# On the Security of Cryptosystems with Quadratic Decryption:
## The Nicest Cryptanalysis

Guilhem Castagnos

PRISM — UVSQ

Grenoble — mardi 16 juin

Travail commun avec Fabien Laguillaumie

PRISM

# Plan



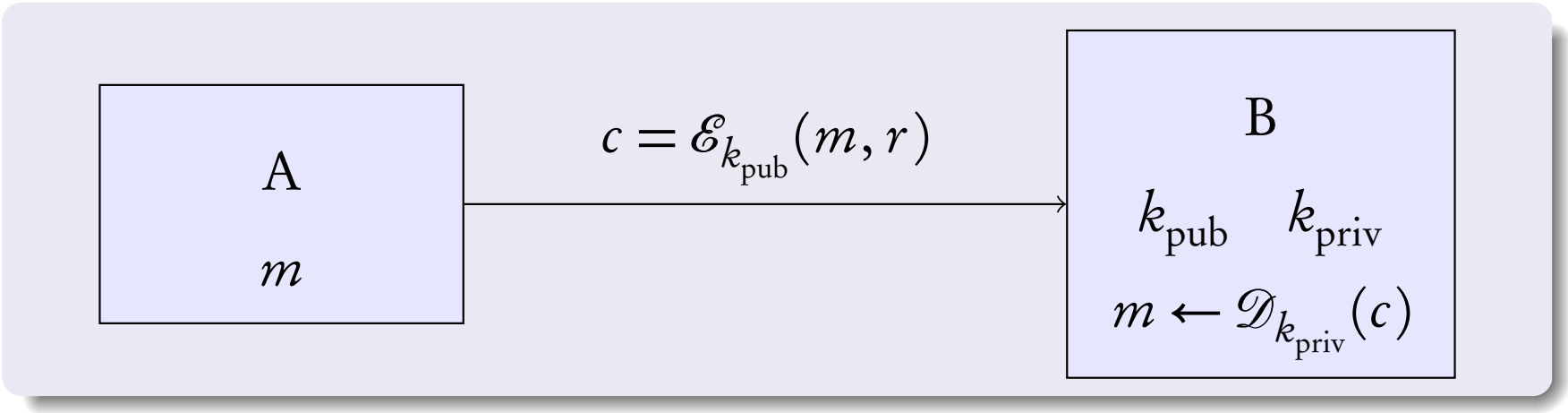
PRISM

# Plan



PRISM

# Schéma de chiffrement asymétrique




- Génération de clefs :
  - Entrée : un paramètre de sécurité $\lambda$
  - Sortie : une paire $(k_{\text{pub}}, k_{\text{priv}})$, clef publique et privée
- Chiffrement :
  - Entrée : un message $m$ et $k_{\text{pub}}$
  - Sortie : un chiffré $c = \mathcal{E}_{k_{\text{pub}}}(m, r)$ pour un aléa $r$
- Déchiffrement :
  - Entrée : un chiffré $c$ et $k_{\text{priv}}$
  - Sortie : $m = \mathcal{D}_{k_{\text{priv}}}(c)$ tel que $\mathcal{D}_{k_{\text{priv}}}(\mathcal{E}_{k_{\text{pub}}}(m, r)) = m$

PRISM

# Sécurité

## Moyens de l'attaquant :

- Attaques à messages clairs choisis : accès à l'algorithme de chiffrement (CPA)
- Attaques à chiffrés choisis : accès plus ou moins limité à l'algorithme de déchiffrement (CCA1, CCA2)

## Types d'attaques :

- Bris total (TB) : retrouver la clef secrète
- Attaque contre la notion de sens-unique (OW) : Étant donné un chiffré, retrouver le message correspondant
- Attaque contre l'indistinguabilité des chiffrements (IND) :
  - un attaquant choisit deux messages
  - il reçoit un challenge : un chiffré de l'un des deux messages
  - l'attaquant doit deviner quel message a été chiffré

# Construction classique

- G groupe abélien fini multiplicatif
- M et H deux sous-groupes tels que $G = MH$ et $M \cap H = \{1\}$
- Clef publique : G, algorithmes de génération d'éléments de M et de H
- Chiffrement : $\mathscr{E}(m,h) = mh$ où $m \in M$ et $h$ est un élément aléatoire de H

**Morphisme $\pi$ :**

$$G \simeq M \times H \qquad c$$
$$\downarrow \qquad\qquad \downarrow$$
$$M \qquad\qquad \pi(c)$$

- Déchiffrement :
  $\mathscr{D}(c) = \pi(c) = \pi(mh) = m$
  Système homomorphe :
  $\mathscr{D}(m_1 h_1 m_2 h_2) = m_1 m_2$

- Clef privée : donnée permettant de calculer $\pi$

# Sécurité

- Clef publique : G, algorithmes de génération d'éléments de M et de H
- TB-CPA : Retrouver la donnée permettant de calculer $\pi$
- OW-CPA :
  - Étant donné $c = mh$, retrouver $m$
  - calcul ponctuel de $\mathrm{G} \xrightarrow{\sim} \mathrm{M} \times \mathrm{H}$
  - *Subgroup Decomposition problem*
- IND-CPA :
  - Étant donné $x \in \mathrm{G}$ est-ce que $x \in \mathrm{H}$ ?
  - *Subgroup Membership problem*
- Exemples de tels schémas : Goldwasser-Micali (84), Paillier (99), Boneh-Goh-Nissim (06)...

PRISM

# Exemple dans $\mathbf{Z}/n\mathbf{Z}$

- Soit $n = pq$, un entier RSA, produit de deux premiers de $\lambda$ bits
- On prend $G = (\mathbf{Z}/n\mathbf{Z})^\times$, $M \simeq (\mathbf{Z}/p\mathbf{Z})^\times$, $H \simeq (\mathbf{Z}/q\mathbf{Z})^\times$

**Morphisme $\pi$ :**

$$\begin{array}{ccc} (\mathbf{Z}/n\mathbf{Z})^\times & & x \\ \downarrow & & \downarrow \\ (\mathbf{Z}/p\mathbf{Z})^\times & & x \mod p \end{array}$$

- Chiffrement de $m$ : $mh \in (\mathbf{Z}/n\mathbf{Z})^\times$ où $h$ est un élément aléatoire de $H = \ker \pi$ : $h \in H \Rightarrow \pi(h) = 1$
- Déchiffrement rapide en appliquant $\pi$

# Exemple dans $\mathbf{Z}/n\mathbf{Z}$

- Soit $n = pq$, un entier RSA, produit de deux premiers de $\lambda$ bits
- On prend $G = (\mathbf{Z}/n\mathbf{Z})^\times$, $M \simeq (\mathbf{Z}/p\mathbf{Z})^\times$, $H \simeq (\mathbf{Z}/q\mathbf{Z})^\times$

**Morphisme $\pi$ :**

$$\begin{array}{ccc} (\mathbf{Z}/n\mathbf{Z})^\times & & x \\ \downarrow & & \downarrow \\ (\mathbf{Z}/p\mathbf{Z})^\times & & x \mod p \end{array}$$

- Chiffrement de $m$ : $mh \in (\mathbf{Z}/n\mathbf{Z})^\times$ où $h$ est un élément aléatoire de $H = \ker \pi$ : $h \in H \Rightarrow \pi(h) = 1$
- Déchiffrement rapide en appliquant $\pi$

Clef publique : $n$ et $h$ un générateur de $\ker \pi$

PRISM

# Description de l'algorithme

- Clef publique : $n = pq, h$
- Clef privée : $p$ de $\lambda$ bits
- Chiffrement : Soit $m$ de $\lambda - 1$ bits,

$$\mathcal{E}(m, r) = mh^r \mod n$$

- Déchiffrement :

$$\mathcal{D}(c) = \pi(c) = c \mod p$$

# Description de l'algorithme

- Clef publique : $n = pq, h$
- Clef privée : $p$ de $\lambda$ bits
- Chiffrement : Soit $m$ de $\lambda - 1$ bits,

$$\mathcal{E}(m, r) = mh^r \mod n$$

- Déchiffrement :

$$\mathcal{D}(c) = \pi(c) = c \mod p$$

**Correct**

$$\pi(c) = \pi(m)\pi(h^r) = \pi(m) = m$$

# Cryptanalyse

## Morphisme $\pi$ :

$$\begin{array}{ccc} (\mathbf{Z}/n\mathbf{Z})^\times & & x \\ \downarrow & & \downarrow \\ (\mathbf{Z}/p\mathbf{Z})^\times & & x \mod p \end{array}$$

$h$ générateur de $\ker \pi$

$$\Downarrow$$

$$\begin{cases} h \equiv 1 \pmod{p} \\ h \not\equiv 1 \pmod{q} \end{cases}$$

# Cryptanalyse

## Morphisme π :

$$\begin{array}{ccc} (\mathbf{Z}/n\mathbf{Z})^\times & & x \\ \downarrow & & \downarrow \\ (\mathbf{Z}/p\mathbf{Z})^\times & & x \mod p \end{array}$$

$h$ générateur de $\ker \pi$

$$\Downarrow$$

$$\begin{cases} h \equiv 1 \pmod{p} \\ h \not\equiv 1 \pmod{q} \end{cases}$$

## Cryptanalyse

$$\mathrm{pgcd}(h-1, n) = p$$

# Plan



PRISM

# Groupe de classes (1)

## Corps quadratique imaginaire :

- $K = \mathbf{Q}(\sqrt{\Delta_K})$, $\Delta_K < 0$
- Discriminant fondamental :
  - $\Delta_K \equiv 1 \pmod 4$ sans facteur carré
  - $\Delta_K \equiv 0 \pmod 4$ et $\Delta_K/4 \equiv 2, 3 \pmod 4$ sans facteur carré
- Discriminant non fondamental :
  - $\Delta_\ell = \ell^2 \Delta_k$
  - $\ell$ est appelé le conducteur

PRISM

# Groupe de classes (2)

## Groupe de classes d'idéaux de discriminant $\Delta$ :

- Noté $C(\Delta)$
- Cardinal (fini) appelé le nombre de classes noté $h(\Delta)$
- En moyenne $h(\Delta) \approx 0.461559\sqrt{|\Delta|}$
- Éléments : classe d'équivalence de formes quadratiques (ou d'idéaux) de discriminant $\Delta$

PRISM

# Éléments du groupe de classes

## Forme quadratique définie positive de discriminant $\Delta$

- $f(x,y) = ax^2 + bxy + cy^2$ avec $b^2 - 4ac = \Delta < 0$ et $a > 0$
- On note $f = (a,b,c)$
- Norme de $f$ : $\mathrm{N}(f) = a$

## Relation d'équivalence

- $f \sim g$ si et seulement si il existe $\mathrm{M} = \begin{pmatrix} \mathrm{A} & \mathrm{B} \\ \mathrm{C} & \mathrm{D} \end{pmatrix}$ avec
  $\mathrm{A},\mathrm{B},\mathrm{C},\mathrm{D} \in \mathbf{Z}$ et $\det(\mathrm{M}) = \mathrm{AD} - \mathrm{BC} = 1$ et
  $g(\mathrm{A}x + \mathrm{B}y, \mathrm{C}x + \mathrm{D}y) = f(x,y)$
- Représentant d'une classe : unique $f = (a,b,c)$ tel que
  - $-a < b \leq a \leq c$
  - et de plus $b \geq 0$ si $a = c$
- Si $a < \sqrt{|\Delta|/4}$ et $-a < b \leq a$, $(a,b,c)$ est réduite

# Calcul dans le groupe de classe

## Représentant d'une classe :

- Algorithme de réduction de Lagrange–Gauss, complexité quadratique

## Produit :

- Algorithme de composition des formes quadratiques de Gauss correspond à un produit d'idéaux, complexité quadratique
- Neutre : $[(1, \Delta, \Delta(\Delta-1)/2)]$
- Opposé : $[(a, b, c)]^{-1} = [(a, -b, c)]$

PRISM

# Relations entre deux groupes de classes

## Théorème

- $\Delta_K$ un discriminant fondamental négatif différent de $-3$ et $-4$, $\ell$ un conducteur, et $\Delta_\ell = \ell^2 \Delta_K$,
- Il existe un morphisme surjectif, noté $\bar{\varphi}_\ell$ entre $C(\Delta_\ell)$ et $C(\Delta_K)$

## En pratique

- $\bar{\varphi}_\ell$ est calculable effectivement avec complexité quadratique si et seulement si $\ell$ est connu

PRISM

# Plan



PRISM

# Description de NICE

- Soit $p$ et $q$ deux premiers de $\lambda$ bits avec $p \equiv 3 \pmod 4$, $\Delta_K = -p$, $\Delta_q = -pq^2$

**Morphisme $\bar{\varphi}_q$ :**

$$\begin{array}{cc} \mathrm{C}(\Delta_q) & [f] \\ \downarrow & \downarrow \\ \mathrm{C}(\Delta_K) & [\bar{\varphi}_q(f)] \end{array}$$

- Chiffrement de $[m]$ : $[m][h] \in \mathrm{C}(\Delta_q)$ où $h$ est un élément aléatoire de $\ker \bar{\varphi}_q$
- Déchiffrement rapide en appliquant $\bar{\varphi}_q$

# Description de NICE

- Soit $p$ et $q$ deux premiers de $\lambda$ bits avec $p \equiv 3 \pmod 4$, $\Delta_K = -p$, $\Delta_q = -pq^2$

**Morphisme $\bar{\varphi}_q$ :**

$$\begin{array}{cc} \mathrm{C}(\Delta_q) & [f] \\ \downarrow & \downarrow \\ \mathrm{C}(\Delta_K) & [\bar{\varphi}_q(f)] \end{array}$$

- Chiffrement de $[m]$ : $[m][h] \in \mathrm{C}(\Delta_q)$ où $h$ est un élément aléatoire de $\ker \bar{\varphi}_q$
- Déchiffrement rapide en appliquant $\bar{\varphi}_q$

On publie $[h]$ un élément de $\ker \bar{\varphi}_q$

# Description de l'algorithme

- Hartmann, Hühnlein, Paulus et Takagi (ICISC'98, CHESS'99, SAC'99, JoC 00)
- Clef publique : $\Delta_q = -pq^2$, $[h] \in \ker \bar{\varphi}_q$
- Clef privée : $q$
- Chiffrement : $m$ de petite norme, est codé par $[m] \in \mathrm{C}(\Delta_q)$,

$$\mathscr{E}(m, r) = [m][h]^r$$

- Déchiffrement :

$$\mathscr{D}(c) = \bar{\varphi}_q([m][h]^r) = \bar{\varphi}_q([m]) \rightsquigarrow m$$

# Caractéristiques de NICE

## Avantage du système NICE :

- Déchiffrement quadratique grâce à l'utilisation de $[h]$

## Sécurité :

- TB-CPA : supposé reposer sur la factorisation de $\Delta_q = -pq^2$
- Repose en fait sur le *Kernel Problem* :

> Étant donné $\Delta_q$ et $[h] \in \ker \bar{\varphi}_q$, factoriser $\Delta_q$

- Attaque TB-CCA par Jaulmes et Joux (Eurocrypt'00) : schéma réparable en rajoutant de la redondance au message

PRISM

# Caractéristiques de NICE

## Sécurité (suite) :

- OW-CPA et IND-CPA sous des hypothèses *ad hoc*
- Version IND-CCA basée sur REACT par Buchmann, Sakurai and Takagi (ICISC'01)

## Schémas de signatures basés sur le *Kernel Problem* :

- Hühnlein et Merkle (PKC'00, RSA-CT'01)
- Signatures indéniables par Biehl, Paulus et Takagi (DCC 04)

PRISM

# Plan



PRISM

# Principe de la cryptanalyse (1)

**_Kernel Problem_**

Étant donné $\Delta_q$ et $[h] \in \ker \bar{\varphi}_q$, factoriser $\Delta_q$

**Lemme**

Il existe un isomorphisme effectif

$$\left(\mathcal{O}_{\Delta_K}/q\mathcal{O}_{\Delta_K}\right)^\times/(\mathbf{Z}/q\mathbf{Z})^\times \xrightarrow{\sim} \ker \bar{\varphi}_q$$

PRISM

# Principe de la cryptanalyse (2)

**Théorème**

Dans chaque classe non triviale de $\ker \bar{\varphi}_q$, il existe une forme de norme $q^2$

# Principe de la cryptanalyse (2)

## Théorème

Dans chaque classe non triviale de $\ker \bar{\varphi}_q$, il existe une forme de norme $q^2$

## Démonstration (sketch)

- Système de représentants de $\left(\mathcal{O}_{\Delta_K}/q\mathcal{O}_{\Delta_K}\right)^\times/(\mathbf{Z}/q\mathbf{Z})^\times$ :

$$1 \text{ et } \alpha_x = x + \frac{\Delta_K + \sqrt{\Delta_K}}{2} \text{ avec } x \in \{0, \ldots, q-1\},$$

- Calcul de

$$\left(\mathcal{O}_{\Delta_K}/q\mathcal{O}_{\Delta_K}\right)^\times/(\mathbf{Z}/q\mathbf{Z})^\times \longrightarrow \ker \bar{\varphi_q}$$

# Principe de la cryptanalyse (2)

## Théorème

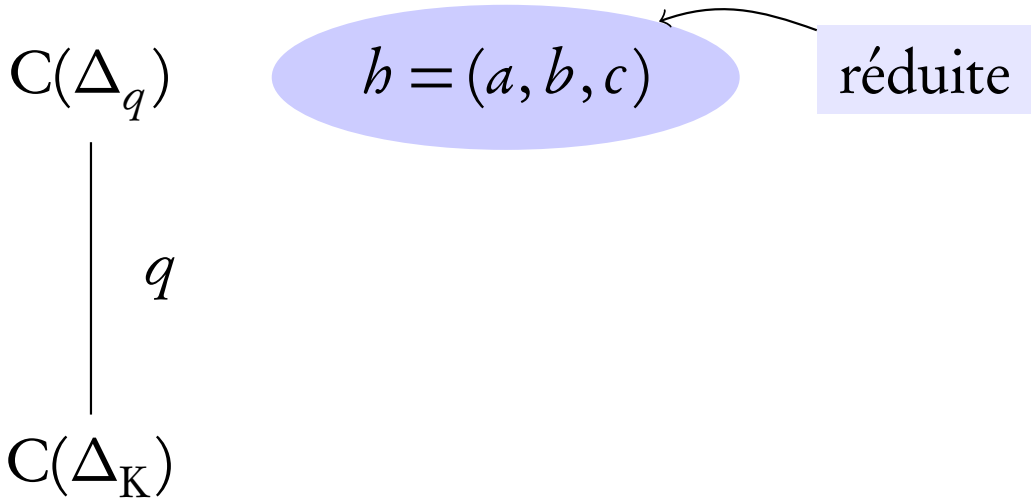
Dans chaque classe non triviale de $\ker \bar{\varphi}_q$, il existe une forme de norme $q^2$

## Conséquence

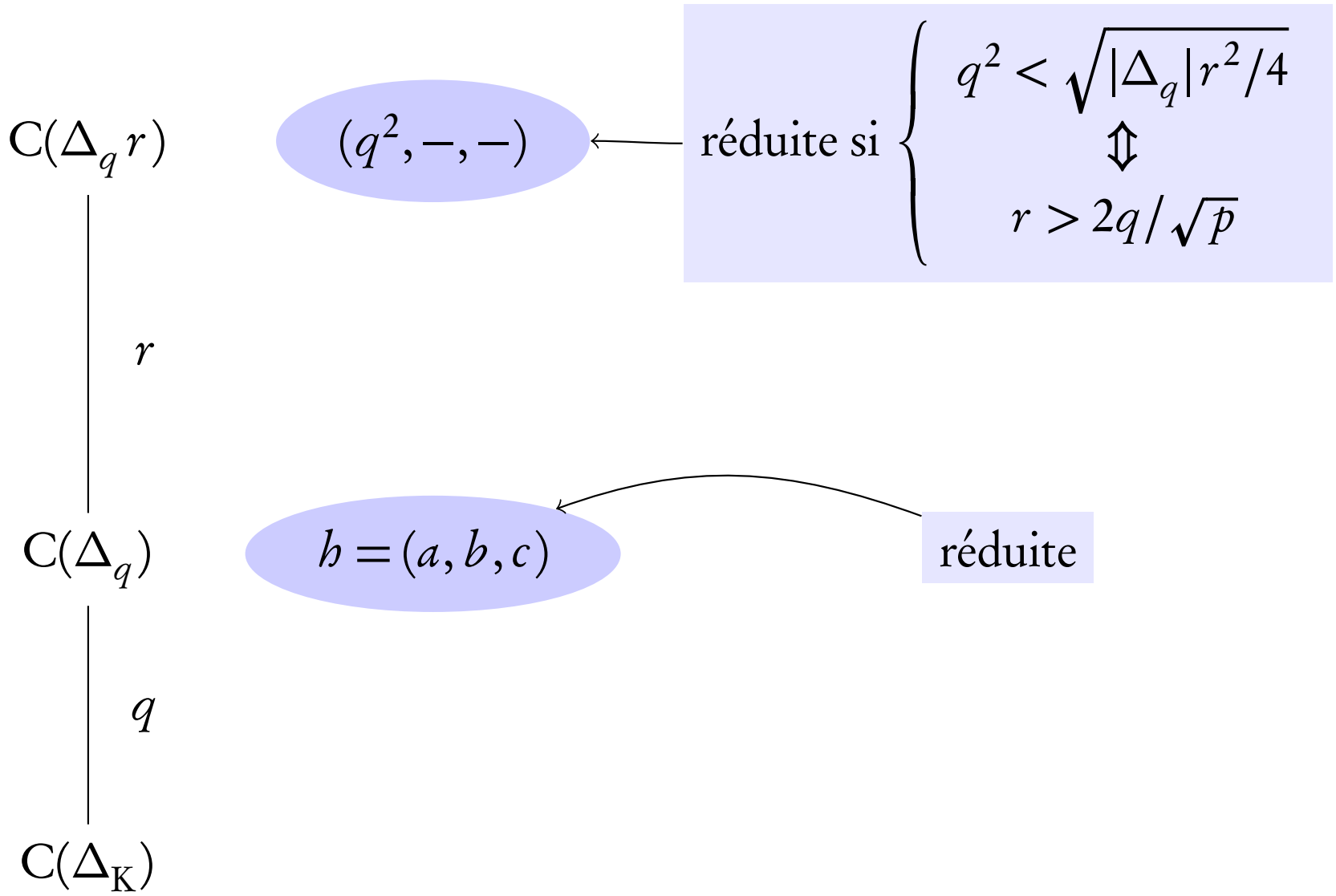
- Dans la clef publique de NICE, la forme réduite $h$ est équivalente à une forme non réduite de norme $q^2$ : $(q^2, -, -)$

PRISM

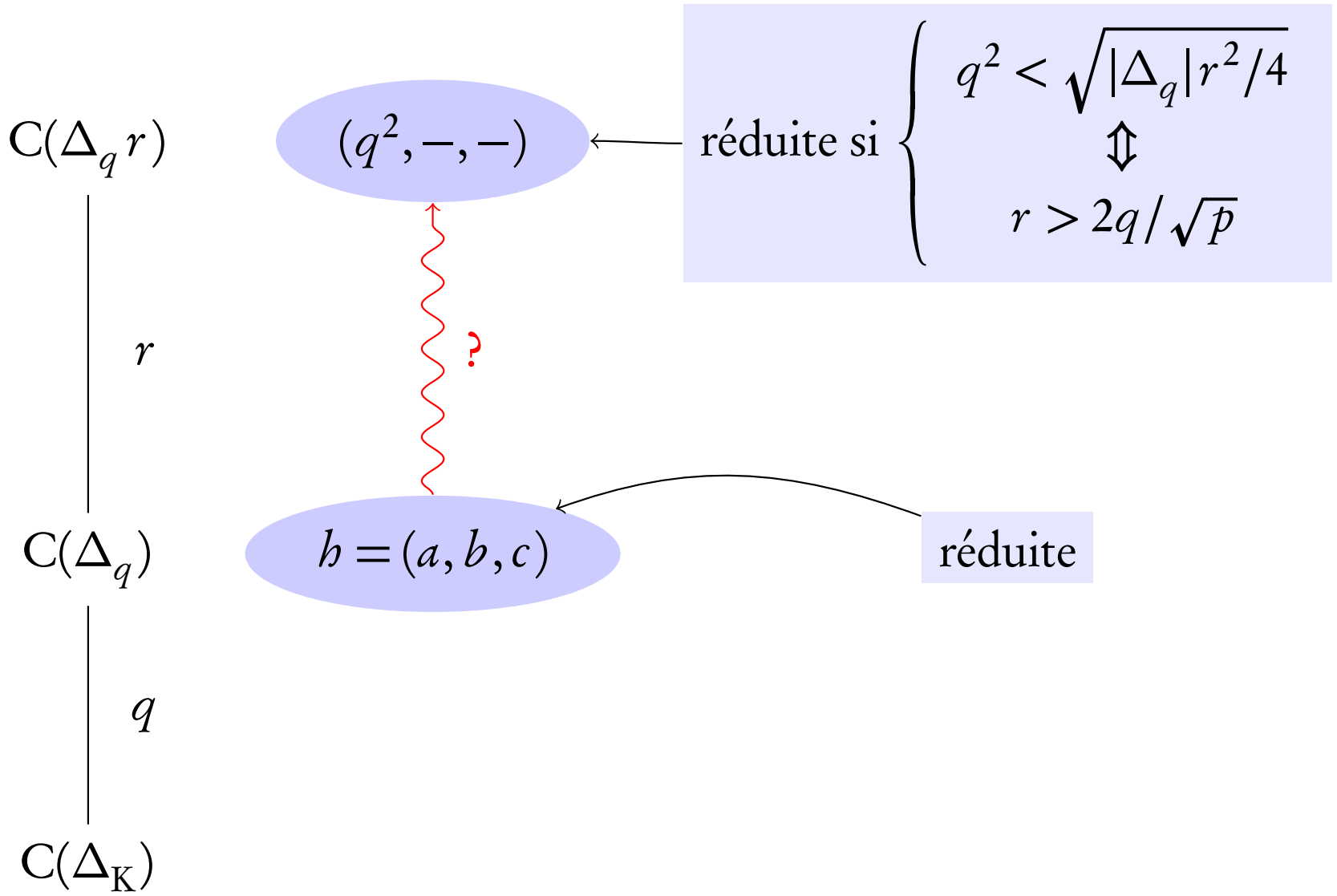
# Relever $[h]$



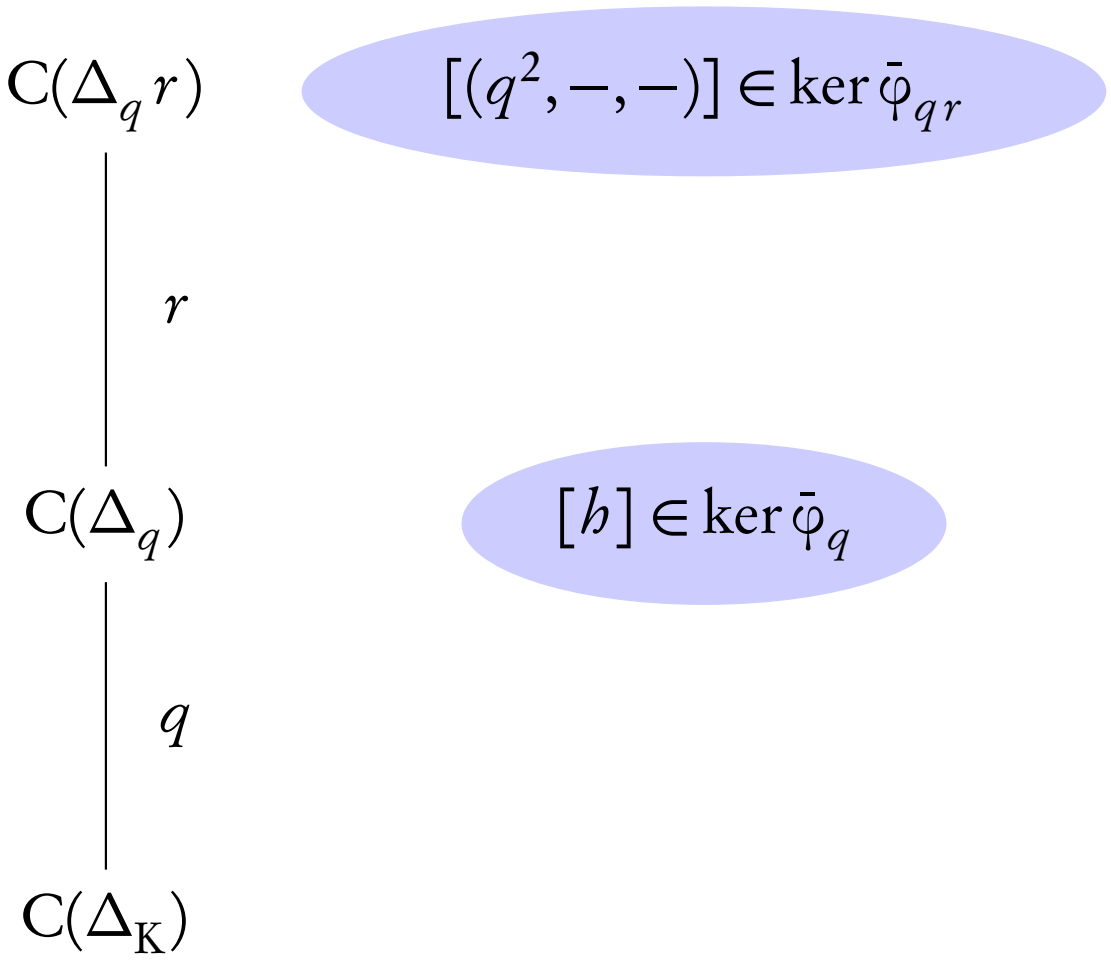
# Relever $[h]$


$C(\Delta_q r)$
$(q^2,-,-)$
réduite si
$q^2 < \sqrt{|\Delta_q| r^2/4}$
$\Updownarrow$
$r > 2q/\sqrt{p}$
$r$
$C(\Delta_q)$
$h = (a,b,c)$
réduite
$q$
$C(\Delta_K)$

# Relever $[h]$


$C(\Delta_q r)$
$(q^2,-,-)$
réduite si
$q^2 < \sqrt{|\Delta_q| r^2/4}$
$\Updownarrow$
$r > 2q/\sqrt{p}$
$r$
?
$C(\Delta_q)$
$h = (a,b,c)$
réduite
$q$
$C(\Delta_K)$

# Relever $[h]$


$C(\Delta_q r)$
$[(q^2,-,-)] \in \ker \bar{\varphi}_{qr}$
$r$
$C(\Delta_q)$
$[h] \in \ker \bar{\varphi}_q$
$q$
$C(\Delta_K)$

# Comment relever $[h]$ ?

$$\ker \bar{\varphi}_{qr} \xrightarrow{\sim} \mathrm{G}_{qr} \xrightarrow{\sim} \mathrm{G}_q \times \mathrm{G}_r$$

**Notation :**

$$\mathbf{G}_\ell := \left(\mathcal{O}_{\Delta_\mathrm{K}}/\ell\,\mathcal{O}_{\Delta_\mathrm{K}}\right)^\times / (\mathbf{Z}/\ell\mathbf{Z})^\times \text{ et } \phi_{\Delta_\mathrm{K}}(\ell) := \#\mathbf{G}_\ell$$

# Comment relever $[h]$ ?

$$\ker \bar{\varphi}_{qr} \xrightarrow{\sim} \mathrm{G}_{qr} \xrightarrow{\sim} \mathrm{G}_q \times \mathrm{G}_r$$

$[(q^2, -, -)]$ $\qquad$ $([\bar{\alpha}], [\bar{1}])$ avec $[\bar{\alpha}] \neq [\bar{1}]$

**Notation :**

$$\mathrm{G}_\ell := \left(\mathcal{O}_{\Delta_\mathrm{K}}/\ell\,\mathcal{O}_{\Delta_\mathrm{K}}\right)^\times / (\mathbf{Z}/\ell\mathbf{Z})^\times \text{ et } \phi_{\Delta_\mathrm{K}}(\ell) := \#\mathrm{G}_\ell$$

# Comment relever $[h]$ ?

$$\ker \bar{\varphi}_{qr} \xrightarrow{\sim} G_{qr} \xrightarrow{\sim} G_q \times G_r$$

$[(q^2, -, -)]$ $\quad$ $([\bar{\alpha}], [\bar{1}])$ avec $[\bar{\alpha}] \neq [\bar{1}]$

$$\ker \bar{\varphi}_q \xrightarrow{\sim} G_q$$

$[h]$

**Notation :**

$$G_\ell := \left(\mathcal{O}_{\Delta_K}/\ell\mathcal{O}_{\Delta_K}\right)^\times / (\mathbf{Z}/\ell\mathbf{Z})^\times \text{ et } \phi_{\Delta_K}(\ell) := \#G_\ell$$

# Comment relever $[h]$ ?

$$\ker \bar{\varphi}_{qr} \xrightarrow{\sim} \mathrm{G}_{qr} \xrightarrow{\sim} \mathrm{G}_q \times \mathrm{G}_r$$

$[(q^2, -, -)]$ $\quad$ $([\bar{\alpha}], [\bar{1}])$ avec $[\bar{\alpha}] \neq [\bar{1}]$

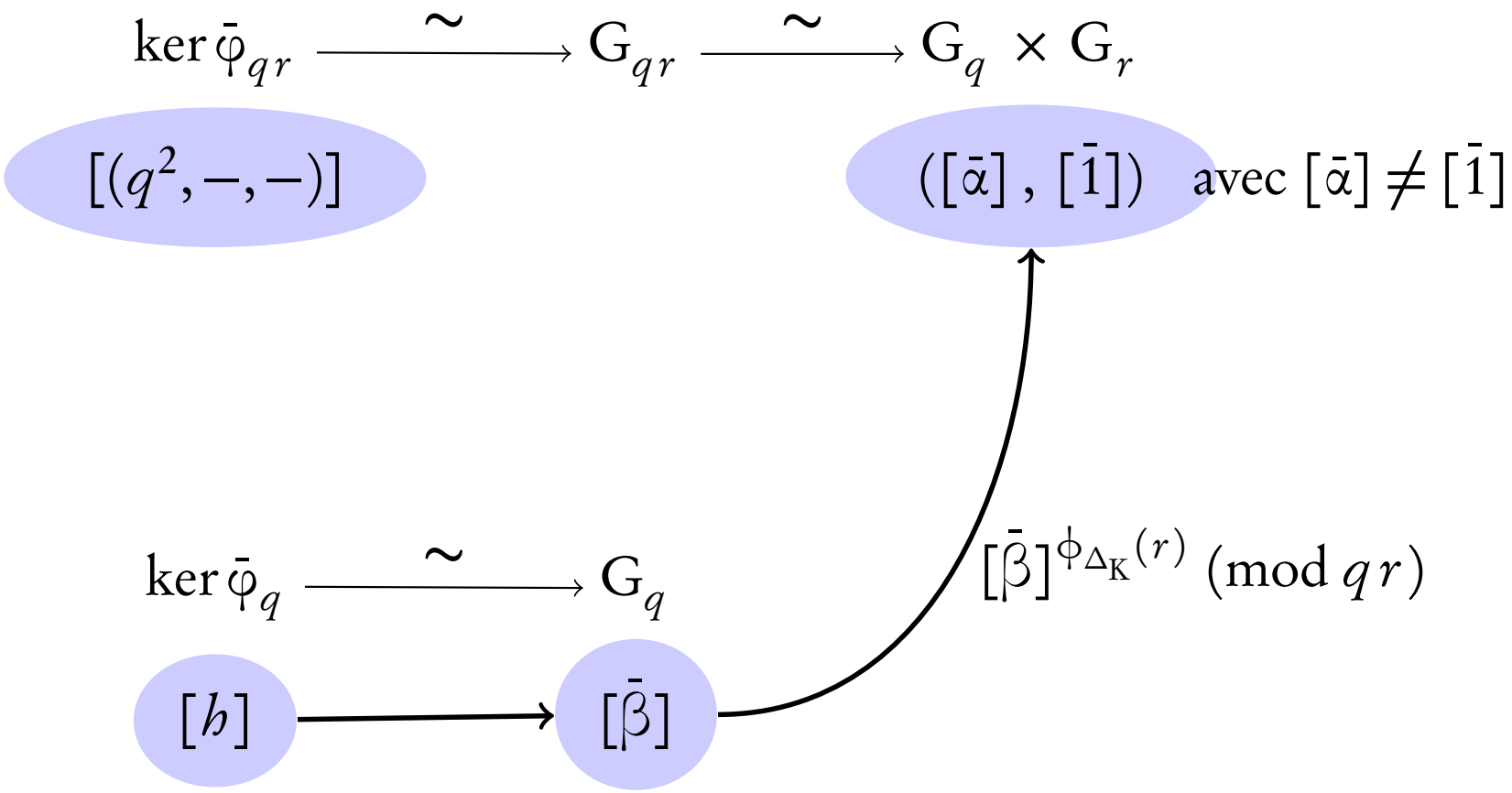
$$\ker \bar{\varphi}_q \xrightarrow{\sim} \mathrm{G}_q$$

$[h] \longrightarrow [\bar{\beta}]$

**Notation :**

$$\mathbf{G}_\ell := \left(\mathcal{O}_{\Delta_K}/\ell\mathcal{O}_{\Delta_K}\right)^\times / (\mathbf{Z}/\ell\mathbf{Z})^\times \text{ et } \phi_{\Delta_K}(\ell) := \#\mathbf{G}_\ell$$

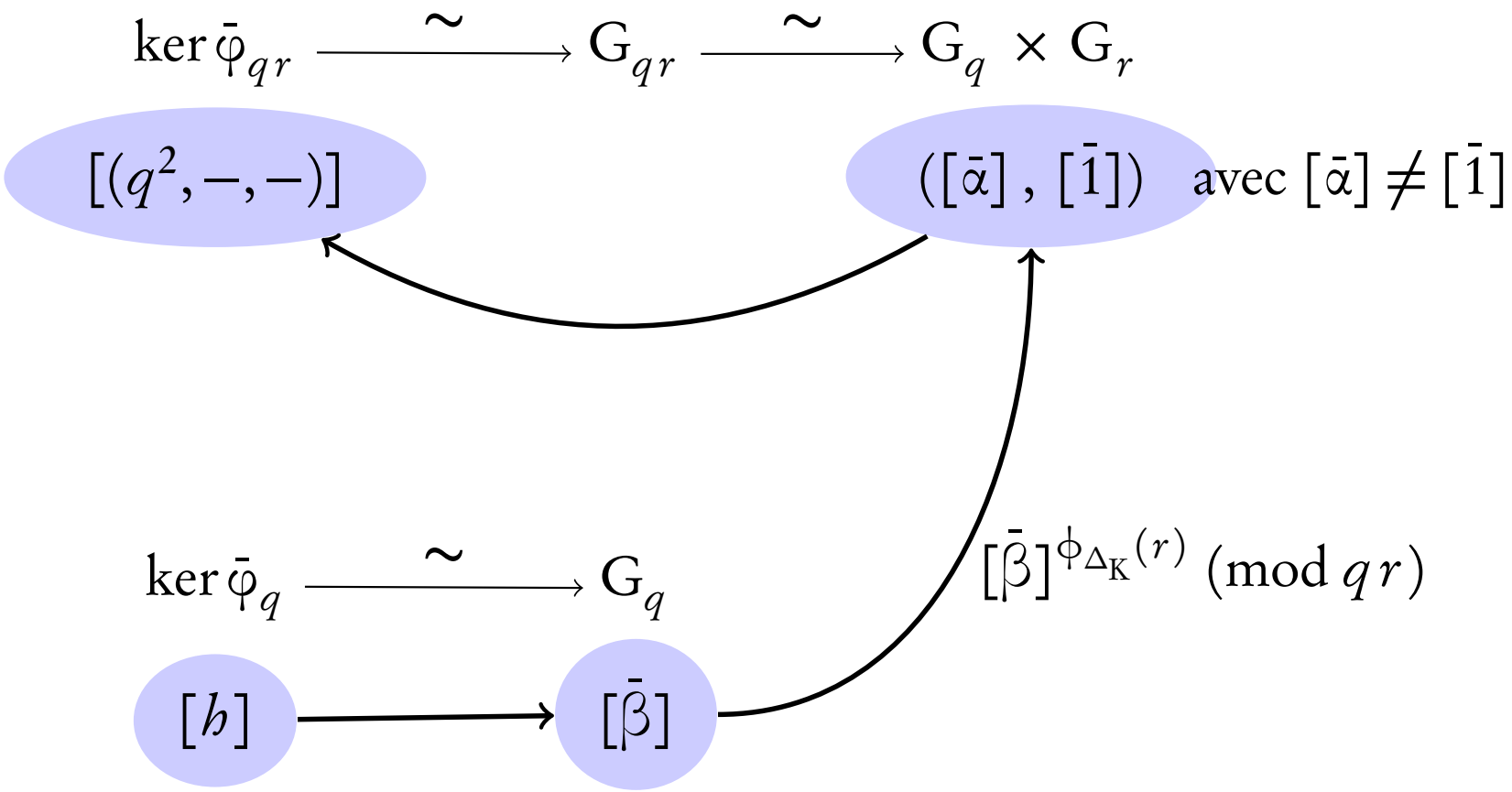
# Comment relever $[h]$ ?




**Notation :**

$$G_\ell := \left(\mathcal{O}_{\Delta_K}/\ell\mathcal{O}_{\Delta_K}\right)^\times / (\mathbf{Z}/\ell\mathbf{Z})^\times \text{ et } \phi_{\Delta_K}(\ell) := \#G_\ell$$

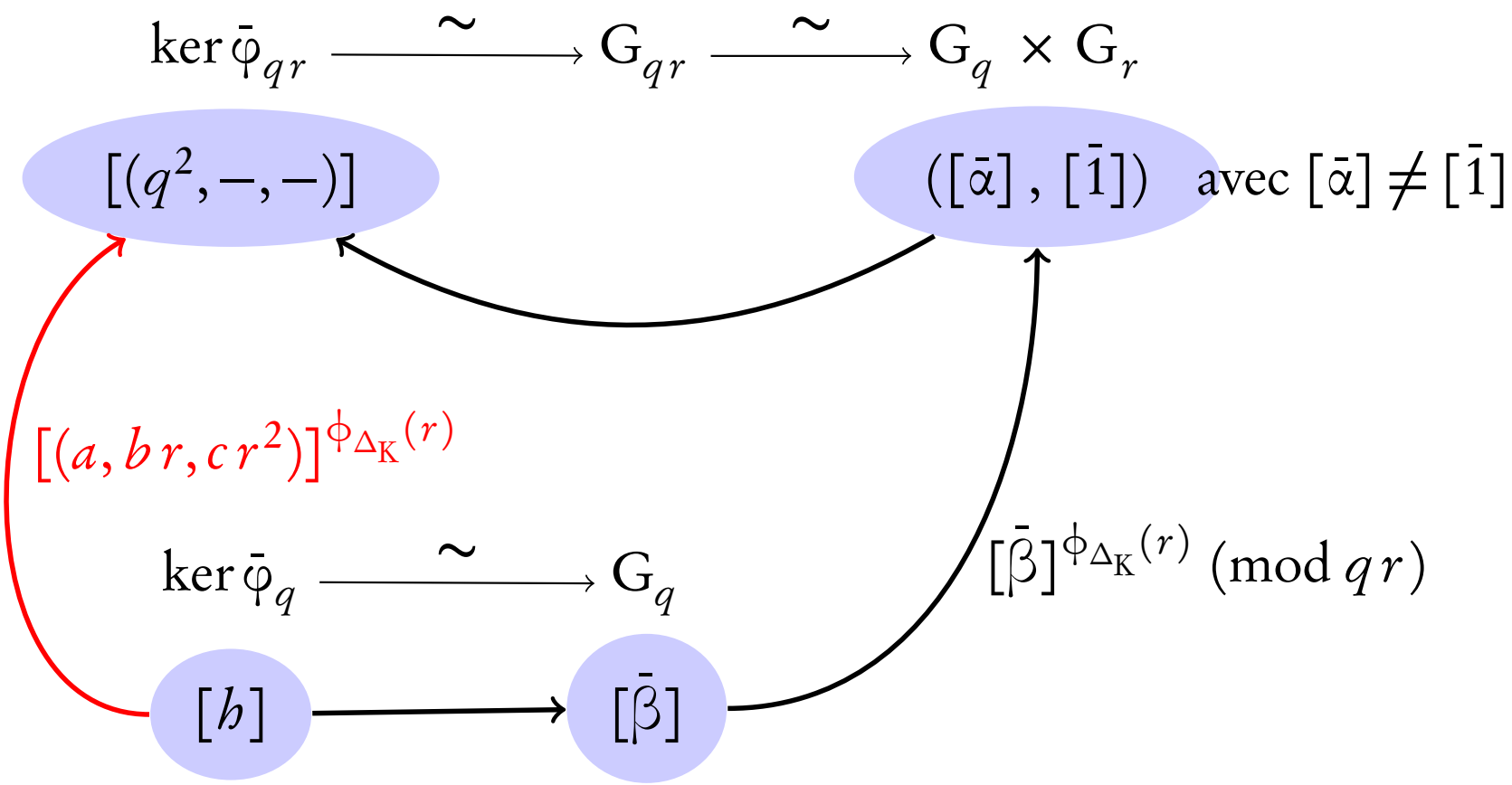
# Comment relever $[h]$ ?




**Notation :**

$$G_\ell := \left(\mathcal{O}_{\Delta_K}/\ell\mathcal{O}_{\Delta_K}\right)^\times / (\mathbf{Z}/\ell\mathbf{Z})^\times \text{ et } \phi_{\Delta_K}(\ell) := \#G_\ell$$

# Comment relever $[h]$ ?




**Notation :**

$$G_\ell := \left(\mathcal{O}_{\Delta_K}/\ell\,\mathcal{O}_{\Delta_K}\right)^\times / (\mathbf{Z}/\ell\mathbf{Z})^\times \text{ et } \phi_{\Delta_K}(\ell) := \#G_\ell$$

# Plan



PRISM

# Autre approche

Travail commun avec A. Joux, F. Laguillaumie and P. Q. Nguyen

## Comment retrouver $q^2$ à partir de $h = (a, b, c)$ ?

- $(a, b, c)$ est la réduction de $(q^2, -, -)$
- $\exists (x_0, y_0) \in \mathbf{Z}$, $a x_0^2 + b x_0 y_0 + c y_0^2 = q^2$
- En pratique, $x_0$ et $y_0$ sont relativement petits par rapport à $\Delta_q = -pq^2$
- On peut retrouver $(x_0, y_0)$ en temps polynomial par réduction d'un réseau euclidien (variante de l'attaque de Coppersmith)

PRISM

# Cas réel

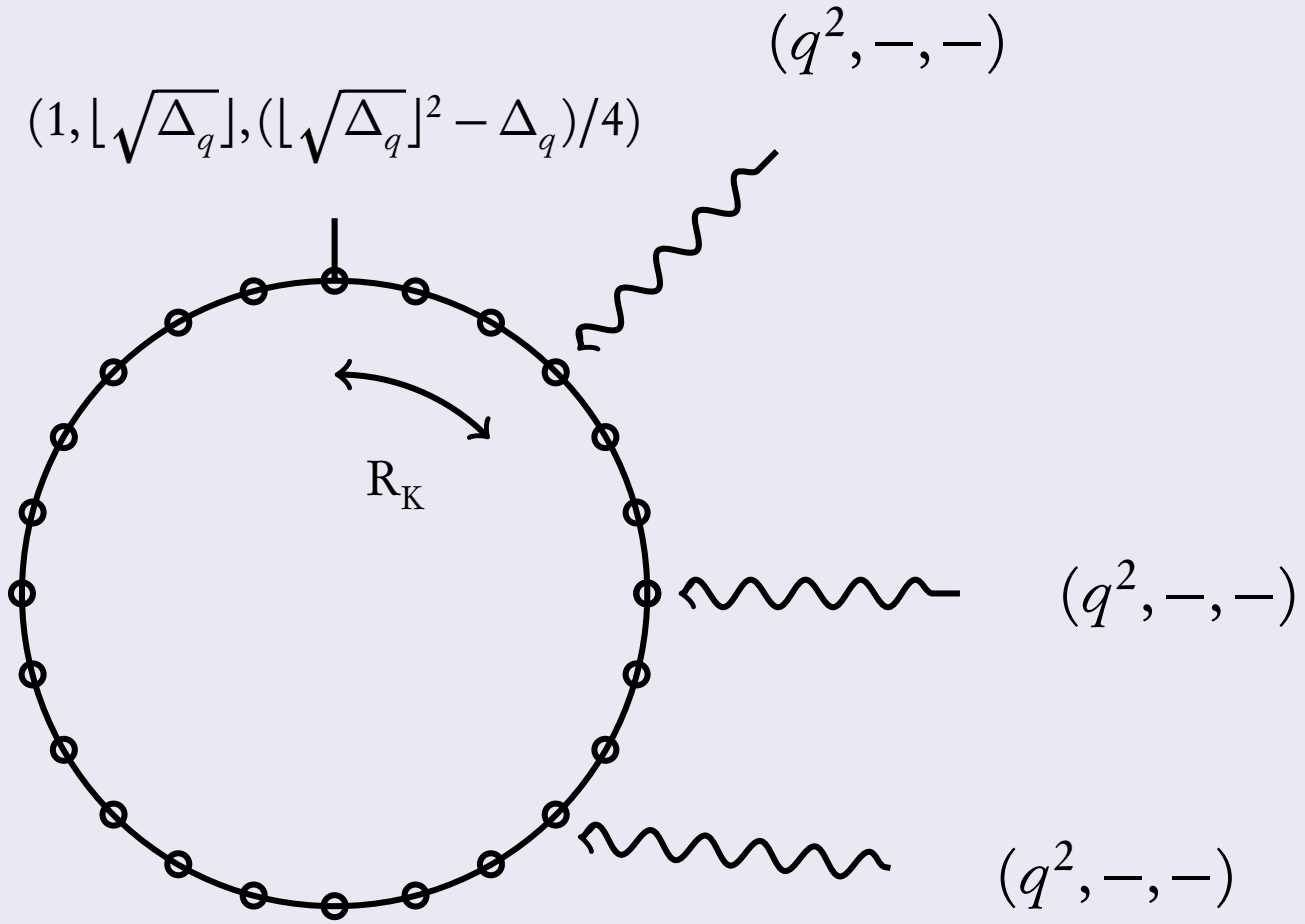
## NICE réel

- Jacobson, Scheidler, Weimer (AFRICACRYPT'08)
- Résiste à la première attaque
- Déchiffrement toujours quadratique
- Différence avec le cas imaginaire : pas une unique forme réduite par classe mais un cycle de formes réduites
- TB-CPA : Équivalent à la factorisation de $\Delta_q = pq^2$ où le régulateur $R_K$ de $\mathbf{Q}(\sqrt{p})$ est petit

PRISM

# Cryptanalyse

## Où trouver les réductions des formes $(q^2, -, -)$ ?



# Conclusion

- Cryptanalyse totale des schémas basés sur NICE
- Suggère qu'il y a peu d'espoir d'avoir un déchiffrement quadratique à partir de l'arithmétique des corps quadratiques
- Nouvel algorithme déterministe (heuristique) de factorisation de $N = pq^2$, complexité en le régulateur de $\mathbf{Q}(\sqrt{p})$, usuellement autour de $\sqrt{p}$

PRISM