Fully Secure Attribute Based Encryption from Multilinear Maps

Sanjam Garg  IBM Research  UC Berkeley
Craig Gentry  IBM Research
Shai Halevi  IBM Research
Mark Zhandry  Stanford University
ABE for Circuits
ABE for Circuits

Circuit $C, CT = Enc(C,m)$

$x_1 \quad C(x_1) = 0$

$x_2 \quad C(x_2) = 0$

$x_4 \quad C(x_4) = 1$

$x_3 \quad C(x_3) = 0$

$x_5 \quad C(x_5) = 0$

$x_7 \quad C(x_7) = 1$

$x_6 \quad C(x_6) = 1$
ABE for Circuits

Circuit $C, CT = Enc(C, m)$

- $x_1$ with $C(x_1) = 0$
- $x_2$ with $C(x_2) = 0$
- $x_3$ with $C(x_3) = 0$
- $x_4$ with $C(x_4) = 1$
- $x_5$ with $C(x_5) = 0$
- $x_6$ with $C(x_6) = 1$
- $x_7$ with $C(x_7) = 1$
Desired Security Model: Adaptive Security

\[ b \leftarrow \{0,1\} \]

\[ \text{Enc}(\mathsf{PP}, \mathsf{C}, m_b) \]

\[ \mathsf{C} \text{ such that } \mathsf{C}(x_i) = 0 \forall i, m_0, m_1 \]

\[ x_i \text{ such that } \mathsf{C}(x_i) = 0 \]

\[ \mathsf{sk}_{x_i} \]

\[ \mathsf{x}_i \]

\[ \mathsf{sk}_{x_i} \]

\[ \mathsf{pp} \]
Previous Constructions: Selective Security*

[GVW’13, GGHSW’13, …]

\[ b \leftarrow \{0,1\} \]

\[ \text{Enc}(PP, C, m_b) \]

\[ x_i \text{ such that } C(x_i) = 0 \]

\[ \text{sk}_{x_i} \]

* Independent and concurrent work: [Wat’14] adaptively secure FE from iO
Our Contribution

Adaptively secure ABE

• Based on dual system framework
• Composite order asymmetric m-maps
• (Relatively) simple assumptions
  • Related to common dual system assumptions
  • Circuit independent
• New garbling technique
• No complexity leveraging

ePrint: 2014/622