암호 알고리즘의 발전 방향

지도교수 : 김 윤
연 구 자 : 노 현 기

< 목 차 >

요 약

고대부터 다양한 국가, 계급 등 특정한 사람들만 사용하던 암호가 현재에 이르러서는 개인마다 암호를 사용하고 수학과 물리학의 발전으로 다양한 기계적 장치와 이를 기반을 둔 알고리즘이 등장하여 사용되어왔다. 수학의 발전과 동시에 발전해온 암호학을 고대 로마 시대부터 현재까지 사용된 알고리즘 소개와 구조 파악부터 차세대 기용될 알고리즘까지 파악하고 이해하는 시간을 가져본다. 각 알고리즘을 수학적, 구조적으로 구분과 이해를 통해 알고리즘마다 특징과 흐름을 파악한다. 특히 암호에서 중요한 요소인 키의 생성과 사용을 중점으로 살펴보고 알고리즘마다 키를 알아내기 어려운 이유를 살펴본다. 암호화의 흐름 분석을 통해 알고리즘들을 대조 및 비교하고 나날이 발전하는 기술과 장치, 수학적 알고리즘을 위한 배경을 고려한다.

주요어 : 암호, 알고리즘, 암호화, 해시, 공개키, 대칭키, 키

1. 서론

1.1. 암호의 배경

암호(crypto)는 국가 개념의 등장 이전부터 사용됐으나 국가가 형성되고 나선 나라 간의 경쟁을 위해 암호를 적극 사용하기 시작했다. 중세시대까지의 암호는 특정 계층, 권력층, 국가가 통솔하는 집단 혹은 분야에서 한정적으로 사용되어왔다. 이 당시는 컴퓨터 같은 고 기술 기계적 장치가 없었기에 그 당시 암호를 사용하는 이들은 가죽이나 종이에 특정 암호문을 적어 근현대 암호화 알고리즘에 비해 간단한 방식의 암호화 알고리즘을 사용해왔다.

대표적인 방식으로는 전치(transposition) 암호와 치환(substitution) 암호, 악보 암호, 다중 치환 암호 등이 있다. 암호를 사용하는 배경, 방식이 단순하고 간단했기에 현대인들의 시점에서는 부실한 암호로 보이게 된다. 그리고 앞서 언급했듯 제한된 각종 전자 기기나 비전자 기기에도 보안을 설정하고 사용하는 현대인들과 달리 오래전에는 특정 계급, 집단에서 사용했기에 현대보다 제한적으로 사용됐다.

1.2. 근현대 암호

중세시대까지의 암호와 20세기 이후 근현대 암호와는 크고 작은 사건으로 특징이 판이해졌다. 산업 혁명, 세계 1차, 2차 전쟁, 냉전 등의 상황이 발발하면서 과학과 기술이 급격하게 발전하였고 그렇게 발전한 과학기술로 전기와 기계를 더 직접 다룰 수 있게 되었다. 이후로 근대의 대표적인 암호인 에니그마(ENIGMA) 같은 암호화 알고리즘이 등장했고 이후로는 컴퓨터 같은 고성능 기기와 네트워크의 등장과 현대에 들어서 이동식 전자 기기의 등장과 하드웨어와 소프트웨어의 발전, 인터넷의 발전으로 암호 역시 급격한 발전을 이루게 되었다.

근현대 암호와 기존 암호와 차별화된 특징으로는 대중성과 복잡성, 신체 친화도, 제한된 시간, 전기적/수학적 특성을 말할 수 있다. 수학의 발전으로 인류가 전기를 다룰 수 있게 되면서 전기를 사용하는 계산에 최적한 기계를 사용하면서 단순한 알고리즘을 사용하는 암호는 가치가 떨어지게 되었다. 발전과 제약으로 암호를 사용하는 사람은 더욱 복잡하고 방대한 값을 지닌 암호를 사용하거나 고유한 특징 즉, 유일성을 지닌 것을 사용하기 시작했다. 복잡하고 큰 값을 지닌 암호는 DES나 RSA 등이 있고 유일성을 요구하는 암호는 지문이나 홍채 등 인간의 신체 부위를 사용하는 암호 혹은 제한된 시간에만 인증을 확인해야만 하는 원 타임 패드(one-time-pad, OTP)를 사용하고 있다.

현대는 정보의 시대라고 불리는 만큼 정보가 큰 가치를 지니고 수많은 시각은 이를 민감하게 바라보고 있다. 이제는 이동식 전자 기기와 무선 통신 기술이 등장하고 발전하면서 특정 계층만이 사용하는 것이 아닌 다양한 사람들이 암호를 사용하기 시작했고 더 나아가 암호보단 광범위하고 총괄적인 의미로 사용되는 보안에 중점을 두고 있다. 그만큼 현대인들에게는 각각 다른 형태의 암호를 다양한 분야, 기기 등에 사용한다. 더욱이 개인 정보의 중요성이 대두하는 요즘 날에는 이를 지켜내기 위해 개개인들이 다양한 보안 방법을 사용한다.

1.3. 기밀성을 위한 암호학적 요소

암호에서 중요한 두 가지 요소가 있다. 키와 난수다. 키는 암호화 및 복호화에 사용되는 값으로 키는 대칭키와 공개키로 구분된다. 대칭키는 암호화와 복호화에 필요한 키가 같은 경우이고 공개키는 암호화와 복호화에 필요한 키가 다른 경우를 말한다. 따라서 암호에서는 제삼자는 해독하기 불가능하여야 하고 수신자는 복호화가 정상적으로 가능한지를 결정짓는 것은 키다.

그러한 키를 결정짓는 것은 수학적으로 만들어진 값이나 난수(random number)를 많이 사용한다. 난수를 사용함으로써 키의 일관성이 없어 보이는 것처럼 효과를 보이거나 수학적 복잡성을 지니거나 매우 큰 값을 사용함으로써 보안에 대한 좋은 효과를 기대할 수 있다. 사실 기본적으로 사용되는 난수에는 정해진 테이블이 있어 온전한 난수가 될 수 없지만, 특정 값을 기준으로 난수 테이블을 만들거나 앞서 말한 수학적으로 복잡성을 띠거나 매우 큰 수를 난수로 사용하여 이러한 문제를 해결할 수 있다.

2. 본론

2.1. 암호화 알고리즘 종류와 분류

2.1.1. 중세시대까지 암호화 알고리즘

중세시대부터 사용된 대표적인 암호화 알고리즘은 환자 암호(Substitution cipher)와 전치 암호(transposition cipher)가 있다.

전치 암호는 문자의 위치를 재배치하여 암호화하는 방식이다. 우선, 키가 없는 방식은 무작위 배열로 문자를 재배치한다. 키를 사용하는 방식은 행 또는 열에 우선순위를 키를 통해 각 행 또는 열마다 키를 바꾸거나 일관된 문자 재배치를 통해 암호화하는 방식이다. 대표적으로는 스키테일(scytale) 방법이 있다. 특정 굵기의 막대에 가죽을 전체적으로 둘러 감는다. 이 감아진 가죽에 옆으로 평문을 적어 풀어낼 시 이상한 문자열로 보이게 하는 방법이다. 이를 복호화하기 위해선 수신자도 같은 굵기의 막대를 가지고 가죽을 감아야 한다.

환자 암호는 각 평문 문자를 암호 문자와 1:1 대응하여 암호화하는 방식이다. 또한, 환자 암호 내에서 대표적으로 시프트 암호와 단순 환자 암호, 다표식 암호가 있다. 시프트 암호(카이사르 암호, Caesar cipher)는 문자에 +n 혹은 -n 씩 이동하여 각 평문 문자를 암호 문자로 바꾸는 것이다. 로마 제국 황제였던 카이사르에서 이름을 가져왔으며 이 당시에는 +3씩 문자를 바꾸어 사용했다. 복호화하는 방법은 암호화의 역이다. 단순 환자 암호는 각각의 평문 문자를 무작위 암호 문자와 1:1로 대응하여 바꾸는 기법이다. 복호화 방법은 빈도수 분석을 통해 영문은 e 같은 모음의 빈도수가 많아 이를 통계로 확인하여 각각의 문자로 치환해서 복호화한다. 다표식 암호는 비즈네르 암호(Vigenère cipher)가 대표적이다. 영문 알파벳을 26 * 26 행렬에 열마다 1씩 좌측으로 시프트된 형태로 각각의 알파벳이 채워진 표를 가지고 암호화하는 방법이다. 암호화할 평문에 키로 사용할 문자를 선정하여 각 행렬에 대응되는 알파벳으로 치환한다.

원문	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

[사진 1] 비즈네르 암호에서 사용되는 문자 치환 테이블

키	p	y	t	h	o	n	p	y	t	h
원문	h	e	l	l	o	w	o	r	l	d
암호문	w	c	e	s	c	j	d	p	e	k

[표 1] 비즈네르 알고리즘으로 치환 표

위처럼 평문 알파벳을 키와 대응하는 행렬 값으로 변환하여 암호화할 수 있어 빈도수 분석에 내성이 있다. 복호화하는 방법으로는 수신자는 키를 알고 있어야 하므로 키와 암호문을 이용해 복호화할 수 있다. 다만 제삼자도 복호화할 수 있는데 카지스키 방법과 프리드먼 방법을 혼용해서 사용한다. 카지스키 방법은 반복되는 문자열을 찾아 그사이 값의 약수나 공약수 값이 대부분 정확한 키의 길이로 추정한다. 프리드먼 방법은 카지스키 방법에 키 길이만큼 암호문을 잘라 빈도수 분석을 하는 방법과 무작위 하게 고른 두 문자가 같은 문자일 확률을 구하는 함수를 사용해 복호화를 한다.

2.1.2. 근현대 암호화 알고리즘

근대부터는 수학과 물리학의 발전으로 다양한 기계들이 일상에 녹아들었다. 이는 전쟁에서도 기존과는 다른 정묘한 기계 장치들이 전쟁에 사용되기 시작했다. 암호 역시 이러한 발전에 힘입어 종이와 펜이 아닌 정교하게 이루어진 기계 장치로 이루어진 형태로 구축하기 시작했다. 일례로 세계 2차 대전에서 나치 군이 사용한 그 당시 파훼법이 없었던 강력한 암호이자 그 자체로 기계적인 장치로 동작하는 에니그마(ENIGMA)가 유명하다. 에니그마는 언뜻 보면 모니터가 없는 자판기로 보일 수 있으나 그 안에는 전기 회로와 회전자, 알파벳 자판기와 램프 보드 등으로 구성되어 있다.

회전자와 플러그를 통해 자판의 알파벳은 그 자신을 제외한 다른 알파벳으로 누를 때마다 자판기 위의 알파벳 램프가 같거나 다른 알파벳 램프에 불이 켜지는 방식으로 작동한다. 이는 플러그가 연결된 알파벳 쌍과 자판을 입력할 때마다 첫 번째 위치의 회전자가 한 바퀴 돌아가면 두 번째 위치의 회전자가 한 칸씩 움직이다 또 한 바퀴를 돌면 그 뒤의 회전자가 한 칸씩 증가하는 원리로 동작한다.

에니그마 자체 알고리즘은 플러그를 통한 다중 환자 암호지만 그 당시 나치군은 회전자의 순서와 회전자와 알파벳에 대응되는 숫자를 매일 새롭게 설정하면서 경우의 수가 상당한 크기를 지니게 되므로 통상적인 빈도수 분석을 통한 제삼자의 복호화가 불가능에 수렴한다. 따라서 에니그마를 엘런 튜링이 모든 경우의 수를 가지고 빠르게 계산할 수 있는 계산기를 만들기 전까지 해독할 수 없었다.

세계 2차 전쟁이 종식된 이후 고성능 계산기는 크기는 점차 작아지면서도 더 복잡한 연산을 압도적인 속도로 처리할 수 있는 성능을 지니게 되었다. 이런 고성능 계산기는 컴퓨터라는 이름으로 대중들에게, 더욱 넓은 분야에서 보급되어 사용되기 시작했다. 고성능 컴퓨터가 보급이 이루어진 후에 기존의 알고리즘으로는 암호의 기능을 만족할 수 없었기에 더욱 복잡하고 안전한 암호 알고리즘을 개발할 수밖에 없었다. 이러한 복합적인 상황에 키 또한 발전해야 했다. 전기적인 신호의 형태로 통신 되는 기계들이 보급되자 키 또한 단순하고 간결함과 거리를 두어야 했다. 복잡한 요구를 충당하기 위해 현재 알고리즘 대부분은 해독에 필요한 엄청난 시간을 요구하는 것에 기반을 둔다. 대표적인 알고리즘은 DES(데이터 암호화 표준, Data Encryption Standard)와 RSA가 있다.

DES는 64bit 암호문으로 암호화하는 대칭 암호(symmetric-key) 알고리즘이다. 키 또한 64bit 크기지만 7bit마다 1bit의 오류 검출 비트를 사용하기에 실질적으로는 56bit의 크기를 가진다. DES는 평문을 하나의 블록 단위로 처리하기에 블록 암호로 분류되며 대표적인 블록 암호이다. 많은 블록 암호는 페이스텔 구조(Feistel cipher)를 사용하고 DES 역시 이 구조를 사용한다. 페이스텔 구조는 라운드(round) 단위로 암호화가 진행되는데 DES는 16번 반복 수행한다.

페이스텔 구조는 64bit 평문을 좌측 32bit, 우측 32bit로 구분하여 각각 L과 R로 칭한다. 나누어진 L을 56bit 키로부터 만들어진 서브키과 R을 이용해 암호화 함수 F와 XOR 연산을 통해 암호화된 L을 출력한다. 이러한 과정이 한번 실행되는 라운드다. 암호화되지 않은 R을 암호화하기 위해 다음 라운드가 진행하기 전 L과 R을 바꾸어 라운드를 진행한다.

다만 현재 기술의 시점에서는 고작 56bit 크기의 키를 지닌 DES는 수 시간 내로 해독할 수 있다. 이를 보완하기 위해 3-DES(triple-DES)와 AES(고급 암호화 표준, Advanced Encryption Standard), HDES(확장된 DES, Extended DES)를 사용한다. 3-DES는 암호화-복호화-암호화 과정을 거치는 DES로 킷값은 168bit의 크기를 지닌다. 첫 번째 암호화와 세 번째 암호화에서 사용하는 킷값이 같으면 DES-EDE3, 다를 경우 DES-EDE2로 구분한다.

AES의 경우 DES를 대체하기 위해 개발된 표준으로 NIST(미 표준화 기구)에서 공모하여 선정

된 알고리즘을 사용하는 것으로 Rijndael 알고리즘이 선정되었다. AES는 키 길이에 따라 AES-128, AES-256 등으로 구분되며 16바이트(128bit) 입력 값을 4 * 4 행렬과 치환표를 사용하여 대수적인 라운드를 진행한다. 라운드가 진행될 동안 4바이트 단위로 행 값을 좌측으로 시프트하고 4바이트 단위로 열값을 다른 4바이트로 변환한 값을 서브키를 사용하여 XOR 연산을 함으로써 하나의 라운드가 종료되며 이를 반복하는 방법이다.

RSA는 연구자인 Rivest, Shamir, Adleman의 이름에서 가져온 것이며 Diffie와 Hellman이 착안한 공개키 암호화 알고리즘의 대표적인 방법이다. RSA는 상당한 크기의 소수와 소인수 분해, 나머지 연산을 통해 수학적으로 암호화와 복호화 처리를 진행한다. 현재의 고성능 컴퓨터로도 대수의 소인수 분해의 어려움을 이용한 방법이다. 그러므로 후술할 양자 컴퓨터가 보급되어 많은 사람이 사용하기 시작하면 시대에 맞지 않는 알고리즘이 될 것이다. 다만, 아직은 좋은 성능의 알고리즘으로 광범위하게 사용되고 있는 암호다. RSA를 암호화, 복호화하는 식은 다음과 같다.

우선 암호화, 복호화에 필요한 공개키(public-key), 개인키를 생성하기 위해 2개의 큰 소수 p, q를 구하고 이를 곱한 값인 N을 사용한다. 그리고 p-1과 q-1의 최소공배수의 값을 지닌 임의의 값 L을 구한다. p-q과 q-1은 큰 소인수와 최대 공약수는 작은 수여야 한다. 공개키인 E를 구하기 위해선 다음과 같은 조건을 충족해야 한다. 1 < E < L을 만족하면서 E와 L의 최대 공약수가 1이 여야 하는 수를 사용해야 한다. 개인키 D를 구하기 위해선 다음과 같은 조건을 충족해야 한다. 1 < D < L이면서 ED = 1 mod L (혹은 ED mod L = 1)을 충족하는 값이어야 한다. 이렇게 생성한 공개키와 개인키를 암호화와 복호화에 사용한다. 암호화는 다음과 같다. 암호문 C = M(평문 크기) ^ E mod N, 즉 공개키를 가지고 암호화를 진행하게 된다. 복호화는 평문 M = 암호문 C ^ D mod N으로 개인키를 사용하여 복호화를 진행한다.

SHA-3(Secure Hash Algorithm 3)는 기존 사용됐던 MD5, SHA-1, SHA-2를 대체하는 암호화 단방향 해시함수(hash function)다. 입력된 가변적인 길이의 메시지를 고정된 bit 값으로 출력하는 알고리즘이다. 해시함수는 출력된 해시 값이 메시지에 대응하여 고정된 출력값을 지니고 메시지의 내용이 변경되면 출력되는 해시 값 역시 바뀌는 성질을 가지고 있다. 이런 특징으로 해시함수는 해시 값을 검증함으로써 무결성을 보장받는다.

SHA-1가 SHA-2가 나온 이후로도 사용됐지만, SHA-1의 수학적 취약점이 발견되기 시작하였고 이와 유사한 구조를 가진 SHA-2 역시 기밀성을 보장받지 못할 상황에서 새로운 구조를 지닌 일방향 해시함수의 필요성이 나날이 증가했고 NIST(미국 국립표준기술연구소)에서 새로운 해시함수를 공개 모집하였고 이에 다양한 알고리즘이 후보에 올랐다. 이에 여러 방면에서 검증한 끝에 KECCAK(케챡) 알고리즘이 선정되었다. KECCAK은 스펀지 구조를 가지는데 이는 페이스텔 구조와 유사하게 순열 함수와 입력 값을 균등하게 나누기 위한 추가적인 패딩 bit을 사용한다. 균등하게 나누어진 문자열을 라운드마다 XOR 연산을 진행하여 값을 출력한다.

페이스텔 구조처럼 라운드마다 XOR 연산을 진행하고 균등한 크기의 bit로 나누는 과정을 진행한다. 따라서 SHA-1과 SHA-2보다 속도가 더디지만, CPU의 발전에 따라 이는 상쇄되었고 기존의 해시함수보다 안정성 있는 알고리즘이 되었다.

2.1.3. 차세대 암호화 알고리즘과 양자 컴퓨터

차세대 암호화 알고리즘은 현대의 전자계산기 기반이 아닌 양자의 특성을 수학적, 통계적으로 표현하여 양자의 상태, 위치 등을 나타내는 함수기반으로 양자적 특성을 잘 표현한 회로로 구상한 장치가 양자 컴퓨터다. 이는 수학적 난제가 아닌 양자의 상태를 관측하기 전까지 불확정적인 특성을 고려하여 양자의 상태를 중첩된 상태로 존재하는 이론인 양자 중첩과 양자를 구성하는 두 개의 작은 입자 중 하나를 관측하여 입자의 상태를 고정한다면 다른 하나의 입자 역시 순식간에 다른 상태로 고정되는 양자 얽힘을 기반을 둔다. 이를 통해 양자 컴퓨터와 양자 알고리즘이 탄생하게 되었다.

양자 컴퓨터는 현대 컴퓨터가 사용하는 디지털 방식(0과 1)이 아닌 양자 비트(quantum bit, qubit라고도 불린다.)를 사용해 데이터를 표현한다. 또한, 위의 양자 중첩과 얽힘 이론으로 N자릿수 bit가 2^N 가지 모든 가능성을 담아내고 있다. 따라서 기존의 컴퓨터처럼 0과 1을 사용하여 기존의 논리회로를 사용하는 것보다 빠른 속도의 연산이 가능하다.

양자 컴퓨터를 기반으로 구성된 차세대 암호는 대표적으로 양자 내성 암호와 동형암호가 있다. 슈퍼컴퓨터를 비롯해 양자 컴퓨터의 등장으로 공개키 암호화 키가 상당한 시간 내로 키 소인수 분해를 통해 키를 파악할 수 있는 Shor(쇼어) 알고리즘과 확률과 통계를 통해 답을 관측할 확률을 최대로 하여 가장 빠르게 답을 도출하는 Grover(그루버) 알고리즘 등이 대두하였다. 이론상 기존의 알고리즘들이 계산기의 연산 속도 때문에 안정성에 문제가 발생했고 이를 해결하기 위해 등장한 개념이 양자 내성과 동형암호다.

동형 암호(Homomorphic Encryption)는 복호화를 거치지 않고도 데이터를 이용해 추가적인 연산이 가능한 기술이다. 동형암호는 덧셈과 곱셈 연산을 지원하며 하나의 연산만 지원하는 부분동형암호, 연산 횟수에 제한이 있는 준동형암호, 연산의 종류 지원, 횟수 제한이 없는 완전동형암호로 분류된다. 특히 완전동형암호는 동형암호의 연산 시 발생하는 부분적인 추가 값(노이즈)으로 인해 연산이나 횟수를 제한하지 않아 보다 발전된 방식으로 취급한다. 이러한 특성으로 동형암호는 기밀성을 효과적으로 보장할 수 있는 방식이지만 처리 속도가 느리고 처리 시간이 상당히 필요하며 암호문의 크기가 상당히 커지는 단점이 존재한다.

NIST, ISO 등을 비롯한 다양한 국제적 표준화 기구들이 SHA-3 때처럼 양자 내성 알고리즘을 공개 모집을 시작했다. 1차, 2차, 3차 검증을 통해 최종적으로 표준이 될 모델을 선정하는 작업을 진행 중이며 현재 2차 최종 후보군이 선정됐다. 이는 아래 그림과 같다.

종류	구분	Finalist	Alternate	장점	단점
격자 기반	암호화/키교환	CRYSTALS-KYBER, NTRU, SABER	FrodoKEM, NTRU Prime	빠른 연산 속도	파라미터 설정 어려움
	전자서명	CRYSTALS-DILITHIUM, FALCON	-		
다변수 다항식 기반	암호화/키교환	-	-	작은 서명 크기와 빠른 연산 속도	큰 키 사이즈
	전자서명	Rainbow	GeMSS		
해시 기반	암호화/키교환	-	-	안전성 증명 가능	큰 서명 사이즈
	전자서명	-	SPHINCS+		
아이소지니 기반	암호화/키교환	-	SIKE	작은 키 사이즈	느린 연산속도
	전자서명	-	-		
코드 기반	암호화/키교환	Classic McEliece	BIKE, HQC	빠른 암호화 및 복호화 속도	큰 키 사이즈
	전자서명	-	-		
영지식 기반	암호화/키교환	-	-	number-theoretic 혹은 structured hardness에 기반하지 않음	큰 서명 사이즈
	전자서명	-	Picnic		

[사진 2] NIST 양자 내성 암호 2차 합격 알고리즘 리스트

위의 그림은 처리 방식에 따른 종류와 목적에 따른 구분을 통해 2차 합격 알고리즘들의 장단점을 나타낸 표다. N차원 공간 W에서 점이 격자무늬로 배열된 집합체인 격자(Lattice)에서 계산의 어려움을 이용한 격자 기반, 유한한 필드 위 다양한 변수로 이루어진 다항식의 어려움을 기반을 둔 다변수 기반, 임의의 두 타원 곡선 a, b가 동형이면 a와 b 사이 유한한 핵의 그룹을 나타내는 아이소지니(isogeny)를 구하기 어려운 것을 기반으로 한 아이소지니 기반, 다수의 직선(Linear)이 배타적인 기울기를 가지게 하여 디코딩에 어려움을 주는 코드 기반, 해시함수의 안정성을 기반으로 한 해시 기반, 상대에게 어떤 사항에 대해 참이라는 것을 증명할 때 문장의 참 거짓 여부를 제외한 정보를 일절 주지 않고 상대를 이해되도록 하면서 참 거짓 외엔 아무것도 모르는 방식의 증명법인 영지식증명(zero-knowledge proof)을 사용한 영지식 기반으로 세세히 구분되어 후보 목록에 이름을 올렸다.

2.2. 암호화 알고리즘 간 비교

암호화는 기밀성을 향상하기 위한 대표적인 기법의 하나다. 처리 속도가 빠른 대칭키, 대수의 소인수 분해의 어려움을 이용한 대칭키 보다 느리지만 그만큼 안전한 공개키, 전자 서명이나 인증을 목적으로 하는 해시함수, 무자비한 수를 이용하여 키를 결정하는 난수 발생으로 구분된다. 이들은 목적과 환경에 따라 사용세가 달라 단순한 비교가 어렵다. 따라서 암호가 사용된 시대별로 구분 지어 알고리즘의 우위성을 판단하기로 한다.

중세시대까지 많이 사용됐던 전치암호와 치환암호가 있다. 이 암호들이 사용되던 시기는 전반적인 학문과 배경이 발달하지 못한 시기였기 때문에 현대적인 관점에서 보면 사칙연산을 비롯해 간단한 통계적 분류가 가능한 사람이라면 간단하게 암호화와 복호화를 처리할 수 있다.

하지만 현대에 이르러서 비약적으로 발전한 수학과 장치, 전기 등으로 빠르게 계산할 수 있는 함수와 기계 장치들이 대두하기 시작했다. 특히 수학과 기계의 발전으로 인간이 처리하는 속도보다 빠르게 기존의 암호화 알고리즘을 간단하게 파훼되기 시작하면서 보다 복잡하고 사상적으로 난해하고 어려운 알고리즘들의 필요성을 중요하게 여기게 되었다. 따라서 키의 발생 원인을 파악하기 힘들게 하거나 크기를 비약적으로 늘리거나 킷값을 추출하기 어려운 형태로 알고리즘이 등장하기 시작했다. 때문에, 알고리즘을 전문적으로 다루는 전문가 영역에서 개발되고 배포되기 시작했다.

컴퓨터의 등장으로 비약적으로 함수 처리가 가능하게 됐지만, 차세대 알고리즘과 양자 컴퓨터의 등장으로 기존 현재 사용 중인 암호화 알고리즘이 압도적으로 빠른 처리 속도로 안정성에 위기가 대두했다. 이는 기존 알고리즘들이 문제를 해결하는 데 있어 장황한 시간이 필요로 하는 난해한 성질을 토대로 작성되었기 때문이다. 앞으로 배포되어 민간인들에게도 사용될 때를 대비해야 한다. 실제로 많은 국제기구가 21세기 들어 각종 제도나 환경을 고려한다. 양자 컴퓨터의 등장으로 기능을 상실할 현대 암호화 알고리즘들을 보호하고 양자 컴퓨터 기반에서 정상적으로 구동될 수 있는 환경을 갖춰야 한다.

당장 예시로 현재 슈퍼컴퓨터로도 RSA의 키를 분석하기에 최대 수개월을 요구하지만, Shor 알고리즘으로 양자 컴퓨터는 이론상 수십 시간 내로 RSA 키를 알아낼 수 있는 상황에 놓여있다. 이는 앞서 말한 양자가 중첩되는 특성으로 다양한 상태를 내포하고 있어 압도적인 처리 속도 가능하게 된다. 이렇게 보면 양자 컴퓨터는 기존 컴퓨터에서 장점만 가져간 장치라고 볼 수 있지만, 양자 중첩과 양자 얽힘으로 인해 데이터 복사가 어렵고 이를 뒷받침할 기계적, 법학적 설비가 부족하다. 현재 많은 사람이 사용하는 이동식 전자 기기나 블루투스 통신 등이 점점 취약해지고 이들 역시 양자역학적으로 구현에 시간을 상당히 요구한다. 기존에 사용하던 프로토콜, 기기, 포트 등 컴퓨터와 연관이 깊은 학문, 분야, 기술 등에도 양자 컴퓨터에 기반을 둔 시스템을 구축해야 하는 점 역시 시간이 있어야 하는 이유다.

실제로 양자 컴퓨터에서 데이터 전송을 위해 양자 얽힘 원리를 이용해 데이터를 전달하는 Superdense code 알고리즘과 양자가 파동과 같다는 성질을 이용하여 주파수 위상을 표현하는 것처럼 나타낸 양자 공개키 알고리즘인 BB84 프로토콜 등 다양한 기술들이 지속해서 등장하고 있다. 기존의 알고리즘들이 양자 컴퓨터에 무력한 모습을 보이는 부분을 보완하는 더 나은 알고리즘들이 사용될 것이다.

4. 결론

이처럼 현재를 넘어 차세대까지 사용되고 사용될 다양한 암호화 알고리즘을 알아보았다. 초기 컴퓨터의 등장 때도 에니그마를 파악했고 앞으로 많은 사람이 사용할 양자 컴퓨터로 RSA나 ECC(타원 곡선 암호화) 등의 현재로서는 다소 난해한 암호화 알고리즘도 간단하게 복호화 할 것이다. 양자 컴퓨터와 관련된 학문은 1900년대 후반부터 학문적으로 많은 학자가 다루었다. 기존의 계산기에서 사용되던 모든 요소를 대체하기에 시간이 필요하다. 이에 많은 국제기구가 기존의 요소를 대체할 알고리즘을 구상하고 선정하여 표준화 작업에 박차를 가하고 있다. 따라서 이후의 전망이 체계적임을 부정할 수 없을 것이며 꽤 희망적인 상황에 직면하고 있다고 생각한다. 양자 컴퓨터에 대한 다양한 표준화 작업, 알고리즘 선정, 개발 등 이후 이동식 전자 기기나 무선 통신, IoT(사물 인터넷) 등 다양한 분야에서도 낙관적인 시선으로 적용될 것으로 보인다.

참고문헌

[1] [特輯]암호학 이론 - 정진욱
[2] 현대 암호학 - 박근수
[3] 암호학 - 최영주
[4] 비즈네르 암호 - 위키백과, 우리 모두의 백과사전 (wikipedia.org)
[5] 개인정보암호화에 효율적인 새로운 형태보존암호화 알고리즘 - 송경환, 강형철, 성재철
[6] 확장된 DES(HDES) 암호알고리즘의 설계 및 구현 - 배영선, 한승조
[7] 소인수 분해와 암호학 - 임종인, 김창한
[8] RSA를 이용한 공개키 암호 알고리즘 설계 - 우찬일, 김범식, 송영상, 유종상, 신인철
[9] 해쉬함수 SHA-3 개발 동향 - 섭, 이제상, 강진건, 홍석희, 성재철
[10] SHA-3 해시 함수의 최적화된 하드웨어 구현 - 김동성, 신경욱
[11] SHA-3의 암호알고리즘 구현 적합성 검정 프로그램 개발 - 이희웅, 김현일, 홍도원, 서창호
[12] 양자컴퓨터 기술 동향 및 산업 응용 - 이혁성
[13] 양자컴퓨터를 이용한 암호분석 최신 동향 - 장경배, 김현지, 송경주, 서화정
[14] 양자컴퓨터의 소개 및 전망 - 김태현
[15] 양자 암호 - 김재완
[16] 양자물리학과 새로운 정보과학 - 김제완
[17] 양자 알고리즘 소개 - 박정훈, 허준
[18] Technical Trend and Challenging Issues for Quantum Computing Control System - 정용화, 최병수
[19] 프라이버시 보호를 위한 동형암호의 필요성 - 서진범, 조영복
[20] [Vol.6] 2021년도 양자 내성 암호 표준화 동향 - HIIC
[21] 격자기반 양자내성 키 교환 알고리즘 구현 - 박찬희, 윤영여, 박해룡, 최은영, 김호원
[22] 초특이 아이소제니 Diffie-Hellman의 구현 및 모바일 보안 제품에서의 응용 - 윤기순, 이준영, 김수리, 권지훈, 박영호
[23] 양자내성암호 및 양자암호기술 표준화 동향 및 전략 - 권대성
[24] 양자암호 연동 표준화 현황 - 김정윤, 최태상
[25] 양자컴퓨터 상에서의 양자 알고리즘의 위협과 양자 내성을 가지는 양자 내성 암호에 대한 최신 연구 동향 - 장경배, 김현지, 송경주, 서화정
[26] 양자 통신 및 양자 암호의 개요 - 손일권, 이성훈, 박주윤, 허준
[27] 양자내성암호 표준화, 연구 동향 및 전망 - 박대환, 김호원