Chiffrement Unidirectionnel et Chiffrement Bidirectionnel

Constructions, Modèle de Sécurité et Applications

Mamadou Makhtar LO

January 9, 2021

Introduction

Contexte

- Développements Technologiques: Cloud Storage, Cloud Computing, IoT etc..

Introduction

Contexte

- Développements Technologiques: Cloud Storage, Cloud Computing, IoT etc..
- Partage de fichiers entre utilisateurs

Introduction

Contexte

- Développements Technologiques: Cloud Storage, Cloud Computing, IoT etc..
- Partage de fichiers entre utilisateurs
- Besoins en Sécurité: Délégation, Contrôle d'accès..

Introduction

Contexte

- Développements Technologiques: Cloud Storage, Cloud Computing, IoT etc..
- Partage de fichiers entre utilisateurs
- Besoins en Sécurité: Délégation, Contrôle d'accès..
  Comment partager un fichier sans divulguer le message ou les clé de déchiffrements ?

Introduction

Objet:

Serveur de re-chiffrement (ou Proxy Re-Encryption)

Introduction

Objet:

Serveur de re-chiffrement (ou Proxy Re-Encryption)

- Transforme un texte chiffré pour une clé particulière en un texte chiffré pour une autre clé:

Introduction

Objet:

Serveur de re-chiffrement (ou Proxy Re-Encryption)

- Transforme un texte chiffré pour une clé particulière en un texte chiffré pour une autre clé:
  sans avoir accès au texte clair,

Introduction

Objet:

Serveur de re-chiffrement (ou Proxy Re-Encryption)

- Transforme un texte chiffré pour une clé particulière en un texte chiffré pour une autre clé:
  sans avoir accès au texte clair,
  sans avoir accès aux clés de déchiffrement.

Introduction

Objet:

Serveur de re-chiffrement (ou Proxy Re-Encryption)

- Transforme un texte chiffré pour une clé particulière en un texte chiffré pour une autre clé:
  sans avoir accès au texte clair,
  sans avoir accès aux clés de déchiffrement.
- Selon le sens de la délégation:

Introduction

Objet:

Serveur de re-chiffrement (ou Proxy Re-Encryption)

- Transforme un texte chiffré pour une clé particulière en un texte chiffré pour une autre clé:
  sans avoir accès au texte clair,
  sans avoir accès aux clés de déchiffrement.
- Selon le sens de la délégation: Chiffrement Unidirectionnel

Introduction

Objet:

Serveur de re-chiffrement (ou Proxy Re-Encryption)

- Transforme un texte chiffré pour une clé particulière en un texte chiffré pour une autre clé:
  sans avoir accès au texte clair,
  sans avoir accès aux clés de déchiffrement.
- Selon le sens de la délégation: Chiffrement Unidirectionnel Chiffrement Bidirectionnel.

Introduction

Objet:

Serveur de re-chiffrement (ou Proxy Re-Encryption)

- Transforme un texte chiffré pour une clé particulière en un texte chiffré pour une autre clé:
  sans avoir accès au texte clair,
  sans avoir accès aux clés de déchiffrement.
- Selon le sens de la délégation: Chiffrement Unidirectionnel Chiffrement Bidirectionnel.

Introduction

Problématique

- Construction de serveurs de re-chiffrement (unidirectionnel/Bidirectionnel)

Introduction

Problématique

- Construction de serveurs de re-chiffrement (unidirectionnel/Bidirectionnel)
- Preuves de Sécurité

Introduction

Problématique

- Construction de serveurs de re-chiffrement (unidirectionnel/Bidirectionnel)
- Preuves de Sécurité
- Applicabilité et efficacité

Introduction

Problématique

- Construction de serveurs de re-chiffrement (unidirectionnel/Bidirectionnel)
- Preuves de Sécurité
- Applicabilité et efficacité

Introduction

Objectifs

- Aspects définitionnels de la notion de PRE (définitions, particularités, modèles existants ...)

Introduction

Objectifs

- Aspects définitionnels de la notion de PRE (définitions, particularités, modèles existants ...)
- Aspects cryptographiques théoriques (Proposition de modèles, analyse de la sécurité, applications...)

Introduction

Objectifs

- Aspects définitionnels de la notion de PRE (définitions, particularités, modèles existants ...)
- Aspects cryptographiques théoriques (Proposition de modèles, analyse de la sécurité, applications...)
- Aspects cryptographiques pratiques (Implémentation, tests d'applicabilité...)

Introduction

Objectifs

- Aspects définitionnels de la notion de PRE (définitions, particularités, modèles existants ...)
- Aspects cryptographiques théoriques (Proposition de modèles, analyse de la sécurité, applications...)
- Aspects cryptographiques pratiques (Implémentation, tests d'applicabilité...)

Serveur de re-chiffrement (PRE)

Proxy Re-Encryption

- Proposé en 1998 par Blaze, Bleumer et Strauss

Serveur de re-chiffrement (PRE)

Proxy Re-Encryption

- Proposé en 1998 par Blaze, Bleumer et Strauss
- "Atomic Proxy function"

Serveur de re-chiffrement (PRE)

Proxy Re-Encryption

- Proposé en 1998 par Blaze, Bleumer et Strauss
- "Atomic Proxy function"
- Développement (Méthode générique 2003 (), Formalisation en 2005 (Ateniese) etc..)

Serveur de re-chiffrement (PRE)

Proxy Re-Encryption

- Proposé en 1998 par Blaze, Bleumer et Strauss
- "Atomic Proxy function"
- Développement (Méthode générique 2003 (), Formalisation en 2005 (Ateniese) etc..)

Principe de fonctionnement

PRE: $\{$*Clé*, *Délégation*, *Chiffrer*, *Re-Chiffrer*, *Dechiffrer*$\}$ tels que:

Serveur de re-chiffrement (PRE)

Proxy Re-Encryption

- Proposé en 1998 par Blaze, Bleumer et Strauss
- "Atomic Proxy function"
- Développement (Méthode générique 2003 (), Formalisation en 2005 (Ateniese) etc..)

Principe de fonctionnement

PRE: $\{$*Clé*, *Délégation*, *Chiffrer*, *Re-Chiffrer*, *Dechiffrer*$\}$ tels que:

- *Clé* génère les clés de chiffrement et déchiffrement.

Serveur de re-chiffrement (PRE)

Proxy Re-Encryption

- Proposé en 1998 par Blaze, Bleumer et Strauss
- "Atomic Proxy function"
- Développement (Méthode générique 2003 (), Formalisation en 2005 (Ateniese) etc..)

Principe de fonctionnement

PRE: $\{$*Clé*, *Délégation*, *Chiffrer*, *Re-Chiffrer*, *Dechiffrer*$\}$ tels que:

- *Clé* génère les clés de chiffrement et déchiffrement.
- *Délégation* génère la clé de délégation ou *clé proxy*.

Serveur de re-chiffrement (PRE)

Proxy Re-Encryption

- Proposé en 1998 par Blaze, Bleumer et Strauss
- "Atomic Proxy function"
- Développement (Méthode générique 2003 (), Formalisation en 2005 (Ateniese) etc..)

Principe de fonctionnement

PRE: $\{$*Clé*, *Délégation*, *Chiffrer*, *Re-Chiffrer*, *Dechiffrer*$\}$ tels que:

- *Clé* génère les clés de chiffrement et déchiffrement.
- *Délégation* génère la clé de délégation ou *clé proxy*.
- *Chiffrer* chiffre le message à l'aide de la clé de chiffrement.

Serveur de re-chiffrement (PRE)

Proxy Re-Encryption

- Proposé en 1998 par Blaze, Bleumer et Strauss
- "Atomic Proxy function"
- Développement (Méthode générique 2003 (), Formalisation en 2005 (Ateniese) etc..)

Principe de fonctionnement

PRE: $\{Clé, Délégation, Chiffrer, Re\text{-}Chiffrer, Dechiffrer\}$ tels que:

- *Clé* génère les clés de chiffrement et déchiffrement.
- *Délégation* génère la clé de délégation ou *clé proxy*.
- *Chiffrer* chiffre le message à l'aide de la clé de chiffrement.
- *Re-Chiffrer* transforme (re-chiffre) à l'aide de la *clé proxy* un texte chiffré pour A en un texte chiffré pour B.

Serveur de re-chiffrement (PRE)

Proxy Re-Encryption

- Proposé en 1998 par Blaze, Bleumer et Strauss
- "Atomic Proxy function"
- Développement (Méthode générique 2003 (), Formalisation en 2005 (Ateniese) etc..)

Principe de fonctionnement

PRE: $\{Clé, Délégation, Chiffrer, Re\text{-}Chiffrer, Dechiffrer\}$ tels que:

- *Clé* génère les clés de chiffrement et déchiffrement.
- *Délégation* génère la clé de délégation ou *clé proxy*.
- *Chiffrer* chiffre le message à l'aide de la clé de chiffrement.
- *Re-Chiffrer* transforme (re-chiffre) à l'aide de la *clé proxy* un texte chiffré pour A en un texte chiffré pour B.
- *Dechiffrer* déchiffre le texte chiffré à l'aide de la clé de déchiffrement.

Serveur de re-chiffrement (PRE)

Proxy Re-Encryption

- Proposé en 1998 par Blaze, Bleumer et Strauss
- "Atomic Proxy function"
- Développement (Méthode générique 2003 (), Formalisation en 2005 (Ateniese) etc..)

Principe de fonctionnement

PRE: $\{Clé, Délégation, Chiffrer, Re\text{-}Chiffrer, Dechiffrer\}$ tels que:

- *Clé* génère les clés de chiffrement et déchiffrement.
- *Délégation* génère la clé de délégation ou *clé proxy*.
- *Chiffrer* chiffre le message à l'aide de la clé de chiffrement.
- *Re-Chiffrer* transforme (re-chiffre) à l'aide de la *clé proxy* un texte chiffré pour A en un texte chiffré pour B.
- *Dechiffrer* déchiffre le texte chiffré à l'aide de la clé de déchiffrement.

Chiffrement Unidirectionnel

- A peut déléguer à B mais pas inversement.

Chiffrement Unidirectionnel

- A peut déléguer à B mais pas inversement.
- Premier modèle avec Alan en 2003.

Chiffrement Unidirectionnel

- A peut déléguer à B mais pas inversement.
- Premier modèle avec Alan en 2003.
- Confiance de A en B.

Chiffrement Unidirectionnel

- A peut déléguer à B mais pas inversement.
- Premier modèle avec Alan en 2003.
- Confiance de A en B.
- Formalisation:

Chiffrement Unidirectionnel

- A peut déléguer à B mais pas inversement.
- Premier modèle avec Alan en 2003.
- Confiance de A en B.
- Formalisation:
  Soit E l'événement "la clé $\pi_{A \to B}$ est calculable en temps polynomial à partir de $\pi_{B \to A}$"

Chiffrement Unidirectionnel

- A peut déléguer à B mais pas inversement.
- Premier modèle avec Alan en 2003.
- Confiance de A en B.
- Formalisation:
  Soit E l'événement "la clé $\pi_{A \to B}$ est calculable en temps polynomial à partir de $\pi_{B \to A}$"
  $P(E)$ est à distance négligeable de 0.

Chiffrement Unidirectionnel

- A peut déléguer à B mais pas inversement.
- Premier modèle avec Alan en 2003.
- Confiance de A en B.
- Formalisation:
  Soit E l'événement "la clé $\pi_{A \to B}$ est calculable en temps polynomial à partir de $\pi_{B \to A}$"
  $P(E)$ est à distance négligeable de 0.
- Délégation "pure".

Chiffrement Unidirectionnel

- A peut déléguer à B mais pas inversement.
- Premier modèle avec Alan en 2003.
- Confiance de A en B.
- Formalisation:
  Soit E l'événement "la clé $\pi_{A \to B}$ est calculable en temps polynomial à partir de $\pi_{B \to A}$"
  $P(E)$ est à distance négligeable de 0.
- Délégation "pure".

Chiffrement Bidirectionnel

- A peut déléguer à B et inversement.

Chiffrement Bidirectionnel

- A peut déléguer à B et inversement.
- Premier modèle avec Blaze et Al. en 1998.

Chiffrement Bidirectionnel

- A peut déléguer à B et inversement.
- Premier modèle avec Blaze et Al. en 1998.
- Confiance mutuelle entre A et B.

Chiffrement Bidirectionnel

- A peut déléguer à B et inversement.
- Premier modèle avec Blaze et Al. en 1998.
- Confiance mutuelle entre A et B.
- Formalisation:

Chiffrement Bidirectionnel

- A peut déléguer à B et inversement.
- Premier modèle avec Blaze et Al. en 1998.
- Confiance mutuelle entre A et B.
- Formalisation:
  Soit E l'événement "la clé $\pi_{A \to B}$ est calculable en temps polynomial à partir de $\pi_{B \to A}$"

Chiffrement Bidirectionnel

- A peut déléguer à B et inversement.
- Premier modèle avec Blaze et Al. en 1998.
- Confiance mutuelle entre A et B.
- Formalisation:
  Soit E l'événement "la clé $\pi_{A \to B}$ est calculable en temps polynomial à partir de $\pi_{B \to A}$"
  $P(E)$ est à distance négligeable de 1.

Chiffrement Bidirectionnel

- A peut déléguer à B et inversement.
- Premier modèle avec Blaze et Al. en 1998.
- Confiance mutuelle entre A et B.
- Formalisation:
  Soit E l'événement "la clé $\pi_{A \to B}$ est calculable en temps polynomial à partir de $\pi_{B \to A}$"
  $P(E)$ est à distance négligeable de 1.
- Clé proxy souvent de la forme x_A/x_B ou $x_A - x_B$

Chiffrement Bidirectionnel

- A peut déléguer à B et inversement.
- Premier modèle avec Blaze et Al. en 1998.
- Confiance mutuelle entre A et B.
- Formalisation:
  Soit E l'événement "la clé $\pi_{A \to B}$ est calculable en temps polynomial à partir de $\pi_{B \to A}$"
  $P(E)$ est à distance négligeable de 1.
- Clé proxy souvent de la forme x_A/x_B ou $x_A - x_B$
- Partage d'accès, répertoire de travail...

Chiffrement Bidirectionnel

- A peut déléguer à B et inversement.
- Premier modèle avec Blaze et Al. en 1998.
- Confiance mutuelle entre A et B.
- Formalisation:
  Soit E l'événement "la clé $\pi_{A \to B}$ est calculable en temps polynomial à partir de $\pi_{B \to A}$"
  $P(E)$ est à distance négligeable de 1.
- Clé proxy souvent de la forme x_A/x_B ou $x_A - x_B$
- Partage d'accès, répertoire de travail...

Le schéma Generalized Elgamal

Algorithme de génération de clé

- Choisir un groupe cyclique G d'ordre suffisamment large d tel que $G = \langle g \rangle$.

Le schéma Generalized Elgamal

Algorithme de génération de clé

- Choisir un groupe cyclique G d'ordre suffisamment large d tel que $G = \langle g \rangle$.
- Choisir aléatoirement deux entiers r et k suffisamment large avec $2 < k < d$ et r et calculer kd.

Le schéma Generalized Elgamal

Algorithme de génération de clé

- Choisir un groupe cyclique G d'ordre suffisamment large d tel que $G = \langle g \rangle$.
- Choisir aléatoirement deux entiers r et k suffisamment large avec $2 < k < d$ et r et calculer kd.
- Avec l'algorithme de la division euclidienne, calculer (s, t) tel que $kd = rs + t$ où $t = kd \mod s$.

Le schéma Generalized Elgamal

Algorithme de génération de clé

- Choisir un groupe cyclique G d'ordre suffisamment large d tel que $G = \langle g \rangle$.
- Choisir aléatoirement deux entiers r et k suffisamment large avec $2 < k < d$ et r et calculer kd.
- Avec l'algorithme de la division euclidienne, calculer (s, t) tel que $kd = rs + t$ où $t = kd \mod s$.
- Calculer $\gamma = g^s$ et $\delta = g^t \in G$; avec $\gamma \neq 1$ et $\delta \neq 1$.

Le schéma Generalized Elgamal

Algorithme de génération de clé

- Choisir un groupe cyclique G d'ordre suffisamment large d tel que $G = \langle g \rangle$.
- Choisir aléatoirement deux entiers r et k suffisamment large avec $2 < k < d$ et r et calculer kd.
- Avec l'algorithme de la division euclidienne, calculer (s, t) tel que $kd = rs + t$ où $t = kd \mod s$.
- Calculer $\gamma = g^s$ et $\delta = g^t \in G$; avec $\gamma \neq 1$ et $\delta \neq 1$.

La clé publique est $((\gamma, \delta), G)$ et la clé privée (r, G).

Le schéma Generalized Elgamal

Algorithme de génération de clé

- Choisir un groupe cyclique G d'ordre suffisamment large d tel que $G = \langle g \rangle$.
- Choisir aléatoirement deux entiers r et k suffisamment large avec $2 < k < d$ et r et calculer kd.
- Avec l'algorithme de la division euclidienne, calculer (s, t) tel que $kd = rs + t$ où $t = kd \mod s$.
- Calculer $\gamma = g^s$ et $\delta = g^t \in G$; avec $\gamma \neq 1$ et $\delta \neq 1$.

La clé publique est $((\gamma, \delta), G)$ et la clé privée (r, G).

Le schéma Generalized Elgamal

Algorithme de Chiffrement

Pour chifrrer un message m avec $((\gamma, \delta), d, G)$:

Le schéma Generalized Elgamal

Algorithme de Chiffrement

Pour chifrrer un message m avec $((\gamma, \delta), d, G)$:

- Choisir aléatoirement un entier $2 < \alpha < d = \#G$ tel que α et $\#G$ premiers entre eux.

Le schéma Generalized Elgamal

Algorithme de Chiffrement

Pour chifrrer un message m avec $((\gamma, \delta), d, G)$:

- Choisir aléatoirement un entier $2 < \alpha < d = \#G$ tel que α et $\#G$ premiers entre eux.
- Calculer $c_1 = \gamma^\alpha$ et $\lambda = \delta^\alpha \in G$ avec $c_1 \neq 1$ et $\lambda \neq 1$.

Le schéma Generalized Elgamal

Algorithme de Chiffrement

Pour chifrrer un message m avec $((\gamma, \delta), d, G)$:

- Choisir aléatoirement un entier $2 < \alpha < d = \#G$ tel que α et $\#G$ premiers entre eux.
- Calculer $c_1 = \gamma^\alpha$ et $\lambda = \delta^\alpha \in G$ avec $c_1 \neq 1$ et $\lambda \neq 1$.
- Transformer m en un élément de G et calculer $c_2 = \lambda m$ in G.

Le schéma Generalized Elgamal

Algorithme de Chiffrement

Pour chifrrer un message m avec $((\gamma, \delta), d, G)$:

- Choisir aléatoirement un entier $2 < \alpha < d = \#G$ tel que α et $\#G$ premiers entre eux.
- Calculer $c_1 = \gamma^\alpha$ et $\lambda = \delta^\alpha \in G$ avec $c_1 \neq 1$ et $\lambda \neq 1$.
- Transformer m en un élément de G et calculer $c_2 = \lambda m$ in G.

Le texte chiffré est (c_1, c_2).

Le schéma Generalized Elgamal

Algorithme de Chiffrement

Pour chifrrer un message m avec $((\gamma, \delta), d, G)$:

- Choisir aléatoirement un entier $2 < \alpha < d = \#G$ tel que α et $\#G$ premiers entre eux.
- Calculer $c_1 = \gamma^\alpha$ et $\lambda = \delta^\alpha \in G$ avec $c_1 \neq 1$ et $\lambda \neq 1$.
- Transformer m en un élément de G et calculer $c_2 = \lambda m$ in G.

Le texte chiffré est (c_1, c_2).

Algorithme de Dechiffrement.

Pour déchiffrer on a juste besoin de calculer $c_1^r c_2$.

Le schéma Generalized Elgamal

Algorithme de Chiffrement

Pour chifrrer un message m avec $((\gamma, \delta), d, G)$:

- Choisir aléatoirement un entier $2 < \alpha < d = \#G$ tel que α et $\#G$ premiers entre eux.
- Calculer $c_1 = \gamma^\alpha$ et $\lambda = \delta^\alpha \in G$ avec $c_1 \neq 1$ et $\lambda \neq 1$.
- Transformer m en un élément de G et calculer $c_2 = \lambda m$ in G.

Le texte chiffré est (c_1, c_2).

Algorithme de Dechiffrement.

Pour déchiffrer on a juste besoin de calculer $c_1^r c_2$.

PRE basé sur ElGamal Généralisé

- Étude de la sécurité du schéma

PRE basé sur ElGamal Généralisé

- Étude de la sécurité du schéma
- Construction des algorithmes de Délégation et de Re-chiffrement

PRE basé sur ElGamal Généralisé

- Étude de la sécurité du schéma
- Construction des algorithmes de Délégation et de Re-chiffrement
- Preuves de Sécurité

PRE basé sur ElGamal Généralisé

- Étude de la sécurité du schéma
- Construction des algorithmes de Délégation et de Re-chiffrement
- Preuves de Sécurité
- Applications: Implémentation, test etc..

PRE basé sur ElGamal Généralisé

- Étude de la sécurité du schéma
- Construction des algorithmes de Délégation et de Re-chiffrement
- Preuves de Sécurité
- Applications: Implémentation, test etc..

Conclusion

- Utilité des Serveurs de Re-chiffrement

Conclusion

- Utilité des Serveurs de Re-chiffrement
- Développement des PRE et problématiques

Conclusion

- Utilité des Serveurs de Re-chiffrement
- Développement des PRE et problématiques
- Objectifs et Contributions

Conclusion

- Utilité des Serveurs de Re-chiffrement
- Développement des PRE et problématiques
- Objectifs et Contributions
- Méthodologie de recherche

Conclusion

- Utilité des Serveurs de Re-chiffrement
- Développement des PRE et problématiques
- Objectifs et Contributions
- Méthodologie de recherche
- Résultats attendus

Conclusion

- Utilité des Serveurs de Re-chiffrement
- Développement des PRE et problématiques
- Objectifs et Contributions
- Méthodologie de recherche
- Résultats attendus

MERCI POUR VOTRE ATTENTION