Présentation des protocoles RSAES-OAEP et RSASSA-PSS

M2 MIC - Cryptographie asymétrique

Jérémie Nekam et Daniel Resende

université PARIS DIDEROT PARIS 7

Mardi 24 octobre 2017

Sommaire

Sommaire

Sommaire

Sommaire

Sommaire

Introduction

Deux protocoles pour deux utilisations différentes :

Introduction

Deux protocoles pour deux utilisations différentes :

RSAES-OAEP Protocole de chiffrement/déchiffrement

Introduction

Deux protocoles pour deux utilisations différentes :

RSAES-OAEP Protocole de chiffrement/déchiffrement

RSASSA-PSS Protocole de signature

Sommaire

Le protocole RSAES-OAEP se décompose en deux parties :

- EM-OAEP
- RSAEP (resp. RSADP) pour le chiffrement (resp. déchiffrement)

Pourquoi utiliser OAEP ?

D. Bleichembacher a trouvé une attaque CCA-2 sur le protocole suivant :

Definition (PKCS 1 v1)

Soit M le message à chiffrer. On note $EB = 00 \parallel 02 \parallel Padding \parallel 00 \parallel M$

Le schéma OAEP standard

Algorithme 1 Schéma OAEP

Require: Un message m, un aléa r et deux oracles G et H.
Ensure: Un message m' tel que $m' = s \parallel t$.

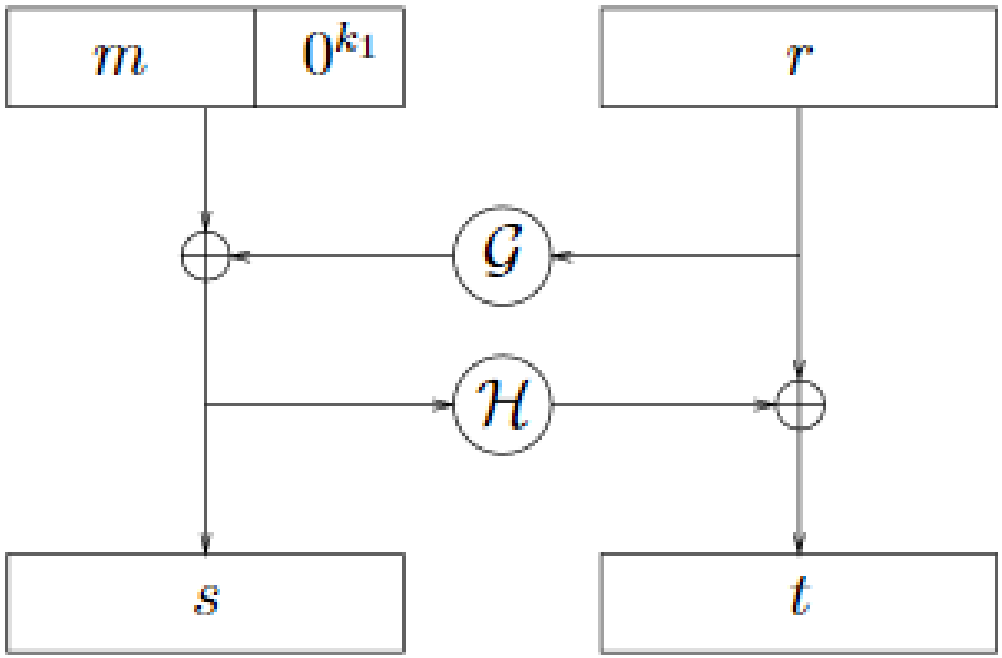

Figure – OAEP

Génération des clés RAES-OAEP

Clés publiques

On garde les mêmes clés (n, e) avec les mêmes propriétés que le RSA classique.

Clés privées

- soit (p, q, d) tel que $e \cdot d = 1 \ mod \ (ppcm(p-1, q-1))$,
- soit $(p, q, dP, dQ, qInv)$ où $q \cdot qInv = 1 \ mod \ p$, $e \cdot dP = 1 \ mod \ q$ et $e \cdot dP = 1 \ mod \ q$.

Le schéma EM-OAEP

Algorithme 2 Schéma EM-OAEP

Require: Un message m, un aléa $seed$ et $Hash$ des données spécifiant la fonction de hachage à utiliser

Ensure: Un message EM.

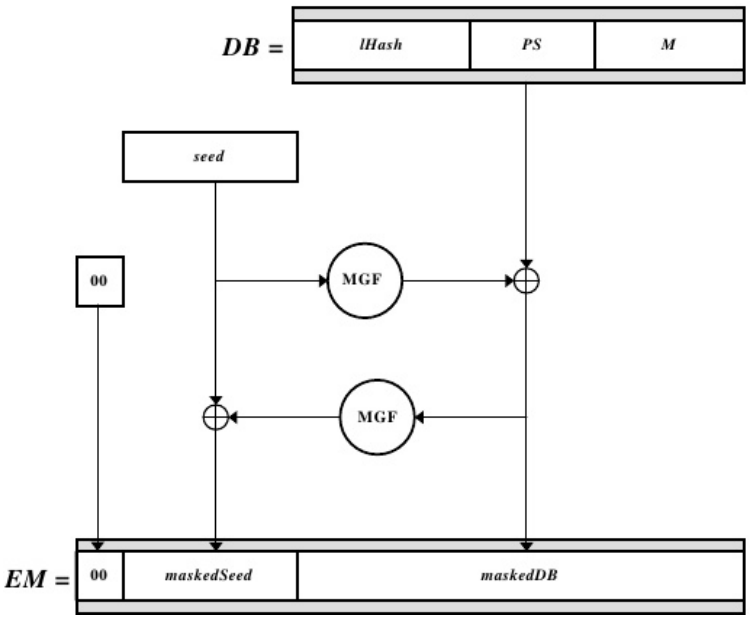

Figure – EM-OAEP

Chiffrement/déchiffrement de RAES-OAEP

RSAEP - Chiffrement

On garde les mêmes paramètres et propriétés que le RSA classique.

Algorithme 3 RSADP - Déchiffrement

Require: Un message chiffré c et une clé privé $K = (n, p, q, d)$ ou $(p, q, dP, dQ, qInv)$.

Ensure: Un message clair m

if c n'est pas une entrée valide **then**

return ERREUR

end if

if $K = (n, p, q, d)$ **then**

return $m = c^d \ mod \ n$

end if

$m_1 = c^{dP} \ mod \ p$

$m_2 = c^{dQ} \ mod \ q$

$h = (m_1 - m_2) \cdot qInv \ modp$

return $m = m_2 + q \cdot h$

Sécurité du protocole

Definition (Sécurité sémantique)

Soit m_0, m_1 deux messages choisies par l'attaquant. Soit c un challenge qui est le chiffré de m_0 ou m_1. On dit qu'un protocole est sémantiquement sûr si l'attaquant ne peut pas distinguer m_0 ou m_1.

Attaque de Shoup

Proposition

Le protocole f-OAEP n'est pas totalement sémantiquement sûr.

Idées de preuve pour l'attaque de Shoup

Definition (Xor-malléable)

Soit f une permutation à sens unique avec trappe. On dit que f est xor-malléable, si on a une probabilité non-négligeable de pouvoir calculer $f(t \oplus a)$ en connaissant $f(t)$ et a.

Soient c un chalenge, H un oracle aléatoire et f telle que $f(s \parallel t) = s \parallel f(t)$ une fonction xor-maléable.

1. On pose $c = f(s \parallel t) = s \parallel f(t)$.
2. On choisi aléatoirement s' et on calcul $a = H(s) \oplus H(s')$

Sommaire

Sommaire

OAEP Il est préférable de plus utiliser OAEP, et plutôt REACT.

PSS

Bibliographie