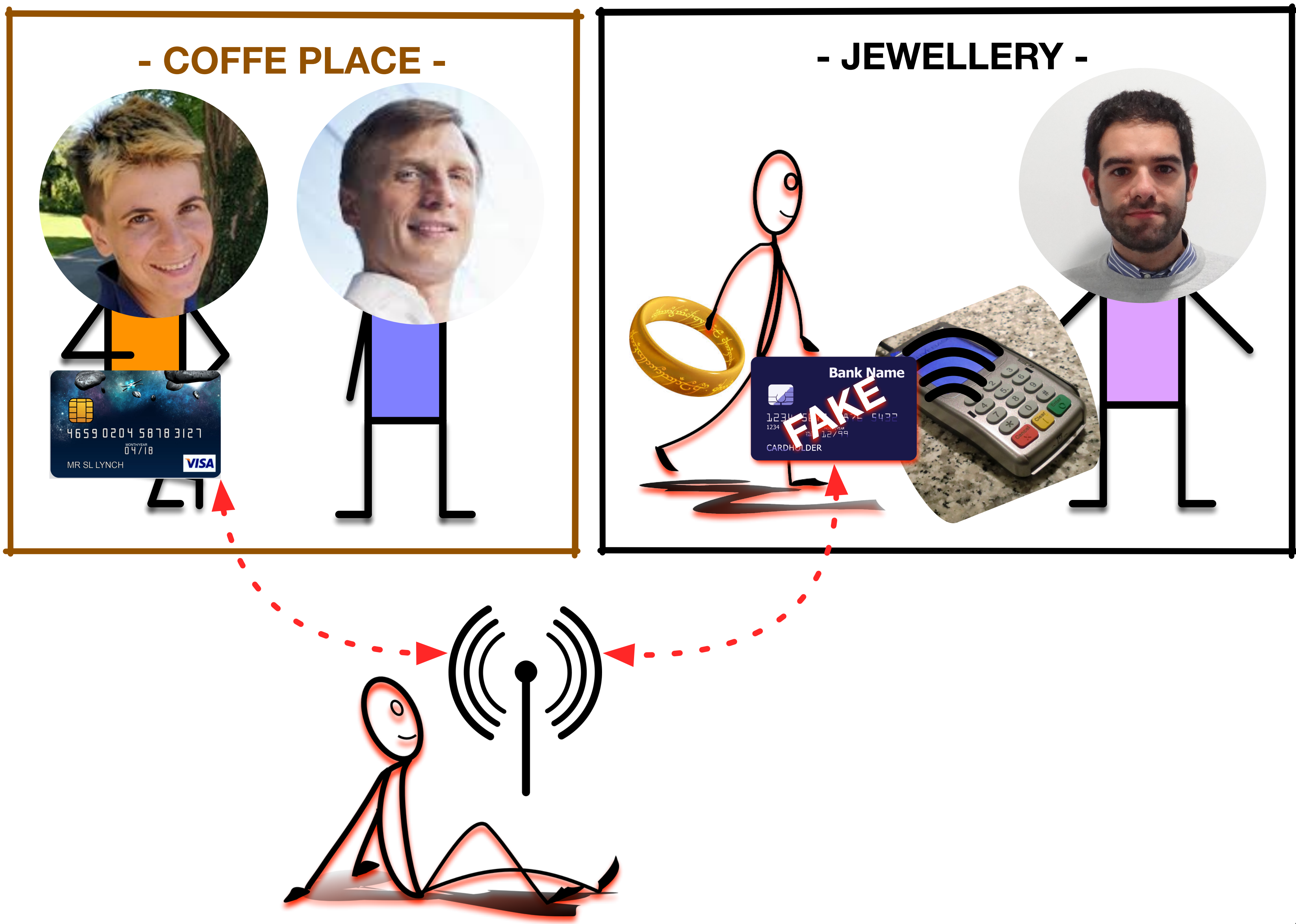
HB+DB, mitigating man in the middle attacks agains HB+ with distance bounding WISEC ‘15


- COFFE PLACE -
4659 0204 5878 3127
04/18
MR SL LYNCH
VISA
- JEWELLERY -

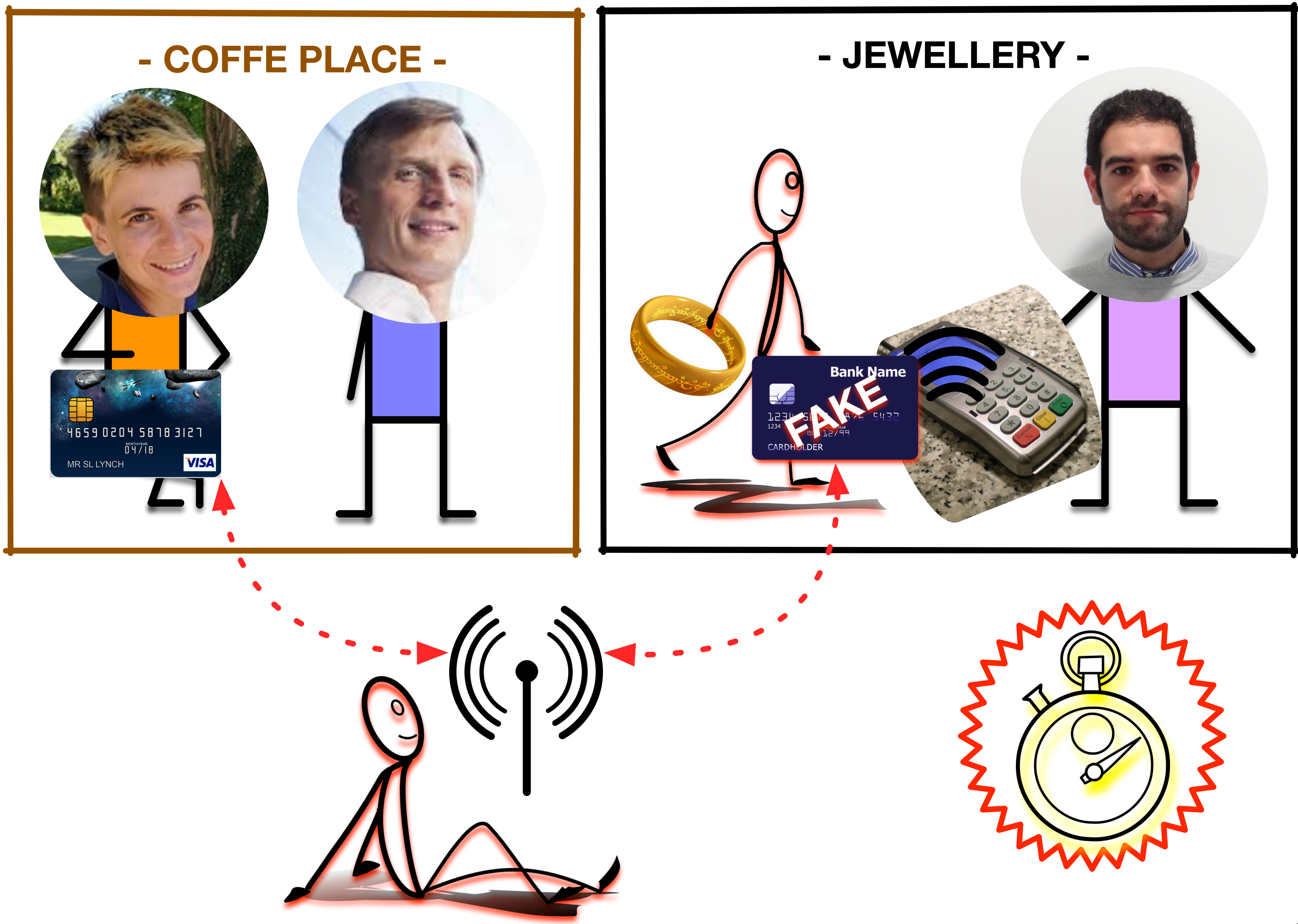

- COFFE PLACE -
4659 0204 5878 3127
MONTH/YEAR
04/18
MR SL LYNCH
VISA
- JEWELLERY -


- COFFE PLACE -
4659 0204 5878 3127
04/18
MR SL LYNCH
VISA

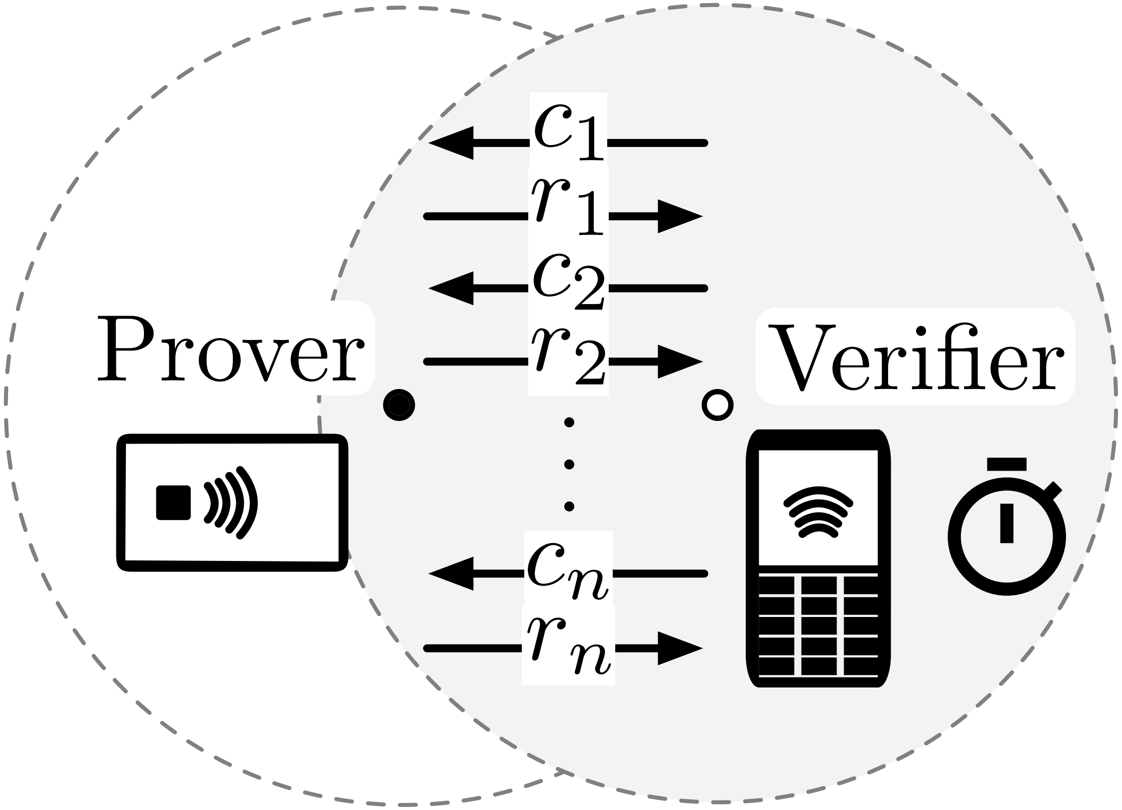

- JEWELLERY -



Be More and Be Merry



Be More and Be Merry

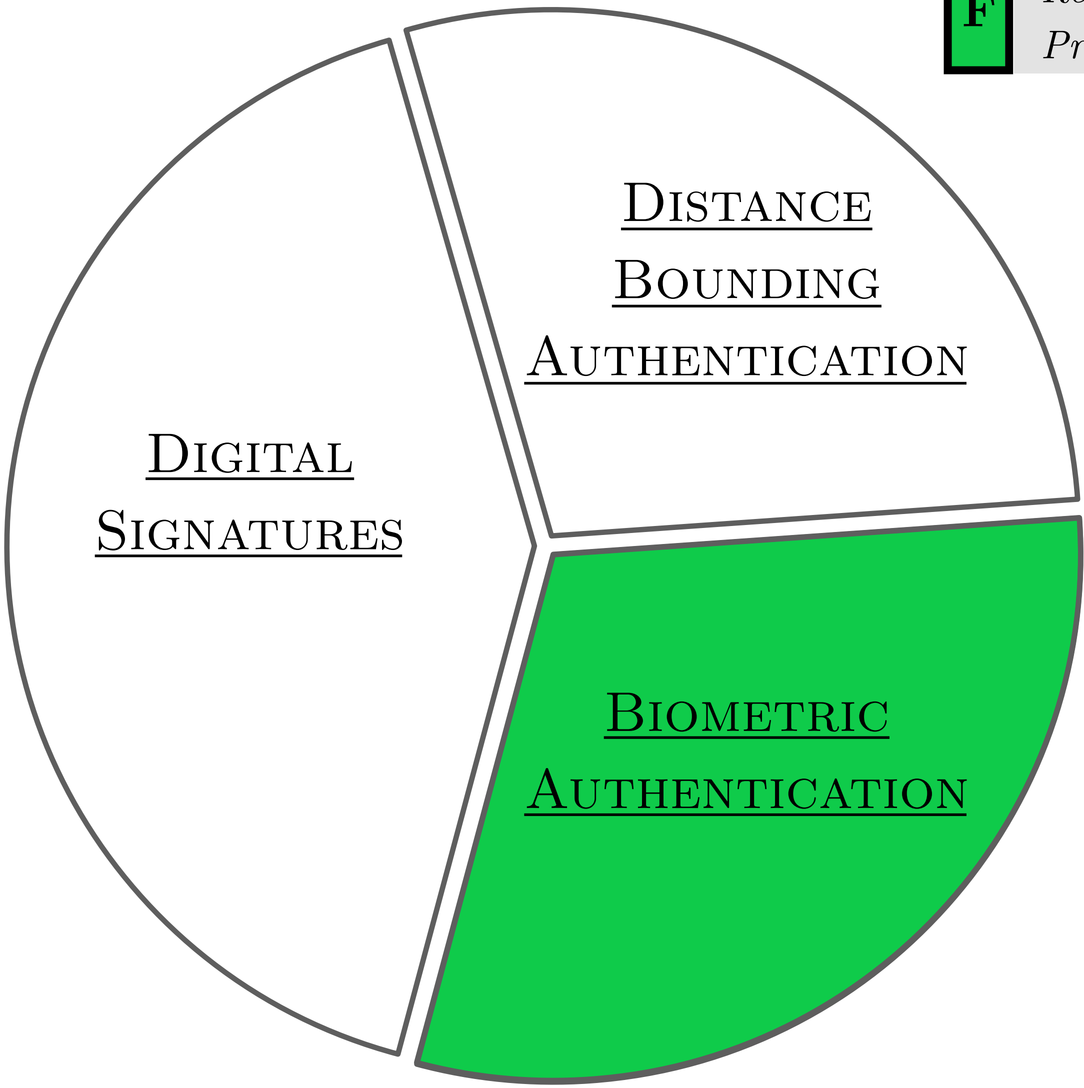


propose a new protocol: ***HB+DB***

extend authentication to ***two-hop scenarios***

Paper D: *"Two-hop Distance-Bounding Protocols: Keep your Friends Close"* (IEEE TMC, 2018)

Be More and Be Merry



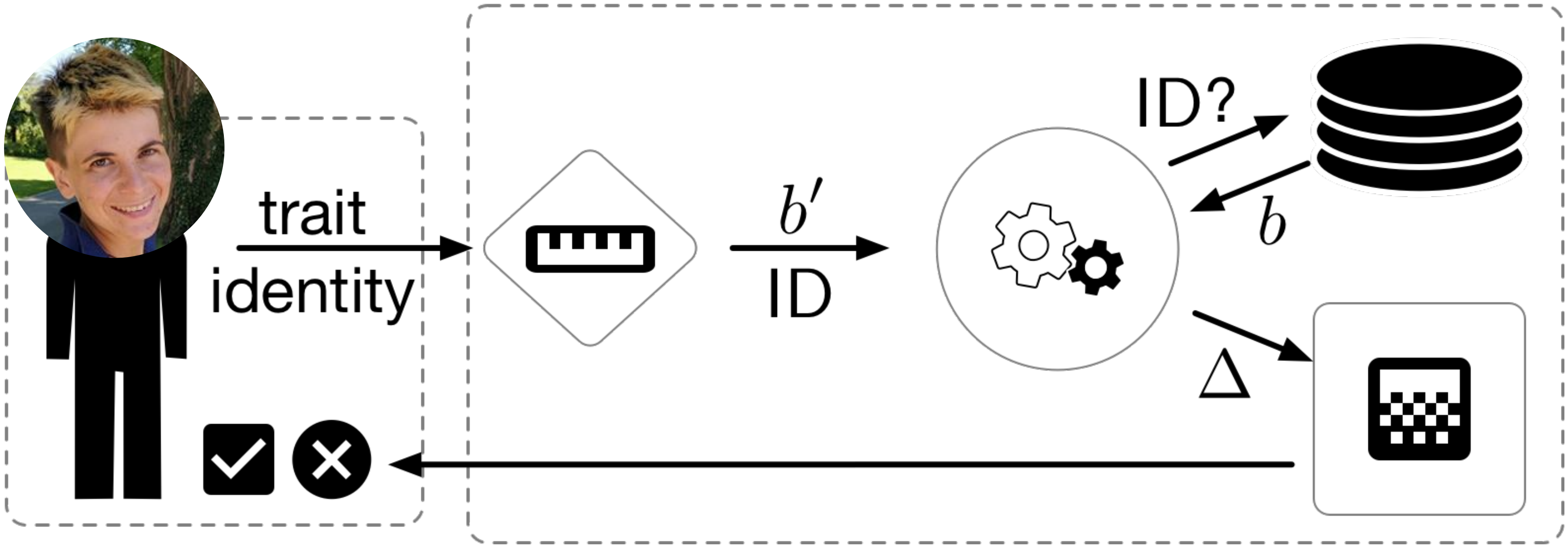
E *On the Leakage of Information in Biometric Authentication* INDOCRYPT '14

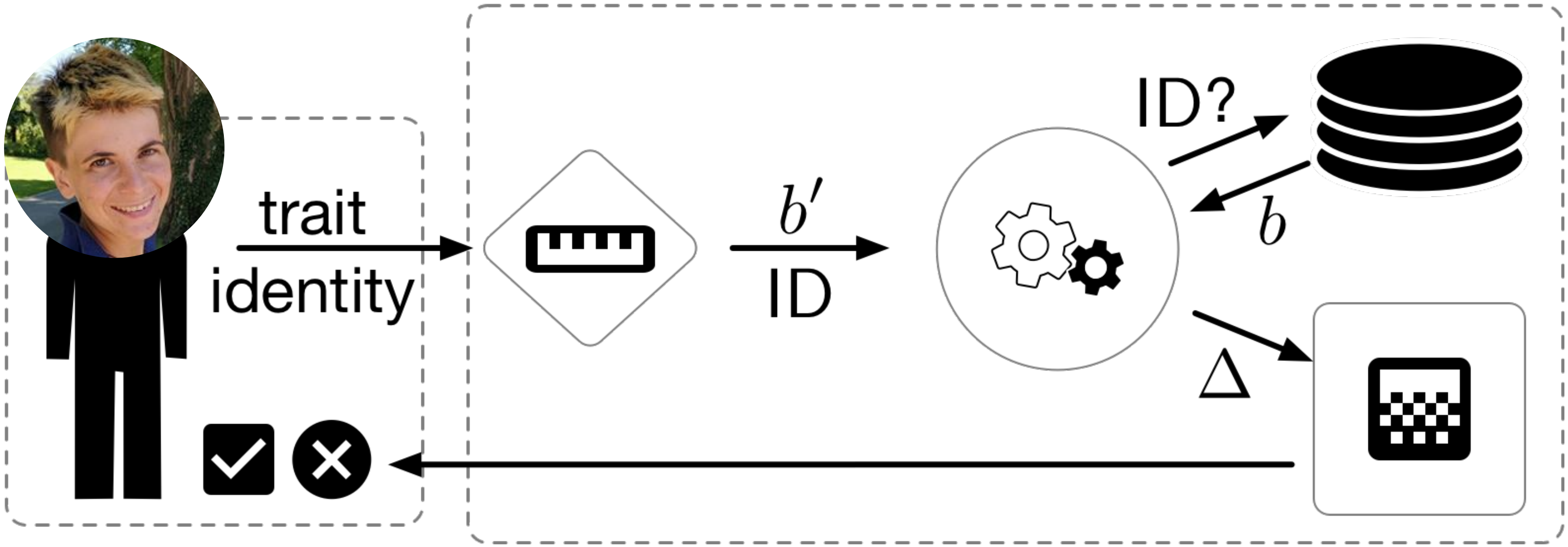
F *Revisiting Yasuda et al.'s Biometric. Auth. Protocol: Are you Private Enough?* CANS '17

Privacy-preserving biometric authentication: challenges and directions SEC.COM.NET 2018

Attacks on privacy-preserving biometric authentication NORDSEC '14

Biometric Authentication





Paper E: *"On the Leakage of Information in Biometric Authentication"* (INDOCRYPT, 2014)

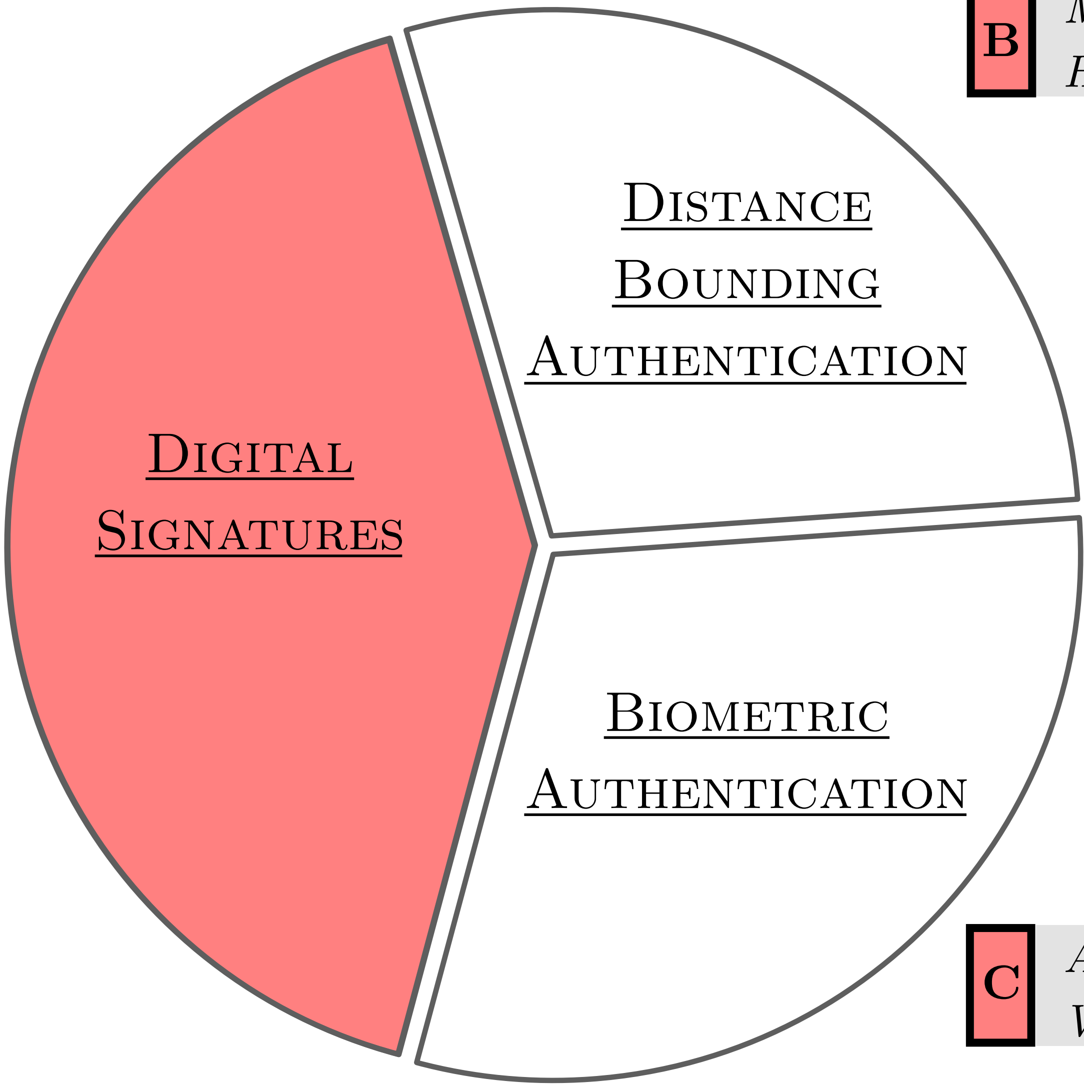
attacks against some biometric authentication protocols (BAP)

BFR+SHE: a new privacy-preserving BAP

challenges and **suggestions** for the design of new BAP

Paper F: *"Revisiting Yasuda et al.'s BAP: Are you Private Enough?"* (CANS, 2017)

Contributions overview and implications



A *Multi-Key Homomorphic Authenticators* ASIACRYPT '16

B *Matrioska: a Compiler for Multi-key Homomorphic Signatures* SCN '18

C *Anonymous Single-Round Server-Aided Verification* LATINCRYPT '17

(signer)

(verifier)

Background on Digital Signatures

(signer)

label message signature

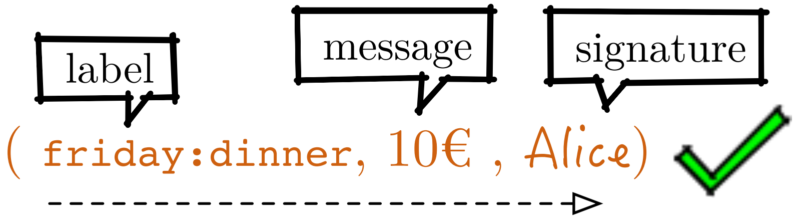
(friday:dinner, 10€ , Alice)

(verifier)

Be More and Be Merry

Background on Digital Signatures

(signer)



(verifier)

Alice spent
10€ for **dinner**
on **Friday**

Background on Digital Signatures

(signer)

label · message · signature

(`friday:dinner`, 10€ , Alice) ✓

(verifier)

How much did Alice spend this week ?

(signer)

(monday:lunch, 8€ , Alice)
(monday:dinner, 18€ , Alice)
(tuesday:coffe, 5€ , Alice)
⋮
⋮
(friday:dinner, 10€ , Alice)

(verifier)

How much did Alice spend this week ?

(signer)

(monday:lunch, 8€ , Alice)

(monday:dinner, 18€ , Alice)

(tuesday:coffe, 5€ , Alice)

:

:

(friday:dinner, 10€ , Alice)

(verifier)

Alice spent
8+18+5+..+10
= **123 euro**
this **week**

How much did Alice spend this week ?

Be More and Be Merry

Background on Digital Signatures

INEFFICIENT

(signer)

(monday:lunch, 8€ , Alice)

(monday:dinner, 18€ , Alice)

(tuesday:coffe, 5€ , Alice)

:

:

(friday:dinner, 10€ , Alice)

(verifier)

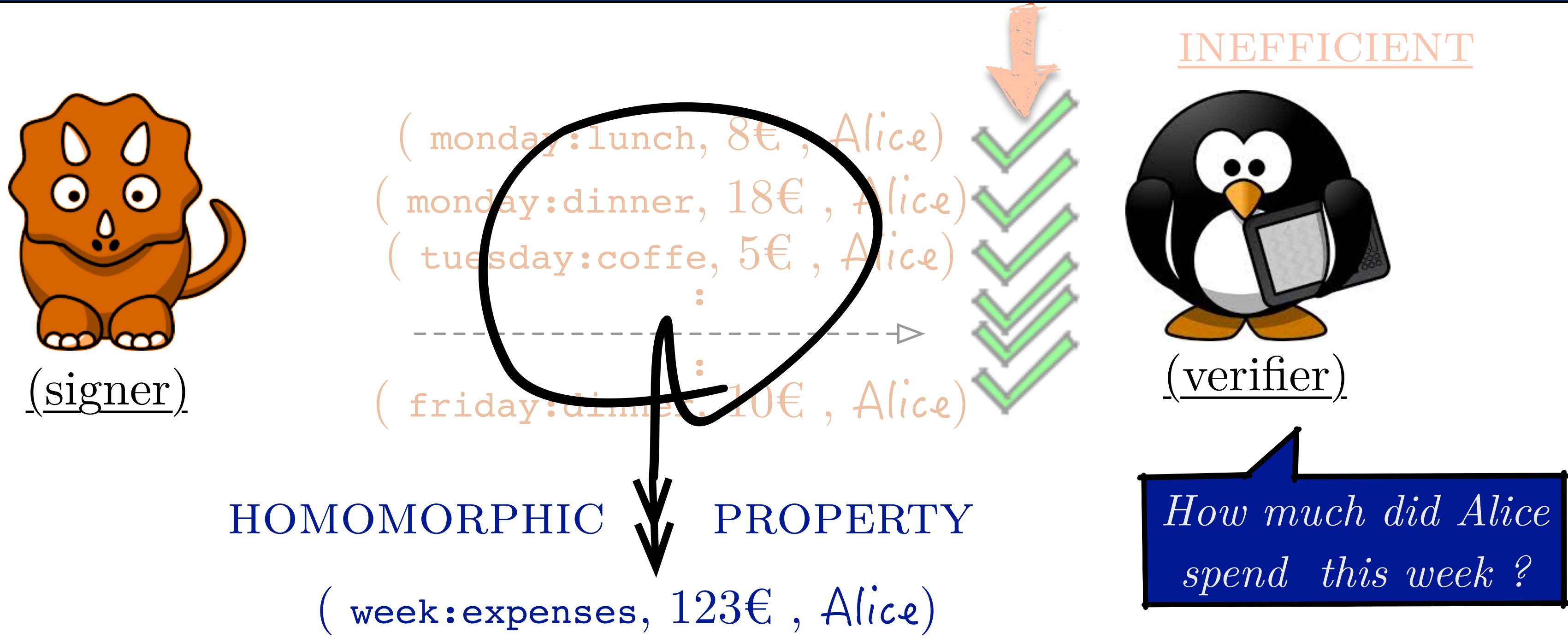
Alice spent

8+18+5+..+10

= **123 euro**

this **week**

How much did Alice spend this week ?


INEFFICIENT
(signer)
(monday:lunch, 8€ , Alice)
(monday:dinner, 18€ , Alice)
(tuesday:coffe, 5€ , Alice)
(friday:dinner, 10€ , Alice)
(verifier)
How much did Alice spend this week ?
HOMOMORPHIC PROPERTY
(week:expenses, 123€ , Alice)

Background on Digital Signatures

INEFFICIENT

(signer)

(monday:lunch, 8€ , Alice)
(monday:dinner, 18€ , Alice)
(tuesday:coffe, 5€ , Alice)
⋮
⋮
(friday:dinner, 10€ , Alice)

HOMOMORPHIC PROPERTY

(week:expenses, 123€ , Alice)

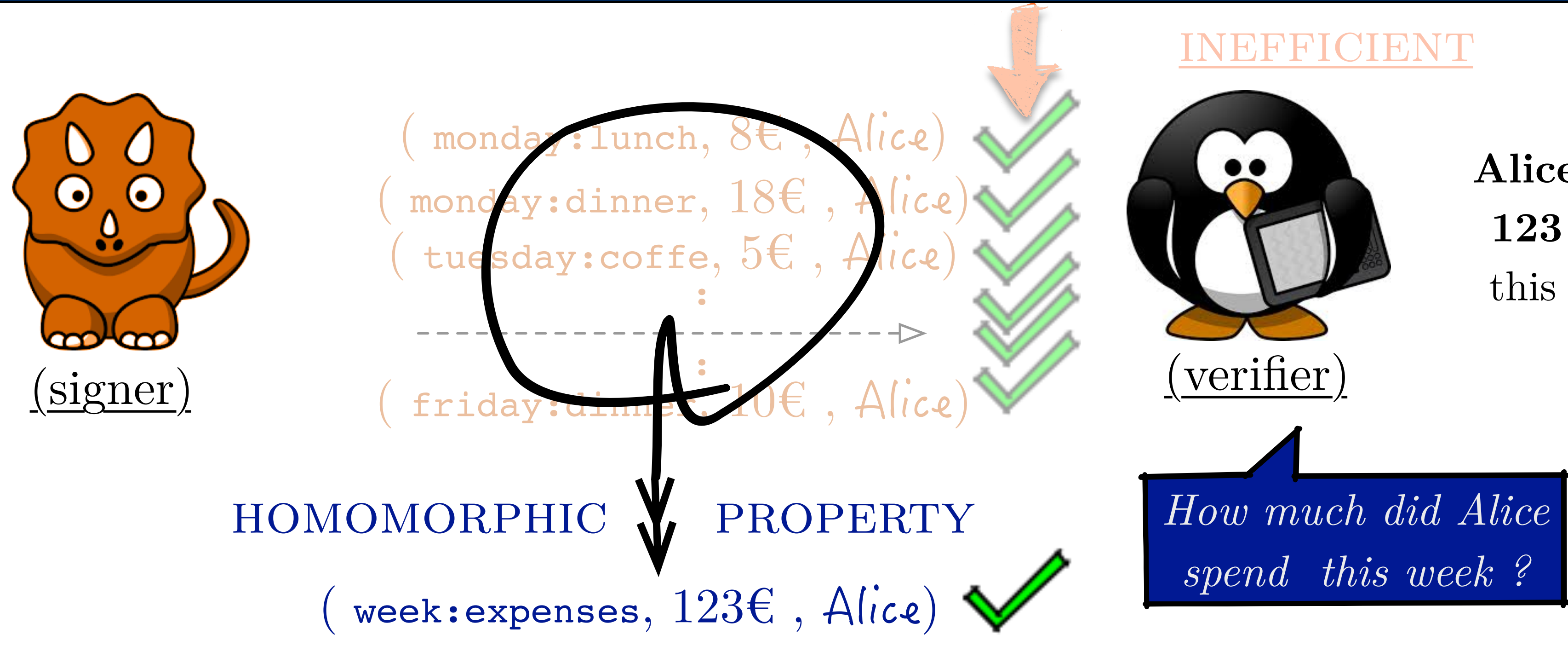
(verifier)

Alice spent **123 euro** this **week**

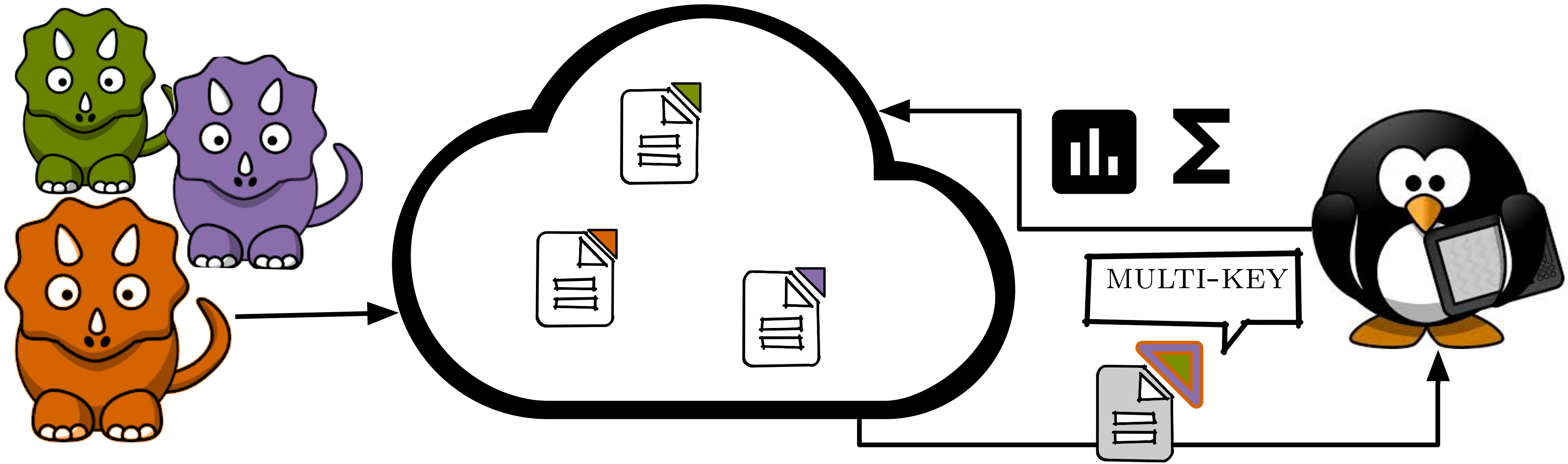
How much did Alice spend this week ?

Be More and Be Merry

Background on Digital Signatures



how about collaborative scenarios?



Be More and Be Merry

1- A suitable **definition** of **M**ulti-**K**ey **H**omomorphic **A**uthenticators

Be More and Be Merry

1- A suitable **definition** of **M**ulti-**K**ey **H**omomorphic **A**uthenticators

2- The **first** construction of a **M**ulti-**K**ey **H**omomorphic **S**ignature

- supports evaluation of *circuits of bounded polynomial depth*
- security reduces to *SIS over standard lattices*
- tolerates *adaptive corruption* (but no insider corruption)
- works for data items authenticates and outsources in a *streaming* fashion

1- A suitable **definition** of **M**ulti-**K**ey **H**omomorphic **A**uthenticators

2- The **first** construction of a **M**ulti-**K**ey **H**omomorphic **S**ignature

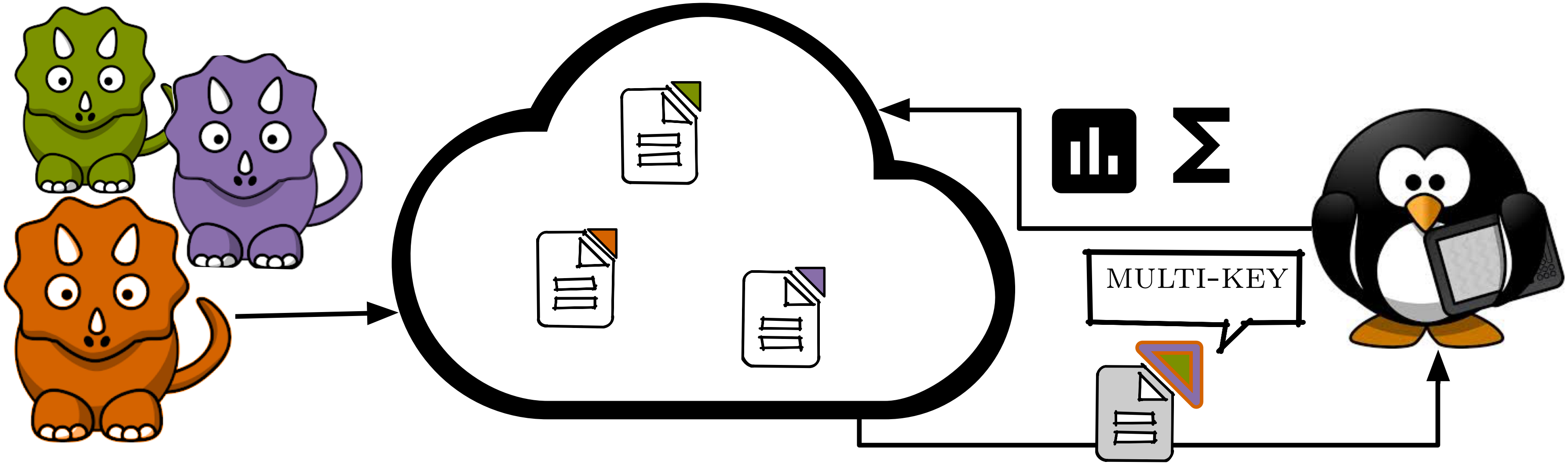
supports evaluation of *circuits of bounded polynomial depth*
security reduces to *SIS over standard lattices*
tolerates *adaptive corruption* (but no insider corruption)
works for data items authenticates and outsources in a *streaming* fashion

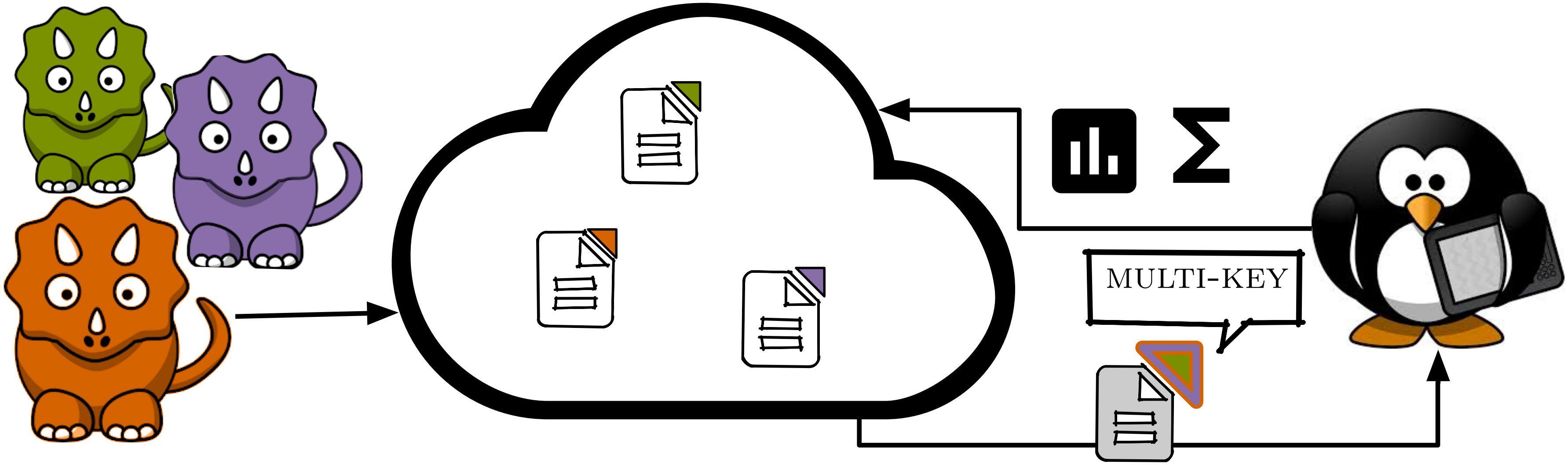
3- The **first** construction of a **M**ulti-**K**ey **H**omomorphic **M**essage **A**uthentication **C**ode

supports evaluation of *arithmetic circuits of low-degree*
security reduces to *one-way functions* (PRF)
tag size independent of the number of messages $\binom{users + degree}{degree}$
efficient as the arithmetics on finite multi-variate polynomial ring

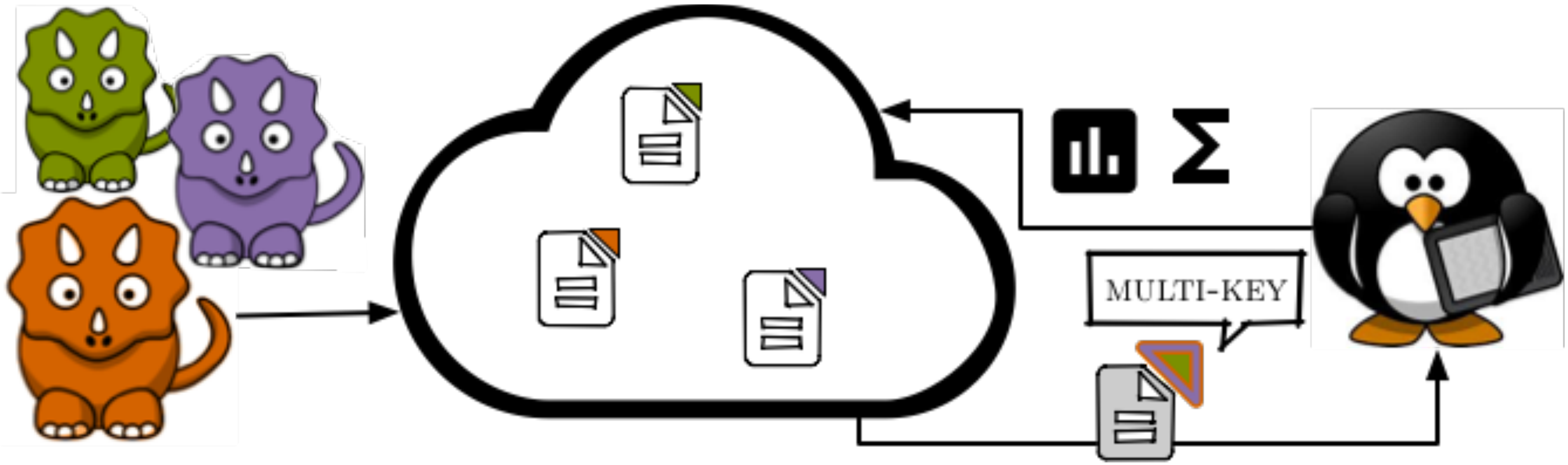
Be More and Be Merry

Now we can...





is there a **general way** to:
construct a ***multi***-key homomorphic scheme
from a ***single***-key homomorphic scheme?



is there a **general way** to:
construct a ***multi***-key homomorphic scheme
from a ***single***-key homomorphic scheme?

YES !
via our Matrioska compiler

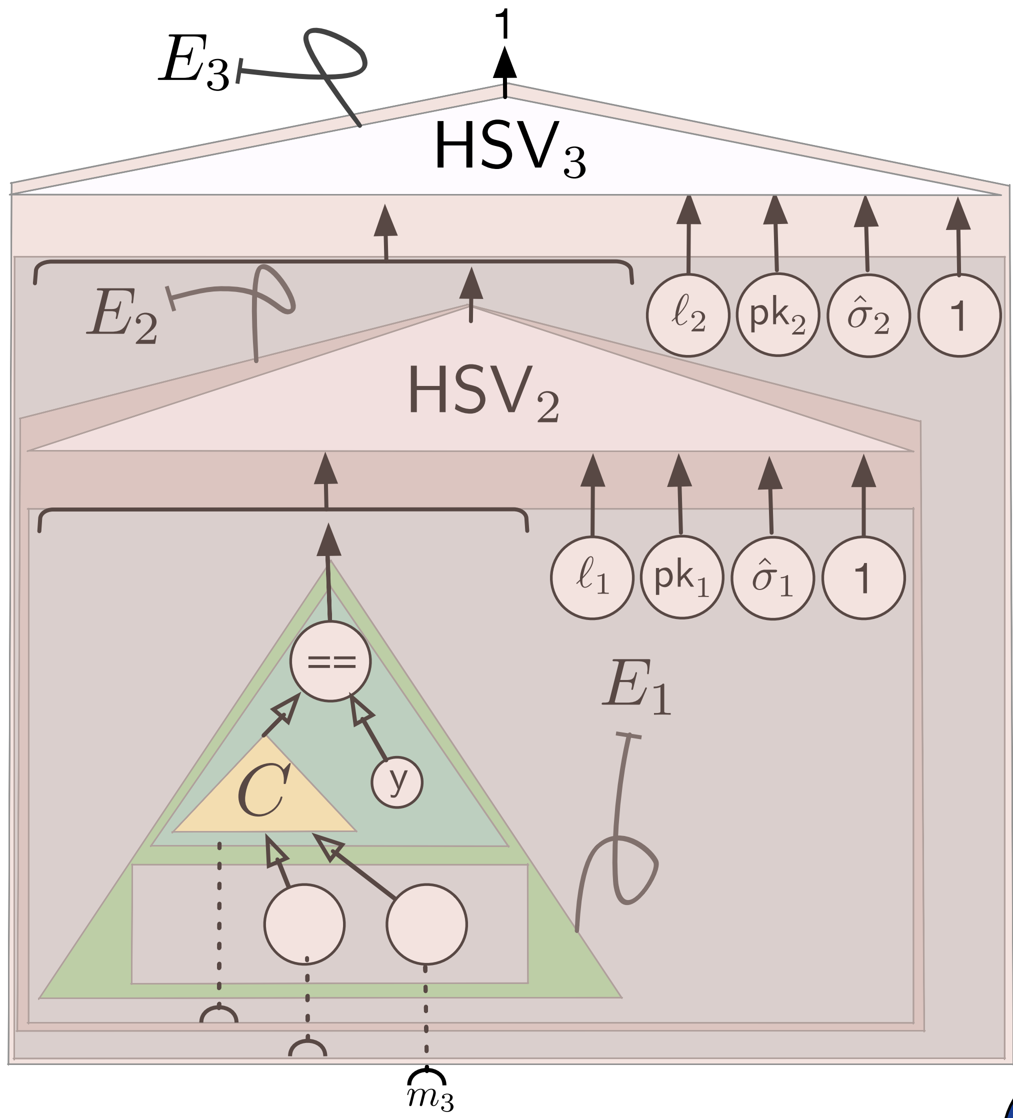
A **compiler** for **multi-key homomorphic signatures**

HS for circuits of poly.**depth**
and | $\boldsymbol{\sigma}$ | = **poly($\boldsymbol{\lambda}$)**

⇓ Matrioska

for any fixed number ***t*** *of distinct* ***sk***

MKHS for circuits of poly.**size**
and | $\boldsymbol{\sigma}$ | = ***t*** * **poly($\boldsymbol{\lambda}$)**



Be More and Be Merry

Digital Signatures are a Powerful tool

(signer)

(friday:dinner, 10€ , *Alice*) ✓

(verifier)

fully-homomorphic
multi-key
group
structure-preserving
anonymous
identity-based
ring
sanitizable
hierarchical
redactable
post-quantum
linearly-homomorphic
context-hiding

advanced functionalities often imply computationally heavy verification

Signature Scheme:

$\mathsf{SetUp}(1^\lambda) \to \mathsf{gp}$

$\mathsf{KeyGen}(\mathsf{gp}) \to (\mathsf{pk}, \mathsf{sk})$

$\mathsf{Sign}(\mathsf{sk}, m) \to \sigma$

$\mathsf{Verify}(\mathsf{pk}, m, \sigma) \to 0/1$

What is Server-Aided Verification?

Signature Scheme:

$\mathsf{SetUp}(1^\lambda) \rightarrow \mathsf{gp}$

$\mathsf{KeyGen}(\mathsf{gp}) \rightarrow (\mathsf{pk}, \mathsf{sk})$

$\mathsf{Sign}(\mathsf{sk}, m) \rightarrow \sigma$

$\mathsf{Verify}(\mathsf{pk}, m, \sigma) \rightarrow 0/1$

Example: the **BLS** [BonehLS04]

$\mathsf{gp} = \mathsf{BilinGroup}$

$\mathsf{pk} = g^{\mathsf{sk}}, \ \mathsf{sk} \leftarrow \mathbb{Z}_p$

$\sigma = \mathsf{Hash}(m)^{\mathsf{sk}}$

$e(\sigma, g) \stackrel{?}{=} e(\mathsf{Hash}(m), \mathsf{pk})$

[BonehLS04] : D. Boneh, B. Lynn, and H. Shacham. Short signatures from the weil pairing. Journal of Cryptology, 17(4):297–319, 2004.

What is Server-Aided Verification?

Signature Scheme:

$$\mathsf{SetUp}(1^\lambda) \to \mathsf{gp}$$

$$\mathsf{KeyGen}(\mathsf{gp}) \to (\mathsf{pk}, \mathsf{sk})$$

$$\mathsf{Sign}(\mathsf{sk}, m) \to \sigma$$

$$\mathsf{Verify}(\mathsf{pk}, m, \sigma) \to 0/1$$

<u>Example</u>: the **BLS** [BonehLS04]

$$\mathsf{gp} = \mathsf{BilinGroup}$$

$$\mathsf{pk} = g^{\mathsf{sk}},\ \mathsf{sk} \leftarrow \mathbb{Z}_p$$

$$\sigma = \mathsf{Hash}(m)^{\mathsf{sk}}$$

$$e(\sigma, g) \stackrel{?}{=} e(\mathsf{Hash}(m), \mathsf{pk})$$

$$cost(\mathsf{Verify}) > cost(\mathsf{Sign})$$

Be More and Be Merry

[BonehLS04] : D. Boneh, B. Lynn, and H. Shacham. Short signatures from the weil pairing. Journal of Cryptology, 17(4):297–319, 2004.

Signature Scheme:

$\mathsf{SetUp}(1^\lambda) \rightarrow \mathsf{gp}$

$\mathsf{KeyGen}(\mathsf{gp}) \rightarrow (\mathsf{pk}, \mathsf{sk})$

$\mathsf{Sign}(\mathsf{sk}, m) \rightarrow \sigma$

Server-Aided Verification (SAV)

Example: the **BLS** [BonehLS04]

$\mathsf{gp} = \mathsf{BilinGroup}$

$\mathsf{pk} = g^{\mathsf{sk}}, \ \mathsf{sk} \leftarrow \mathbb{Z}_p$

$\sigma = \mathsf{Hash}(m)^{\mathsf{sk}}$

$e(\sigma, g) \stackrel{?}{=} e(\mathsf{Hash}(m), \mathsf{pk})$

$\mathit{cost}(\mathsf{Verify}) > \mathit{cost}(\mathsf{Sign})$

Be More and Be Merry

SERVER-AIDED VERIFICATION

VERIFIER

interactive protocol

SERVER

[BonehLS04] : D. Boneh, B. Lynn, and H. Shacham. Short signatures from the weil pairing. Journal of Cryptology, 17(4):297–319, 2004.

1. **First generic compiler** for server-aided verification of signatures

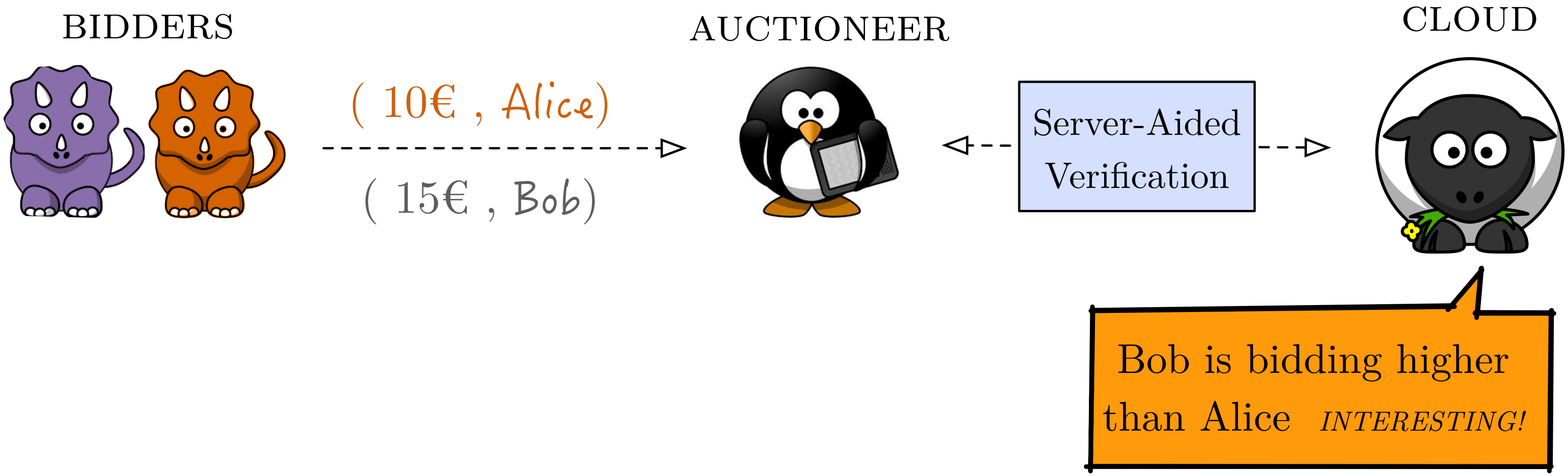
Be More and Be Merry

1. **First generic compiler** for server-aided verification of signatures
2. **Three novel** server-aided verification **schemes**

1. **First generic compiler** for server-aided verification of signatures
2. **Three novel** server-aided verification **schemes**
3. **Introduce** the notion of **signer anonymity**

Paper C: Anonymous Single-Round Server-Aided Verification

1. **First generic compiler** for server-aided verification of signatures
2. **Three novel** server-aided verification **schemes**
3. **Introduce** the notion of **signer anonymity**

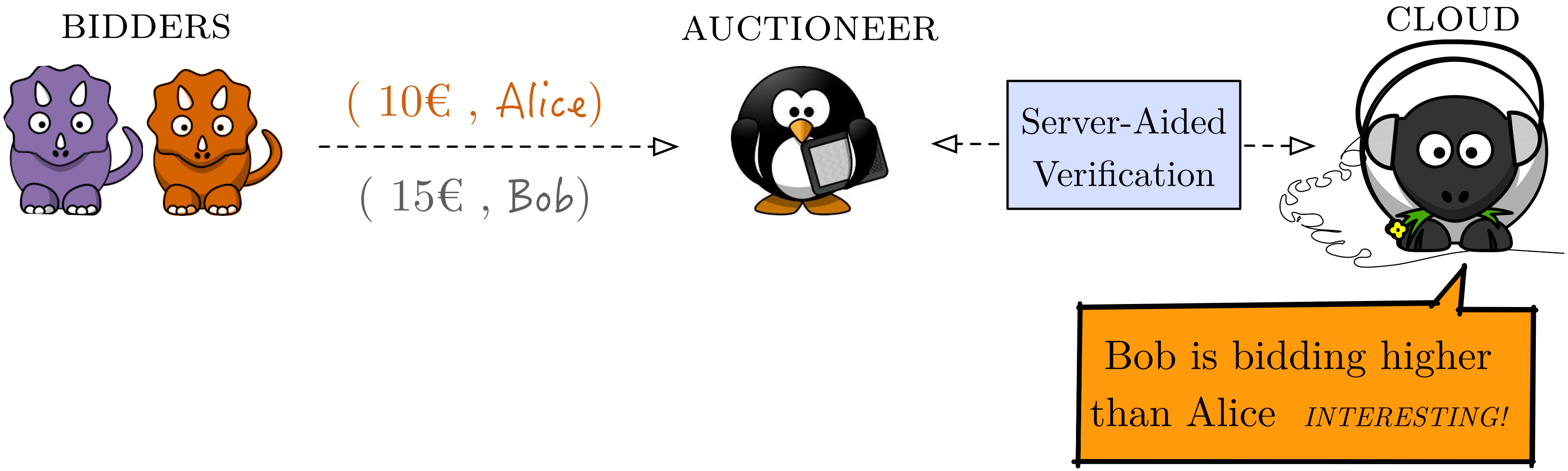


Paper C: Anonymous Single-Round Server-Aided Verification

1. **First generic compiler** for server-aided verification of signatures

2. **Three novel** server-aided verification **schemes**

3. **Introduce** the notion of **signer anonymity**



targeted advertisement / robbery / dating, estimate on bidders' financial situation / interests

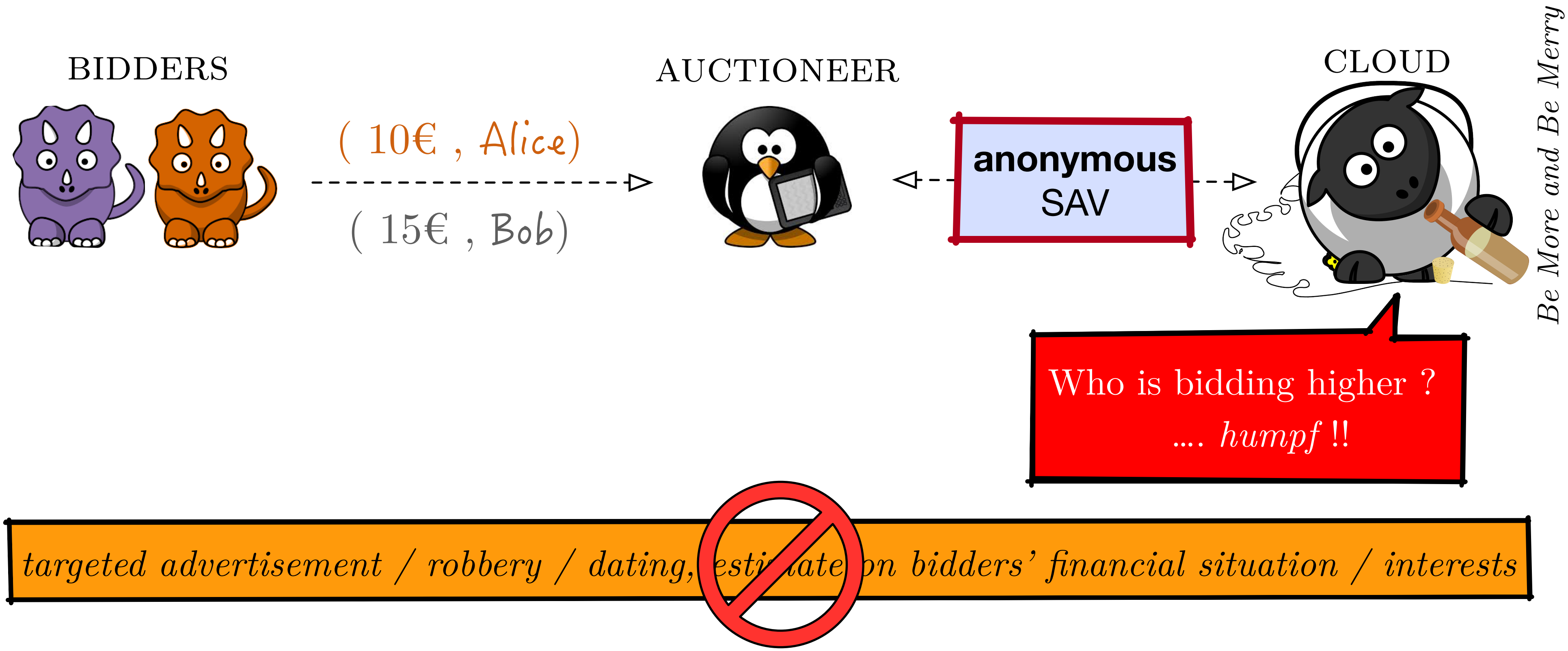
Be More and Be Merry

Paper C: Anonymous Single-Round Server-Aided Verification

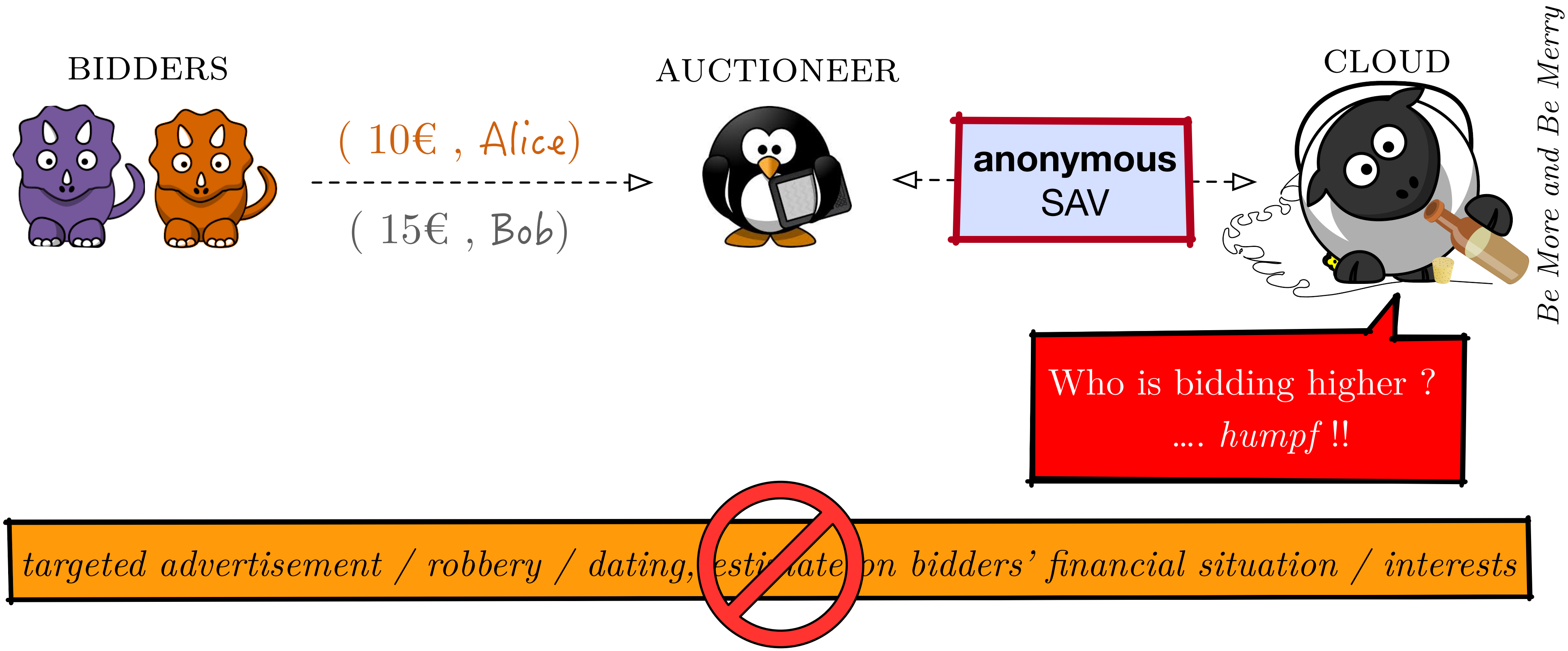
1. **First generic compiler** for server-aided verification of signatures

2. **Three novel** server-aided verification **schemes**

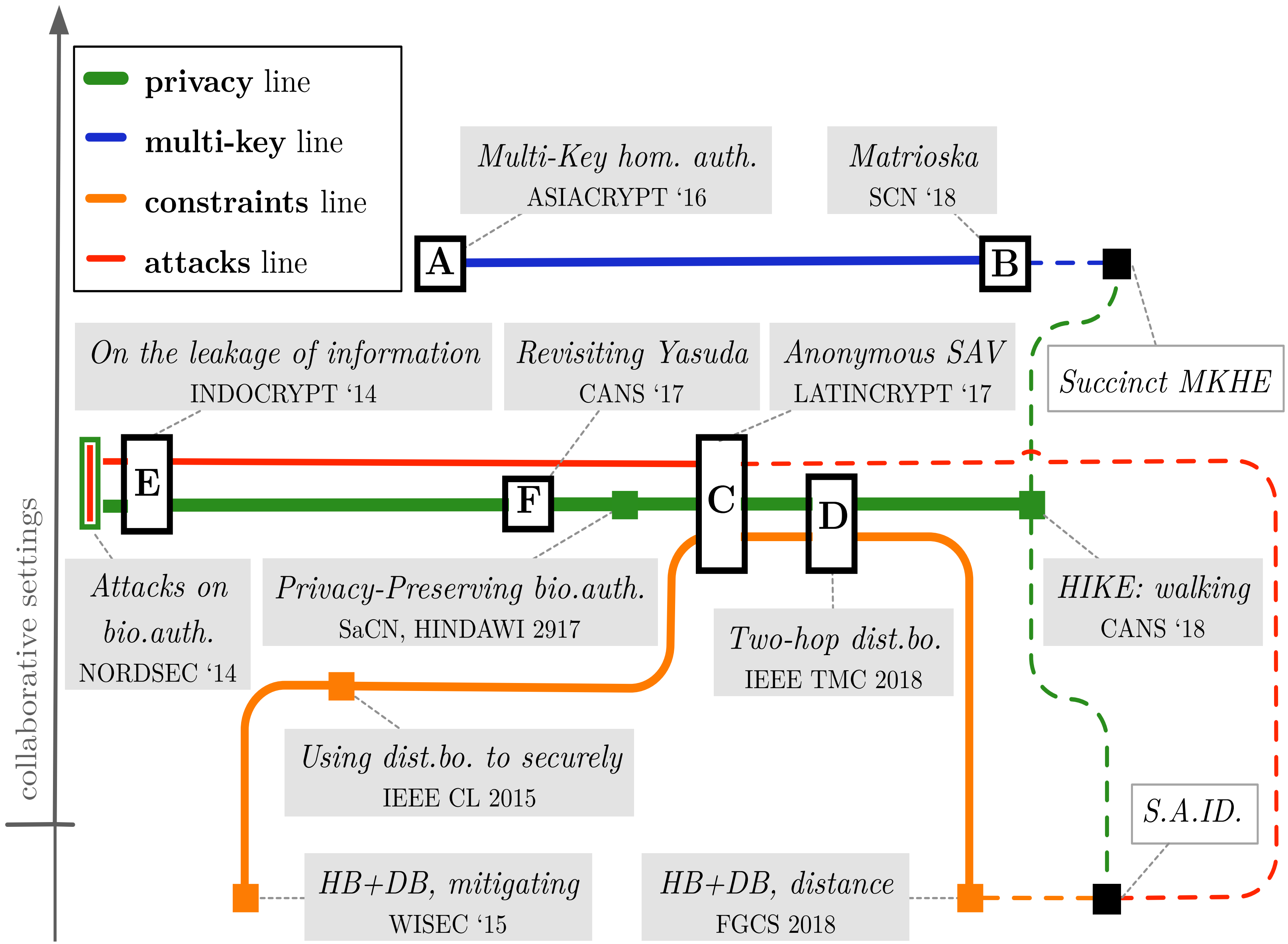
3. **Introduce** the notion of **signer anonymity**



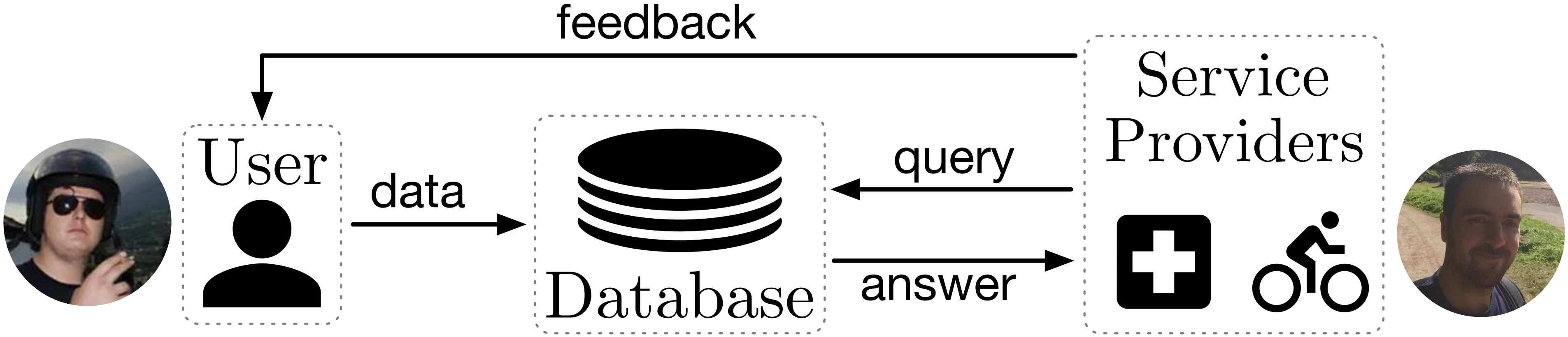
1. **First generic compiler** for server-aided verification of signatures
2. **Three novel** server-aided verification **schemes**
3. **Introduce** the notion of **signer anonymity**



4. **Extended** notion of **unforgeability**



This presentation may contain copyrighted images the use of which has not always been specifically authorized by the copyright owner. I am making the material available for educational purposes only and I believe this constitutes a 'fair use'.



data-secrecy: confidentiality of the clients' data;

token-secrecy: clients have full control on who can decrypt their data (only the intended service providers can decrypt, and no one else);

forgettability: clients can ask for their data to be destroyed.

GDPR-oriented security model

Paper A
Paper B
Paper C
Paper D
Paper E
Paper F

Multi-Key Homomorphic Authenticators

Dario Fiore, Aikaterini Mitrokotsa, Luca Nizzardo, Elena Pagnin

Abstract. Homomorphic authenticators (HAs) enable a client to authenticate a large collection of data elements $m_1, \ldots, m_t$ and outsource them, along with the corresponding authenticators, to an untrusted server. At any later point, the server can generate a *short* authenticator vouching for the correctness of the output y of a function f computed on the outsourced data, i.e., $y = f(m_1, \ldots, m_t)$. Recently researchers have focused on HAs as a solution, with minimal communication and interaction, to the problem of delegating computation on outsourced data. The notion of HAs studied so far, however, only supports executions (and proofs of correctness) of computations over data authenticated by a single user. Motivated by realistic scenarios (ubiquitous computing, sensor networks, etc.) in which large datasets include data provided by multiple users, we study the concept of *multi-key homomorphic authenticators*. In a nutshell, multi-key HAs are like HAs with the extra feature of allowing the holder of public evaluation keys to compute on data authenticated under different secret keys. In this paper, we introduce and formally define multi-key HAs. Secondly, we propose a construction of a multi-key homomorphic signature based on standard lattices and supporting the evaluation of circuits of bounded polynomial depth. Thirdly, we provide a construction of multi-key homomorphic MACs based only on pseudorandom functions and supporting the evaluation of low-degree arithmetic circuits. Albeit being less expressive and only secretly verifiable, the latter construction presents interesting efficiency properties.

Theory and Application of Cryptology and Information Security (ASIACRYPT), 2016.

Paper A

Paper B

Paper C

Paper D

Paper E

Paper F

Matrioska: A Compiler for Multi-Key Homomorphic Signatures

Dario Fiore and Elena Pagnin

Abstract. Multi-Key Homomorphic Signatures (MKHS) enable clients in a system to sign and upload messages to an untrusted server. At any later point in time, the server can perform a computation C on data provided by t different clients, and return the output y and a short signature $\sigma_{C,\mathsf{y}}$ vouching for the correctness of y as the output of the function C on the signed data. Interestingly, MKHS enable verifiers to check the validity of the signature using solely the public keys of the signers whose messages were used in the computation. Moreover, the signatures $\sigma_{C,\mathsf{y}}$ are succinct, namely their size depends at most linearly in the number of clients, and only logarithmically in the total number of inputs of C.

Existing MKHS are constructed based either on standard assumptions over lattices (Fiore *et al.*, ASIACRYPT'16), or on non-falsifiable assumptions (SNARKs) (Lai *et al.*, ePrint'16). In this paper, we investigate connections between single-key and multi-key homomorphic signatures. We propose a generic compiler, called Matrioska, which turns any (sufficiently expressive) single-key homomorphic signature scheme into a multi-key scheme. Matrioska establishes a formal connection between these two primitives and is the first alternative to the only known construction under standard falsifiable assumptions. Our result relies on a novel technique that exploits the homomorphic property of a single-key HS scheme to compress an arbitrary number of signatures from t different users into only t signatures.

Proceedings of the 11th Conference on Security and Cryptography for Networks (SCN), 2018.

Anonymous Single-Round Server-Aided Verification

Elena Pagnin, Aikaterini Mitrokotsa and Keisuke Tanaka

Abstract. Server-Aided Verification (SAV) is a method that can be employed to speed up the process of verifying signatures by letting the verifier outsource part of its computation load to a third party. Achieving fast and reliable verification under the presence of an untrusted server is an attractive goal in cloud computing and internet of things scenarios.

In this paper, we describe a simple framework for SAV where the interaction between a verifier and an untrusted server happens via a single-round protocol. We propose a security model for SAV that refines existing ones and includes the new notions of SAV-*anonymity* and *extended unforgeability*. In addition, we apply our definitional framework to provide the first generic transformation from any signature scheme to a single-round SAV scheme that incorporates verifiable computation. Our compiler identifies two independent ways to achieve SAV-anonymity: *computationally*, through the privacy of the verifiable computation scheme, or *unconditionally*, through the adaptibility of the signature scheme.

Finally, we define three novel instantiations of SAV schemes obtained through our compiler. Compared to previous works, our proposals are the only ones which simultaneously achieve existential unforgeability and soundness against collusion.

Proceedings of Cryptology and Information Security (LATINCRYPT), 2017.

Paper A

Paper B

Paper C

Paper D

Paper E

Paper F

Two-hop Distance-Bounding Protocols: Keep your Friends Close

Anjia Yang, Elena Pagnin, Aikaterini Mitrokotsa, Gerhard P. Hancke and Duncan S. Wong

Abstract. Authentication in wireless communications often depends on the physical proximity to a location. Distance-bounding (DB) protocols are cross-layer authentication protocols that are based on the round-trip-time of challenge-response exchanges and can be employed to guarantee physical proximity and combat relay attacks. However, traditional DB protocols rely on the assumption that the prover (e.g., user) is in the communication range of the verifier (e.g., access point); something that might not be the case in multiple access control scenarios in ubiquitous computing environments as well as when we need to verify the proximity of our two-hop neighbour in an ad-hoc network. In this paper, we extend traditional DB protocols to a two-hop setting i.e. when the prover is out of the communication range of the verifier and thus, they both need to rely on an untrusted in-between entity in order to verify proximity. We present a formal framework that captures the most representative classes of existing DB protocols and provide a general method to extend traditional DB protocols to the two-hop case (three participants). We analyse the security of two-hop DB protocols and identify connections with the security issues of the corresponding one-hop case. Finally, we demonstrate the correctness of our security analysis and the efficiency of our model by transforming five existing DB protocols to the two-hop setting and we evaluate their performance with simulated experiments.

IEEE Transactions on Mobile Computing (2018)

Paper A
Paper B
Paper C
Paper D
Paper E
Paper F

On the Leakage of Information in Biometric Authentication

Elena Pagnin, Christos Dimitrakakis, Aysajan Abidin, Aikaterini Mitrokotsa

Abstract. In biometric authentication protocols, a user is authenticated or granted access to a service if her fresh biometric trait *matches* the reference biometric template stored on the service provider. This matching process is usually based on a suitable *distance* which measures the similarities between the two biometric templates. In this paper, we prove that, when the matching process is performed using a specific family of distances (which includes distances such as the Hamming and the Euclidean distance), then information about the reference template is leaked. This leakage of information enables a *hill-climbing* attack that, given a sample that matches the template, could lead to the full recovery of the biometric template (*i.e.* centre search attack) even if it is stored encrypted. We formalise this "leakage of information" in a mathematical framework and we prove that centre search attacks are feasible for any biometric template defined in $\mathbb{Z}_q^n, (q \geq 2)$ after a number of authentication attempts linear in n. Furthermore, we investigate brute force attacks to find a biometric template that matches a reference template, and hence can be used to run a *centre search attack*. We do this in the binary case and identify connections with the *set-covering* problem and *sampling without replacement*.

Proceedings of the 15th International Conference on Cryptology in India (INDOCRYPT), 2014.

Paper A

Paper B

Paper C

Paper D

Paper E

Paper F

Revisiting Yasuda et al.'s Biometric Authentication Protocol: Are you Private Enough?

Elena Pagnin, Jing Liu, Aikaterini Mitrokotsa

Abstract. Biometric Authentication Protocols (BAPs) have increasingly been employed to guarantee reliable access control to places and services. However, it is well-known that biometric traits contain sensitive information of individuals and if compromised could lead to serious security and privacy breaches. Yasuda *et al.* [3] proposed a distributed privacy-preserving BAP which Abidin *et al.* [1] have shown to be vulnerable to biometric template recovery attacks under the presence of a malicious computational server. In this paper, we fix the weaknesses of Yasuda *et al.*'s BAP and present a detailed instantiation of a distributed privacy-preserving BAP which is resilient against the attack presented in [1]. Our solution employs Backes *et al.*'s [2] verifiable computation scheme to limit the possible misbehaviours of a malicious computational server.

Proceedings of 16th International Conference on Cryptology and Network Security (CANS), 2017.