

Les canaux subliminaux dans DSA

Marin HANNACHE

Résidus

Mise en gage

Les canaux subliminaux dans DSA LSE lightning talk

Marin HANNACHE

10 avril 2018







Plan

Les canaux subliminaux dans DSA

Marin HANNACHE

Introduction

Caractéristiques Le logarithme discre Signer un message

Canaux

subliminaux

Canal « haut débit »
Canaux « bas débit »
Résidus
quadratiques

Contremesures Mise en gage Limites

Conclusion

1 Introduction rapide à DSA

- Caractéristiques de DSA
- Le problème du logarithme discret
- Signer un message avec DSA
- Remarques sur DSA

2 Canaux subliminaux

- Définition
- Le canal subliminal « haut débit » de DSA
- Les canaux subliminaux « bas débit » de DSA
 - La méthode des résidus quadratiques
 - Les autres méthodes

3 Contre-mesures

- Mise en gage (commitment scheme)
- Limites des contre-mesures



Plan

Les canaux subliminaux dans DSA

Marin HANNACHE

Introductio

DOA

Caractéristiques

Signer un messag

Remarques

cuhlimina

Sublimina

Canal « haut débit

Résidus quadratique Les autres

Contre-

Mise en gage Limites

Conclusion

1 Introduction rapide à DSA

- Caractéristiques de DSA
- Le problème du logarithme discret
- Signer un message avec DSA
- Remarques sur DSA
- 2 Canaux subliminaux
 - Définition
 - Le canal subliminal « haut débit » de DSA
 - Les canaux subliminaux « bas débit » de DSA
 - La méthode des résidus quadratiques
 - Les autres méthodes
- 3 Contre-mesures
 - Mise en gage (commitment scheme)
 - Limites des contre-mesures



Caractéristiques de DSA

Les canaux subliminaux dans DSA

Marin HANNACHE

Introduction

.....

Caractéristiques

Signer un message

Canaux

Définition

Canaux « bas débit »
Résidus

quadratiques Les autres

Contre-

Mise en gage

- DSA¹ est un algorithme de signature numérique conçu par David W. KRAVITZ en 1991, alors employé par la NSA. C'est un algorithme de cryptographie asymétrique.
- Il est inspiré d'un autre algorithme de signature mis au point par Taher ELGAMAL en 1984.
- DSA est basé sur le problème du logarithme discret.



Caractéristiques de DSA

Les canaux subliminaux dans DSA

Marin HANNACHE

Introduction

Caractéristiques

Le logarithme discr Signer un message

Canaux subliminaux

Définition Canal « haut débit » Canaux « bas débit »

Résidus quadratiques Les autres méthodes

Contre-

Mise en gage

- DSA¹ est un algorithme de signature numérique conçu par David W. KRAVITZ en 1991, alors employé par la NSA. C'est un algorithme de cryptographie asymétrique.
- Il est inspiré d'un autre algorithme de signature mis au point par Taher ELGAMAL en 1984.
- DSA est basé sur le problème du logarithme discret.



Caractéristiques de DSA

Les canaux subliminaux dans DSA

Marin HANNACHE

Caractéristiques

Mise en gage

- DSA¹ est un algorithme de signature numérique conçu par David W. Kravitz en 1991, alors employé par la NSA. C'est un algorithme de cryptographie asymétrique.
- Il est inspiré d'un autre algorithme de signature mis au point par Taher ELGAMAL en 1984.
- DSA est basé sur le problème du logarithme discret.



Plan

Les canaux subliminaux dans DSA

Marin HANNACHE

Introduction

Caractéristiques

Le logarithme discret Signer un message

Remarques

canaux

Définition

Canal « haut débit »
Canaux « bas débit
Résidus

quadratiques Les autres méthodes

Contremesure

Mise en gage Limites

Conclusion

1 Introduction rapide à DSA

- Caractéristiques de DSA
- Le problème du logarithme discret
- Signer un message avec DSA
- Remarques sur DSA
- 2 Canaux subliminaux
 - Définition
 - Le canal subliminal « haut débit » de DSA
 - Les canaux subliminaux « bas débit » de DSA
 - La méthode des résidus quadratiques
 - Les autres méthodes
- 3 Contre-mesures
 - Mise en gage (commitment scheme)
 - Limites des contre-mesures



Le problème du logarithme discret

Les canaux subliminaux dans DSA

Marin HANNACHE

Le logarithme discret

Mise en gage

Il est très simple de calculer une exponentiation modulaire grâce à une variante de l'exponentiation rapide :

Exponentiation modulaire

$$\mathbf{x} = 9$$

$$x = 35$$



Le problème du logarithme discret

Les canaux subliminaux dans DSA

Marin HANNACHE

Le logarithme discret

Mise en gage

Il est très simple de calculer une exponentiation modulaire grâce à une variante de l'exponentiation rapide :

Exponentiation modulaire

- $x \equiv 2^{35} \pmod{11}$
- x = 9

On ne connaît cependant pas de méthode pour effectuer l'opération inverse en temps polynomial :

Logarithme discret

- \blacksquare 9 \equiv 2^x (mod 11)
- x = 35



Plan

Les canaux subliminaux dans DSA

Marin HANNACHE

Introductio

.

O------

Le logarithme dis

Signer un message

Remarqu

canaux sublimin:

Définition

Canal « haut débit : Canaux « bas débit

quadratique Les autres

Contre-

Mise en gage Limites

Conclusion

1 Introduction rapide à DSA

- Caractéristiques de DSA
- Le problème du logarithme discret
- Signer un message avec DSA
- Remarques sur DSA
- 2 Canaux subliminaux
 - Définition
 - Le canal subliminal « haut débit » de DSA
 - Les canaux subliminaux « bas débit » de DSA
 - La méthode des résidus quadratiques
 - Les autres méthodes
- 3 Contre-mesures
 - Mise en gage (commitment scheme)
 - Limites des contre-mesures



Les canaux subliminaux dans DSA

Marin HANNACHE

Introductio

.

Caractéristiques

Signer un message

Remarques

Canaux

subliminau

Canal « haut débit

Canaux « bas débit Résidus quadratiques

Contre-

Mise en gage Limites

Conclusion

- 1 Une fonction de hachage cryptographique H
- 2 Deux nombres premiers p et q tels que $(p-1) \mid q$
- In nombre g dont l'ordre multiplicatif modulo p est q
- Génération d'une paire de clés :
 - 1 Choisir un nombre x tel que 1 < x < q
 - 2 Calculer $y = g^x \mod p$
 - 3 y est la clé publique, x la clé privée.
- Signer un message *m* :
 - 1 On choisit un nombre aléatoire k tel que 1 < k < q.
 - 2 On calcule $r = (g^k \mod p) \mod q$.
 - On calcule $s = k^{-1} (H(m) + rx) \mod q$.
 - 4 La signature est (r, s)



Les canaux subliminaux dans DSA

Marin HANNACHE

Introductio

. . .

Caractéristiques Le logarithme dis

Signer un message Remarques

subliminau

Définition

Canal « haut débit » Canaux « bas débit

Les autres

Contremesures

Mise en gage Limites

Conclusion

- 1 Une fonction de hachage cryptographique H
- 2 Deux nombres premiers p et q tels que $(p-1) \mid q$
- In nombre g dont l'ordre multiplicatif modulo p est q
- Génération d'une paire de clés :
 - 1 Choisir un nombre x tel que 1 < x < q
 - 2 Calculer $y = g^x \mod p$
 - 3 y est la clé publique, x la clé privée.
- Signer un message *m* :
 - On choisit un nombre aléatoire k tel que 1 < k < q.
 - 2 On calcule $r = (g^k \mod p) \mod q$.
 - 3 On calcule $s = k^{-1} (H(m) + rx) \mod q$.
 - 4 La signature est (r, s).



Les canaux subliminaux dans DSA

Marin HANNACHE

Introductio

Caractéristiques
Le logarithme discre
Signer un message

Signer un messag Remarques

subliminau

Canal « haut débit » Canaux « bas débit »

quadratiques
Les autres
méthodes

Contremesures

Mise en gage Limites

Conclusion

- 1 Une fonction de hachage cryptographique H
- 2 Deux nombres premiers p et q tels que $(p-1) \mid q$
- In nombre g dont l'ordre multiplicatif modulo p est q
- Génération d'une paire de clés :
 - 1 Choisir un nombre x tel que 1 < x < q
 - 2 Calculer $y = g^x \mod p$
 - 3 y est la clé publique, x la clé privée.
- Signer un message *m* :
 - 1 On choisit un nombre aléatoire k tel que 1 < k < q.
 - On calcule $r = (g^{\kappa} \mod p) \mod q$.
 - 3 On calcule $s = k^{-1} (H(m) + rx) \mod q$.
 - 4 La signature est (r, s)



Les canaux subliminaux dans DSA

Marin HANNACHE

Signer un message

Mise en gage

- Une fonction de hachage cryptographique H
- 2 Deux nombres premiers p et q tels que $(p-1) \mid q$
- 3 Un nombre g dont l'ordre multiplicatif modulo p est g
- Génération d'une paire de clés :
 - 1 Choisir un nombre x tel que 1 < x < q
 - 2 Calculer $v = q^x \mod p$
 - 3 y est la clé publique, x la clé privée.
- Signer un message m :
 - 1 On choisit un nombre aléatoire k tel que 1 < k < q.
 - 2 On calcule $r = (g^k \mod p) \mod q$.
 - On calcule $s = k^{-1} (H(m) + rx) \mod q$.



Les canaux subliminaux dans DSA

Marin HANNACHE

Introductio

Caractéristiques Le logarithme discre Signer un message

Remarques

Subliminau:
Définition

Canal « haut débit »
Canaux « bas débit s
Résidus

quadratiques Les autres méthodes

mesures
Mise en gage
Limites

Conclusion

- 1 Une fonction de hachage cryptographique H
- 2 Deux nombres premiers p et q tels que $(p-1) \mid q$
- In nombre g dont l'ordre multiplicatif modulo p est q
- Génération d'une paire de clés :
 - 1 Choisir un nombre x tel que 1 < x < q
 - 2 Calculer $y = g^x \mod p$
 - 3 y est la clé publique, x la clé privée.
- Signer un message *m* :
 - 1 On choisit un nombre aléatoire k tel que 1 < k < q.
 - 2 On calcule $r = (g^k \mod p) \mod q$.
 - 3 On calcule $s = k^{-1} (H(m) + rx) \mod q$.
 - 4 La signature est (r, s)



Les canaux subliminaux dans DSA

Marin HANNACHE

Introductio

Caractéristiques Le logarithme dis

Signer un message Remarques

subliminau

Canal « haut débit »
Canaux « bas débit

quadratiques
Les autres
méthodes

Contremesures

Mise en gage Limites

Conclusion

- Une fonction de hachage cryptographique H
- **2** Deux nombres premiers p et q tels que $(p-1) \mid q$
- In nombre g dont l'ordre multiplicatif modulo p est q
- Génération d'une paire de clés :
 - 1 Choisir un nombre x tel que 1 < x < q
 - 2 Calculer $y = g^x \mod p$
 - 3 y est la clé publique, x la clé privée.
- Signer un message *m* :
 - 1 On choisit un nombre aléatoire k tel que 1 < k < q.
 - 2 On calcule $r = (g^k \mod p) \mod q$.
 - 3 On calcule $s = k^{-1} (H(m) + rx) \mod q$.
 - 4 La signature est (r, s).



Plan

Les canaux subliminaux dans DSA

Marin HANNACHE

Introductio

....

Caractéristiques Le logarithme discr

Remarques

Canaux

sublimina

Canal « haut débi

Canaux « bas débi Résidus

Les autres méthodes

Contremesure:

Mise en gage Limites

Conclusion

1 Introduction rapide à DSA

- Caractéristiques de DSA
- Le problème du logarithme discret
- Signer un message avec DSA
- Remarques sur DSA
- 2 Canaux subliminaux
 - Définition
 - Le canal subliminal « haut débit » de DSA
 - Les canaux subliminaux « bas débit » de DSA
 - La méthode des résidus quadratiques
 - Les autres méthodes
- 3 Contre-mesures
 - Mise en gage (commitment scheme)
 - Limites des contre-mesures



Les canaux subliminaux dans DSA

Marin HANNACHE

Remarques

Mise en gage

La dépendance au problème du logarithme discret est immédiate : en sachant le résoudre on peut retrouver la clé privée à partir de la clé publique.

Le paramètre aléatoire k possède des propriétés

■ La connaissance de *k* permet de retrouver la clé privée

- $x = r^{-1}(sk H(m)) \mod q$



Les canaux subliminaux dans DSA

Marin HANNACHE

Introductio

Caractéristiques
Le logarithme discr

Remarques

Canaux

Définition

Canaux « bas débi

quadratiqu Les autres

Contre-

Mise en gage Limites

Conclusion

■ La dépendance au problème du logarithme discret est immédiate : en sachant le résoudre on peut retrouver la clé privée à partir de la clé publique.

- Le paramètre aléatoire k possède des propriétés intéressantes :
 - La connaissance de *k* permet de retrouver la clé privée à partir d'une signature.

- $\blacksquare Rappel: r = (g^k \mod p) \mod q$
- Rappel: $s = k^{-1} (H(m) + rx) \mod q$
- $x = r^{-1} (sk H(m)) \mod q$



Les canaux subliminaux dans DSA

Marin HANNACHE

Introductio

Caractéristiques
Le logarithme discre

Signer un messag Remarques

Canaux

subliminaux

Canal « haut débit

Canaux « bas débit Résidus

Les autres méthodes

Contremesures

Mise en gage Limites

Conclusion

- La dépendance au problème du logarithme discret est immédiate : en sachant le résoudre on peut retrouver la clé privée à partir de la clé publique.
- Le paramètre aléatoire k possède des propriétés intéressantes :
 - La connaissance de *k* permet de retrouver la clé privée à partir d'une signature.

- $\blacksquare Rappel: r = (g^k \mod p) \mod q$
- $\blacksquare Rappel: s = k^{-1} (H(m) + rx) \mod q$
- $x = r^{-1} (sk H(m)) \mod q$



Les canaux subliminaux dans DSA

Marin HANNACHE

Introductio

Caractéristiques
Le logarithme disci

Remarques

subliminaux

Canal « haut débit Canaux « bas débi

Résidus quadratiques Les autres

Contremesures

Mise en gage Limites

Conclusion

- La dépendance au problème du logarithme discret est immédiate : en sachant le résoudre on peut retrouver la clé privée à partir de la clé publique.
- Le paramètre aléatoire k possède des propriétés intéressantes :
 - La connaissance de k permet de retrouver la clé privée à partir d'une signature.

- $\blacksquare Rappel: r = (g^k \mod p) \mod q$
- Rappel: $s = k^{-1} (H(m) + rx) \mod q$



Les canaux subliminaux dans DSA

Marin HANNACHE

Introductio

Caractéristiques
Le logarithme discre

Signer un messag Remarques

∪anaux subliminaux

Bubliminaux

Canal « haut débit Canaux « bas débi

Résidus quadratiques Les autres

Contremesures

Mise en gage Limites

Conclusion

- La dépendance au problème du logarithme discret est immédiate : en sachant le résoudre on peut retrouver la clé privée à partir de la clé publique.
- Le paramètre aléatoire k possède des propriétés intéressantes :
 - La connaissance de *k* permet de retrouver la clé privée à partir d'une signature.

- $\blacksquare Rappel: r = (g^k \mod p) \mod q$
- $\blacksquare Rappel: s = k^{-1} (H(m) + rx) \mod q$
- $x = r^{-1} (sk H(m)) \mod q$



Les canaux subliminaux dans DSA

Marin HANNACHE

Introduction

....

Caractéristiques Le logarithme disc

Signer un messag
Remarques

rioma

Canaux

Sublimina

Canal « haut débi

Canaux « bas d

quadratiqu Les autres

Contre-

Mise en gage Limites

Conclusion

■ Le paramètre aléatoire *k* possède des propriétés intéressantes (suite) :

La réutilisation du même k pour signer deux messages distincts permet de le dériver des signatures et donc de retrouver la clé privée.

```
\blacksquare Rappel: r = (g^k \mod p) \mod q
```

■ Rappel:
$$s_1 = k^{-1} (H(m_1) + rx) \mod q$$

■ Rappel:
$$s_2 = k^{-1} (H(m_2) + rx) \mod q$$

$$= k = (H(m_1) - H(m_2))(s_1 - s_2)^{-1} \mod q$$



Les canaux subliminaux dans DSA

Marin HANNACHE

Introductio

marodaotio

Caractéristiques Le logarithme disc

Signer un messagi Remarques

Canau

Sublimina

Canal « haut

Canaux « bas débi

Résidus quadratique

Les autres

Contre-

Mise en gage Limites

Conclusion

■ Le paramètre aléatoire *k* possède des propriétés intéressantes (suite) :

La réutilisation du même k pour signer deux messages distincts permet de le dériver des signatures et donc de retrouver la clé privée.

- $\blacksquare Rappel: r = (g^k \mod p) \mod q$
- **Rappel**: $s_1 = k^{-1} (H(m_1) + rx) \mod q$
- Rappel: $s_2 = k^{-1} (H(m_2) + rx) \mod q$
- $= k = (H(m_1) H(m_2))(s_1 s_2)^{-1} \mod q$



Les canaux subliminaux dans DSA

Marin HANNACHE

Introduction

Caractéristiques
Le logarithme discr

Le logarithme disc Signer un messag Remarques

Canaux

subliminau

Canal « haut débit

Résidus quadratiques

Les autres méthodes

Contre-

Mise en gage Limites

Conclusion

- Le paramètre aléatoire *k* possède des propriétés intéressantes (suite) :
 - La réutilisation du même k pour signer deux messages distincts permet de le dériver des signatures et donc de retrouver la clé privée.

- Rappel: $r = (g^k \mod p) \mod q$
- Rappel: $s_1 = k^{-1}(H(m_1) + rx) \mod q$
- Rappel: $s_2 = k^{-1} (H(m_2) + rx) \mod q$
- $= k = (H(m_1) H(m_2))(s_1 s_2)^{-1} \mod q$



Les canaux subliminaux dans DSA

Marin HANNACHE

Remarques

Mise en gage

- Le paramètre aléatoire k possède des propriétés intéressantes (suite) :
 - La réutilisation du même *k* pour signer deux messages distincts permet de le dériver des signatures et donc de retrouver la clé privée.

- **Rappel:** $r = (g^k \mod p) \mod q$
- Rappel: $s_1 = k^{-1} (H(m_1) + rx) \mod q$
- Rappel: $s_2 = k^{-1} (H(m_2) + rx) \mod q$ $k = (H(m_1) H(m_2)) (s_1 s_2)^{-1} \mod q$



Les canaux subliminaux dans DSA

Marin HANNACHE

Introductio

DSA

Caractéristiques

Le logarithme disc

Signer un message

Remarques

Canaux

Définition

Canal « haut débi

Canaux « bas débi Résidus

Les autres

Contre-

Mise en gage

Conclusion

■ Le paramètre aléatoire *k* possède des propriétés intéressantes (suite et fin) :

La connaissance de la clé privée permet de retrouver k à partir de la signature!

- $\blacksquare Rappel: r = (g^k \mod p) \mod q$
- Rappel: $s = k^{-1} (H(m) + rx) \mod q$
- $k = s^{-1} (H(m) + rx) \mod q$



Les canaux subliminaux dans DSA

Marin HANNACHE

Remarques

Mise en gage

Le paramètre aléatoire k possède des propriétés intéressantes (suite et fin) :

■ La connaissance de la clé privée permet de retrouver *k* à partir de la signature!

- $k = s^{-1} (H(m) + rx) \mod q$



Les canaux subliminaux dans DSA

Marin HANNACHE

Remarques

Mise en gage

Le paramètre aléatoire k possède des propriétés intéressantes (suite et fin) :

■ La connaissance de la clé privée permet de retrouver k à partir de la signature!

- Rappel: $r = (g^k \mod p) \mod q$
- Rappel: $s = k^{-1} (H(m) + rx) \mod q$
- $= k = s^{-1} (H(m) + rx) \mod q$



Les canaux subliminaux dans DSA

Marin HANNACHE

Introductio

.

Caractéristiques
Le logarithme disc

Remarques

Canaux

subliminau

Définition

Canaux « bas débit

Résidus quadratiques Les autres

Contre-

Mise en gage Limites

Conclusion

- Le paramètre aléatoire *k* possède des propriétés intéressantes (suite et fin) :
 - La connaissance de la clé privée permet de retrouver k à partir de la signature!

- $\blacksquare Rappel: r = (g^k \mod p) \mod q$
- Rappel : $s = k^{-1} (H(m) + rx) \mod q$
- $k = s^{-1} (H(m) + rx) \mod q$



Plan

Les canaux subliminaux dans DSA

Marin HANNACHE

Introductio

....

Caractéristiques Le logarithme discr

Signer un messag Remarques

Canaux

sublimina Définition

Canal « haut

Résidus quadratique

Contre-

Mise en gage Limites

Conclusion

Introduction rapide à DSA

- Caractéristiques de DSA
- Le problème du logarithme discret
- Signer un message avec DSA
- Remarques sur DSA

2 Canaux subliminaux

- Définition
- Le canal subliminal « haut débit » de DSA
- Les canaux subliminaux « bas débit » de DSA
 - La méthode des résidus quadratiques
 - Les autres méthodes
- 3 Contre-mesures
 - Mise en gage (commitment scheme)
 - Limites des contre-mesures



Définition

Les canaux subliminaux dans DSA

Marin HANNACHE

Introductio

DSA
Caractéristiques
Le logarithme discre

Le logarithme discr Signer un message Remarques

subliminau

Définition

Canal « haut débit »
Canaux « bas débit »
Résidus
quadratiques

Contre-

Mise en gage

- Le concept de canal subliminal a été théorisé en 1984 par Gustavus SIMMONS.
- Il s'agit d'un canal de communication sécurisé et caché au sein d'un autre canal de communication qui ne l'est pas.
- Il ne doit pas être possible de distinguer les communications utilisant ces canaux de celles qui ne les utilisent pas.



Définition

Les canaux subliminaux dans DSA Marin

HANNACHE

Introductio

Caractéristiques
Le logarithme discr

Remarques

subliminau

Canal « haut débit »
Canaux « bas débit »
Résidus
quadratiques

Contre-

Mise en gage

- Le concept de canal subliminal a été théorisé en 1984 par Gustavus SIMMONS.
- Il s'agit d'un canal de communication sécurisé et caché au sein d'un autre canal de communication qui ne l'est pas.
- Il ne doit pas être possible de distinguer les communications utilisant ces canaux de celles qui ne les utilisent pas.



Définition

Les canaux subliminaux dans DSA

Marin HANNACHE

Introductio

Caractéristiques
Le logarithme discre
Signer un message

Canaux subliminaux

Définition

Canaux « bas débit Résidus quadratiques Les autres

Contre-

Mise en gage Limites

- Le concept de canal subliminal a été théorisé en 1984 par Gustavus SIMMONS.
- Il s'agit d'un canal de communication sécurisé et caché au sein d'un autre canal de communication qui ne l'est pas.
- Il ne doit pas être possible de distinguer les communications utilisant ces canaux de celles qui ne les utilisent pas.



Exemples

Les canaux subliminaux dans DSA

Marin HANNACHE

Définition

Mise en gage

RSA, ElGamal et d'autres cryptosystèmes sont dotés de canaux subliminaux



Exemples

Les canaux subliminaux dans DSA

Marin HANNACHE

Définition

Mise en gage

RSA, ElGamal et d'autres cryptosystèmes sont dotés de canaux subliminaux

DSA possède un canal « haut débit » de 160 bits et plusieurs canaux « bas débit ». Certains canaux « bas débit » peuvent être utilisés simultanément.



Plan

Les canaux subliminaux dans DSA

Marin HANNACHE

Canal « haut débit »

Mise en gage

- Caractéristiques de DSA
- Le problème du logarithme discret
- Signer un message avec DSA

Canaux subliminaux

- Définition
- Le canal subliminal « haut débit » de DSA
- Les canaux subliminaux « bas débit » de DSA
 - La méthode des résidus quadratiques
 - Les autres méthodes
- - Mise en gage (commitment scheme)
 - Limites des contre-mesures



Les canaux subliminaux dans DSA

Marin HANNACHE

Canal « haut débit »

Mise en gage

- 1 La clé privée du signataire est connue du destinataire.



Les canaux subliminaux dans DSA

Marin HANNACHE

Introduction

Caractéristiques Le logarithme disc

Signer un message Remarques

Canaux subliminau

Définition

Canal « haut débit »

Canaux « bas débit » Résidus quadratiques

Contre-

Mise en gage

- 1 La clé privée du signataire est connue du destinataire.
- Le message subliminal est chiffré à l'aide d'une méthode convenue à l'avance.
- 3 Ou lieu de choisir *k* aléatoirement, on utilise le message chiffré à la place.
- 4 Le destinataire connaissant la clé privée utilisée, il peu retrouver la valeur de *k* à partir de la signature et en déduire le message subliminal.



Les canaux subliminaux dans DSA

Marin HANNACHE

Introduction

DSA Caractéristiques

Le logarithme discr Signer un message

Canaux

Définition

Canal « haut débit » Canaux « bas débit » Résidus

Résidus quadratiques Les autres

Contre-

Mise en gage

- 1 La clé privée du signataire est connue du destinataire.
- 2 Le message subliminal est chiffré à l'aide d'une méthode convenue à l'avance.
- Ou lieu de choisir *k* aléatoirement, on utilise le message chiffré à la place.
- Le destinataire connaissant la clé privée utilisée, il peu retrouver la valeur de *k* à partir de la signature et en déduire le message subliminal.



Les canaux subliminaux dans DSA

Marin HANNACHE

Introduction

Caractéristiques
Le logarithme disc
Signer un message

Canaux subliminaux

Définition

Canal « haut débit » Canaux « bas débit :

Canaux « bas débit Résidus quadratiques Les autres

Contre-

Mise en gage Limites

- 1 La clé privée du signataire est connue du destinataire.
- Le message subliminal est chiffré à l'aide d'une méthode convenue à l'avance.
- 3 Ou lieu de choisir *k* aléatoirement, on utilise le message chiffré à la place.
- 4 Le destinataire connaissant la clé privée utilisée, il peut retrouver la valeur de k à partir de la signature et en déduire le message subliminal.



Plan

Les canaux subliminaux dans DSA

Marin HANNACHE

Introductio

DSA

Caractéristiques
Le logarithme discre
Signer un message

Signer un messaç Remarques

Sublimina

Définition
Canal « haut débit »

Canaux « has débit »

Résidus quadratiques

Contre-

Mise en gage Limites

Conclusion

1 Introduction rapide à DSA

- Caractéristiques de DSA
- Le problème du logarithme discret
- Signer un message avec DSA
- Remarques sur DSA

2 Canaux subliminaux

- Définition
- Le canal subliminal « haut débit » de DSA
- Les canaux subliminaux « bas débit » de DSA
 - La méthode des résidus quadratiques
 - Les autres méthodes
- 3 Contre-mesures
 - Mise en gage (commitment scheme)
 - Limites des contre-mesures



Plan

Les canaux subliminaux dans DSA

Marin HANNACHE

Introductio

DO 4

Caractéristiques
Le logarithme discre
Signer un message

Remarques

sublimina

Définition Canal « haut débit

Canaux « bas débit

quadratiques Les autres

Contre-

mesures Mise en gage Limites

- 1 Introduction rapide à DSA
 - Caractéristiques de DSA
 - Le problème du logarithme discret
 - Signer un message avec DSA
 - Remarques sur DSA
- 2 Canaux subliminaux
 - Définition
 - Le canal subliminal « haut débit » de DSA
 - Les canaux subliminaux « bas débit » de DSA
 - La méthode des résidus quadratiques
 - Les autres méthodes
- 3 Contre-mesures
 - Mise en gage (commitment scheme)
 - Limites des contre-mesures



Résidus quadratiques

Les canaux subliminaux dans DSA

Marin HANNACHE

Introductio

.

Caractéristiques

Le logarithme dis Signer un messa

Remarques

Canaux subliminau

Définition

Canal « haut débi

Résidus quadratiques

Les autres méthodes

Contre

Mise en gage Limites

Conclusion

Définition

On dit d'un entier naturel a qu'il est un résidu quadratique modulo n s'il existe un entier x tel que :

$$x^2 \equiv a \pmod{n}$$

On peut faire le vérification rapidement si *n* est un nombre premier grâce au critère d'Euler :

Critère d'Euler

- Si $a^{(n-1)/2} \equiv 1 \pmod{n}$ alors a est un résidu quadratique modulo n.
- Si $a^{(n-1)/2} \equiv -1 \pmod{n}$ alors a n'est pas un résidu quadratique modulo n.



Résidus quadratiques

Les canaux subliminaux dans DSA

Marin HANNACHE

Résidus quadratiques

Mise en gage

Définition

On dit d'un entier naturel a qu'il est un résidu quadratique modulo *n* s'il existe un entier *x* tel que :

$$x^2 \equiv a \pmod{n}$$

On peut faire le vérification rapidement si *n* est un nombre premier grâce au critère d'Euler :

Critère d'Euler

- Si $a^{(n-1)/2} \equiv 1 \pmod{n}$ alors a est un résidu quadratique modulo n.
- Si $a^{(n-1)/2} \equiv -1 \pmod{n}$ alors a n'est pas un résidu quadratique modulo n.



Les canaux subliminaux dans DSA

Marin HANNACHE

Introductio

minodaone

Caractéristiques
Le logarithme discre

Canaux

subliminau

Canal « haut débit

Résidus quadratiques

Les autres méthodes

Contremesure

mesures Mise en gage Limites

Conclusion

- 1 Les participant conviennent au préalable d'un nombre premier secret *P*.
- Le signataire choisi k de façon à ce que r soit un residu quadratique modulo P, s'il veut transmettre un 1; ou que r ne le soit pas s'il veut transmettre un 0.
- 3 Le destinataire applique le critère d'Euler sur *r* pour retrouver le bit transmi par le canal subliminal.



Les canaux subliminaux dans DSA

Marin HANNACHE

Introductio

DSA

Caractéristiques Le logarithme disc Signer un messag

Canaux

subliminaux

Canal « haut débit

Résidus quadratiques

Les autre méthodes

Mise en gar

Mise en gage Limites

Conclusion

- Les participant conviennent au préalable d'un nombre premier secret P.
- 2 Le signataire choisi k de façon à ce que r soit un residu quadratique modulo P, s'il veut transmettre un 1; ou que r ne le soit pas s'il veut transmettre un 0.
- Le destinataire applique le critère d'Euler sur *r* pour retrouver le bit transmi par le canal subliminal.



Les canaux subliminaux dans DSA

Marin HANNACHE

Introductio

Caractéristiques
Le logarithme disc
Signer un messac

Canaux

Définition

Canal « haut débit

Résidus quadratiques Les autres

Contremesures Mise en gage

Conclusion

- 1 Les participant conviennent au préalable d'un nombre premier secret *P*.
- Le signataire choisi k de façon à ce que r soit un residu quadratique modulo P, s'il veut transmettre un 1; ou que r ne le soit pas s'il veut transmettre un 0.
- Le destinataire applique le critère d'Euler sur *r* pour retrouver le bit transmi par le canal subliminal.



Les canaux subliminaux dans DSA

Marin HANNACHE

Introduction

Caractéristiques Le logarithme disc Signer un messag

Canaux subliminau

Définition
Canal « haut débit
Canaux » has débit

Résidus quadratiques Les autres

Mise en gage

Conclusion

- 1 Les participant conviennent au préalable d'un nombre premier secret *P*.
- Le signataire choisi k de façon à ce que r soit un residu quadratique modulo P, s'il veut transmettre un 1; ou que r ne le soit pas s'il veut transmettre un 0.
- Le destinataire applique le critère d'Euler sur *r* pour retrouver le bit transmi par le canal subliminal.



Plan

Les canaux subliminaux dans DSA

Marin HANNACHE

Introductio

.

Caractéristiques Le logarithme discr

Signer un messag

Remarques

sublimina

Sublimina

Canal « haut débit » Canaux « bas débit Résidus

Les autres méthodes

Contremesures

Mise en gage Limites

Conclusion

1 Introduction rapide à DSA

- Caractéristiques de DSA
- Le problème du logarithme discret
- Signer un message avec DSA
- Remarques sur DSA

2 Canaux subliminaux

- Définition
- Le canal subliminal « haut débit » de DSA
- Les canaux subliminaux « bas débit » de DSA
 - La méthode des résidus quadratiques
 - Les autres méthodes
- 3 Contre-mesures
 - Mise en gage (commitment scheme)
 - Limites des contre-mesures



Les autres méthodes

Les canaux subliminaux dans DSA

Marin HANNACHE

Les autres méthodes

Mise en gage

- Un autre canal subliminal de 1 bit existe, il est basé sur une variante du masque jetable.
- Un canal subliminal de 159 bits existe, il ne nécessite



Les autres méthodes

Les canaux subliminaux dans DSA

Marin HANNACHE

Introductio

Caractéristiques
Le logarithme discre

Remarc

Canaux subliminaux

Définition

Canal « haut dél

Canaux « bas débit Résidus quadratiques

Les autres

Contre-

Mise en gage Limites

- Un autre canal subliminal de 1 bit existe, il est basé sur une variante du masque jetable.
- Un canal subliminal de 159 bits existe, il ne nécessite pas de compromettre sa clé privée mais demande plus de calculs de la part du destinataire.



Plan

Les canaux subliminaux dans DSA

Marin HANNACHE

Introductio

III Oddotio

Caractéristiques Le logarithme discr

Signer un message Remarques

riomarque

sublimina

Définition

Canal « haut débit » Canaux « bas débit Résidus

quadratiques Les autres méthodes

Contremesures

Mise en gage

Conclusion

1 Introduction rapide à DSA

- Caractéristiques de DSA
- Le problème du logarithme discret
- Signer un message avec DSA
- Remarques sur DSA

2 Canaux subliminaux

- Définition
- Le canal subliminal « haut débit » de DSA
- Les canaux subliminaux « bas débit » de DSA
 - La méthode des résidus quadratiques
 - Les autres méthodes

3 Contre-mesures

- Mise en gage (commitment scheme)
- Limites des contre-mesures



Les canaux subliminaux dans DSA

Marin HANNACHE

Introduction

Caractéristiques
Le logarithme discr
Signer un message

Canaux subliminau

Définition

Canaux « bas débit Résidus quadratiques

Contre-

Mise en gage Limites

Conclusion

1 Un tiers intervient dans le protocole pour garantir l'impossibilité d'utiliser les canaux subliminaux. Il choisi une fonction de hachage cryptographique *H* et un nombre *n*.

2 On répète n fois le protocole suivant :

1 Le signataire choisit un nombre k et communique H(k) au tiers.

2 Le tiers choisit un nombre aléatoire k'.

3 Le signataire calcule $r = (g^{k \oplus k'} \mod p) \mod q$ et communique r au tiers.

Le tiers choisit n-1 des k et demande à ce qu'ils lui soient communiqués, il vérifie que le protocol a bien été respecté.

4 Le signataire peut utiliser le *k* resté secret pour signer son message.



Les canaux subliminaux dans DSA

Marin HANNACHE

Introduction

Caractéristiques
Le logarithme discr
Signer un message

Canaux subliminau:

Définition

Canaux « bas débit Résidus quadratiques

Contre-

Mise en gage Limites

Conclusion

1 Un tiers intervient dans le protocole pour garantir l'impossibilité d'utiliser les canaux subliminaux. Il choisi une fonction de hachage cryptographique *H* et un nombre *n*.

2 On répète n fois le protocole suivant :

1 Le signataire choisit un nombre k et communique H(k) au tiers.

2 Le tiers choisit un nombre aléatoire k'.

3 Le signataire calcule $r = (g^{k \oplus k'} \mod p) \mod q$ et communique r au tiers.

3 Le tiers choisit n-1 des k et demande à ce qu'ils lui soient communiqués, il vérifie que le protocol a bien été respecté.

4 Le signataire peut utiliser le *k* resté secret pour signer son message.



Les canaux subliminaux dans DSA

Marin HANNACHE

Introductio

DSV

Le logarithme discr Signer un message

Canaux subliminaux

Canal « haut débit »
Canaux « bas débit »
Résidus

Les autres méthodes

Contremesures

Mise en gage Limites

Conclusion

11 Un tiers intervient dans le protocole pour garantir l'impossibilité d'utiliser les canaux subliminaux. Il choisi une fonction de hachage cryptographique *H* et un nombre *n*.

On répète n fois le protocole suivant :

1 Le signataire choisit un nombre k et communique H(k) au tiers.

2 Le tiers choisit un nombre aléatoire k'.

Le signataire calcule $r = (g^{k \oplus k'} \mod p) \mod q$ et communique r au tiers.

3 Le tiers choisit n-1 des k et demande à ce qu'ils lui soient communiqués, il vérifie que le protocol a bien été respecté.

4 Le signataire peut utiliser le *k* resté secret pour signer son message.



Les canaux subliminaux dans DSA

Marin HANNACHE

Introductio

Caractéristiques
Le logarithme discr

Signer un messag Remarques

subliminau

Canal « haut débit »

Canaux « bas débit »

Résidus

quadratiques

Contre-

Mise en gage

Conclusion

11 Un tiers intervient dans le protocole pour garantir l'impossibilité d'utiliser les canaux subliminaux. Il choisi une fonction de hachage cryptographique *H* et un nombre *n*.

- 1 Le signataire choisit un nombre k et communique H(k) au tiers.
- 2 Le tiers choisit un nombre aléatoire k'.
- Le signataire calcule $r = (g^{k \oplus k'} \mod p) \mod q$ et communique r au tiers.
- Le tiers choisit n-1 des k et demande à ce qu'ils lui soient communiqués, il vérifie que le protocol a bien été respecté.
- 4 Le signataire peut utiliser le *k* resté secret pour signer son message.



Les canaux subliminaux dans DSA

Marin HANNACHE

Introductio

Caractéristiques
Le logarithme discr
Signer un message

Canaux subliminaux

Définition Canal « haut débi Canaux « bas dét

Résidus quadratiques Les autres méthodes

Contremesures

Mise en gage Limites

Conclusion

11 Un tiers intervient dans le protocole pour garantir l'impossibilité d'utiliser les canaux subliminaux. Il choisi une fonction de hachage cryptographique H et un nombre n.

- 1 Le signataire choisit un nombre k et communique H(k) au tiers.
- **2** Le tiers choisit un nombre aléatoire k'.
- 3 Le signataire calcule $r = (g^{k \oplus k'} \mod p) \mod q$ et communique r au tiers.
- Le tiers choisit n-1 des k et demande à ce qu'ils lui soient communiqués, il vérifie que le protocol a bien été respecté.
- 4 Le signataire peut utiliser le *k* resté secret pour signer son message.



Les canaux subliminaux dans DSA

Marin HANNACHE

Introductio

Caractéristiques
Le logarithme discr
Signer un message

Canaux

Définition
Canal « haut débit
Canaux « bas débi
Résidus

quadratiques Les autres méthodes

mesures Mise en gage

Limites

Conclusion

1 Un tiers intervient dans le protocole pour garantir l'impossibilité d'utiliser les canaux subliminaux. Il choisi une fonction de hachage cryptographique *H* et un nombre *n*.

- 1 Le signataire choisit un nombre k et communique H(k) au tiers.
- 2 Le tiers choisit un nombre aléatoire k'.
- 3 Le signataire calcule $r = (g^{k \oplus k'} \mod p) \mod q$ et communique r au tiers.
- 3 Le tiers choisit n-1 des k et demande à ce qu'ils lui soient communiqués, il vérifie que le protocol a bien été respecté.
- 4 Le signataire peut utiliser le k resté secret pour signer son message.



Les canaux subliminaux dans DSA

Marin HANNACHE

Introduction

Caractéristiques Le logarithme disc Signer un message

Canaux

Définition Canal « haut débit » Canaux « bas débit » Résidus quadratiques

Contremesures

Mise en gage Limites

Conclusion

11 Un tiers intervient dans le protocole pour garantir l'impossibilité d'utiliser les canaux subliminaux. Il choisi une fonction de hachage cryptographique *H* et un nombre *n*.

- 1 Le signataire choisit un nombre k et communique H(k) au tiers.
- **2** Le tiers choisit un nombre aléatoire k'.
- 3 Le signataire calcule $r = (g^{k \oplus k'} \mod p) \mod q$ et communique r au tiers.
- 3 Le tiers choisit n-1 des k et demande à ce qu'ils lui soient communiqués, il vérifie que le protocol a bien été respecté.
- 4 Le signataire peut utiliser le *k* resté secret pour signer son message.



Plan

Les canaux subliminaux dans DSA

Marin HANNACHE

Mise en gage Limites

- Caractéristiques de DSA
- Le problème du logarithme discret
- Signer un message avec DSA
- - Définition
 - Le canal subliminal « haut débit » de DSA
 - Les canaux subliminaux « bas débit » de DSA
 - La méthode des résidus quadratiques
 - Les autres méthodes
- Contre-mesures
 - Mise en gage (commitment scheme)
 - Limites des contre-mesures





Les canaux subliminaux dans DSA

Marin HANNACHE

Introduction

Caractéristiques Le logarithme disc Signer un message

Canaux sublimina

Définition

Canal « haut débit »

Canaux « bas débit

Résidue

Résidus quadratiques Les autres méthodes

mesures
Mise en gage
Limites

Conclusion

Ce protocole dispose lui-même d'un canal subliminal entre le tiers de confiance et le signataire.

Canal subliminal dans le protocole de mise en gage

Les k sont choisis de manière à ce qu'on puisse appliquer la méthode des résidus quadratiques à H(k).

■ Tout protocole naïf visant à garantir l'absence d'un canal subliminal dispose en réalité lui-même d'un canal subliminal de 1 bit.

Canal subliminal dans tout protocole de contre-mesure





Les canaux subliminaux dans DSA

Marin HANNACHE

Introduction

.....

Caractéristiques
Le logarithme disc

Signer un message Remarques

subliminau

Canal « haut débit » Canaux « bas débit Résidus

quadratiques
Les autres
méthodes

mesures
Mise en gage
Limites

Conclusion

Ce protocole dispose lui-même d'un canal subliminal entre le tiers de confiance et le signataire.

Canal subliminal dans le protocole de mise en gage

Les k sont choisis de manière à ce qu'on puisse appliquer la méthode des résidus quadratiques à H(k).

■ Tout protocole naïf visant à garantir l'absence d'un canal subliminal dispose en réalité lui-même d'un canal subliminal de 1 bit.

Canal subliminal dans tout protocole de contre-mesure



Les canaux subliminaux dans DSA

Marin HANNACHE

Introductio

miroddom

Caractéristiques Le logarithme disc Signer un messag

Canaux subliminau:

Définition Canal « haut débit » Canaux « bas débit Résidus

Canaux « bas débi Résidus quadratiques Les autres méthodes

Contremesures Mise en gage Limites

Conclusion

Ce protocole dispose lui-même d'un canal subliminal entre le tiers de confiance et le signataire.

Canal subliminal dans le protocole de mise en gage

Les k sont choisis de manière à ce qu'on puisse appliquer la méthode des résidus quadratiques à H(k).

 Tout protocole naïf visant à garantir l'absence d'un canal subliminal dispose en réalité lui-même d'un canal subliminal de 1 bit.

Canal subliminal dans tout protocole de contre-mesure



Les canaux subliminaux dans DSA

Marin HANNACHE

Introduction

DSA

Caractéristiques
Le logarithme disci
Signer un message

Canaux subliminaux Définition

Canal « haut débit Canaux « bas débi Résidus quadratiques Les autres

Contremesures Mise en gage Limites

Conclusion

Ce protocole dispose lui-même d'un canal subliminal entre le tiers de confiance et le signataire.

Canal subliminal dans le protocole de mise en gage

Les k sont choisis de manière à ce qu'on puisse appliquer la méthode des résidus quadratiques à H(k).

 Tout protocole naïf visant à garantir l'absence d'un canal subliminal dispose en réalité lui-même d'un canal subliminal de 1 bit.

Canal subliminal dans tout protocole de contre-mesure



Conclusion

Les canaux subliminaux dans DSA

Marin HANNACHE

Introduction

DSA

Le logarithme discre Signer un message

Remarques

sublimina

Définition

Canal « haut débit Canaux « bas déb

Résidus quadratique

Contre-

Mise en gage

Conclusion

Il ne faut *jamais* faire confiance à une implémentation de DSA que l'on ne peut pas auditer.



Questions

Les canaux subliminaux dans DSA

Marin HANNACHE

Introduction

Introductio

DSA

Le logarithme discret

Signer un messa

Remarques

Canaux

Subiimina

Canal « haut déb

Résidus

Les autres

Contre-

Mise en gage

