Émergence de la cryptographie elliptique

Robert Rolland

17 novembre 2007

R. Rolland, C.N.R.S. Institut de Mathématiques de Luminy
Luminy Case 930, F13288 Marseille CEDEX 9
e-mail : rolland@iml.univ-mrs.fr
web : http ://iml.univ-mrs.fr/∼rolland/

Présentation réalisée avec la classe beamer de LaTeX

Références

http ://www.acrypta.fr

Cryptographie principes et mises en œuvre P. Barthélemy, R. Rolland, P. Véron, Hermes Science, Lavoisier

Plan

1. Introduction
   - Cryptographie à clé publique
   - Fonctions à sens unique
   - Problèmes difficiles
   - Le problème du logarithme discret
   - La cryptographie elliptique

Plan

1. Introduction
   - Cryptographie à clé publique
   - Fonctions à sens unique
   - Problèmes difficiles
   - Le problème du logarithme discret
   - La cryptographie elliptique
2. Coubes elliptiques
   - La définition
   - La structure de groupe
   - Courbes elliptiques sur $\mathbb{Z}/p\mathbb{Z}$

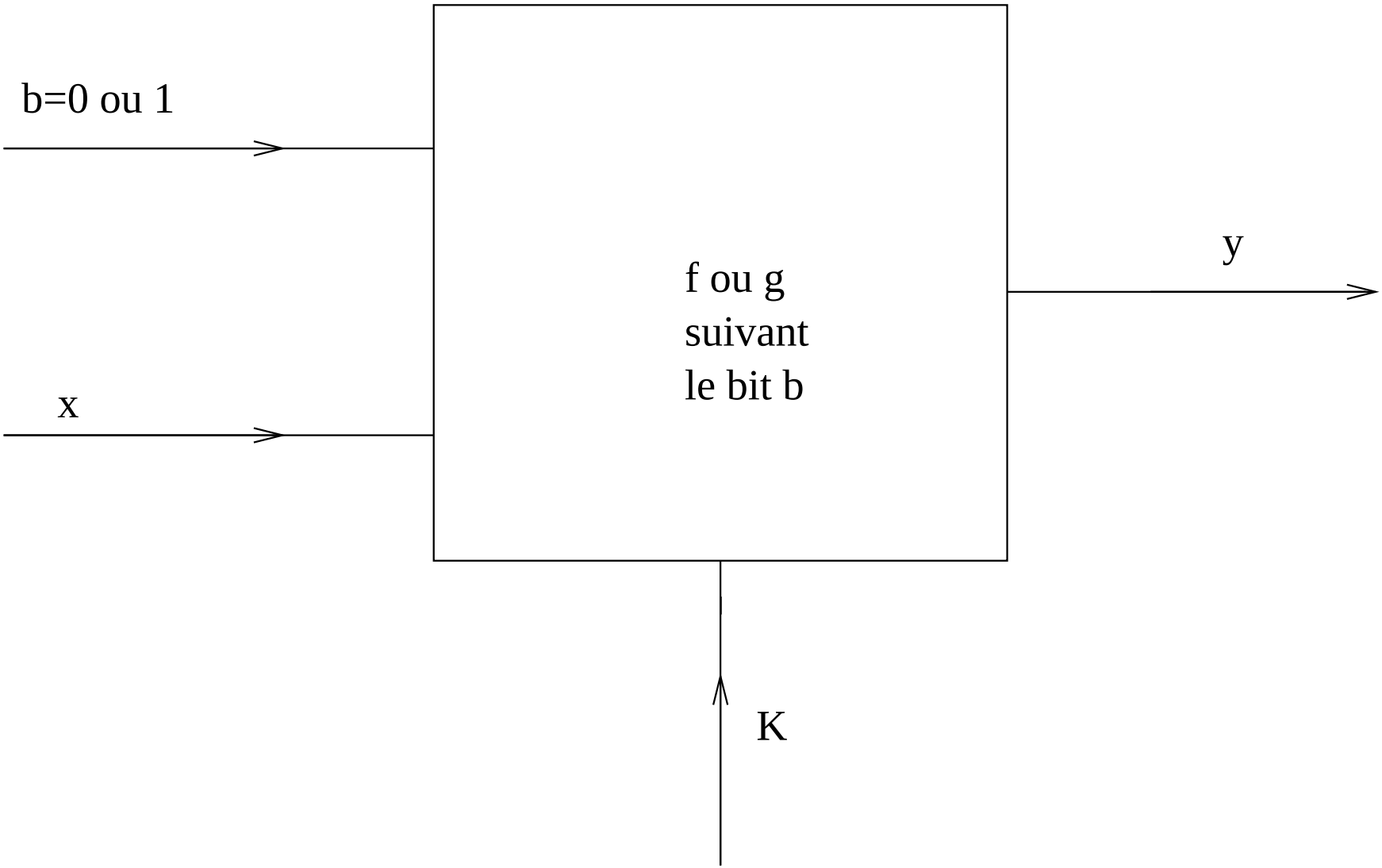
Plan

1. Introduction
   - Cryptographie à clé publique
   - Fonctions à sens unique
   - Problèmes difficiles
   - Le problème du logarithme discret
   - La cryptographie elliptique
2. Coubes elliptiques
   - La définition
   - La structure de groupe
   - Courbes elliptiques sur $\mathbb{Z}/p\mathbb{Z}$

Cryptographie à clé secrète

En cryptographie à **clé secrète (ou symétrique)**, l'expéditeur et le destinataire doivent partager une clé secrète K. Cette clé K sert à la fois au chiffrement et au déchiffrement. Les deux interlocuteurs disposent d'une **fonction publique de chiffrement** f et d'une **fonction publique de déchiffrement** g. Pour obtenir le chiffré du texte clair x avec la clé K on calcule $y = f(x, K)$. On retrouve x à partir du chiffré y en calculant $x = g(y, K)$.

Le problème du **partage de la clé secrète** se pose.


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

Cryptographie à clé publique

En cryptographie à **clé publique (ou asymétrique)** chaque utilisateur A possède une paire de clés :

- 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 :

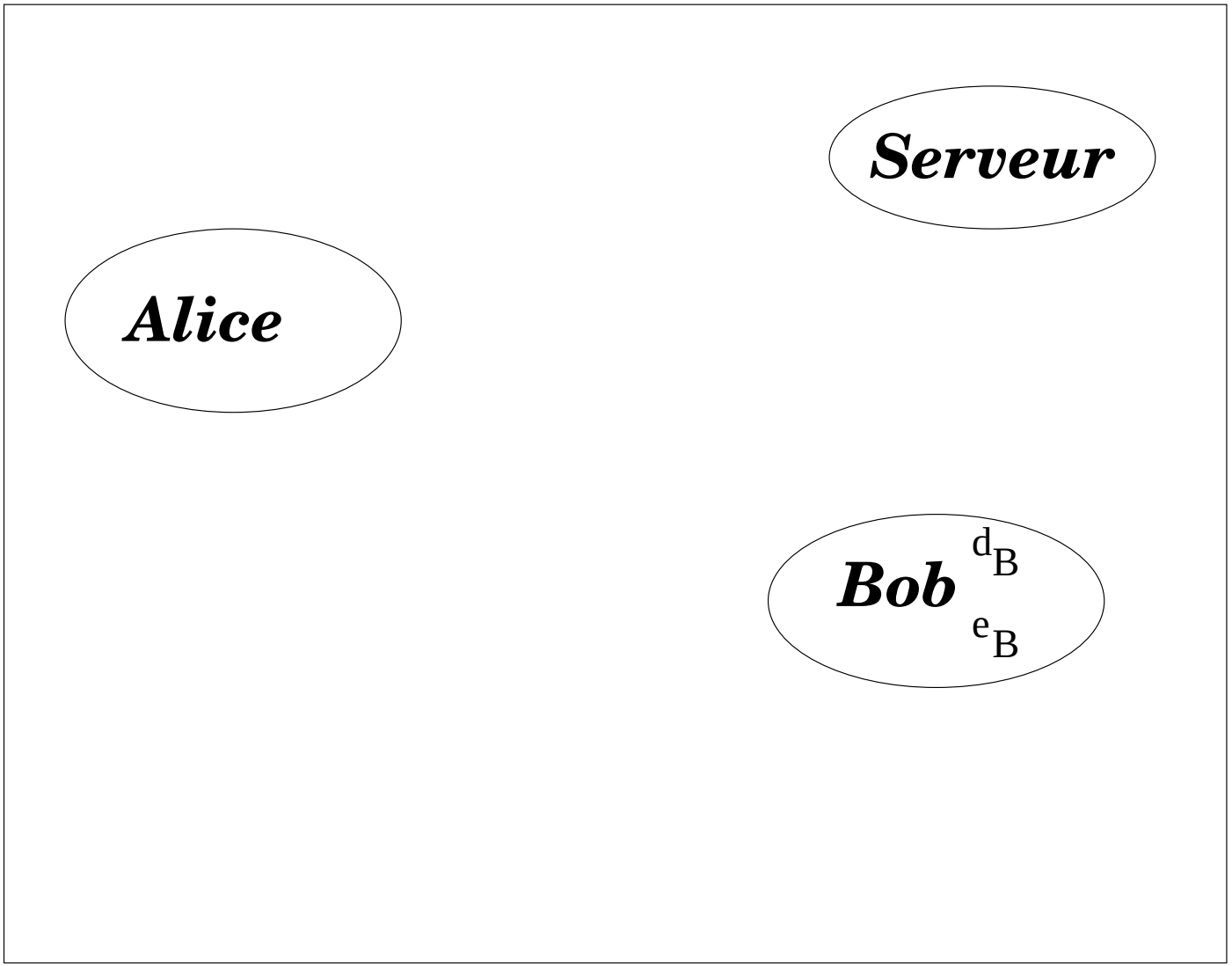
- une fonction de **chiffrement** f qui à un texte clair x et à la clé publique e_A fait correspondre le texte chiffré $y = f(x, e_A)$ à destination de A ;
- une fonction de **déchiffrement** g qui au texte chiffré y et à la clé privée d_A redonne le texte clair $x = g(y, d_A)$.

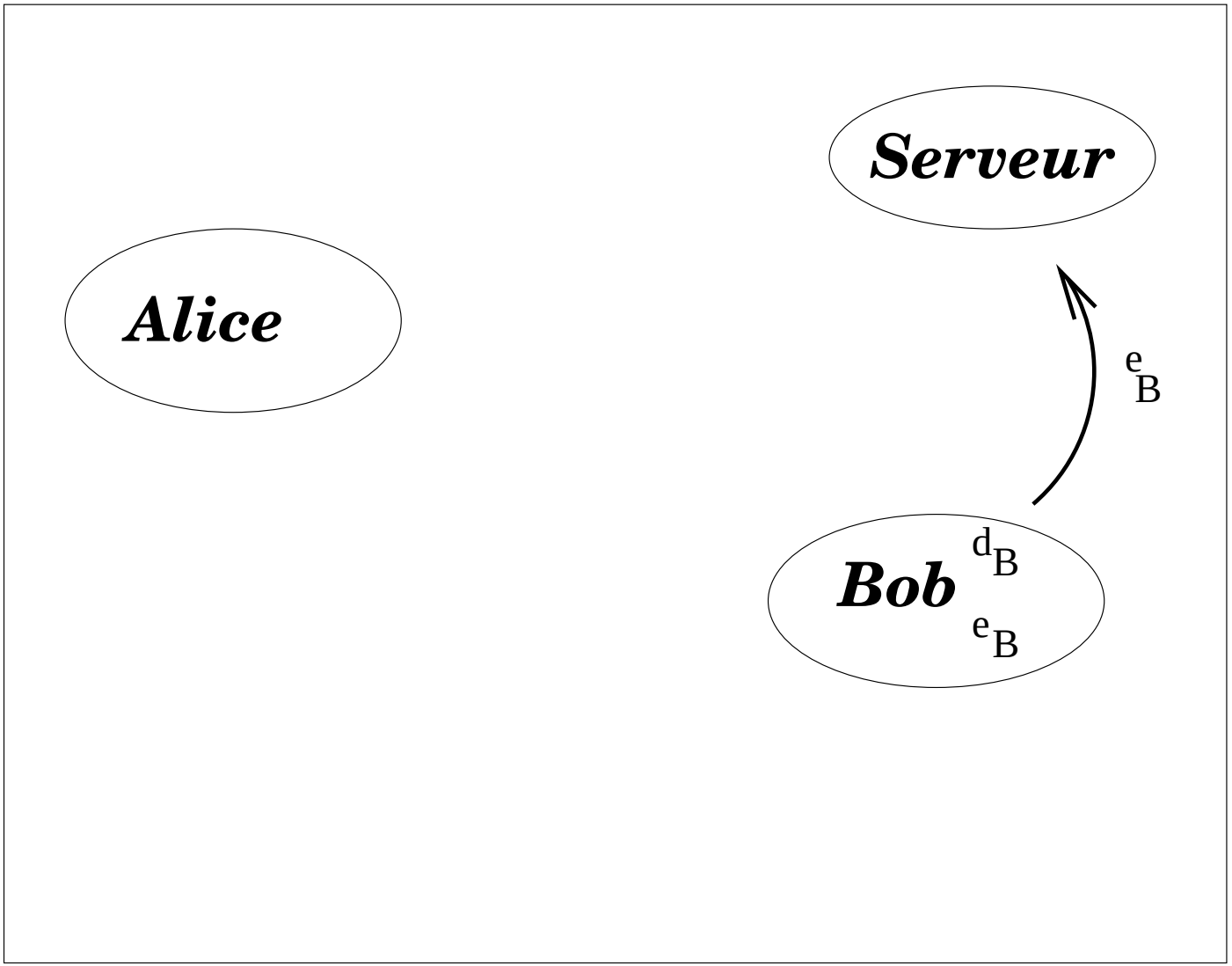
  Cette fois, **il n'y a plus besoin d'échanger une clé secrète**.

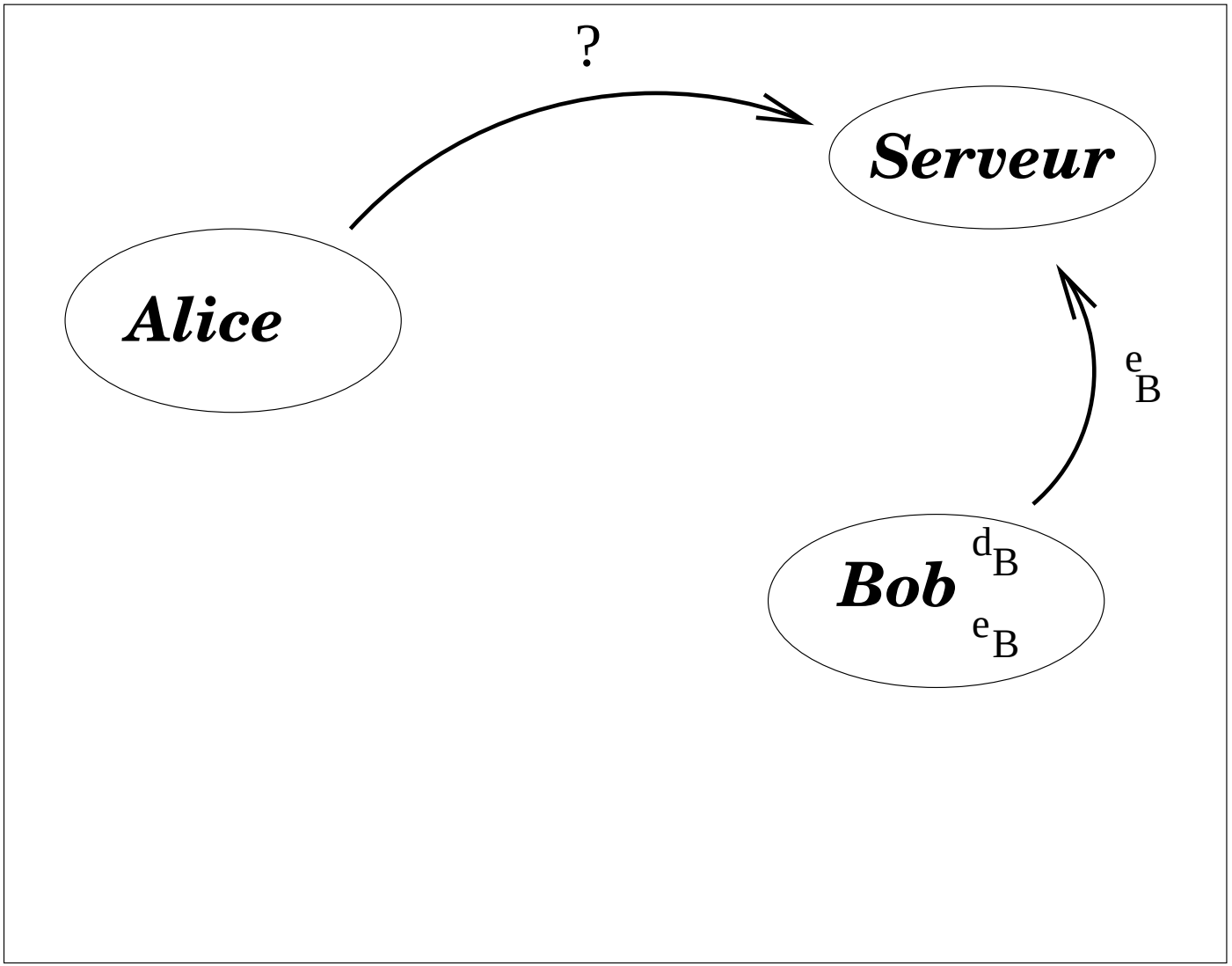
En pratique

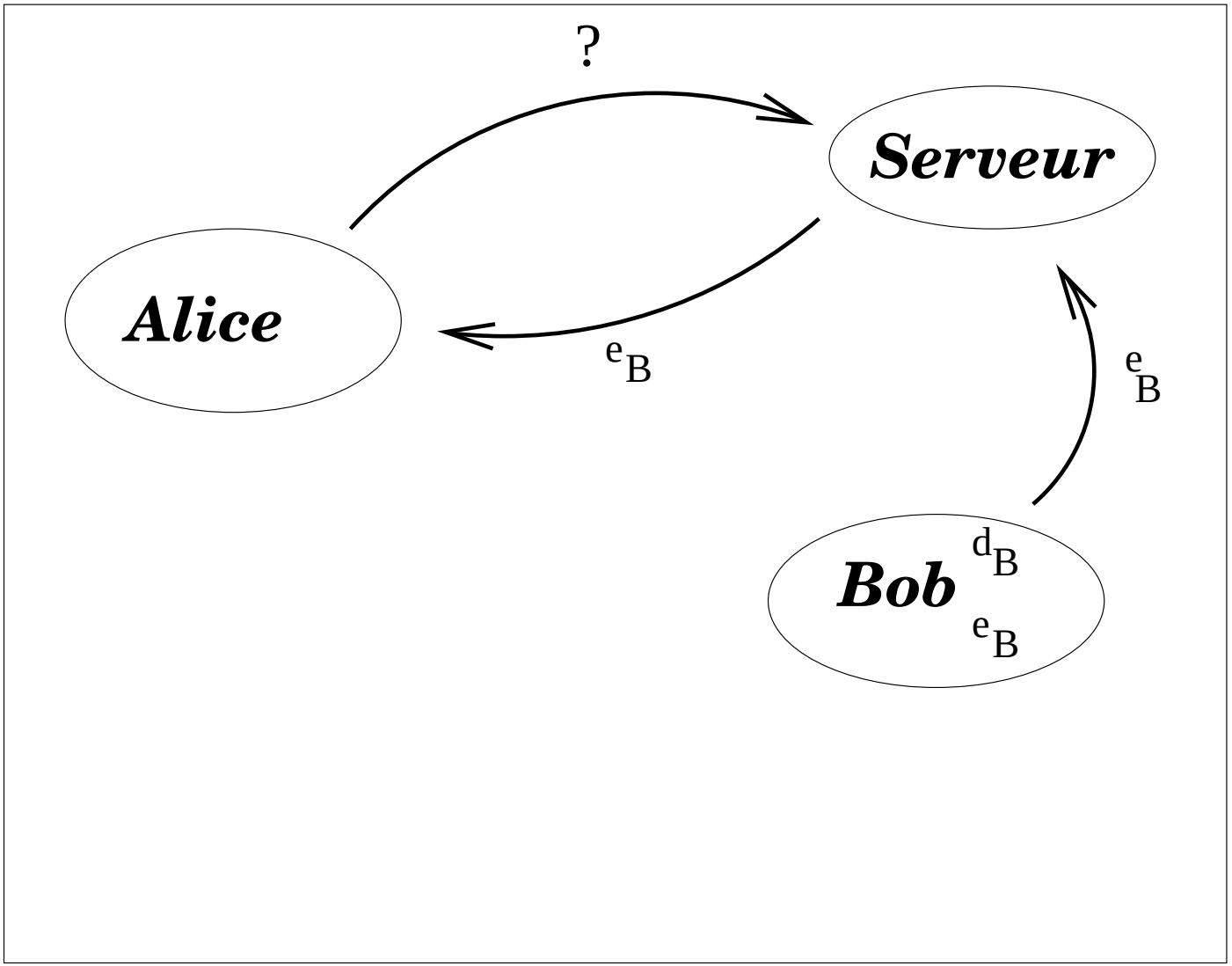
La cryptographie à clé publique est trop lente pour chiffrer de gros flux de données. Pour cette tâche on utilise la cryptographie symétrique, la clé secrète, tirée au sort à chaque session (clé de session) étant échangée grâce à de la cryptographie à clé publique. Celle-ci sert aussi à la signature numérique.

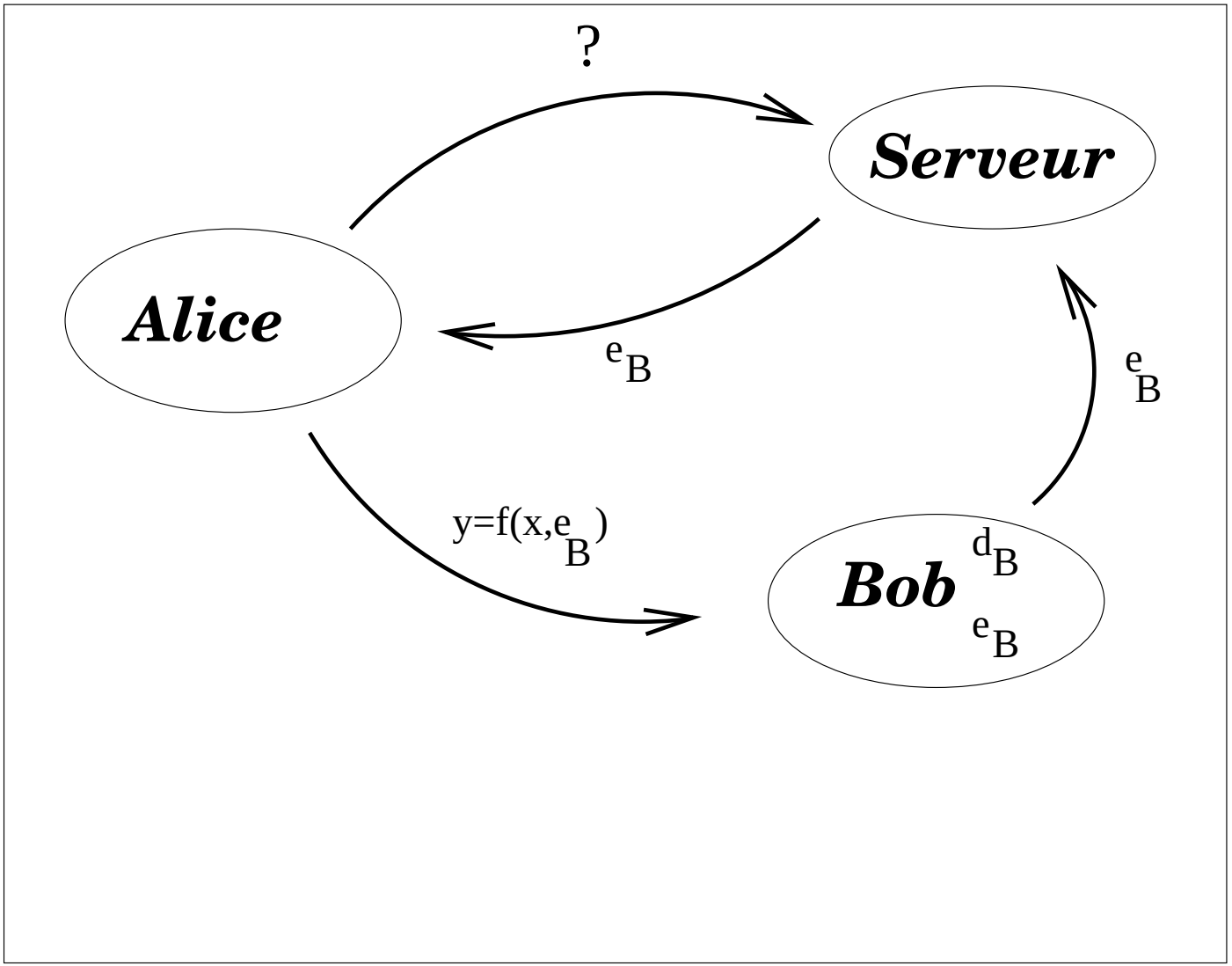
- chiffrement de messages courts
- échange de clé
- signature

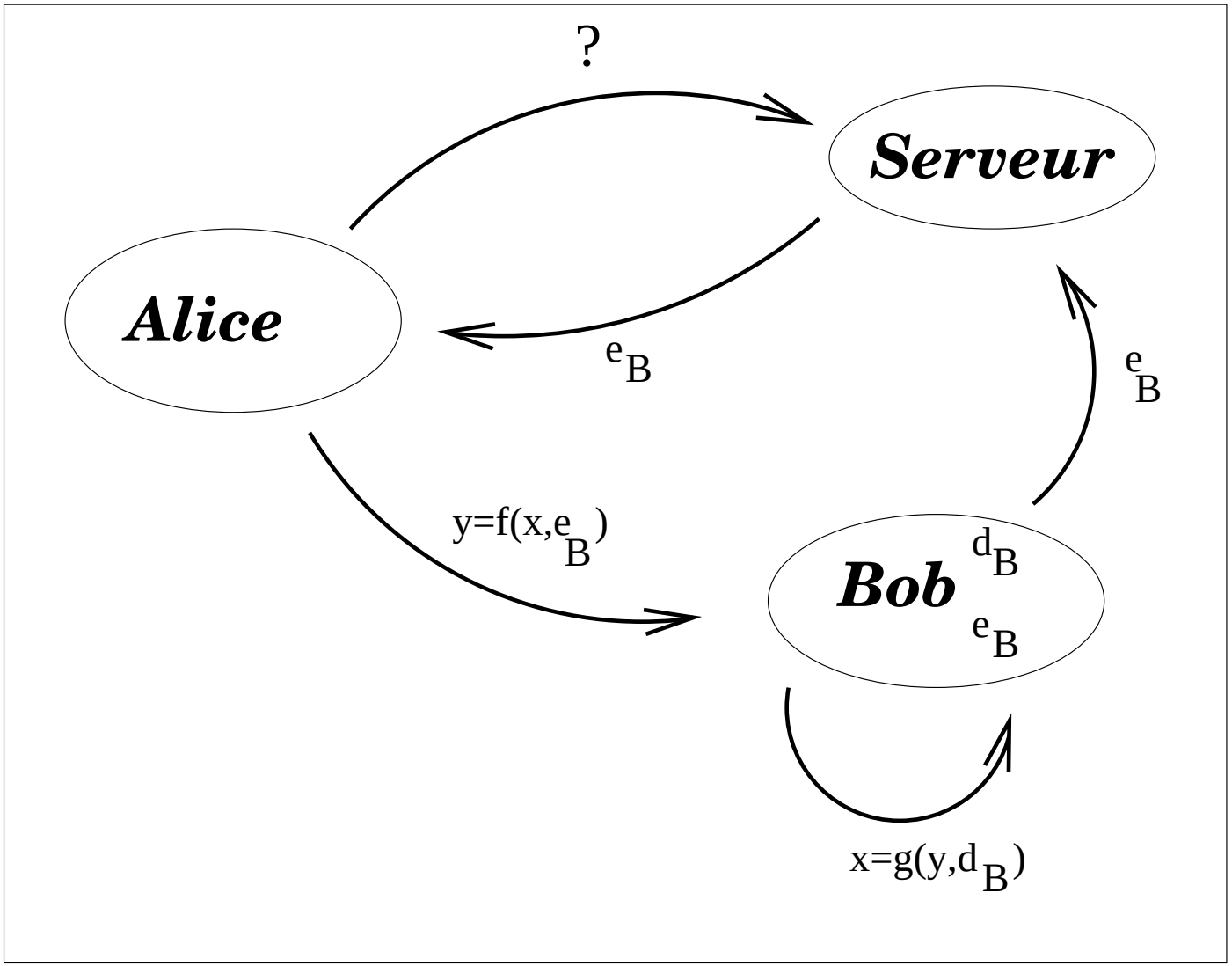

Serveur
Alice
Bob
d_B
e_B


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
$x=g(y,d_B)$

Plan

1. Introduction
   - Cryptographie à clé publique
   - Fonctions à sens unique
   - Problèmes difficiles
   - Le problème du logarithme discret
   - La cryptographie elliptique
2. Coubes elliptiques
   - La définition
   - La structure de groupe
   - Courbes elliptiques sur $\mathbb{Z}/p\mathbb{Z}$

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 pour lesquelles il est difficile de calculer une pré-image.

- facile à calculer : $y = f(x)$
- quasi-impossible à calculer : étant donné y trouver x tel que $f(x) = y$.

Plan

1 Introduction
- Cryptographie à clé publique
- Fonctions à sens unique
- Problèmes difficiles
- Le problème du logarithme discret
- La cryptographie elliptique

2 Coubes elliptiques
- La définition
- La structure de groupe
- Courbes elliptiques sur $\mathbb{Z}/p\mathbb{Z}$

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.

Plan

1. Introduction
   - Cryptographie à clé publique
   - Fonctions à sens unique
   - Problèmes difficiles
   - Le problème du logarithme discret
   - La cryptographie elliptique
2. Coubes elliptiques
   - La définition
   - La structure de groupe
   - Courbes elliptiques sur $\mathbb{Z}/p\mathbb{Z}$

Exemple

Prenons l'exemple du groupe multiplicatif :

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

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 $2^m = 5$.

Le problème du logarithme discret

Soit G un groupe dont on notera l'opération aditivement engendré par un élément a. Soit $b \in G$. Trouver m tel que

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

Plan

1. Introduction
   - Cryptographie à clé publique
   - Fonctions à sens unique
   - Problèmes difficiles
   - Le problème du logarithme discret
   - La cryptographie elliptique
2. Coubes elliptiques
   - La définition
   - La structure de groupe
   - Courbes elliptiques sur $\mathbb{Z}/p\mathbb{Z}$

La cryptographie elliptique

La **cryptographie elliptique** repose sur le problème de logarithme discret et problèmes connexes dans le groupe des points d'une courbe elliptique sur un corps fini. On va donc s'intéresser aux questions suivantes :

- **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). Pour simplifier nous étudierons les courbes sur les corps $\mathbb{Z}/p\mathbb{Z}$.

Plan

1 Introduction
- Cryptographie à clé publique
- Fonctions à sens unique
- Problèmes difficiles
- Le problème du logarithme discret
- La cryptographie elliptique

2 Coubes elliptiques
- La définition
- La structure de groupe
- Courbes elliptiques sur $\mathbb{Z}/p\mathbb{Z}$

La définition

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

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

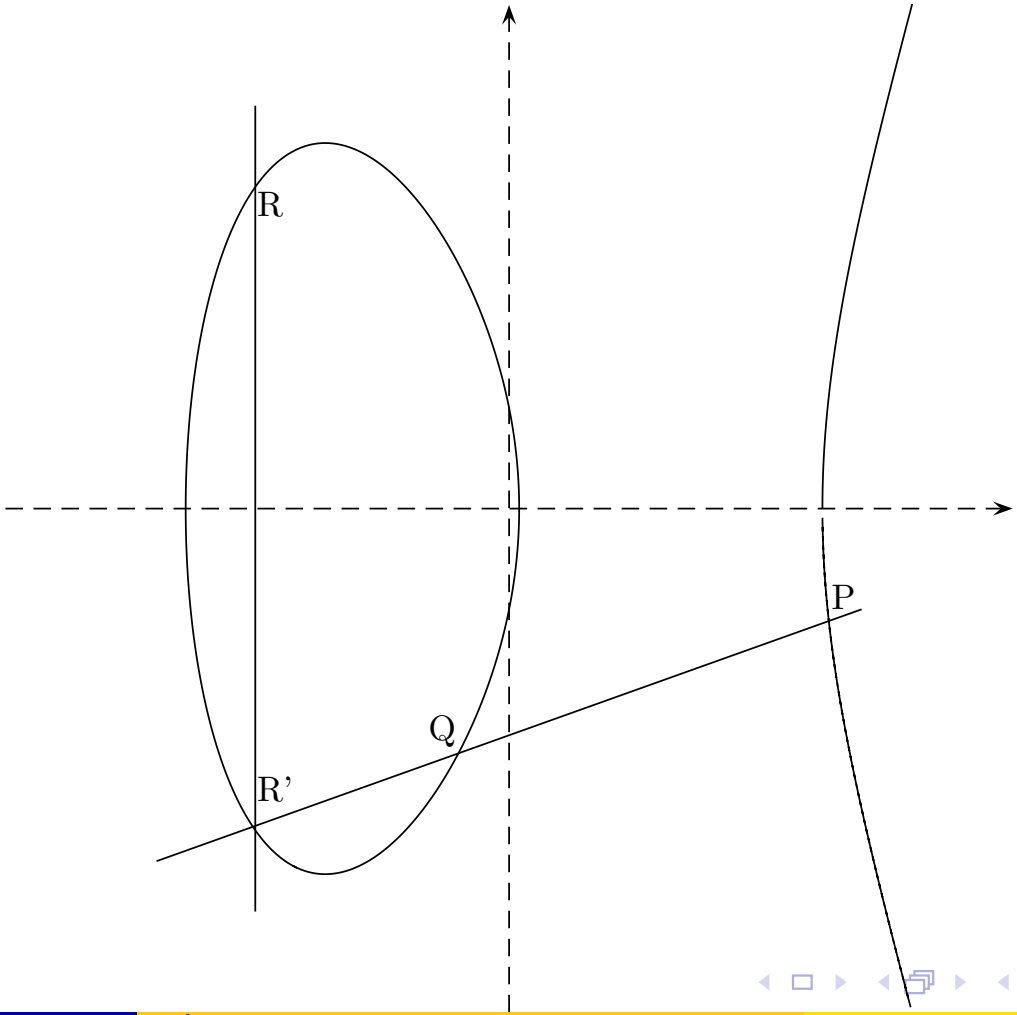
avec $4a^3 + 27b^2 \neq 0$.

Plan

1 Introduction
- Cryptographie à clé publique
- Fonctions à sens unique
- Problèmes difficiles
- Le problème du logarithme discret
- La cryptographie elliptique

2 Coubes elliptiques
- La définition
- La structure de groupe
- Courbes elliptiques sur $\mathbb{Z}/p\mathbb{Z}$

La structure de groupe



La structure de groupe

On calcule $R = P + Q$ en prenant le symétrique R du point R', troisième point d'intersection de la droite PQ avec la courbe. Il y a quelques cas particuliers : par exemple le cas $P = Q$, on prend alors la tangente, ou encore P et Q sont symétriques par rapport à l'axe des x, dans ce cas la droite PQ coupe la courbe au point à l'infini (qui est le zéro du groupe) et donc $Q = -P$.

Plan

1 Introduction
- Cryptographie à clé publique
- Fonctions à sens unique
- Problèmes difficiles
- Le problème du logarithme discret
- La cryptographie elliptique

2 Coubes elliptiques
- La définition
- La structure de groupe
- Courbes elliptiques sur $\mathbb{Z}/p\mathbb{Z}$

Un exemple

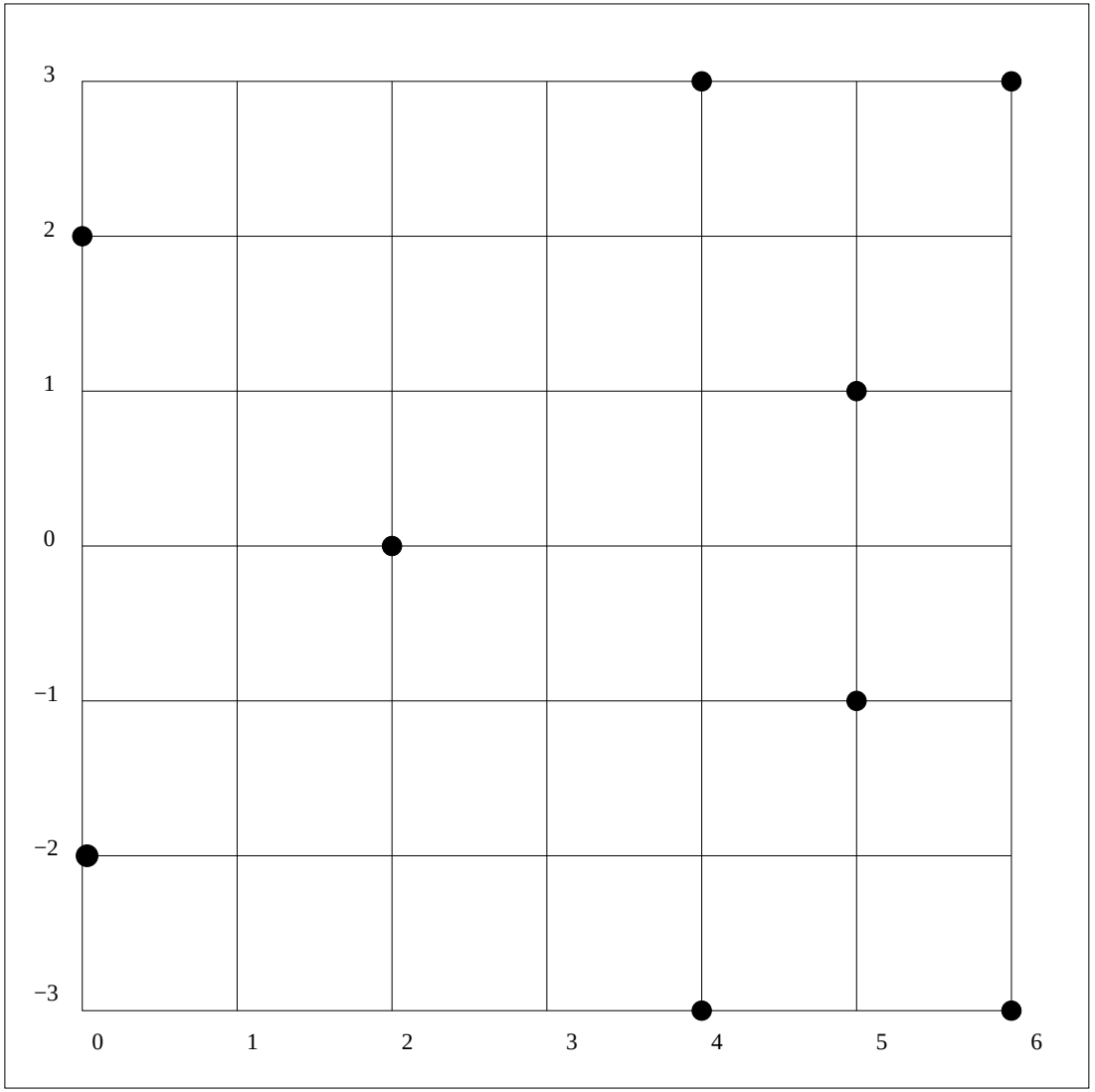
Prenons pour exemple $p = 7$ et la courbe d'équation :

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

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

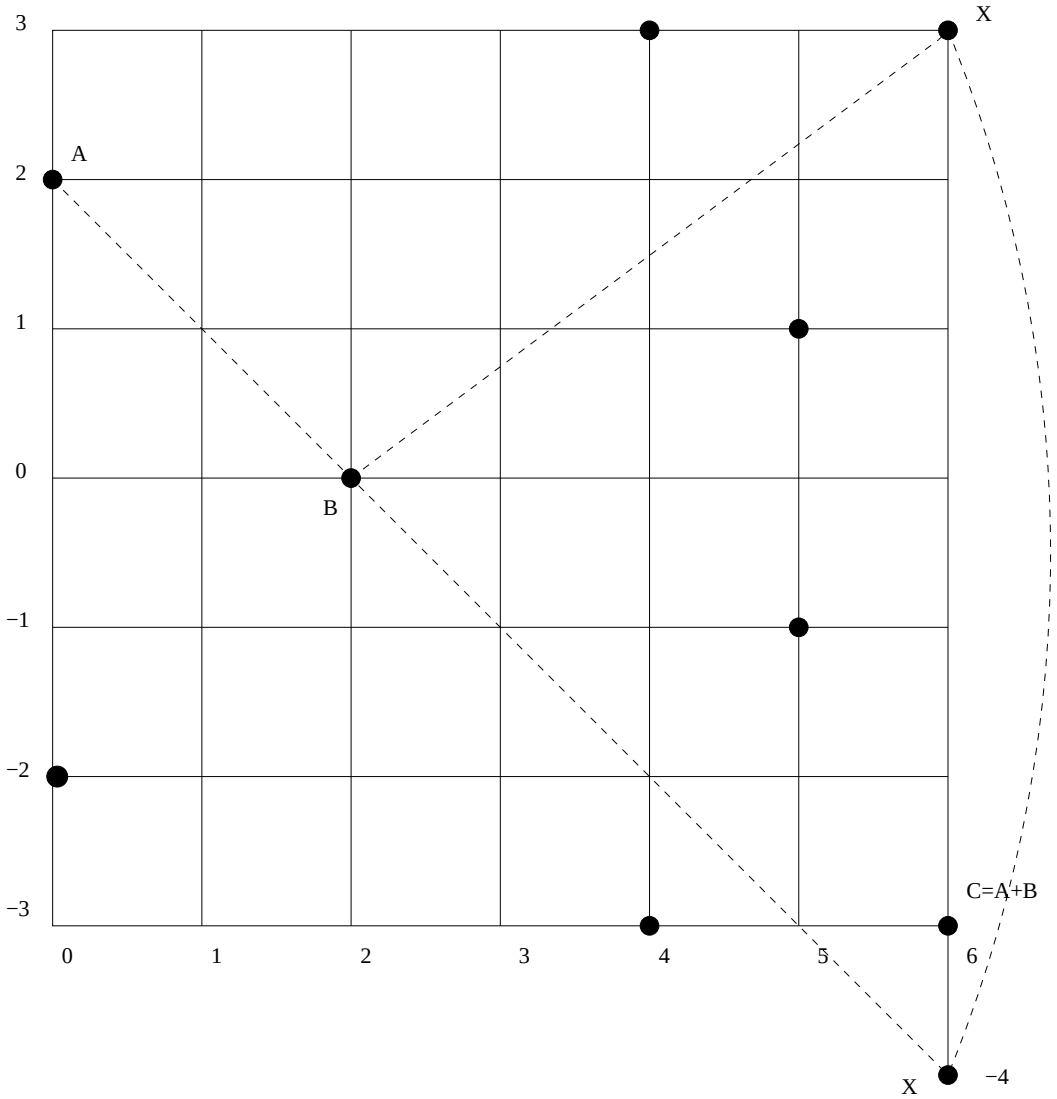


Table d'addition

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

Plan

3 Les avantages

Plan

3 Les avantages

4 Les inconvénients

Plan

3 Les avantages

4 Les inconvénients

5 Les utilisations

Pourquoi la cryptographie elliptique

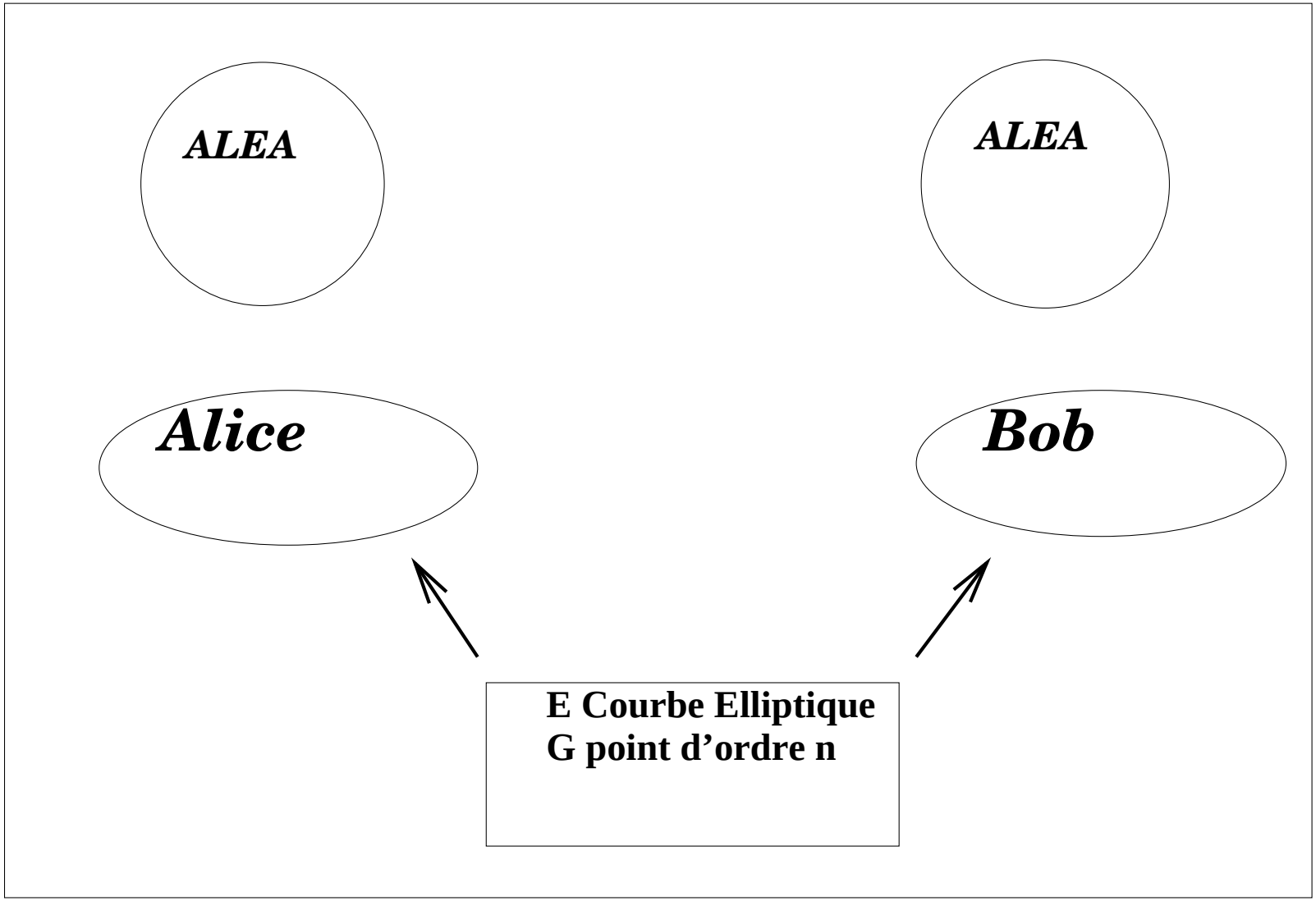
Le problème du logarithme discret sur une courbe elliptique bien choisie est pour le moment plus résistant que celui sur les groupes $\mathbb{Z}/p\mathbb{Z}$. De ce fait les tailles de clé à prendre pour la même résistance sont plus petites : par exemple 1024 bits pour RSA, 160 bits pour un chiffrement ou une signature à base de courbe elliptique, 128 bits pour un circuit à clé secrète. Si on passe à 256 bits de clé pour un circuit à clé secrète, alors *RSA* ne convient plus. Il faudrait une clé bien trop grosse (peut être 15000 bits). En revanche la cryptographie elliptique peut suivre. On doit par exemple dans ce cas prendre de l'ordre de 400 bits de clé.
En outre les courbes elliptiques permettent l'implémentation de systèmes où les clés publiques sont basées sur l'identité.

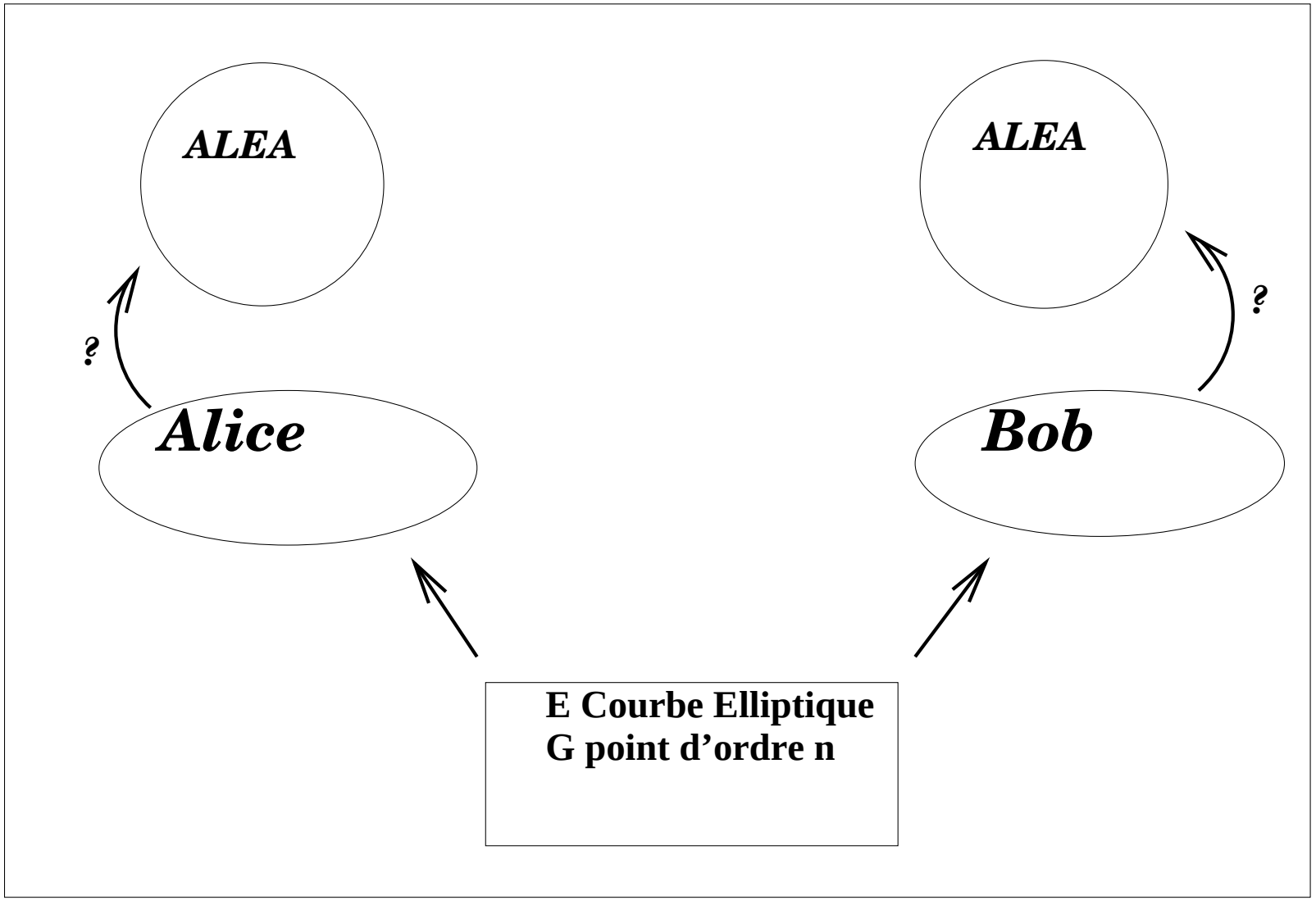
Inconvénients

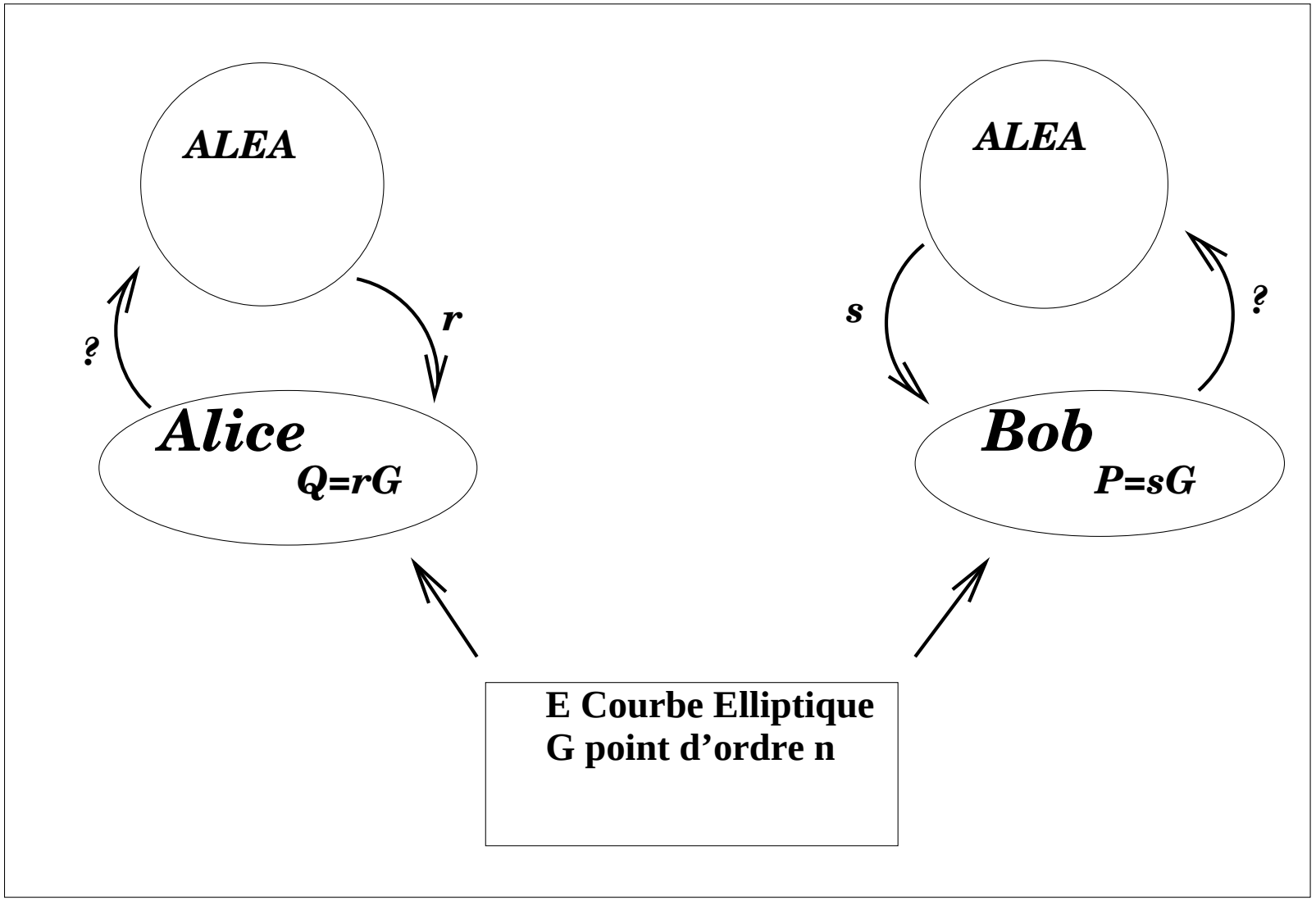
Les principaux inconvénients sont :

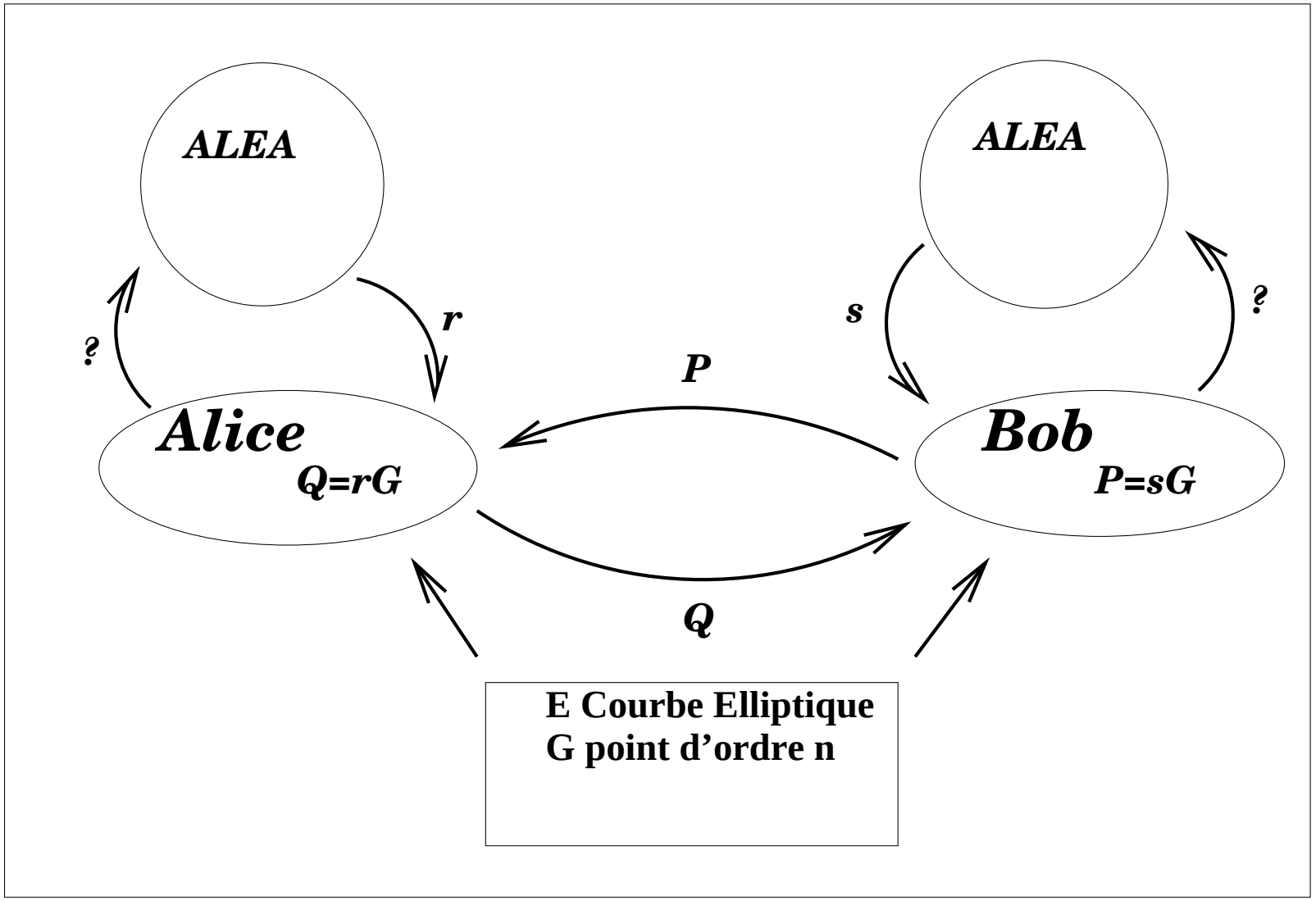
- la mise en place du système, en particulier le choix judicieux des courbes, le comptage de points sur la courbe.
- l'implémentation d'une opération efficace.
- difficultés de la protection contre les attaques « side channel »

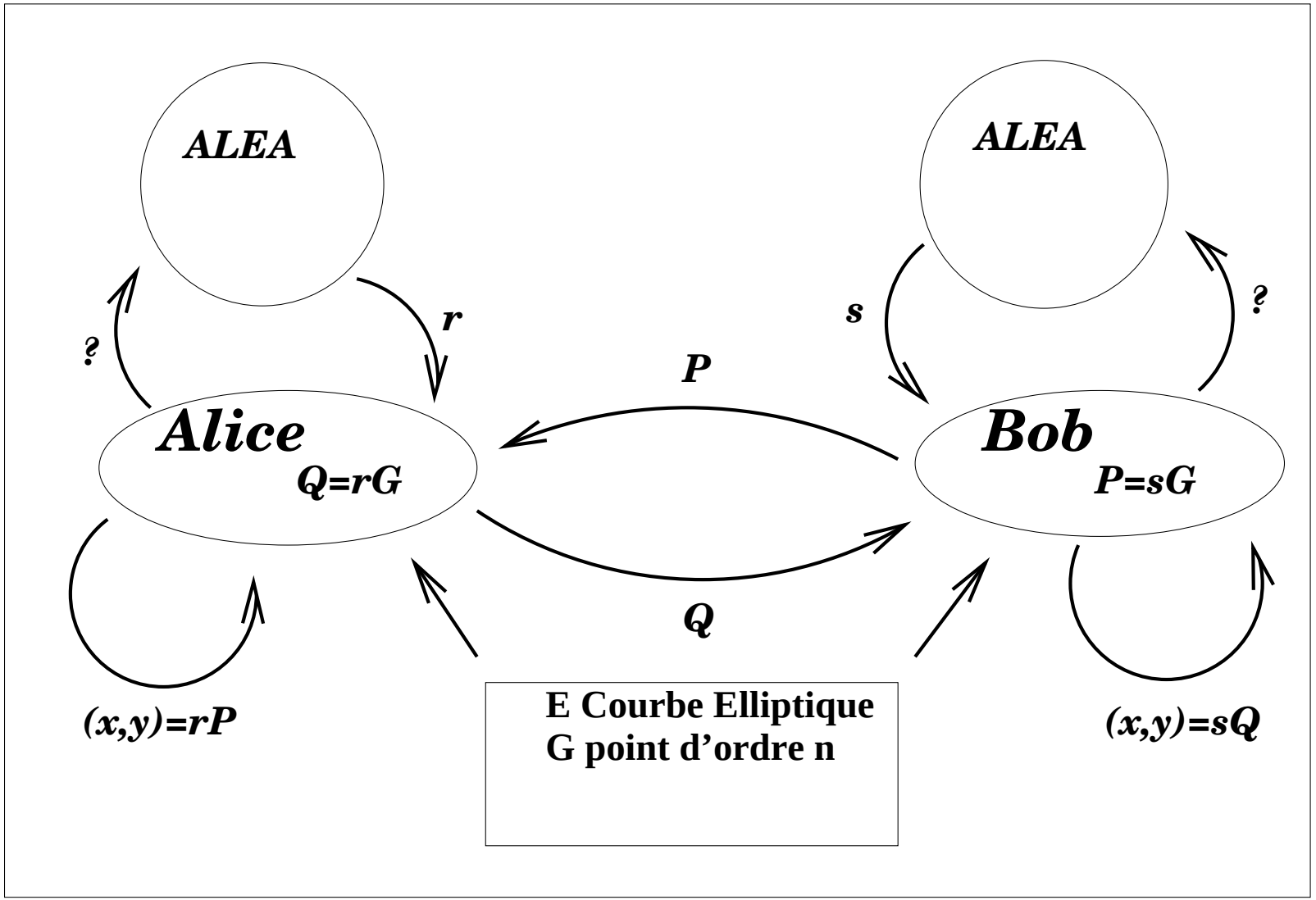
ECDH : Echange de clé de Diffie-Hellman




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


ALEA
ALEA
?
r
s
?
Alice
Q=rG
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

ECDSA, mise en place

On prend un point P d'ordre premier $n > 2^{160}$ d'une courbe elliptique définie sur $\mathbb{Z}/p\mathbb{Z}$:

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

On dispose aussi d'une fonction de hachage H. Tout ceci est public.

On choisit maintenant s entre 1 et $n-1$ et on calcule $Q = sP$. La **clé publique** est Q. La **clé privée** est s.

Signons un message

On veut signer le message m.
On tire au sort k entre 1 et $n-1$.
on calcule $(x, y) = kP$.
On calcule $z = x \mod n$.
on calcule $t = k^{-1}(H(m) + sz) \mod n$.
Si $z = 0$ ou $t = 0$ on recommence.
La signature est (z, t). On transmet donc (m, z, t), message suivi de l'appendice.

Vérifions la signature

On reçoit (m, z, t).
On contrôle que $1 \leq z, t \leq n-1$.
Calculer

$$(u, v) = t^{-1}\left((H(m) \mod n)P + (z \mod n)Q\right).$$

Vérifier que $z = u \mod n$.