電波伝搬特性に基づく秘密鍵共有方式に関する一考察

A Study on Secret Key Agreement Based on Radio Propagation Characteristics

情報セキュリティ大学院大学

若尾　聡

＜要旨＞

無線通信を使用する機器には常に盗聴の危険性があり、これらの脅威に対抗するために、暗号技術を採用しているが、現在において主流として使用されている暗号技術の大半は安全性の根拠を解読に必要な計算量においている。近年、安全性の根拠を情報理論におく、移動体無線通信を利用した秘密鍵共有等のセキュリティ技術方式の研究が急速に進展しており、IC タグといった無線を使用する小型機器への展開が可能になると考えられる。

そこで本論文では、移動体無線通信における電波伝搬特性を利用して秘密鍵の生成と共有を行う方式にて生成した鍵の乱数性に関する評価を、IC タグからの電波を使用して、実際の使用状況を想定した環境下において、FIPS140-2 に基づいて行ったのでその報告を行う。

評価の結果、想定環境と本論文で採用した鍵共有方式との組み合わせでは、乱数検定をパスするような秘密鍵は生成できないことが判明した。

また上記の原因が「鍵生成時におけるパラメータが、電波伝播特性が変化する速度を考慮した値になっていなかったことにある」ことを突き止めた。

＜Abstract＞

As a countermeasure for the risk of eavesdropping the secret information in wireless communications, it is usual to use cryptography such as public key cryptosystem and symmetric key cryptosystem that are based on amount of computation. Recently information-theoretically secure cryptographic techniques such as secret key agreement based on the radio propagation characteristics have been studied. These techniques will be able to be applied for IC tag that has wireless communication equipment.

This paper discusses randomness of secret key that are generated using radio propagation characteristics. The randomness of secret key is evaluated in the environment of using radio wave actually. As the results of evaluation, it found that our scheme cannot generate the secret key conforming to tests described at FIPS140-2 in our test environment. It further investigated the cause of low randomness, and found that parameter in key generation are not adaptive to the change of radio propagation characteristics.