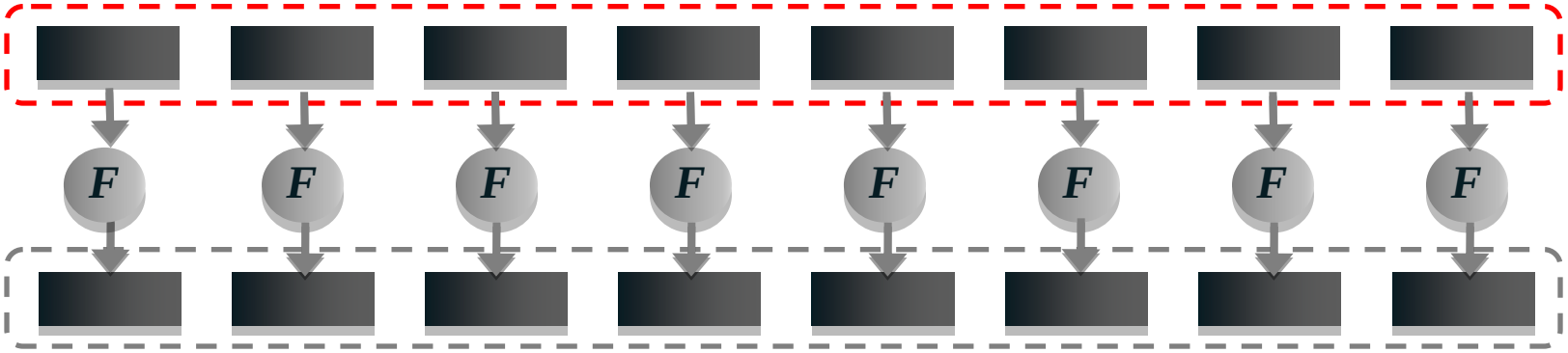
Compact asymmetric authentication using hash-based signatures

David McGrew, Cisco Fellow

mcgrew@cisco.com

Key Generation

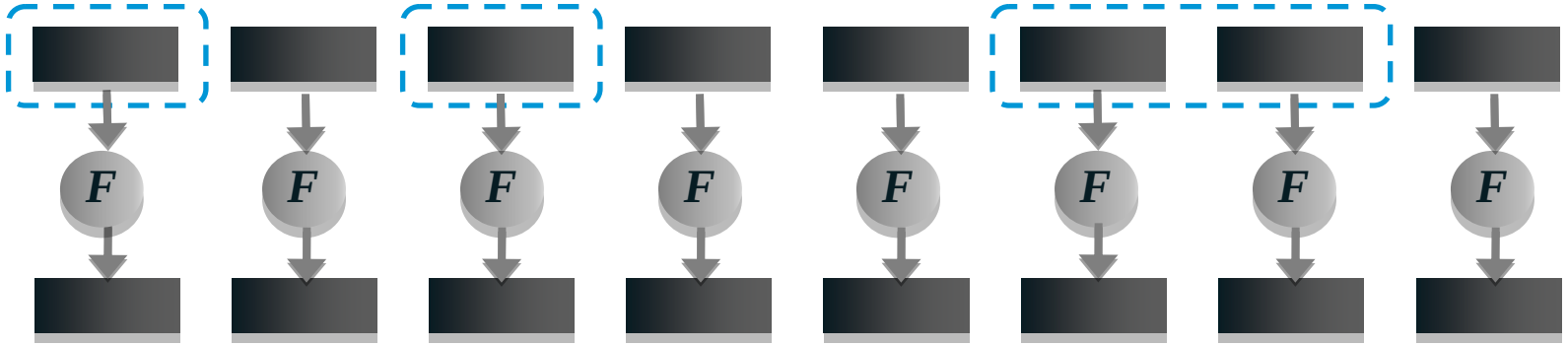
Private Key



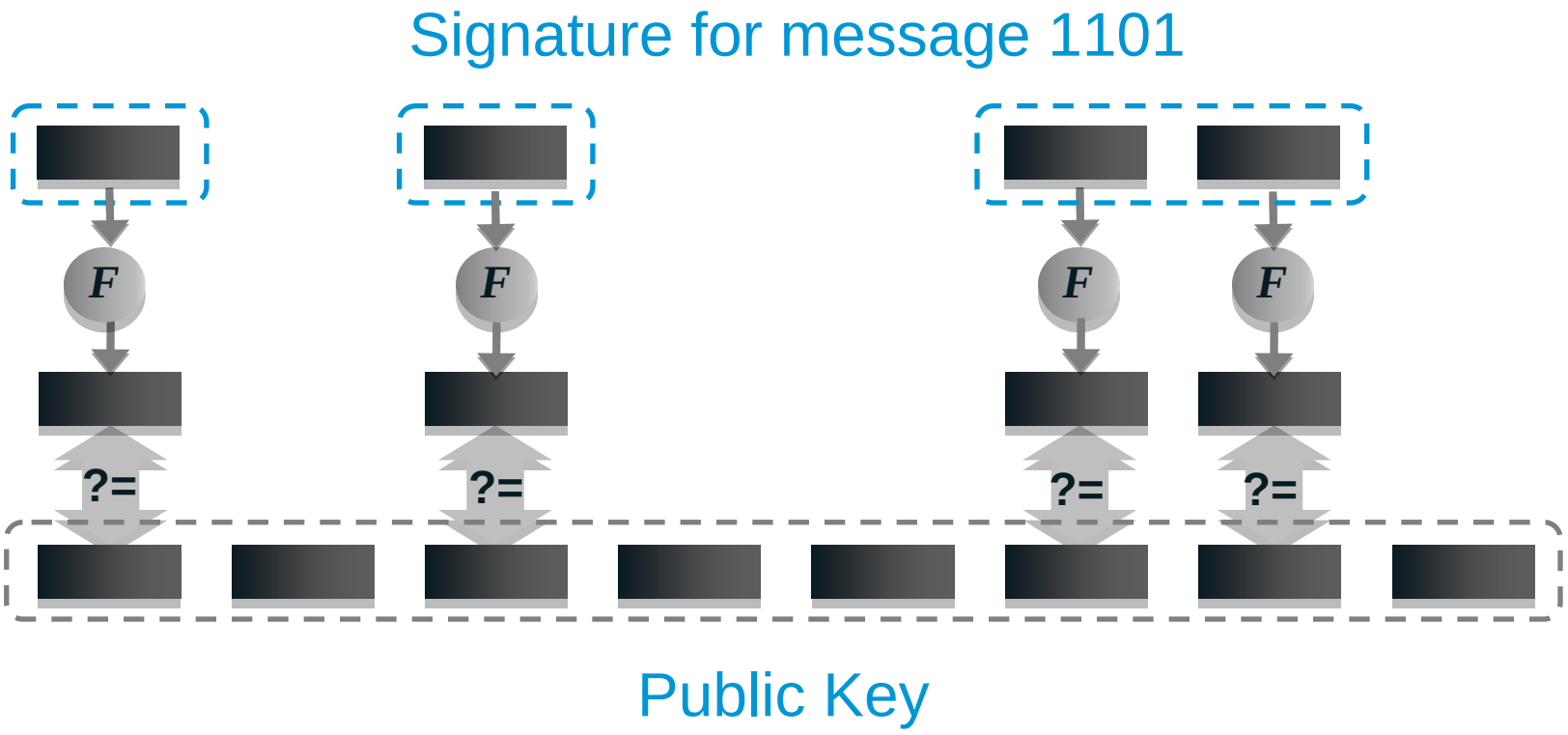
Public Key

Signature Generation

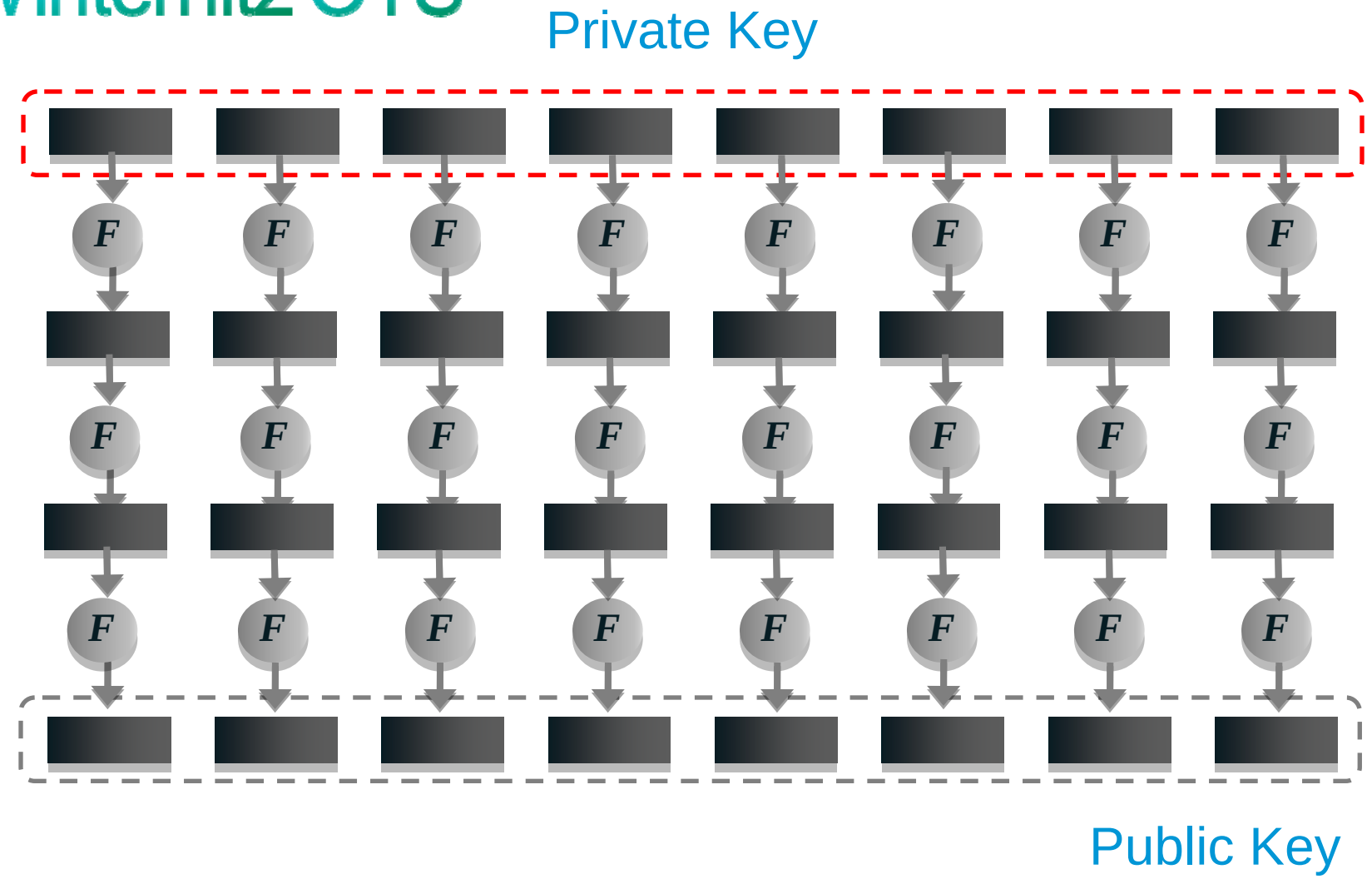
Signature for message 1101



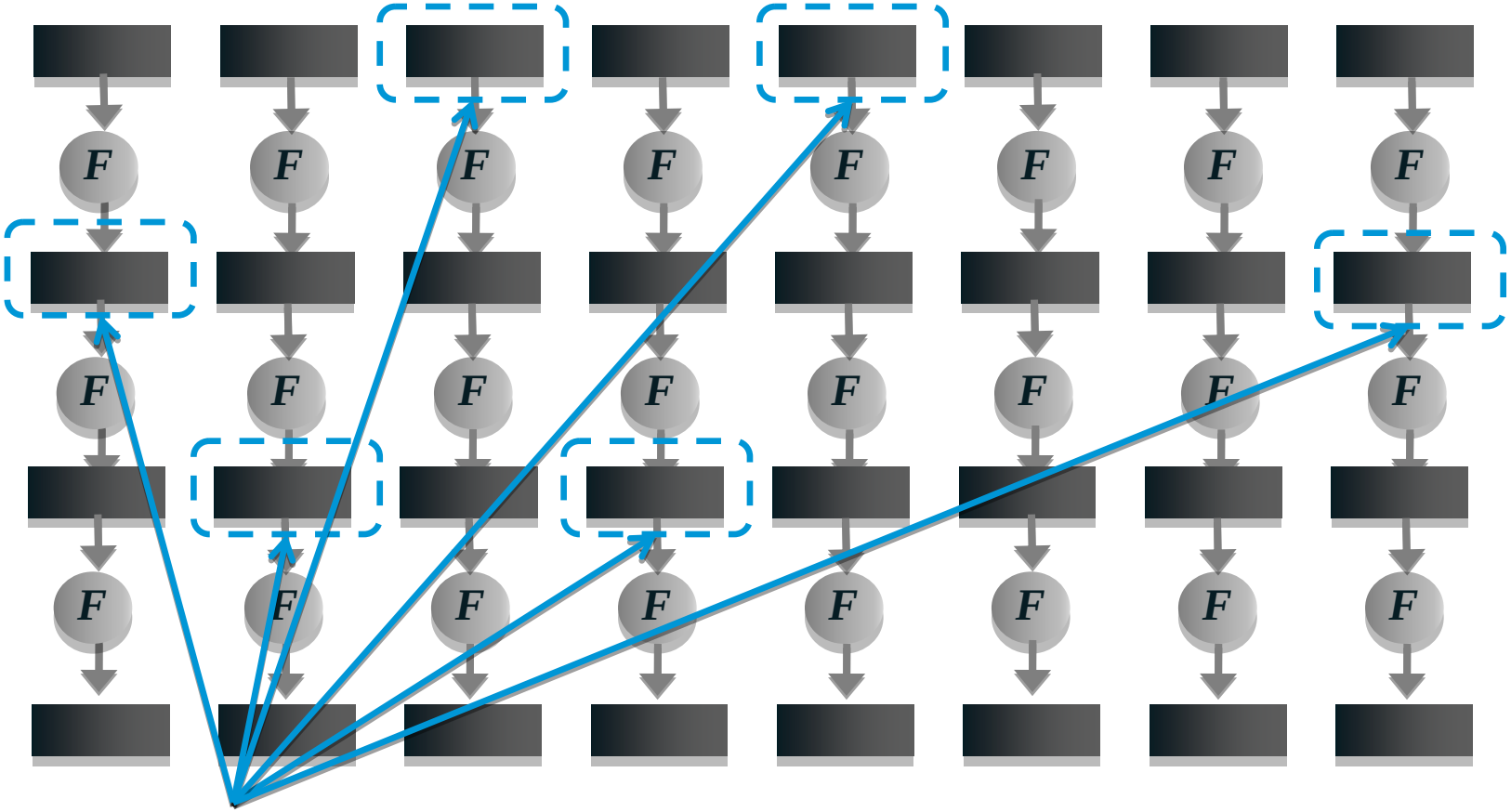
Signature Verification



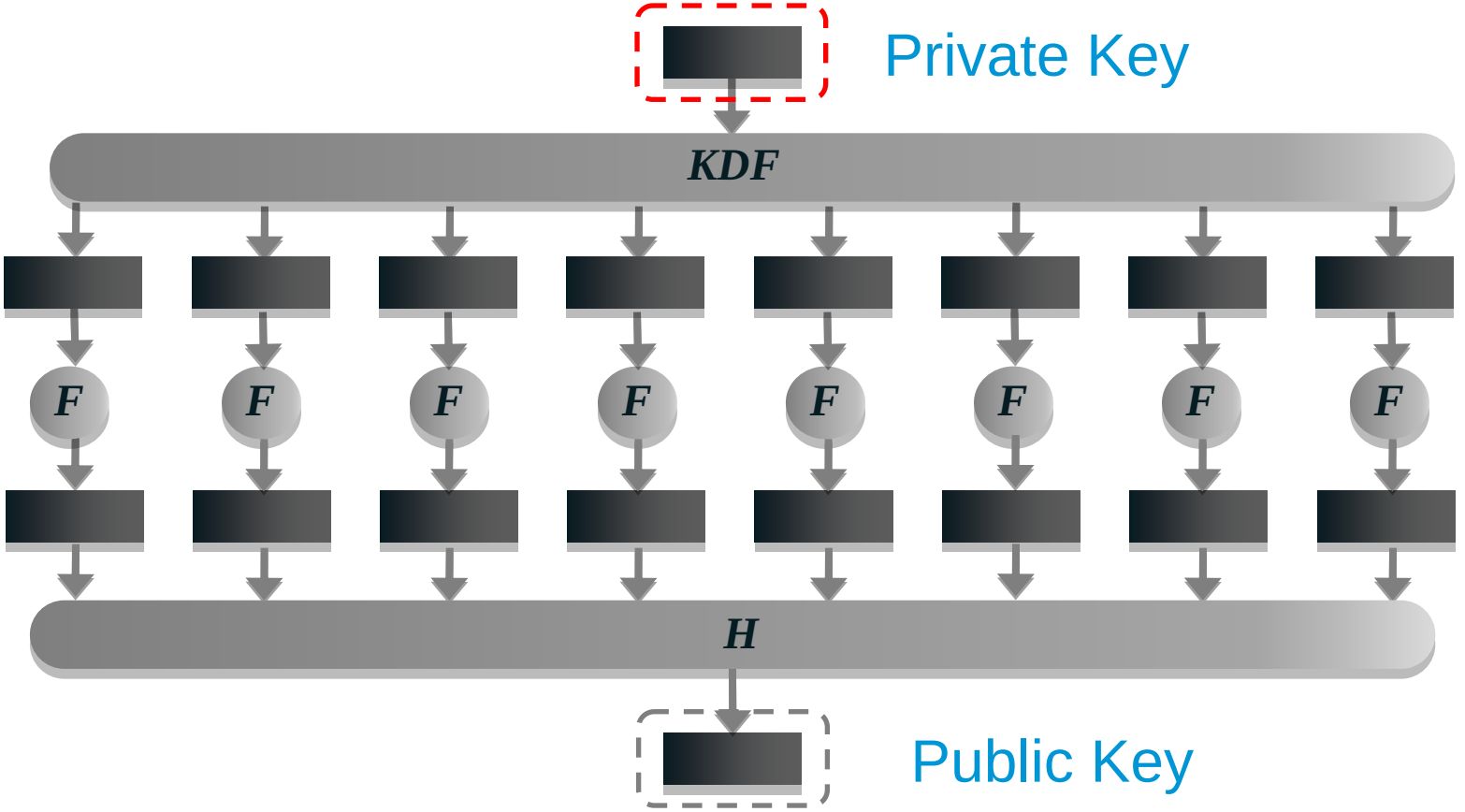
Winternitz OTS



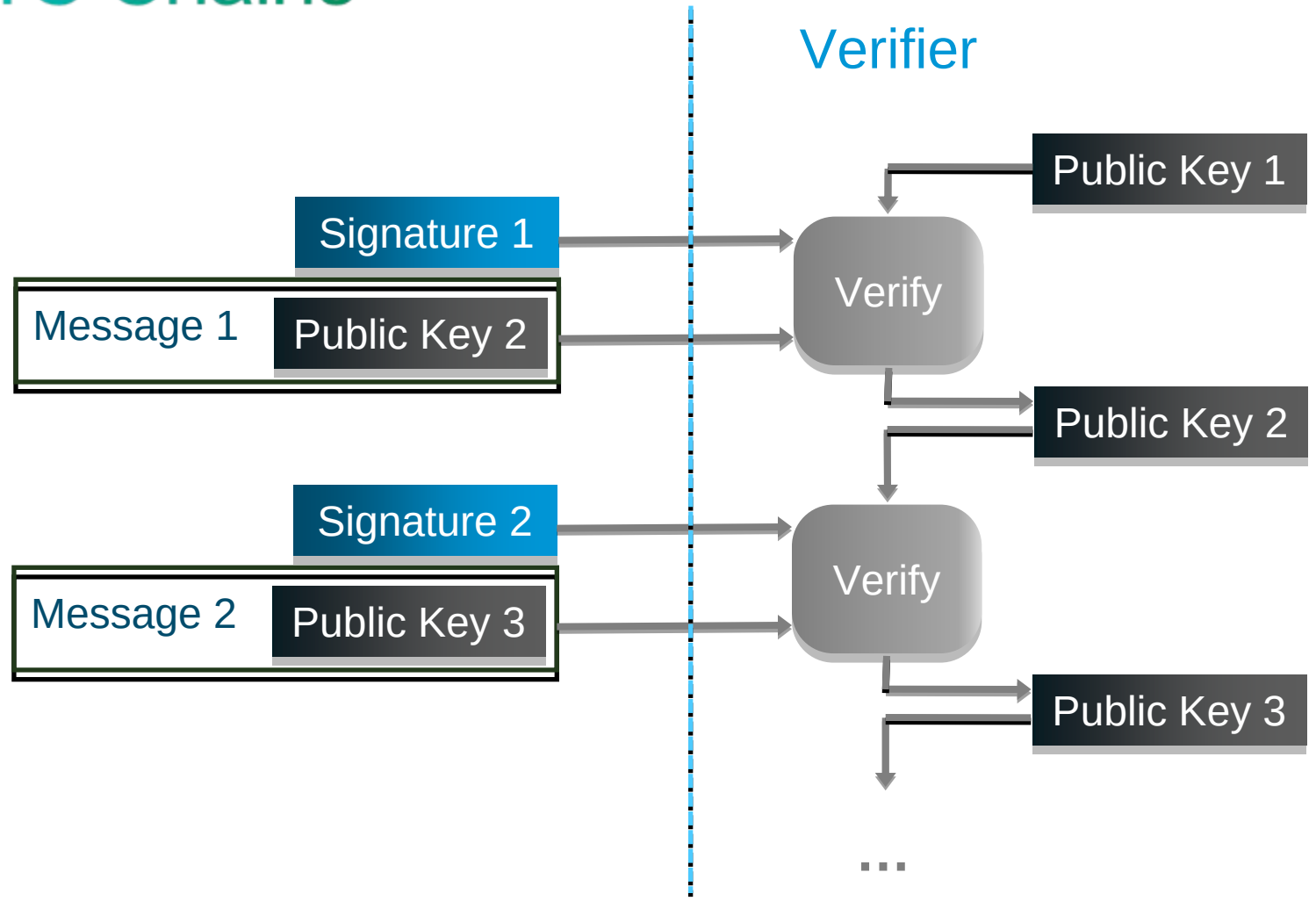
Winternitz OTS



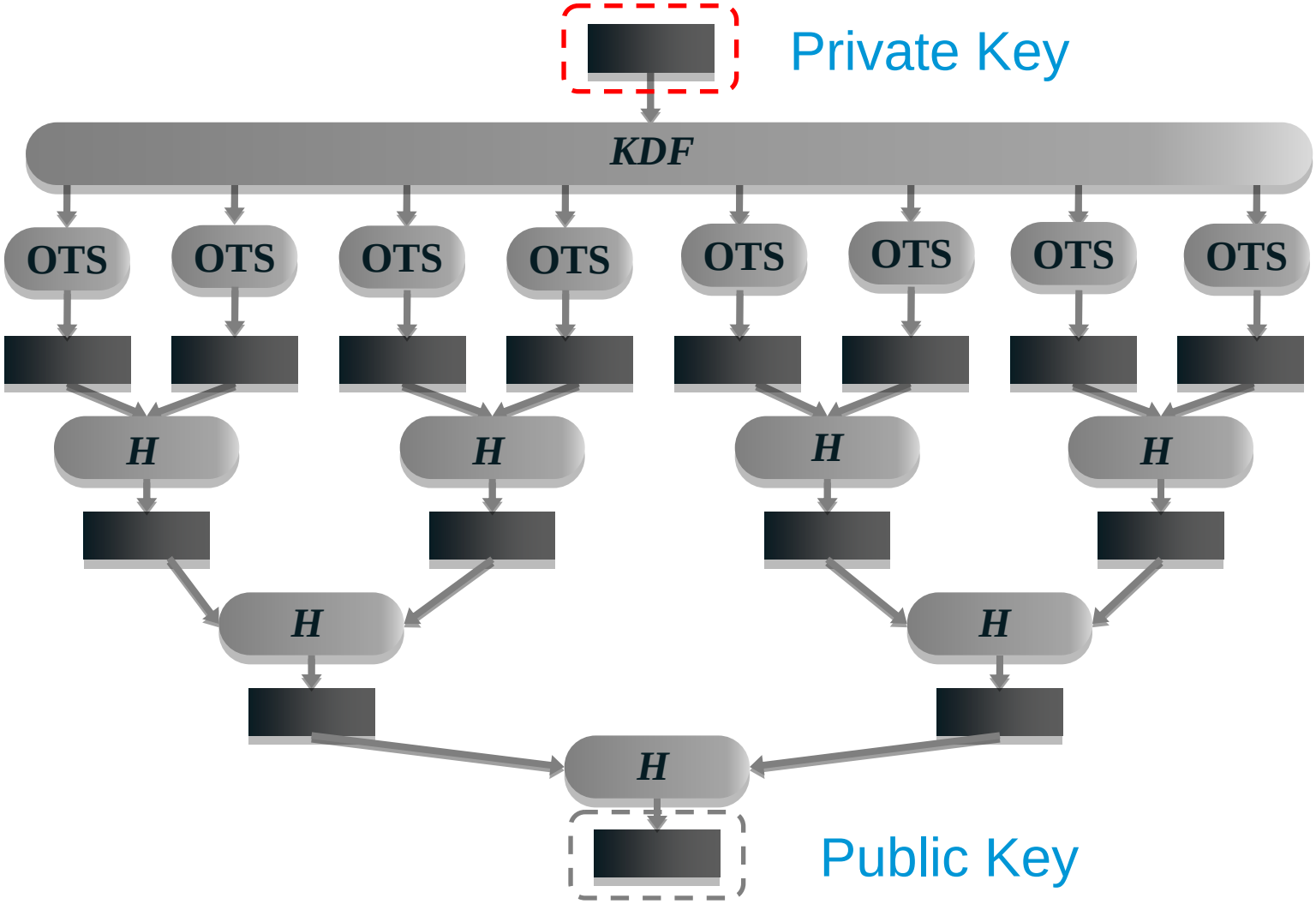
Merkle (‘80) OTS



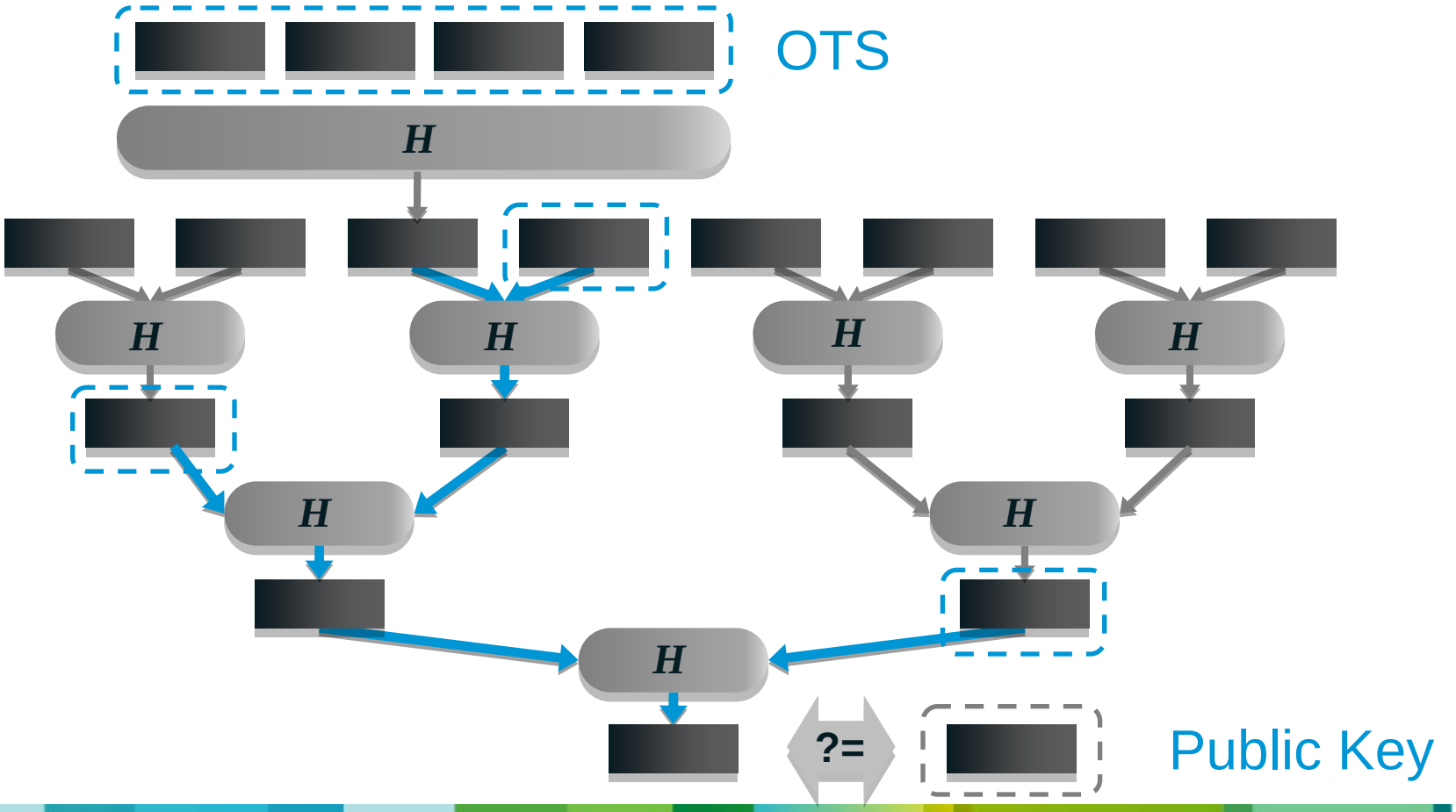
OTS Chains



Merkle Tree Key Generation



Merkle Tree Signature



Security

- Transparent security properties
- Requirements
  - ***H*** must be collision-resistant
  - ***F*** must be pseudorandom (preimage resistant)
- Analyses
  - *The Provable Security of Graph-Based One-Time Signatures and Extensions to Algebraic Signature Schemes* [Hevia, Micciancio '02]
  - *On the Security of the Winternitz One-Time Signature Scheme* [Buchmann, Dahmen, Ereth, Hulsing, Ruckert, '11]
- Post-Quantum Security
  - Unique strength

Summary

- Lamport, Winternitz, Merkle
  - Private key ~ 128 bits
  - Public key ~ 256 bits
  - Signatures ~ 860+ bytes
  - Key generation ~ 1 second (to sign 10^6 messages)
  - Signature generation - fast
  - Signature verification – fast
- Two levels of signatures
  - Double sizes of signatures and keys, double verification time
  - Number of signatures increases to 10^{12}
  - *CMSS - An Improved Merkle Signature Scheme* [Buchmann, Garcıa, Dahmen, Doring, Klintsevich ’06]

Energy Usage

- *Power Consumption Evaluation of Efficient Digital Signature Schemes for Low Power Devices* [Seys and Preneel, ’06]

Communication cost of MTS ~ 10-100x **worse** that of ECDSA

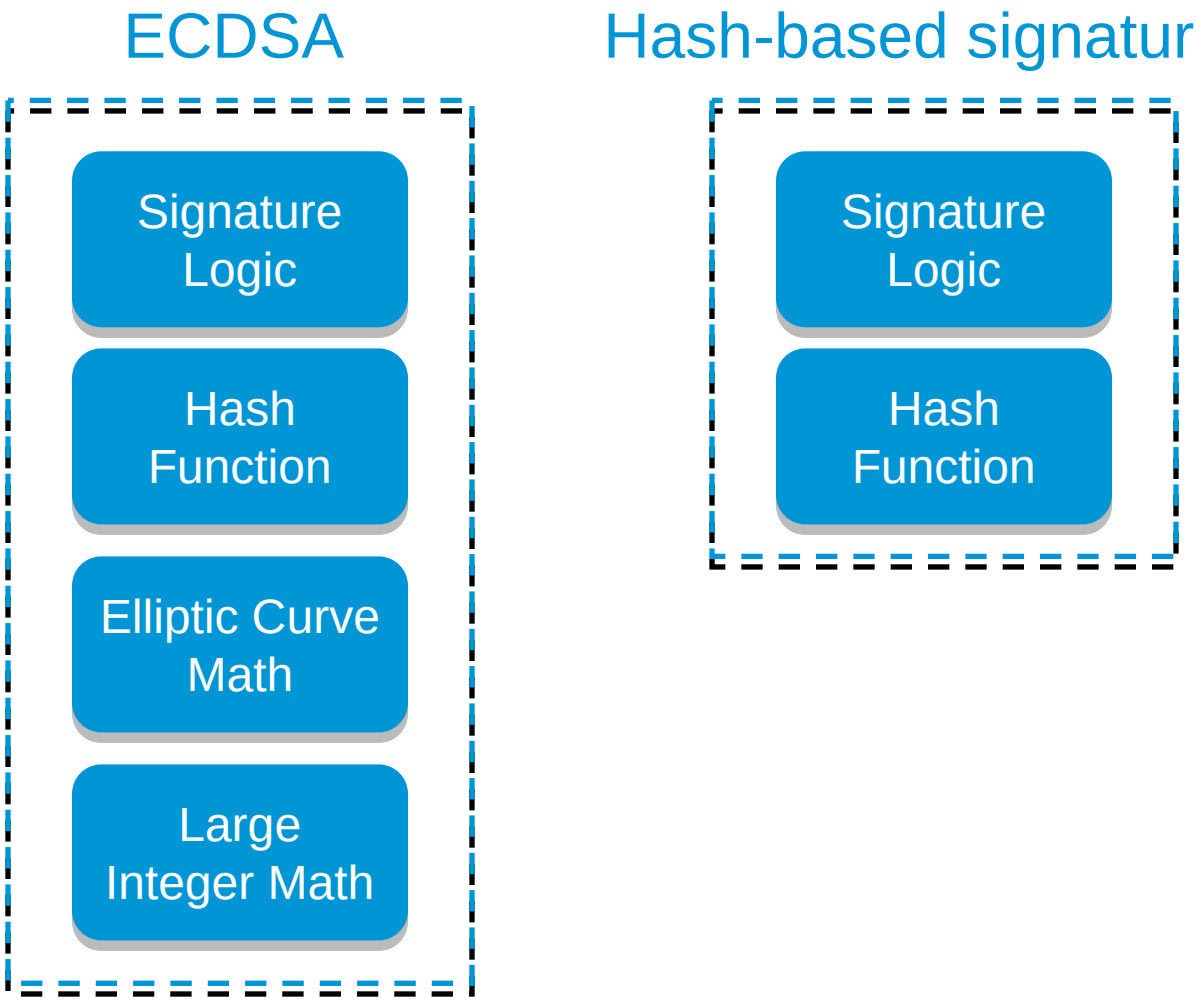
Energy cost of MTS **verification**~ 30x **better** than ECDSA

Energy cost of MTS **signature generation about the same** as ECDSA

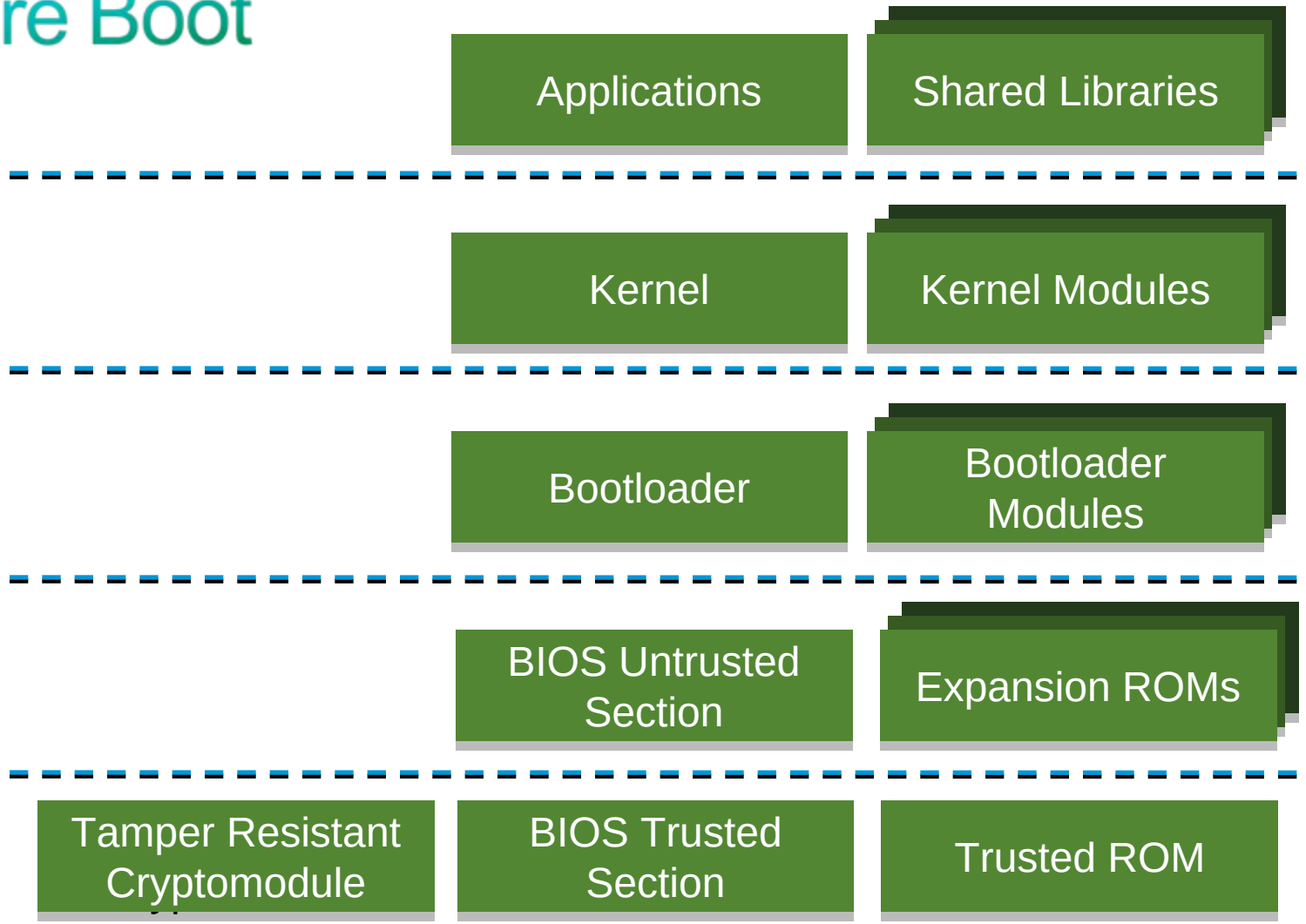
But MTS efficiency goes down as number of signatures increases

Conclusion: ECDSA 2-7x less efficient, but easier to manage

Implementation Compactness



Secure Boot

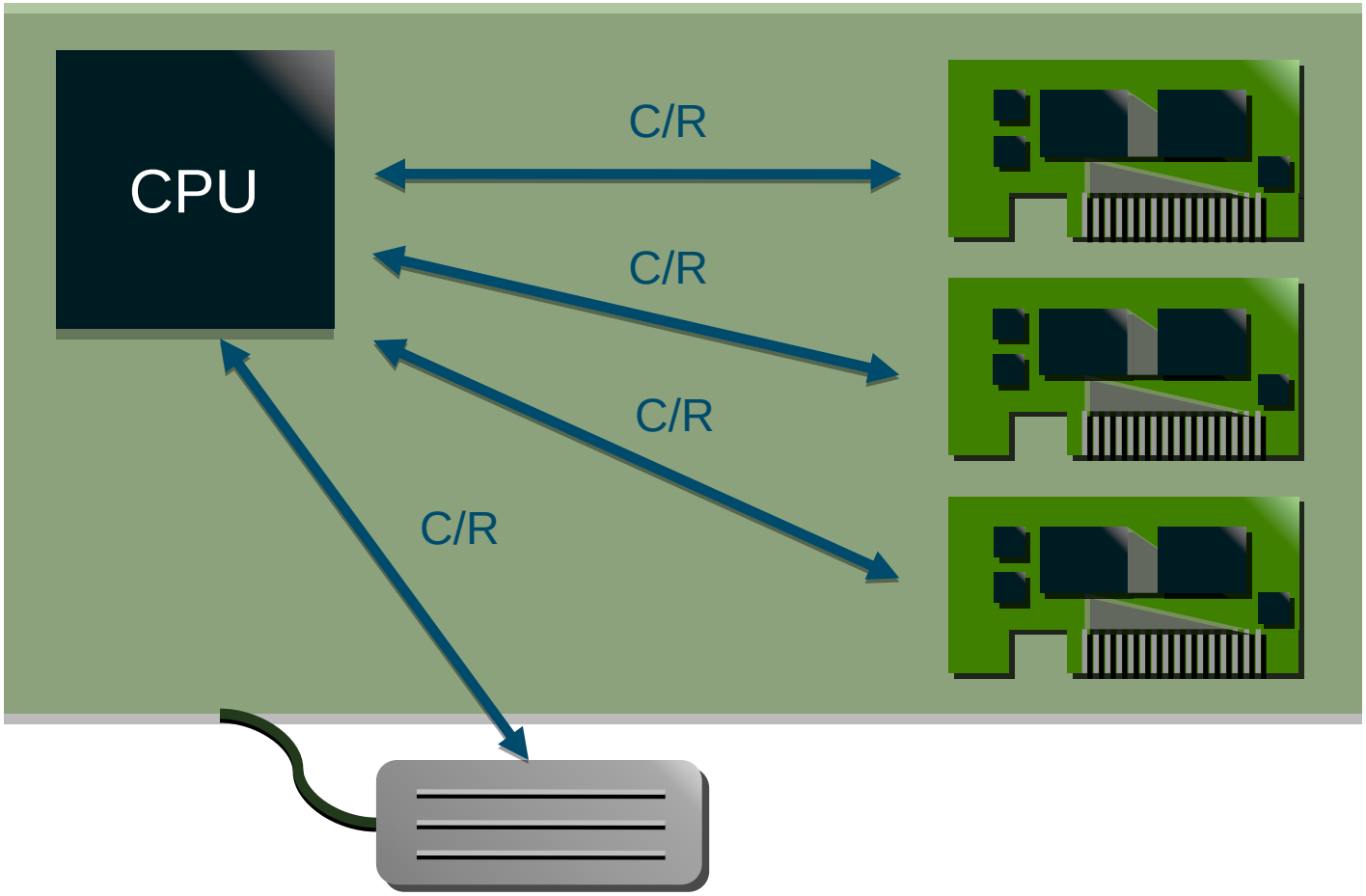


Executable sizes on linux-2.6

	Size (Bytes)			Count
	Average	Min	Max	
GRUB module	6,706	690	98,304	168
Kernel module	35,968	3,272	1,179,608	2499
/sbin	50,356	333	756,784	123
/bin	58,747	63	926,536	101
/usr/sbin	42,362	64	828,304	229
/lib/*.so*	120,266	3,704	1,432,968	80
/usr/lib/*.so*	541,390	218	49,214,336	850
Kernel	2,420,384			

Source: debian vmlinuz-2.6.32-5-amd64

Secure Hardware Systems



Standards

	Compact Implementation	Fast Implementation
H	SHA-2	SHA-2
F	SHA-2	AES
KDF	SP 800-108 with SHA-2	SP 800-108 with AES

- Flexible signature format, with minimal mandatory-to-implement
- X.509/PKIX specification
  - But ASN.1 should not be used for signature format
  - Compact implementations benefit from uniformity (e.g. no RSA signatures)

Conclusions

- Hash-based signatures can be valuable for authenticating trusted systems software and hardware components
- Attractive and well-understood security properties
- Good fit into standards
- May be useful in other areas
  - Low-power wireless

Thank you.