La Sécurité Sémantique en Pratique

David Pointcheval

CNRS / LIENS
École Normale Supérieure

David.Pointcheval@ens.fr

http ://www.dmi.ens.fr/~pointche

Plan

- Quelques Problèmes et les Chiffrements associés
  - Diffie-Hellman
  - Factorisation/RSA
  - Logarithme Discret
- Les "Dependent–RSA Problems"
  - Présentation
  - Relations avec RSA
  - Nouveau Schéma DRSA
- Attaques à Chiffrés Choisis
  - OAEP
  - DRSA-v2
- Comparaison

Problème : Diffie-Hellman [DH76]

- Calculatoire (C-DH) :
  Étant donnés $\alpha = g^x$ et $\beta = g^y$,
  Trouver $\gamma = g^{xy}$
- Décisionnel (D-DH) :
  Étant donnés $\alpha = g^x$, $\beta = g^y$ et $\gamma = g^z$
  Décider si $z = xy \bmod \mathrm{Ord}(g)$

La Sécurité Sémantique en Pratique

Chiffrement El Gamal [EG85]

Initialisation :
p grand premier, $g \in \mathbb{Z}_p^\star$ d'ordre élevé q Clés : $x \in \mathbb{Z}_q^\star$, $\alpha = g^x \bmod p$
Chiffrement : $m \to (\beta, B)$
$y \in_R \mathbb{Z}_q^\star$, $\beta = g^y \bmod p$, $\gamma = \alpha^y \bmod p$ $B = \gamma \times m \bmod p$
Déchiffrement : $(\beta, B) \to m$
$m = B/\beta^x \bmod p$

Sécurité

Sens-Unique (OW) :
$\mathcal{A}(\beta, B) \rightarrow m$ permet de résoudre C-DH : $\gamma = B/m$

Sécurité Sémantique (IND) :
Décider si (β, B) est un chiffré de m_0 ou de m_1
revient à décider si $\gamma = B/m_0$ est le DH(α, β)

À condition que $m_0 \in \langle g \rangle$! !

Donc IND-CPA $\Longrightarrow$ D-DH ssi $m \in \langle g \rangle$

De plus, D-DH facile si q pas premier !
Donc $p = 2q + 1$ et m un RQ(p)
$\Longrightarrow$ exponentiations coûteuses

Non-Malléabilité (NM) :
$B' = 2B \bmod p \Longrightarrow m' = 2m \bmod p.$

Problème : RSA [RSA78]

Étant donnés $N = pq$, e et $y \in \mathbb{Z}_N^\star$,
Trouver x tel que $x^e = y \bmod N$

Chiffrement RSA

Initialisation :
$N = pq$, $d = e^{-1} \bmod \phi(N)$
Chiffrement : $m \rightarrow y$
$y = m^e \bmod N$
Déchiffrement : $y \rightarrow m$
$m = y^d \bmod N$

Sécurité

Sens-Unique (OW) :
$\mathcal{A}(y) \rightarrow m$ permet de résoudre le problème RSA

Sécurité Sémantique (IND) :
En raison de l'aspect déterministe,
ce schéma ne peut pas être sémantiquement sûr

Non-Malléabilité (NM) :
Très facile à malléer :

$$y' = x^e y \bmod p \implies m' = xm \bmod N.$$

Problème : Logarithme Discret

Étant donnés $g \in G$ et $y \in \langle g \rangle$,
Trouver x tel que $y = g^x$

Malheureusement, ce problème est toujours "difficile" :
il n'admet pas de trappe, et ne peut donc pas être utilisé
pour du chiffrement asymétrique.

En revanche, des trappes permettent de retrouver
partiellement x en travaillant dans le groupe $G = \mathbb{Z}_N^\star$:
la factorisation de N.

Naccache-Stern '98

$\phi(N) = \sigma \times A$ avec σ lisse : $h = g^A \bmod N$,
$y^A = h^x \bmod N$ avec h d'ordre σ (lisse) :
Pohlig-Hellman $\Longrightarrow$ $x \bmod \sigma$

Okamoto-Uchiyama '98

$N = p^2 q \Longrightarrow \phi(N) = p(p-1)(q-1)$
$\mathcal{U}_p = \{y | y = 1 \bmod p\}$, $L_p(y) = \frac{y-1}{p} \bmod p$
Rq : $L_p(ab \bmod p^2) = L_p(a) + L_p(b) \bmod p$
$\Longrightarrow L_p(x^k \bmod p^2) = k \times L_p(x) \bmod p$.
Or, $\forall y$, $y^{p-1} \in \mathcal{U}_p$: $L_p(y^{p-1})/L_p(g^{p-1}) = x \bmod p$

Paillier '99

$N = n^2$ où $n = pq \Longrightarrow \phi(N) = n\phi(n)$ et $\lambda(N) = n\lambda(n)$
$\forall y$, $y^{\lambda(n)} \in \mathcal{U}_n$: $L_n(y^{\lambda(n)})/L_n(g^{\lambda(n)}) = x \bmod n$

Sécurité

Sens-Unique (OW) :
[NS98] : Résiduosité de Haut Degré
[OU98] : Factorisation de N
[Pa99] : Log Discret Partiel ou Classe de Résiduosité

Sécurité Sémantique (IND) :
Haute Résiduosité : $r | \phi(N)$, $\exists ? x$ tel que $y = x^r \bmod N$

Non-Malléabilité (NM) :
Tous très faciles à malléer

Avantages/Inconvénients

[NS98] : Bande passante très faible
σ sur 160 bits et N sur 768 bits
$\Longrightarrow$ expansion : $\times$ 5 !
Pas de problème bien défini quant à la OW.

[OU98] : Expansion plus faible : $\times$ 3,
Mais une attaque à 1 chiffré choisi fournit p !

[Pa99] : Expansion très faible : $\times$ 2,
Plus de cassage total (extraction de la clé secrète)
selon des attaques à chiffrés choisis
Mais sécurité fondée sur un nouveau problème

Les "Dependent–RSA Problems"

- Calculatoire (C-DRSA(N, e)) :
  Étant donné $\alpha = a^e \bmod N$,
  Trouver $\beta = (a+1)^e \bmod N$
- Décisionnel (D-DRSA(N, e)) :
  Étant donnés $\alpha = a^e \bmod N$ et $\beta = b^e \bmod N$,
  Décider si $b = a + 1 \bmod N$
- Extraction (E-DRSA(N, e)) :
  Étant donnés $\alpha = a^e \bmod N$ et $\beta = (a+1)^e \bmod N$,
  Trouver $a \bmod N$

Relations avec RSA

$\boxed{\text{C-DRSA} + \text{E-DRSA} \iff \text{RSA}}$

$$a^e \xrightarrow{C-DRSA} a^e, (a+1)^e \xrightarrow{E-DRSA} a$$

$\boxed{\text{C-DRSA, E-DRSA} \implies \text{D-DRSA}}$

$\boxed{\text{E-DRSA peut être résolu en } \mathcal{O}(e \log^2 e)}$ [CFPR96]

$\boxed{\text{Pour de petits exposants } e\text{, C-DRSA} \iff \text{RSA}}$

Schéma DRSA

Initialisation
$N = pq$ $d = e^{-1} \bmod \phi(N)$
Chiffrement : $m \to (\alpha, B)$
$k \in_R \mathbb{Z}_N^\star$ $\alpha = k^e \bmod N$, $\beta = (k+1)^e \bmod N$ $B = \beta \times m \bmod N$
Déchiffrement : $(\alpha, B) \to m$
$k = \alpha^d \bmod N$, $\beta = (k+1)^e \bmod N$ $m = B/\beta \bmod N$

Sécurité

Sens-Unique (OW) :
$\mathcal{A}(\alpha, B) \rightarrow m$ permet de résoudre C-DRSA :
$\beta = (k+1)^e = B/m \bmod N$

Sécurité Sémantique (IND) :
Décider si (α, B) est un chiffré de m_0 ou de m_1
revient à décider si $\beta = B/m_0$ est le DRSA(α)
Donc IND-CPA $\Longrightarrow$ D-DRSA

Non-Malléabilité (NM) :
Très facile à malléer : $B' = xB \bmod N \implies m' = xm \bmod N$.

À cause de D-DRSA, on doit utiliser un grand exposant e.

Récapitulatif

	RSA 78	EG 85	NS 98	OU 98	Pa 99	DRSA
OW-CPA	RSA	DH	HR	Fact	LDP	C-DRSA
IND-CPA	–	DDH	HR	HR	HR	D-DRSA

	OAEP 94	CS 98
OW-CPA	RSA	DH
IND-CPA	RSA	DDH
IND-CCA	RSA	DDH

- [CS 98] est le seul à être IND-CCA dans le modèle standard
  extension de [EG 85] relativement pratique,
  mais pas suffisamment efficace : 4 exp. modulaires
- OAEP [BR94], padding appliqué à RSA,
  est le plus efficace connu à ce jour (coût d'un RSA),
  mais défini dans le modèle de l'oracle aléatoire.

OAEP [BR94]

Initialisation
$N = pq$, $d = e^{-1} \bmod \phi(N)$ g,h, fonctions de hachage
Chiffrement : $m \rightarrow c$
$r \in_R \{0,1\}^{k_0}$, $M = m\|0^{k_1}$ $A = g(r) \oplus M$, $B = h(A) \oplus r$ $c = (A\|B)^e \bmod N$
Déchiffrement : $c \rightarrow m$
$A\|B = c^d \bmod N$ $r = B \oplus h(A)$ $M = A \oplus g(r)$ Si $M = x\|0^{k_1}$ alors $m = x$

Sécurité : CCA

La forme $M = m\|0^{k_1}$ garantit que
celui qui a produit le chiffré connaît le clair.

En effet, si le chiffré n'a pas été produit correctement
(en posant les questions $g(r)$ et $h(A)$),
M a très peu de chance d'être valide.
$\Longrightarrow$ un chiffré valide doit faire apparaître le couple (r, A)
dans les listes des questions posées à g, h.

Pour simuler l'oracle de déchiffrement,

il suffit de regarder tous les $(r, G = g(r))$ et $(A, H = h(A))$

- si en posant $B = H \oplus r$, $c = (A\|B)^e \bmod N$,
  $\Longrightarrow$ alors $M = A \oplus G$, etc.
- sinon, on refuse le chiffré

Sécurité : RSA

Si la question $g(r)$ n'a pas été posée,
il est impossible d'avoir la moindre information sur M.

Sans $h(A)$, aucune information sur r.

$\Longrightarrow$ A dans la liste des questions posées à h
et r dans la liste des questions posées à g
et alors $B = h(A) \oplus r$.

Il suffit d'essayer toutes ces paires (A, B) possibles
$\Longrightarrow$ $x = A \| B$ vérifie $x^e = c \bmod N$.

OAEP : IND-CCA = RSA

$\Longrightarrow$ nouveau standard RSA PKCS #1 v2.0
adopté par SET, etc

DRSA v2

Initialisation
$N = pq$, $d = e^{-1} \bmod \phi(N)$ g,h, fonctions de hachage
Chiffrement : $m \rightarrow (\alpha, B, H)$
$k \in_R \mathbb{Z}_N^\star$ $\alpha = k^e \bmod N$, $\beta = (k+1)^e \bmod N$ $B = g(\beta) \oplus m$ $H = h(m, k)$
Déchiffrement : $(\alpha, B, H) \rightarrow m$
$k = \alpha^d \bmod N$, $\beta = (k+1)^e \bmod N$ $m = B \oplus g(\beta)$ $H \stackrel{?}{=} h(m, k)$

Sécurité : CCA

L'oracle aléatoire h produit un "tag"
dont la vérification garantit que
celui qui a produit le chiffré connaît le clair.

En effet, un H non obtenu à partir de h
a très peu de chance d'être valide.

$\Longrightarrow$ un chiffré valide doit faire apparaître le couple (m, k)
dans la liste des questions posées à h.

Pour simuler l'oracle de déchiffrement,

il suffit de regarder dans la liste des questions posées à h :
- si un couple (m, k) mène à (α, B), m est le clair
- sinon, on refuse le chiffré

La Sécurité Sémantique en Pratique

Sécurité : C-DRSA

L'oracle aléatoire g masque β.
$\Longrightarrow$ Sans poser directement la question β à g,
nul ne peut apprendre même un bit d'information sur m

$\Longrightarrow$ β se trouve dans le liste des questions posées à g.

Comment le trouver en raison de la difficulté de D-DRSA ?

Puisque la sécurité repose sur C-DRSA,
on peut prendre un petit exposant e
$\Longrightarrow$ E-DRSA est facile (et donc D-DRSA).

Du même coup, C-DRSA = RSA

$$\boxed{\text{IND-CCA} \iff \text{RSA}}$$

Efficacité

Schémas	**El Gamal** 512	**OAEP** 1024	**DRSA** 1024	**DRSA v2** 1024
Sécurité				
OW-CPA	DH	RSA	C-DRSA	RSA
IND-CPA	DDH	RSA	D-DRSA	RSA
IND-CCA	–	RSA	–	RSA
Taille (en bits)				
Clair	511	448	1024	1024
Chiffré	1024	1024	2048	2208
Expansion	2	2.3	2	2.2
Chiffrement				
Coût/kO	6144	311	1112	280
Déchiffrement				
Coût/kO	3072	7022	4184	3352