KU LEUVEN

Practically usable Identity Based Encryption for Online Social Networks

Bringing privacy control to Facebook users

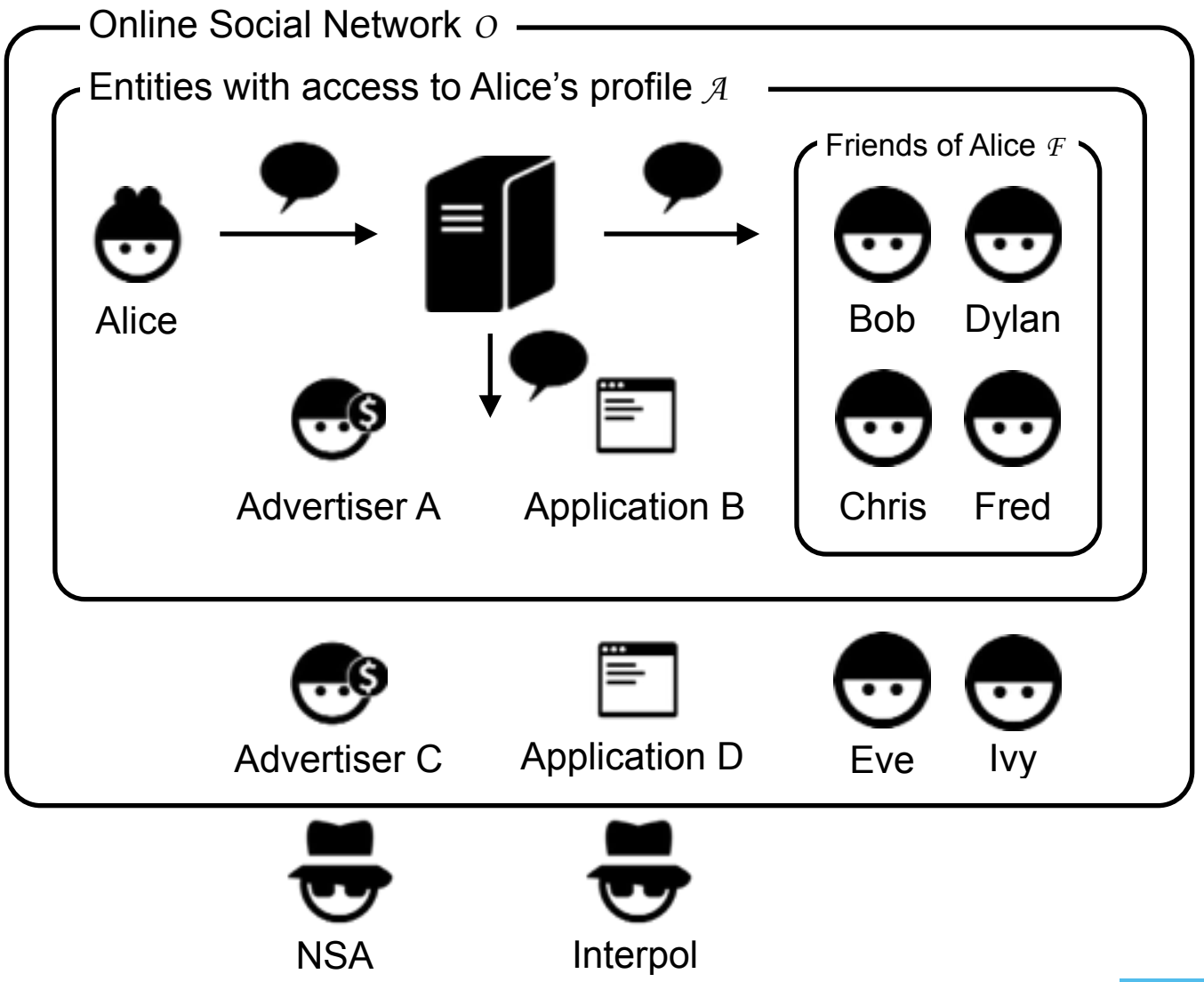

Our Mission:
To make the world more open and connected

Current Situation

The model as it is today

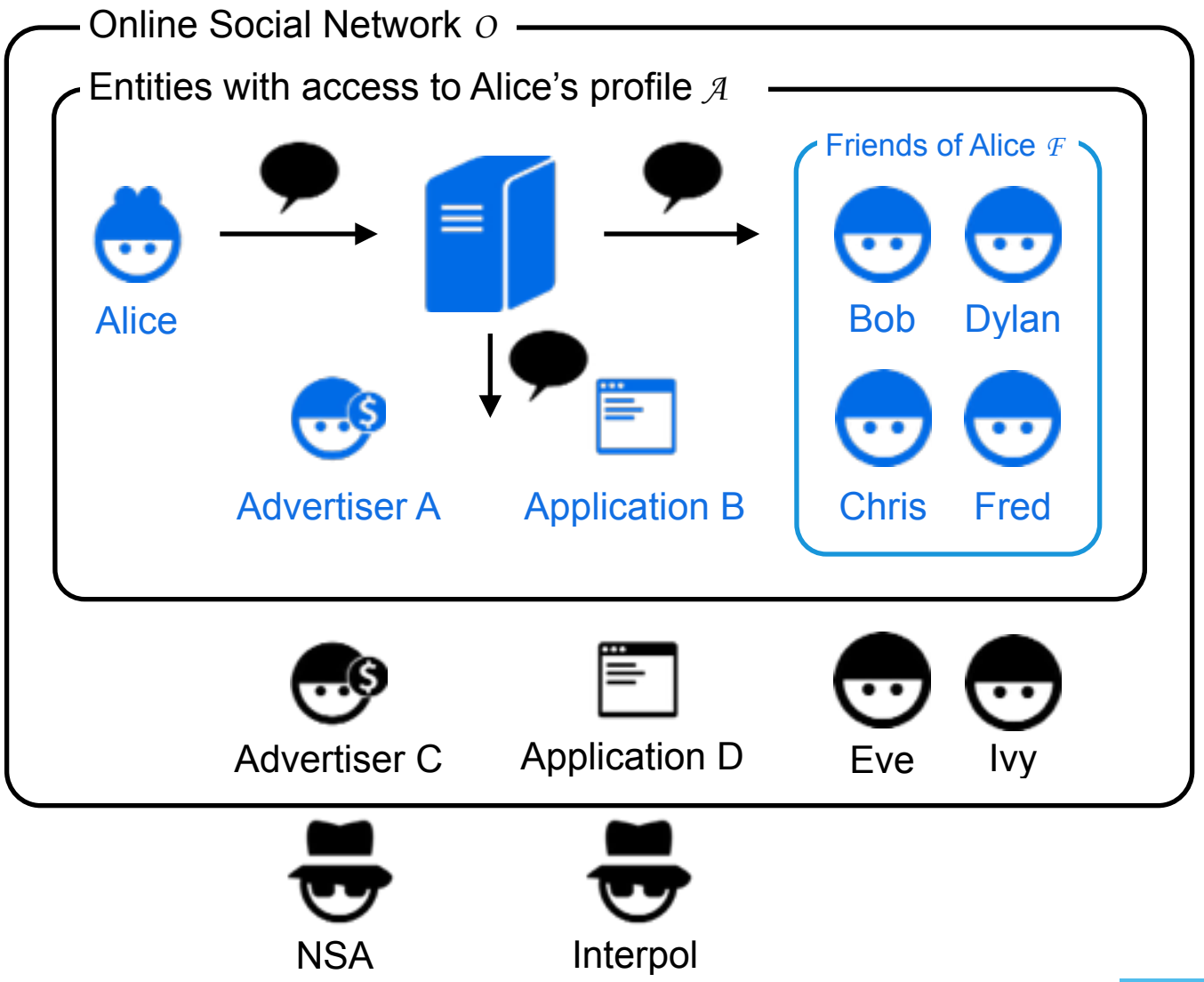
KU LEUVEN

Model of the current situation



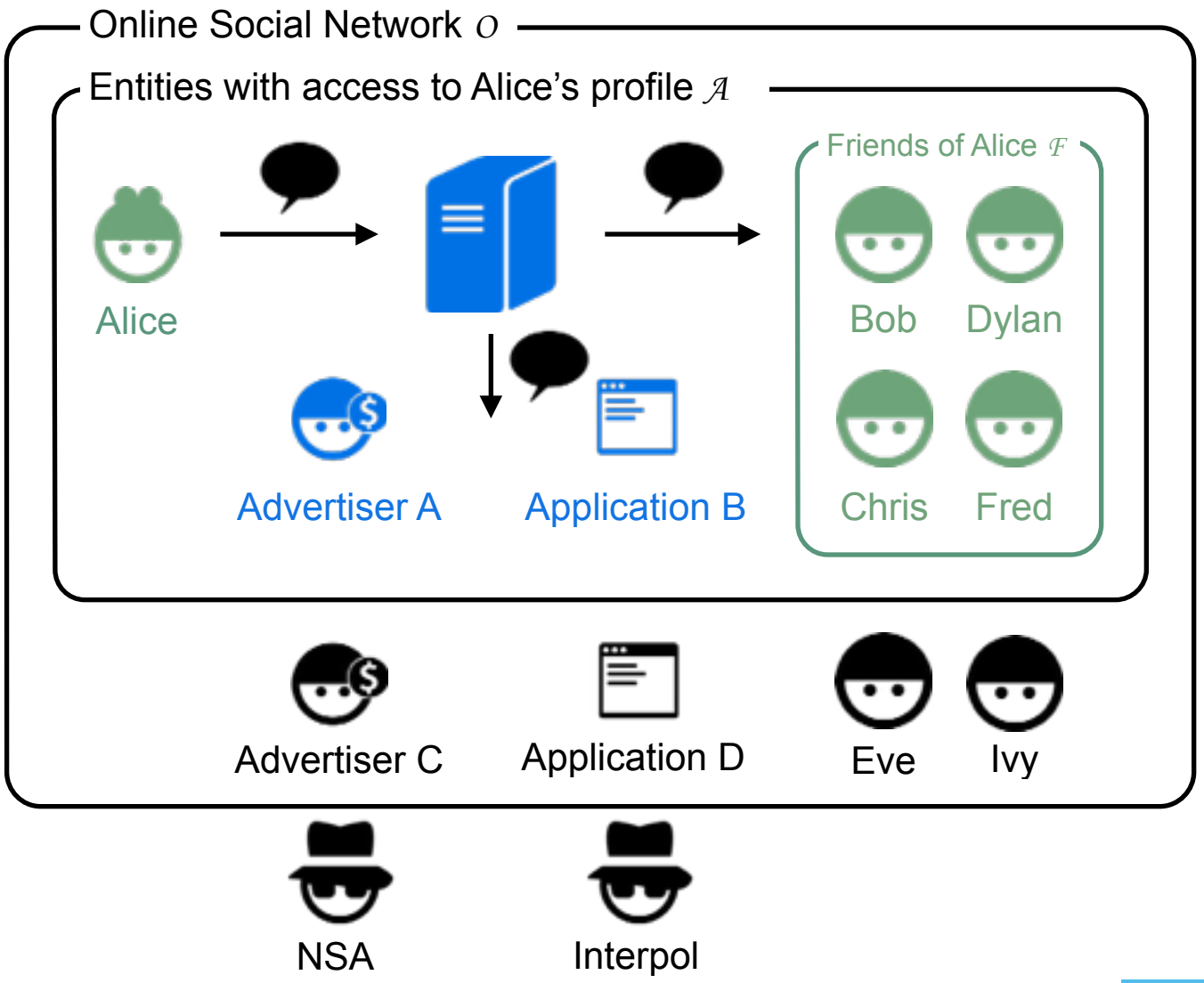
KU LEUVEN

Current situation - Who can read the message



KU LEUVEN

Current situation - What Alice expects



KU LEUVEN

KU LEUVEN

Issues with the current situation

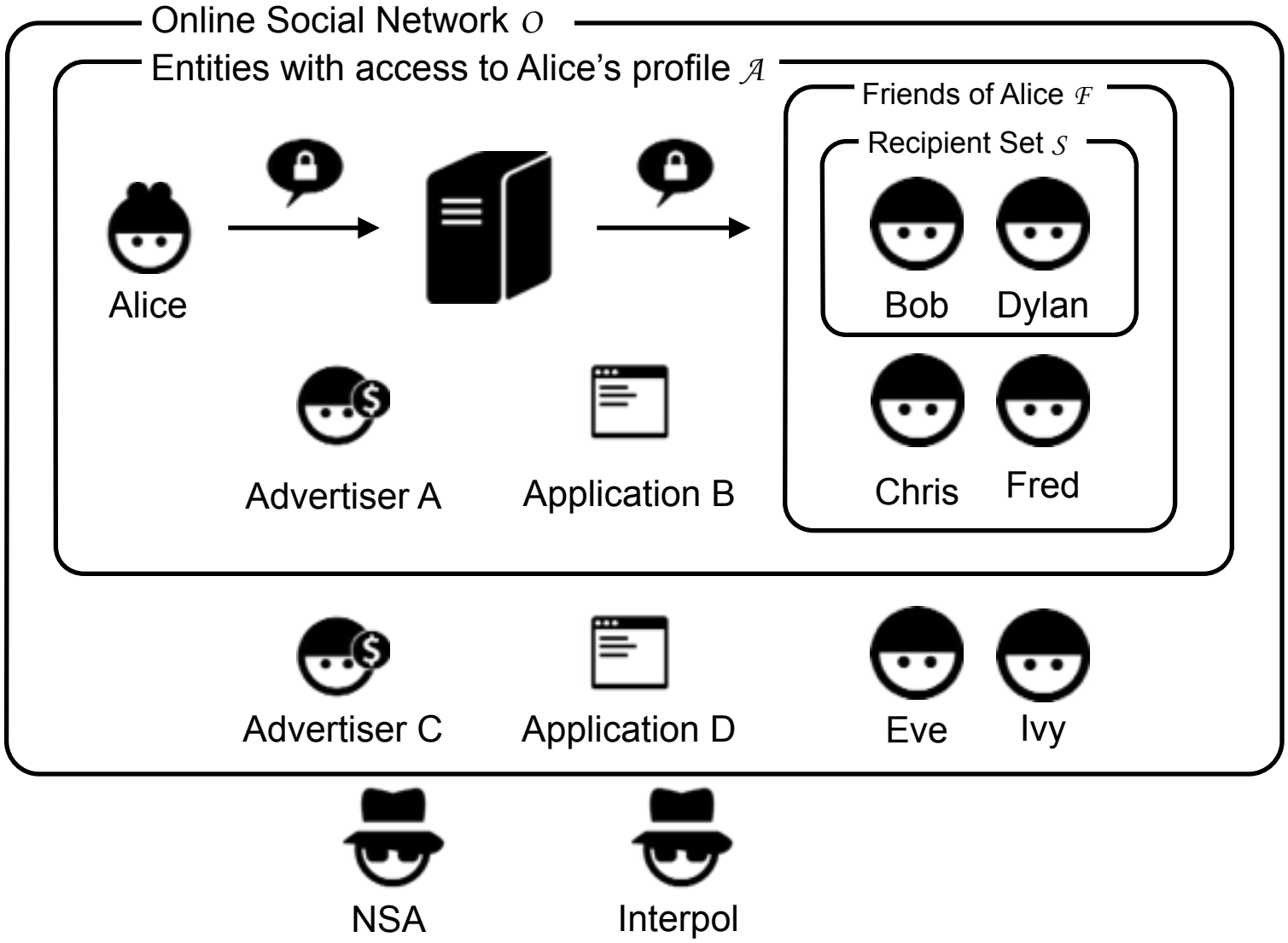
- OSN stores all data
- User has to rely on the privacy features and policies the OSN offers
  - Subject to changes
  - Average user does not read this
- OSN has a corporate mentality

Utopia

The model as it should be

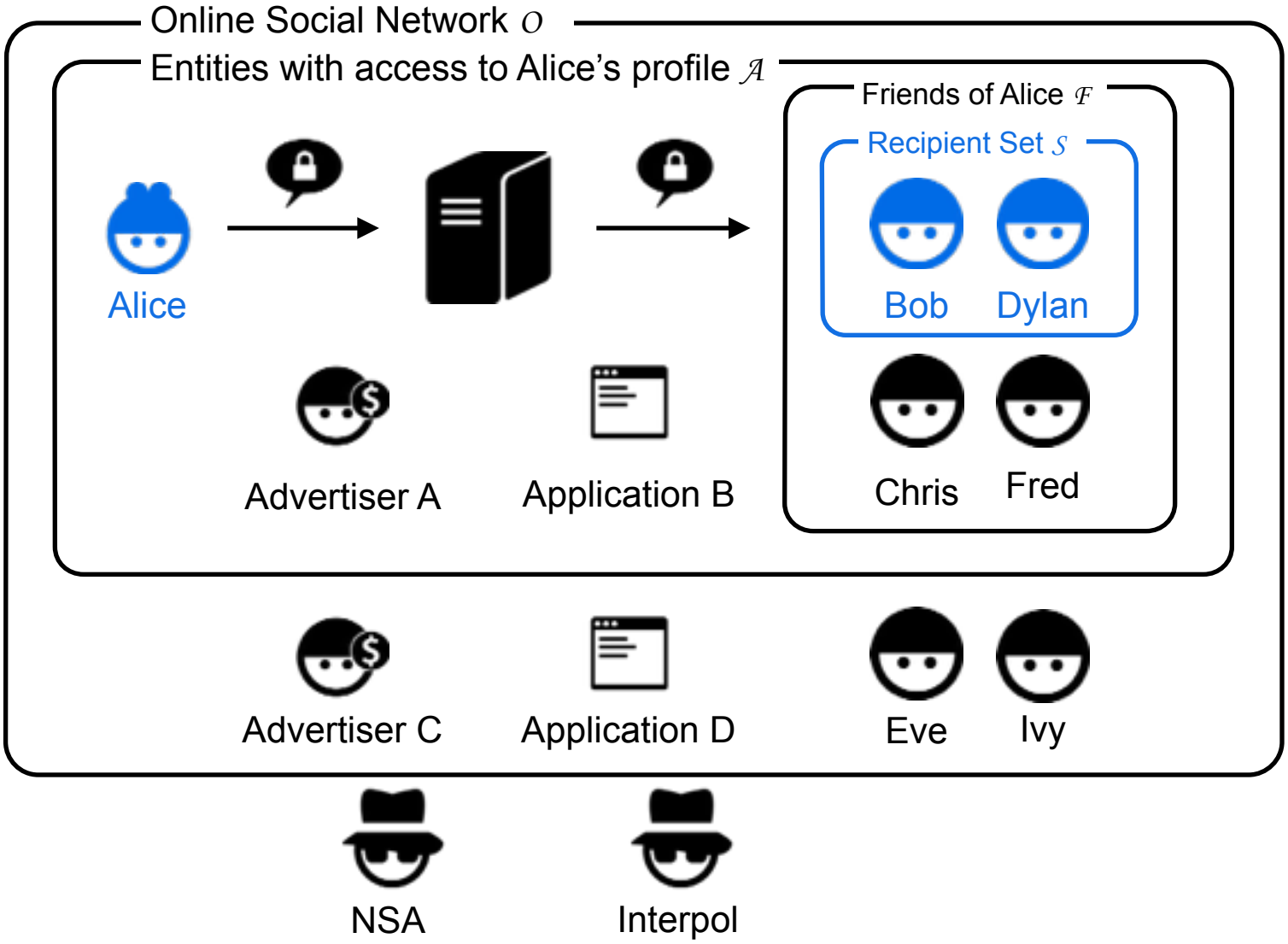
KU LEUVEN

Desired Security Model



KU LEUVEN

Desired Security Model



KU LEUVEN

Design Goals

- The OSN environment should not be altered
- An average OSN user should be able to use it
- As soon as the user is subscribed to the OSN, every other user can start sending him encrypted messages
- The encrypted message should be only posted once to reach all intended recipients
- Keys should be easily memorisable
- Users not necessarily need to be friends to see each other's updates

Security Goals

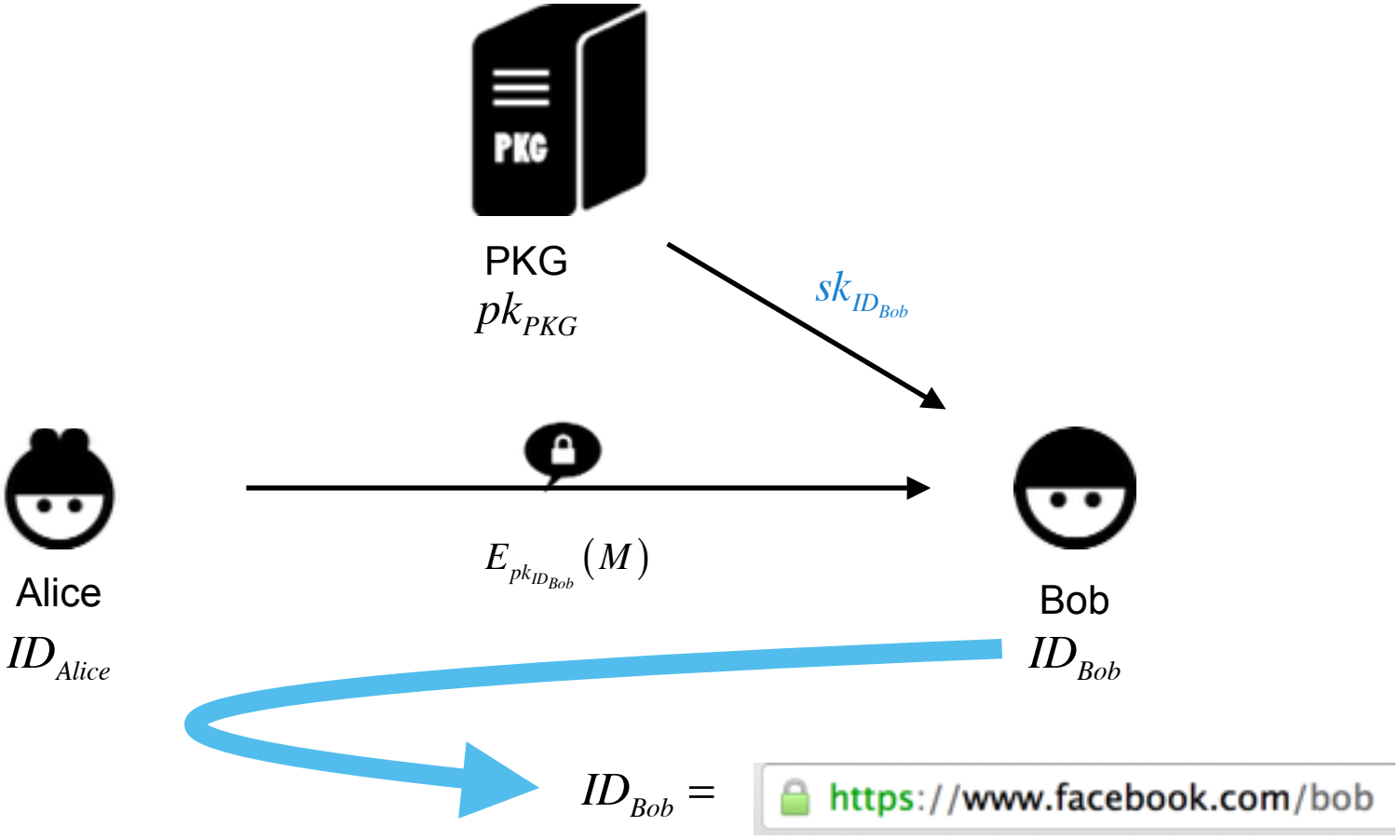
- Confidentiality
- (Outsider) Recipient Anonymity
  - Only authorised recipients are aware of the members in the recipient set S
- Data Integrity and authenticity

Implementation

How Utopia can be realised

KU LEUVEN

Identity-Based Encryption



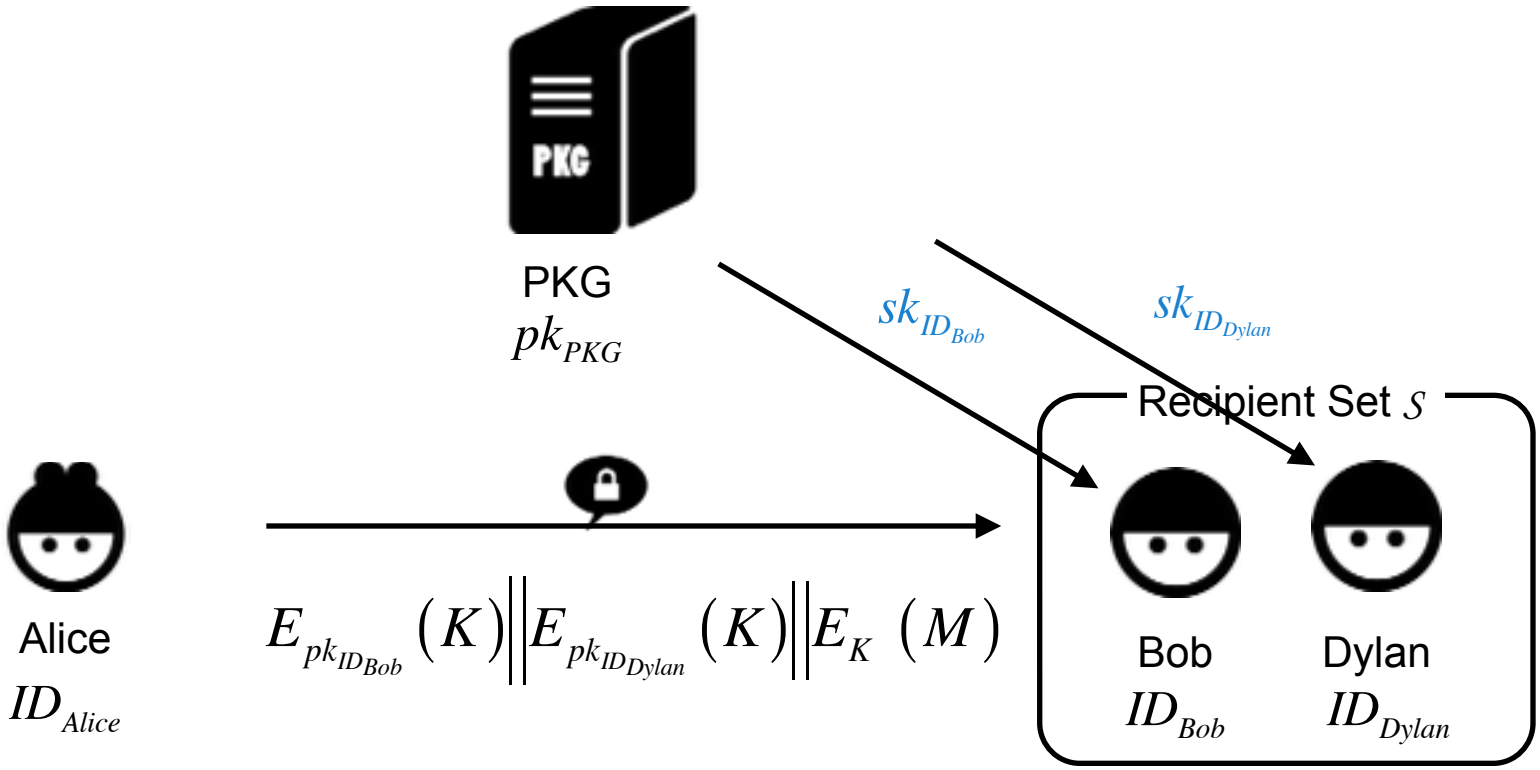
Issues

- Key escrow with regards to the PKG
- No revocation mechanism

Solutions

- Multiple PKGs could use secret sharing techniques
  - Using an (n,t)-Distributed Key Generation protocol
- Append an expiration date such that the public key becomes $ID_{Bob} \| date$ or use a tree based revocation system as proposed by Boldyreva, Goyal and Kumar (6)

Anonymous Identity-Based Broadcast Encryption



Issues

- Receivers should decrypt in a trial and error fashion

Solutions

- Append a hint so that only the intended recipient knows where his ciphertext is

Concrete Proposal

KU LEUVEN

Known Schemes for Anonymous Broadcast Encryption

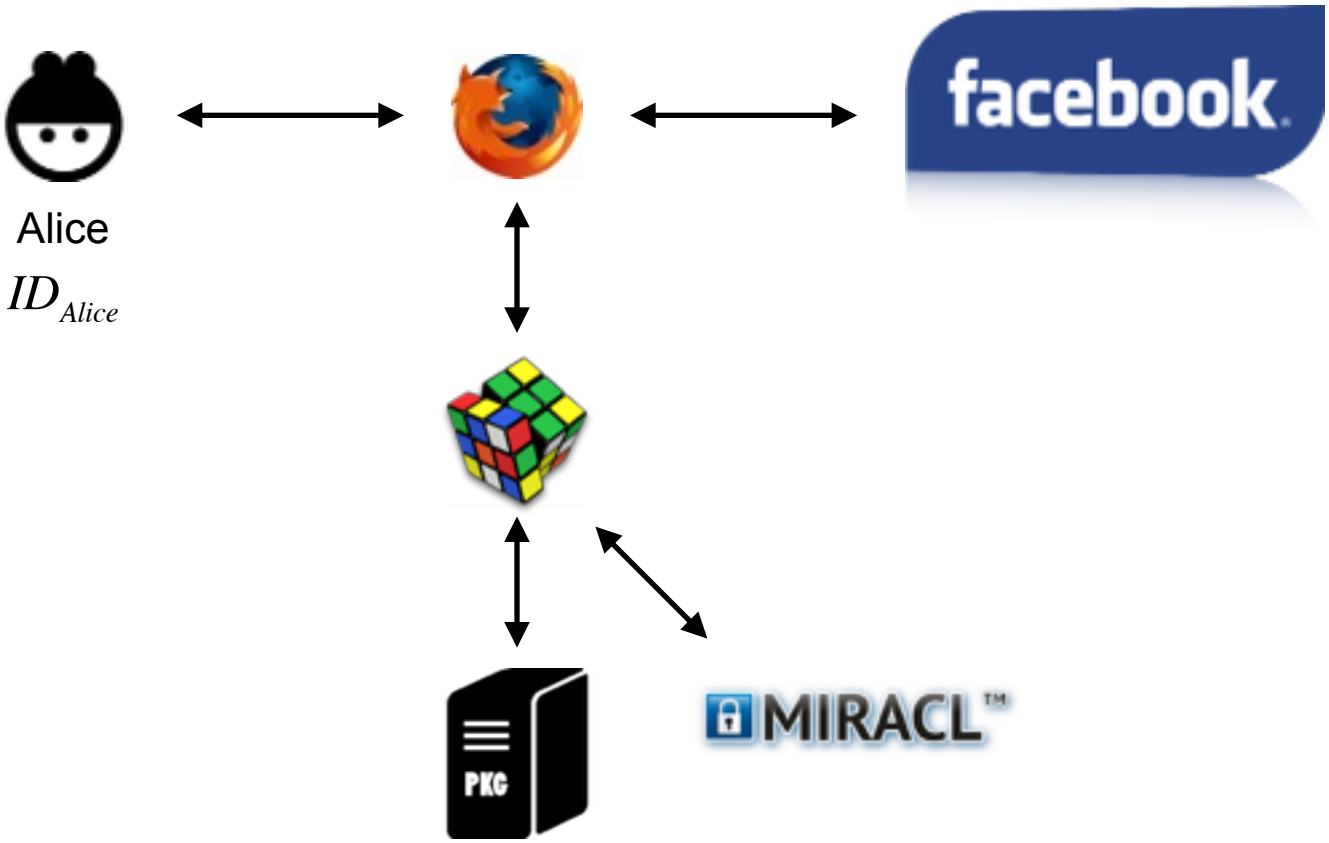
Paper	Public master key (PKG)	Secret Key	Ciphertext	Decryption Attempts	Pro's and Con's
Fazio and Perera [4]	O(N)	O(log N)	O(r log(N/r))	1	- IBE can not be used for any key
Barth, Boneh and Waters [5]	**Dependent on underlying encryption**	**O(1)**	**O(S)**	**1**	**- Random oracle assumption**
Libert, Patterson and Quaglia [2]	O(N) and dependent on encryption	O(1)	O(S)	1	+ Secure in standard model

Revocation Techniques

Author of paper	Revocation Mechanism	Advantages	Disadvantages
Boneh and Franklin [1]	Append expiration date to public key	Only pk||expiry_date gets compromised	No forward secrecy
Boldyreva, Goyal and Kumar [6]	Use ID-based efficient tree revocation	Forward secrecy	Revoked users can never re-use their public key

Implementation

- Use Facebook identifier concatenated with an expiry date as a public key
- Use the IBE scheme as proposed by Gentry [3] for encryption
  - Shorter public parameters than original IBE scheme from Boneh and Franklin [1]
  - No linear dependency on the number of users for the public master key of the PKG
- Use the broadcast encryption scheme from Barth, Boneh and Waters [5]


Alice
ID_{Alice}
facebook
PKG
MIRACL™

In Comparison with Existing Solutions

Name of Solution	Method	Disadvantages
flyByNight	Classic asymmetric crypto with a database for key storage	- Uses Facebook interface for key management - Stores encrypted (based on rememberable password) private keys in a database to increase usability
Persona	Uses Attribute Based Encryption	- Complex infrastructure to broadcast user defined groups - ABE is 100 times more inefficient than RSA
FaceCloak	Replace message text with random Wikipedia citations, store original content encrypted on server	- Trusted flyByNight server that manages keys
Scramble!	Based on Open PGP	User has to rely on chain of trust
Scramble! with IBE (proposed solution)	IBE infrastructure with secret sharing for the PKGs	No revocation possible

Current Status and Planning

- First semester
  - ✓ Reading and gathering background knowledge
  - ✓ Proposing a concrete architecture
  - ✓ Intermediate presentation
- Second semester
  - Implementation (2 months)
    - Single user, single PKG
    - Multiple users, single PKG
    - (optional) Multiple users, multiple PKGs?
  - Writing (1 month)
    - Thesis text
    - Article

Questions?

KU LEUVEN

References

(1) D. Boneh and M. K. Franklin, “Identity based encryption from the Weil pairing,” *IACR Cryptology ePrint Archive*, vol. 2001, p. 90, 2001.

(2) B. Libert, K. G. Paterson, and E. A. Quaglia, “Anonymous broadcast encryption: Adaptive security and efficient constructions in the standard model,” in *Public Key Cryptography, ser. Lecture Notes in Computer Science*, M. Fischlin, J. Buchmann, and M. Manulis, Eds., vol. 7293. Springer, 2012, pp. 206–224.

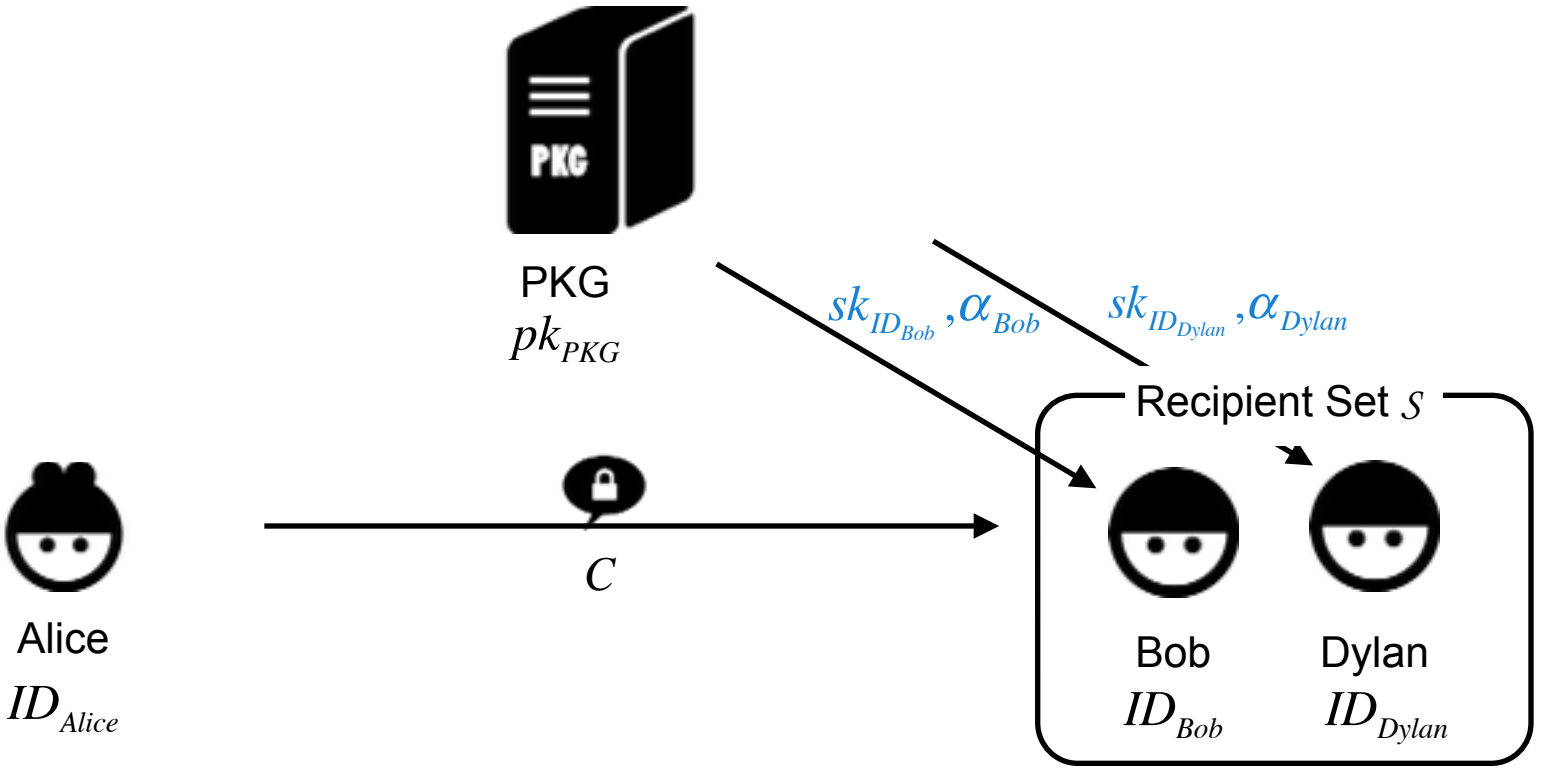
(3) C. Gentry, “Practical identity-based encryption without random oracles,” in *Advances in Cryptology - EUROCRYPT 2006*, ser. Lecture Notes in Computer Science, S. Vaudenay, Ed. Springer Berlin Heidelberg, 2006, vol. 4004, pp. 445–464

(4) N. Fazio and I. M. Perera, “Outsider-anonymous broadcast encryption with sublinear ciphertexts,” *IACR Cryptology ePrint Archive*, vol. 2012, p. 129, 2012.

(5) A. Barth, D. Boneh, and B. Waters, “Privacy in encrypted content distribution using private broadcast encryption,” in *Financial Cryptography*, ser. Lecture Notes in Computer Science, G. D. Crescenzo and A. D. Rubin, Eds., vol. 4107. Springer, 2006, pp. 52–64.

(6) A. Boldyreva, V. Goyal, and V. Kumar, “Identity-based encryption with efficient revocation,” *IACR Cryptology ePrint Archive*, vol. 2012, p. 52, 2012.

Anonymous Identity-Based Broadcast Encryption by Barth, Boneh and Waters [5]



$$C = \sigma \| g^r \| H\left(g^{r\alpha_{Bob}}\right) \| E_{pk_{ID_{Bob}}}\left(vk \| g^{r\alpha_{Bob}} \| K\right) \| H\left(g^{r\alpha_{Dylan}}\right) \| E_{pk_{ID_{Dylan}}}\left(vk \| g^{r\alpha_{Dylan}} \| K\right) \| E_K\left(M \| ID_{Bob} \| ID_{Dylan}\right)$$

$$\sigma = Sig_{sk}\left\{ g^r \| H\left(g^{r\alpha_{Bob}}\right) \| E_{pk_{ID_{Bob}}}\left(vk \| g^{r\alpha_{Bob}} \| K\right) \| H\left(g^{r\alpha_{Dylan}}\right) \| E_{pk_{ID_{Dylan}}}\left(vk \| g^{r\alpha_{Dylan}} \| K\right) \| E_K\left(M \| ID_{Bob} \| ID_{Dylan}\right) \right\}$$