Fully Secure Attribute Based Encryption from Multilinear Maps

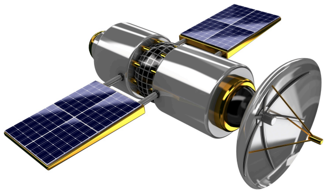
Sanjam Garg
IBM Research
UC Berkeley

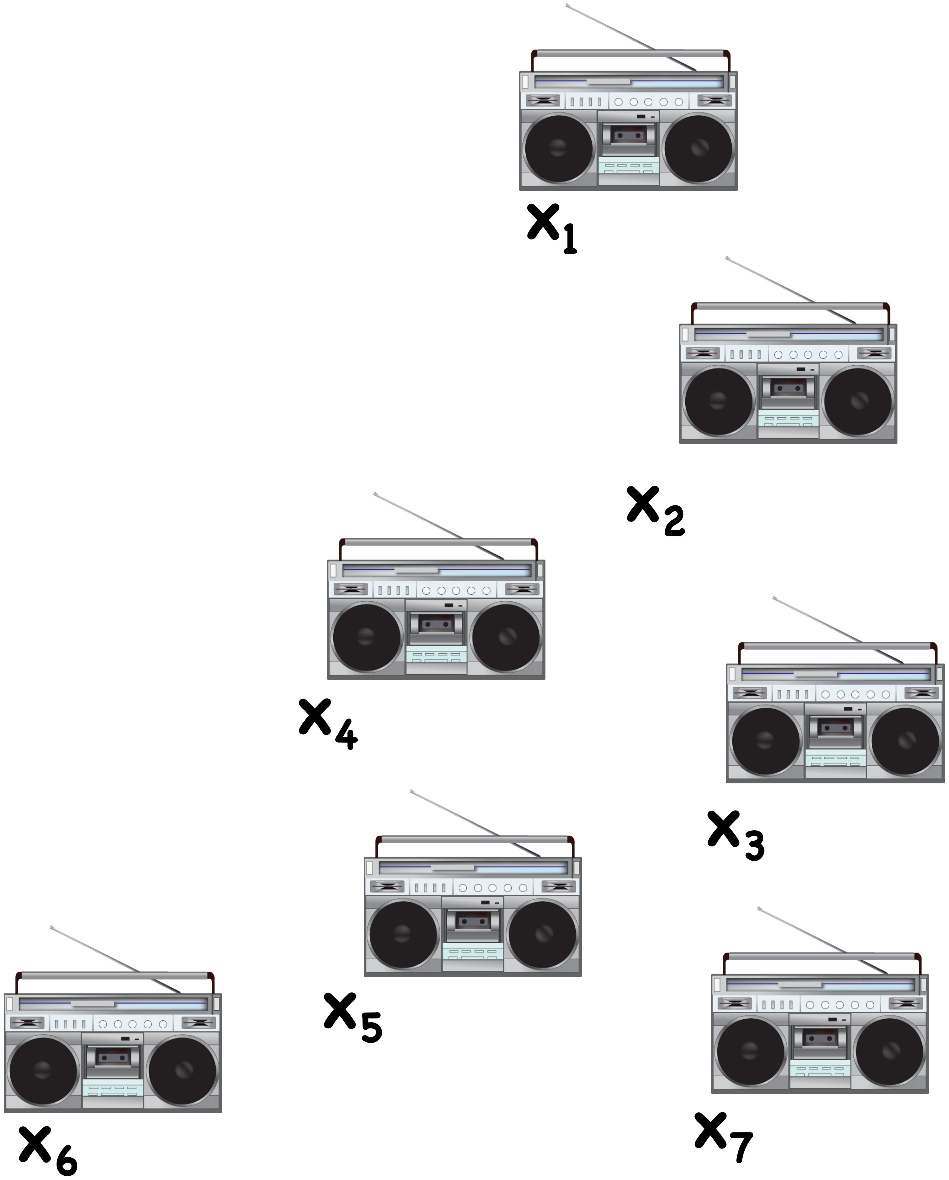
Craig Gentry
IBM Research

Shai Halevi
IBM Research

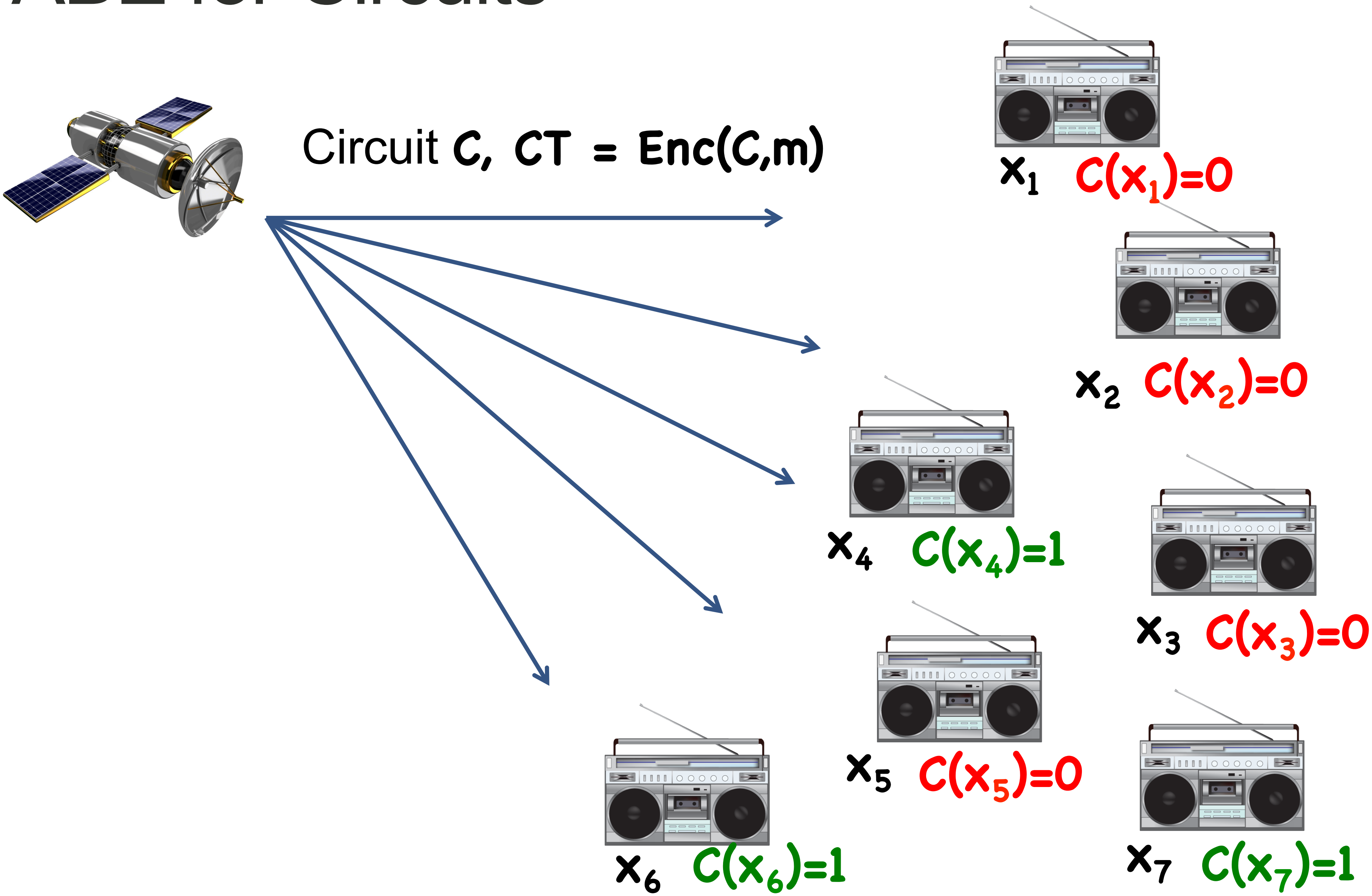
Mark Zhandry
Stanford University

ABE for Circuits





ABE for Circuits



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

x_1 $C(x_1)=0$

x_2 $C(x_2)=0$

x_4 $C(x_4)=1$

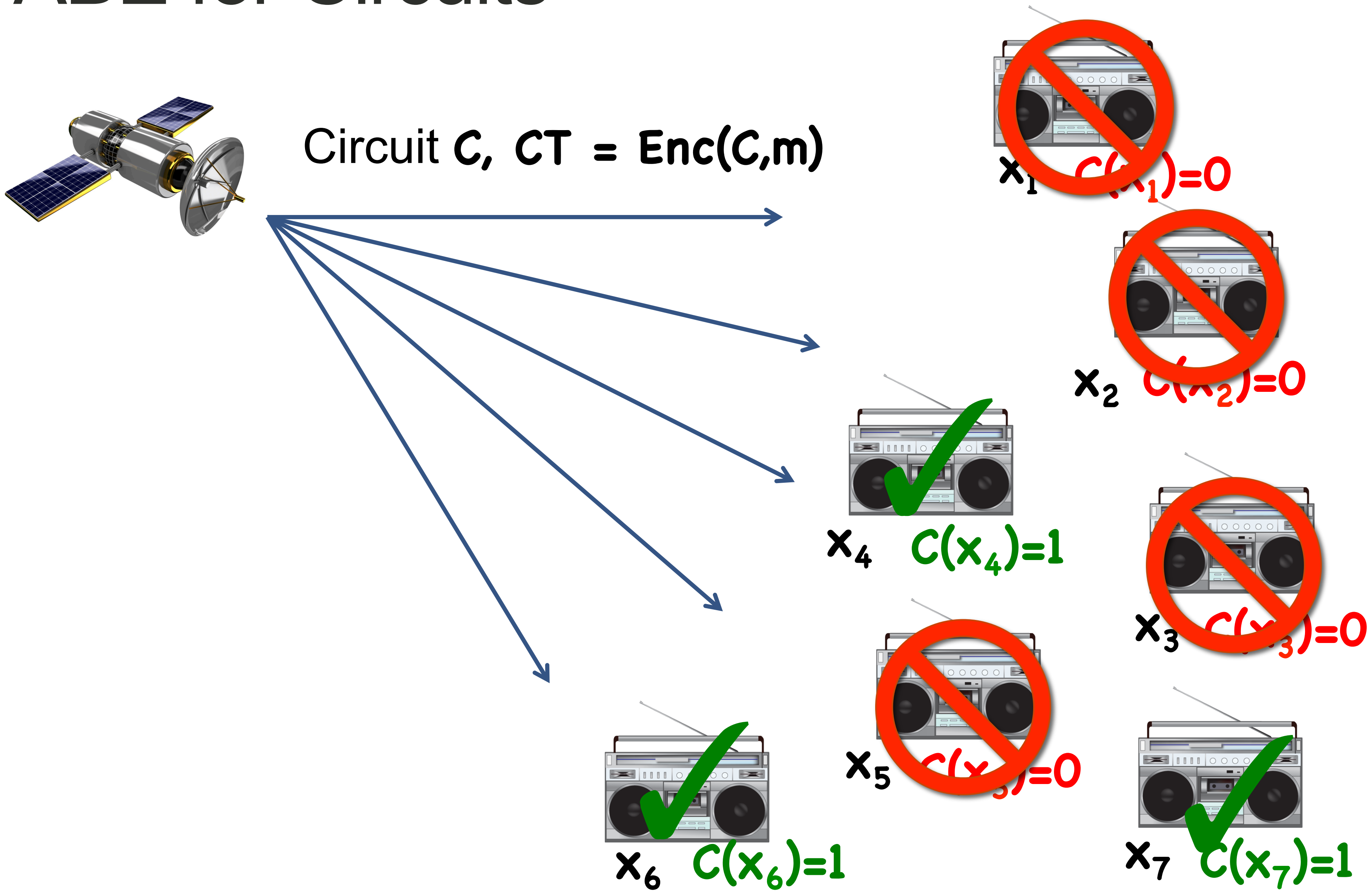
x_3 $C(x_3)=0$

x_5 $C(x_5)=0$

x_6 $C(x_6)=1$

x_7 $C(x_7)=1$

ABE for Circuits



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

x_1 $C(x_1)=0$

x_2 $C(x_2)=0$

x_4 $C(x_4)=1$

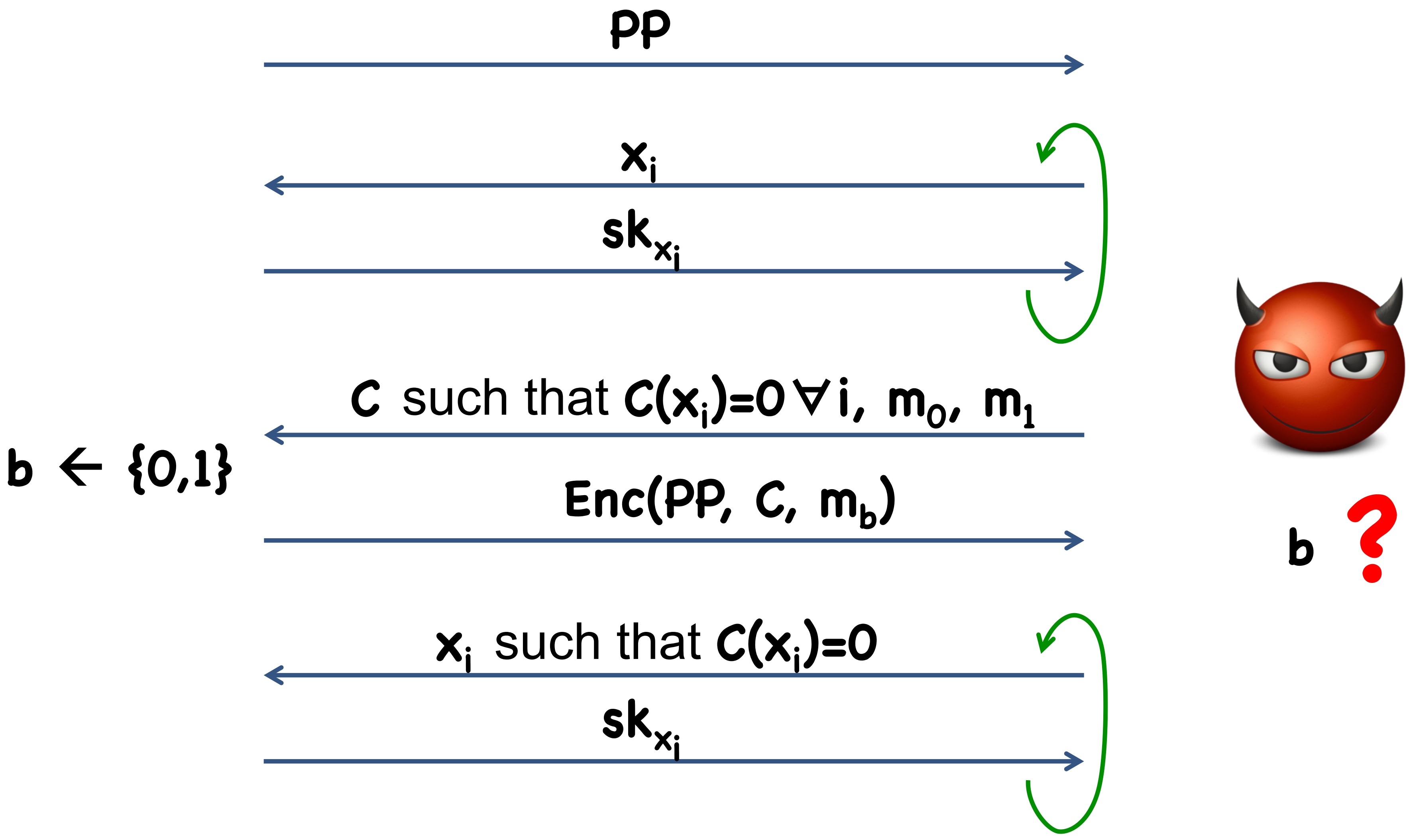
x_3 $C(x_3)=0$

x_5 $C(x_5)=0$

x_6 $C(x_6)=1$

x_7 $C(x_7)=1$

Desired Security Model: Adaptive Security



PP

x_i

sk_{x_i}

C such that $C(x_i)=0 \; \forall i$, m_0, m_1

$b \leftarrow \{0,1\}$

Enc(PP, C, m_b)

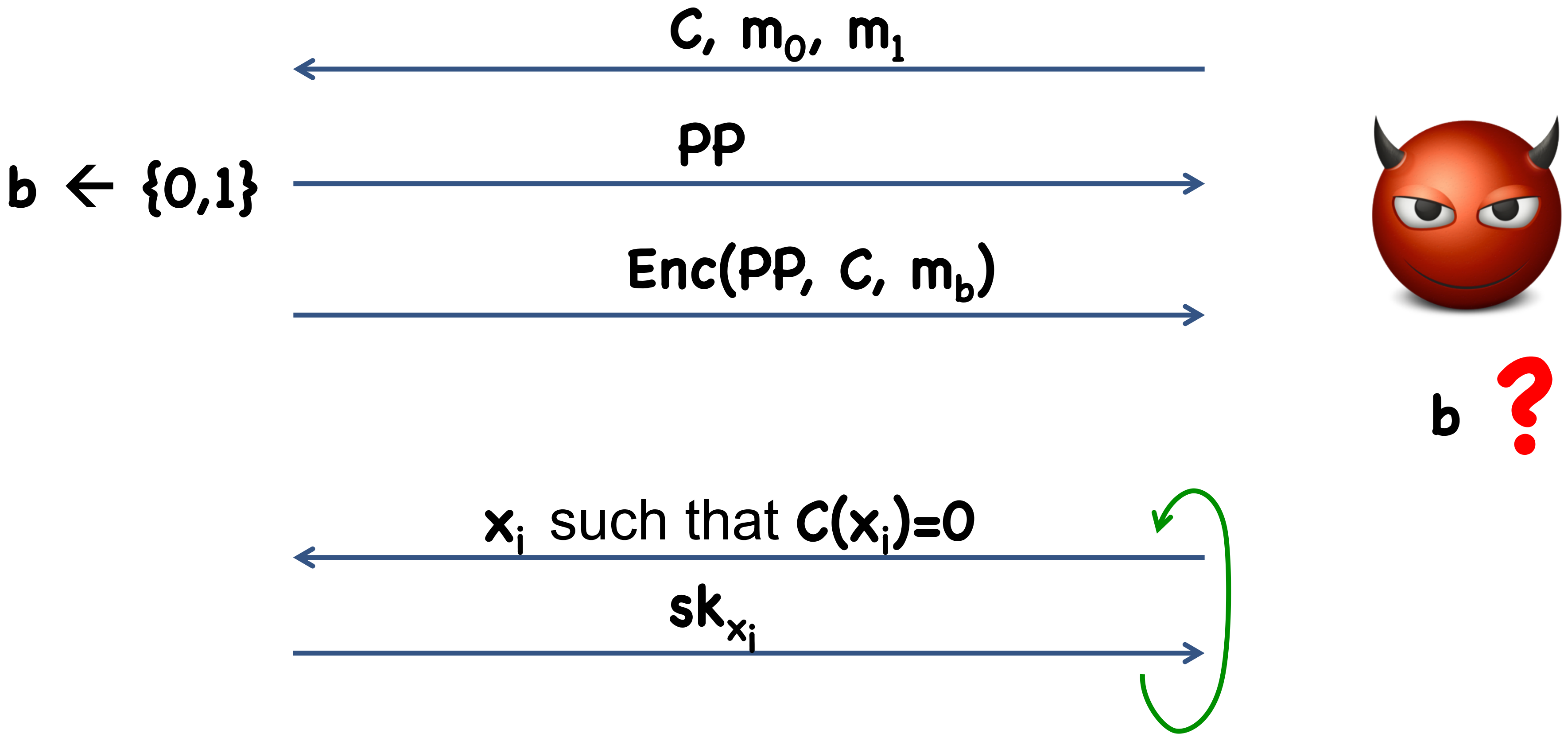
b ?

x_i such that $C(x_i)=0$

sk_{x_i}

Previous Constructions: Selective Security*

[GVW'13, GGHSW'13, …]



C, m_0, m_1

PP

$b \leftarrow \{0,1\}$

$\mathrm{Enc}(PP, C, m_b)$

b ?

x_i such that $C(x_i)=0$

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