

Présentation des protocoles RSAES-OAEP et RSASSA-PSS

M2 MIC - Cryptographie asymétrique

Jérémie Nekam et Daniel Resende



Mardi 24 octobre 2017

- 1 Introduction
 - OAEP

1 Introduction

- OAEP

2 RSAES-OAEP

- Génération des clés RAES-OAEP
- Utilisation d'OAEP avec RSA
- Chiffrement/déchiffrement de RAES-OAEP
- Sécurité du protocole

1 Introduction

- OAEP

2 RSAES-OAEP

- Génération des clés RAES-OAEP
- Utilisation d'OAEP avec RSA
- Chiffrement/déchiffrement de RAES-OAEP
- Sécurité du protocole

3 RSASSA-PSS

- PSS
- Utilisation de PSS avec RSA
- Sécurité du protocole

1 Introduction

- OAEP

2 RSAES-OAEP

- Génération des clés RAES-OAEP
- Utilisation d'OAEP avec RSA
- Chiffrement/déchiffrement de RAES-OAEP
- Sécurité du protocole

3 RSASSA-PSS

- PSS
- Utilisation de PSS avec RSA
- Sécurité du protocole

4 Conclusion/Recommandation

1 Introduction

- OAEP

2 RSAES-OAEP

3 RSASSA-PSS

4 Conclusion/Recommandation

Deux protocoles pour deux utilisations différentes :

Deux protocoles pour deux utilisations différentes :

RSAES-OAEP Protocole de chiffrement/déchiffrement

Deux protocoles pour deux utilisations différentes :

RSAES-OAEP Protocole de chiffrement/déchiffrement

RSASSA-PSS Protocole de signature

Pourquoi utiliser OAEP ?

D. Bleichenbacher a trouvé une [attaque CCA-2](#) sur le protocole suivant :

Pourquoi utiliser OAEP ?

D. Bleichenbacher a trouvé une [attaque CCA-2](#) sur le protocole suivant :

Definition (PKCS 1 v1)

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

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 $m' = s \parallel t$.

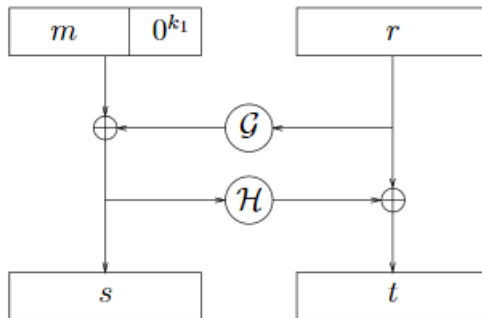


Figure – OAEP

1 Introduction

2 RSAES-OAEP

- Génération des clés RAES-OAEP
- Utilisation d'OAEP avec RSA
- Chiffrement/déchiffrement de RAES-OAEP
- Sécurité du protocole

3 RSASSA-PSS

4 Conclusion/Recommandation

Protocole RSAES-OAEP Le protocole RSAES-OAEP se décompose en trois parties :

Protocole RSAES-OAEP Le protocole RSAES-OAEP se décompose en trois parties :

- La génération des clés,

Protocole RSAES-OAEP Le protocole RSAES-OAEP se décompose en trois parties :

- La génération des clés,
- Le schéma EM-OAEP,

Protocole RSAES-OAEP Le protocole RSAES-OAEP se décompose en trois parties :

- La génération des clés,
- Le schéma EM-OAEP,
- La primitive RSAEP (resp. RSADP) pour le chiffrement (resp. déchiffrement).

Clés publiques

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

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 $e \cdot d = 1 \bmod (\text{ppcm}(p - 1, q - 1))$,

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 $e \cdot d = 1 \bmod (\text{ppcm}(p-1, q-1))$,
- soit $(p, q, dP, dQ, qInv)$ où $q \cdot qInv = 1 \bmod p$, $e \cdot dP = 1 \bmod q$ et $e \cdot dQ = 1 \bmod p$.

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 .

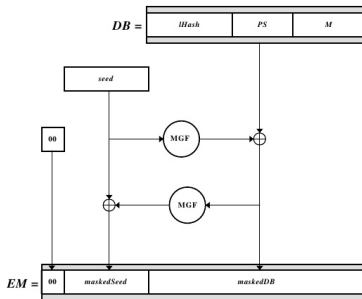


Figure – EM-OAEP

RSAEP - Chiffrement

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

RSAEP - Chiffrement

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

Algorithme 4 RSADP - Déchiffrement

Require: Un message chiffré c et une clé privée $K = (n, p, q, d)$ 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 $m = c^d \bmod n$

end if

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

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

$h = (m_1 - m_2) \cdot qInv \bmod p$

return $m = m_2 + q \cdot h$

Définition (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 .

Proposition

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

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 .

Idées de preuve pour l'attaque de Shoup [Sho01]

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 .

Théorème

S'il existe un schéma xor-malléable alors il existe une permutation à sens-unique avec trappe qui tel que lorsqu'on utilise OEAP le schéma de chiffrement qui en résulte n'est pas sûr dans un modèle d'oracle aléatoire.

Soit f_0 xor-malléable sur k_0 bits. Soit un A algorithme qui calcule $f_0(t \oplus \delta)$ à partir de $(f_0, f_0(t), \delta)$.

Soit f telle que $f(s \parallel t) = s \parallel f(t)$ une permutation à sens-unique avec trappe où $s \in \{0, 1\}^{n+k_1}$ et $t \in \{0, 1\}^{k_0}$.

On pose que le schéma OAEP utilise f .

L'attaquant reçoit le challenge y' , il peut l'écrire tel que $y' = s' \parallel f_0(t')$.

L'attaquant choisi un message arbitraire différent de zéro Δ tel que :

$$s = s' \oplus (\delta \parallel 0^{k_1})$$

$$v = A(f_0, f_0(t'), H(s) \oplus H(s'))$$

$$y = s \parallel v$$

Si y est un chiffrement valide de $x = x' \oplus (\delta 0^{k_1})$ et $v = f_0(t' \oplus H(s) \oplus H(s'))$.

$$t = t' \oplus H(s') \oplus H(s)$$

$$\begin{aligned} r &= H(s) \oplus t \\ &= H(s') \oplus t' \\ &= r' \end{aligned}$$

$$\begin{aligned} z &= G(r) \oplus s \\ &= G(r) \oplus s' \oplus (\delta 0^{k_1}) \\ &= (x' \oplus \delta) \parallel 0^{k_1} \end{aligned}$$

Si l'attaquant déchiffre y à l'aide d'un oracle aléatoire, alors il a x . Et peut donc calculer x' .

Idées de preuve pour l'attaque de Shoup [Sho01]

Théorème

Il existe un oracle aléatoire tel que une permutation à sens-unique avec trappe existe.

La deux théorèmes précédents nous donnent le corollaire suivant :

Corollaire

Il existe un oracle aléatoire tel que la construction d'OAEP n'est pas sûr.

Proposition ([FOPS00])

- 1 *Le problème d'inverser partiellement la fonction RSA se réduit au problème de sécurité de RSA-OAEP en complexité (en temps) quadratique.*

Proposition ([FOPS00])

- 1 *Le problème d'inverser partiellement la fonction RSA se réduit au problème de sécurité de RSA-OAEP en complexité (en temps) quadratique.*
- 2 *Le problème d'inverser complètement la fonction RSA se réduit au problème d'inverser partiellement la fonction RSA en complexité (en temps) quadratique.*

Proposition ([FOPS00])

- 1 *Le problème d'inverser partiellement la fonction RSA se réduit au problème de sécurité de RSA-OAEP en complexité (en temps) quadratique.*
- 2 *Le problème d'inverser complètement la fonction RSA se réduit au problème d'inverser partiellement la fonction RSA en complexité (en temps) quadratique.*

Exemple

Pour une clés de 1024 bits, la complexité de la réduction est de 2^{40} .

- 1 Introduction
- 2 RSAES-OAEP
- 3 RSASSA-PSS**
 - PSS
 - Utilisation de PSS avec RSA
 - Sécurité du protocole
- 4 Conclusion/Recommandation

- 1 Introduction
- 2 RSAES-OAEP
- 3 RSASSA-PSS
- 4 Conclusion/Recommandation**

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

Bibliographie



Hieu Phan Duong.



Eiichiro Fujisak, Tatsuaki Okamoto, David Pointcheval, and Jacques Stern.
Rsa-oaep is secure under the rsa assumption.
2000.



RSA Laboratory.
Pkcs 1 v2.2 : Rsa cryptography standard.
2000.



RSA Laboratory.
Rsaes-oaep encryption scheme.
2000.



Victor Shoup.
Oaep reconsidered.
2001.