Sécurité de l'information
Introduction à la cryptologie
"Les Principes"

Stéphane Ballet

20 février 2014

C.N.R.S. Institut de Mathématiques de Marseille
Luminy Case 930, F13288 Marseille CEDEX 9
e-mail : stephane.ballet@univ-amu.fr

Plan

Théorie de l'information

Sécurité de l'information

Cryptologie

Cryptographie

Cryptanalyse

Les couches sectorielles de l'activité de recherche

GL algorithmique

Protocoles, systèmes complexes
Techniques cryptographiques
Techniques mathématiques
Mathématiques pures et effectives

GL = Grille de lecture

La grille de lecture algorithmique

La complexité algorithmique

Objet : étude du nombre d'opérations (estimation) nécessaire pour effectuer un algorithme accomplissant une tâche particulière.

Exemple : $a \in G$, où G est un groupe fini avec certaines propriétés (ex : $G = \mathbb{Z}/n\mathbb{Z}$).

- Calcul d'une puissance (a, n) : $a^n \longrightarrow$ coût : $O(\log n)$

La complexité est linéaire en la taille de l'entrée n.

- Calcul du log discret $(z = a^n, a)$: $a^n \longrightarrow$ coût : $O(n)$

La complexité est expontielle en la taille de l'entrée n.

Un calcul ou un algorithme est considéré comme :

- **facile ou "faisable en temps raisonnable"** : si son exécution peut se faire **en temps polynomial** : la complexité est polynomiale en la taille de l'entrée.

- **difficile ou "infaisable en temps raisonnable"** : si son execution ne peut se faire qu'**en temps exponentiel** : la complexité est exponentielle en la taille de l'entrée.

Quelques techniques cryptographiques :

- **Buts :**
  - secret, confidentialité, chiffrement.
  - Intégrité des données : prévention d'une modification non autorisée.
  - Authentification (ou identification) :
  - Non-répudiation : mécanisme empêchant de nier un contrat.
  - Signature : mécanisme qui garantit l'authentification, l'intégrité et la non-répudiation.
  - Gestion des clés : distribution, intégrité.

Principes généraux

La notion de clé : une clé est un paramètre utilisé en entrée d'une opération cryptographique (chiffrement, déchiffrement, signature numérique, vérification de signature).

Principe de Kerckhoff : "Le sécurité du système doit reposer sur la robustesse de la clé."

Et non pas sur le fait que : le système de chiffrement est inconnu de l'ennemi.

La cryptanalyse :

- attaquer et casser les cryptosystèmes.

- la sécurité des cryptosystèmes.

La sécurité parfaite :

Aucune information sur **le message clair** ou **la clé secrète** ne peut être obtenue à partir du **"message chiffré"**.

La sécurité calculatoire :

- l'impossibilité de réaliser en pratique certains calculs.

- la théorie de la complexité algorithmique :

  - évaluation du temps d'exécution
  - étude de la résistance des fonctions cryptographiques.

Cryptographie à clé secrète

Cryptographie à clé secrète (ou symétrique) :

- l'expéditeur et le destinataire doivent partager une clé secrète K.

- la clé K sert à la fois au chiffrement et au déchiffrement.

- Les deux interlocuteurs disposent d'une **fonction publique de chiffrement** E et d'une **fonction publique de déchiffrement** D.

Problème : *le partage de la clé secrète*.

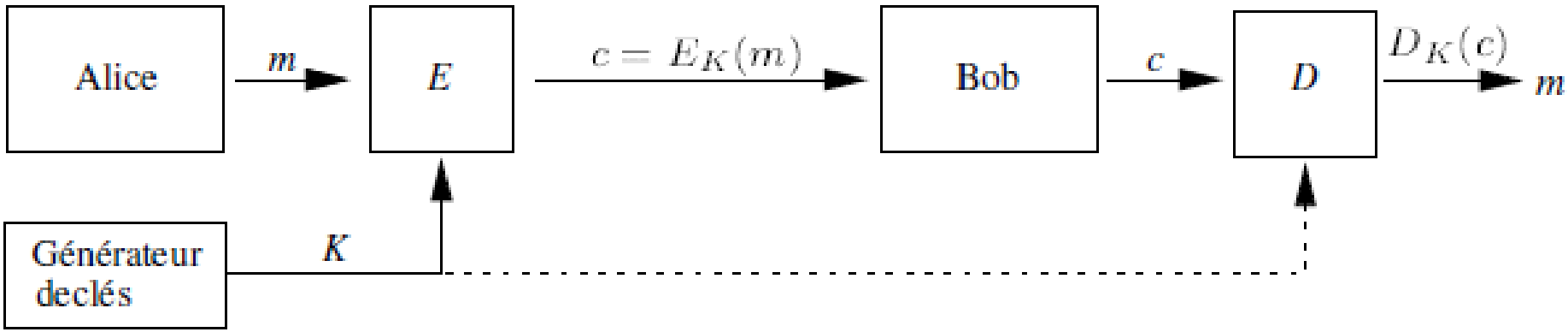


Figure 1.1. *Schéma classique d'un système de chiffrement à clé secrète*

1) Le chiffrement à flot

Exemple : Le chiffrement de Vernam ou One Time Pad

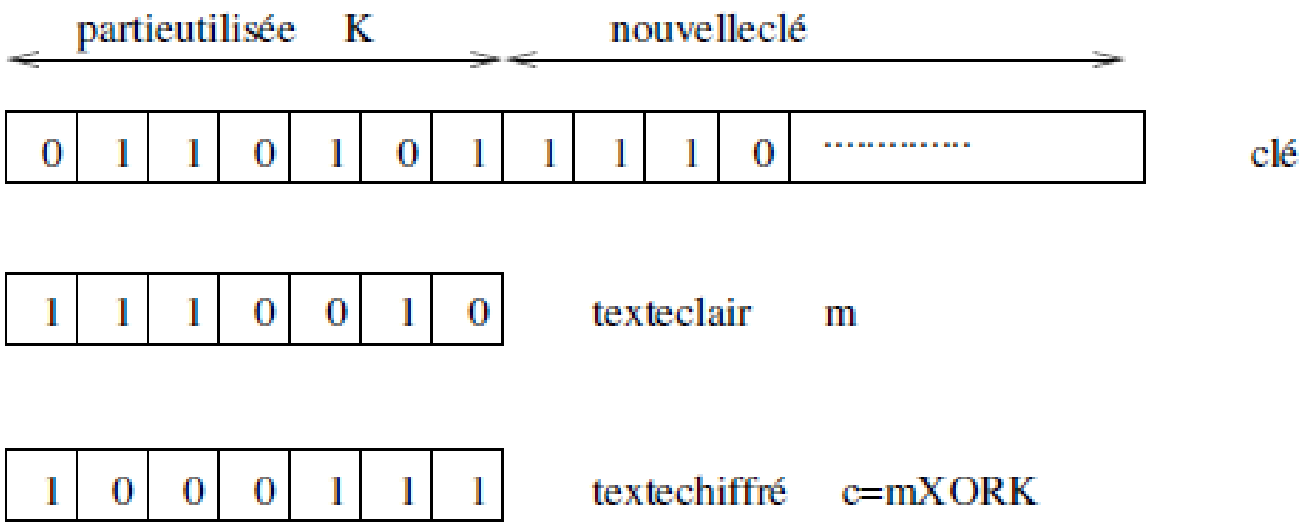


Figure 1.2. *Le masque jetable*

Théorème de Shannon :

La sécurité parfaite pour un chiffrement symétrique n'est atteinte que si :

- la longueur de la clé est aussi longue que le message.

- l'ensemble des clés est équiréparti.

2) Le chiffrement par bloc

Exemple : Le système AES (Advanced Encryption Standard, 1998)

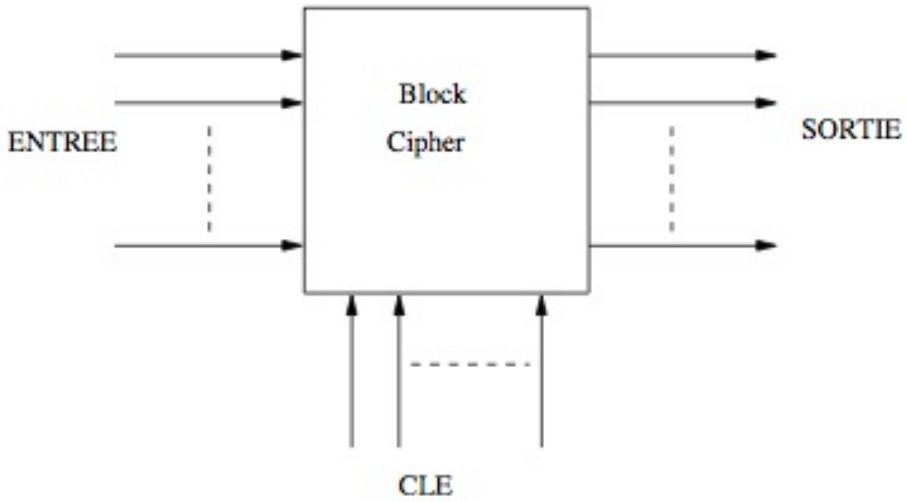
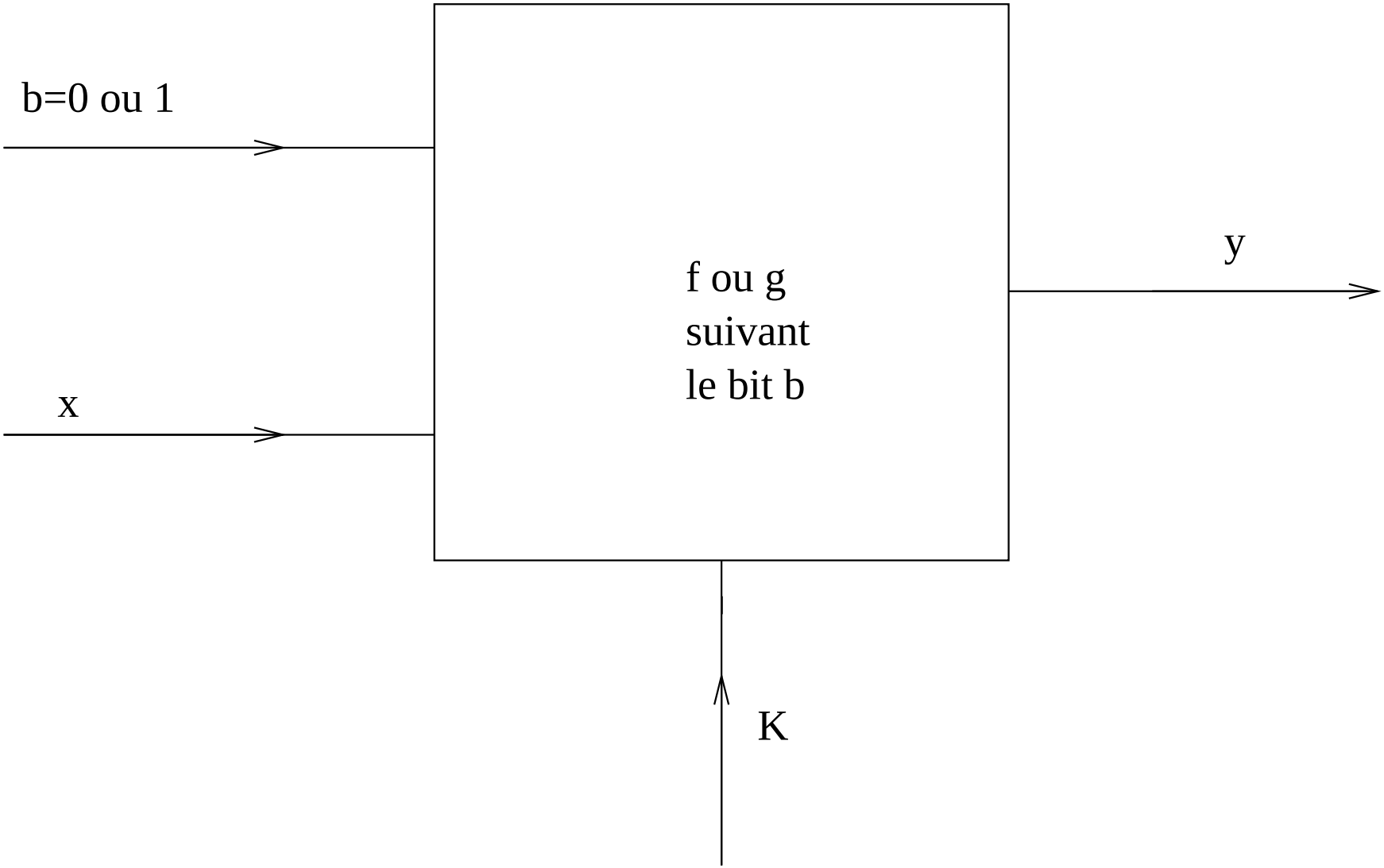


Figure 1.3. *Chiffrement par bloc*


b=0 ou 1
x
f ou g
suivant
le bit b
y
K

Principes généraux :

- La confusion : structures algébriques et statistiques.

- La diffusion : nombre de modifications de bits de sortie.

Contre-exemple : le système One Time Pad.

Dans les systèmes actuels :

- N_r itérations d'une fonction de tour "cryptographiquement faible" à l'aide d'une clé de tour K_r.

- augmentation de la sécurité du système

Problème : compromis entre sécurité et efficacité.

" Most ciphers are secure after sufficiently many rounds"
(L. O'Connor)

" Most ciphers are too slow after sufficiently many rounds"
(J. Massey)

Cryptographie à clé publique

Cryptographie à clé publique ou asymétrique

Chaque utilisateur A possède :

- une **clé publique** e_A connue de tous, publiée sur un serveur ;
- une **clé privée** d_A qui n'est connue que de A.

On dispose par ailleurs de deux fonctions publiques :

- une fonction de **chiffrement** f qui à un texte clair x et à la clé publique e_A fait correspondre le texte chiffré $y = f(x, e_A)$ à destination de A ;
- une fonction de **déchiffrement** g qui au texte chiffré y et à la clé privée d_A redonne le texte clair $x = g(y, d_A)$.

  Cette fois, **il n'y a plus besoin d'échanger une clé secrète**.

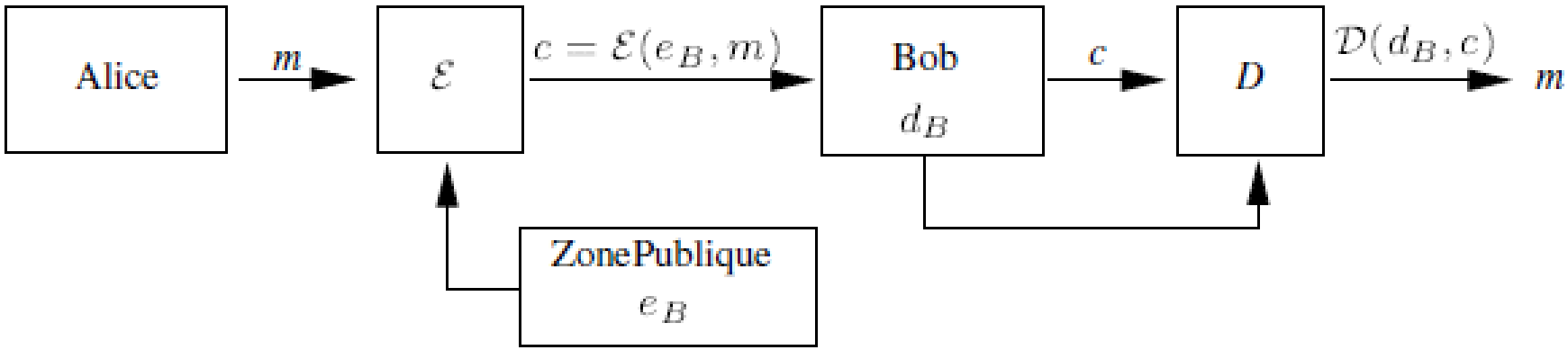
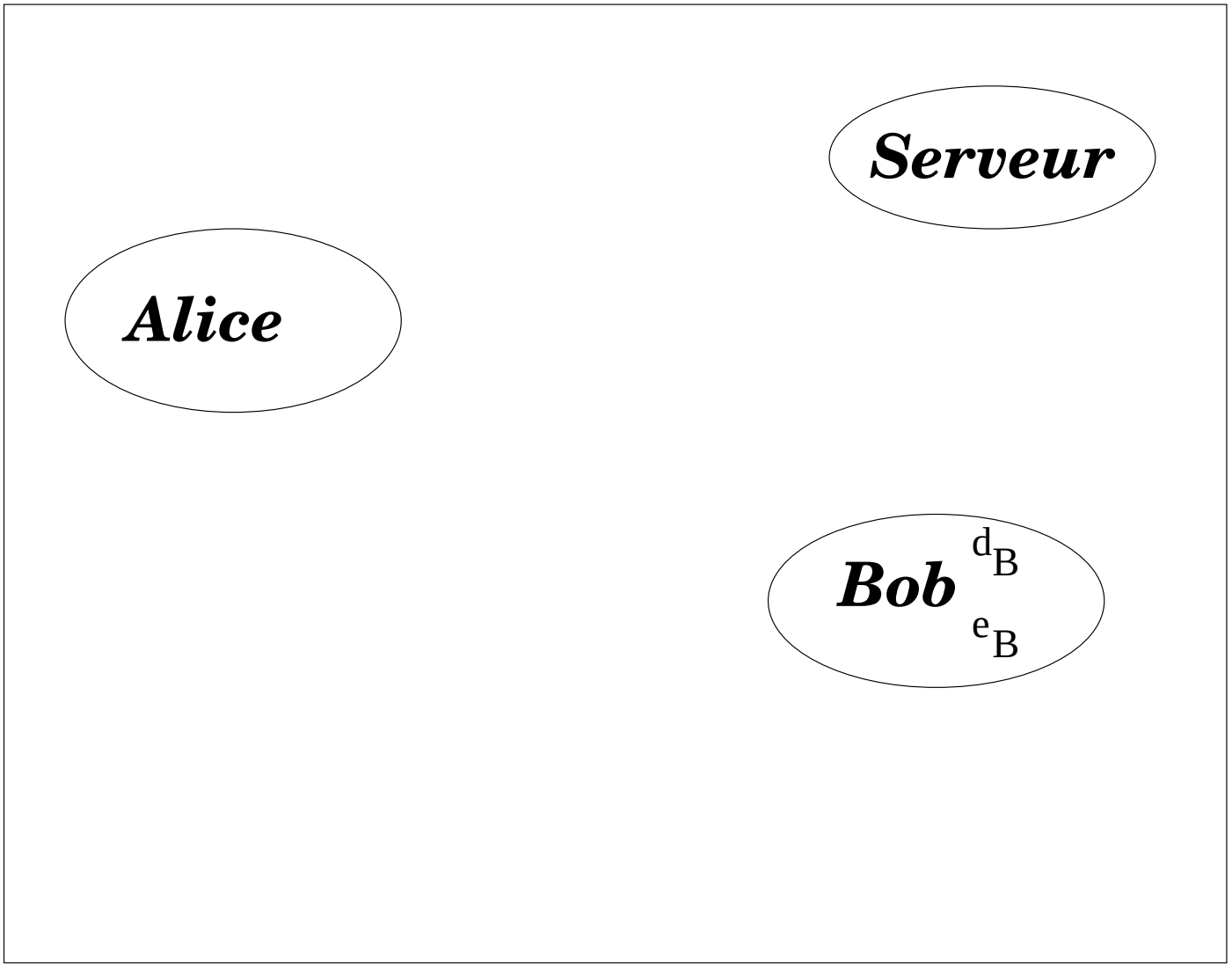
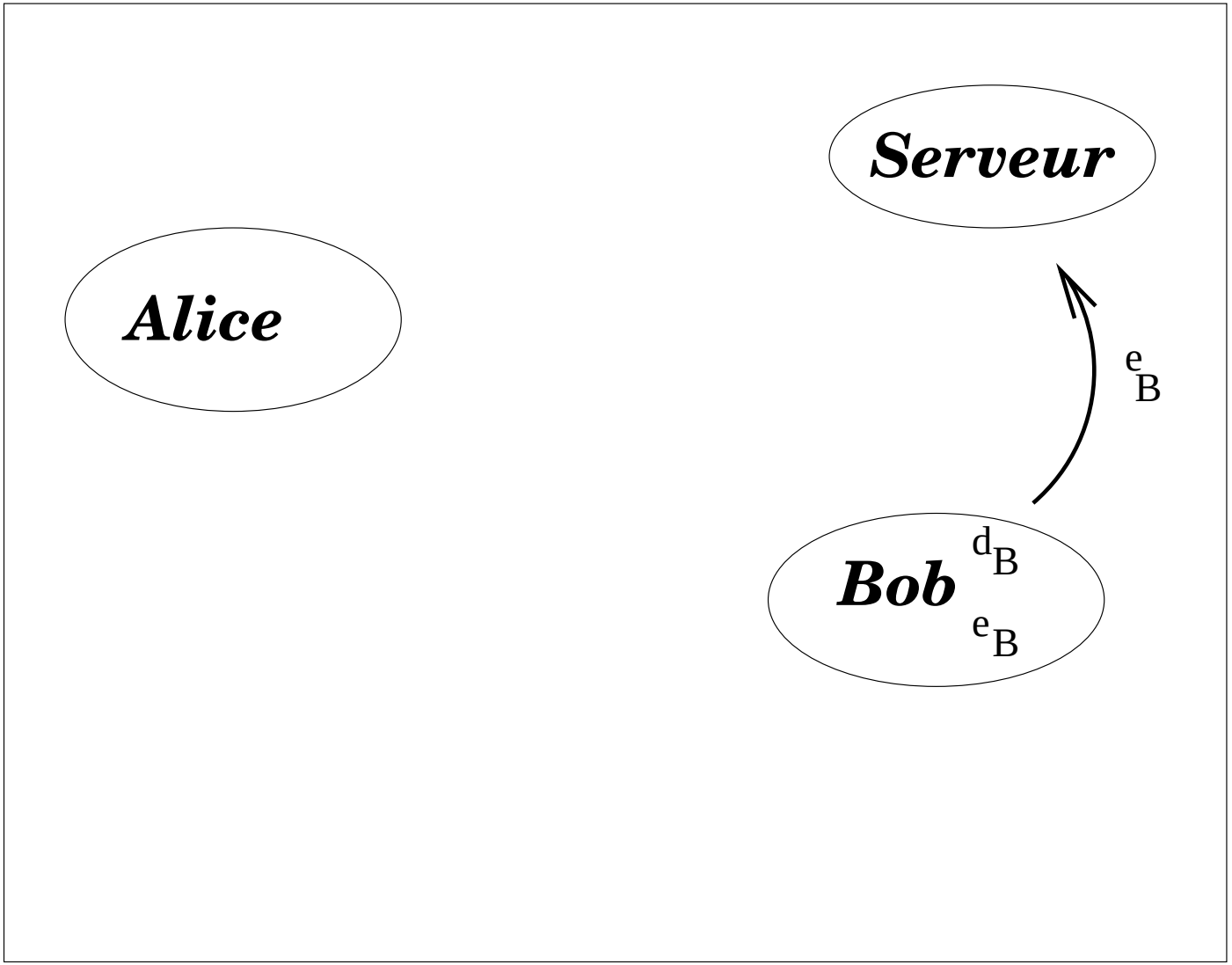
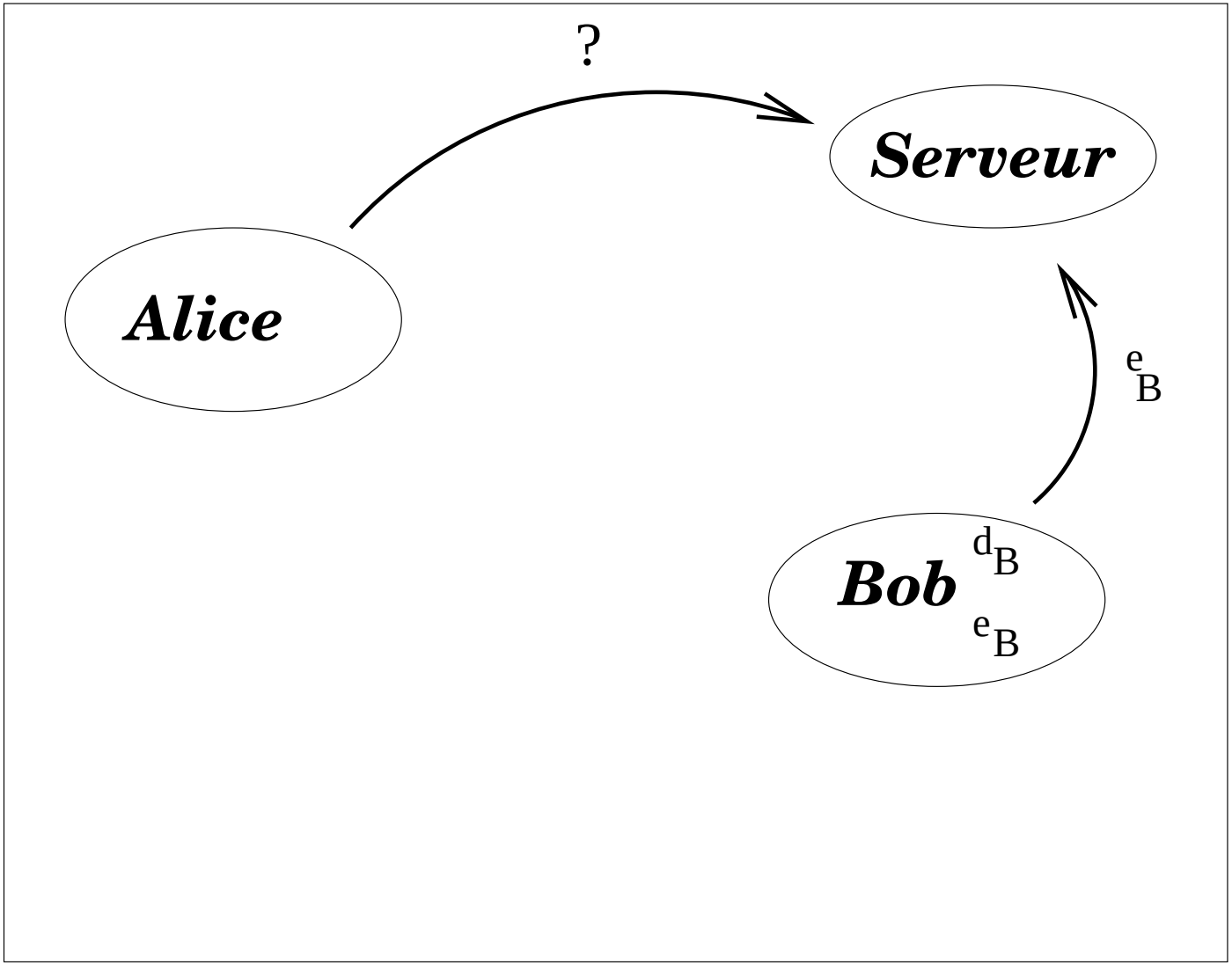
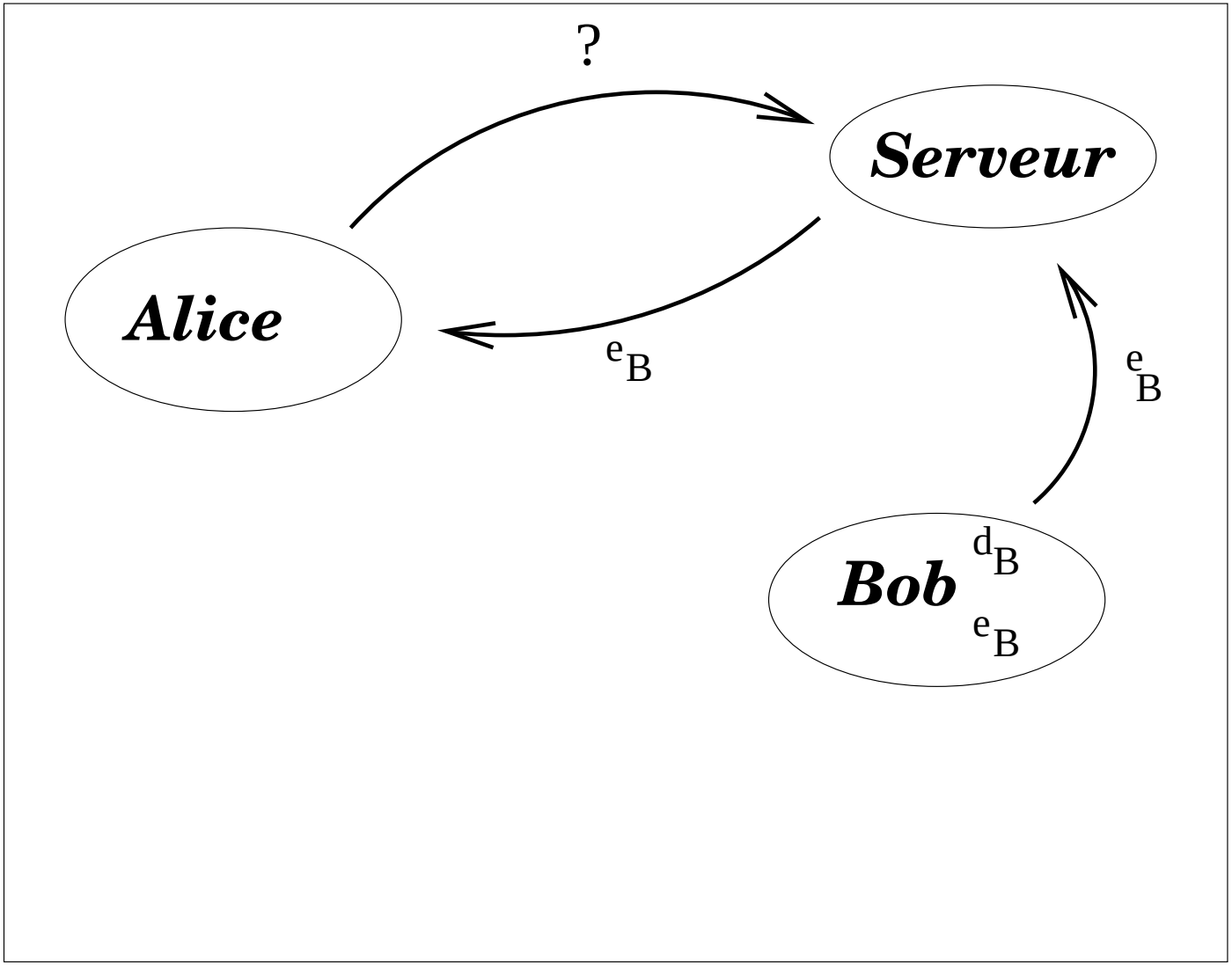


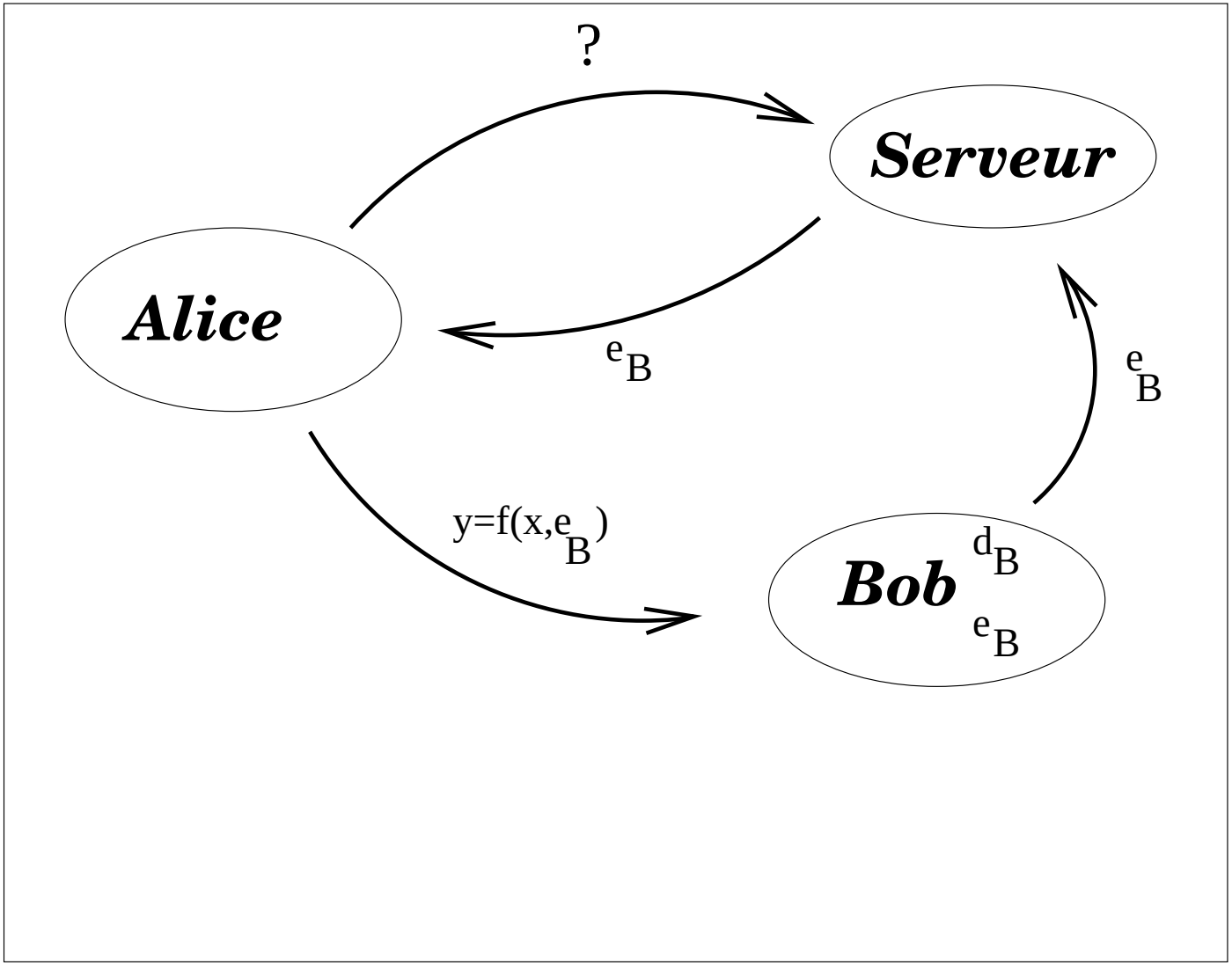
Figure 1.4. *Schéma classique d'un système de chiffrement à clé publique*

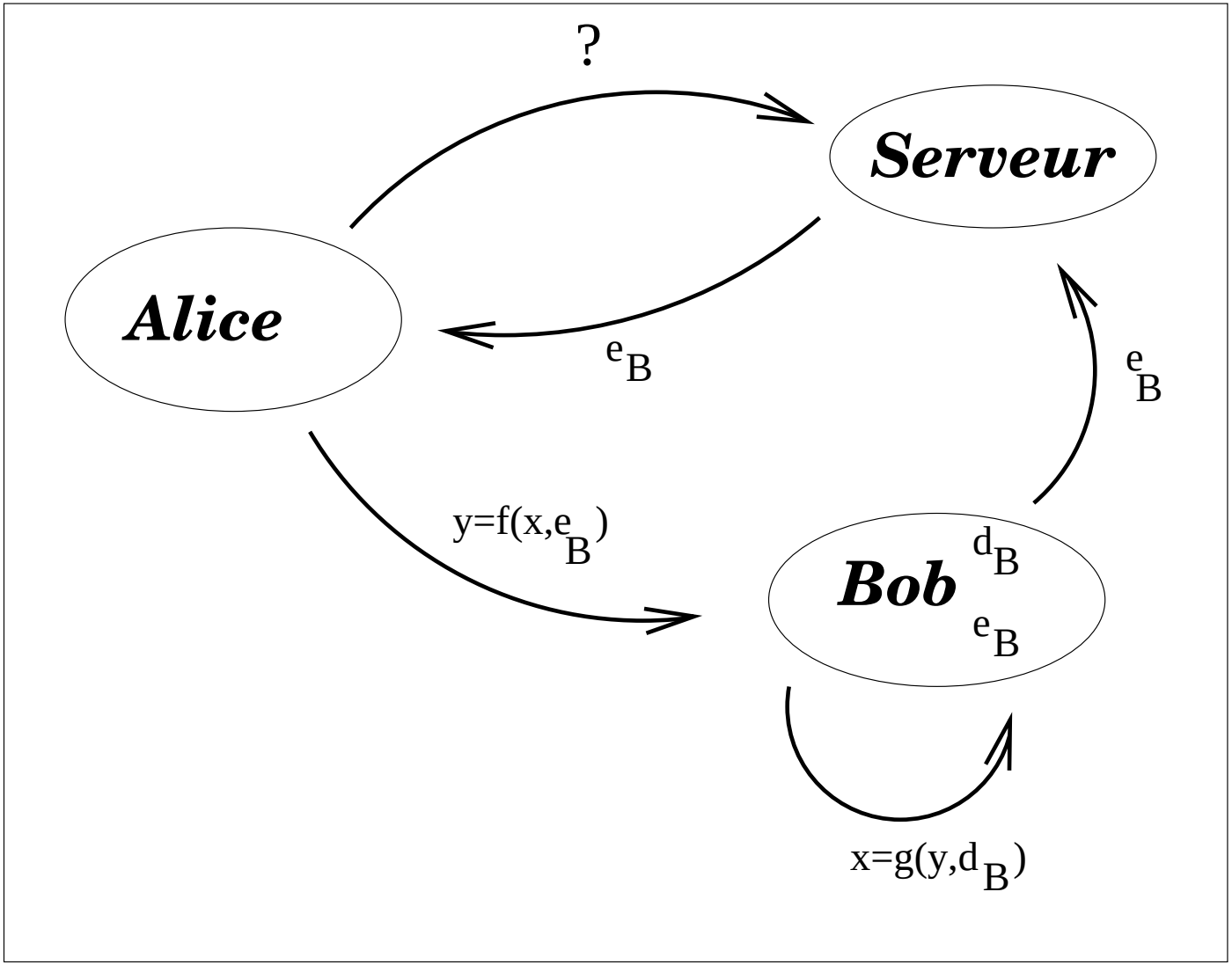

Serveur
Alice
Bob
d_B
e_B


Serveur
Alice
e_B
Bob
d_B
e_B


?
Serveur
Alice
e_B
Bob
d_B
e_B


?
Serveur
Alice
e_B
e_B
Bob
d_B
e_B


?
Serveur
Alice
e_B
e_B
$y=f(x,e_B)$
Bob
d_B
e_B


?
Serveur
Alice
e_B
e_B
$y=f(x,e_B)$
Bob
d_B
e_B
$x=g(y,d_B)$

Fonctions à sens unique

Les systèmes à clé publique sont construits à partir de :

- **fonctions à sens unique** c'est-à-dire de fonctions qu'il est facile de calculer, mais difficile à inverser,
  - facile à calculer : $y = f(x)$
  - quasi-impossible à calculer : étant donné y trouver x tel que $f(x) = y$.

Exemple : le fonction $E_\alpha(x) = \alpha^x$

- **fonctions à sens unique avec trappe (ou brèche secrète)** c'est-à-dire des fonctions à sens unique qui deviennent facile à inverser si on connait une valeur secrète.

Les problèmes réputés difficiles

La plupart des problèmes mathématiques qui donnent naissance à des fonctions à sens unique sont issus de l'arithmétique :

- **le problème de la factorisation** : soit n un nombre produit de deux grands nombres premiers p et q ; retrouver p et q à partir de n ;
- **le problème du logarithme discret**
- **extraction d'une racine carrée** modulo un produit de deux grands nombres premiers.

Quelques exemples

Rappel historique :

1976 : apparition de la cryptographie asymétrique avec le système de Diffie et Hellman.

1977 : apparition du système RSA développé par Rivest, Shamir et Adleman.

Le système RSA

Espace des clairs : $\mathbb{Z}/n\mathbb{Z}$.
Espace des chiffrés : $\mathbb{Z}/n\mathbb{Z}$.

Clé publique : (n, e) où $n = pq$ et $(e, \phi(n)) = 1$.

Clé privée : d tel que $ed \equiv 1 \pmod{\phi(n)}$.

Chiffrement

$$m \longrightarrow c = m^e \mod n.$$

Déchiffrement

$$c \longrightarrow m = c^d \mod n.$$

Tableau 2.1. *Le cryptosystème RSA*

Cryptosystèmes basés sur le PLD

Exemple :

$$G = (\mathbb{Z}/13\mathbb{Z})^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\},$$

où l'opération $\times$ se fait en prenant la multiplication habituelle modulo 13, c'est-à-dire par exemple :

$$6 \times 7 = (42 \mod 13) = 3.$$

On remarque que :

$2^0 = 1$	$2^4 = 3$	$2^8 = 9$
$2^1 = 2$	$2^5 = 6$	$2^9 = 5$
$2^2 = 4$	$2^6 = 12$	$2^{10} = 10$
$2^3 = 8$	$2^7 = 11$	$2^{11} = 7$

On dit que l'élément 2 engendre le groupe G.

Question : trouver m tel que $2^m = 5$.

Transcription en loi additive du PLD

Soit G un groupe additif engendré par un élément a.
Soit $b \in G$.

Trouver m tel que

$$m.a = \overbrace{a + a + \cdots a}^{m \text{ fois}} = b.$$

La cryptographie elliptique

La **cryptographie elliptique** repose sur **le problème de logarithme discret** dans le groupe des points d'une courbe elliptique sur un corps fini.

- **courbe elliptique sur un corps fini**.
- **la structure de groupe**.
- **cryptosystèmes basés sur les courbes elliptiques**.

Actuellement la cryptographie elliptique utilise essentiellement les corps finis premiers $\mathbb{Z}/p\mathbb{Z}$ ou ceux de caractéristique 2 (corps à 2^n éléments).

Courbe elliptique (CE)

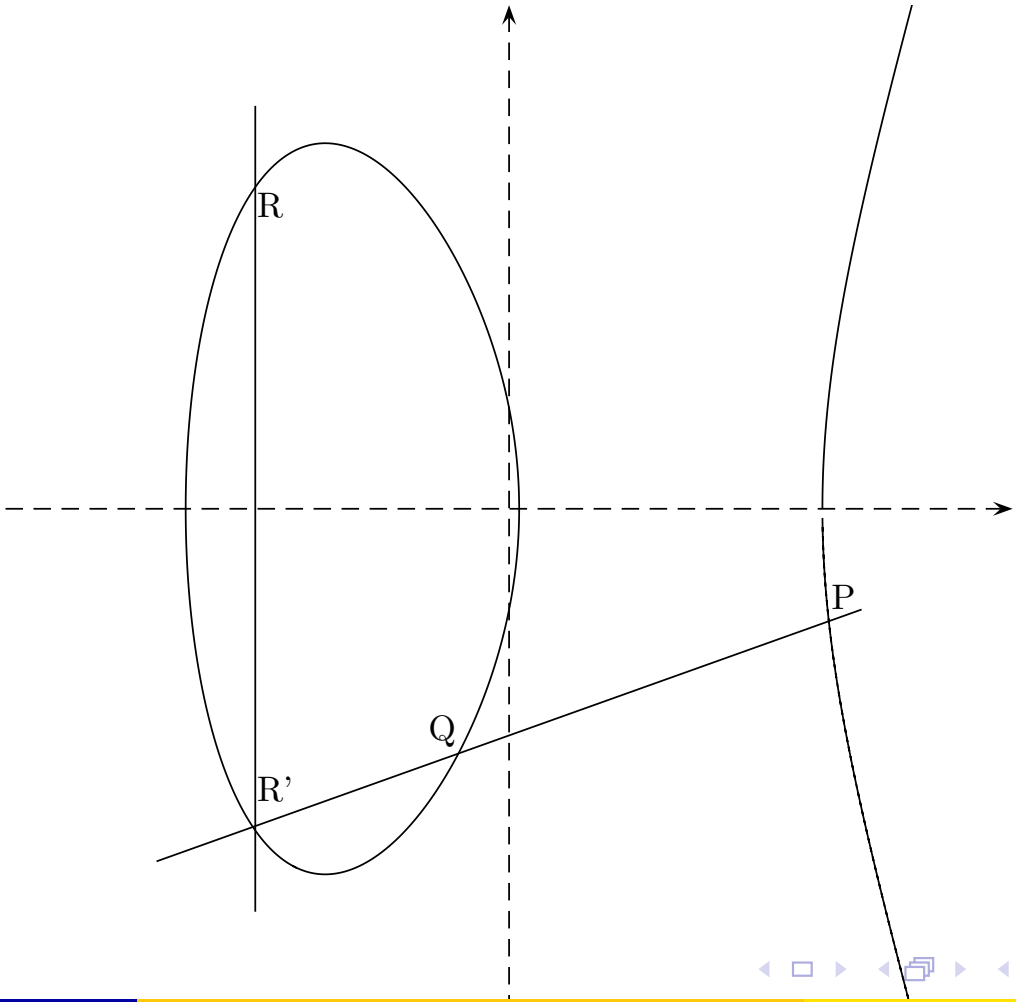
Définition :

Une courbe elliptique sur $\mathbb{Z}/p\mathbb{Z}$ avec p premier grand est une courbe d'équation (ou qui se ramène à cette équation) :

$$y^2 = x^3 + ax + b,$$

avec $4a^3 + 27b^2 \neq 0$.

La structure de groupe



Un exemple

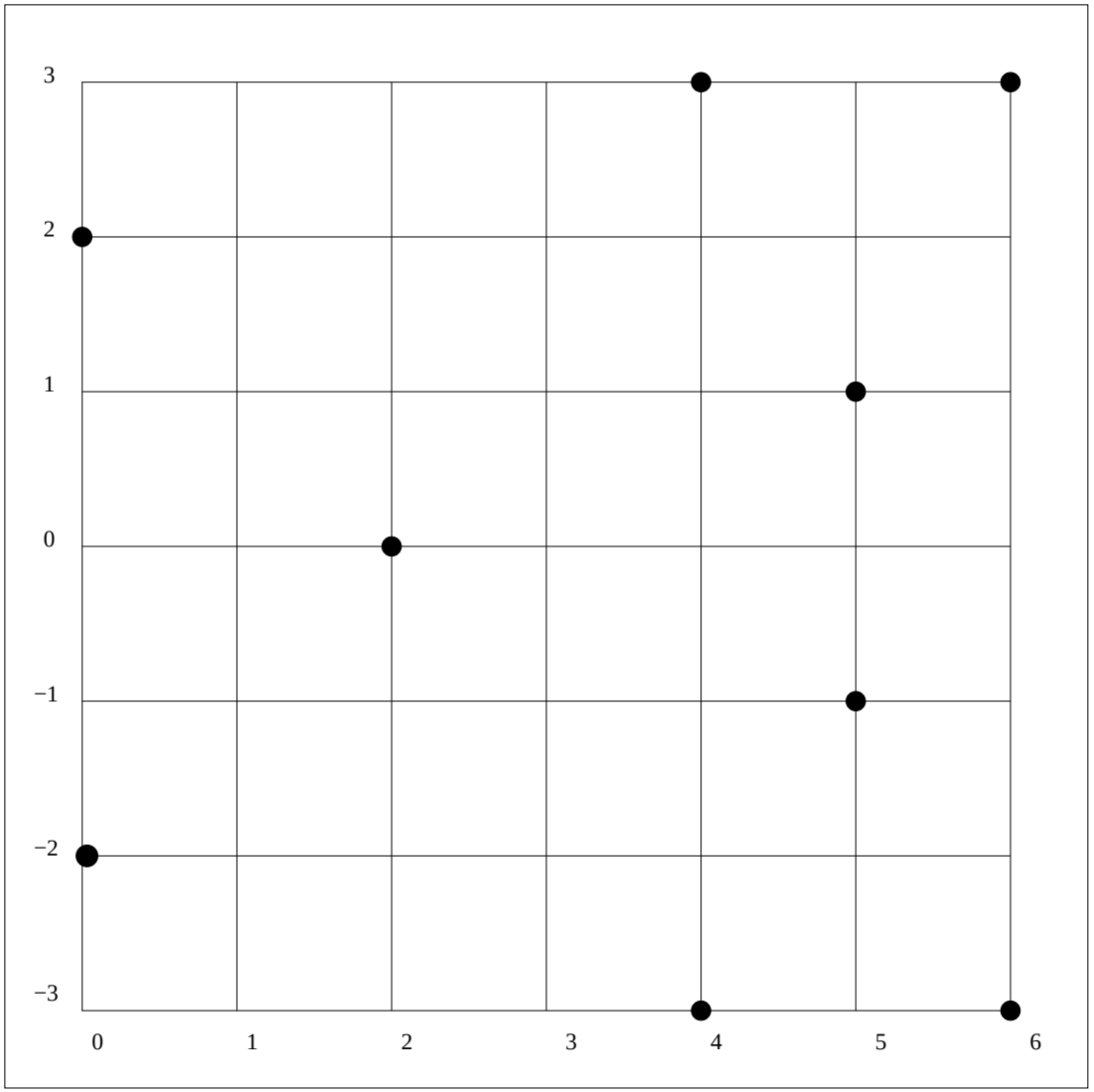
Prenons pour exemple $p = 7$ et la courbe d'équation :

$$y^2 = x^3 + x + 4.$$

Cette courbe a 10 point :

$(0,2)$	$(2,0)$	$(4,3)$	$(5,1)$	$(6,3)$	P_∞
$(0,5)$		$(4,4)$	$(5,6)$	$(6,4)$	

Le dessin



Une addition

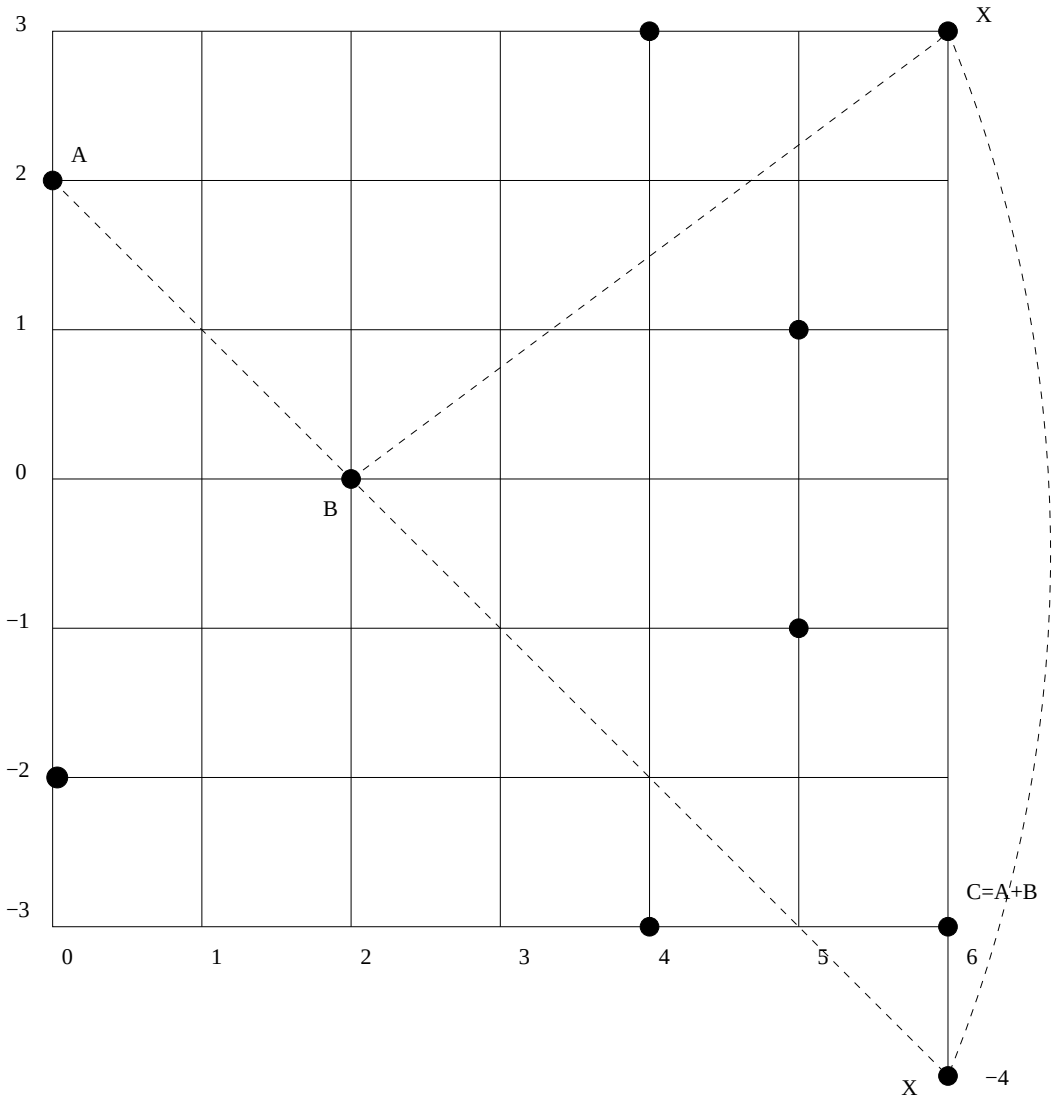


Table d'addition

$+$	$(0,2)$	$(2,0)$	$(4,3)$	$(5,1)$	$(6,3)$	$(0,5)$	$(4,4)$	$(5,6)$	$(6,4)$
$(0,2)$	$(4,4)$	$(6,4)$	$(0,5)$	$(4,3)$	$(2,0)$	P_∞	$(5,6)$	$(6,3)$	$(5,1)$
$(2,0)$	$(6,4)$	P_∞	$(5,6)$	$(4,4)$	$(0,5)$	$(6,3$	$(5,1)$	$(4,3)$	$(0,2)$
$(4,3)$	$(0,5)$	$(5,6)$	$(6,4)$	$(2,0)$	$(4,4)$	$(5,1)$	P_∞	$(0,2)$	$(6,3)$
$(5,1)$	$(4,3)$	$(4,4)$	$(2,0)$	$(6,3)$	$(0,2)$	$(6,4)$	$(0,5)$	P_∞	$(5,1)$
$(6,3)$	$(2,0)$	$(0,5)$	$(4,4)$	$(0,2)$	$(4,3)$	$(5,6)$	$(6,4)$	$(5,1)$	P_∞
$(0,5)$	P_∞	$(6,3)$	$(5,1)$	$(6,4)$	$(5,6)$	$(4,3)$	$(0,2)$	$(4,4)$	$(2,0)$
$(4,4)$	$(5,6)$	$(5,1)$	P_∞	$(0,5)$	$(6,4)$	$(0,2)$	$(6,3)$	$(2,0)$	$(4,3)$
$(5,6)$	$(6,3)$	$(4,3)$	$(0,2)$	P_∞	$(5,1)$	$(4,4)$	$(2,0)$	$(6,4)$	$(0,5)$
$(6,4)$	$(5,1)$	$(0,2)$	$(6,3)$	$(5,1)$	P_∞	$(2,0)$	$(4,3)$	$(0,5)$	$(4,4)$

Pourquoi la cryptographie elliptique

Avantages

- PLD sur une CE est plus résistant que sur les groupes multiplicatifs associés aux corps finis (Ex : $\mathbb{Z}/p\mathbb{Z}$).

- les tailles de clé à prendre pour la même résistance sont plus petites.

Par exemple :

- 1024 bits pour RSA

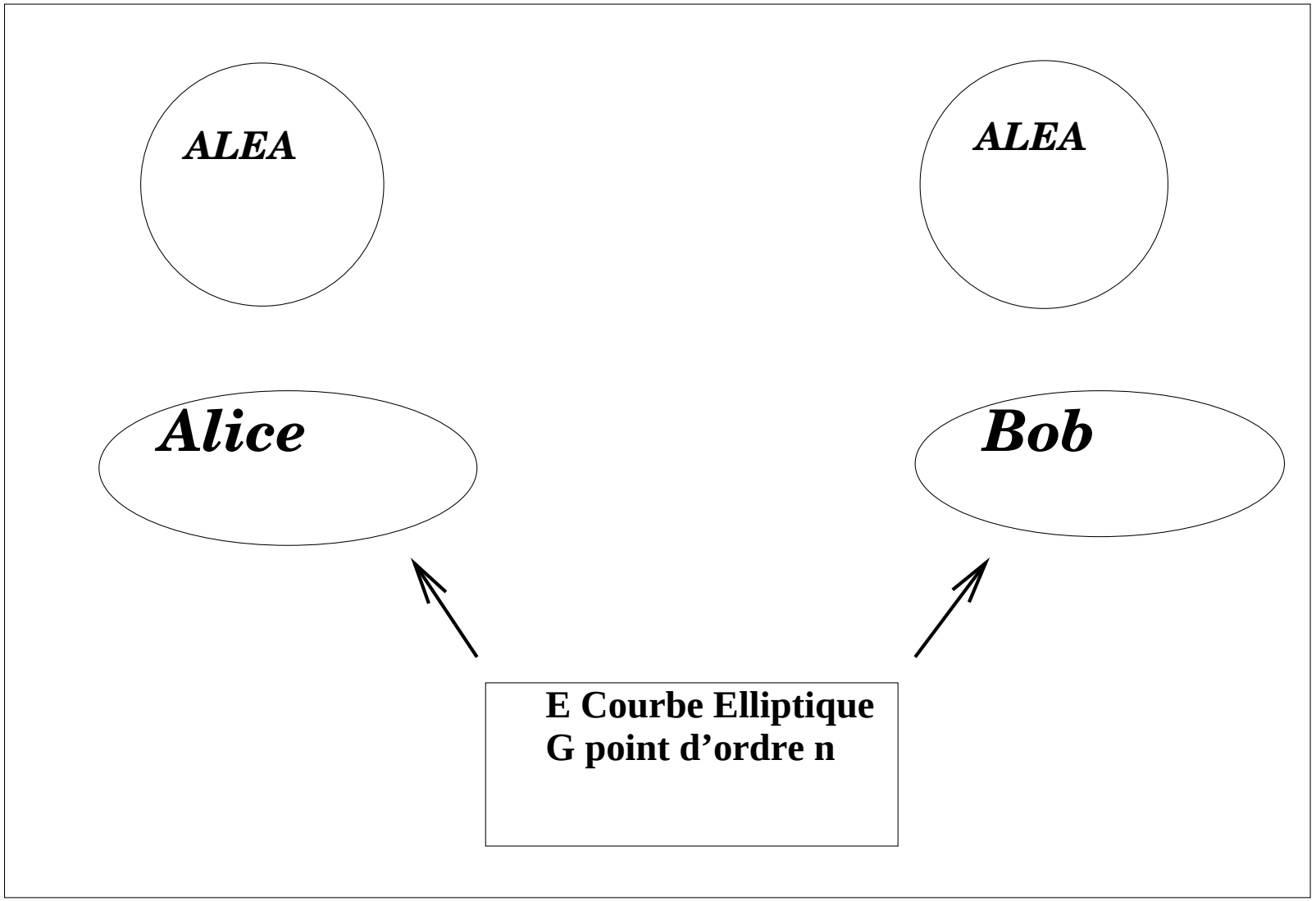
- 160 bits pour un chiffrement ou une signature à base de courbe elliptique.

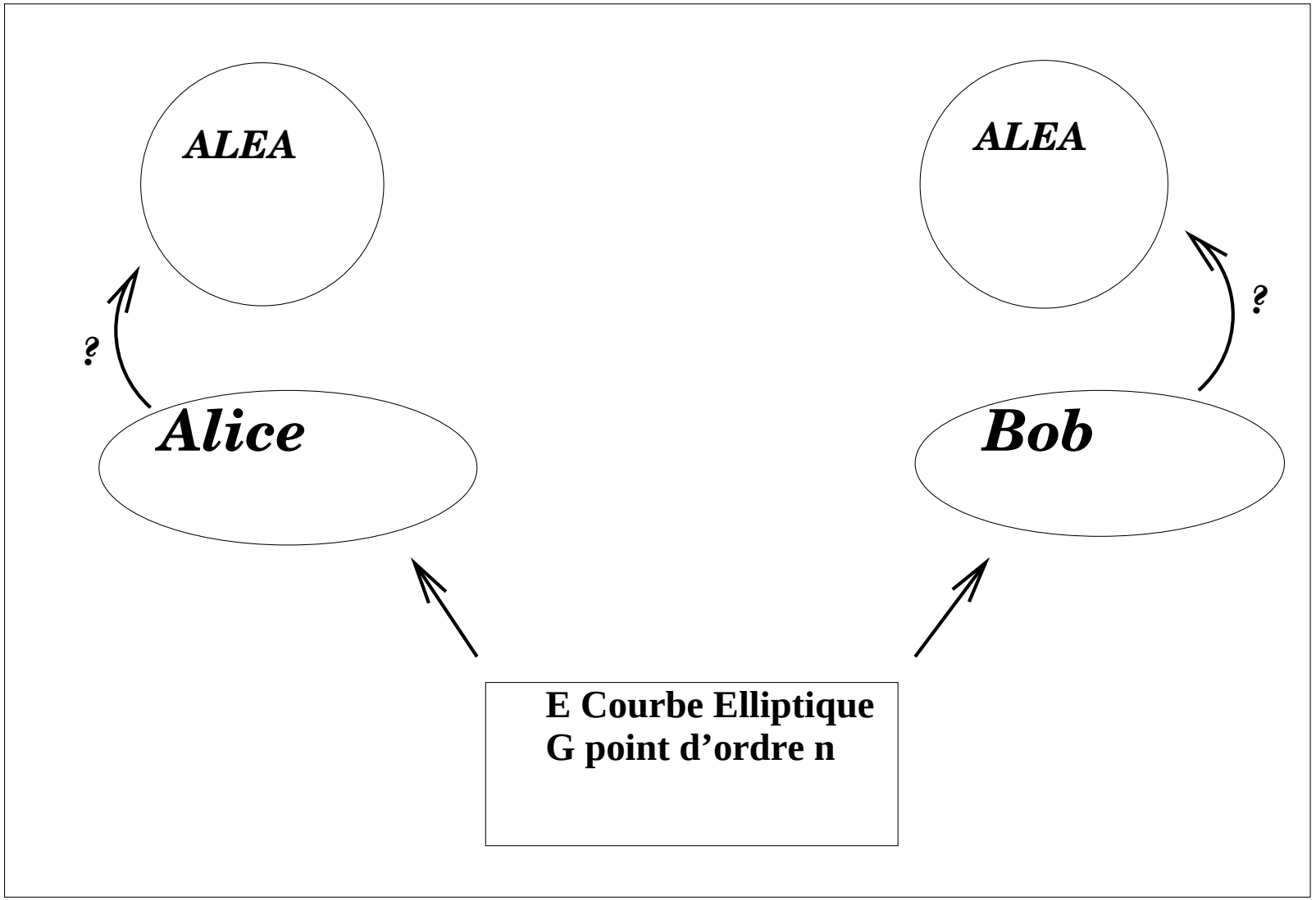
Inconvénients

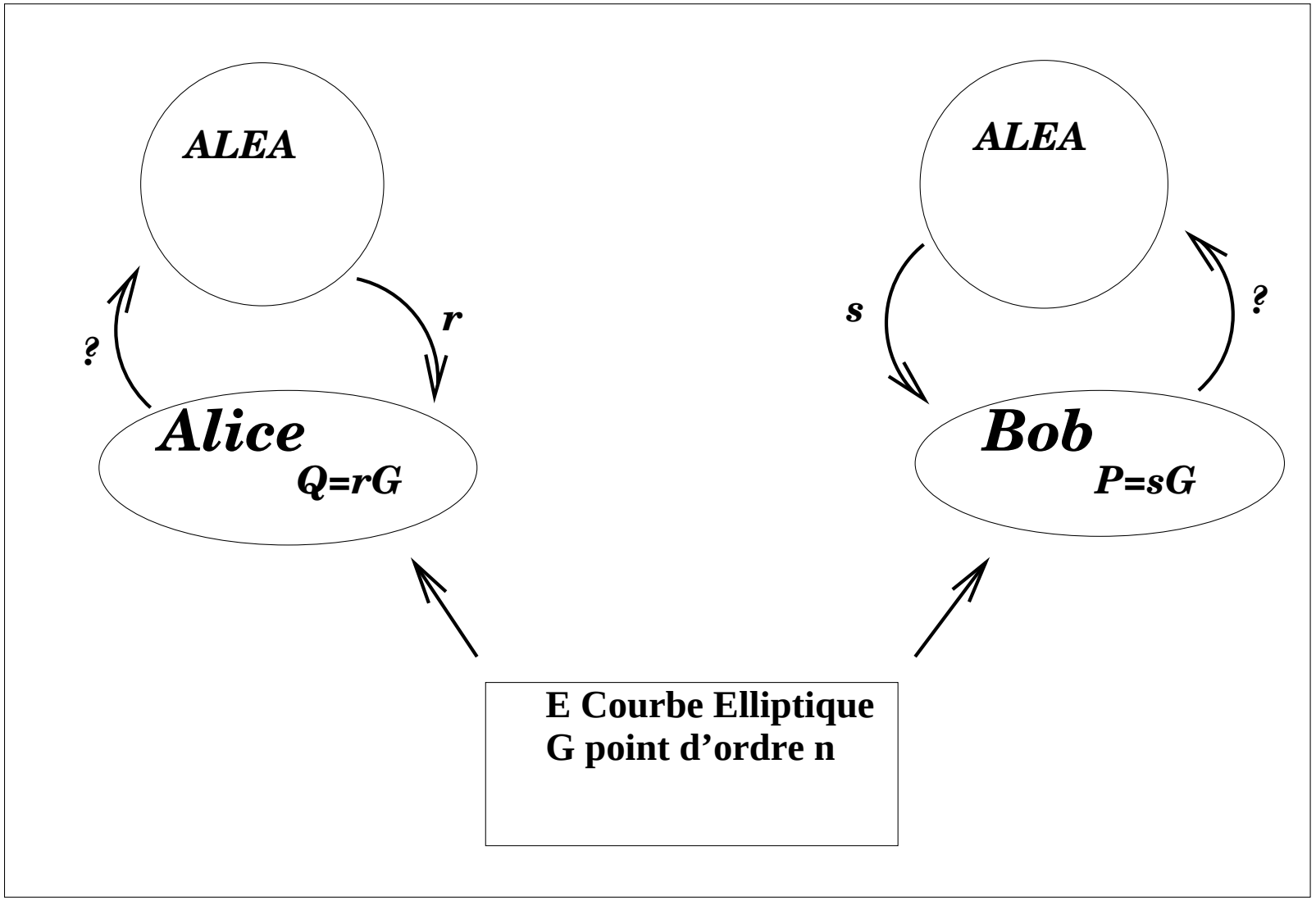
Les principaux inconvénients sont :

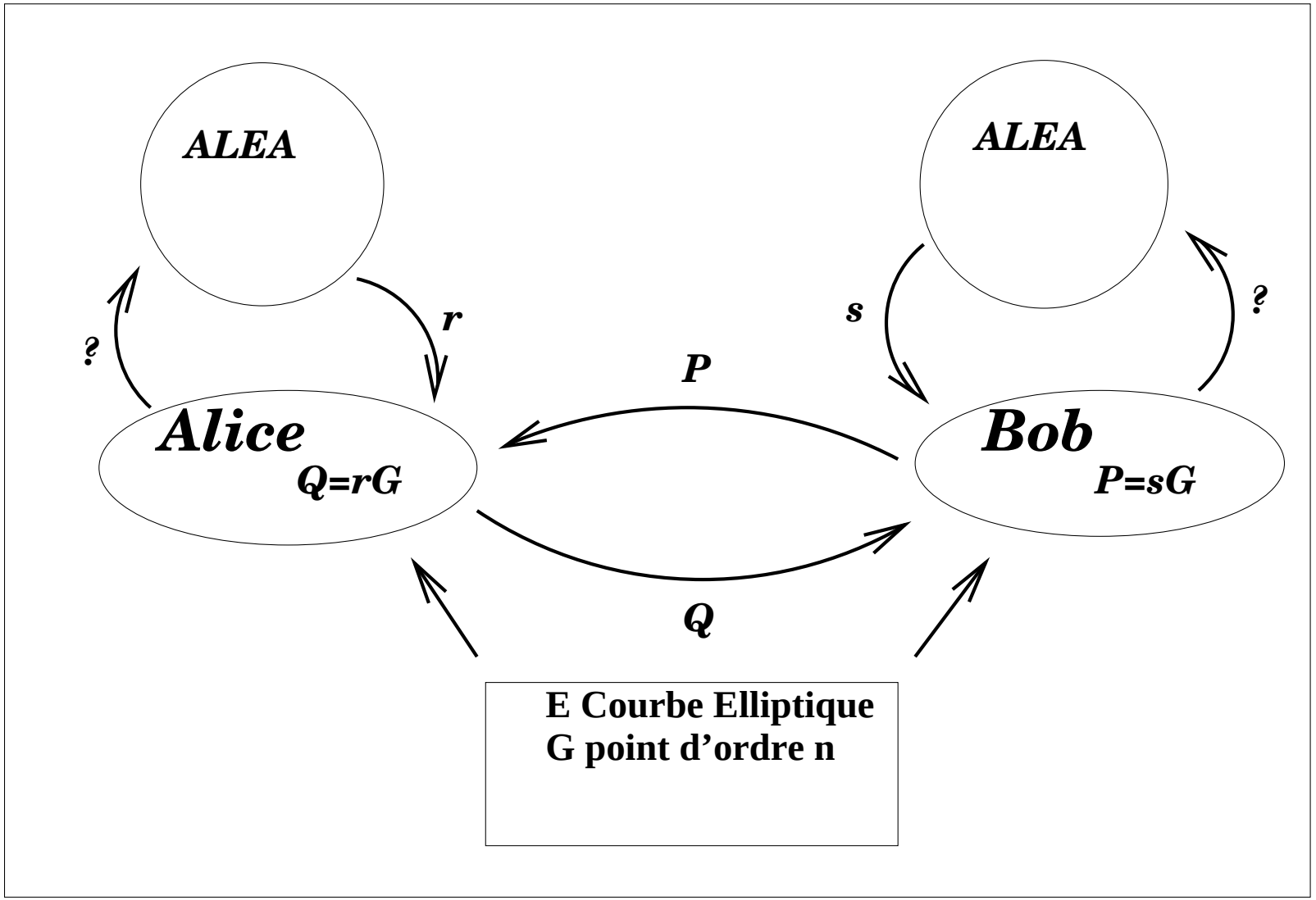
- la mise en place du système, en particulier le choix judicieux des courbes, le comptage de points sur la courbe.
- l'implémentation d'une opération efficace.
- difficultés de la protection contre les attaques ≪ side channel ≫.

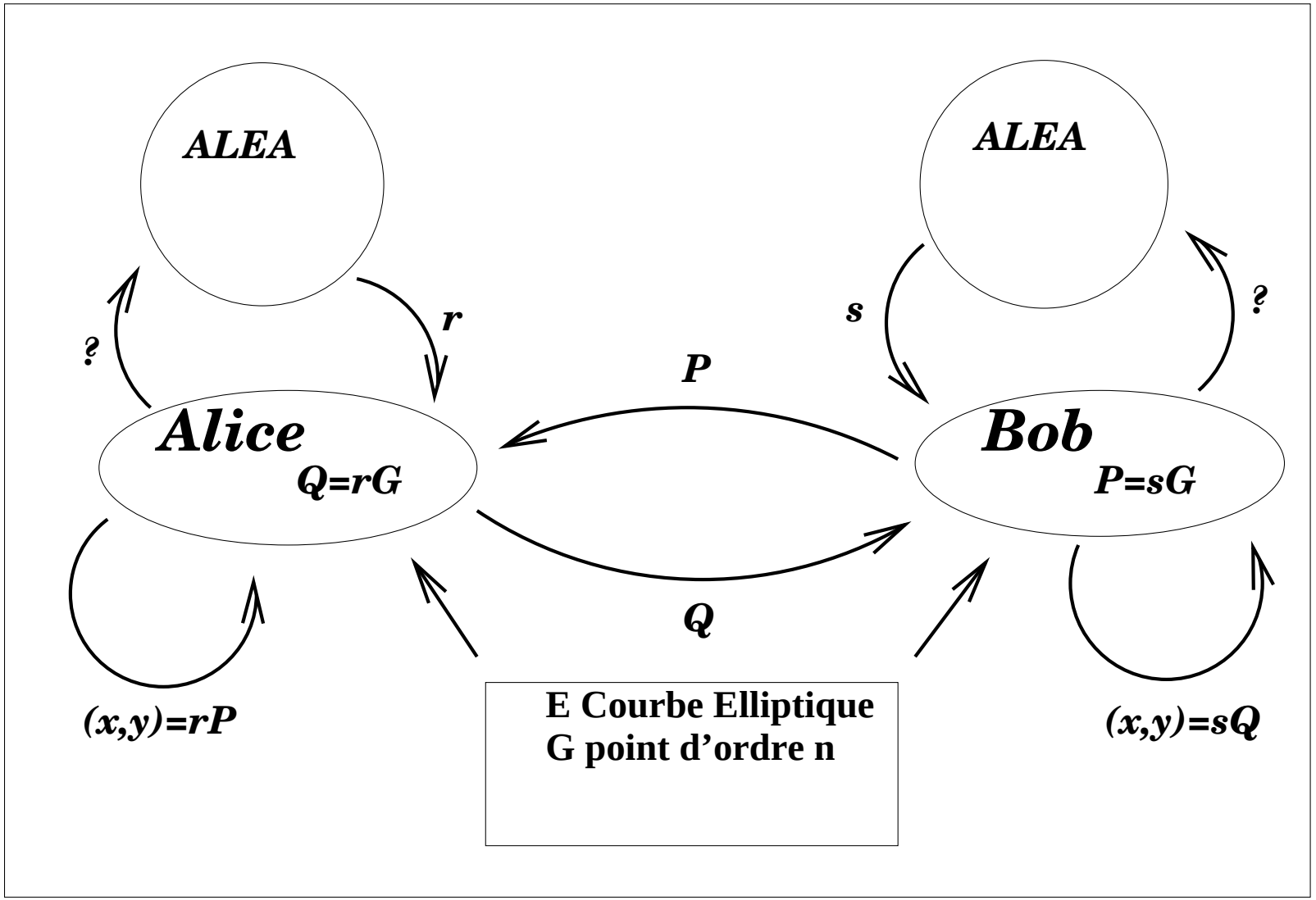
ECDH : Echange de clé de Diffie-Hellman




ALEA
ALEA
?
?
Alice
Bob
E Courbe Elliptique
G point d'ordre n


ALEA
?
r
Alice
Q=rG
ALEA
s
?
Bob
P=sG
E Courbe Elliptique
G point d'ordre n


ALEA
ALEA
?
r
s
?
P
Alice
Q=rG
Bob
P=sG
Q
E Courbe Elliptique
G point d'ordre n


ALEA
ALEA
?
r
s
?
P
Alice
Q=rG
Bob
P=sG
Q
(x,y)=rP
E Courbe Elliptique
G point d'ordre n
(x,y)=sQ

En pratique

La cryptographie à clé publique :

- trop lente pour chiffrer de gros flux de données.

Pour cette tâche on utilise **la cryptographie symétrique**, la clé secrète, tirée au sort à chaque session (clé de session) étant échangée grâce à de la cryptographie à clé publique. Celle-ci sert aussi à la signature numérique.

Rôle de la cryptographie à clé publique :

- chiffrement de messages courts
- échange de clé
- signature

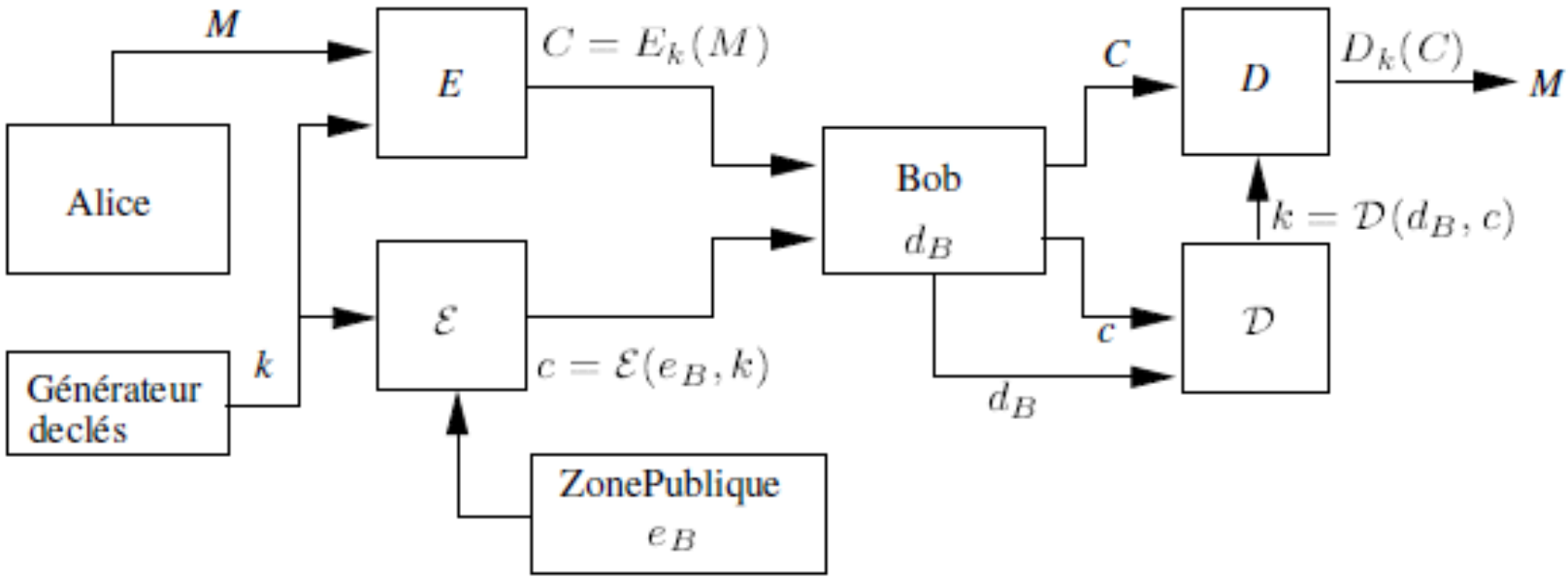


Figure 2.1. *Utilisation conjointe d'un système à clé secrète et d'un système à clé publique*

Système	Meilleure attaque	taille 1	taille 2	taille 3	taille 4	taille 5
bloc	brutale	80 bits	112 bits	128 bits	192 bits	256 bits
RSA	factorisation	1024 bits	2048 bits	4096 bits	trop (15000)	
DSA	log discret	1024 bits	2048 bits	4096 bits	trop (15000)	
hachage	anniversaire	160 bits	224 bits	256 bits	384 bits	512 bits
EC	EC log discret	160 bits	224 bits	256 bits	384 bits	512 bits

Tableau 1.1. *Correspondances entre tailles des systèmes*

Loi de Moore

Loi de Moore :

Doublement de la puissance des ordinateurs tous les 18 mois.

Année	Cryptosystème symétrique	Module RSA ou taille de p pour le pb. du log discret	Taille du sous-groupe pour le pb. du log discret	Courbes Elliptiques	Nombre d'années sur un PII 450 Mhz
1982	*56*	*417*	*102*	*105*	1.11×10^3
2005	74	1149	131	139	2.26×10^8
2010	78	1369	138	146	3.22×10^9
2015	82	1613	145	154	4.59×10^{10}
2020	86	1881	151	188	6.54×10^{11}
2025	89	2174	158	169	9.33×10^{12}
2030	93	2493	165	176	1.33×10^{14}
2040	101	3214	179	191	2.7×10^{16}

Tableau 1.2. *Évolution de la taille des clés pour différentes primitives cryptographiques*

Références

Site web :

http ://www.acrypta.fr

Ouvrage

"Cryptographie : principes et mises en œuvre." (Hermes Science, Lavoisier)

par

P. Barthélemy, R. Rolland et P. Véron