Proofs of Plaintext Knowledge for the Regev Cryptosystems

草川恵太/河内亮周/田中圭介/東京工業大学

お詫び

予稿集に載っている結果には
間違いがあります。
詳しくはフルヴァージョンで。

http://www.is.titech.ac.jp/research/research-report/C/C-236.pdf

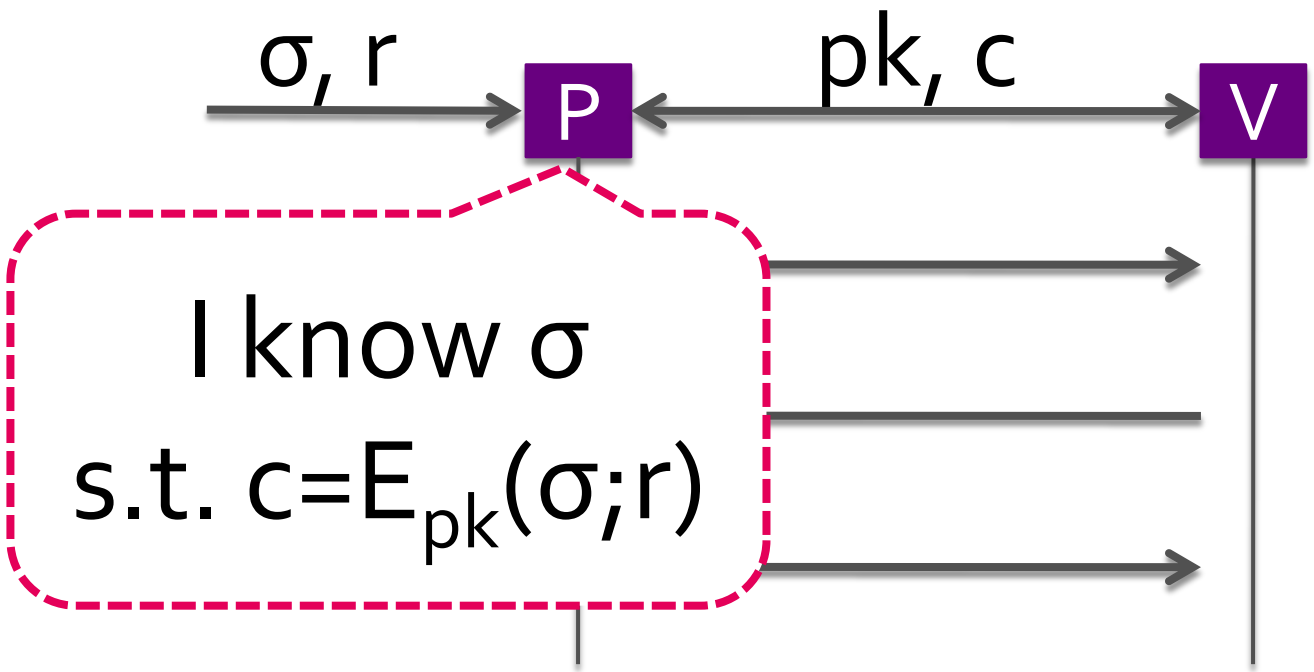
発表の流れ

- 平文知識証明
- 既存の結果 - Goldwasser and Kharchenko
- 今回の結果
  - 具体例:Regevo4暗号の平文知識証明

平文知識証明

平文知識証明

- “暗号文cの平文σを知っている”ことを証明するプロトコル



平文知識証明

- 数論系では既に存在する
- 安全性を高める重要なツールでもある
  - IND-CPA+PPK→Interactive IND-CCA1
  - IND-CPA+NI-PPK→IND-CCA1
  - IND-CPA+NI-NM-PPK→IND-CCA2
  - 直観的には, 復号オラクルを使う意味がなくなるので上の関係が言える

既存の結果 ー
Goldwasser and Kharchenko

Goldwasser and Kharchenko

- Goldwasser and Kharchenko (TCC 2005)
- "Proof of Plaintext Knowledge for the Ajtai-Dwork Cryptosystem"
  - 証明者は（Ajtai-Dwork暗号の）暗号文の平文を知っていることを証明する
  - 入力: 公開鍵pkと暗号文**c**
  - 証拠: 平文σと乱数r (**c**=$E_{pk}(\sigma;r)$)
  - 5ラウンド公開コインCZKPoK

Goldwassr and Kharchenko

- 構成に以下のアイデアを利用
  - Nguyen and Stern (CRYPTO 1998)
    - AD暗号とGapCVP$_\gamma$の関係
  - Micciancio and Vadhan (CRYPTO 2003)
    - GapCVP$_\gamma$に関するゼロ知識証明
- Regev04暗号用の平文知識証明が未解決

今回の結果

やったこと

- Regev04暗号とRegev05暗号に対する平文知識証明を構成した
  - 具体的にはRegev04暗号とGapCVP, Regev05暗号とGapCVPの関係を示した
  - GK05ではNguyen and Sternを使ってAD暗号とGapCVPの関係を示している
  - 全体の構成はGK05と同じ

Regev04暗号

- Regev04
  - 秘密鍵: d
  - 公開鍵: $(a_1,\ldots,a_m,k,N=2^{8n^2})$
    - $\mathrm{dist}(a_i/d,Z)$と$\mathrm{dist}(N/d,Z)$は小さい
    - a_k/dは奇数周辺かつa_kは偶数
  - 暗号化: 平文σと乱数r
    - $c=\sigma a_k/2+\Sigma_i\, r_i a_i \bmod N$
  - 復号: 暗号文c
    - $\mathrm{dist}(c/d,Z)<1/4$ならば0に, そうでないなら1に

R04とGapCVP$_\gamma$

- (pk,c)とGapCVP$_\gamma$の関係
- GapCVP$_\gamma$
  - 入力: (**B**,**x**,t)
  - YES: $\|\mathbf{Bw}-\mathbf{x}\| \leqq t$となる$\mathbf{w} \in Z^n$が存在
  - NO: 任意の$\mathbf{w} \in Z^n$で$\|\mathbf{Bw}-\mathbf{x}\| \geqq \gamma t$
  - 近似度γのCVPの決定版

Ro4とGapCVP$_\gamma$

- $c=\Sigma_i r_i a_i \bmod N=\alpha N+\Sigma_i r_i a_i$ならば
  - （cが正しいoの暗号文ならば）
- $\|\mathbf{x}_c'-\mathbf{x}_c\|^2 = \alpha^2+K_2^2\Sigma_i r_i^2$ が小さい

$$\mathbf{B}_{pk}=\begin{bmatrix} K_1N & K_1a_1 & \cdots & K_1a_m \\ 1 & & & \\ & K_2 & & \\ & & \ddots & \\ & & & K_2 \end{bmatrix},\quad \mathbf{x}_c=\begin{bmatrix} K_1c \\ o \\ o \\ \vdots \\ o \end{bmatrix},\quad \mathbf{x}_c'=\begin{bmatrix} K_1c \\ \alpha \\ K_2r_1 \\ \vdots \\ K_2r_m \end{bmatrix}$$

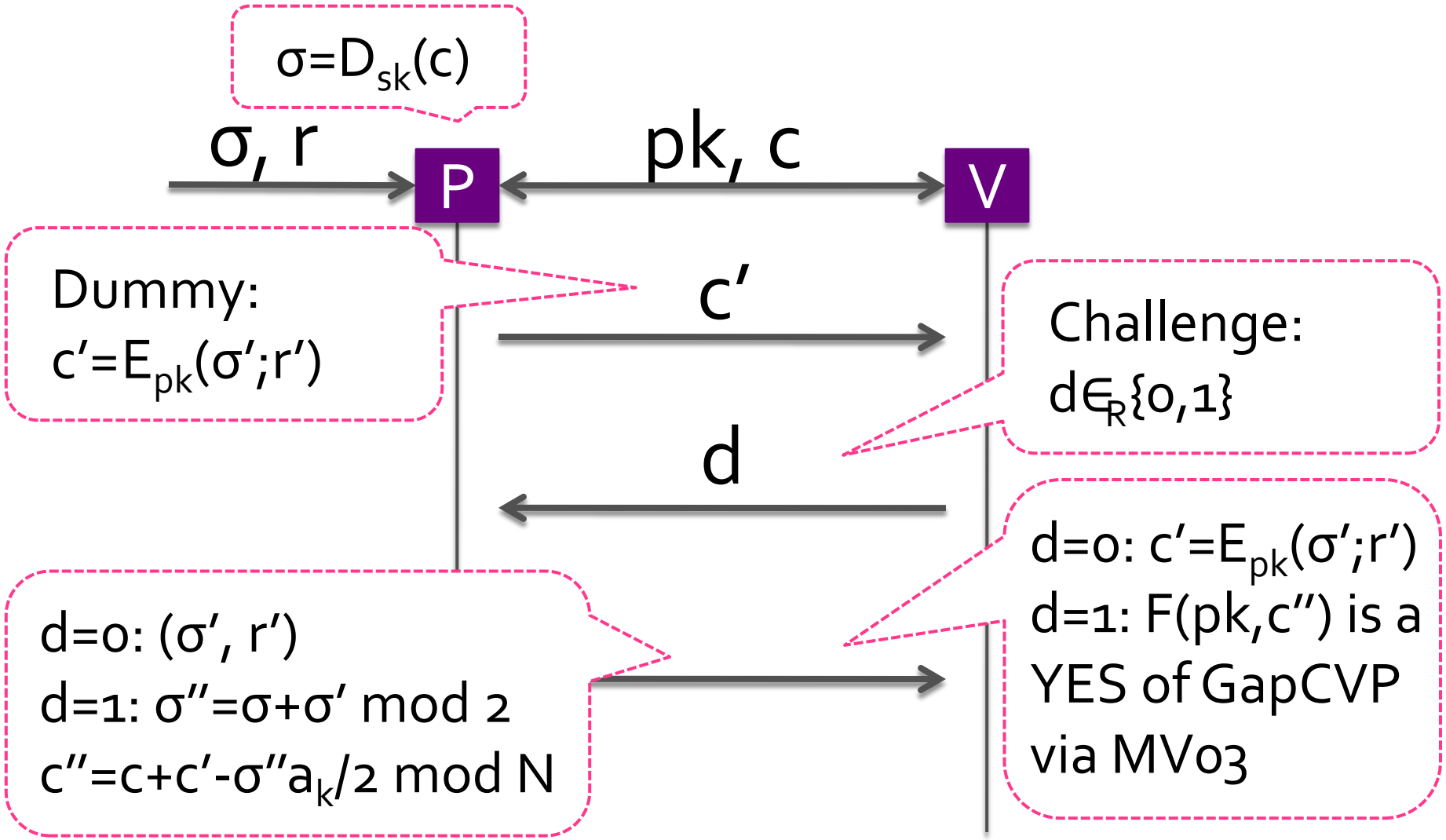
R04とGapCVP$_\gamma$

- F(・,・)と適当なtについて
- cが正しい0の暗号文
  - ➔F(pk,c)はYESインスタンス
- cが1に復号される暗号文
  - ➔F(pk,c)はNOインスタンス
- cが正しい1の暗号文
  - ➔F(pk,c-a_k/2 mod N)はYESインスタンス
- cが0に復号される暗号文
  - ➔F(pk,c-a_k/2 mod N)はNOインスタンス

Ro4とGapCVP$_\gamma$

- F(・,・)と適当なtについて
- c := c_1+c_2 mod N
- 証明者が"cはσの暗号文"と主張
- c_1とc_2が正しいσ_1とσ_2の暗号文かつ$\sigma=\sigma_1+\sigma_2$ mod 2
  - →F(pk,c-σa_k/2 mod N)はYESインスタンス
- そうでなければ
  - →F(pk,c-σa_k/2 mod N)はNOインスタンス

平文知識証明


σ=D_sk(c)
σ, r
P
pk, c
V
Dummy:
c′=E_pk(σ′;r′)
c′
Challenge:
d∈_R{0,1}
d
d=0: (σ′, r′)
d=1: σ″=σ+σ′ mod 2
c″=c+c′-σ″a_k/2 mod N
d=0: c′=E_pk(σ′;r′)
d=1: F(pk,c″) is a
YES of GapCVP
via MV03

まとめ

- Regevo4暗号とRegevo5暗号に対する平文知識証明を構成した
  - GKo5に基づいている
- 未解決問題
  - Non-Malleableな平文知識証明
  - Non-Interactiveな平文知識証明

参考文献

- Goldwasser and Kharchenko (TCC 2005)
  - Proof of Plaintext Knowledge for the Ajtai-Dwork Cryptosystem
- Micciancio and Vadhan (CRYPTO 1993)
  - Statistical Zero-Knowledge Proofs with Efficient Provers: Lattice Problems and More
- Nguyen and Stern (CRYPTO 1998)
  - Cryptanalysis of the Ajtai-Dwork Cryptosystem
- Regev (JACM 2004)
  - New Lattice Based Cryptographic Constructions
- Regev (STOC 2005)
  - On Lattices, Learning with Errors, Random Linear Codes, and Cryptography