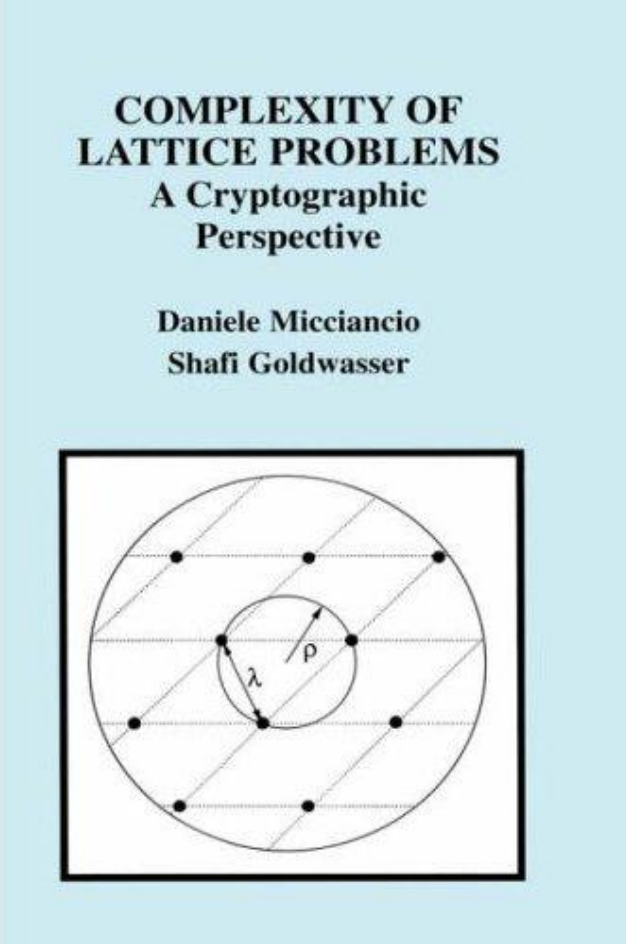
Lattice-Based Cryptosystems, Proof of Knowledge on Its Secret Key, and Signature Schemes

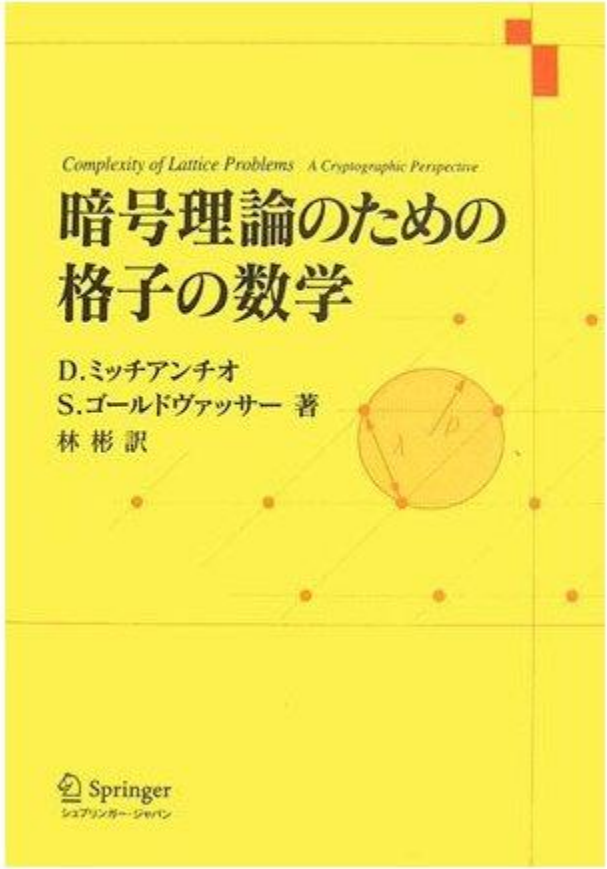
草川恵太/河内亮周/田中圭介/東京工業大学

格子暗号
知識証明
署名

草川恵太/河内亮周/田中圭介/東京工業大学

格子については説明しません





動機 — 既存方式

格子暗号

- 格子暗号(A) - GGH, NTRU
  - 多ビット公開鍵暗号
  - 安全性がよく分からない
- 格子暗号(B) - Ajtai-Dwork, Regev04, Regev05
  - 1ビット公開鍵暗号
  - 安全性が格子問題の最悪時から保証できる

二種類の格子暗号と署名

- 格子暗号(A)を使った署名
  - GGH署名, NTRUSign
    - 安全性がよく分からない
  - Nguyen and Regev (Eurocrypt 2006)
    - GGH署名, NTRUSign (without purtarbation)を攻撃
- 格子暗号(B)の方から署名ができないか?
  - 認証方式ができれば署名方式もできる
    - Fiat-Shamir変換を使う
  - 既存の認証方式は使えないのか?

既存の認証方式

- 格子
  - Goldreich and Goldwasser (2000)
    - coGapCVP/ZK Proof
  - Micciancio and Vadhan (2003)
    - GapCVP/ZK Proof
  - Hayashi and Tada (2006, SCIS 2007 3D2-5)
    - BNELVP/Witness Hiding
- 符号
  - Stern (1996)
    - Syndrome Decoding Problem (SDP)/ZK Argument

認証機能を持つ格子暗号

- 既存方式の公開情報が暗号の公開鍵として使えるかどうかが分からない
- 格子暗号(B)の公開鍵を使って認証方式を構成したい
  - 認証方式ができれば署名方式もできる

Regevo5暗号の紹介と改造

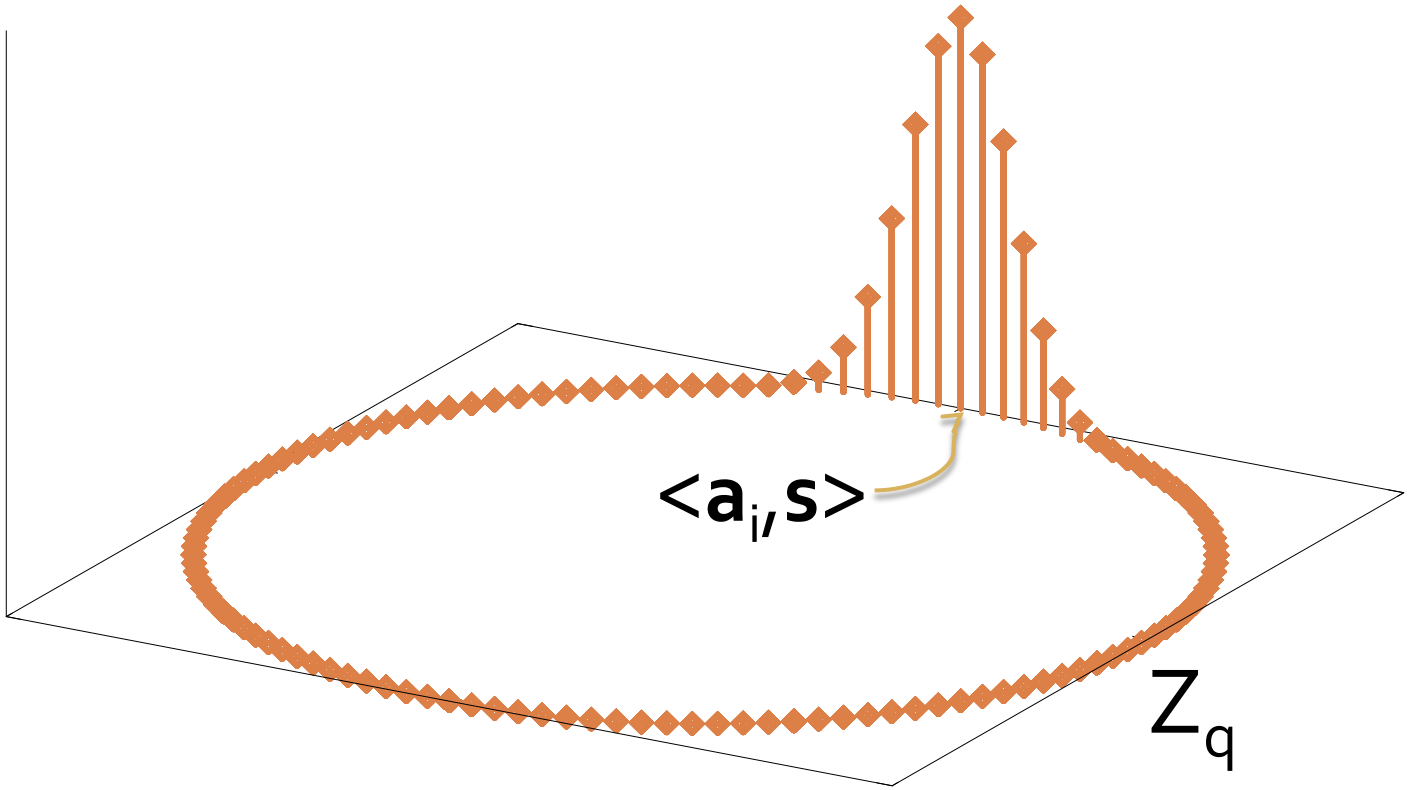
Regev05暗号－1

- Regev (STOC 2005)
- 以下R05と呼ぶ
- 1ビット公開鍵暗号方式
- 基となる問題
  - 古典帰着だとLWE_{q,ψ_α}の最悪時
    - LWE_{q,ψ_α}: 学習問題の一種
  - 量子帰着だと$SVP_{O\tilde{}(n)}$の最悪時
    - $SVP_{O\tilde{}(n)}$:近似度O~(n)の最短ベクトル問題

図：R05 - 鍵

秘密鍵: $\mathbf{s} \in Z_q^n$

公開鍵: $\mathbf{a}_i \in Z_q^n$, $b_i = \langle \mathbf{a}_i, \mathbf{s} \rangle + e_i$ $(i = 1, \ldots, m)$

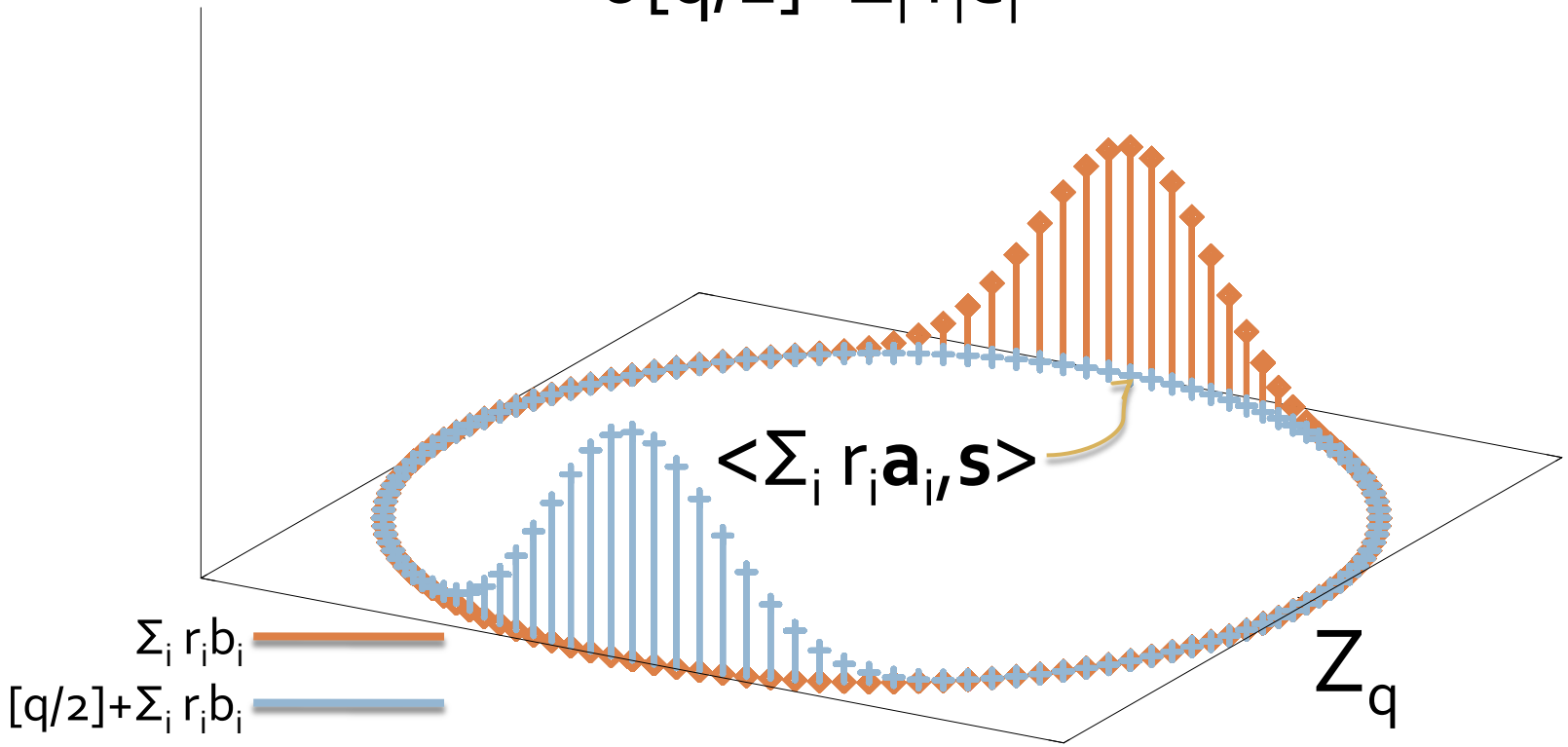


図：R05 - 暗号文

暗号化: $(\mathbf{a},b)=(\Sigma_i r_i\mathbf{a}_i,\ \sigma[q/2]+\Sigma_i r_i b_i)$

復号: $b-\langle\mathbf{a},\mathbf{s}\rangle=\sigma[q/2]+\Sigma_i r_i b_i-\langle\Sigma_i r_i\mathbf{a}_i,\mathbf{s}\rangle$

$=\sigma[q/2]+\Sigma_i r_i e_i$



R05 – 鍵について

- 秘密鍵: $\mathbf{s} \in Z_q^n$
- 公開鍵: $\mathbf{a}_i \in Z_q^n$, $b_i = \langle \mathbf{a}_i, \mathbf{s} \rangle + e_i \ (i=1,\ldots,m)$

$$\mathbf{b} = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix} = \begin{bmatrix} {}^t\mathbf{a}_1 \\ \vdots \\ {}^t\mathbf{a}_m \end{bmatrix} \mathbf{s} + \begin{bmatrix} e_1 \\ \vdots \\ e_m \end{bmatrix}$$

$$= \mathbf{A}\mathbf{s} + \mathbf{e}$$

生成行列　メッセージ　エラー

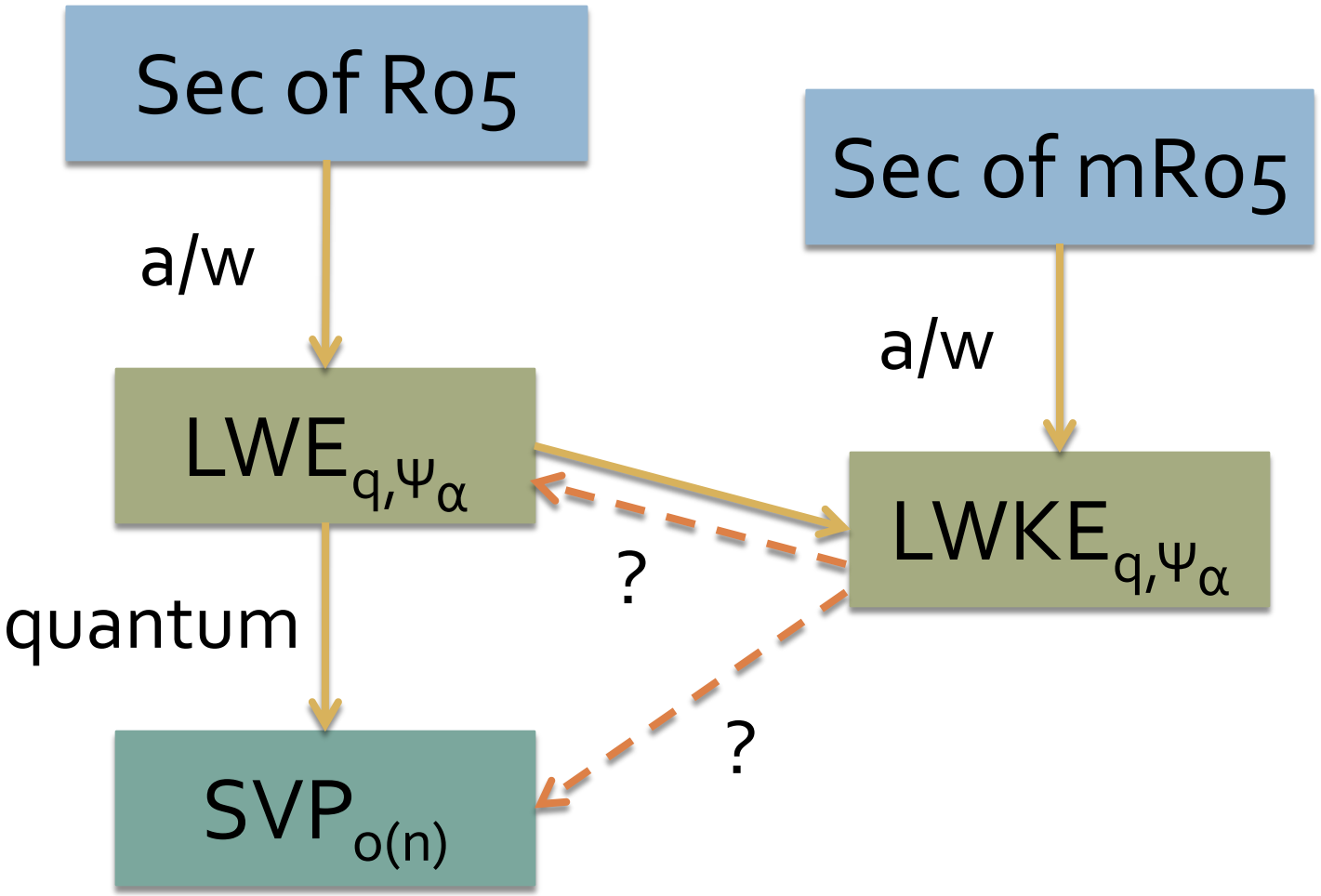
R05の改造 – mR05

- R05の公開鍵は**A**と**b=As+e**
- **A**のパリティ検査行列**H**が存在する
  - **Hb=HAs+He=He**
- 改造の方針:証拠を0-1ベクトルにする

R05の改造 – mR05

- 改造の方針:証拠を0-1ベクトルにする
- 秘密鍵: $\mathbf{s} \in Z_q^n$, $\mathbf{s}' \in \{0,1\}^{m_1}$ s.t. $w_H(\mathbf{s}') = m_2$
- 公開鍵: $\mathbf{A} = {}^t[\mathbf{a}_1, \ldots, \mathbf{a}_m], \mathbf{E} = [\mathbf{e}_1, \ldots, \mathbf{e}_{m_1}], \mathbf{b} = \mathbf{As} + \mathbf{Es}'$
- すると $\mathbf{Hb} = \mathbf{HAs} + \mathbf{HEs}' = \mathbf{HEs}'$
  - $\mathbf{s}'$を証拠として知識証明を行う
  - Sternの知識証明のインスタンスになっている
    - $w_H(\mathbf{x}) = k$, $\mathbf{Hx} = \mathbf{y}$となる$\mathbf{x}$を探す問題

mR05とR05の安全性の比較

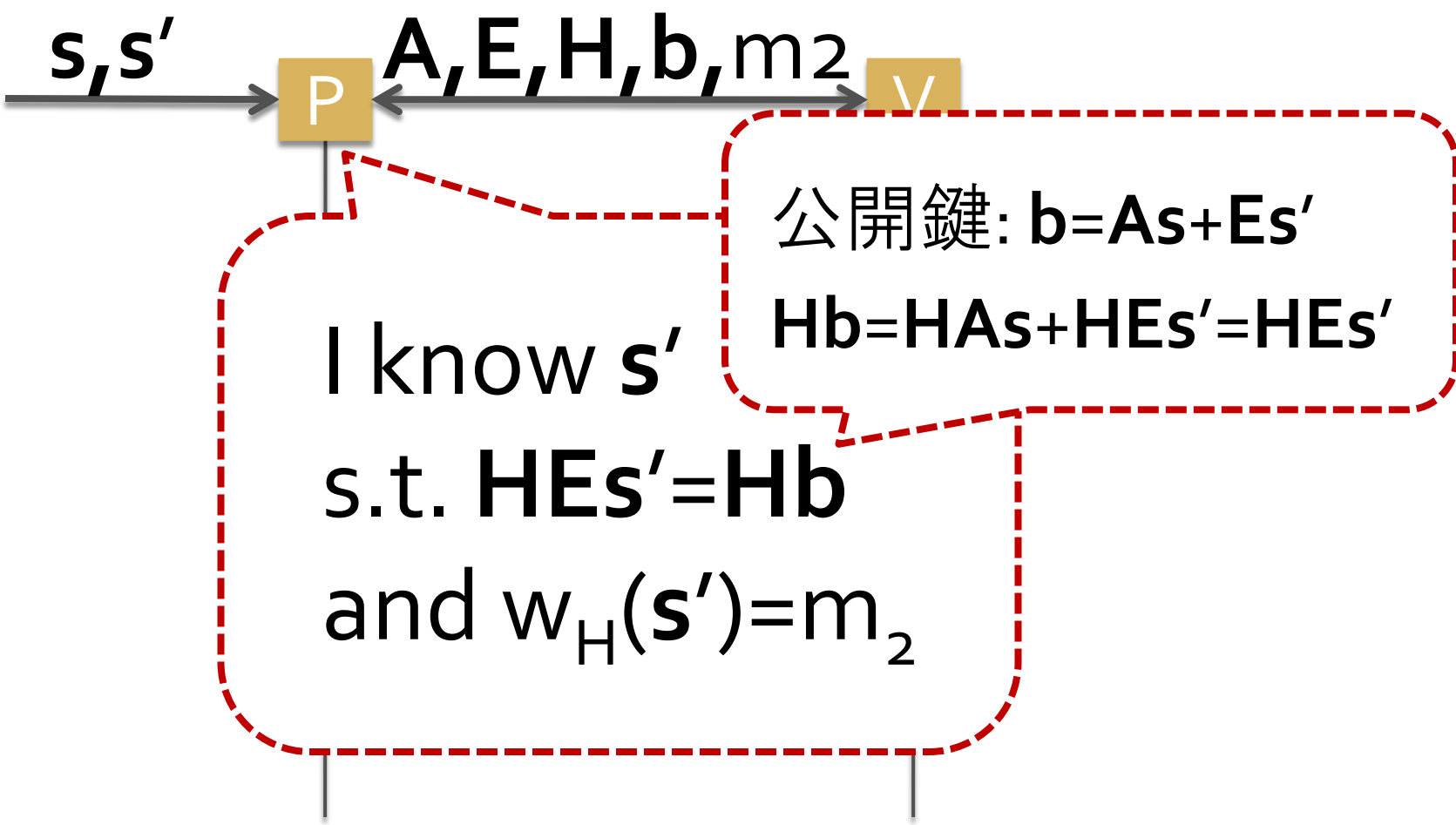


秘密鍵についての知識証明

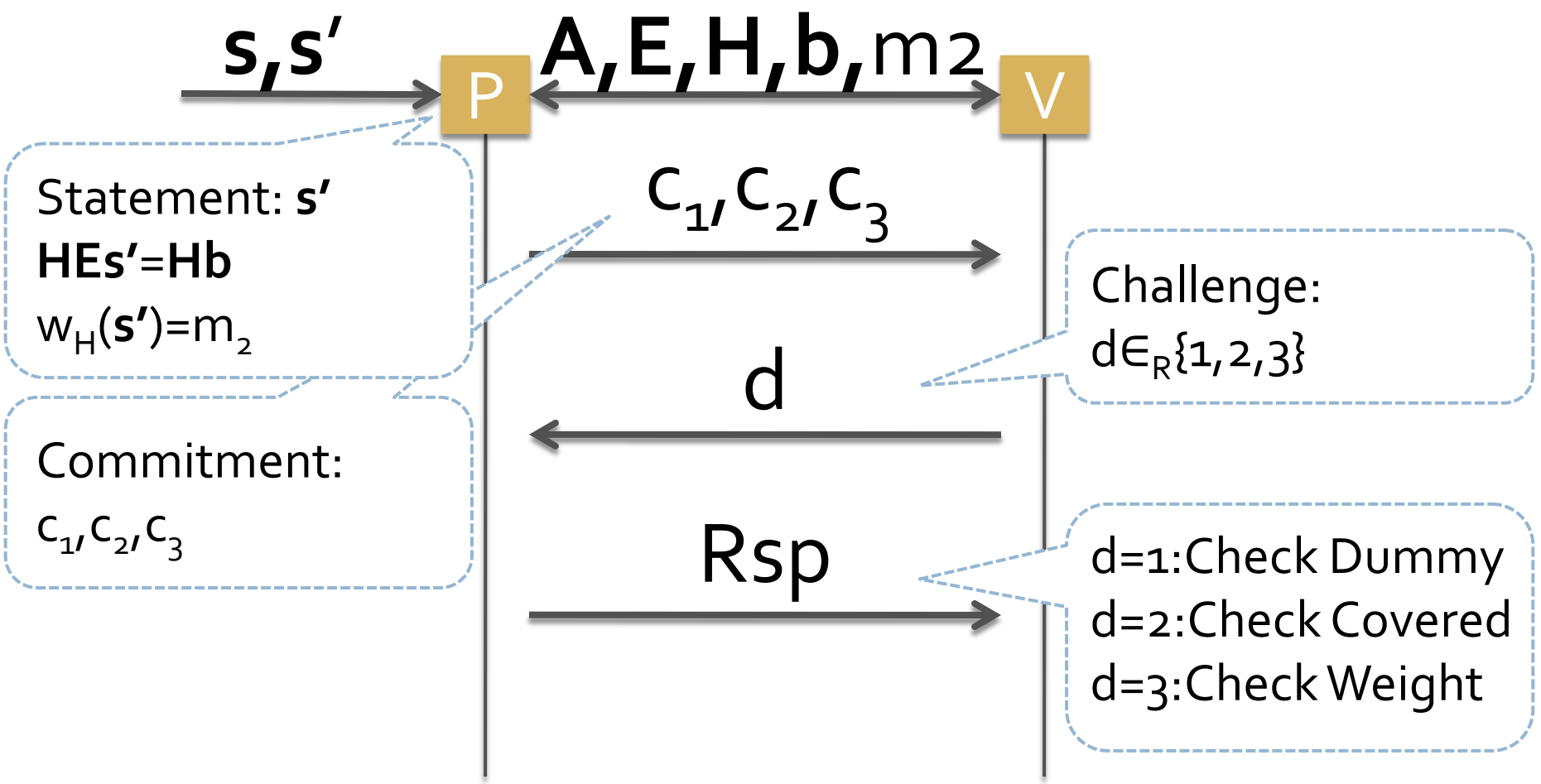
Syndrome Decoding Problem

- Stern (1996)
  - SDPに対するゼロ知識アーギュメントの構成
  - stat.-hiding comp.-binding commitmentを利用
- Berlekamp, McEliece, van Tilborg (1978)
  - SDPのNP困難性

プロトコル


s,s′
P
A,E,H,b,m2
V
公開鍵: b=As+Es′
Hb=HAs+HEs′=HEs′
I know s′
s.t. HEs′=Hb
and $w_H(s')=m_2$

プロトコル 概要

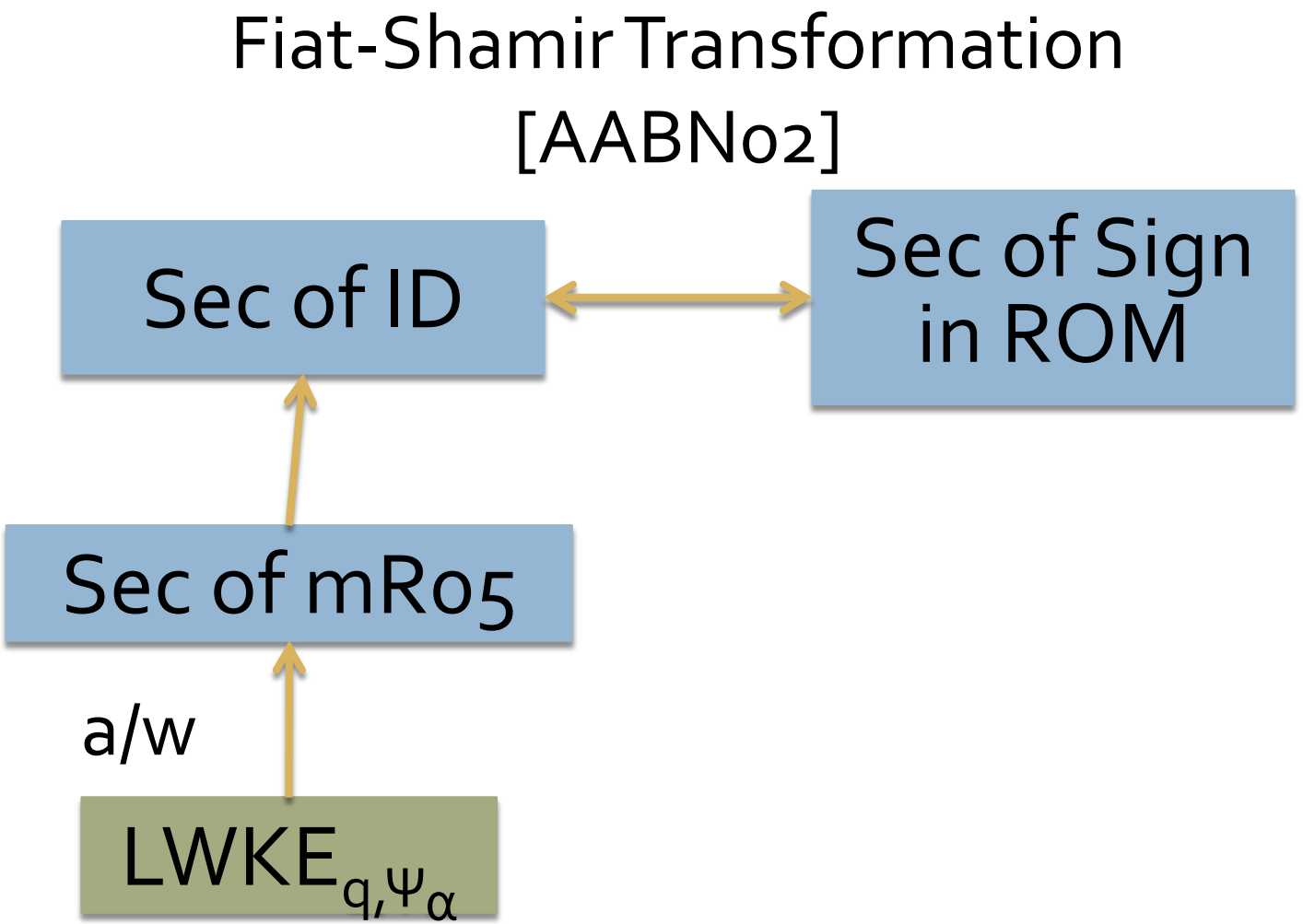

s,s′
A,E,H,b,m2
P
V
Statement: s′
HEs′=Hb
$w_H(s')=m_2$
Commitment:
c_1,c_2,c_3
c_1,c_2,c_3
Challenge:
$d \in_R \{1,2,3\}$
d
Rsp
d=1:Check Dummy
d=2:Check Covered
d=3:Check Weight

署名方式

署名方式

- 知識証明を並列に行うと認証方式になる
- 認証方式からFiat-Shamir変換で署名方式へ
  - mR05の公開鍵で検証可能
  - mR05の秘密鍵で署名可能

署名方式の安全性


Fiat-Shamir Transformation
[AABN02]
Sec of ID
Sec of Sign in ROM
Sec of mR05
a/w
LWKE$_{q,\Psi_\alpha}$

まとめ

- 結果
  - 暗号方式mRo5の提案
    - mRo5の安全性は$\mathrm{LWKE}_{q,\psi_\alpha}$の最悪時から保証
    - Sternの知識証明を利用可能
  - 署名の構成
    - 署名の安全性も$\mathrm{LWKE}_{q,\psi_\alpha}$の最悪時から保証
- 未解決問題
  - Ro5の秘密鍵に対するゼロ知識証明
  - mRo5の安全性
    - $\mathrm{LWKE}_{q,\psi_\alpha}$から$\mathrm{LWE}_{q,\psi_\alpha}$または$\mathrm{SVP}_\gamma$への帰着

参考文献

- Abadalla, An, Bellare, and Namprepre (EUROCRYPT 2002)
  - From Identification to Signatures via the Fiat-Shamir Transform: Minimizing Assumptions for Security and Forward-Security
- Hayashi and Tada (ISITA 2006, SCIS 2007)
  - A Public-Key Identification Scheme based on a New Lattice Problem
- Micciancio and Vadhan (CRYPTO 1993)
  - Statistical Zero-Knowledge Proofs with Efficient Provers: Lattice Problems and More
- Nguyen and Regev (EUROCRYPT 2006)
  - Learning a Parallelepiped: Cryptanalysis of GGH and NTRU Signatures
- Regev (STOC 2005)
  - On Lattices, Learnin with Errors, Random Linear Codes, and Cryptography
- Stern (CRYPTO 1993, IEEE Trans. on IT, 1996)
  - A New Paradigm for Public Key Identification