

An abstract painting in a cubist style, featuring a vibrant cityscape. The scene is composed of numerous rectangular and triangular shapes in a variety of colors including red, blue, yellow, green, and purple. These shapes represent buildings, houses, and possibly a sailboat in the upper left. The overall effect is a dynamic and colorful representation of an urban environment.

Building Cryptography for Big Data

Shweta Agrawal
IIT Madras

Road Map

- Motivation
- Some partial solutions
- Challenges and Opportunities for women in science



Big Data is Useful

- Cloud computing
- Efficiencies in cost, productivity, innovation
- Development: fighting poverty
 - Scientists combined satellite imagery and machine learning to predict poverty
- Smart Cities & Meters
- Healthcare



Can we use all this technology without violating individual privacy?



Paranoia about Privacy →
Reluctance to share data →
Conflict with Big Data Benefits



Personalized Medicine

“The dream for tomorrow’s medicine is to understand the links between DNA and disease — and to tailor therapies accordingly. But scientists have a problem: how to keep genetic data and medical records secure while still enabling the massive, cloud-based analyses needed to make meaningful associations.”

Erika Check Hayden, *Nature*, 2015



Case Study: Cloud Computing

- Functionality:

- Store big data on cloud
- Cloud can perform expensive computations for us

Plus Security:

- Access control on encrypted data
- Compute on encrypted data (eg medical research)

Plus Efficiency:

- Running time should not depend on database size
- Support inputs of variable size



Cloud Computing

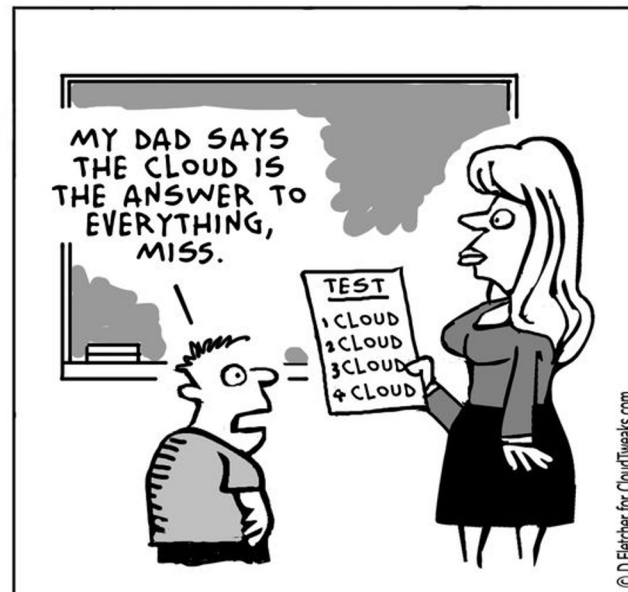
Having secure access to all your applications and data from any network device

What we want from a database in the cloud?

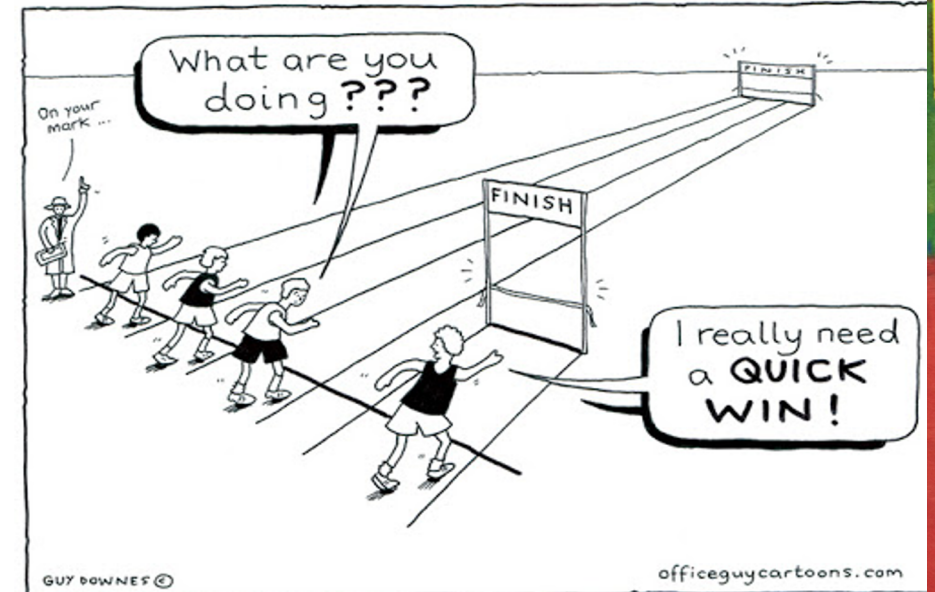
SECURITY



FUNCTIONALITY



EFFICIENCY

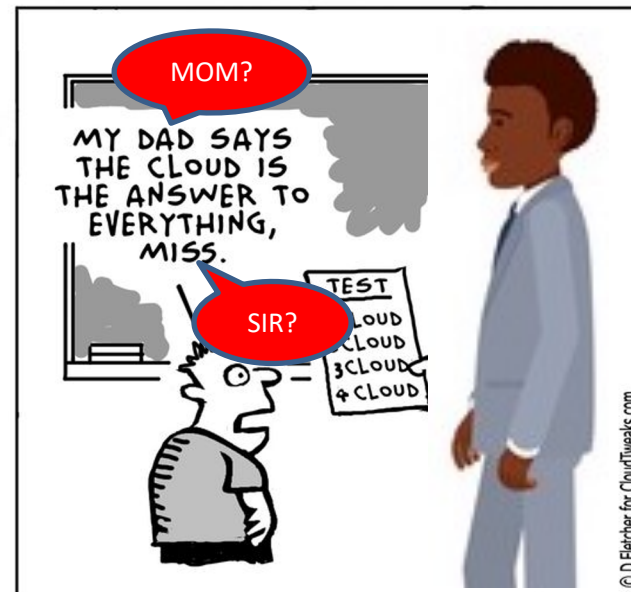


What we want from a database in the cloud?

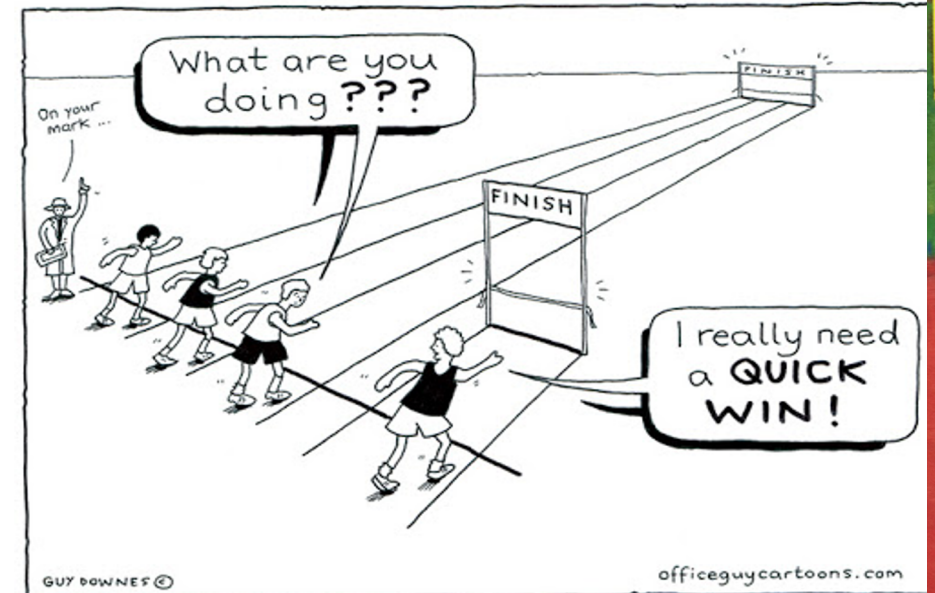
SECURITY



FUNCTIONALITY



EFFICIENCY



The background is an abstract composition of various colored rectangles and squares. The colors include red, blue, green, orange, yellow, and white. The shapes are arranged in a non-repeating, geometric pattern, reminiscent of Piet Mondrian's De Stijl movement. The colors are vibrant and the shapes are of different sizes, creating a complex visual texture.

Can cryptography meet the challenge?

Public Key Encryption



$(PK_{\text{Bob}}, SK_{\text{Bob}})$



$(PK_{\text{Alice}}, SK_{\text{Alice}})$

Public Key Encryption



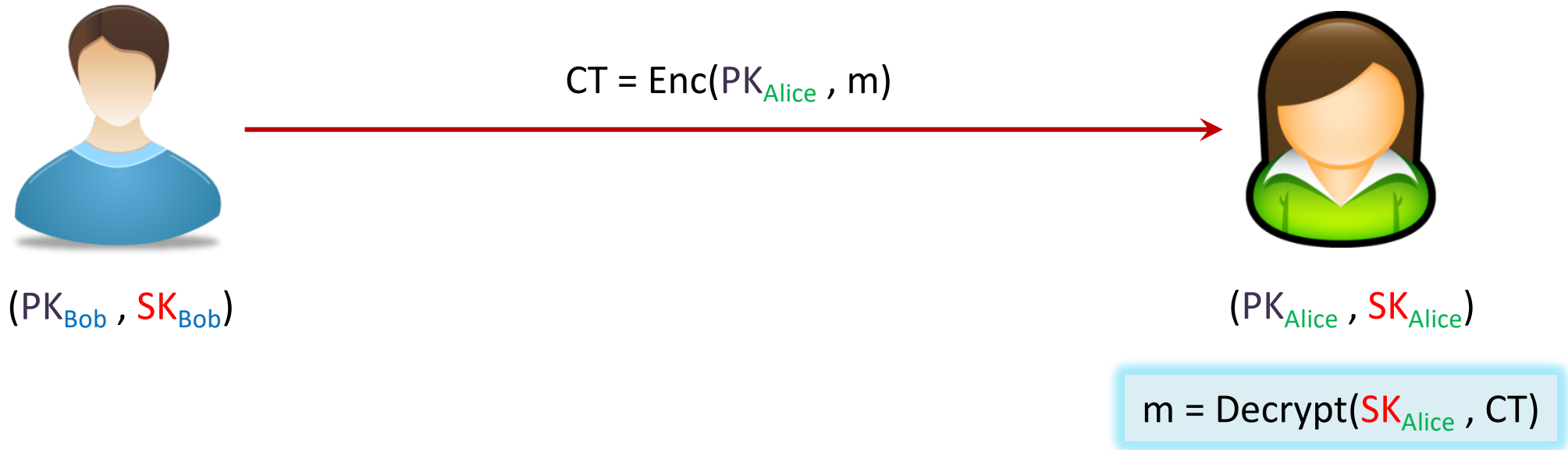
$(PK_{\text{Bob}}, SK_{\text{Bob}})$

$$CT = \text{Enc}(PK_{\text{Alice}}, m)$$

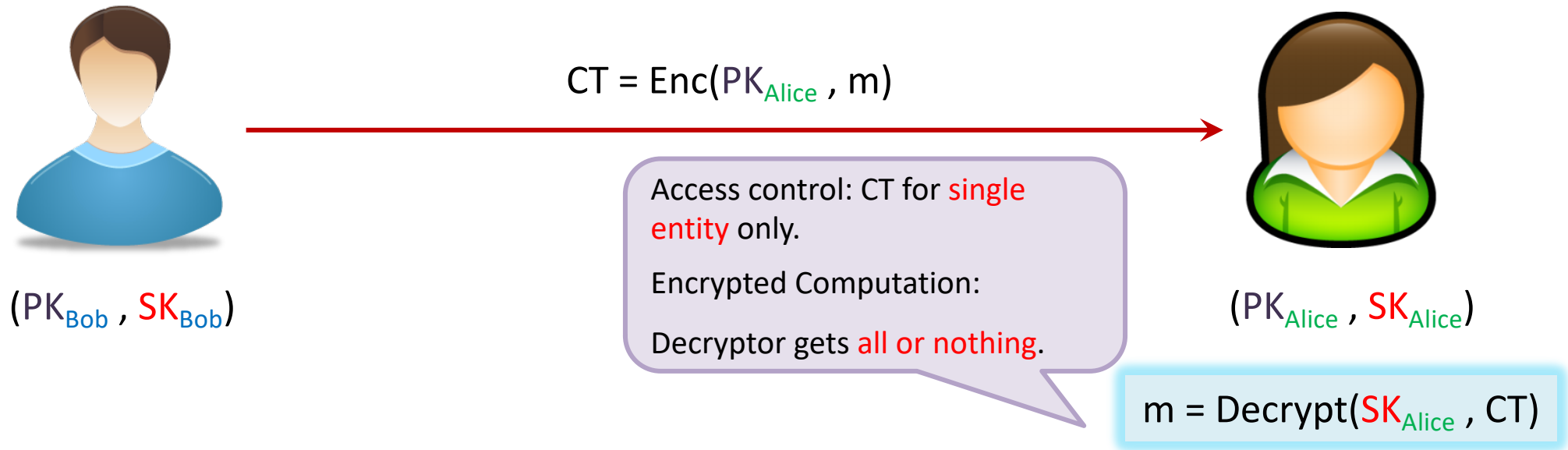


$(PK_{\text{Alice}}, SK_{\text{Alice}})$

Public Key Encryption



Public Key Encryption





Basic Requirement

Access control over encrypted data

Attribute Based Encryption!



Attribute based Encryption (ABE) [SW05, GPSW06]



File 1



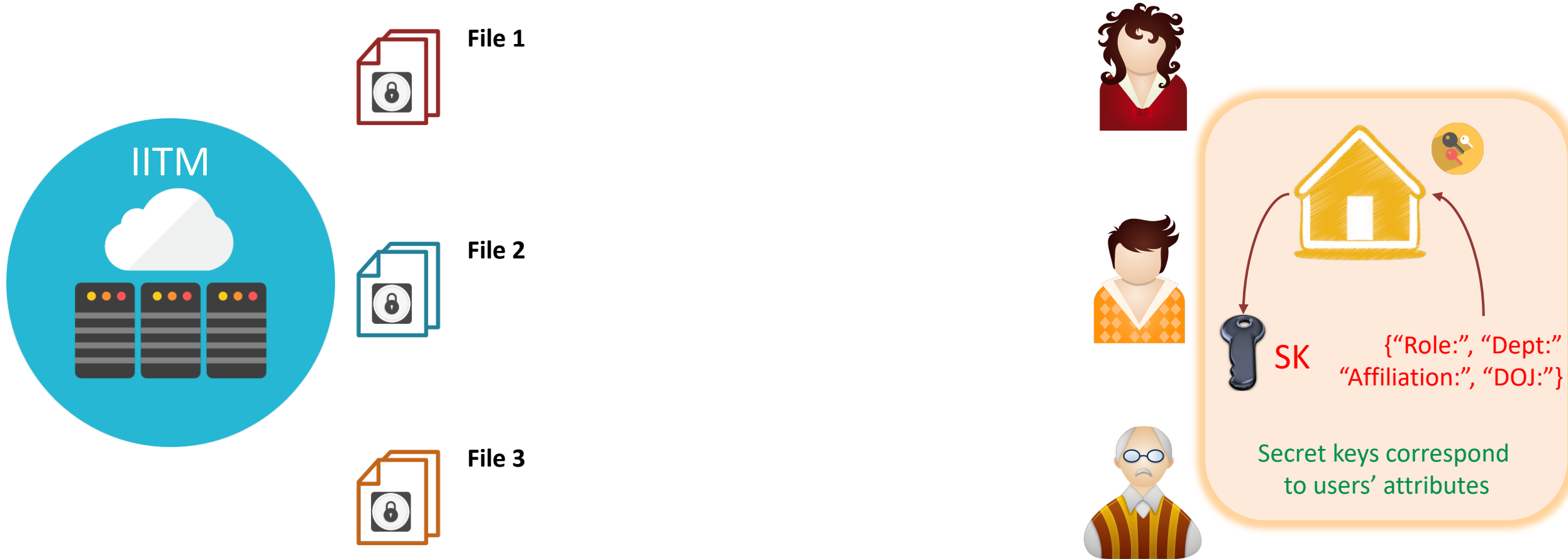
File 2



File 3



Attribute based Encryption (ABE) [SW05, GPSW06]

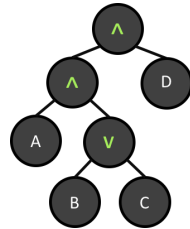


Attribute based Encryption (ABE) [SW05, GPSW06]

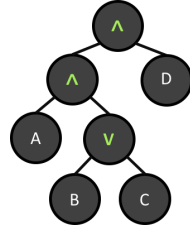
Encrypted with **same** PK
but **different** "policies"



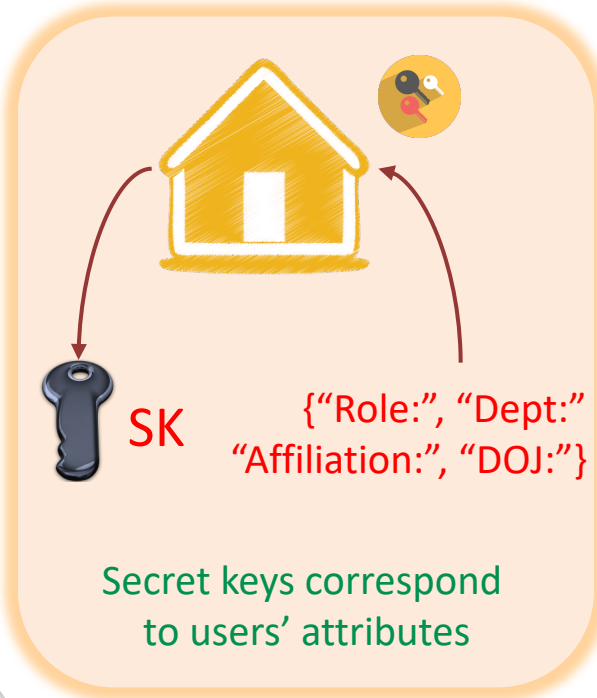
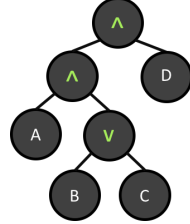
File 1



File 2



File 3

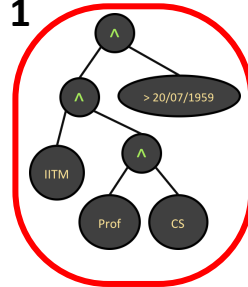


Attribute based Encryption (ABE) [SW05, GPSW06]

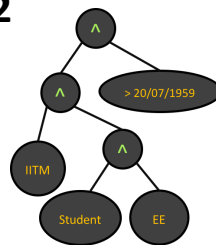
Encrypted with **same** PK
but **different** “policies”



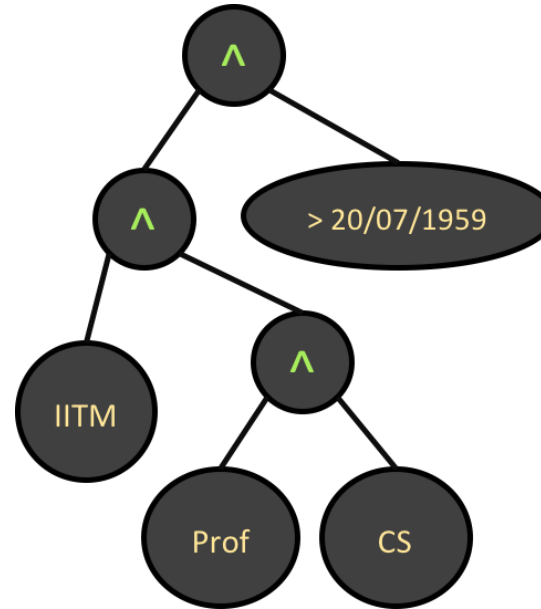
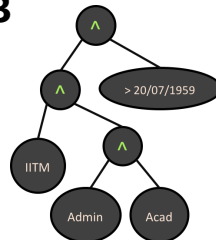
File 1



File 2



File 3



SK_{Prof}

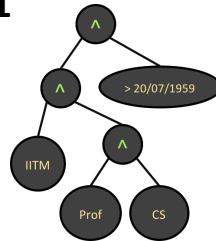
“Role: Professor”
“Dept: CS”
“Affiliation: IITM”
“DOJ: 01/01/95”

Attribute based Encryption (ABE) [SW05, GPSW06]

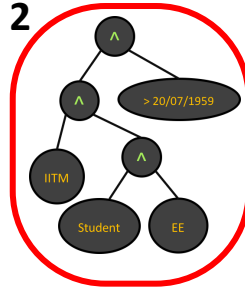
Encrypted with **same** PK
but **different** “policies”



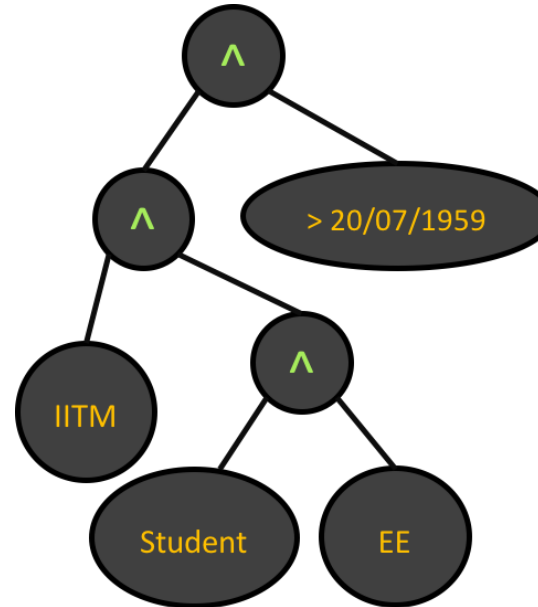
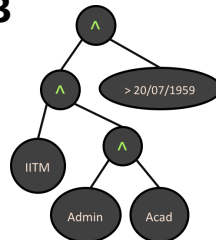
File 1



File 2



File 3



SK_{Stud}

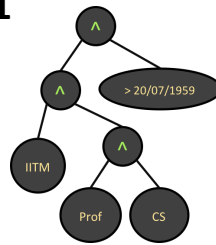
“Role: Student”
“Dept: EE”
“Affiliation: IITM”
“DOJ: 14/07/15”

Attribute based Encryption (ABE) [SW05, GPSW06]

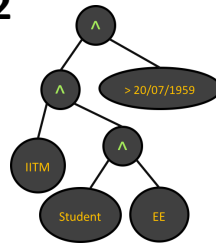
Encrypted with **same** PK
but **different** “policies”



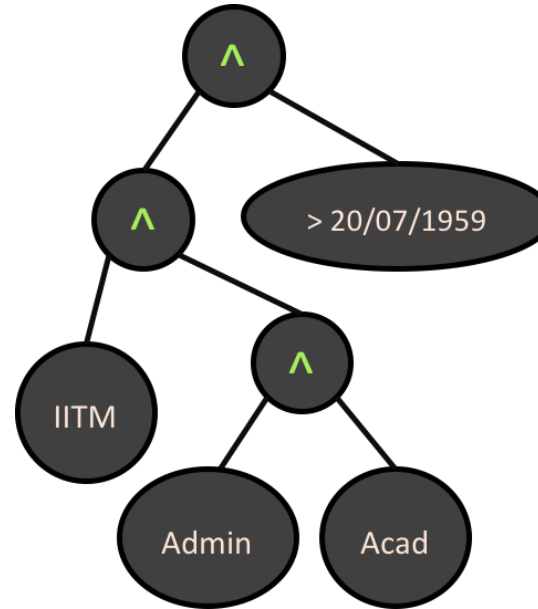
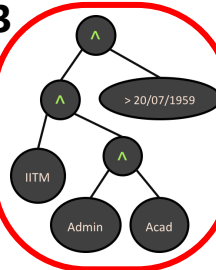
File 1



File 2



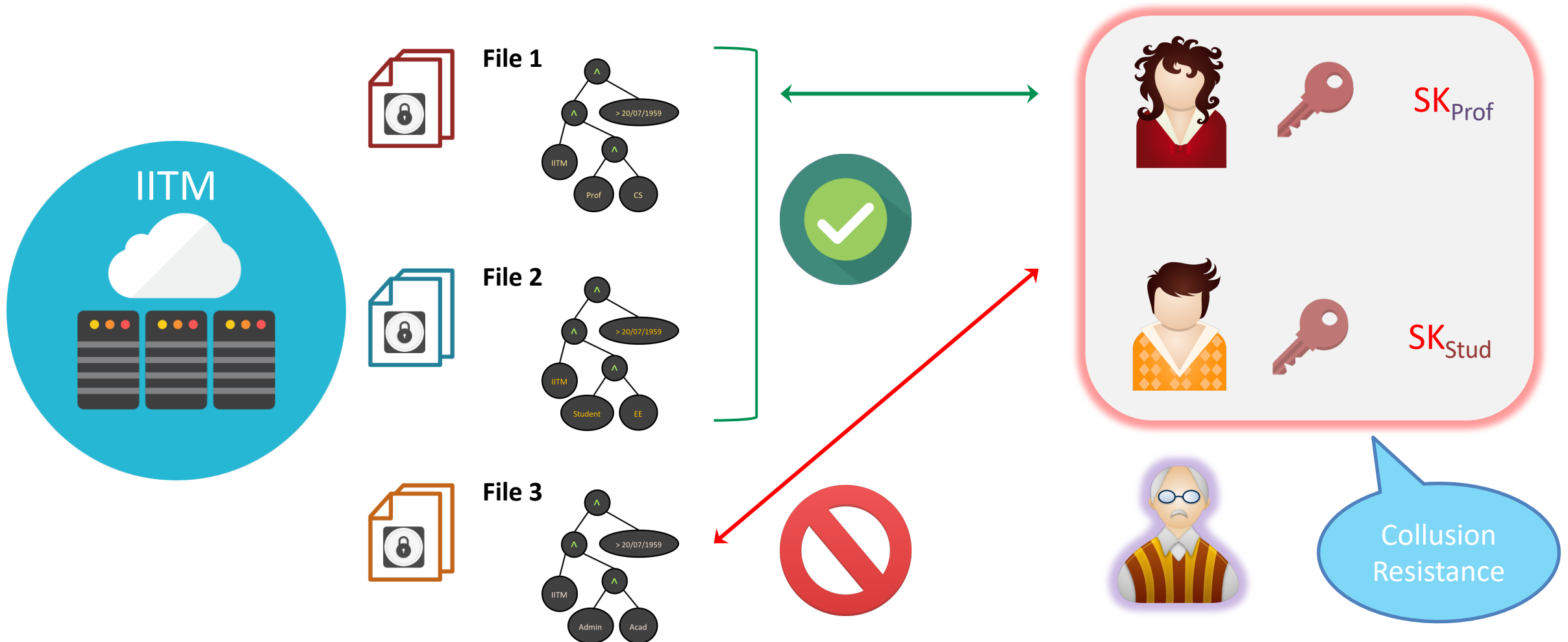
File 3



SK_{Admin}

“Role: Admin”
“Dept: Acad”
“Affiliation: IITM”
“DOJ: 28/02/14”

Attribute based Encryption (ABE) [SW05, GPSW06]

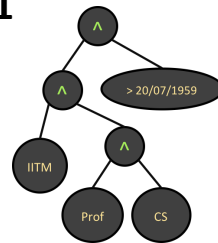


Ciphertext-Policy ABE

Encrypted w.r.t. "policies"



File 1

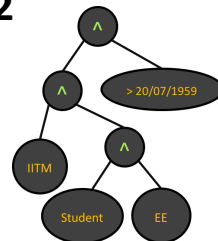


SK_{Prof}

"Role: Professor"
"Dept: CS"
"Affiliation: IITM"
"DOJ: 01/01/95"



File 2

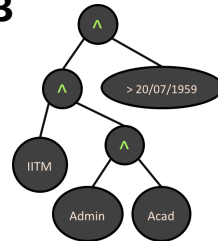


SK_{Stud}

"Role: Student"
"Dept: EE"
"Affiliation: IITM"
"DOJ: 14/07/15"



File 3



SK_{Admin}

"Role: Admin"
"Dept: Acad"
"Affiliation: IITM"
"DOJ: 28/02/14"

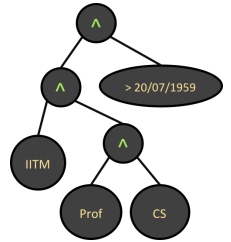
Key-Policy ABE [SW05]

Encrypted w.r.t. "attributes"



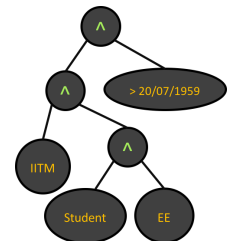
File 1

"Role: Professor"
"Dept: CS"
"Affiliation: IITM"
"DOJ: 01/01/95"



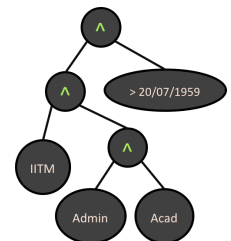
File 2

"Role: Student"
"Dept: EE"
"Affiliation: IITM"
"DOJ: 14/07/15"



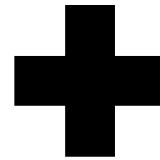
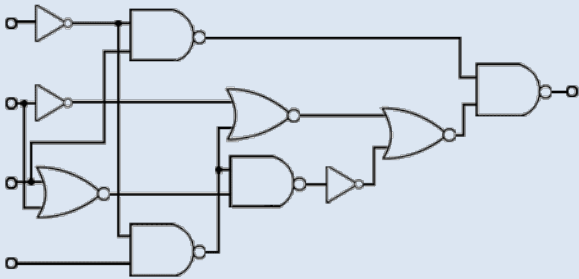
File 3

"Role: Admin"
"Dept: Acad"
"Affiliation: IITM"
"DOJ: 28/02/14"

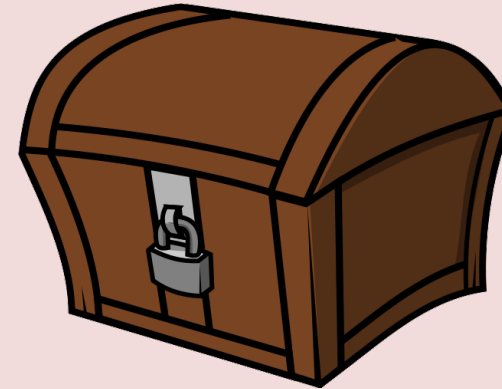


Generalization: Functional Encryption [BSW11, O'N10]

Secret Keys
for function f



Ciphertexts
for input x



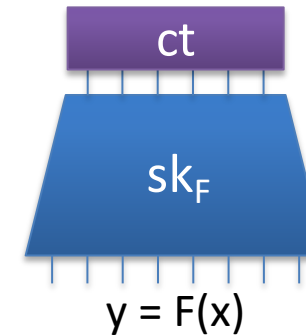
Decrypt to learn $f(x)$

Encryption with Partial Decryption Keys

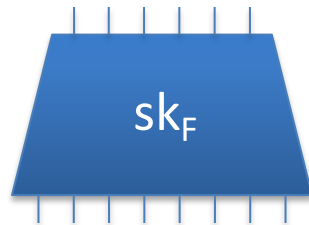
Encrypt (x):



Decrypt (sk_F, ct):



Keygen(F):

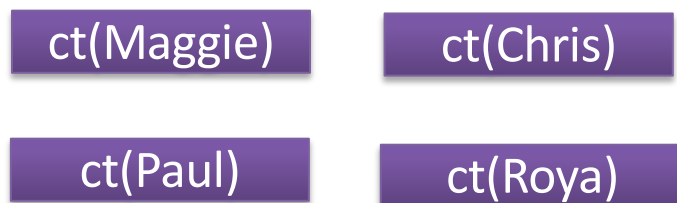


Security:

Adversary possessing keys for multiple circuits F_i cannot distinguish $Enc(x_0)$ from $Enc(x_1)$ unless $F_i(x_0) \neq F_i(x_1)$

Personalized Medicine?

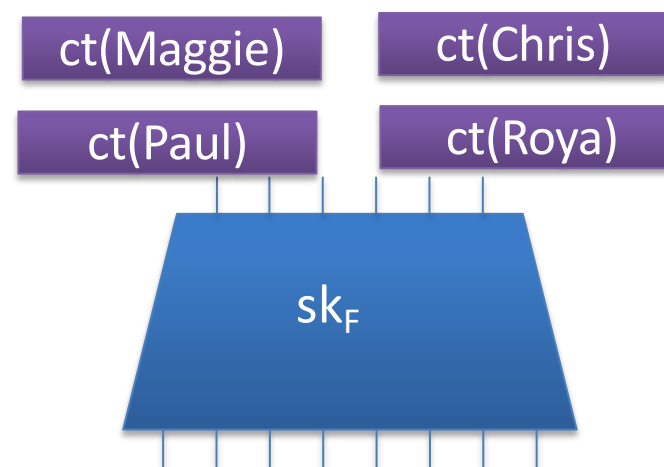
Encrypt(x) x = genomic data of users



Keygen(F) F : some medical research algo



Decrypt (sk_F, ct):

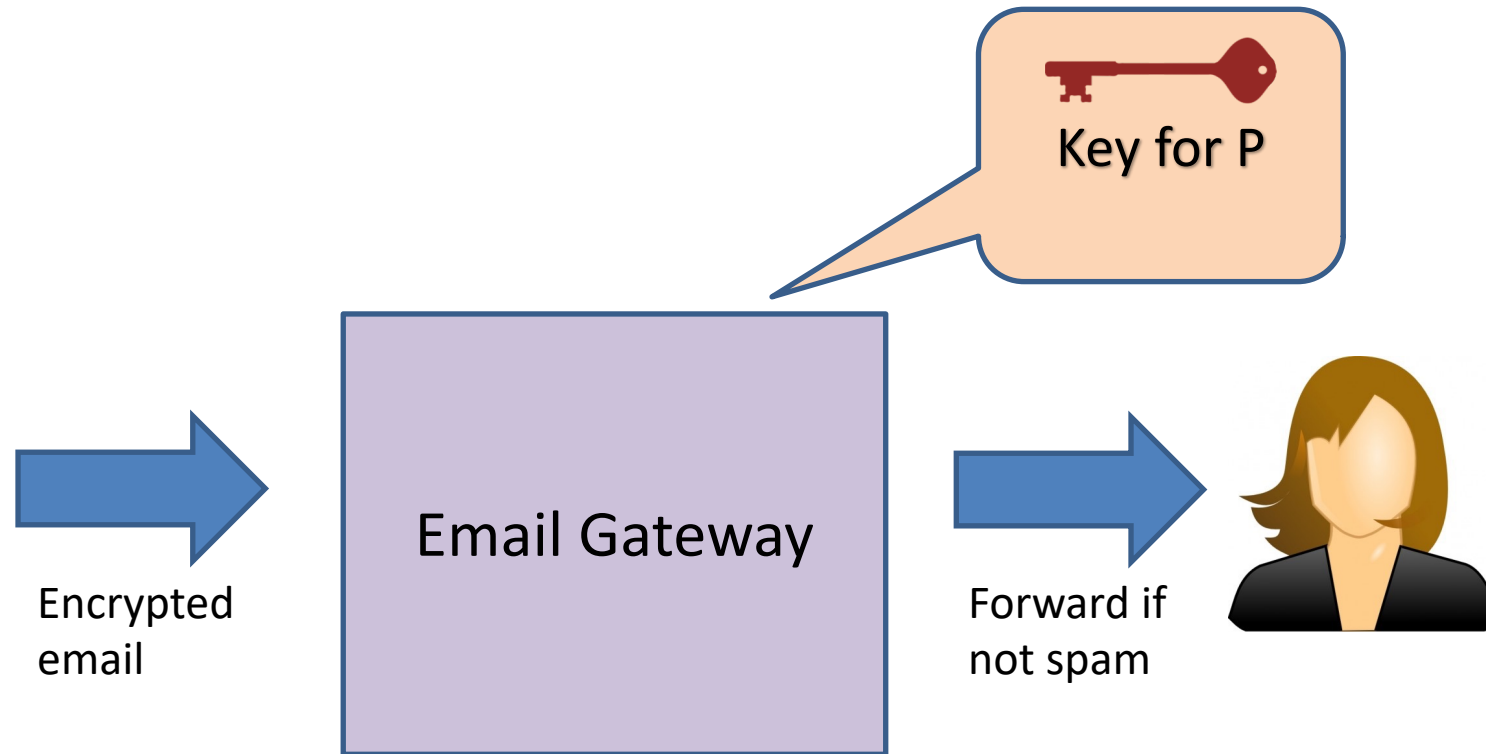


$$y = F(x)$$

Security: No one's personal genomic data is leaked!

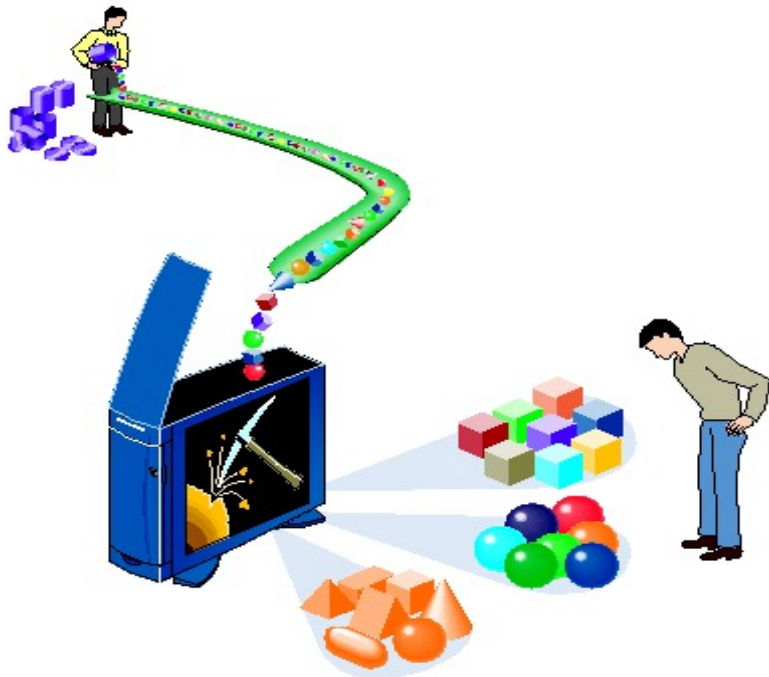
Spam Detection on Encrypted Email

Say we have a program P to detect spam on unencrypted email.

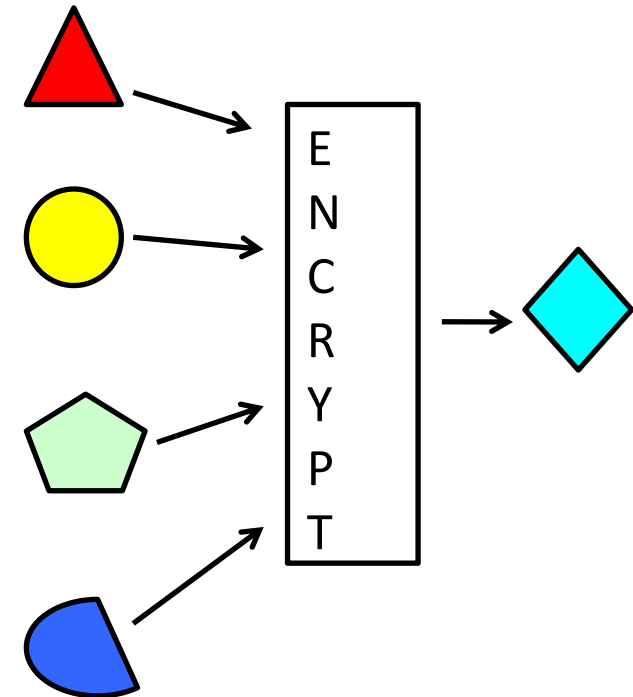


Challenges: Walking the Fine Line

Want to compute on encrypted data so as to be useful, e.g. Data Mining



All encrypted data should look “the same” so as to hide underlying plaintext



The background of the slide is an abstract composition of various colored rectangles and squares. The colors include bright orange, red, blue, green, and yellow. The shapes are arranged in a non-representational, geometric pattern, some overlapping others. The overall effect is vibrant and modern.

Attribute Based Encryption



Prior Work

Key Policy

- **Restricted circuit classes** (point functions, threshold functions, NC_1 circuits...) : [SW05, GPSW06, BW07, KSW08, LOS+10, OT10, OT12, CW14, AFDV11, LW11, LW12, Wat12, Wee14, Att14, GV15, AF18, AMY19a, AMY19b]
- **Polynomial Sized Circuits**: GVW13, BGG+14, GVW15, BV16

Ciphertext Policy

- **Restricted circuit classes** (point functions, threshold functions, NC_1 circuits...): BSW07, Wat11, LOS+10, OT10, LW12, RW13, Att14, Wee14, AHY15, CGW15, AC17, KW19, AMY19b, Tsa19,KNYY20,AY20a]
- **Polynomial Sized Circuits**: ?

Our Results

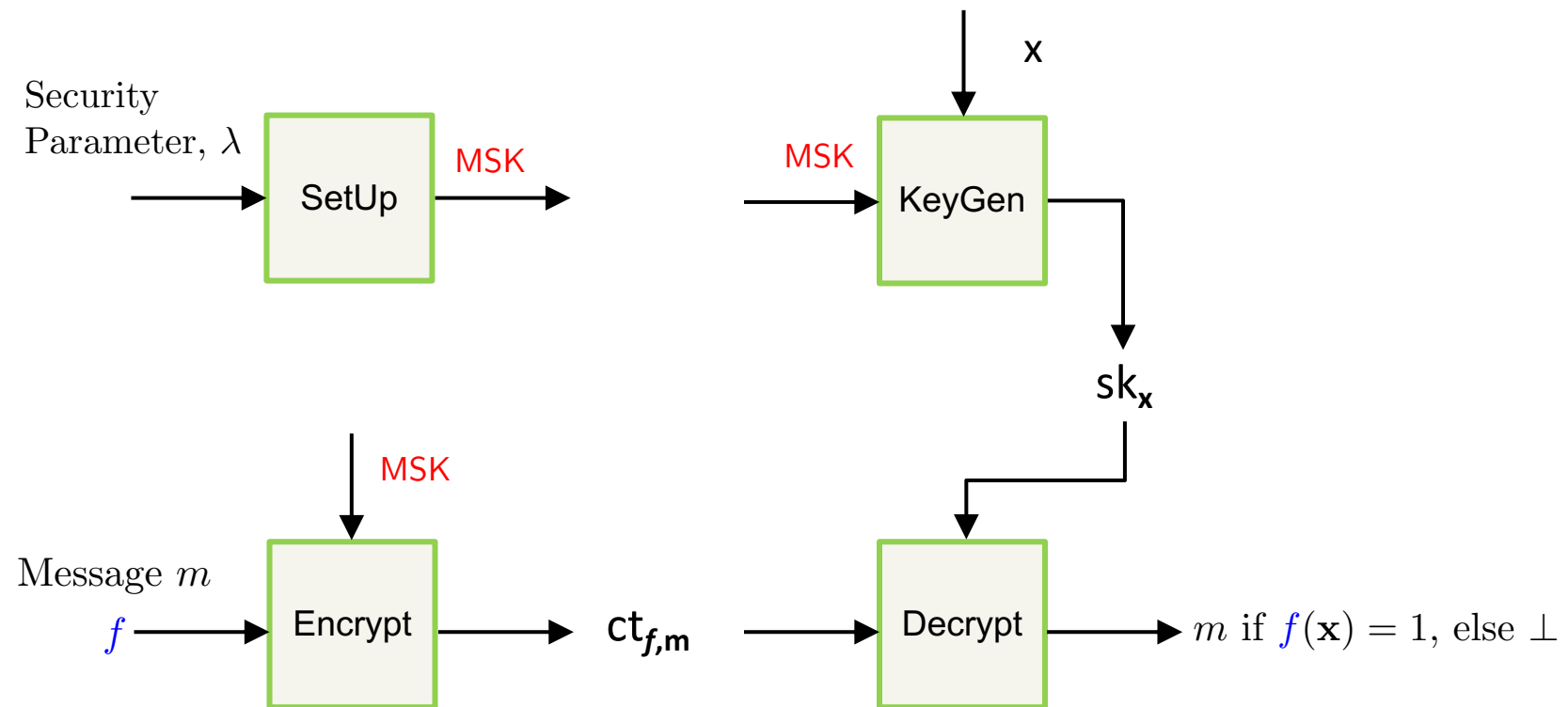
Key Policy

- **Restricted circuit classes** (point functions, threshold functions, NC_1 circuits...) : [SW05, GPSW06, BW07, KSW08, LOS+10, OT10, OT12, CW14, **AFV11**, LW11, LW12, Wat12, Wee14, Att14, GV15, AF18, **AMY19a**, **AMY19b**]
- **Polynomial Sized Circuits**: GVW13, BGG+14, GVW15, BV16

Ciphertext Policy

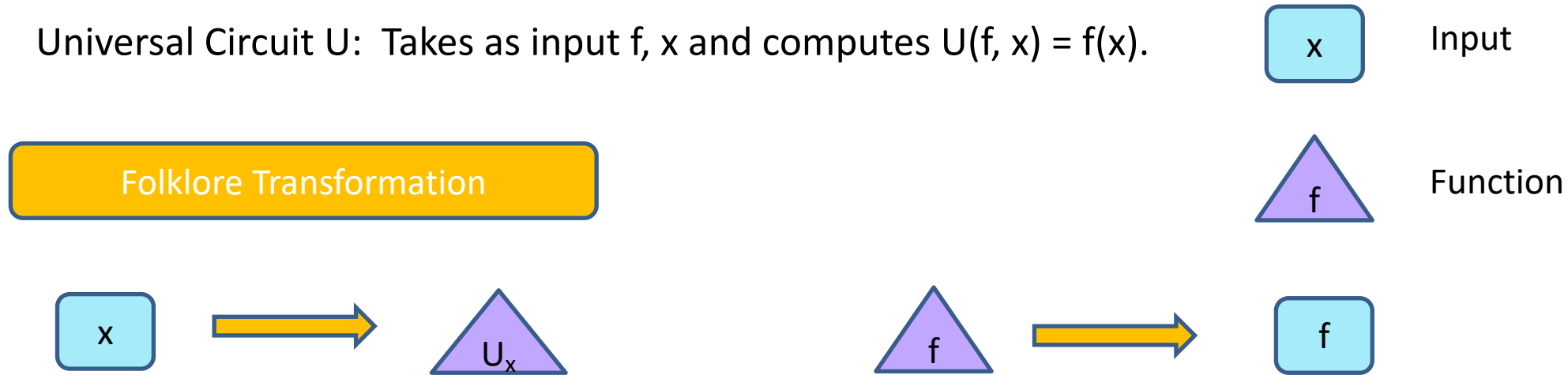
- **Restricted circuit classes** (point functions, threshold functions, NC_1 circuits...): BSW07, Wat11, LOS+10, OT10, LW12, RW13, Att14, Wee14, AHY15, CGW15, AC17, KW19, **AMY19b**, Tsa19,KNYY20,**AY20a**]
- **Polynomial Sized Circuits**: **AY20** (**symmetric key**, from **Learning With Errors**)

SK Ciphertext-Policy ABE [SW05, GPSW06]



Folklore Approach: Via Universal Circuits

Universal Circuit U : Takes as input f, x and computes $U(f, x) = f(x)$.



Use key policy ABE for circuits (GVW13,BGG+14) to build ciphertext policy ABE.

- CP-ABE Encryption creates KP-ABE ciphertext for (f, m)
- CP-ABE KeyGen creates KP-ABE key for function U_x
- CP-ABE Decryption is same as KP-ABE decryption

Drawbacks:

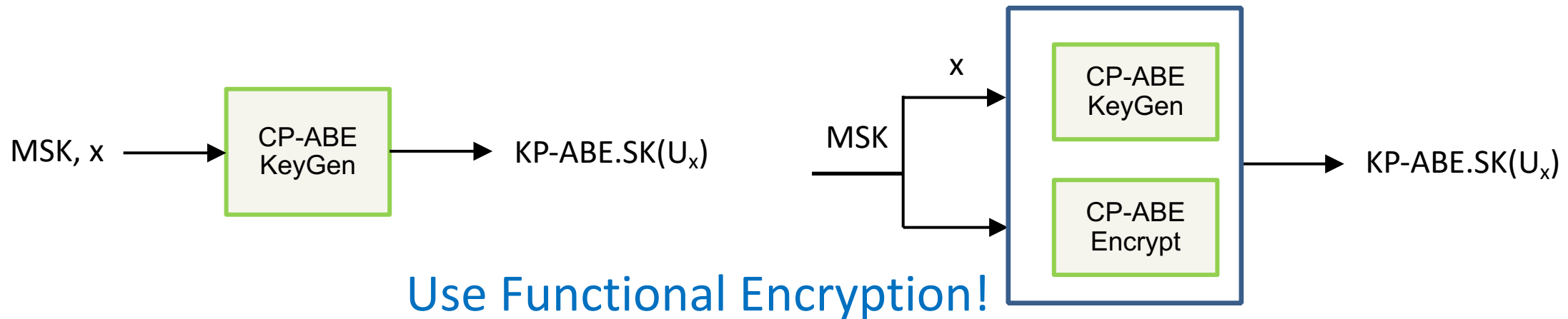
1. Size of PK, CT, runtime of setup, Kgen, Enc, Dec grow with max function size f_{\max}
2. Cannot support unbounded size circuits

Redistributing Computation [AMY19]

To support unbounded circuits: Only encrypt and decrypt should depend on circuit size

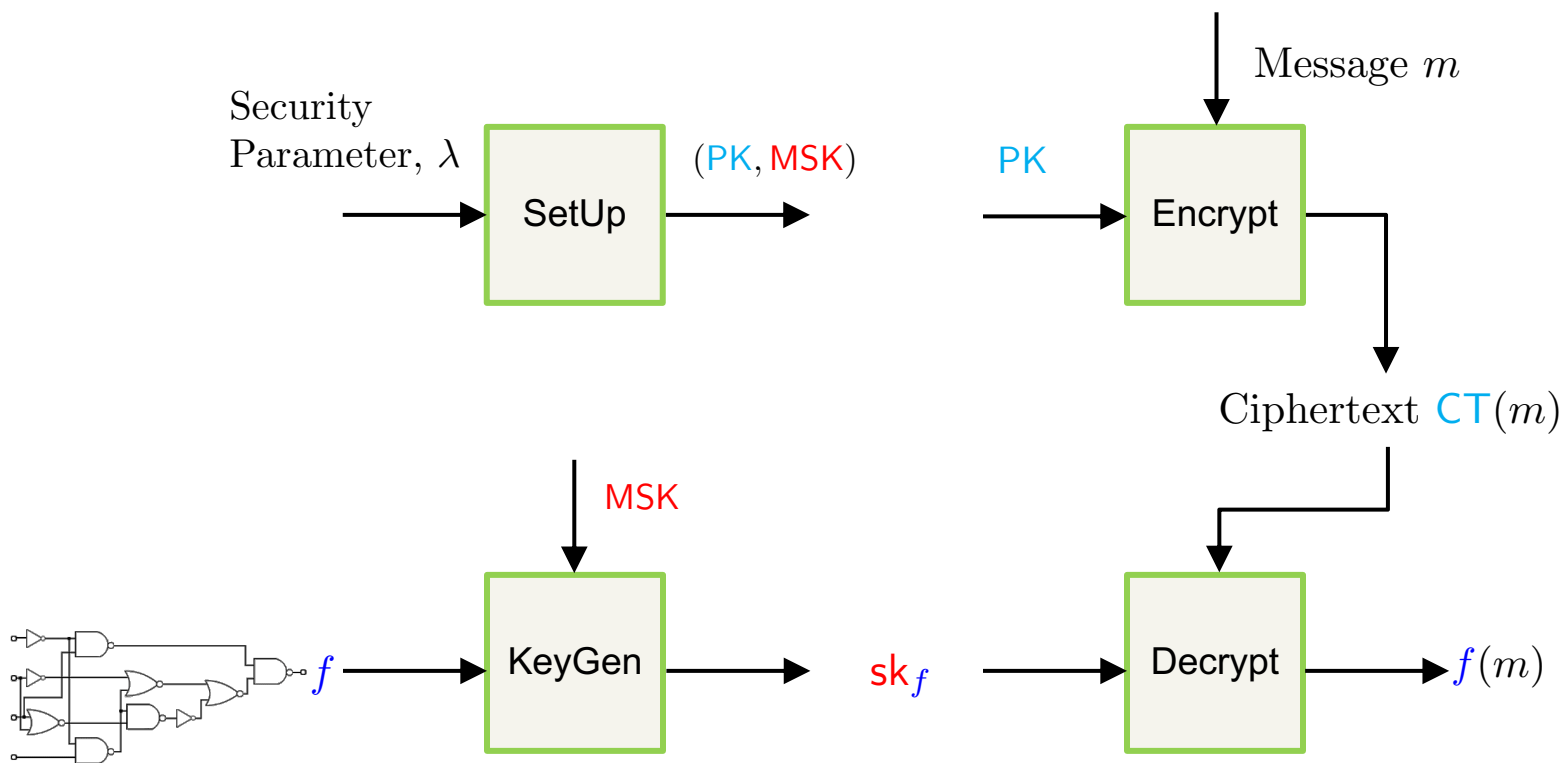
Problem : Computing KP-ABE keygen for function U_x forces CP-ABE keygen to depend on f_{\max} since U_x must support inputs of size f_{\max}

Idea: Distribute computation of KP-ABE keygen for function U_x between CP-ABE encrypt and CP-ABE keygen so that each respects efficiency requirement of CP-ABE



(Key Policy) Functional Encryption (FE)

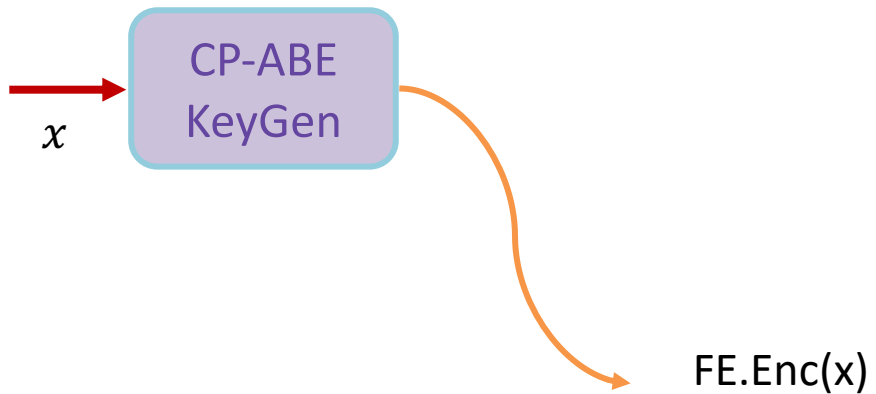
[SW05, BSW11, O'N10]



For **single key** security, can be based on LWE (GKPVZ13, Agr17)

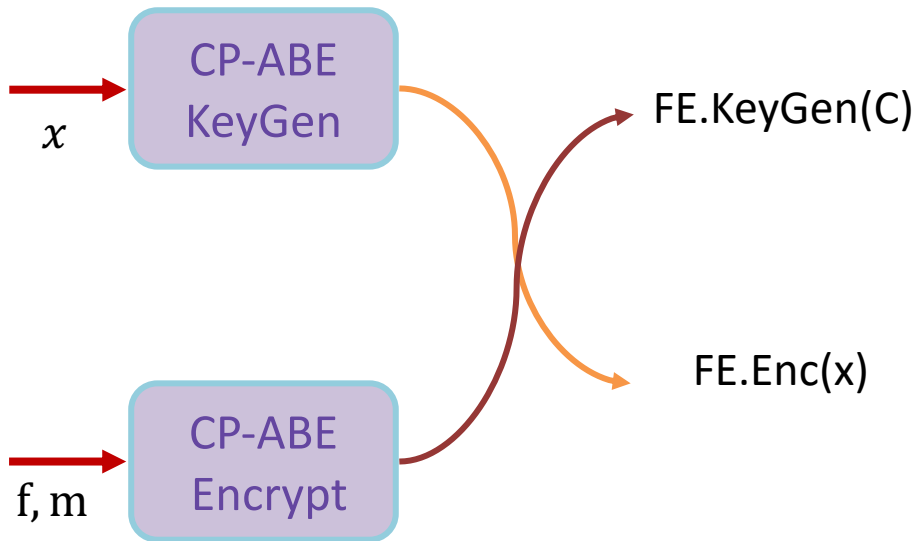
Redistributing Computation

Solution: FE helps to **defer** the computation of KP-ABE KeyGen



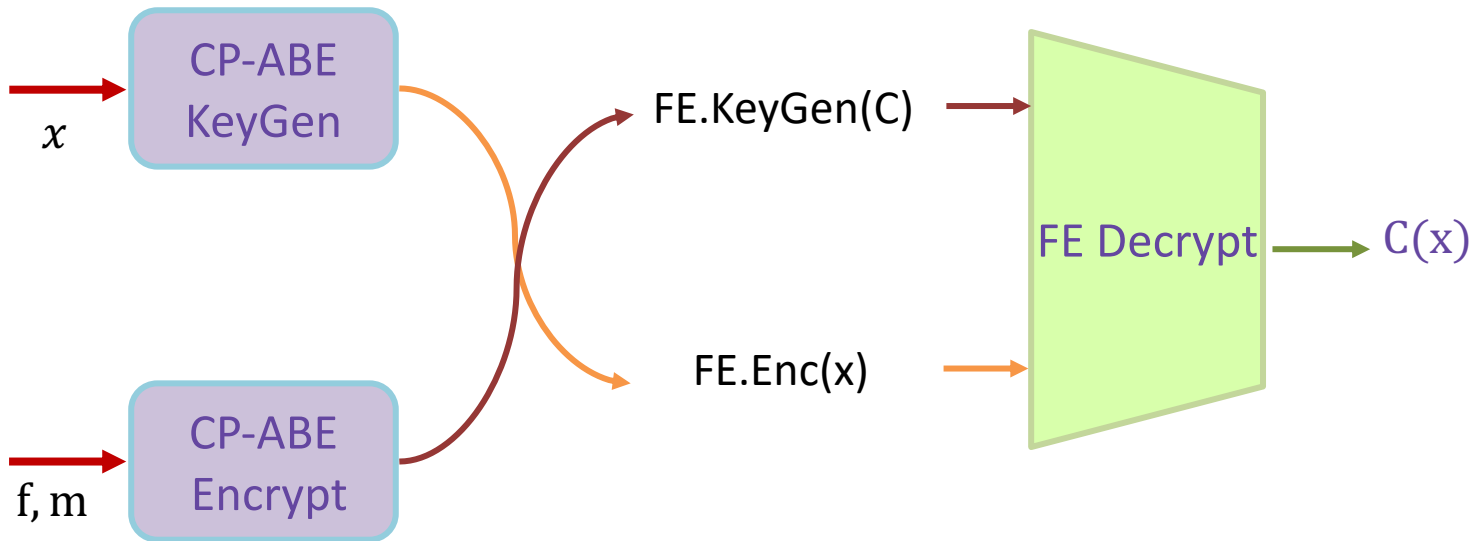
Redistributing Computation

Solution: FE helps to **defer** the computation of KP-ABE KeyGen



Redistributing Computation

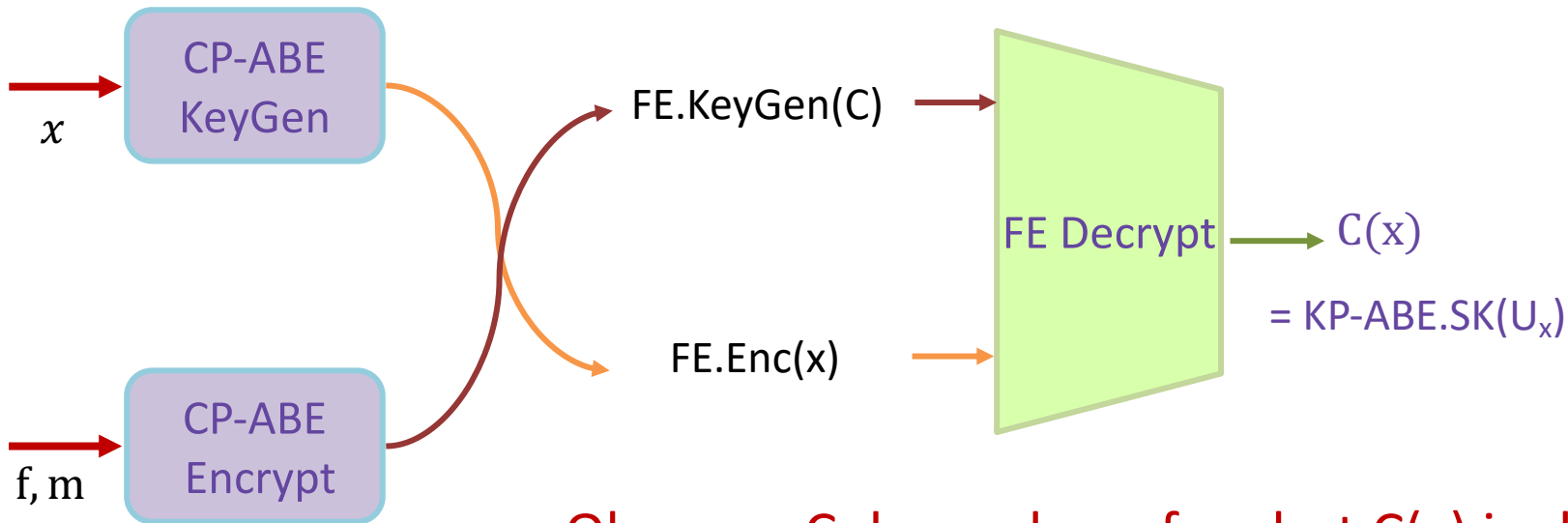
Solution: FE helps to **defer** the computation of KP-ABE KeyGen



Redistributing Computation

Solution: FE helps to **defer** the computation of KP-ABE KeyGen

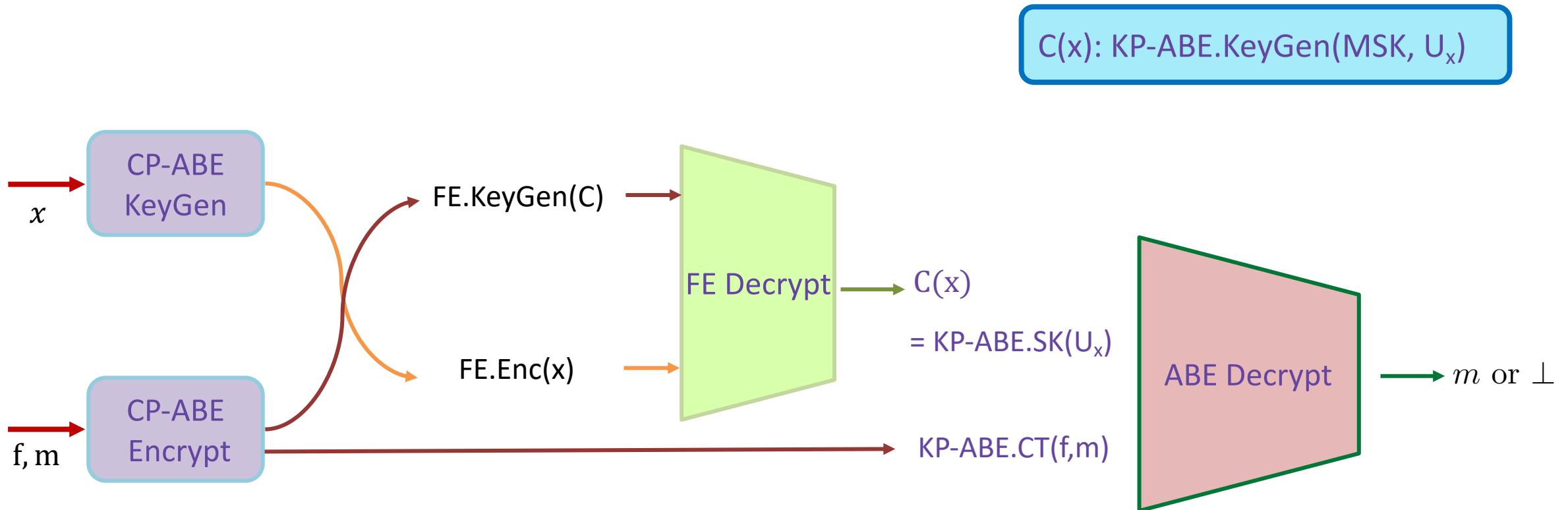
$C(x): \text{KP-ABE.KeyGen}(\text{MSK}, U_x)$



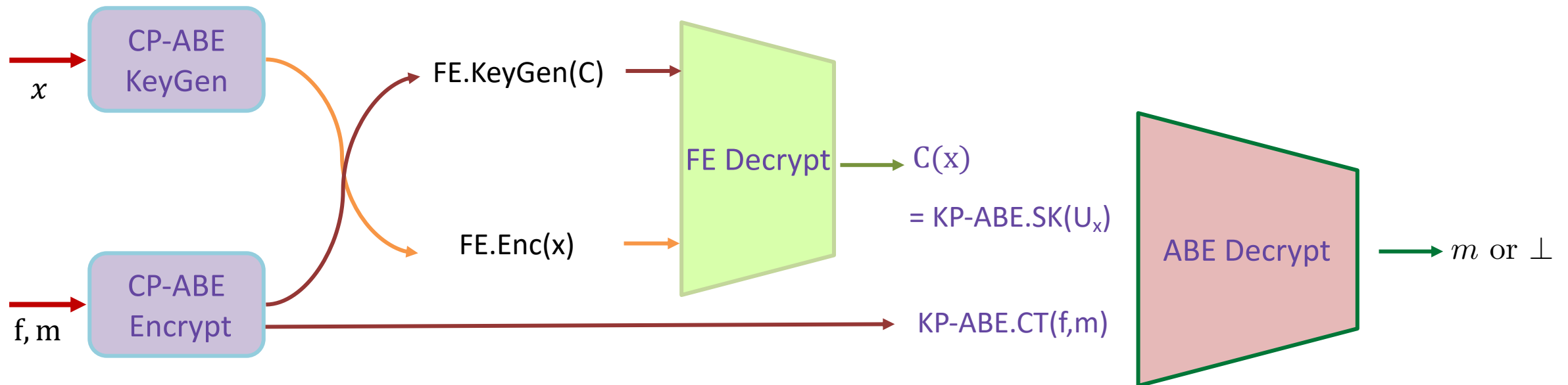
Observe: C depends on f_{\max} but $C(x)$ is short by BGG+14

Redistributing Computation

Solution: FE helps to **defer** the computation of KP-ABE KeyGen

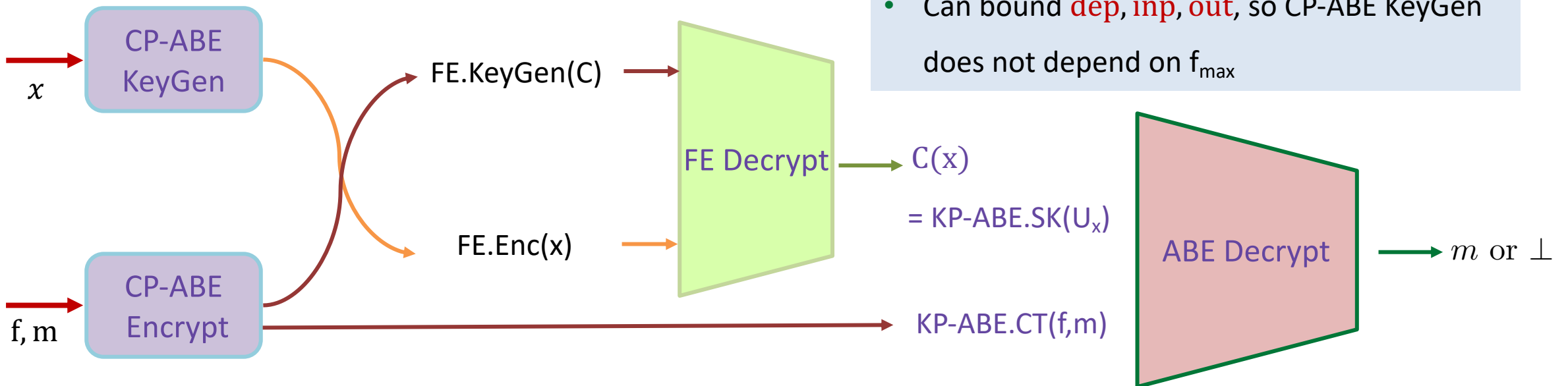


Redistributing Computation

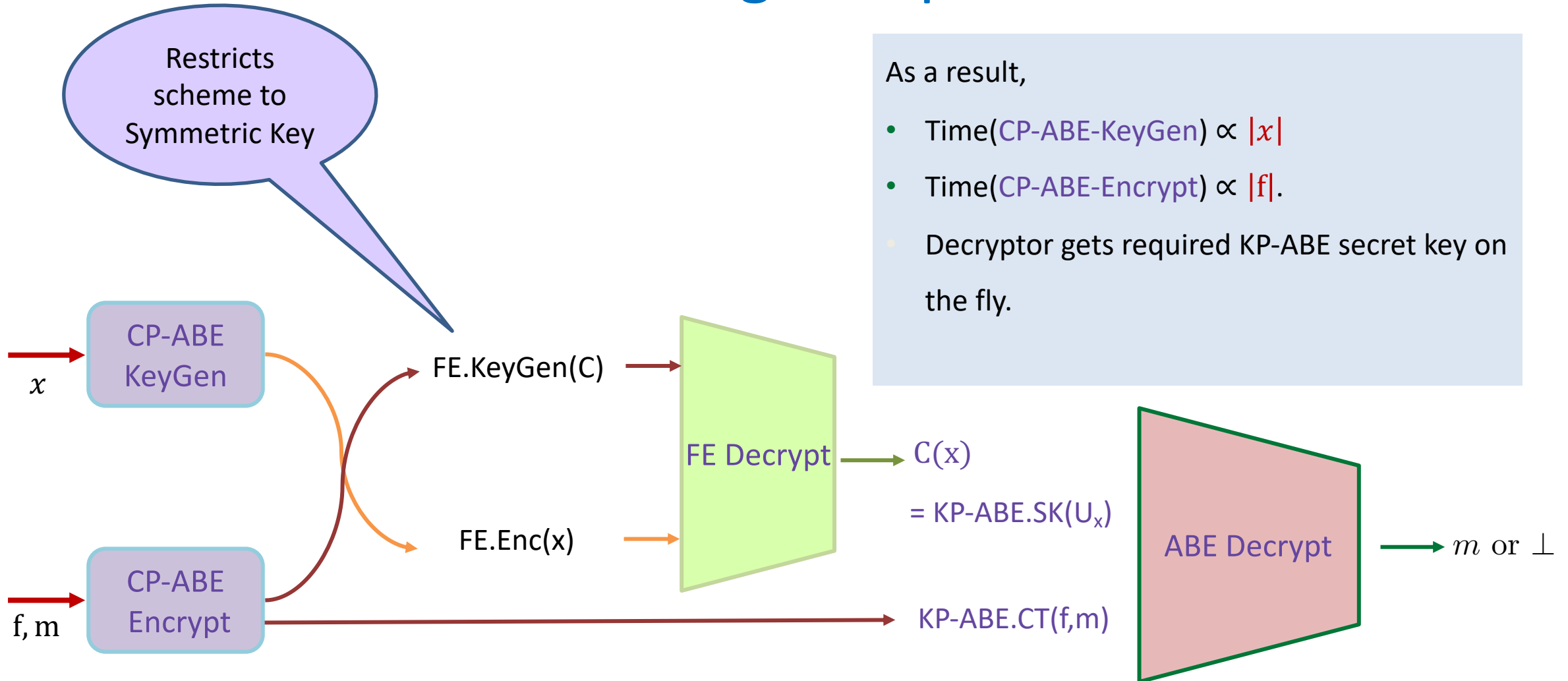


Redistributing Computation

- FE needs a **careful implementation**.
- Need FE.Enc(x) does not grow with $|C|$
- Use **1-key, succinct FE** [GKP⁺13] (from **LWE**).
- Ensures $|FE \text{ ciphertext}| \propto \text{dep, inp, out}$
- Can bound **dep, inp, out**, so CP-ABE KeyGen does not depend on f_{\max}



Redistributing Computation





Supporting Circuits of Unbounded Size

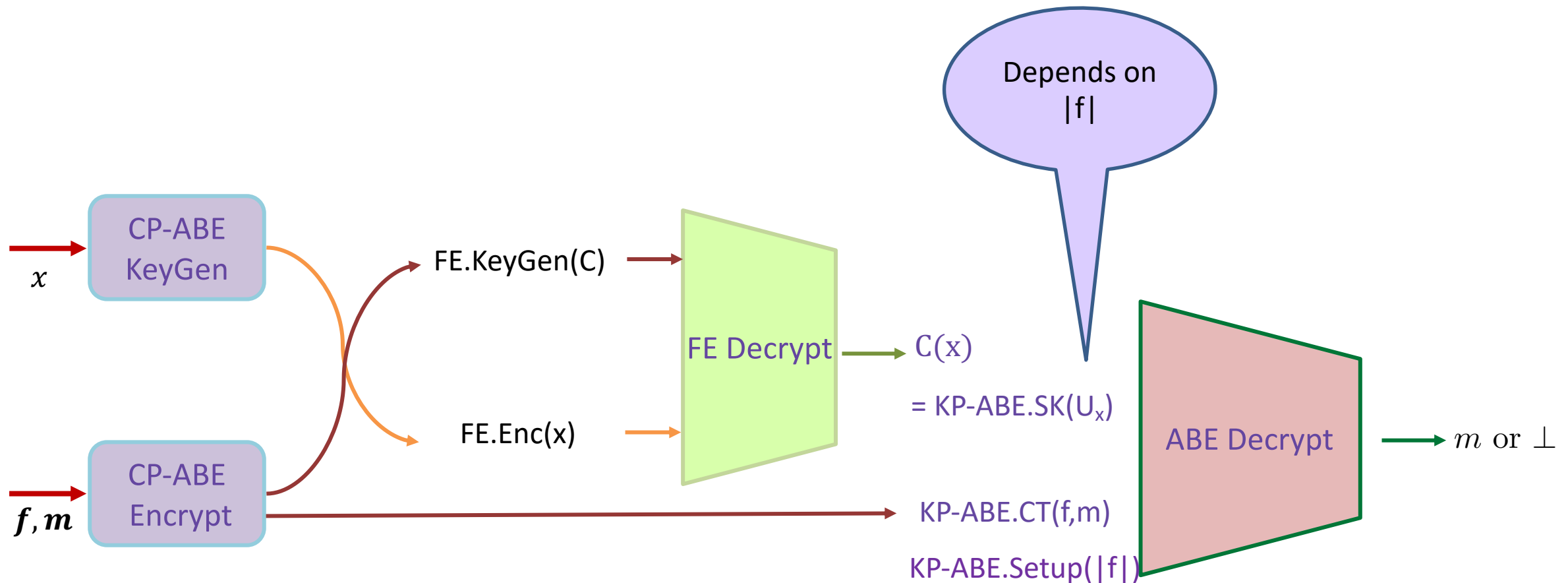
So far, only bounded size circuits....

Problem: If KP-ABE must encrypt f , KP-ABE setup must be initialized with bound f_{\max}
→ only supports bounded circuits.

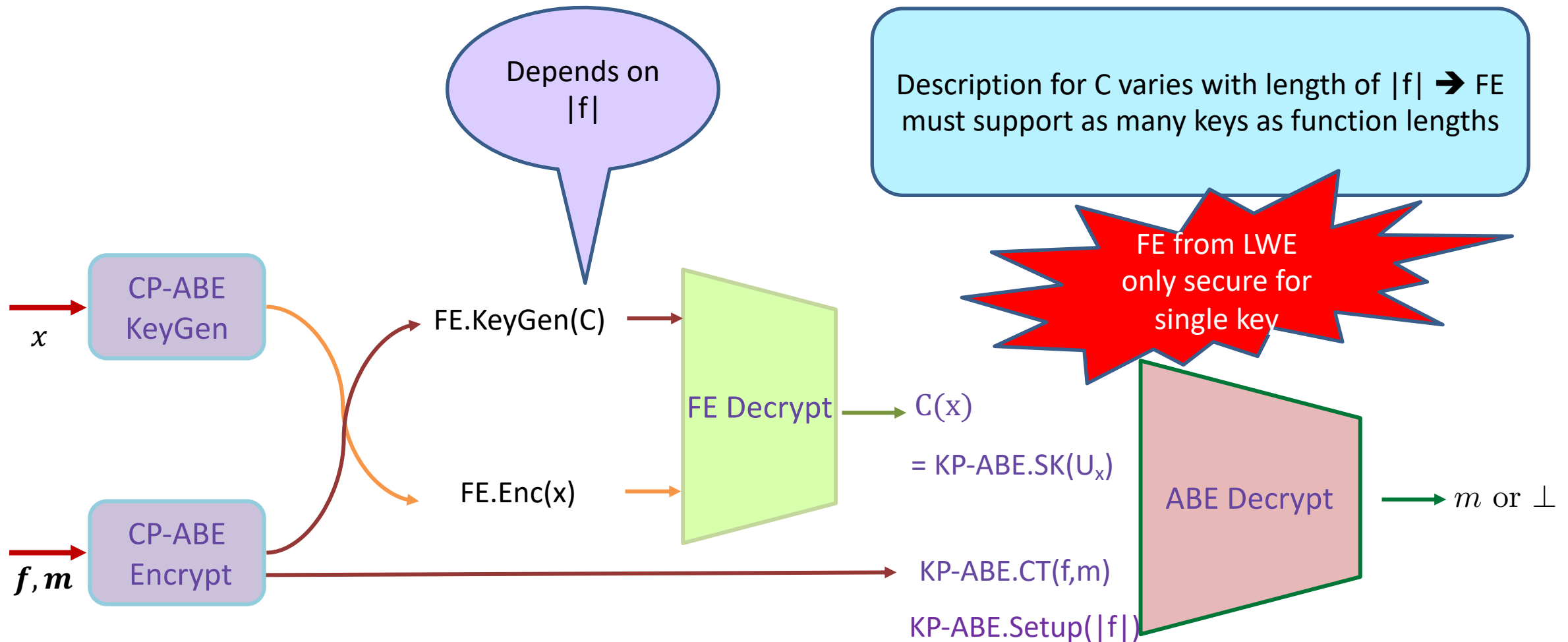
Idea: Let CP-ABE Encrypt, which knows $|f|$, run KP-ABE setup.
Possible since symmetric Key



Supporting Circuits of Unbounded Size



Supporting Circuits of Unbounded Size





Supporting Circuits of Unbounded Size

Solution: Pad circuit size to power of 2, and run λ instances of single key FE

CP-ABE KeyGen does not know $|f|$ so computes Fe.Enc for all λ FEs

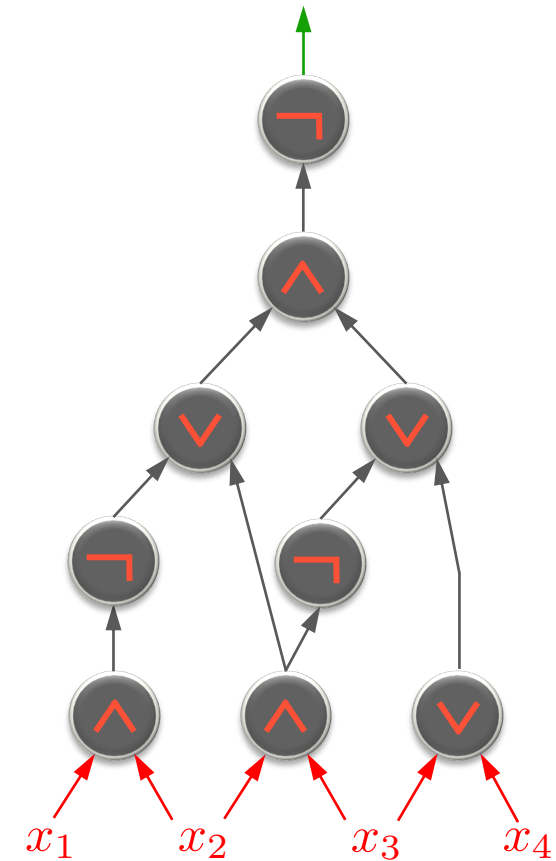


The background is a complex abstract painting. It features a dense arrangement of colors including deep blue, bright yellow, fiery red, and earthy brown. The composition is filled with dynamic, gestural brushstrokes and fine, swirling lines that create a sense of movement and depth. Some areas show more defined shapes, like a red curved form in the lower center and a greyish-yellow shape in the upper right, while others are more chaotic and layered. The overall effect is one of intense energy and visual complexity.

What about supporting inputs of
unbounded lengths?

Circuits are powerful, but...

- Non uniform model of computation
 - Support fixed length inputs
 - Function description changes based on input length
 - Incurs worst-case runtime over all inputs of a certain length



Uniform Models of Computation

Finite automata, Turing Machines, RAM:

- Supports **arbitrary length** inputs
- **Fixed description** for all inputs
- **Input-specific** runtime

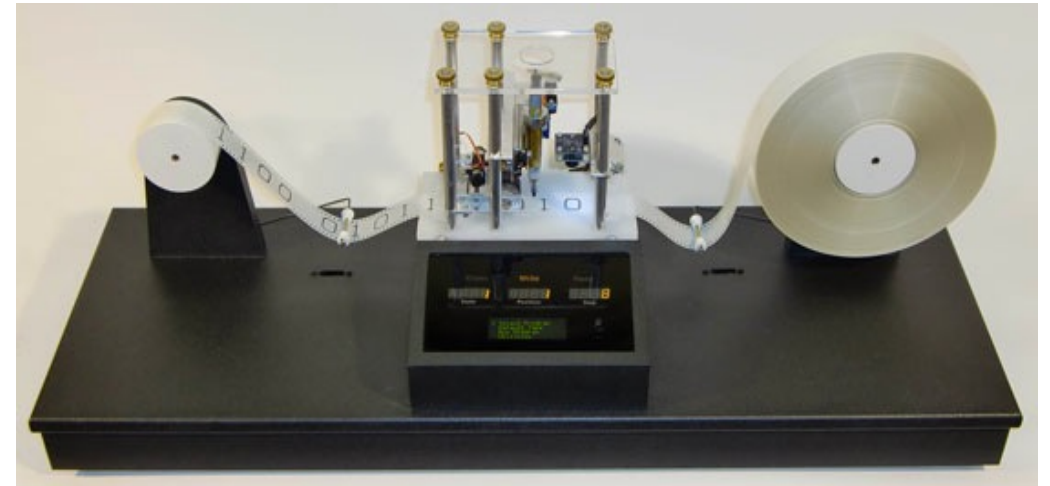


Image Courtesy: <http://aturingmachine.com/>

What is known (unbounded inputs)


Construction	Model	KP / CP	Number of Keys	Assumption
[Wat12]	DFA	KP	Unbounded	q-type assumption on bilinear maps
[Att14]	DFA	KP & CP	Unbounded	q-type assumption on bilinear maps
[AS17]	DFA	KP	Single	LWE
[AMY19a]	NFA	KP	Unbounded	LWE
[AMY19b]	DFA	KP & CP	Unbounded	DLIN
[AMSY21]	TM	KP	Bounded	LWE



Goal: ABE for uniform models of computation

- Encryptor chooses attribute of unbounded (poly) length
- Key corresponds to machine (DFA/NFA/TM/...)
 - Keygen does not know input length.
 - Same key for any input length
- Decryption succeeds iff machine accepts input

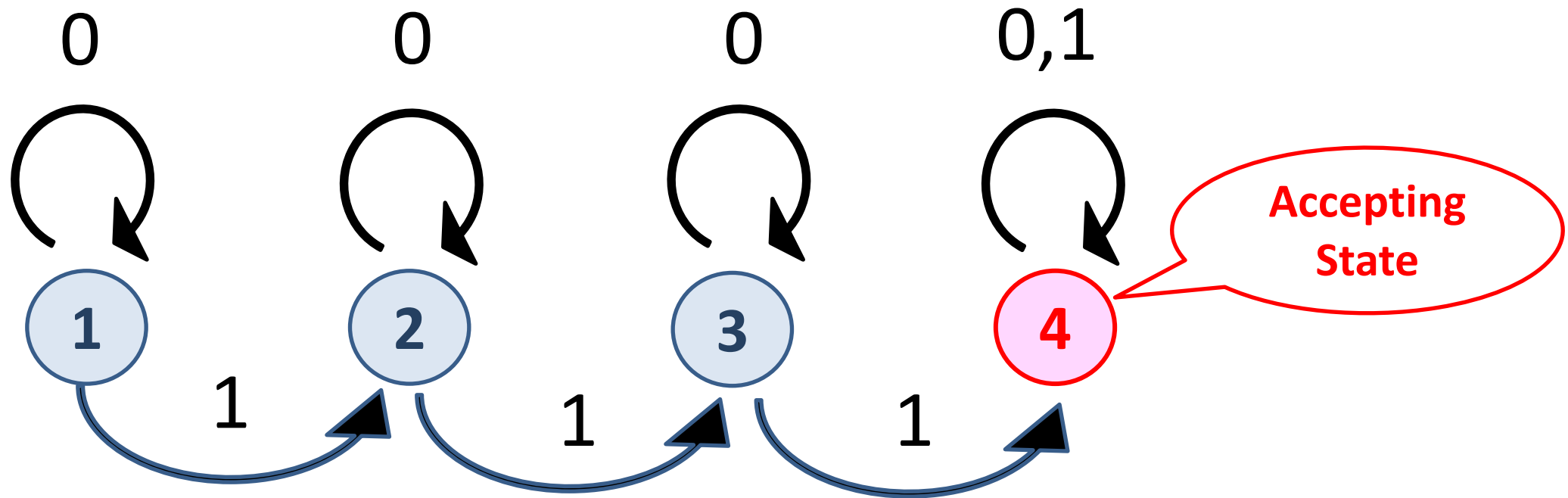
Main challenges?

- Previously, encryptor and key generator could agree on input length n
 - Assign common “PK component” PK_i (matrix or group element) for each index $i \in [n]$, use to compute both CT and SK
- 

Deterministic Finite Automata

Alphabet: $\Sigma = \{0,1\}$,

Set of States = $\{1,2,3,4\}$, Accepting state = $\{4\}$,

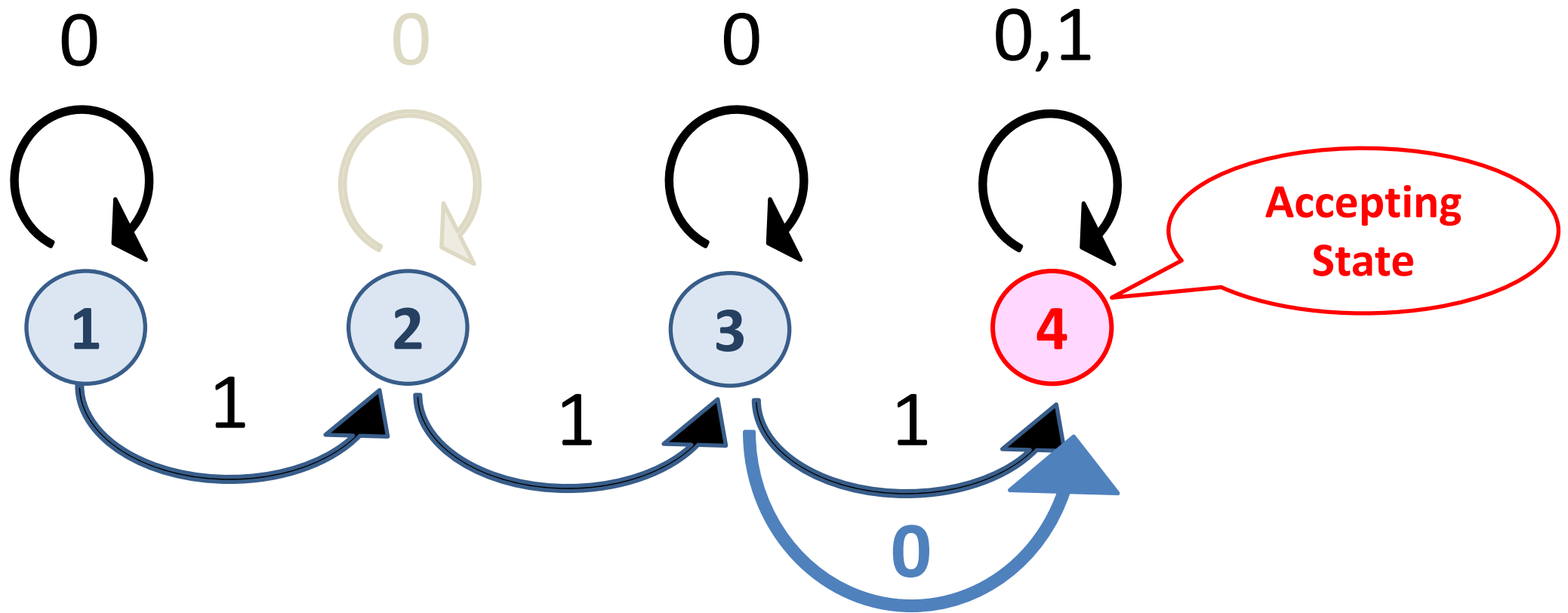


Single outgoing edge from a state w.r.t an alphabet.

111000 \Rightarrow Accept

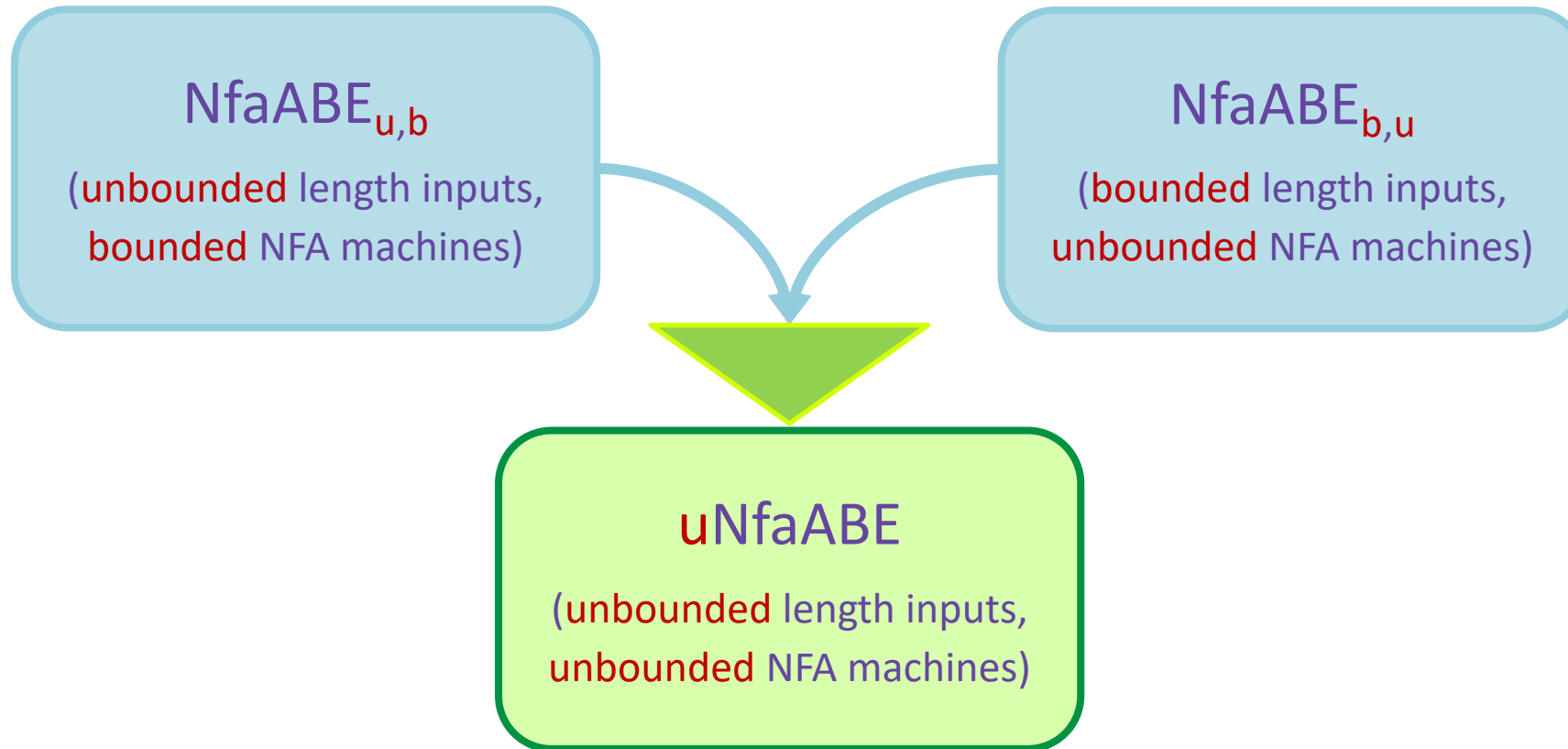
010100 \Rightarrow Reject

Non Deterministic Finite Automata



- Number of outgoing edges from a state w.r.t an alphabet can be arbitrary.
- The input is accepted if there is an accepting path.

ABE for NFA: A Two Step Solution [AMY19a]



Constructing $\text{NfaABE}_{u,b}$

Naive solution:

- For security parameter λ , input (attribute) length $|\mathbf{x}| \leq 2^\lambda$. MSK for $\text{NfaABE}_{u,b}$ is a PRF key K .

Constructing $\text{NfaABE}_{u,b}$

Naive solution:

- For security parameter λ , **input (attribute) length** $|\mathbf{x}| \leq 2^\lambda$. **MSK** for $\text{NfaABE}_{u,b}$ is a **PRF key** K .
- Use an **ABE** scheme for circuits to sample 2^λ key pairs (using K) for **each input length**.

$(\text{ABE.PK}_1, \text{ABE.MSK}_1)$

$(\text{ABE.PK}_2, \text{ABE.MSK}_2)$

\dots

$(\text{ABE.PK}_{2^\lambda}, \text{ABE.MSK}_{2^\lambda})$

Constructing $\text{NfaABE}_{u,b}$

Naive solution:

- For security parameter λ , **input (attribute) length** $|\mathbf{x}| \leq 2^\lambda$. **MSK** for $\text{NfaABE}_{u,b}$ is a **PRF key** K .
- Use an **ABE** scheme for circuits to sample 2^λ key pairs (using K) for **each input length**.

$(\text{ABE.PK}_1, \text{ABE.MSK}_1)$

$(\text{ABE.PK}_2, \text{ABE.MSK}_2)$

\dots

$(\text{ABE.PK}_{2^\lambda}, \text{ABE.MSK}_{2^\lambda})$

- Encrypt message m under attribute \mathbf{x} with $\text{ABE.PK}_{|\mathbf{x}|}$.

Constructing NfaABE_{u,b}

Naive solution:

- For security parameter λ , **input (attribute) length** $|\mathbf{x}| \leq 2^\lambda$. **MSK** for NfaABE_{u,b} is a **PRF key** K .
- Use an **ABE** scheme for circuits to sample 2^λ key pairs (using K) for **each input length**.

(ABE.PK₁, ABE.MSK₁)

(ABE.PK₂, ABE.MSK₂)

...

(ABE.PK_{2^λ}, ABE.MSK_{2^λ})

- Encrypt message m under attribute \mathbf{x} with ABE.PK _{$|\mathbf{x}|$} .
- Convert NFA M to a set of 2^λ circuits

Constructing NfaABE_{u,b}

Naive solution:

- For security parameter λ , **input (attribute) length** $|\mathbf{x}| \leq 2^\lambda$. **MSK** for NfaABE_{u,b} is a **PRF key K**.
- Use an **ABE** scheme for circuits to sample 2^λ key pairs (using **K**) for **each input length**.

(ABE.PK₁, ABE.MSK₁)

(ABE.PK₂, ABE.MSK₂)

...

(ABE.PK_{2^λ}, ABE.MSK_{2^λ})

- Encrypt message m under attribute \mathbf{x} with ABE.PK _{$|\mathbf{x}|$} .
- Convert NFA M to a set of 2^λ circuits, **one for each input length**.

\widehat{M}_1

\widehat{M}_2

...

\widehat{M}_{2^λ}

Constructing $\text{NfaABE}_{u,b}$

Naive solution:

- For security parameter λ , **input (attribute) length** $|\mathbf{x}| \leq 2^\lambda$. **MSK** for $\text{NfaABE}_{u,b}$ is a **PRF key** K .
- Use an **ABE** scheme for circuits to sample 2^λ key pairs (using K) for **each input length**.

$(\text{ABE.PK}_1, \text{ABE.MSK}_1)$

$(\text{ABE.PK}_2, \text{ABE.MSK}_2)$

\dots

$(\text{ABE.PK}_{2^\lambda}, \text{ABE.MSK}_{2^\lambda})$

- Encrypt message m under attribute \mathbf{x} with $\text{ABE.PK}_{|\mathbf{x}|}$.
- Convert NFA M to a set of 2^λ circuits, **one for each input length**. Generate a **secret key for each circuit**.

\widehat{M}_1



$\text{ABE.sk}_{\widehat{M}_1}$

\widehat{M}_2



$\text{ABE.sk}_{\widehat{M}_2}$

\dots

\widehat{M}_{2^λ}



$\text{ABE.sk}_{\widehat{M}_{2^\lambda}}$

Constructing NfaABE_{u,b}

Naive solution:

- Note $|\mathbf{x}| \leq 2^\lambda$. Let MSK: **PRF key K**.
- Use an **ABE** scheme for circuits to sample 2^λ key pairs (using **K**) for **each input length**.

(ABE.PK₁, ABE.MSK₁)

(ABE.PK₂, ABE.MSK₂)

...

(ABE.PK_{2^λ}, ABE.MSK_{2^λ})

- Encrypt message m under attribute \mathbf{x} with ABE.PK _{$|\mathbf{x}|$} .
- Convert NFA M to a set of 2^λ circuits, **one for each input length**. Generate a **secret key for each circuit**.



- Decryptor **knows** $i = |\mathbf{x}|$, chooses $\text{ABE.sk}_{\widehat{M}_i}$ accordingly; decrypts to get m , if M accepts \mathbf{x} .



Constructing NfaABE_{u,b}

Problem #1: Too many keys

- Key size exponential, via 2^λ instances of ABE.





Constructing NfaABE_{u,b}

Problem #1: Too many keys

- Key size exponential, via 2^λ instances of ABE.

Solution: Handle only inputs of length $2^i, \forall i \in [0, \lambda]$.



Constructing NfaABE_{u,b}

Problem #1: Too many keys

- Key size exponential, via 2^λ instances of ABE.

Solution: Handle only inputs of length $2^i, \forall i \in [0, \lambda]$. Generate ABE keys for $\lambda + 1$ instances only.

(ABE.PK_{2⁰}, ABE.MSK_{2⁰})

(ABE.PK_{2¹}, ABE.MSK_{2¹})

...

(ABE.PK_{2 ^{λ}} , ABE.MSK_{2 ^{λ}})

- Pad \mathbf{x} (such that $2^{i-1} < |\mathbf{x}| \leq 2^i$) with \perp to make $\mathbf{x}' = (\mathbf{x}, \perp, \dots, \perp)$ of length 2^i .

Constructing NfaABE_{u,b}

Problem #1: Too many keys

- Key size exponential, via 2^λ instances of ABE.

Solution: Handle only inputs of length $2^i, \forall i \in [0, \lambda]$. Generate ABE keys for $\lambda + 1$ instances only.

(ABE.PK_{2⁰}, ABE.MSK_{2⁰})

(ABE.PK_{2¹}, ABE.MSK_{2¹})

...

(ABE.PK_{2 ^{λ}} , ABE.MSK_{2 ^{λ}})

- Pad \mathbf{x} (such that $2^{i-1} < |\mathbf{x}| \leq 2^i$) with \perp to make $\mathbf{x}' = (\mathbf{x}, \perp, \dots, \perp)$ of length 2^i .
- Encrypt message m under attribute \mathbf{x}' with ABE.PK _{$|\mathbf{x}'|$}

Constructing NfaABE_{u,b}

Problem #1: Too many keys

- Key size exponential, via 2^λ instances of ABE.

Solution: Handle only inputs of length $2^i, \forall i \in [0, \lambda]$. Generate ABE keys for $\lambda + 1$ instances only.

(ABE.PK_{2⁰}, ABE.MSK_{2⁰})

(ABE.PK_{2¹}, ABE.MSK_{2¹})

...

(ABE.PK_{2^λ}, ABE.MSK_{2^λ})

- Pad \mathbf{x} (such that $2^{i-1} < |\mathbf{x}| \leq 2^i$) with \perp to make $\mathbf{x}' = (\mathbf{x}, \perp, \dots, \perp)$ of length 2^i .
- Encrypt message m under attribute \mathbf{x}' with ABE.PK _{$|\mathbf{x}'|$}
- Convert NFA M to a set of $\lambda + 1$ circuits.

\widehat{M}_{2^0}

\widehat{M}_{2^1}

...

\widehat{M}_{2^λ}

Constructing NfaABE_{u,b}

Problem #1: Too many keys

- Key size exponential, via 2^λ instances of ABE.

Solution: Handle only inputs of length $2^i, \forall i \in [0, \lambda]$. Generate ABE keys for $\lambda + 1$ instances only.

(ABE.PK_{2⁰}, ABE.MSK_{2⁰})

(ABE.PK_{2¹}, ABE.MSK_{2¹})

...

(ABE.PK_{2^λ}, ABE.MSK_{2^λ})

- Pad \mathbf{x} (such that $2^{i-1} < |\mathbf{x}| \leq 2^i$) with \perp to make $\mathbf{x}' = (\mathbf{x}, \perp, \dots, \perp)$ of length 2^i .
- Encrypt message m under attribute \mathbf{x}' with ABE.PK _{$|\mathbf{x}'|$}
- Convert NFA M to a set of $\lambda + 1$ circuits. Generate $\lambda + 1$ ABE secret keys.



Constructing NfaABE_{u,b}

Problem #2: Too large keys

- Secret key size $|\text{ABE.sk}_{\widehat{M}_{2^i}}|$ may be exponential

Possible way out:

- Use suitable ABE [BGG⁺14]. SK sizes short : $\text{poly}(\lambda, d)$ for depth d circuits

How to bound circuit depth?

- Naïve conversion of M to circuit results in circuits of depth 2^i
- Use **divide-and-conquer** technique to evaluate M .
- Ensures **circuit depth = $\text{polylog}(|\mathbf{x}|)$** $\Rightarrow |\text{ABE.sk}_{\widehat{M}_{2^i}}|$ is **$\text{poly}(\lambda)$** .

Constructing $\text{NfaABE}_{u,b}$

Problem #3: Inefficient keygen

- $|\widehat{M}_{2i}|$ too large to even be read
- Keygen cannot know input length
- Even if it did, runtime must be independent of this

Solution: Redistribute computation

- Encryptor and decryptor know input length, and can run in time $O(|x|)$
- Delegate inefficient part of keygen to enc and dec!
- Key Tool: Functional Encryption



Women in Science

Is Science Objective?

“Whenever the subject of women in science comes up, there are people fiercely committed to the idea that sexism does not exist. They will point to everything and anything else to explain differences while becoming angry and condescending if you even suggest that discrimination could be a factor. But these people are wrong. This data shows they are wrong.”

[Ilana Yurkiewicz, Scientific American 2012]

Can we be open to this idea?

Society has biases!

A girl receives literally **thousands of suggestions over time** that tell her what her place/role is...

- My earliest memory: Blessings received when touching feet of elders
- Today's experience: Society accepts women who need, not women who lead
- Enormous pressure felt by (esp.) MS/PhD students about "own desires" versus family/expectations. Seen many bright young girls giving up or compromising heavily on career

Sometimes, discards/rebels.
Often internalizes/compromises.

Bank of India

Relationship beyond banking

Shopping is good.
Getting rewarded for it
is even better.

Earn more reward points on using your

BOI ★ **Debit Card**



This festive season is even more exciting... and rewarding too. Use your Debit Card for shopping and get more reward points. You will get 1 to 2 reward points depending upon the amount of spending over ₹ 100. So make the most of this



Let's talk
marriage.
Let's talk
certainties.



Insurance plans for the certainties of life.

Life isn't full of accidents waiting to happen.
In fact, it's full of certainties like getting married,



Gender Biased Forms

Faculty daughter or wife?

Students referred as "boys"

Prof. X and Shweta, Dr. Uday and wife

Future of country depends on "these guys"

"A parent had shared a snapshot of her six-year-old pupils to research a scientist or inventor. So far, so normal. But the question, in jaunty Comic Sans, read: "Who was he? How old were they when they began inventing?"

-- Laura Bates, The Guardian

Hubby is coming back...
I must look fit and pretty

THIS VALENTINE'S DAY

A MAID

with abdominal tyres killing my body shape. I was literally shocked when I know that he is coming for a short vacation and started dieting and vigorous work out for one week which made me weak and unhealthy but couldn't reduce more than 1.5 Kg. It was Dr. Honey Saji (B.A.M.S) of SBM Ayurveda Tablet for my weight issues. I was very suspicious because many of my friends were

I am no longer worried about my body and beauty. I completely

Careta

Society has biases! And Science?

Scientists are supposed to be objective, able to evaluate data and results without being swayed by emotions or biases. This is a fundamental tenet of science. What this extensive literature shows is, in fact, scientists are people, subject to the same cultural norms and beliefs as the rest of society.

[Prof. Alison Coil, UCSD]

Things I've heard



times

- Women can't do math
- Women are good at rote learning not reasoning
- It is not feminine to argue
- Why would Google pay so much to hire a woman whose just going to go on maternity leave
- I saw a very beautiful woman on our floor today and I wondered, what she is doing on the science floor?
- Your paper has better chances since it will get sympathy, being an all woman paper
- You left your parents to follow your desires? Our daughters would never do that
- If you study so much, who will marry you?
- Women need to put family first

So... what next?

- Is this daunting/depressing? Seeing it is overcoming it!

It only matters if you let it!

- Reject these suggestions and they cannot touch you.
- Calling it out? Take a call.
- Preserve creative energy: results talk loudest!
- Cultivate support system
- Personally: Follow(ed) gut even when no support. Willing to accept consequences.

No Looking Back!

Life is not easy for any of us. But what of that? We must have perseverance and above all confidence in ourselves. We must believe that we are gifted for something and that this thing must be attained.

--- Marie Curie

(first scientist to be awarded a Nobel Prize in two different categories)



Thank You

Images Credit: MF Hussain, Hans Hoffman