1. Preuves Zero-Knowledge

1.1 Preuve de connaissance d'un logarithme discret

On considère un groupe cyclique G, engendré par g, d'ordre premier q.

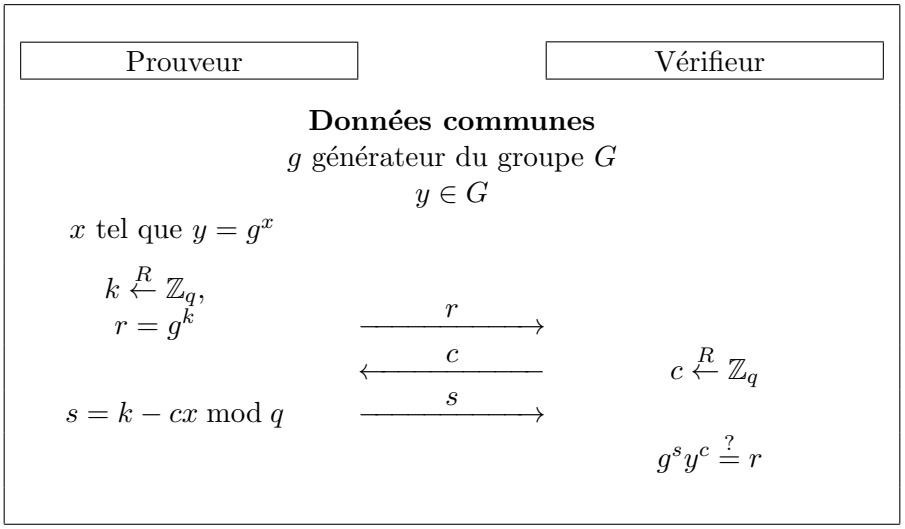

FIGURE 1 – Schéma de Schnorr

Q-1. Montrer la complétude et la correction.

Dans une approche exacte, on considère un adversaire probabiliste qui est accepté avec probabilité $\varepsilon > 1/q$ et dont le temps de calcul est T.

Q-2. Evaluer le temps de calcul moyen T' et la probabilité de succès ε' de l'extracteur en fonction de T, ε, q et τ, où τ est le temps d'exécution du schéma élémentaire.

Q-3. Montrer que ce protocole est ZK face à un vérifieur honnête, et évaluer la complexité de la simulation. Qu'en est-il face à un vérifieur malhonnête ?

1.2 Preuve de connaissance d'une information parmi plusieurs

On considère m utilisateurs d'un système d'identification du type Guillou-Quisquater. On veut proposer un schéma par lequel l'un quelconque de ces utilisateurs peut s'identifier sans qu'il soit possible de déterminer lequel. On note n l'entier RSA sur lequel le Guillou-Quisquater est basé, e l'exposant premier, ℓ un paramètre de sécurité tel que $2^\ell < e$, et t le nombre d'itérations du protocole. On propose le schéma présenté figure 2, répété t fois, dans lequel le j-ième utilisateur joue le rôle du prouveur.

Q-4. Montrer la complétude et la correction. (On se bornera à expliciter ce qu'est une situation favorable, et comment on en extrait la racine e-ième de l'un des x_i.)

Q-5. Expliquer pourquoi le protocole est ZK et pourquoi un adversaire ne peut déterminer lequel des utilisateurs s'est identifié.

Q-6. Dans une approche asymptotique, quel type d'hypothèse doit-on faire sur ℓ, t et m ? On notera k le paramètre de sécurité $k = \log n$.

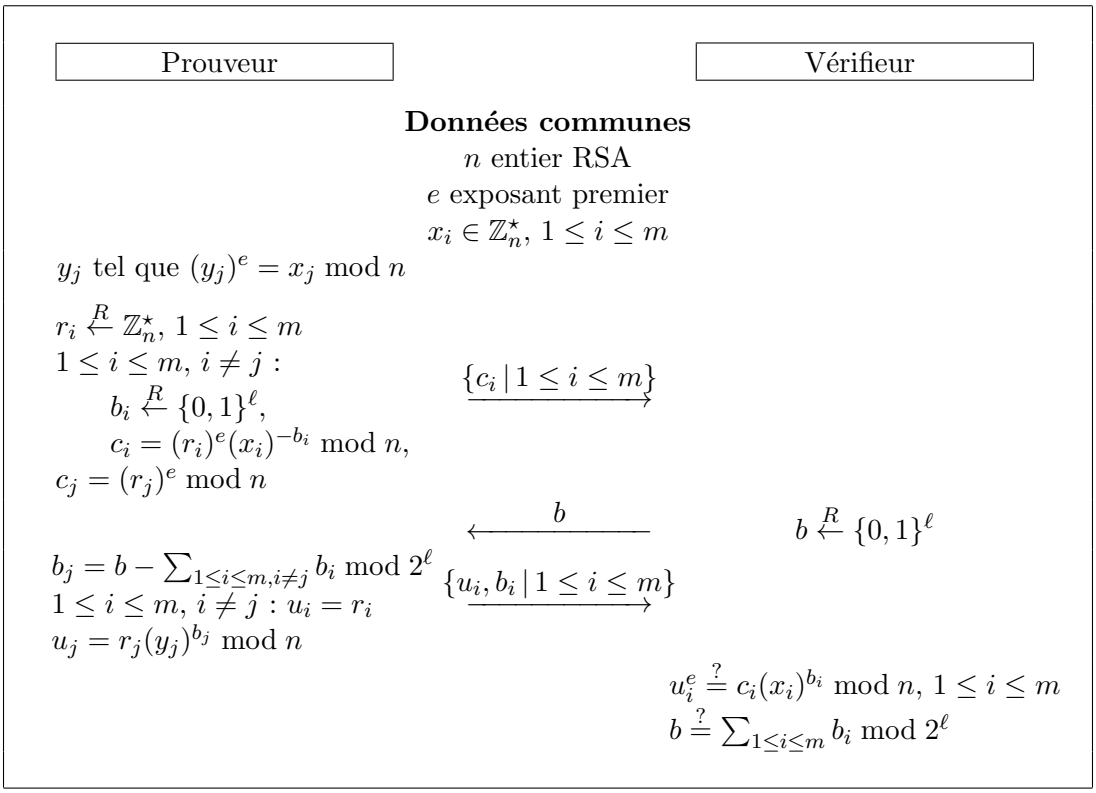

FIGURE 2 – Schéma de un-parmi-m GQ