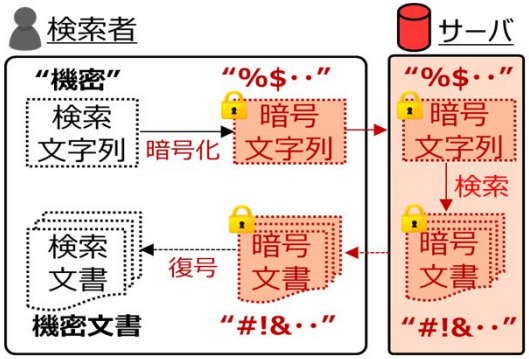
検索可能暗号における攻撃の軽減について

Attack mitigation in searchable encryption

佐藤 敬恒・法制倫理分科会・情報セキュリティ大学院大学

1.研究の背景

クラウドの活用が浸透する中で、データを暗号化したまま検索を実現できる**検索可能暗号**の研究が盛んに行われている。



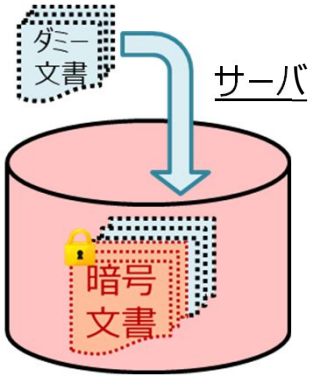
サーバは検索にあたり、以下の情報を入手する。

①	検索者からの問い合わせ暗号文字列と、レスポンスとして紐づく暗号文書情報
②	同じ暗号文字列での問い合わせを前に受けたことがあるかどうか。
③	問い合わせのために登録された暗号文字列や暗号文書情報の件数。

これらは回避できない漏洩情報として整理されてきたが、**一定条件の下で問い合わせ暗号文字列の復元のために活用しうる**ことが指摘されている。信頼できないサーバからの推測攻撃に備える必要性がある。

2.先行研究調査

攻撃を軽減する手段の一つとして、**サーバに登録する暗号文書にダミー文書を含め、任意の問い合わせに対してレスポンス件数を揃える**パディング手順が考察されており、その中でも多くの提案が生まれている。



3.今後の研究計画

推測攻撃を軽減する方式についての継続調査を進めていく中で、既存の手段よりも利点を持った新規方式の提案につなげたい。

23年 3月～23年 6月 先行調査・方式(案)考察

23年 7月～23年11月 方式(案)の検討と改良

23年12月～24年 1月 修士論文の作成