



Rapor: RFID Asıllama Protokolü HB ve Türevleri

Hopper ve Blum tarafından önerilen (2001) HB protokolü, düşük güç ve işlem kapasiteli ortamlarda –RFID gibi– asıllama yapılmasını sağlar. Temel olarak NP sınıfı bir problem kabul edilen LPN (Learning Parity with Noise) problemine dayanır. Protokole geçmeden önce bu problemi (HB’de kullanılan halini) açıklayalım:

LPN Problemi

$GF(2)$ ’de M , $r \times k$ ’lık bir matris, $x = (x_1, x_2, \dots, x_k)^T$ bir kolon vektörü ve $b = Mx$ olsun. $0 < \eta < 1/2$ olmak üzere $c = (c_1, c_2, \dots, c_r)^T$ vektöründe $\text{Prob}[c_i = 1] = \eta$ eşitliği her i için geçerli ise; M , η ve $b' = b(\text{XOR})c$ verildiğinde x ’i bulma problemine LPN problemi adı verilir.

M ve b verildiğinde (çözüm varsa) Gauss eleme metodu ile x ’i bulmak kolaydır. Fakat gürültü faktörü (c vektörü), hangi denklemlerin doğru olduğunu gizler. Tek bilinen $r\eta$ denklemin doğru olduğudur (hangileri olduğu bilinmiyor). $r = 80$ ve $\eta = 1/4$ için yaklaşık 2^{62} farklı (sadece doğru denklemlerden oluşması istenen) denklem kümesi oluşturulabilir, ve bunlardan sadece bir tanesi gerçek x değerlerini verir. Bu da kaba kuvvet atağına yakın bir zorluk verir.

HB ve HB+ Protokolleri

| | | |
|--|---------------------------------------|---|
| Etiket (x) $\nu \in \{0, 1 \mathcal{P}(\nu = 1) = \eta\}$ | | Okuyucu (x) |
| $z = a \cdot x \oplus \nu$ hesapla | \xleftarrow{a} \xrightarrow{z} | Rastsal $a \in_R \{0, 1\}^k$ oluştur Kontrol et: $a \cdot x \approx z$? |

HB protokolünün 1 çevrimi

Şekilde görüldüğü gibi HB protokolünde tek taraflı asıllama yapılır (etiket–okuyucuya). Burada x etiket ve okuyucu arasında paylaşılan k bit anahtar ($k \approx 250$), a k bitlik rastsal bir vektör, ν gürültü biti (η olasılıkla $\nu = 1$), \cdot ise nokta çarpımını gösterir. Okuyucu, farklı a 'lar ile yukarıdaki çevrimi r defa tekrarlar (tipik olarak $r \approx 80$). Okuyucu, yaklaşık olarak $r\eta$ hatalı gönderimi kabul eder ve asıllama olur. Yani eğer $r = 80$ ve $\eta = 1/4$ ise, 20 civarında hata ($ax \neq z$ durumu) okuyucu tarafından kabul edilir.

Bu protokolün pasif saldırganlara karşı güvenli olduğu LPN problemi sayesinde ispat edilmiştir. Aktif bir saldırgan ise herhangi bir asıllama sırasında okuyucu gibi davranarak sürekli aynı a 'yı vererek anahtar hakkında bir bitlik bir bilgi elde edebilir. Buna karşı 2005'te Juels ve Weis, etiketin de rastsal bir vektör oluşturduğu aşağıdaki protokolü önerdi;

HB+ Protokolü

HB+

| | | |
|---|---------------------------------------|--|
| Etiket (x, y) $\nu \in \{0, 1 \mathcal{P}(\nu = 1) = \eta\}$ | | Okuyucu (x, y) |
| Körleştirme vektörü $b \in_R \{0, 1\}^k$ | \xrightarrow{b} | |
| Hesapla: $z = a \cdot x \oplus b \cdot y \oplus \nu$ | \xleftarrow{a} \xrightarrow{z} | Rastsal $a \in_R \{0, 1\}^k$ Kontrol et: $a \cdot x \oplus b \cdot y \approx z$ |

HB+'ya da Gilbert ve diğerleri (2005) atak yapınca, 2006'da Bringer ve diğerleri HB++'yı duyurdu. Aynı yıl içerisinde Piramuthu da HB++'ya atak yaptı ve kendi önerisini sundu. 2007'de ise Munilla ve Peinada, olasılıksal öğeler ekleyerek HB-MP protokolünü, 2008'de de Hammouri ve

Sunar PUF tabanlı çalışan PUF-HB protokolünü önerdiler. İstanbul'daki EUROCRYPT 2008'de ise Gilbert, Robshaw ve Seurin hammingweight özelliğini kullanan, ve iletişimde HB'nin diğer türevlerine göre çok daha az sayıda bit transferi içeren HB# protokolünü tanıttılar.

Buradan da anlaşılacağı gibi, özellikle 2005'ten sonra HB üzerine bir çok araştırma yapılmış, ve RFID etiketlerde kullanılabilecek pratiklik ve güvenlik özelliklerini kazanması için geliştirilmiştir. Bilinen kriptografik öğelerden (simetrik-asimetrik şifreleme, özet fonksiyonlar, vb.) farklı yapılar kullanması (LPN problemi), HB'ye olan ilgiyi arttırmıştır.

Kaynaklar

1. A. Juels and S. Weis. "Authenticating Pervasive Devices with Human Protocols", in V. Shoup (ed.) *Advanced in Cryptology - CRYPTO'05, Volume 3126, Lecture Notes in Computer Science*, pp. 293-308, Springer-Verlag, 2005.
2. G. Hammouri and B. Sunar. "PUF-HB: A Tamper-Resilient HB Based Authentication Protocol" in *ACNS 2008, LNCS 5037*, pp. 346-365, 2008. Springer-Verlag Berlin Heidelberg 2008.
3. H. Gilbert, M. Robshaw, and H. Sibert. "An Active Attack Against HB+ - A Provably Secure Lightweight Protocol." *Cryptology ePrint Archive, Report 2005/237*, 2005. <http://eprint.iacr.org>.
4. H. Gilbert, M. Robshaw, and Y. Seurin. "HB#: Increasing the Security and Efficiency of HB+" in *EUROCRYPT 2008, LNCS 4965*, pp. 361-378, Springer, Istanbul 2008.
5. J. Bringer, H. Chabanne, and E. Dottax. "HB++: a Lightweight Authentication Protocol Secure Against Some Attacks," *IEEE International Conference on Pervasive Services, Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing – SecPerU*, 2006.

6. J. Munilla, A. Peinado. "HB-MP: A further step in the HB-family of lightweight authentication protocols" in *Elsevier Computer Networks*, 51 (2007) 2262–2267, 2007.
<http://www.sciencedirect.com>.
7. N.J. Hopper and M. Blum. "Secure Human Identification Protocols." In *C. Boyd (ed.) Advances in Cryptology - ASIACRYPT 2001*, Volume 2248, Lecture Notes in Computer Science, pp. 52-66, Springer-Verlag, 2001.
8. S. Piramuthu. "HB and Related Lightweight Authentication Protocols for Secure RFID Tag/Reader Authentication" in *COLLECTeR Europe Conference, Basel, Switzerland, 2006*.