형태보존암호는 필요한가?

송정환 한양대학교 교수

1. 머리말

"닭 잡는 데 소 잡는 칼을 쓴다."라는 말이 있다. 필요한 것보다 과도하게 많은 비용을 지불할 때 이런 표현을 사용한다. 돈, 물, 에너지, 시간 등 현대 사회에서는 모든 것들을 아껴야 하는데 암호에도 이와 비슷하게 아껴야 하는 것들이 있다. 암호학자들은 경량암호를 개발하여 암호화에 드는 시간과 소비전력, 그리고 암호화에 필요한 메모리를 최대한 낮추었다. 그리고서 더 줄일 수 있는 게 없을까 고민하다 형태보존암호를 개발하게 되었다.

2. 형태보존암호

형태보존암호(Format-preserving encryption)란 평문과 암호문의 형태를 동일하도록 하게 하는 암호로서, 이때 형태는 일반적으로 정의역의 크기를 의미한다. 형태보존암호는 보통 작은 크기의 평문을 암호화할 때 사용하는데, 평문과 암호문의 형태가 동일하기 때문에 암호문의 크기가 평문의 크기만큼 되므로 일반적인 블록암호에서 상대적으로 긴 길이의 암호문을 전부 저장할 필요가 없게 된다. 예를 들어 16자리 10진수의 신용카드 번호 중 일부 6자리를 암호화한다고 하자. 만약 128비트 블록사이즈의 블록암호 AES를 이용하여 암호화한다면 암호문의 길이는 128비트 길이가 될 것이다. 평문인 6자리 10진수는 $10^6 \approx 2^{19.93}$ 이므로 약 20비트 길이밖에 안 되는데 암호문은 무려 6배 이상인 128비트 길이가 된다.

[그림 1] 신용카드 번호의 일반 블록암호화와 형태보존암호화

따라서 신용카드 회사에서 모든 카드번호를 암호화하여 저장한다면, 평문을 저장하는데 비해서 암호문을 저장하는데 필요한 저장용량이 6배 이상 된다.

그러나 형태보존암호를 사용하게 되면 어떨까? 형태보존암호를 이용하여 6자리 10진수의 신용카드 번호를 암호화하면 암호문은 마찬가지로 6자리 10진수가 된다. 따라서 평문 대신 암호문을 저장하는 데에 추가적인 저장용량이 필요하지 않게 된다. 그 외에도 다음과 같은 여러 장점들이 있다. 지금까지 개인정보를 비롯한 각종 정보를 암호화하지 않고 저장 및 사용하는 시스템을 가지고 있는 기업이 있다고 하자. 정부의 정책이나 다른 필요에 의해 그 정보들을 암호화 해야 하게 되는 경우, 이 기업에서 사용하던 시스템은 평문의 형태에 맞춰 작동하고 있었기 때문에, 이제는 암호문의 형태에 맞게 시스템이 운용될 수 있도록 주변 모든 시스템을 수정하거나 교체해야 한다. 이는 상당한 시간과 비용을 요하기 때문에 기업 입장에서 부담스럽다. 그러나 형태보존암호를 이용하는 경우 기존의 시스템을 그대로 사용할 수 있다. 기존의 시스템을 수정하거나 교체할 필요가 없게 된다.

이처럼 유용한 형태보존암호는 대표적으로 prefix cipher, cycle-walking cipher, VFPE, FF1, FF3-1, FEA 등이 있다. prefix cipher는 모든 평문에 대해 임의의 블록암호를 이용하여 암호문들을 얻고, 암호문들을 오름차순으로 정렬한 뒤에, 다시 복호화한 것을 제일 처음의 평문들의 prefix cipher 암호문으로 대응시키는 방식이다. 그러나 한번 암호화할 때마다 평문의 크기만큼 암호화를 하고 정렬해야 하므로 효율적이지는 않다. cycle-walking cipher는 임의의 블록암호에 대하여 원하는 형태의 암호문이 나올 때까지 계속 같은 키로 암호화하는 방식이다. 사용되는 블록암호에 비해 원하는 형태의 크기가 작으면 반복 횟수가 많이 증가할 수 있어 위험하다. VFPE(Visa Format Preserving Encryption)는 VISA 카드회사에서 채택한 형태보존암호로서 카운터 모드를 사용하는데, 각 카운터에서 얻어진 블록암호의 암호문에 법 연산을 취해 원하는 형태의 암호문을 얻는다. 예를 들어 카드번호인 16자리 10진수의 암호문은, 16개의 카운터로부터 얻어진 블록암호의 암호문들에 각각 법 10 연산을 취함으로써 얻을 수 있다. FF1, FF3-1은 미국 NIST 표준 형태보존암호로서 임의의 평문 길이에 모두 적용이 가능한 feistel 구조의 형태보존암호로 내부 F 함수로 일반 블록암호를 사용한다. 그리고 매 라운드에서 법 연산을 취함으로써 평문의 길이가 유지되도록 한다. 마지막으로 FEA는 한국의 국가보안기술연구소에서 개발한 형태보존암호로서 feistel 구조를 사용한다. 그러나 FF1이나 FF3-1과 달리 내부 F 함수로서 FEA 전용 함수를 사용하며, F 함수의 출력 길이를 조정하여 평문의 길이가 유지되도록 한다.

3. 형태보존암호의 표준화

형태보존암호는 처음에 산업계의 요구로 표준화의 필요성이 대두되었다. 2017년 10월 제55차 ISO/IEC JTC1 SC27 국제표준화 회의에서 한국대표단은 형태보존암호 FEA를 소개하여 산업계의 형태보존암호 표준화 요청에 따라 형태보존암호의 표준화 필요성을 제시하였다. 이에 따라 형태보존암호의 필요성과 적합성 검토를 위해 SP 'Suitability of standardization of format-preserving encryption schemes in ISO/IEC standards'가 시작되었다. 그리고 SP의 rapporteur는 한국 송정환 교수, co-rapporteur로 미국의 Lily Chen이 맡게 되었다. 그러나 이후 형태보존암호에 대하여 한국과 미국을 제외한 나라들에서 의견이 많이 나오지 않았고, 2018년 4월 중국에서 열린 제56차 ISO/IEC JTC1 SC27 국제표준화 회의에서 형태보존암호에

관한 의견을 많이 모으고자, 각국의 전문가들에게 구체적인 질문을 보내기로 의견을 모아 SP를 연장하였다. 이후 한국에서는 FEA-2를, 그리고 미국에서는 미국 NIST 표준 형태보존암호 FF1과 FF3를 표준화 후보 알고리즘으로 제안하였다. 그러나 형태보존암호가 작은 정의역을 갖는다는 특성을 이용한 키 복구 공격이나 코드북 공격 등으로 형태보존암호의 안전성이 우려된다는 프랑스와 러시아의 의견이 제시되었다. 이에 따라 작은 정의역 특성을 이용한 공격들에 대한 전반적인 논의를 위해 SP 기간을 다시 6개월 연장하였다. 작은 크기의 정의역을 이용한 공격은 상당히 효과적이어서 미국 NIST 표준 형태보조암호인 FF3는 코드북 공격으로 완전히 깨졌다. FF1과 한국의 FEA-2 또한 안전성 분석에서 자유롭지 못하였고, 이를 위해서 형태보존암호는 작은 정의역을 갖는다는 특성을 이용한 공격에 저항하기 위해 정의역의 최소 크기에 대한 제한이 필요하다는 의견이 나오게 되었다. 작은 크기의 정의역을 이용한 공격에서 한국의 FEA-2의 경우 정의역의 크기가 218 이상인 경우 안전하다는 결론이 나오게 되었는데, 이는 18비트 길이로 약 5자리의 10진수가 되는 매우 짧은 길이이다. 반면에 미국의 FF1과 FF3는 FEA-2의 분석에 적용한 것과 같은 조건에서 32비트 길이의 정의역 크기가 필요하였다. 특히 FF3는 코드북 공격으로 완전히 깨진 상황에서 알고리즘을 수정할 수밖에 없었고, 결국 FF3를 FF3-1로 수정하여 2019년 2월 28일 NIST 800-38G revision 1이라는 draft 문서를 발행하였다. 2019년 4월 이스라엘에서 열린 제58차 ISO/IEC JTC1 SC27 국제표준화 회의에서 러시아와 프랑스는 공통적으로 형태보존암호의 안전성 분석에 관하여 충분히 논의되지 않았으므로 표준화를 시작하기에는 시기상조라고 의견을 제시하였다. 이는 형태보존암호에 대한 공격이 비교적 적고, 발표된 논문들은 최근 2016~2018년에 몰려있기 때문이다. 마침 개선된 미국의 새 형태보존암호에 대한 공개검증이 4월 15일까지 완료되어야 하기 때문에 다시 SP 기간을 6개월 연장하기로 결정하였다.

4. 맺음말

형태보존암호의 표준화는 쉬운 일이 아니다. 한국과 미국을 제외한 나라들의 형태보존암호의 표준화 필요성에 대한 인식이 저조하기 때문에 이들을 설득하기 위해 한국에서는 2017년부터 형태보존암호의 표준화의 필요성과 적합성을 어필하기 위해 노력하였다. 이 중 필요성은 산업계의 요구와 이미 여러 분야에서 형태보존암호가 자체적으로 사용되고 있다는 점에서 충분하지만, 적합성에 앞에서 설명하였다시피 많은 의문이 있을 수 있다. 보통 ISO 등재암호기법들이 표준화되기 위해서는 최소 3년의 국제적인 공개검증 기간이 있어야 한다. 이를 성숙도라고 부르는데, 2014년 발표된 FEA는 이 조건을 만족하지만, 최근 개정된 FF3-1은 이 부분에 있어 의견이 나뉠 수 있다. 이뿐만이 아니다. 형태보존암호가 표준화가 시작된다고 해도, 어느 과제에 배치할지에 대하여 논의해야 한다. 사실 FF1과 FF3-1은 일반적인 블록암호를 내부함수로 사용하므로 암호화 운영모드라고 볼 수도 있다. 그러나 FEA는 전용 블록암호를 사용하므로 명확한 블록암호이다. 따라서 이들을 블록암호 표준 문서인 ISO/IEC 18033의 새 파트로 포함시킬지, ISO/IEC 10116(블록암호 운영모드)에 넣을지 아니면 새로운 과제번호로 생성할지 고려해야 한다.

급한 길도 돌아가라고 하였다. 이를 마음에 새겨 형태보존암호의 표준화는 긴 기간을 두고 조급해하지 말고 천천히 진행해야 할 것으로 사료된다.