韓國컴퓨터情報學會 論文誌
第16卷 第5號, 2011. 05.

2011-16-5-3-2

디지털 홀로그래피와 DES 알고리즘을 이용한 전수키 공격 대응 기법

노 창 오*, 문 인 규**, 조 범 준 **

A Countermeasure against Brute-force Attack using Digital Holography and DES Algorithm

Chang-Oh Noh *, In-Kyu Moon **, Beom-Joon Cho **

요 약

정보 보안을 위해 사용되는 DES 암호화 알고리즘은 강력한 쇄도효과를 갖고 있으며, 그 처리 속도 또한 매우 빠른 알고리즘이다. 하지만 H/W의 발달로 인해 DES의 비밀키의 길이가 56bits로 너무 짧기 때문에 전수키 조사 공격에 쉽게 노출되어 있다. 본 논문에서는 전수키 조사 공격에 취약한 DES 알고리즘의 비밀키 길이 문제 해결을 위하여 디지털 홀로그래피와 DES 알고리즘을 결합하여 DES의 비밀키 길이를 크게 증가시키는 새로운 방법론을 제시한다. 또한 제안한 DES 알고리즘의 암호성능을 테스트하기 위하여 쇄도효과를 측정하여 가능성을 검증한다.

▸ Keyword : 디지털 홀로그래피, DES, 쇄도효과, 전수키 공격

Abstract

The DES encryption algorithm employed in information security has a strong avalanche effect, and the processing speed to encrypt is also fast. However, due to the H/W advances, the secret key length of DES having 56bits is not enough so that it is easily exposed to brute force attack. In this paper, we present a new method to significantly increase the secret key length in the DES by integration of digital holography and DES algorithm. In addition, we evaluate the encryption performance of the proposed method by measuring the avalanche effect and verify the possibility of it.

▸ Keyword : Digital Holography, DES, Avalanche Effect, Brute-force attack

• 제1저자 : 노창오 교신저자 : 문인규
• 투고일 : 2011. 03. 30, 심사일 : 2011. 04. 30, 게재확정일 : 2011. 05. 11.
* 조선대학교 컴퓨터공학과(Dept. of Computer Engineering, Chosun University)
** 조선대학교 컴퓨터공학부(School of Computer Engineering, Chosun University)
* 석사학위 논문을 인용하였음

I. 서 론

전기/전자 시스템의 발달과 초고속 광 통신망의 사용과 인터넷의 발달로 인해 대용량의 정보를 빠르게 전송/수신할 수 있게 되었다. 하지만 비약적인 발달로 인하여 개인/국가의 정보에 대한 보안 측면은 빠르게 발전하지 못하고 보안에 취약한 성향이 나타났다.

정보의 유출과 변경을 막고 보안 문제점을 해결하고자 암/복호화 방법론이 제기되었고, 이에 따라 다양한 암호학 이론으로 DES, AES, RSA, AHS 등이 개발되었다. 은행 등의 웹 페이지에 접속하면 여러 개의 보안 프로그램들이 설치되는데, 대체로 키보드 보안이나 인증서 보안 모듈이다. 이런 모듈은 대부분 DES 혹은 AES 암/복호화 알고리즘을 사용한다.

DES 암/복호화 알고리즘은 수학적으로 복잡하지 않으면서 매우 효율적인 알고리즘으로 알려져 있지만 비밀키의 길이가 56bits로 설계되어 있기 때문에 전수키 공격에 매우 취약한 상태이다. 그러므로 효율적인 기존의 DES 암/복호화 알고리즘을 사용하면서 DES의 비밀키 길이만을 확장시킬 수 있는 방법이 필요하다.

한편, 디지털 홀로그래피[1-3]를 이용한 영상보안 기술에 관한 연구가 최근 활발히 진행되고 있다. 이 기술은 가상광학을 이용하여 입력영상을 백색잡음 형태의 암호영상으로 변환시켜 영상을 암호화하는 알고리즘이다[4-8]. 본 논문에서는 전수키 조사에 강인한 DES의 암/복호화 알고리즘을 위하여 DES와 디지털 홀로그래피를 결합하여 DES의 비밀키 길이를 확장하는 새로운 DES 알고리즘을 제안한다.

II. 관련 연구

1. DES 알고리즘

DES 암호화 알고리즘은 1970년대에 IBM Lucifer 암호를 기반으로 만들어진 대칭형 블록 알고리즘이다[9]. DES의 암호화는 그림 1의 과정을 통해 이루어지며, DES는 16번 회전하는 페이스텔 암호구조를 갖는다. 입력평문은 64 비트의 블록길이를 가지며, 비밀키의 길이는 56 비트이다. 각 회전에서 48 비트의 보조키와 라운드 f 함수을 이용하여 혼돈과 확산이 존재하는 암호문을 생성한다.

$$L_i = R_{i-1} \qquad \cdots\cdots\cdots\cdots\cdots\cdots (1)$$
$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

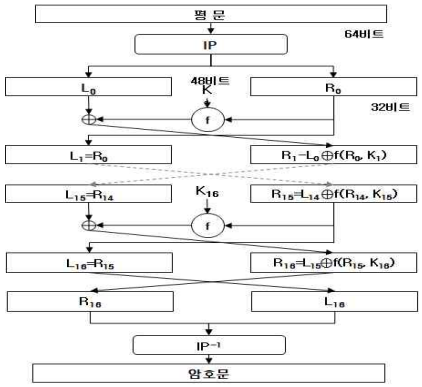


그림 1. DES의 암호화 과정
Fig. 1. Encryption architecture of DES

식(1)에서 L_0과 R_0은 첫 번째 라운드에서의 입력 평문(64bits)의 좌우의 32bits 값이다. 여기서 $i(=1,2,...,16)$는 라운드 번호이며, K_i은 각 라운드에서의 보조키이다. 총 16번의 라운드 f 함수를 통하여 암호문 L_{16}과 R_{16}이 생성된다. 또한 DES 암호화 알고리즘에서는 라운드 f 함수 뿐 만 아니라 P-Box, 전치/치환 Table 등이 사용된다.

2. DES의 전수키 공격의 취약성

DES 암호화 알고리즘은 비밀키의 길이가 56bits 로써 전수키 공격에 취약함을 보인다[9]. 이는 H/W의 성능의 발달로 인하여 하루 반 정도면 2^{56}개의 비밀키 순열이 모두 대입 가능하여 암호화된 데이터가 해독되어 버린다.

무차별 대입공격인 전수키 조사 공격은 암호알고리즘의 비밀키 길이의 한도 내에서 생성가능한 모든 비밀키 순열을 암호화 알고리즘에 대입하여 공격하는 기법이다.

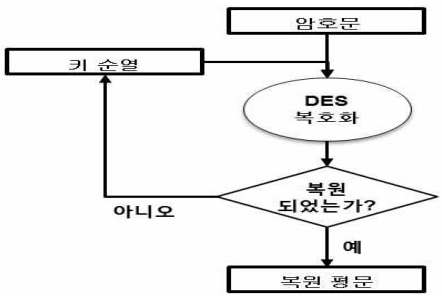


그림 2. DES의 전수키 조사 공격
Fig. 2. Brute-force attack against DES

그림 2는 이러한 전수키 조사 공격의 개요도이다. 암호체

계에서 사용되는 비밀키의 길이가 길어질수록 전수키 조사 공격시 대입될 수 있는 비밀키의 길이 역시 증가되기 때문에 가능한 큰 길이의 비밀키를 사용하면서 효율적으로 데이터를 암호화할 수 있는 암호체계 개발이 필요하다.

3. 디지털 홀로그래피

일반적으로 홀로그래피는 물체빔과 참조빔의 간섭패턴을 특수한 매질에 기록하여 물체의 3차원 영상을 복원하는 기술이다[1]. 디지털 홀로그래피는 3차원 물체의 홀로그램 패턴 기록을 위하여 저장매체로 CCD 카메라를 사용하며, 이 기록된 디지털 홀로그램 패턴으로부터 컴퓨터상에서 가상광학을 이용하여 물체에 대한 3차원 영상을 복원하게 된다[1-3].

3차원 물체에 대한 디지털 홀로그램은 백색잡음 형태의 패턴을 보이기 때문에 본 논문에서는 디지털 홀로그램 패턴을 이용하여 DES의 비밀키 길이를 증가시키는 새로운 방법을 제시한다.

3차원 물체, $U_o(x',y',z)$에 대한 임의의 전파거리 $z=d_0$ 에서의 디지털 홀로그램 패턴, $U_h(x,y,z=d_0)$은 식(2)의 프레넬 전파로부터 얻게 된다[1-3].

$$U_h(x,y,z=d_0) = FrT[U_o(x',y',z)]_{z=d_0} \quad \cdots\cdots(2)$$

물체빔의 크기와 위상정보가 디지털 홀로그램 패턴에 기록되기 때문에 디지털 홀로그램은 일반적으로 복소수 값을 갖는다.

디지털 홀로그래피에 의하여 3차원 물체가 백색잡음 형태의 디지털 홀로그램 패턴으로 코드화 될 수 있기 때문에 본 논문에서는 디지털 홀로그램 3차원 패턴 정보와 DES의 16라운드 암호화 과정을 결합하여 DES의 비밀키 길이를 확장하는 새로운 DES 알고리즘을 제안한다.

III. 전수키 공격에 대응하기 위한 방법

전수키 조사 공격에 취약한 DES의 성능개선을 위해서 비밀키의 길이를 기하급수적으로 확장시키는 방법을 제안한다. DES 암호화 알고리즘에서 비밀키 길이를 증가시키기 위한 기존 연구로는 삼중 DES 암호화 알고리즘 등이 있다. 그러나 이 알고리즘은 기본적으로 단일 DES 암호화 알고리즘에 동일한 DES 암호화 알고리즘을 순차적으로 두 번 더 적용하기 때문에 실시간 암호문 생성을 위한 고속 병렬 컴퓨팅 기술이 적용될 수 없게 된다. 그러므로 암/복호화 속도 등에 있어서 문제점을 보인다. 본 논문에서 제안하는 방법은 한번에 MXN 개의 64 bits 데이터에 대한 디지털 홀로그램 패턴 정보를 얻을 수 있으며, 이 디지털 홀로그램 패턴 생성을 위하여 초고속 병렬 컴퓨팅이 사용될 수 있기 때문에 실시간 암호문 생성이 가능해 진다[10].

본 논문에서는 DES 암호화 알고리즘에서 비밀키의 길이 증가를 위해서 디지털 홀로그램 패턴에서의 복소수 값이 DES의 입력 평문으로 사용된다.

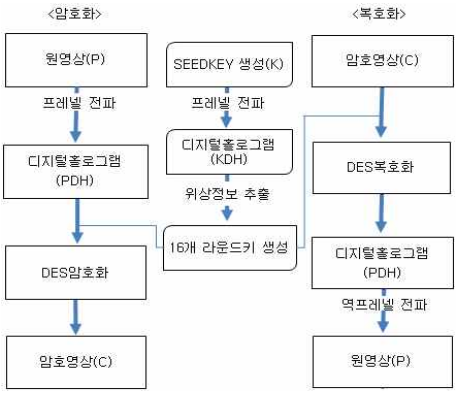
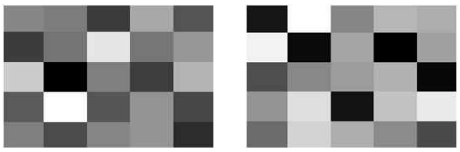


그림 3. 제안하는 암/복호화 구조도
Fig. 3. The proposed encryption/decryption block diagram

그림 3은 제안되는 디지털 홀로그래피 기반 DES 암/복호화의 구조도이다. 픽셀당 64 bits의 복소수 값을 갖는 MXN 크기의 행렬 값을 제안되는 암호체계에서의 입력문 혹은 원영상으로 사용한다. 원영상 P를 암호화하기 위하여 첫 번째로 식(2)의 프레넬 전파를 이용하여 원영상 P에 대한 디지털 홀로그램 패턴(PDH)을 생성한다. 그런 다음 생성된 원영상의 디지털 홀로그램이 DES의 입력으로 사용된다. 원영상에 대한 디지털 홀로그램 패턴에서의 임의의 픽셀 값이 $a+bi$ 형태의 64bits 복소수 값이므로, 디지털 홀로그램의 각각의 픽셀 값에 DES가 적용된다. 또한 DES에서의 라운드키(16개의 48bits 키) 생성을 위하여 이진 위상 값을 갖는 SeedKey(K)로부터 디지털 홀로그램 패턴(KDH)을 생성하며, 이렇게 생성된 디지털 홀로그램 패턴(KDH)으로부터 16개의 픽셀 위상 값들을 무작위로 선택함으로써 DES의 각 회전에서의 라운드키가 생성된다. 무작위로 선택된 위상 값들은 상관관계가 매우 작기 때문에 DES에서 요구하는 라운드키를 생성 할 수 있게 된다. 이렇게 생성된 라운드키가 원영상 디지털 홀로그램의 각 픽셀에 동일하게 적용된다.

1. 암호화 과정 및 실험 결과

본 논문에서 제안하는 전수키 조사 공격에 강인한 새로운 DES 알고리즘 구현을 위하여 그림 4를 복소수 값을 갖는 원영상 P로 사용하였다. 여기서 원영상 P의 크기는 5X5이다.

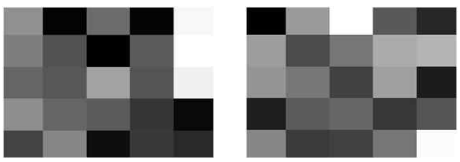


(a) (b)

그림 4. 복소수 값을 갖는 원영상 (a) Real 부분 (b) Imaginary 부분

Fig. 4. Complex values of original image (a) Real part (b) Imaginary part

그림 5는 원영상(P)을 8mm의 전파거리로 프레넬 전파시킨 원영상 P의 디지털 홀로그램(PDH)이다. 여기서 그림 5(a)는 디지털 홀로그램 패턴의 real 부분이고, 그림 5(b)는 디지털 홀로그램 패턴의 imaginary 부분이다. 그림 6은 원영상 P의 디지털 홀로그램(PDH)의 각 픽셀에 동일한 라운드 키를 갖는 DES 암호화 알고리즘을 적용한 결과이다.



(a) (b)

그림 5. 원영상 P의 디지털 홀로그램(PDH) (a) Real 부분 (b) Imaginary 부분

Fig. 5. Digital hologram of original plain image (a) Real part (b) Imaginary part

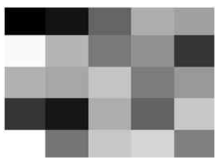


그림 6. 암호화된 암호영상(C)

Fig. 6. Encrypted cipher image

DES의 결과물을 살펴보면 각 픽셀이 암호화 되어 원영상과 다르게 변형된 것을 볼 수 있다.

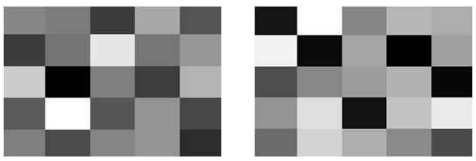
본 논문에서 제안하는 새로운 방법론은 DES 알고리즘 자체의 수정 없이 DES의 비밀키 길이를 무한대로 증가시킬 수 있다. 원영상(P)에 대한 디지털 홀로그램은 파라미터인 전파거리(z)에 의해 그 패턴이 변화되기 때문에 본 논문에서 제안하는 DES 알고리즘의 비밀키 크기는 전파거리의 비트 값에 의존하게 된다. 이 전파거리 값의 범위는 [$-\infty$,$+\infty$]로 가정할 수 있으며, 실질적인 전파거리의 크기는 64bits, 128bits 혹은 256bits 등이다. 그러므로 본 논문에서 제안하는 DES 알고리즘의 비밀키 크기는 식(3)으로 표현될 수 있다.

$$Key\,Size = 2^{56} \times 2^{k_z} \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (3)$$

여기서 k_z는 전파거리의 비트 값이다.

2. 복호화 과정 및 실험 결과

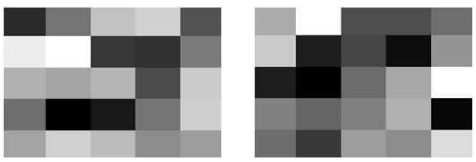
원영상(P) 복호화 과정은 원영상 암호화 과정과 역순으로 처리된다.



(a) (b)

그림 7. True 키로 복호화된 영상 (a) Real 부분 (b) Imaginary 부분

Fig. 7. Decrypted image by true key (a) Real part (b) Imaginary part



(a) (b)

그림 8. False 키로 복호화된 영상 (a) Real 부분 (b) Imaginary 부분

Fig. 8. Decrypted image by false key (a) Real part (b) Imaginary part

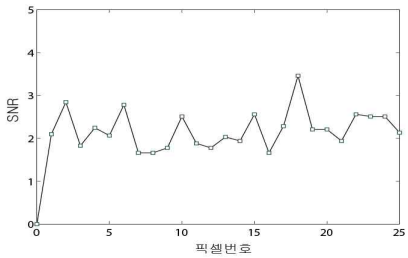


그림 9. 그림 4와 그림 8의 서로 대응되는 픽셀 값 사이에서 측정된 SNR

Fig. 9. SNR measured by using pixel values of fig. 4 and fig. 8

암호화에서 사용된 라운드 키를 이용하여 그림 6의 암호문

(C)에 역 DES를 적용한 후 디지털 홀로그램을 복원시키며, 복원된 디지털 홀로그램에 역프레넬 전파를 통하여 원영상(P)을 얻는다. 그림 7은 암호화 할 때 사용했던 동일한 라운드 키와 전파거리(=8mm)를 사용하여 복호화된 결과이다. 그림 4의 원영상과 동일한 영상을 얻었다. 그림 8은 동일한 라운드 키와 전파거리(=8.01mm)를 사용하여 복호화된 결과이다. 제안되는 방법에서 비밀키로 사용되는 전파거리 값의 sensitivity를 측정하기 위하여 그림 4와 그림 8 사이에서 식(4)의 SNR을 측정하였다. 여기서 P_i는 그림 4의 원영상의 i번째 픽셀에서의 64비트 값이고 $\widehat{P}_i$는 임의의 복호화된 영상의 i번째 픽셀에서의 64비트 값이다.

$$SNR = \frac{P_i}{P_i - \widehat{P}_i} \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(4)$$

그림 9는 그림 4 와 그림 8 사이에서 측정된 SNR 결과이다. 서로 대응되는 픽셀 간에서 픽셀 값 길이인 64 bits중 약 32 bits가 차이가 있음을 볼 수 있다.

3. 쇄도 효과의 측정 및 실험 결과

본 논문에서 제안하는 전수키 공격에 강인한 새로운 DES 알고리즘 성능평가를 위하여 제안된 암호화 알고리즘의 쇄도 효과(Avalanche Effect)를 측정하였다. 쇄도 효과는 식(5)로 정의될 수 있다.

$$E(P,K_r) \oplus E(P,K_i) = D \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(5)$$

여기서 $E(P,K_r)$은 평문 P를 참조(reference) 비밀키 K_r로 암호화 시킨 참조 암호문이며, $E(P,K_i)$은 평문 P를 테스트 비밀키 K_i로 암호화 시킨 테스트 암호문이다. $E(P,K_r)$와 $E(P,K_i)$의 XOR 연산 결과 값인 D에서 입력평문의 길이 n에 대하여 50%의 비율인 0의 개수 혹은 1의 개수를 측정함으로써 제안된 암호화 알고리즘의 쇄도효과를 평가한다.

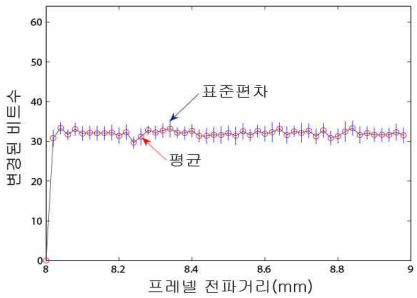


그림 10. 참조 암호영상과 전파거리에 따른 테스트 암호영상들 사이에서의 쇄도효과
Fig. 10. Avalanche Effect of reference image and encrypted test image according to the propagation distance

쇄도효과 측정을 위한 참조 암호영상으로는 참조 비밀키인 전파거리 8mm로 암호화된 그림 6이 사용되었다. 또한 원영상(P)의 프레넬 전파시 10um 간격으로 전파거리 값을 증가시키면서 테스트 비밀키 값들을 사용하여 테스트 암호영상들을 생성하였다. 그림 10은 식(5)를 이용하여 참조 암호영상과 전파거리에 따른 테스트 암호영상들 사이에서 계산된 쇄도효과 D 값의 결과이다. 전파거리가 8.01mm부터 D값이 50%에 근접함을 보인다. 그러므로 원영상의 디지털 홀로그램 생성에 필요한 전파거리 값이 DES의 비밀키 길이 확장을 위해 사용될 수 있음을 확인할 수 있다. 또한 그림 10의 결과는 DES 알고리즘의 비밀키 크기가 식(3)으로 표현될 수 있음을 입증한다.

IV. 결 론

본 논문에서는 전수키 조사에 취약한 DES의 비밀키 길이에 대한 문제점을 해결하기 위하여 디지털 홀로그래피 기반의 방법론을 제시하였다. 디지털 홀로그램 패턴을 이용하여 기존의 DES 암/복호화 알고리즘을 사용하면서 DES의 비밀키 길이만을 증가시키는 방법을 실험을 통하여 보였으며, DES의 비밀키 길이는 디지털 홀로그램 생성을 위한 파라미터인 전파거리의 비트 값에 비례함을 쇄도효과 실험을 통하여 입증하였다. 그러므로 전수키 공격에 강인한 DES 알고리즘 사용이 가능할 것으로 기대한다.

참고문헌

[1] J. W. Goodman, “Introduction to Fourier Optics,” McGraw-Hill, New York, USA, 1996.

[2] I. Yamaguchi and T. Zhang, "Phase-shifting digital holography," Opt. Lett. Vol. 22, pp. 1268-1270, 1997.

[3] B. Javidi and E. Tajahuerce, "Three dimensional object recognition by use of digital holography," Opt. Lett. Vol. 25, pp. 610-612, 2000.

[4] H. Kim, D. Kim, and Y. Lee, "Encryption of digital hologram of 3-D object by virtual optics," Optics Exp. Vol. 12, pp. 4912-4921, 2004.

[5] O. Matoba, T. Nomura, E. Perez-Cabre, M. S. Millan, and B. Javidi, "Optical Techniques for Information Security," Proceedings of the IEEE, Vol. 97, pp. 1128-1148 2009.

[6] Y. Frauel, A. Castro, T. Naughton, and B. Javidi, "Resistance of the double random phase encryption against various attacks," Optics Exp. Vol. 15, pp. 10253-10265, 2007.

[7] S. Kishk and B. Javidi, "3D object watermarking by a 3D hidden object," Optics Exp. Vol. 11, pp. 874-888, 2003.

[8] E. Tajahuerce and B. Javidi, "Encrypting three-dimensional information with digital holography," Appl. Opt. Vol. 39, pp. 6595-6601, 2000.

[9] W. Stallings, "Crytography and network security," Pearson, New York, USA, 2011.

[10] T. Shimobaba, Y. Sato, J. Miura, M. Takenouchi, and T. Ito, "Real-time digital holographic microscopy using the graphic processing unit," Optics Exp. Vol. 16, pp. 11776-11781, 2008.

저 자 소 개

노 창 오

2009: 조선대학교 컴퓨터공학과 공학사.
2011: 조선대학교 컴퓨터공학과공학 석사.
현 재: (주)아이디스 연구소 / 주임연구원
관심분야: 영상보안, 알고리즘, 패턴인식
Email : shckddh@gmail.com

문 인 규

1996: 성균관대학교 전자공학과 공학사.
1998: 성균관대학교 전자공학과 공학석사.
2007: University of Connecticut Electrical & Computer Engineering M.S.
2007: University of Connecticut Electrical & Computer Engineering ph.D.
2008~2009: University of Connecticut 연구원
2008~2009: BJ Information Technology 연구원
현 재: 조선대학교 컴퓨터공학부 조교수
관심분야: 정보보호, 영상보안 광정보처리, 3차원 영상
Email : inkyu.moon@chosun.ac.kr

조 범 준

1980: 조선대학교 전기공학과 BS, MS
1988: 한양대학교 전기공학과 공학박사.
2004: KAIST 전자전산학과 공학 박사
현 재: 조선대학교 컴퓨터공학부 교수
관심분야: 인공지능, 패턴인식, 뉴로 컴퓨터
Email : bjcho@chosun.ac.kr