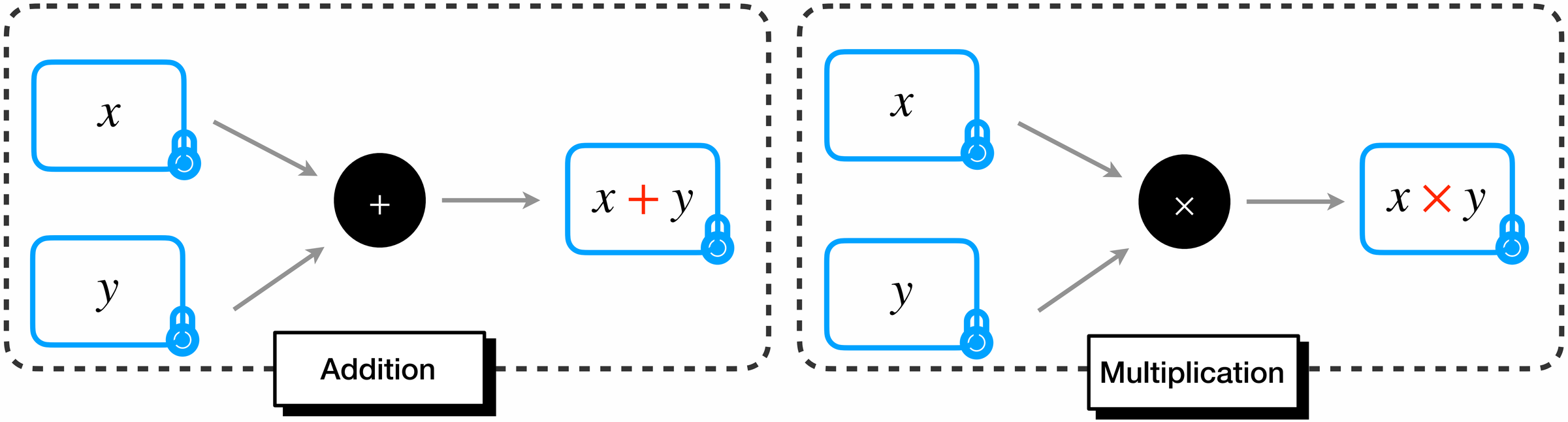
Loris Bergerat, Ilaria Chillotti, Damien Ligier, Jean-Baptiste Orfila,
Adeline Roux-Langlois & Samuel Tap

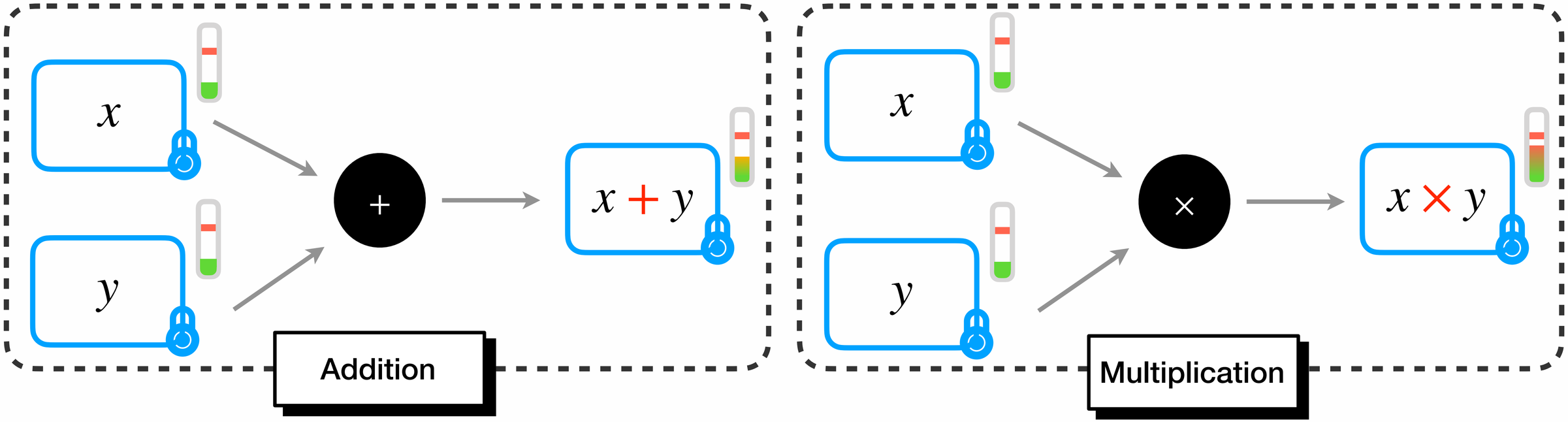
17 October 2023

Faster Secret Keys for (T)FHE

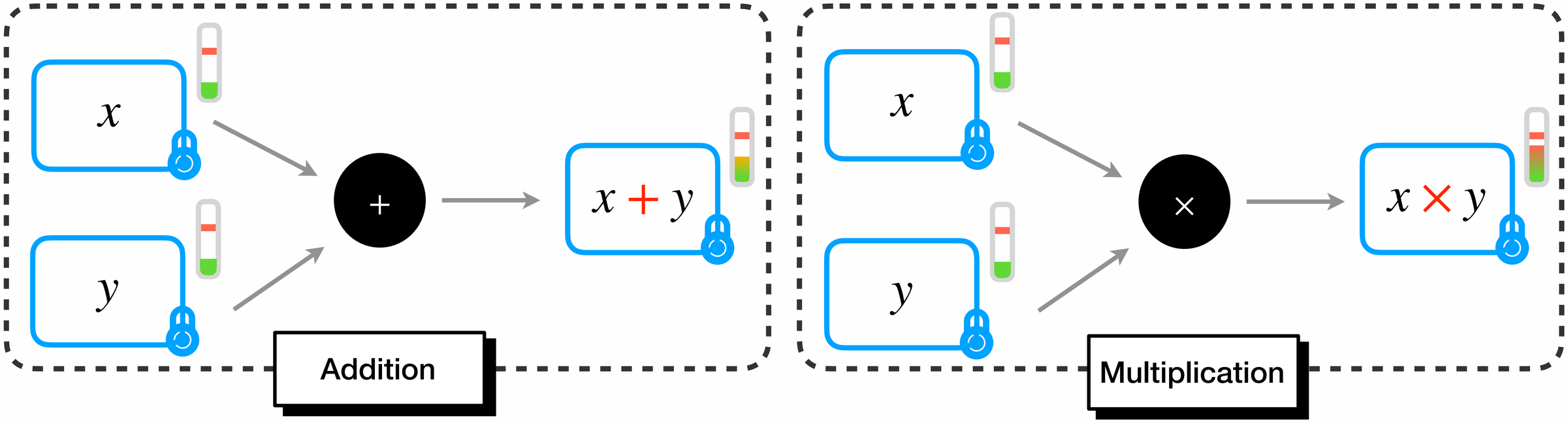
Homomorphic Encryption



Homomorphic Encryption

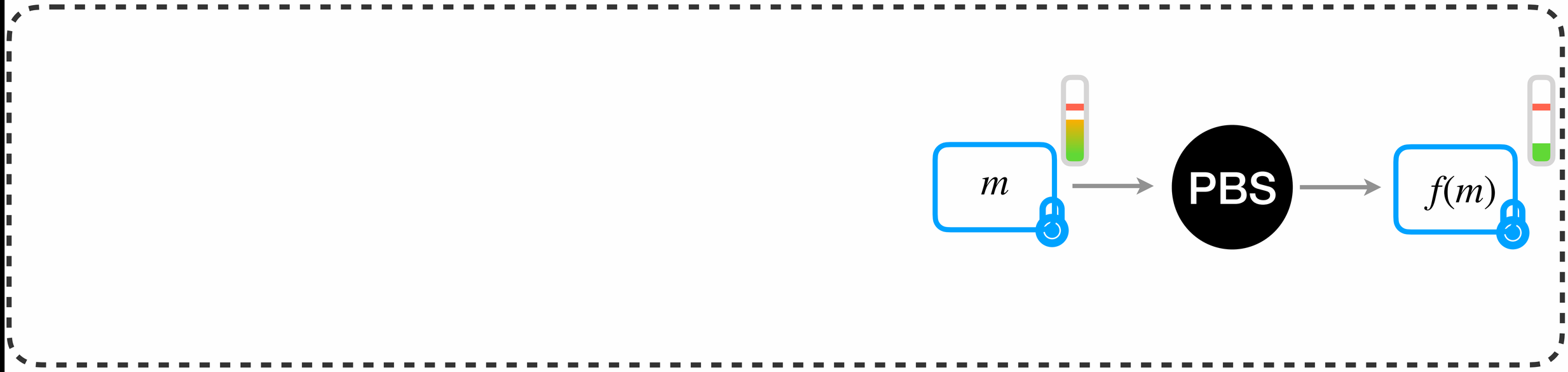


Homomorphic Encryption



too much noise $\Longrightarrow$ incorrect decryption

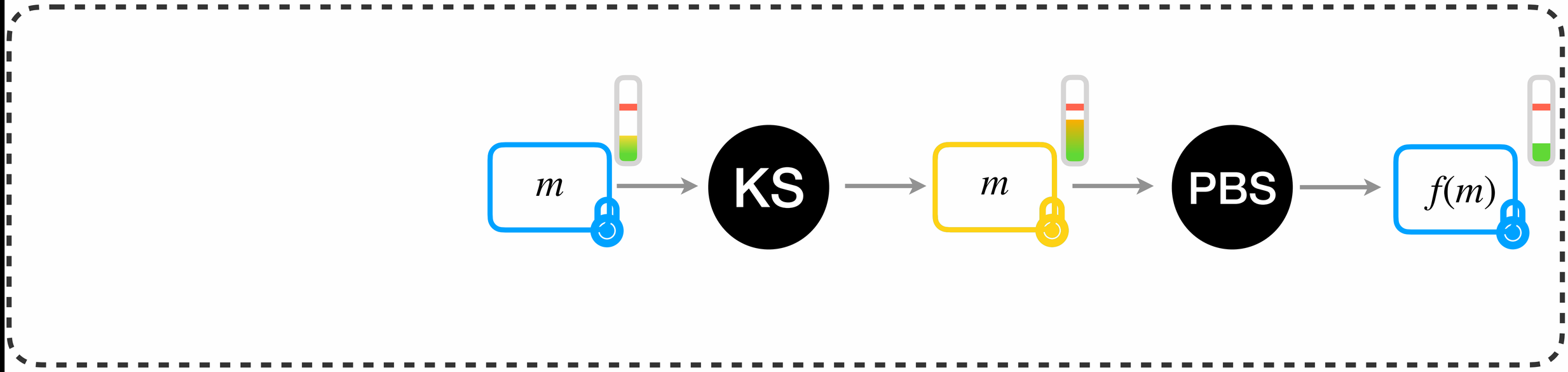
Bootstrapping graph



Programmable Bootstrapping

Evaluate univariate function,
Reduce the noise

Bootstrapping graph



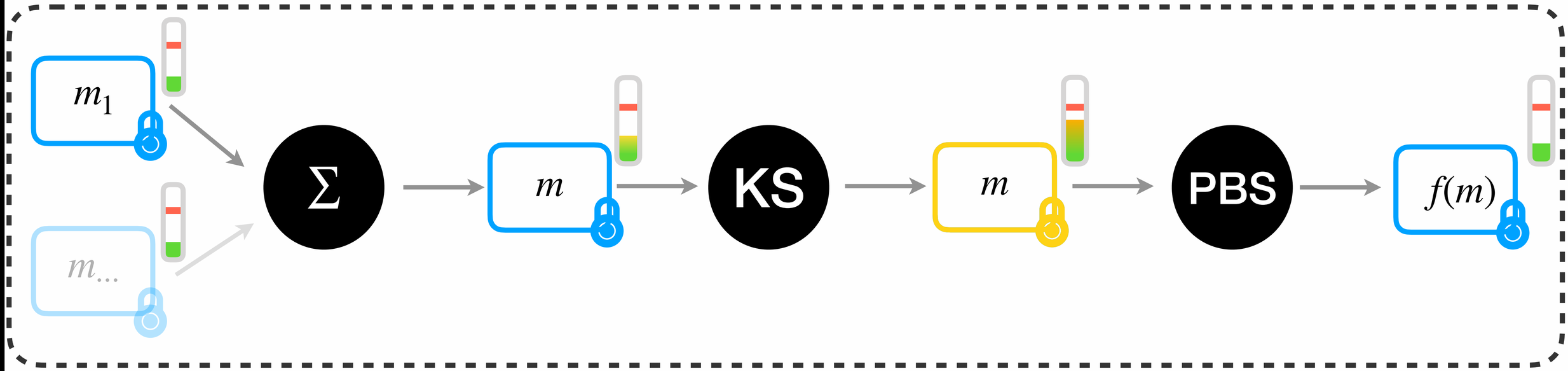
Keyswitching

Switch from a secret key s to another secret key s.

Programmable Bootstrapping

Evaluate univariate function, Reduce the noise

Bootstrapping graph



Leveled Operations

Scalar multiplication,
Addition

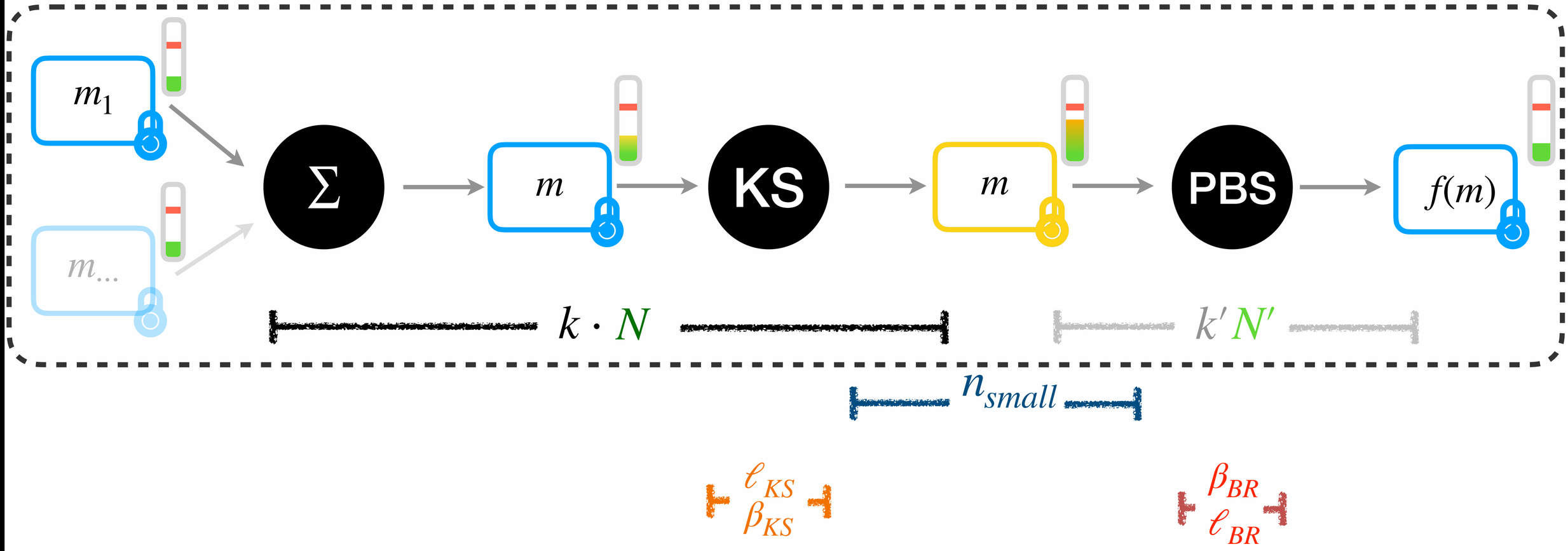
Keyswitching

Switch from a secret key s to
another secret key s.

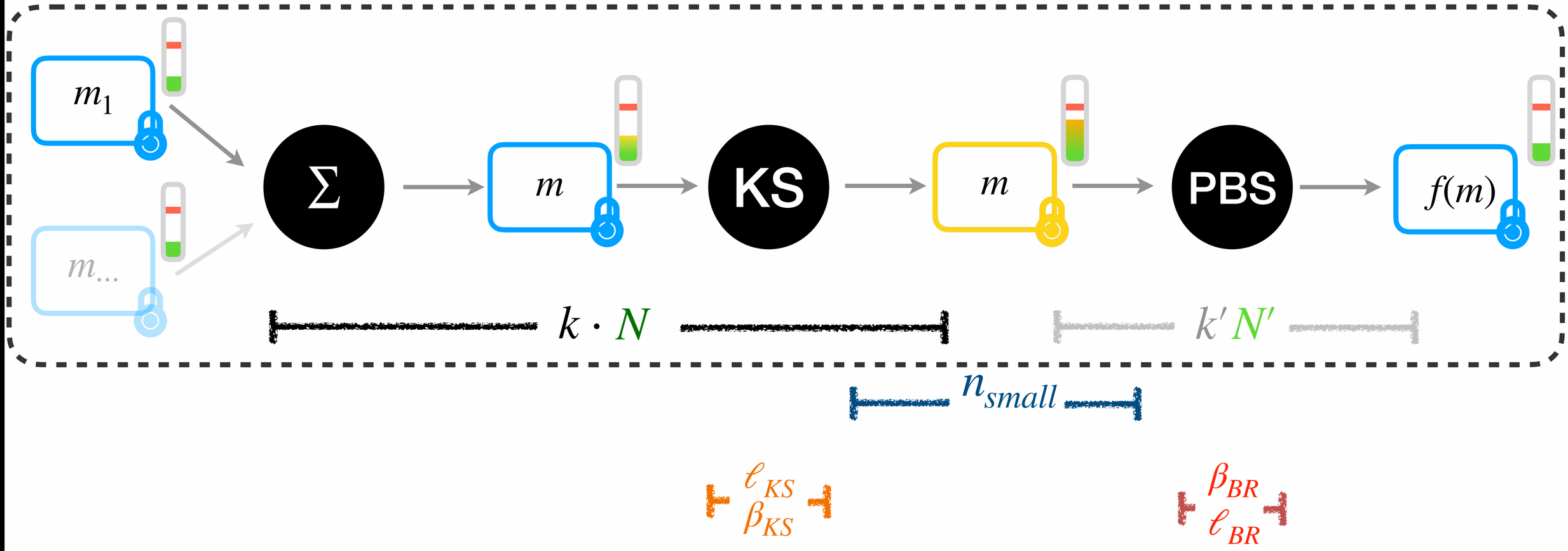
Programmable Bootstrapping

Evaluate univariate function,
Reduce the noise

Bootstrapping graph



Bootstrapping graph



A lot of parameters, changing <u>one</u> parameter impact :
the <u>correctness</u>, the <u>other parameters</u> and the <u>execution time</u>.

Ideas

Bootstrapping graph is fast but still slow ($\simeq$10ms)

Ideas

Bootstrapping graph is fast but still slow ($\simeq$10ms)

Can we explore new assumptions to improve the bootstrapping graph ?

Ideas

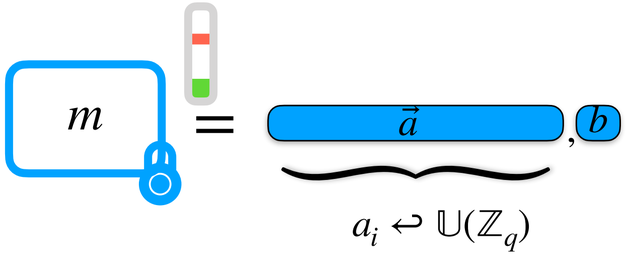
Bootstrapping graph is fast but still slow ($\simeq$10ms)

Can we explore new assumptions to improve the bootstrapping graph ?

Explore new assumption for the secret keys

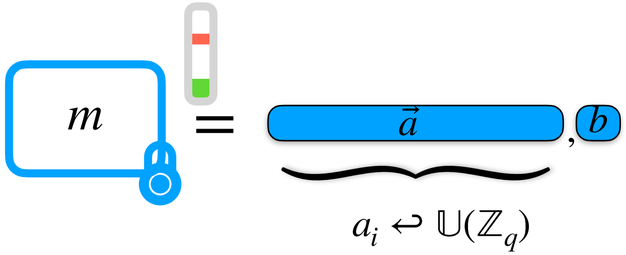
LWE ciphertext

Encrypt:

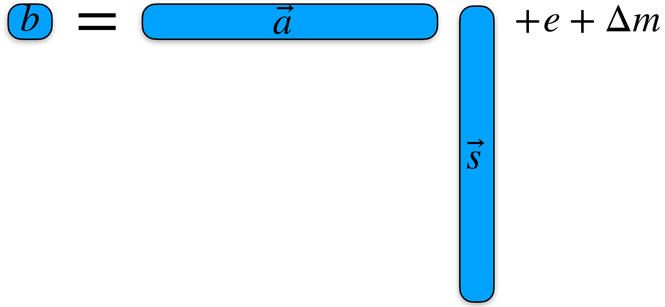


LWE ciphertext

Encrypt:

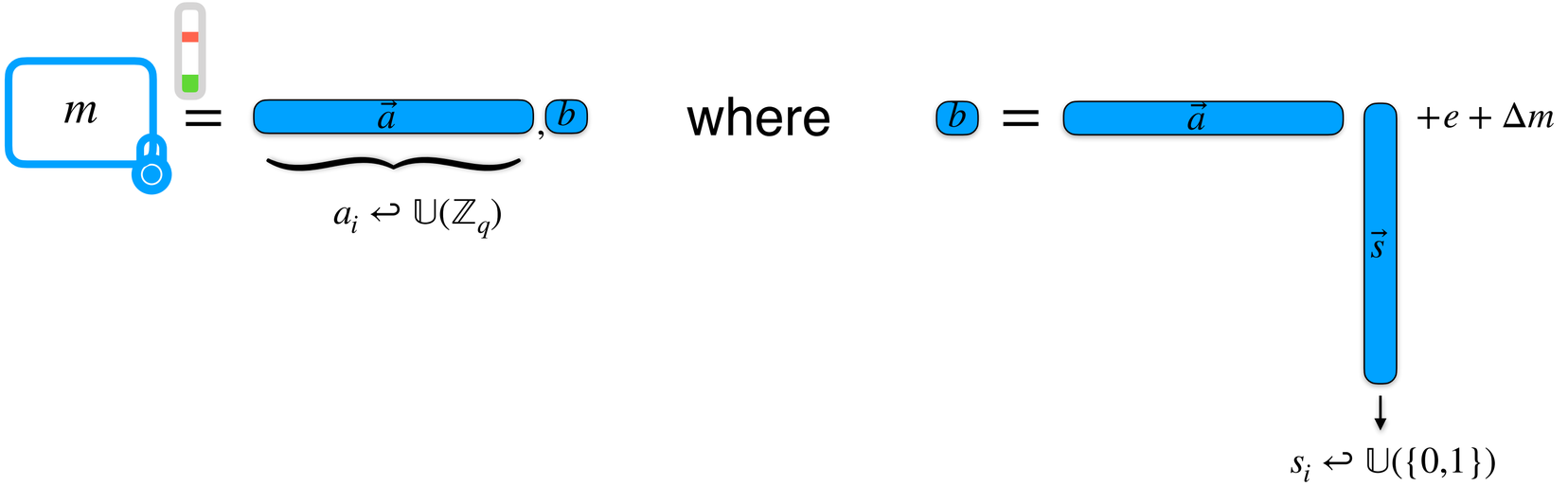


where



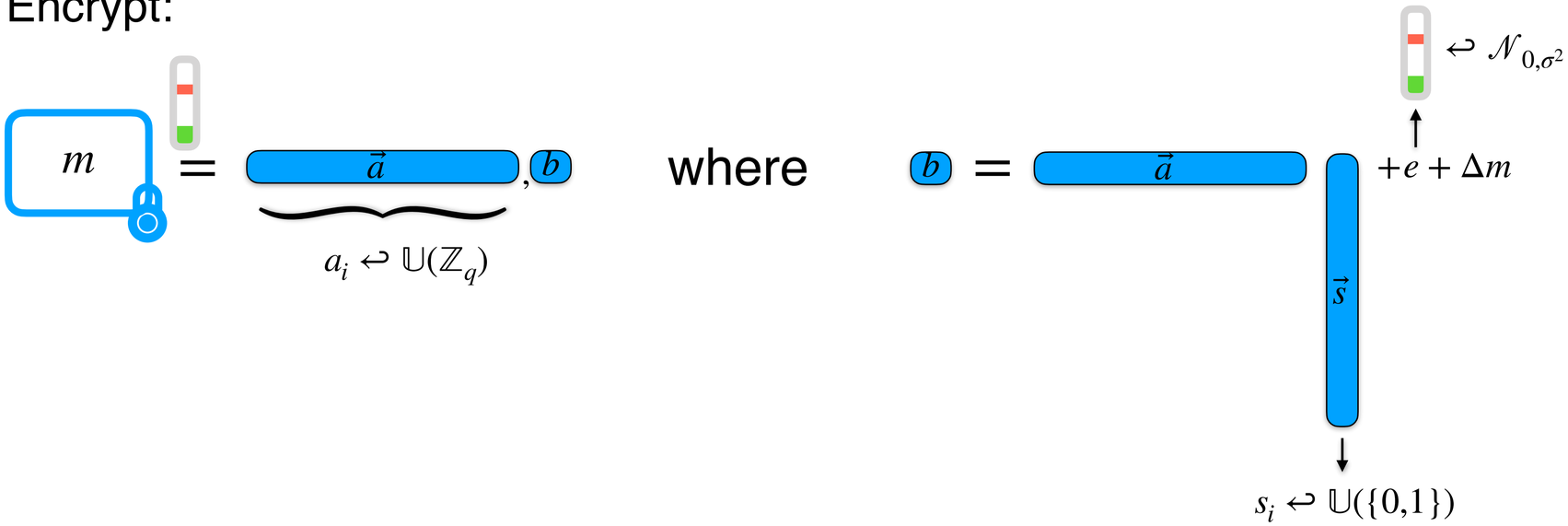
LWE ciphertext

Encrypt:

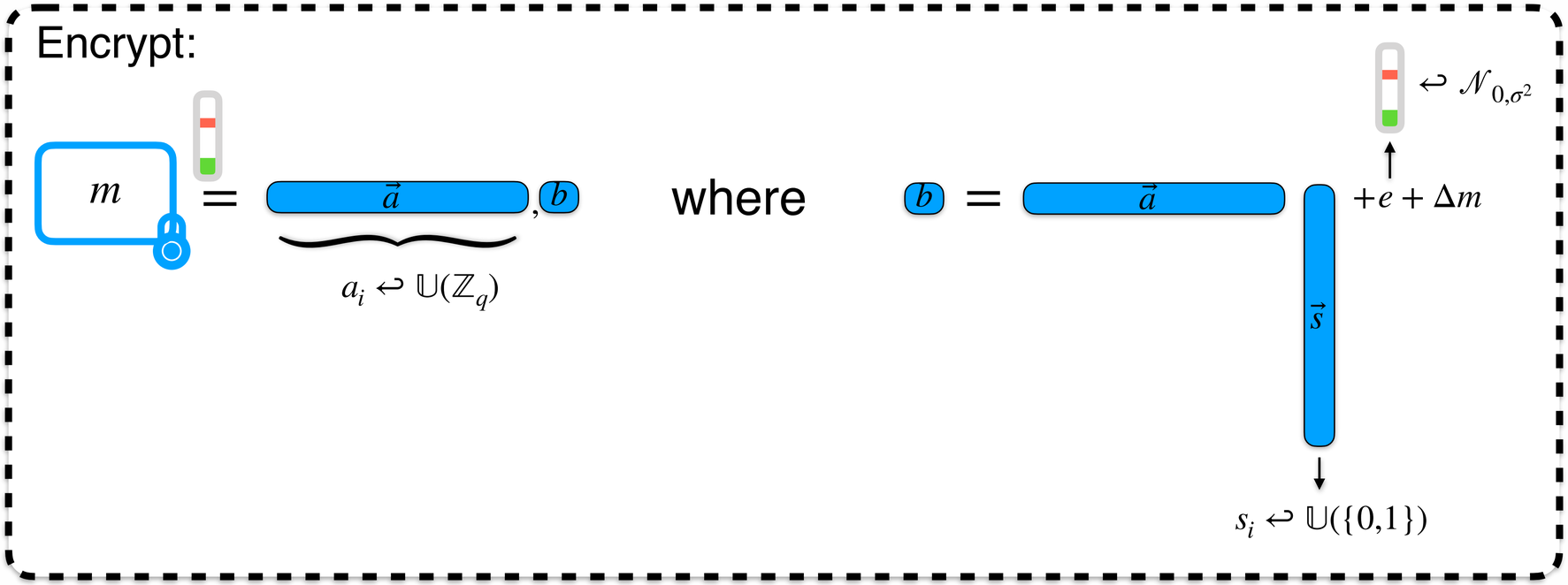


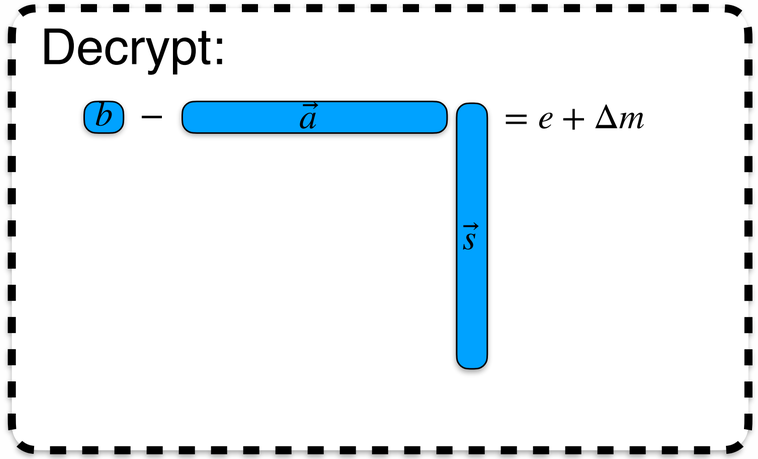
LWE ciphertext

Encrypt:

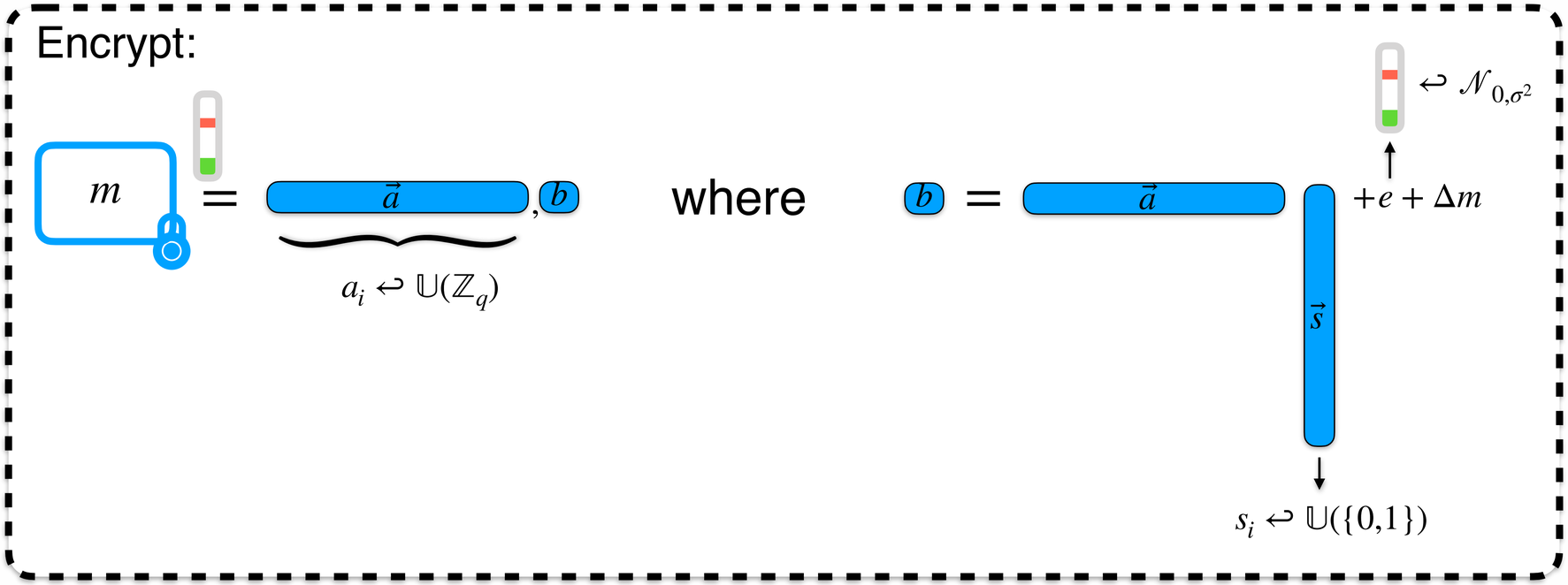


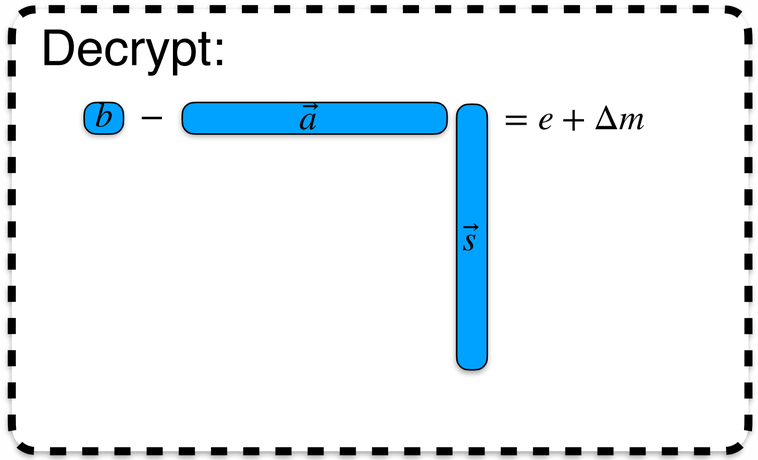
LWE ciphertext

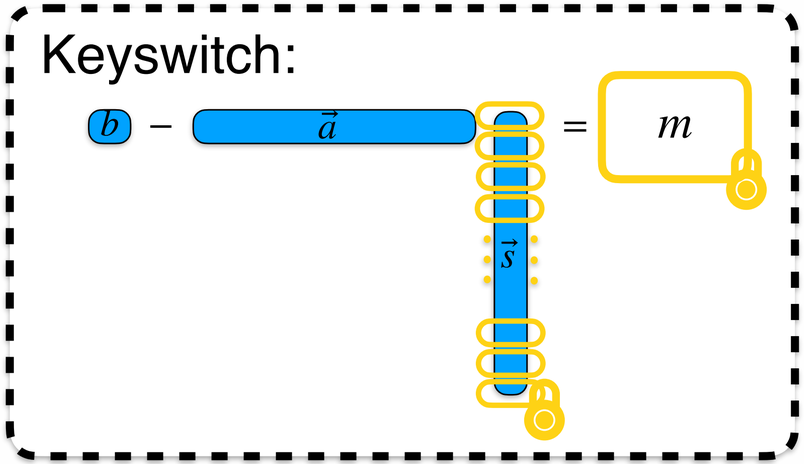




LWE ciphertext







Our Contributions

Two new types of secret keys

Our Contributions

Two new types of secret keys

Shared randomness secret keys

Partial secret keys

Our Contributions

Two new types of secret keys

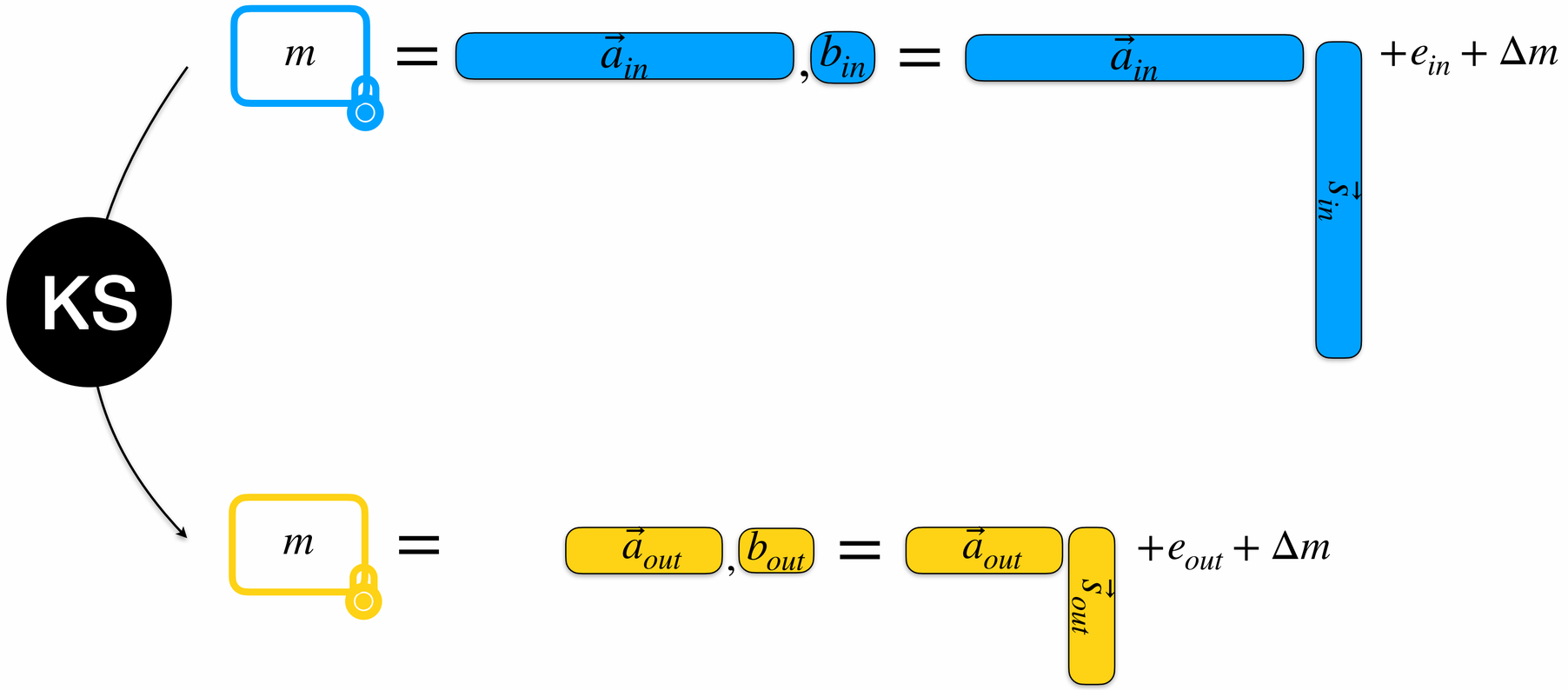
Shared randomness secret keys

Partial secret keys

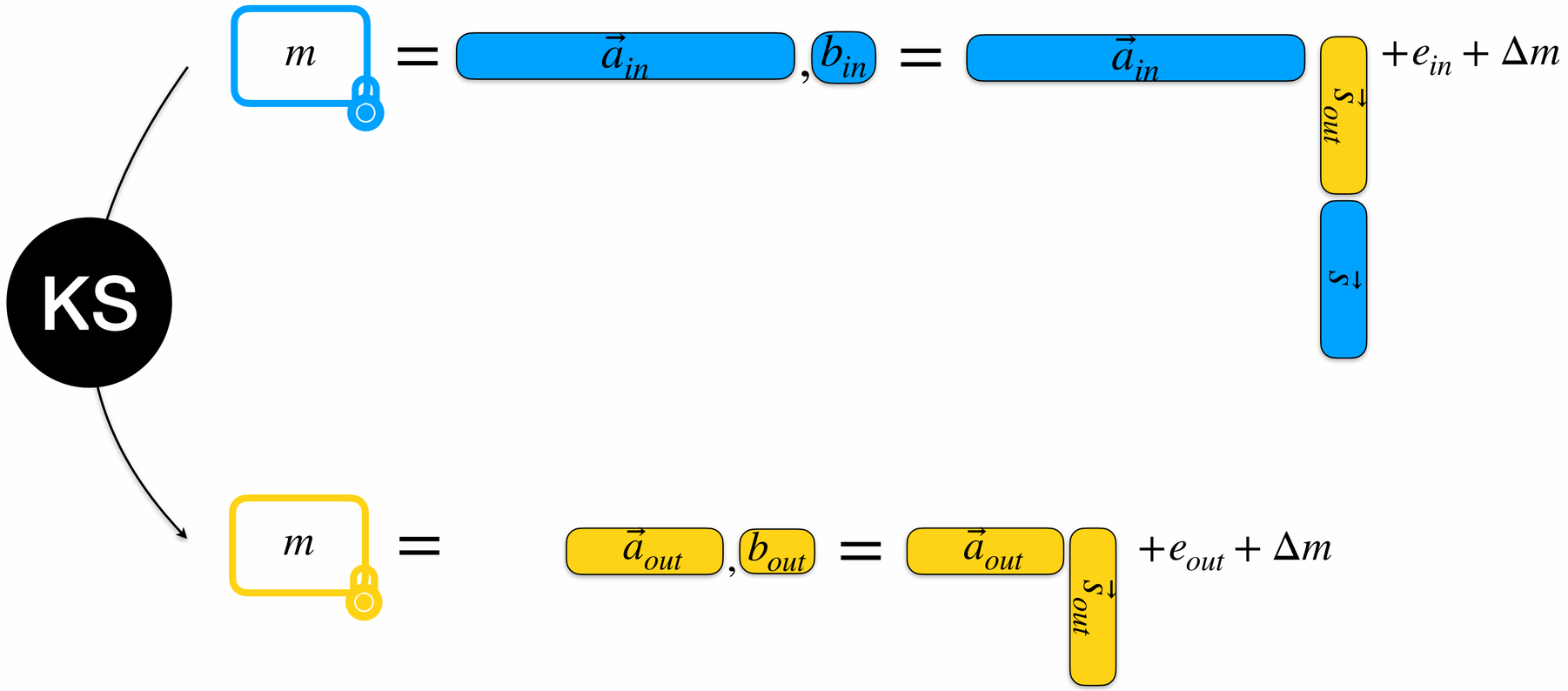
This both keys can be combined

Shared Randomness Secret Keys

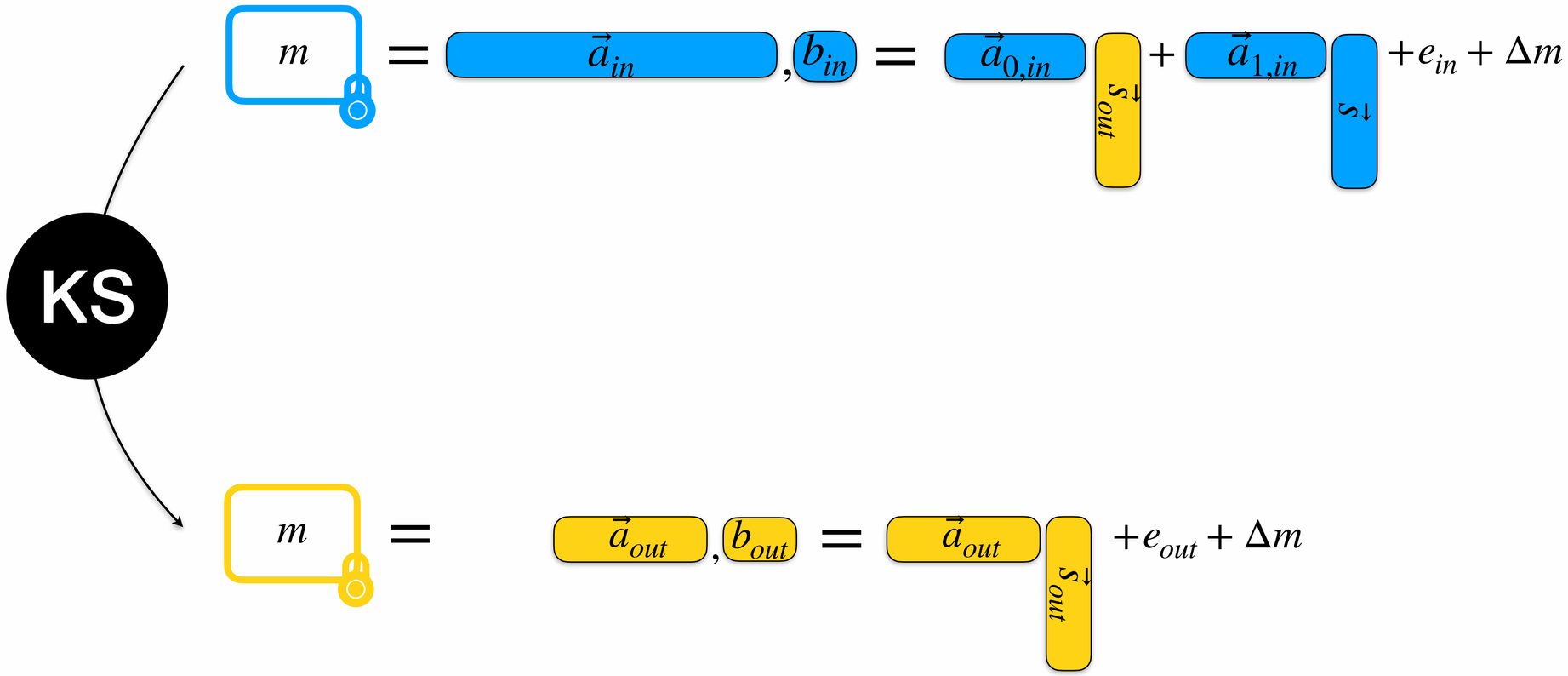
Shared Randomness Secret Keys



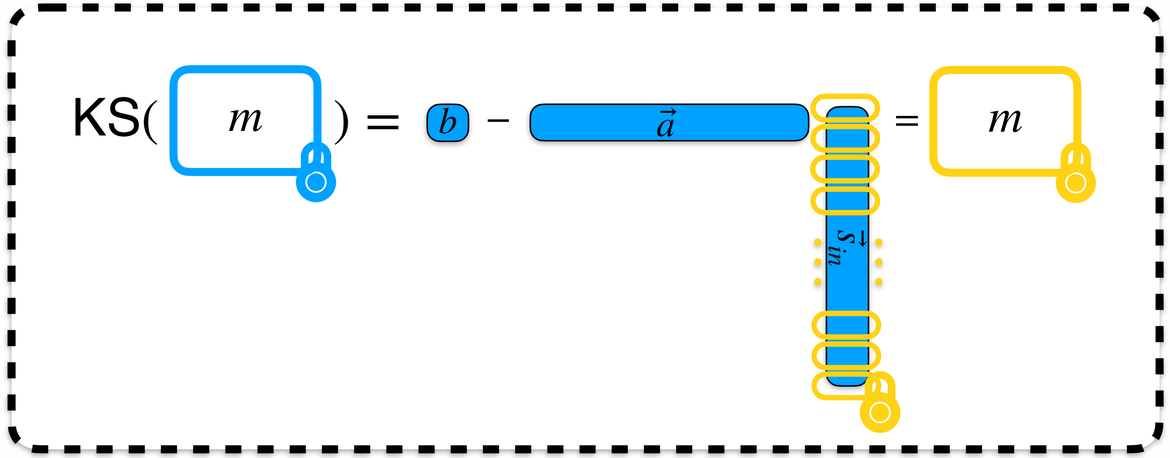
Shared Randomness Secret Keys

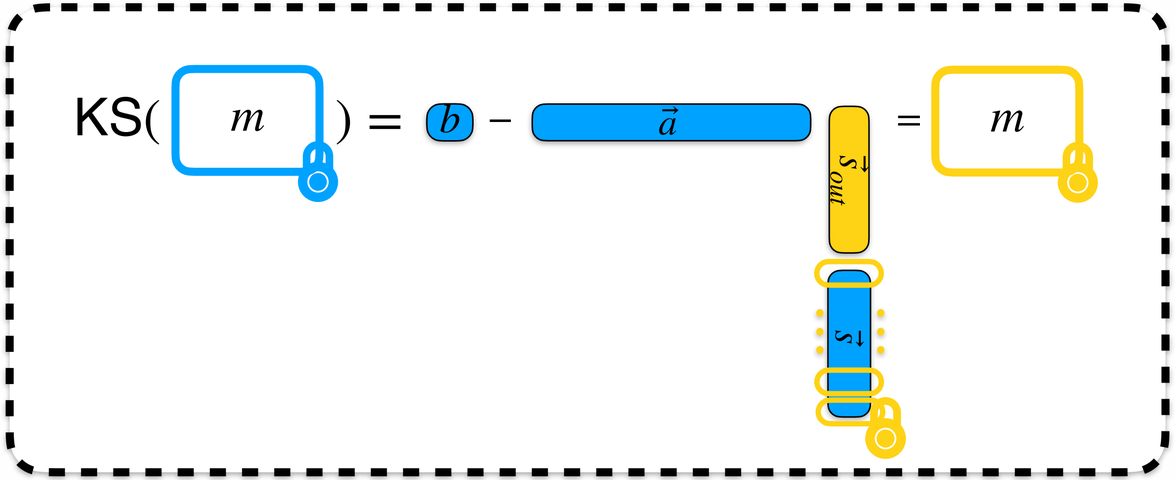


Shared Randomness Secret Keys

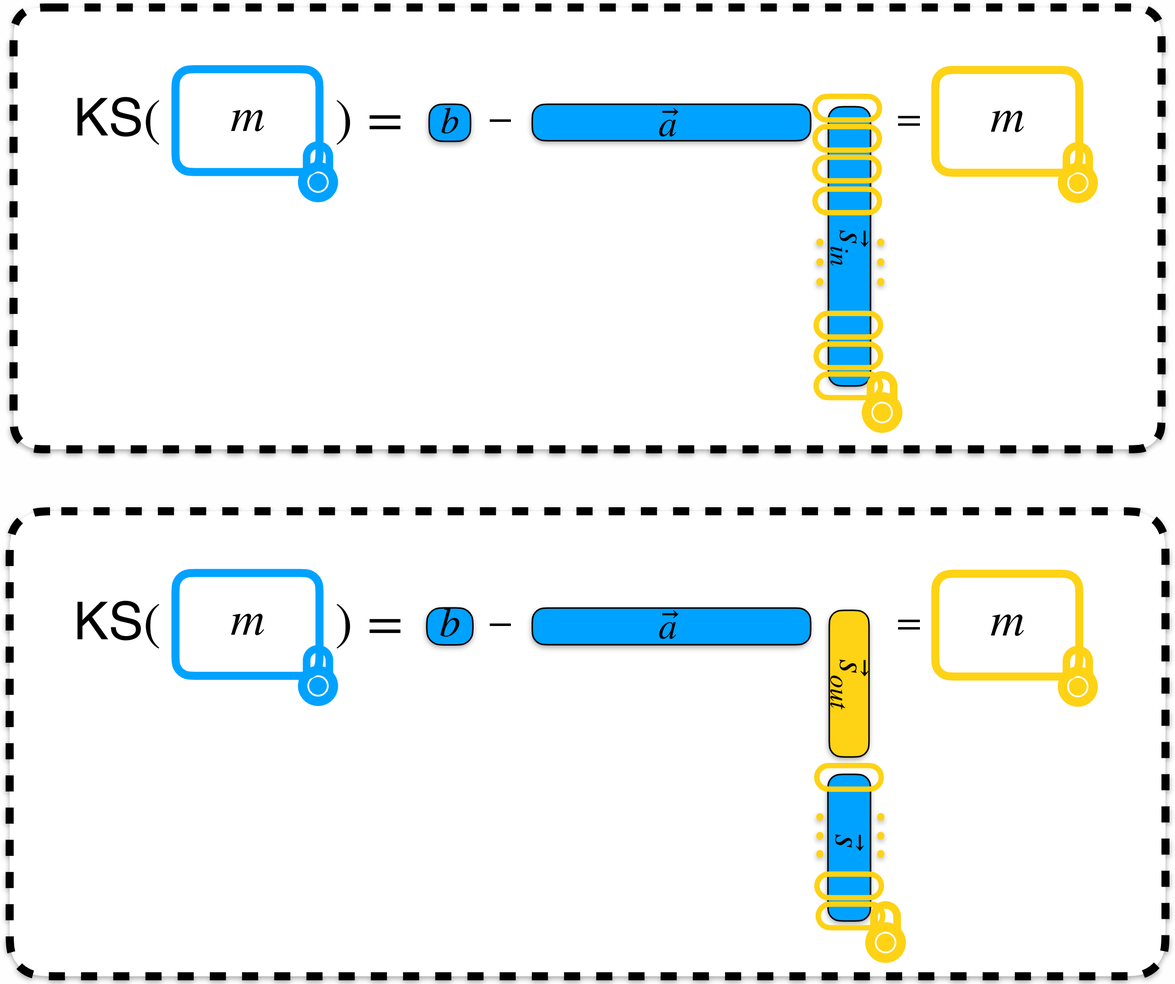


Shared Randomness Secret Keys





Shared Randomness Secret Keys



Less computations

Smaller public keys

Less noise

Recap & Generalization

Generalization of the keys to the polynomials (RLWE , GLWE)

Recap & Generalization

Generalization of the keys to the polynomials (RLWE , GLWE)

New (G)LWE assumptions and Security

Recap & Generalization

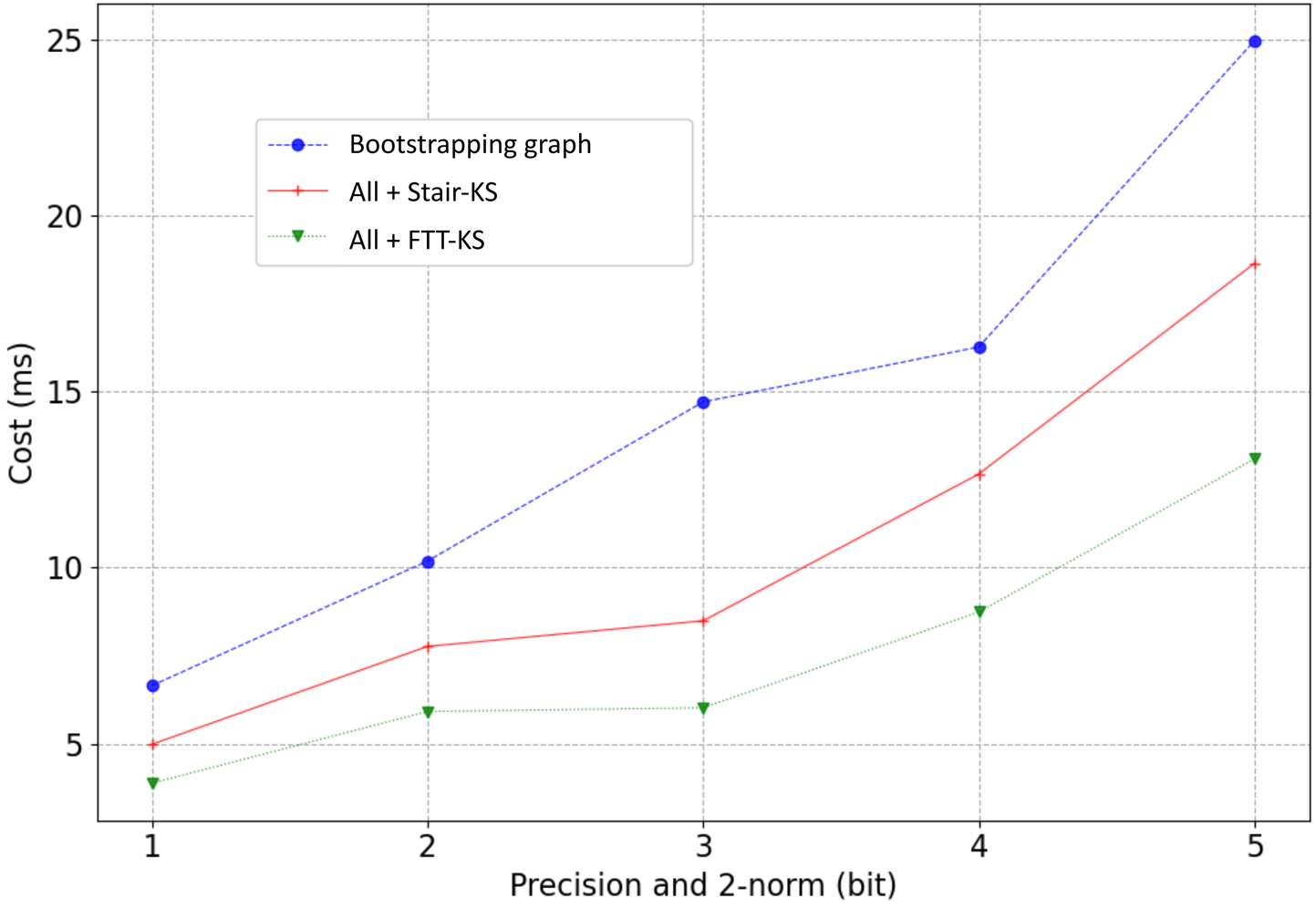
Generalization of the keys to the polynomials (RLWE , GLWE)

New (G)LWE assumptions and Security

Keyswitch with Shared and Partial secret Keys
=> less noise and faster algorithms
=> Bootstrapping graph becomes faster

Practical Results

Results



speed-ups between **1.3** and **2.4**

Conclusion

Conclusion

Partial Secret Keys

Shared Randomness
Secret keys

Conclusion

Partial Secret Keys

Shared Randomness
Secret keys

New algorithms

Speed-ups between
1.3 and 2.4

Conclusion

Partial Secret Keys

Shared Randomness Secret keys

New algorithms

Speed-ups between 1.3 and 2.4

Security Analysis

Reduction of the size of the public material

Conclusion

Partial Secret Keys

Shared Randomness
Secret keys

New algorithms

Speed-ups between
1.3 and 2.4

Security Analysis

Reduction of the size
of the public material

Thank you.

eprint 2023/979