

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

2022 年 1 月 23 日

1 はじめに

2 者間で鍵を共有する手法に DH(Diffie-Hellman) 鍵共有がある. DH 鍵共有では, 素数 p (以下は全て $\text{mod } p$ とする) と生成元 g を決め, A さん, B さん, C さんがそれぞれが秘密の整数値 a, b, c を持っている. g^a, g^b, g^c は公開されるので, A さんと B さんの 2 者間であれば g^{ab} を共有できる. 3 者間で同じ値を共有したいとき, 例えば A さんは $(g^b \cdot g^c)^a = g^{ab+ac}$ を計算できるが, B さんと C さんは g^{ab+ac} を計算できない. 共有できそうな値として, g^{a+b+c}, g^{abc} が挙げられる. このうち g^{a+b+c} は $g^a \cdot g^b \cdot g^c$ で誰でも計算できてしまうので秘密鍵として使えない. g^{abc} を共有できることが理想だが, それぞれが知っている情報で g^{abc} は計算できない.

複数人に同じメッセージを送る場合, グループで鍵共有できれば便利である. 以下では, 3 者間で鍵を共有するための手法を紹介する.

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}_p への写像である [1, p.80]. P, Q を E 上の点, 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.

$$\begin{array}{ccc} e: & E \times E & \longrightarrow \mathbb{F}_p \\ & \Downarrow & \Downarrow \\ & (P, Q) & \longmapsto g^{S(P, Q)} \end{array}$$

ここで $S(P, Q)$ とは, 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. 辺の長さを a 倍したとき, 面積も a 倍されるので, $a, b \in \mathbb{Z}$ としたとき, S について以下が成り立つ.

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

つまり、ペアリングでは

$$e(aP, bQ) = g^{S(aP, bQ)} = g^{abS(P, Q)} = \left(g^{S(P, Q)}\right)^{ab} = e(P, Q)^{ab}$$

が成り立つ。この性質を使えば、以下のように 3 者間鍵共有ができる。

1. 楕円曲線上の P, Q を固定して A さん, B さん, C さんで共有する。
2. それぞれ秘密の整数値 a, b, c を持ち, $(aP, aQ), (bP, bQ), (cP, cQ)$ を公開する。
3. A さんは $e(bP, cQ)^a = e(P, Q)^{abc}$ を計算する。B さん, C さんも同様に $e(P, Q)^{abc}$ を計算する。

この手法で 3 者間鍵共有が実現できるが、共有する値が多く、計算順序も考慮しなければならない。そこで、写像 e' を

$$\begin{array}{ccc} e': & \langle P \rangle \times \langle P \rangle & \longrightarrow \mathbb{F}_p \\ & \Downarrow & \Downarrow \\ & (aP, bP) & \longmapsto e(aP, \psi(bP)) \end{array}$$

と定義する。ここで ψ は、楕円曲線上の P を、 P の巡回群 $\langle P \rangle := \{nP \mid n \in \mathbb{Z}\}$ に含まれない Q に移す線形写像 (distortion 写像) である [1, p.86]。 ψ の線形性から、

$$e'(aP, bP) = e(aP, \psi(bP)) = e(aP, b\psi(P)) = e(P, \psi(P))^{ab} = e'(P, P)^{ab}$$

となり、 e と同様の性質が成り立つ。 P どうして e を計算すると、

$$e(P, P) = g^{S(P, P)} = g^0 = 1$$

より鍵として使えないが、 e' であれば

$$e'(P, P) = e(P, \psi(P)) = e(P, Q) \neq 1$$

なので、 P のみで鍵を作れる。 e' を使った 3 者間 DH 鍵共有は以下になる。

1. 楕円曲線上の P を固定して A さん, B さん, C さんで共有する。
2. それぞれ秘密の整数値 a, b, c を持ち, aP, bP, cP を公開する。
3. A さんは $e'(bP, cP)^a = e'(P, P)^{abc}$ を計算する。B さん, C さんも同様に $e'(P, P)^{abc}$ を計算する。

これにより、 Q を共有する必要がなく、鍵の計算順序を考慮しなくてよい 3 者間鍵共有が実現できる。

3 まとめ

DH 鍵共有では 2 者間の鍵共有しかできないが、楕円曲線上のペアリングを用いることで 3 者間鍵共有ができる。さらに一般化して n 者間鍵共有ができればマルチキャストに便利と考えられるが、2015 年初頭で実用的な手法は見つかっていない [1, p.84]。

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>