

MIT Open Access Articles

A Low-Power Elliptic Curve Pairing Crypto-Processor for Secure Embedded Blockchain and Functional Encryption

The MIT Faculty has made this article openly available. **Please share** how this access benefits you. Your story matters.

Citation: Banerjee, Utsav and Anantha P. Chandrakasan. "A Low-Power Elliptic Curve Pairing Crypto-Processor for Secure Embedded Blockchain and Functional Encryption." 2021 IEEE Custom Integrated Circuits Conference, April 2020, Austin, Texas, Institute of Electrical and Electronics Engineers, May 2021. © 2021 IEEE

As Published: <http://dx.doi.org/10.1109/cicc51472.2021.9431552>

Publisher: Institute of Electrical and Electronics Engineers (IEEE)

Persistent URL: <https://hdl.handle.net/1721.1/131207>

Version: Author's final manuscript: final author's manuscript post peer review, without publisher's formatting or copy editing

Terms of use: Creative Commons Attribution-Noncommercial-Share Alike



A Low-Power Elliptic Curve Pairing Crypto-Processor for Secure Embedded Blockchain and Functional Encryption

Utsav Banerjee, Anantha P. Chandrakasan
Massachusetts Institute of Technology, Cambridge, MA, USA

Pairing-based cryptography (PBC), a variant of elliptic curve cryptography (ECC), uses bilinear maps between elliptic curves and finite fields to enable several novel applications beyond traditional key exchange and signatures [1]. Fig. 1 shows two such applications – (a) signature aggregation, where arbitrarily large number of signatures are aggregated into one to resolve communication bottleneck in mesh networks such as blockchain [9], and (b) functional encryption, which allows computation on encrypted data with a function embedded in the decryption key [7]. In particular, pairing-based function-hiding inner product functional encryption [10] can be used for privacy-preserving data classification, thus enabling a new paradigm in the field of secure computation.

of our design. A lookup table (LUT) stores micro-code for basic functions such as extension field arithmetic and elliptic curve point and line operations, which together constitute the pairing computation. A 15.375KB memory is used as stack for cryptographic functions, while a 1 KB instruction memory can be programmed using a set of 90 custom instructions to implement various ECC and PBC algorithms. Hardware accelerators for AES-128/256 and SHA2-256 are used for pseudo-random number generation and hashing. For further configurability, these cryptographic units are integrated, using a memory-mapped interface, with a low-power RISC-V micro-processor supporting the RV32IM instruction set [11]. The RISC-V, AES, SHA and pairing cores all have dedicated clock gates, which can be independently configured for power savings.

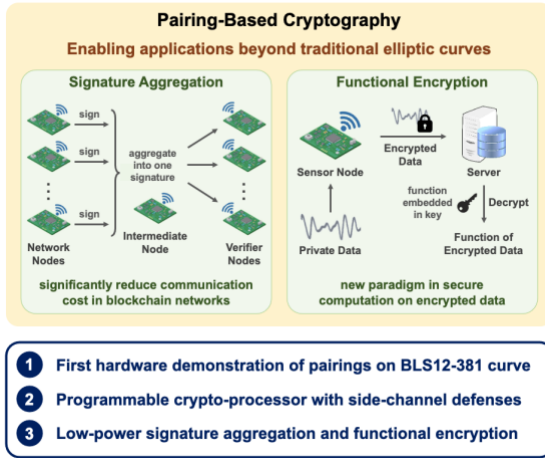


Fig. 1: Pairing-based cryptography in IoT – signature aggregation in blockchain and functional encryption for secure computation.

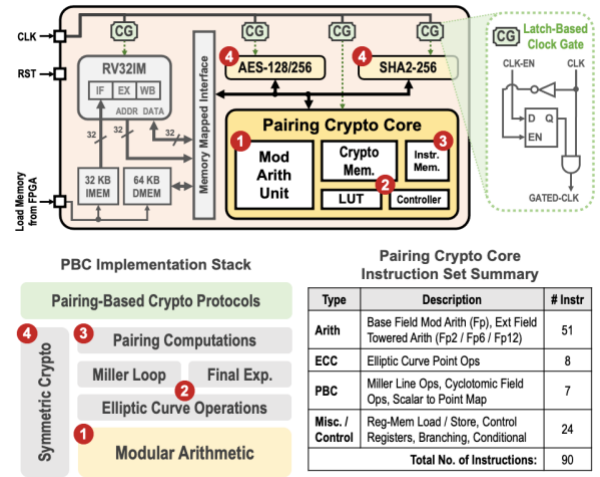


Fig. 2: Chip architecture with different components accelerating the PBC implementation stack and crypto-processor instructions.

Fig. 2 shows our chip architecture, along with the PBC implementation stack and a summary of crypto instructions supported by our pairing core. A 381b modular arithmetic unit forms the backbone

Modular arithmetic accounts for majority of the computation cost in pairing implementations. Fig. 3

shows our design of an energy-efficient modular arithmetic unit for the BLS12-381 curve. Modular arithmetic in Montgomery domain is standard for such large prime fields, and previous work on pairing accelerators use either high-performance parallel pipelined architectures with large area overhead [3, 4] or compact serial multipliers with lower energy-efficiency [2]. To balance area and energy-efficiency, we implement Montgomery modular multiplication using the coarsely integrated operand scanning (CIOS) approach [5], which splits zero-padded inputs into six 64b words and operates on them iteratively using a $64b \times 64b$ multiplier and a $128b + 64b + 64b$ adder, both utilizing carry-save structures for shorter critical path delay. We profiled various CIOS multipliers on our test chip and verified that energy consumption saturates at 64b word size, with 50% and 25% lower energy than conventional 16b and 32b architectures respectively. It is also more energy-efficient than previous work [2, 3, 4] when normalized with respect to prime size. A pair of cascaded 381b adder-subtractors is used for modular addition and subtraction, while modular inversion is implemented using exponentiation following Fermat’s theorem. Our hardware-accelerated modular arithmetic implementation is constant-time to prevent side-channel leakage.

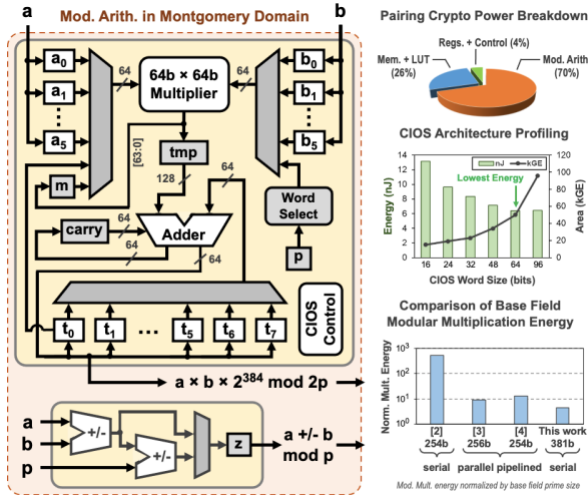


Fig. 3: Architecture of modular arithmetic unit with energy-efficient CIOS Montgomery multiplier.

Fig. 4 shows the detailed architecture of our pairing crypto-processor with algorithm-architecture co-

optimizations. The cryptographic memory is hierarchical, with a small register file M0 closest to the modular arithmetic unit and larger SRAMs M1 and M2 interfacing with the top-level controller. Each memory module is dynamically clock gated based on the function under execution, providing up to 20% power savings. The function micro-codes and constant values are stored in LUTs implemented using logic gates, which is 53k-gate and 34k-gate smaller than SRAM-based and ROM-based implementations respectively. Extension field multiplication and squaring are implemented using Karatsuba-style divide-and-conquer techniques to speed up Miller Loop (ML) and Final Exponentiation (FE), the two main parts of a pairing computation, by 35% and 28% respectively. Verification of aggregate signatures involves the multiplication of several pairings, also known as a multi-pairing. While previous work [4] shares only the FE computation for multi-pairing, we share both ML and FE leading to 30% additional energy savings. Furthermore, to accelerate inner product encryption, we utilize special properties of the BLS12-381 elliptic curve such as Frobenius endomorphism and GLV scalar decomposition [6] to achieve 1.8 \times reduction in energy consumption compared to the baseline algorithm [10].

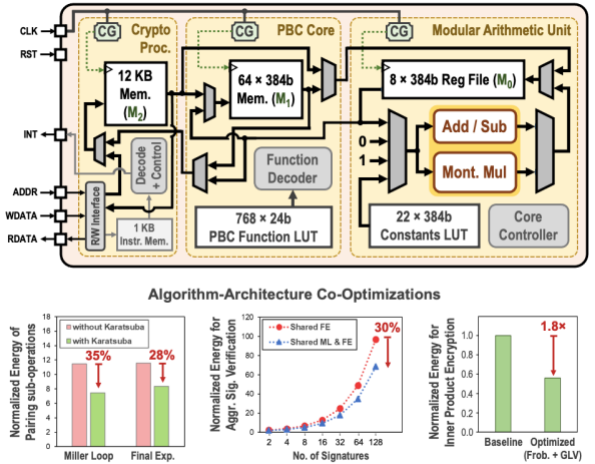


Fig. 4: Detailed architecture of the pairing crypto core along with algorithm-architecture co-optimizations.

Fig. 5 summarizes side-channel defenses supported by our chip and PBC protocol benchmarks. To ensure security against timing and simple power

analysis (SPA) attacks [8], our elliptic curve scalar multiplication (ECSM) and pairing implementations employ complete point addition formulas and the double-and-add-always technique. In high security use cases, our chip can also be configured to protect against stronger differential power analysis (DPA) attacks [8], with the same logic area but increased energy consumption. Along with randomized projective coordinates, our DPA-secure ECSM uses random scalar splitting and our DPA-secure pairing utilizes random exponents with the bilinear property. We evaluated several pairing-based public key cryptography protocols on our chip – signature aggregation, ID-based signatures, ID-based encryption, inner product encryption and multi-party key exchange [7, 8]. Our hardware-accelerated implementations are 130-140× more energy-efficient compared to software implemented on the RISC-V processor in our chip. Owing to the programmability of our pairing crypto core, new protocols, algorithm optimizations and side-channel countermeasures can be easily implemented using the same chip.

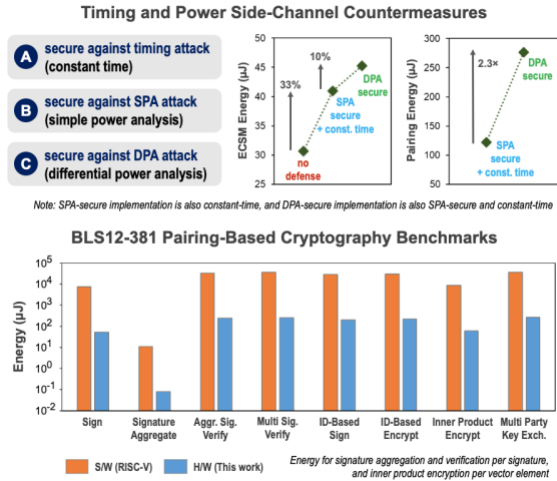


Fig. 5: Countermeasures against timing and power side-channel attacks with PBC protocol implementation benchmarks.

Fig. 6 compares this work with recent literature on pairing hardware accelerators. While [2, 3, 4] implement 254b BN curves, we are the first to demonstrate the newly proposed 381b higher security BLS12-381 curve in hardware. Our design

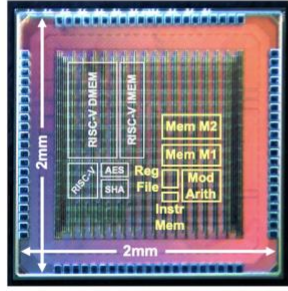
is an order of magnitude more energy-efficient than the embedded-scale accelerator in [2], enabled, in part, by our choice of modular arithmetic architecture. Compared to the high-performance accelerators in [3, 4], our design is an order of magnitude smaller with significantly lower power consumption due to power-performance trade-offs. We also achieve the lowest area-energy product compared to previous designs, implement timing and power side-channel countermeasures for stronger security, and the flexibility to accelerate signature aggregation, functional encryption and several other pairing-based protocols in hardware.

	CHES '14 [2] ^a	TVLSI '15 [3]	A-SSCC '19 [4] ^b	This work
Technology	130nm	65nm	65nm FDSOI	40nm
Supply Voltage	1.2 V	1.2 V	1.33 V	0.66 V (1.1 V)
Frequency	48 MHz	800 MHz	250 MHz	16 MHz (90 MHz)
Total Area	—	2.42 mm ²	12.8 mm ²	0.2 mm ²
Logic Gates	58 kGE	354 kGE	2793 kGE	112 kGE
SRAM	—	24 KB	—	16 KB
Avg. Power	9.96 mW	266.5 mW	2850 mW	0.58 mW (8.08 mW)
Pairing Curve	254b BN curve (low security)	256b BN curve (low security)	254b BN curve (low security)	BLS12-381 curve (recommended)
Side-Channel Countermeasures	const. time	—	—	const. time, SPA / DPA-sec.
Pairing Energy	1.61 mJ	170.6 μJ	94.0 μJ	122.1 μJ (SPA-sec.) 276.2 μJ (DPA-sec.)
Norm. Energy ^c	31.125	3.25	1.875	1 ^d
Area \times Energy ^e	93	60	263	14 ^d

^a [2] reported post-synthesis simulation results ^b [4] implemented FDSOI body-bias tuning for minimum energy
^c normalized by prime size as energy / (prime size)² ^d calculated for SPA-secure ^e calculated as kGE \times mJ

Fig. 6: Comparison with previous work on pairing hardware accelerators.

The chip was fabricated in a 40nm low-power CMOS process and supports voltage scaling from 1.1V down to 0.66V. All measurements are reported at 16MHz and 0.66V. Our pairing crypto core occupies 112k NAND Gate Equivalents (GE) and uses 16KB of SRAM. Using efficient algorithms and low-power architectures, we demonstrate practical side-channel-resistant hardware-accelerated BLS12-381 pairing-based protocols which enable novel cryptographic applications to secure resource-constrained IoT devices.



Chip Specifications	
Technology	40nm LP CMOS
Supply Voltage	0.66 – 1.1 V
Package	64-pin QFN
Die Size	2 mm x 2 mm
Pairing Crypto-Processor Core	
Total Area	0.2 mm ² (logic gates & SRAM)
Logic Gates	112k (NAND2 equiv.)
SRAM	16 KB
Maximum Frequency	16 MHz at 0.66 V 90 MHz at 1.1 V
Average Power	0.58 mW at 0.66 V & 16 MHz 8.08 mW at 1.1 V & 90 MHz
Pairing Curve	BLS12-381 (sec. level ~128-bit)
Supported Computations	Mod. Arith., Optimal Ate Pairing, G ₁ / G ₂ ECSM, G ₂ Exp., Hash to Curve, Multi-Pairing, BLS Sign / Verify, Sig. Aggr., Functional Encryption, etc
Side-Channel Defenses	Constant Time, SPA-Secure, DPA-Secure

Fig. 7: Chip micrograph and performance summary.

Acknowledgements:

The authors would like to thank Texas Instruments for funding this work, and the TSMC University Shuttle Program for chip fabrication support.

References:

- [1] Y. Sakemi et al., “Pairing-Friendly Curves,” *IETF CFRG Internet Draft*, Jun. 2020.
- [2] T. Unterluggauer et al., “Efficient Pairings and ECC for Embedded Systems,” *IACR CHES*, pp. 298-315, Sep. 2014.
- [3] J. Han et al., “A 65 nm Cryptographic Processor for High Speed Pairing Computation,” *IEEE TVLSI*, vol. 23, no. 4, pp. 692-701, Apr. 2015.
- [4] M. Ikeda et al., “33us, 94uJ Optimal Ate Pairing Engine on BN Curve over 254b Prime Field in 65nm CMOS FDSOI,” *IEEE A-SSCC*, pp. 263-266, Nov. 2019.
- [5] C. K. Koc et al., “Analyzing and Comparing Montgomery Multiplication Algorithms,” *IEEE Micro*, vol. 16, no. 3, pp. 26-33, Jun. 1996.
- [6] R. P. Gallant et al., “Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms,” *IACR CRYPTO*, pp. 190-200, Aug. 2001.
- [7] R. Dutta et al., “Pairing-Based Cryptographic Protocols: A Survey,” *Cryptology ePrint Archive*, Report 2004/064, Jun. 2004.
- [8] Mrabet et al., “Guide to Pairing-Based Cryptography,” *CRC Press*, Jan. 2017.

[9] D. Boneh et al., “Compact Multi-Signatures for Smaller Blockchains,” *IACR ASIACRYPT*, pp. 435-464, Dec. 2018.

[10] S. Kim et al., “Function-Hiding Inner Product Encryption is Practical,” *IACR SCN*, pp. 544-562, Sep. 2018.

[11] U. Banerjee et al., “Sapphire: A Configurable Crypto-Processor for Post-Quantum Lattice-based Protocols,” *IACR TCHES*, vol. 2019, no. 4, pp. 17-61, Aug. 2019.

A revised version of this paper was published in 2021 IEEE Custom Integrated Circuits Conference (CICC) - DOI: [10.1109/CICC51472.2021.9431552](https://doi.org/10.1109/CICC51472.2021.9431552)