YENİ SALDIRIYA KARŞI KOYABİLEN İKİ IFEA-M MODİFİKASYONU

Aleksandr G. Çefranov
Doğu Akdenız Üniversitesi, Gazımağusa, KKTC
Alexander.chefranov@emu.edu.tr

ABSTRACT

Improved fast encryption algorithm for multimedia IFEA-M is modified to withstand recently discovered vulnerability to differential known plaintext-ciphertext attack. Proposed here algorithms PIFEA-M and I^{2}FEA-M have about 10% and 30% better performance respectively than that of IFEA-M.

Key words: Boolean matrices, encryption, differential known plaintext-ciphertext attack

1. GİRİŞ

Giriş metni (10 punto) IFEA-M(Improved Fast Encyrption Algorithm for Multimedia)[2] algoritmasının saldırıya açık olduğu kaynaklar[1] tarafından ortaya çıkarılmıştır. Sözde-rastgele süreçin kurcalanması durumunda böyle bir atağın olması mümkündür. Bu durumlardan biri, sözde-rasgele sürecin sadece bir dış kaynak tarafından kontrol edildiği zamanlardır[1]. Esas FEA-M algoritması, [3],[4]'de önerilmiştir. FEA-M'in zayıf tarafları, blok zincirlerinin kullanılması ve ilk ve ardışık blokların şifrelemesinin değişik yollarının olmasından kaynaklanmaktadır([2], [5], ve [6]). [2] ve [3]'e göre, FEA-M gerçekleştirim performansı küçük sayıda $n \times n$-bitlik matris çalışmaları kullanıldığında 196 mikro-çalışma olarak bulunmuştur: Şifreleme ve şifre çözme için n=64 olduğunda sadece m=3 çarpım ve a=2 toplama gereklidir. Hesaplama, aşağıdaki formül kullanılarak elde edilmiştir. (Formülün diğer şekli için, [3] p.-107 bakınız).

(1) $mo(m,a;n) = m \cdot n + 2 \cdot a$.

FEA-M'in performansına en yakın algoritma, 616 mikro-çalışmayı gerektiren AES (Rijndael) algoritmasıdır [2]-[3]. IFEA-M [2], şifreleme ve çözme için beş matris çarpımı ve iki matris toplamasını kullanır ve $mo(5,2;64) = 324$ mikro-çalışma gerektirir[1]. Buna rağmen IFEA-M'in performansı AES (Rijndael)'in performansından pratik olarak iki kez daha iyidir. Bu metinde Parameterized IFEA-M (PIFEA-M) and Improved twice FEA-M (I^{2}FEA-M), iki algoritma önerilmektedir. PIFEA-M ve I^{2}FEA-M algoritmaları, FEA-M ve IFEA-M tarafından bilinen ve karşı konulabilen saldırılara,IFEA-M'e göre sırasıyla 10% ve 30% daha iyi performansla karşı koyabilmektedirler. Şifreleme için üç matris çarpımı, şifreyi açmak için ise 4 işlem gerekmektedir. Metinin kalanı şu şekilde düzenlenmiştir.İkinci bölümde IFEA-M ve zayıf yönleri hakkında genel bilgi verilmektedir. Üçüncü bölümde önerilen PIFEA-M ve I^{2}FEA-M algoritmaları sunulmaktadır. Dördüncü bölümde elde edilen neticeler tartışılmaktadır.

2. IFEA-M'E GENEL BAKIŞ

Algoritma, bir şifresiz metini, P, alır ve onu bir şifreli metin, C, üretmek için şifreler. Şifresiz ve şifreli metin, $n \times n$-bit matris blokları dizisi şeklinde temsil edilir ve n=64'dür. Bu matrislerde kullanılan işlemler toplama (Toplama modulo2, $\oplus$) ve alan GF(2)'in üzerinde çarpımdır. IFEA-M, aşağıdaki şifreleme-çözme şemasını kullanır:

$$\begin{aligned} C_i &= K \cdot (P_i \oplus K \cdot V \cdot K^i) \cdot K^{n+i} \\ &\oplus K \cdot V \cdot K^i, \\ P_i &= K^{-1} \cdot (C_i \oplus K \cdot V \cdot K^i) \cdot K^{-n-i} \\ &\oplus K \cdot V \cdot K^i, \end{aligned} \quad (2)$$

K, V aralarında bağlantı olan kullanıcıların oturum anahtar matrisleri ile paylaşılır, K^{-1}, K matrisinin evriğidir. (2)'deki oturum anahtar matrislerinin yeni oturum başlamadan önce bir gönderen tarafından oluşturulduğu farz edilir. Gönderen ve alıcı, ana anahtar matrisini, K_0, paylaşır. Bu ana anahtar matrisi gönderenden alıcıya oturum anahtarlarını emniyetle taşımak için şu şekilde kullanılır:

$$\begin{aligned} K^* &= K_0 \cdot K^{-1} \cdot K_0, \\ V^* &= K_0 \cdot V \cdot K_0. \end{aligned} \quad (3)$$

Alıcı, elde edilen veriyi şu şekilde ortaya çıkarır

$$\begin{aligned} K^{-1} &= K_0^{-1} \cdot K^* \cdot K_0^{-1}, \\ V &= K_0^{-1} \cdot V^* \cdot K_0^{-1}. \end{aligned} \quad (4)$$

IFEA-M'de, FEA-M'in aksine, ne blok zincirleri kullanılmıştır, ne de ilk bloğun işlemesi diğer blokların işlemesinden farklıdır. IFEA M'de bir

saldırı [1], onun uygunsuz gerçekleştirimlerinde, iki ardışık oturumda aynı anahtarı kullanması için bir izinsiz kullanıcıya izin verebildiği bir varsayımını kullanır (Bu, sözde-rasgele jeneratörün kontrolünün izinsiz kullanıcı tarafından yeni anahtarları oluşturmak için kullanıldığı zaman olabilir) ve izinsiz kullanıcı, türevsel olarak seçilmiş şifresiz metin (şifreli metin), saldırısını yapar. İzinsiz kullanıcı bilinmiş bir farkla şifresiz metin (şifreli metin) blokları oluşturabilir, ve kendi şifreli metin (şifresiz metin) bloğu arasındaki farkları görebilir. Saldırı şu şekilde devam eder:

Varsayım. İzinsiz kullanıcının aynı oturum anahtar matrislerini, K ve V, iki oturumda kullanıldığı ve iki şifresiz-şifreli metin blok sırasının $P_i^1, P_i^2, C_i^1, C_i^2$ olduğu varsayılır.

Tanım 1 [1]. Eğer varsayım doğruysa, IFEA M'in anahtar matrisleri K ve V, çizgisel matris denklemlerinin çözülmesi ile açığa vurulabilir.

Kanıt. Şifreli metin bloklarının toplamı şu şekilde hesaplanır:

$$\begin{aligned}\Delta C_i = C_i^1 \oplus C_i^2 = (K\cdot(P_i^1 \oplus K\cdot V\cdot K^i)\cdot \\ K^{n+i} \oplus K\cdot V\cdot K^i)\oplus(K\cdot(P_i^2 \oplus K\cdot V\cdot \\ K^i)\cdot K^{n+i} \oplus K\cdot V\cdot K^i) = \\ K\cdot(P_i^1 \oplus P_i^2)\cdot K^{n+i} = K\cdot \Delta P_i \cdot K^{n+i}.\end{aligned} \quad (5)$$

Şimdiye kadar, (5)'den, izlenirse:

$$\begin{aligned}\Delta C_i = K\cdot \Delta P_i \cdot K^{n+i}, \\ \Delta C_{i+1} = K\cdot \Delta P_{i+1}\cdot K^{n+i+1}.\end{aligned} \quad (6)$$

Eğer iki ardışık şifresiz metin matrisleri $P_i^1, P_{i+1}^1, P_i^2, P_{i+1}^2$ şu şekilde seçilirse:

$$\Delta P_i = \Delta P_{i+1}, \quad (7)$$

Sonra, (6) ve (7)'den izlenirse :

$$\begin{aligned}\Delta C_{i+1} = K\cdot \Delta P_{i+1}\cdot K^{n+i+1} = \\ K\cdot \Delta P_i \cdot K^{n+i+1} = \Delta C_i \cdot K.\end{aligned} \quad (8)$$

(Bu arada, [1]'de (9)'daki temsilcideki "+ 1" unutulmuştur, ama son sonuç (8)'de gösterilenle tam olarak aynıdır.)

Böylece, eğer, ΔC_i dönüştürülürse, denklem (8) gizli bir oturum anahtarını, K, verir:

$$K = (\Delta C_i)^{-1}\Delta C_{i+1}. \quad (9)$$

K matrisi (9) ile kırıldıktan sonra , V matrisi (2)'deki çizgisel matris denklemlerinin çözülmesi ile açığa vurulabilir.

$$\begin{aligned}K^{-2}\cdot(C_i \oplus K\cdot P_i\cdot K^{n+i})\cdot K^{-i} = \\ V\cdot K^{n+i} \oplus K^{-1}\cdot V.\end{aligned} \quad (10)$$

[1]'de bahsedilen türevsel olarak bilinen şifreli metin saldırısı aynı matematiği kullanmaya devam eder, ama, şimdi şifresiz metin farklarının yerine şifreli metin farkları (7) eşitlenmiştir.

3. I²FEA-M AND PIFEA-M ALGORİTMALARININ TASARIM VE ANALİZİ

(8)'de sunulan basitleştirme, (2)'de ilk katkıda bulunanın en sağdaki çoğaltanı olarak kullanılan i-bağlı (Dinamik) terimden, K^{n+i}, dolayı mümkündür . Eğer dinamik terim, orta bir terim olarak kullanılsaydı bu mümkün olmayacaktı. Biz, (2)'ye (5)-(8)'deki gibi dönüşümlerde en sağdaki (en soldaki) terim olmaması için dinamik bir çoğaltanla birlikte parantez koyacağız

Çoğulortam için geliştirilen iki kez hızlı şifreleme algoritması I²FEA-M, aşağıdaki gibidir:

$$\begin{aligned}B_i = K^n\cdot V\cdot K^{n+i} \\ B_i^{-1} = K^{-n-i}\cdot V^{-1}\cdot K^{-n} \\ C_i = B_i\cdot(P_i \oplus B_i)\cdot B_i \oplus B_i, \\ P_i = B_i^{-1}\cdot(C_i \oplus B_i)\cdot B_i^{-1} \oplus B_i,\end{aligned} \quad (11)$$

B_i'nin birinci çarpanındaki n kuvveti algoritmanın direncini artırmak, sonuncu çarpanında kullanılan n kuvveti ise i'nin küçük değerlerinde K'nın düşük kuvvet almasını engellemek için kullanılmıştır.

Tanım 2 [7]. Varsayım koşullarında, (11), (3), ve (4) ile temsil edilen I2FEA- M, eğer K ve V 'nin değişme özelliği yoksa, türevsel olarak bilinen şifresiz ve şifreli metin saldırısına direnir.

Eğer güçlerin artan hesabı ve sabit matris çarpanları kullanırsa, I²FEA-M 'in performansı şifreleme için üç matris çarpımı ve iki toplama ile tanımlanır.

Böyle bir durumda şifreyi açmak için ise dört matris çarpımı ve iki toplama gereklidir. Ortalama olarak, şifreleme-şifreyi açma için 3.5 matris çarpımı ve iki toplama gereklidir.

Dolayısıyla I²FEA-M için gerekli mikro-işlem sayısı (1)'e göre ,

$$mo(4.5,2;64) = 3.5\cdot 64 + 2\cdot 2 = 228,$$

ve I²FEA-M'in performansı IFEA-M'e göre 30% daha iyidir.

Şimdi başka bir yaklaşımı düşünelim. Çoğulortam için geliştirilen parametrize hızlı şifreleme algoritmasını PIFEA-M aşağıdaki gibidir:

$$
\begin{aligned}
C_i &= (P_i \oplus A_{r_1 r_2}) \cdot B_{r_3 r_4 r_5, i} \oplus A_{r_1 r_2}, \\
P_i &= (C_i \oplus A_{r_1 r_2}) \cdot B^{-1}_{r_3 r_4 r_5, i} \oplus A_{r_1 r_2}, \\
A_{r_1 r_2} &= V^{r_1} \cdot K^{r_2}, \\
B_{r_3 r_4 r_5, i} &= V^{r_3} \cdot K^{r_4 + i} \cdot V^{r_5},
\end{aligned} \tag{12}
$$

Burada $r_k \geq 1, k = \overline{1,5}$, bir gönderen tarafından bir alıcıya oturum anahtar matrisleriyle, K, V, beraber gönderilen oturum parametreleridir. $r_k, k = \overline{1,5}$, parametreleri ekstra parametre matrisi R 'nin ilk beş satırı ile temsil edilen tamsayılardır. R 'nin geriye kalan satırları sıfırdır.

Oturum anahtar matrislerinin dağılımı (3) ve (4)'deki gibidir ve parametre matrisi benzer bir şekilde gönderilir.

$$
\begin{aligned}
R^* &= K_0 \cdot R \cdot K_0, \\
R &= K_0^{-1} \cdot R^* \cdot K_0^{-1}.
\end{aligned} \tag{13}
$$

Tanım 3 [8]. Varsayım koşullarında, (12), (13), (3) ve (4) ile temsil edilen PIFEA- M, eğer K ve V 'nin değişme özelliği yoksa türevsel olarak bilinen şifresiz ve şifreli metin saldırısına direnir.

Eğer güçlerin artan hesabı ve sabit matris çarpanları kullanırsa, PIFEA-M 'in performansı şifreleme için dört matris çarpımı ve iki toplama ile tanımlanır.

Böyle bir durumda şifreyi açmak için ise beş matris çarpımı ve iki toplama gereklidir. Ortalama olarak, şifreleme-şifreyi açma için 4.5 matris çarpımı ve iki toplama gereklidir.Dolayısıyla PIFEA-M için gerekli olan mikro-işlem sayısı (1)'e göre

$$mo(4.5,2;64) = 4.5 \cdot 64 + 2 \cdot 2 = 292,$$

ve PIFEA-M'in performansı IFEA-M'e göre 10% daha iyidir.

4. SONUÇLAR

Bu noktaya kadar Parametrized ve twice Improved FEA-M algoritmaları önerildi ve analiz edildi. Bunların IFEA-M'e göre yaklaşık olarak sırasıyla 10% ve 30% daha iyi performansları vardır. Bu algoritmalar IFEA-M'in dayanıklı olduğu bütün ataklara dayanıklıdırlar.(Çünkü bu algoritmalarda zincir bağlantısı kullanılmamıştır ve ilk şifreleme işlemi de diğerleriyle aynı şekilde yapılmaktadır) ve IFEA-M de belirtilen türevsel olarak bilinen şifresiz-şifreli metin saldırılarına dinamik terimin bulunduğu yerden dolayı karşı koyabilir. PIFEA-M'de kullanılan 5 tane 64-bitlik parametre kümeleri olası saldırıların olmasını güçleştirmektedir. Bu parametreler parametre matrisinin $R(64,64)$ ilk 5 satırı olduğundan ve geriye kalanlar 0 olarak varsayıldığından, şu anda kullanmayan 0 satırlarını kullanarak parametre sayısını artırmak mümkündür. Her parametre $2^{12}/5$ bitlik boyuta sahip olabilir. PIFEA-M'in performansı I^2FEA-M'in performansından daha kötüdür fakat kullanılan ek parametreler onun kırılmasını zorlaştırmaktadır.

KAYNAKLAR

[1] S. Li and K.-T. Lo, "Security problems with improper implementations of improved FEA-M," *Journal of Systems and Software*, vol. 80, no. 5, May 2007, pp. 791-794; *arXiv*: cs: cr/0509036 v2 25 Jun 2006

[2] M.J. Mihaljevic, "On vulnerabilities and improvements of fast encryption algorithm for multimedia FEA-M," *IEEE Transactions on Consumer Electronics*, vol. 49, no. 4, Nov. 2003, pp. 1199-1207.

[3] X. Yi, C.H. Tan, C.K. Siew, and M.R. Syed, "Fast encryption for multimedia," *IEEE Transactions on Consumer Electronics*, vol. 47, no. 1, Feb. 2001, pp. 101-107.

[4] X. Yi, C.H. Tan, C.K. Siew, and M.R. Syed, "ID-based key agreement for multimedia encryption," *IEEE Transactions on Consumer Electronics*, vol. 48, no. 2, May 2002, pp. 298-303.

[5] M.J. Mihaljevic and R. Kohno, "Cryptanalysis of fast encryption algorithm for multimedia FEA-M," *IEEE Communications Letters*, vol. 6, no. 9, Sep. 2002, pp. 382-384.

[6] A.M. Youssef and S.E. Tavares, "Comments on the security of fast encryption algorithm for multimedia (FEA-M)," *IEEE Transactions on Consumer Electronics*, vol. 49, no. 1, Feb. 2003, pp. 168-170.

[7] A.G. Chefranov, "Improved Twice Fast Encryption Algorithm for Multimedia I^2FEA-M," *IEEE Transactions on Dependable and Secure Computing* (gönderilen).

[8] A.G. Chefranov, "Parameterized Improved Fast Encryption Algorithm for Multimedia PIFEA-M," *IEEE Communications Letters* (yayınlanması kabul edilen makale).