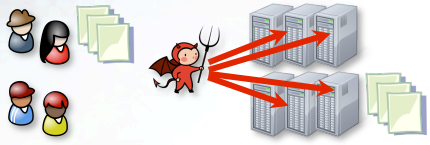
情報セキュリティ研究センター
Research Center for Information Security
Nuttapong Attrapdung

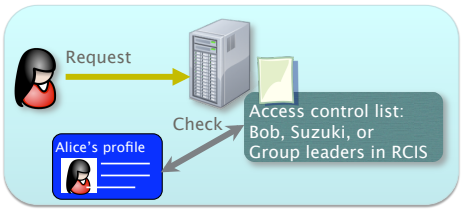
Dual-Policy Attribute Based Encryption
フルアクセス制御機能を持つ暗号方式

モチベーション：安全なオンライン共有ファイルストレージ



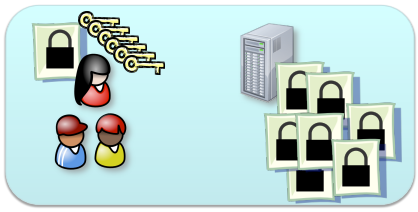
オンラインファイルストレージシステムの持つべき性質:
1. Scalability（拡張性）
2. Reliability（信頼性）
3. Security（安全性）
4. Flexibility（柔軟性）

直観的な方法、その1: 信頼できるサーバーを使う方法。この方法では、各ファイルはアクセス制御リストとともに格納される。ユーザがファイルを取得出来るのは、自分の属性がアクセス制御リストを満たす場合だけである。



利点: 1. 細かいアクセス制限ポリシーを表現可能。
2. 送信者はオンラインでなくてよい。
欠点: 1. 信頼できるサーバーが必要。
2. 暗号化されていないため、データ漏洩の可能性もある。

直観的な方法、その2: 各ファイルを個別の鍵で暗号化する方法。この方法では、すべてのユーザはサーバーにあるすべての暗号文データを取得出来るが、暗号化されているためデータ自体はアクセス出来ない。内容をアクセスするには、そのファイルを暗号化したユーザ（送信者）に要求し、秘密鍵を取得する。



利点: 1. 信頼できるサーバーは不要。
2. 安全性は暗号により保証される。
欠点: 1. 送信者は常にオンラインでなければならない(鍵1個/一つのファイルの場合)か、
2. 細かいアクセス制限が不可能(鍵1個/複数のファイルの場合)。

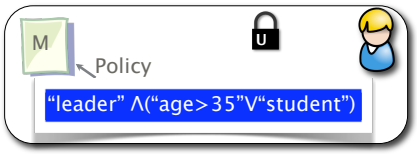
適切な方法のーつ: アトリビュートベース暗号を適用する。結果として、上記の両方のナイーブな方法の良い点を持つシステムが得られる。

アトリビュートベース暗号

公開鍵暗号 (1976–): 公開鍵で暗号化を行う暗号プロトコル。例： RSA

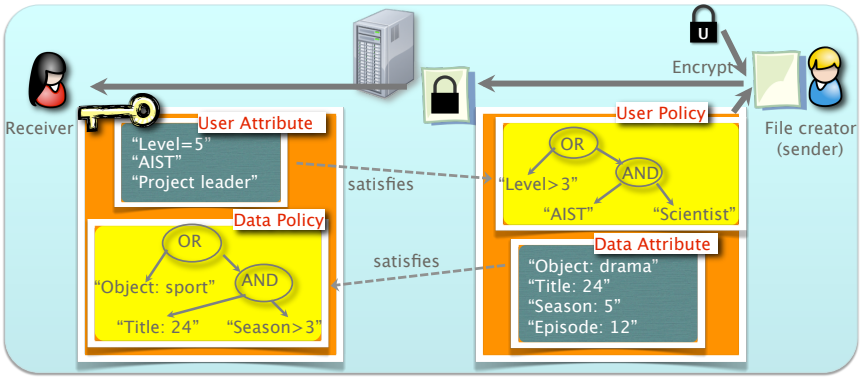
IDベース暗号 (IBE) (1984,2001–): 受信者のメールアドレスなどの「アイデンティティ」が公開鍵として使える暗号方式。

アトリビュートベース暗号 (ABE) (2005–):アトリビュート（属性）の「アクセスポリシー」が公開鍵として使える暗号プロトコル。



問題点: 既存のアトリビュートベース暗号はCiphertext-policyとKey-policyという二つの種類が提案されている。前者はアクセスポリシーをデータの方に関連付けるもので、後者はアクセスポリシーを受信者の鍵の方に関連付けるものである。つまり、データか受信者かどちらかしかアクセス制限をすることが出来なかった。送信者が送るデータと受信者の持っている鍵で同時に「フル」なアクセス制御するような機能を持つシステムは現時点まではまだ研究の課題であった。

本研究の提案：二重ポリシーアトリビュートベース暗号



Dual-policy ABE 二重ポリシーアトリビュートベース暗号: 受信者の鍵の方は受信者の属性とどういう暗号文を復号できるかのアクセスポリシーから定義される。暗号文の方はデータの属性とどういう受信者が複合できるかのアクセスポリシーから定義される。よって、送信者が送るデータと受信者の持っている鍵の両方から同時にフルにアクセス制御を実現することができる。

応用例: オンライン共同ファイルストレージ、Package Pay-TV放送システム、著作権メディア(DVD, Blu-ray)の配信システム、安全なメーリングリストなど。

This work will appear at *Applied Cryptography and Network Security (ACNS 2009)* Conference 2–5 June 09 (in Paris, France).

提案方式はBilinear pairingを適用している。詳細は論文を参照。

National Institute of Advanced Industrial Science and Technology
AIST

Research Center for Information Security

Dual-Policy Attribute-Based Encryption
フルアクセス制御機能を持つ暗号方式

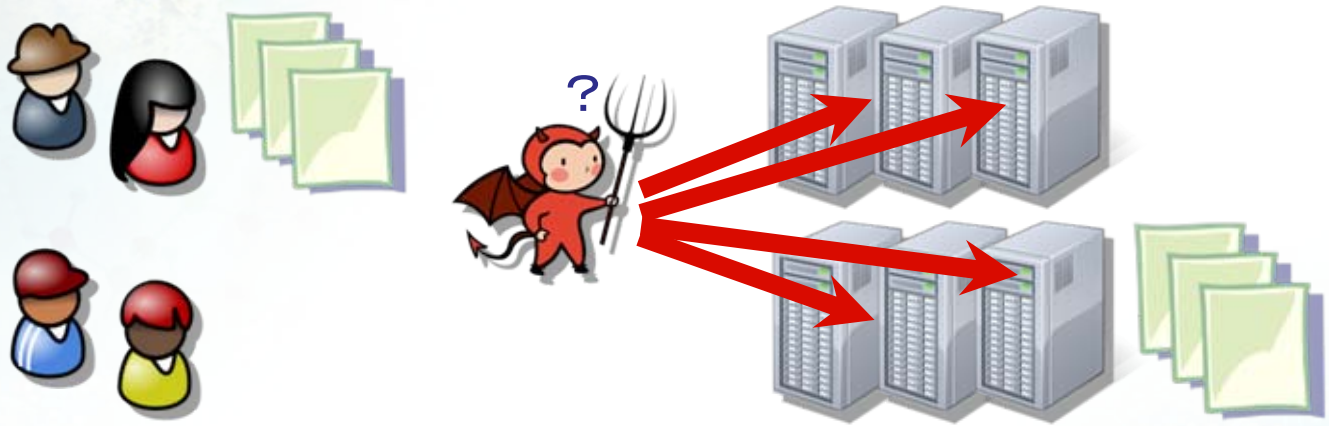
セキュリティ基盤技術研究チーム
Nuttapong Attrapadung
ナッタポン　アッタラパドゥン

National Institute of Advanced Industrial Science and Technology
AIST

モチベーション

Research Center for Information Security

安全なオンライン共有ファイルストレージ



オンラインファイルストレージシステムの持つべき性質:

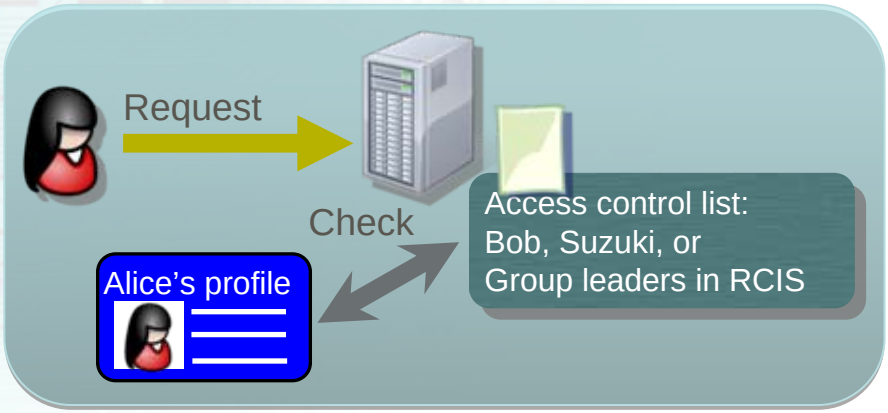
1.Scalability（拡張性）
2.Reliability（信頼性）
3.Security（安全性）
4.Flexibility（アクセス制御の柔軟性）

National Institute of Advanced Industrial Science and Technology
AIST

直観的な方法

Research Center for Information Security

1. 信頼できるサーバーを使う方法。



利点: 1. 細かいアクセス制限ポリシーを表現可能。
2. 送信者はオンラインでなくてよい。

欠点: 1. 信頼できるサーバーが必要。
2. 暗号化されていないため、データ漏洩の可能性もある。

2. 個別に暗号化をする方法。

利点: 1. 信頼できるサーバーは不要。
2. 安全性は暗号により保証される。

欠点: 1. 送信者は常にオンラインでなければならない(鍵1個/一つのファイルの場合)か、
2. 細かいアクセス制限が不可能(鍵1個/複数のファイルの場合)。

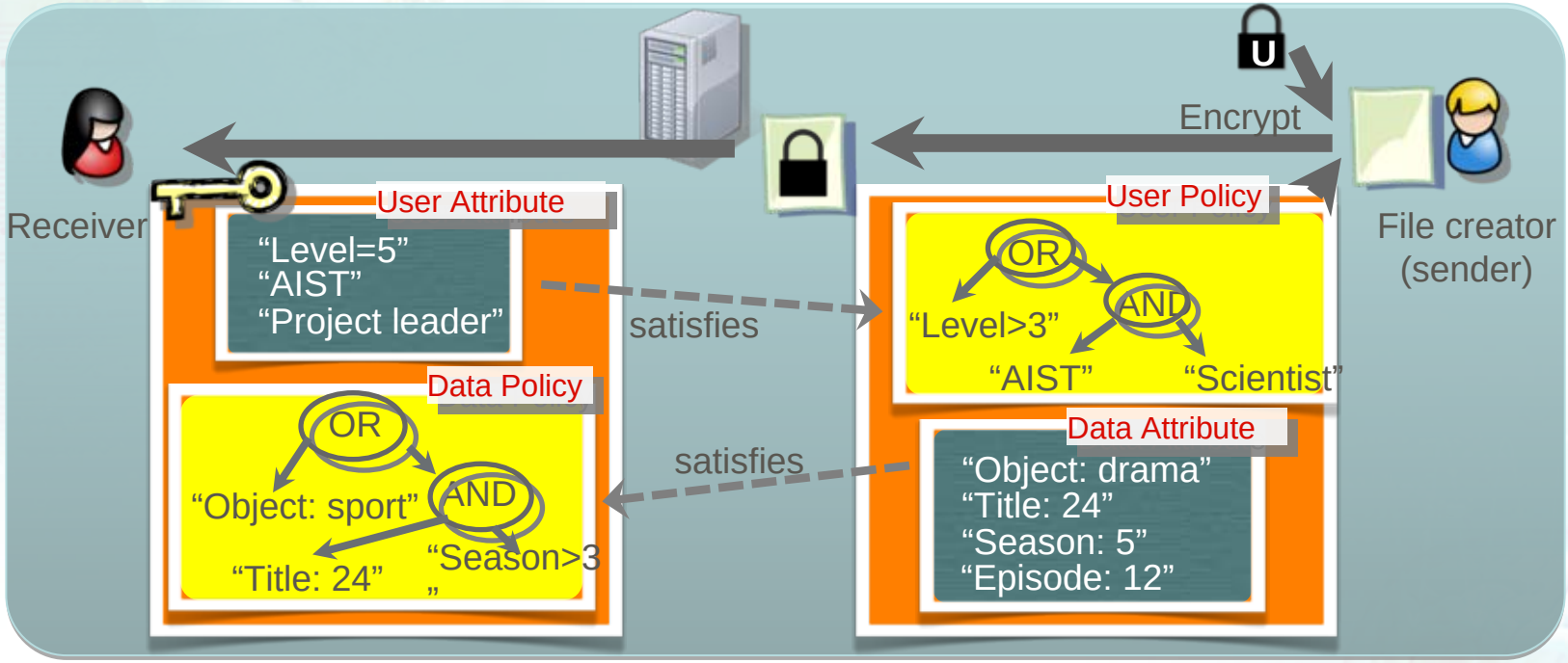
National Institute of Advanced Industrial Science and Technology
AIST

今回の提案

Research Center for Information Security

Dual-policy Attribute-Based Encryption

二重ポリシーアトリビュートベース暗号



特徴

- 両方の直間的な方法からの利点を両立する。
- 「フル」なアクセス制御機能を持つ初めての方式：受信者の持っている鍵と送信者の送るデータの両方から同時にアクセス制御が実現可能。

他のアプリケーション

- Package Pay-TV放送システム、
- 著作権メディア(DVD, BD)の配信、
- 安全なメーリングリスト
- 安全なContext-awareアプリケーション