Rijndael과 Crypton의 향상된 불능 차분공격

천정희∗ 김문주∗∗ 김광조∗ 이정연∗
∗한국정보통신대학원 대학교 ∗∗브라운대학교 수학과

Jung Hee Cheon∗, MunJu Kim∗∗, Kwangjo Kim∗, Jung Yeun Lee∗
∗Information and Communications University
∗∗Brown University

요 약

현재까지 5 라운드의 Rijndael과 Crypton에 대한 불능 차분공격이 제안되어 있지만 본 논문에서는 6 라운드의 Rijndael과 Crypton에 대한 불능 차분공격을 소개한다. 이 공격에서는 5 라운드 불능 차분공격에 사용된 것과 같은 4 라운드 불능 차분을 이용하고 있지만 4 라운드 불능 차분의 앞과 뒤에 한 라운드씩을 더하여 6 라운드 불능 차분공격을 완성하였다.

제 1 절 서론

Rijndael [6]과 Crypton [7]은 AES (Advanced Encryption Standard) 공모에 응모한 암호로서 Rijndael은 AES [1]로 최종 선정되었다. 이들은 모두 정방암호 [5]이며 confusion을 주는 비선형층과 diffusion을 주는 선형층이 교대로 나타나는 SPN구조를 가지고 있다. 이들 암호에 대한 공격은 여러 가지가 있을 수 있지만 설계 단계에서 이미 현존하는 공격들에 대하여 안전하도록 설계하였다. 그래서 두 암호는 차분공격과 선형공격을 비롯한 여러 공격들에 대하여 현재까지는 안전한 것으로 파악되고 있다. 이들 공격을 자세히 살펴보면 다음과 같다.

- *차분공격 (DC):* 차분공격은 몇 개의 라운드를 제외한 모든 라운드에 대하여 2^{1-n} 보다 상당히 큰 확률을 가진 예측 가능한 입출력 차분의 있어야 가능하다. 하지만 이들 암호는 4 라운드에 대하여 이러한 예측 가능한 차분을 찾을 수 없다.

- *선형공격 (LC):* 선형 공격은 몇 개의 라운드를 제외한 모든 라운드에서 $2^{n/2}$ 보다 훨씬 큰 확률을 가진 예측 가능한 입력과 출력의 상관관계가 있어야 가능하다. 하지만 이것 역시 4 라운드 이상에서는 이들 두 암호에 대하여 예측 불가능하다.

- *Square attack [3, 4]:* 이 공격은 정방암호를 처음 소개한 설계자에 의해 제안된 정방암호에 대한 공격방법이다. 이 공격은 선택평문 공격으로, 선형층과 비선형층을 이루는 함수들의 단사적 성질을 기반으로 Branch number를 활용하여 축소된 암호의 일부 입출력간의 단사적 성질을 찾아내는 공격이다. 그리고 그런 성질은 선형층 혹은 비선형층의 선택과 무관하다. 이 공격은 한 바이트를 제외한 모든 바이트를 제로로 갖는 모든 평문들에 대하여 고려하는 것으로부터 시작한다. 이들 평문들은 4 라운드의 암호화가 진행된 후에는 각각의 바이트에 대하여 256개의 서로 다른 바이트를 가지게 된다. 그래서 이들 256개의 암호문을 XOR 하면 모든 바이트에서 제로가 된다. 이러한 사실을 이용하여 앞 또는 앞뒤에 한 라운드씩을 붙이고 그 라운드의 라운드 키를 가정하여 공격함으로서, 5 라운드와 6 라운드의 Square Attack을 성공할 수 있었다 [3]. 최근에는

평문의 길이가 192 비트, 256 비트인 Rijndael에 대하여 7 라운드의 라운드 키를 모두 가정하여 7 라운드 공격을 성공하였다. [10].

- *불능 차분공격 [3, 9]:* 이들 두 암호에 대하여 하나의 바이트를 제외한 모든 바이트가 동일한 평문 쌍에 대하여 4 라운드 후의 암호문은 특정 바이트에 위치한 어느 바이트에서 동일할 수 없다. 우리는 그것을 불능 차분이라 부른다. 지금까지는 불능차분을 이용하여 5 라운드를 뒤쪽에 더하고 5 라운드 키를 가정하여 5라운드를 복호화한 후 위의 불능 차분에서 동일한 바이트가 나오는지를 확인하여 라운드 키를 찾아내는 방법을 통하여 5 라운드까지의 불능 차분공격을 진행하였다 [3, 9].

- 뿐만 아니라 이들 암호는 각 라운드마다 서로 다른 라운드 상수를 사용함으로서 Weak-key, Equivalent-key, Related-key를 이용한 공격도 불가능하도록 설계되었다.

앞에서 설명한 불능 차분공격에 쓰일 불능 차분은 비선형층의 성질과는 무관하며 단지 선형층의 성질과 관련되어 있다. 선형층은 비선형층의 confusion을 보다 많은 바이트로 확산시키는데 의미가 있다. 그래서 이들 암호의 설계자 들은 Confusion Power의 척도로 Branch number를 소개하였다.

정 의 1.1 (Branch number) *선형층의 함수를 F라 할때 Branch number는 $min_{a\neq0}(W(a)+W(F(a)))$ 이다. 여기에서 함수 $W()$는 각 바이트에 있는 1의 개수를 의미한다.*

Branch number를 이용하여 이들 두 암호가 갖는 선형층의 성질을 살펴보자.

- *Rijndael :* Branch number 5를 갖는다. 즉 선형층 (MC)의 입력 바이트 4개중에 하나의 바이트를 제외한 모든 바이트가 제로이면 선형층의 연산후에는 네개의 바이트가 모두 제로가 아니다.

- *Crypton :* Branch number 4를 갖는다 (설계자는 Diffusion orderf로 정의 하였다). 선형층의 입력 바이트 4개중에 하나의 바이트를 제외한 모든 바이트가 제로이면 선형층의 연산후 적어도 3개이 바이트에서 제로가 아니다.

위와같은 선형층의 성질을 이용하면 특정 입력 차분을 가정하였을 경우 4라운드 후에 절대 나타날 수 없는 불능 차분을 찾을 수 있다. 우리는 논문에서 이런 4 라운드의 불능 차분을 이용하여 앞과 뒤에 하나씩의 라운드가 더해진 6 라운드의 불능 차분공격을 진행하였다. 첫 라운드와 마지막 라운드의 라운드 키의 몇 바이트를 가정하여 사실상 4 라운드의 암호로 만들어 위의 4 라운드 불능 차분을 이용 가능하게 함으로서 6 라운드 불능 차분공격을 했다 .

이 공격의 복잡도는 6 라운드 Square attack의 복잡도 보다는 훨씬 더 크지만 여전히 전수조사 공격보다는 작다. 우리는 이 공격방법이 다른 SPN구조의 암호에도 적용 가능할 것으로 기대한다.

이 논문은 2장과 3장에서 각각 Rijndael과 Crypton 대한 소개와 그에 대한 6 라운드 불능 차분공격을 제안한다. 마지막으로 4장에서 이 논문의 결론을 정리하도록 하겠다.

제 2 절 Rijndael

2.1 Rijndael

Rijndael은 블록암호이다. 블록의 길이와 키의 길이는 128, 192 그리고 256 비트로 정해져 있으며, 이들의 길이는 독립적으로 결정된다. 이 논문에서는 128 비트의 블록과 128 비트의 키를 가정한다. 이 경우에 이 암호는 10 라운드로 구성된다. 그리고 각 데이터는 4×4 행렬에 128 비트 단위로 그림 1에서 처럼 표현된다 (각 위치마다 1바이트씩 놓이게 된다). 마지막 라운드를 제외한 모든 라운드는 다음과 같은 4개의 층으로 구성되어 있다.

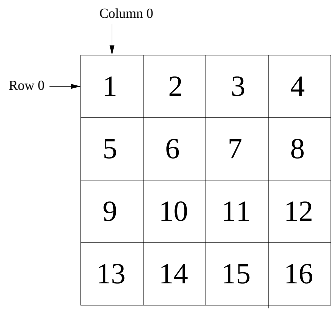

그림 1: 128 비트의 바이트 조합

- *ByteSubstitution (BS):* 유일한 비선형층으로 S-box를 이용하여 데이터의 각 바이트에 적용된다.
- *ShiftRow (SR):* 각 행에 대하여 바이트 단위로 순환적으로 우측으로 옮긴다. 블록의 길이에 따라 우측으로 순환하는 바이트의 크기는 결정된다.
- *MixColumn (MC):* 각 열에 적용되는 선형 변환이다. MC의 Branch Number는 5이다. 이 성질에 의해 4 라운드 불능 차분의 정리가 유도된다.
- *AddRoundKey (ARK):* 각 라운드 키를 XOR를 한다 .

첫 번째 라운드가 시작되기 전에 ARK를 라운드 키로서 키를 사용하여 수행한다. 그리고 마지막 라운드에서는 MC가 생략된다. 여기에서 우리는 MC가 하나의 열에 대하여, 즉, 네개의 입력 바이트들에 대한 선형변환이기 때문에, 입력 차분에 대하여 생각해 보면 MC는 여전히 입력 차분에 대해서도 선형변환임을 확인할 수 있다. 그리고 MC는 일대일대응이므로, 출력 차분이 네개중에 세개의 바이트가 제로인 입력 차분의 가짓수는 $(2^8 - 1)$개임을 쉽게 알 수 있다. 출력 차분의 제로가 아닌 바이트의 선택에 있어서 4가지가 있기 때문에 세개의 바이트에서 출력 차분이 제로가 될 확률은 약 $4 \times (2^8)/2^{32}$이다.

정리 2.1 *MC의 출력 (또는 MC^{-1})이 세개의 바이트에서 제로 차분을 가질 확률은 모든 입력쌍에 대하여 약 2^{-22}이다.*

이 정리는 고정된 바이트들에 대하여 입력 차분의 값이 제한적일 때도 여전히 성립한다. 우리는 이 정리를 제안하는 불능 차분공격의 복잡도를 계산하는데 사용할 것이다.

2.2 불능 차분

우리는 [3]에서 설명 되고 있는 것과 동일한 불능 차분을 이용한다.
아래 그림에서 잘 설명되고 있다.

MC의 출력에서는 MC의 Branch Number가 5이기 때문에 그 바이트가 위치한 열에 있는 모든 바이트가 서로 달라진다. 그러면 이제 오직 하나의 바이트만이 서로 다른 두개의 평문쌍을 고려해보자. 첫 번째 라운드의 MC의 출력에서는 그 바이트가 위치한 열에 있는 모든 바이트가 서로 달라진다. 그리고 두 번째 라운드의 SR에 의해 그 바이트들은 각 열에 하나씩 놓이게 된다. 그 후 두 번째 라운드의 MC에 의해 결과적으로 16개의 모든 바이트에서 달라지게 된다. 이것이 다음의 재미있는 성질을 만들어낸다.

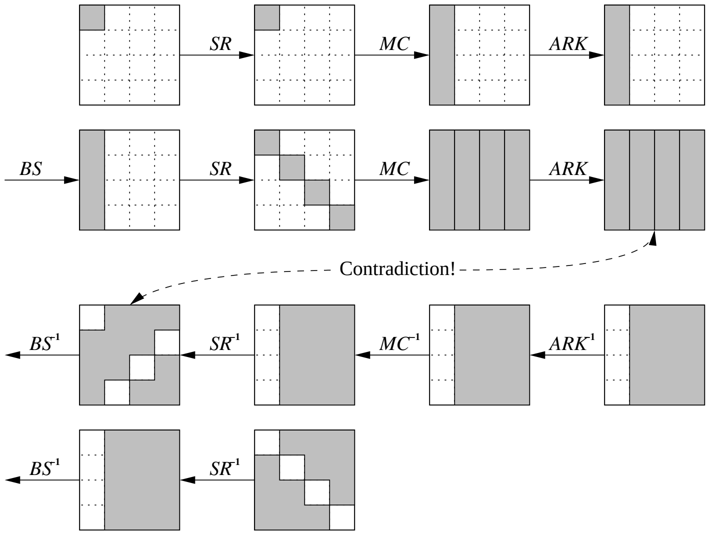

그림 2: 4라운드 Rijndaeld의 불능 차분

정 리 2.2 (Rijndael의 불능 차분 성질) *하나의 바이트를 제외한 모든 바이트가 동일한 평문 쌍에 대하여 4라운드 후의 암호문은 다음의 금지된 조합에 위치한 어느 바이트도 동일할 수 없다: (1,6,11,16), (2,7,12,13), (3,8,9,14),(4,5,10,15).*

이 성질을 이용하여 이미 4 라운드와 5 라운드의 불능 차분공격은 제안 되었다. 우리도 역시 이 성질을 이용하여 6 라운드 불능 차분공격을 할 수 있었다.

2.3 6라운드의 Rijndael

이 장에서는 Rijndael의 6 라운드 불능 차분공격을 자세히 설명한다. 공격은 4 라운드의 불능 차분공격을 바탕으로 그림 3 에서 처럼 시작과 끝부분에 하나씩의 라운드를 더하여 6 라운드의 불능 차분공격을 완성하였다. 여기에서 우리는 Rijndael의 마지막 라운드의 MC는 생략됨을 유념해야 한다.

6라운드 불능 차분공격은 다음의 순서를 따른다:

1. 하나의 structure를 (1,8,11,14)의 네개의 바이트를 제외한 모든 바이트가 고정된 값을 갖는 평문들의 집합으로 정의하자. 그러면 하나의 structure는 2^{32}개의 평문과 $2^{32} \times 2^{32} \times \frac{1}{2} = 2^{63}$개의 평문 쌍으로 이루어져있다.

2. $2^{59.5}$개의 structures : ($2^{91.5}$ 평문, $2^{122.5}$ 평문쌍)를 택하자. 그리고 각 평문 쌍을 암호화하여 암호문 쌍이 행 2와 3에서 제로 차분을 갖는 평문 쌍을 고르자. 그와 같은 평문 쌍의 개수에 대한 기대치는 $2^{122.5} \times 2^{-64} = 2^{58.5}$이다.

3. 그 후 마지막 라운드키 K_6의 행 0과 1의 64 비트를 가정하자.

4. 각 암호문쌍 (C, C^*)에 대하여, $C_5 = BS^{-1} \circ SR^{-1}(C + K_6)$와 $C_5^* = BS^{-1} \circ SR^{-1}(C + K_6)$를 구하자. 그리고 그들의 MC의 역상에 의한 차분 $MC^{-1}(C_5 + C_5^*)$이 금지된 네개의 바이트 조합 (1,6,11,16), (2,7,12,13), (3,8,9,14), (4,5,10,15)에서 제로가 되는 쌍들을 택하자. 각 평문 쌍에 대하여 이렇게 될 확률은 $p = 2^{-32} \times 4 = 2^{-30}$이고 택해지는 평문 쌍의 개수에 대한 기대치는 $2^{58.5} \times 2^{-30} = 2^{28.5}$이다.

5. 위에서 택해진 평문 쌍과 첫 번째 라운드키 K_0의 네개의 바이트(1,8,11,14)의 2^{32}개의 비트 값들에 대하여

$$MC \circ SR(BS(P + K_0) + BS(P^* + K_0))$$

를 계산하고, 이들중 오직 하나의 바이트를 제외한 모든 바이트에서 제로 차분을 가지는 쌍을 고르자. MC는 일대일대응이기 때문에 위의 경우가 일어날 확률은 약 $q = 2^{-24} \times 4 = 2^{-24}$이다.

6. 하지만 Step 4와 Step 5에서 나타나는 바이트의 조합은 동시에 나타날 수 없기때문에 그러한 차분을 만들어 내는 모든 키는 잘못된 키이다. 여기에서 우리는 2^{96}개의 키쌍 (K_0, K_6)을 가정하고 있고 각각의 키쌍에 대하여 확률 2^{-52}로 불능 차분공격을 하고 있다. Step 2를 통과한 암호문 쌍을 분석한 후에는 약 $2^{32}(1-2^{-22})^{2^{28.5}} \approx 2^{32}e^{-2^{6.5}} \approx 2^{-98.5}$개의 잘못된 키쌍 (K_0, K_6)만이 남게된다. 즉, 옳지 못한 키쌍이 위의 과정을 모두 통과할 가능성이 희박하다. 같은 방볍으로 Step 2에서 Step 5까지를 2와 3행에서 0과 1행으로 바꾸어 실행해보면 6 라운드키 전체를 얻을 수 있다.

7. Step 4에서는 가정하고 있는 64 비트의 키로 $2^{28.5}$개의 평문 쌍에 대한 연산이 이루어지므로 한 라운드 연산을

$$2^{123.5} (= 2 \times 2^{64} \times 2^{58.5})$$

정도 요구한다. Step 5에서는 많아야

$$2^{64} \times 2^{28.5} \times 2^{32} \times 2 = 2^{125.5}$$

정도의 연산량을 요구한다. 하지만 한번 잘못된 키로 판명된 키에 대하여는 더 이상의 연산이 필요 없기 때문에 기대되는 연산량은

$$2^{64} \times 2 \times 2^{32}\{1 + (1-2^{-22}) + (1-2^{-22})^2 + \cdots + (1-2^{-22})^{2^{28.5}}\} \approx 2^{119}$$

이다. 그래서 Step 5에서의 한 라운드 연산으로 약 2^{119}정도 요구한다. 결과적으로 우리가 위의 과정을 두 번 반복하면 이 공격에는 약 $2^{91.5}$개의 선택된 평문이 필요하며 6 라운드 Rijndael의 2^{122}번의 암호화가 필요하다.

제 3 절 Crypton

3.1 Crypton

Crypton은 128 비트의 블록암호이다. 각 평문 128 비트의 데이터를 4×4 행렬에 그림 1에서처럼 나타내고 일련의 라운드 함수를 이용하여 암호화한다. 각 라운드 함수는 다음의 4단계를 거친다.

- γ는 바이트 단위의 비선형 대체함수이다. γ는 두 종류의 버전이 있다: 홀수 라운드에 쓰일 γ_o와 짝수 라운드에 쓰일 γ_e가 있다.

- π는 비트단위의 선형 치환함수이다. 이것은 각 열에 있는 4바이트를 섞는다. 이것도 역시 두개의 버전이 있다: 홀수 라운드에 쓰일 π_o와 짝수 라운드에 쓰일 π_e가 있다. 중요한 것은 이들 두 버전 모두 4바이트의 입력과 출력을 갖는 함수로서 branch number 4를 갖는다는 것이다.

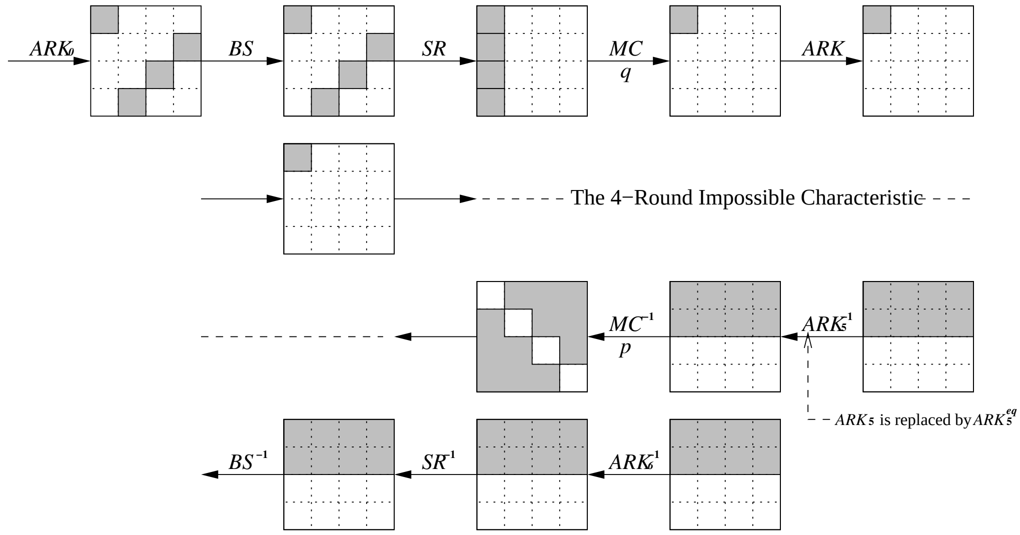

그림 3: Rijndael의 6 라운드 불능 차분공격

- τ는 선형 변환이다. A$[i][j]$의 바이트는 A$[j][i]$로 변환된다.
- σ는 라운드 키를 XOR한다. 주어진 키가 K일때 이 함수를 σ_K로 표시한다.

Crypton의 $2n$라운드 암호화는 다음과 같이 수행된다.

$$\phi_e \circ \rho_{e_{K_{2n}}} \circ \rho_{o_{K_{2n-1}}} \cdots \circ \rho_{e_{K_2}} \circ \rho_{e_{K_1}} \circ \sigma_{K_0},$$

여기에서 $\rho_{o_{K_i}} = \sigma_{K_i} \circ \tau \circ \pi_o \circ \gamma_o$는 홀수 라운드 버전이고, $\rho_{e_{K_i}} = \sigma_{K_i} \circ \tau \circ \pi_e \circ \gamma_e$는 짝수 라운드 버전이다. 그리고 선형변환 $\phi_e = \tau \circ \pi_e \circ \tau$는 마지막 라운드에서 사용된다.

3.2 불능 차분

먼저 Crypton의 4 라운드 불능 차분을 소개하면 그림 4에서 처럼 불능 차분의 한 패턴이 나타난다. 이와 같은 불능 차분은 아래의 사실로 부터 발견되어진다.

1. 만약 입력 쌍의 차분이 하나의 바이트에서 제로이면, σ, γ, σ^{-1}, 또는 γ^{-1}의 출력 쌍의 차분은 동일한 바이트에서 제로이다.
2. 입력 차분이 한 바이트 $[i][j]$에서 제로 차분을 가지면, τ 또는 τ^{-1} 의 출력의 $[j][i]$바이트의 차분은 제로이다.
3. π는 워드 변환으로서 branch number가 4이다. 즉 입력 쌍이 네개의 바이트중 오직 하나의 바이트에서만 차분이 제로이면 출력 차분은 적어도 세개의 바이트에서 제로 차분을 갖지 않는다.

정 리 3.1 (Crypton의 불능 차분) *하나의 바이트를 제외한 모든 바이트에서 제로 차분을 갖는 τ의 입력 쌍에 대하여 τ로 시작하여 γ로 끝나는 4 라운드 Crypton의 출력 쌍의 차분은 첫 번째와 두 번째 열의 두행을 제외한 모든 바이트에서는 제로일 수 없다.*

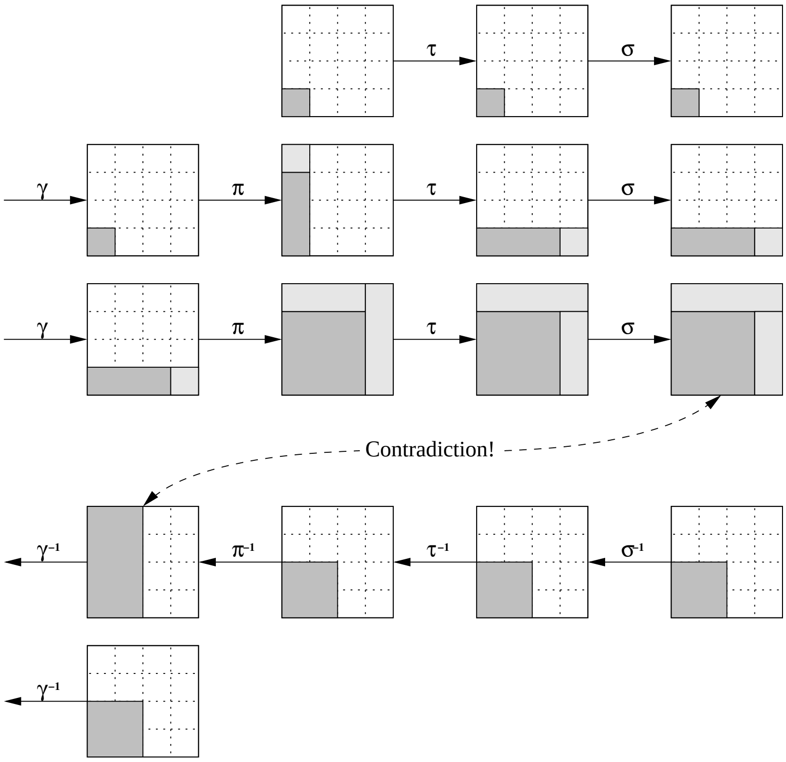

그림 4: Crypton의 4 라운드 불능 차분

3.3 6라운드 Crypton의 불능 차분공격

이 장에서 우리는 6 라운드 Crypton의 불능 차분공격을 제시한다. 이 공격은 4 라운드 불능 차분에 바탕을 두고 있으며, 그림 5에서 처럼 6 라운드 불능 차분공격을 설명할 것이다. σ_{K_5}와 σ_{K_6} 는 제로 키를 사용한 σ_{null}로 대신할 것이다. 그리고 5 라운드와 6 라운드의 γ와 π 사이에 $\sigma_{K_5^{eq}}$ 와 $\sigma_{K_6^{eq}}$를 각각 수행하게 함으로서 동일한 암호화 시스템을 구성할 수 있다. 여기에서 K^{eq}는 동일한 키 즉, $\pi_e^{-1} \circ \tau^{-1}(K)$ 을 의미한다.

Crypton의 불능 차분공격은 다음과 같다:

1. 하나의 structure를 1, 2, 3열을 특정 값으로 고정시킨 평문들의 집합으로 정의한다. 하나의 structure는 2^{32}개의 평문으로 구성되어 있고 $2^{32} \times 2^{32} \times \frac{1}{2} = 2^{63}$개의 평문 쌍을 만들어 낼 수 있다.

2. 2^{59}개의 structures : (2^{91}개의 평문, 2^{122}개의 평문 쌍)을 택하자. 각 평문P의 암호문C에 대하여 $C_6 = \pi_e^{-1} \circ \tau^{-1} \circ \sigma_{null} \circ \tau^{-1} \circ \pi_e^{-1} \circ \tau^{-1}(C)$을 구하자. 다음으로 암호문 쌍 (C_6, C_6^*)의 0행과 1행의 차분이 제로인 평문 쌍 (P, P^*)을 고르자. 그런 쌍의 개수의 기대치는 $2^{122} \times 2^{-64} = 2^{58}$이다.

3. 마지막 라운드키 K_6^{eq}의 2행과 3행의 64 비트 값을 가정하자.

4. Step 2를 만족하는 각각의 암호문 쌍 (C_6, C_6^*)에 대하여, $C_5 = \gamma_e^{-1}(C_6 + K_6^{eq})$와 $C_5^* = \gamma_e^{-1}(C_6^* + K_6^{eq})$를 구하고 그들의 차분 $\pi_o^{-1} \circ \tau^{-1}(C_5 + C_5^*)$이 임의의 두행에서 제로인 쌍을 고르자. 그것의 확률은 $p = 2^{-32} \times 6 \approx 2^{-29.5}$이기 때문에, 남는쌍의 기대치는 $2^{58} \times 2^{-29.5} = 2^{28.5}$이다.

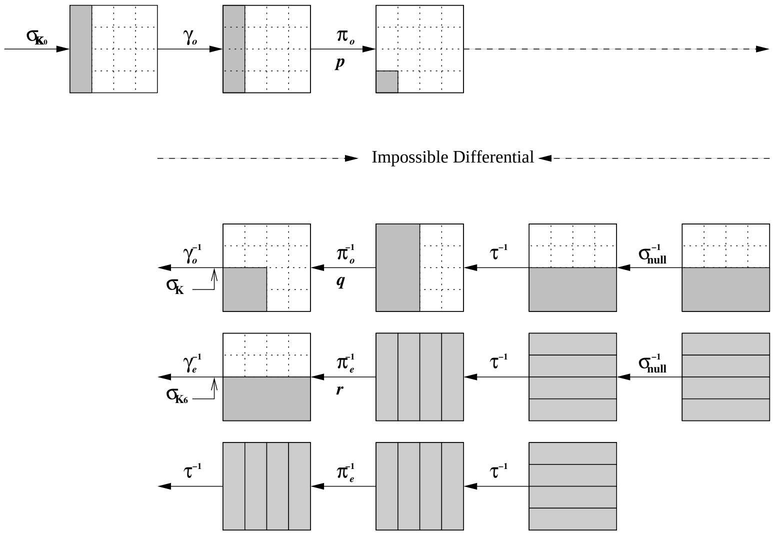

그림 5: Crypton의 6 라운드 불능 차분공격

5. Step 4를 만족하는 평문쌍 (P, P^*)에 대하여 $\pi_0(\gamma_o(P+K_0)+\gamma_o(P^*+K_0))$의 첫 번째 열이 한 바이트를 제외한 모든 바이트에서 제로가 되도록하는 K_0의 첫 번째 열의 32 비트 값을 고려하자. 그러면 각 키에 대하여 위의 사건이 일어날 확률은 $q = 2^{-24} \times 4 = 2^{-22}$이다.

6. 하지만 Step 4와 Step 5에서 고려하는 차분이 동시에 나타날 수 없기 때문에 그러한 차분을 생성하는 모든 키는 Step 3에서 선택된 키 K_6^{eq}와 함께 불능키가 된다. $2^{28.5}$개의 평문 쌍을 분석한 후에는 K_0의 첫 번째 열의 네 바이트에 대하여 약 $2^{32}(1-2^{-22})^{2^{28.5}} \approx 2^{32}e^{-2^{6.5}} \approx 2^{-98.5}$정도의 키쌍만이 남게된다. 사실상 남아 있을 가능성이 없게 되는것이다.

7. 마지막 라운드키 K_6^{eq}에 대한 처음의 가정이 옳지 못하면, 잘못된 (K_0, K_6^{eq})이 확률 $2^{64} \times 2^{-98.5} = 2^{-34.5}$로 남아 있을 수 있기 때문에 K_6^{eq}의 각각의 64 비트 값에 대하여 K_0의 32 비트 전체 값을 제거할 수 있다. 그렇기 때문에 K_0의 하나의 값이 남아 있다면 우리는 키 K_6^{eq} 가 옳다고 가정할 수 있다. 그러면 우리가 0행과 1행을 2행과 3행으로 바꾸어 Step 2에서 Step 6를 반복하면 K_6^{eq}의 전체 값을 얻을 수 있다.

8. 계산량을 살펴보면 Step 2는 $\pi_e^{-1} \circ \pi_e^{-1} \circ \tau^{-1}$의 약 $2^{123}(= 2 \times 2^{122})$정도의 계산량을 요구한다. Step 4는 $\pi_o^{-1} \circ \tau^{-1} \circ \sigma^{-1}$의 약 $2^{125.5}(= 2^{64} \times 2 \times 2^{60.5})$정도의 계산량을 요구하며 Step 6는

$$2^{64} \times 2 \times 2^{32}\{1 + (1-2^{-22}) + (1-2^{-22})^2 + \cdots + (1-2^{-22})^{2^{28.5}}\} \approx 2^{119}$$

이기 때문에 $\pi_o \circ \gamma_o$ 의 약 2^{119}정도의 계산량을 요구한다. 결과적으로 우리는 이 과정을 두 번 반복하므로, 이 공격은 약 2^{91}정도의 선택평문이 필요하며 2^{124} 정도의 6 라운드 Crypton의 암호화가 요구된다.

3.4 메모리를 이용한 불능 차분공격의 변형

이 장에서는 앞장에서 제시한 불능 차분공격의 메모리공간을 이용한 변형을 소개한다.

Precomputation Stage 오직 하나의 바이트에서만 서로 다른 첫 번째 열 안에 있는 네개의 바이트의 $2^{32}\times 2^{8}\times 4 = 2^{42}$개의 모든 쌍을 고려하자 (이 데이터는 첫 라운드의 σ는 수행하기 전까지의 암호화가 이루어진 데이터이다.) 이들 쌍에 대하여 다시 첫 라운드 복호화 즉, τ^{-1}, π^{-1}, γ^{-1}를 행하고 γ변환의 입력중의 하나와 γ변환의 입력 x와 y의 XOR ($x \oplus y$로 표시)를 포함한 해쉬 데이블을 만든다.

Step 4' 먼저 $2^{93.5}$개의 모든 암호문에 대하여 $\pi^{-1}\circ\gamma^{-1}\circ\pi^{-1}\circ\tau^{-1}$를 수행하고, 암호문 C와 그것의 π^{-1} 변형을 한 후의 결과물인 U_C를 하나의 쌍 (C, U_C)으로 저장한다. 각각의 암호문 쌍 (C, C^*)에 대하여, U_C와 U_{C^*}를 비교하고 그들의 차분$U_C + U_{C^*}$이 0행과 1행에서 제로가 되는 쌍을 고르자. 그 확률이 $p = 2^{-32}$이기 때문에, 남는 쌍의 개수에 대한 기대치는 $2^{60.5}\times 2^{-32} = 2^{28.5}$이다.

Step 5' Step 4'를 만족하는 암호문 쌍에 대한 평문 쌍 (P, P^*)들에 대하여 우리는 $x\oplus y$를 하고 해쉬테이블을 이용하여 그 계산된 $x\oplus y$에 대응하는 약 2^{10}개 정도의 x를 찾을 수 있다. 이 과정을 통해 평문과 위의 x들을 XOR를 하여 2^{10}정도의 잘못된 키를 찾을 수 있다.

우리가 만약 Precomputation을 이용하여 Step 4와 Step 5를 Step 4'와 Step 5'로 대신하면 복잡도는 다음과 같다:

- Step 4는 $2^{93.5}$번의 $\pi^{-1}\circ\gamma^{-1}\circ\pi^{-1}\circ\tau^{-1}$ 연산과 two times memory access 연산을 $2^{124.5}$만큼 해야한다. 그러면 6 라운드 Crypton 보다 2^{14} 정도 빠르기 때문에 Step 4는 $2^{110.5}$정도의 암호화와 같다. 그리고 Step 4에서 $2^{93.5}\times 128\times 128 = 2^{104.5}$의 memory가 필요하다.

- Step 5'에서 $2^{28.5}$개의 남는 평문 쌍에 대하여 각각의 가정된 키 (K_6^{eq})를 이용하여 2^{32}정도의 암호화가 필요로 하는 x와 평문의 XOR를 통하여 2^{10}개의 불가능키를 제거할 수 있다.

- 종합해 보면, 이 공격은 $2^{93.5}$개의 평문과 $2^{110.5}$번의 암호화 그리고 $2^{104.5}$바이트의 메모리가 필요하다.

암호	공격	라운드	선택 평문의 수	복잡도
Rijndael	Square Attack	6라운드	2^{32}	2^{72}
	불능 차분공격	5라운드	$2^{29.5}$	2^{31}
		6라운드	$2^{91.5}$	2^{122}
Crypton	불능 차분공격	6라운드	2^{91}	2^{124}

표 1: 각 암호에 대한 6 라운드 공격의 복잡도

제 4 절 결론

이 논문에서 우리는 Rijndael과 Crypton의 6 라운드 불능 차분공격을 소개했다. 6라운드 Rijndael에 대한 공격은 약 $2^{91.5}$ 정도의 선택평문과 2^{122}번의 암호화가 필요하다. 6 라운드 Crypton에 대한 공격은 약 2^{91} 정도의 선택평문과 2^{124}번의 암호화가 필요하다. 또는 $2^{93.5}$ 개의 평문과 $2^{110.5}$번의 암호화와 $2^{104.5}$ 바이트의 메모리가 필요하다 [표1]. 우리는 이 방법이 SPN 구조의 대부분의 블록 암호에 대하여 적용 가능할 것으로 기대한다.

참고 문헌

[1] The Advanced Encryption Standard, *http://www.nist.gov/aes.*

[2] E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems," J. of Cryptology, Vol. 3, pp.27-41, 1990.

[3] E. Biham and N. Keller, "Cryptanalysis of Reduced Variants of Rijndael," *http://csrc.nist.gov/encryption /aes/round2/conf3/aes3papers.html.*

[4] C. D'Halluin, G. Bijnens, V. Rijmen, and B. Preneel, "Attack on Six Rounds of Crypton," Proc. of Fast Software Encryption'99, Lecture Notes in Computer Science Vol. 1636, pp. 46 – 59, Springer-Verlag, 1999.

[5] J. Daemen, L. Knudsen, and V. Rijmen, "The Block Cipher Square," Proc. of Fast Software Encryption'97, Lecture Notes in Computer Science Vol. 1267, pp. 149–165, 1997.

[6] J. Daemen and V. Rijmen, "AES Proposal: Rijndael," *http://csrc.nist.gov/encryption /aes/rijndael/.*

[7] C. Lim, "A Revised Version of Crypton - Crypton V1.0," Proc. of Fast Software Encryption'99, Lecture Notes in Computer Science Vol. 1636, pp. 31 – 45, Springer-Verlag, 1999.

[8] M. Matsui, "Linear Cryptanalysis Method for DES cipher," Proc. of Eurocrypt'93, Lecture Notes in Computer Science Vol. 765, pp.386 – 397, Springer-Verlag, 1993.

[9] H. Seki and T. Kaneko, "Cryptanalysis of Five Rounds of CRYPTON Using Impossible Differentials," Proc. of Asiscrypt'99, Lecture Notes in Computer Science Vol. 1716, pp.43-51,1999.

[10] Stefan Lucks, "Attacking Seven Rounds of Rijndael under 192-bit and 256-bit Keys," Proc. of Third AES Candidate Conference, AES3, 2000.