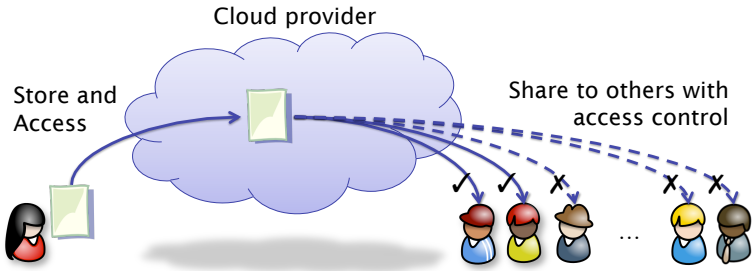
情報セキュリティ研究センター
Research Center for Information Security
Nuttapong Attrapadung

Compact Functional Encryption

クラウドストレージに適したアクセス制御機能を持つ暗号方式

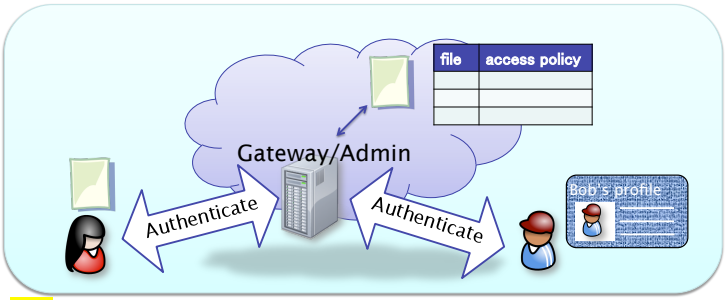
Motivating Problem: Secure Cloud Storage and File sharing

近年、クラウドコンピュティングが注目を集めている。特にクラウドストレージは、データモビリティだけでなく、オンライン共有ストレージも実現可能にした。しかし、クラウドストレージにおけるセキュリティはまだ重要な課題である。従来のセキュリティ対策は下記のように二つの代表的な方法が考えられるが、それぞれ欠点がある。本研究は、この課題の解決方法として高度かつ効率の良い暗号方式「Compact Functional Encryption」を提案した。



Solution 1: Trusted cloud provider

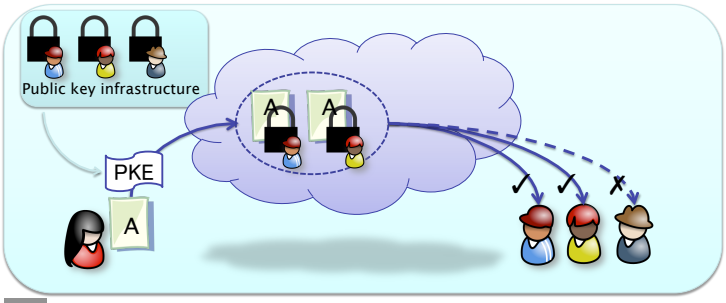
クラウドプロバイダの信頼性を仮定し、すべてのアクセス制御はクラウドプロバイダに任せる。（現状はほとんどこのタイプ）。



☺ 1. 細かいアクセス制御ポリシー表現が可能。
☺ 2. 必要なストレージサイズが小さい。
☹ 3. クラウドプロバイダを信頼しなくてはならない。
☹ 4. 暗号化されていないため、データ漏洩の可能性もある。

Solution 2: Public key infrastructure

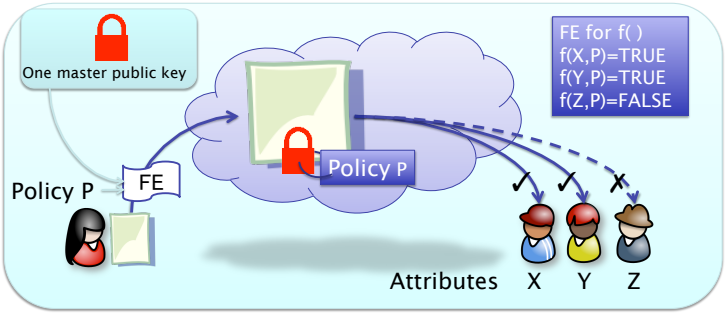
ユーザはPKIを使用しローカルに暗号化してからクラウドにアップロードする。簡単なアクセス制御はユーザが行う。



☹ 1. 細かいアクセス制御ポリシー表現が不可能。
☹ 2. 必要なストレージサイズが大きい。
☺ 3. クラウドプロバイダの信頼性の仮定は必要ない。
☺ 4. 安全性は暗号により保証される。

Functional Encryption (FE): A new perspective for public-key crypto

☺ 1,3,4 ☹ 2

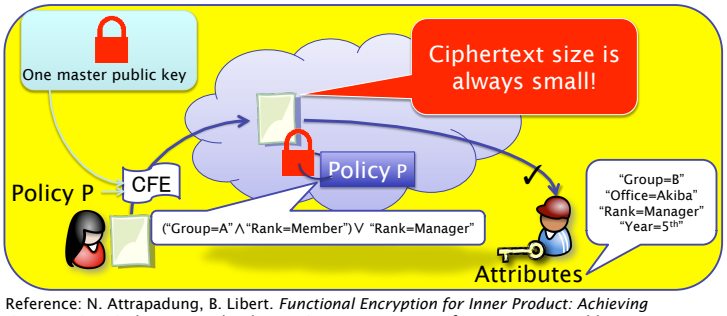


FEは公開鍵暗号の拡張で次の特徴を持つ：(1)マスター公開鍵はすべてのユーザに対応する（IDベース暗号と同様）(2)「関数fのFE」の定義では、属性「X」に対する鍵は、ポリシー「P」で暗号化された暗号文を復号できるのは、f(X,P)=TRUEの時である。さまざまなクラスの関数のFEが提案された。Attributeベース関数クラスの使用で細かいアクセス制御が表現可能になる。

関数のクラス	鍵の属性 X= （例）	暗号文のポリシー P= （例）	f(X,P)=TRUEの定義
IDベース暗号	ID	ID'	ID=ID'
Broadcast暗号	ID	S	ID∈S
Attributeベース暗号	{A,C,D,F,G}	(A∧B)∨(C∧D)∨E	X satisfies P
Inner product述語暗号	Vector X	Vector Y	X·Y=0

Our Solution: Compact Functional Encryption (CFE)

☺ 1,2,3,4



Reference: N. Attrapadung, B. Libert. *Functional Encryption for Inner Product: Achieving Constant-Size Ciphertexts with Adaptive Security or Support for Negation.* In Public Key Cryptography (PKC 2010) Conference. May 2010. To appear.

FEは一般的に上記の利点1,3,4の性質を持つ（つまり、細かいアクセス制御が可能、クラウドプロバイダの信頼性の仮定は必要ない、安全性は暗号により保証される）。しかし、既存のFE方式は暗号文サイズが大きいという欠点(上記の2)がまだ課題として残った。本研究では、この課題を解決し上記のすべての利点の性質を持つシステムとして「Compact FE」を提案した。つまりCFEの特徴は**FEの従来の機能を失うことなく、暗号文サイズが小さい**（特にユーザ数やPolicy Pのサイズなどに依存しない）。さらに、既存のFEは弱いモデルでの安全性評価のみが行われていたのに対して、本研究は強い安全性モデル「Adaptive security」で安全性証明可能となった。提案方式の詳細は論文を参照。