Attribute-Based Signatures for Circuit from Bilinear Map

Yusuke Sakai (AIST, Japan)

Nuttapong Attrapadung (AIST, Japan)

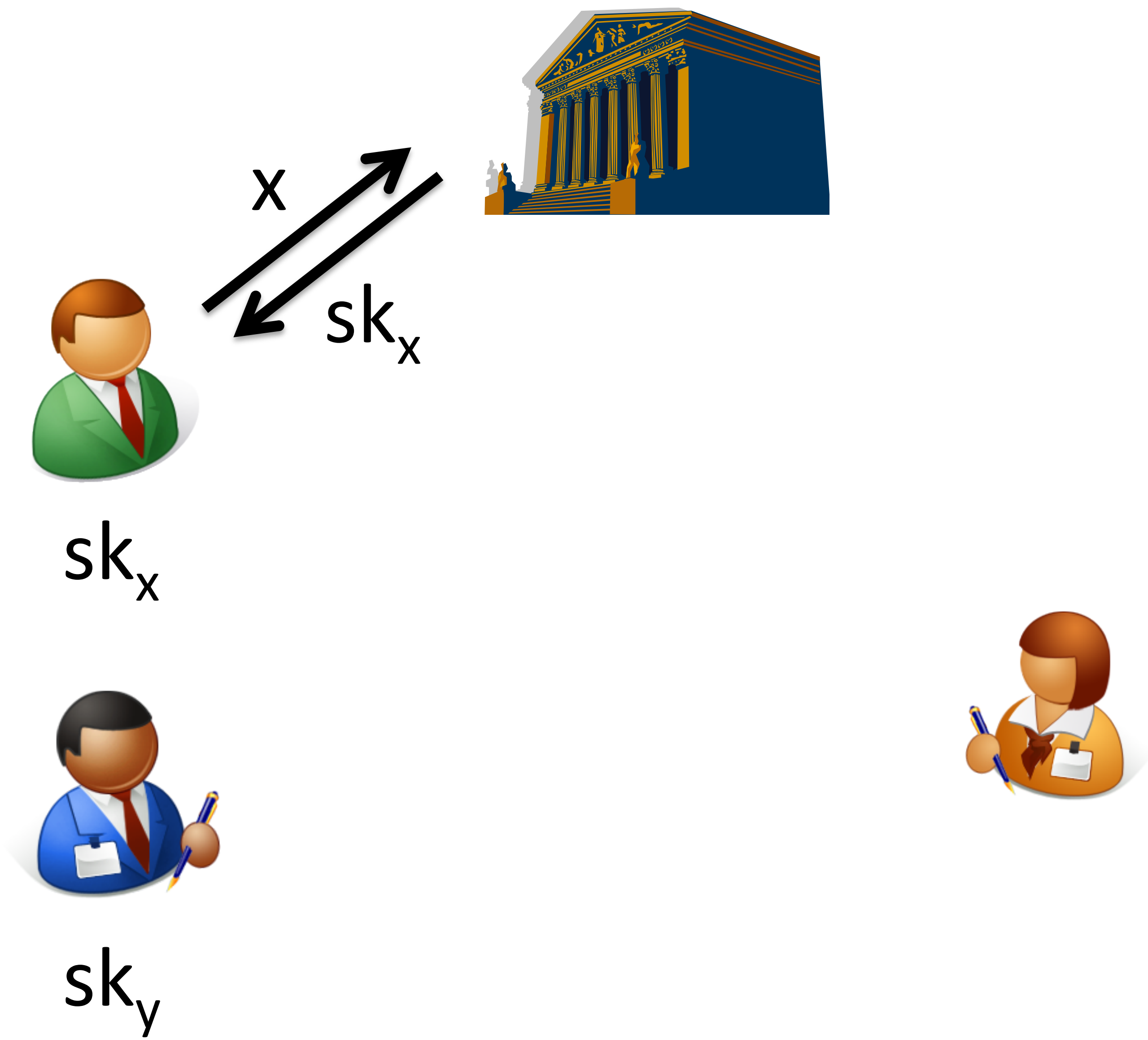
Goichiro Hanaoka (AIST, Japan)

Our Contribution

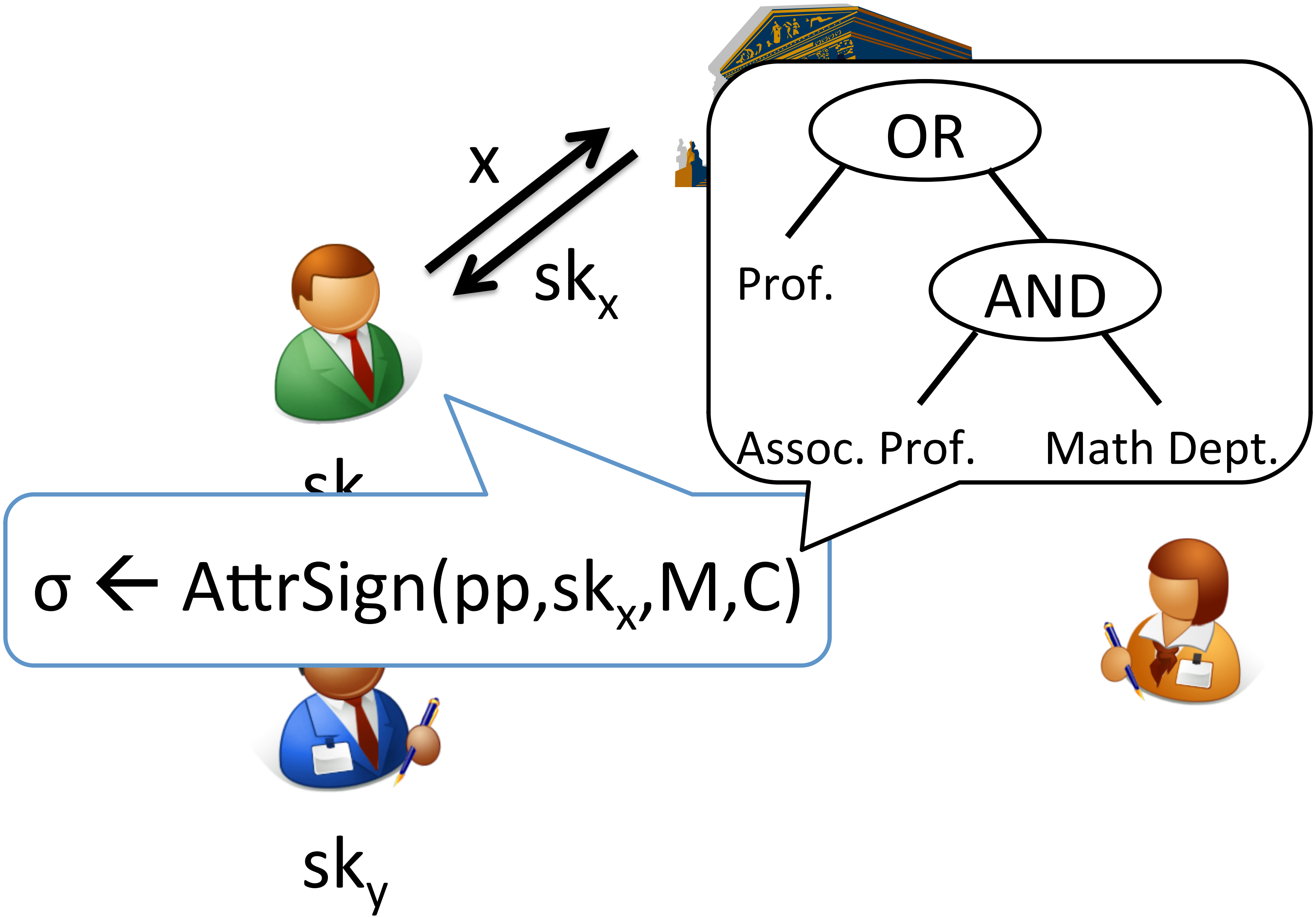
- Propose attribute-based signature scheme for ***arbitrary circuits***
  - Secure under SXDH assumption in ***bilinear groups***
  - Fairly practical
  - No a priori bound on size and depth of circuits

The first scheme that simultaneously achieves ***simplicity of assumption***, ***efficiency***, and ***expressiveness of predicates!***

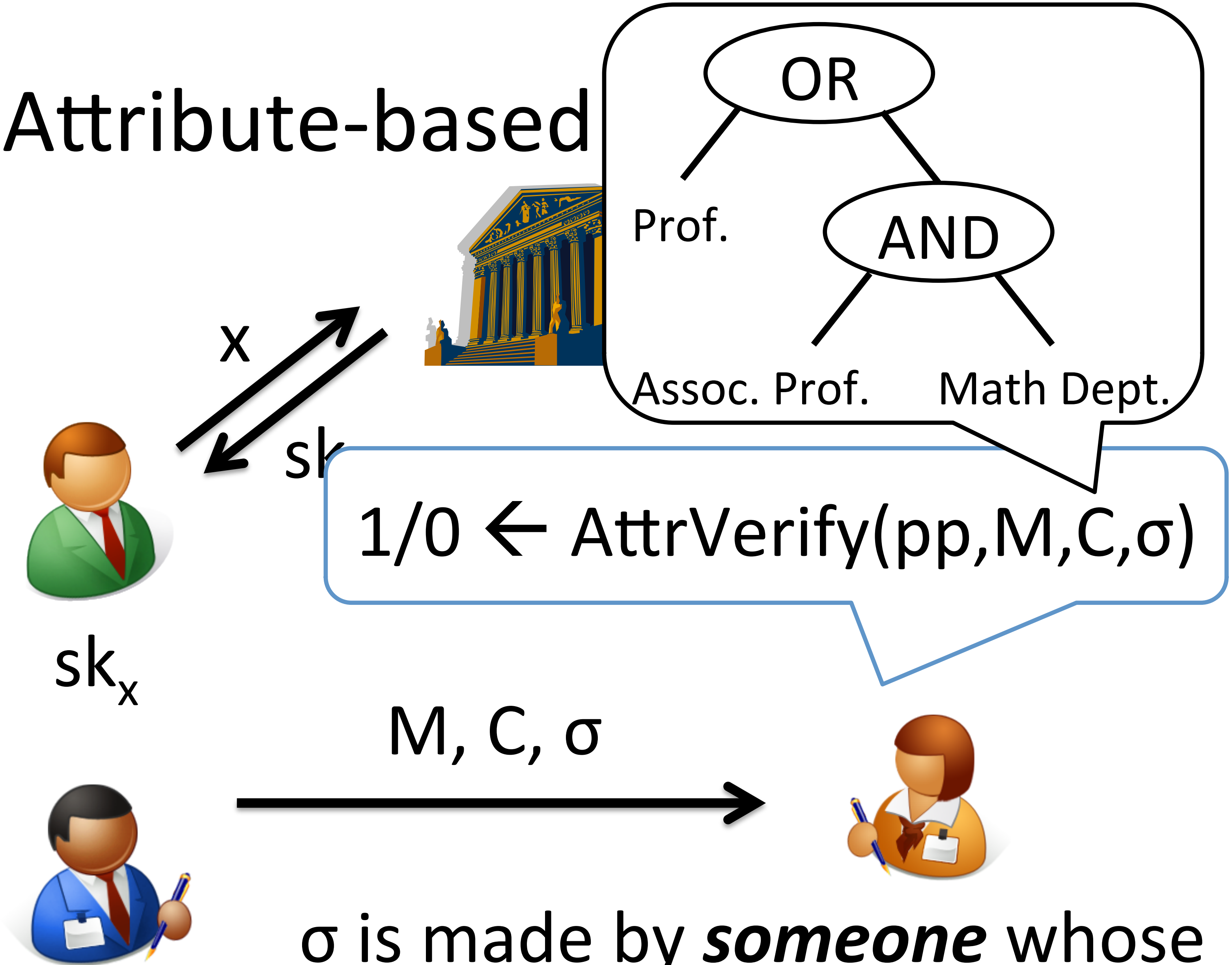
Attribute-based Signatures



Attribute-based Signatures



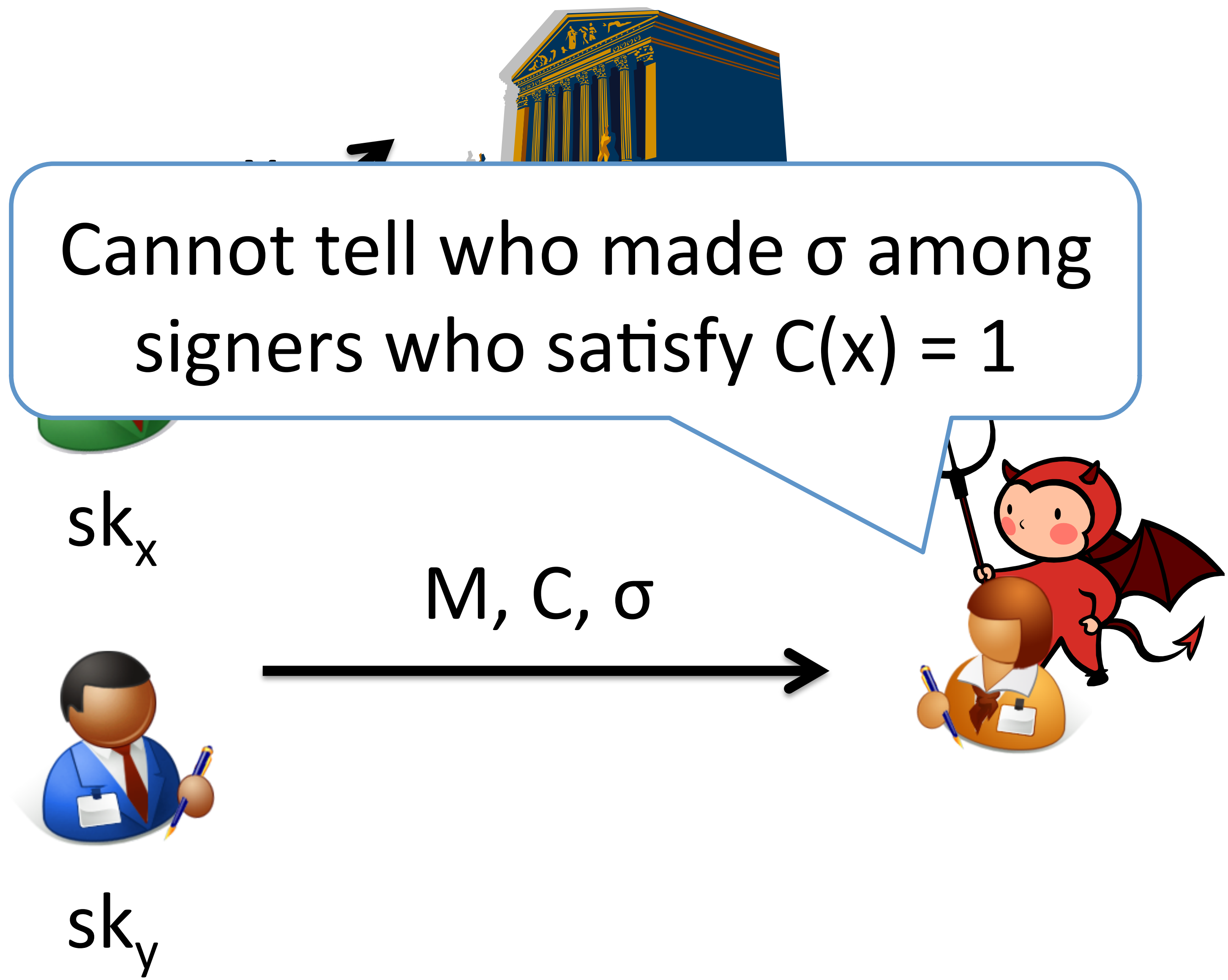
Attribute-based



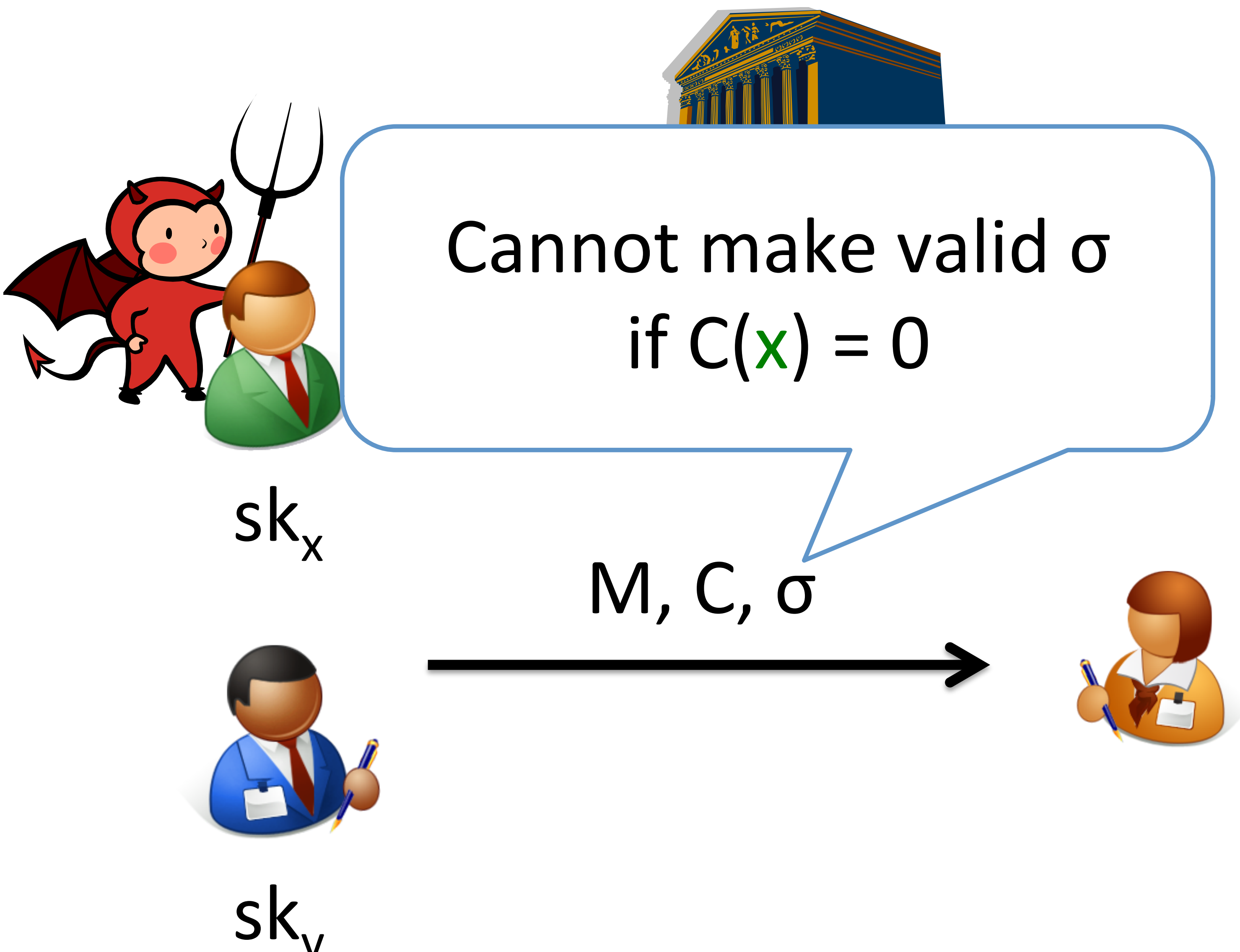
sk_y

σ is made by ***<u>someone</u>*** whose attributes x satisfy C(x) = 1

Anonymity


Cannot tell who made σ among signers who satisfy C(x) = 1
sk_x
M, C, σ
sk_y

Unforgeability



Previous Work

[MPR11] The notion, schemes monotone span programs
(bilinear groups)

[OT11] non-monotone span programs
(bilinear groups)

[BF14] (1) AND/OR of pairing product equation
(2) Arbitrary circuit via Karp reduction (implicit)
(generic construction from policy-based signature)

[TLL14] bounded-depth circuits (multilinear maps)

Previous Work

[MPR11] The notion, schemes ***monotone span programs***
(bilinear groups)

[OT11] ***non-monotone span programs***
(bilinear groups)

[BF14] (1) ***AND/OR of pairing product equation***
(2) Arbitrary circuit via ***Karp reduction*** (implicit)
(generic construction from policy-based signature)

[TLL14] bounded-depth circuits (***multilinear maps***)

Previous Work

[MPR11] The notion, schemes ***monotone span programs***
(bilinear groups)

[O

No known scheme simultaneously achieves
simplicity of assumption, ***efficiency***, and
expressiveness of predicates!

[E

(2) Arbitrary circuit via ***Karp reduction*** (implicit)
(generic construction from policy-based signature)

[TLL14] bounded-depth circuits (***multilinear maps***)

Our Contribution

- Propose attribute-based signature scheme for ***arbitrary circuits***
  - Secure under SXDH assumption in bilinear groups
  - Fairly practical
  - No a priori bound on size and depth of circuits
- Use NIZK and signature as building blocks
  - Make a ***"fusion"*** of Groth-Sahai proofs and Groth-Ostrovsky-Sahai proofs

Groth-Sahai (GS) Proofs

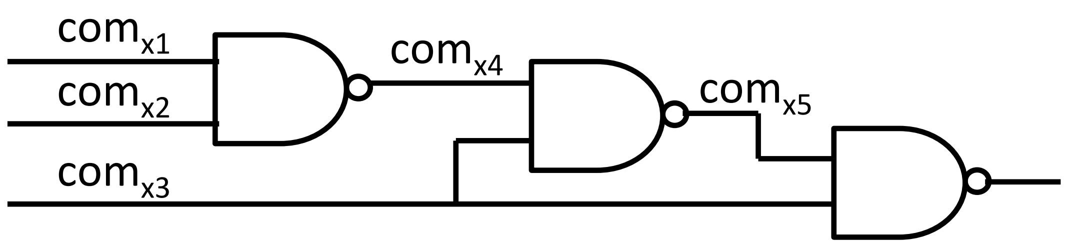
- Non-interactive proofs suitable for proving algebraic equation

$$\prod_{i=1}^{n} e(\mathcal{A}_i, \mathcal{Y}_i) \prod_{j=1}^{m} e(\mathcal{X}_j, \mathcal{B}_j) \prod_{i=1}^{n} \prod_{j=1}^{m} e(\mathcal{X}_i, \mathcal{Y}_j)^{\gamma_{i,j}} = T$$

- Proof consists of two phases:
  – To commit to the witness group elements
  – To prove the elements committed to satisfies the equation to be proven

Groth-Ostrovsky-Sahai (GOS) Proofs

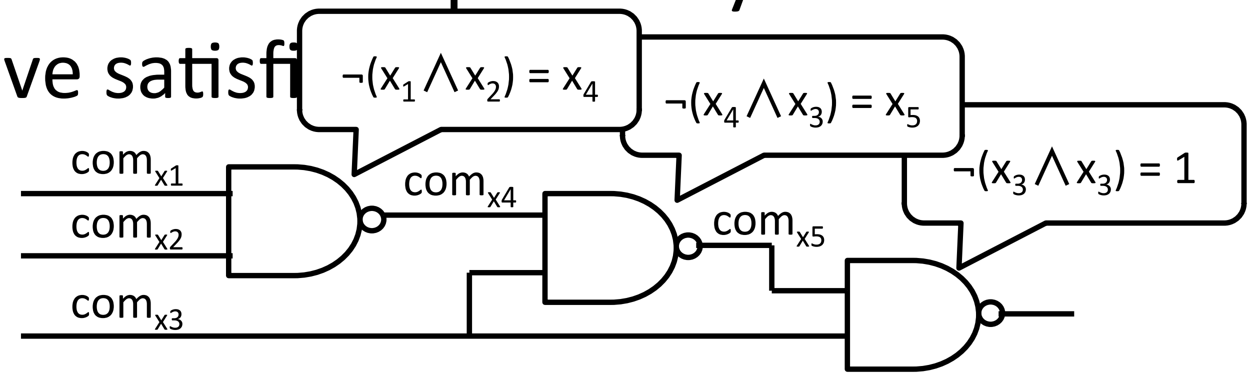
- Non-interactive proofs system which can prove satisfiability of circuits



- Proof consists of two phases:
  - To commit to each assignments to wires
  - To prove the assignments committed to follows input/output relation of each gate

Groth-Ostrovsky-Sahai (GOS) Proofs

- Non-interactive proofs system which can prove satisfi



- Proof consists of two phases:
  - To commit to each assignments to wires
  - To prove the assignments committed to follows input/output relation of each gate

Overview of the Proposed Scheme

msk

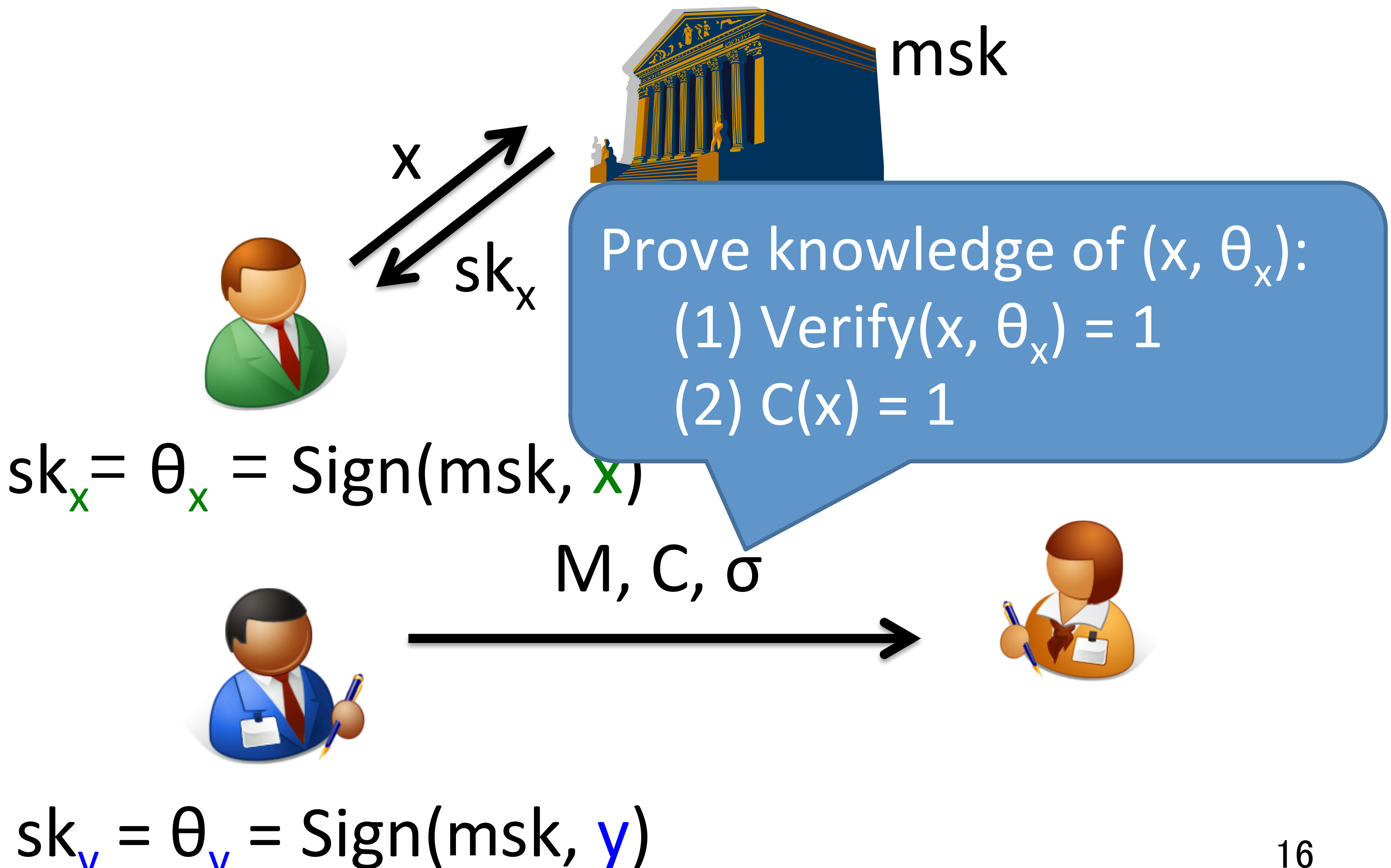
x

Each signer receives ***a signature on his attribute***

$sk_x = \theta_x = \mathrm{Sign}(msk, x)$

$sk_y = \theta_y = \mathrm{Sign}(msk, y)$

Overview of the Proposed Scheme



Overview of the Proposed Scheme

Prove knowledge of (x, θ_x):

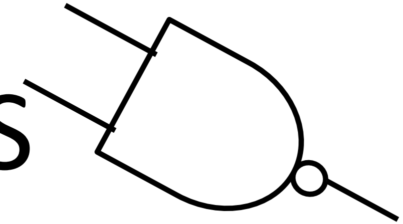
(1) $\mathrm{Verify}(x, \theta_x) = 1$

(2) $C(x) = 1$

- GS proofs are suitable for (1), while GOS proofs are suitable for (2)
- If we have a “fusion” of GS proofs and GOS proofs…?

$e(g^x, h^y) = T$

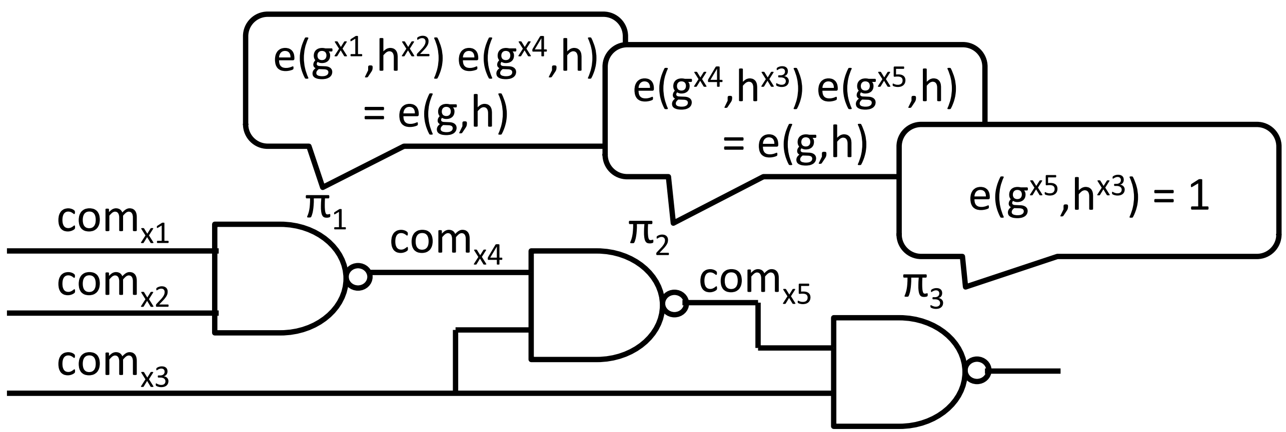
"Fusion" of GS and GOS



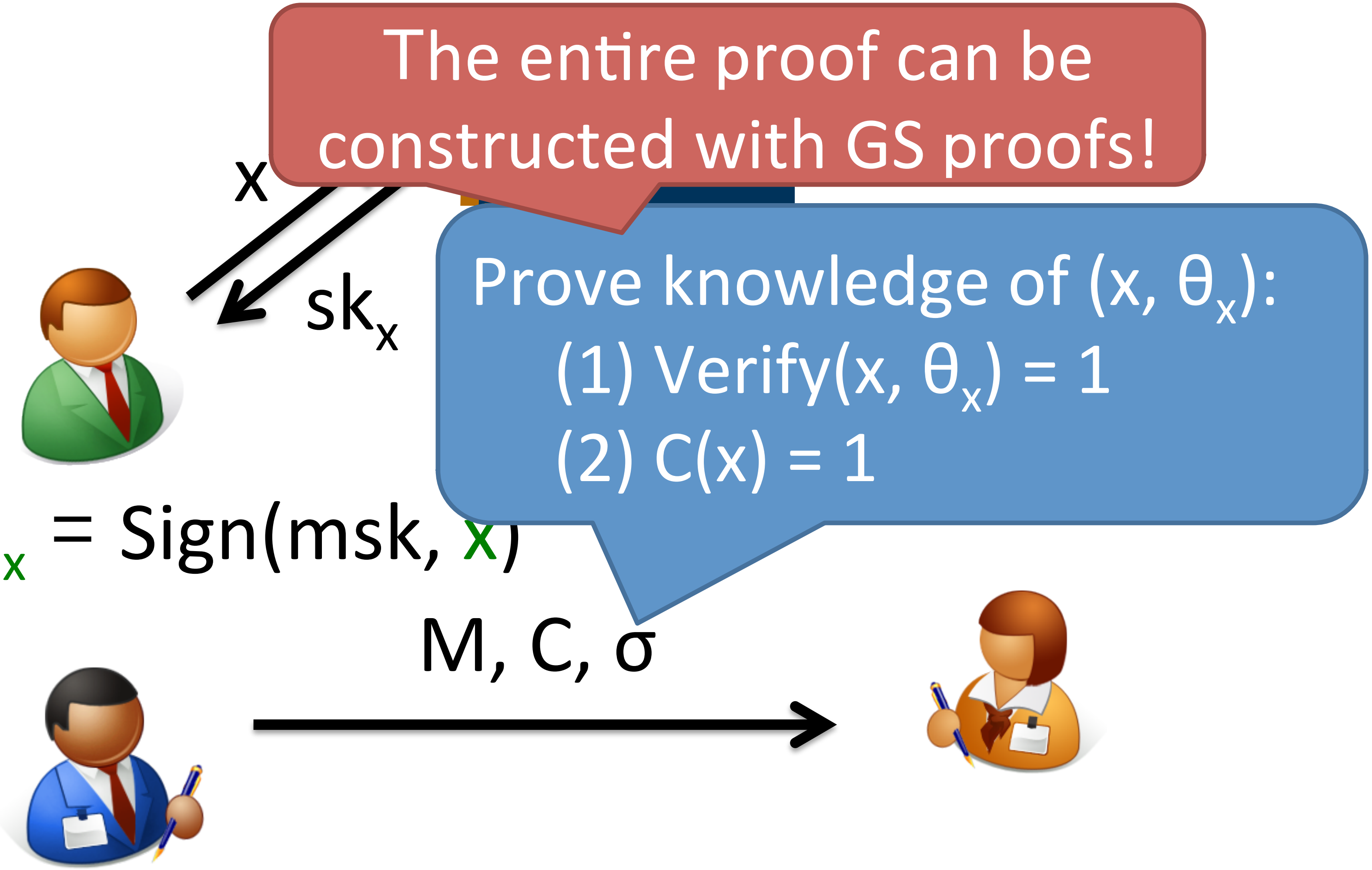
- Both follow the ***"commit-and-prove"*** structure
- Translate ***"$\neg(x \wedge y) = z$"*** into algebraic equation
- $\neg(x \wedge y) = z$

  $\Leftrightarrow 1 - xy = z$

  $\Leftrightarrow$ ***$e(g, h)\, e(g^x, h^y)^{-1} = e(g^z, h)$***



Overview of the Proposed Scheme

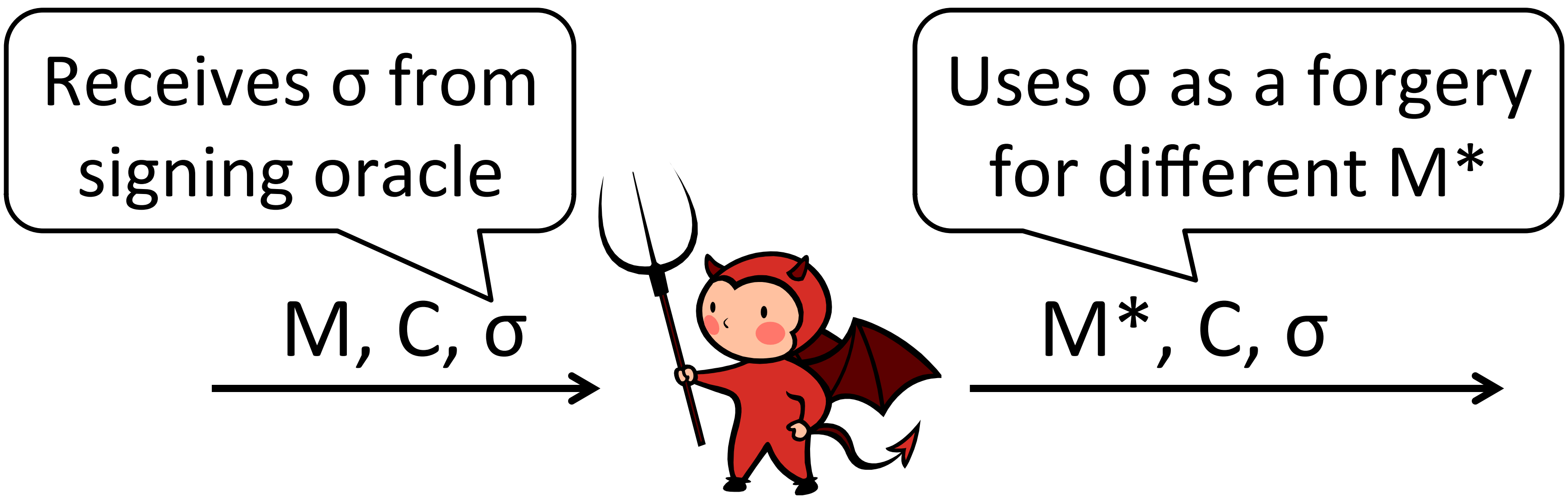


$sk_x = \theta_x = \text{Sign}(msk, x)$

$sk_y = \theta_y = \text{Sign}(msk, y)$

But…

- It doesn’t provide ***<u>CMA security</u>***
- σ is not bound to M



Dummy Attribute [MPR11]

M, C, σ

Prove knowledge of (x, θ_x):

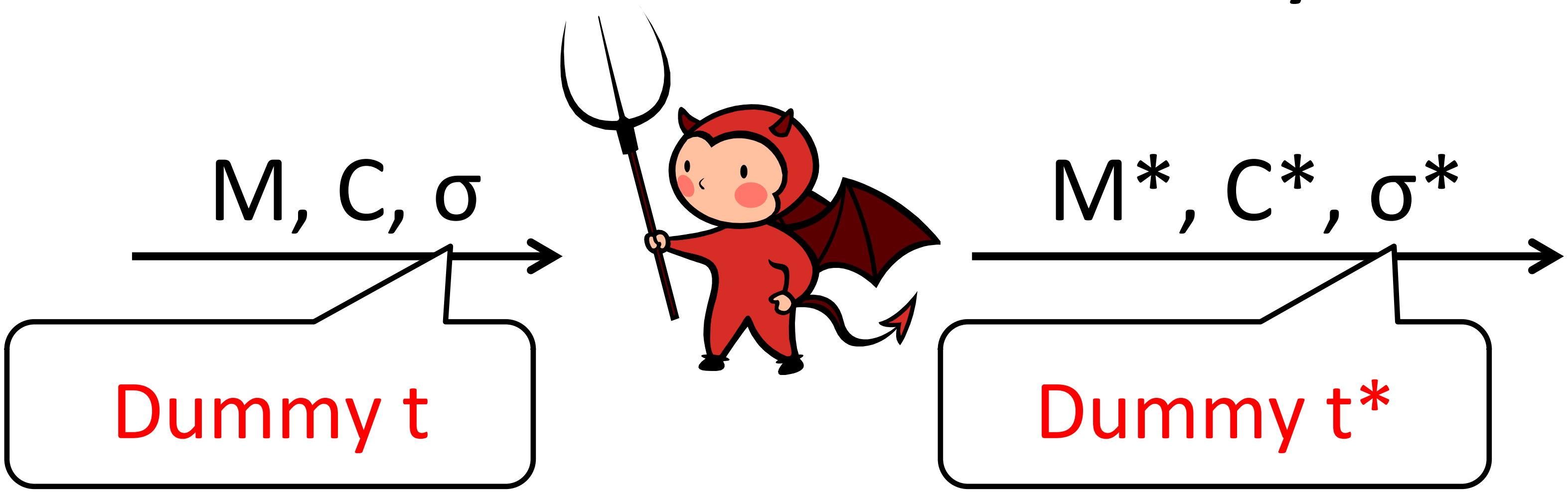
θ_x is (a) Signature on x s.t. $C(x) = 1$ ***OR*** (b) Signature on dummy t defined by M

Point

Use different t for different M

[MPR11] Hemanta K. Maji, Manoj Prabhakaran, Mike Rosulek: Attribute-Based Signatures. CT-RSA 2011: 376-392

Intuition for Security



- If adversary sees (M, C, σ) and outputs (M*, C*, σ*), the reduction
  - uses ***signature on t*** for simulating σ,
  - extracts ***signature on t**** from σ*
    - Reduction works successfully because t ≠ t*

Main Theorem

Theorem Non-interactive proof system is witness-indistinguishable and extractable, signature scheme is unforgeable, the proposed scheme is anonymous and unforgeable

Instantiate this with
GS proofs in SXDH setting and
Kiltz-Pan-Wee structure-preserving signature

Theorem If SXDH assumption holds, the proposed scheme satisfies anonymity and unforgeability

Performance

	Signature size [Group Elements]	Assumption	Predicate
[MPR11] (1)	36s+2t+24ks	q-SDH, SXDH	Monotone Span Program
[MPR11] (2)	28s+2t+12k+8	SXDH	Monotone Span Program
[MPR11] (3)	s+t+2	Generic Group	Monotone Span Program
[OT11]	9s+11	DLIN	Non-Monotone Span Program
Ours	$12\ell+20N+26$	SXDH	Non-monotone Circuit

k: Security parameter
s×t: Size of span program
ℓ: Input size of circuit
N: Number of gates in circuit

Almost same performance
as previous schemes
while more expressive!!!

Our Contribution

- Propose attribute-based signature scheme for ***arbitrary circuits***
  - Secure under SXDH assumption in bilinear groups
  - Fairly practical
  - No *a priori* bound on size and depth of circuits
  - Use Groth-Sahai proofs and Kiltz-Pan-Wee structure-preserving signature as building blocks