安全性理論と方式の動向

パネル2「公開鍵暗号技術の最新動向について」

田中 圭介
東京工業大学 数理・計算科学専攻

CRYPTRECシンポジウム2010
2010年3月3日 コクヨホール(品川)

安全性理論

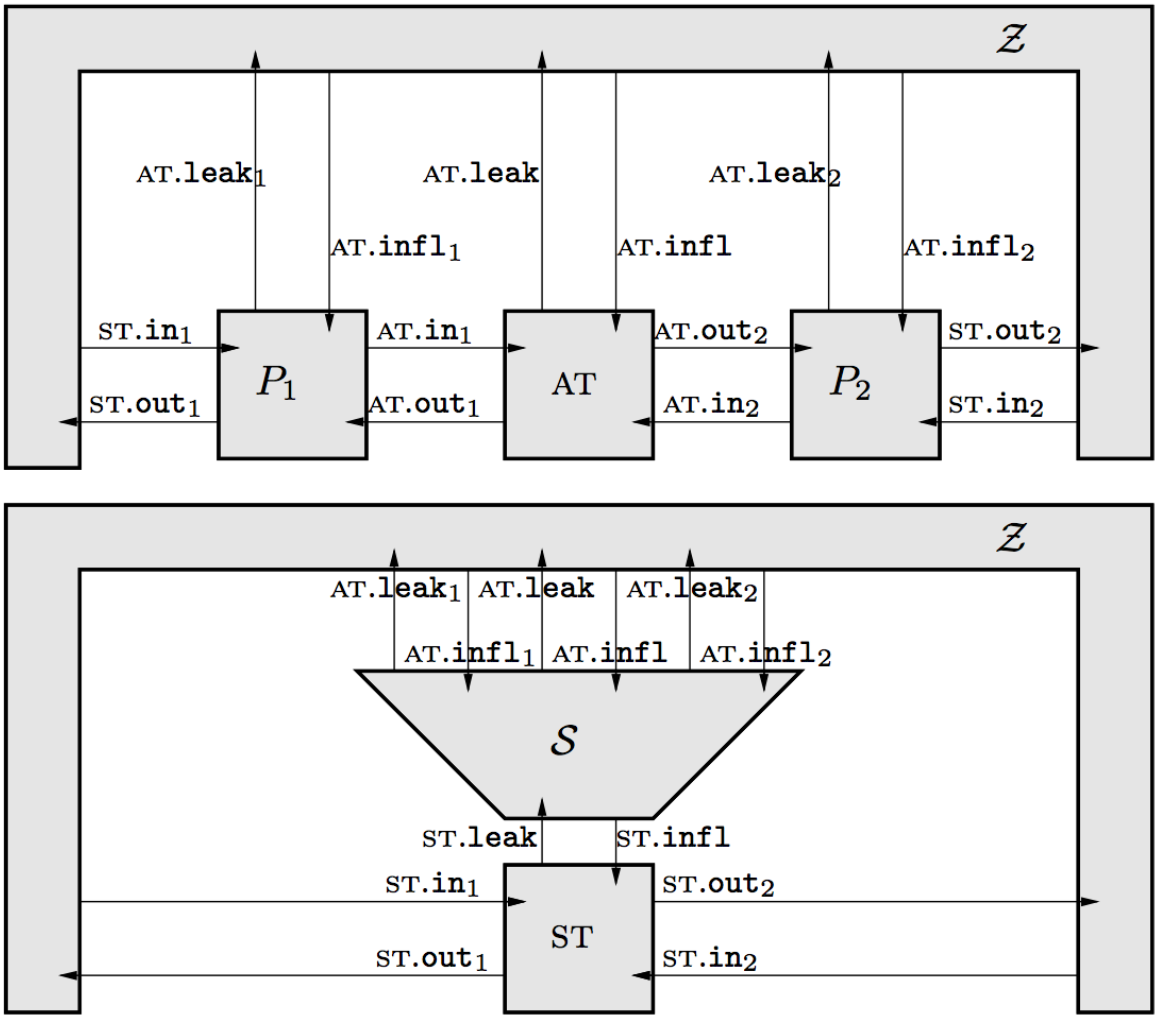
ランダム・オラクル モデル

- ハッシュ関数を理想化したもの
  - H: $\{0,1\}^* \rightarrow \{0,1\}^\lambda$
  - 出力は一様ランダムな値をとる。
- 一般的に、軽いシステムを構成可能
  - RSA-OAEP、RSA-FDH など

現状

- 様々なバリエーションが考察され、モデル上の方式の提案、モデルの限界が示されている。
  - プログラム可能性が取り除かれたモデル
  - 付加的情報が手に入るモデル
  - 情報漏洩を考慮したモデル
  - 安全性が弱められたモデル
    - 衝突困難性をもたない
    - 一方向性をもたない

UC安全性


$\mathcal{Z}$
AT.leak$_1$
AT.leak
AT.leak$_2$
AT.infl$_1$
AT.infl
AT.infl$_2$
ST.in$_1$
AT.in$_1$
AT.out$_2$
ST.out$_2$
P_1
AT
P_2
ST.out$_1$
AT.out$_1$
AT.in$_2$
ST.in$_2$
$\mathcal{Z}$
AT.leak$_1$
AT.leak
AT.leak$_2$
AT.infl$_1$
AT.infl
AT.infl$_2$
$\mathcal{S}$
ST.leak
ST.infl
ST.in$_1$
ST.out$_2$
ST
ST.out$_1$
ST.in$_2$

現状

- 基本的な構成要素に関する Ideal Functionality の定義は落ち着いている。
- 機能をもつ署名などのやや複雑なものについての Ideal Functionality も定義がされ始めている。
- Common Reference String や Random Oracle などのハイブリッドモデルは、複雑なものには、ほぼ必須。
- Indifferentiabilty は UC のバリエーションとみなせる。

漏洩を考慮した安全性

- サイド・チャネル攻撃を含む。
- 公開鍵暗号
  - 復号に使う秘密鍵、暗号化に使う乱数
- 署名
  - 署名生成に使う秘密鍵、署名生成に使う乱数
- モデルの例: f: SK $\rightarrow \{0,1\}^{\lambda}$: 任意の関数
  - モデルは多数提案されている。

ゲーム理論と安全性

- 暗号理論では通常、安全性証明を行う際に、パーティーの誰かが正しくプロトコルに従うことを仮定する。
  - 暗号: 送信者
  - 署名: 署名者
  - マルチパーティー・コンピュテーション: 参加プレイヤー半数など

さらに...

- 敵は、もてる力を最大限に発揮して攻撃すると仮定する。
  - 計算量的安全性: 任意の多項式時間
  - 攻撃失敗をおそれない。
  - マルチパーティー・コンピュテーション: 結託する敵は、仲間同士のコミュニケーションが完全に秘密に行うことができる。

現実には..

- アルゴリズムの記述どおりに行わない。
  - 適当に労力を省く。
  - 高速化などのために特殊な処理を行う。
- 参加プレイヤー全員が、自分の都合のいいように行動する。
- 攻撃するためのリソースは限られている。

現状

- 合理的なパーティーを考察する。
  - すべてのパーティーは自分の利得が最も高くなる行動を選択する。
- 秘密分散方式が主に研究されている。
  - 特殊な通信路、信頼できるパーティーを仮定。
  - 結託耐性、考慮する均衡点は限定的。

形式的検証可能アプローチ

- 記号論的アプローチと計算論的アプローチの融合を目指す。
- 論文、研究者ともに徐々に増えている。
- アルゴリズムの記述を自動検証用に書き換えるのはエキスパートの人には比較的簡単な作業 (Bogdan Warinschi によると)。

KEM/DEM パラダイム

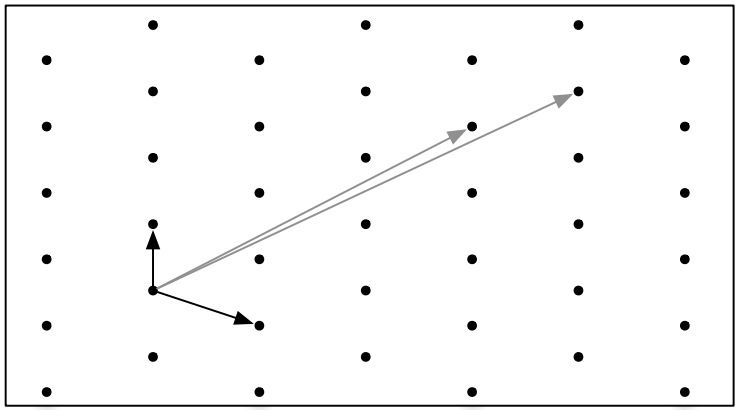
- KEM と DEM は組み合わせ自由。
- KEM: 鍵は平文と異なりランダムでよい。
- Tag-KEM/DEM などもある。
- ランダム・オラクルモデル、スタンダード・モデル、ともに多くの方式が提案されている。
- 組み合わせの解析も一通りされている。

方式

数論以外に用いられるもの

- 格子 (Lattice)
- ナップザック問題 (Knapsack, Subset Sum)
- 符号 (McEliece)
- 多変数多項式 (Multivariate Polynomial)
- 代数曲面 (Algebraic Surface)
- 組み紐 (Braid)

格子



- $\mathbb{R}^m$: m 次元ユークリッド空間
- $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$: $\mathbb{R}^m$ 上の n 個の線形独立なベクトルの集合 (格子の基底)
- 格子: $L(\mathbf{B}) = \{\sum_{i=1}^{n} x_i \mathbf{b}_i : x_i \in \mathbb{Z}\}$

格子ベース方式のカテゴリー

1. 平均/最悪ケース複雑さの等価性をもつもの
   - Ajtai-Dwork97，Regev05, Peikert-Waters08
2. 平均/最悪ケース複雑さの等価性をもたないもの
   - Goldreich-Goldwasser-Halevi97
   - NTRU(Hoffstein-Pipher-Silverman)98
3. 特殊機能をもつもの
   - Gentry09

おわりに

- 現実的な状況に対応するために、理論の歩み寄りが見えてきている。
  - 安全性証明のための理想化を弱める
  - 漏洩を考慮
  - ゲーム理論
- 格子ベースの暗号については効率を優先したい。