IoT 向け超低消費電力暗号の設計理論の確立とアルゴリズム開発

Designing Low-Energy Symmetric-Key Primitives or IoT Devices

五十部　孝典（Takanori Isobe, Ph. D.）
兵庫県立大学大学院　情報科学研究科　教授
(Professor, University of Hyogo, Information Science)

受賞：電子情報通信学会 末松安晴賞 (2023 年)　文部科学大臣表彰 若手科学者賞 (2023 年)　国際暗号学会 Fast Software Encryption Best Paper Award (2011, 2022, 2023 年) 電子情報通信学会 暗号と情報セキュリティシンポジウム(SCIS) イノベーション論文賞 (2014, 2018, 2021 年), 電子情報通信学会 論文賞 (2014))他

研究専門分野：情報セキュリティ、暗号

あらまし

超スマート社会では、IoT デバイスを用いてプライバシー情報や生体情報などのセンシティブな情報を収集し、クラウドで分析を行う。そのため、従来の通信ネットワークやサーバに対するセキュリティのみではなく、IoT デバイスでの暗号化技術が極めて重要になる。一般的に、IoT デバイスはハードウェアリソースが制限されているため、軽い処理での演算が可能な暗号が求められる。本研究では、IoT デバイス向けの低消費電力暗号の開発を行う。具体的には、暗号の安全性を維持したまま、暗号演算や構造の軽量化を実現するアプローチを採用し、暗号演算時の消費電力の最小化を目指す。結果として、共通鍵暗号プリミティブであるブロック暗号 WARP、ストリーム暗号 Atom、擬似ランダム置換 Orthros の 3 つのアルゴリズムを設計し、既存技術を大幅に上回る低消費電力特性を持つことを示す。

１．研究の目的

本研究の目的は、IoTデバイス向けの低消費電力暗号の開発である。初めに、既存の低消費電力暗号として知られるブロック暗号 Midori[1]やストリーム暗号 Plantlet[2]の安全性を、数理ソルバーを利用して厳密に評価する。この評価技術を基に、安全かつ超低消費電力を実現する暗号アルゴリズムの設計に取り組む。

Midori は、消費電力の削減を目指して設計されたブロック暗号である。その構成や構造は、低消費電力のブロック暗号、ストリーム暗号、擬似ランダム関数の設計にも応用可能だが、そのままの適用は安全性の問題を引き起こす可能性がある。そこで、Midori の低消費電力特性を保ちつつ、各プリミティブの解析結果をもとに、安全で効率的なアルゴリズム設計を進める。そして、低消費電力と安全性を重視した構成要素の最適化や、適切なパラメータ選択を行う。

アルゴリズムの安全性評価では、差分や線形、積分攻撃に対する安全性に関して、数理ソルバーを用いた評価を行う。達成目標としては、既存技術であるAESやMidoriと比較して大幅な消費電力の削減を実現することである。これによりバッテリーの寿命を顕著に延ばすことが期待される。

２．研究の背景

超スマート社会（Society5.0）では、エッジデバイスから情報を取得し、クラウドで分析を行い、システム全体としての適切な情報処理技術を実施する。大量のエッジデバイスは、プライバシー情報や生体情報などのセンシティブな情報を収集するため、従来の通信ネットワークやサーバに対するセキュリティのみならず、エッジデバイスでの暗号化技術が極めて重要となる。実際、EU の一般データ保護法や個人情報保護法の施行に伴い、エッジデバイスで収集したセンシティブ情報の暗号化は法的に義務付けられ、暗号技術は社会的に不可欠となっている。

一般的に、IoT エッジデバイスはセンサーノードなどのリソースが限られたデバイスを対象とし、軽量な処理での演算が可能な暗号が求められる。さらに、センサーは多様な場所や環境に配置され、医療用途では体内への埋め込みも考慮されるため、バッテリー駆動が前提となる。この観点から、センサーの寿命を延ばすためには、超低消費電力の暗号技術が必要とされている。実際、2019 年から NIST(アメリカ国立標準技術研究所)により、軽量の暗号の標準を決めるプロジェクトが実施されており、産業的にも学術的にも非常に重要な研究テーマである。

IoT 向け超低消費電力暗号の設計理論の確立とアルゴリズム開発

Designing Low-Energy Symmetric-Key Primitives or IoT Devices

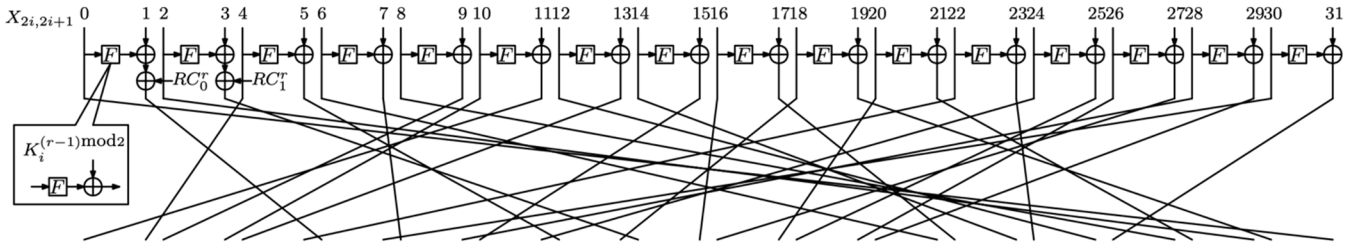

図 1　WARP のラウンド関数

３．研究の方法および結果

本研究では、低消費電力暗号としてブロック暗号 WARP、ストリーム暗号 Atom、擬似ランダム置換 Orthros の 3 つの暗号プリミティブの設計を実施した。

3-1. ブロック暗号 WARP

■　背景

制約のあるデバイスにおける暗号化と認証の必要性の増加に伴い、軽量暗号は共通鍵暗号のテーマの一つとして注目を集めている。第一世代の軽量ブロック暗号として、PRESENT[3]、KATAN[4]、 Piccolo[5]などが挙げられる。これらは 64 ビットのブロックサイズを持つブロック暗号で、主にハードウェアの回路規模を最小化することを目的とした設計が採用されている。米国標準のブロック暗号 AES と比較し、ブロックサイズを 128 ビットから 64 ビットにすることでレジスタ数の削減し、非線形関数や線形関数も AES と比較し、軽量なものを採用している。その後の第二世代の軽量暗号では、回路規模のみではなく、さまざまな要件、例えば低遅延や低消費電力消費、サイドチャネル攻撃に対する耐性などに焦点を当てて開発された。

本研究では、128 ビットのブロックと 128 ビットの鍵を持つ軽量ブロック暗号の開発を行う。128 ビット入出力サイズは AES と同じであるため、その代替としてそのまま使用可能であり、実社会利用において有用である。さらに、既存の軽量暗号では、ブロックサイズが 64 ビットであることから、誕生日攻撃のような脅威が現実の問題となる可能性があり、暗号の長期利用の観点では安全性の問題がある。したがって、128 ビットの軽量ブロック暗号は安全性と実利用の両面でも重要である。

■　仕様

本研究では 128 ビットブロック暗号 WARP を提案する。WARP は 128 ビット鍵をサポートし、図 1 で示す 32 ブランチの Generalized Feistel Network（GFN）構造をベースにしている。GFN の特徴として、暗号化と復号化の演算が等価であるため、暗号化回路のみで復号化回路を構築することができ、これによりハードウェアのサイズを大幅に削減できる。

GFN の設計における最も大きな課題は 32 ブランチの置換を適切に決定することである。この課題に対処するため、本研究では数理ソルバーである MILP ソルバーを用いて適切な部分集合の中から安全性の観点で最適な置換を探索し、設計した。WARP の置換は 10 ラウンドの拡散性能を持っており、差分・線形攻撃への安全性の指標であるアクティブ S-box 数の観点から非常に良い性能を示している。

低遅延性と回路規模の観点から S-box は Midori[1]のものを採用しており、これによってサイドチャネル攻撃が可能である場合にもその対策は非常に効率的にできる。WARP の鍵スケジュールは非常にシンプルであり、128 ビット鍵を半分の 64 ビットに分割し、それらを交互に使用する。これによって追加のレジスタの必要性がなくなる。また、Feistel 構造の補完特性を避けるため、各サブキーは S-box が適用された後に排他的論理和をとる Piccolo[5]のアイデアに従っている。

■　実装性能

STM 90nm 標準セルライブラリで合成されたラウンドベース実装の性能指標の比較を行なった結果を表 1 に示す。消費電力の面では、2 ラウンドアンロールの構成が WARP 最も優れており、既存のブロック暗

号と比較して、最も小さい消費電力で暗号化が可能である。さらに回路規模、電力に関しても最小の数値を達成している。

表 1　STM 90nm 標準セルライブラリで合成されたラウンドベースの実装の性能指標の比較（1R、2R、4R は 1 回、2 回、4 回のアンロールされた回路を指す）

	Area (GE)	Power (μW) (@10MHz)	Energy (pJ)
GIFT-128-128	1997	116.6	478.1
SKINNY-128-128	2104	132.5	543.3
SIMON 128/128	2064	105.6	728.6
MIDORI 128(E)	2522	89.2	187.3
MIDORI 128(ED)	3661	108.7	228.3
AES 128	7215	730.3	803.3
WARP (1R) (E)	1187	55.5	233.2
WARP (1R) (ED)	1390	59.5	250.0
WARP (2R) (E)	1456	58.4	128.5
WARP (2R) (ED)	1824	69.9	153.7
WARP (4R) (E)	2223	117.5	141.0
WARP (4R) (ED)	3075	177.4	212.9

3-2. ストリーム暗号 Atom

■　背景

一般的な Time Memory Tradeoffs（TMD）攻撃に対して安全なストリーム暗号の条件として、内部状態のサイズが秘密鍵の長さの 2 倍以上である必要があると考えられていた。しかし、FSE 2015 で提案された Sprout[6]と呼ばれるストリーム暗号では、内部状態のサイズが秘密鍵の長さと等しいにも関わらず、TMD 攻撃に対して耐性を持っていることが示された。これに触発され、Sprout と同じ Grain 構造を持つ Lizard[7]や Plantlet などの内部状態の短いストリーム暗号の設計が次々と生まれたが、Sprout を含めていずれも脆弱性が発見されている。以上から、内部状態のサイズの軽量化と安全性の両立が可能であるかどうかはストリーム暗号において重要な問題である。本研究では、内部状態のサイズが秘密鍵と同等の大きさであり、なおかつ提案されているすべての攻撃に対する耐性を持った低消費電力スストリーム暗号の設計を目的とする。

■　仕様

本研究で提案するストリーム暗号 Atom は、秘密鍵 128 ビットに対して内部状態のサイズが 159 ビットであり、内部状態のサイズが小規模であるという条件を満たしている。また、Atom は NFSR(Non-linear Feedback Shift Register）と呼ばれるキーフィルタが新たに追加されている。これと従来の LFSR(Linear Feedback Shift Register)の 2 つのキーフィルタにより、TMD 攻撃を含む多くの暗号解読手法に対する耐性が得られる。

また、Atom は従来のストリーム暗号と同様に、初期化フェーズとキーストリーム生成フェーズで構成されている。図 2 にキーストリーム生成フェーズの概要を示す。

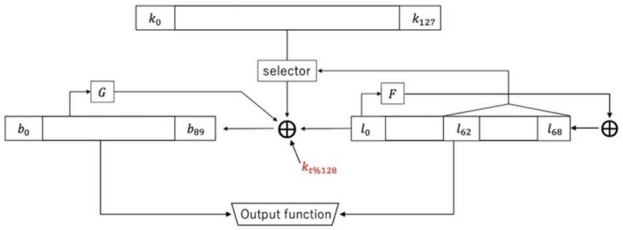

図 2　キーストリーム生成フェーズの概要

■　実装性能

表 2 は、Atom やその他の軽量ストリーム暗号を STM 90 nm 標準セルライブラリを使用した回路で実装した場合のハードウェア測定値である。表より、Atom は 128 ビットのセキュリティレベルを持つ暗号としては最も消費電力が低く、さらに比較的コンパクトな回路面積での実装が可能であることが確認できる。

表 2:Atom および他の軽量ストリーム暗号の
ハードウェア測定値（STM90nm）

	Key Size	Area (GE)	Power (μ W, 100 MHz)	Energy (pJ/bit)
Grain-v1	80	979.52	372.7	3.78
Trivium	80	1502.7	607.7	6.21
Sprout	80	681.25	234.8	2.37
Plantlet	80	782.70	276.4	2.79
Lizard	120	1250.5	358.2	3.65
Grain-128	128	1457.2	562.9	5.75
Kreyvium	128	2954.2	1019	10.60
Trivium-MB	128	1613.7	614.5	6.29
Trivia	128	2041.7	803.5	8.29
AES-CTR	128	2093.5	1099.0	15.10
Atom	128	1490.5	490.5	5.02

IoT 向け超低消費電力暗号の設計理論の確立とアルゴリズム開発

Designing Low-Energy Symmetric-Key Primitives or IoT Devices

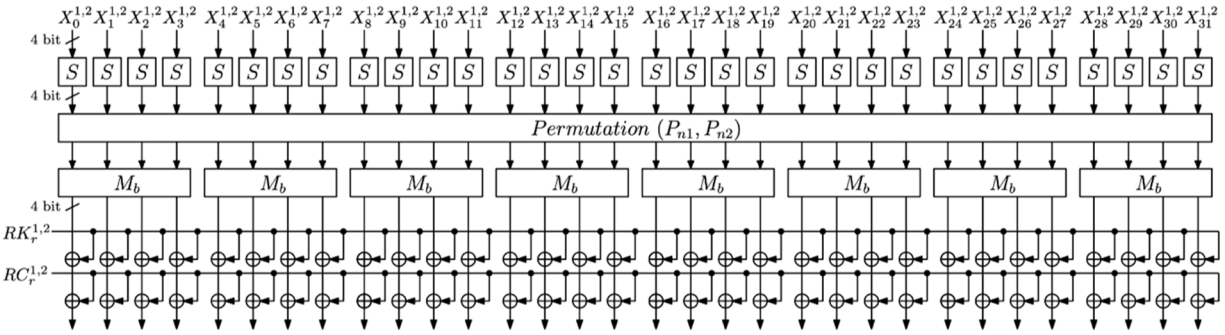

図 3　Orthros のラウンド関数

3-3. 擬似ランダム置換 Orthros

■　背景

IoT 社会の発達にともない，より少ない遅延で暗号化が実行可能な 128 ビット低遅延擬似ランダム関数が求められている。既存の軽量暗号である GIFT[8]、KATAN、LED[9]、Piccolo[5]、PRESENT[3]、SIMON[10]は回路規模の最小化の観点では優れているが、暗号演算の多くのサイクルが必要であり、暗号に必要な遅延は非常に大きい。一方、既存の低遅延の暗号技術としては、PRINCE[11]、QARMA[12]、Mantis[13]、Midori[1]などが知られているが、これらはブロック暗号であり、擬似ランダム置換は提案されていない。擬似ランダム置換は、特定の暗号化モードは高い安全性を達成可能であるとともに、逆演算関数の必要がないため、回路規模の観点でも優れている。また、その不可逆性より、特定の攻撃手法に対して高い耐性を持つ可能性があり、大幅に遅延を削減可能である。また、消費電力は遅延性能と回路規模に比例するため、低遅延暗号の設計はそのまま低消費電力の設計に繋がる。

■　仕様

本研究で提案する擬似ランダム置換 Orthros は 128 ビットの鍵を持つ。ラウンド関数と全体構成をそれぞれ図 3 と 4 に示す。Orthros の全体構造は、Branch1 と Branch2 と呼ばれる 2 つの SPN 型の鍵付き置換の排他的論理で構成されている。Orthros のラウンド関数は、Midori に基づいており低遅延暗号に適しているが、新しい線形層と S-box を採用することで遅延をさらに最小化した。

線形層に関しては、Midori128 はビット順列とニブル順列の両方を含む単一の線形層を使用しているが、Orthros ではビット順列とニブル順列のハイブリッドを提案している。これにより短いラウンド数で安全性を達成可能である。この線形層の変更は、アンロール実装では追加のハードウェアコストを必要としない。

S-box に関しては、擬似ランダム置換では、Midori や QARMA のようなインボリューション特性が必要ないため、探索空間が大幅に広がり、既存のものより遅延が大幅に小さい新しい 4 ビットの S-box を開発することが可能である。

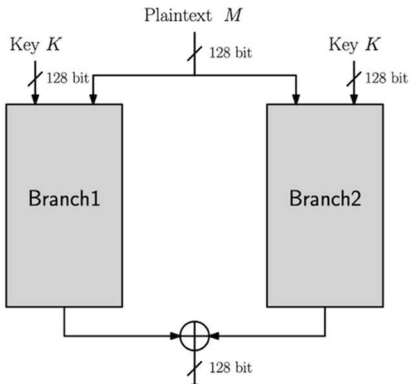

図 4　Orthros の概要

■　実装性能

STM90nm のライブラリ実装結果を表 3 に示す。この結果から、Midori や QARMA よりも暗号化に必要な Latency の値が小さくなることがわかる。また、消費電力に関して既存技術よりも小さくなる。

表 3　STM90nm ライブラリの実装結果

Cipher	Area (μm^2)	Area (GE)	Power (mW)	Energy (pJ)	Latency (ns)	Max TP (Gbps)
Orthros	98150.7	22307	6.647	664.69	10.60	11.246
	99258.2	22559	6.025	602.50	9.00	13.245
	102286.4	23247	6.214	621.40	8.00	14.901
	108582.3	24678	7.220	722.02	7.00	17.030
	123160.6	27991	9.612	961.24	6.00	19.868
	133931.3	30430	10.751	1075.07	5.00	23.842
	148432.8	33735	12.614	1261.35	4.00	29.802
	177991.2	40453	16.591	1659.12	3.00	39.736
	298855.6	67922	27.628	2762.76	2.40	49.671
Midori-128	85435.0	19417	10.205	1020.49	18.54	6.430
	86470.0	19652	9.671	967.14	16.00	7.451
	89648.7	20375	9.748	974.81	14.00	8.515
	96225.5	21869	11.275	1127.54	12.00	9.934
	107393.6	24408	15.687	1568.7	10.00	11.921
	122584.4	27860	17.887	1788.72	8.00	14.901
	144109.4	32752	24.011	2401.09	5.99	19.868
	277950.7	63171	46.464	4646.39	4.10	29.075
QARMA$_9$-128-σ_0	104118.3	23663	10.044	1004.38	19.41	6.142
	104686.9	23792	9.810	981.04	17.00	7.012
	106848.1	24284	9.911	991.05	15.00	7.947
	112157.2	25490	11.571	1157.09	13.00	9.170
	128032.8	29098	16.816	1681.62	11.00	10.837
	147874.2	33608	20.438	2043.83	9.00	13.245
	182268.6	41425	27.714	2771.37	6.96	17.128
	234453.9	53285	41.508	4150.79	4.99	23.890
	319634.3	72644	58.119	5811.87	4.38	27.217
Kangaroo12-PRF[1600] *	498909.7	113389	59.533	5953.25	17.52	6.804
	552581.2	125587	58.170	5817.01	12.00	9.934
	590922.6	134301	57.350	5735.03	8.00	14.901
	1184290.6	269157	140.664	14066.38	3.99	29.877
Kangaroo12-PRF[400] *	133662.4	30378	16.674	1667.36	18.47	6.454
	144600.0	32864	14.388	1438.84	12.00	9.934
	167258.9	38013	18.260	1825.96	8.00	28.725
	339374.6	77131	39.311	3931.14	4.15	14.901
Subterranean-PRF *	130206.1	29592	9.976	997.59	17.45	6.831
	139879.2	31791	8.467	846.6	12.00	9.934
	177843.0	40419	18.475	1847.46	8.00	14.901
	375592.1	85362	40.271	4027.13	3.63	32.840

４．将来展望

情報セキュリティの研究分野では､Beyond5G(B5G)用の暗号開発が学術､産業分野ともに活発になっている。B5G 用の暗号技術は、IoT 用の暗号と比べて、性能や安全性要件が非常に厳しく、既存の暗号技術では対応が不可能である。B5G の世界では宇宙、深海、航空、砂漠などバッテリー交換が非常に困難なユースケースが多数あり、性能面においては特に超低消費電力での暗号処理が求められる。また、収集されたビッグデータを処理するデータセンターにおいても、サステナビリティとプライバシーの両立の観点で低消費電力での暗号処理は喫緊の課題である。

安全性に関しては、量子計算機に対して強固な安全性が求められる。量子計算機による危殆化の影響が大きい公開鍵暗号(鍵交換や署名に利用)に関しては、米国立標準技術研究所が現在標準化を進めている。国内においても、2022 年に NICT が凸版印刷と共同で耐量子計算機暗号を IC カードシステムに実装するなど、実用化に向けて準備が進んでいる。一方、実データを暗号する共通鍵暗号に関しては、低消費性などの実装面の要求が非常に厳しく、実装要求と量子計算機への安全性を満たす暗号は学術レベルでも実現しておらず、2030 年の B5G の普及に備えて早急な研究開発が求められている。

おわりに

本研究では、IoT 向け低消費電力暗号の開発を行った。具体的には、暗号の安全性を維持したまま、演算や構造の軽量化を実現するアプローチをとった。結果として、共通鍵暗号プリミティブであるブロック暗号 WARP、ストリーム暗号 Atom、擬似ランダム置換 Orthros の３つのアルゴリズムを設計した。

参考文献

[1] Subhadeep Banik, Andrey Bogdanov, Takanori Isobe, Kyoji Shibutani, Harunaga Hiwatari, Toru Akishita, and Francesco Regazzoni. Midori: A block cipher for low energy. In Tetsu Iwata and Jung Hee Cheon, editors, *ASI- ACRYPT 2015, Part II*, volume 9453 of *LNCS*, pages 411–436. Springer,2015.

[2] Vasily Mikhalev, Frederik Armknecht, and Christian Müller. On Ciphers that Continuously Access the Non-Volatile Key. *IACR Trans. Symmetric Cryptol.*, 2016(2):52–79, 2016.

[3] Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe. PRESENT: An ultra-lightweight block cipher. In Pascal Paillier and Ingrid Verbauwhede, editors, CHES 2007, volume 4727 of LNCS, pages 450–466. Springer, 2007.

[4] Christophe De Canni`ere, Orr Dunkelman, and Miroslav Kne˘zevi ´c. KATAN and KTANTAN - a family of small and efficient hardware-oriented block ciphers. In Christophe Clavier and Kris Gaj, editors, CHES 2009, volume 5747 of LNCS, pages

272–288. Springer, 2009.

[5] Kyoji Shibutani, Takanori Isobe, Harunaga Hiwatari, Atsushi Mitsuda, Toru Akishita, and Taizo Shirai. Piccolo: An ultra-lightweight blockcipher. In Bart Preneel and Tsuyoshi Takagi, editors, CHES 2011, volume 6917 of LNCS, pages 342–357. Springer, Heidelberg, 2011.

[6] Frederik Armknecht and Vasily Mikhalev. On Lightweight Stream Ciphers with Shorter Internal States. In Fast Software Encryption - 22nd International Workshop, FSE 2015, Istanbul,Turkey, March 8-11, 2015, Revised Selected Papers, pages 451–470, 2015.

[7] Matthias Hamann, Matthias Krause, and Willi Meier. LIZARD - A Lightweight Stream Cipher for Power-constrained Devices. IACR Trans. Symmetric Cryptol., 2017(1):45–79, 2017.

[8] Subhadeep Banik, Sumit Kumar Pandey, Thomas Peyrin, Yu Sasaki, Siang Meng Sim, and Yosuke Todo. GIFT: A small present - towards reaching the limit of lightweight encryption. In Wieland Fischer and Naofumi Homma, editors, CHES 2017, volume 10529 of LNCS, pages 321–345. Springer, 2017.

[9] Jian Guo, Thomas Peyrin, Axel Poschmann, and Matthew J. B. Robshaw. The LED block cipher. In Bart Preneel and Tsuyoshi Takagi, editors, CHES 2011, volume 6917 of LNCS, pages 326–341. Springer, 2011.

[10] Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, and Louis Wingers. The SIMON and SPECK families of lightweight block ciphers. Cryptology ePrint Archive, Report 2013/404, 2013. http://eprint.iacr.org/2013/404.

[11] Julia Borghoff, Anne Canteaut, Tim Güneysu, Elif Bilge Kavun, Miroslav Knežević, Lars R. Knudsen, Gregor Leander, Ventzislav Nikov, Christof Paar, Christian Rechberger, Peter Rombouts, Søren S. Thomsen, and Tolga Yalçin. PRINCE - A low-latency block cipher for pervasive computing ap- plications - extended abstract. In Xiaoyun Wang and Kazue Sako, editors, ASIACRYPT 2012, volume 7658 of LNCS, pages 208–225. Springer, 2012.

[12] Moses Liskov, Ronald L. Rivest, and David Wagner. Tweakable block ciphers. In Moti Yung, editor, CRYPTO 2002, volume 2442 of LNCS, pages 31–46. Springer, 2002.

[13] Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim. The SKINNY family of block ciphers and its low-latency variant MANTIS. In Matthew Robshaw and Jonathan Katz, editors, CRYPTO 2016, Part II, volume 9815 of LNCS, pages 123–153. Springer, 2016.

関連文献

Subhadeep Banik and Zhenzhen Bao and Takanori Isobe and Hiroyasu Kubo and Kazuhiko Minematsu and Fukang Liu and Kosei Sakamoto and Nao Shibata and Maki Shigeri, "WARP : Revisiting GFN for Lightweight 128-bit Block Cipher", Conference on Selected Areas in Cryptography (SAC) 2020, Lecture Note in Computer Science, vol. 12804, pp. 535--564. Springer, 2020

Subhadeep Banik, Andrea Caforio, Takanori Isobe,

IoT 向け超低消費電力暗号の設計理論の確立とアルゴリズム開発

Designing Low-Energy Symmetric-Key Primitives or IoT Devices

Fukang Liu, Willi Meier, Kosei Sakamoto and Santanu Sarkar, "Atom: A Stream Cipher with Double Key Filter", IACR Trans. Symmetric Cryptol (ToSC/FSE), issue 1, pp.5-36, 2021.

Subhadeep Banik, Takanori Isobe, Fukang Liu, Kazuhiko Minematsu and Kosei Sakamoto, "Orthros: A Low-Latency PRF", IACR Trans. Symmetric Cryptol (ToSC/FSE), 2021, issue 1, pp.37-77, 2021.

この研究は、令和元年度ＳＣＡＴ研究助成の対象として採用され、令和２～４年度に実施されたものです。