格子問題に基づく高い安全性をもつ認証方式

2008-01-24
SCIS 3D3-1

草川恵太/河内亮周/田中圭介（東京工業大学）

結果

- Stern認証方式の安全性についての考察
  - Stern 1993
- より高い安全性を持つこと格子問題の仮定から示す

概要

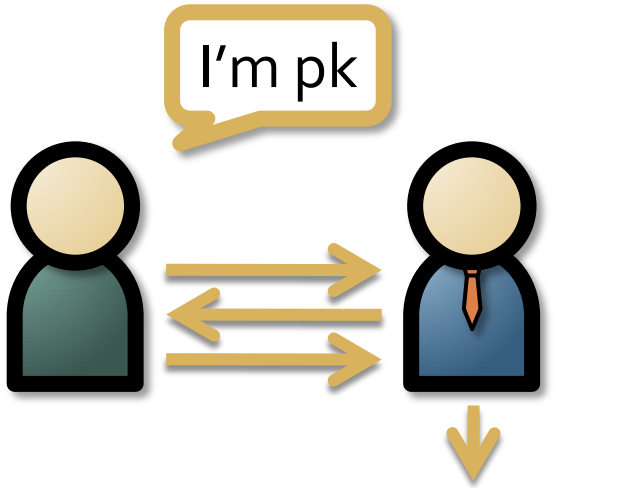
- 導入
  - 認証方式
  - 格子問題
- Stern認証方式
- 結果
  - Stern認証方式の安全性の解析
  - アドホック匿名認証方式の構成

認証方式

公開鍵認証のモデル

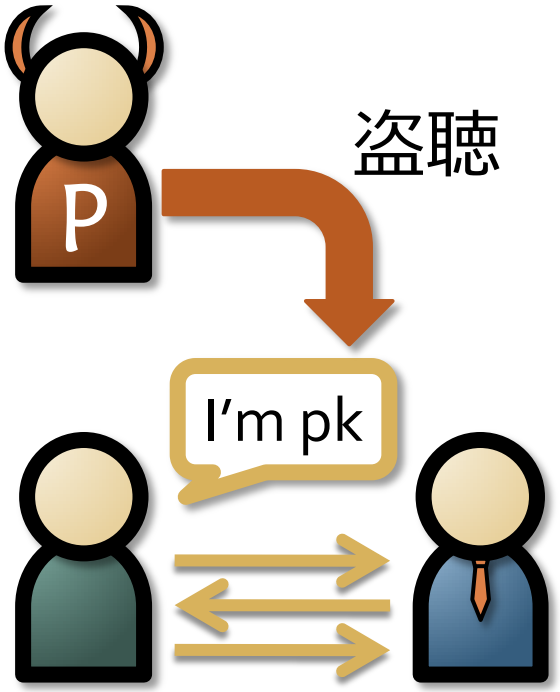
鍵生成

認証

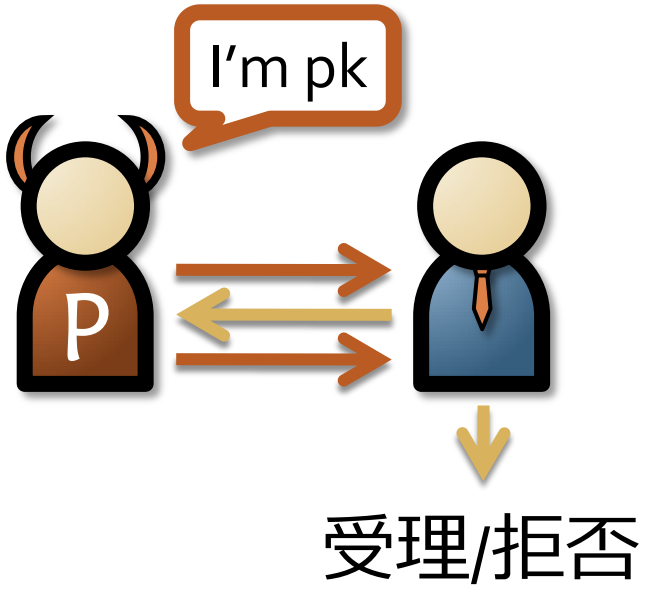


受動的攻撃

学習

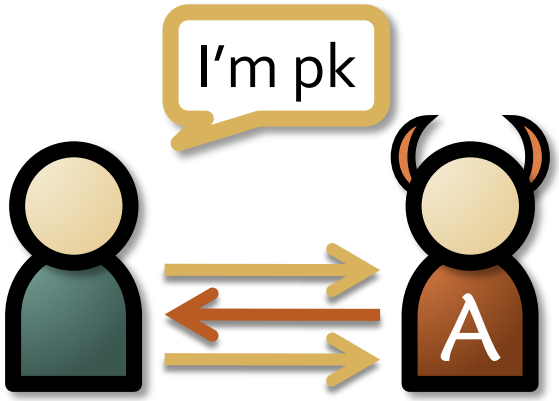


なりすまし

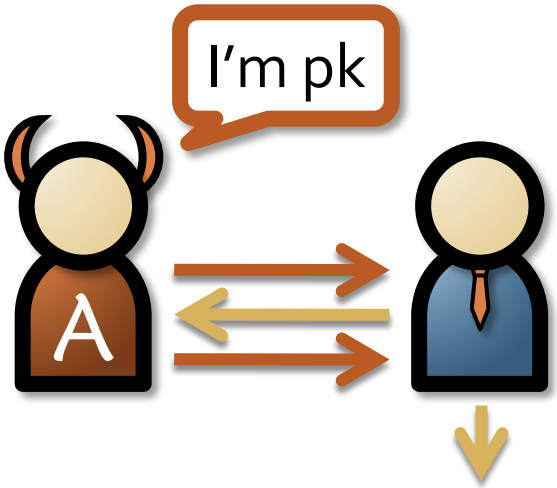


能動的攻撃

学習

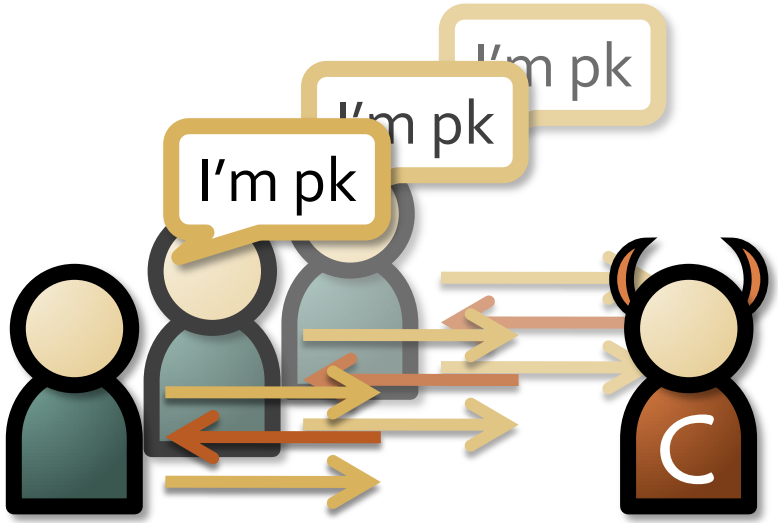


なりすまし



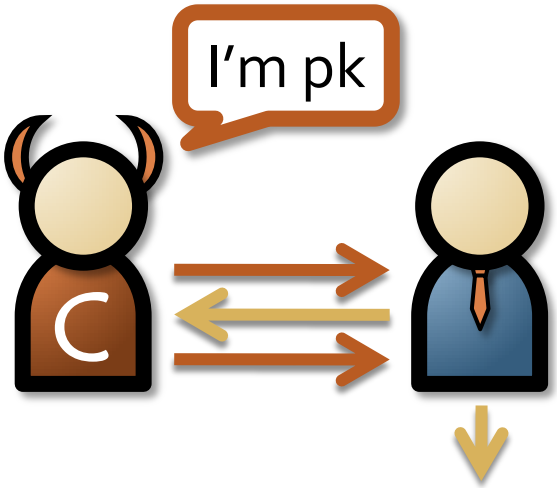
コンカレント攻撃

学習



証明者

なりすまし



受理/拒否

安全性の証明技法

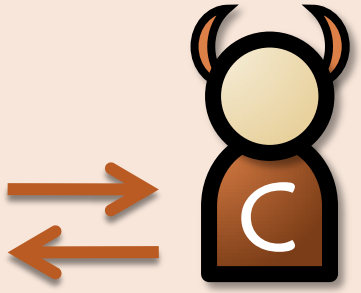
- コンカレント攻撃に対する安全性の場合
  - OneMoreDL等の仮定を用いる
  - 証拠識別不可能性(WI)を用いる

証明技法

Sim

ランダムインスタンス

1. 鍵 (pk, sk) を生成
2. 証明者をシミュレート
3. 敵Cを用いてsk'を得る
4. skとsk'から問題を解く

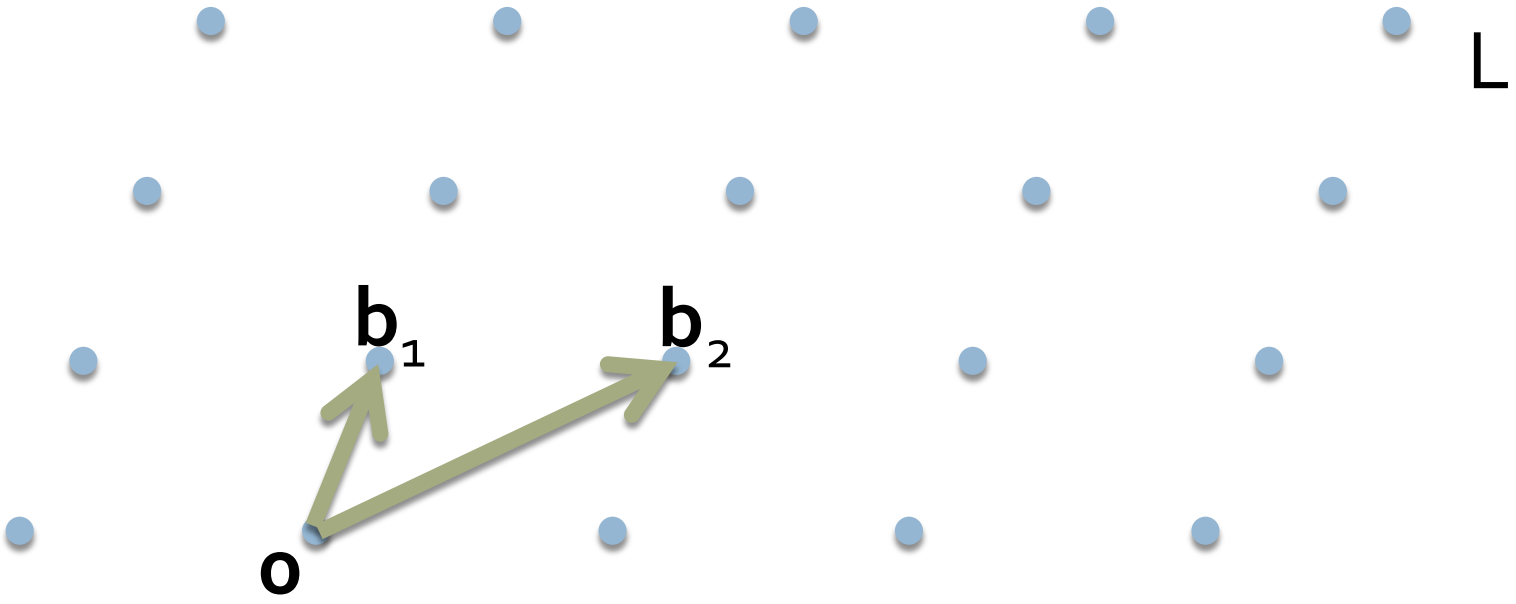


解

格子と格子問題

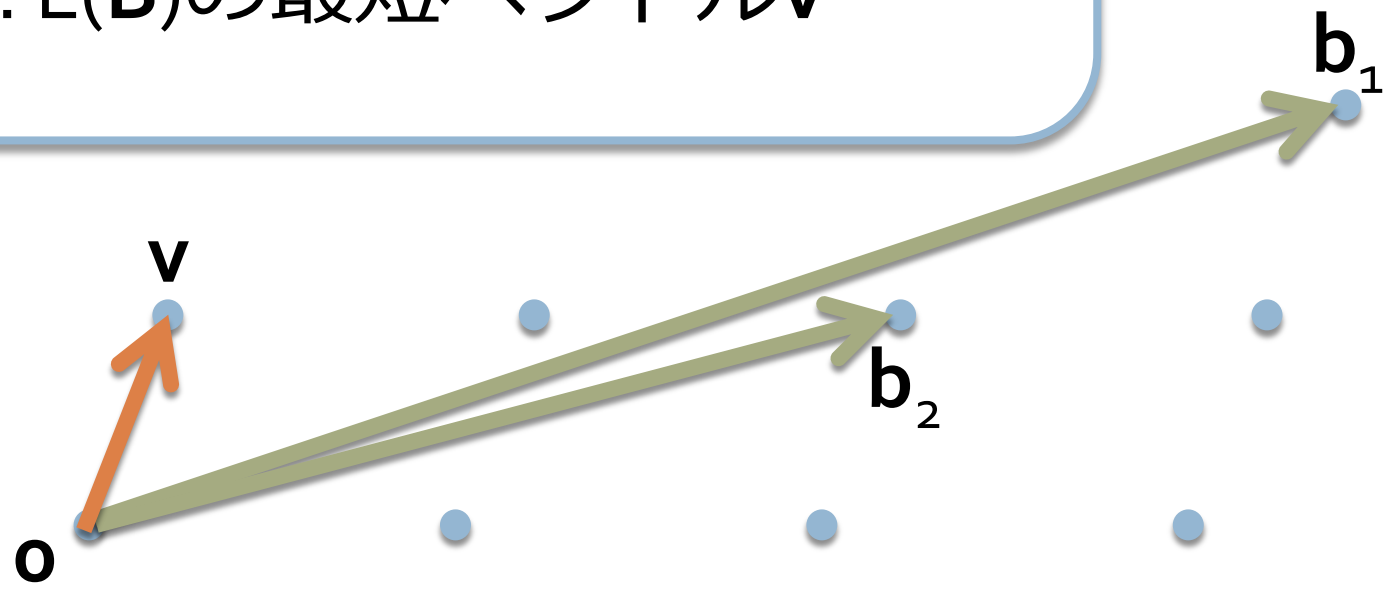
格子

- 基底: $\mathbf{B}=[\mathbf{b}_1,\ldots,\mathbf{b}_n]$ $(\mathbf{b}_i \in R^m)$
- 格子: $L(\mathbf{B}) := \{\Sigma_i \alpha_i \mathbf{b}_i \mid \alpha_i \in Z \text{ for all } i\}$
- R^mの離散な加法的部分群



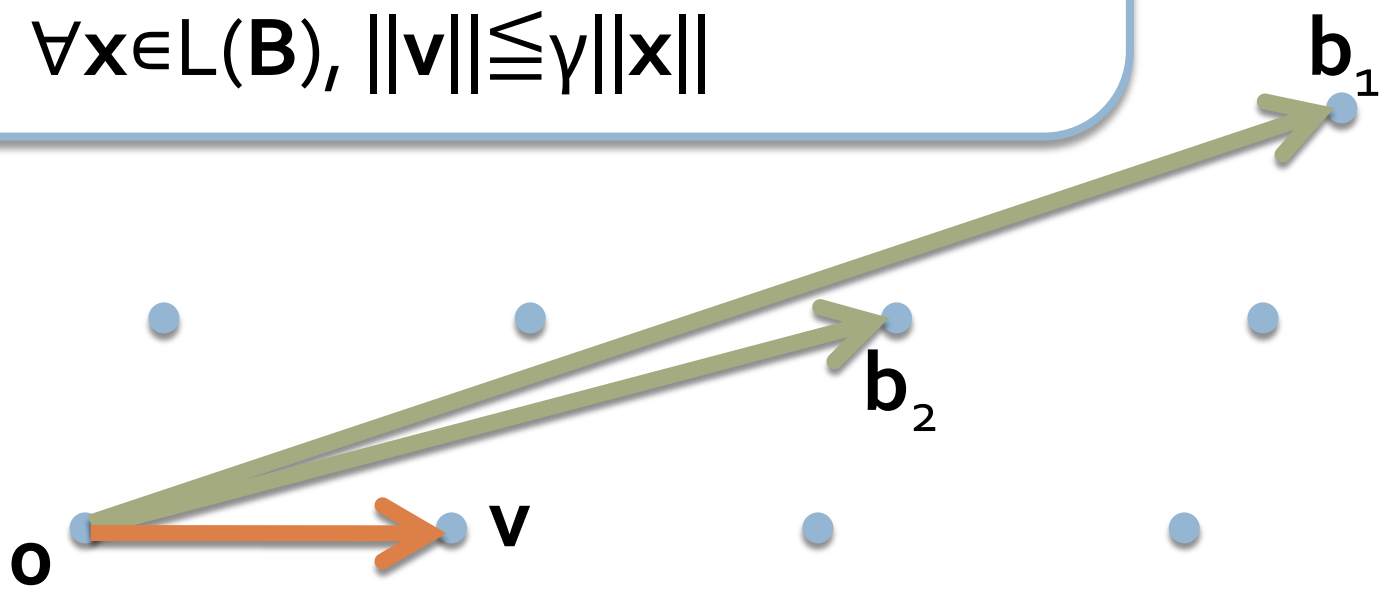
SVP (最短ベクトル問題)

SVP:
入力: **B**
出力: L(**B**)の最短ベクトル**v**



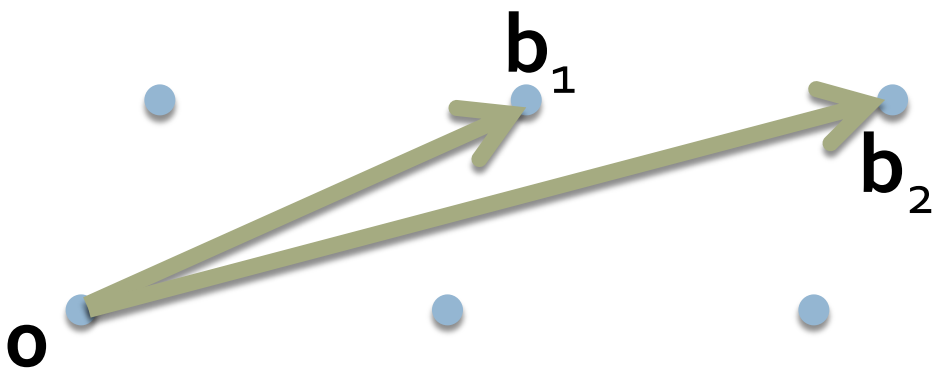
SVP_γ (近似版SVP)

SVP_γ:
入力: $\mathbf{B}$
出力: $\mathbf{v} \in L(\mathbf{B})$ s.t.
$\forall \mathbf{x} \in L(\mathbf{B}), \|\mathbf{v}\| \leqq \gamma \|\mathbf{x}\|$



GapSVP$_\gamma$ (ギャップ版)

GapSVP$_\gamma$:
入力: $\mathbf{B}$, t
出力: YES, if $\exists \mathbf{v} \in L(\mathbf{B})$ s.t. $\|\mathbf{v}\| \leqq t$
NO, if $\forall \mathbf{v} \in L(\mathbf{B})$, $\|\mathbf{v}\| > \gamma t$



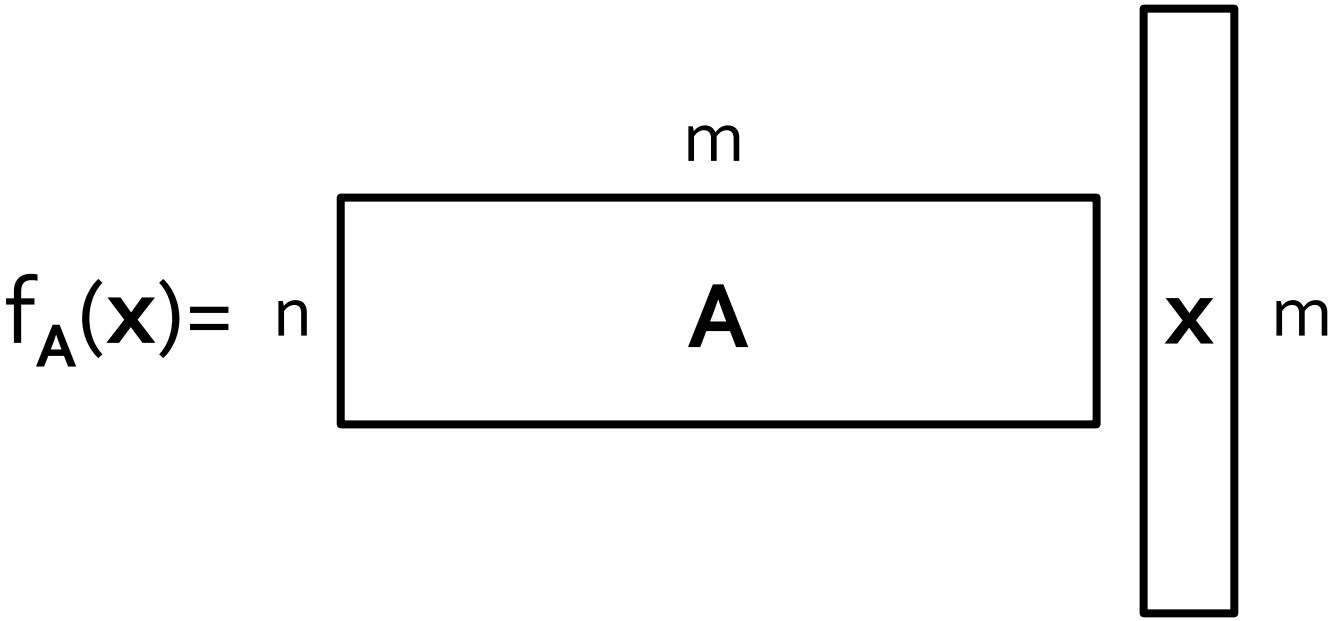
アプリケーション

- ハッシュ関数
- 公開鍵暗号
- 署名

格子ハッシュ

- $\mathcal{H}_{GL}=\{f_A \mid \mathbf{A}\in Z_q^{n*m}\}$

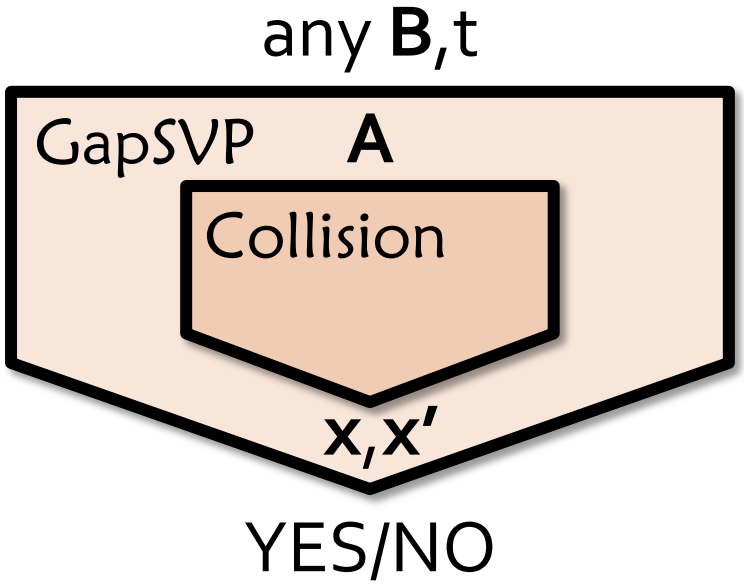
  $f_A(\mathbf{x})=\mathbf{A}\mathbf{x}$ $(\mathbf{x}\in\{0,1\}^m)$



格子ハッシュ

- $\mathcal{H}_{GL}=\{f_A \mid A \in Z_q^{n*m}\}$
- GapSVP$_\gamma$の最悪時が困難ならば
  $\mathcal{H}_{GL}$は衝突耐性を持つ

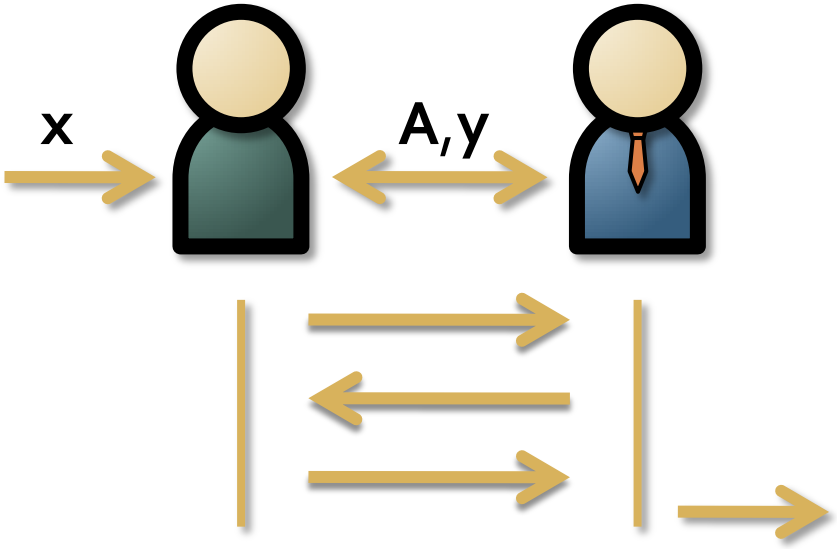
Collision:
入力: $A \in Z_q^{n*m}$
出力: $x \neq x' \in \{0,1\}^m$
s.t. $Ax=Ax'$



Stern認証方式

Stern認証方式

- Stern (1993, 1996)
  - シンドローム復号問題(SDP)に基づく
  - HVSZKArgument (POK)
  - 受動的攻撃に対して安全



Stern認証方式の仮定

SDP:
入力: $\mathbf{A} \in Z_q^{n*m}, \mathbf{y} \in Z_q^n$
出力: $\mathbf{x} \in \{0,1\}^m$ s.t. $\mathbf{Ax}=\mathbf{y}$

- $\mathcal{H}_{GL}$の一方向性を仮定している
  - $\mathcal{H}_{GL}=\{f_A \mid \mathbf{A} \in Z_q^{n*m}\}$

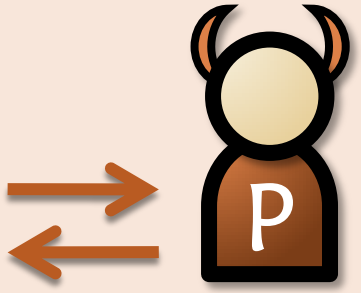
    $f_A(\mathbf{x})=\mathbf{Ax}$ $(\mathbf{x} \in \{0,1\}^m)$

Sternの証明

A, y

SDP

1. 証明者をシミュレート
2. 敵Pを用いて**x′**を得る (**Ax′=y**)
3. **x′**を出力する



x′

結果

Stern認証方式の安全性

- コンカレント攻撃に耐えられないのか?

- $\mathcal{H}_{GL}$はGapSVP$_\gamma$仮定のもと衝突耐性アリ
  - $\mathcal{H}_{GL}=\{f_{\mathbf{A}} \mid \mathbf{A}\in Z_q^{n*m}\}$

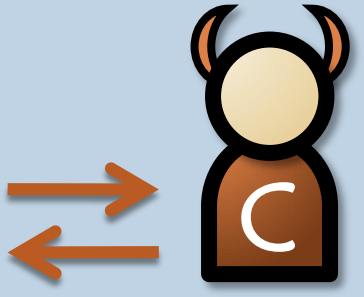
    $f_{\mathbf{A}}(\mathbf{x})=\mathbf{A}\mathbf{x}$ $(\mathbf{x}\in\{0,1\}^m)$

証明

A

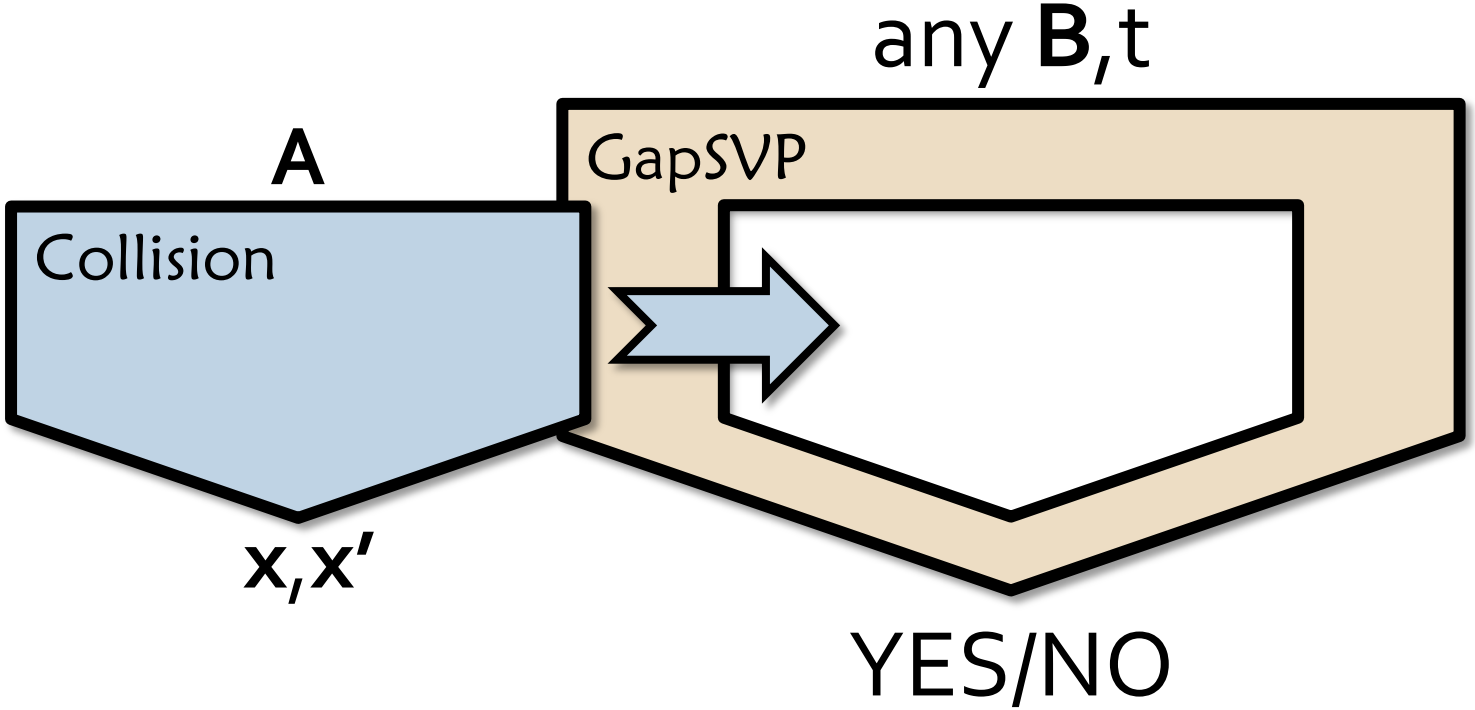
Collision

1. 鍵 ($y=Ax$, x) を生成
2. 証明者をシミュレート
3. 敵Cを用いてx'を得る ($Ax'=y$)
4. xとx'を出力する



x, x'

証明 (続き)

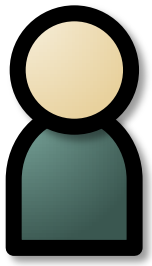


GapSVP$_\gamma$の最悪時が困難ならば
Stern認証方式はコンカレント攻撃に対して安全

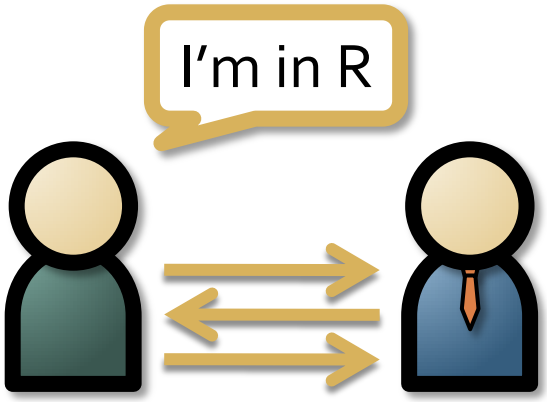
アドホック匿名認証

鍵生成

認証



pk, sk



$R=(pk_1,\ldots,pk_l)$

受理/拒否

比較

	IDs	仮定	安全性
Stern	ID	SDP 平均時	受動的
Ours1	ID	GapSVP$_\gamma$ 最悪時	コンカレント
Ours2	AID	GapSVP$_\gamma$ 最悪時	コンカレント

※ ID=認証方式, AID=アドホック匿名認証方式

参考文献

- Stern
  - A new paradigm for public key identification (CRYPTO 1993, IEEE Trans. on IT 1996)
- Ajtai
  - Generating hard Instances of lattice problems (STOC 1996)
- Micciancio and Regev
  - Worst-case to average-case reductions based on Gaussian measure (FOCS 2004, SIAM J. on Comp. 2007)