Cryptography

Encryption Schemes

Seminar Nov 12, 2019

Kimheng SOK
PhD Student supervised by Professor Jean-Noël COLIN
PReCISE Research Center
University of Namur
Namur, Belgium
kimheng.sok@student.unamur.be

UNIVERSITÉ DE NAMUR

AGENDA

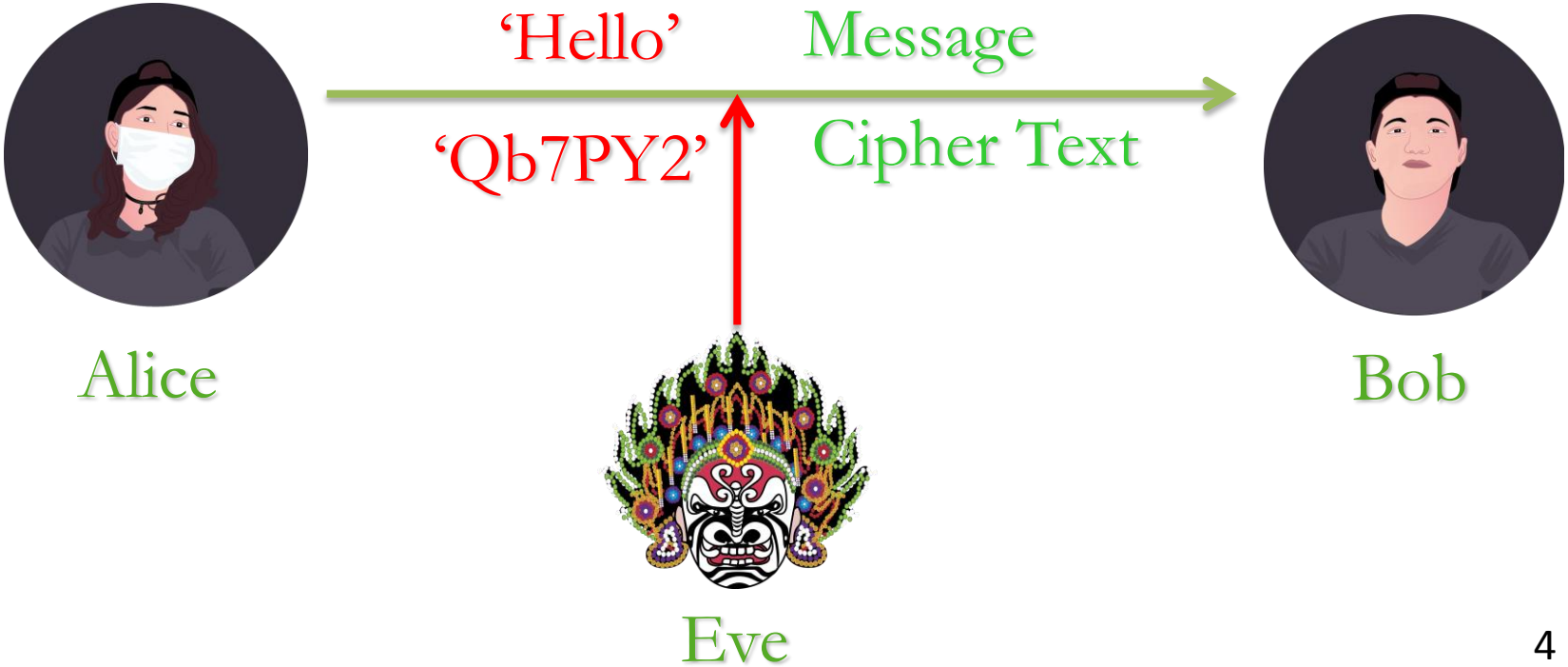
- Introduction
- Prior Knowledge
- Symmetric Cryptography
- Asymmetric Cryptography
- IBE
- ABE (KP-ABE, CP-ABE, MAA-CP-ABE)
- References

Introduction

Introduction

Cryptography = Crypto (Secret) + Graphy (Write,Study)

Cryptography is the science of writing or creating secret.



Introduction

Why do we need to keep our message secret?

- ✓ We have some secret that don't want somebody to know
- ✓ We only want to share the secret with only the people we want to share
- ✓ Some sensitive transaction online such as payment, health information, business, government need to keep secret
- ✓ Even a simple chat messaging, we need private chat

"Our message need to be encrypted"

Introduction

Notation	Description
P, M	Plaintext, Message
CT	Cipher Text
K, PK, SK, MSK	Key, Public Key, Secret Key, Master Secret Key
ENC	Encryption
DEC	Decryption

Encryption: The process of encoding a message into a cipher text.

Decryption: The process of decoding a cipher text into a message.

Prior Knowledge

Prior Knowledge

Discret Log $g, g^x \longrightarrow x$

CDH $g, g^x, g^y \longrightarrow g^{xy}$

DDH $g, g^x, g^y, g^z \longrightarrow \begin{cases} 0 \text{ if } z=xy \\ 1 \text{ otherwise} \end{cases}$

CDH: Computational Diffie Hellman
DDH: Decisional Diffie Hellman

"RANDOMNESS IS THE KEY"

Symmetric Cryptography

UNAMUR INFOSEC

www.unamur.be

UNIVERSITÉ DE NAMUR

Symmetric Cryptography

Aka Secret Key Cryptography or Private Key Cryptography

Encryption: CT = Enc (M , K)
Ex: Qb7PY2 = Enc('Hello',123456)

Decryption: M = Dec (CT , K)
Ex: Hello= Dec('Qb7PY2',123456)

"Encryption and Decryption Key is the same"

Symmetric Cryptography

Key Size (bits): 128, 256, 512, 1024, 2048,4096,…
Strength: randomness

Algorithm: Caesar Cipher, Vigenère Cipher, Enigma, DES, AES, RC4, …
Mode of operation: ECB, CBC, CFB, CTR, GCM, …
Help: $ openssl help

Symmetric Cryptography

Advantage and Disadvantage of symmetric cryptography?

- ✓ Secure and Fast computation

- ❖ Secret key need to be transferred all the time that create high risk of key compromising

=> **Diffie Hellman Key Exchange** [1]

- ❖ Secret key is leaving the owner of the message to other receiver or at the attacker hand, which means the same key is on the hand of many people

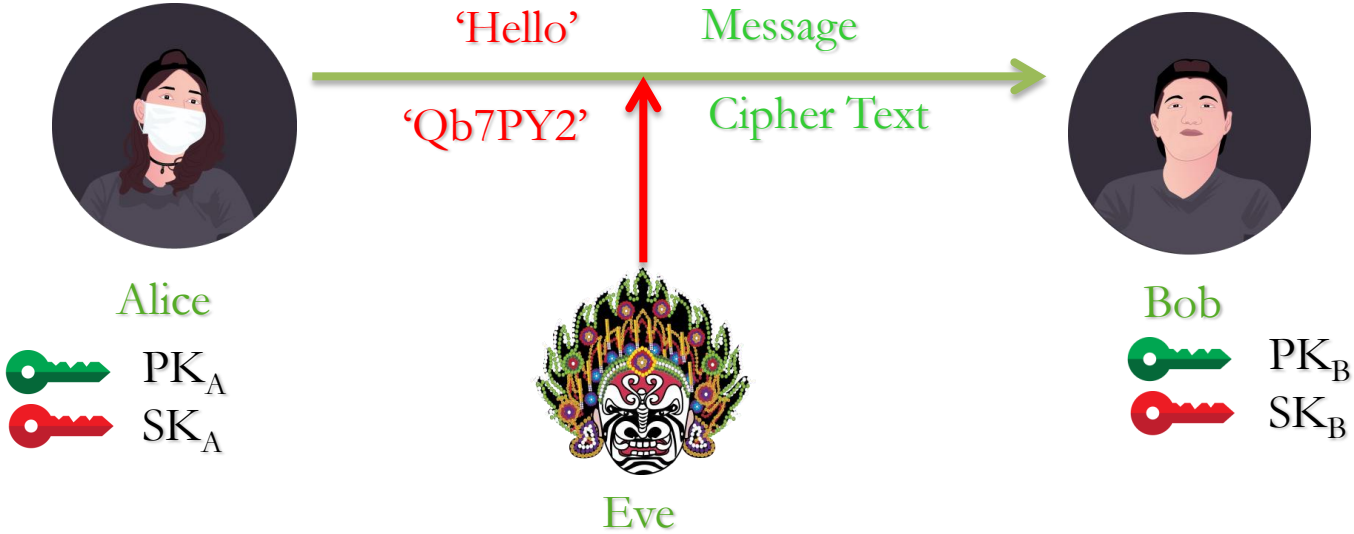
Asymmetric Cryptography

Asymmetric Cryptography

Aka Public Key Cryptography

Public Key (PK)

Secret Key (SK) Aka. Private Key

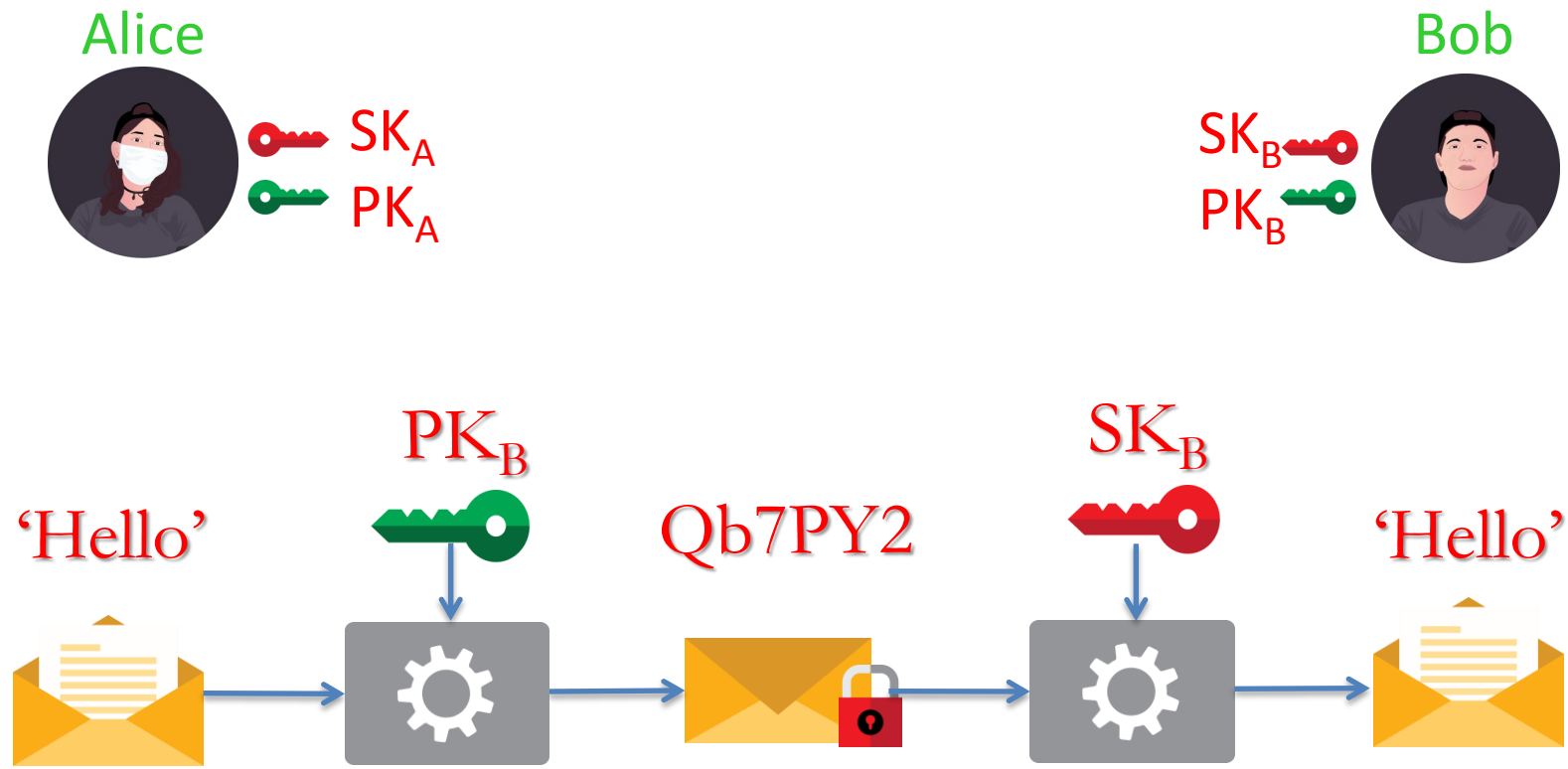


Asymmetric Cryptography

What is asymmetric cryptography?

- ✓ The algorithm that use the two different keys, one for encryption and another for decryption.
- ✓ Public Key (PK) is used for encryption and can be share to public, everyone can see it.
- ✓ Secret Key (SK) *aka. Private Key* is used for decryption and this key need to keep secret only on the owner hand.

Asymmetric Cryptography



Encryption: $CT = Enc(M, PK_B)$

Decryption: $M = Dec(CT, SK_B)$

Asymmetric Cryptography

Key Size (bits): 128, 256, 512, 1024, 2048,4096,…
Strength: randomness

Algorithm: RSA, El Gamal, ECC, Pairing…

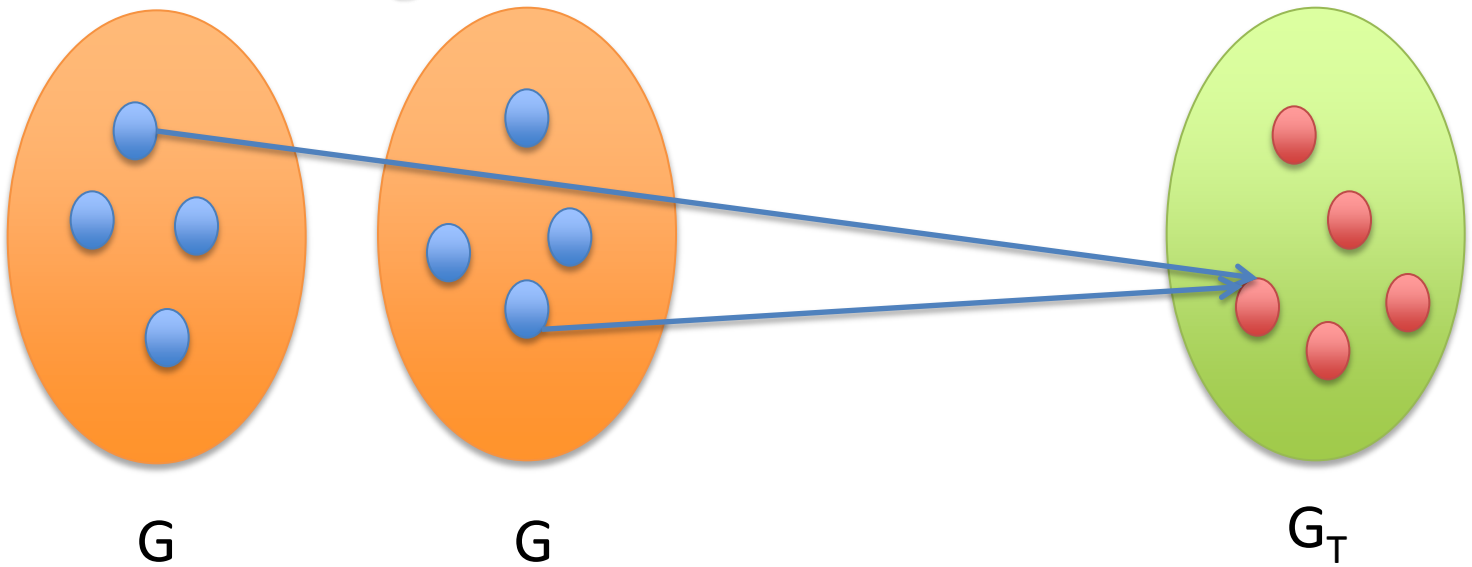
2^{λ} Best known attack time

Algorithm	Signature Size	$\lambda = 128$
RSA	$O(\lambda^3)$	2048 bits
EC-DSA	4λ	512 bits
Schnorr	3λ	384 bits
BLS (Ecc,Pairing)	2λ	256 bits

IBE
Identity-Based Encryption

IBE: Identity-Based Encryption

What is Pairing [2]?



Pairing $G \times G \rightarrow G_T$ where $G \in E(Fp)$, $G_T \in Fp$, $a,b \in Zp$, g:generator

$$e(g^a,g^b) = e(g^b,g^a) = e(g,g)^{ab}$$

G: Cyclic Group, G_T: Target Group
Fp: Finite Field
E(Fp): Elliptic Curve over Finite Field

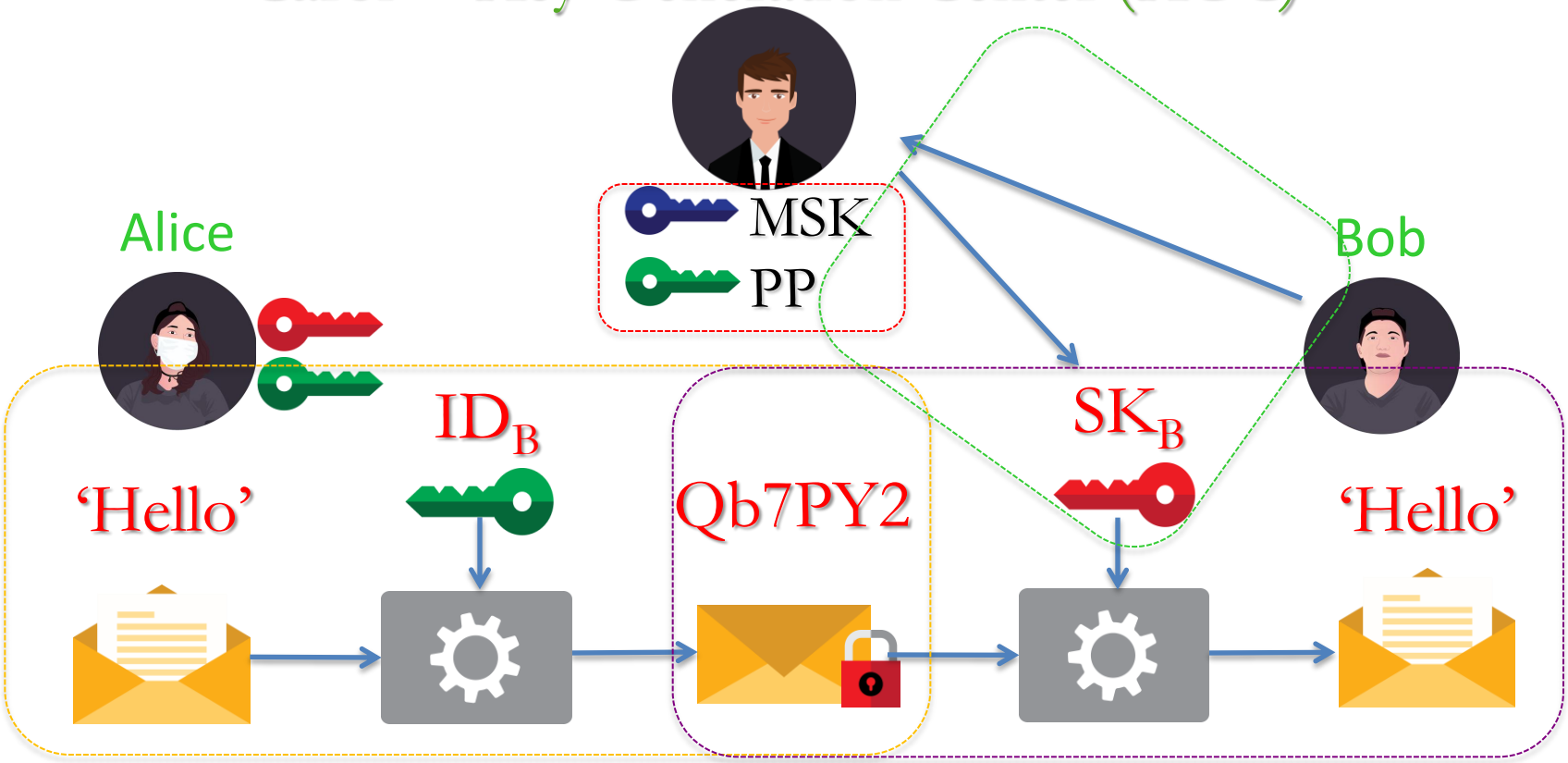
IBE: Identity-Based Encryption

What is Identity-Based Encryption [3,4]?

- ✓ The algorithm that encrypt the message with receiver identity such as name or email address.
- ✓ Only the receiver who possess the key with encrypted identity could decrypt the cipher text
- ✓ The encryption process could be done, even before the receiver exist
- ✓ The receiver need to get the secret key from Key Generation Center **(KGC)** to decrypt the cipher text

IBE: Identity-Based Encryption

Carol = Key Generation Center (KGC)



Set up | Enccryption | Keygen | Decryption

IBE: Identity-Based Encryption

Set up (λ) : PK, SK

Enc (M,PK) : CT

Dec (CT,SK) : M

Set up (λ) : PP, MSK

Enc (M,ID,PP) : CT

Keygen (ID,MSK) : SK

Dec (CT,SK) : M

IBE

IBE : Identity-Based Encryption

Set up (λ) : PP, MSK

$MSK = \alpha$, $PP=\{g, g^{\alpha}, H_1, H_2\}$

Enc (M,ID,PP) : CT

ID="bob", alice ($SK_A=a$, $PK_A=g^a$)

$CT\{U,V\}$, $\{U=g^a, V=M \oplus H_2(e(H_1(\text{"bob"}), g^{\alpha})^a)\}$

Keygen (ID,MSK) : SK

ID="bob", $SK=H_1(\text{"bob"})^{\alpha}$

Dec (CT,SK) : M

$CT\{U,V\}$

$M=V \oplus H_2(e(SK,U))$

$M=M \oplus H_2(e(H_1(\text{"bob"}), g^{\alpha})^a)\} \oplus H_2(e(H_1(\text{"bob"})^{\alpha}, g^a)$

H1,H2: Hash Function

H = f(h(m)): SWU(Shallue-WoestijneUlas), Icart function

ABE
Attribute-Based Encryption

ABE: Attribute-Based Encryption

FUZZY IBE[5]

- ✓ In Fuzzy IBE, the author extend a single identity into multiple identities
- ✓ The total set of identity is called **Identity Universe**
- ✓ The message is encrypted with some identities
- ✓ The receiver whose key contains identities match with The encrypted identities could be able to decrypt the cipher text

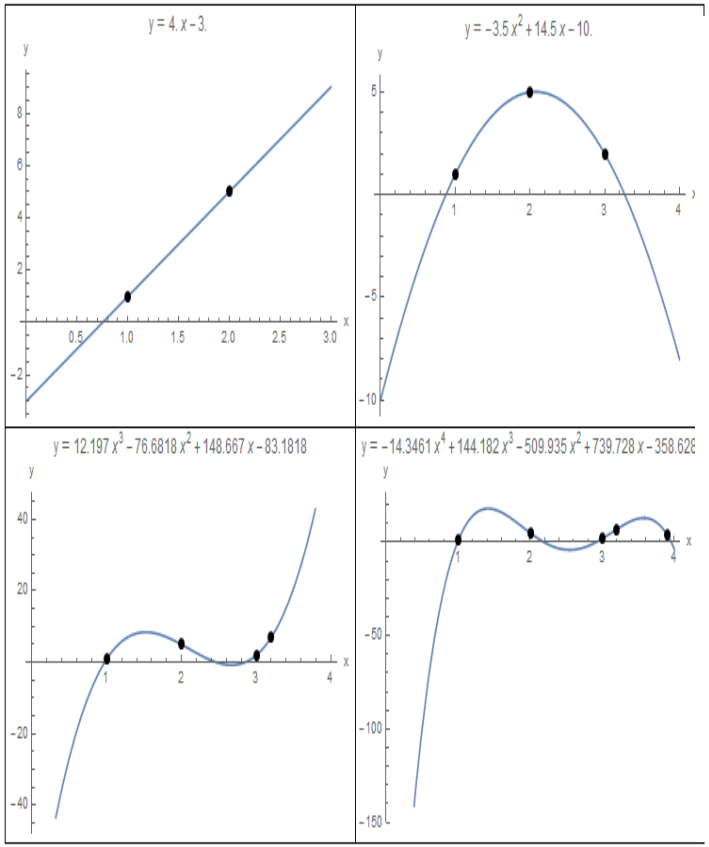
Suppose:

- U: Identity Universe
- $\omega \in U$: Identity encrypt in the cipher text
- $\acute{\omega}$: (where $|\omega \cap \acute{\omega} \geq d|$) Identity in the key that could decrypt the cipher text

ABE: Attribute-Based Encryption

FUZZY IBE[5]

Prior Knowledge: Shamir Secret Sharing[6]



Given a set of $k + 1$ data points where no two x_j are the same

$$(x_0, y_0), \ldots, (x_j, y_j), \ldots, (x_k, y_k)$$

$$L(x) := \sum_{j=0}^{k} y_j \ell_j(x)$$

$$\ell_j(x) := \prod_{\substack{0 \le m \le k \\ m \ne j}} \frac{x - x_m}{x_j - x_m}$$

$$= \frac{(x - x_0)}{(x_j - x_0)} \cdots \frac{(x - x_{j-1})}{(x_j - x_{j-1})} \frac{(x - x_{j+1})}{(x_j - x_{j+1})} \cdots \frac{(x - x_k)}{(x_j - x_k)}$$

ABE: Attribute-Based Encryption

FUZZY IBE[5]

Set up (λ) : PP, MSK

$MSK = \{t_1,\ldots,t_{|u|}\}$, $PP=\{T_1=g^{t1},\ldots,T_u=g^{tu}, Y=e(g,g)^y\}$

Enc (M,ID,PP) : CT

$CT=\{\acute{\omega}, E'=MY^s, \{E_i=T_i^s\}$ where $i\in\acute{\omega}\}$

Keygen (ID,MSK) : SK

$\omega\in U$, $q(0) = y$

$SK=\{D_i, i\in\omega\}$ $D_i=g^{q(i)/ti}$

Dec (CT,SK) : M

$M=E'/\prod_{i\in s}(e(D_i,E_i))^{\Delta i,s(0)}$

$M=M.e(g,g)^{sy}/\prod_{i\in s}(e(g^{q(i)/ti}, T_i^s))^{\Delta i,s(0)}$

$M=M.e(g,g)^{sy}/\prod_{i\in s}(e(g^{q(i)/ti}, g^{st(i)}))^{\Delta i,s(0)}$

$M=M.e(g,g)^{sy}/\prod_{i\in s}(e(g, g)^{sq(i)})^{\Delta i,s(0)}$

$M=M.\cancel{e(g,g)^{sy}}/\cancel{e(g, g)^{sy}}$

Shamir Secret Sharing

ABE: Attribute-Based Encryption

What is Attributed-Based Encryption[7]?

- ✓ In ABE, the author change the ideas of multiple identities into attributes
- ✓ The total set of attribute is called **Attributes Universe**
- ✓ The message is encrypted with some attributes in the form of **policy access structure**.
- ✓ The receiver whose key contains attributes match with the encrypted attributed policy could be able to decrypt the cipher text

ABE: Attribute-Based Encryption

ABE[7,8]

Set up (λ) : PP, MSK

$MSK = \{g^{\alpha},\beta\}$, $PP=\{G_0,g,h=g^{\beta},f=g^{1/\beta}, Y=e(g,g)^{\alpha}\}$

Enc (M,P,PP) : CT

$CT=\{P, C'=MY^{s},C=h^{s},C_y=g^{\lambda i}, C_{y'}=H(i)^{\lambda i}\}$

Keygen (ID,MSK) : SK

$SK=\{D=g^{(\alpha+r)/\beta},D_i=g^{r}.H(i)^{ri},D_{i'}=g^{ri}\}$

Dec (CT,SK) : M

$M=C'/e(C,D)/e(C_y,D_i)/e(C_{y'},D_{i'})$

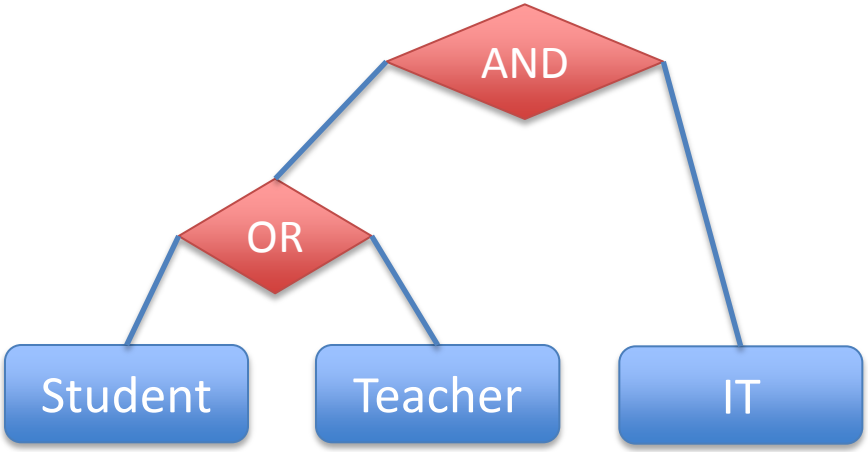
ABE: Attribute-Based Encryption

Cipher Text

Message

Secret Key

Policy Access Structure

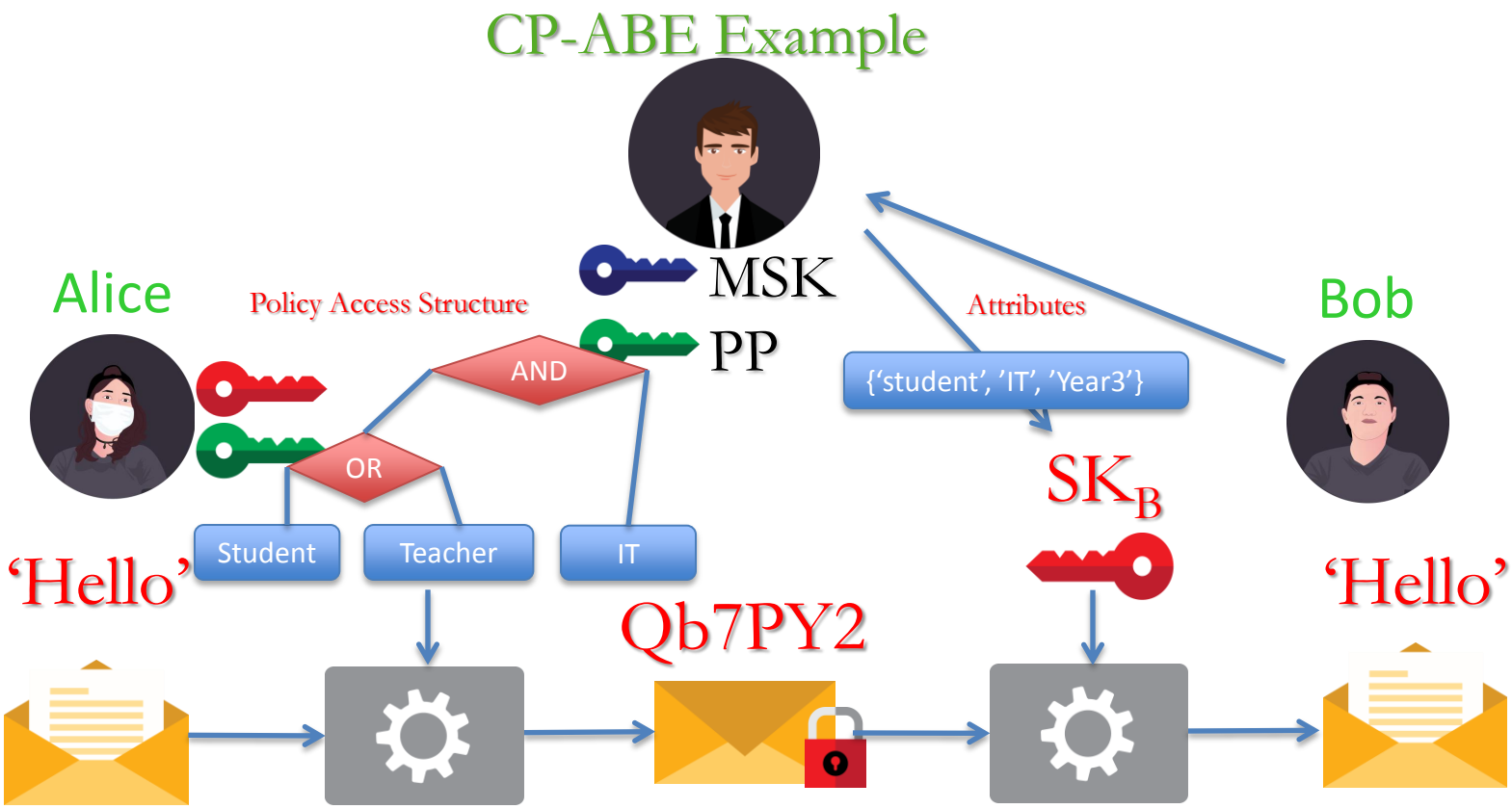


Attributes

{‘student’, ’IT’, ’Year3’}

CP-ABE / KP-ABE

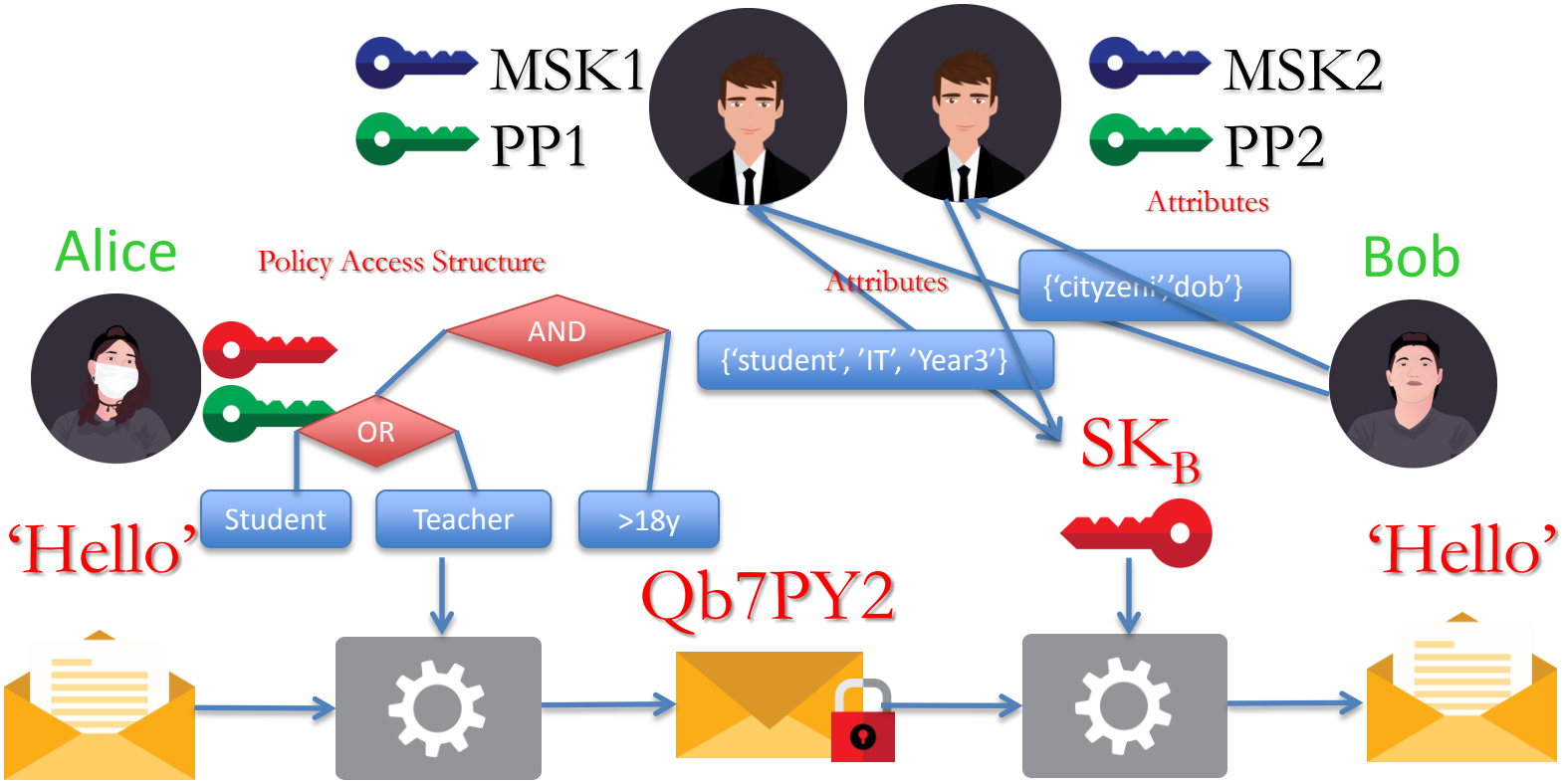
ABE: Attribute-Based Encryption



Set up | Enccryption | Keygen | Decryption

MAA-CP-ABE

Multi-Attribute Authorities Cipher Text-Policy Attribute-Base Encryption[9]



Set up | Enccryption | Keygen | Decryption

References

References

[1] W.Diffie and M. E. Hellman. 1976. New directions in cryptography. IEEE Transactions on Information Theory (1976).
[2] C. Costello. Pairings for Beginners. https://www.craigcostello.com.au/pairings/PairingsForBeginners.pdf
[3] A. Shamir. 1984. Identity-based cryptosystems and signature schemes. Advances in Cryptology - Crypto' 84 (1984).
[4] Matthew K. Franklin Dan Boneh. 2001. Identity-based encryption from the Weil pairing. In Proceddings of the 21st Annual International Cryptology Conference on Advances in Cryptology, Pages 213-229. Springer-Verlag (2001).
[5] B. Waters A. Sahai. 2005. Fuzzy Identity Based Encryption. In Advances in Cryptology-Ecurocrypt, volume 3494 of LNCS, pages 457-473. Springer (2005).
[6] Adi Shamir. 1979. How to share a secret. Communications. ACM, 22(11):612-613.
[7] A. Sahai B. Waters V. Goyal, O. Pandey. 2006. Attribute Based Encryption for Fine-Grained Access Control of Encrypted Data. In ACM conference on Computer and Communications Security (ACM CCS) (2006).
[8] B. Waters J. Bethencourt, A. Sahai. 2007. Ciphertext-Policy Attribute-Based Encryption. IEEE Symposium on Security and Privacy (SP'07) (2007).
[9]Y. Rouselakis, B. Waters. 2015. Efficient Statically-Secure Large_Universe Multi-Authority Attribute-Based Encryption. https://eprint.iacr.org/2015/016.pdf
[10] A. Joux. 2000. A one round protocol for tripartite Diffie-Hellman. Proc. Fourth Algorithmic Number Theory Sumposium, Lecture Notes in Computer Science, Vol. 1838, Springer-Verlag, pp. 385-394 (2000).

THANK YOU
Q&A
DEMO

Diffie-Hellman Key Exchange

Diffie-Hellman Key Exchange[1]

Alice

Eve

Bob

$SK_A = a$

$PK_A = g^a \% p$

$SK_B = b$

$PK_B = g^b \% p$

PK_A →

← PK_B

Share Secret Key

$SSK=(g^b)^a \% p$

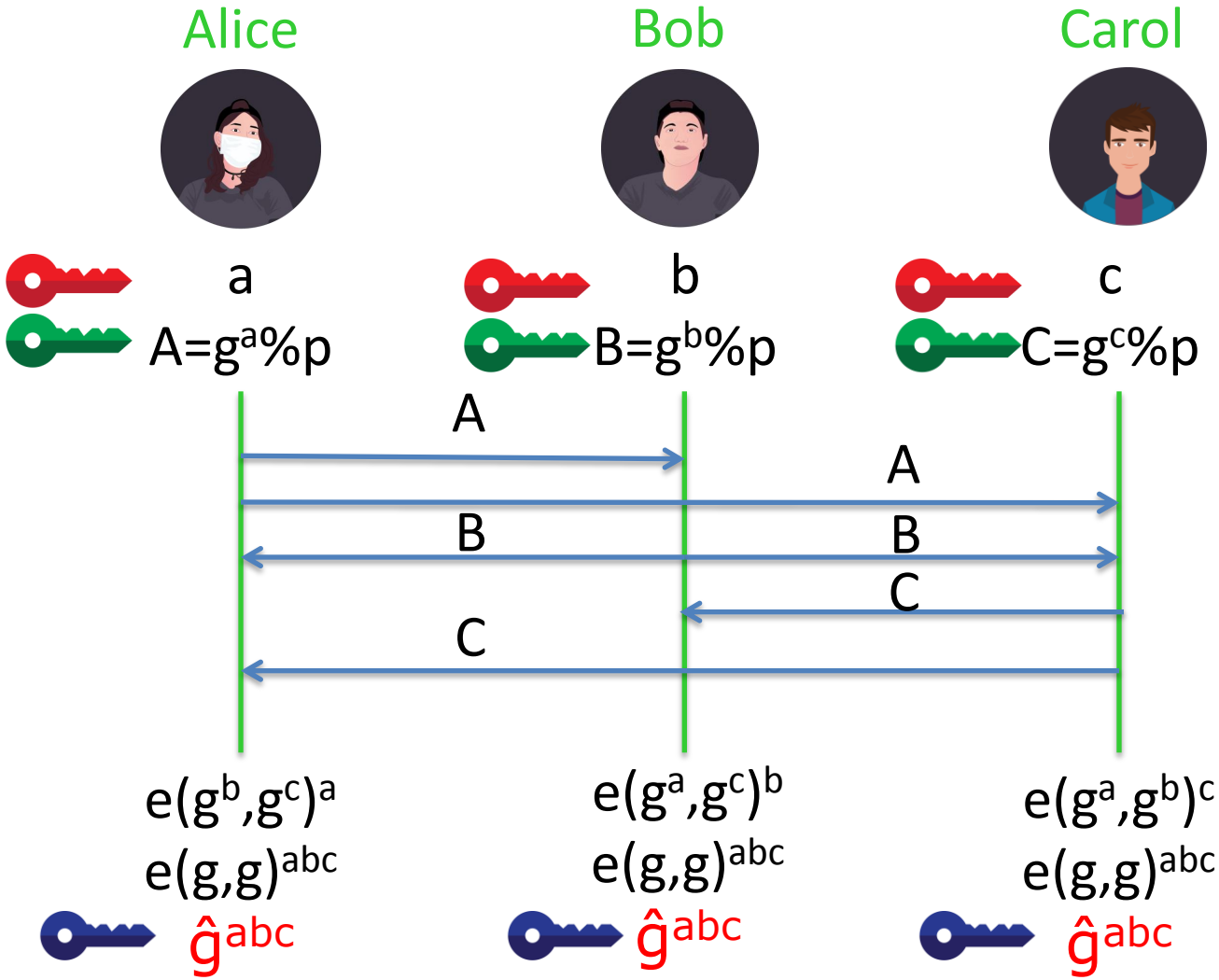
Share Secret Key

$SSK=(g^a)^b \% p$

Discret Log	g , g^x	→	x
CDH	g , g^x, g^y	→	g^{xy}

g : generator

p: prime number

JOUX Protocol

Joux Protocol[10]