ASIC-Resistant Proof of Work based on PowerAnalysis of Low-end Microcontrollers

ASIC

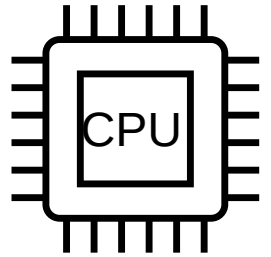
ASIC **특정한 목적에** 적합하게 설계된 주문형 반도체

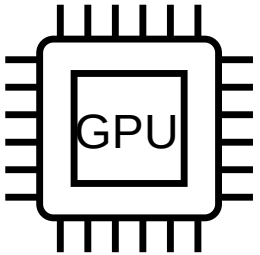
일반 하드웨어보다 훨씬 효율적으로
암호 화폐를 채굴

일반 채굴자의 참여를 방해

**네트워크
안정성 보안 손상**

x10,000





ASIC 저항 알고리즘

2 ~ 3 YEAR

	알고리즘	도입	AISC 등장
Bitcoin	SHA-256	2009	2013
Litecoin	Scrypt	2011	2014
Dash	X11	2013	2015
Monero	CryptoNigt	2014	2017
Ethereum	Ethash	2015	2018

ASIC 저항 알고리즘의 기존연구

- 일반 참여자들의 진입장벽을 **낮추어 참여를 높이고** 네트워크의 **안전성과 보안을 높이는 것**을 목표
- ASIC 구현 시 이점을 최소화 하며 **CPU, GPU 기반 상용 컴퓨터**에서 작동

다중 해시	메모리 하드	프로그래밍
연속으로 연결된 다중 해싱	병목 현상을 일으키는	임의의 코드를 실행하여 계산
병렬 처리의 이점을 상쇄	메모리 액세스를 시도	다양성 높여 ASIC 구축 힘듬
Quark, X 계열	Ethash, CryptNight	ProgPoW, RandomX

부채널 분석의 기존 연구

암호 알고리즘이 수행되는 순간에 발생되는 누수 정보로부터
기밀 정보를 식별하는 분석 기법

↓

코드 실행 시 수집되는 **전력 소비를 비교**하여
코드의 저작권을 보호하는 IP 보호 기술이 제안

↓

Microcontroller에서 수행 했다는 근거로 사용

기여

Microcontroller의 소비 전력을 기반으로 한 **새로운 PoW 알고리즘**을 제시

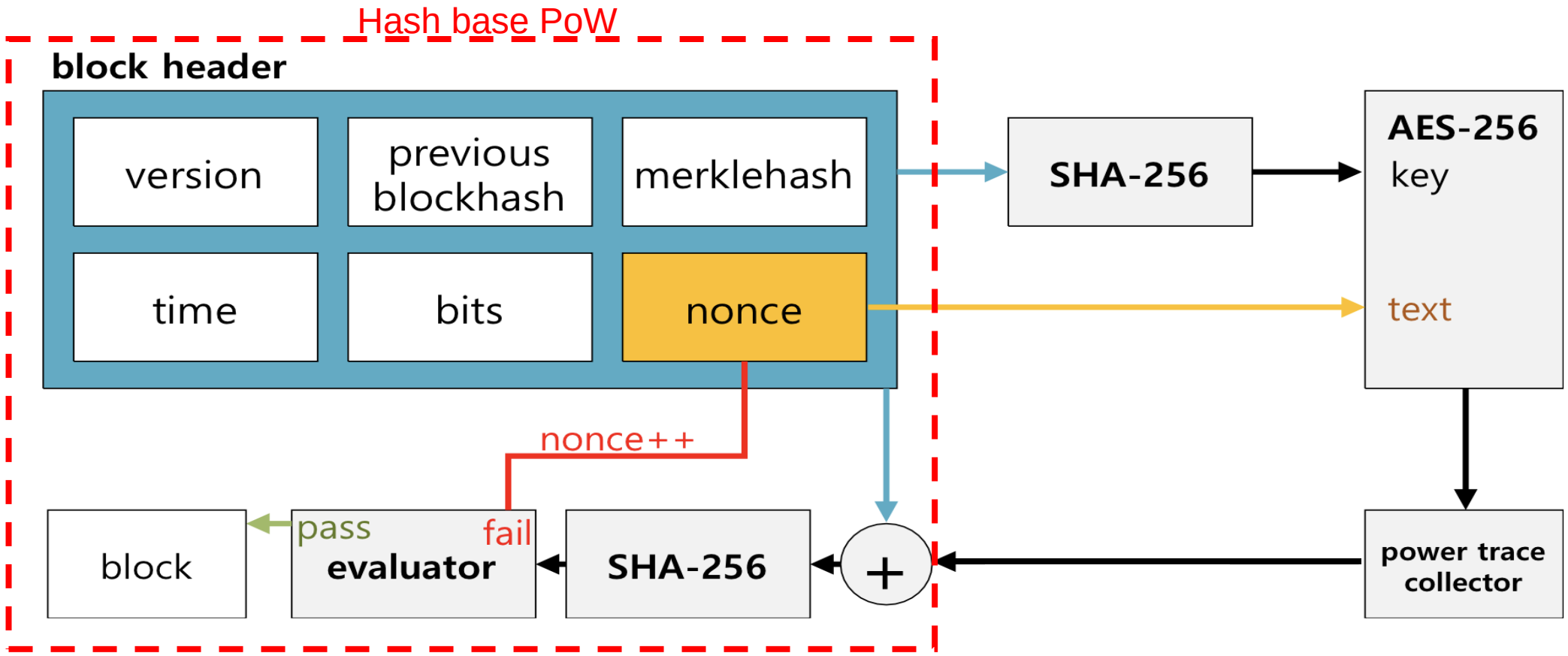
ASIC 이나, GPU, CPU 의 채굴이 아닌, **Microcontroller 특성에 기반** 된 채굴 방식

다양한 블록 암호 기반으로 제안하는 새로운 PoW에 대하여 분석

적은 비용과 저전력에서 동작하기 **때문에 누구나 쉽게 채굴에 참여** 가능

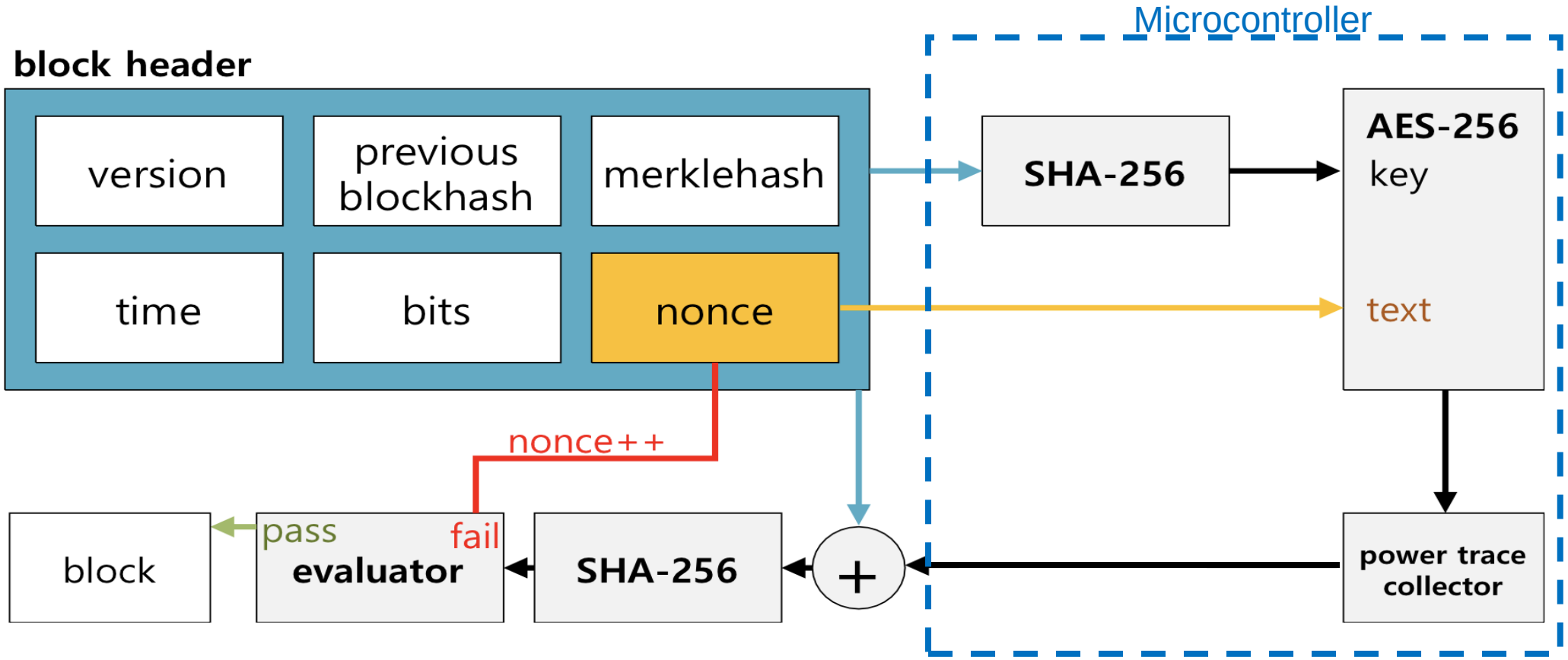
안전한 분산 네트워크 블록체인 형성

블록 생성



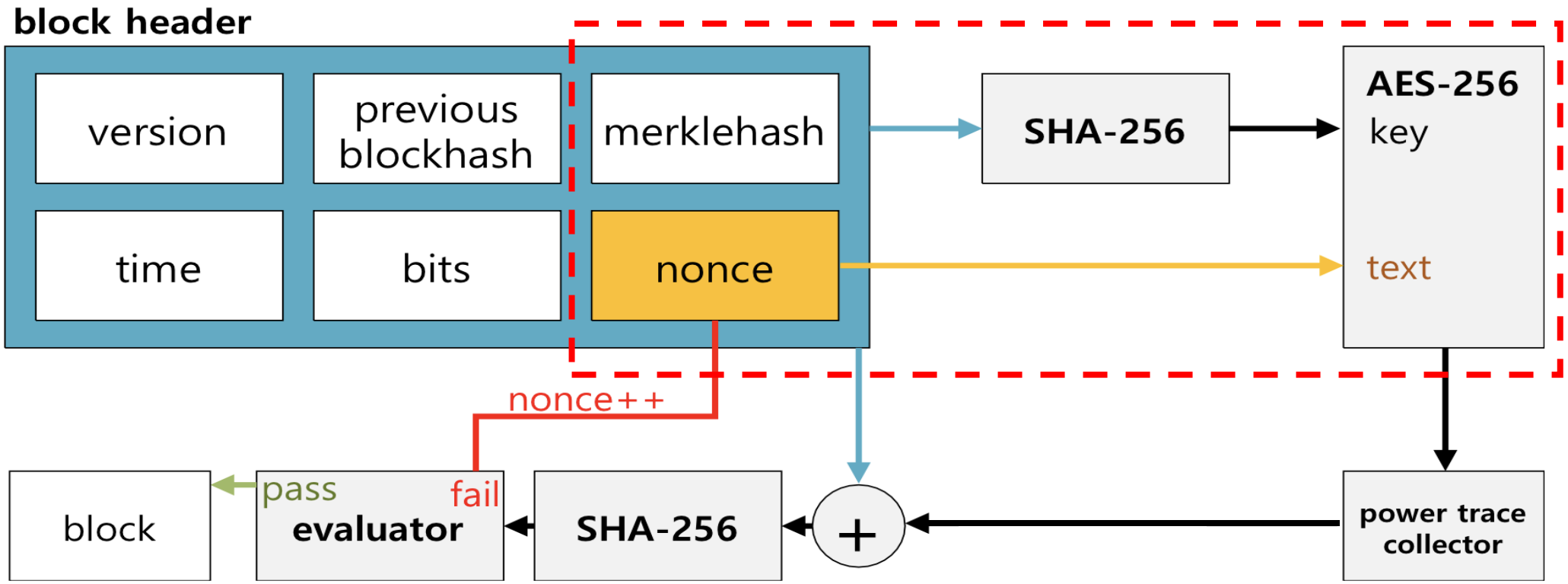
Microcontroller에서 **암호 모듈을 작동**하는 과정 추가

블록 생성



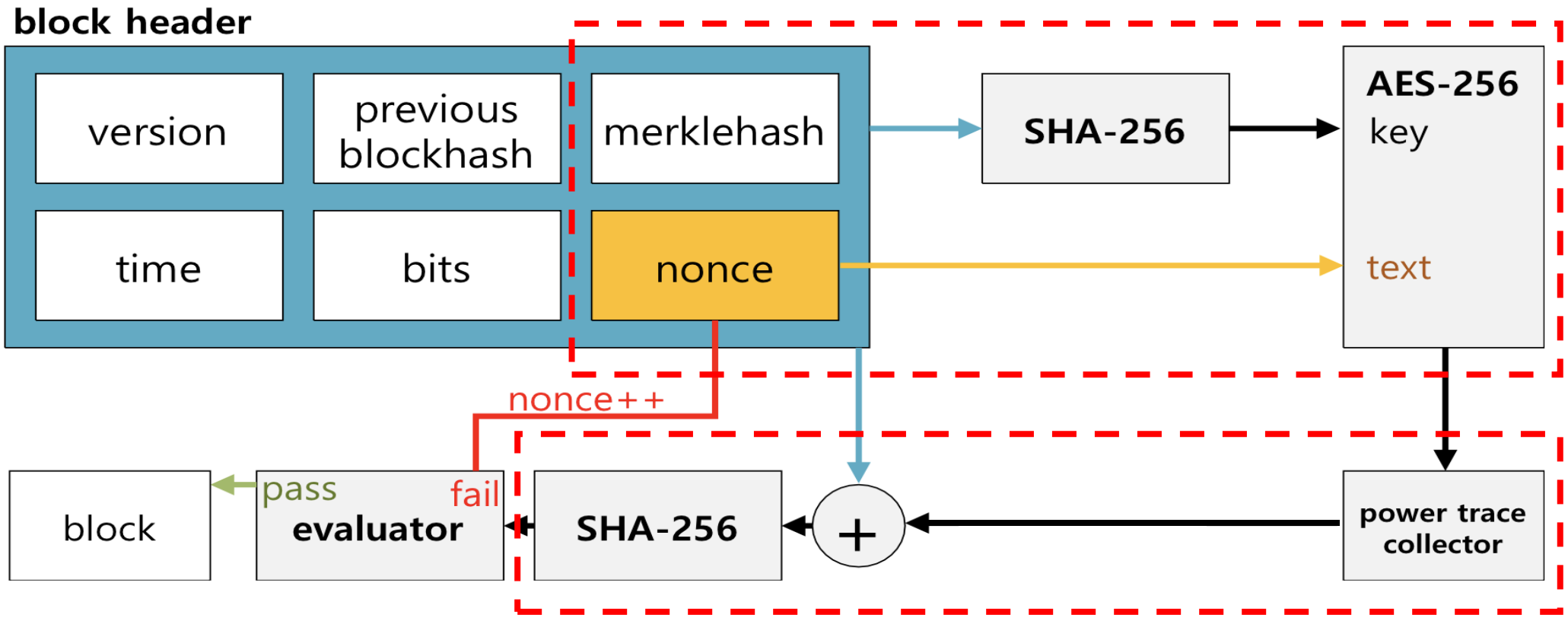
Microcontroller에서 **암호 모듈을 작동**하는 과정 추가

블록 생성



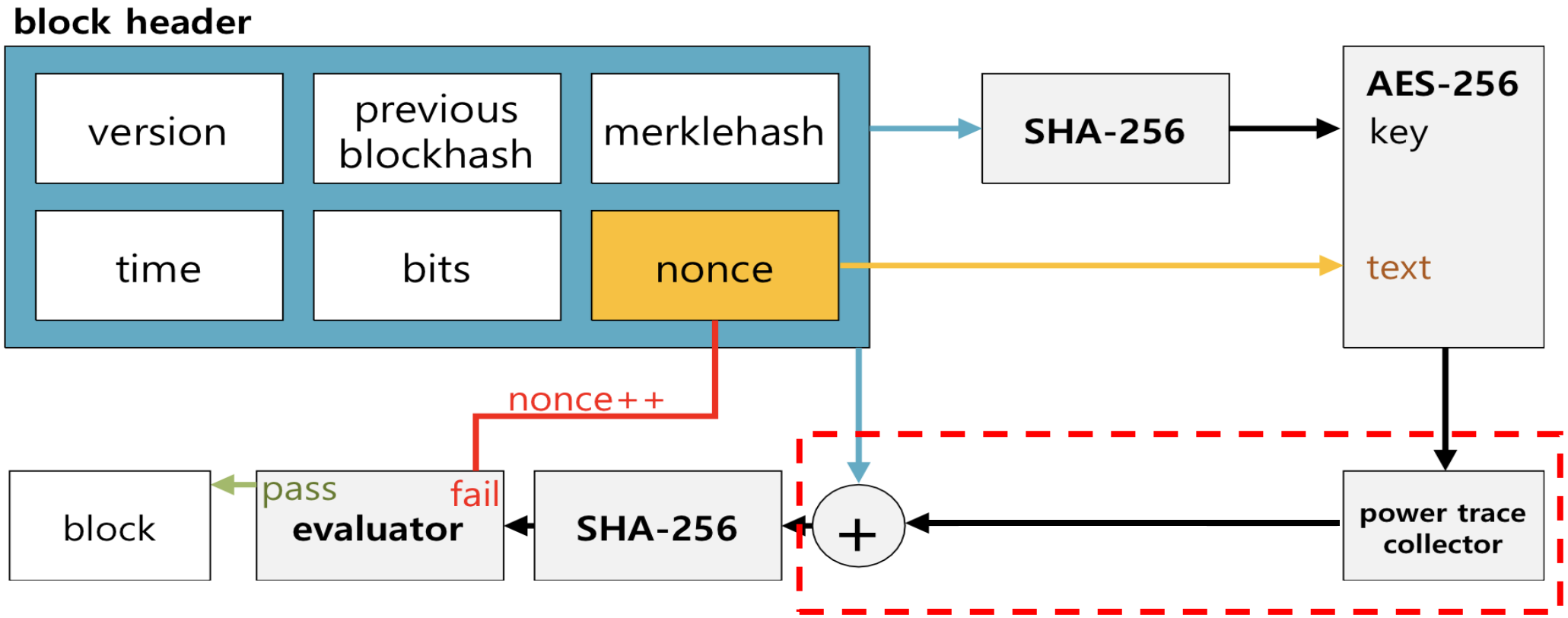
암호 모듈의 입력값은 **블록헤더를 해싱한 값**과 **nonce 값**을 입력으로 사용

블록 생성



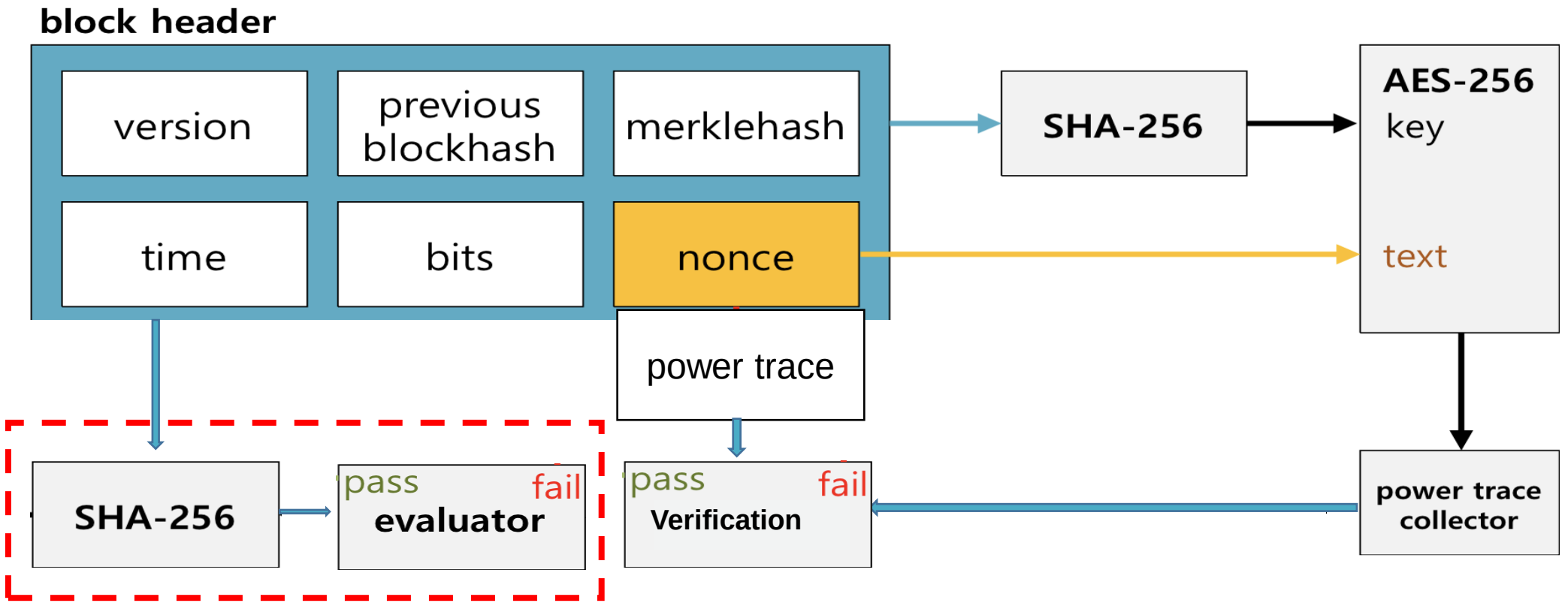
암호모듈의 입력값과 해시연산의 입력값으로 **병렬적인 해시계산을 방해**

블록 생성



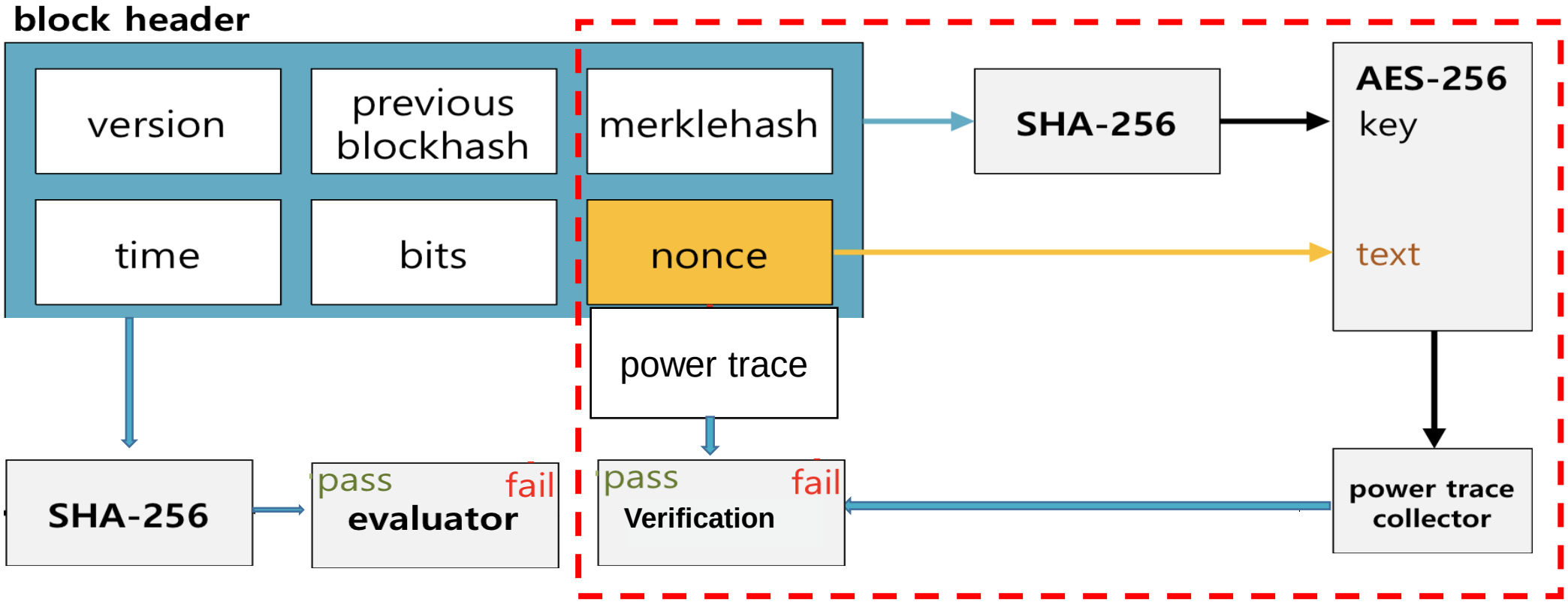
소비 전력 파형은 Microcontroller에서 연산을 **수행한 증거**

검증



블록헤더의 해시 값이 **목표 값 보다 작은** 지 확인

검증



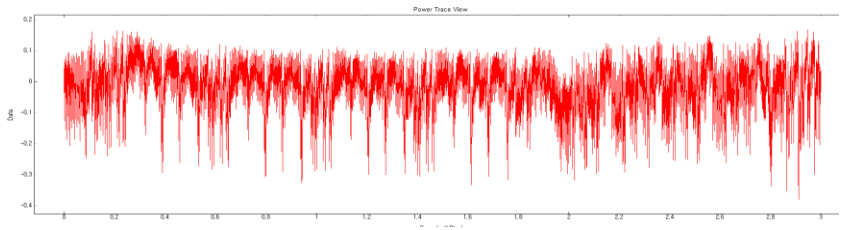
블록 작성자가 **헤더 정보와 동일**한 코드와
입력 값으로 **Microcontroller에서 작업했는지 확인**

소비 전력 파형 검증

1. 검증자는 블록에 저장되어 있는 키 값, 평문 값으로 암호 알고리즘을 수행하였을 때의 소비 전력 파형을 수집

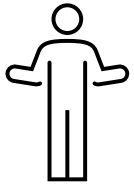
2. 두개의 소비 전력 파형을 상관계수를 계산하여 블록의 유효성을 검증
   - 높은 상관계수를 나타날 경우 통과

채굴자

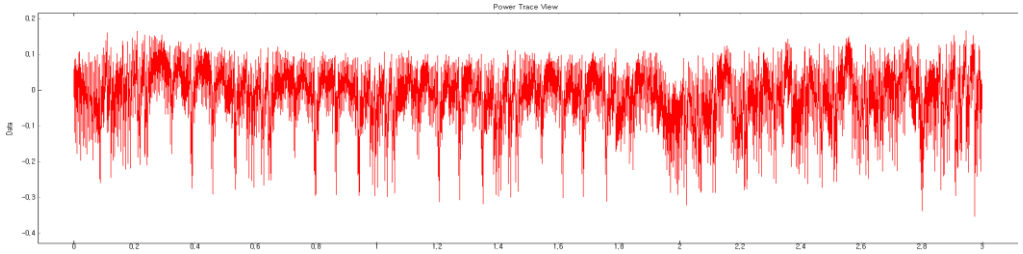


< 블록에 저장되어 있는 파형 정보 >

≠



검증자

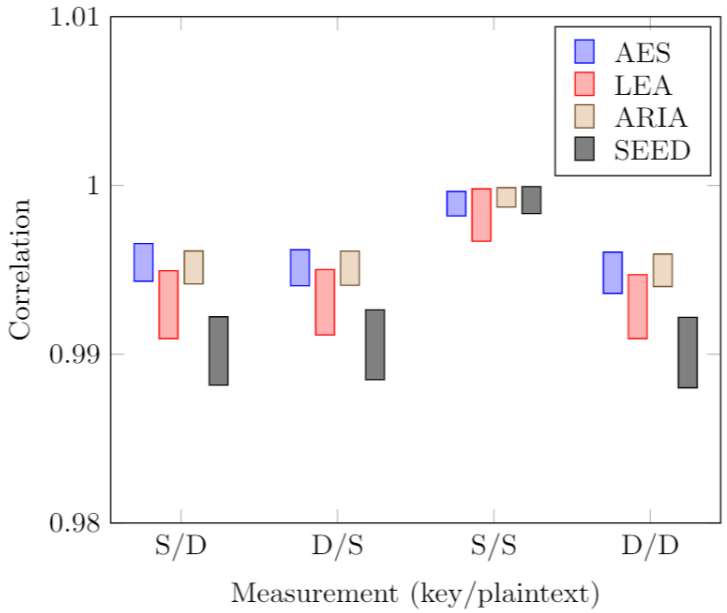


< 블록의 키값, 평문 값으로 수집한 파형정보 >

소비 전력 파형의 개별성

두개의 소비 전력 파형을 상관계수를 계산하여 블록의 유효성을 검증?

같은 입력값에 경우 높은 상관 관계



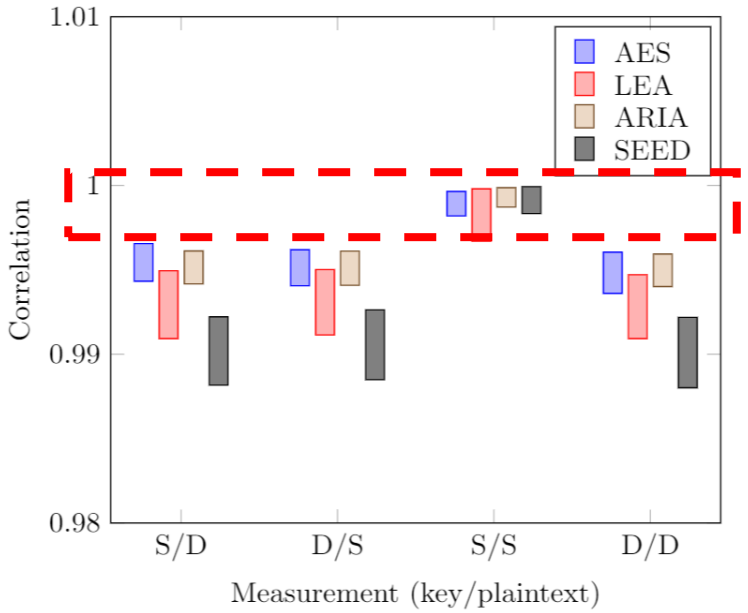
- 실험환경
  - ChipWhispererLite XMEGA
  - 샘플링 속도는 7.38MS
  - C 언어로 작성
  - AVR-GCC로 컴파일

- 같은 평문과 키 / 같은 키, 다른 평문 / 다른 키, 같은 평문 / 키, 평문 모두 다른 경우
- 각각 1,000 개의 수집 그룹 간의 상관 계수 획득
- AES, LEA, ARIA, SEED 대상으로 각각 수행

소비 전력 파형의 개별성

두개의 소비 전력 파형을 상관계수를 계산하여 블록의 유효성을 검증?

같은 입력값에 경우 높은 상관 관계



- 실험환경
  - ChipWhispererLite XMEGA
  - 샘플링 속도는 7.38MS
  - C 언어로 작성
  - AVR-GCC로 컴파일

- 같은 평문과 키 / 같은 키, 다른 평문 / 다른 키, 같은 평문 / 키, 평문 모두 다른 경우
- 각각 1,000 개의 수집 그룹 간의 상관 계수 획득
- AES, LEA, ARIA, SEED 대상으로 각각 수행

상용 컴퓨터 상에서의 비효율

최적화 할 수 있는 유일한 방법은 해시 알고리즘을 빠르게 계산

Processor	DMIPS	Speed ratio	Efficiency
Atmega128	32	1:1	0%
Raspberry Pi			
ARM 1176	850	1:26.6	93%
Cortex-A7	1500	1:46.9	97%
Cortex-A53	3500	1:109	98%
Commercial PC			
Phenom II	12000	1:375	99.5%
Core i7 930	16500	1:516	99.6%
Core i7 4820K	23600	1:738	99.7%

- 암호모듈과 해시 작업을 수행 장치가 **동일한 작업을 수행**한다고 가정
- Microcontroller 장치 보다 크게 **효율적이지 않음**
- **채굴자**들은 더 저렴한 **Microcontroller 장치를 사용** 할 것

다른 ASIC 저항 알고리즘과 비교

Method	ASIC Development	Low-end IoT
Multi-hash PoW	Possible	-
Memory-hard PoW [16]	Possible	-
Memory-bound PoW [27–29]	Possible	-
Programmatic PoW [31, 32]	Possible	-
This work (Power-trace PoW)	Partially possible	√

- ASIC로 **부분적으로 구현** 가능

  마이크로컨트롤러 부분을 제외한 ASIC로 해시연산 부분만 부분적으로 구현 가능하나 큰 효율을 내지 못함

- Microcontroller 장치를 위한 **최초의 PoW 방법**

결론

전력 분석을 기반으로 한 **새로운 ASIC 내성 PoW**

입력 값에 따른 소비 전력의
고유한 특징을 사용 **ASIC 저항 달성**

결론

IoT에 사용되는 Low-end Microcontrollers 대상

ASIC 저항성

일반 채굴자의 접근성 증가

블록체인의 **분산화에 기여**

Q & A

S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

G. Woodet al., “Ethereum: A secure decentralised generalised transaction ledger,”Ethereum project yellow paper, vol. 151, no. 2014, pp. 1–32, 2014.

S. Noether and A. Mackenzie, “Ring confidential transactions,” vol. 1, pp. 1–18,2016.

C. Dwork and M. Naor, “Pricing via processing or combatting junk mail,” inAnnual International Cryptology Conference, pp. 139–147, Springer, 1992.5. J.-Y. Cai, R. J. Lipton, R. Sedgewick, and A.-C. Yao, “Towards uncheatable bench-marks,” in[1993] Proceedings of the Eigth Annual Structure in Complexity TheoryConference, pp. 2–11, IEEE, 1993.

V. Buterin, “Dagger: A memory-hard to compute, memory-easy to verify scryptalternative,” tech. rep., Technical Report, 2013. URL http://www. hashcash.org/papers/dagger. html, 2013.

P. Kocher, J. Jaffe, and B. Jun, “Differential power analysis,” inAnnual Interna-tional Cryptology Conference, pp. 388–397, Springer, 1999.

F. Durvaux, B. Gerard, and S. Kerckhof, “Intellectual property protection forintegrated systems using soft physical hash functions,” inInternational Workshopon Information Security Applications, pp. 208–225, Springer, 2012.

P. Samarin and K. Lemke-Rust, “Detecting similar code segments through sidechannel leakage in microcontrollers,” inInternational Conference on InformationSecurity and Cryptology, pp. 155–174, Springer, 2017.

D. Kwon, J. Kim, S. Park, S. H. Sung, Y. Sohn, J. H. Song, Y. Yeom, E.-J. Yoon,S. Lee, J. Lee,et al., “New block cipher: ARIA,” inInternational Conference onInformation Security and Cryptology, pp. 432–445, Springer, 2003.

D. Hong, J.-K. Lee, D.-C. Kim, D. Kwon, K. H. Ryu, and D.-G. Lee, “LEA: A128-bit block cipher for fast encryption on common processors,” inInternationalWorkshop on Information Security Applications, pp. 3–27, Springer, 2013.

J. Park, S. Lee, J. Kim, and J. Lee, “The SEED encryption algorithm,” 2005