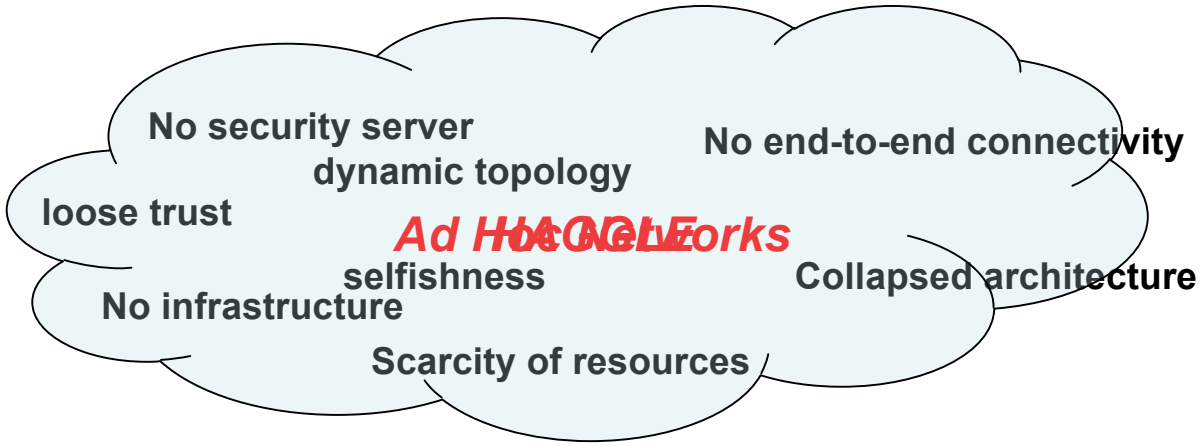
Trusted Communities & Secure Communications

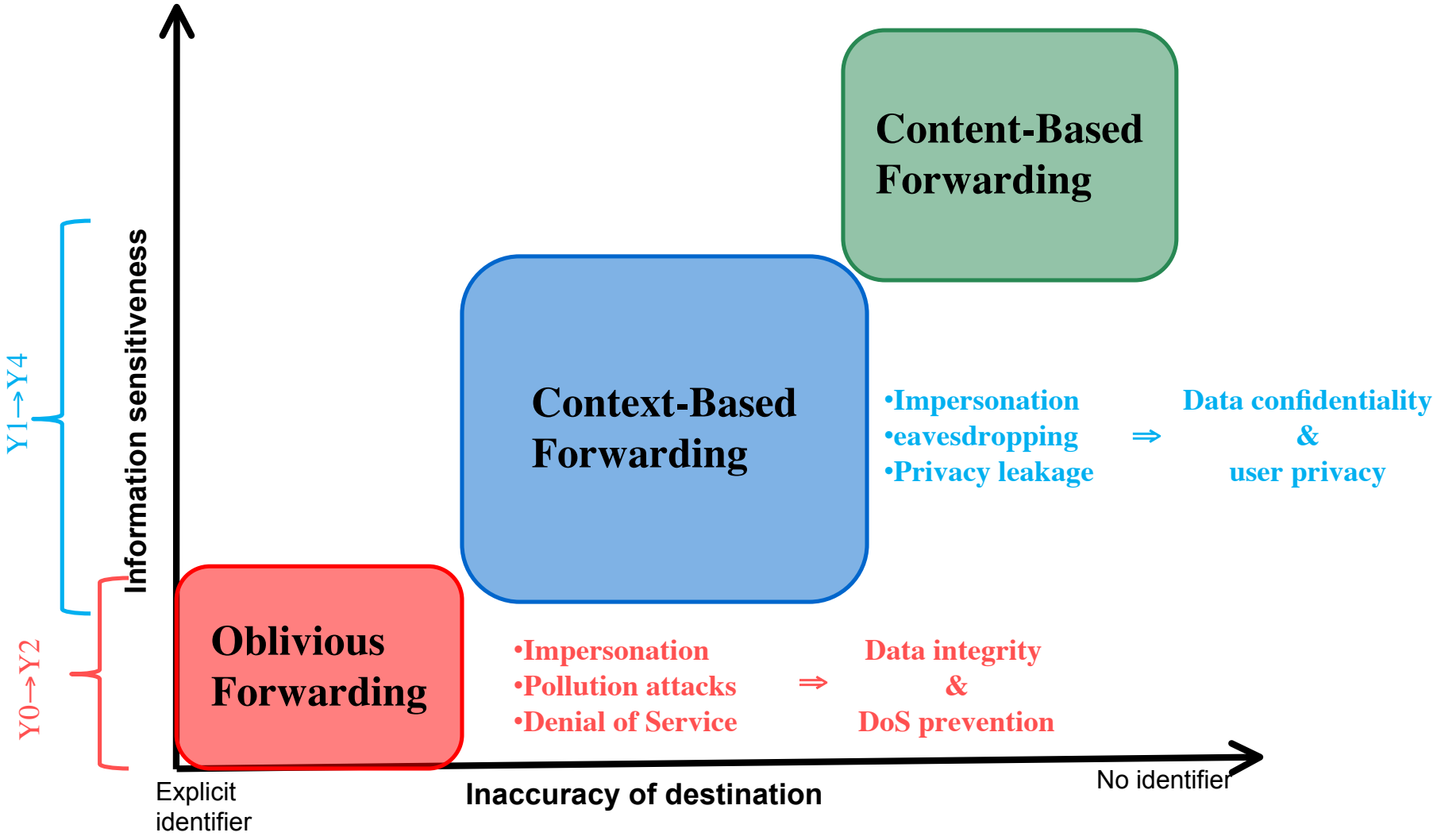
From materials by
Refik Molva, Melek Önen, Abdullatif Shikfa

HAGGLE – New challenges



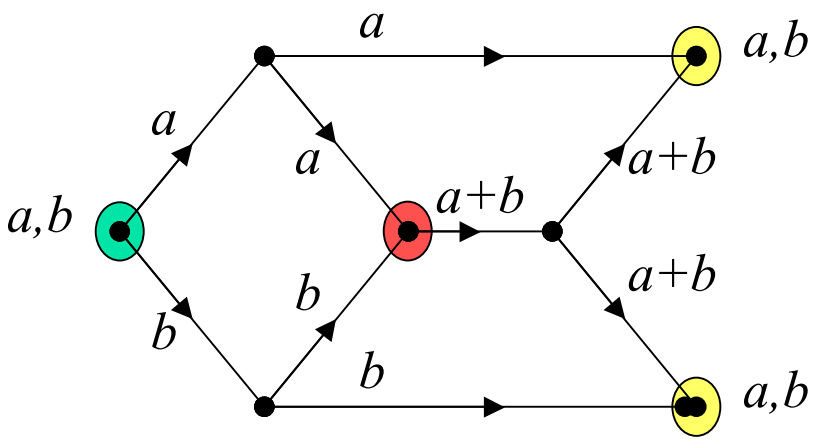
- Security Requirements
  - trust establishment
  - end-to-end confidentiality
  - data integrity
  - Local and self-organizing key management
  - secure and privacy preserving forwarding

Forwarding in HAGGLE: Classification



Network Coding [Alswede et al'00]

- **Example**



sender

receiver

coding node

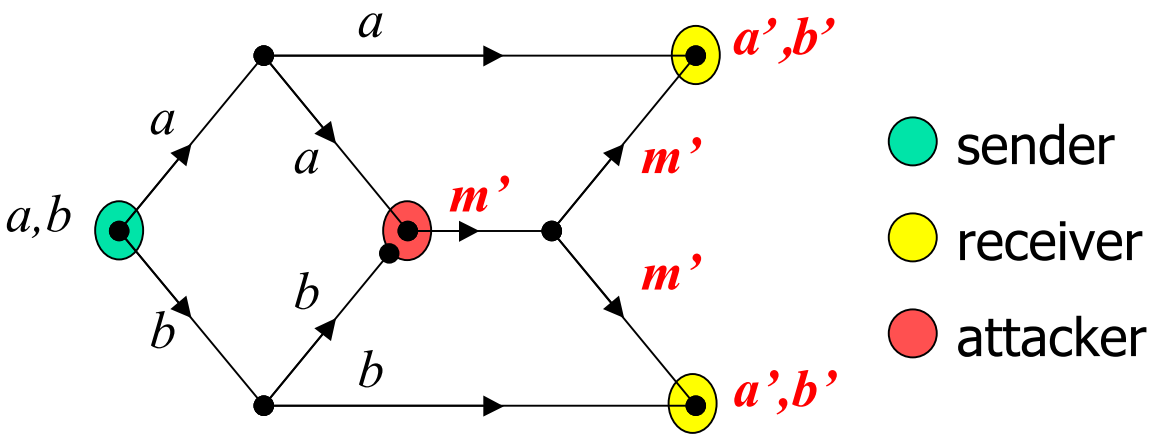
- **Source**
  - **File F=** $b_1b_2b_3\ldots\ldots b_n$
- **Network coding**
  - **e =** $\Sigma c_i b_i$
- **Decoding**
  - **Receive *n* encoded messages**

{(e_1, [c_{1j}]),(e_2, [c_{2j}]),…,(e_n, [c_{nj}])}

  - **Interpolate to retrieve original file**

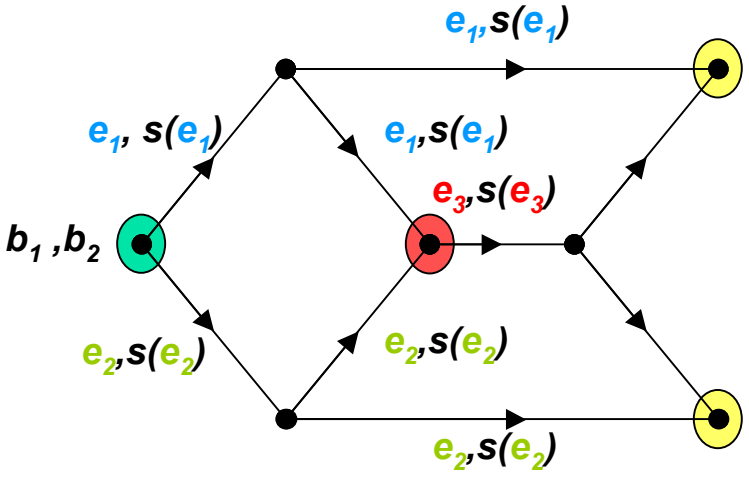
F= $b_1b_2b_3\ldots\ldots b_n$

Pollution Attack



- Single failure ⇒ **global impact**
  - Prevent unauthorized encoding
- GOAL: sign & verify each encoded message ⇒Homomorphism
  - Output encoding: c= αa + βb
  - How to compute s(c) from s(a) and s(b) without knowing the private key of the origin?
  - → Homomorphism (linearity) of s:
    s(c)= s(α.a + β.b)= α ⊗ s(a) ⊕ β ⊗ s(b)

SigNCode: Signatures for Network coding



File F= $b_1 b_2$ S(F)=<$s(b_1), s(b_2)$>

$e_1 = \alpha_1 b_1 + \beta_1 b_2$

$e_2 = \alpha_2 b_1 + \beta_2 b_2$

$e_3 = \gamma_3 e_1 + \delta_3 e_2$

- Source
  - **Encode:** $e_1 = \alpha_1 b_1 + \beta_1 b_2$, $e_2 = \alpha_2 b_1 + \beta_2 b_2$
  - **Sign:** $s(e_1) = s(\alpha_1 b_1 + \beta_1 b_2)$, $s(e_2) = s(\alpha_2 b_1 + \beta_2 b_2)$
- Intermediate node
  - **Verify** $s(e_1)$, $s(e_2)$ **only with Source ID**
  - **Encode** $e_3 = \gamma_3 e_1 + \delta_3 e_2 \Rightarrow e_3 = \alpha_3 b_1 + \beta_3 b_2$
  - **Compute** $s(e_3) = \gamma_3 s(e_1) + \delta_3 s(e_2) \Rightarrow s(e_3) = s(\alpha_3 b_1 + \beta_3 b_2)$
- Receivers
  - **Verify** $\{s(e_i)\}$
  - **Decode** $\Rightarrow b_1, b_2$

ID based ⇒ No need to transmit S(F)

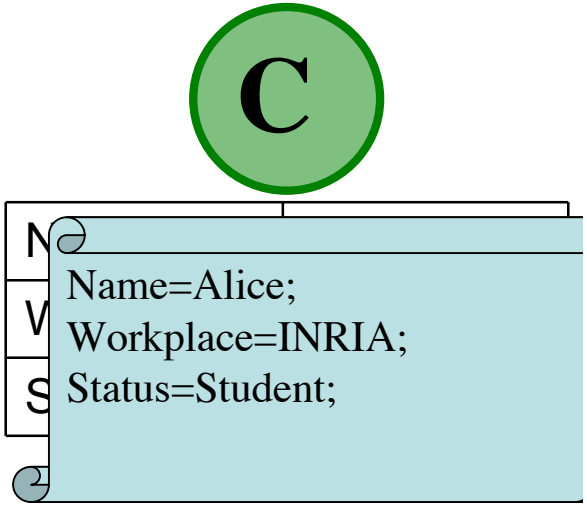
Bilinear maps ⇒ Homomorphism

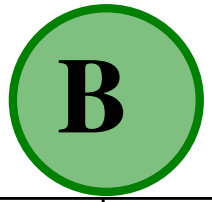
Proof by reduction based on CDH

Context based forwarding

Matching ratio: 2/3
⇒ B is not a destination

Matching ratio: 1
⇒ A is a destination





Name	Bob
Workplace	INRIA
Status	Student

Name	Alice
Workplace	INRIA
Status	Student

Matching ratio: 1/3
⇒ D is not a destination

Name	Dan
Workplace	EURECOM
Status	Student

Security Requirements

- Data Confidentiality (Payload)
  - End-to-end encryption without explicit destination
  - Public encryption function : Anyone can encrypt
  - Multi-user setting
  - Private decryption function: only destination can decrypt

  ⇒ dedicated Multiple id based encryption (MIBE)

Workplace=EURECOM;
Status=Faculty;
Payload=ε(“Haggle Review”)

- User privacy (header)
  - Public and randomized encryption function
  - discover matching attributes
  - restricted verification

  ⇒ new privacy preserving forwarding mechanism

Workplace=ε(EURECOM);
Status= ε(Faculty);
Payload=ε(“Haggle Review”)

Privacy/trust Models

[Shikfa,Önen,Molva WON'09]

- Privacy oblivious
  - Full trust on all forwarding nodes
  - Match? ⇒ forward

  ⇒ No privacy, No encryption

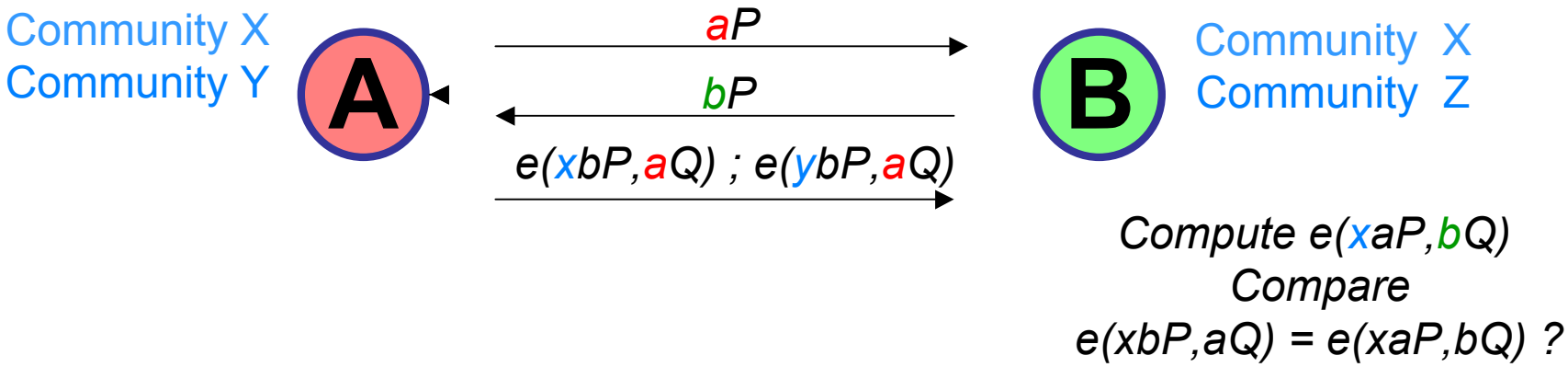
- Intra-community privacy
  - Community based trust
  - Decrypt ⇒ lookup, match?⇒ encrypt⇒ forward

  ⇒ Secure handshake, Group key management

- Full privacy
  - No trust on any intermediate node
  - Forward based on encrypted information

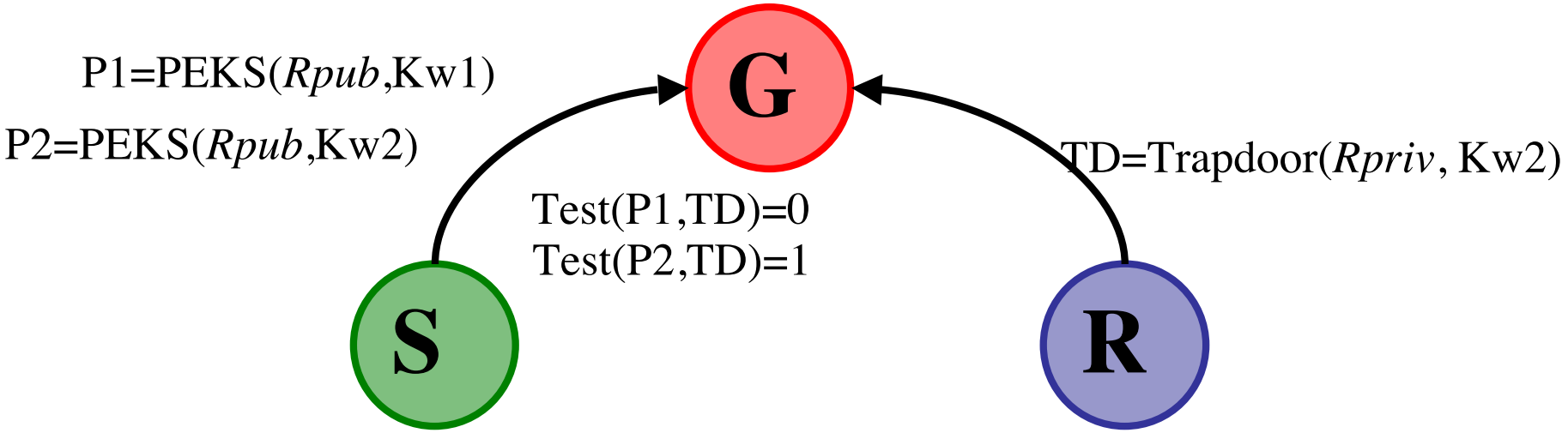
  ⇒ Dedicated encryption mechanism, key management

Model 2: Secure Handshake, secret matching [Sorniotti,Molva IFIPSEC'09]



- Goal: only reveal membership to X
- Our solution: Secret matching with bilinear pairings
  - "bilinear" $\Rightarrow e(aP,bQ)=e(bP,aQ)=e(P,Q)^{ab}$
  - Hard problems
    - *ECDLP* : given <*P,aP*> **find** *a*
    - *CDHP :* given <*P,aP,bP*> **find** *abP*

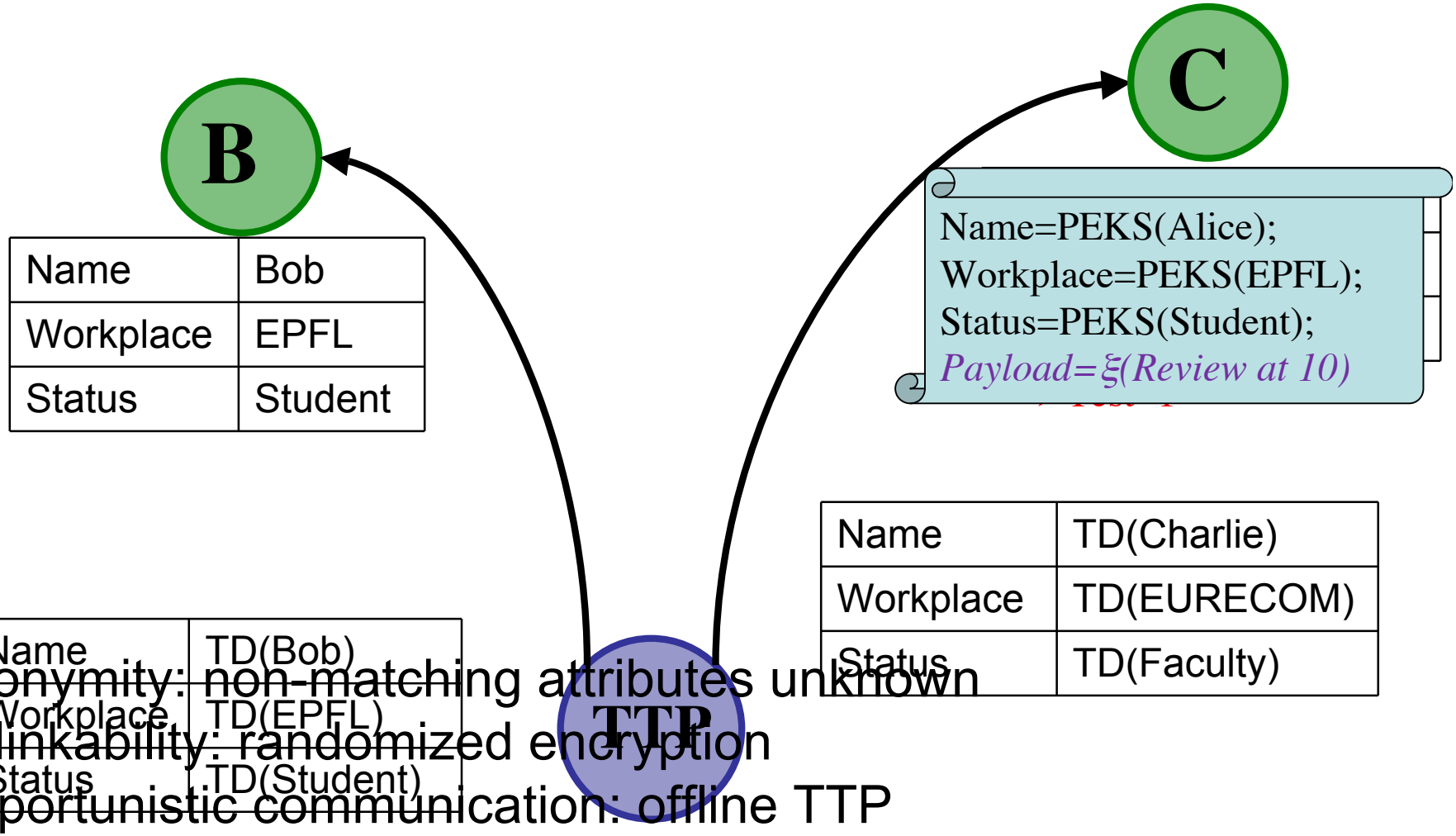
Searchable encryption for secure context based forwarding



- Searchable encryption vs secure context based forwarding
  - PEKS : header encryption
  - Trapdoor: matching capability
  - Test : matching operation

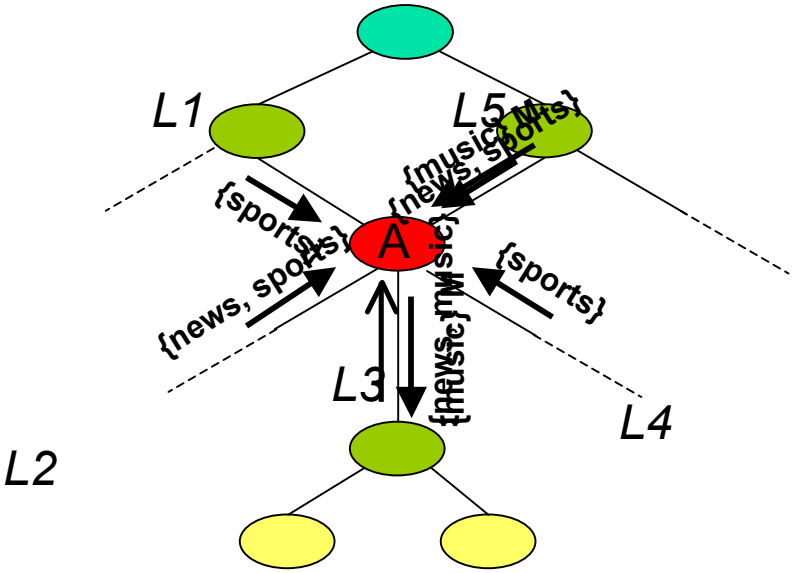
- Conflict with HAGGLE
  - Specific destination
  - Trapdoor distribution

Searchable encryption for secure forwarding



- Anonymity: non-matching attributes unknown
- Unlinkability: randomized encryption
- Opportunistic communication: offline TTP

Content Based Forwarding



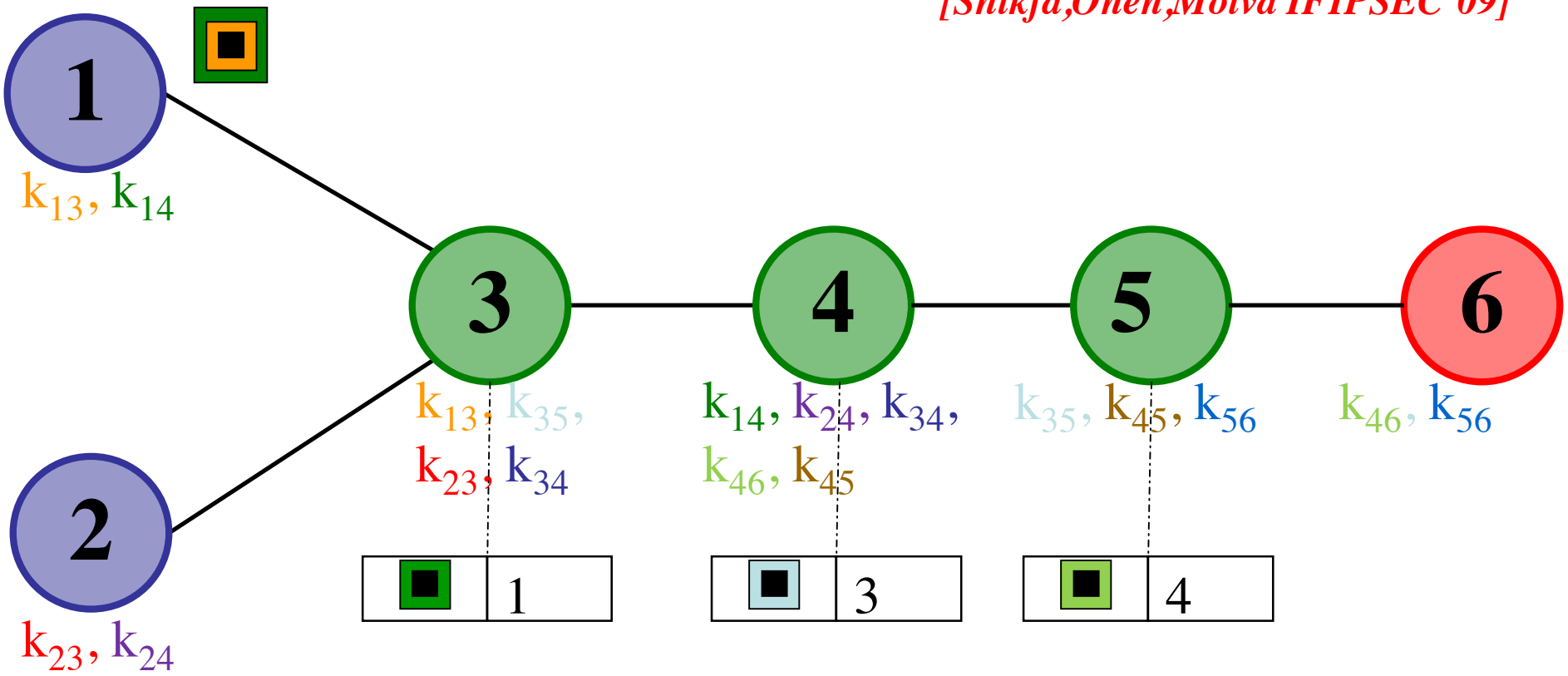
news, sports	*L2, L5*
music, news	*L3*
sports	*L4, L1*

Forwarding Table of A

- Privacy & Confidentiality ⇒ Encryption
- Haggle : opportunistic, Application=Network
- New primitives:
  - Encrypted Interest ⇒ Secure Setup of forwarding tables & Secure Aggregation
  - Encrypted Content ⇒ Secure Lookup

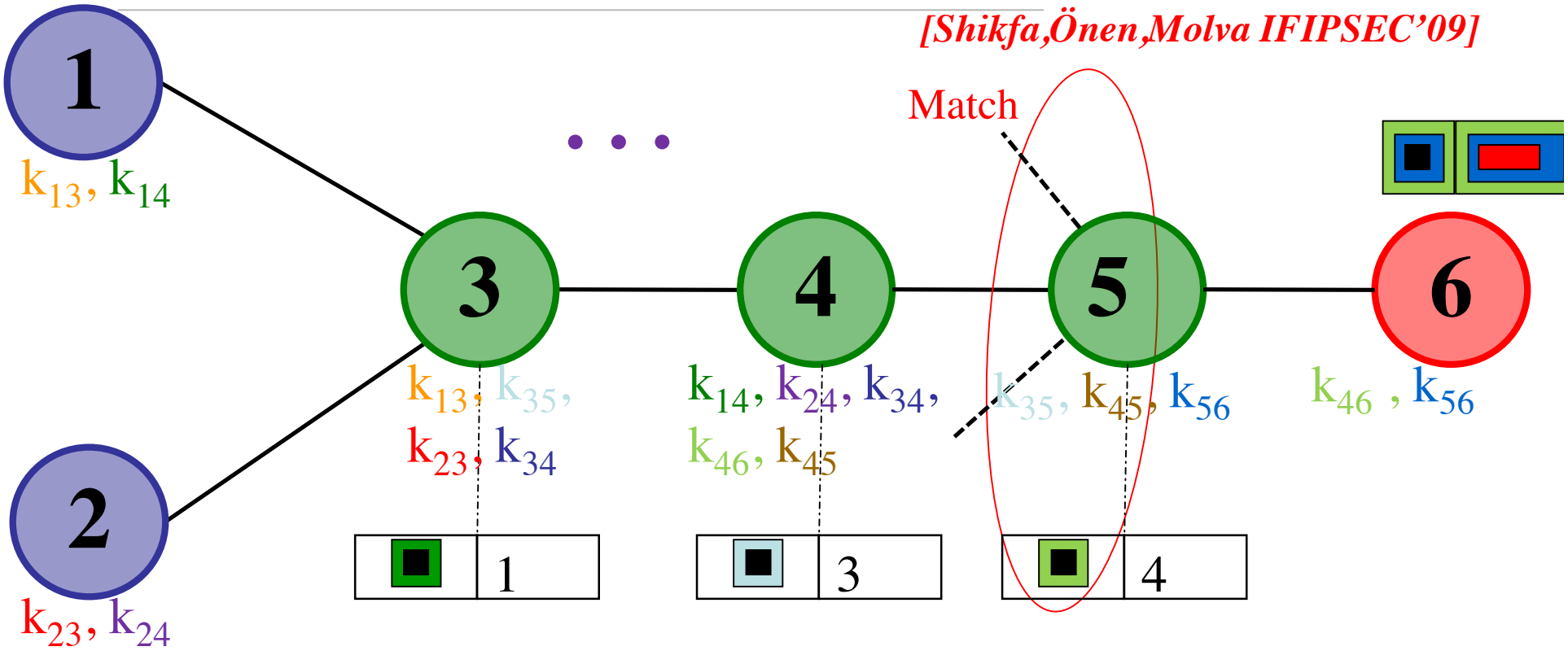
Secure content based forwarding with multiple layer encryption

[Shikfa,Önen,Molva IFIPSEC'09]



- Encryption ⇒ confidentiality and privacy
- Multiple-layer encryption ⇒ easy re-encryption without access on the content
- local key management ⇒no end-to-end security
- Commutative encryption ⇒ secure lookup (Pohlig - Hellman)

Secure content based forwarding with multiple layer encryption



- Encryption ⇒ confidentiality and privacy
- Multiple-layer encryption ⇒ easy re-encryption without access on the content
- local key management ⇒no end-to-end security
- Commutative encryption ⇒ secure lookup (Pohlig - Hellman)

Conclusion: HAGGLE & Security

- Comprehensive study of security issues
  - No end-to-end connectivity, collapsed architecture

  ⇒ New security challenges

- Complete security toolkit
  - Secure Oblivious forwarding
    - Vulnerabilities in epidemic forwarding
    - SignCode : Homomorphic signatures for network coding
  - Secure context based forwarding
    - Data confidentiality: multiple id based encryption
    - User privacy: searchable encryption
  - Secure content based forwarding
    - Confidentiality & Privacy: Multi layer commutative encryption
    - Key management: local and self-organizing

- Prototype: Security Manager
  - Attribute Certificates
  - Secure Community based forwarding