Fully Key-Homomorphic Encryption and Applications: Arithmetic ABE with Short Keys and Compressed Garbled Circuits

D. Boneh, C. Gentry, S. Gorbunov, S. Halevi, Valeria Nikolaenko, G. Segev, V. Vaikuntanathan, D. Vinayagamurthy
Decrypt using secret key for \([x, f]\):

**Fully Key-Homomorphic Encryption (FKHE): Intuition**

\[
\text{Enc}(pp, k, m) \xrightarrow{f} \text{Enc}(pp, [f(k), f], m) \xrightarrow{g} \text{Enc}(pp, [g(f(k)), g\cdot f], m)
\]

**Setup**
- Public key
- Message
- New public key

**KeyGen for \([x, f]\)**
- Secret key

**Decrypt using secret key for \([x, f]\)**
- New public key

\[
\begin{align*}
&\text{if } f(k) = x & m \\
&\text{otherwise} & \bot
\end{align*}
\]
FKHE Syntax

- Setup($1^\lambda$) → pp, msk

- Enc(pp, k, message) → c[k]
  Encryption under pk = [k]

- Eval(pp, f, c[k]) → c[f(k), f]
  Encryption under pk = [f(k), f]

- KeyGen(msk, [x, f]) → sk[x, f]
  Secret key for pk = [x, f]

- Dec(c[f(k), f], sk[x, f]) → message iff f(k) = x
Application: KP-ABE with short secret keys (review key policy ABE) [SW05]

User holding $SK_f$ & $Enc_{PK}(x, m)$ learns $m$ if $f(x) = 1$ ⊥ otherwise
Application: KP-ABE with short secret keys (review key policy ABE) [SW05]

Charlie

\[ \text{Enc}_{PK}(x, m) \]

Alice: PhD student \( \land (\text{CS} \lor \text{EE}) \)

\( SK_{f_1} \)

Bob: PhD student \( \land \text{Law} \)

\( SK_{f_2} \)

\[ x = (\text{PhD student, CS}) \]

Alice learns m
Bob learns nothing about m
KP-ABE from FKHE (key generation)

Alice

Policy: $f$

sk for $[1, f] \leftarrow$ FKHE-KeyGen(...)

$\text{pp, msk} \leftarrow$ FKHE-Setup($1^\lambda$)
KP-ABE from FKHE (decryption)

Key for policy $f$ is $sk[1, f]$

Alice: $sk[1, f]$

Charlie

$FKHE$-$Enc(pp, X, m) \xrightarrow{f} FKHE$-$Enc(pp, [f(x), f], m)$

If $f(x) = 1$ can decrypt with $sk[1, f]$
Our new KP-ABE (key policy)

• Short secret keys: key size depends on depth, not on size (despite large policy embedded in secret key)

• Expressive policies: arithmetic circuits, not just boolean

• Arbitrary fan-in gates

• Delegatable ABE
Simple KP-ABE Delegation

Our scheme supports delegation:
Alice can create a custom restricted secret key \textit{herself}.

\begin{align*}
\text{Policy:} & \quad f \\
\text{Alice:} & \quad \text{sk}[1, f] \\
\text{Delegate:} & \quad \text{sk}[1, f\land g]
\end{align*}
## Previous work on KP-ABE

<table>
<thead>
<tr>
<th>Polices</th>
<th>Security</th>
<th>Key size</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPSW06, HW13</td>
<td>Monotone formulas</td>
<td>O(size)</td>
</tr>
<tr>
<td>OT10</td>
<td>Span programs</td>
<td>O(size)</td>
</tr>
<tr>
<td>Wat12</td>
<td>DFA</td>
<td>O(size)</td>
</tr>
<tr>
<td>OSW12</td>
<td>Any formula</td>
<td>O(size)</td>
</tr>
<tr>
<td>SW12, GGH12, GGHSW13</td>
<td><strong>Boolean circuits</strong></td>
<td>O(size)</td>
</tr>
<tr>
<td>Boy13</td>
<td>Boolean formulas</td>
<td>O(size)</td>
</tr>
<tr>
<td>GVW13</td>
<td><strong>Boolean circuits</strong></td>
<td>O(size)</td>
</tr>
<tr>
<td><strong>This</strong></td>
<td>Arithmetic circuits</td>
<td>short: O(depth)</td>
</tr>
</tbody>
</table>
FKHE Security definition ("selective")

Note: Selective security to adaptive security by complexity leveraging more queries

Easy Thm: FKHE is secure ⇒ KP-ABE is secure
Compressed Garbled Circuits [Yao’86]

Alice (x) \[\text{garbled circuit: LARGE}\] \[\text{garbled input: small}\] \[\text{For new x or y, repeat}\] \[\text{f(x, y)}\] Bob (y)

Using our ABE: becomes small

[This] \[\Rightarrow \]

“One-time” garbled circuits
FHE
KP-ABE with short keys
\[\Rightarrow \] Reusable succinct garbled circuit

[GKPVZ’13]
## Compressed Garbled Circuits

| Garbled Circuit | $O(|C| \times \text{poly}(\lambda))$ | $O(|C| + \text{poly}(\lambda)^*)$ |
|-----------------|--------------------------------------|-----------------------------------|
| Garbled Input   | $O(|x| \times \text{poly}(\lambda))$ |                                   |
|                 | GC: All “classical” constructions     | GC + Reusable-GC:                 |
|                 | Reusable-GC: [GKPVZ’13]              | [This] (assuming LWE)             |
|                 |                                       | (from fully key homomorphic enc.)|
|                 | $O(|x| + \text{poly}(\lambda)^*)$   |                                   |
|                 | GC: [AIKW’13]                        |                                   |
|                 | (assuming RSA, DDH etc.)             | [This] (assuming multilinear maps) |
|                 | (exploit add. key hom.)              |                                   |
|                 | Reusable-GC:                         |                                   |
|                 | [This]                               |                                   |
|                 |                                       | ????

- GC: Generalized Circuits
- Reusable-GC: [GKPVZ’13] (assuming RSA, DDH etc.)
- GC + Reusable-GC: [This] (assuming LWE)
Constructing FKHE
FKHE from LWE (encryption) (similar to [ABB10, AFV11, MP12])

- **Setup** ($1^λ, 2$)
  - Create $pp \leftarrow (A, B_1, B_2, D)$, $msk = T_A$ (trapdoor of A)

- **Enc**(pp, $x_1, x_2, \mu$)

  $$c = (A \mid x_1G + B_1 \mid x_2G + B_2 \mid D)^T s + e + (0|0|0|\mu \cdot \left\lfloor \frac{q}{2} \right\rfloor)$$

  **Eval:**

  $$f \quad G \in \mathbb{Z}_{q}^{n \times m} \quad (\text{fixed matrix with a known trapdoor})$$

  $$c = (A \mid f(x_1, x_2)G + B_f \mid D)^T s + e' + (0|0|\mu \cdot \left\lfloor \frac{q}{2} \right\rfloor)$$

We show: this encryption scheme is fully key-homomorphic
FKHE from LWE (evaluation)

• Consider two ciphertexts:

\[ c_1 = (x_1 \cdot G + B_1)^T s + e_1 \]
\[ c_2 = (x_2 \cdot G + B_2)^T s + e_2 \]

Encryption under \( \text{pk} = [x_1, x_2] \)

Encryption under \( \text{pk} = [x_1 + x_2, +] \)

• Addition

\[ c_1 + c_2 = ( (x_1 + x_2) \cdot G + (B_1 + B_2) )^T s + e \]

Encoding of ‘+’
FKHE from LWE \textit{(evaluation)}

- Consider two ciphertexts:
  
  \[ c_1 = (x_1 \cdot G + B_1)^T s + e_1 \]
  \[ c_2 = (x_2 \cdot G + B_2)^T s + e_2 \]

- **Multiplication** \textit{(small \( x_2 \))}:
  - find low norm \( R \) s.t. \( G \cdot R = -B_1 \)
  - \( x_2 \cdot c_1 + c_2 \cdot R = ( (x_1 x_2) \cdot G + B_2 \cdot R )^T s + e \)

\begin{itemize}
  \item Encryption under \( \text{pk} = [x_1, x_2] \)
  \item Encryption under \( \text{pk} = [x_1 x_2, \times] \)
\end{itemize}
FKHE from LWE (evaluation)

- Evaluate arithmetic circuit $f$ gate-by-gate

- Output ciphertext:
  \[ c_f = (f(x_1, x_2) \cdot G + B_f)^\top s + e_f \]

- Secret key:
  \[ sk[y, f] = R \in \mathbb{Z}_q^{2m \times m} \quad \text{s.t.} \quad (A | y \cdot G + B_f) \cdot R = D \]
Conclusion

• New primitive: Fully Key-Homomorphic Encryption (FKHE)
• Construction from LWE with short secret keys
• Two applications:
  • Key Policy Attribute Based Encryption
    • Short keys: size depends only on depth of policy circuit
    • Arithmetic circuits with arbitrary fan-in gates
    • Delegatable
  • Reusable **compressed** garbled circuits
• Reusable **compressed garbled inputs** from Mmaps

Short ciphertext KP-ABE from Mmaps

Thank you! Questions? valerini@stanford.edu