ÇİN KALAN TEOREMİNİ KULLANAN BİR GİZLİLİK PAYLAŞIM ŞEMASI

[1]Derya ARDA **[2]Ercan BULUŞ**

[1]Trakya Ünv. Müh.Mim.Fak.
Bilgisayar Müh. Bölümü 22030 Edirne
[2]Namık Kemal Ünv. Çorlu Müh. Mim.
Fak. Bilgisayar Müh. Bölümü Çorlu

[1]deryaa@trakya.edu.tr [2]ercanbulus@corlu.edu.tr

ÖZET

İlerleyen teknoloji ile birlikte dijital ortamda verilerin saklanması, korunması ve güvenlik gereksinimleri sürekli artmaktadır. Verilerin gizli bir şekilde iletilmesi gereken durumlarda anahtarın korunması oldukça önemlidir. Gizlilik paylaşım şeması kriptografik anahtar yönetiminde kullanılan oldukça önemli bir yapıdır. Gizlilik paylaşım şeması yapılacak saldırılara karşı anahtarın tek bir kullanıcıda bulunmaktansa pek çok kullanıcıya dağıtılarak güvenliğini arttırmak için tasarlanmış bir yapıdır. Bu şema ilk olarak 1979 yılında Shamir ve Blakley tarafından birbirlerinden bağımsız olarak ortaya atılmıştır. Shamir'in Gizlilik Paylaşım Şeması Lagrange İnterpolasyon polinomu tabanlıdır. Temel olarak kısmi bilgi içeren her bir paylaşımlar kümesinden S gizliliğini yeniden elde edebilmektir. Bunun için gizlilik en fazla *n* kullanıcı arasında paylaştırılır ve en az *t* kullanıcı paylaşımlarını birleştirerek gizliliği yeniden elde edebilir. Bu (t,n) eşik gizlilik paylaşımı olarak adlandırılır. Literatürde pek çok gizlilik paylaşım şemaları mevcuttur. Bu şemalardan bir tanesi bu çalışmada kullanacağımız Asmuth ve Bloom tarafından önerilen Çin Kalan Teoremi tabanlı eşik şemasıdır. Bu şemadaki paylaşımlar gizlilik ile ilişkilendirilmiş K tam sayısının kongüranslarının sınıfıdır. Biz bu çalışmada çin kalan teoremi tabanlı bir (t,n) eşik gizlilik paylaşım şemasının bir uygulamasını gerçekleştirdik.

Anahtar Kelimeler: Çin Kalan Teoremi, Gizlilik Paylaşım Şeması

1. Giriş

Açık anahtar sistemlerinin önemli konularından birisi anahtar yönetimidir. Gerçek yaşamda yatırım sektörü göz önünde bulundurulduğunda gizli dokümanların güvenli bir şekilde muhafaza edilmesi ya da kaybolmasını engellemek gereklidir. Bu durumda gizli anahtarın dürüst bir kişi tarafından muhafaza edilmesi gerekmektedir. Ancak böyle bir gizlilik durumunda anahtarın kaybolması ya da değişikliğe uğraması söz konusu olabilir. Gizli anahtarın kaybolması durumunda ise depolanan bilgilere bir daha ulaşılması mümkün olamayacaktır. O yüzden bundan daha iyi bir alternatif olarak anahtar yönetimi sorumluluğu pek çok kişi arasında dağıtılarak anahtarın kaybolması riskini aza indirmektir. Mesela gizli anahtar birkaç parçaya bölünür ve daha sonra farklı bireylere gönderilir. Etkin katılımcılar istediklerinde diğer katılımcılarla bir araya gelerek kendilerindeki anahtar parçalarını birleştirerek orijinal gizli anahtarı yeniden elde edebilirler.[1]

Gizlilik paylaşım şeması kriptografik anahtar yönetiminde kullanılan oldukça önemli bir yapıdır. Gizlilik paylaşım şeması yapılacak saldırılara karşı anahtarın tek bir kullanıcıda bulunmaktansa pek çok kullanıcıya dağıtılarak güvenliğini arttırmak için tasarlanmış bir yapıdır. Bu şema ilk olarak 1979 yılında Shamir[2] ve Blakley[3] tarafından birbirlerinden bağımsız olarak ortaya atılmıştır. Shamir'in Gizlilik Paylaşım Şeması Lagrange İnterpolasyon polinomu tabanlıdır. George Blakley gizliliği yeniden elde etmek için geometrik metot kullanan geometrik gizlilik paylaşım şemasını ortaya çıkarmıştır. Çin kalan teoremi tabanlı eşik gizlilik paylaşım şemaları Mignotte[5] ve Asmuth-Bloom[4] tarafından bulunmuştur. Bu şemalarda çin kalan teoremi boyunca özel seçilmiş tam sayı dizileri kullanılır.
Bu çalışmada Asmuth-Bloom tarafından önerilen çin kalan teoremi tabanlı bir (t,n) eşik gizlilik paylaşım

şemasının uygulaması bir örnekle açıklandı. Güvenlik açısından bakıldığında, çin kalan teoremi tabanlı eşik gizlilik paylaşım şemasının, gizliliği yeniden elde edebilme konusunda t eşik değerden daha az kümeler için mükemmel bir şema olmamasına rağmen dikkatlice seçilen parametrelerle, güvenliği arttırmaya önderlik edebildiği sonucuna varılabilir.

2. Gizlilik Paylaşım Şeması

Gizlilik paylaşım problemine ilk çözümler 1979 yılında Shamir[2] ve Blakley[3] tarafından birbirlerinden bağımsız olarak üretilmiştir. Bir (t,n) gizlilik paylaşım şemasında d gizliliği n kişi arasında dağıtılır ve her hangi t kişi veya daha fazlası birleşerek gizliliği yeniden elde edebilir. Ancak t-1 veya daha az kişi gizliliği elde edemezler.

2.1.Shamir'in Lagrange İnterpolasyon Polinom Şeması

Shamir[2] tarafından önerilen gizlilik paylaşımı için ilk şema polinom interpolasyon tabanlıdır. Bir (t,n) gizlilik paylaşımını elde etmek için, $p \rangle n$ büyük bir asal sayı ve Z_p sonlu bir cisim, t eşik değer ve $a_0 \in Z_p$ gizlilik olsun. $a_1, \ldots, a_{t-1} \in Z_p$ rastgele elemanları seçip t-1 dereceli polinomu kuralım.

$$f(x)=a_{t-1}x^{t-1}+\ldots+a_1x+a_0 \in Z_p[x]$$

Paylaşımlar aşağıdaki denklemle elde edilir ve kullanıcılara dağıtılır.

$$h(x) \equiv (a_{t-1}x^{t-1} + \ldots + a_1x + a_0) \bmod p \text{ [6].}$$

i.parçanın paylaşımları $1 \le i \le n$ aralığında $y_i = h(x_i) \bmod p$ eşitsizliğine göre anahtar parçaları (x_i,y_i) şeklinde kullanıcılara dağıtılır. t noktası *t-1* dereceli polinomu, h(x)'i ve a_0 gizliliğini belirlemek için yeterlidir.

Verilen t adet (x_k,y_k) parçası için (burada $y_k = h(x_k)$ ve $(1 \le k \le t)$ h(x) lagrange polinomundan yeniden elde edilir. İlk olarak $l_k(x)$ polinomu şu şekilde tanımlanır.

$$l_k(x) = \prod_{\substack{i=1 \\ i \ne k}}^{t} \frac{x - x_i}{x_k - x_i} \bmod(p).$$

Lagrange interpolasyon polinomu:

$$p(x) = \sum_{k=1}^{t} y_k l_k(x)$$

Denklemi ile tanımlanır ve $p(x_j) = y_j için 1 \le k \le t.$ şartını sağlar.

H(x) polinomunu ve gizli mesajı yeniden elde etmek için p(x) polinomunu hesaplamalıyız.

$$h(x) \equiv \sum_{k=1}^{t} y_k \prod_{\substack{j=1 \\ j \ne k}}^{t} \frac{x - x_j}{x_k - x_j} (\bmod p) \text{ [7][8]}$$

Bu şema ile ilgili bir örnek [9] numaralı kaynakta bulunmaktadır.

3. Çin Kalan Teoremi Genel Yapısı

Tanım1: Bir m pozitif tamsayısı verilmiş olsun. $a, b \in Z$ için $m|(a-b)$ ise a ve b m modülüne göre kongruenttirler denir ve $a \equiv b(\bmod m)$ yazılır. Böylece ortaya çıkan bağıntıya m modülüne göre kongruans bağıntısı denir. Kongruans bağıntısı bir denklik bağıntısıdır.

Teorem1: (Çin Kalan Teoremi) Çin kalan teoremi belirli kongruans sistemlerini çözme metodur. Farzedelim ki $m_1, m_2, \ldots, m_r$ pozitif tamsayılar ver her $i \ne j$ için $ebob(m_i, m_j) = 1$ olsun. $a_1, a_2, \ldots, a_r$ tamsayıları verildiğinde

$$x \equiv a_1 \bmod m_1$$

$$x \equiv a_2 \bmod m_2$$

$$\ldots$$

$$x \equiv a_r \bmod m_r$$

kongruans sisteminin Z de bir x çözümü vardır ve kongruans kümelerinin çözümü şöyledir. $M = m_1 m_2 \ldots m_r$ modülüne göre

$$x \equiv a_1 b_1 \frac{M}{m_1} + \ldots + a_r b_r \frac{M}{m_r} (\bmod M)$$

ve

$$b_i \frac{M}{m_i} \equiv 1 \bmod(m_i)$$

hesaplanır.[8,13,14]

4. Çin Kalan Teoremi Tabanlı Eşik Gizlilik Paylaşım Şemaları

Çin kalan teoremi tabanlı eşik gizlilik paylaşımı için birkaç çeşit şema önerilmiştir. Bu şemalar Mignotte[5] ve Asmuth-Bloom[4] tarafından bulunmuştur. Bu şemalarda çin kalan teoremi boyunca özel bir sırada tam sayı dizileri kullanılır.

4.1.Asmuth-Bloom Gizlilik Paylaşım Şeması

Asmuth-Bloom gizlilik paylaşım şemasında gizliliği dağıtma ve yeniden elde etme işlemleri aşağıdaki gibi yapılmaktadır.

- *Dağıtım İşlemleri:* n kullanıcılı bir gurup arasında K gizliliğini paylaştırmak için dağıtıcı şu işlemleri yapar:

İkili guruplar halinde birbirlerine göre asal olan pozitif tamsayılar kümesinde m_0>K bir asal sayı olmak şartı ile

$m_0 < m_1 < m_2 ..... < m_n$ olarak seçilmektedir. Bunun sonucunda da aşağıdaki eşitsizlik sağlanmaktadır.

$$\prod_{i=1}^{t} m_i > m_0 \prod_{i=1}^{t-1} m_{n-i+1} \qquad (1)$$

M, $\prod_{i=1}^{t} m_i$ 'yi göstersin. Daha sonra dağıtıcı aşağıdaki değeri hesaplar.

$$y = K + \alpha m_0$$

Buradaki α , $0 \le y < M$ koşulunu sağlayan rastgele üretilmiş pozitif bir tamsayıdır.
i.kullanıcının paylaşımları $1 \le i \le n$ aralığında, aşağıdaki denklemden elde edilir.

$$y_i = y \bmod m_i$$

- *Birleştirme İşlemi: t* kullanıcının gizliliği yeniden elde etmek için bir araya gelerek oluşturduğu küme *S* olsun. M_S, $\prod_{i \in S} m_i$ demektir.

Çin kalan teoremi kullanılarak $i \in S$ için Z_{M_S} 'deki y aşağıdaki denklem sistemi ile bulunur.

$$y \equiv y_i (\bmod m_i)$$

Gizlilik ise

$$K = y \bmod m_0$$

ile bulunur.
Çin kalan teoremine göre *y,* Z_{M_S} 'de tek bir çözümdür. $y < M \le M_S$ olduğu için, çözüm aynı zamanda Z_M'de de tektir.
Asmuth-Bloom gizlilik paylaşım şeması t-1 veya birkaç paylaşım şeklinde anahtar uzayı ile sınırlanamayan mükemmele yakın bir şemadır. Bu şema t-1 paylaşım bilindiğinde tamamıyla mükemmel bir şema değildir. Anahtar adaylarının her biri gizliğe ulaşabilecek eşit güce sahip değildir.[10,11]
Çin kalan teoremi tabanlı eşik şemanın güvenliği üzerine bir çalışma [12] numaralı kaynakta detaylı bir şekilde açıklanmıştır.

5. Çin Kalan Teoremi Tabanlı Asmuth-Bloom (t,n)=(4,5) Gizlilik Paylaşım Şeması Uygulaması

$2 \le t \le n$ şartını sağlayan (t,n)=(4,5) gizlilik paylaşım şemasını kuralım. Asmuth-Bloom tarafından önerilen çin kalan teoremi tabanlı eşik şemaya göre özel bir sırada tamsayılar seçilir. Seçilen sayılar birbirlerine göre asal sayılardır. Paylaşımlar K gizli değerle ilişkili bir sayının kongruans sınıflarıdır. Seçilen tam sayılar kümesi aşağıdaki şartları sağlamalıdır.[7]

1. $m_0 \rangle K$
2. $m_0 \langle m_1 \langle ... \langle m_n$
3. $\text{ebob}(p, m_i) = 1, \forall i$
4. $\text{ebob}(m_i, m_j) = 1,\ i \ne j$ için
5. $m_0 m_{n-t+2} .. m_n \langle m_1 .. m_t$

Buna göre sayıları şu şekilde seçelim.
$m_0 \langle m_1 \langle m_2 \langle m_3 \langle m_4 \langle m_5$
$11 \langle 13 \langle 17 \langle 19 \langle 21 \langle 23$
K=10 paylaşılacak gizlilik(anahtar) olsun.

$M=m_1.m_2.m_3.m_4=13.17.19.21=88179$ sayısı alınır. Ve $[0,(M/m_0)-1]$ oranında rastgele bir α sayısı seçilir. Buna göre $\alpha = 7$ alalım.

$K' = K + \alpha m_0$ formulü ile yeni anahtar elde edilir.

$K' = 10 + 7.11 = 87$

5 kişi arasında dağıtılan paylaşımlar şöyledir.

$K_1 = K' \bmod m_1 = 87 \bmod 13 = 9$
$K_2 = K' \bmod m_2 = 87 \bmod 17 = 2$
$K_3 = K' \bmod m_3 = 87 \bmod 19 = 11$
$K_4 = K' \bmod m_4 = 87 \bmod 21 = 3$
$K_5 = K' \bmod m_5 = 87 \bmod 23 = 18$

$I_1 = (K_1, m_1) = (9,13)$
$I_2 = (K_2, m_2) = (2,17)$
$I_3 = (K_3, m_3) = (11,19)$
$I_4 = (K_4, m_4) = (3,21)$
$I_3 = (K_5, m_5) = (18,23)$

bunlar 5 kullanıcı arasında dağıtılan anahtarlardır.

Şimdi K anahtarını eşik değerdeki kullanıcı ile yeniden elde etmeye çalışalım. Kullandığımız örnekte beş paylaşımdan rastgele seçilen dört paylaşımcı K gizli anahtarı yeniden elde edebilirler. Örneğin (I_1,I_2,I_3,I_4) kullanıcıları K'yı yeniden elde etmek istesinler.

$x \equiv 9 \bmod 13$
$x \equiv 2 \bmod 17$
$x \equiv 11 \bmod 19$
$x \equiv 3 \bmod 21$

Çin kalan teoremi standartları kullanılarak yukarıdaki kongruans denklem sisteminin çözümünden K' elde edilir. Bunun için öncelikle

$y_1 = inv(M/m_1, m_1) = inv(88179/13,13) = 4$
$y_2 = inv(M/m_2, m_2) = inv(88179/17,17) = 9$
$y_3 = inv(M/m_3, m_3) = inv(88179/19,19) = 4$
$y_4 = inv(M/m_4, m_4) = inv(88179/21,21) = 20$

Burada sayıların birbirlerine göre terslerinin hesaplanmasında genişletilmiş öklit algoritmasından faydalanılmıştır.

$$K' = \left[\frac{M}{m_1} y_1 K_1 + \frac{M}{m_2} y_2 K_2 + \frac{M}{m_3} y_3 K_3 + \frac{M}{m_4} y_4 K_4 \right] \bmod M$$

$$K' = 87$$

$K = K' - \alpha m_0 = 10$ olarak gizli anahtara ulaşılır.

6. Sonuçlar

Açık anahtar sistemlerinin önemli konularından birisi anahtar yönetimidir. Etkili eşik(threshold) şemaları kriptografik anahtar yönetiminde çok yararlıdır. Bu şemalar sağlam anahtar yönetim şemaları veya kriptografik şemaları inşa etmede etkindir. Parçalar kaybolsa bile fonksiyon korunaklı ve güvenilirdir. İncelenen şema güvenlik ve etkinlik açısından şöyle değerlendirilebilir.

Güvenlik açısından bakıldığında çin kalan teoremi tabanlı eşik gizlilik paylaşım şeması, gizliliği yeniden elde edebilme konusunda t'den daha az kümeler için mükemmel bir şema olmamasına rağmen dikkatlice seçilen parametrelerle, güvenliği arttırmaya önderlik edebilir. Oldukça fazla rastgele ve özel parametreler içerdiği için Asmuth- Bloom şemasına güvenlidir denebilir.

Etkinlik açısından değerlendirildiğinde, Asmuth-Bloom şeması K'yı yeniden elde etmek için O(t) zaman ve O(n) uzayı gerektiren etkin bir algoritma tanımlar. Shamir'in polinom şeması $O(t\log^2 t)$ zaman gerektirir. Böylece bu şema asimptotik olarak Shamir'in polinom şemasından daha etkilidir.

7. Kaynakça

[1] Han-Yu Lin, Yi-Shiung Yeh, Dynamic Multi-Secret Sharing Scheme, Int. J. Contemp. Math. Sciences, Vol.3, 2008, no. 1, 37-42.

[2] A. Shamir, How to share a secret, Communications of the ACM 22 (11) (1979) 612-613.

[3] Blakely, G. R., Safeguarding cryptography keys, Proc. AFIPS 1979 National Computer Conference, 48, (1979), 313-317.

[4] C. A. Asmuth and J. Bloom., A modular approach to key safeguardin, IEEE Transactions on Information Theory, IT-29(2): 208-210,1983.

[5] M. Mignotte., How to share a secret, In T. Beth, editor, Cryptography- Proceedings of the Workshop on Cryptography, Burg Feuertein, 1982, volume 149 of Lecture Notes in Computer Science, pages 371-375. Springer- Verlag,1983.

[6] Zhu B., Bao F., Deng R.H., Kankanhalli M. S., Wang G., Efficient and robust key management for large mobile ad hoc networks, Computer Networks, Volume 48, Issue 4, 15 July 2005, Pages 657-682

[7] Dorothy Elizabeth Robling Denning, Cryptography and Data Security, Addison-Wesley Publishing Company, 1982.

[8] Trappe W., Washington L., Introduction to Cryptography with Coding Theory Second Edition, Pearson Prentice Hall, 2006.

[9] Arda D., Buluş E., Akgün F., Yerlikaya T., Secret Sharing Schemes in Cryptographic Key Management Problem, International Science Conference, November 2008, Gabrovo

[10] K. Kaya and A. A. Selçuk. Threshold cryptography based on Asmuth-Bloom secret sharing. Information Sciences, 177(19):4148{4160, 2007.

[11] Sorin Iftene, Secret Sharing Schemes with Applications in Security Protocols, Ph.D. Thesis, January 2007.

[12] Michaël Quisquater , Bart Preneel , Joos Vandewalle, On the Security of the Threshold Scheme Based on the Chinese Remainder Theorem, Proceedings of the 5th International Workshop on Practice and Theory in Public Key Cryptosystems: Public Key Cryptography, p.199-210, February 12-14, 2002

[13] Mezenes, A., J., Van Oorschot, P., C. And Vanstone, S., A., Handbook of Applied Crptography, CRC Press, October 1996.

[14] Stinson, Douglas R., Cryptography: Theory and Practice, CRC Press, 1995