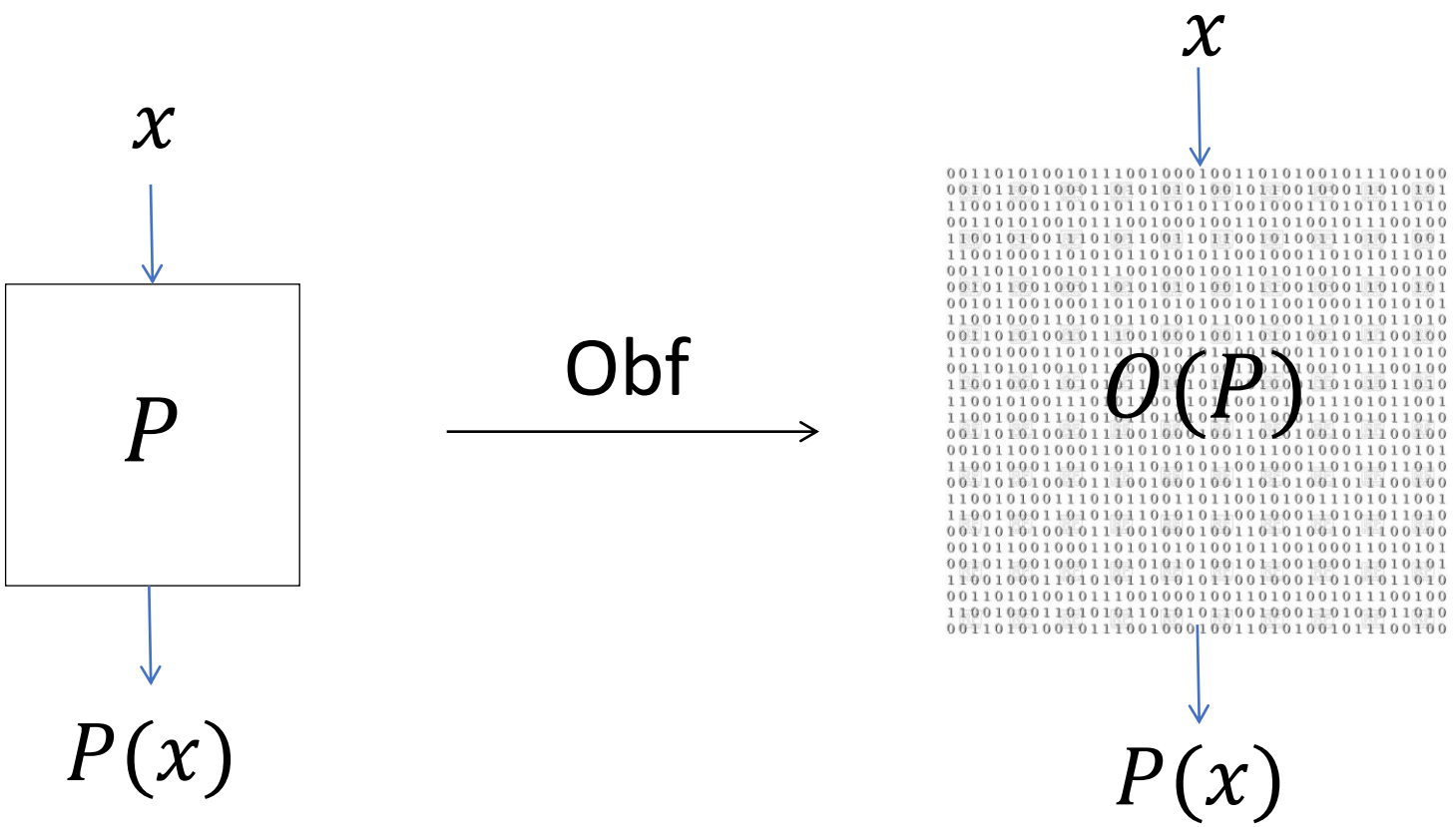
Breaking the Sub-Exponential Barrier in Obfustopia

Sanjam Garg, University of California, Berkeley
Omkant Pandey, Stony Brook University
Akshayaram Srinivasan, University of California, Berkeley
Mark Zhandry, Princeton University

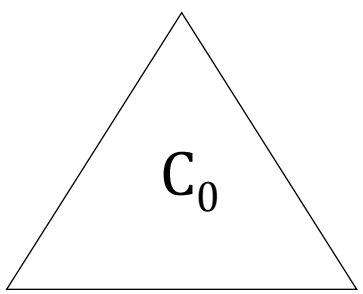
Program Obfuscation

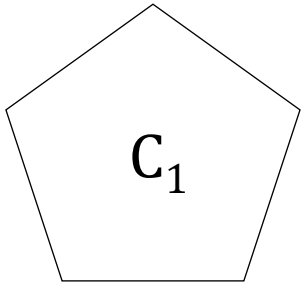
[Barak-Goldreich-Impagliazzao-Rudich-Sahai-Vadhan-Yang 01]



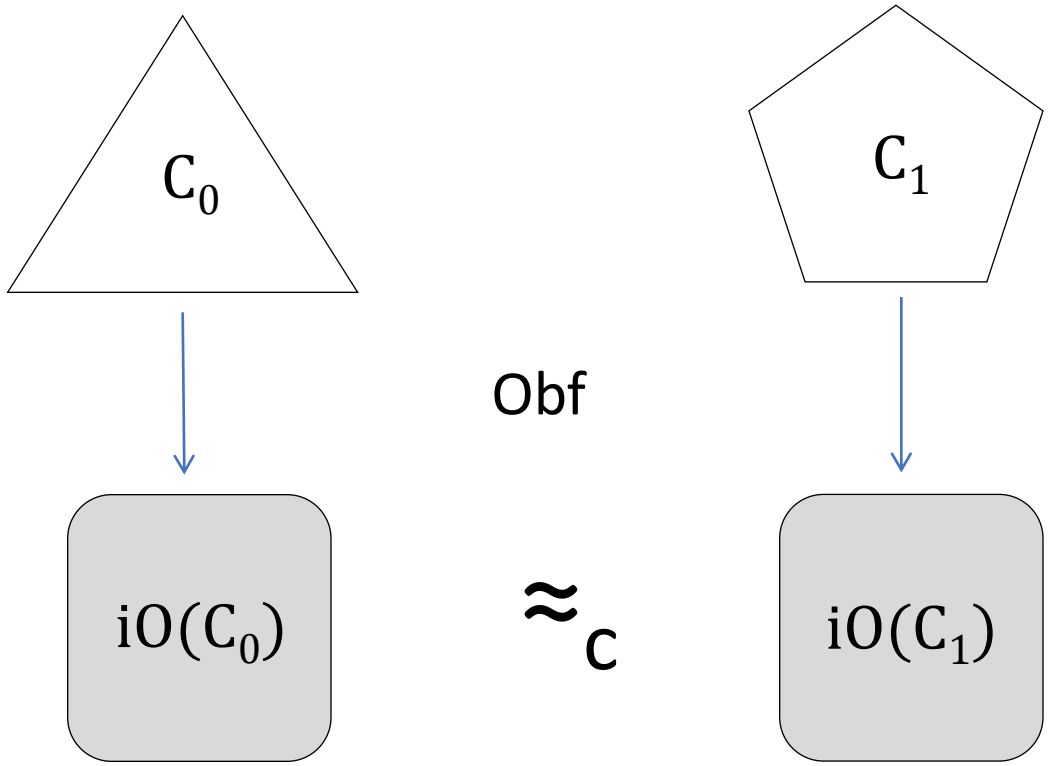
Indistinguishability Obfuscation

Indistinguishability Obfuscation

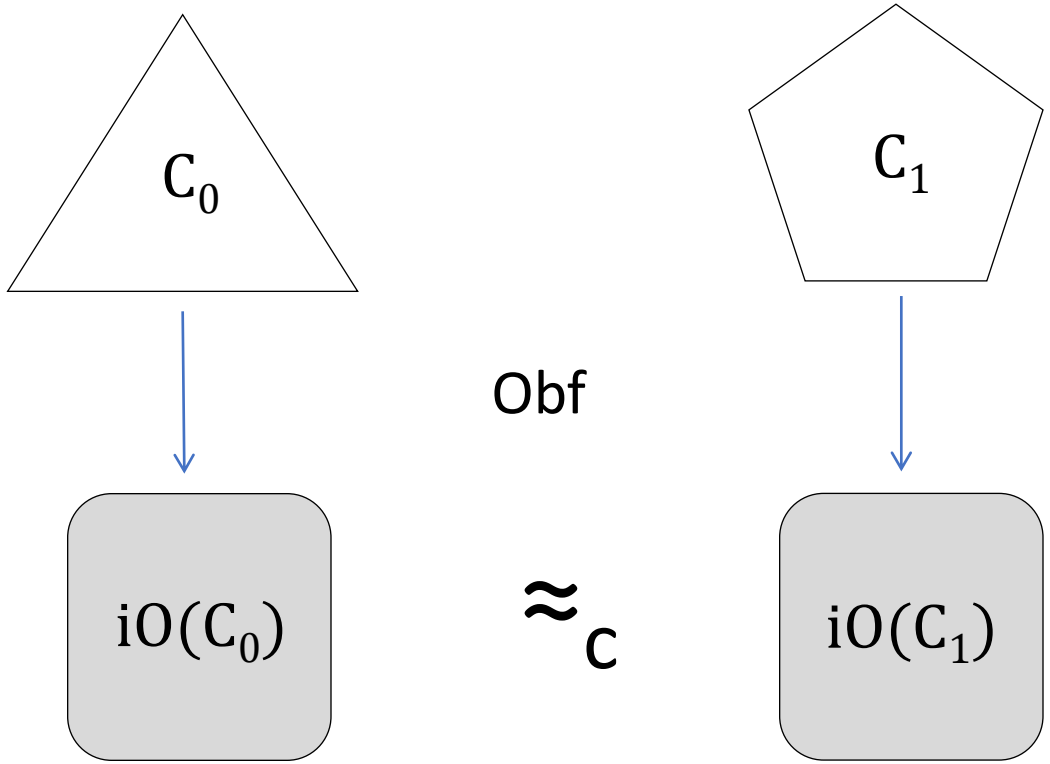




Indistinguishability Obfuscation

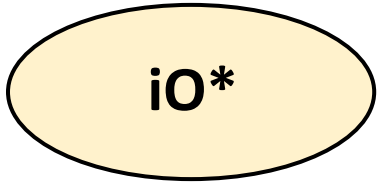


Indistinguishability Obfuscation



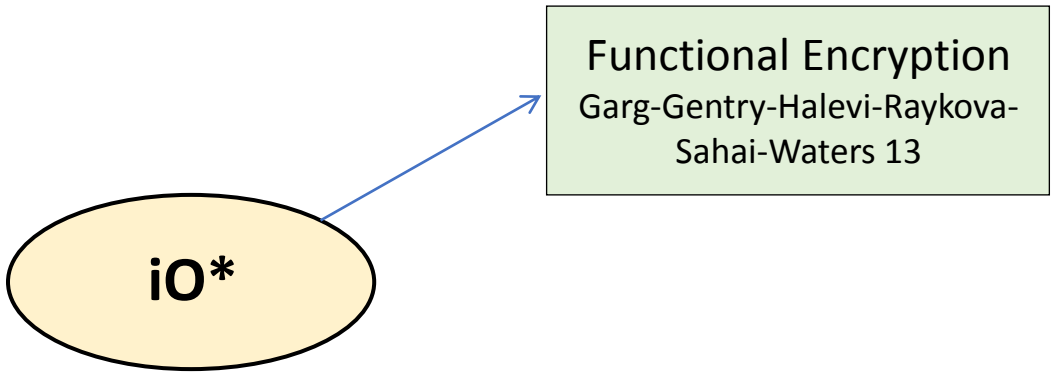
Several constructions of iO: [GGHRSW13], [BGKPS14], [AGIS14], [BR14],[GLSW15], [AJ15], [BV15], [AJS15], [BMSZ16], [L16], [LV16], [GMMS**S**Z16], [L17], [LT17] …

Applications of iO



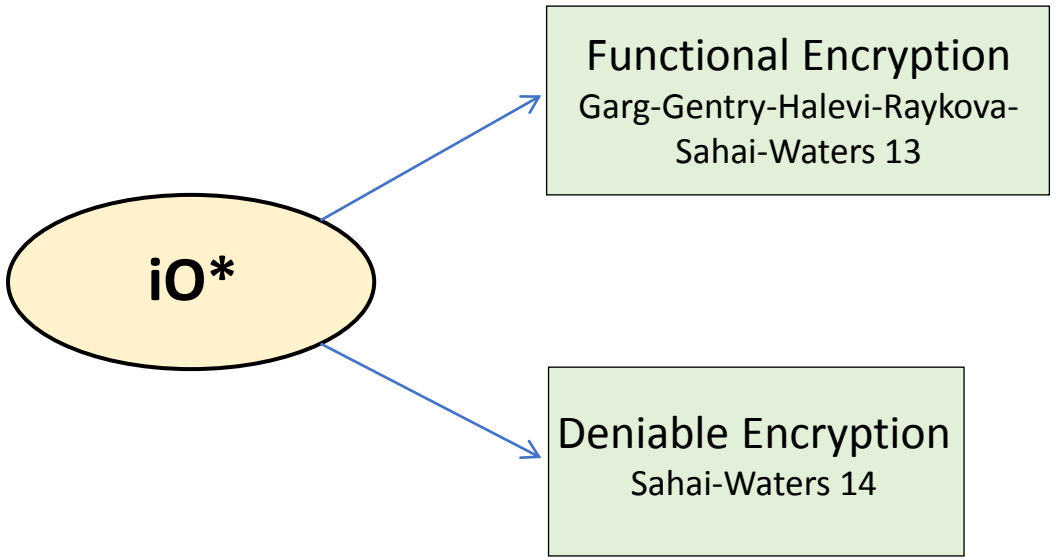
* + other assumptions

Applications of iO



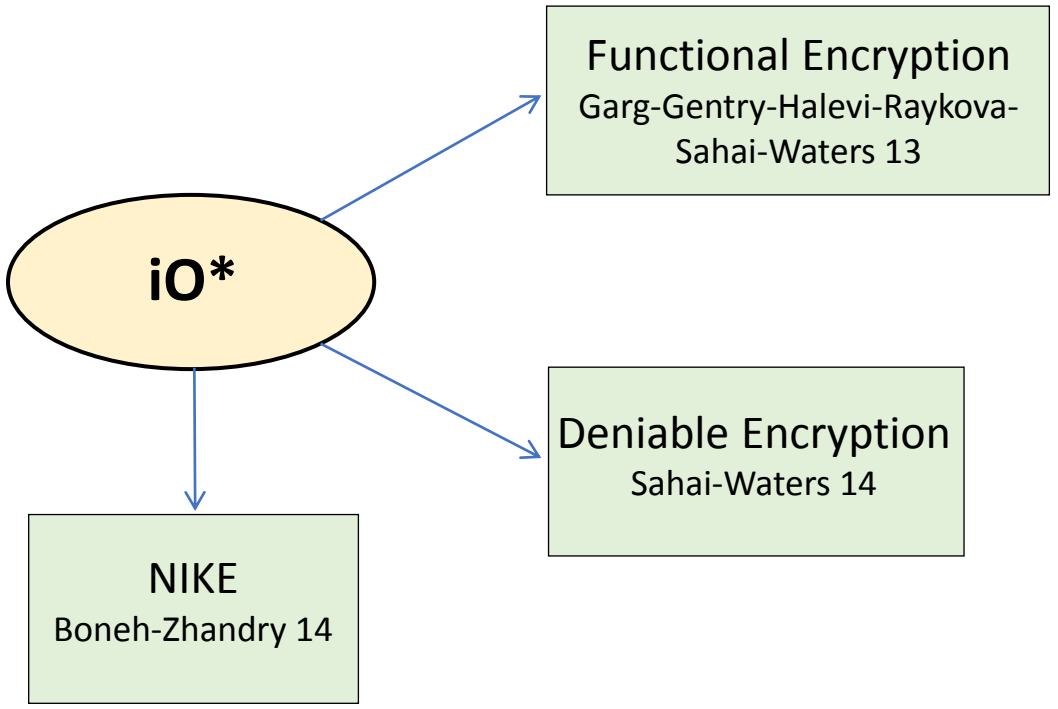
* + other assumptions

Applications of iO



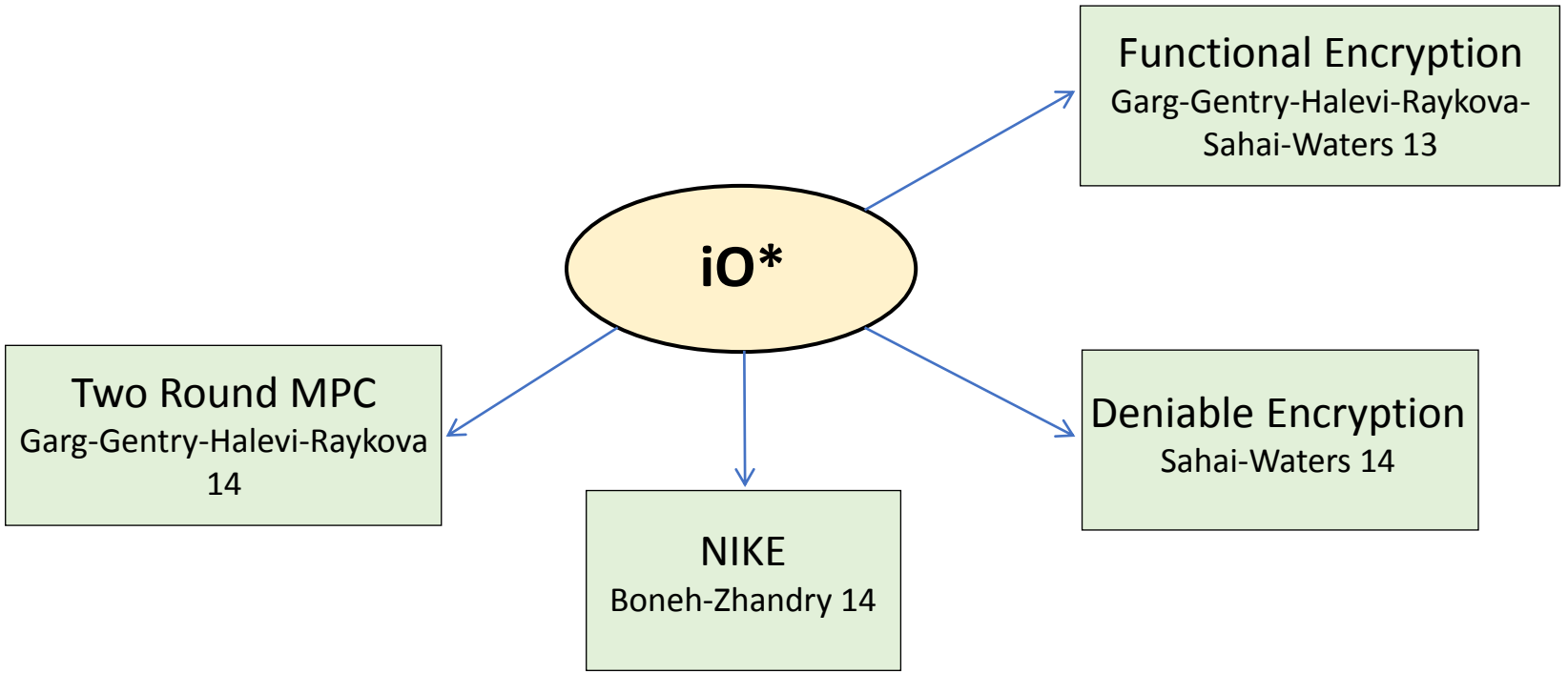
* + other assumptions

Applications of iO



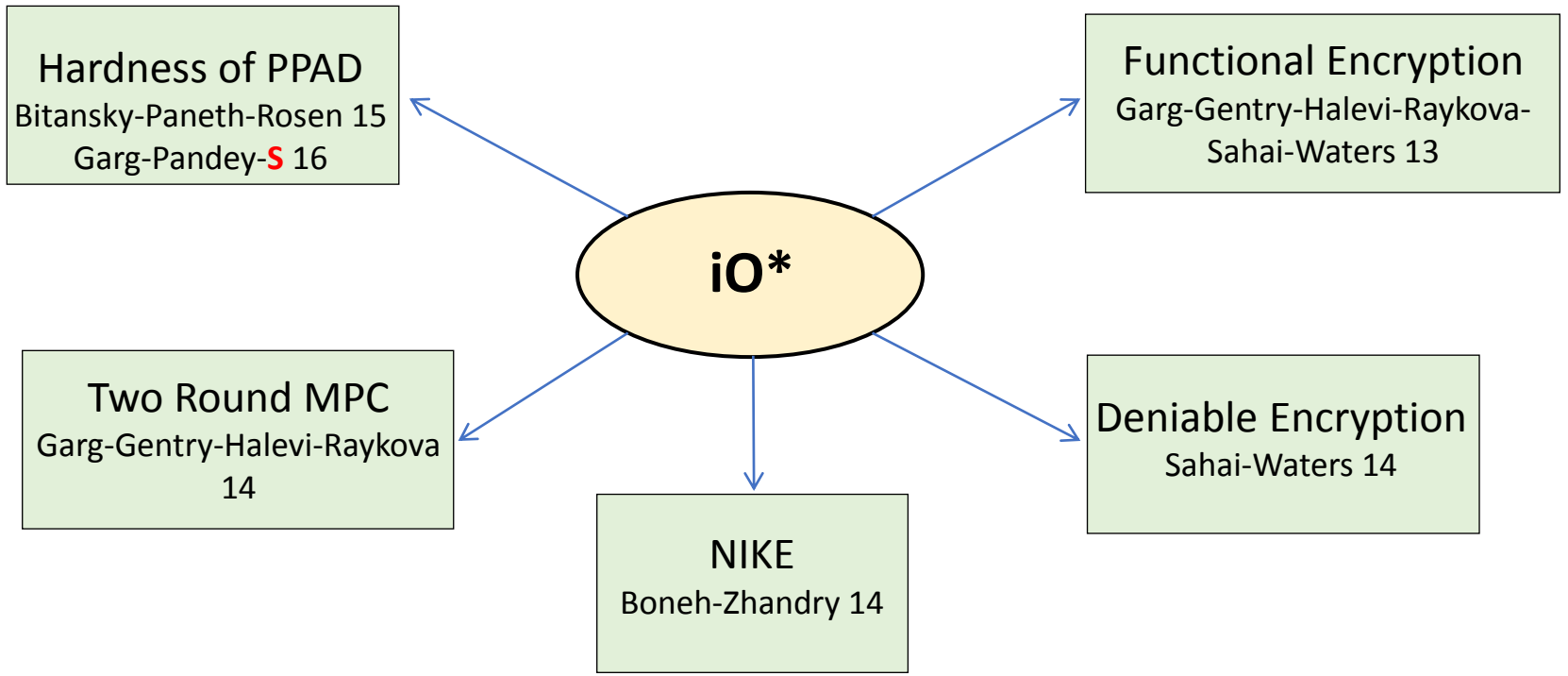
* + other assumptions

Applications of iO



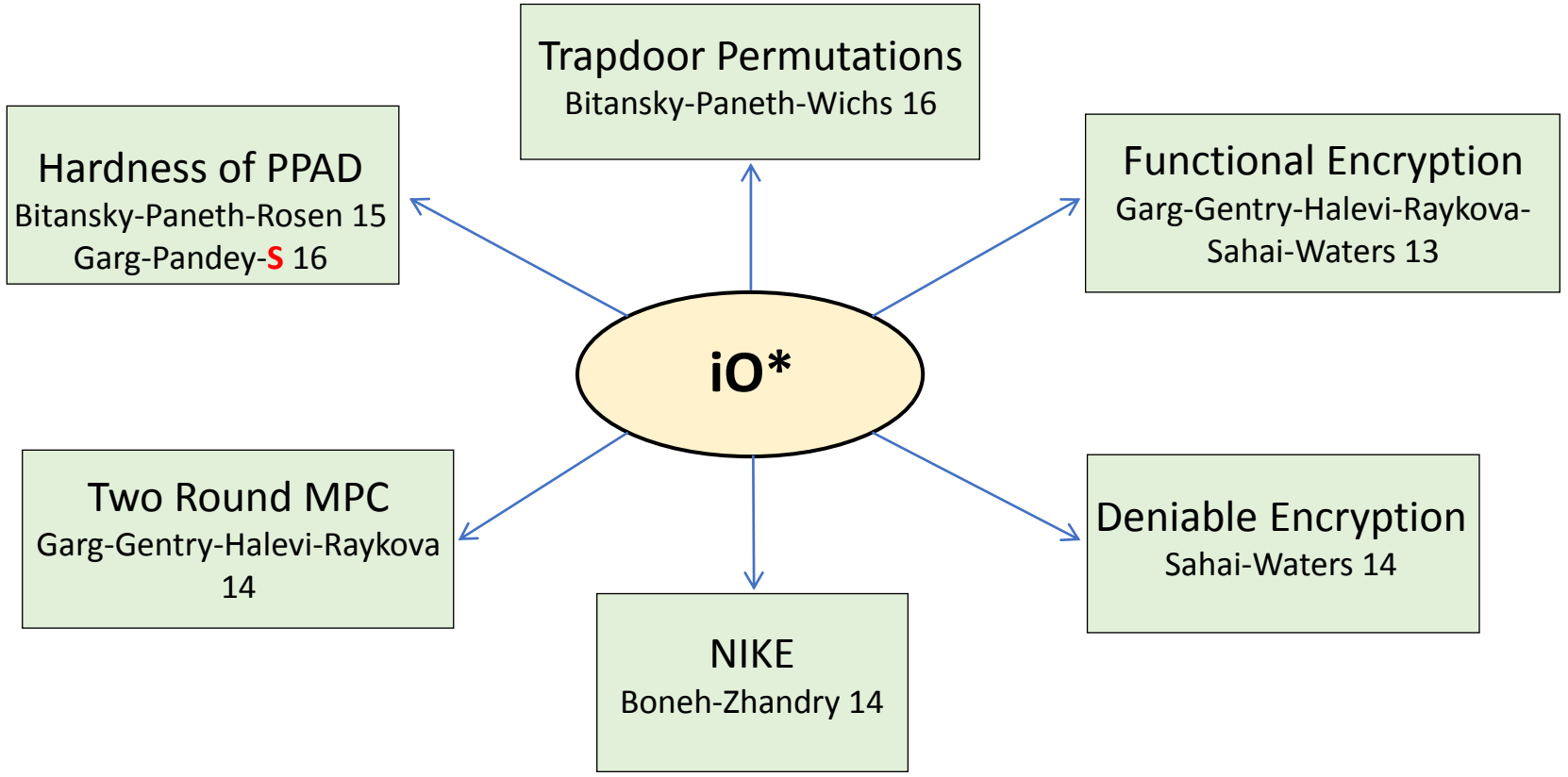
* + other assumptions

Applications of iO



* + other assumptions

Applications of iO



* + other assumptions

Sub-Exponential Barrier

Sub-Exponential Barrier

- Sub-exponential loss in the security reduction in construction of iO.

Sub-Exponential Barrier

- Sub-exponential loss in the security reduction in construction of iO.
- **Observation:** All known constructions of iO require either an exponential number of assumptions or results in a sub-exponential loss in security.

Sub-Exponential Barrier

- Sub-exponential loss in the security reduction in construction of iO.
- **Observation:** All known constructions of iO require either an exponential number of assumptions or results in a sub-exponential loss in security.
- **Belief:** Sub-exponential loss is inherent in iO construction.

Sub-Exponential Barrier

- Sub-exponential loss in the security reduction in construction of iO.
- **Observation:** All known constructions of iO require either an exponential number of assumptions or results in a sub-exponential loss in security.
- **Belief:** Sub-exponential loss is inherent in iO construction.
- Several applications require sub-exponentially hard iO.

Sub-Exponential Barrier

- Sub-exponential loss in the security reduction in construction of iO.
- **Observation:** All known constructions of iO require either an exponential number of assumptions or results in a sub-exponential loss in security.
- **Belief:** Sub-exponential loss is inherent in iO construction.
- Several applications require sub-exponentially hard iO.

Can we break the sub-exponential barrier?

Our Contribution

- In this work, we show that certain applications of iO can be based on a *polynomial falsifiable assumption*.

Our Contribution

- In this work, we show that certain applications of iO can be based on a *polynomial falsifiable assumption*.
- **Assumption:** Compact, public-key Functional Encryption.

Our Contribution

- In this work, we show that certain applications of iO can be based on a *polynomial falsifiable assumption*.
- **Assumption:** Compact, public-key Functional Encryption.

Theorem: Assuming polynomially hard compact, public-key functional encryption there exists

1. Trapdoor permutations.
2. Non-Interactive Key Exchange for unbounded number of parties without a trusted setup.

Our Contribution

- In this work, we show that certain applications of iO can be based on a *polynomial falsifiable assumption*.
- **Assumption:** Compact, public-key Functional Encryption.

Theorem: Assuming polynomially hard compact, public-key functional encryption there exists

1. Trapdoor permutations.
2. Non-Interactive Key Exchange for unbounded number of parties without a trusted setup.

[AJ15,BV15]: Sub-exponentially hard compact public-key FE implies iO

Our Contribution

- In this work, we show that certain applications of iO can be based on a *polynomial falsifiable assumption*.
- **Assumption:** Compact, public-key Functional Encryption.

Theorem: Assuming polynomially hard compact, public-key functional encryption there exists

1. Trapdoor permutations.
2. Non-Interactive Key Exchange for ~~un~~bounded number of parties with~~ou~~t a trusted setup.

[AJ15,BV15]: Sub-exponentially hard compact public-key FE implies iO

Outline

Outline

- Functional Encryption – Definition and Security

Outline

- Functional Encryption – Definition and Security
- Outline of Ananth-Jain and Bitansky-Vaikuntanathan FE to iO transformation.

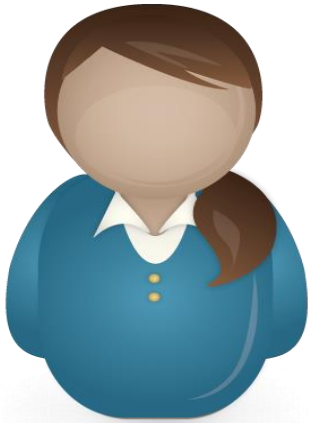
Outline

- Functional Encryption – Definition and Security
- Outline of Ananth-Jain and Bitansky-Vaikuntanathan FE to iO transformation.
- Key technique to break the sub-exponential barrier.

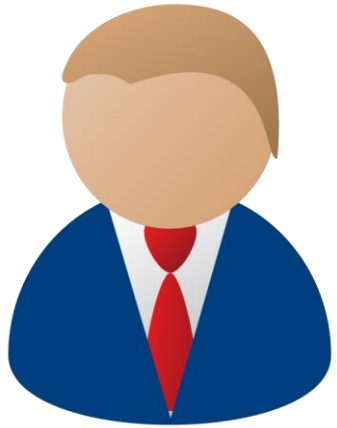
Outline

- Functional Encryption – Definition and Security
- Outline of Ananth-Jain and Bitansky-Vaikuntanathan FE to iO transformation.
- Key technique to break the sub-exponential barrier.
- How to use this technique to construct NIKE?

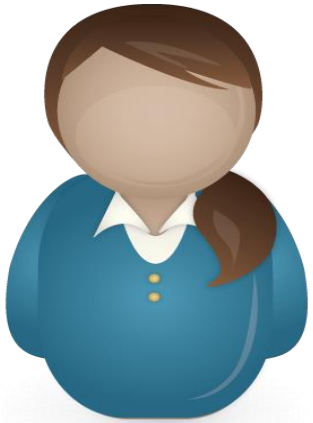
Functional Encryption [Boneh-Sahai-Waters 11]

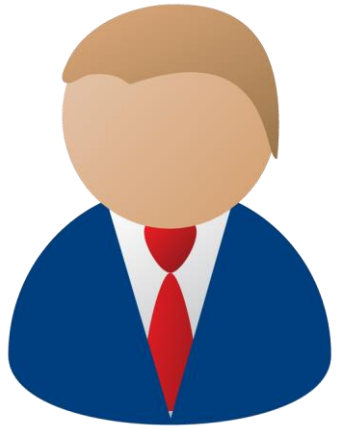


Data D



Functional Encryption [Boneh-Sahai-Waters 11]

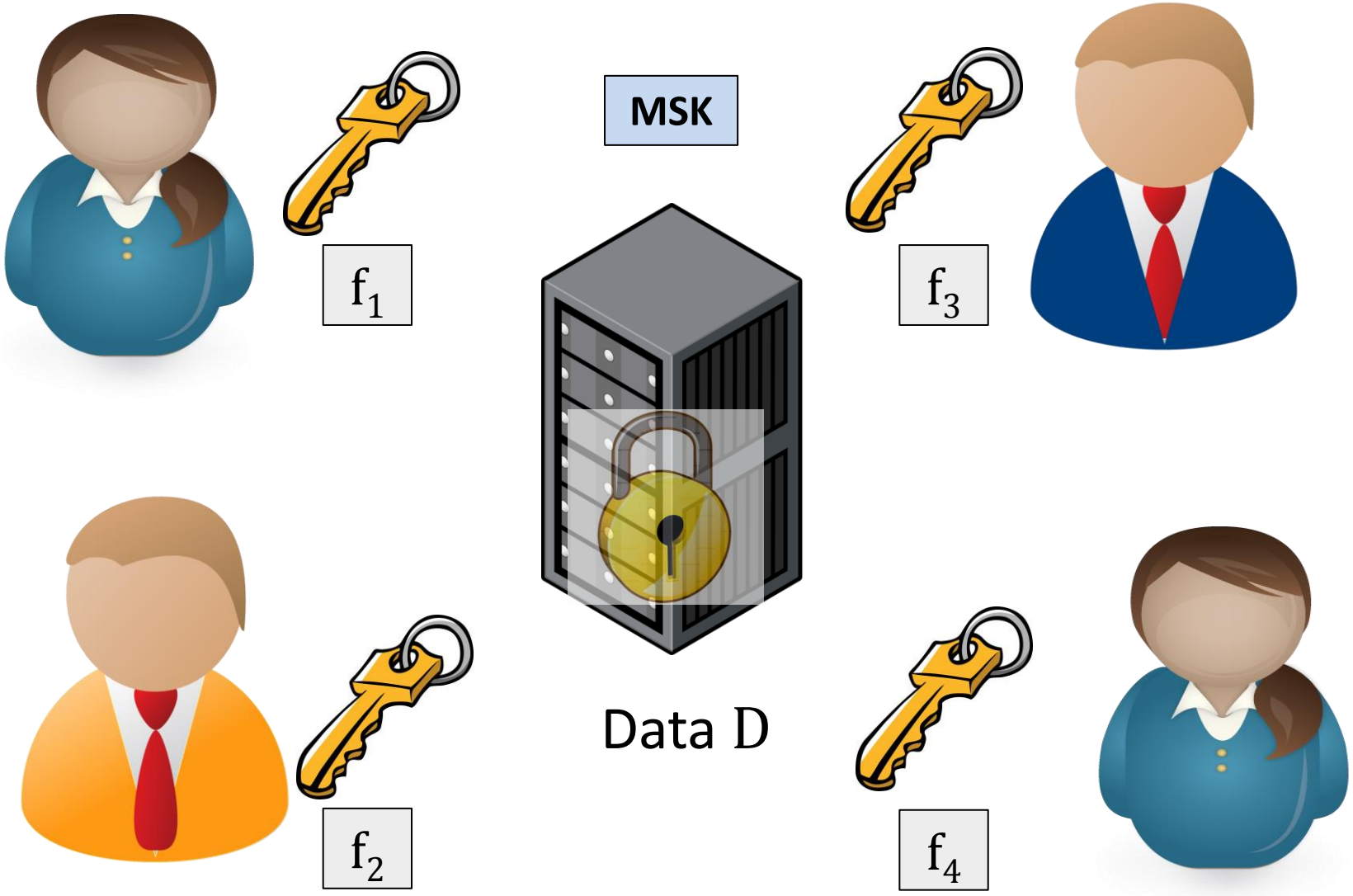




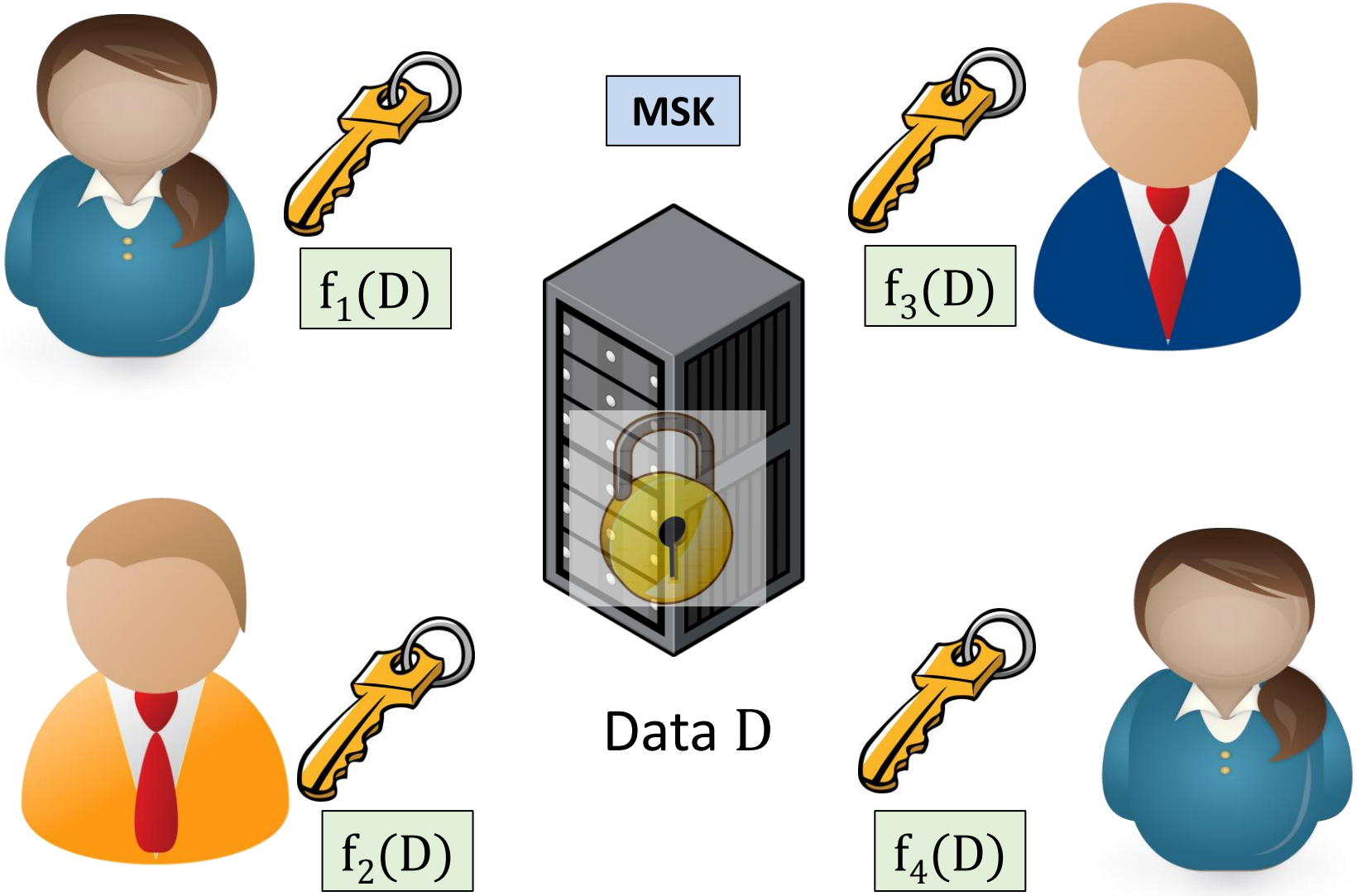
MSK

Data D

Functional Encryption [Boneh-Sahai-Waters 11]



Functional Encryption [Boneh-Sahai-Waters 11]



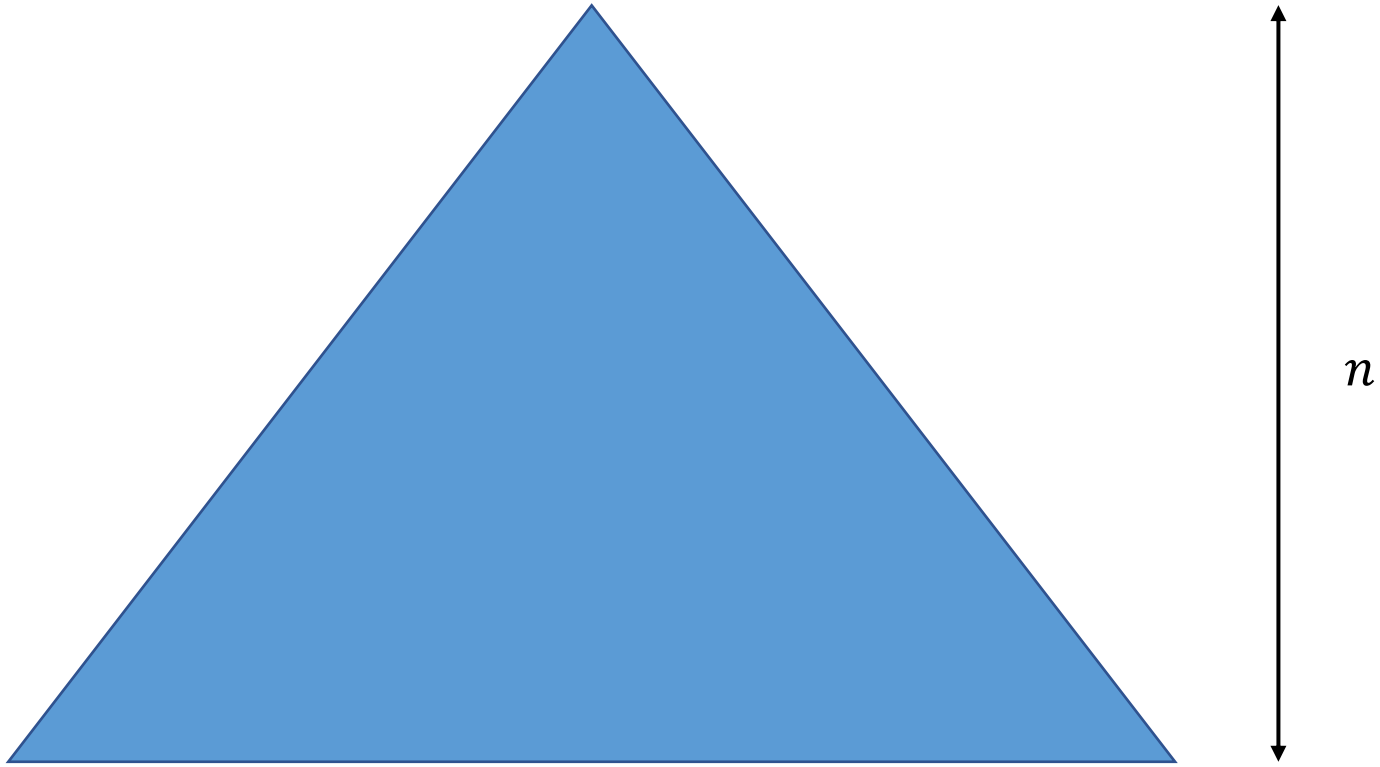
Outline of [AJ15] and [BV15] FE to iO transformation

Outline of [AJ15] and [BV15] FE to iO transformation

$C: \{0,1\}^n \to \{0,1\}^m$

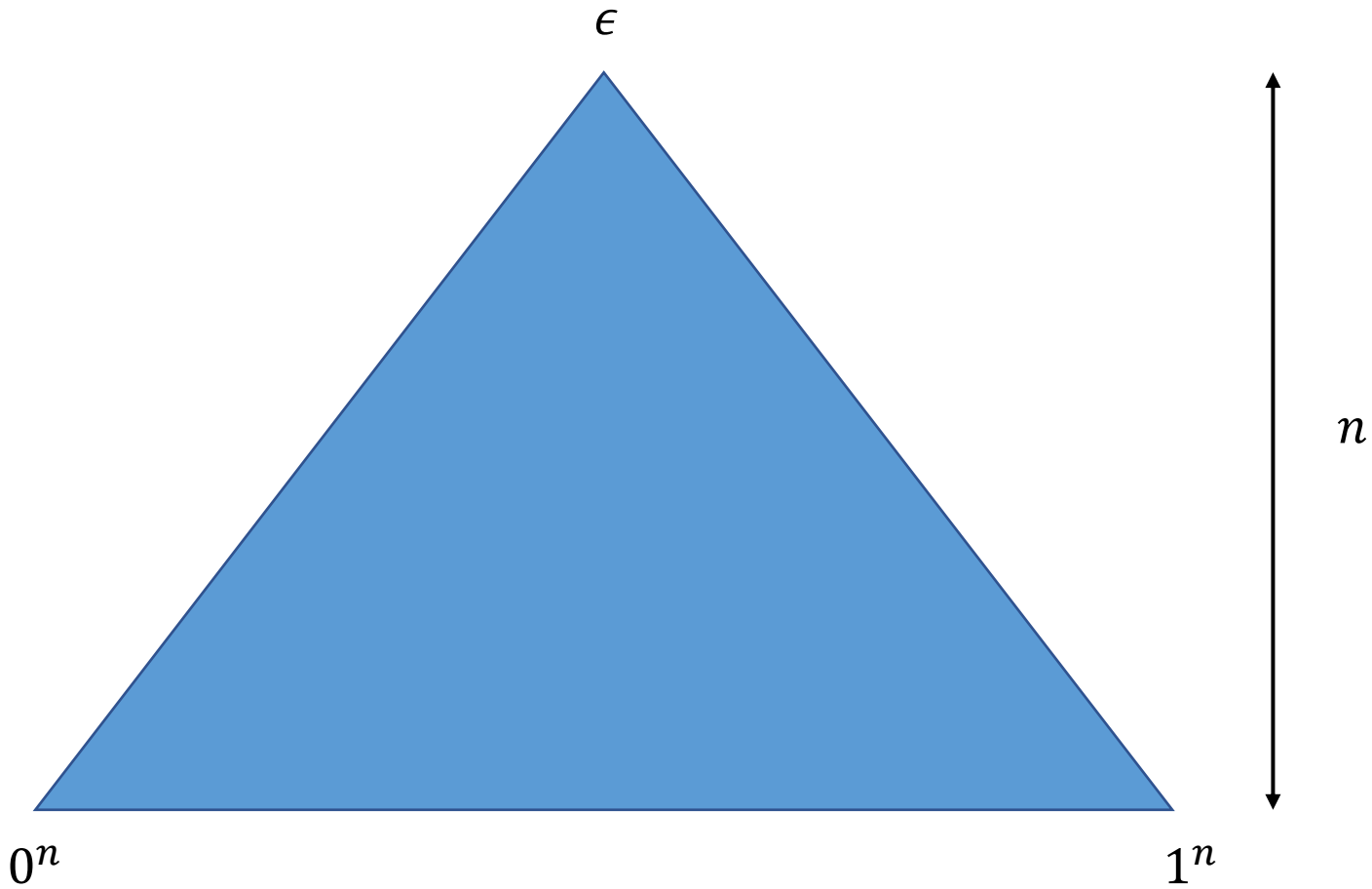
Outline of [AJ15] and [BV15] FE to iO transformation

$C: \{0,1\}^n \rightarrow \{0,1\}^m$



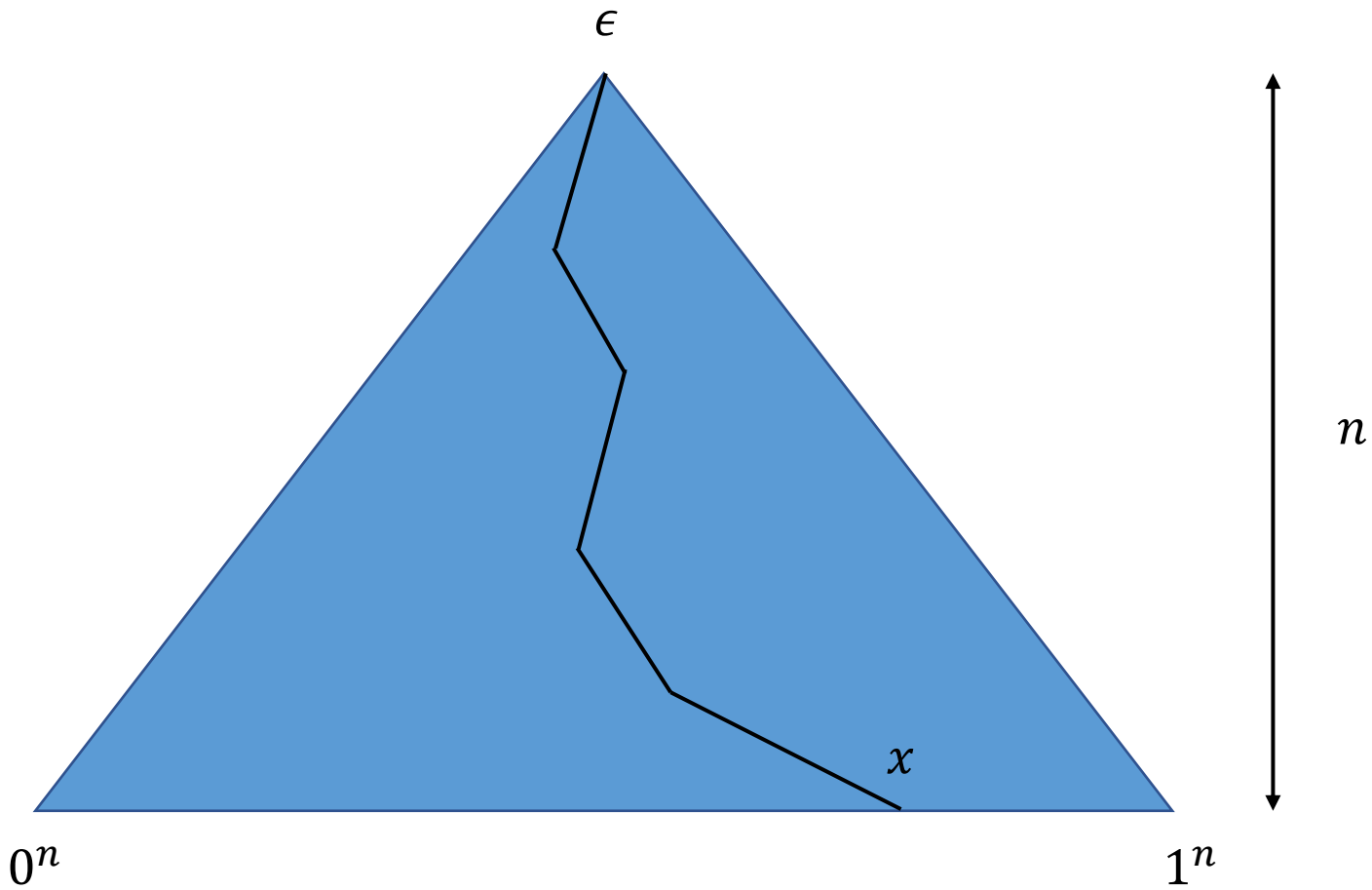
Outline of [AJ15] and [BV15] FE to iO transformation

$C: \{0,1\}^n \rightarrow \{0,1\}^m$



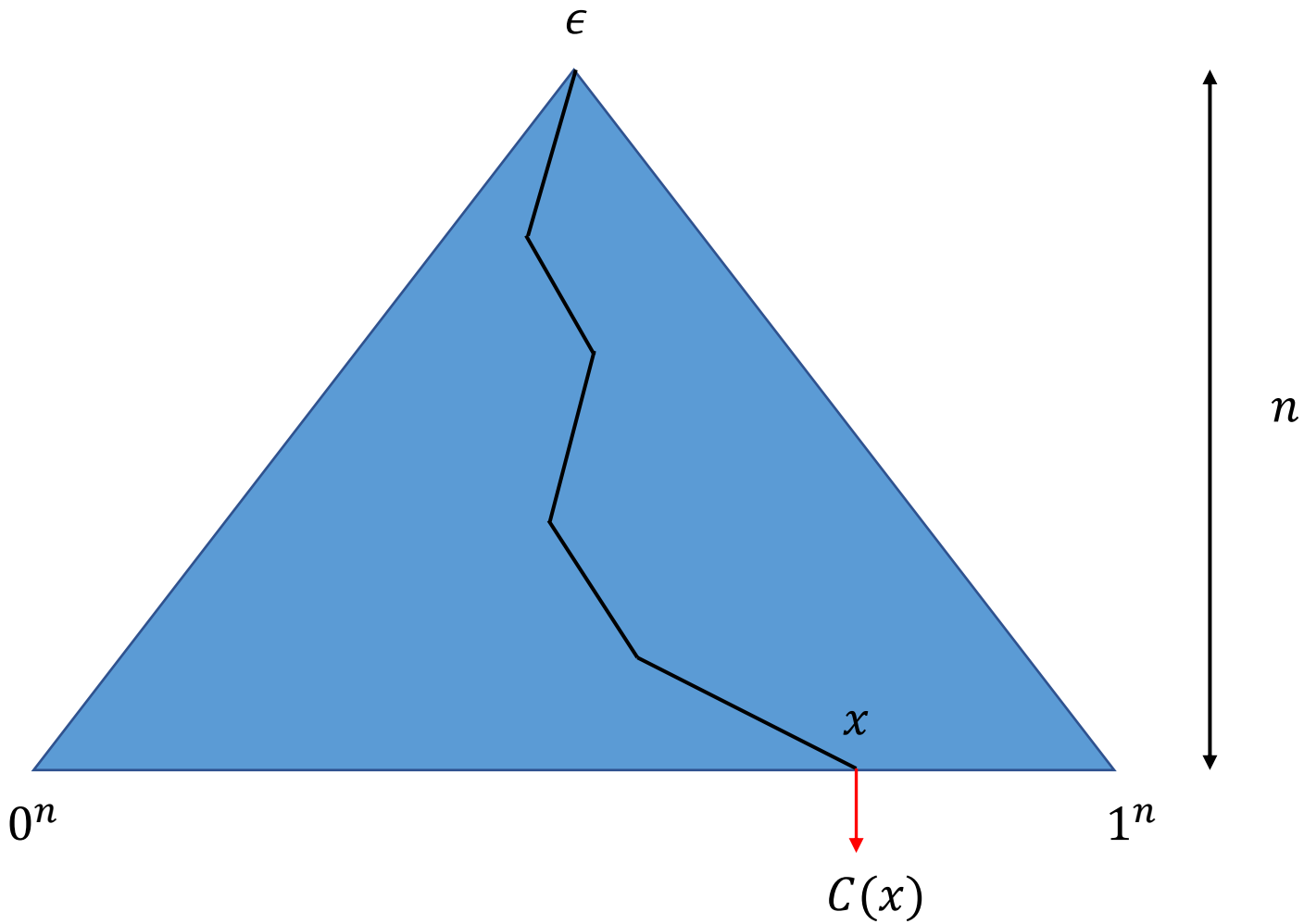
Outline of [AJ15] and [BV15] FE to iO transformation

$C: \{0,1\}^n \rightarrow \{0,1\}^m$



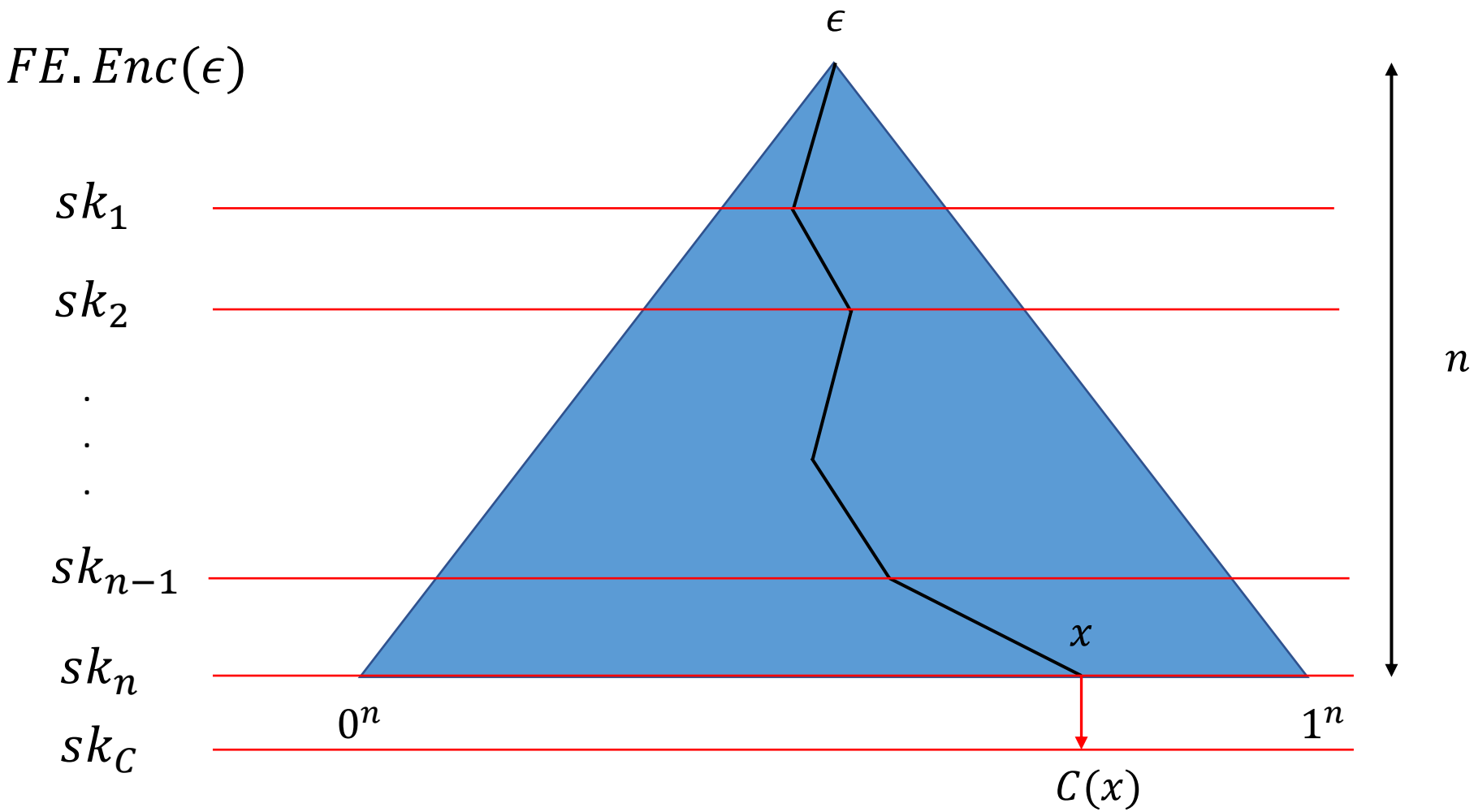
Outline of [AJ15] and [BV15] FE to iO transformation

$C: \{0,1\}^n \rightarrow \{0,1\}^m$



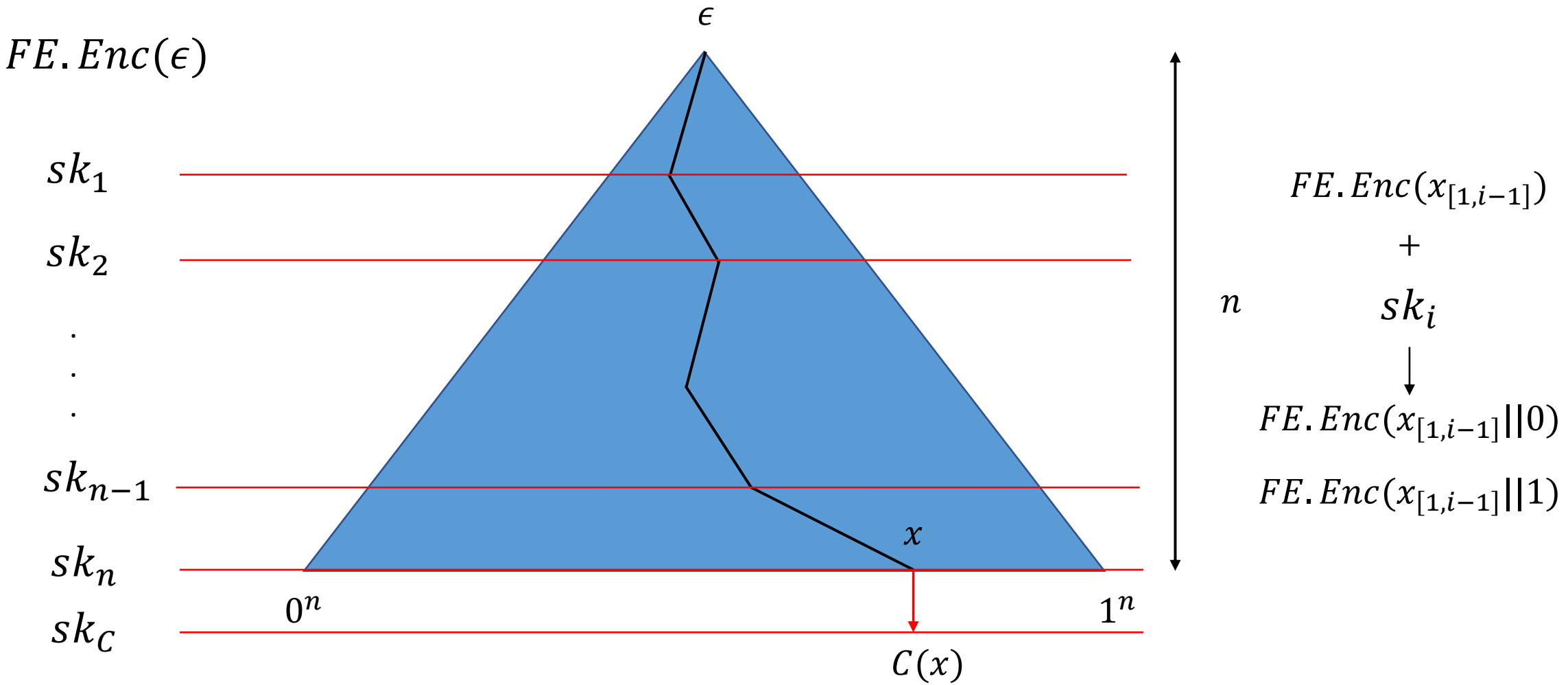
Outline of [AJ15] and [BV15] FE to iO transformation

$C: \{0,1\}^n \rightarrow \{0,1\}^m$



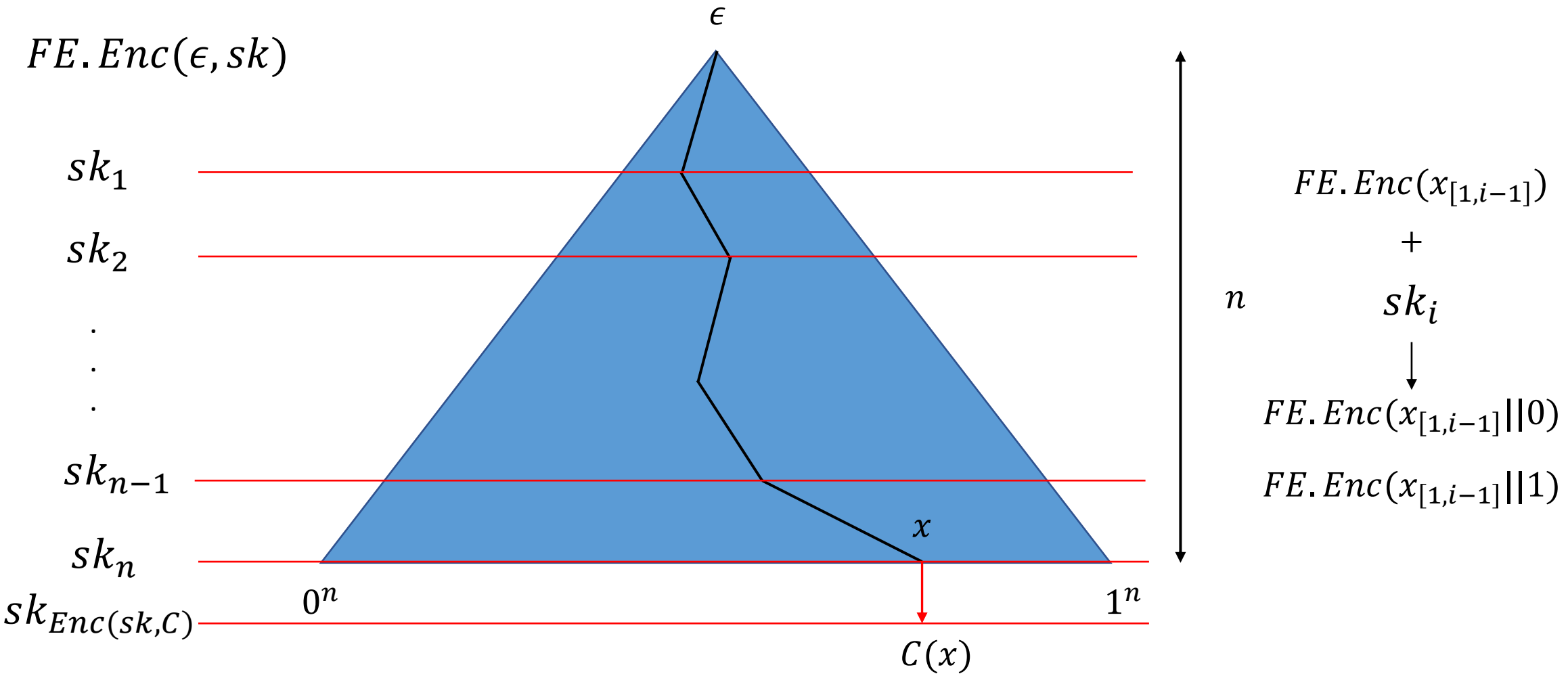
Outline of [AJ15] and [BV15] FE to iO transformation

$C: \{0,1\}^n \rightarrow \{0,1\}^m$



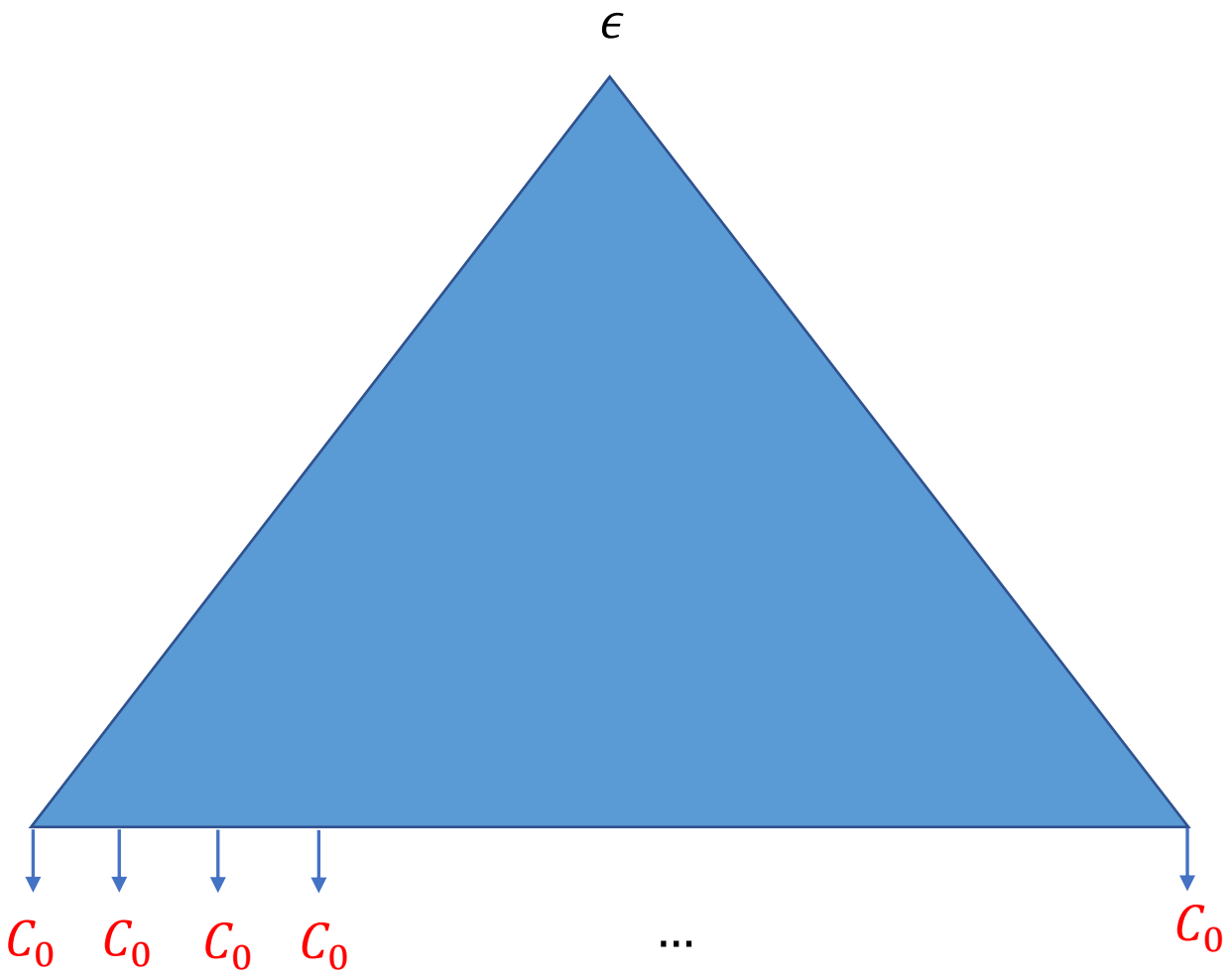
Outline of [AJ15] and [BV15] FE to iO transformation

$C: \{0,1\}^n \rightarrow \{0,1\}^m$



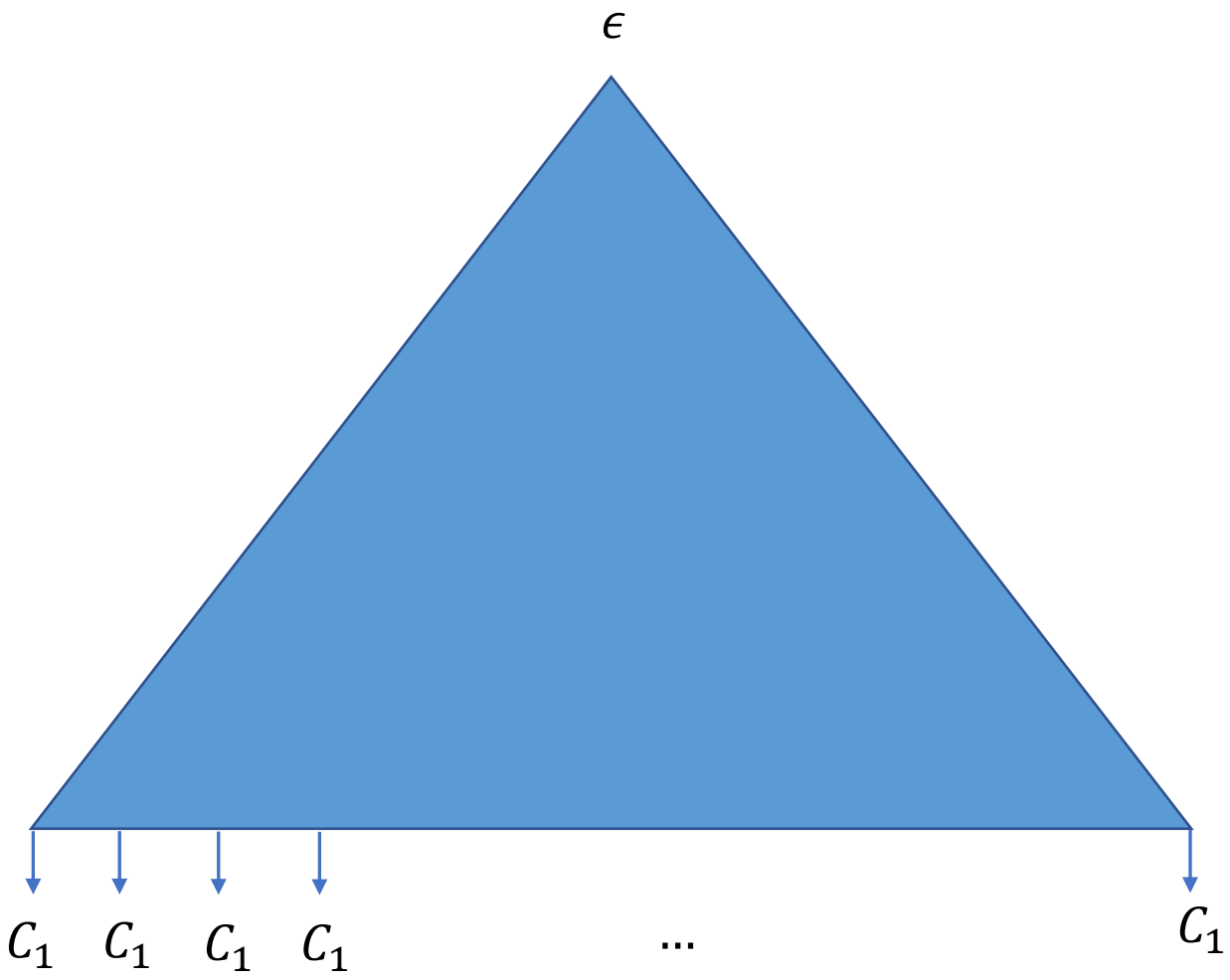
Sub-Exponential Barrier

$C_0 \equiv C_1$



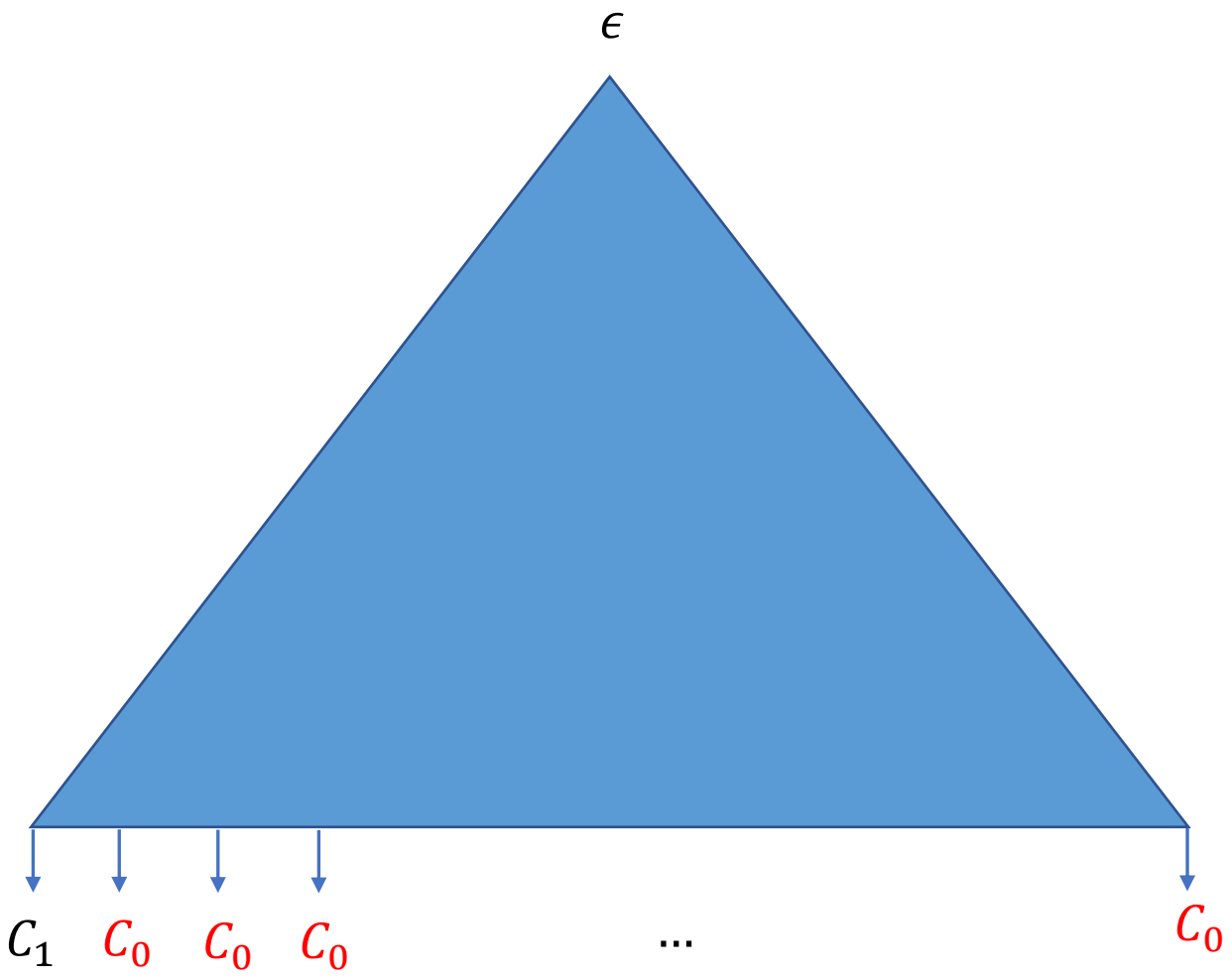
Sub-Exponential Barrier

$C_0 \equiv C_1$



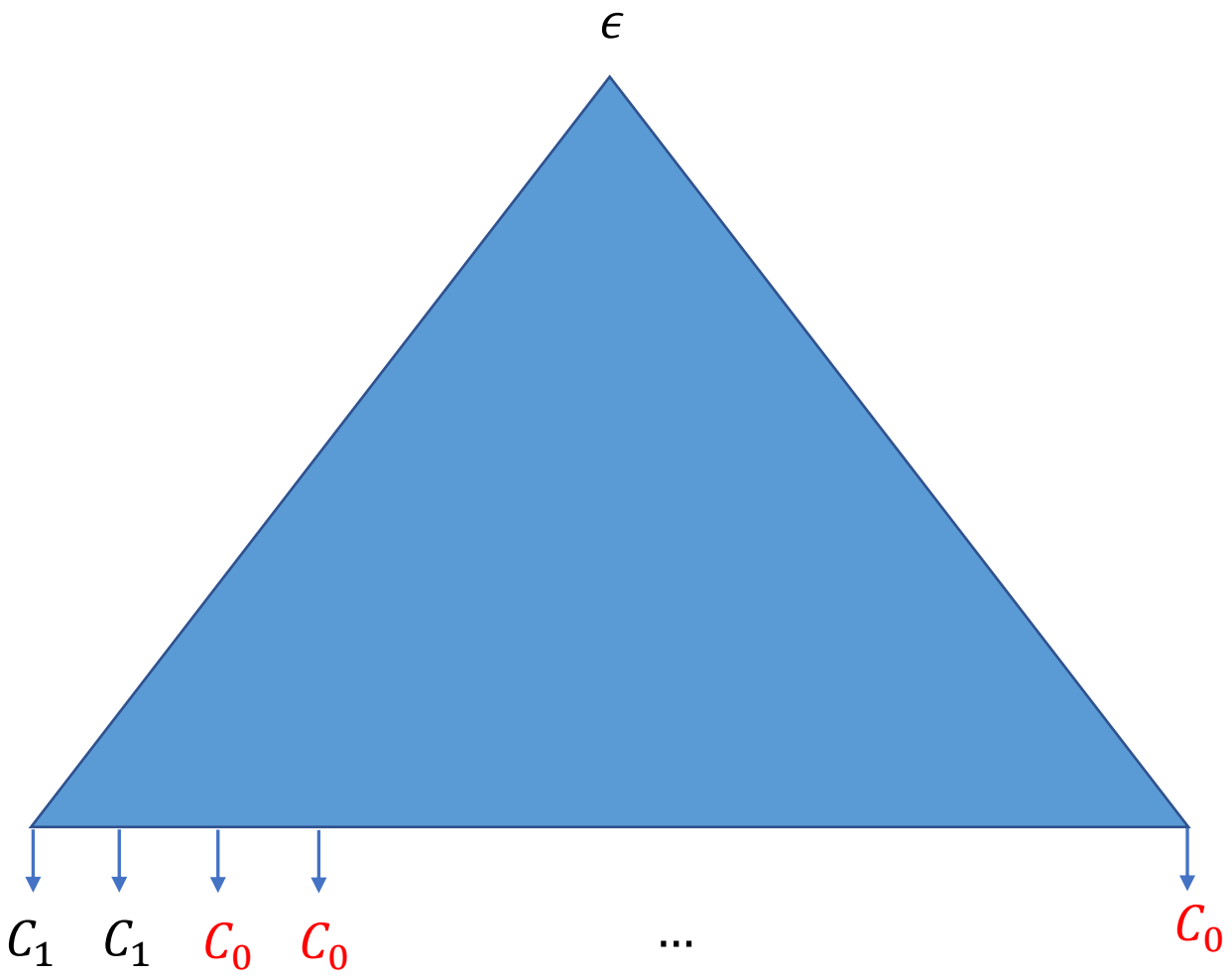
Sub-Exponential Barrier

$C_0 \equiv C_1$



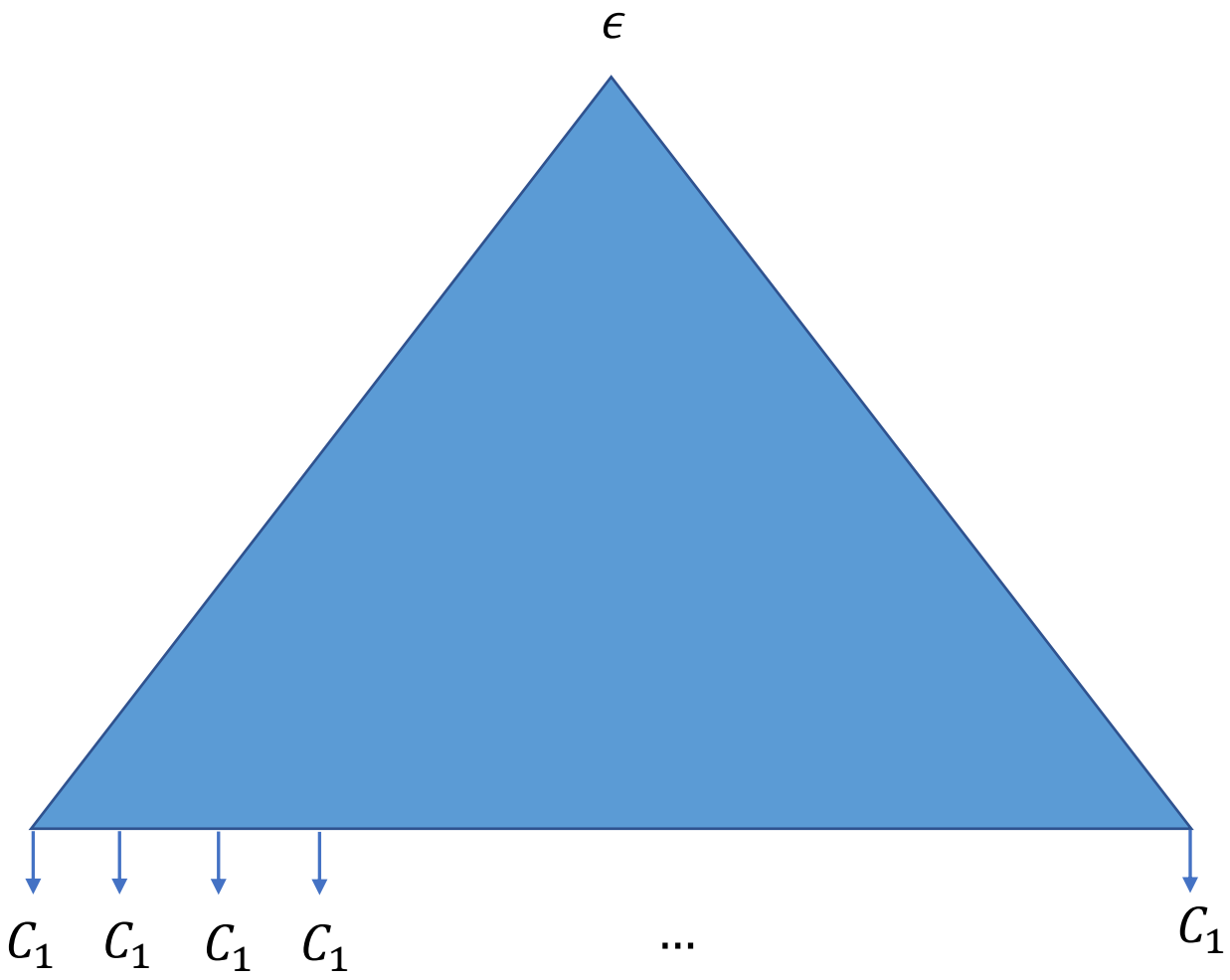
Sub-Exponential Barrier

$C_0 \equiv C_1$



Sub-Exponential Barrier

$C_0 \equiv C_1$



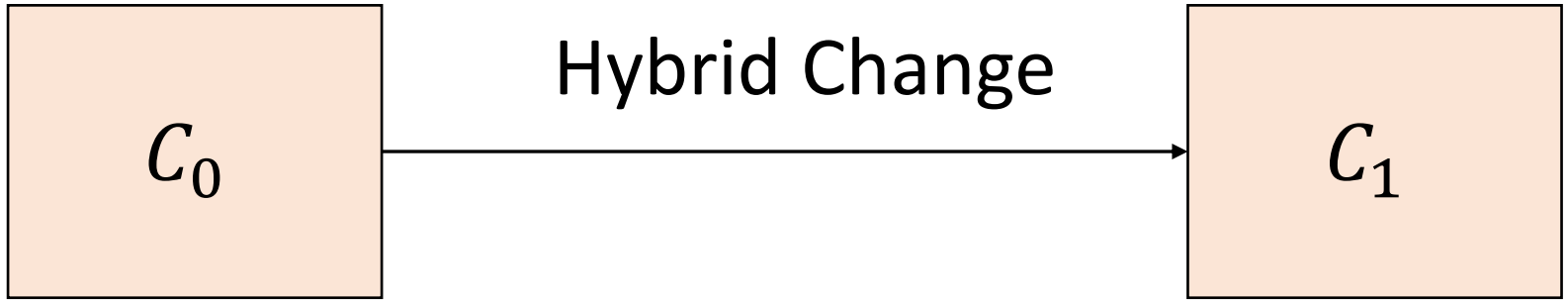
Key Technique to break the Sub-Exponential barrier

Key Technique to break the Sub-Exponential barrier

Insight: Typical circuits encountered in iO proofs have similar structure.

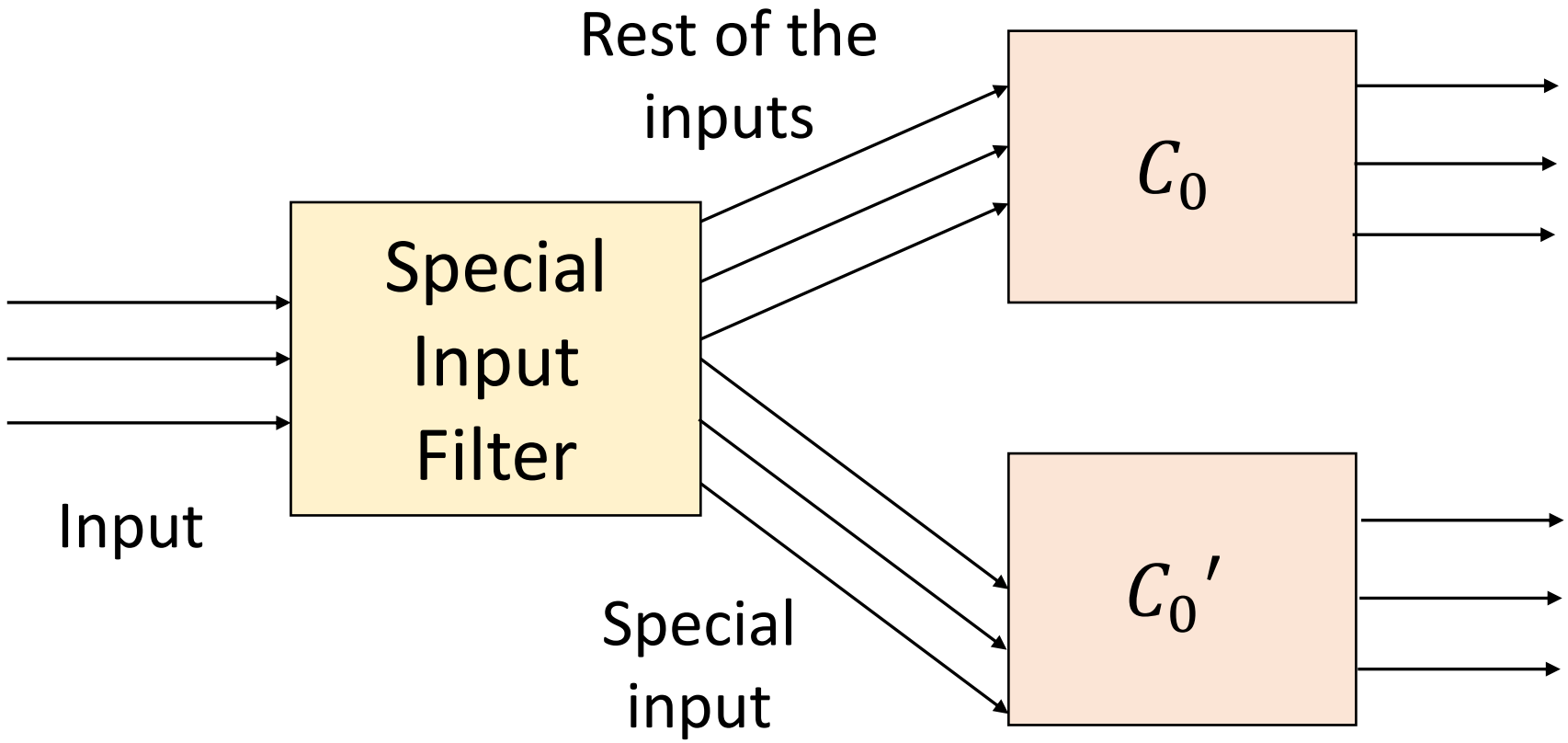
Key Technique to break the Sub-Exponential barrier

Insight: Typical circuits encountered in iO proofs have similar structure.



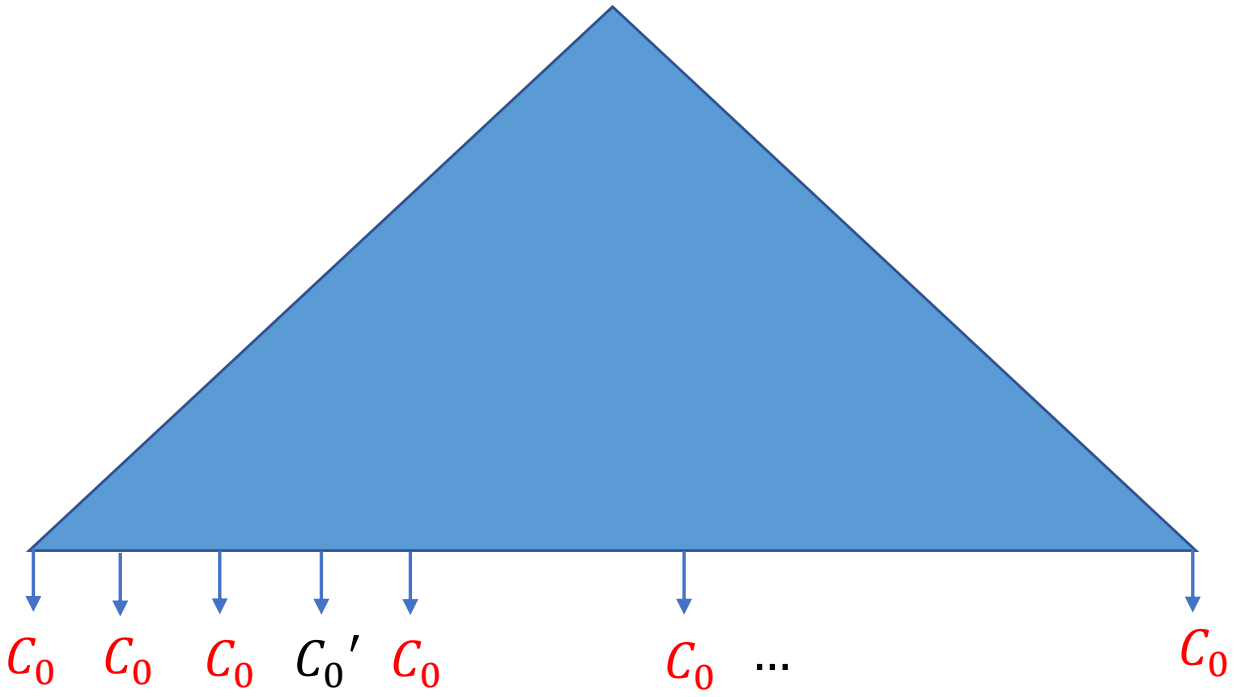
Key Technique to break the Sub-Exponential barrier

Structure of C_1



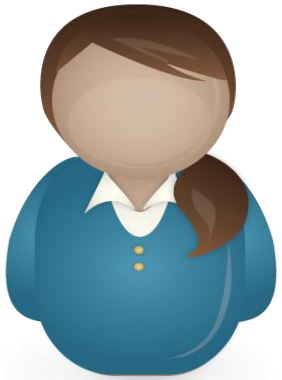
Key Technique to break the Sub-Exponential barrier

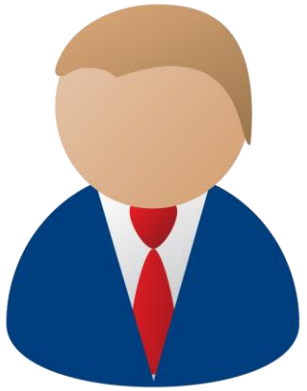
Key Technique to break the Sub-Exponential barrier

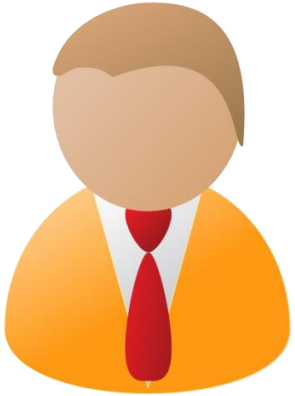


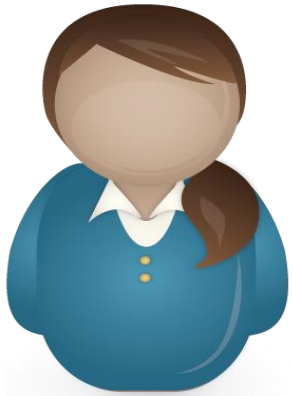
Non-Interactive Key Exchange

Non-Interactive Key Exchange



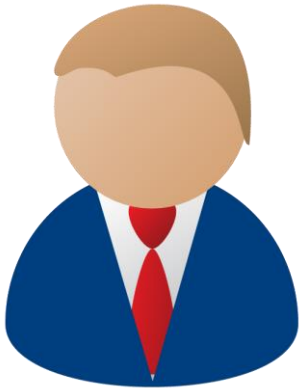


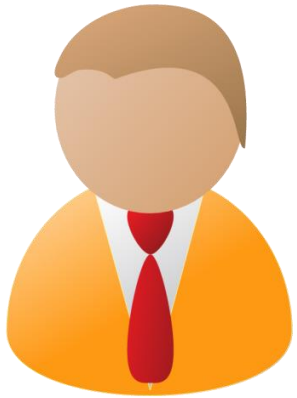


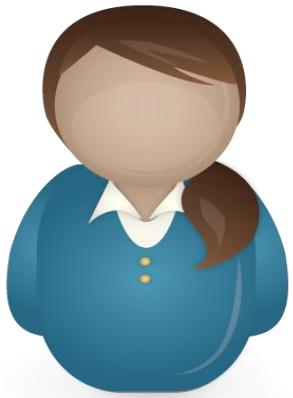


Non-Interactive Key Exchange

Public Bulletin Board







Non-Interactive Key Exchange

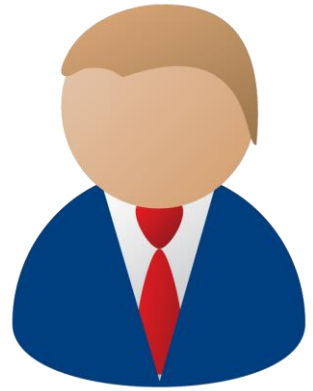
sk_1

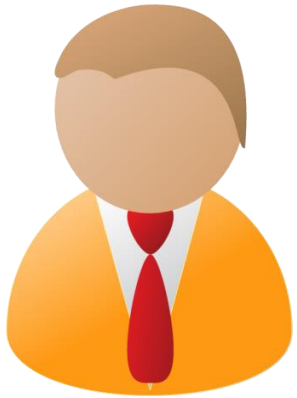
Public Bulletin Board

pk_1 pk_2

pk_4 pk_3

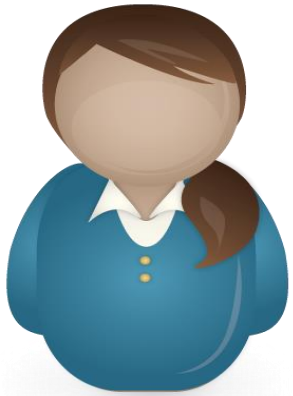
sk_2





sk_4

sk_3



Non-Interactive Key Exchange

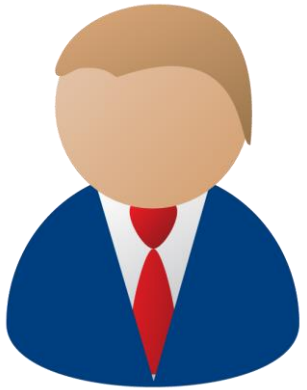
sk_1

K

Public Bulletin Board

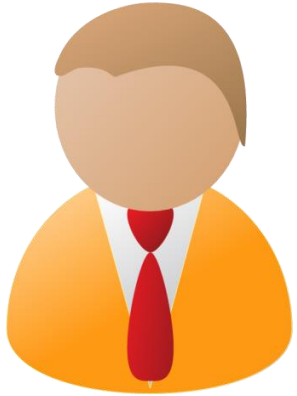
pk_1 pk_2

pk_4 pk_3



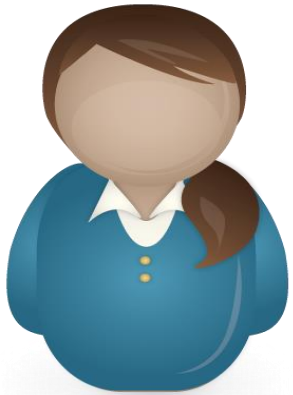
sk_2

K



sk_4

K



sk_3

K

Boneh-Zhandy NIKE from iO

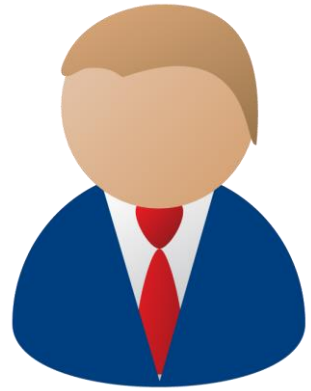
sk_1

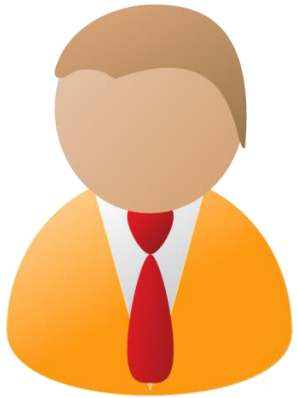
Public Bulletin Board

pk_1 pk_2

pk_4 pk_3

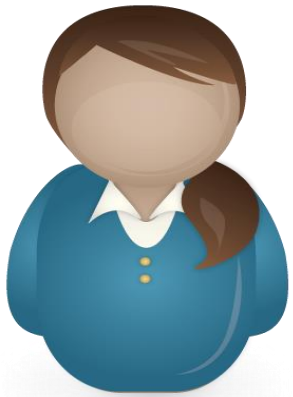
sk_2





sk_4

sk_3



Boneh-Zhandy NIKE from iO

sk_1

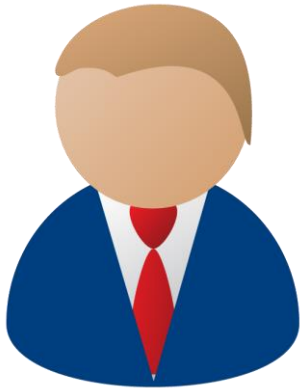
$K = PRF_S(pk_1|| \ \ldots||pk_4)$

Public Bulletin Board

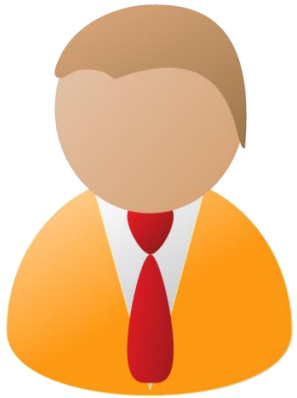
pk_1 pk_2

pk_4 pk_3

sk_2



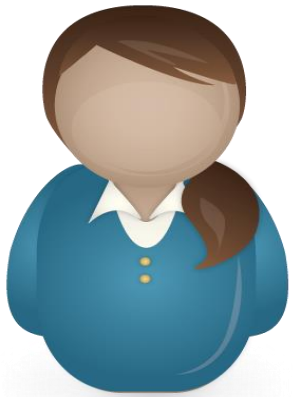
$K = PRF_S(pk_1|| \ \ldots||pk_4)$



sk_4

$K = PRF_S(pk_1|| \ \ldots||pk_4)$

sk_3



$K = PRF_S(pk_1|| \ \ldots||pk_4)$

Introduce trusted Party

Program P

Input: pk_1, pk_2, pk_3, pk_4

Constants: A PRF key S

- Compute $K = PRF_S(pk_1 || \dots || pk_4)$.
- Output $\{PKE.Enc_{pk_i}(K)\}_i$

Introduce trusted Party

Program P

Input: pk_1, pk_2, pk_3, pk_4

Constants: A PRF key S

- Compute $K = PRF_S(pk_1 || \dots || pk_4)$.
- Output $\{PKE.Enc_{pk_i}(K)\}_i$

Proof of Security: At a high level

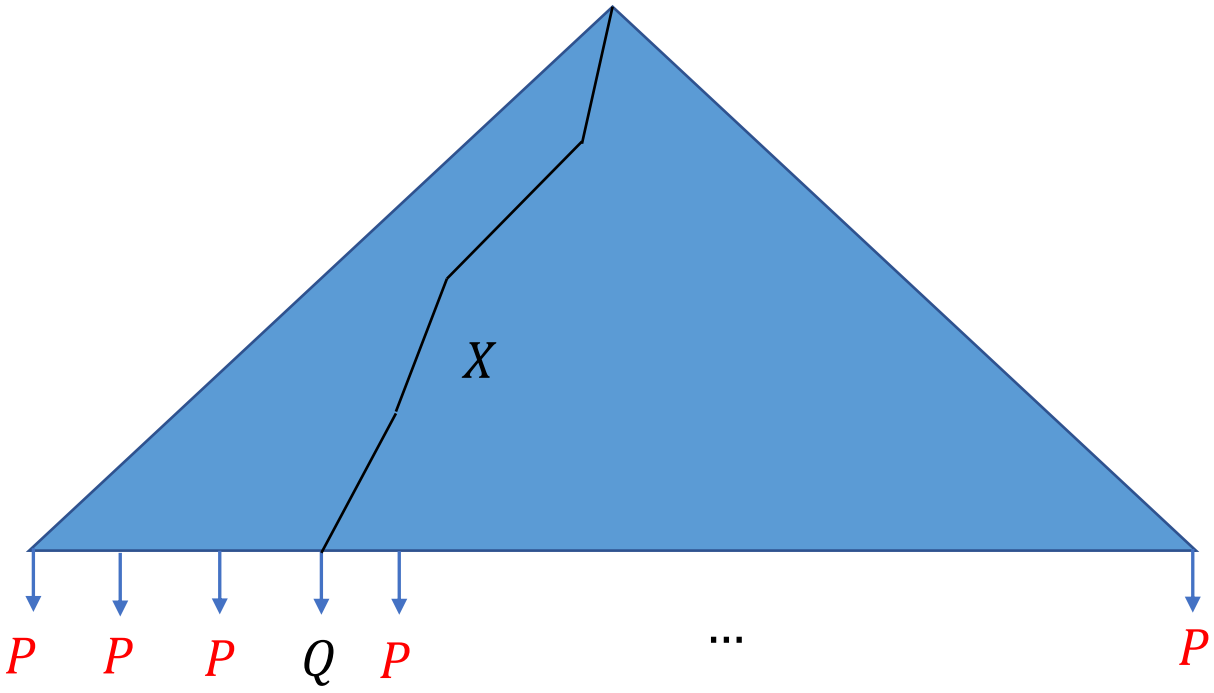
Program P

Input: pk_1, pk_2, pk_3, pk_4
Constants: A PRF key S
Compute
$K = PRF_S(pk_1 || \ldots || pk_4)$.
Output $\{PKE.Enc_{pk_i}(K)\}_i$

Program P'

Input: pk_1, pk_2, pk_3, pk_4
Constants: A PRF key S, X, Z
If($\boldsymbol{pk_1} || \ldots || \boldsymbol{pk_4}) = \boldsymbol{X}$) then
output $\boldsymbol{Z}$
Else, compute
$K = PRF_S(pk_1 || \ldots || pk_4)$.
Output $\{PKE.Enc_{pk_i}(K)\}_i$

Applying our technique



Conclusion

Conclusion

- We identify a property that is shared by many applications of iO that enables us to base security on polynomial hardness assumptions.

Conclusion

- We identify a property that is shared by many applications of iO that enables us to base security on polynomial hardness assumptions.
- Not all applications can be obtained! Ex. NIZK (Sahai-Waters)

Conclusion

- We identify a property that is shared by many applications of iO that enables us to base security on polynomial hardness assumptions.
- Not all applications can be obtained! Ex. NIZK (Sahai-Waters)
- Follow-up work by Liu-Zhandry provides a simple interface for constructing applications from polynomial hardness assumptions.

Thank you!