# Multi-input Inner-Product Functional Encryption from Pairings



Michel Abdalla, CNRS and ENS

Romain Gay, ENS

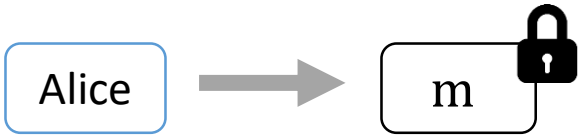
Mariana Raykova, Yale University

Hoeteck Wee, CNRS and ENS



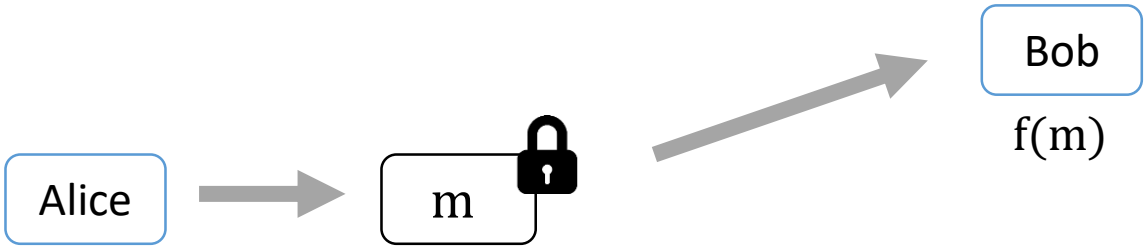
# Functional Encryption

[Boneh, Sahai, Waters 11]



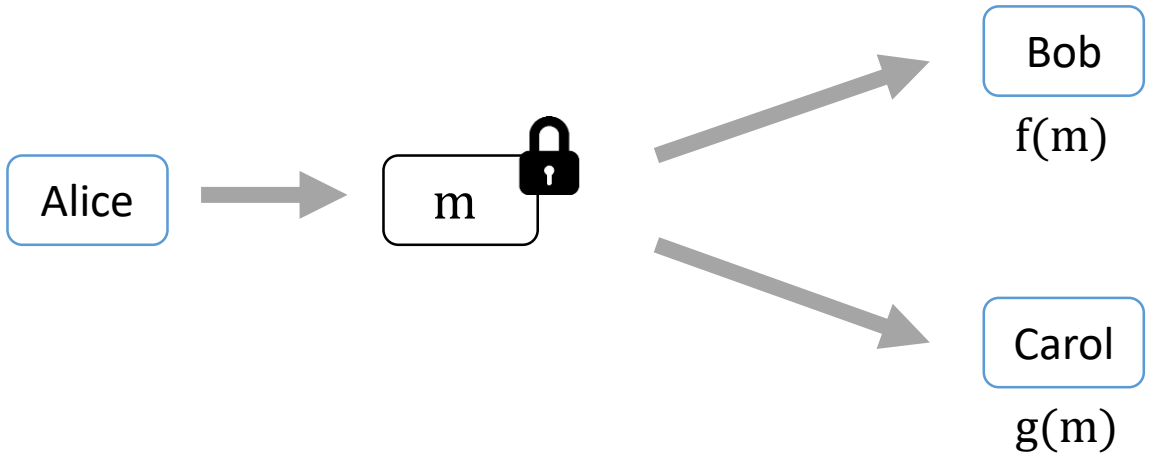
# Functional Encryption

[Boneh, Sahai, Waters 11]



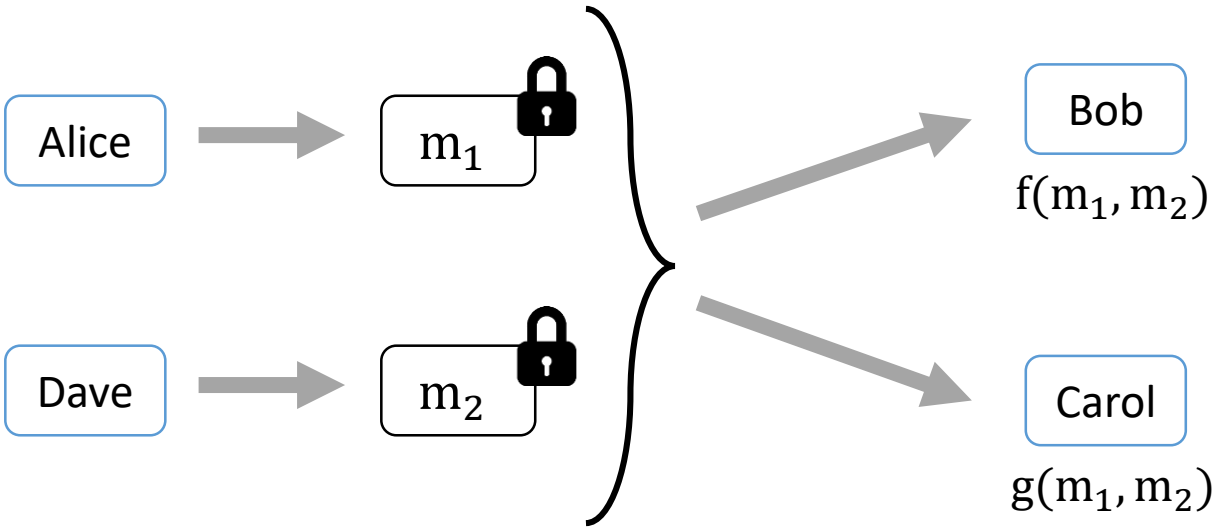
# Functional Encryption

[Boneh, Sahai, Waters 11]



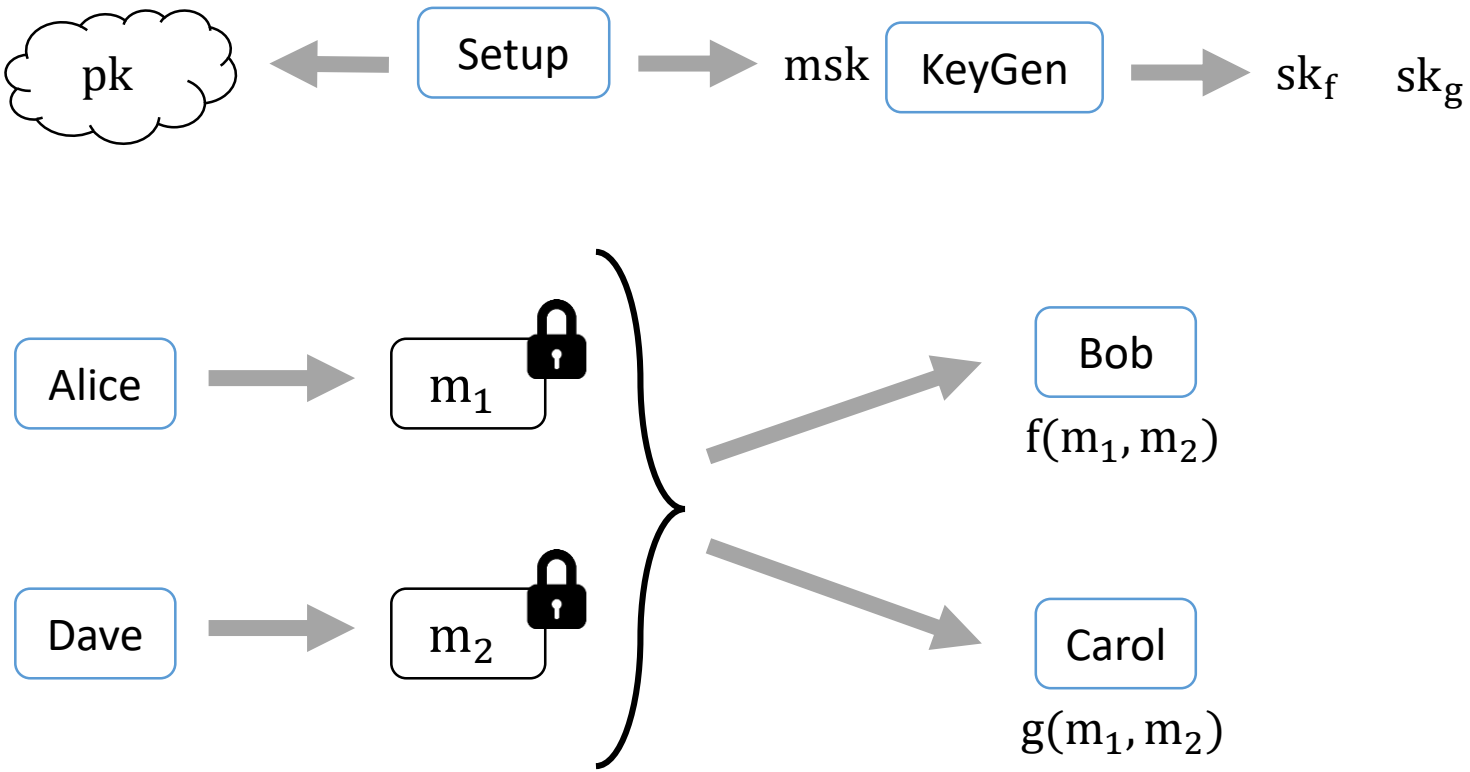
# Multi-input Functional Encryption

[Goldwasser, Gordon, Goyal, Jain, Katz, Liu, Sahai, Shi, Zhou 14]



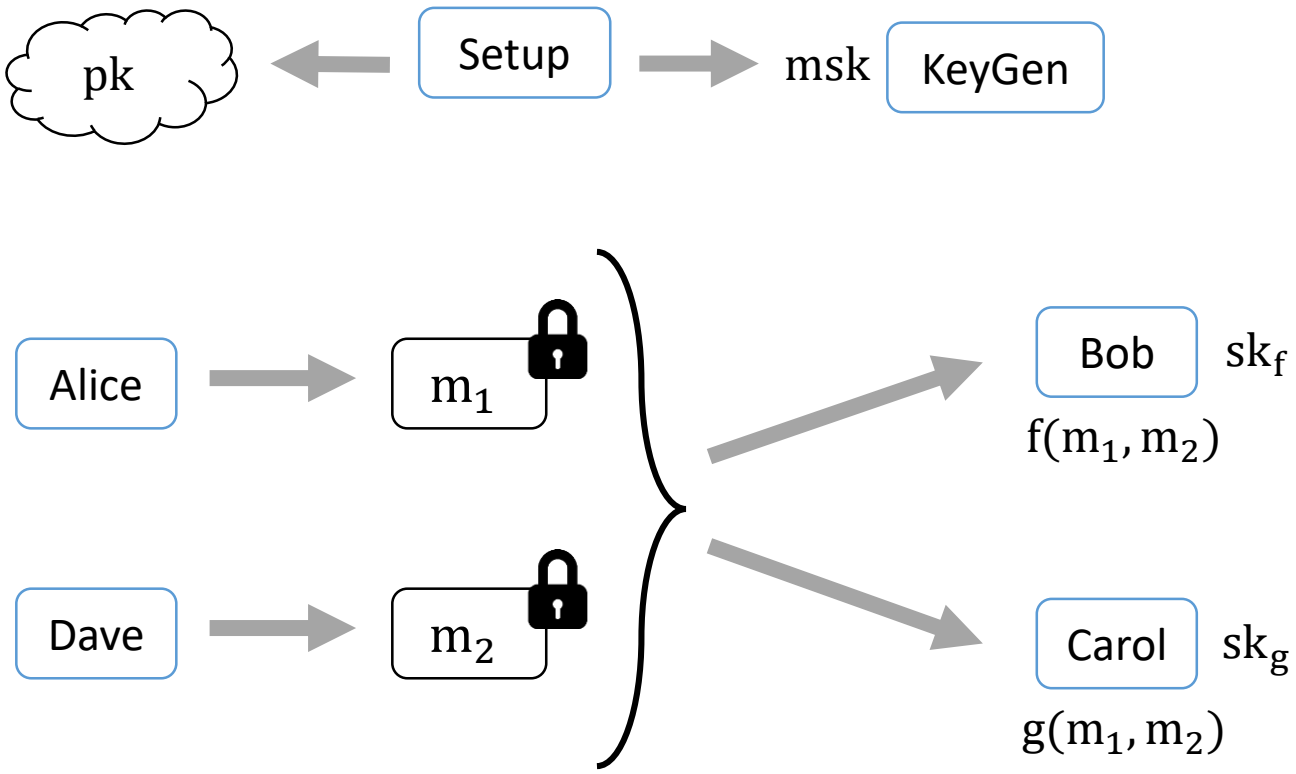
# Multi-input Functional Encryption

[Goldwasser, Gordon, Goyal, Jain, Katz, Liu, Sahai, Shi, Zhou 14]



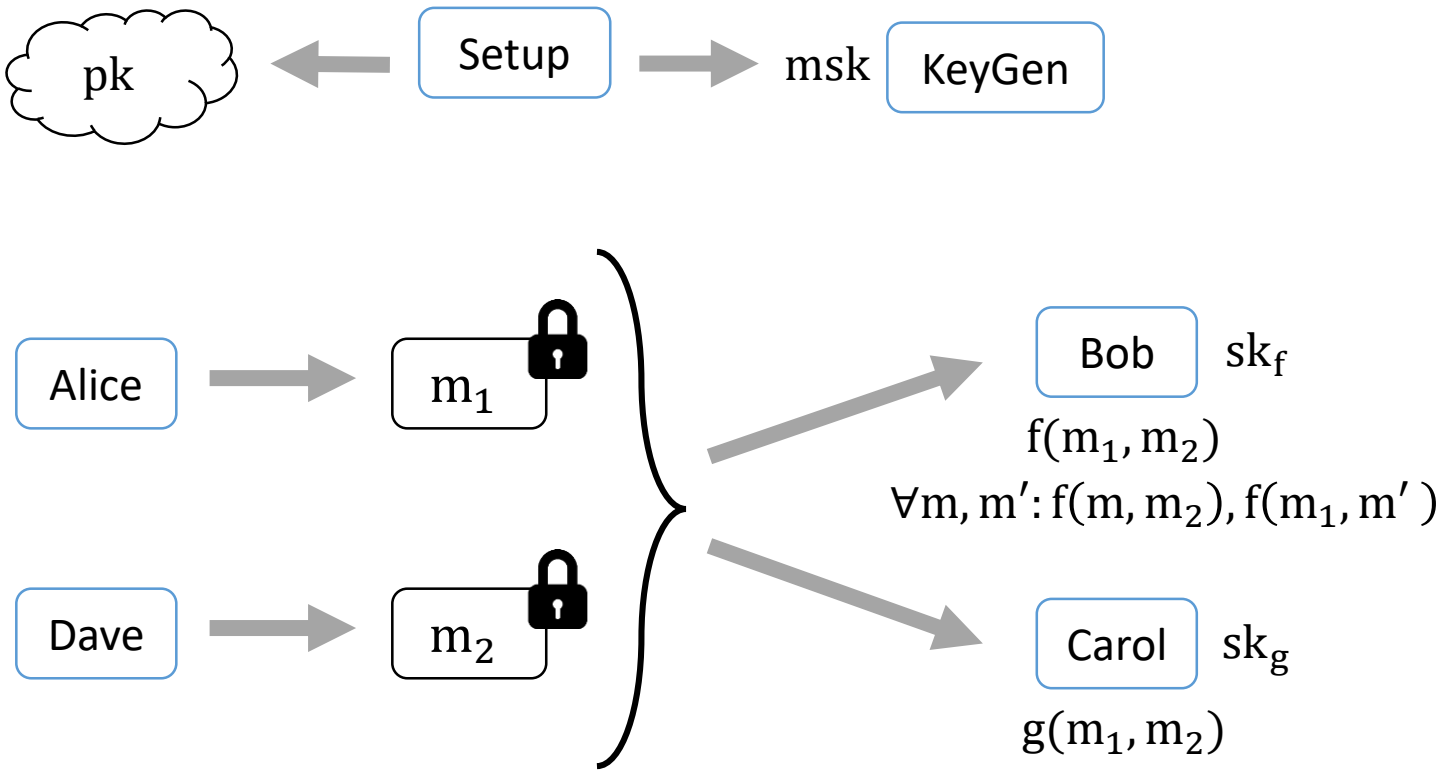
# Multi-input Functional Encryption

[Goldwasser, Gordon, Goyal, Jain, Katz, Liu, Sahai, Shi, Zhou 14]



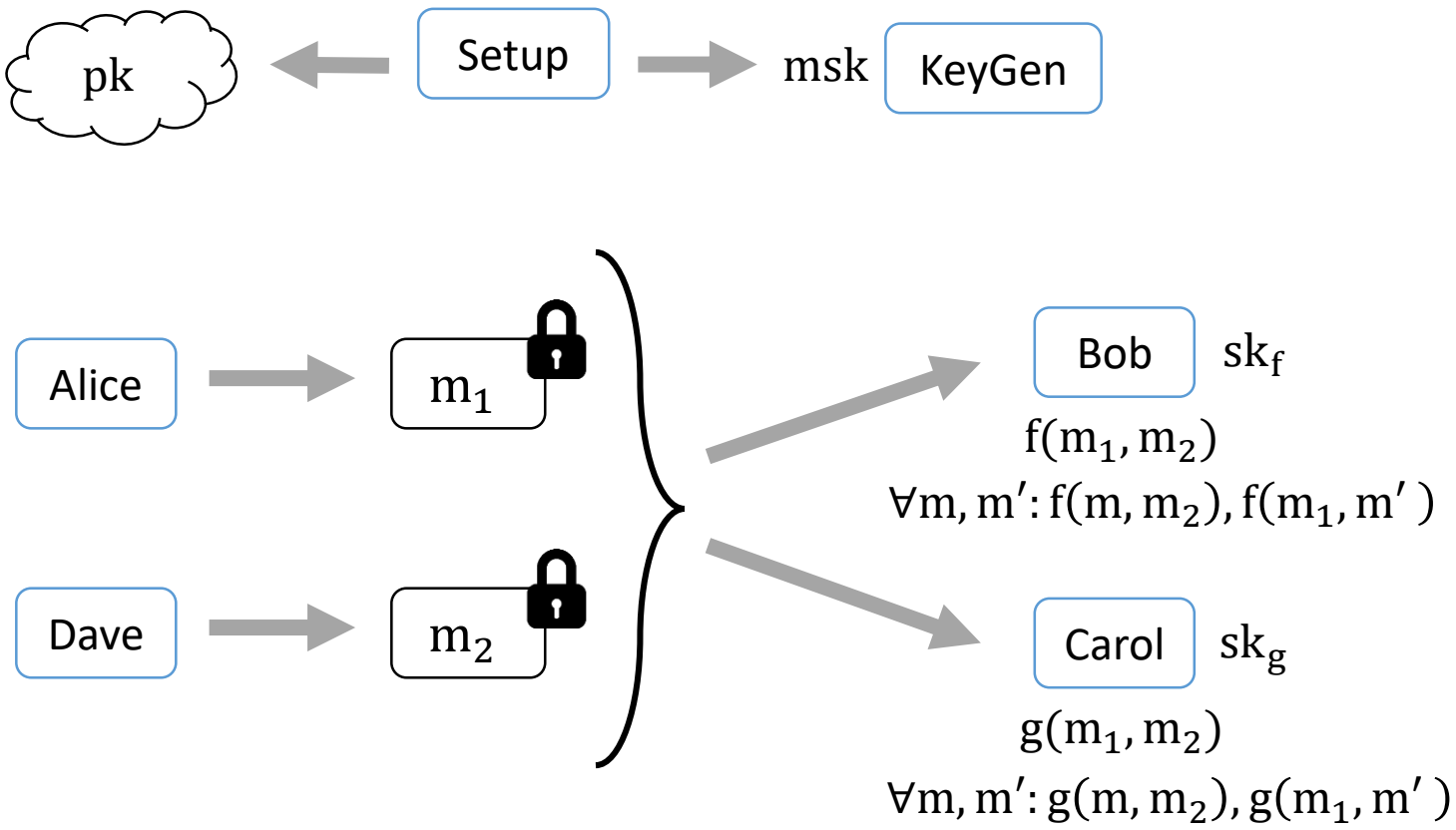
# Multi-input Functional Encryption

[Goldwasser, Gordon, Goyal, Jain, Katz, Liu, Sahai, Shi, Zhou 14]



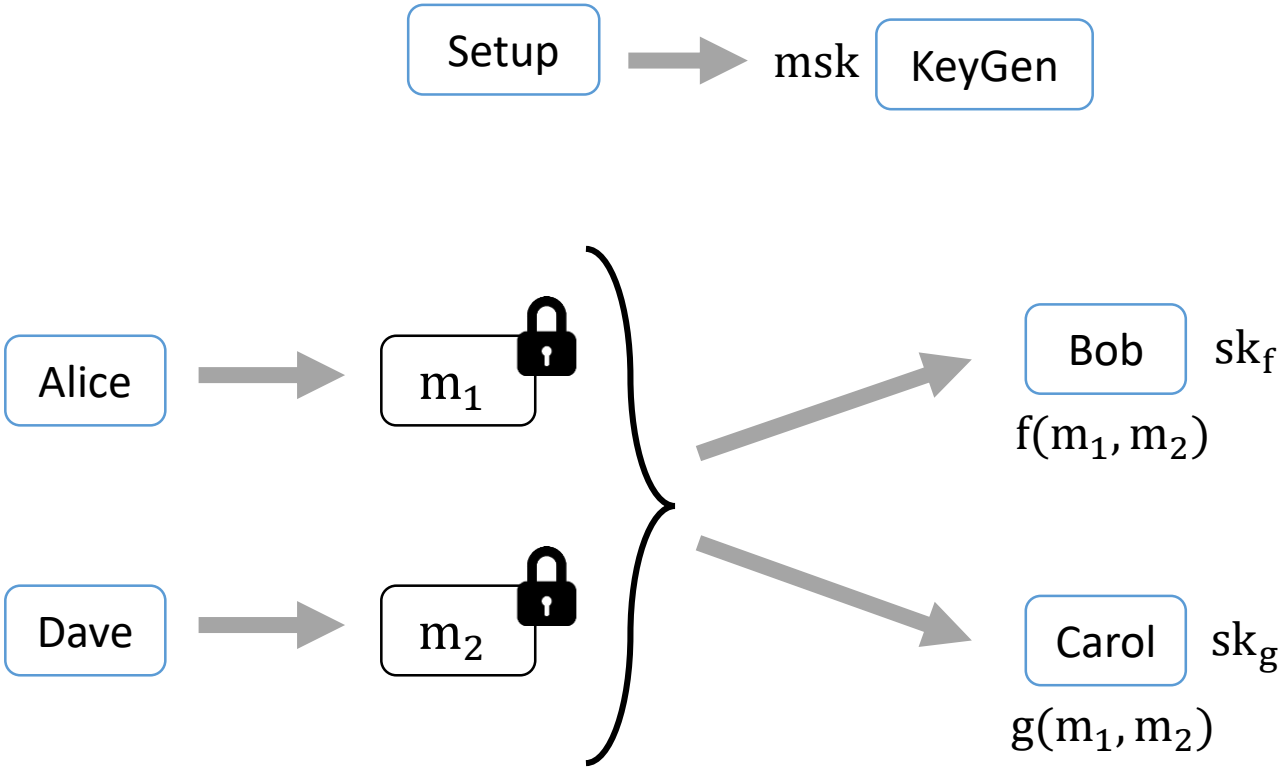
# Multi-input Functional Encryption

[Goldwasser, Gordon, Goyal, Jain, Katz, Liu, Sahai, Shi, Zhou 14]



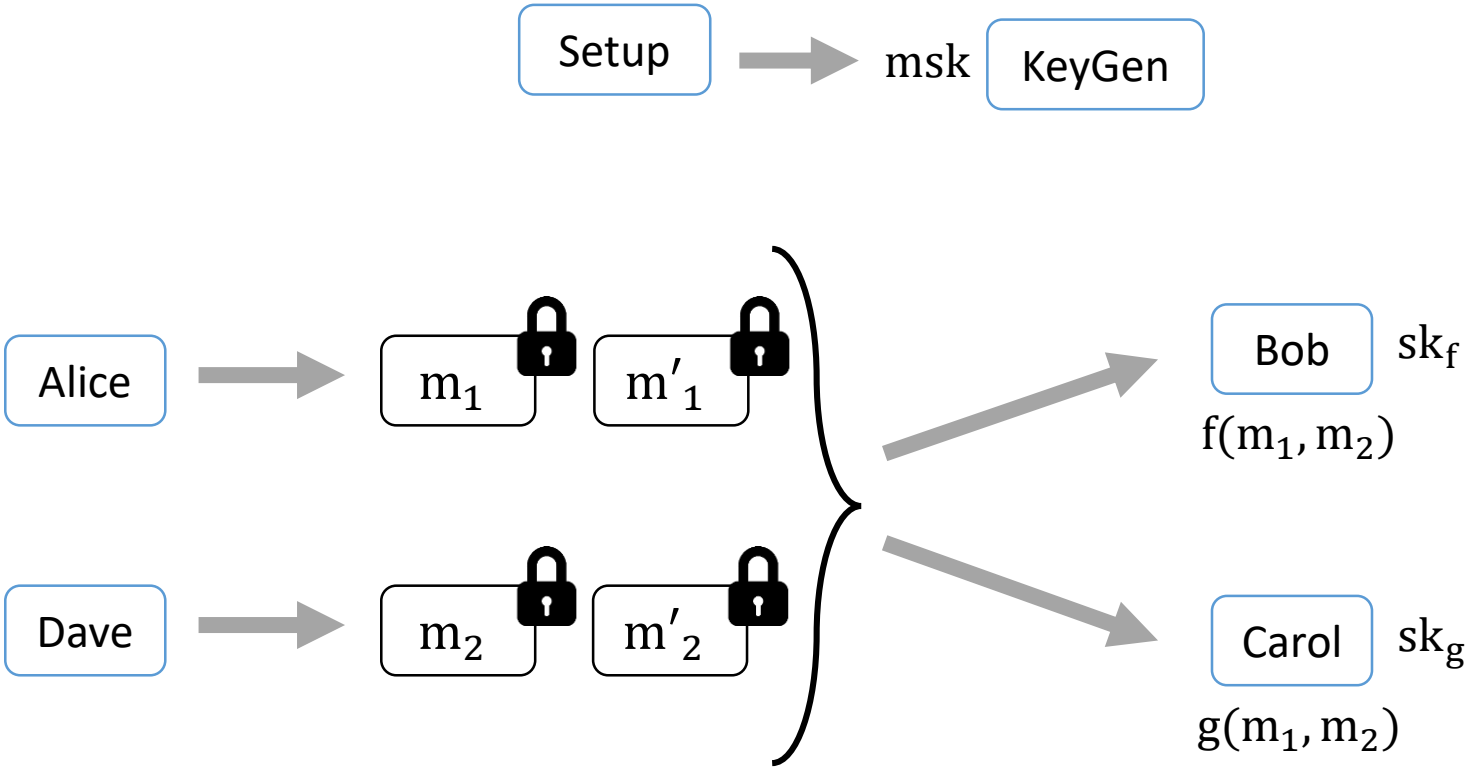
# Multi-input Functional Encryption

[Goldwasser, Gordon, Goyal, Jain, Katz, Liu, Sahai, Shi, Zhou 14]



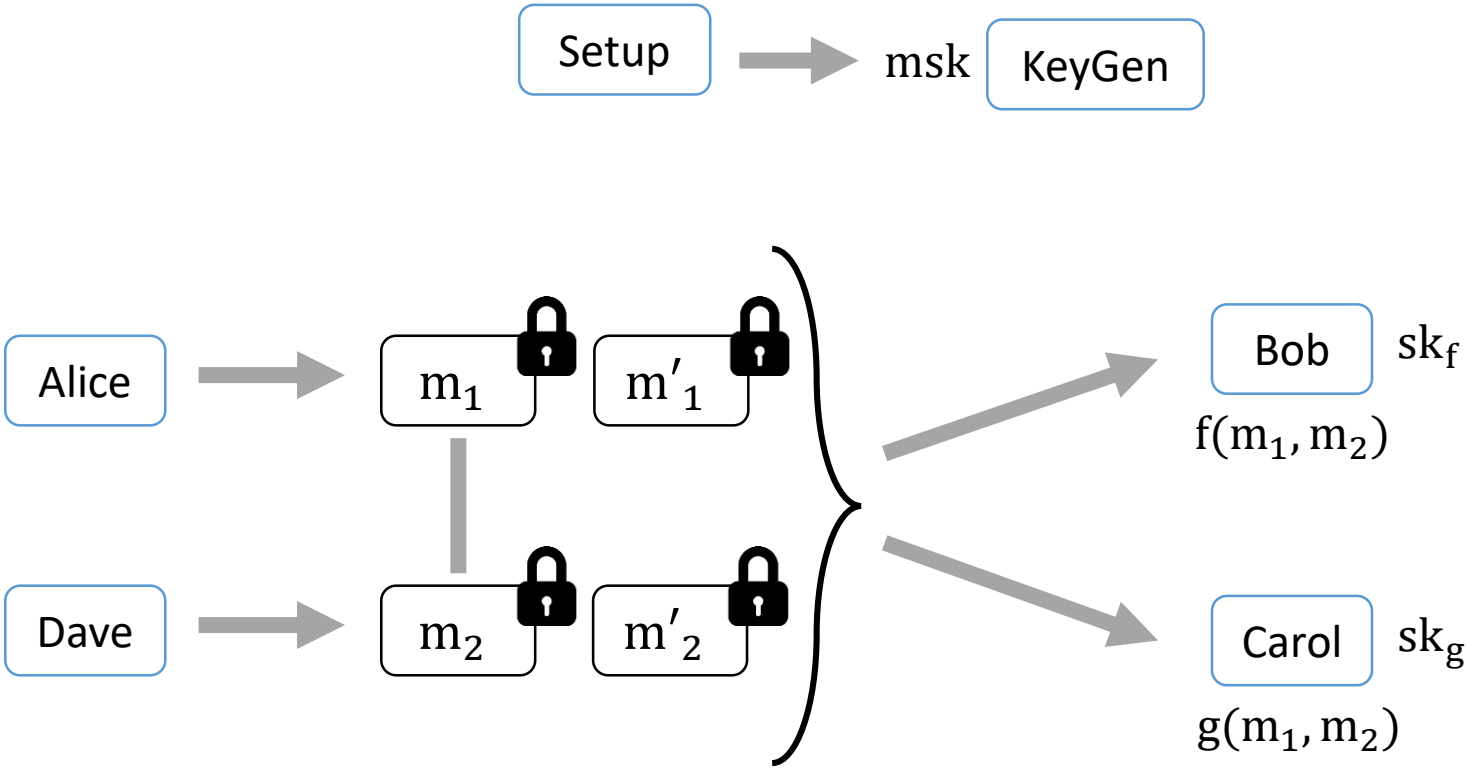
# Multi-input Functional Encryption

[Goldwasser, Gordon, Goyal, Jain, Katz, Liu, Sahai, Shi, Zhou 14]



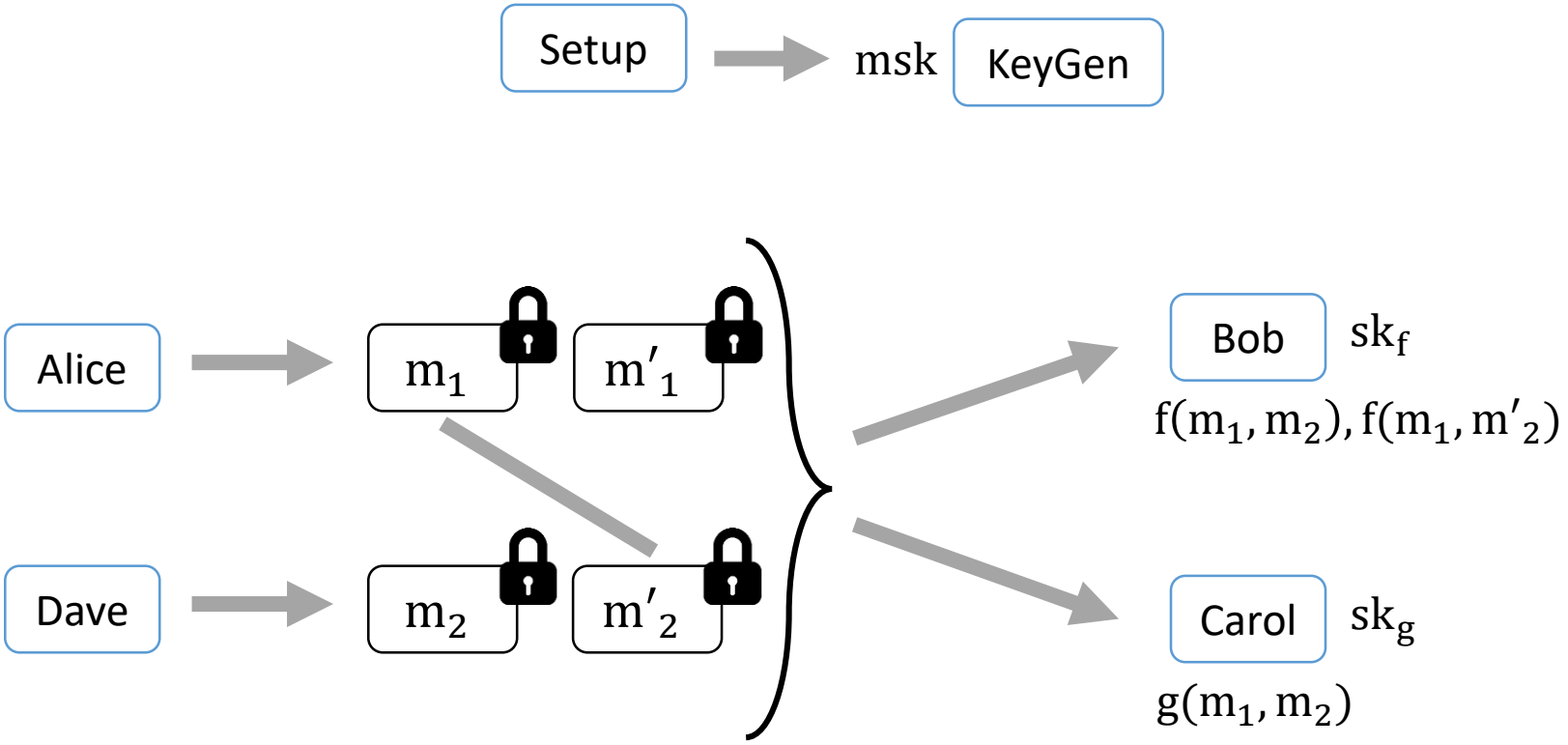
# Multi-input Functional Encryption

[Goldwasser, Gordon, Goyal, Jain, Katz, Liu, Sahai, Shi, Zhou 14]



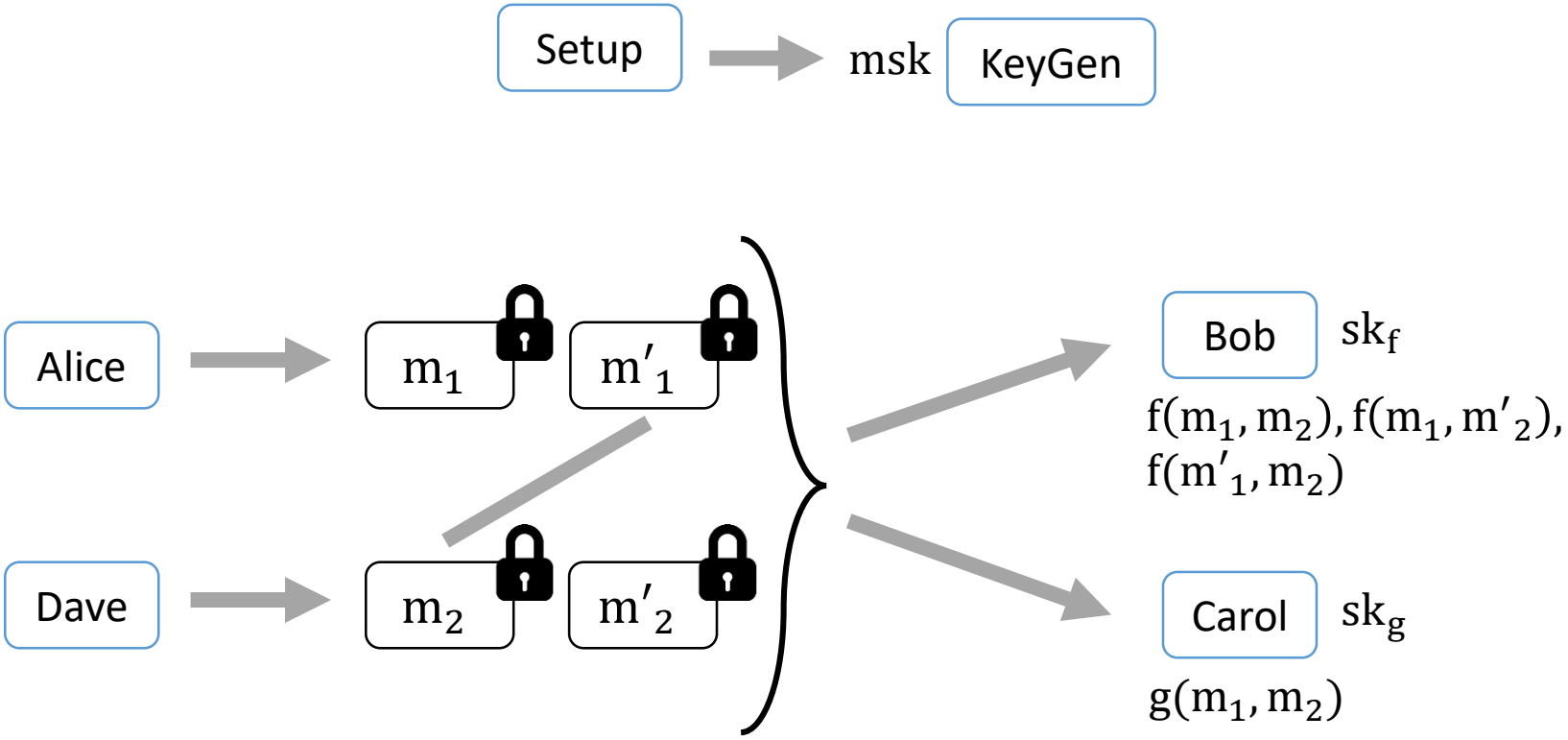
# Multi-input Functional Encryption

[Goldwasser, Gordon, Goyal, Jain, Katz, Liu, Sahai, Shi, Zhou 14]



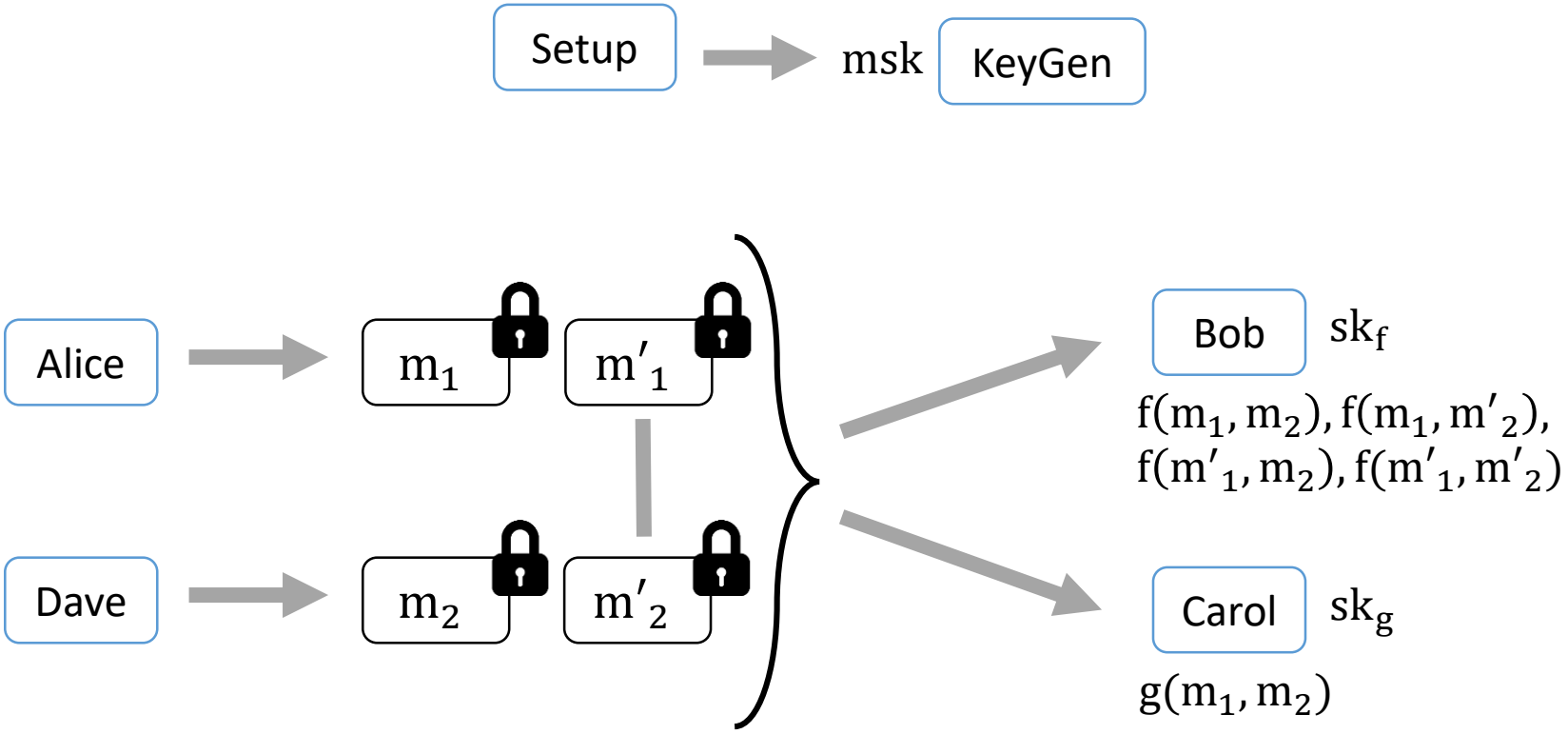
# Multi-input Functional Encryption

[Goldwasser, Gordon, Goyal, Jain, Katz, Liu, Sahai, Shi, Zhou 14]



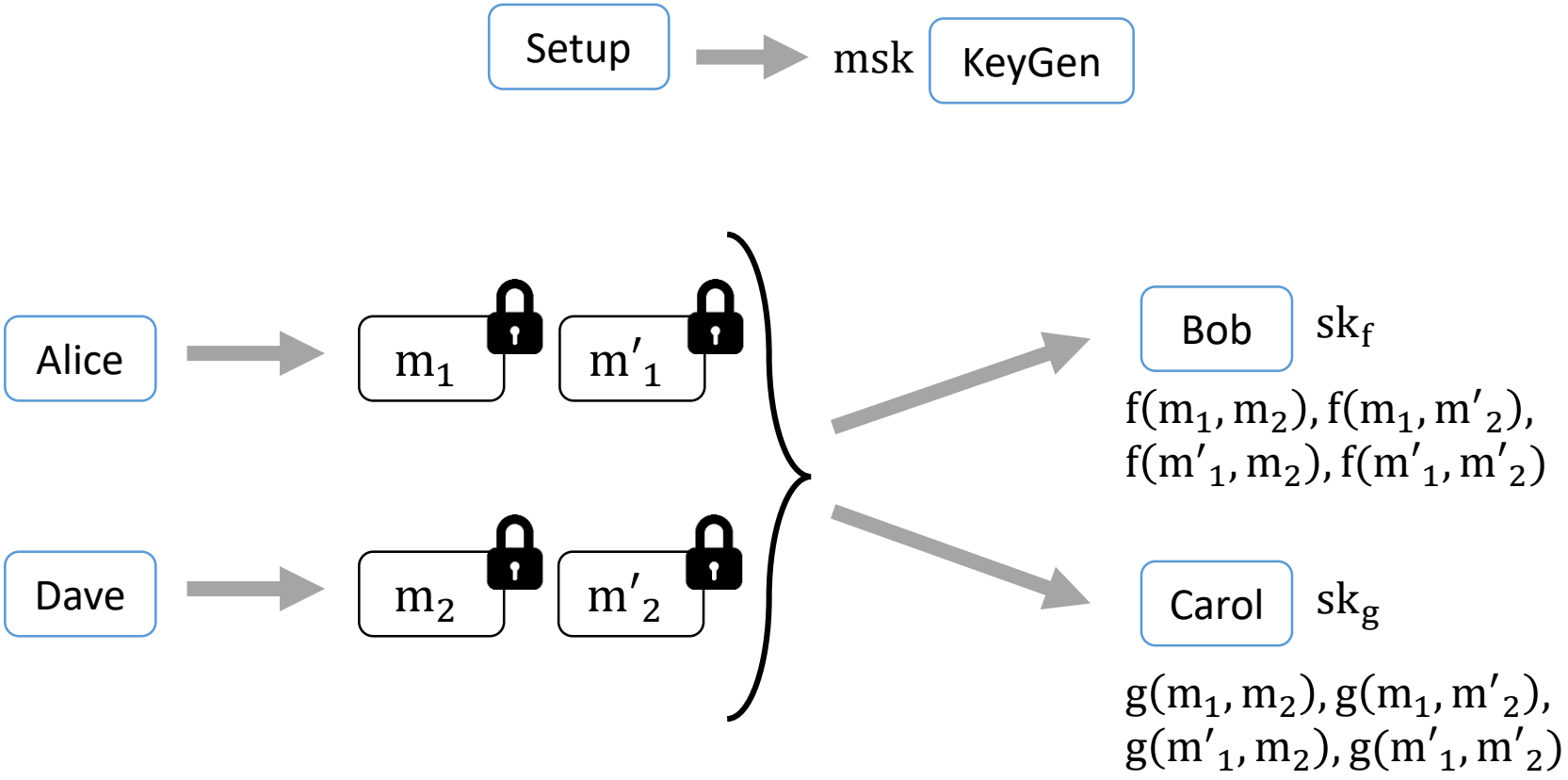
# Multi-input Functional Encryption

[Goldwasser, Gordon, Goyal, Jain, Katz, Liu, Sahai, Shi, Zhou 14]



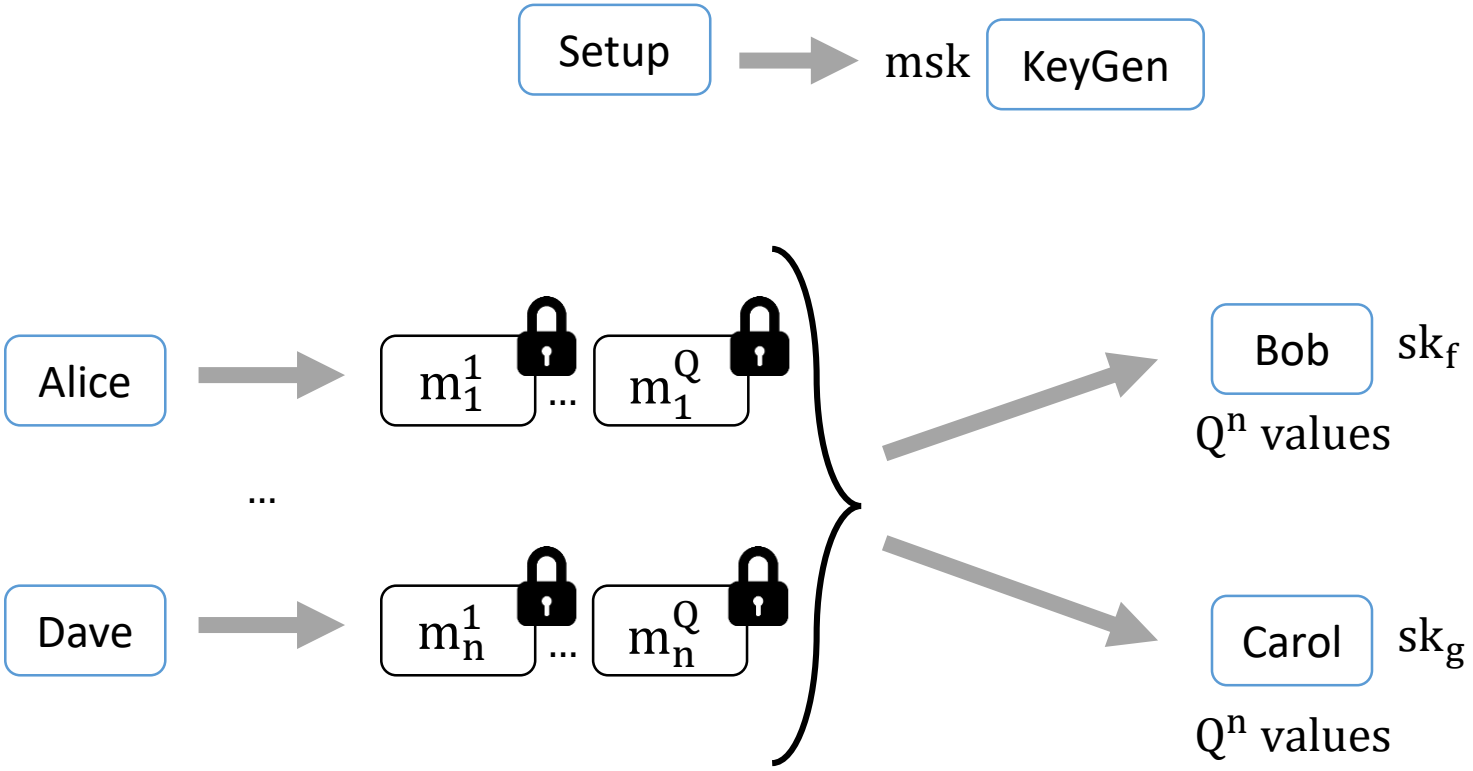
# Multi-input Functional Encryption

[Goldwasser, Gordon, Goyal, Jain, Katz, Liu, Sahai, Shi, Zhou 14]



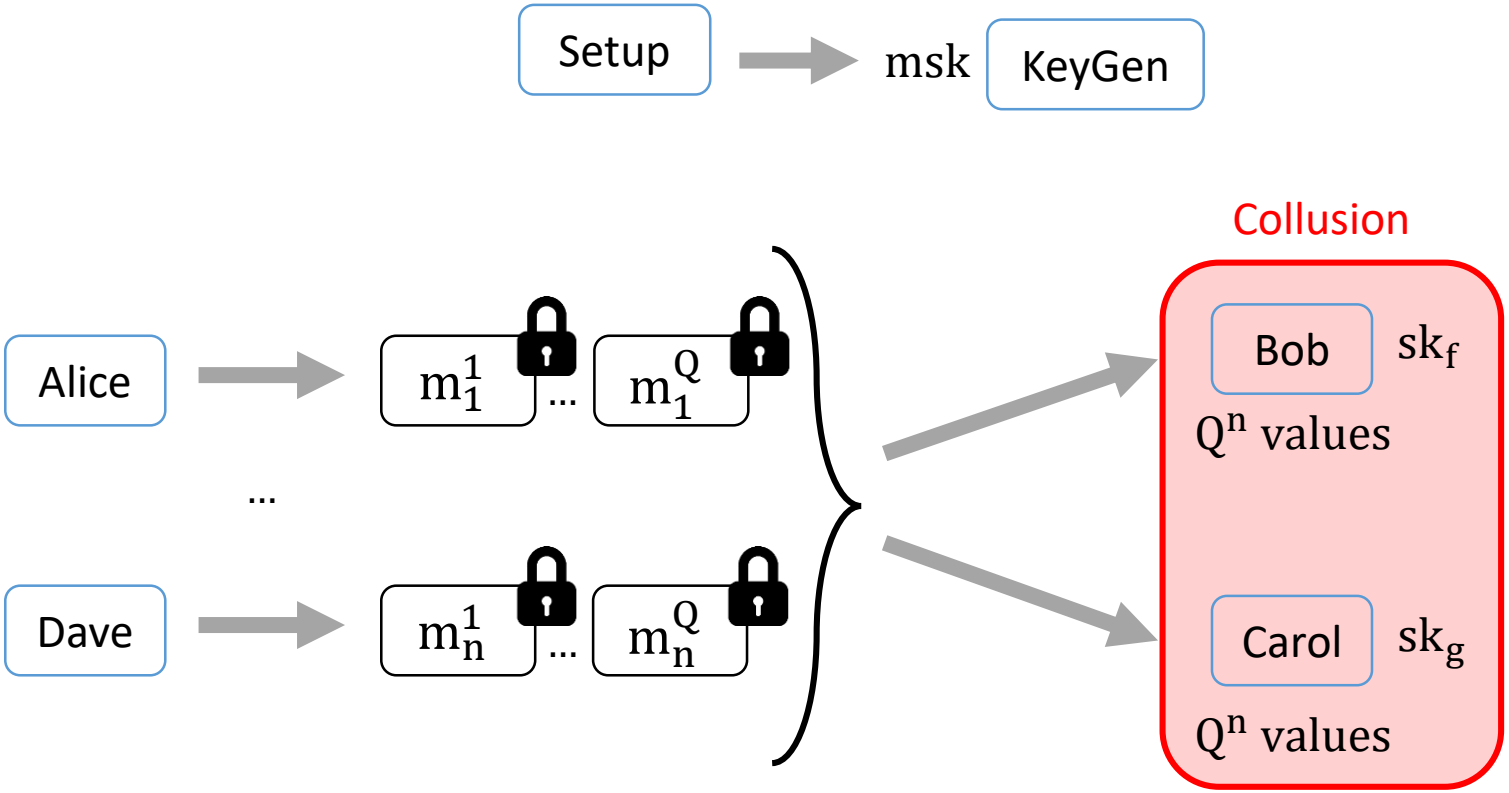
# Multi-input Functional Encryption

[Goldwasser, Gordon, Goyal, Jain, Katz, Liu, Sahai, Shi, Zhou 14]



# Multi-input Functional Encryption

[Goldwasser, Gordon, Goyal, Jain, Katz, Liu, Sahai, Shi, Zhou 14]

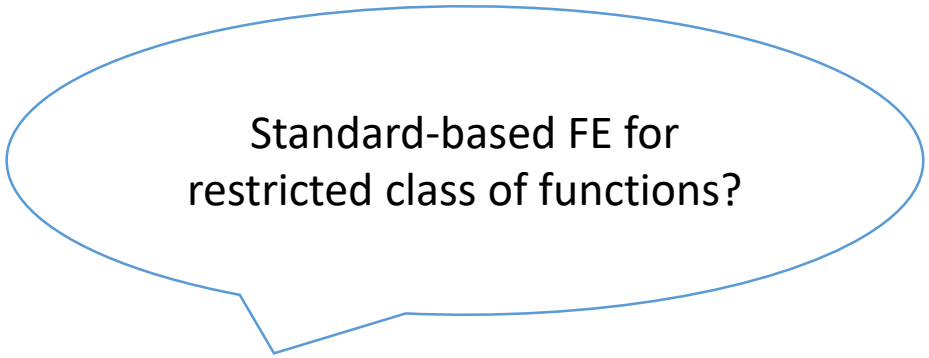


# Prior works

| Construction: | Functions: | Assumption: | # slots: |
|---|---|---|---|
| [BLRSZZ 14, GGGJKLSSZ 14, AJ 15, BGJS 15, BKS 16,KS 17] | any circuit | Non standard | Poly, unbounded |

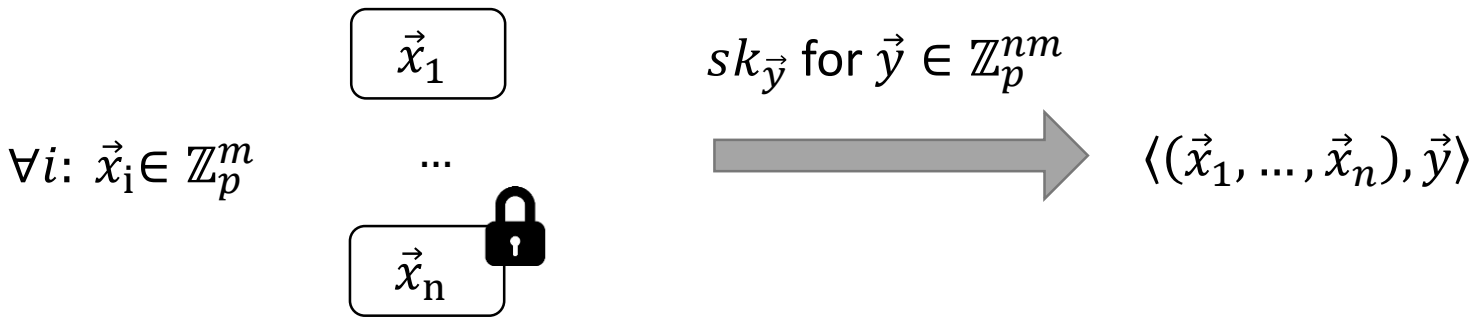
# Prior works

| Construction: | Functions: | Assumption: | # slots: |
|---|---|---|---|
| [BLRSZZ 14, GGGJKLSSZ 14, AJ 15, BGJS 15, BKS 16,KS 17] | any circuit | Non standard | Poly, unbounded |



# Prior works

| Construction: | Functions: | Assumption: | # slots: |
|---|---|---|---|
| [BLRSZZ 14, GGGJKLSSZ 14, AJ 15, BGJS 15, BKS 16,KS 17] | any circuit | Non standard | Poly, unbounded |
| Ours | Inner Product | 2maps (SXDH) | poly |



# Prior works

| Construction: | Functions: | Assumption: | # slots: |
|---|---|---|---|
| [BLRSZZ 14, GGGJKLSSZ 14, AJ 15, BGJS 15, BKS 16,KS 17] | any circuit | Non standard | Poly, unbounded |
| Ours | Inner Product | 2maps (SXDH) | poly |
| [ABDP 15, ALS 15, ABDP 16] | Inner Product | 1maps (DDH) | 1 |

# Concurrent works

| Construction: | Functions: | Assumption: | # slots: |
|---|---|---|---|
| [BLRSZZ 14, GGGJKLSSZ 14, AJ 15, BGJS 15, BKS 16,KS 17] | any circuit | Non standard | Poly, unbounded |
| Ours | Inner Product | 2maps (SXDH) | poly |
| [ABDP 15, ALS 15, ABDP 16] | Inner Product | 1maps (DDH) | 1 |
| [LL 16] | Inner Product | 2maps (SXDH & 3DH) | 2 |

# Our construction

**Single-input Inner Product FE**

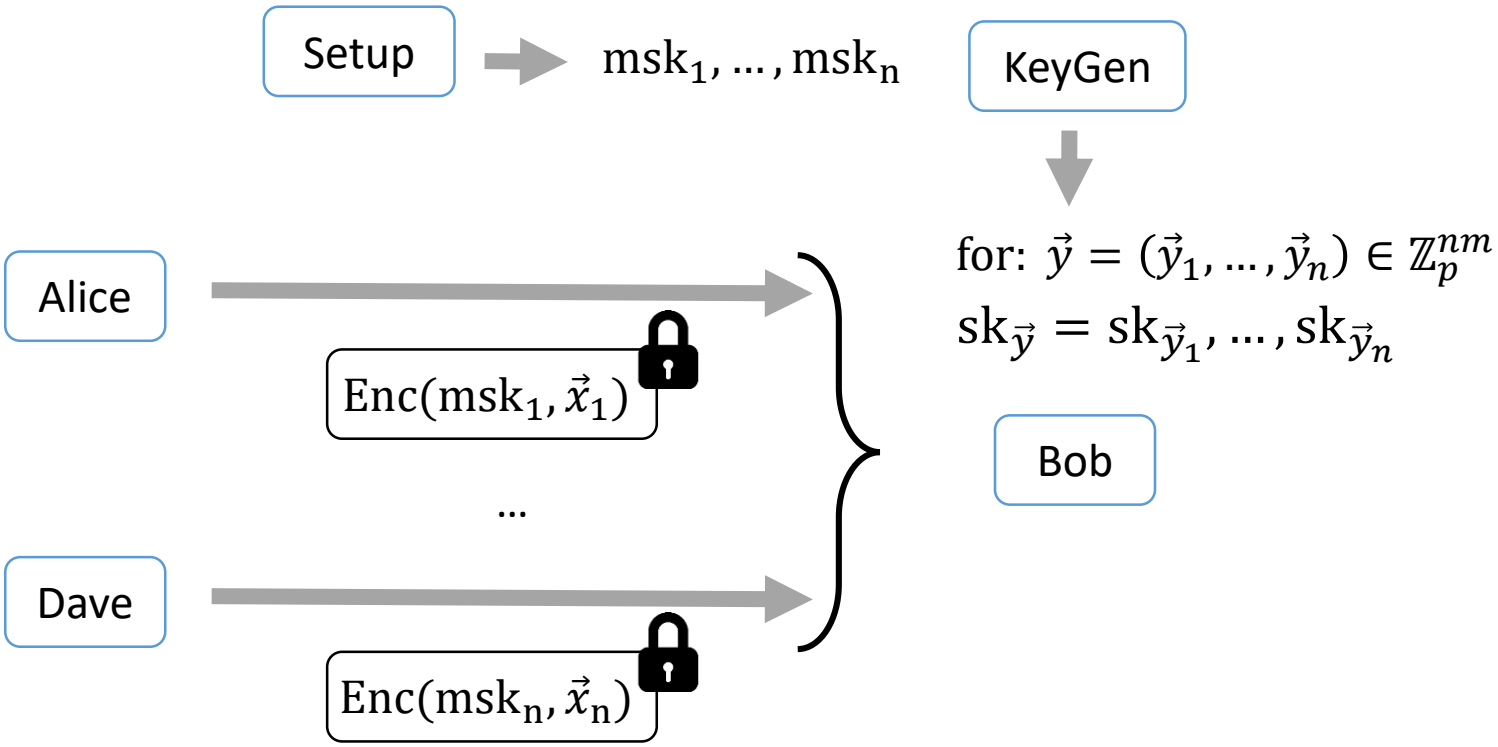
**Multi-input Inner Product FE**

1 Generic, naive

2 [Agrawal, Libert, Stehlé] single input FE

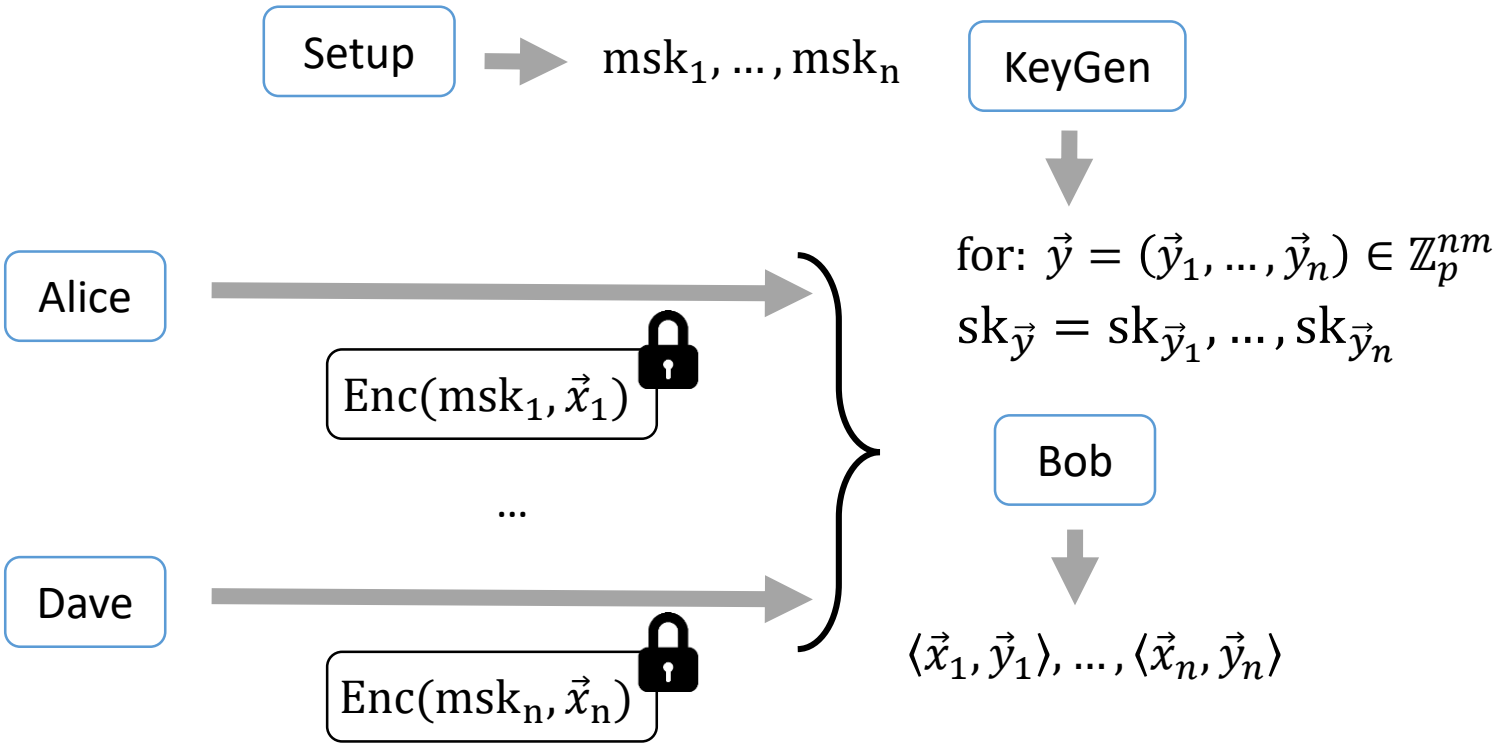
# Multi-input Functional Encryption

Naive Attempt



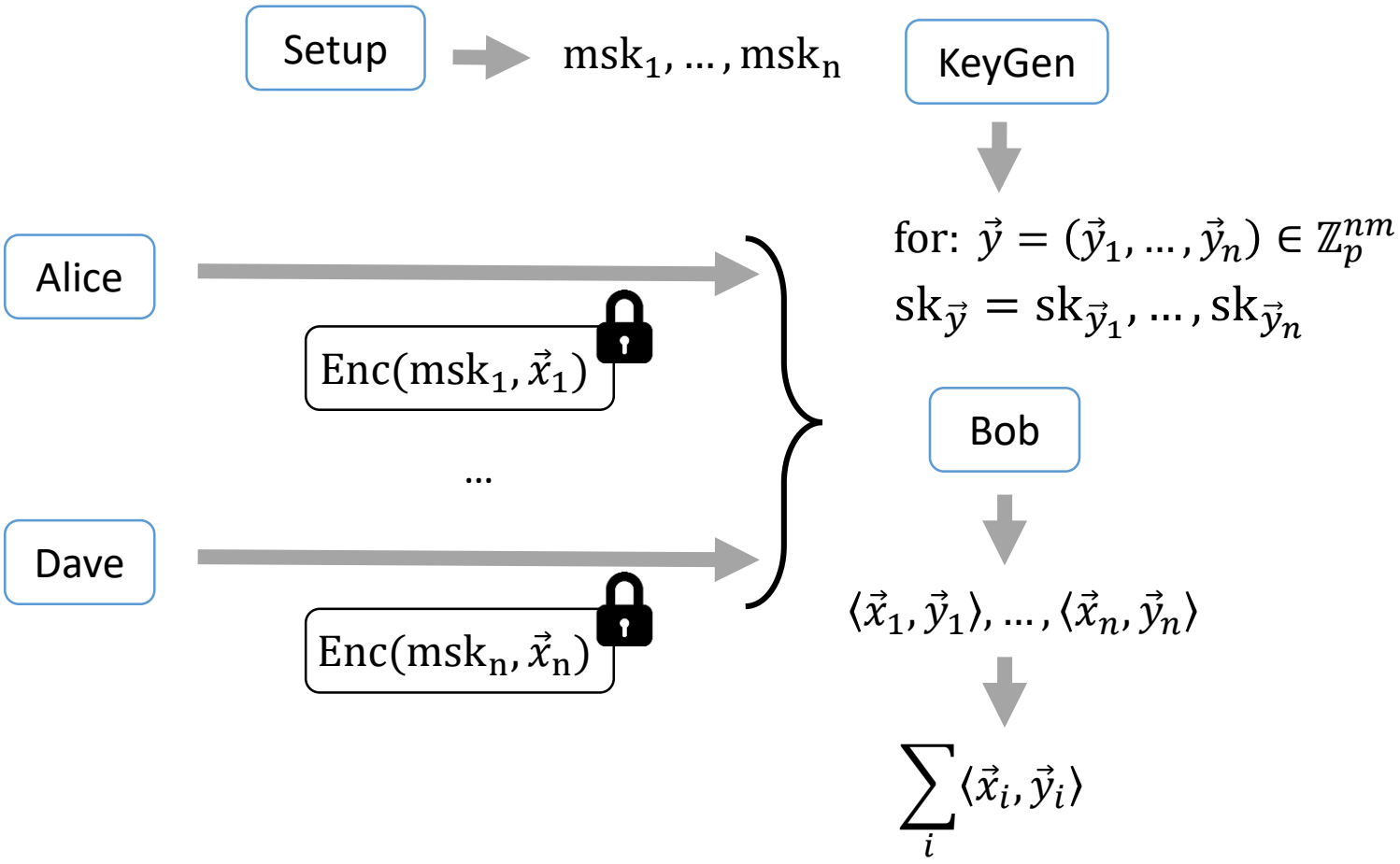
# Multi-input Functional Encryption

Naive Attempt



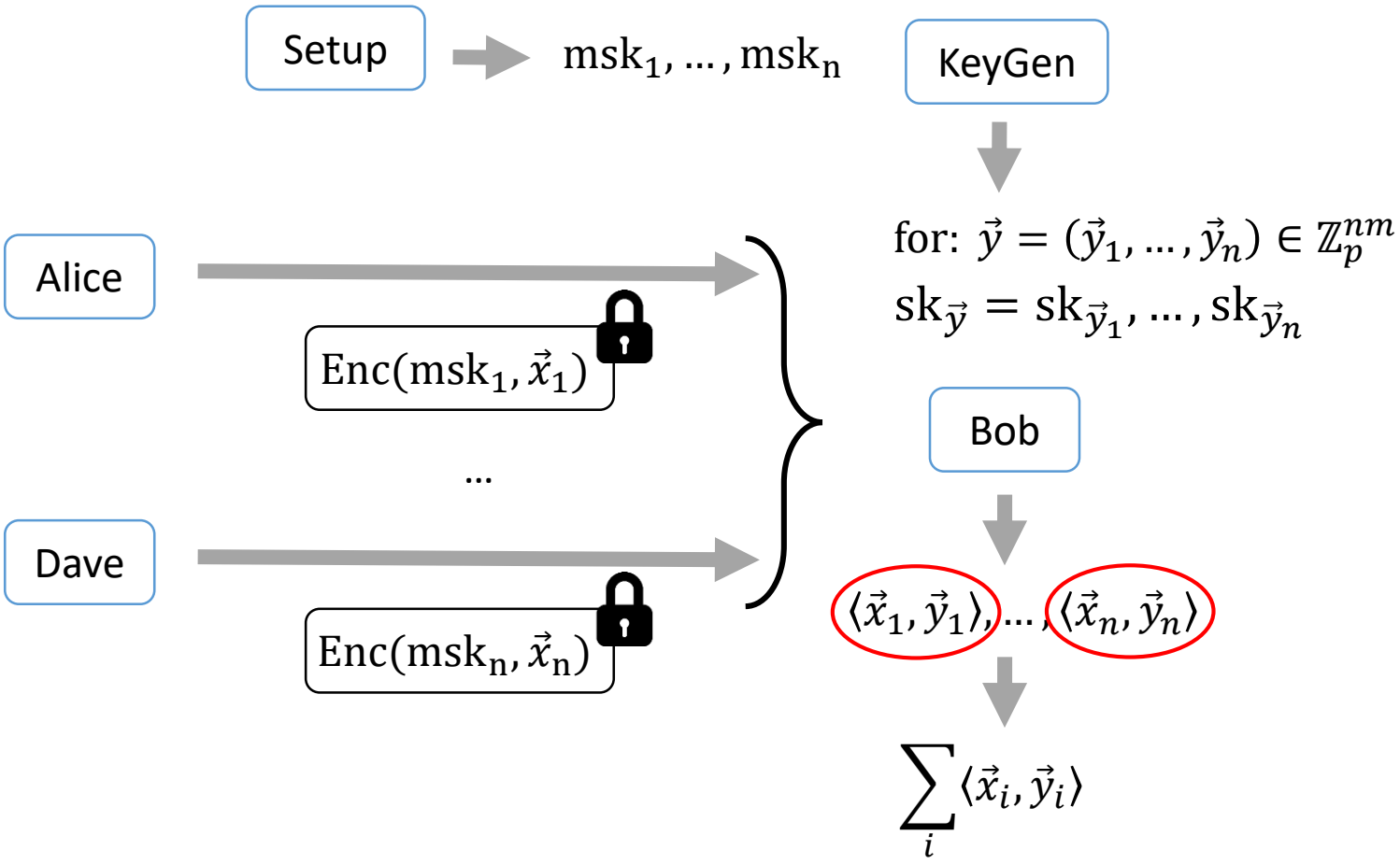
# Multi-input Functional Encryption

Naive Attempt

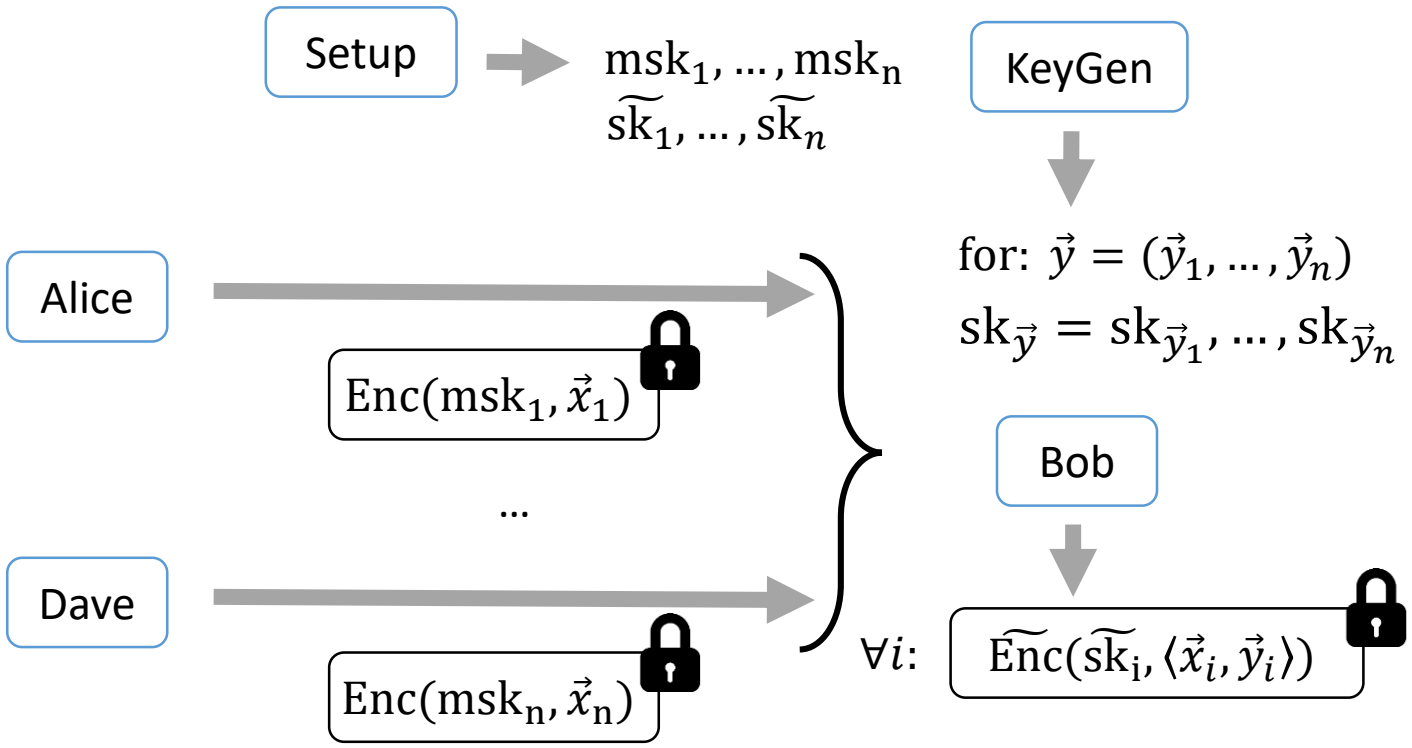


# Multi-input Functional Encryption

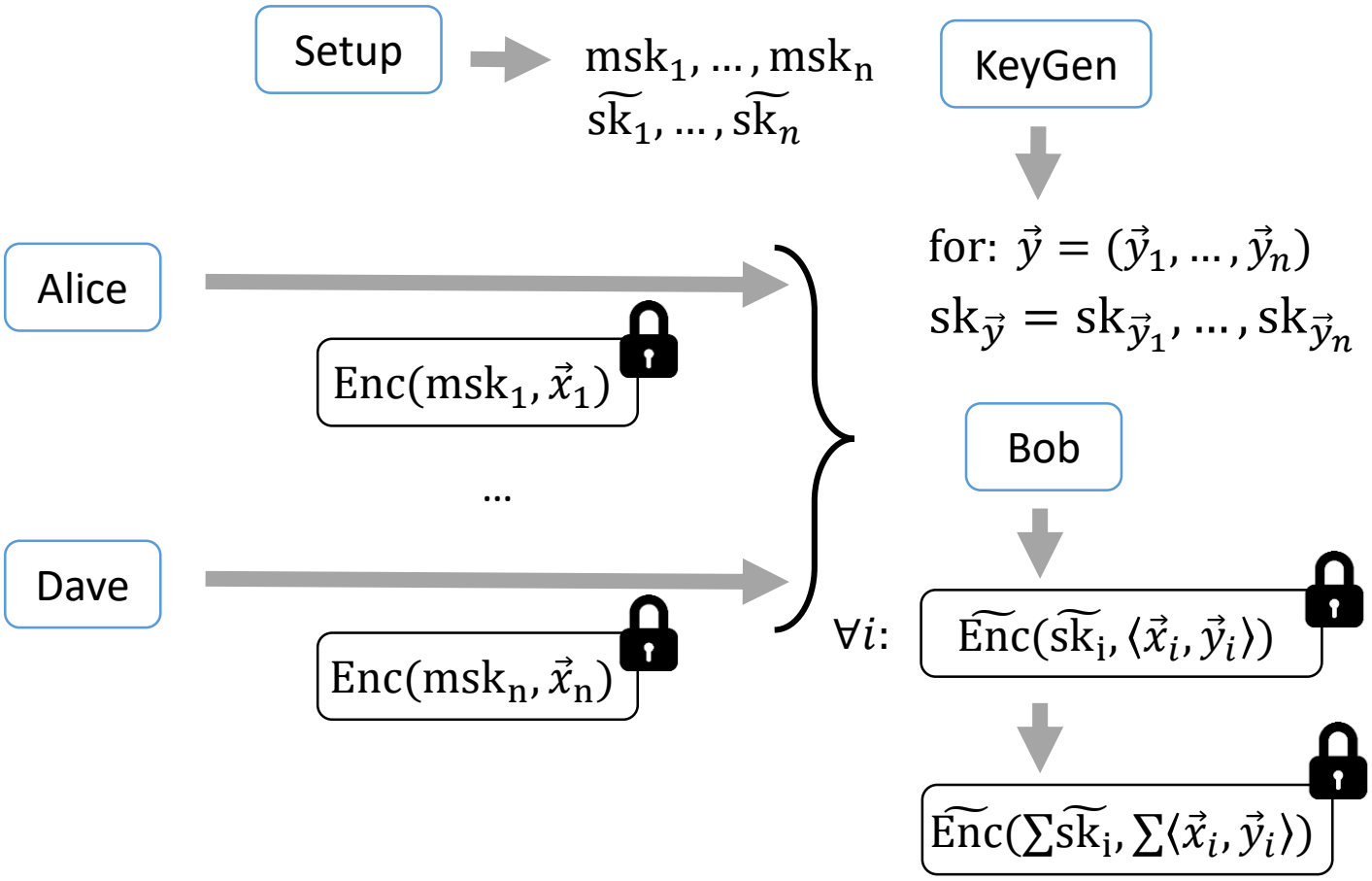
Naive Attempt



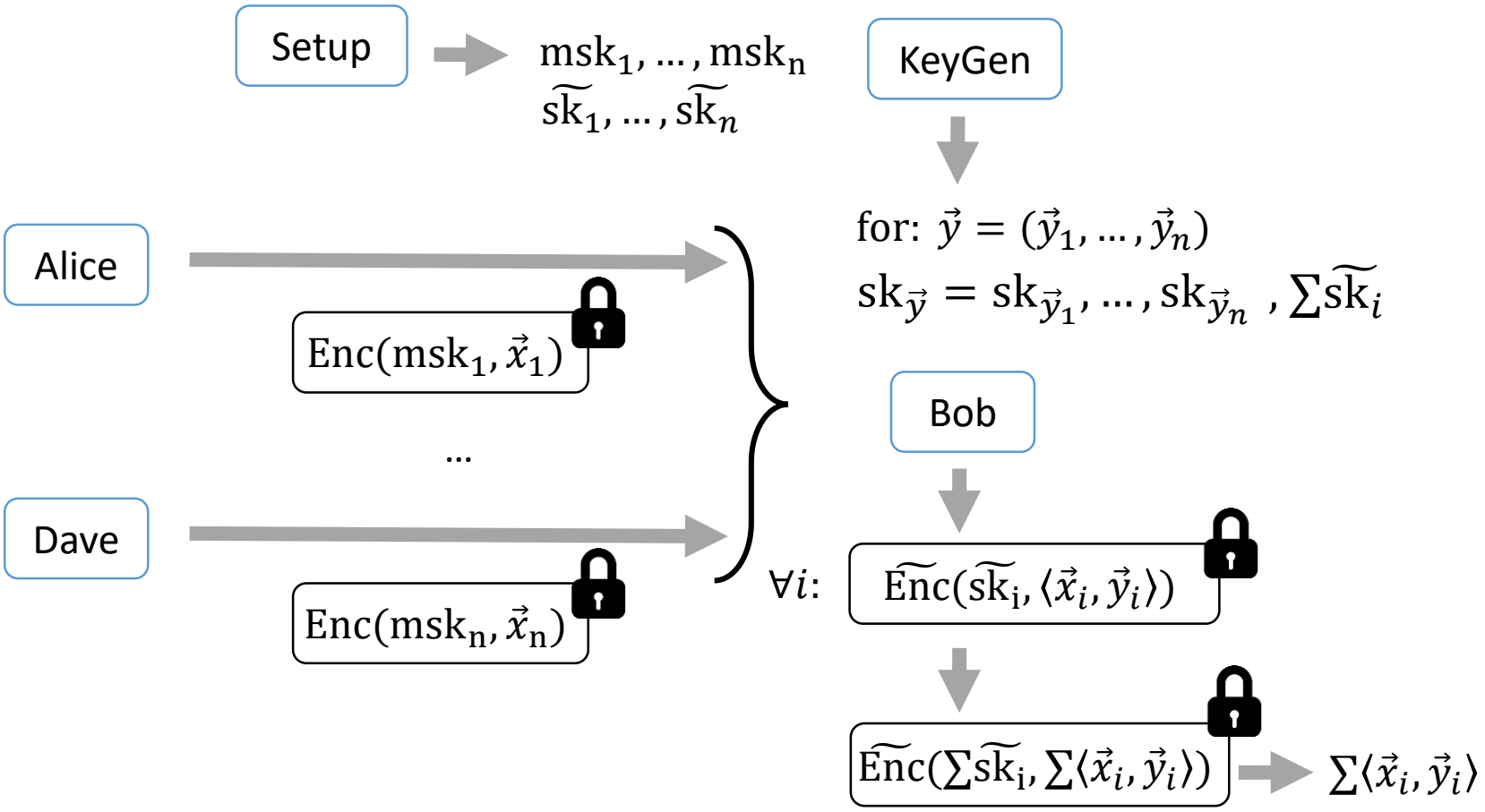
# Multi-input Functional Encryption



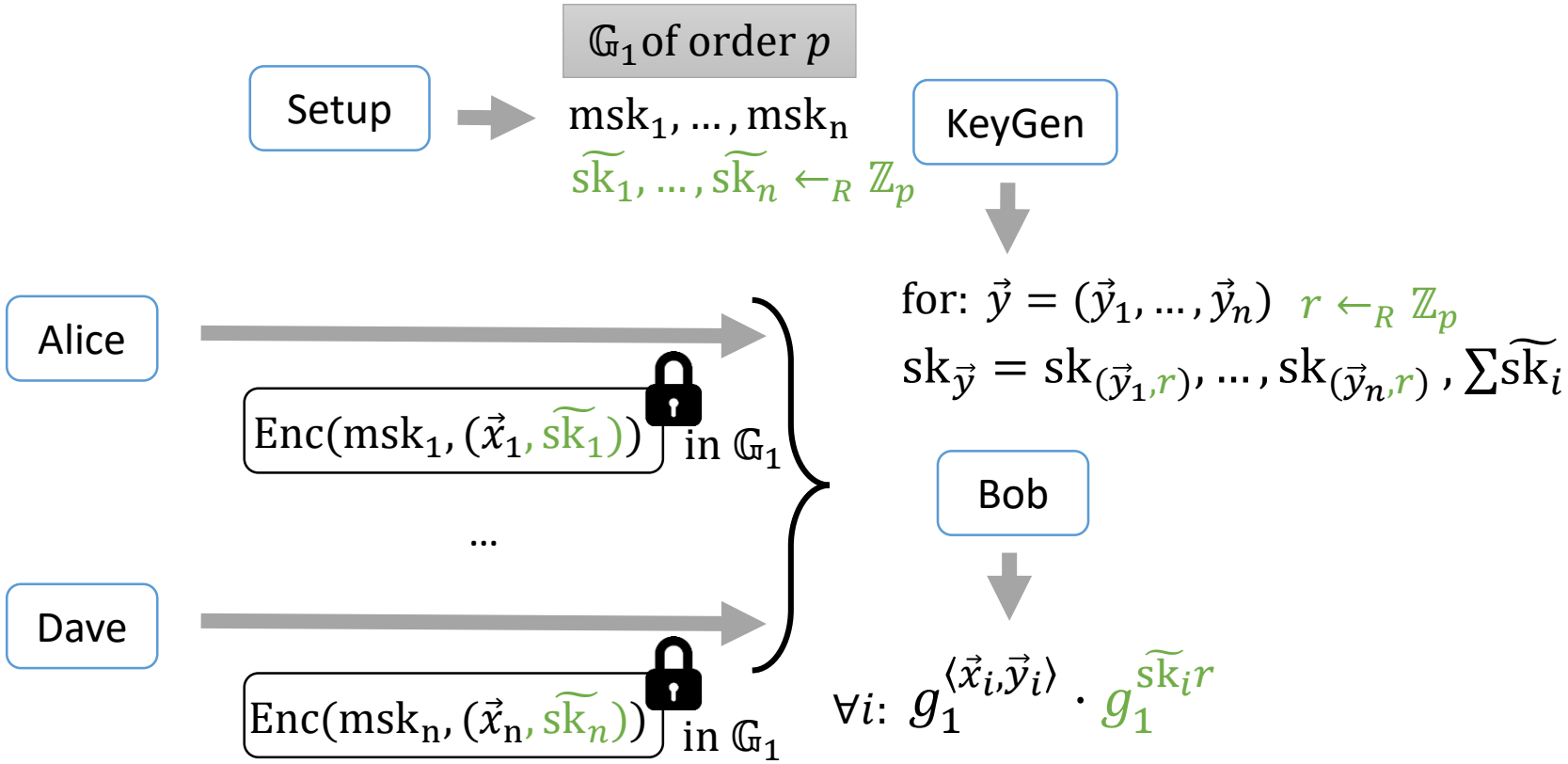
# Multi-input Functional Encryption



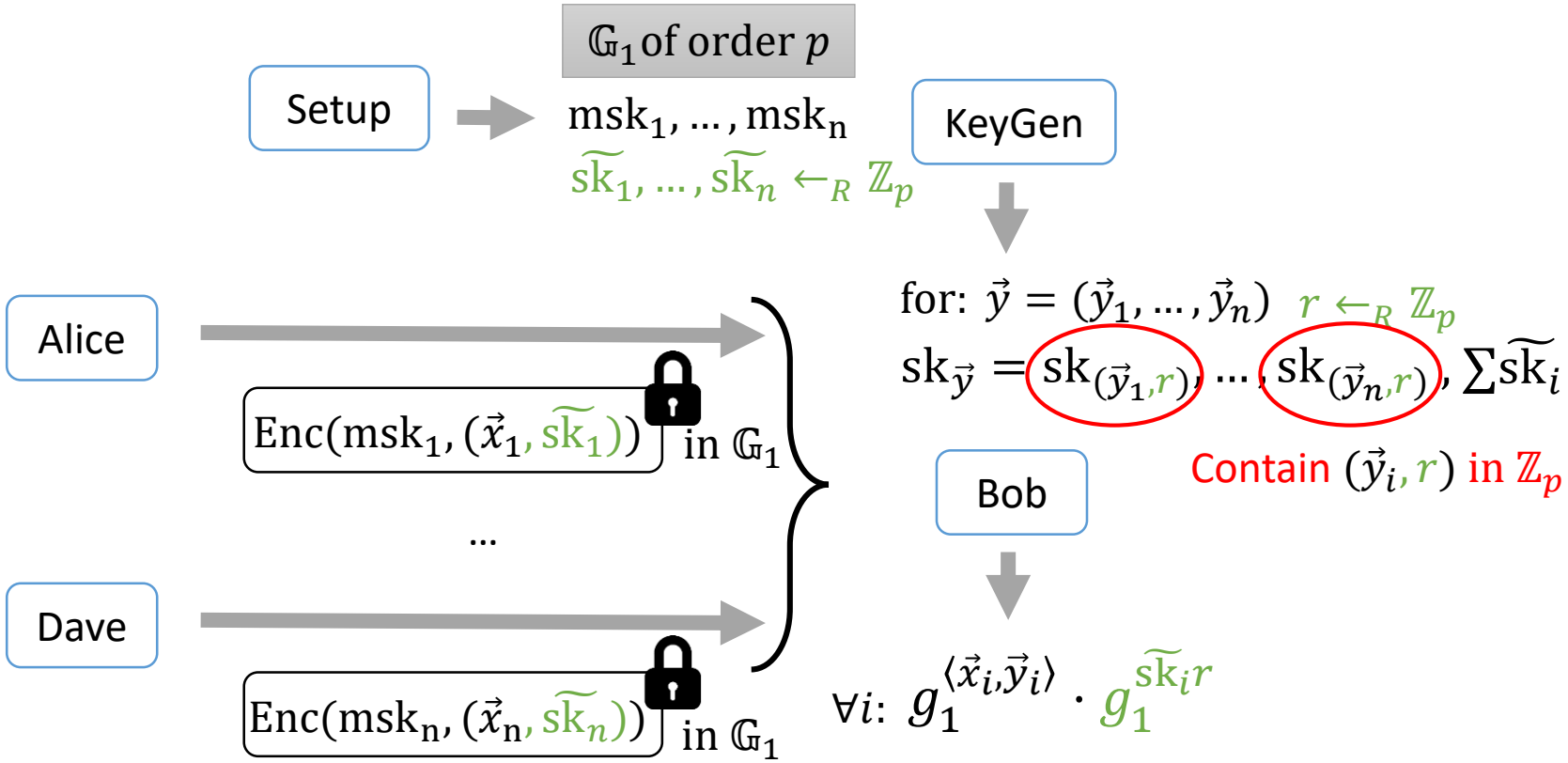
# Multi-input Functional Encryption



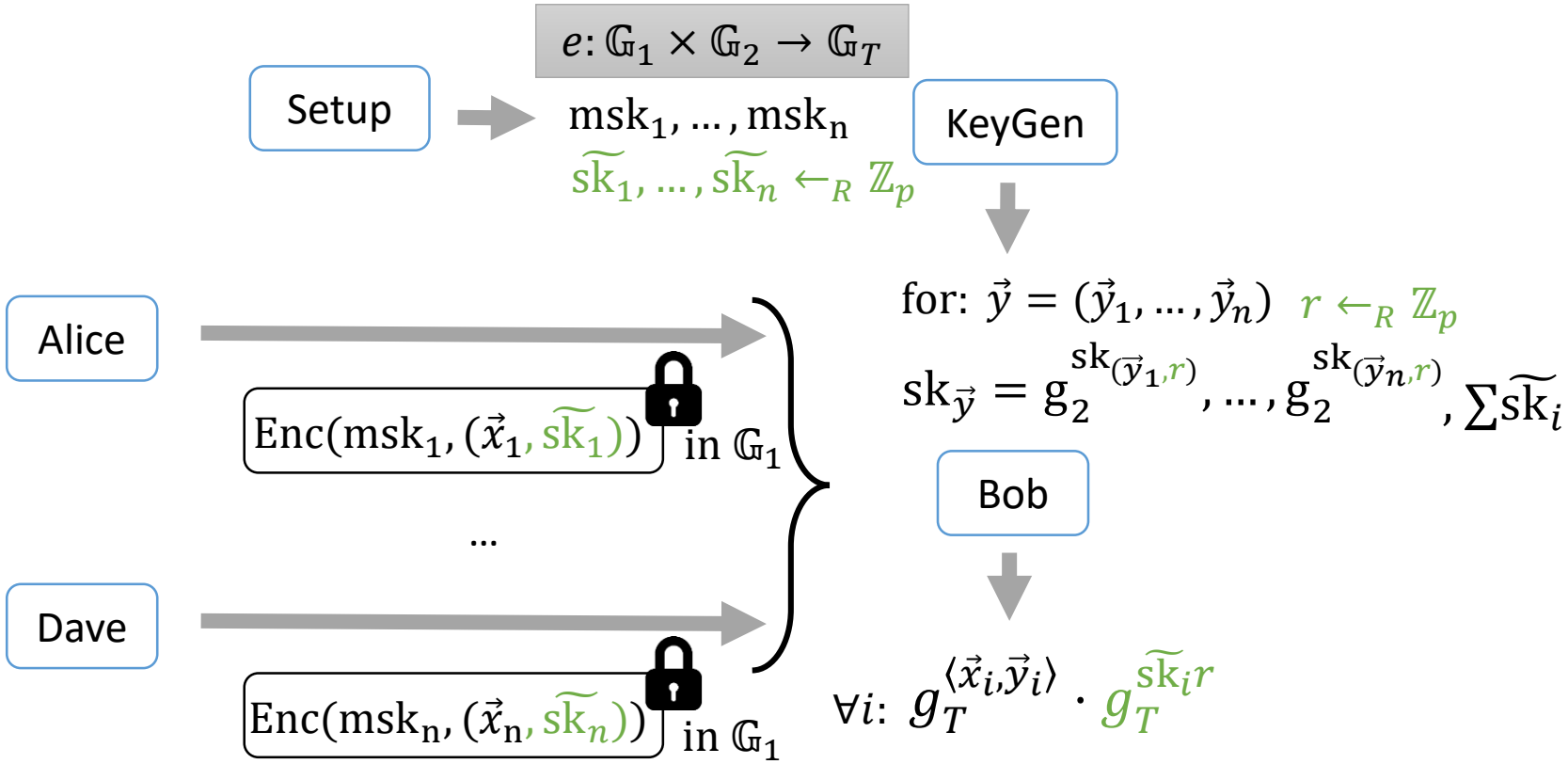
# Multi-input Functional Encryption



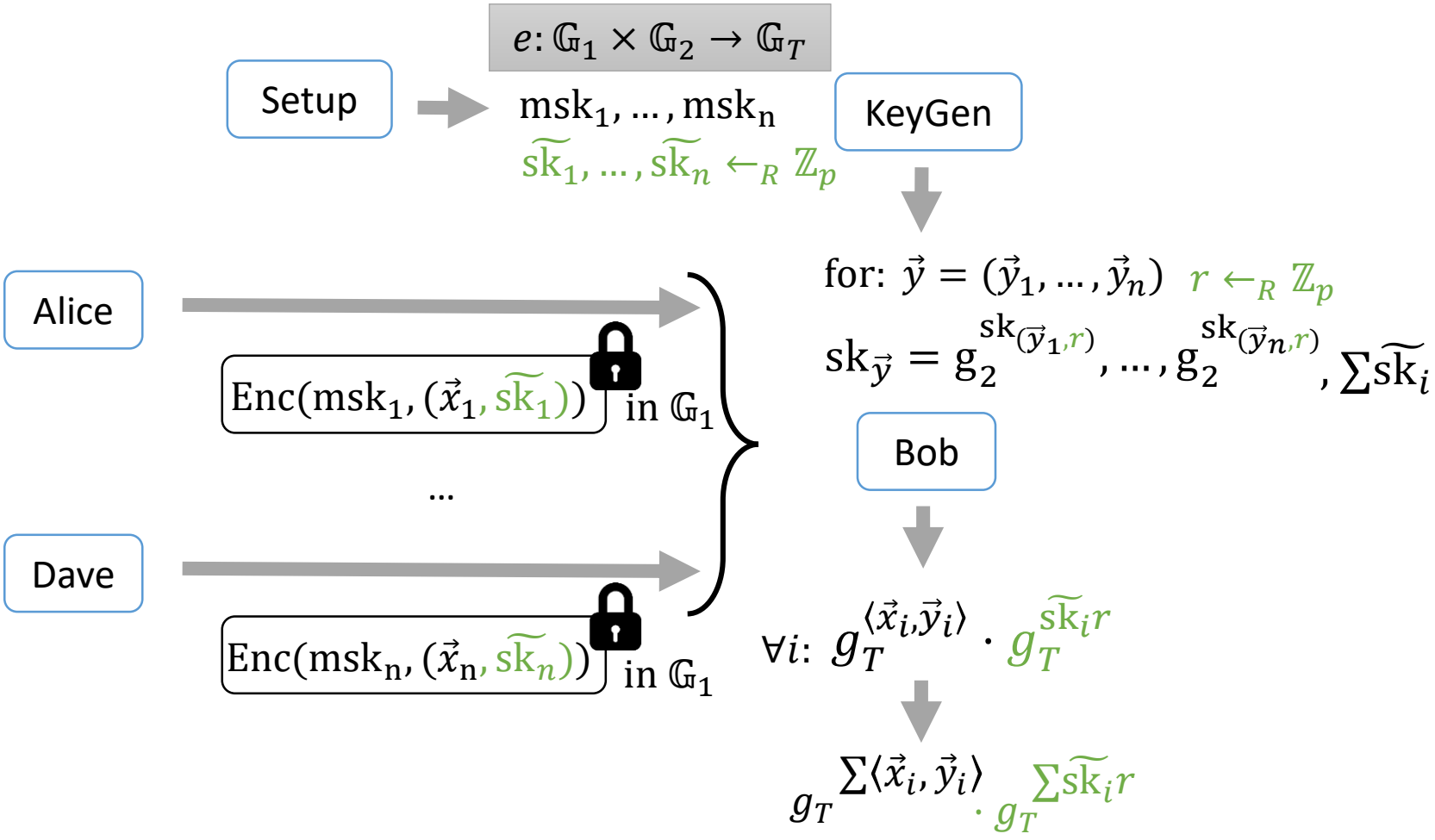
# Multi-input Functional Encryption



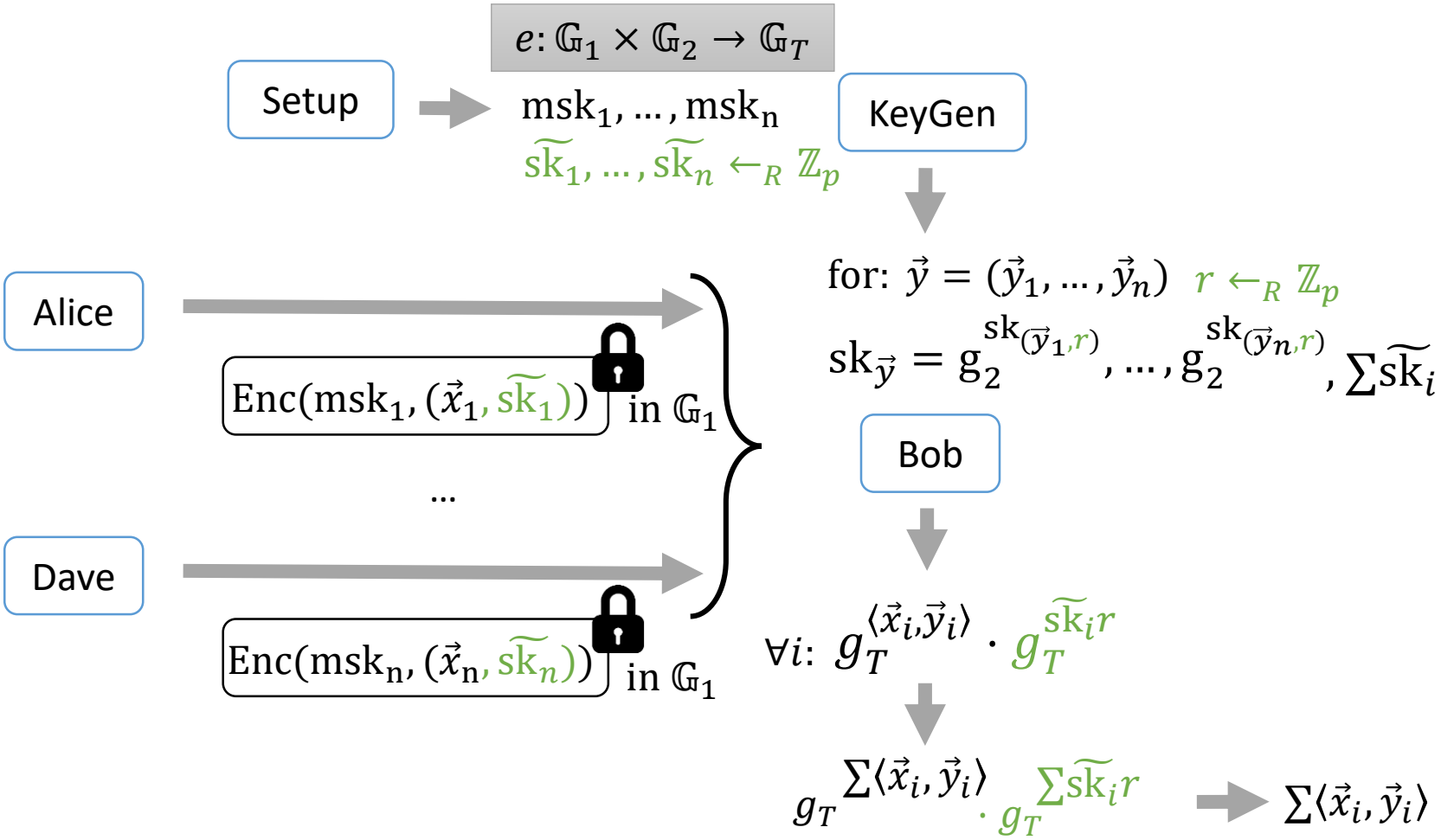
# Multi-input Functional Encryption



# Multi-input Functional Encryption



# Multi-input Functional Encryption



# Open problems

| Construction: | Functions: | Assumption: | # slots: |
|---|---|---|---|
| [BLRSZZ 14, GGGJKLSSZ 14, AJ 15, BGJS 15, BKS 16,KS 17] | any circuit | Non standard | Poly, unbounded |
| Ours | Inner Product | 2maps (SXDH) | poly |
| [ABDP 15, ALS 15, ABDP 16] | Inner Product | 1maps (DDH) | 1 |
| [LL 16] | Inner Product | 2maps (SXDH & 3DH) | 2 |

# Open problems

| Construction: | Functions: | Assumption: | # slots: |
|---|---|---|---|
| [BLRSZZ 14, GGGJKLSSZ 14, AJ 15, BGJS 15, BKS 16,KS 17] | any circuit | Non standard | Poly, unbounded |
| Ours | Inner Product | 2maps (SXDH) | poly |
| [ABDP 15, ALS 15, ABDP 16] | Inner Product | 1maps (DDH) | 1 |
| [LL 16] | Inner Product | 2maps (SXDH & 3DH) | 2 |

# Open problems

| Construction: | Functions: | Assumption: | # slots: |
|---|---|---|---|
| [BLRSZZ 14, GGGJKLSSZ 14, AJ 15, BGJS 15, BKS 16,KS 17] | any circuit | Non standard | Poly, unbounded |
| Ours | Inner Product | 2maps (SXDH) | poly |
| [ABDP 15, ALS 15, ABDP 16] | Inner Product | 1maps (DDH) | 1 |
| [LL 16] | Inner Product | 2maps (SXDH & 3DH) | 2 |

Remove the use of pairing?

Larger classes of functions from standard assumptions?

# Open problems

| Construction: | Functions: | Assumption: | # slots: |
|---|---|---|---|
| [BLRSZZ 14, GGGJKLSSZ 14, AJ 15, BGJS 15, BKS 16,KS 17] | any circuit | Non standard | Poly, unbounded |
| Ours | Inner Product | 2maps (SXDH) | poly |
| [ABDP 15, ALS 15, ABDP 16] | Inner Product | 1maps (DDH) | 1 |
| [LL 16] | Inner Product | 2maps (SXDH & 3DH) | 2 |

Thank you

Remove the use of pairing?

Larger classes of functions from standard assumptions?