Polynômes de permutation à trappe et chiffrement à clef publique

Guilhem Castagnos

Équipe Algo – GREYC

Mardi 18 mars

(Travail commun avec Damien Vergnaud)

Plan

Schéma de chiffrement asymétrique

Trois algorithmes :

- Génération de clefs :
  - Entrée : un paramètre de sécurité k
  - Sortie : une paire $(k_{\text{pub}}, k_{\text{priv}})$, clef publique et privée
- Chiffrement :
  - Entrée : un message m et k_{pub}
  - Sortie : un chiffré $c \leftarrow \mathcal{E}_{k_{\text{pub}}}(m)$, noté aussi $c = \mathcal{E}_{k_{\text{pub}}}(m, r)$ pour un aléa r
- Déchiffrement :
  - Entrée : un chiffré c et k_{priv}
  - Sortie de $\mathcal{D}_{k_{\text{priv}}}(c)$: un message m ou le symbole spécial $\perp$
  - $\mathcal{D}_{k_{\text{priv}}}(\mathcal{E}_{k_{\text{pub}}}(m, r)) = m$

Sécurité

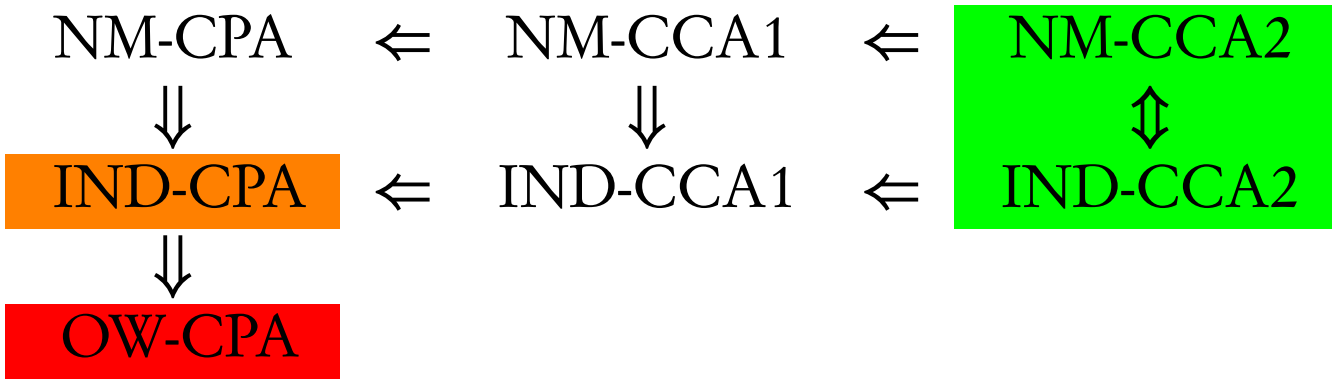
- Buts de l'attaquant :
  - Sens-unique : Étant donné un chiffré, un attaquant ne peut retrouver le message correspondant (OW)
  - Sécurité sémantique : Étant donné un chiffré, un attaquant ne peut extraire aucune information sur le message correspondant
  - Équivalent à la notion d'indistinguabilité (IND), Goldwasser et Micali 1984 :
    - 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
  - Non malléabilité : Étant donné un chiffré, un attaquant ne peut produire un autre chiffré tel que les messages correspondants soient reliés (NM), Dolev, Dwork et Naor, 1991

Sécurité

- Moyens de l'attaquant :
  - Attaques à messages clairs choisis : accès à un oracle de chiffrement (CPA)
  - Attaques non adaptatives à messages chiffrés choisis : accès à un oracle de déchiffrement avant le challenge (CCA1), Naor et Yung, 1990
  - Attaques adaptatives à messages chiffrés choisis : accès illimité sauf sur le challenge, (CCA2), Rackoff et Simon, 1991

Sécurité

- Relations :



Sécurité

- Comment prouver la sécurité :
  - Preuve par réduction : si un attaquant IND-CPA existe alors tel problème algorithmique peut-être résolu
  - Pour les attaques CCA :
    - modèle de l'oracle aléatoire (ROM), idéalise les fonctions de hachages, Bellare et Rogaway, 1993 : les fonctions de hachages sont modélisées par un oracle aléatoire
    - notion de *Plaintext-awareness* : un attaquant ne peut construire un chiffré valide sans connaître le message correspondant (PA1) : formalisé dans le modèle standard par Bellare et Palacio, 2004

Dans le modèle standard

$$\text{PA1} + \text{IND-CPA} \Rightarrow \text{IND-CCA1}$$

Plan

Polynômes de permutation à trappe de $\mathbf{Z}/n\mathbf{Z}$

- Soit $n = pq$ un entier RSA (p et q deux grands premiers distincts)
- P sera dit polynôme de permutation à trappe de $\mathbf{Z}/n\mathbf{Z}$:
  - si P induit une bijection de $\mathbf{Z}/n\mathbf{Z}$
  - si étant donné a, $\mathrm{P}(a)$ est calculable en temps polynomial
  - si étant donné $\mathrm{P}(a)$ il est difficile de retrouver a à moins de connaître une trappe (factorisation de n ou description de la fonction inverse)
- On note P^{-1} et on appelle problème de l'inversion ponctuelle de P le problème suivant : étant donné $\alpha = \mathrm{P}(a) \in \mathbf{Z}/n\mathbf{Z}$, retrouver a
- Un polynôme de permutation à trappe P de $\mathbf{Z}/n\mathbf{Z}$ induit un système de chiffrement OW-CPA sous l'hypothèse que P^{-1} est difficile

RSA

- Rivest, Shamir, Adleman, 1978
- Soit e premier avec $\varphi(n) = (p-1)(q-1)$
- $\mathrm{P}(\mathrm{X}) = \mathrm{X}^e$ est un polynôme de permutation à trappe de $\mathbf{Z}/n\mathbf{Z}$
- La trappe est d l'inverse de e modulo $\varphi(n)$
- P s'évalue en moyenne en $\frac{3}{2}|e|\mathrm{M}$

LUC

- Smith et Lennon, 1993
- Soit la suite de Lucas $V(a,b)$, suite d'entiers définie par :

$$\forall k \geqslant 1, V_{k+1}(a,b) = aV_k(a,b) - bV_{k-1}(a,b)$$

et $V_1(a,b) = a, V_0(a,b) = 2$

- Le polynôme de degré e, $P(X) = V_e(X,1)$ avec e premier à $(p^2-1)(q^2-1)$ est un polynôme de permutation à trappe de $\mathbf{Z}/n\mathbf{Z}$ (polynôme de Dickson)
- La trappe est d l'inverse de e modulo $(p^2-1)(q^2-1)$
- P s'évalue en $2|e|M$

Autres polynômes de permutation à trappe de $\mathbf{Z}/n\mathbf{Z}$

- Le polynôme utilisé dans LUC provient de « l'automorphisme RSA », $\alpha \mapsto \alpha^e$, du groupe des entiers algébriques de norme 1 modulo n d'un corps quadratique, que l'on transporte sur $\mathbf{Z}/n\mathbf{Z}$ en utilisant l'application trace

- Cet automorphisme peut aussi être transporté sur $\mathbf{Z}/n\mathbf{Z}$ par paramétrisation du tore algébrique : on obtient alors des fonctions de Rédéi. Proposé pour construire un cryptosystème par Lidl et Muller (1983)

- L'automorphisme $P \mapsto e.P$ d'une courbe elliptique définie sur $\mathbf{Z}/n\mathbf{Z}$ peut aussi être transporté sur $\mathbf{Z}/n\mathbf{Z}$ en utilisant les polynômes de division (Demytko 1993)

Plan

Notations et définitions

- Dans la suite n sera toujours un entier RSA, P et Q seront deux polynômes de permutations de $\mathbf{Z}/n\mathbf{Z}$ de degrés respectifs e_P et e_Q et $R \in \mathbf{Z}/n\mathbf{Z}[X, Y]$ un polynôme bivarié avec $e_R = \deg_X(R)$

- On définit un nouvelle famille de problèmes algorithmiques :

Computational Polynomial DH : C-POL-DH(n, P, Q, R)

Étant donnés $\alpha = P(a) \in (\mathbf{Z}/n\mathbf{Z})^\times$ et $\beta = Q(b) \in (\mathbf{Z}/n\mathbf{Z})^\times$
Trouver : $R(a, b) \in (\mathbf{Z}/n\mathbf{Z})^\times$

Notations et définitions

Computational Polynomial DH : C-POL-DH(n, P, Q, R)

Étant donnés $\alpha = P(a) \in (\mathbf{Z}/n\mathbf{Z})^\times$ et $\beta = Q(b) \in (\mathbf{Z}/n\mathbf{Z})^\times$
Trouver : $R(a, b) \in (\mathbf{Z}/n\mathbf{Z})^\times$

- On se limitera aux cas suivants :
  - $R(X, Y) = XY$, noté C-POL1(n, P, Q)
  - $R(X, Y) = P\left((XY)^\ell\right)$, noté C-POL2$(n, \ell, P, Q)$
  - $R(X, Y) = Q(X)$ noté C-DPOL(n, P, Q)

- C-DPOL(n, P, Q) peut être ré-écrit : étant donné $P(a)$ calculer $Q(a)$: généralisation de Dependent-RSA : étant donné a^e, calculer $(a+1)^e$ (Pointcheval 1999)

Notations et définitions

- On définit la variante décisionnelle :

Decision Polynomial DH : D-POL-DH$(n, \mathrm{P}, \mathrm{Q}, \mathrm{R})$

Étant donnés $\alpha = \mathrm{P}(a) \in (\mathbf{Z}/n\mathbf{Z})^\times$, $\beta = \mathrm{Q}(b) \in (\mathbf{Z}/n\mathbf{Z})^\times$ et $\gamma \in (\mathbf{Z}/n\mathbf{Z})^\times$
Décider si $\gamma = \mathrm{R}(a, b)$

- On définit également 3 problèmes décisionnels D-POL1$(n, \mathrm{P}, \mathrm{Q})$, D-POL2$(n, \ell, \mathrm{P}, \mathrm{Q})$ et D-DPOL$(n, \mathrm{P}, \mathrm{Q})$ pour les trois cas $\mathrm{R}(\mathrm{X}, \mathrm{Y}) = \mathrm{XY}$, $\mathrm{R}(\mathrm{X}, \mathrm{Y}) = \mathrm{P}\left((\mathrm{XY})^\ell\right)$ et $\mathrm{R}(\mathrm{X}, \mathrm{Y}) = \mathrm{Q}(\mathrm{X})$

Notations et définitions

- Pour l'étude des relations entre les problèmes on définit un problème d'extraction

E-POL-DH(n, P, Q, R)

Étant donnés $\alpha = P(a) \in (\mathbf{Z}/n\mathbf{Z})^\times$, $\beta = Q(b) \in (\mathbf{Z}/n\mathbf{Z})^\times$ et $\gamma = R(a,b) \in (\mathbf{Z}/n\mathbf{Z})^\times$
Trouver a and b

- On définit également les 3 problèmes E-POL1, E-POL2, E-DPOL pour les trois cas $R(X,Y) = XY$, $R(X,Y) = P\left((XY)^\ell\right)$ et $R(X,Y) = Q(X)$

Les problèmes C-POL1 et C-POL2

Théorème

$$\text{D-POL1}(n,\mathrm{P},\mathrm{Q}) \overset{\mathscr{P}}{\Longleftarrow} \text{C-POL1}(n,\mathrm{P},\mathrm{Q}) \overset{\mathscr{P}}{\Longleftrightarrow} \mathrm{P}^{-1}(n) \wedge \mathrm{Q}^{-1}(n)$$

Théorème

$$\text{C-POL2} \wedge \text{E-POL2} \overset{\mathscr{P}}{\Longleftrightarrow} \mathrm{P}^{-1} \wedge \mathrm{Q}^{-1} \overset{\mathscr{P}}{\Longrightarrow} \begin{matrix}\text{C-POL2}\\ \text{E-POL2}\end{matrix} \overset{\mathscr{P}}{\Longrightarrow} \text{D-POL2}$$

Les problèmes D-POL1 et D-POL2

- Pour résoudre les problèmes décisionnels on résout les problèmes d'extraction (cf. Coppersmith, Franklin, Patarin, Reiter, 1996)
- Étant donnés $P(a)$, $Q(b)$ et $R(a,b)$ on veut trouver a et b
- On calcule

$$S(X) = \operatorname{Res}_Y(R(X,Y) - R(a,b),\ Q(Y) - Q(b))$$

- $S(X)$ est un polynôme de degré $e_R e_Q$ avec $S(a) = 0$, donc

$$(X - a) \mid \operatorname{pgcd}(S(X), P(X) - P(a))$$

- En fait, on a très souvent égalité et on retrouve donc a
- Dans le cas E-POL1, on connaît ab, donc on retrouve b
- Pour le cas E-POL2, on peut retrouver b par le calcul de $\gcd(R(a,Y) - R(a,b), Q(Y) - Q(b))$

Les problèmes D-POL1 et D-POL2

- Le calcul du résultant peut se faire en $\mathcal{O}(e_R^2 e_Q \log^2(e_R e_Q) \log\log(e_R e_Q))$ opérations dans $\mathbf{Z}/n\mathbf{Z}$
- On a $e_R = 1$ pour E-POL1 et $e_R = \ell e_P$ pour E-POL2, donc même si e_P est petit, si ℓ est assez large cette méthode échouera
- Le calcul du premier pgcd peut être fait en $\mathcal{O}(e \log^2 e \log\log e)$ opérations dans $\mathbf{Z}/n\mathbf{Z}$, où $e = \max(e_R e_Q, e_P)$ et celui du second en $\mathcal{O}(e \log^2 e \log\log e)$ opérations avec $e = \max(e_R, e_Q)$

Les problèmes C-DPOL et D-DPOL

Théorème

$$\text{C-DPOL} \wedge \text{E-DPOL} \overset{\mathscr{P}}{\Longleftrightarrow} \text{P}^{-1} \overset{\mathscr{P}}{\Longrightarrow} \begin{matrix}\text{C-DPOL}\\ \text{E-DPOL}\end{matrix} \overset{\mathscr{P}}{\Longrightarrow} \text{D-DPOL}$$

- Pour le problème E-DPOL, on connaît $\text{P}(a)$ et $\text{Q}(a)$ et on veut calculer a
- On a
$$(\text{X} - a) \mid \text{pgcd}(\text{P}(\text{X}) - \text{P}(a), \text{Q}(\text{X}) - \text{Q}(a))$$
- Et encore, on a très souvent égalité et on retrouve donc a
- Calcul du pgcd en $\mathscr{O}(e \log^2 e \log\log e)$ opérations dans $\mathbf{Z}/n\mathbf{Z}$, avec $e = \max(e_\text{P}, e_\text{Q})$. Si e_P et e_Q sont supérieurs à 2^{60}, cette méthode échoue

Relations entre les trois classes de problèmes

- On peut également définir plusieurs réductions entre les trois classes de problèmes
- Et d'autres dans le cas particulier où les polynômes induisent des morphismes de $(\mathbf{Z}/n\mathbf{Z})^\times$

Plan

Cryptosystèmes IND-CPA

- Clef publique : $(n, \mathrm{P}, \mathrm{Q})$ ou $(n, \mathrm{P}, \mathrm{Q}, \mathrm{R})$
- Clef secrète : P^{-1} ou $(\mathrm{P}^{-1}, \mathrm{Q}^{-1})$
- Fonctions de chiffrement :
  - Fonction 1 : $(m, r_0, r_1) \mapsto \left(\mathrm{P}(r_0), \mathrm{Q}(r_1), m\mathrm{R}(r_0, r_1)\right)$
  - Fonction 2 : $(m, r) \mapsto \left(\mathrm{P}(mr), \mathrm{Q}(r^{-1})\right)$
- Déchiffrement : on utilise P^{-1} ou $(\mathrm{P}^{-1}, \mathrm{Q}^{-1})$ pour récupérer l'aléa et on en déduit m

Cryptosystèmes IND-CPA

Théorème

Les schémas sont OW-CPA et IND-CPA sûrs relativement aux problèmes suivants :

Fonction de chiffrement	OW	IND
$F_1, R(X,Y) = XY$	C-POL1(n,P,Q)	D-POL1(n,P,Q)
$F_1, R(X,Y) = P((XY)^\ell)$	C-POL2(n,ℓ,P,Q)	D-POL2(n,ℓ,P,Q)
F_2	C-POL1(n,P,Q)	D-POL1$(n,P,Q)^{(*)}$

$^{(*)}$ Si P ou Q est un morphisme

$$F_1 : (m, r_0, r_1) \mapsto \big(P(r_0), Q(r_1), mR(r_0, r_1)\big),$$
$$F_2 : (m, r) \mapsto \big(P(mr), Q(r^{-1})\big)$$

Efficacité

- On utilise pour P le polynôme issu de LUC et pour Q le polynôme RSA, paramétrés par le même exposant e
- On ajuste e et ℓ pour avoir une sécurité de 2^{80}

Schéma	Chiffré	Clef publique
Schéma 1	$V_e(r_0, 1), {r_1}^e, m r_0 r_1$	$e = 2^{67} + 3$
Schéma 2	$V_e(r_0, 1), {r_1}^e, m V_e\left((r_0 r_1)^\ell\right)$	$e = 5$ et $\ell = 2^{31} + 65$
Schéma 3	$V_e(m r, 1), r^{-e}$	$e = 2^{67} + 3$

Efficacité

- On compare l'efficacité de ces schémas avec le Dependent RSA de Pointcheval ($e = 2^{67} + 3$) et Catalano *et al.*($e = 2^{16} + 1$)
- L'unité est la multiplication modulo n

Schéma	D-RSA	Catalano	Schéma 1	Schéma 2	Schéma 3
Entrée	1024				
Sortie	2048		3072		2048
Chiffrement	139	52	205	**44**	214
Déchiffrement	567	570	1204	1228	1196

Cryptosystèmes IND-CCA2 dans le ROM

- On modifie la construction précédente pour avoir un niveau de sécurité IND-CCA2, dans le ROM
- Clef publique : $(n, \mathrm{P}, \mathrm{Q}, h)$ ou $(n, \mathrm{P}, \mathrm{Q}, \mathrm{R}, h)$ avec h une fonction de hachage vu comme un oracle aléatoire
- Clef secrète : P^{-1} ou $(\mathrm{P}^{-1}, \mathrm{Q}^{-1})$
- Fonctions de chiffrement :
  - Fonction 1 : $(m, r_0, r_1) \mapsto \left(\mathrm{P}(r_0), \mathrm{Q}(r_1), m\mathrm{R}(r_0, r_1), h(m \| r_0 \| r_1)\right)$
  - Fonction 2 : $(m, r) \mapsto \left(\mathrm{P}(mr), \mathrm{Q}(r^{-1}), h(m \| r)\right)$
- Déchiffrement : on utilise P^{-1} ou $(\mathrm{P}^{-1}, \mathrm{Q}^{-1})$ pour récupérer l'aléa et on en déduit m et on le retourne si le haché est correct

Cryptosystème IND-CCA1 dans le modèle standard

- *Knowledge of preimage assumption* (KPA) : Étant donnés P_1 et P_2 deux polynômes de permutation de $\mathbf{Z}/n\mathbf{Z}$, si un adversaire produit un couple (x, y) tel qu'il existe $a \in \mathbf{Z}/n\mathbf{Z}$ tel que $(x, y) = (P_1(a), P_2(a))$ alors il connaît a
- Nouveau système :
  - Clef publique : (n, P_1, P_2, Q) avec P_1, P_2 et Q des polynômes de permutation de $\mathbf{Z}/n\mathbf{Z}$
  - Clef secrète : P_1^{-1}
  - Fonction de chiffrement :

$$(m, r) \mapsto (P_1(r), P_2(r), mQ(r))$$

  - Déchiffrement : étant donné un chiffré (x, y, C), on vérifie que $P_2(P_1^{-1}(x)) = y$, si c'est le cas, on retourne $C/Q(P_1^{-1}(x))$, sinon on retourne $\perp$

Cryptosystème IND-CCA1 dans le modèle standard

- On montre que ce système est IND-CPA sous l'hypothèse que le problème D-DPOL(n, P_1, Q) est difficile
- De plus, le système est PA1 sous KPA
- Le système est donc IND-CCA1 sous ces deux hypothèses, dans le modèle standard
- En prenant $P_1(X) = X^e$, $P_2(X) = (X+1)^e$ and $Q(X) = (X+2)^e$ avec e de 60 bits, on obtient un système plus rapide que le Damgård's ElGamal, autre schéma prouvé sûr IND-CCA1 dans le modèle standard sous les hypothèses DDH et KEA (hypothèse qui a inspirée KPA !)

Plan

Conclusion

- Nouveaux problèmes algorithmiques, généralisant le problème RSA et étude de leurs difficultés
- Construction de nouveaux systèmes IND-CPA sûrs et IND-CCA2 sûrs dans le ROM
- Construction du système le plus rapide IND-CCA1 sûr dans le modèle standard