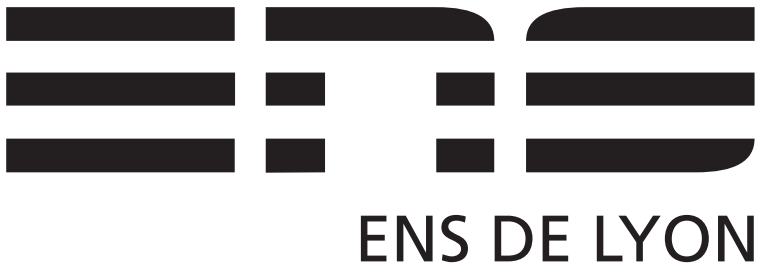
Un schéma de chiffrement à clé publique basé sur le problème de *subset-sum*

Jérémie Dumas

École Normale Supérieure de Lyon

Janvier 2011



Introduction

Dans [LPS10], schéma de chiffrement à clé publique semblable à GPV vu en cours, mais basé sur subset-sum.

- Preuves de sécurité et correction assez courtes
- Applications : *key-leakage attacks*, *oblivious transfert*

Vadim Lyubashevsky, Adriana Palacio, and Gil Segev.
Public-Key Cryptographic Primitives Provably as Secure as Subset Sum.
In Daniele Micciancio, editor, *Theory of Cryptography*, volume 5978 of *Lecture Notes in Computer Science*, pages 382–400. Springer Berlin / Heidelberg, 2010.

Sommaire

Le problème de subset-sum

Énoncé

Étant donnés $a_1, \ldots, a_n$, une cible T, trouver un sous-ensemble $\mathbf{s} \in \{0,1\}^n$ tel que $\sum a_i s_i = T$.

Ici

- $\mathbf{a} \in \mathbb{Z}_{q^m}^n$ et $\mathbf{s} \in \{0,1\}^n$ sont tirés aléatoirement (uniformes).
- Paramètres : n et $M = q^m$.

Difficulté

- Facile quand $\frac{n}{\log M}$ trop petit ou trop grand.
- $SS(n, q^m)$ difficile signifie que $(\mathbf{a}, \mathbf{a} \cdot \mathbf{s})$ est algorithmiquement indistinguable de l'uniforme.

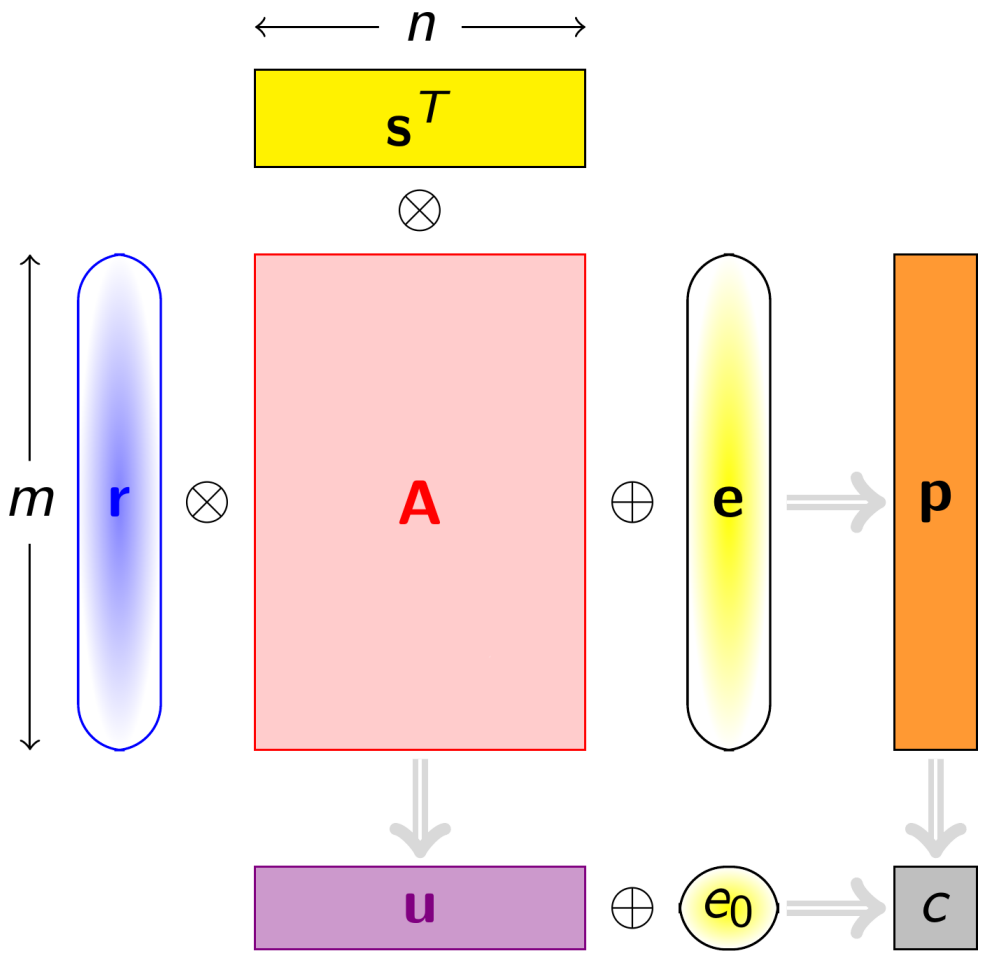
Notations

Opération de subset-sum

- Soient $\mathbf{a} \in \mathbb{Z}_{q^m}^n$ et $\mathbf{s} \in \{0,1\}^n$.
- $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ la représentation matricielle en base q des composants de $\mathbf{a}$
- $\mathbf{t}$ vecteur colonne, décomposition en base q de $\mathbf{a} \cdot \mathbf{s} \in \mathbb{Z}_{q^m}$.
- On a alors $\mathbf{t} = \mathbf{A}\mathbf{s} + \mathbf{c}$ où $\mathbf{c}$ vecteur de retenue.
- On notera donc $\mathbf{t} = \mathbf{A} \odot \mathbf{s}$ l'opération subset-sum, tel que $|t_i| \leqslant \frac{q-1}{2}$.

Remarque : on travaille ici avec des représentants centrés en 0 (pour $\mathbf{e} \in \mathbb{Z}_q^n$, les e_i sont dans $[-\frac{q-1}{2}, \frac{q-1}{2}]$).

Chiffrement GPV



- Paramètres : n, m, q.
- $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ uniforme.
- Clé secrète : $\mathbf{r} \in \mathcal{E}^m$ tiré selon une gaussienne bien choisie.
- Chiffrer $z \in \{0,1\}$: renvoyer $(\mathbf{p}, c) = (\mathbf{A}\mathbf{s}+\mathbf{e}, \mathbf{u}\cdot\mathbf{s}+e_0+[\frac{q}{2}]z)$
- $\mathbf{e}, e_0$ sont des termes de bruit "pas trop gros".
- Déchiffrer $(\mathbf{p}, c)$: on compare $|c - \mathbf{r}^T\mathbf{p}|$ à $\frac{q}{4}$.

Chiffrement LPS

Vue d'ensemble

- GPV repose sur le fait que $(\mathbf{p}, c)$ indistinguable de l'uniforme.
- Dans LPS, c'est un peu pareil : pour des éléments $\mathbf{A}' \in \mathbb{Z}_q^{n \times n}$ et $\mathbf{s} \in \{0,1\}^n$ tirés uniforméments, la distribution $(\mathbf{A}', \mathbf{A}' \odot \mathbf{s})$ sera indistinguable de l'uniforme.
- Le "bruit" $\mathbf{e}$ correspond au veceur de retenue c (coef. "petits" $< n$).
- Possibilité d'encrypter directement $\mathbf{z} \in \{0,1\}^k$ pour k par trop gros (après subset-sum devient facile).

Chiffrement LPS

Chiffrage d'un bit $z \in \{0,1\}$

Définition

Paramètres : n et $q > 10n\log^2(n)$.

KeyGen Échantillonner $\mathbf{A}' \in \mathbb{Z}_q^{n\times n}$ et $\mathbf{s} \in \{0,1\}^n$ uniformes indépendamment. Calculer $\mathbf{A} = [\mathbf{A}' \| \mathbf{A}' \odot \mathbf{s}]$.
Renvoyer le couple $(PK, SK) = (\mathbf{A}, \mathbf{s})$.

Enc(z) Échantillonner $\mathbf{r} \in \{0,1\}^n$ de manière uniforme.
Renvoyer le chiffré $\mathbf{u}^T = \mathbf{r}^T \odot \mathbf{A} + \frac{q-1}{2}[0^n \| z]$.

Dec($\mathbf{u}^T$) Décomposer $\mathbf{u}^T = [\mathbf{v}^T \| w]$. Calculer $y = \mathbf{v}^T\mathbf{s} - w \in \mathbb{Z}_q$.
Si $|y| < q/4$ renvoyer 0, sinon renvoyer 1.

Correction de LPS

Idée de la preuve

- On veut montrer que $\mathtt{Dec}(\mathbf{u}^T) = z$ avec forte proba.
- Il faut voir que $\odot$ "ressemble" à la multiplication de matrices.
- Ce qui impliquera que $|\mathbf{v}^T\mathbf{s} - w| \approx \frac{q-1}{2}z$.
- Pour cela, utilise deux lemmes intermédiaires sur l'opérateur $\odot$.

Correction de LPS

Lemmes intermédiaires

Lemme 1

Pour tout $\mathbf{r} \in \{0,1\}^n$, on a $\|\mathbf{r}^T \odot \mathbf{A} - \mathbf{r}^T\mathbf{A}\|_\infty < \sqrt{n}\log n$ avec forte proba.

Idée de preuve

Décomposer les retenues c_i sous la forme $x_i + y_i$, avec les x_i variables indépendantes, et les y_i très petits. Appliquer ensuite une borne due à Hoeffding pour s'en sortir.

Lemme 2

Pour tout $r, s \in \{0,1\}^n$, on a $\|(\mathbf{r}^T \odot \mathbf{A})\mathbf{s} - \mathbf{r}^T\mathbf{A}\mathbf{s}\|_\infty < n\log^2 n$ avec forte probabilité.

Correction de LPS

Corollaire

$\mathtt{Dec}(\mathbf{u}^T) = z$ avec forte proba.

- Rappel : $\mathbf{u}^T = [\mathbf{v}^T \| w] = \mathbf{r}^T \odot \mathbf{A} + \frac{q-1}{2}[0^n \| z]$.
- On a $w = \mathbf{r}^T(\mathbf{A}' \odot \mathbf{s}) + \eta + \frac{q-1}{2}z$.
- Écrire y sous la forme $(\mathbf{r}^T \odot \mathbf{A}')\mathbf{s} + \nu s_n - \mathbf{r}^T(\mathbf{A}' \odot \mathbf{s}) - \eta - \frac{q-1}{2}z$.
- Où ν et η = termes de retenue, petits, $< n$. Déduire que :

$$\begin{aligned} |\mathbf{v}^T\mathbf{s} - w - \frac{q-1}{2}z| &\leqslant |(\mathbf{r}^T \odot \mathbf{A}')\mathbf{s} - \mathbf{r}\mathbf{A}'\mathbf{s}| + |\mathbf{r}^T(\mathbf{A}' \odot \mathbf{s}) - \mathbf{r}\mathbf{A}'\mathbf{s}| \\ &\quad + |\nu s_n| + |\eta| \\ &\leqslant n\log^2 n + n\log^2 n + 2n \end{aligned}$$

- D'où $y = \mathbf{v}^T\mathbf{s} - w$ est proche de $\frac{q-1}{2}z$.

Sécurité de LPS

- Notion de sécurité sémantique ou sécurité cpa telle que vue en cours.
- L'adversaire ne doit pas pouvoir distinguer deux messages m_0 et m_1 encryptés avec LPS.
- Difficulté de SS : $(\mathbf{A}, \mathbf{r}^T \odot \mathbf{A})$ indistinguable de l'uniforme.
- Donc $(PK, \mathtt{Enc}_{PK}(m_0))$ et $(PK, \mathtt{Enc}_{PK}(m_1))$ sont indisinguables pour l'adversaire cpa.

Attaques avec fuite d'informations sur la clé

Généralités

- Même cadre de jeu que pour cpa.
- Fonction de fuite $f : \mathcal{SK}_n \to \{0,1\}^\lambda$, paramètre λ fixé.
- Notion d'attaques adaptative et non-adaptative.
- Ici sécurité dans le cas non-adaptatif seulement.

Attaques avec fuite d'informations sur la clé

Primitives

Paramètres : n, m, q, T

`KeyGen` Échantillonner $\mathbf{A}' \in \mathbb{Z}_q^{n \times m}$ et $\mathbf{s} \in \{-\frac{T-1}{2}, \ldots, \frac{T-1}{2}\}^m$ uniformes indépendamment. Calculer $\mathbf{A} = [\mathbf{A}' \| \mathbf{A}'\mathbf{s}]$. Renvoyer $(PK, SK) = (\mathbf{A}, \mathbf{s})$.

`Enc` et `Dec` idem que dans LPS classique.

Sécurité

Distributions $(PK, \mathtt{Enc}_{PK}(0), f(SK))$ et $(PK, \mathtt{Enc}_{PK}(1), f(SK))$ algorithmiquement indistinguables.

Transfert inconscient

Principe

- Émetteur $\mathcal{E}$ possède deux messages $\mathbf{z}_0, \mathbf{z}_1$.
- Receveur $\mathcal{R}$ choisit $b \in \{0, 1\}$.
- À la fin du transfert, $\mathcal{R}$ a reçut $\mathbf{z}_b$, et ignore tout de $\mathbf{z}_{1-b}$.
- $\mathcal{E}$ ignore tout de b.

- Sécurité pour le receveur / l'émetteur.
- Notion de protocole honnête.
- Transformer un protocole *honnête* en un protocole général.

Transfert inconscient

Protocole proposé dans [LPS10]

Paramètres $n, k \in \mathbb{N}$, pour le receveur $b \in \{0,1\}$, pour l'émetteur $\mathbf{z}_0, \mathbf{z}_1$.

Receveur	Génère (PK_b, SK_b), tire PK_{1-b} dans $\mathbb{Z}_q^{n\times(n+k)}$. Envoie (PK_0, PK_1).
Émetteur	Chiffre $\mathbf{u}_i^T = \mathtt{Enc}_{PK_i}(\mathbf{z}_i)$. Envoie $(\mathbf{u}_0^T, \mathbf{u}_1^T)$
Receveur	Déchiffre $z_b = \mathtt{Dec}_{SK_b}(\mathbf{u}_b^T)$

Sécurité

- Pour le receveur contre des émetteurs malicieux.
- Pour l'émetteur contre des émetteurs honnêtes-mais-curieux.

Conclusion

- Nouveau schéma de chiffrement à clé publique.
- Sécurité sémantique, sécurité contre les attaques avec fuites d'informations (cas non-adaptatif).
- Protocole de transfert inconscient, honnêteté pour le receveur.
- Problèmes ouverts : attaques adaptatives, cryptage direct de k bits avec k plus élevé, etc.

Merci de votre attention.