岐阜大学工学部
電気電子・情報工学科
令和 6 年度卒業論文

セキュアな V2V アドホックネットワーク ルーティングプロトコルのための EdDSA 署名方式の評価

三嶋研究室

学籍番号：1213033107

永野 正剛

指導教員：三嶋 美和子 教授

目次

はじめに

第 1 章　準備

1.1　VANET

vanet 書くよ

1.2　GPSR

GPSR 書くよ

1.3　楕円曲線

1.3.1　EdDSA

1.4　デジタル署名

1.4.1　EdDSA

実験に導入した Ed25519 のプロトコル内で使用されるリトルエンディアン、エンコーディング、プルーニングについて説明する.

リトルエンディアン

(1)　最下位バイトから順に配置する形式.　プロトコル内では、秘密スカラーの生成や公開鍵の生成において、リトルエンディアンの整数を使用する.

エンコーディング

(1)　すべての値はオクテット文字列としてコード化され、整数はリトルエンディアン規則を使用してコード化される.

(2) 楕円曲線上の点のエンコード

y 座標をリトルエンディアン形式の 32 オクテット文字列にエンコードし、32 バイト目の最上位ビットを 0 に設定する. x 座標の最下位ビットを y 座標の 32 バイト目の最上位ビットに埋め込む.

プルーニング（ビット操作）

(1) 最初のバイトの下位 3 ビットを 0 にクリアする.

(2) 最後のバイトの最上位ビットを 0 に設定し、最上位 2 ビット目を 1 に設定する.

EdDSA の 3 つのアルゴリズムの手順を以下に述べる.

鍵生成

1. 法とする素数 p、楕円曲線 E、基準点 G、鍵のサイズ b、ハッシュ関数 H、コファクター c、位数 L を定める.
2. b バイトのランダムな値 sk を生成し、秘密鍵とする.
3. $h = H(sk)$ を計算し、h（オクテット文字列）を前半部分 h[0] から h[31] と後半部分 h[32] から h[63] に分ける.
4. 前半部分 s[0] から s[31] を使ってプルーニングしたものをリトルエンディアンの整数として解釈し、スカラー $s \pmod{L}$ を生成する.
5. 基準点 G を使って $A = sG$ を計算し、A のエンコードを公開鍵とする.

署名生成フェーズ

1. 秘密鍵 sk を使って、ハッシュ値 $h = H(sk)$ を計算する.
2. h の後半部分 h[32] から h[63] を使って、$r = DEC(H())$.
3.
4.

署名検証フェーズ

1.
2.

第 2 章　EdDSA

2.1　EdDSA パラメータ

EdDSA のパラメータは以下のようである.

- p : 法となる素数. EdDSA は $\mathbb{F}_p$ 上の楕円曲線を使用する.
- b : $p < 2^{b-1}$ となる正整数. 公開鍵の長さを表す.
- E' : エンコーディング関数.
- H : ハッシュ関数. 2b ビット長のハッシュ値を出力する.
- (a, d, c, l) : 楕円曲線 E を決定するパラメータ.

$$E := \{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p \mid ax^2 + y^2 = 1 + dx^2y^2\}$$

  - a は $\mathbb{F}_p$ 上平方剰余、d は非ゼロの非剰余.
  - $c = 2$ または 3. l は奇素数で E の位数 $\#E = 2^c l$ となるような数.
- n : $c \leq n < b$ となる整数.
- B : E 上のベースポイント. $B \neq (0, 1)$
- PH : プレハッシュ関数. HashEdDSA の場合に用いる

2.2　Ed25519

2.3　ECDSA と EdDSA の比較

第 3 章　提案手法

第 4 章　シミュレーション環境

第 5 章　シミュレーション実験

第 6 章　EdDSA に関する実装評価まとめ

おわりに

謝辞

参考文献