정 보 보 호 학 회 지
제 30 권 제3호, 2020. 6

경량 블록암호 알고리즘 설계 연구 동향

홍 득 조*

요 약

하드웨어 및 소프트웨어의 최적화는 제품의 성능 및 기능 향상, 개발 비용 최소화 등에 직접적인 영향을 미치는 매우 중요한 요소이다. 이러한 필요성에 따라, 암호학자들은 경량 암호 알고리즘을 가용 자원이 제한된 다양한 환경에서 효율적으로 구현 및 동작할 수 있는 암호 알고리즘으로 정의하고, 그것에 맞는 다양한 설계 방법들이 연구해왔다. 본고에서는 경량 블록암호 알고리즘 설계 연구 동향을 소개하고, 향후 전망에 대해 논의한다.

Ⅰ. 서 론

경량 대칭키 암호 알고리즘은 2001년 블록암호 AES의 표준화 이후 본격적으로 연구되기 시작했다. 서버나 PC 등 대부분의 환경에서 AES[1]가 암호화를 담당하게 되었으나, 경량 환경은 AES의 설계에서 고려된 것이 아니었기 때문이다. 게다가, 컴퓨터 시스템 및 네트워크 기술의 발달은 모든 장비의 소형화 및 지능화로 이어지고 있기 때문에, 하드웨어 및 소프트웨어의 최적화는 제품의 성능 및 기능 향상, 개발 비용 최소화 등에 직접적인 영향을 미치는 매우 중요한 요소이다.

암호학자들은 경량 암호 알고리즘을 가용 자원이 제한된 다양한 환경에서 효율적으로 구현 및 동작할 수 있는 암호 알고리즘으로 정의하고, 그것에 맞는 다양한 설계 방법들이 연구하였다. 암호 알고리즘의 설계는 알고리즘 개발, 취약점 분석, 새로운 설계 방법 제안으로 이어지는 정반합의 연속으로 발전해왔다. 이 글에서는 경량 블록암호 알고리즘 설계 발전 과정 및 연구 동향을 소개하고, 향후 전망에 대해 논의한다.

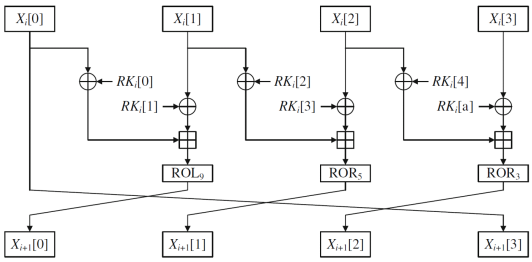
Ⅱ. 경량 블록암호의 등장

초기 경량 블록암호 알고리즘 설계의 초점은 하드웨어 구현 면적의 최소화에 있었다. CHES 2006에서 발표된 경량 블록암호 HIGHT[2]가 하드웨어 구현 면적을 최소화하기 위해 선택한 방법은 8비트 산술연산(Add ition mod 256, Bitwise Rotation, XOR)으로 라운드 함수를 구성하는 것이다. 이렇게 설계되는 구조를 사용된 연산자들의 앞글자를 따서 ARX 구조라고 부른다. 8비트 산술 연산의 장점은 하드웨어 구현비용이 저렴하며 대부분의 CPU에서 채택하고 있는 보편적인 연산이기 때문에 소프트웨어 구현에서도 어느 정도의 효율을 보장해준다는 것이다.

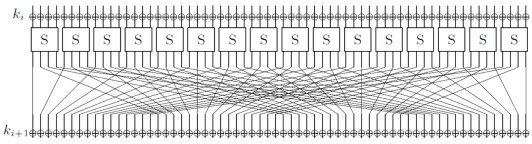
이듬해, CHES 2007에서 발표된 경량 블록암호 PRESENT[3]가 하드웨어 구현 면적의 최소화를 위해 선택한 방법은 4비트 S-box와 비트 치환(Bitwise Permutation)으로 라운드 함수를 구성하는 것이다. 4비트 S-box는 AES에 사용된 8비트 S-box에 비해 복잡도가 현저히 낮기 때문에 하드웨어 구현 면적이 작고 비트 치환은 단순히 비트의 위치를 옮겨 주는 연산이므로 하드웨어 구현 비용이 발생하지 않는다.

AES와 차별되는 HIGHT 및 PRESENT의 설계 기준 중 하나는 블록 길이를 64비트, 키 길이를 128비트로 설정했다는 것인데, 이것은 필요한 레지스터의 크기를 줄여주어 면적 최소화에 중요한 요소이지만, 두 블록암호가 제공하는 안전성 수준이 AES 보다 낮다는 의문을 제기하게 되는 이유이기도 하다. 그러나, 경량 환경에서의 블록암호의 용법이 서버나 PC에서와는 차이가 있다는 점도 고려된 설계 방향이다. 단순히 라운드 함수의 복잡도를 낮추는 것은 블록암호의 안전성을 크게 저하시키며 라운드 수의 급격한 증가가 일어날 수 있기 때문에 확산계층(Diffusion Layer)의 정교한 설계가 필요하다. 이 문제에 대처하는 방법으로 HIGHT의 설계자

* 전북대학교 IT정보공학과 (부교수, deukjo.hong@jbnu.ac.kr)



〔그림 1〕 블록암호 HIGHT의 라운드 함수



〔그림 2〕 블록암호 PRESENT의 라운드 함수

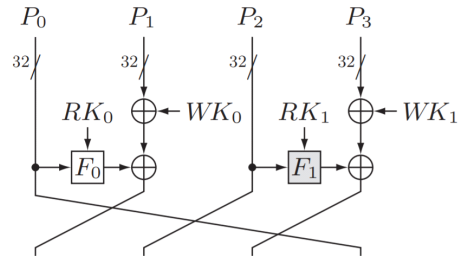
들은 두 가지 종류의 로테이션 수 조합의 사용을, PRESENT의 설계자들은 최대차분확률 증명이 가능한 비트 치환의 사용을 선택했다.

FSE 2007에서 발표된 경량 블록암호 CLEFIA는 위의 두 블록암호와는 다른 경량성의 정의에 기반하여 설계되었다. CLEFIA의 설계자들은 AES와 동일한 블록 길이와 키 길이를 고수하여 동일한 안전성을 제공하도록한 반면, 더 강력한 확산계층을 적용하여 라운드 수를 줄임으로써 암호화 속도를 높였다. 즉, 동일한 안전성과 구현 면적에서 암호화 속도가 더 빠르다면 전력소모가 감소한다는 관점으로 경량성을 강조한 것이다. 전력소모의 감소는 배터리의 수명과 밀접하며, 대부분의 소형 장비는 배터리 기반으로 작동한다는 점에서 경량 설계에 중요한 목표가 될 수 있다.

경량 블록암호의 개념을 정립하며 설계의 새로운 방향을 제시했던 이 세 알고리즘들은 현재 국제 표준 ISO/IEC 18033-3[4]과 ISO/IEC 29192-2[5]에 포함되어 있다.

Ⅲ. 경량 블록암호 연구의 발전 및 영향

HIGHT와 PRESENT 발표 이후의 경량 블록암호 설계 관련 연구 경향은 대략 네 가지로 정리할 수 있다. 첫 번째는 경량 블록암호 구현 방법의 다양화이다. 하드웨어 경량 구현에서는 면적 최소화 구현, 면적 대비 속도 최대화 구현에 관한 연구가 진행되었으며, 적용된 ASIC 구현 프로세스에 따른 구현 결과의 비교 분석도



〔그림 3〕 블록암호 CLEFIA의 라운드 함수

많이 연구되었다.

두 번째는 소프트웨어 경량의 개념의 등장이다. 저가형 CPU 및 MCU의 발전으로 더 이상 소형화의 영역이 하드웨어만의 것이 아니게 된 상황에서, 경량 소프트웨어 구현에 적합한 암호 알고리즘의 필요성이 증가하였다. 블록암호의 소프트웨어 경량 구현에서는 코드 크기 최소화 구현, 코드 크기 대비 속도 최대화 구현, 속도 최대화 구현에 관한 연구가 진행되었으며, 각 CPU에서 지원하는 연산 및 레지스터의 장점을 최대한 활용하기 위하여 어셈블리 수준에서의 구현 방법 또한 많이 연구되었다.

세 번째는 하드웨어 및 소프트웨어 경량 구현에 적합한 연산들에 대한 연구이다. 블록암호에 사용되어온 대표적인 비선형 연산인 S-box에 대해 ANF(Algeb raic Normal Form), CNF(Conjunctive Norm al Form)에서의 복잡성에 관한 연구 및 최적의 S- box 탐색 방법 등이 연구되었으며[6, 7], 선형 연산인 MDS 행렬에 대해 경량 구현이 가능한 형태의 행렬 구성 방법이 연구되었다[8, 9, 10, 11].

네 번째는 블록암호에 대한 가장 대표적인 안전성 분석 방법인 차분 공격(Differential Cryptanaly sis)와 선형 공격(Linear Cryptanalysis)에 사용될 수 있는 특성들(Characteristics)을 효율적으로 탐색하는 방법들이 연구되었다[12, 13, 14]. 이러한 특성 탐색 방법의 발전으로 상대적으로 블록 길이가 짧은 경량 블록암호들에 대해 실시간 실험이 가능하게 되어 매우 정교하게 안전성 분석을 수행할 수 있게 되었으며, 그러한 과정을 통해 안전성 분석과 설계에서 많은 연구 결과들이 양산되었다.

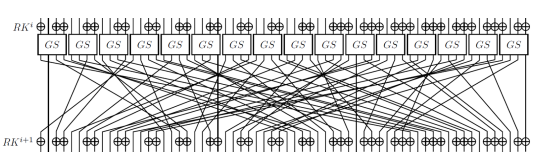
소프트웨어 경량 구현을 고려한 설계의 개념은 블록암호 KLEIN[15], LEA[16], SPECK & SIMON[17] 등에서 확인할 수 있다. 블록암호 LED[18]는 반복적인

네 단계로 구성될 수 있는 MDS 행렬을 채택함으로써 암호화 속도를 버리는 대신 면적 최소화 구현에 적합하게 AES와 유사한 구조를 만들 수 있음을 보여주었다.

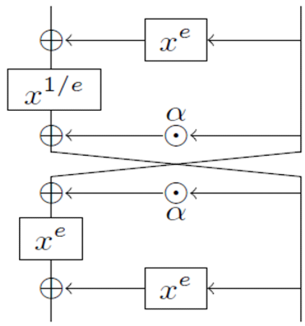
직관적으로 보자면, 안전성 조건은 경량성에 반비례하는 개념이다. 라운드 함수의 반복 횟수를 증가시킬수록, 라운드 함수의 구조가 복잡해질수록 안전성이 증가할 확률이 높기 때문이다. 블록암호 PRINCE[19]와 CHASKEY[20]는 전형적으로 블록암호에 대해 요구되는 안전성 수준을 대폭 낮춤으로써, 다른 알고리즘 보다 더욱 경량인 구조를 구성하는 것을 설계 목표로 하였으나, 일반적인 접근법은 아니다. 키스케줄이 거의 필요없는 특유의 형태로 인하여 지속적인 관심을 받고 있는 Even-Mansour 구조[21]가 실제로는 잘 사용되지 않고 있는 것도 동일한 블록 길이와 키 길이를 사용하는 다른 블록암호 구조에 비해 안전성 수준이 크게 떨어지기 때문이다.

블록암호 GIFT[22]는 PRESENT의 설계전략을 개선했다. PRESENT는 가능한 입력차분과 출력차분 쌍의 해밍웨이트 합계가 3이상이어야 한다는 조건을 만족하는 S-box를 사용했는데, 이것은 PRESEN T의 안전성 분석에서 가장 중요한 조건이다. 반면에, GIFT는 그러한 조건을 고수하지 않고 하드웨어 구현 시 PRESENT의 것 보다 더 구현 비용이 저렴한 S-box를 사용하였는데, 그럼으로써 발생할 수 있는 안전성의 손실을 비트 치환을 정교하게 설계함으로써 방지하였을 뿐만 아니라 오히려 더 개선하였다. GIF T의 설계자들이 제시한 BOGI(Bad Output Good Input)라는 설계전략은 최적의 안전성 결과를 만들어줄 수 있는 S-box와 비트 치환의 절묘한 결합 방법을 보여준다.

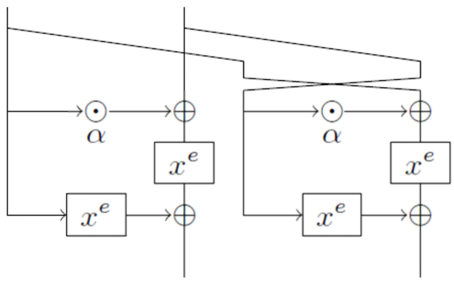
블록암호에 사용되는 비선형 논리에 관한 색다른 연구로는 버터플라이 구조[23]를 들 수 있다. 이 연구는 작은 입출력 길이를 갖는 비선형 연산을 이용하여 큰 입출력 길이를 갖는 비선형 연산을 만드는 것이 주된 목적이다. 물론, 작은 입출력 길이를 갖는 S-box를 기반으로 어떤 블록암호 구조를 적용하여 큰 입출력 길이를 갖는 S-box를 만드는 시도는 많이 있었으나, 버터플라



〔그림 4〕 블록암호 GIFT의 라운드 함수



〔그림 5〕 열린 버터플라이(Open Butterfly) 구조



〔그림 6〕 닫힌 버터플라이(Closed Butterfly) 구조

이 구조는 수학적으로 APN(Almost Perf ect Nonlinear) 함수를 지향한다는 점에서 차별화된다.

경량 블록암호에 관하여 연구된 다양한 안전성 분석 방법, 기본 연산자, 라운드 함수, 키스케줄 설계 방법들은 다른 암호 알고리즘들의 설계에 많은 영향을 주었다. SHA-3 프로젝트 이후 경량 해시함수(Hash Function)의 개념을 가진 알고리즘들이 발표되었고, 인증암호화(Authenticated-Encryption) 알고리즘 개발을 목적으로 수행된 CAESAR 공모전에서 최종적으로 생존한 알고리즘들 중 경량성과 관계된 것들은 'Lightweight Applications'라는 이름으로 정리되었다. 최근에 NIST에서도 경량 대칭키 암호 알고리즘의 표준화 추진을 위한 공모전을 수행하고 있다. 또한 ICISC 2019에서 발표된 CHAM[24]은 경량 블록암호 설계기술을 기반으로 개발된 경량 형태보존 암호 알고리즘이다.

Ⅳ. 향후 전망

앞으로는 부채널 분석 대응 구현 시 면적이 최소화될 수 있는 설계 방법을 제시한 블록암호 CRAFT[25] 처럼 설계 단계에서 기존에 요구되는 안전성과 효율성 조

건을 만족시키는 것 뿐만 아니라, 적용환경, 구현 방법, 부가적인 특수한 상황에서 최적화되는 설계 방법에 관한 다양한 연구 결과들이 발표될 것으로 예상된다.

마지막으로, 흥미로운 두 가지 연구 방향을 소개하고자 한다. 경량 블록암호의 공통적인 특징 중 하나는 키 스케줄이 극도로 단순하다는 것이다. 거의 모든 암호시스템에서 키는 랜덤하게 선택되는 것으로 가정하기 때문에, 오랜기간 동안 키스케줄 복잡도 증가의 원인이 되어왔던 연관키 공격의 실제 발생가능성은 난수발생기가 공격되지 않는 한, 0으로 수렴하고 있는 상황이다. 그렇지만, 바이클릭 공격(Biclique Attack)이나 비선형 불변 공격(Nonlinear Invariant Attack)은 단순한 키 스케줄이 블록암호 전체 구조를 취약하게 만들 수도 있음을 보여준다. 따라서 단순한 키스케줄의 적용으로 인한 위험 요소와 보완 방법에 대한 연구는 블록암호 설계 분야에서 파급 효과가 클 것이다. 또한, PGV 등 해시함수 모드에 적용될 경우 키스케줄의 단순한 구조 때문에 키 입력 부분으로부터 취약점이 발생할 수 있다. 이것은 기존의 블록암호 운영모드에 경량 블록암호를 적용하면 안전성에 문제가 있을 수 있음을 암시하는 반면, 현재의 PRF (Pseudo-Random Function), PRP(Pseudo-Random Permutation), 또는 이상 암호(Ideal Cip her) 기반의 운영모드 증명방법으로는 이러한 차이를 반영한 안전성 분석이 불가능하다. 그러므로, 키스케줄의 복잡도가 반영되는 안전성 증명 기법의 개발은 경량 블록암호에 적합한 운영모드와 직결된다는 점에서 매우 흥미롭다.

참 고 문 헌

[1] J. Daemen and V. Rijmen, *The Design of Rijndael: AES - The Advanced Encryp tion Standard*, Springer, 2002.

[2] D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B. Koo, C. Lee, D. Chang, J. Lee, K. Jeong, H. Kim, J. Kim, S. Chee, “HIGHT: A New Block Cipher Suitable for Low-Resource Device,” *CHES 2006*, LNCS 4249, Springer, pp. 46-59, 2006.

[3] A. Bogdanov, L. R. Knudsen, G. Lea nder, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, C. Vikkelsoe, “PRE SENT: An Ultra-Lightweight Block Cipher,” *CHES 2007*, LNCS 4727, Spri nger, pp. 450-466, 2007.

[4] ISO/IEC 18033-3:2010, Information tech nology − Security techniques − Encrypt ion algorithms − Part 3: Block ciphers

[5] ISO/IEC 29192-2:2019, Information secu rity − Lightweight cryptography − Part 2: Block ciphers

[6] MJ.O. Saarinen, “Cryptographic Analysi s of All 4 × 4-Bit S-Boxes,” *SAC 2011*, LNCS 7118, Springer, pp. 118-133, 2011.

[7] L. Perrin, A. Udovenko, and A. Biryuko v, “Cryptanalysis of a Theorem: Decomp osing the Only Known Solution to the Big APN Problem,” *CRYPTO 2016*, LNC S 9815, Springer, pp. 93-122, 2016.

[8] S. Wu, M. Wang, and W. Wu, “Recursive Diffusion Layers for (Lightweight) Block Ciphers and Hash Functions,” *SAC 2012*, LNCS 7707, Springer, pp 355-371, 2012.

[9] S. M. Sim, K. Khoo, F. Oggier, and T. Peyrin, “Lightweight MDS Involution M atrix,” *FSE 2015*, LNCS 9054, Springer, pp. 471-493, 2015.

[10] M. Liu and S. M. Sim, “Lightweight MDS Generalized Circulant Matrices,” *FSE 2016*, LNCS 9783, Springer, pp. 101-120, 2016.

[11] Y. Li and M. Wang, “On the Constru ction of Lightweight Circulant involut ory MDS Matrices,” *FSE 2016*, LNCS 9783, Springer, pp. 121-139, 2016.

[12] N. Mouha, Q. Wang, D. Gu, and B. Preneel, “Differential and Linear Crypt analysis Using Mixed-Integer Linear Pr ogramming,” *Inscrypt 2011*, LNCS 7537, Springer, pp. 57-76, 2011.

[13] K. Fu, M. Wang, Y. Guo, S. Sun, and L. Hu, “MILP-Based Automatic Search Algorithms for Differential and Linear Trails for Speck,” *FSE 2016*, LNCS 9783, Springer, pp. 268-288, 2016.

[14] A. Biryukov, V. Velichkov, and Y. Le Corre, “Automatic Search for the Best Trails in ARX: Application to Block Cipher Speck,” *FSE 2016*, LNCS 9783, Springer, pp. 289-310, 2016.

[15] Z. Gong, S. Nikova, and Y. W. Law, “KLEIN: A New Family of Lightweight Block Ciphers,” *RFIDSec 2011*, LNCS 7055, Springer, pp. 1-18, 2011.

[16] D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B. Koo, C. Lee, D. Chang, J. Lee, K. Jeong, H. Kim, J. Kim, and S. Chee, “HIGHT: A New Block Cipher Suitable for Low-Resource Device,” *CHES 2006*, LNCS 4249, Springer, pp. 46-59, 2006.

[17] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Win gers, “The SIMON and SPECK Families of Lightweight Block Ciphers,” *Cryptol ogy ePrint Archive*: Report 2013/404.

[18] J. Guo, T. Peyrin, A. Poschmann, and M. Robshaw, “The LED Block Cipher,” *CHES 2011*, LNCS 6917, Springer, pp 326-341, 2011.

[19] J. Borghoff, A. Canteaut, T. Güneysu, E. B. Kavun, M. Knezevic, L. R. Knudse n, G. Leander, V. Nikov, C. Paar, C. Rechberger, P. Rombouts, S. S. Thomse n, and T. Yalçın, “PRINCE – A Low-Lat ency Block Cipher for Pervasive Comput ing Applications,” ASIACRYPT 2012, LN CS 7658, pp. 208-225, 2012.

[20] N. Mouha, B. Mennink, A. Van Herre wege, D. Watanabe, B. Preneel, and I. Verbauwhede, “Chaskey: An Efficient M AC Algorithm for 32-bit Microcontrollers,” SAC 2014, LNCS 8781, Springer, pp. 306-323, 2014.

[21] O. Dunkelman, N. Keller, and A. Sham ir, “Minimalism in Cryptography: The Even-Mansour Scheme Revisited,” EUR OCRYPT 2012, LNCS 7237, Springer, pp. 336-354, 2012.

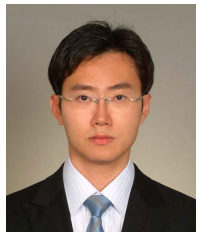
[22] S. Banik, S. K. Pandey, T. Peyrin, Y. Sasaki, S. M. Sim, and Y. Todo, “GIFT: A Small Present - Towards Reaching the Limit of Lightweight Encryption,” CHES 2017, LNCS 10529, Springer, pp. 321-345, 2017.

[23] L. Perrin, A. Udovenko, and A. Biryukov, “Cryptanalysis of a Theorem: Decomposing the only known Solution to the big APN Problem,” CRYPTO 2016, LNCS 9815, Springer, pp. 93-122, 2016.

[24] D. Roh, B. Koo, Y. Jung, I. Jeong, D. Lee, D. Kwon, and W.-H. Kim, “Revised Version of Block Cipher CHAM,” ICISC 2019, LNCS 11975, Springer, pp. 1-19, 2019.

[25] C. Beierle, G. Leander, A. Moradi, and S. Rasoolzadeh, “CRAFT: Lightweight Tweakable Block Cipher with Efficient Protection Against DFA Attacks,” IACR Transactions on Symmetric Cryptology, 2019(1), pp. 5-45.

〈저자소개〉



홍 득 조 (Deukjo Hong)

정회원

1999년 8월 : 고려대학교 수학과 졸업

2001년 8월 : 고려대학교 정보보호대학원 석사

2006년 2월 : 고려대학교 정보보호대학원 박사

2006년 3월~2007년 12월 : 고려대학교 정보보호기술연구센터 연구교수

2007년 12월~2015년 8월 : 국가보안기술연구소 선임연구원

2015년 9월~현재 : 전북대학교 IT정보공학과 부교수

<관심분야> 정보보호, 시스템 및 네트워크 보안