Function-Private Subspace Membership Enc. and Its Applications

Dan Boneh
Stanford

Ananth Raghunathan
Stanford

Gil Segev
Hebrew University
Predicate Encryption [BW07, KSW08]

Predicate $p: \Sigma \rightarrow \{0,1\}$
attribute $x$ in $\Sigma$

$pp$: public

$(pp, msk)$

$sk_p \downarrow p \uparrow p$

Bob can recover $m$ only if $p(x)=1$

$p$: predicate

$\Sigma \rightarrow \{0,1\}$

Applications: spam filtering encrypted email routing encrypted bank transactions
**Question:** must $\text{sk}_p$ reveal $p$?

Can we build schemes where $\text{sk}_p$ reveals no information about $p$?

In previous works, $\text{sk}_p$ may leak $p$. In several schemes, $p$ is leaked explicitly.
Function Privacy [Boneh-R.-Segev13]

Motivated by the question of **keyword privacy** in Public Key Encryption with Keyword Search (PEKS) [BCOP04]

Routing Proxy

Does the proxy learn information about keywords?

Enc(pp, from, m)

From/subj:
- bills
- doctor
- crypto-chair
- ...

Spam
Urgent!
Later
(In a nutshell)

• Define function privacy of Identity-Based Encryption (IBE implies encrypted keyword search [BCOP04])

• Observe that given $sk_{id}$, semantic security for $id$ is not possible (due to the public-key nature of encryption)

• Construct IBE schemes where the secret key reveals no information about the identity
  – identity must have some min-entropy
  – constructions in RO and STD model
  – constructions from pairings and lattices
Subspace-Membership Enc.

\[ p_W(x) = \begin{cases} 1 & \text{if } (W \cdot x = 0 \text{ in } \mathbb{F}_q) \\ 0 & \text{otherwise} \end{cases} \]

- Predicate \( p \) corresponds to matrix \( W \) over \( \mathbb{F}_q \)
- Ciphertext attribute \( x \) is a vector over \( \mathbb{F}_q \)
  \( sk_p \) can decrypt if \( W \cdot x = 0 \)
- \( k=1 \) is inner-product encryption [KSW08, Fre10, AFV11]
- Subspace membership with delegation [OT09, OT12]
- Security requirement:
  given secret keys for predicates \( p_1, \ldots, p_Q \),
  semantic security for ciphertexts with attribute \( x \) where
  \( p_i(x)=0 \) (for all \( i \))
SME – Applications

- Predicates that are *roots of polynomials*
  - ciphertexts encrypted to an attribute $x$ in $F_q$
  - secret keys derived for polynomial predicates
    \[ p(x) = 1 \text{ iff } (p_0 + p_1 x + p_2 x^2 + \ldots + p_d x^d = 0) \]
  - *Basic idea:* encrypt to vector \((1 \ x \ x^2 \ \ldots \ x^d)\)
    - subspace is orthogonal to \((p_0 \ p_1 \ p_2 \ \ldots \ p_d)\)

- Hidden Vector Encryption [BW07]
  - predicates for comparison and set membership queries

- Subsumes Identity-Based Encryption
  - attribute $x = (1, id)$, subspace is $W = (-id, 1)$

- Predicates with conjunction and disjunctions
This Paper

• Extend the framework and techniques of [BRS13] to subspace membership encryption (SME)
• Define function-private SME: schemes where the secret key reveals no information about the subspace
  – identify minimal necessary restrictions
• Black-box constructions of function-private SME from non-function-private inner-product encryption schemes
  – First black-box constructions of function-private schemes
• Applications with function privacy (discussed later)
Function Privacy for SME

- What information does $sk_W$ leak about $W$?
- Given $sk_W$ and a guess for $W$, due to the public-key nature of $Enc$, guess can be verified (up to constant factors)

(assume $W$ is a vector)

encrypt $m$ with $x = \begin{bmatrix} w_1 & -1 & 0 & \ldots & 0 & 0 \end{bmatrix}$

If decryption recovers $m$ then $w_1$ guessed correctly!
Function Privacy for SME

- What information does $sk_W$ leak about $W$?
- Given $sk_W$ and a guess for $W$, due to the public-key nature of $Enc$, guess can be verified (up to constant factors)

(assume $W$ is a vector)

Next, encrypt $m$ with $x = \begin{bmatrix} w_2 & 0 & -1 & \ldots & 0 & 0 \end{bmatrix}$

If decryption recovers $m$ then $w_2$ guessed correctly!
Function Privacy for SME

- What information does $sk_w$ leak about $W$?
- Given $sk_w$ and a guess for $W$, due to the public-key nature of $Enc$, guess can be verified (up to constant factors)

(assume $W$ is a vector)

$sk_w$  

$1 \ w_1 \ w_2 \ ... \ w_{m-1}$

Finally, encrypt $m$ with $x = w_{m-1} \ 0 \ 0 \ ... \ 0 \ -1$

Can verify guess only given $sk_w$!
Function Privacy for SME

• **Is unpredictability** of $W$ sufficient (like in IBE)?

• **No!**

  Following test works even if $w_1$ and $w_2$ are unpredictable so long as $w_1/w_2 = a$

$$\begin{array}{c|c|c|c|c}
\text{sk}_W & 1 & w_1 & w_2 & \ldots & w_{m-1} \\
\end{array}$$

guess

encrypt $m$ with $x = 0 \ -1 \ a \ \ldots \ 0 \ 0$

Can **still** verify guess only given $\text{sk}_W$!
Minimal necessary restriction:

\( sk_W \) reveals no information if columns of \( W \) come from a distribution with *conditional min-entropy*, i.e., \( j^{th} \) column still unpredictable given \( w_1, \ldots, w_{j-1} \)

**KeyGen**\((\text{msk}, \cdot)\)  

\[ \text{pp} \]  

(distribution) \( D \)  

\[ sk = \text{KeyGen}(\text{msk}, W_b) \]  

**Guess** \( b \)  

Fix random \( b \leftarrow \{0, 1\} \)  

\( W_0 \leftarrow D \)  

\( W_1 \leftarrow U \)

**Adversary cannot guess** \( b \) **with probability better than** \( 1/2 \)
Inner Product Predicate Encryption

\[ p_v(x) = \begin{cases} 
1 & \text{if } (v^T \cdot x = 0 \text{ in } F_q) \\
0 & \text{otherwise}
\end{cases} \]

- Predicate \( p \) corresponds to a vector \( v \) over \( F_q \)
- Ciphertext attribute \( x \) is a vector over \( F_q \)
  - \( sk_p \) can decrypt if \( v^T \cdot x = 0 \)

We construct function-private SME from any underlying (non-function-private) inner prod. scheme
  - black-box manner
  - modify the KeyGen algorithm by \textit{pre-processing} subspace \( W \) to derive an inner-prod sk vector \( v \)
Construction from Inner Prod. Enc.

**Key idea:** apply extractor on columns of $W$
run (underlying) inner prod

$\text{KeyGen}$ on extracted vector

$W = \begin{bmatrix} w_{00} & w_{01} & w_{02} & \ldots & w_{0m} \\ w_{10} & \ldots & \ldots & \ldots & \ldots \\ w_{20} & \ldots & \ldots & \ldots & w_{2m} \end{bmatrix}$

$V = \begin{bmatrix} v_{00} \end{bmatrix}$
Construction from IPE

**Key idea:** apply extractor on columns of $W$ run (underlying) inner prod

**KeyGen** on extracted vector

$$W = \begin{pmatrix}
  w_{00} & w_{01} & w_{02} & \ldots & w_{0m} \\
  w_{10} & \ldots & & & \\
  w_{20} & \ldots & & & w_{2m}
\end{pmatrix}$$

$$V = \begin{pmatrix}
  v_{00} & v_{01}
\end{pmatrix}$$
Construction from IPE

Key idea: apply extractor on columns of $W$ run (underlying) inner prod $\text{KeyGen}$ on extracted vector

$W = \begin{pmatrix} w_{00} & w_{01} & w_{02} & \ldots & w_{0m} \\ w_{10} & \ldots \\ w_{20} & \ldots \end{pmatrix}$

$V = \begin{pmatrix} v_{00} & v_{01} & v_{02} & \ldots & v_{0m} \end{pmatrix}$

Re-use the same seed due to conditional min-entropy!
Construction from IPE

• $V$ extracts entropy from $W$

• Therefore, $sk_V$ reveals no information about $W$ so long as columns of $W$ have conditional min-entropy

Function Privacy!

• Correctness and attribute-hiding security follows from the structure of the extractor:
  $\text{Ext}^\dagger((w_1, \ldots, w_k), (s_1, \ldots, s_k)) = w_1s_1 + \ldots + w ks_k \pmod{q}$

• \textbf{(In the paper)} Additional work to consider the case when $q$ is “small” (poly in security param.)
Applications

• Function privacy when encrypting to *roots of polynomials*
  – *minimal requirement:*
    coefficients of polynomials \( (p_0 \ p_1 \ p_2 \ ... \ p_d) \) must come from a distribution with *joint* min-entropy
  – *no conditional* min-entropy (public-key attacks can only use “Vandermonde vectors”)

  – *key idea:* construct appropriate subspace during key generation with conditional min-entropy property

\[
W = \begin{bmatrix}
\text{coefficients of } p(x) \cdot r_1(x) \cdot s_1(x) \\
\text{coefficients of } p(x) \cdot r_2(x) \cdot s_2(x) \\
\text{coefficients of } p(x) \cdot r_3(x) \cdot s_3(x)
\end{bmatrix}_{3 \times 5}
\]

\[
p(x) = p_0 + p_1 x + p_2 x^2
\]

\[
r_i(x) = r_{0,i} + r_{1,i} x
\]

\[
s_i(x) = s_{0,i} + s_{1,i} x
\]
Applications

- Function privacy when encrypting to *roots of polynomials*
  - *minimal requirement:*
    - coefficients of polynomials \((p_0 \ p_1 \ p_2 \ ... \ p_d)\) must come from a distribution with *joint* min-entropy
  - no *conditional* min-entropy (public-key attacks can only use “Vandermonde vectors”)

- *key idea:* construct **appropriate subspace** during key generation with *conditional min-entropy property*

\[
W = \begin{bmatrix}
\text{coefficients of } p(x) \cdot r_1(x) \cdot s_1(x) \\
\text{coefficients of } p(x) \cdot r_2(x) \cdot s_2(x) \\
\text{coefficients of } p(x) \cdot r_3(x) \cdot s_3(x)
\end{bmatrix}^{3 \times 5}
\]

\[
p(x) = p_0 + p_1 x + p_2 x^2
\]

\[
r_i(x) = r_{0, i} + r_{1, i} x
\]

\[
s_i(x) = s_{0, i} + s_{1, i} x
\]
Applications

• Function-Private IBE with minimal unpredictability

*Basic idea:* attribute \( \mathbf{x} = (1, \text{id}) \), subspace is \( W = (-\text{id}, 1) \)
Can “boost” entropy by considering \( W = (-\mathbf{r} \cdot \text{id}, \mathbf{r}) \) for uniformly sampled \( \mathbf{r} \) from \( \mathbb{F}_q \)

*Tradeoffs:* Better function privacy, but stronger assumptions \([KSW08]\) for IBE security

• Conjunctions and Disjunctions
Conclusions

• Extend the work of function privacy [BRS13] to the larger class of subspace-membership predicates
• Construct schemes from any underlying non-function-private inner-product scheme
• Function-private applications of SME
  – Roots of Polynomials
  – Function-Private IBE with minimal unpredictability
  – Conjunctions and Disjunctions
Open Problems

- Function privacy from computational assumptions
  - Recent work by Agrawal et al. [AABKPS13]
- Function privacy for Hidden-Vector Encryption
- Function privacy for larger classes of predicates
- Enhanced function privacy
  - preserve function privacy against an adversary that is given ciphertexts on which the challenge predicate evaluates to true
Thank You!
Any Questions?
ananthr@cs.stanford.edu
eprint.iacr.org/2013/403