Computer Security Magazine

urandom

vol.6

目次

IoT 機器の FW 解析 -CBCTF2018 予選問題 Odin 解説-

1 はじめに

いい感じにスマホアプリと通信していい感じの機能を提供してくれるいい感じの組み込み機器（IoT 機器[*1]）が流行りですが、いい感じに通信するにはいい感じの通信手段が必要です。そこで、組み込み機器とスマホアプリを繋ぐための通信手段としてよく使われるのが Bluetooth Low Energy（BLE）です。BLE はその名前の通り低電力通信用に設計された Bluetooth のサブセットで、利用法と機器の設計次第ではボタン電池 1 つで数年動作するような通信機が作れる、いい感じの規格です。

BLE で通信する機器を作る時には BLE 通信用の System on Chip（SoC）を機器に組み込む方法がよく取られます。SoC があるということは、大抵の場合 SoC の中にファームウェアが居る訳で、BLE な IoT 機器のセキュリティについて調べる時には BLE SoC のファームウェアの解析が重要なステップになります。筆者は、BLE で通信する IoT 機器のファームウェア解析を題材として、CODE BLUE CTF 2018 予選[*2]で 2 問のリバースエンジニアリング問題を出題しました。出題にあたっては BLE SoC などを利用して模擬的な BLE 機器を作り、ファームウェアも出題用のものを開発しました。本稿では、筆者が出題した問題について解答過程などを解説します。

[*1] Internet Protocol を喋らない組み込み機器を Internet of Things の名前で呼ぶのおかしくないですか？

[*2] `http://ctf.codeblue.jp/`

素因数分解ゲーム

1　はじめに

量子コンピューターの開発に成功した研究者ボブはアリスにあるゲームを提案しました。そのゲームとは「巨大な 2 つの素数 p, q をかけた合成数 $N := p \cdot q$ を先に素因数分解した方が勝つ」というものです。素因数分解は古典コンピューターにとっては難しい問題ですが、その答えが与えられたとき正しいかどうかを検証することはかけ算を一度行うだけでよいので、古典コンピューターでも高速に行えます。一方で、量子コンピューターにとっては素因数分解そのものも高速に行えます。つまりボブは、このゲームに勝ち、かつボブの解答が正しいとアリスに検証させることでボブが量子コンピューターを確かに持っているということを自慢しようとしました。

このゲームを聞いたとき、アリスはすぐにボブが量子コンピューターを作ったのだと予測しました。実はアリスも友人のチャーリーから量子コンピューターを密かに貰っており、その量子コンピューターを利用してボブを打ち負かしたいと思いました。

さらに暗号の専門家であるアリスは、このゲームに問題があることに気がつきます。参加者がアリスとボブ以外にいないため、このゲームは量子コンピューターを持っている・持っていないに関わらず、合成数 N を作った方が勝つゲームです。なぜなら素数を 2 つ作ってからその乗算で合成数 N を作ることで、素因数分解することなく合成数 N の素因数を知ることができます。このことを直ちにボブへ指摘しようと思ったアリスですが、しかし指摘してしまったらボブはゲームのルールを変更し、アリス自身が密かに入手した量子コンピューターでボブを打ち負かすという計画が破綻するかもしれません。そこでアリスは「2 人だけで、かつ 2 人ともが 2 つの素因数 p, q を知ることなくそれらを乗算した合成数 N を作ることができないか？」という問題にとり組むことにしました。

1.1 本稿の構成

本稿ではまず 2 節で量子コンピューターによる素因数分解のアルゴリズムを量子コンピューターの詳細には立ち入らずに簡単に説明します。そして 3 節では素因数分解と関わりの深い RSA 暗号について説明し、RSA 暗号の鍵を 2 人で作成する方法を 4 節で述べます。そして具体的なプロトコルを 5 節で説明します。最後に 6 節で本稿のまとめを述べ、そして 8 節で本稿を書くにあたって参考にした文献を紹介します。

2 量子コンピューターによる素因数分解

具体的なゲームを構成する前に、まずは量子コンピューターはどのように素因数分解を行うのかについて簡単に解説します。量子コンピューターを利用した素因数分解は *Shor* のアルゴリズム [1] と呼ばれています。ただ、量子コンピューターを利用するとなぜ高速化されるかについて解説することは紙面の都合上困難なので、ここでは量子コンピューターを道具としてどのように使うのかということを中心に解説します。

2 つの素数 p, q を因数に持つ合成数 N が与えられているとき、Shor のアルゴリズムは次のようになります。

1. 古典コンピューターを用いて $2 \leq x < N$ となる適当な整数 x を選択する。ただし x と N は互いに素（$\gcd(x, N) = 1$）である[*1]
2. 量子コンピューターを用いて $x^r \equiv 1 \pmod{N}$ となる最小の整数 r を得る
3. もし r が奇数または $x^{r/2} \equiv \pm 1 \pmod{N}$ ならば手順 1 からやりなおす
4. そうでなければ、$\gcd\left(x^{r/2} \pm 1, N\right)$ が N の 2 つの素因数となる

この方法で本当に素因数分解が可能なのか？ というといまひとつ分からないかもしれません。まず、オイラーの定理により、合成数 N と互いに素な x について次のことが言えます。

$$x^{(p-1)(q-1)} \equiv 1 \pmod{N} \tag{1}$$

つまり、上記の手順 2 で量子コンピューターを用いて求めた r が正しければ $(p-1)(q-1)$ となります。

実はすべての整数 n について次が成り立つ x, y が存在することが知られています。

[*1] $\gcd(a, b)$ は 2 つの数 a, b の最大公約数を意味します。

urandom vol.6

発行者	urandom
表紙デザイン	秋弦めい
発行日	2018 年 8 月 10 日
バージョン	1.00（2018-08-02 17:57:25+09:00）
コミット ID	faa111f
連絡先	`https://blog.urandom.team/`
印刷所	株式会社栄光