Skye: An Expanding PRF based Fast KDF and its Applications

ACM ASIACCS 2024

Amit Singh Bhati
COSIC, KU Leuven

Antonín Dufka
Masaryk University

Elena Andreeva
TU Wien

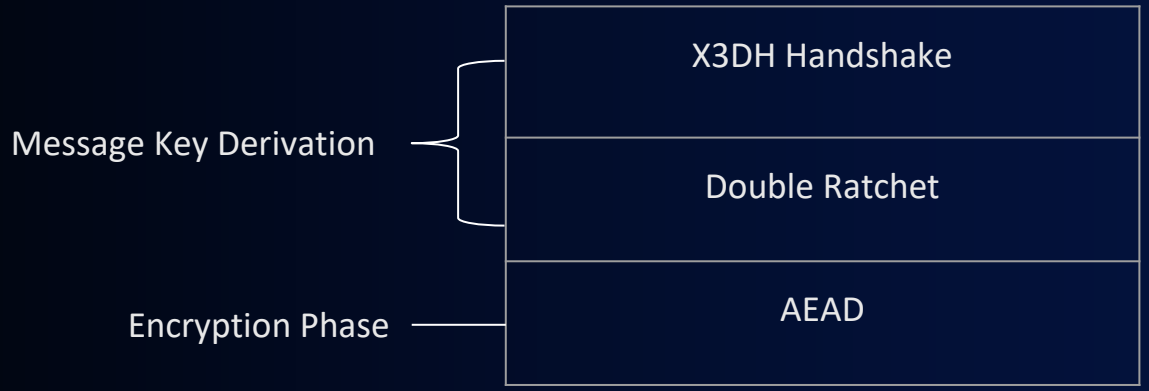
Arnab Roy
University of Innsbruck

Bart Preneel
COSIC, KU Leuven

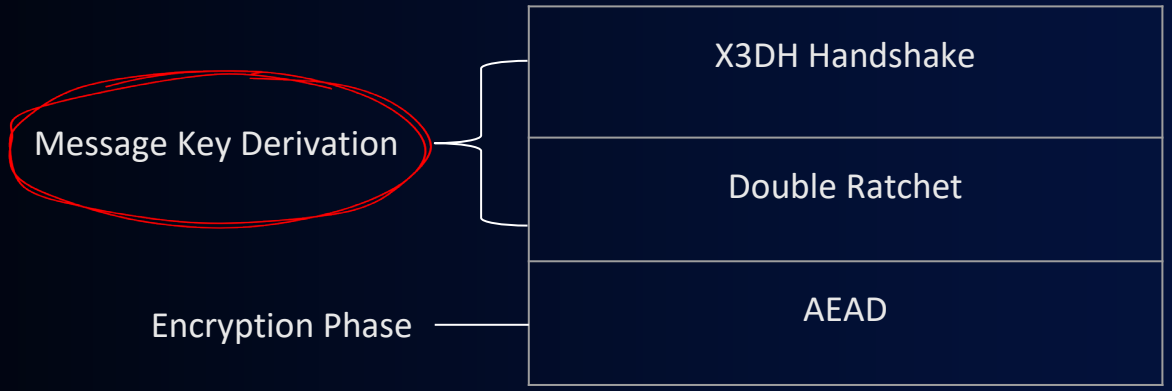
Signal Protocol

- An instant, end-to-end encrypted messaging protocol
- Used for one-to-one and group multimedia messages and calls
- Popular for its provably strong security and privacy features
- Used in many applications such as 

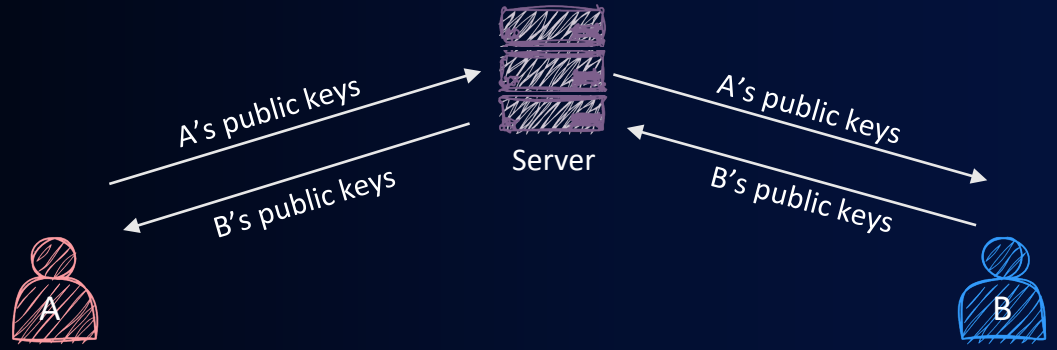
Signal Protocol: Phases



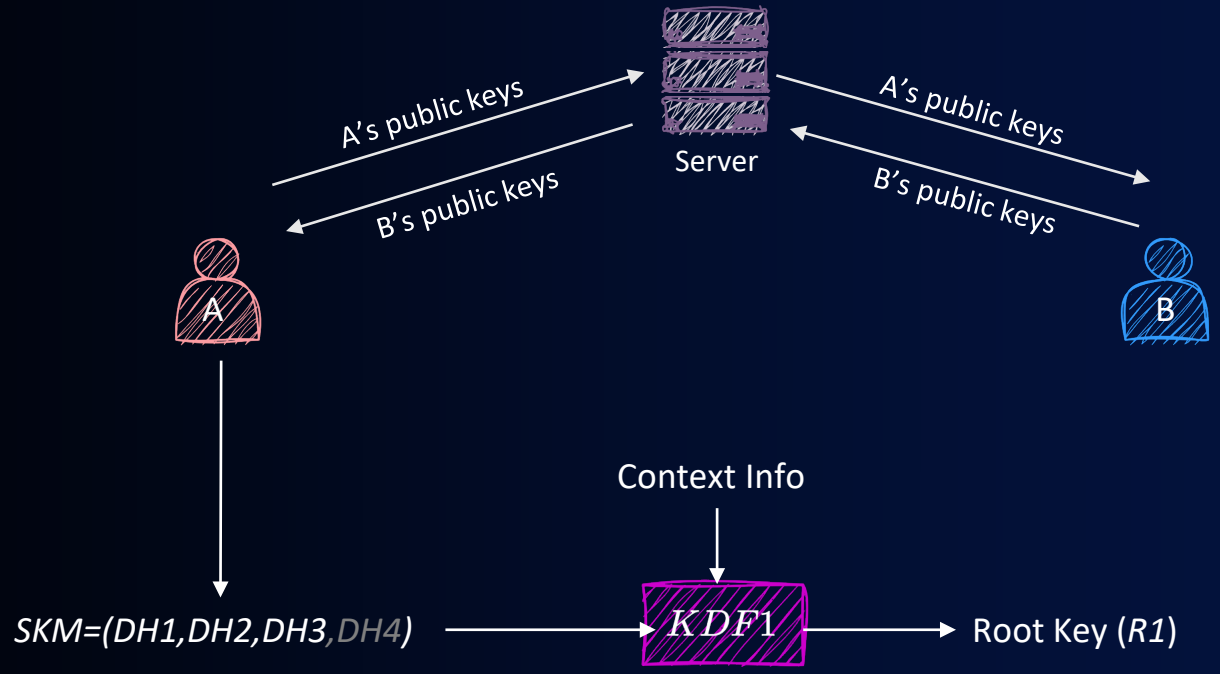
Signal Protocol: Phases



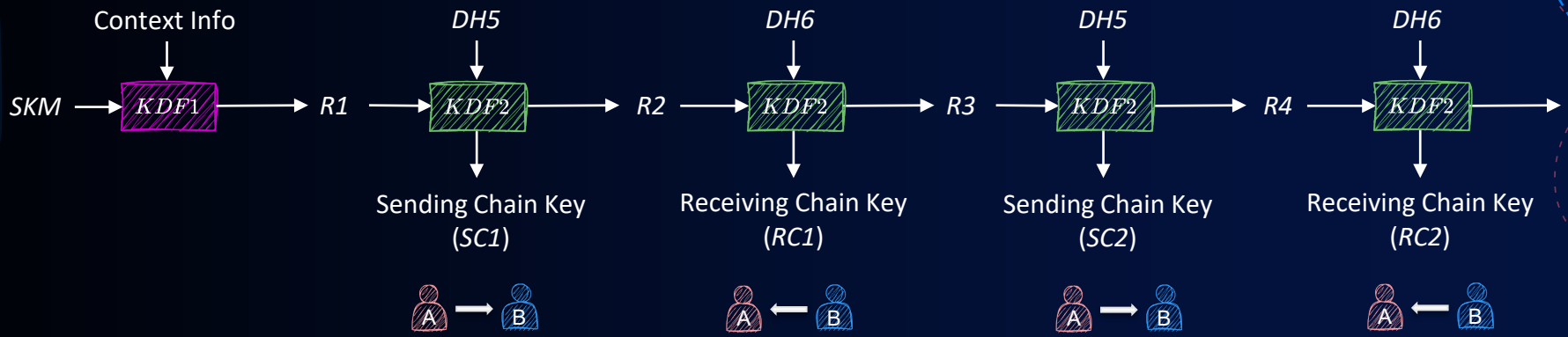
Signal's Key Derivation in a Nutshell



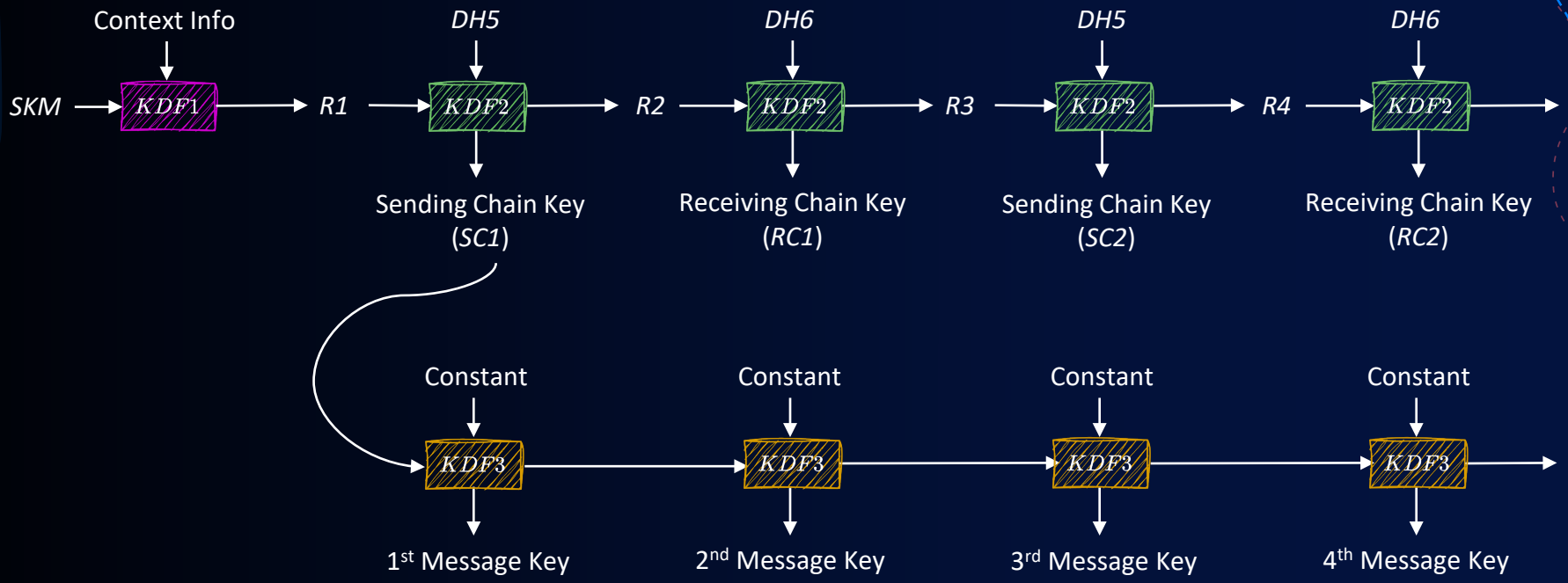
Signal's Key Derivation in a Nutshell



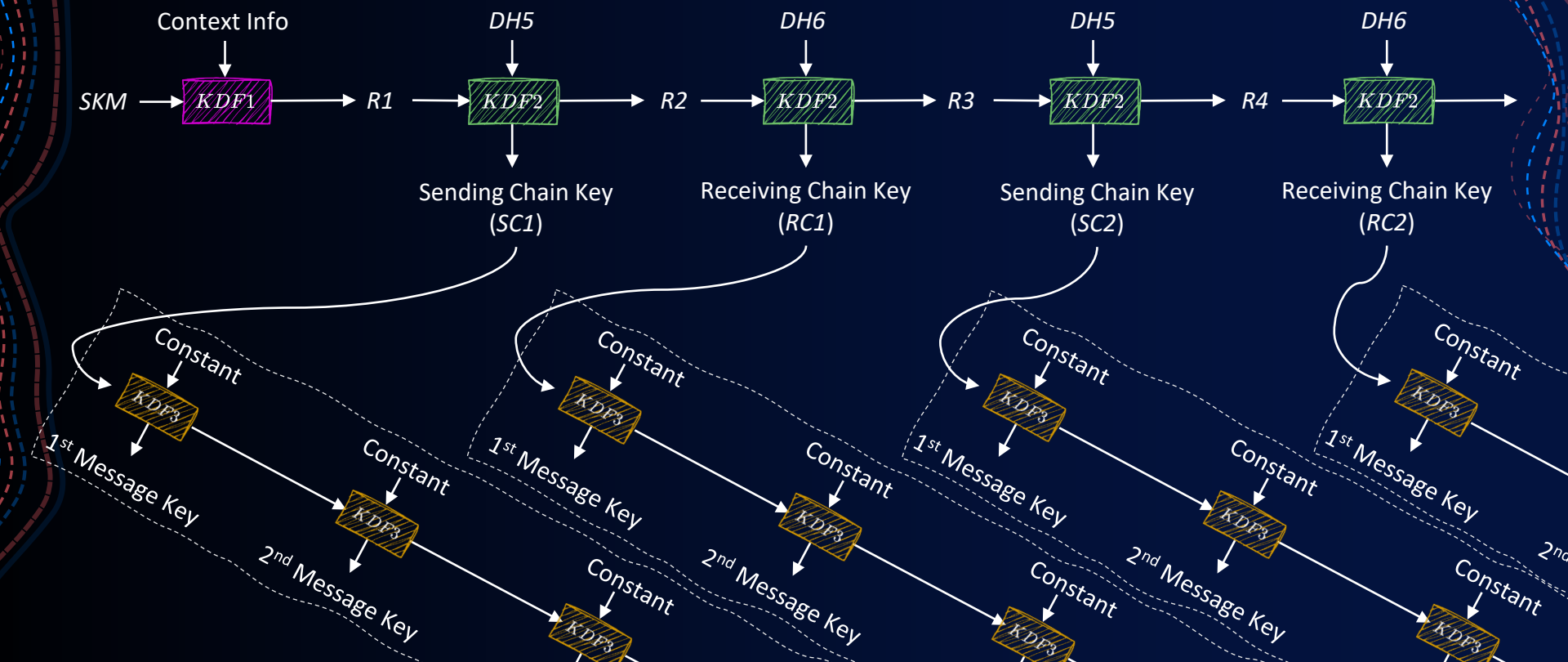
Signal's Key Derivation in a Nutshell



Signal's Key Derivation in a Nutshell



Signal's Key Derivation in a Nutshell



Signal's KDF

- A KDF transforms non-uniform / weakly random keys into uniform / highly random keys
- Signal uses HMAC-based KDF (HKDF[1]) for all types of KDF calls
- Instantiated with HMAC-SHA-256

[1]Krawczyk, H., "Cryptographic extraction and key derivation: The HKDF scheme.", CRYPTO 2010.

HKDF

- Based on extract-then-expand paradigm
- Designed for general input sources

HKDF

+ Based on extract-then-expand paradigm

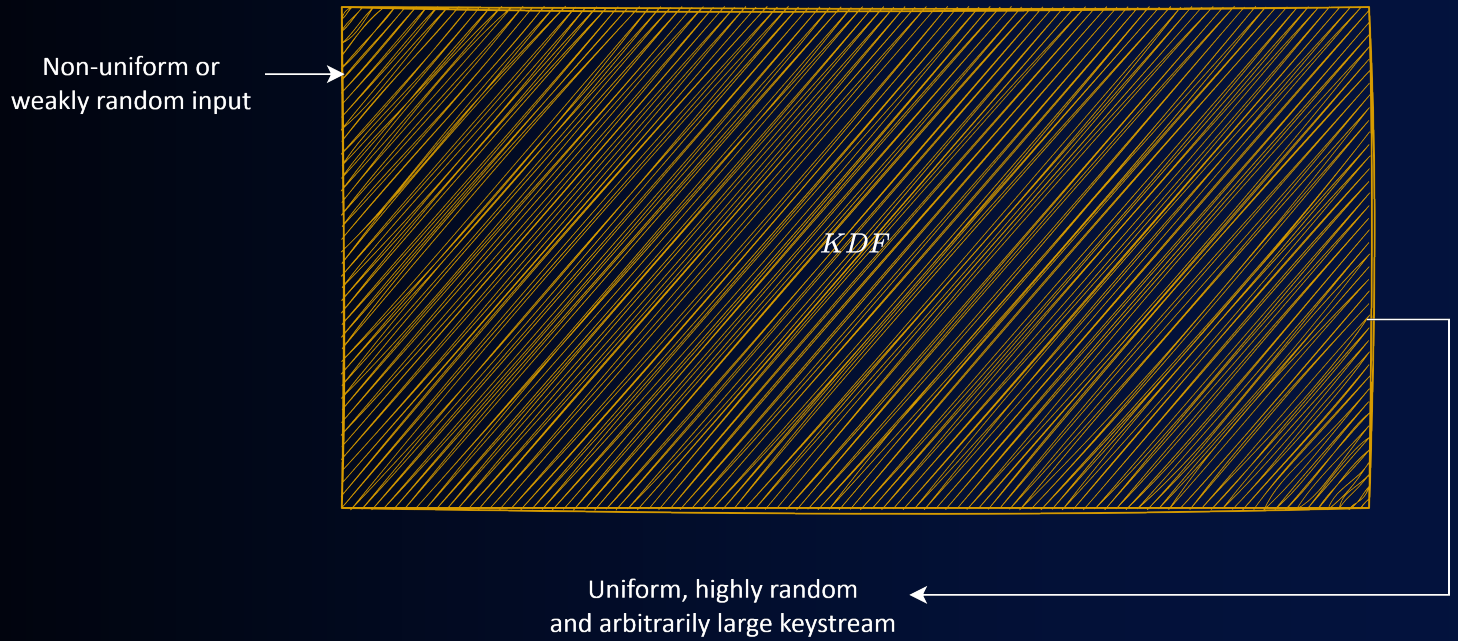
+ Designed for general input sources

- Not optimized for structured input sources such as X3DH

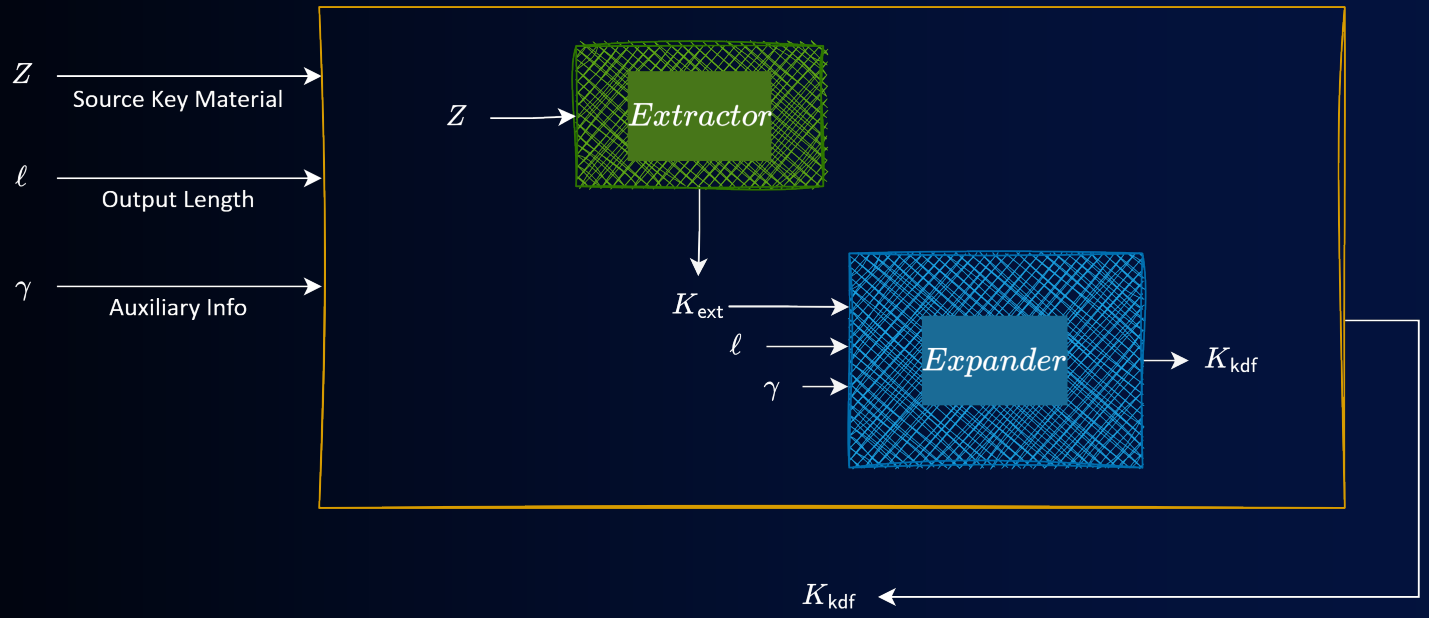
- Highly sequential mode

- Relies on RO assumption of SHA-256 CF for security

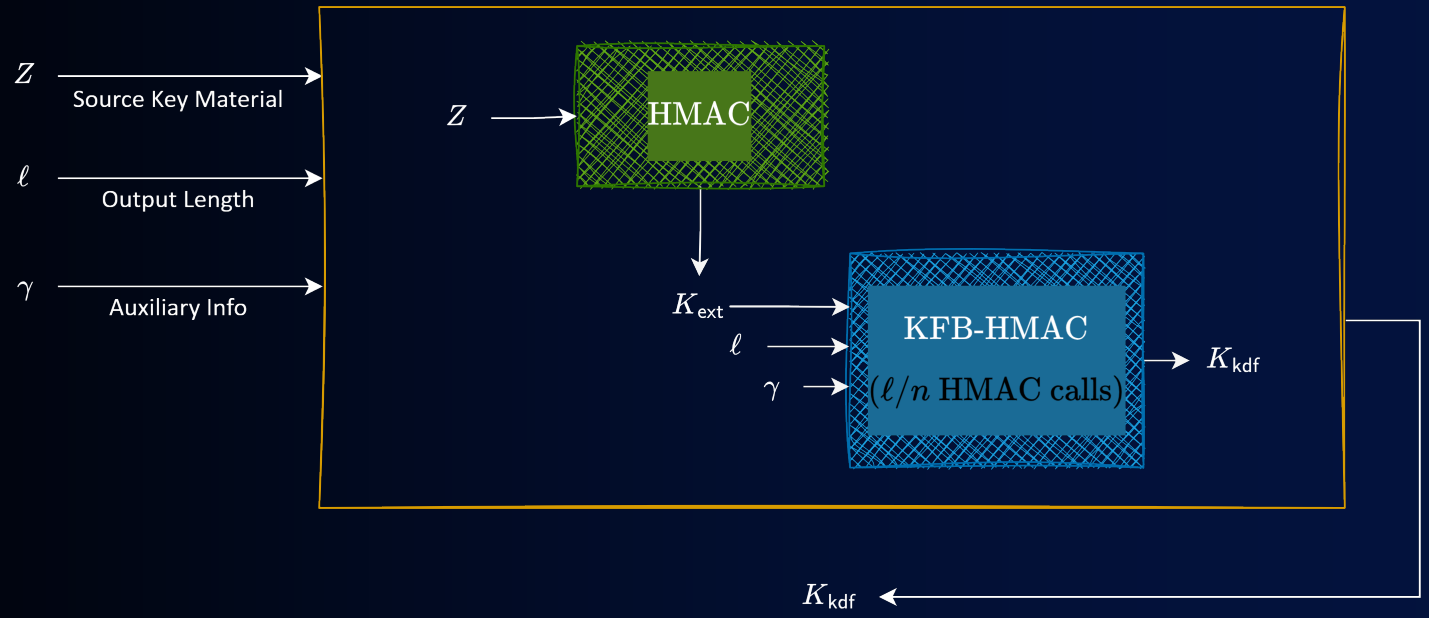
Extract-then-Expand KDF Paradigm



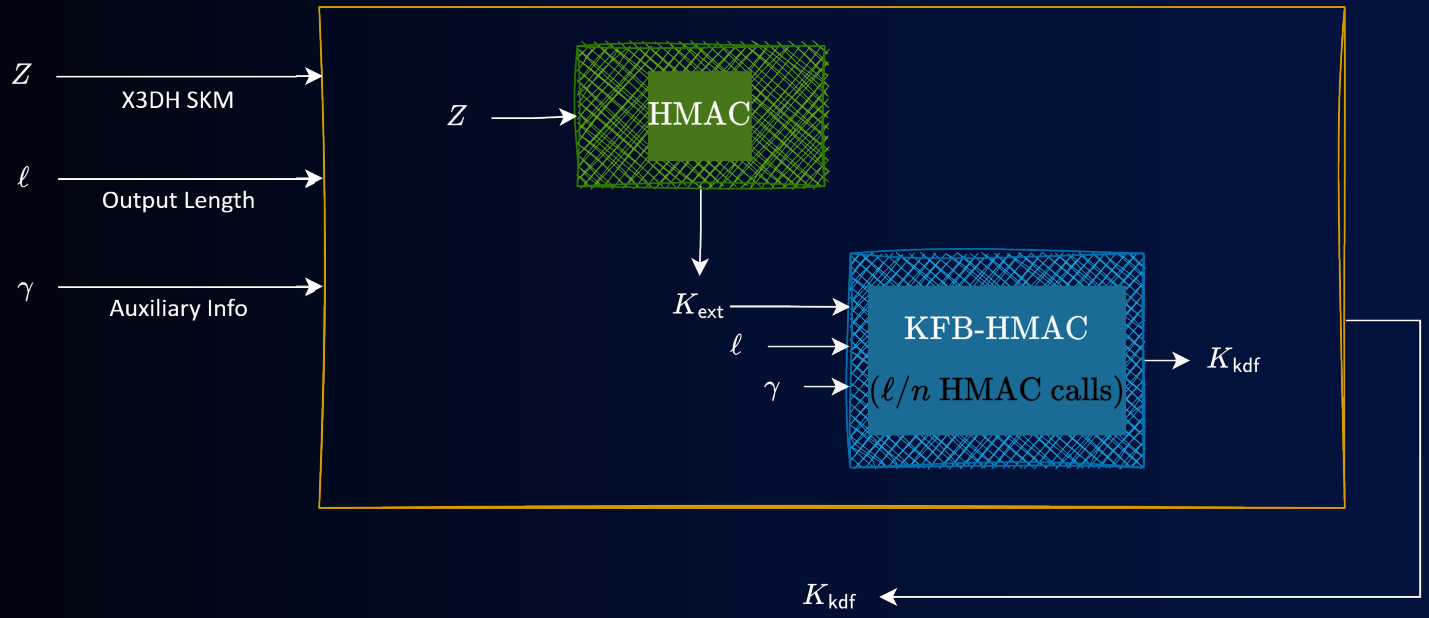
Extract-then-Expand KDF Paradigm



HKDF


Z
Source Key Material
ℓ
Output Length
γ
Auxiliary Info
Z
HMAC
K_{ext}
ℓ
γ
KFB-HMAC
$(\ell/n$ HMAC calls$)$
K_{kdf}
K_{kdf}

HKDF under X3DH Source

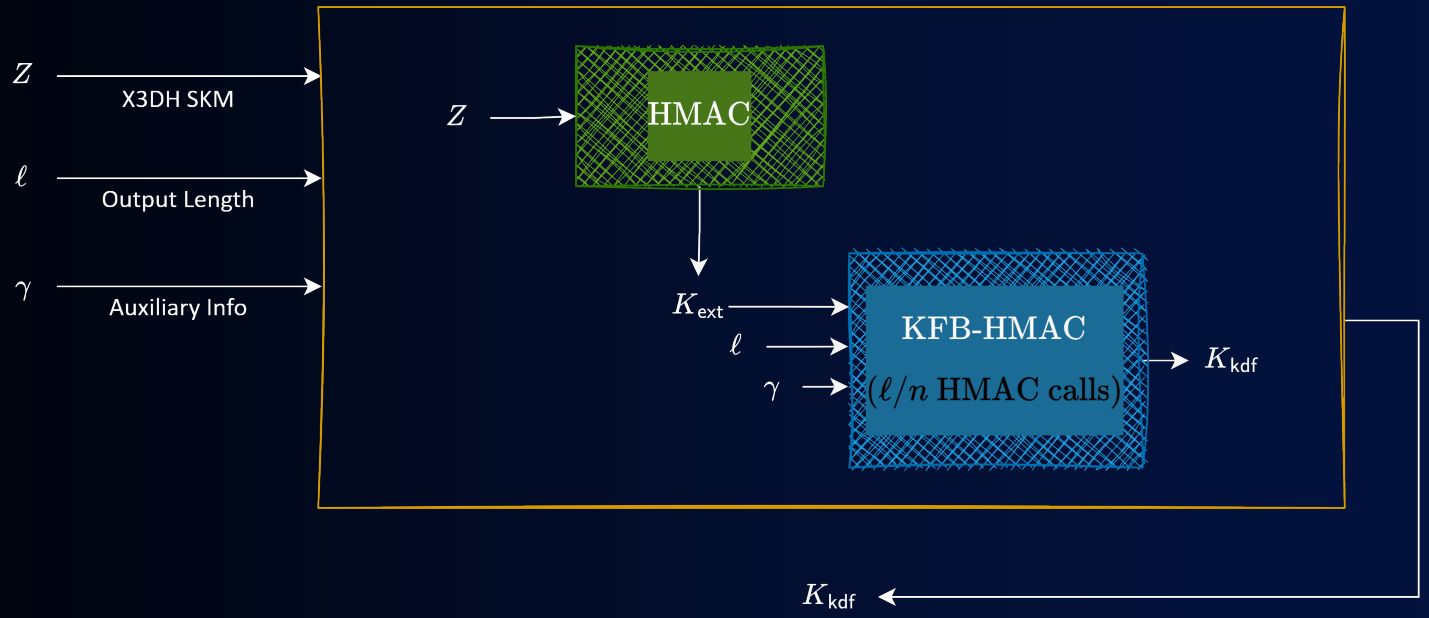


Skye KDF

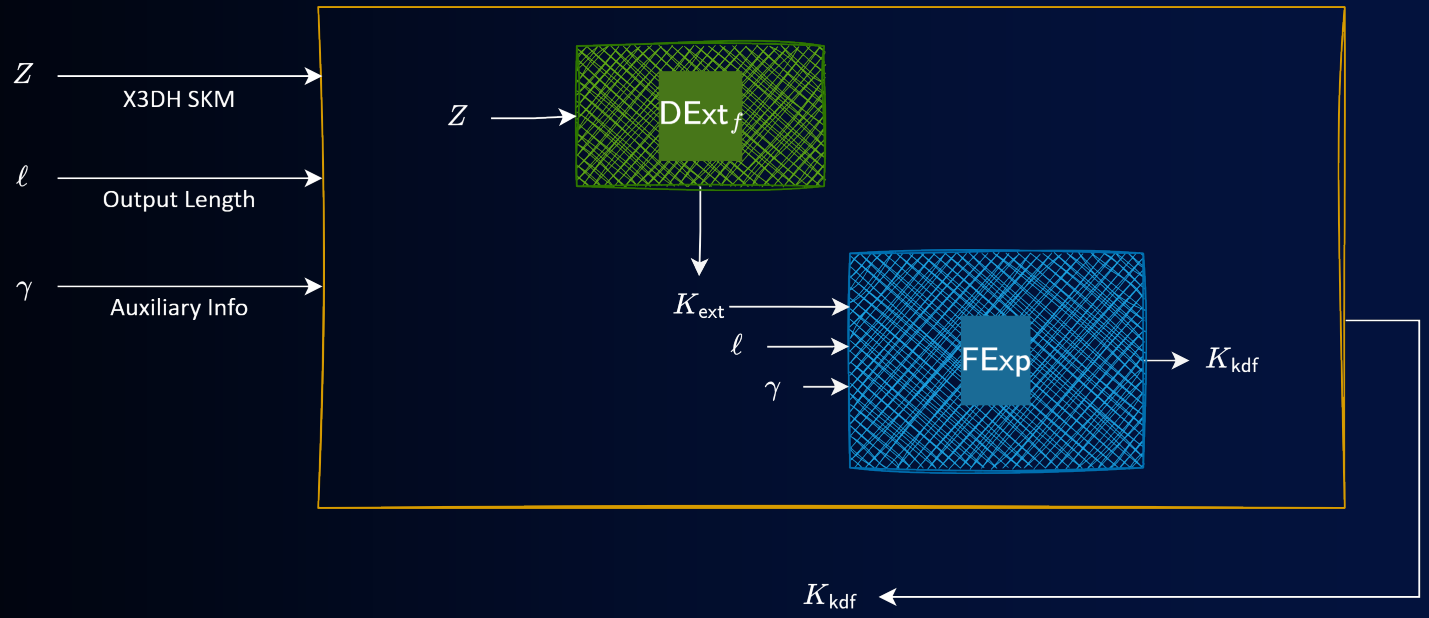
A faster alternative to HKDF for source-specific key derivation



HKDF for X3DH Source



Skye KDF for X3DH Source



DExt_f

- Highly efficient XOR-based extension
- Used to strengthen weak source-specific extractors f

DExt$_f$

- Highly efficient XOR-based extension
- Used to strengthen weak source-specific extractors *f*
- For DH sources, *f* can be simply truncation
- Truncating 256-bit DH element to 82 bits ➔ 82-bit security[2]

[2]Chevalier C., et al., "Optimal Randomness Extraction from a Diffie-Hellman Element", EUROCRYPT 2009.

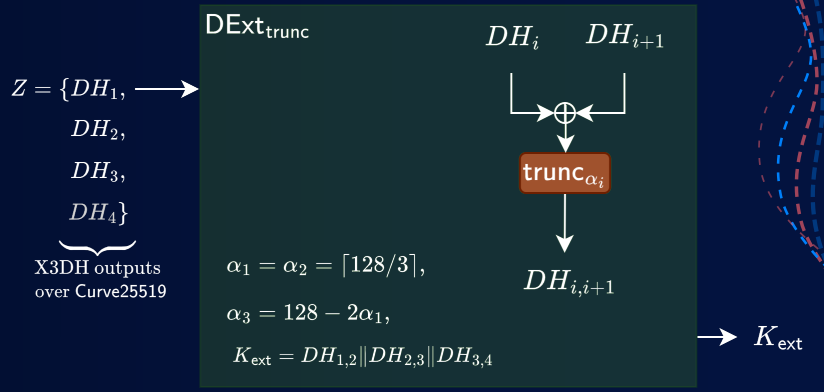
DExt$_f$

- Highly efficient XOR-based extension
- Used to strengthen weak source-specific extractors *f*
- For DH sources, *f* can be simply truncation
- Truncating 256-bit DH element to 82 bits ➔ 82-bit security[2]
- DExt$_f$ improves to 128 bits with 128-bit security

[2]Chevalier C., et al., "Optimal Randomness Extraction from a Diffie-Hellman Element", EUROCRYPT 2009.

DExt$_f$

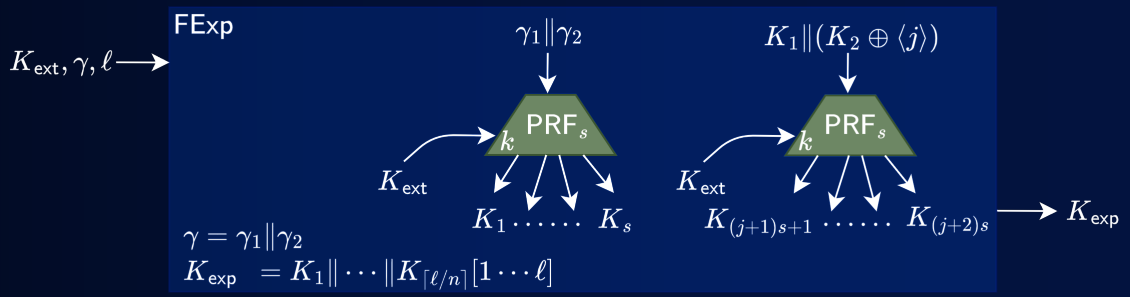
- Highly efficient XOR-based extension
- Used to strengthen weak source-specific extractors *f*
- For DH sources, *f* can be simply truncation
- Truncating 256-bit DH element to 82 bits ➔ 82-bit security[2]
- DExt$_f$ improves to 128 bits with 128-bit security



[2]Chevalier C., et al., "Optimal Randomness Extraction from a Diffie-Hellman Element", EUROCRYPT 2009.

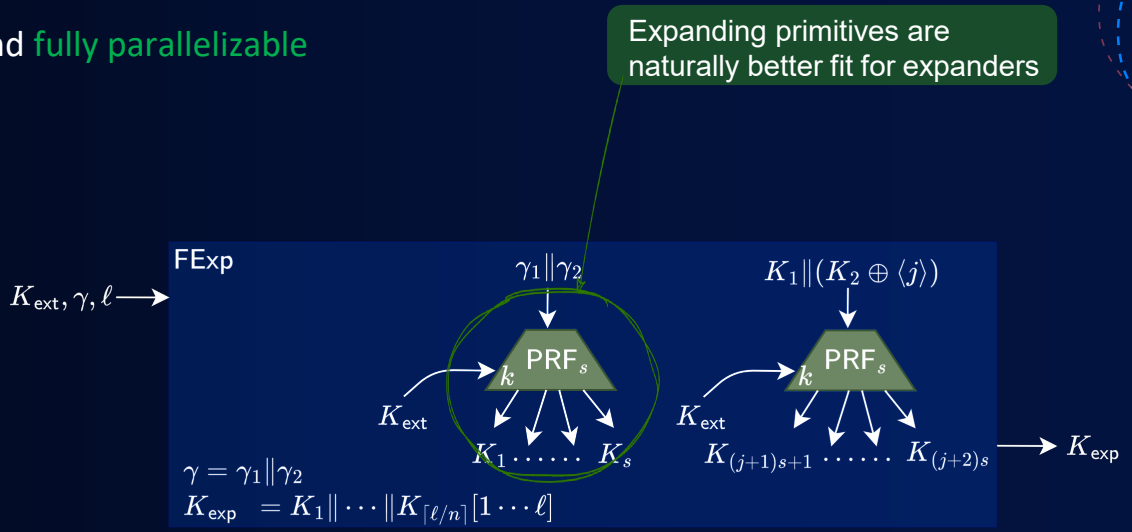
FExp

- A 128-bit provably secure PRF designed for randomness expansion
- Based on expanding primitive and fully parallelizable



FExp

- A 128-bit provably secure PRF designed for randomness expansion
- Based on expanding primitive and fully parallelizable



Skye KDF

- 128-bit secure in same security model as HKDF
- With no RO assumptions
- Instantiated with an AES-based PRF – ButterKnife[3] (expansion rate 4)

[3]Andreeva, E., et al. "Masked Iterate-Fork-Iterate: A New Design Paradigm for Tweakable Expanding Pseudorandom Function.", ACNS 2024.

Benchmarking Setup

- Skye and HKDF are implemented in Rust
- System used: x86_64, AMD Ryzen 7 5800X CPU
- Instruction sets considered: AES-NI and SHA-NI

Performance Results

In Isolation:

- w/o AES-NI and w/o SHA-NI:

  Skye is at least 4x faster than HKDF

- w/ AES-NI and w/ SHA-NI:

  Skye is at least 11x faster than HKDF

- w/ AES-NI and w/o SHA-NI:

  Skye is at least 47x faster than HKDF

Performance Results

Within Signal: (a) Unidirectional Messaging

- w/o AES-NI and w/o SHA-NI:

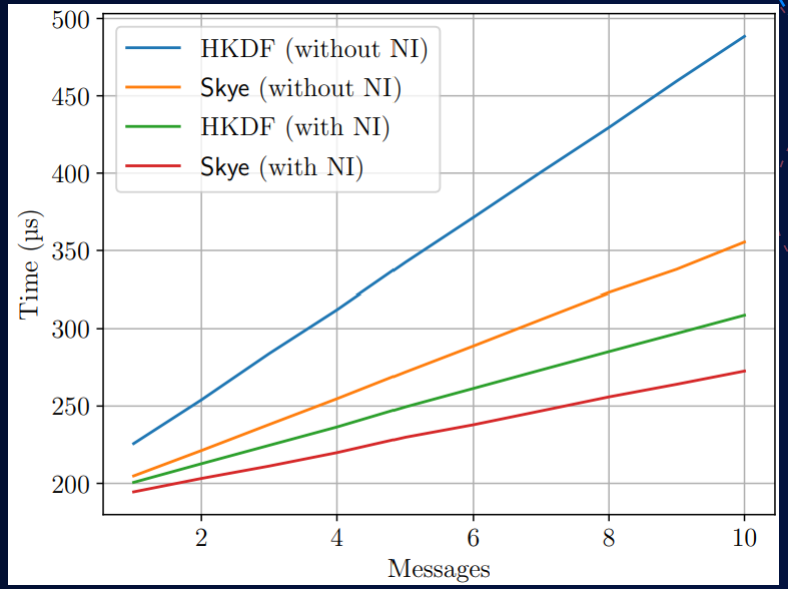
  Skye is 47% faster than HKDF

- w/ AES-NI and w/ SHA-NI:

  Skye is 38% faster than HKDF

- w/ AES-NI and w/o SHA-NI:

  Skye is 64% faster than HKDF



Performance Results

Within Signal: (b) Bidirectional Messaging

- w/o AES-NI and w/o SHA-NI:

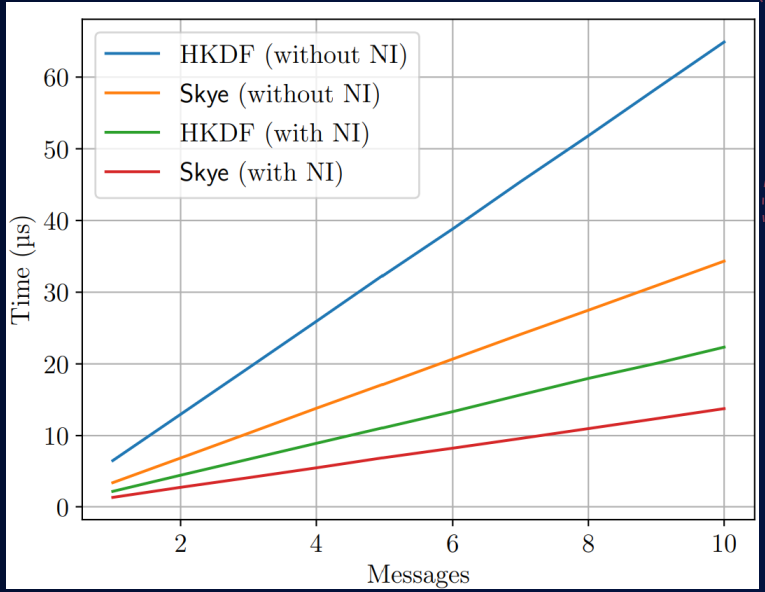
  Skye is 9-27% faster than HKDF for 1-10 messages

- w/ AES-NI and w/ SHA-NI:

  Skye is 3-12% faster than HKDF for 1-10 messages

- w/ AES-NI and w/o SHA-NI:

  Skye is 11-36% faster than HKDF for 1-10 messages



Performance Results

Within Signal: (b) Bidirectional Messaging

- w/o AES-NI and w/o SHA-NI:

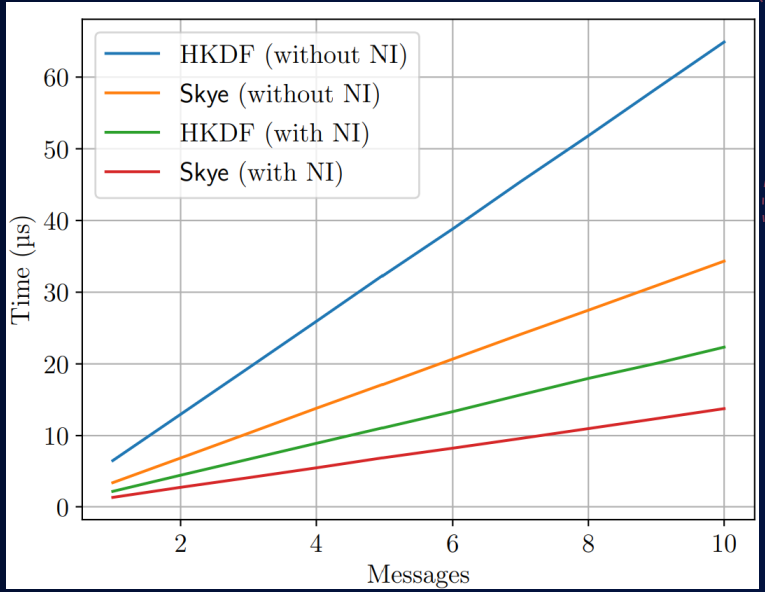
  Skye is 9-27% faster than HKDF for 1-10 messages

- w/ AES-NI and w/ SHA-NI:

  Skye is 3-12% faster than HKDF for 1-10 messages

- w/ AES-NI and w/o SHA-NI:

  Skye is 11-36% faster than HKDF for 1-10 messages



- The percentages converges to unidirectional case for increasing messages

Implications (in Signal)

- Expanding PRF ➔ 78% of the gains
- No extraction in KDF2 and KDF3 ➔ 22% of the gains

Implications (in Signal)

- Expanding PRF ➔ 78% of the gains
- No extraction in KDF2 and KDF3 ➔ 22% of the gains
- Reduced computation ➔ reduced energy consumption
- Highly beneficial for resource-constraint hardware e.g., IoTs and WSNs

Future Directions: Skye beyond Signal

- Skye based on generic extension DExt_f
- Not limited to Curve25519 points or DH sources
- With suitable weak extractor f, can be used in MLS and PQ-Signal protocols
- Finding relevant weak extractors is an interesting future work

Thank You!



(ePrint version)

Contact: Amitsingh.bhati@esat.kuleuven.be

Template Credits: Slidesgo and Freepik
Skye Cartoon: Karllthorn and Deviantart