計算量的ファジィ抽出器

安永 憲司

金沢大学

湯澤孝介、満保雅浩（金沢大学）との共同研究にもとづく

ファジィ抽出器

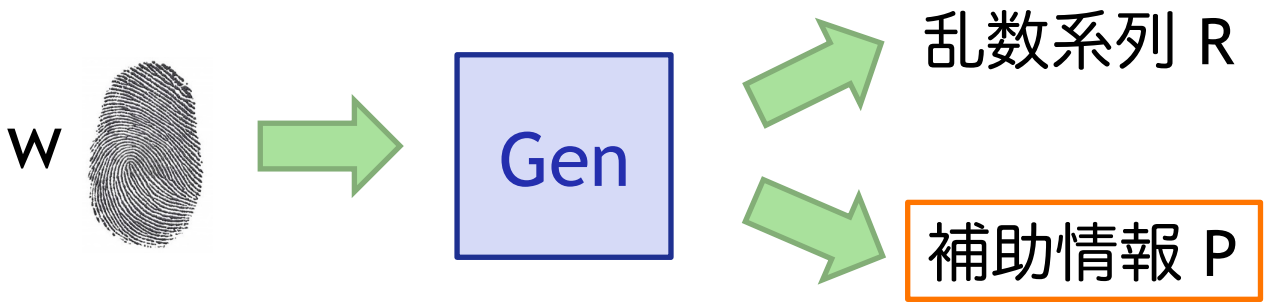
- Dodis ら [DORS08] が提案

- （生体情報等の）ノイズの多い情報源から一様ランダムな系列を抽出する技術
  - 一様ランダムな系列が手に入れば、様々な暗号技術が利用可能

[DORS08] Y. Dodis, R. Ostrovsky, L. Reyzin, A. Smith. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. SIAM J. Comput. 38(1): 97-139 (2008)

ファジィ抽出器 (Gen, Rep)

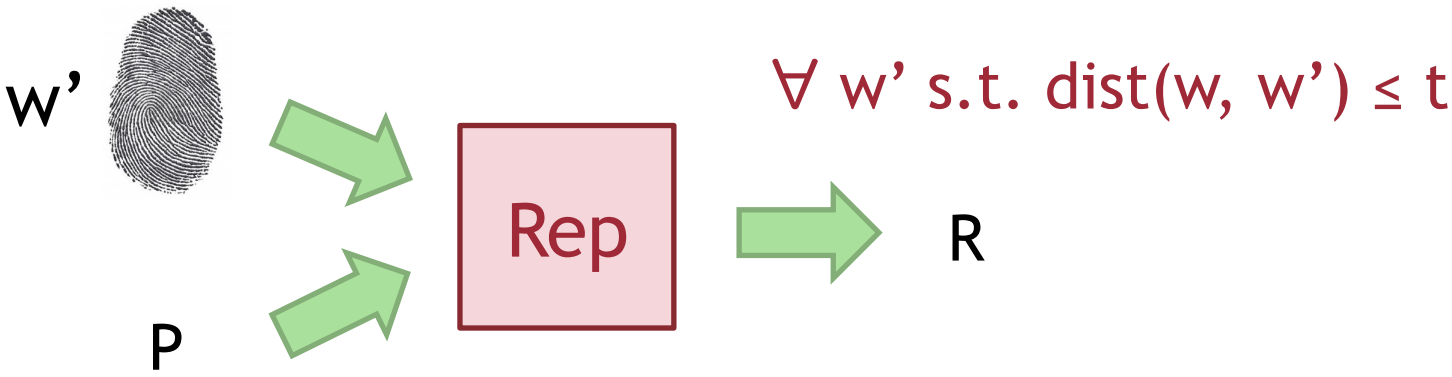
- 鍵生成アルゴリズム Gen:



$SD((R,P), (U_k,P)) \le \varepsilon$

$SD(X,Y) = 1/2 \sum_a |Pr[X=a] - Pr[Y=a]|$

- 再生アルゴリズム Rep:



ファジィ抽出器の構成方法 [DORS08]

- セキュアスケッチ (SS, Rec)
  - エントロピーをあまり減らさず、誤り訂正情報を生成

$H_\infty(W|ss) \geq m$

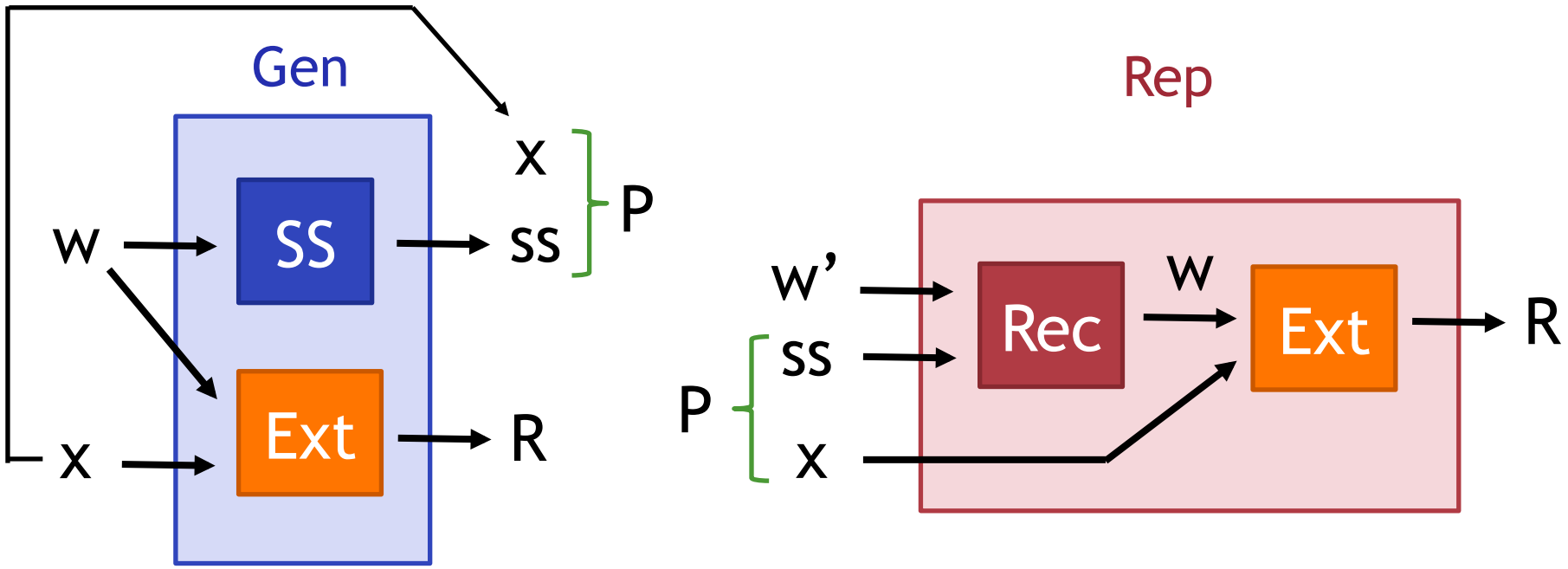
$\forall\ w'$ s.t. $dist(w, w') \leq t$

- 強乱数抽出器
  - シードを公開してもよい乱数抽出器

$SD((R, X), (U_k, X)) \leq \varepsilon$

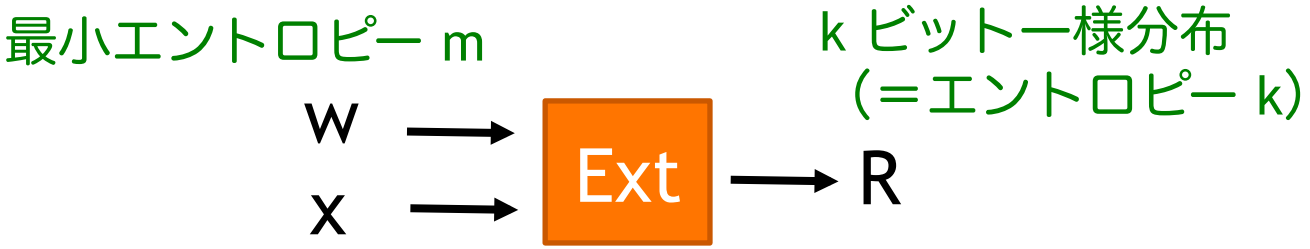
ファジィ抽出器の構成方法 [DORS08]

- セキュアスケッチ ＋ 強乱数抽出器



ファジィ抽出器の限界（1/2）

- 乱数抽出の限界



- $\forall$ W with $H_\infty(W) \geq m$,
  $SD((Ext(W,X), X), (U_k, X)) \leq \varepsilon$

- エントロピーロス $m - k \geq 2 \log(1/\varepsilon)$ [RTS00]

[RTS00] J. Radhakrishnan, A. Ta-Shma: Bounds for Dispersers, Extractors, and Depth-Two Superconcentrators. SIAM J. Discrete Math. 13(1): 2-24 (2000)

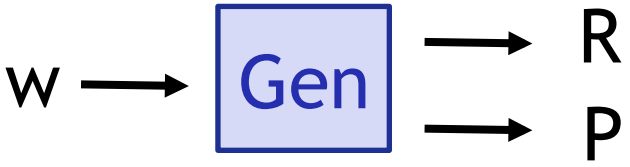
ファジィ抽出器の限界（2/2）

- セキュアスケッチ・ファジィ抽出器の限界 [DORS08]
  - [DORS08] の構成法は以下に関してタイト
    - セキュアスケッチの残存エントロピー m
    - ファジィ抽出器の出力長 |R|
  - 証明方法
    - セキュアスケッチ → 誤り訂正符号 → 符号の限界
    - ファジィ抽出器 → 誤り訂正符号 → 符号の限界

セキュアスケッチ

$H_\infty(W|ss) \geq m$

ファジィ抽出器



既存研究（計算量的ファジィ抽出器）

- [FMR13]
  安全性を計算量的なものに緩和することで、
  長い鍵長を達成できるか？
  - 計算量的セキュアスケッチの限界

    計算量的エントロピーのセキュアスケッチ
    → ほぼ同等の情報理論的セキュアスケッチ
  - LWEベースの計算量的ファジィ抽出器の提案

    セキュアスケッチを使用せず、
    エントロピーロスがない構成法

[FMR13] B. Fuller, X. Meng, and L. Reyzin. Computational fuzzy extractors. Asiacrypt 2013

本研究の成果

- 否定的結果：不可能性の拡張

  計算量的ファジィ抽出器
  → ほぼ同等の情報理論的ファジィ抽出器

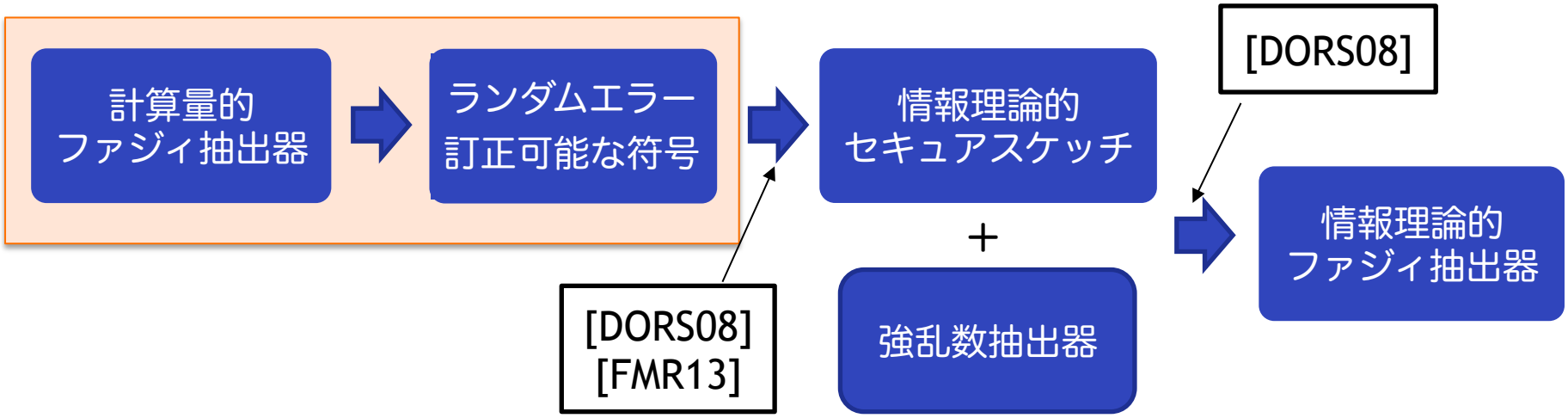
  - 「Gen の逆計算が効率的に可能」
    という仮定のもと

- 肯定的結果：計算量的ファジィ抽出器の構成法
  - 漏洩耐性のある KEM + セキュアスケッチ

否定的結果：不可能性の証明の流れ

[FMR13]

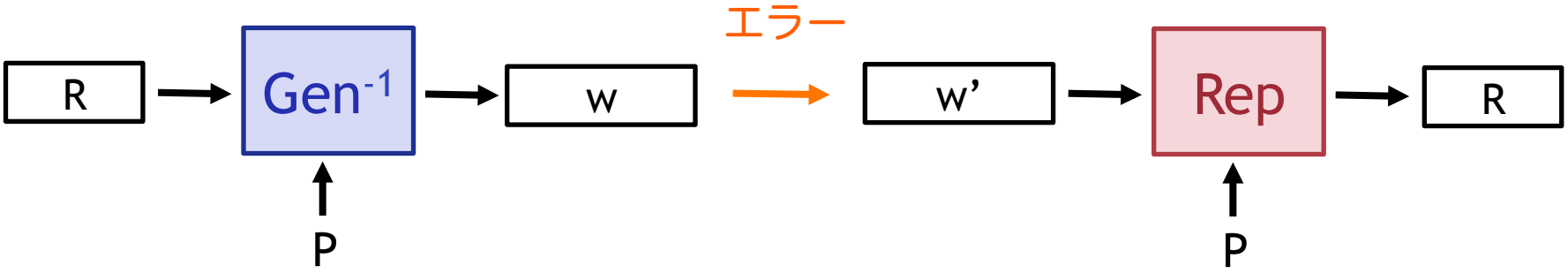
本研究



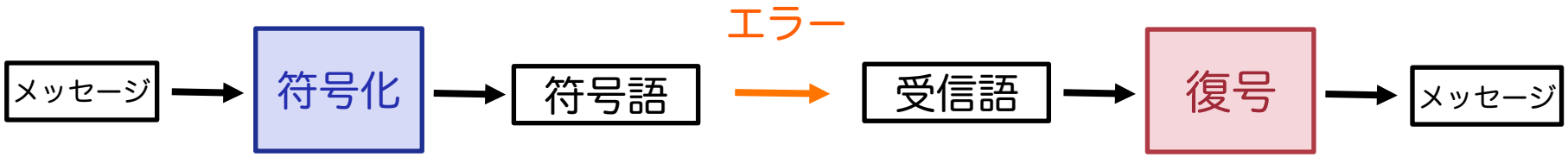
証明のアイディア

計算量的ファジィ抽出器 → ランダムエラー訂正可能な符号

- Gen が逆計算可能と仮定

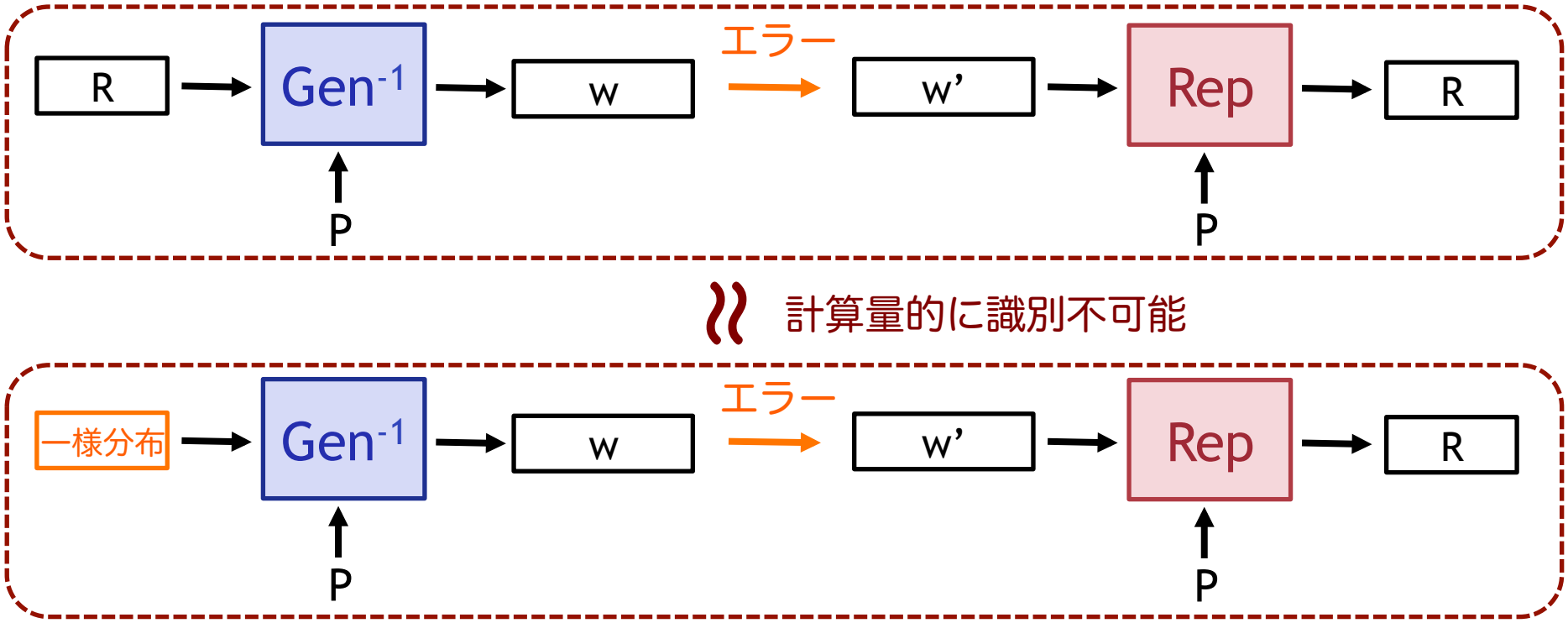


誤り訂正の仕組み



証明のアイディア（やや詳細）

- Gen^{-1} が、誤り訂正符号の符号化関数であることを示す
  - 高いレートの符号であることを示したい
  - しかし、R は擬似ランダムなので低エントロピーかも
    → R を一様分布に置き換えても識別不可能



証明のアイディア（やや詳細）

- R を一様分布に置き換えるとき、
  効率的に検査可能な性質しか受け継がれない
  - 「任意の t 個のエラーを訂正可能」という性質は
    効率的にチェックできないため受け継がれない

    →「ランダムな t 個のエラーを訂正可能」という
    性質ならば効率的にチェック可能

    （さらに、ランダムエラー訂正可能な符号から、
    情報理論的セキュアスケッチは構成可能）

証明のアイディア（やや詳細）

- 誤り訂正の設定では、P を受信者に渡せない
  → ある固定した P で成り立つことを示せばよい
  - P の平均ケースで達成可能な性質
    → ある固定した p でも達成可能

averaging argument

- 「Gen が逆計算可能」をどう定式化するか？
  - (r, p) ← Gen(w)
  - 一般に、$Gen^{-1}(r, p)$ は一意に存在しない
    - $\exists w_1, r_1, w_2, r_2$ s.t. $Gen(w_1;r_1) = Gen(w_2;r_2) = (r, p)$
    - 同一メッセージ r から複数の符号語 w_1, w_2 が生成される状況であり、解析がややこしい（エラーがあると特に）

  → 決定性アルゴリズムで逆計算可能と仮定
  （決定性なので、出力は一意に定まる）

主定理

定理
・(Gen, Rep)： (n, m, k, t, ε, δ)-計算量的ファジィ抽出器
・Gen が効率的に逆計算可能（失敗確率 η）

→ 以下の誤り訂正符号 C が存在
・ $\log|C| \geq -\log(2^{-k} + \rho/|M|) - 1$
・ C は t ビットランダムエラーを誤り率 2ρ で訂正
ただし、$\rho = \varepsilon + \eta + (t+1)\delta$

(n, m, k, t, ε, δ) ファジィ抽出器
・n：入力長
・m：入力エントロピー
・k：出力長
・t：訂正可能なエラービット数
・ε：出力系列と一様分布との(計算量的)統計的距離
・δ：Rep の復元失敗確率

系

系
・(Gen, Rep)： (n, m, k, t, ε, δ)-計算量的ファジィ抽出器
・Gen が効率的に逆計算可能（失敗確率 η）

→ (n, m, k, t, ε’, 2ρ)-情報理論的ファジィ抽出器が存在
- $k \leq m - n - \log(2^{-k} + \rho 2^{-n}) - 2\log(1/\varepsilon') + 1$
- $\rho = \varepsilon + \eta + (t+1)\delta$

特に、m = n かつ $\rho 2^{-n} \leq 2^{-k}$ のとき、
(n, n, k , t, ε, δ)-計算量的ファジィ抽出器
→ (n, n, $k - \log(1/\varepsilon')$, t, ε’, 2ρ)-情報理論的ファジィ抽出器

肯定的結果：計算量的ファジィ抽出器の構成法

- 漏洩耐性のある KEM + セキュアスケッチ

- KEM: ランダムな鍵を共有するための方式
  - 鍵生成: $K.Gen(1^n) \rightarrow (ek, dk)$
  - 暗号化: $K.Enc(ek) \rightarrow (C, K)$
  - 復号: $K.Dec(dk, C) = K$

構成のアイディア

- 漏洩耐性のある KEM
  - K.Gen の乱数の一部が漏洩しても安全な方式
    - 実際は、乱数にエントロピーがあれば安全な方式
  - 構成法 [Naor, Segev 2012]
    - Hash Proof Systems, KEM + 強乱数抽出器

乱数にエントロピーがあれば安全な方式
→ファジィ抽出器の入力 w を K.Gen の乱数として使う

構成法

- 構成法（漏洩耐性 KEM + セキュアスケッチ）
  - Gen(w;r_1,r_2) :
    (ek, dk) ← K.Gen(w), (C,K) ← K.Enc(ek;r_1),
    P = (C, SS(w;r_2)), R = K output (P, R)
  - Rep(w', (C, ss)) :
    w = Rec(w',ss), (ek, dk) ← K.Gen(w),
    K ← K.Dec(dk,C), output K

- 公開鍵ベースである必要はない

提案した構成法の性質

- 抽出乱数を伸ばすことが可能
  - 暗号文/共有鍵を複数生成することに対応
  - 計算量的な安全性でないと達成不可能
    - FE-then-PRG 構成でも達成可能
- 入力 w に対する「ある種」の秘匿性をもつ
  - 抽出乱数 R から w の情報は漏れない
    - FE-then-RPG では一般に達成できない
    - 既存研究では考えられてない安全性（？？）
      - 複数サーバに同じ w で生成しても個々の乱数 R は安全
  - ただし、公開情報 P から w の情報がもれるかも

→ entropic security [Dodis, Smith 2004, 2005] をもつセキュアスケッチを利用すれば大丈夫（？）

今後の研究の方向

- 安全性を計算量的に緩めたので、
  多様な安全性を達成できないか？
  - 入力 w に対する秘匿性
    - 既存手法 [Dodis, Smith 2005] より効率的に可能か？
  - 鍵の再利用可能性 [Boyen 2004]
    - 敵が複数サーバに入力 $\delta_i(w)$ で (R_i, P_i) を生成させて $\{P_i\}$ を得ても、抽出乱数 R_i は安全
  - ロバスト性
    - 公開情報 P が P* に書き換えられても検出可能
    - 加法的 related-key attack 耐性 MAC があれば十分
      - [Dodis, Katz, Reyzin, Smith 2006] の構成法
      - エントロピーレート 1/2 未満は（計算量的でも）未解決

まとめ

- ファジィ抽出器
  - ノイズのある情報源から乱数を抽出する技術
  - 計算量的な安全性にすることの利点は？
- 研究成果
  - 否定的結果：不可能性の拡張
    - 計算量的ファジィ抽出器→ 情報理論的ファジィ抽出器
    - 「Gen の逆計算が効率的に可能」という仮定のもと
  - 肯定的結果：計算量的ファジィ抽出器の構成法
    - 漏洩耐性のある KEM + セキュアスケッチ
- 今後の研究
  - 計算量的な設定で多様な安全性を達成可能か？