情報セキュリティ学特論レポート
3 者間 DH 鍵共有

園田継一郎

2021 年 12 月 30 日

1　はじめに

DH 鍵共有では, 2 者間でしか鍵の共有ができない.

DH 鍵共有は, 以下のように行う. 複数のメッセージに同じメッセージを送る場合, 3 者間で鍵共有ができれば便利である.

2　3 者間 DH 鍵共有

3 者間 DH 鍵共有には, 楕円曲線上のペアリングという演算が使われる. ペアリングは, 楕円曲線 E 上の 2 個の点の組からある有限体 $\mathbb{F}_q$ への写像である [1]. $P, Q \in E$, g を生成元とすると, ペアリング e は以下のように定義される.

$$\begin{array}{rccc} e\colon & E \times E & \longrightarrow & \mathbb{F}_q \\ & \cup & & \cup \\ & (P, Q) & \longmapsto & g^{S(P,Q)} \end{array}$$

ここで $S(P, Q)$ とは, 楕円曲線 E 上の位置ベクトル P, Q で張られる平行四辺形の面積である. ただし, Q が P の半時計回りに位置する場合は正となり, そうでなければ負となる. P を $a(a \in \mathbb{Z})$ 倍したとき面積も a 倍され, 第二成分についても同様である. $a, b \in \mathbb{Z}$ として式で表すと,

$$S(aP, bQ) = abS(P, Q)$$

となる.

3　まとめ

ペアリングを用いることで, 3 者以上との鍵共有ができ, マルチキャストしやすくなる. しかし, まだ実用的ではない.

参考文献

[1] 光成 滋生「クラウドを支えるこれからの暗号技術」秀和システム (2015) https://github.com/herumi/ango/raw/master/ango.pdf