FIPS205(SLH-DSA) 署名生成ハードウェア向け SHA2 演算の最適化

Optimization of SHA2 Operations for Signature Generation Hardware Compliant with FIPS 205 (SLH-DSA)

東京大　○竹島 優太、池田 誠
Tokyo Univ., ○Yuta Takeshima, Makoto Ikeda
E-mail: takeshima@silicon.u-tokyo.ac.jp

【はじめに】

量子コンピュータの進展に伴い、耐量子計算機暗号の研究が進む中、NIST によって標準化されたハッシュベースの署名「SLH-DSA」は高い安全性を持つが、署名生成の計算コストが課題である。本研究では、SHA2 および SHAKE に対応した低レイテンシな署名生成ハードウェアを設計した。ここでは特に計算効率化が求められる SHA2 演算器の最適化について述べる。

【手法】

Chen らの実装 [1] では、クリティカルパスをレジスタで分割し周波数の向上を図っている一方、1 ブロックの計算には 66 サイクル必要となる。本研究ではこれをもとに最適化を行った。SLH-DSA でハッシュを計算する際、最初の 1 ブロックには毎回同じシード値を入力する。そのためその 1 ブロックを計算した後の状態を保存しておくことでサイクル数を半分に抑えることができる。また、SLH-DSA におけるハッシュ計算のほとんどを占める WOTS+の計算においては 1 ブロックの計算を 61 サイクルまで短縮することができる。これはシード値の次のブロックの最初の入力が一定になることを利用している。

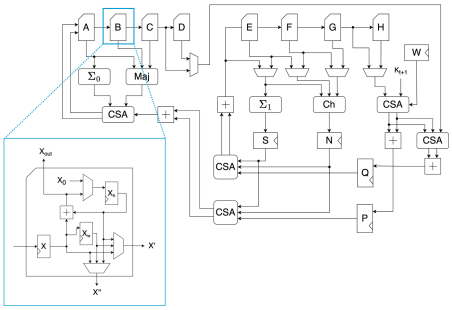

図 1: Architecture of SHA2

【結果】

SHA2 のナイーブな実装ではクロック周期は 0.31 ns となったが、最適化により 0.22 ns まで短縮しつつサイクル数の削減も達成された。表 1 にこの SHA2 を用いた 2 コアと 14 コアの SLH-DSA 署名生成器の合成結果を示す。単体のときよりもクロック周期は長くなったものの、SLotH[2] の約 15 倍の周波数で動作する。面積は大きくなっているがサイクル数の削減の効果もあり面積遅延時間積で比較すると 2 コアでは 8.4 倍、14 コアでは 19.6 倍の性能向上となった。

【参考文献】

[1] Yimeng Chen and Shuguo Li. A high-throughput hardware implementation of sha-256 algorithm. In 2020 IEEE international symposium on circuits and systems (ISCAS), pp. 1–4. IEEE, 2020.
[2] Markku-Juhani O Saarinen. Accelerating slh-dsa by two orders of magnitude with a single hash unit. In Annual International Cryptology Conference, pp. 276–304. Springer, 2024.

表 1: Logic Synthesis Results

	Platform	clk [ns]	area [kGE]	cycles	cycles / hash	latency [us]
SLotH[2]	Nangate45	4	105	9,127,150	87.0	36,509
This work (2-core)	TSMC28nm	0.26	740	3,240,000	30.9	842
This work (14-core)	TSMC28nm	0.27	1,972	497,000	4.7	134