An efficient certificat-less key management architecture

Fifteenth International Workshop on
Algebraic and Combinatorial Coding Theory

Abderrahman Daif - Cédric Tavernier

Paris 8 university - Assystem - The laboratory LAGA

20 June 2016

1 Introduction

2 Public key infrastructure (PKI)

3 Identity based cryptography

4 The proposed solution

5 To summarize

A key management architecture refers to the technical mechanisms, procedures and policies that collectively provide a secure network environment. It provides the following services :

- Authentication
- Confidentiality
- Integrity
- Non-Repudiation

A key management architecture is composed of 4 phases :

- **The enrollment phase** : registration of the users belonging to the concerned group, and the initial distribution of private and public keys ;
- **The re-keying phase** : re-initialization of all private keys periodically ;
- **The communication phase** ;
- **The revocation phase** : revoked user doesn't belong anymore to the group.

A key management architecture is composed of 4 phases :

- **The enrollment phase** : registration of the users belonging to the concerned group, and the initial distribution of private and public keys ;
- **The re-keying phase** : re-initialization of all private keys periodically ;
- **The communication phase** ;
- **The revocation phase** : revoked user doesn't belong anymore to the group.

There are 2 types of architectures :

- Certificate based infrastructures (RSA, ElGamal, ...) ;
- Certificat-less infrastructure (identity based cryptography).

1 Introduction

2 Public key infrastructure (PKI)
- The enrollment/rekeying phase
- The communication Phase
- PKI weaknesses

3 Identity based cryptography

4 The proposed solution

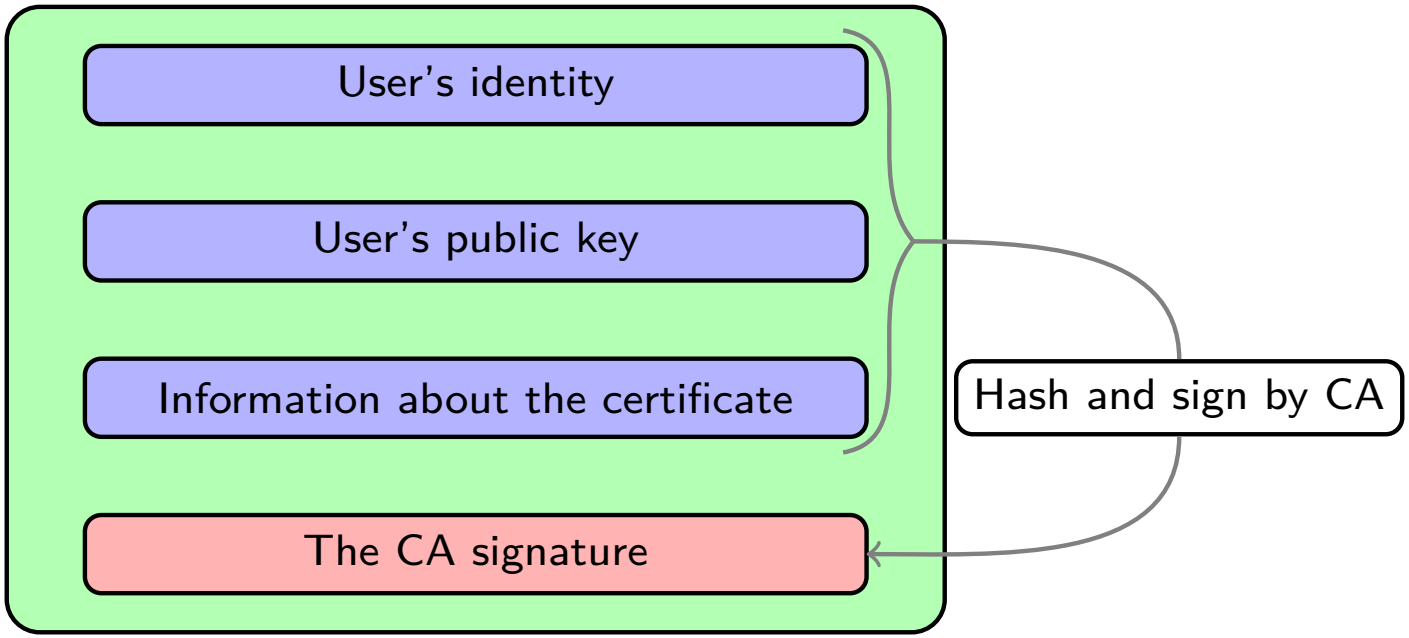
5 To summarize

PKI

Public key infrastructure is a certificate based key management architecture, and it use 2 core elements ; Public Key Cryptography and Certification Authorities.

A certificate

A certificate is an electronic document used to prove ownership of a public key.



The components of a certificate

Usually a PKI is composed of 3 authorities :

- Registration authority (RA) ;
- Certificate authority (CA) ;
- Validation authority (VA).

Other services :

- Directory service (DS) ;
- Certificate revocation list (CRL).

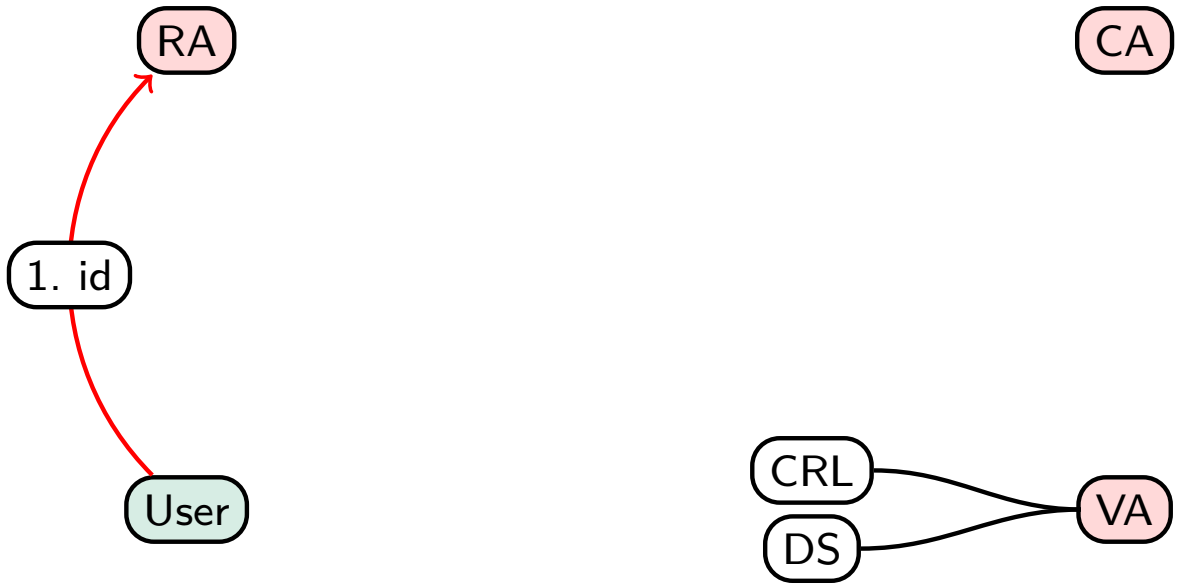


FIGURE: The enrollment/rekeying phase of a PKI

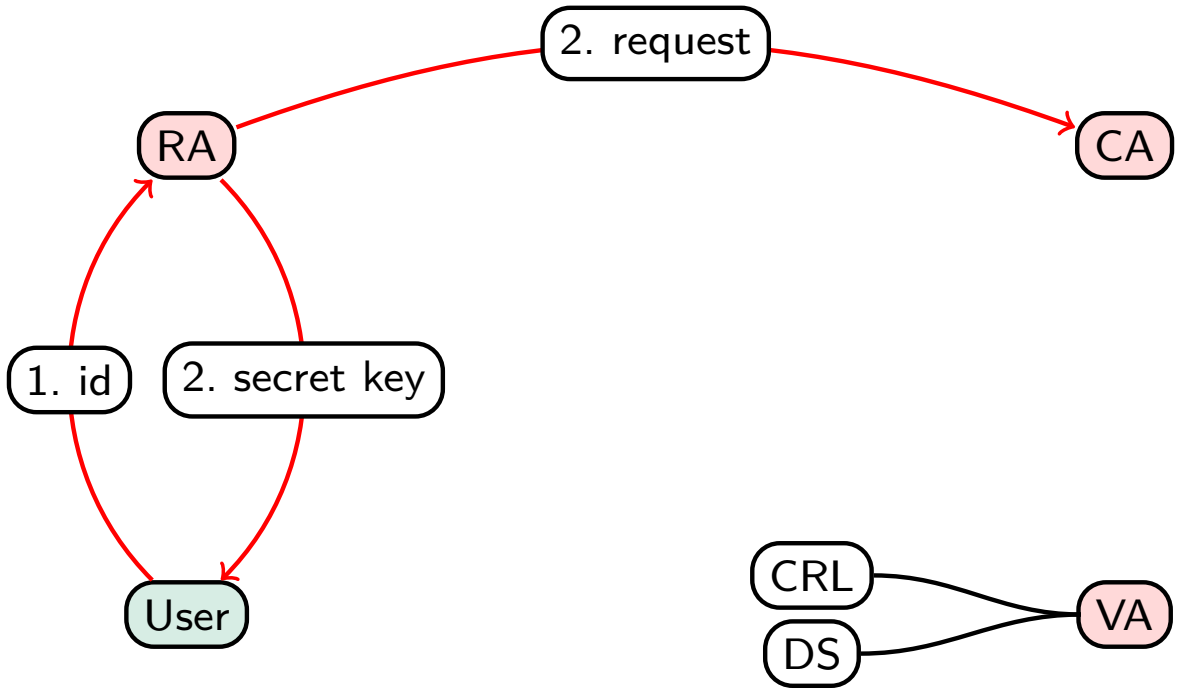


FIGURE: The enrollment/rekeying phase of a PKI

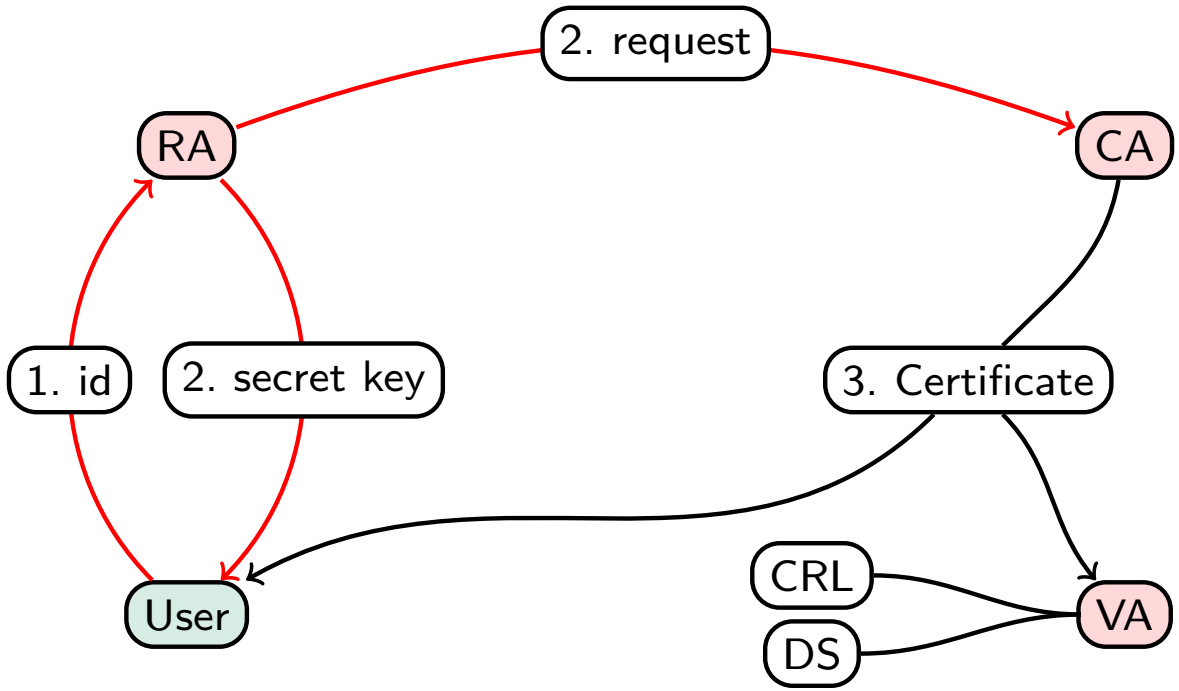


FIGURE: The enrollment/rekeying phase of a PKI

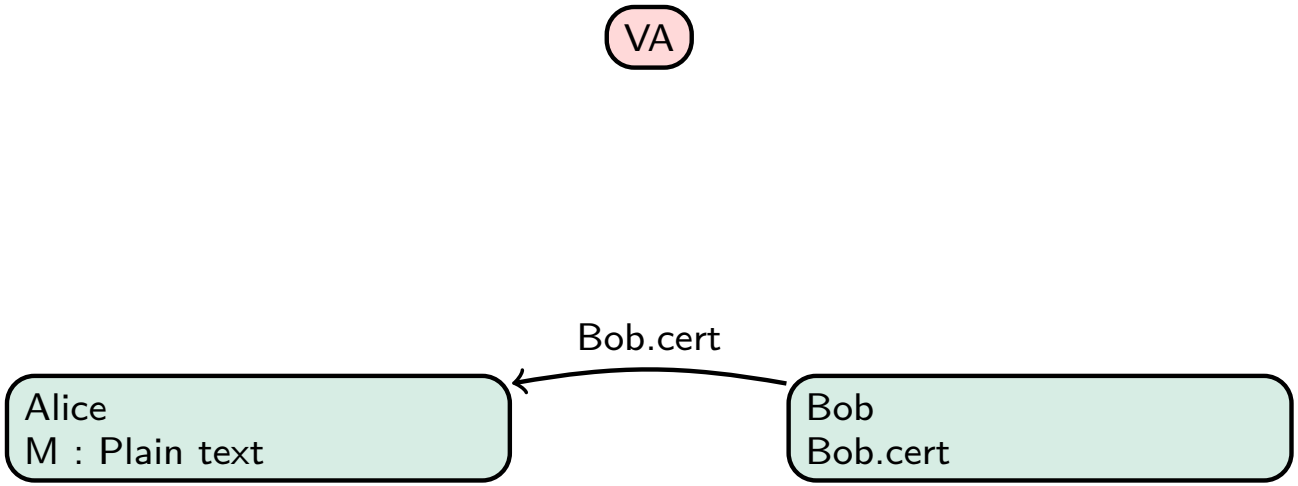


FIGURE: The communication phase of PKI

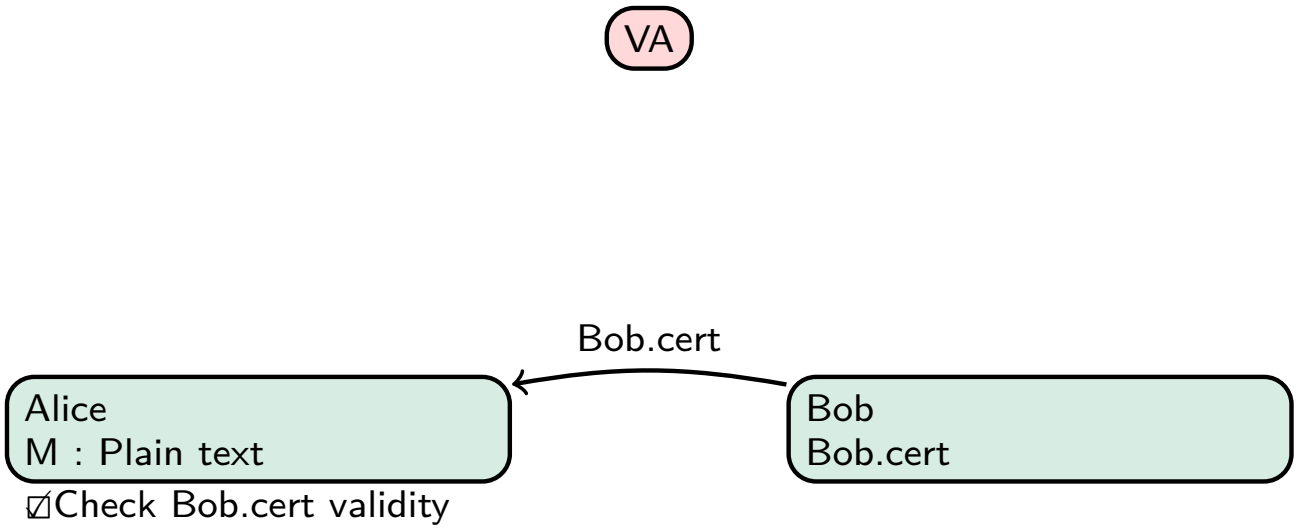


FIGURE: The communication phase of PKI

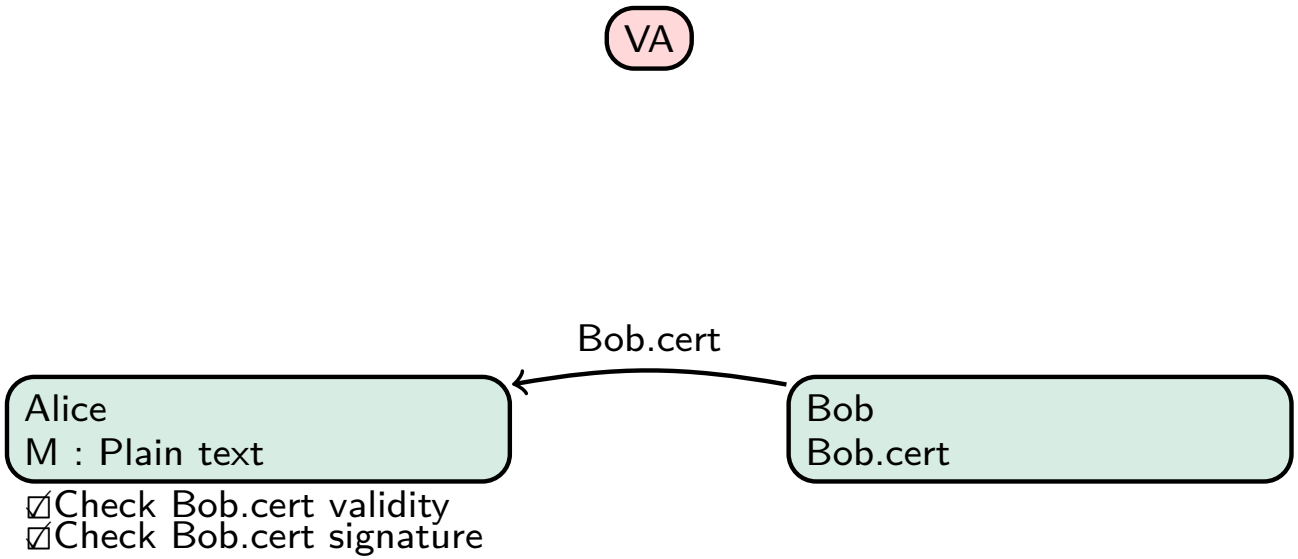


FIGURE: The communication phase of PKI

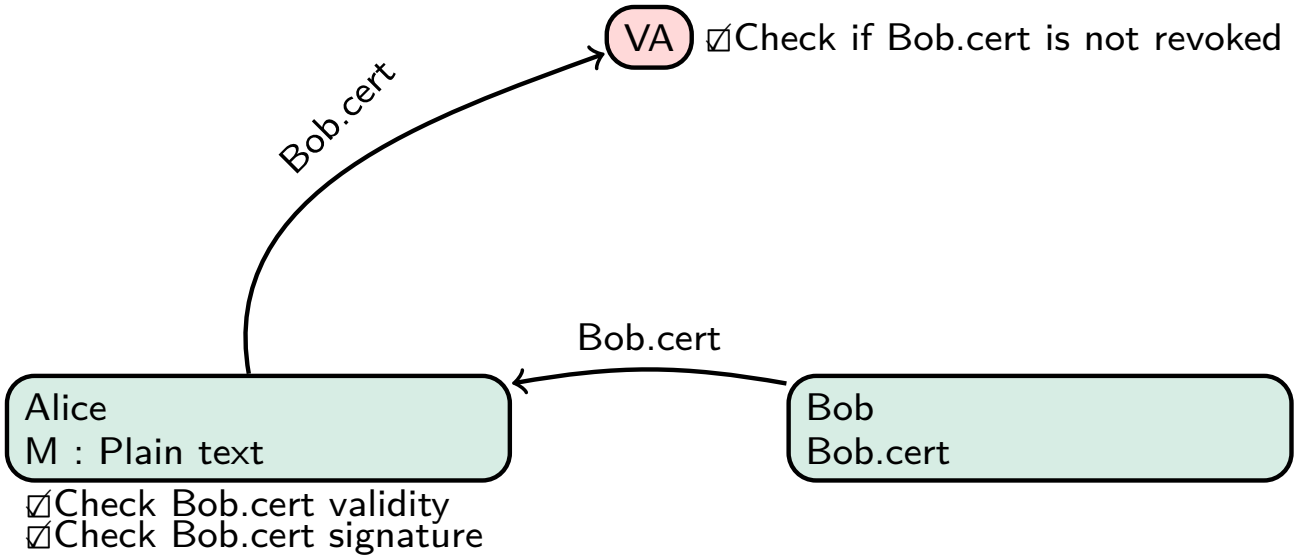


FIGURE: The communication phase of PKI

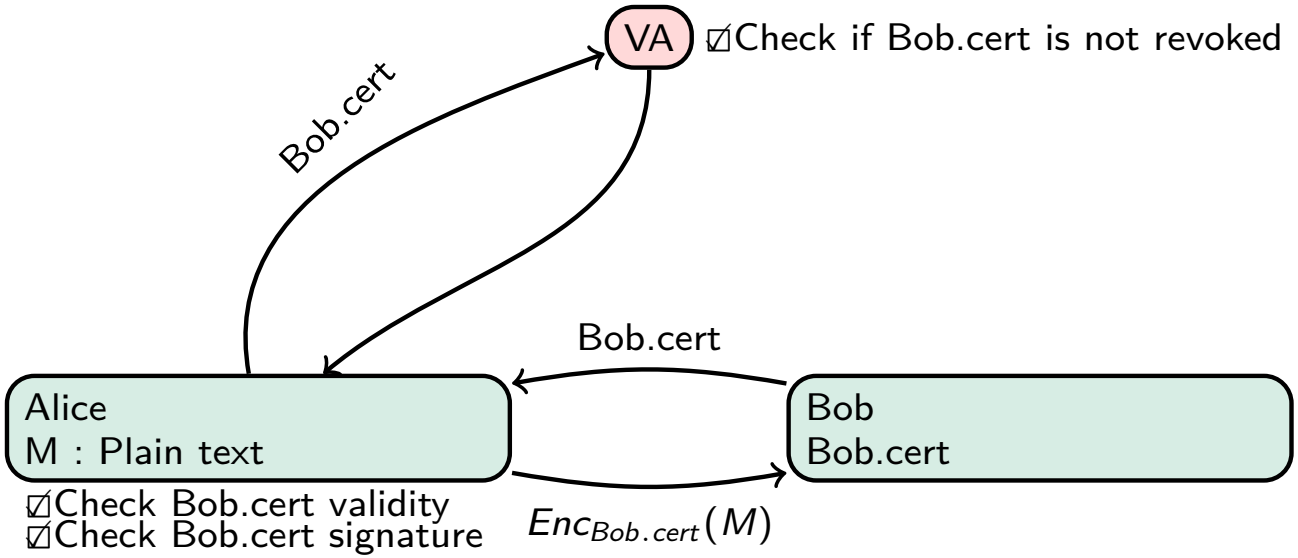


FIGURE: The communication phase of PKI

PKI weaknesses

- Revoked certificates must be stored in a certificate revocation list (CRL) ;
- Secret key is not generated by the user ;
- The CA can sign a fake certificates ;
- Enrolment and rekeying needs to be done via a private channel ;
- The secret keys are not protected.

1 Introduction

2 Public key infrastructure (PKI)

3 Identity based cryptography
- IBE communication phase
- advantages and disadvantages

4 The proposed solution

5 To summarize

- Identity based cryptography was introduced as an open problem by Adi Shamir in 1984 ;
- In 2001 Boneh and Franklin presented an effective IBE based on the bilinear Diffie-Hellman problem ;
- B.F IBE is composed of one authority called PKG (Private Key Generator) that generate/update users keys ;
- The user public key is a hash of his identity ;
- The PKG can calculate users secret keys by using his secret key and the user's identity.

PKG
Master Secret Key (MSK)
Master Public Key (MPK)

Alice
a. Use Bob id to generate Bob's public key.
b. Sign, encrypt and send message.

Bob
c. Use Alice id to generate Alice's public key.
d. Decrypt and verify received message

FIGURE: The communication phase in B.F IBE

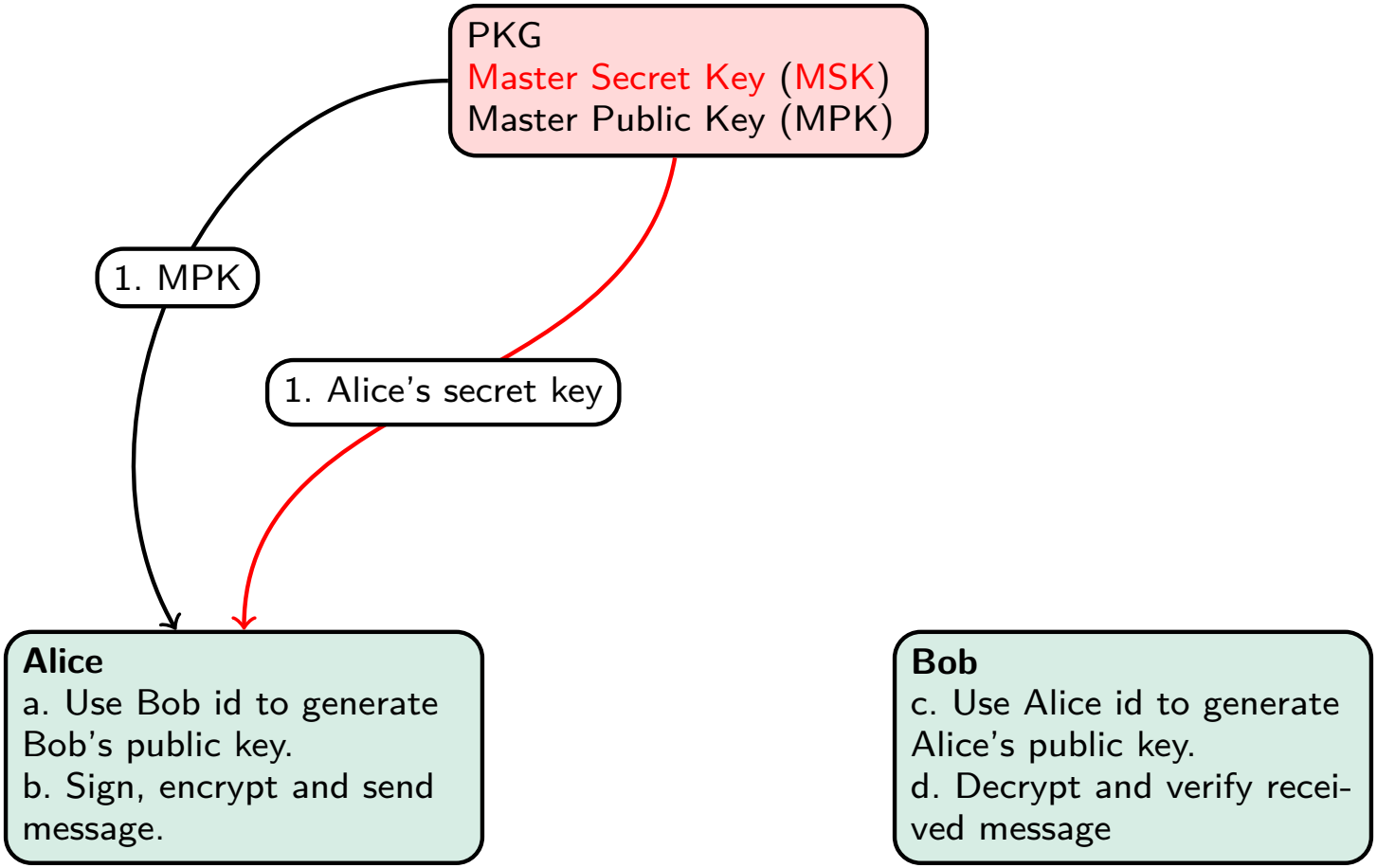


FIGURE: The communication phase in B.F IBE

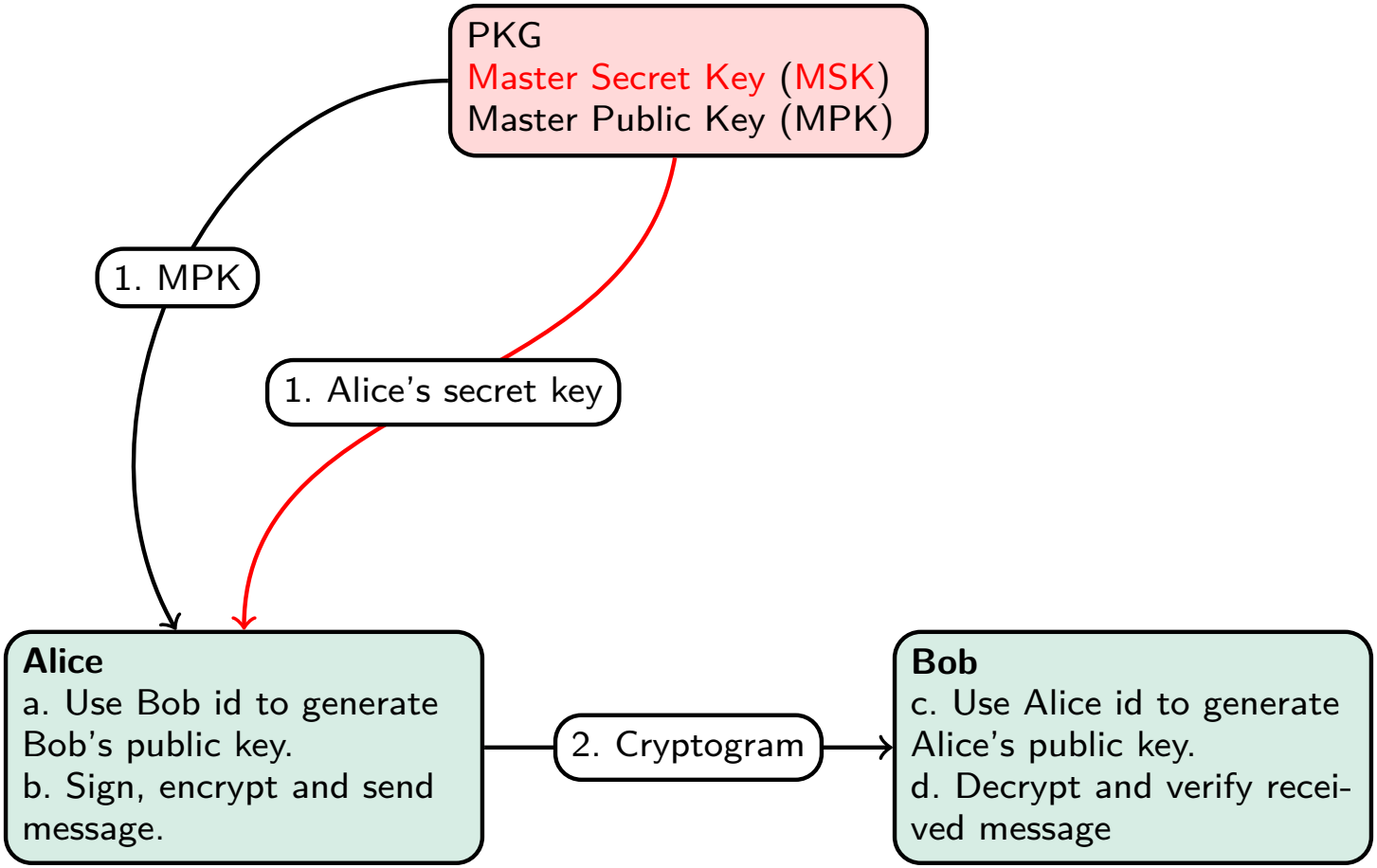


FIGURE: The communication phase in B.F IBE

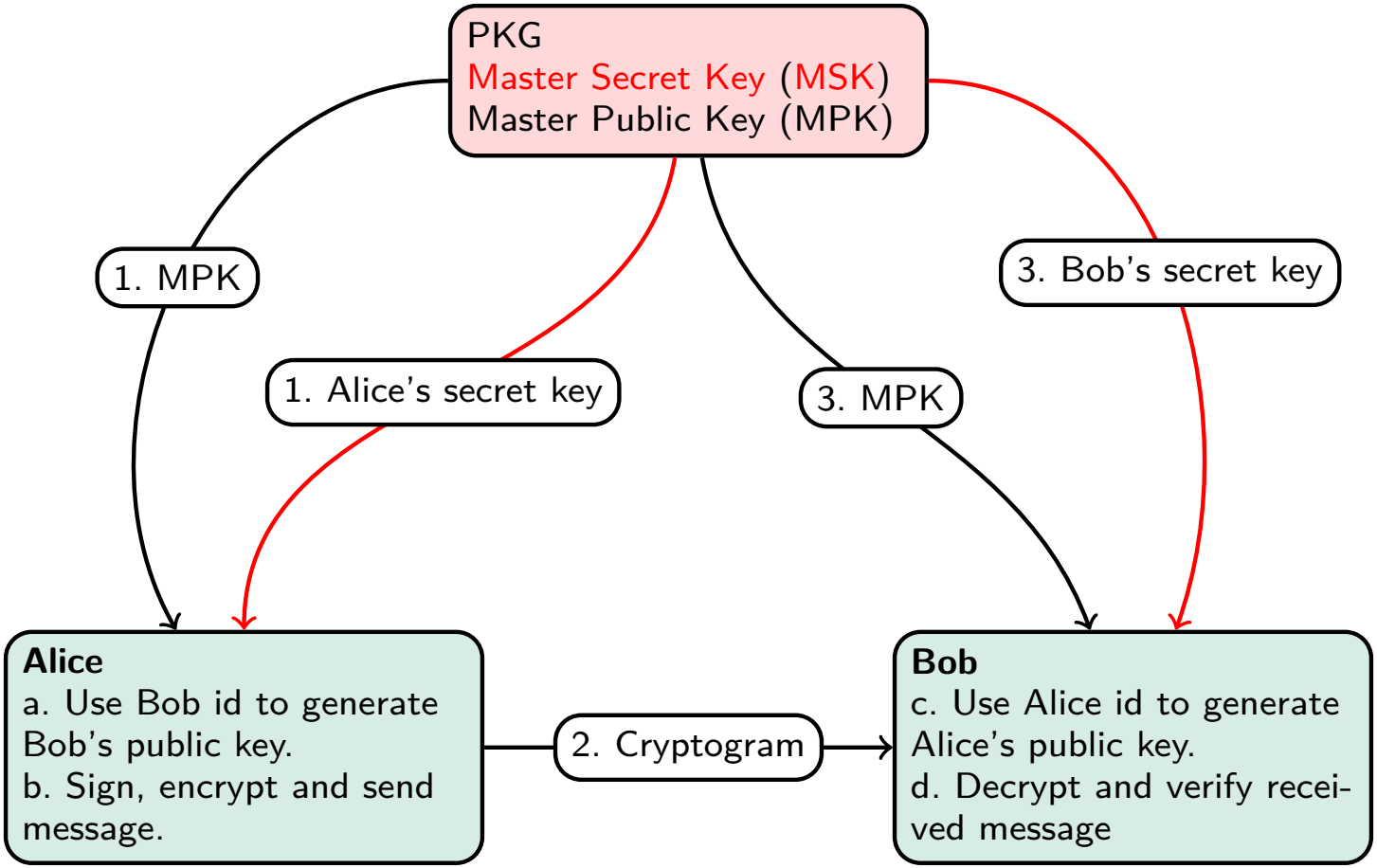


FIGURE: The communication phase in B.F IBE

advantages/ disadvantages

Advantages :

- It doesn't require a CRL to revoke entities ;
- It solves the authentication problem, (no certificates) ;
- A user doesn't need to store his private key.

Disadvantages :

- The system's security is based on a single entity : the PKG ;
- PKG interfere in each communication to provide the secret key, it may slow down the network ;
- The distribution have to be done over a private channel.

1 Introduction

2 Public key infrastructure (PKI)

3 Identity based cryptography

4 The proposed solution
- The enrollment phase
- The rekeying phase
- The revocation phase
- The communication phase
- The hierarchical model

5 To summarize

We want :

- A flexible system regarding the key escrow (law, needs, security policy) ;
- Many authorities that collectively calculate the user's secret key (Lee et al.[5]) ;
- Only the user can construct his secret key (Sattam and Paterson [1]) ;
- A real time revocation that does not depend of a CRL ;
- No list of public keys ;
- Possibility to encrypt a file that could be decrypted only in future.

- We use the **Barreto-Naehring elliptic curves** with **optimal Ate pairing** ;
- $\mathbb{G}_0, \mathbb{G}_1, \mathbb{G}_T$ three groups with prime order q ;
- The optimal Ate pairing is a bilinear function $e : \mathbb{G}_0 \times \mathbb{G}_1 \to \mathbb{G}_T$;
- $\forall a, b \in \mathbb{Z}_q, P, Q \in \mathbb{G}_0 \times \mathbb{G}_1$ we have :

$$e(aP, bQ) = e(abP, Q) = e(P, abQ) = e(P, Q)^{ab} \in \mathbb{G}_T \tag{1}$$

- we use two authorities (at least) :
  - Static PKG : is an off-line server that contributes only during the enrollment phase ;
  - Dynamic PKG : is an on-line server that participate in the construction of the user's secret key, keys update.

PKG_{st}
S.K : $s_0 \in \mathbb{Z}_q^*$
P.K : $P_0 = s_0 P \in \mathbb{G}_0$
$Y = s_0 s_1 P$

PKG_{dy}
S.K : $s_1 \in \mathbb{Z}_q^*$
P.K 1 : $P_1 = s_1 P \in \mathbb{G}_0$
P.K 2 : $P_1' = s_1 P' \in \mathbb{G}_1$

Bob
P.K : $Q_B = \mathcal{H}_1(id_B)$

FIGURE: The enrollment phase in IBE-2

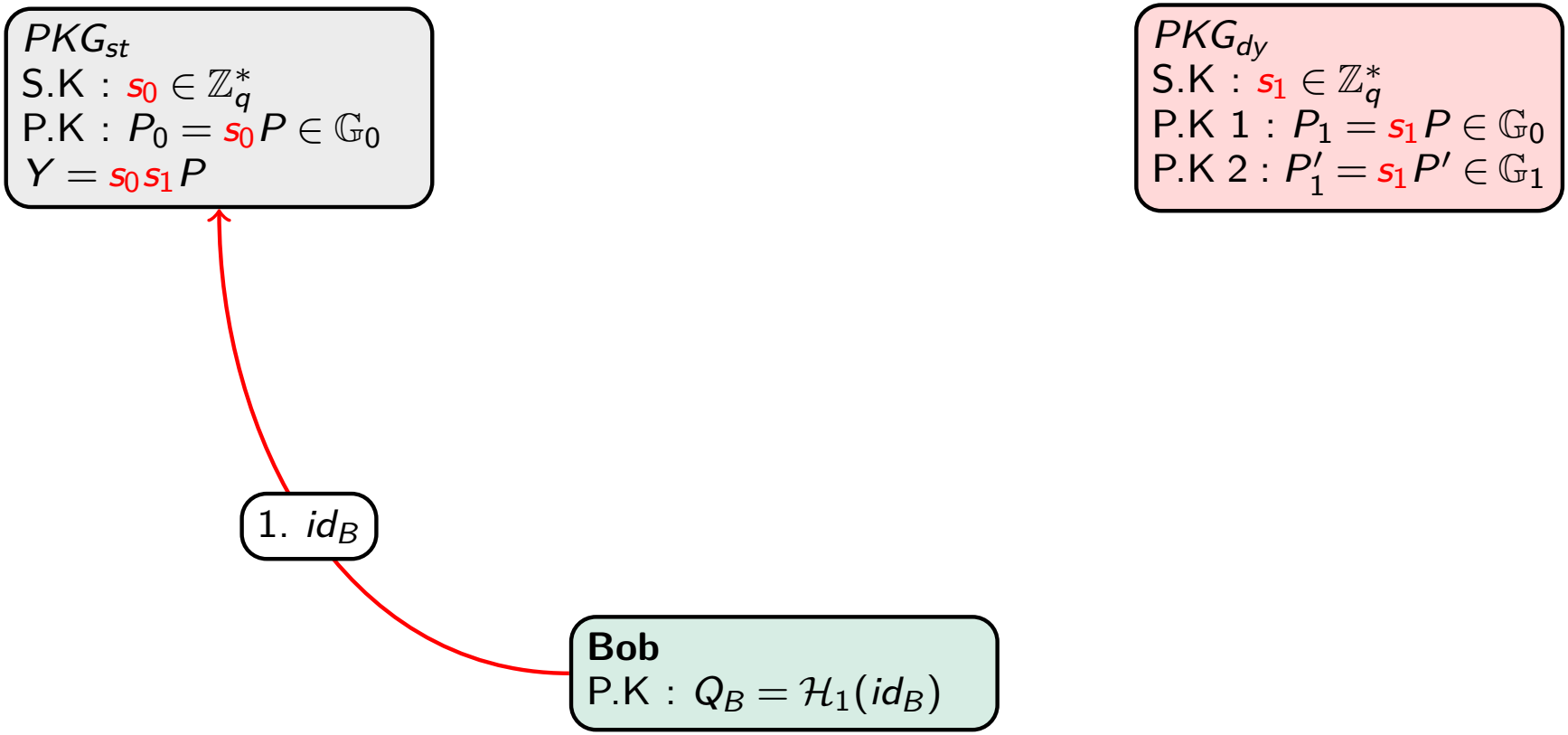


FIGURE: The enrollment phase in IBE-2

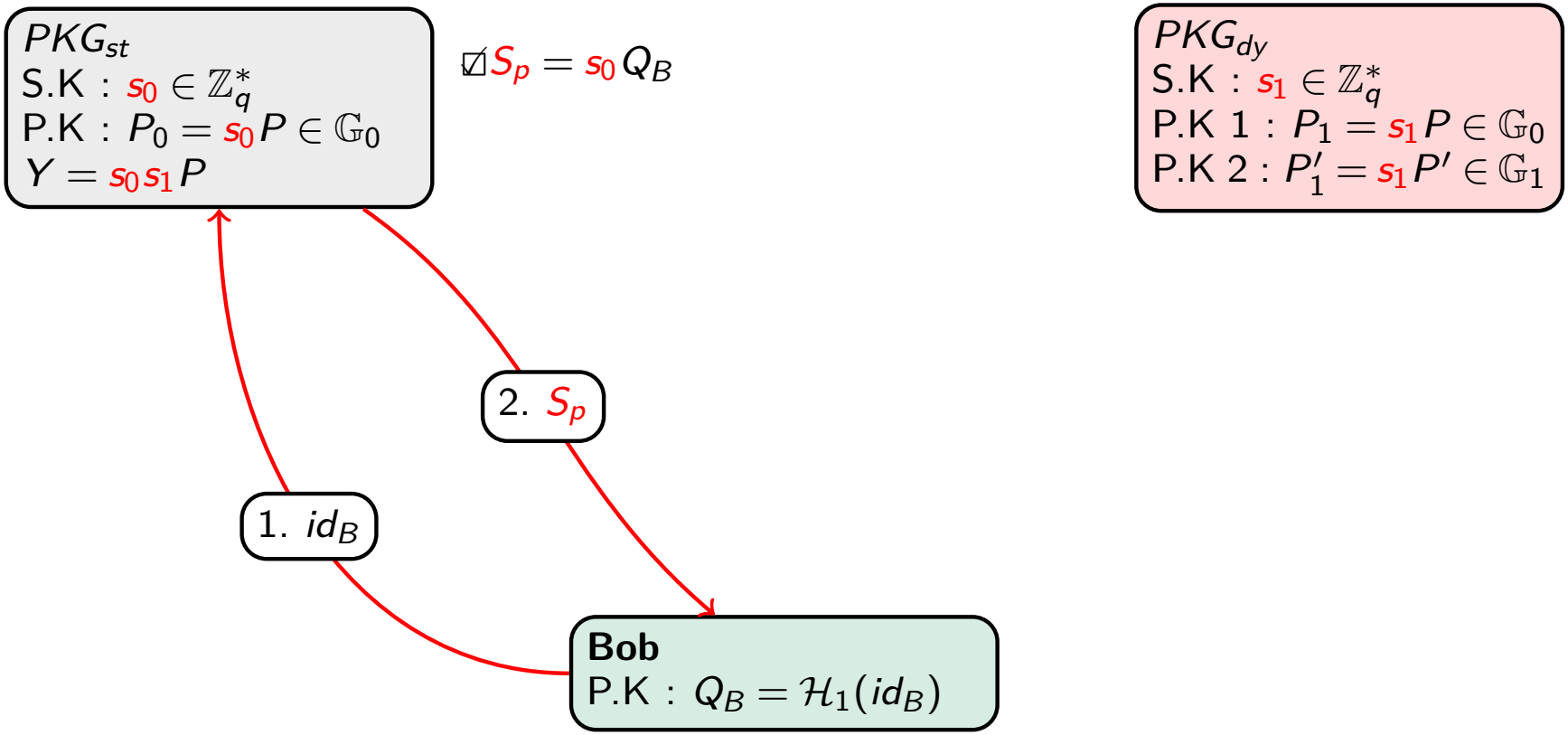


FIGURE: The enrollment phase in IBE-2

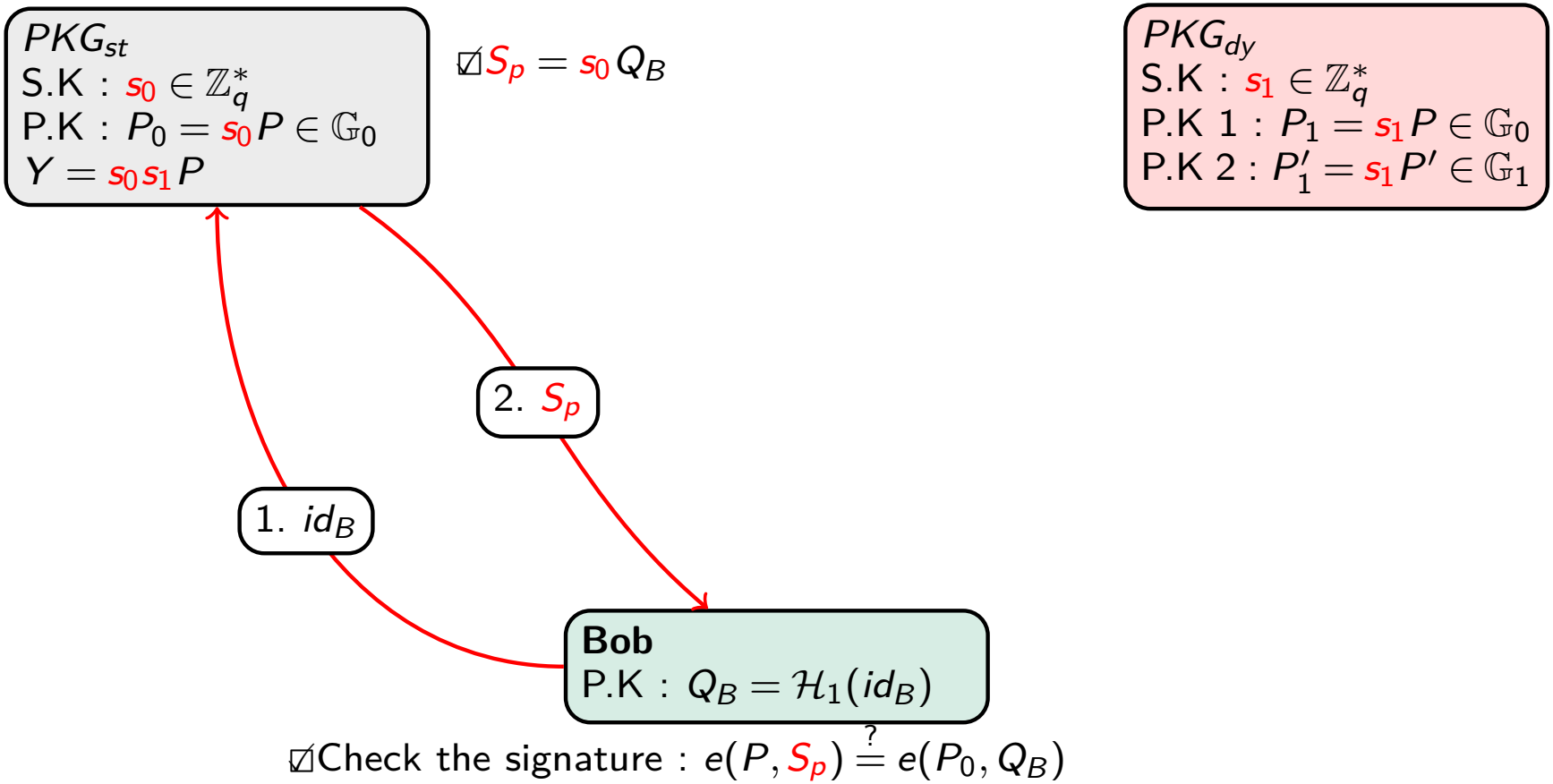


FIGURE: The enrollment phase in IBE-2

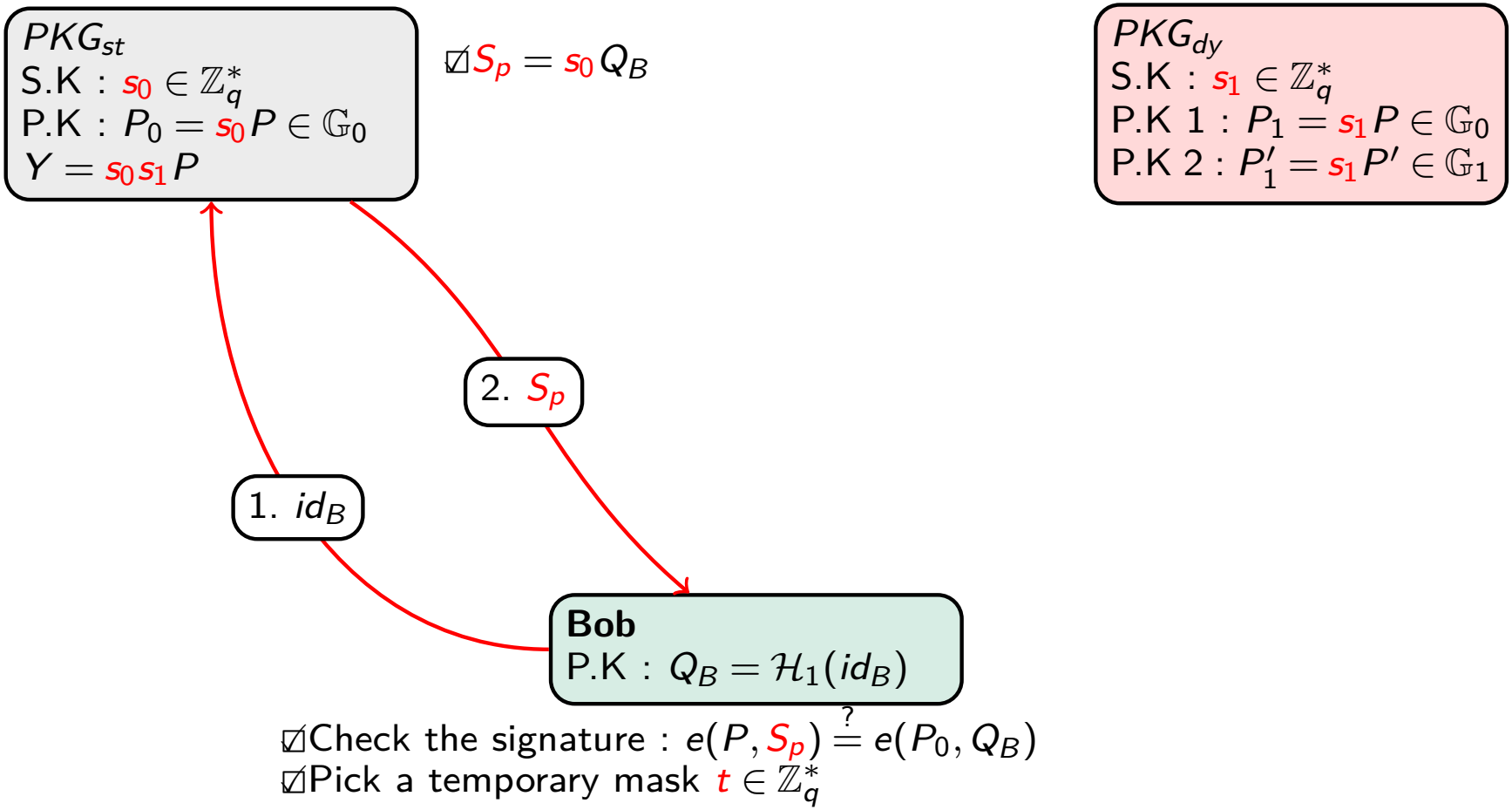


FIGURE: The enrollment phase in IBE-2

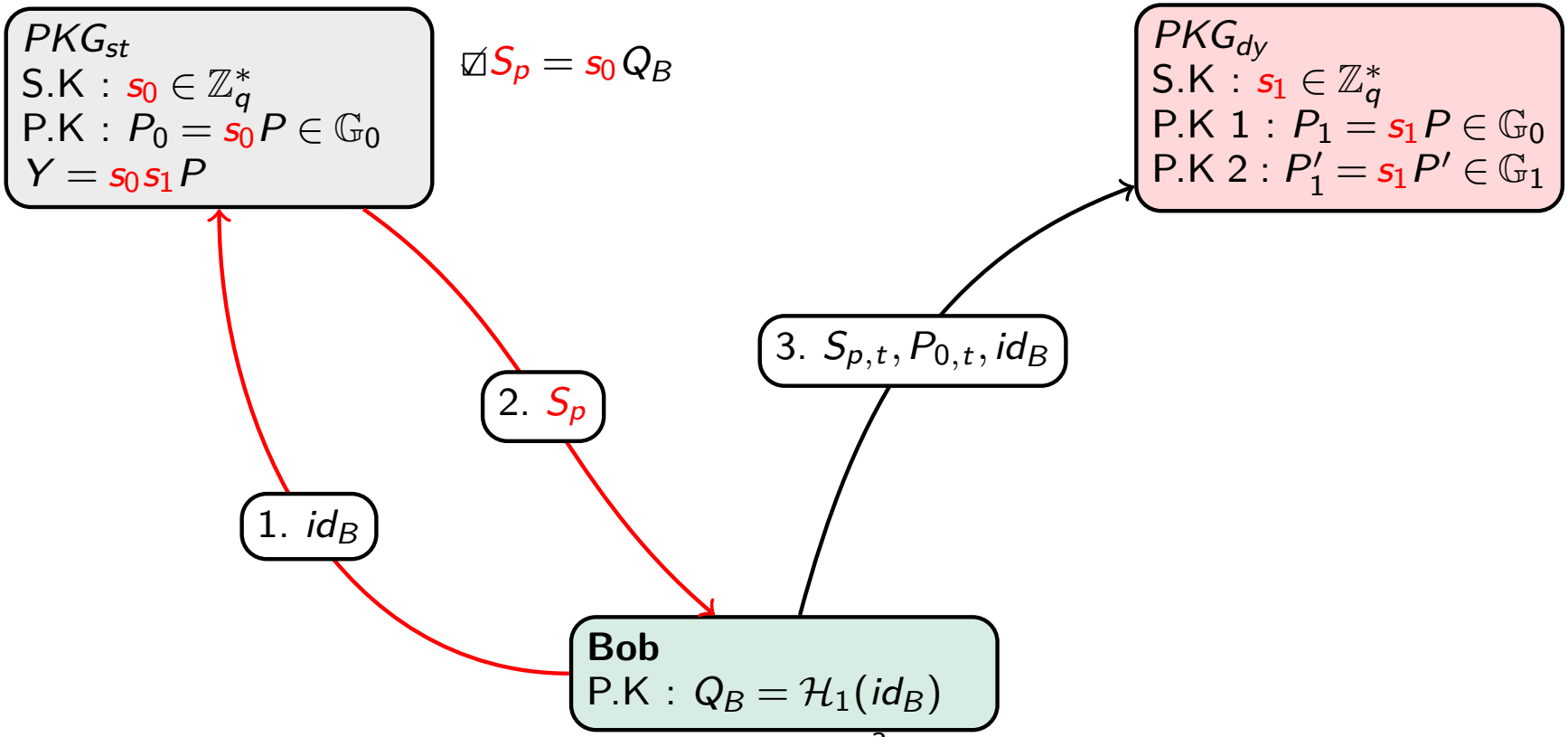


FIGURE: The enrollment phase in IBE-2

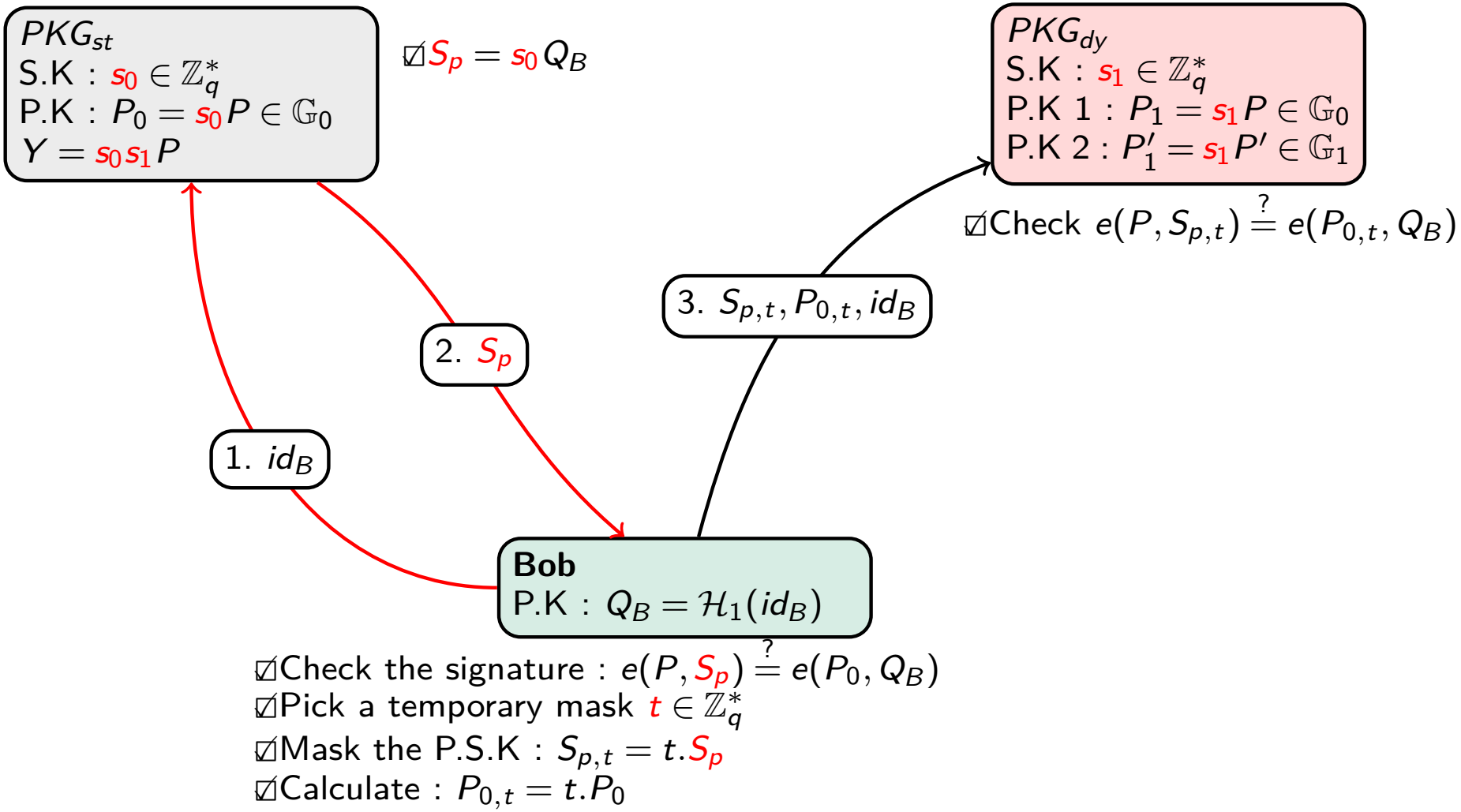


FIGURE: The enrollment phase in IBE-2

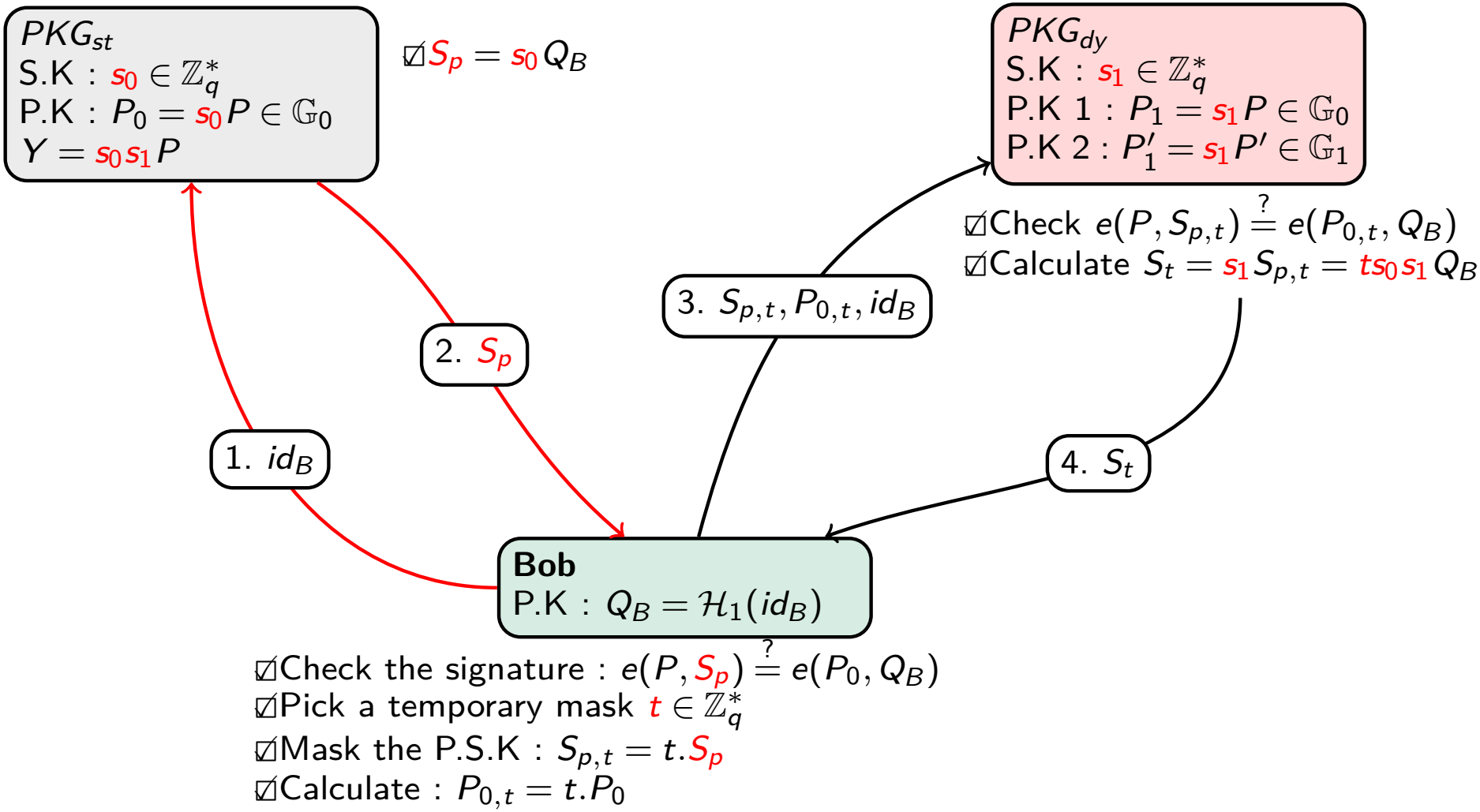
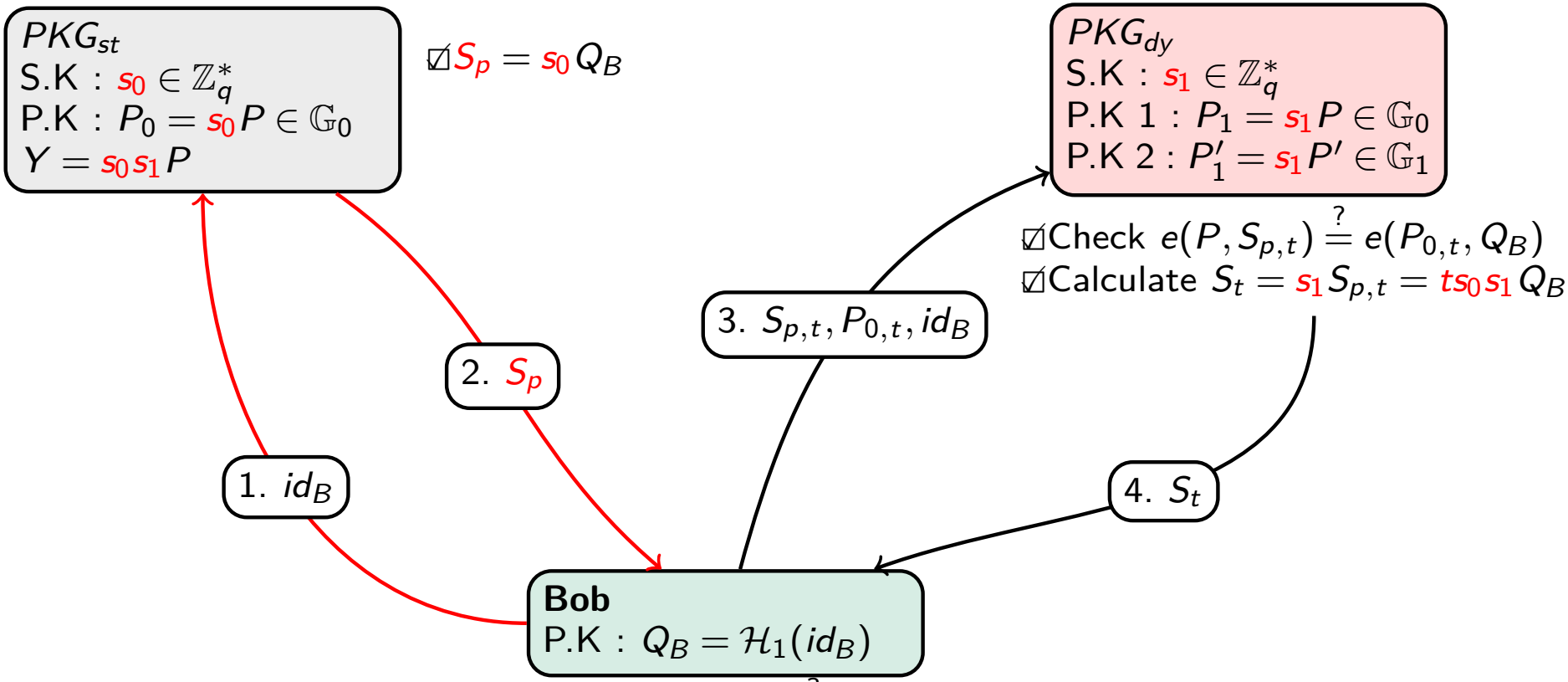


FIGURE: The enrollment phase in IBE-2



☑Check the signature : $e(P, S_p) \stackrel{?}{=} e(P_0, Q_B)$
☑Pick a temporary mask $t \in \mathbb{Z}_q^*$
☑Mask the P.S.K : $S_{p,t} = t.S_p$
☑Calculate : $P_{0,t} = t.P_0$
☑Extract the secret key : $S_B = t^{-1} S_t = s_0 s_1 Q_B$
☑check $e(P, S_B) \stackrel{?}{=} e(Y, Q_B)$

FIGURE: The enrollment phase in IBE-2

PKG_{st}
S.K : $s_0 \in \mathbb{Z}_q^*$
P.K : $P_0 = s_0 P \in \mathbb{G}_0$
$Y = s_0 s_1 P$

PKG_{dy}
S.K : $s_1 \in \mathbb{Z}_q^*$
P.K 1 : $P_1 = s_1 P \in \mathbb{G}_0$
P.K 2 : $P_1' = s_1 P' \in \mathbb{G}_1$

Bob
P.K : $Q_B = \mathcal{H}_1(id_B)$
S.K : $S_B = s_0 s_1 Q_B$
$S_p = s_0 Q_B$

☑Pick a temporary mask $t \in \mathbb{Z}_q^*$

FIGURE: The rekying phase in IBE-2

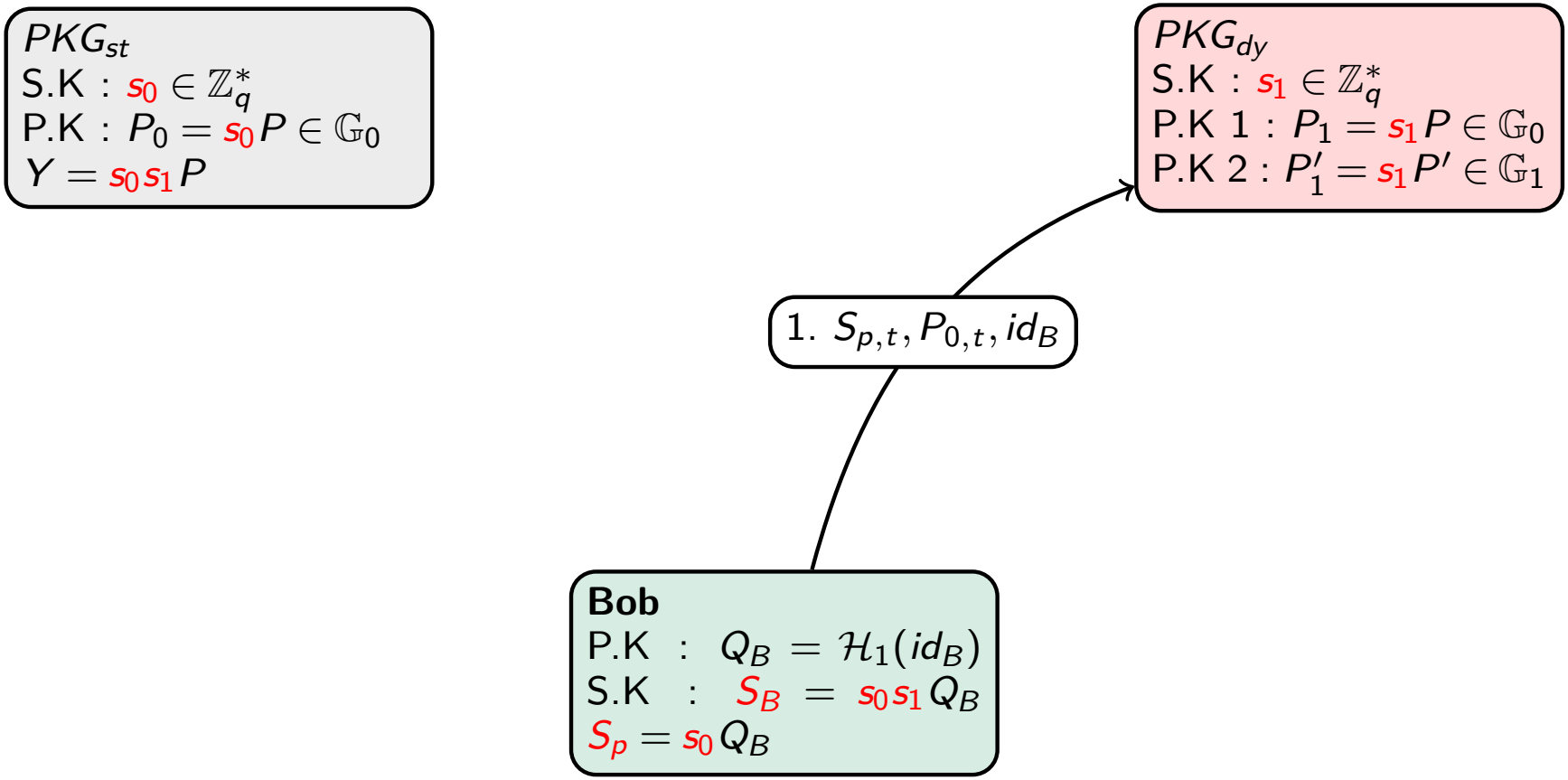


FIGURE: The rekying phase in IBE-2

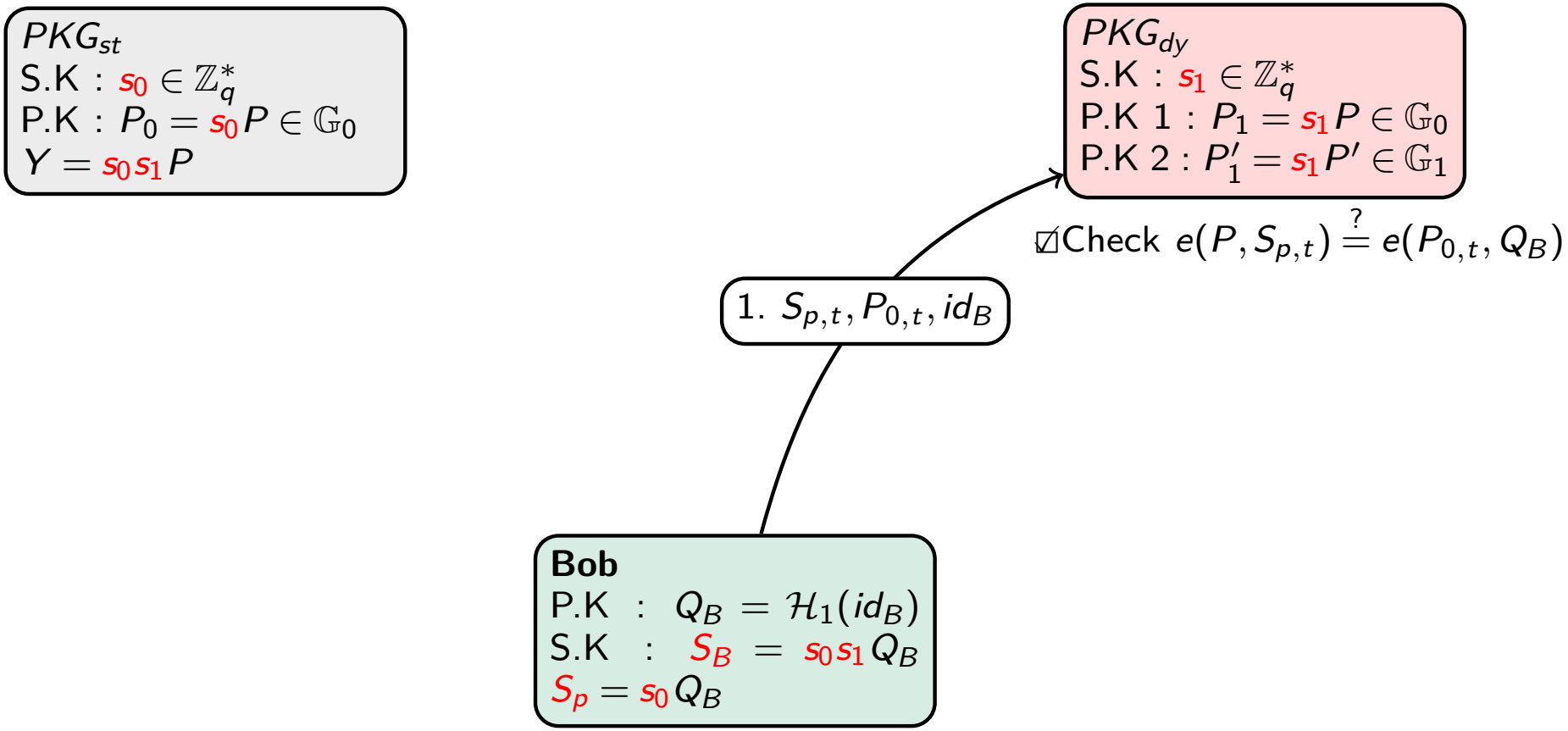


FIGURE: The rekying phase in IBE-2

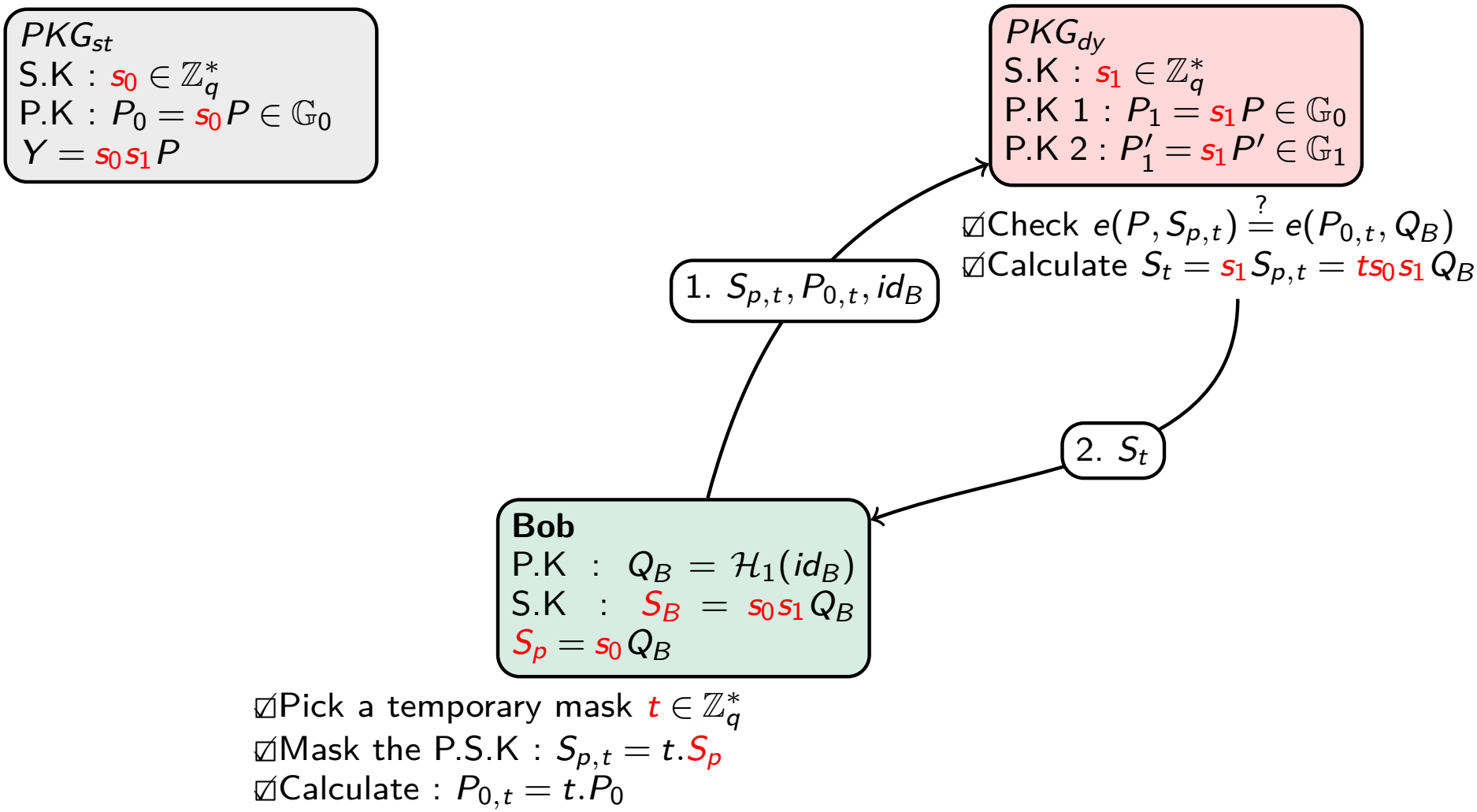


FIGURE: The rekying phase in IBE-2

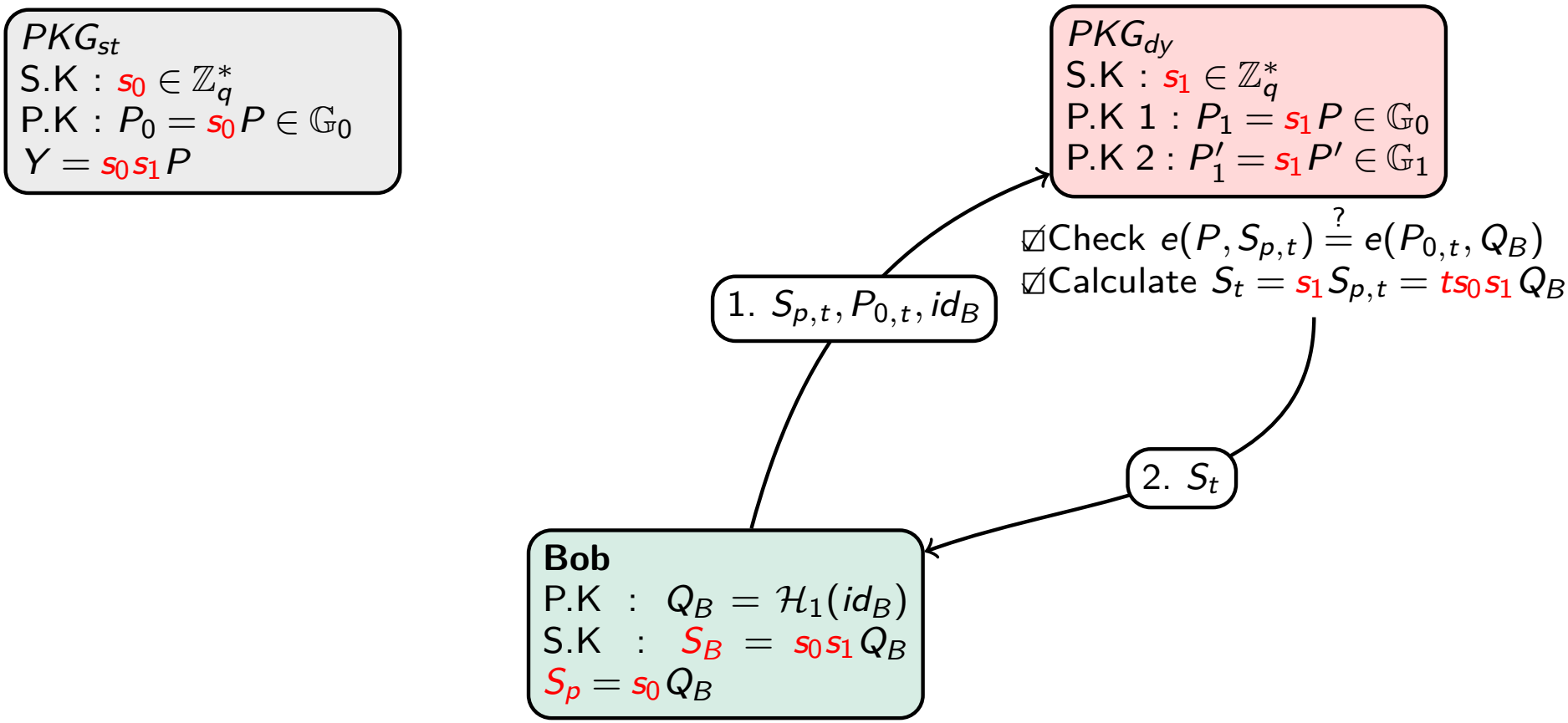


FIGURE: The rekying phase in IBE-2

The revocation phase

We add an IRL (Identity Revocation List) that lists the identity of revoked entities. This list must respect those proprieties :

- Must be cleaned at each re-keying phase. Whence, we can revoke the entities in real time without increasing constantly the IRL ;
- The IRL is a reading only file for which only the security officer can add the revoked identities ;
- The IRL does not require to store keys ;
- The period T must be chosen in order to make the IRL nearly empty a most of the time, so it will not affect the network traffic fluidity.

The revocation phase

We add an IRL (Identity Revocation List) that lists the identity of revoked entities. This list must respect those proprieties :

- Must be cleaned at each re-keying phase. Whence, we can revoke the entities in real time without increasing constantly the IRL ;
- The IRL is a reading only file for which only the security officer can add the revoked identities ;
- The IRL does not require to store keys ;
- The period T must be chosen in order to make the IRL nearly empty a most of the time, so it will not affect the network traffic fluidity.

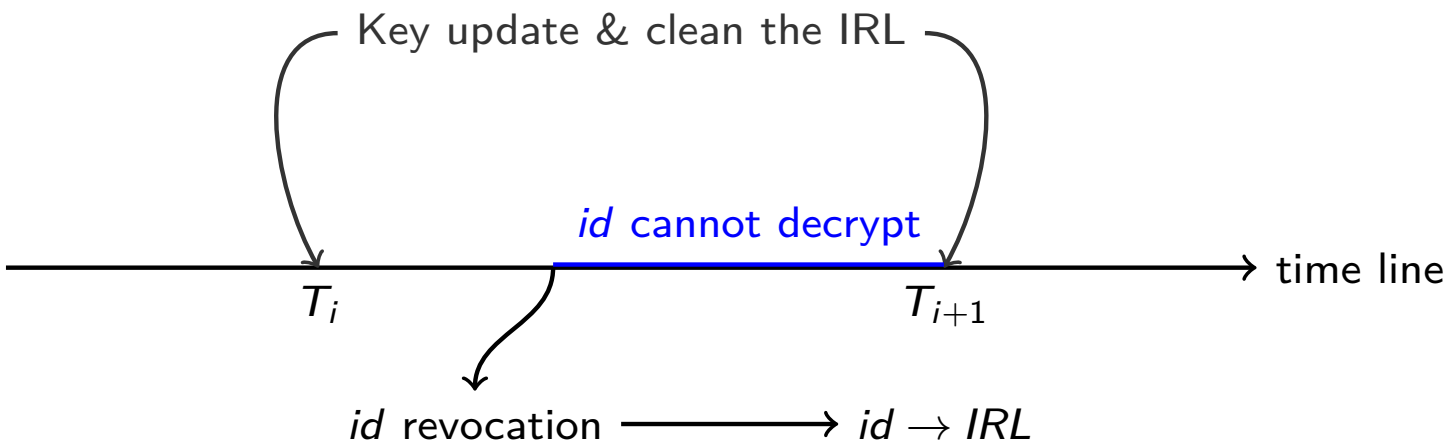


FIGURE: Real-time revocation in IBE-2

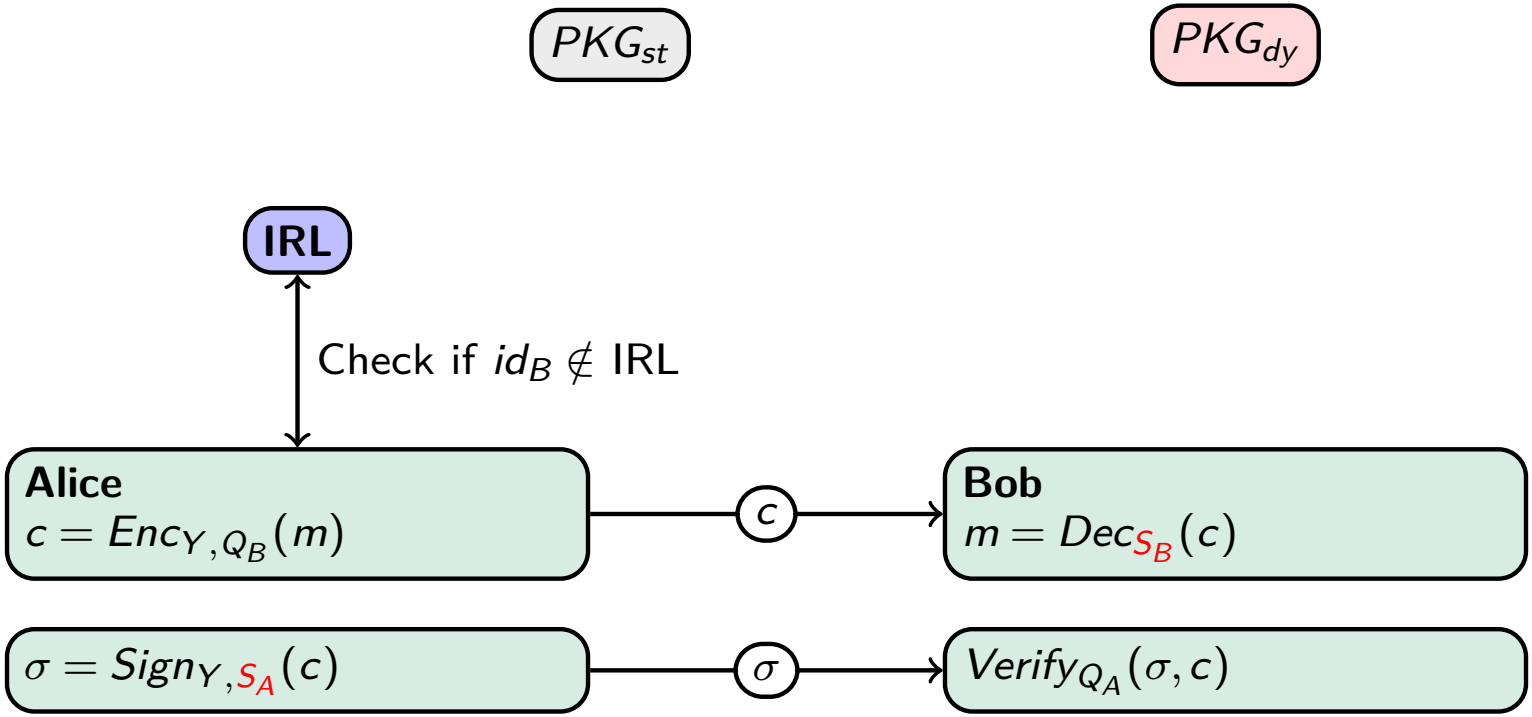
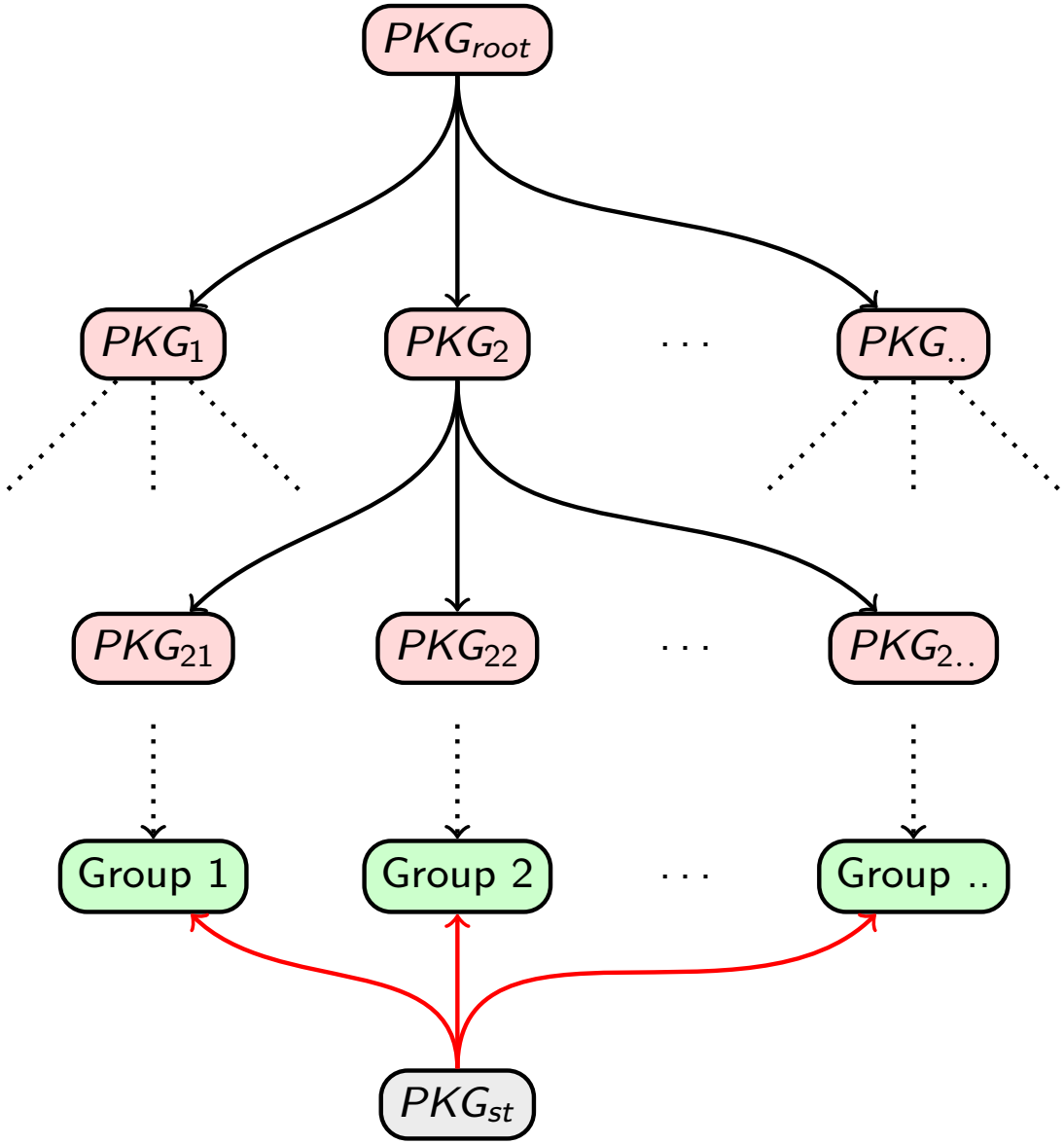


FIGURE: An authenticated encryption in IBE-2

Hierarchical IBE



1 Introduction

2 Public key infrastructure (PKI)

3 Identity based cryptography

4 The proposed solution

5 To summarize

Conclusion :

- The security of the full system is not supported by one authority ;
- Neither PKG_{dy} or PKG_{st} can sign or encrypt instead of the user ;
- A flexible system designed to accept or reject the Key Recovery ;
- The communication with authorities is via a public channel ;
- Real time revocation, without increasing constantly the IRL ;
- The private key can be calculated in case of loss ;
- This infrastructure is fully compatible with the hierarchical model.

Thank you !


Sattam S. Al-Riyami and Kenneth G. Paterson, Certificateless Public Key Cryptography, *asiacrypt*, 2003.


Dan Boneh and Matthew K. Franklin, Identity-Based Encryption from the Weil Pairing Advances in Cryptology, *Proceedings of CRYPTO*, 2001.


Paulo S. L. M. Barreto and Michael Naehrig, Pairing-friendly elliptic curves of prime order, *Springer*, 2006.


XU Chunxiang, ZHOU Junhui and QIN Zhiguang, A Note on Secure Key Issuing in ID-based Cryptography.


Byoungcheon Lee, Colin Boyd, Ed Dawson, Kwangjo Kim, Jeongmo Yang and Seungjae Yoo, Secure Key Issuing in ID-based Cryptography.


Adi Shamir, Identity-Based Cryptosystems and Signature Schemes *Advances in Cryptology : Proceedings of CRYPTO*, 1984.


Peter Gutmann, PKI : It's Not Dead, Just Resting, August, 2002.


Carl Ellison and Bruce Schneier, Ten Risks of PKI : What You're not Being Told about Public Key Infrastructure, *Computer Security Journal*, 2000.


F. Vercauteren, Optimal Pairings, *eprint*, 2008.