Privacy-Preserving Personal Information Management

Mohamed Layouni

PhD Oral Defense
School of Computer Science, McGill University

Designing protocols that are :

- **Secure**
- **Privacy-preserving**
- **User-centric**

- Studied/Surveyed **Privacy-Preserving Credentials**
  - Compared the most complete/elaborate ones
  - Proposed an **extension** to the Camenisch-Lysyanskaya credential system*
- Proposed two privacy-preserving protocols for **controlling access to remotely-stored DB records**, where ***access*** is performed ***according to policies defined by the owners of those records***.

- Proposed protocols to **solve real-world problems** using privacy-preserving credentials:
  - ***Prescription-handling*** for the Belgian Healthcare System* (e.g., protecting patients' privacy from *administrative entities* involved in the processing of insurance claims)
  - ***Tele-monitoring*** of patients' health outside Hospital (Protocol for collecting patients' health measurements in a user-centric and privacy-preserving way)

Presentation Outline

1. Introduction
2. Accredited Symmetrically Private Information Retrieval (ASPIR)
3. Multi-Authorizer ASPIR
4. Conclusion

Settings and Parties Involved

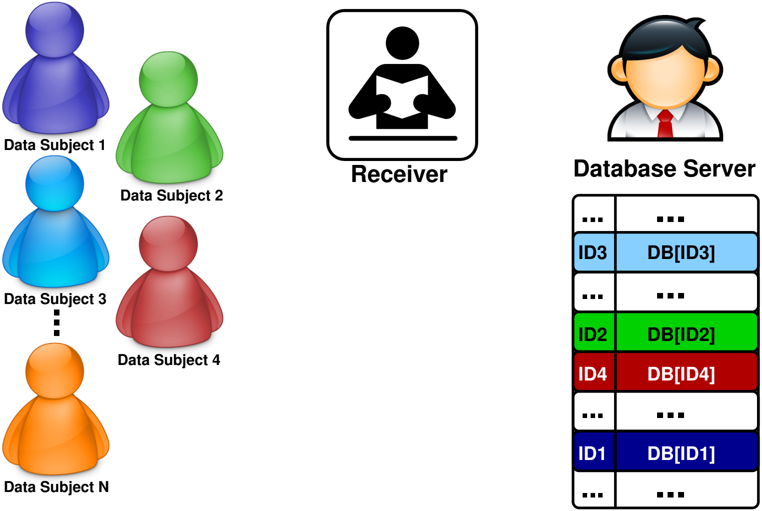

Figure: Setting of the ASPIR Protocol

- **Privacy for Receiver:** DB Server ***should not be able to compute the index*** of the retrieved record (and hence the ID of data-subject)
- **Privacy for DB Server:** For each query, the Receiver can compute ***information only on one record*** (defined in the query), and nothing about the other records in DB.
- **Privacy for Data Subject:**
  - DB records ***cannot be retrieved without authorization***
  - It should be ***intractable*** for a quorum of players to ***forge an authorization*** for a record that none of them owns.
  - DB Server should be able to ***verify the validity of an authorization*** presented by the Receiver, ***without learning the identity*** of the Data-Subject who issued it.

Solution combines **two main building blocks**:

- Privacy-Preserving Credential System (Brands'00)
- Symmetrically Private Information Retrieval System (Lipmaa'05)

Solution combines **two main building blocks**:

- Privacy-Preserving Credential System (Brands'00)
- Symmetrically Private Information Retrieval System (Lipmaa'05)

Symmetrically Private Information Retrieval (SPIR)

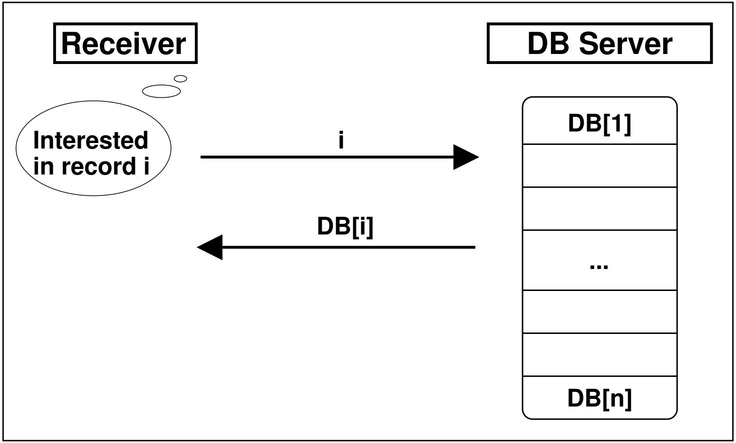

Figure: A Simple Database Query

Symmetrically Private Information Retrieval (SPIR)

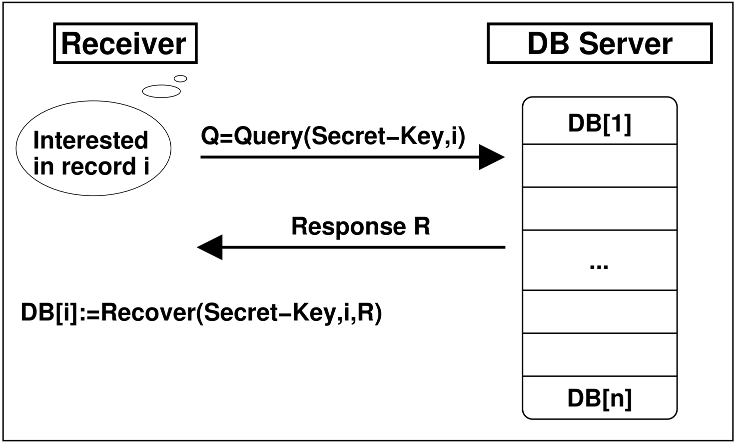

Figure: Symmetrically Private Information Retrieval

Solution combines **two main building blocks**:

- Privacy-Preserving Credential System (Brands'00)
- Symmetrically Private Information Retrieval System (Lipmaa'05)
    - Similar to an **Oblivious Transfer*** scheme,
    - Higher efficiency, *but*
    - Weaker security.

Solution combines **two main building blocks**:

- Privacy-Preserving Credential System (Brands'00)
- Symmetrically Private Information Retrieval System (Lipmaa'05)
  - Similar to an **Oblivious Transfer*** scheme,
  - Higher efficiency, *but*
  - Weaker security.

Privacy-Preserving Credentials

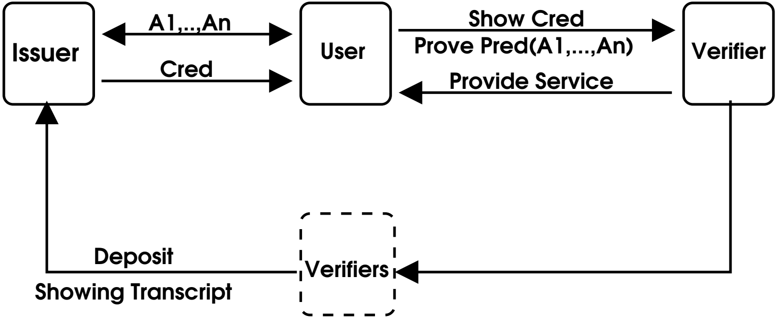

Figure: Privacy-Preserving Credentials Issuing, Showing, and Depositing

Privacy-Preserving Credentials

Properties of Privacy-Preserving Credentials

- **Selective disclosure** (in the sense of Zero Knowledge)
- **Soundness** (no false claims)
- **Untraceability** (showings unlinkable to user's identity)
- **Unlinkability** (between showings)
- **...**

Constructions from the Literature

- **Camenisch and Lysyanskaya** (IBM's **IDEMIX**)
- **Brands** (Microsoft's **U-Prove**)

Solution Overview

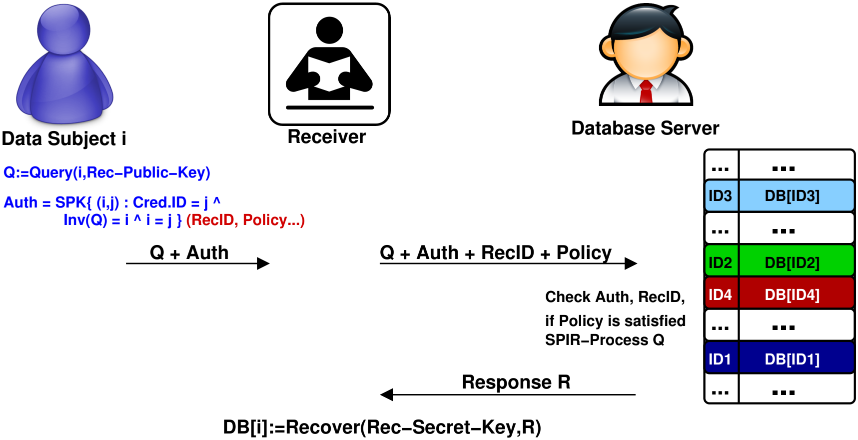

Figure: Accredited SPIR Protocol: High-Level Overview

Multi-Authorizer ASPIR is :

1. A ***new approach*** to constructing ASPIR schemes (also useful for single-Authorizer ASPIR)
2. An ***extension*** of ASPIR to a setting where:
   - A DB record belongs to ***multiple owners*** simultaneously
   - Receiver can recover a DB record only if he:
     - Complies with ***privacy policy*** defined by record owners.
     - Has ***authorizations*** from:

       — ***All owners*** of target record,
       — ***Any subset*** of owners of ***size larger than a threshold***,
       — ***Certain subsets*** of owners (general access structure)

Settings and Parties Involved

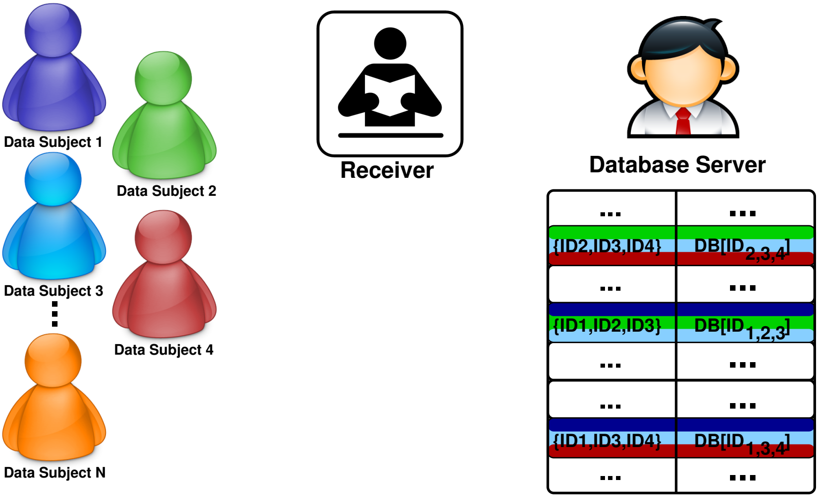

Figure: Setting of the Multi-Authorizer ASPIR Protocol

- **Privacy for Receiver:** DB Server ***cannot compute the index*** of the retrieved record (and hence the IDs of its owners)
- **Privacy for DB Server:** For each query, the Receiver ***learns information only on one record*** (defined in the query), and nothing about the other records in DB.
- **Privacy for Data Subject:**
  - DB records cannot be recovered without the ***necessary authorizations***
  - It should be ***intractable*** for a quorum of players to ***forge an authorization*** for a record that none of them owns.

Multi-Authorizer ASPIR is a ***completely new construction***:

- We use ***different building blocks***:
  Pairing-based signatures *instead* of Credentials.
  (Security relies on Bilinear Diffie-Hellman assumption).
- We use **SPIR schemes in a black-box fashion**;
  Construction works with any SPIR scheme, not only
  Lipmaa's SPIR scheme as in ASPIR.
- The new scheme is ***more efficient*** than previous ASPIR.

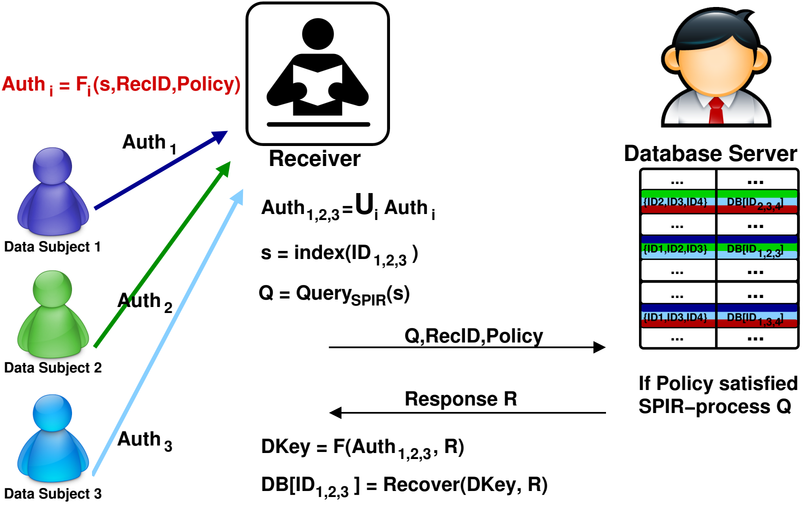

Figure: Multi-Authorizer ASPIR Protocol (Basic Construction)

The proposed protocols have the following extra functionalities:

- Receiver can retrieve ***multiple records*** belonging to a tuple of data-subjects (2 Constructions)

  Idea 1: Change the way the SPIR query is processed (Technique similar to the one used in the *General* and *Threshold* Access Structure variants)

  Idea 2: Two Databases : one for Keys, one for Ciphertexts. Retrieve key with MASPIR, and use it to decrypt all records of owners' tuple being considered.

Summary:

1. Proposed two privacy-preserving protocols for **controlling access to remotely-stored DB records**, where ***access*** is performed ***according to policies defined by the owners of those records***.
2. Proposed **Privacy-Preserving eHealth protocols** (e.g., Prescription-handling for the Belgian Healthcare System)
3. Surveyed the **State of the Art in Privacy-Preserving Credential Systems**, and provided a **Comparison** of the most elaborate/complete ones.

Possible Extensions : Accredited Privately-Searchable Encryption

Same setting as ASPIR, ***except*** that :

- Data records are stored in **encrypted** form, with each record labelled by a set of keywords (also encrypted),
- Querying **by keywords** instead of by indices,
- Data-subjects control **who** can search their records, **what** keywords can be queried, **terms & conditions.**

The solution should be such that :

- Receiver can only retrieve records matching the ***authorized search keywords***,
- DB Manager ***does not learn*** : **ID of data-subject**, **search keywords**, **access pattern**, or **search results.**

Thank you!

Accredited SPIR Protocol – Detailed Description

Public Info

$p, q, (g_i)_{0\le i\le \ell}, h_0, (g_i^{x_0})_{0\le i\le \ell}, h_0^{x_0}, H, k, pk^{(\mathrm{R})}, \mathcal{R}, g_{db},$

$\mathsf{pk}_{\mathsf{EIG}}^{(\mathrm{R})} := (g_{\mathsf{EIG}}, y_{\mathsf{EIG}}), G_q := \langle g_i \rangle := \langle g_{\mathsf{EIG}} \rangle := \langle g_{db} \rangle, n := |\mathrm{DB}| \le q, \lambda_1, \cdots, \lambda_\alpha.$

Authorizer | **Receiver** | **Sender (Database DB)**

Authorizer: $(\mathsf{c}_1, \mathsf{c}_2) := \mathsf{E}_{\mathsf{pk}_{\mathsf{EIG}}^{(\mathrm{R})}}((g_{db})^{\mathrm{ID}_{\mathcal{A}}})$

Authorization (Authorizer → Receiver):

$$\xrightarrow[\mathrm{SPK}\{(\varepsilon_1,\cdots,\varepsilon_\ell,\mu,\nu):h=g_1^{\varepsilon_1}\cdots g_\ell^{\varepsilon_\ell}h_0 \wedge \mathsf{c}_2 = y_{\mathsf{EIG}}^{\mu} g_{db}^{\nu} \wedge \varepsilon_1=\nu\}(m)]{h,\ \sigma_{\mathrm{CA}}(h) := (z', r_0', c_0'),\ (\mathsf{c}_1,\mathsf{c}_2)}$$

Receiver:

For $j := 1$ to α do :
 For $t := 0$ to $\lambda_j - 1$ do :
  $r_{jt} \in_R \mathcal{R}$
  $\beta_{jt} := HomEnc_{pk^{(\mathrm{R})}}(b_{jt}, r_{jt}),$
   where $b_{jt} := 1$ if $t = \mathrm{ID}_{\mathcal{A}}^{(j)}$,
   and $b_{jt} := 0$ otherwise.

$$\xrightarrow{\textbf{Authorization}, \{\beta_{jt}\}_{0\le t<\lambda_j}^{1\le j\le \alpha}}$$

Sender (Database DB):

Check Authorization validity.
For $j := 1$ to n do :
 $\delta_j \in_R [1, q-1]$
 $\mathrm{DB}_0[j] :=$
  $((\mathsf{E}_{\mathsf{pk}_{\mathsf{EIG}}^{(\mathrm{R})}}(g_{db}^{\mathrm{ID}_{\mathcal{A}}}) \otimes g_{db}^{-j})^{\delta_j} \otimes \mathrm{DB}[j])$
For $j := 1$ to $\alpha - 1$ do :
 For $i_{j+1} := 0$ to $\lambda_{j+1} - 1, \cdots,$
  $i_\alpha := 0$ to $\lambda_\alpha - 1$ do :
 $\mathrm{DB}_j(i_{j+1}, \cdots, i_\alpha) :=$
  $\prod_{t\in\mathbb{Z}_{\lambda_j}} (\beta_{jt})^{\mathrm{DB}_{j-1}(t, i_{j+1}, \cdots, i_\alpha)}$
$\mathrm{DB}_\alpha := \prod_{t\in\mathbb{Z}_{\lambda_\alpha}} (\beta_{\alpha t})^{\mathrm{DB}_{(\alpha-1)}(t)}$

$$\xleftarrow{\mathbf{DB}_\alpha}$$

Receiver:

$\mathrm{DB}_\alpha' := \mathrm{DB}_\alpha$
For $j := \alpha$ downto 1 do :
 $\mathrm{DB}_{j-1}' := HomDec_{sk^{(\mathrm{R})}}(\mathrm{DB}_j')$
Output $\mathrm{DB}[\mathrm{ID}_{\mathcal{A}}] := \mathsf{D}_{\mathsf{sk}_{\mathsf{EIG}}^{(\mathrm{R})}}(\mathrm{DB}_0')$

Figure: Accredited SPIR Protocol (DLog-Based Construction)

Public Info

$$p, q, (g_i)_{0 \le i \le \ell}, h_0, (g_i^{x_0})_{0 \le i \le \ell}, h_0^{x_0}, H, k, pk^{(\mathrm{R})}, \mathcal{R}, g_{db},$$
$$\mathrm{pk}_{\mathrm{EIG}}^{(\mathrm{R})} := (g_{\mathrm{EIG}}, y_{\mathrm{EIG}}), G_q := \langle g_i \rangle := \langle g_{\mathrm{EIG}} \rangle := \langle g_{db} \rangle, n := |\mathrm{DB}| \le q, \lambda_1, \cdots, \lambda_\alpha.$$

Authorizer **Receiver**

$$(\mathrm{c}_1, \mathrm{c}_2) := \mathrm{E}_{\mathrm{pk}_{\mathrm{EIG}}^{(\mathrm{R})}}((g_{db})^{\mathrm{ID}_{\mathcal{A}}})$$

$$\left.\xrightarrow[\substack{\mathrm{SPK}\{(\varepsilon_1,\cdots,\varepsilon_\ell,\mu,\nu):h=g_1^{\varepsilon_1}\cdots g_\ell^{\varepsilon_\ell}h_0 \\ \wedge \mathrm{c}_2=y_{\mathrm{EIG}}^{\mu}g_{db}^{\nu}\wedge\varepsilon_1=\nu\}(m)}]{\boldsymbol{h, \sigma_{\mathrm{CA}}(h) := (z', r_0', c_0'), (\mathrm{c}_1, \mathrm{c}_2)}}\right\} \textbf{Authorization}$$

Figure: Accredited SPIR Protocol – Detailed description – Part I

Receiver | **Sender (Database DB)**

For $j := 1$ **to** α **do** :
  For $t := 0$ **to** $\lambda_j - 1$ **do** :
    $r_{jt} \in_R \mathcal{R}$
    $\beta_{jt} := HomEnc_{pk^{(R)}}(b_{jt}, r_{jt})$,
      where $b_{jt} := 1$ if $t = \mathrm{ID}_{\mathcal{A}}^{(j)}$,
      and $b_{jt} := 0$ otherwise.

$$\xrightarrow{\textbf{Authorization}, \{\beta_{jt}\}_{0 \le t < \lambda_j}^{1 \le j \le \alpha,}}$$

Check Authorization validity.
For $j := 1$ **to** n **do** :
  $\delta_j \in_R [1, q-1]$
  $\mathrm{DB}_0[j] :=$
    $((\mathrm{E}_{\mathrm{pk}_{\mathrm{EIG}}^{(\mathrm{R})}}(g_{db}^{\mathrm{ID}_{\mathcal{A}}}) \otimes g_{db}^{-j})^{\delta_j} \otimes \mathrm{DB}[j])$
. . .

Figure: Accredited SPIR Protocol – Detailed description – Part II

Receiver		**Sender (Database DB)**
		Check Authorization validity.
		For $j := 1$ **to** n **do** :
		$\delta_j \in_R [1, q-1]$
		$\mathrm{DB}_0[j] :=$
		$((\mathrm{E}_{\mathrm{pk}^{(\mathrm{R})}_{\mathrm{EIG}}}(g_{db}^{\mathrm{ID}_{\mathcal{A}}}) \otimes g_{db}^{-j})^{\delta_j} \otimes \mathrm{DB}[j])$
		For $j := 1$ **to** $\alpha - 1$ **do** :
		For $i_{j+1} := 0$ **to** $\lambda_{j+1} - 1, \cdots,$
		$i_\alpha := 0$ to $\lambda_\alpha - 1$ do :
		$\mathrm{DB}_j(i_{j+1}, \cdots, i_\alpha) :=$
		$\prod_{t \in \mathbb{Z}_{\lambda_j}} (\beta_{jt})^{\mathrm{DB}_{j-1}(t, i_{j+1}, \cdots, i_\alpha)}$
		$\mathrm{DB}_\alpha := \prod_{t \in \mathbb{Z}_{\lambda_\alpha}} (\beta_{\alpha t})^{\mathrm{DB}_{(\alpha-1)}(t)}$
$\mathrm{DB}'_\alpha := \mathrm{DB}_\alpha$	$\xleftarrow{\quad \mathbf{DB}_\alpha \quad}$	
For $j := \alpha$ **downto** 1 **do** :		
$\mathrm{DB}'_{j-1} := \mathit{HomDec}_{sk^{(\mathrm{R})}}(\mathrm{DB}'_j)$		
Output $\mathbf{DB}[\mathbf{ID}_{\mathcal{A}}] := \mathrm{D}_{\mathrm{sk}^{(\mathbf{R})}_{\mathrm{EIG}}}(\mathbf{DB}'_0)$		

Figure: Accredited SPIR Protocol – Detailed description – Part III

Multi-Authorizer ASPIR Protocol – Detailed Overview

Receiver (*RecID*)	**Public Info**	**Sender (Database DB)**
$(P_m, \sigma_u(P_m))$, $u \in \{A, B, C\}$, for $P_m := H(s, RecID, \mathcal{P})$, where $s := index(ID_A, ID_B, ID_C)$, and $\mathcal{P} := \{\text{usage policy}\}$		
	$\{pk_u\}_{u \in \{A,B,C\}} \triangleq \{pk_{s,i}\}_{1 \le i \le 3}$, $e(\cdot,\cdot)$, P, $\mathbb{G}_1 = \langle P \rangle$, $\mathbb{G}_2$, q, **SPIR scheme**	
$Sig(P_m) = \prod_{u \in \{A,B,C\}} \sigma_u(P_m) = \prod_{u \in \{A,B,C\}} (P_m)^{x_u} = (P_m)^{\sum_u x_u}$		
$Q = Q_{SPIR}(s)$	$\xrightarrow{\mathbf{Q},\ \boldsymbol{RecID},\ \boldsymbol{\mathcal{P}}}$	
		If $\mathcal{P}$ satisfied continue else abort Choose $\delta \in_R \mathbb{Z}_q^*$ **For** $j := 1$ **to** N **do** : $P_{mj} = H(j, RecID, \mathcal{P})$ $DB'[j] = DB[j] \times e\left(P_{mj}, \prod_{u=1}^{3} pk_{j,u}\right)^{\delta}$
		Execute SPIR scheme on DB′ and Q
SPIR-recover DB′[*s*] from Res	$\xleftarrow{\mathbf{Res},\ \boldsymbol{P^{\delta}}}$	**Let Res = $R_{SPIR}(Q, DB')$**
Output $DB_0[s] := DB'[s]\ /\ e(Sig(P_m), P^{\delta})$		

Figure: Multi-Authorizer ASPIR (Basic Construction)