

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. 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. ペアリングという演算は, 楕円曲線 E 上の 2 個の点の組から [1]

3 まとめ

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>