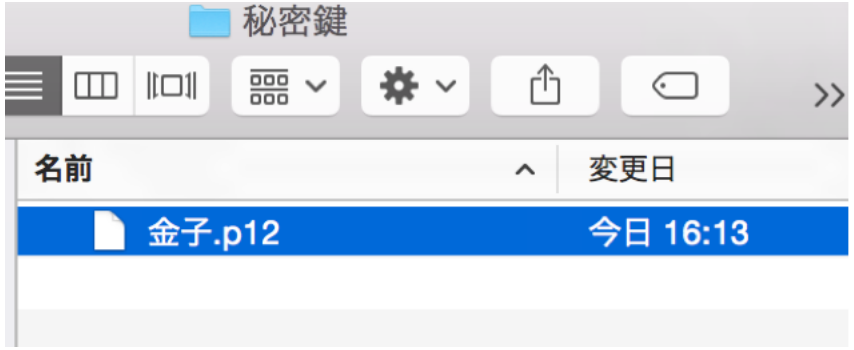
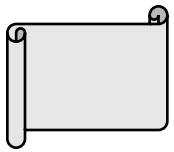
マイナンバーカードを用いた電子署名アプリケーションの開発

明治大学総合数理学部
菊池研４年　金子　曜大

研究背景

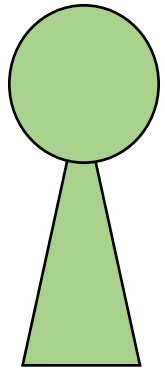


Acrobatで署名をした場合、
PC上にこのような秘密鍵の
ファイルが作成されて漏洩の
危険性がある



Aさんの
電子署名

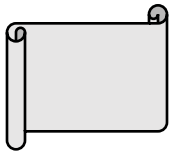
秘密鍵



Aさん(被害者)

Bさん(攻撃者)

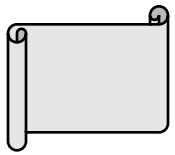
鍵をコピー
してして、
なりすまし
をしよう



Aさんの
電子署名

PC上に秘密鍵を保管している
と、漏洩の恐れがある

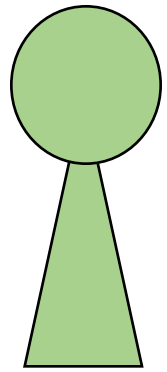
研究目的



Aさんの
電子署名

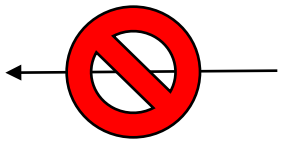
ICカードに内蔵される秘密鍵は本人で
あっても取り出せず、安全性が高い

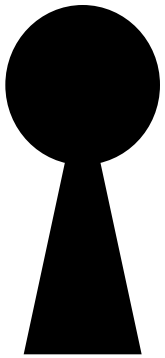
秘密鍵



Aさん(被害者)

マイナンバーカード

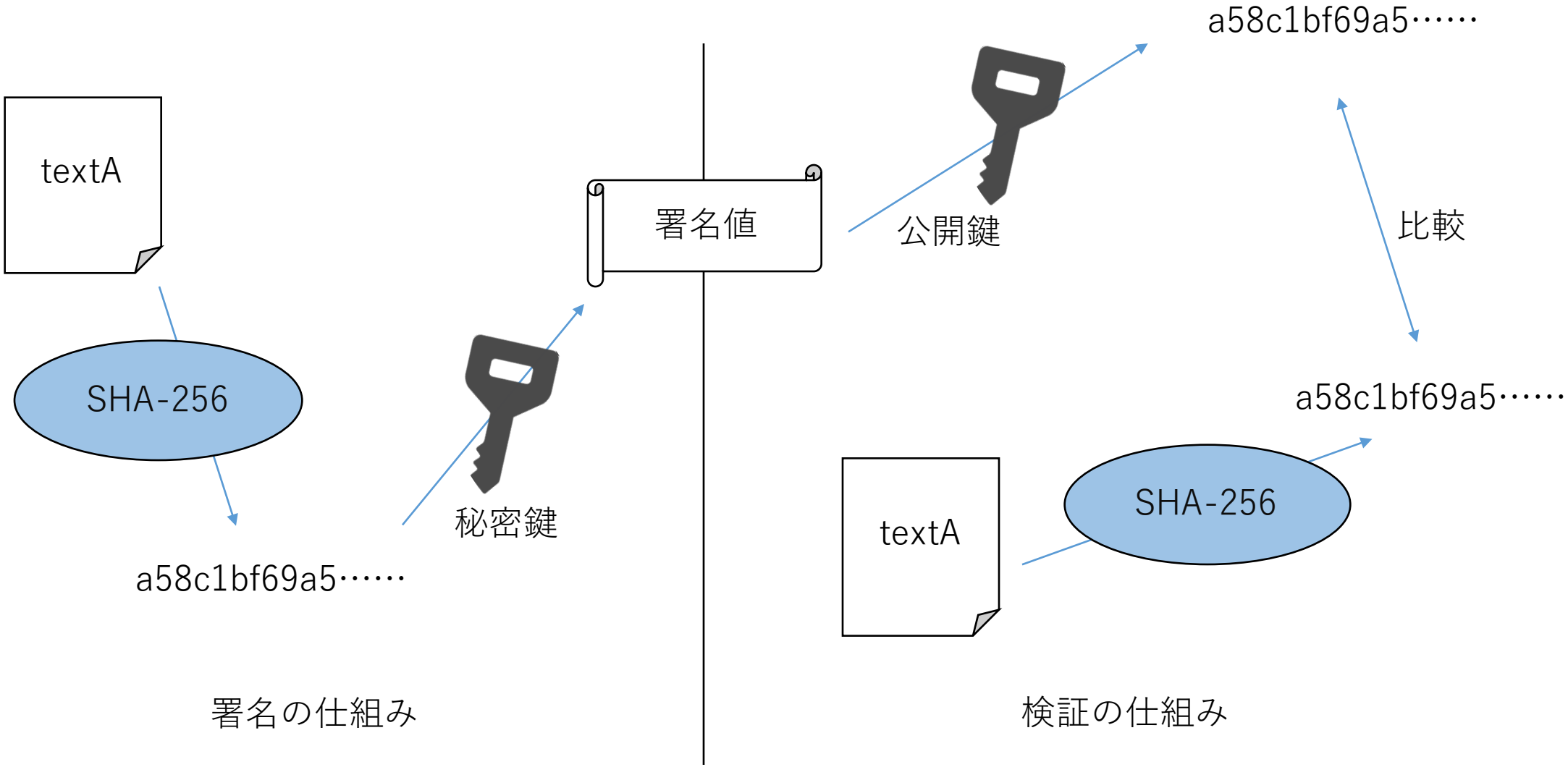




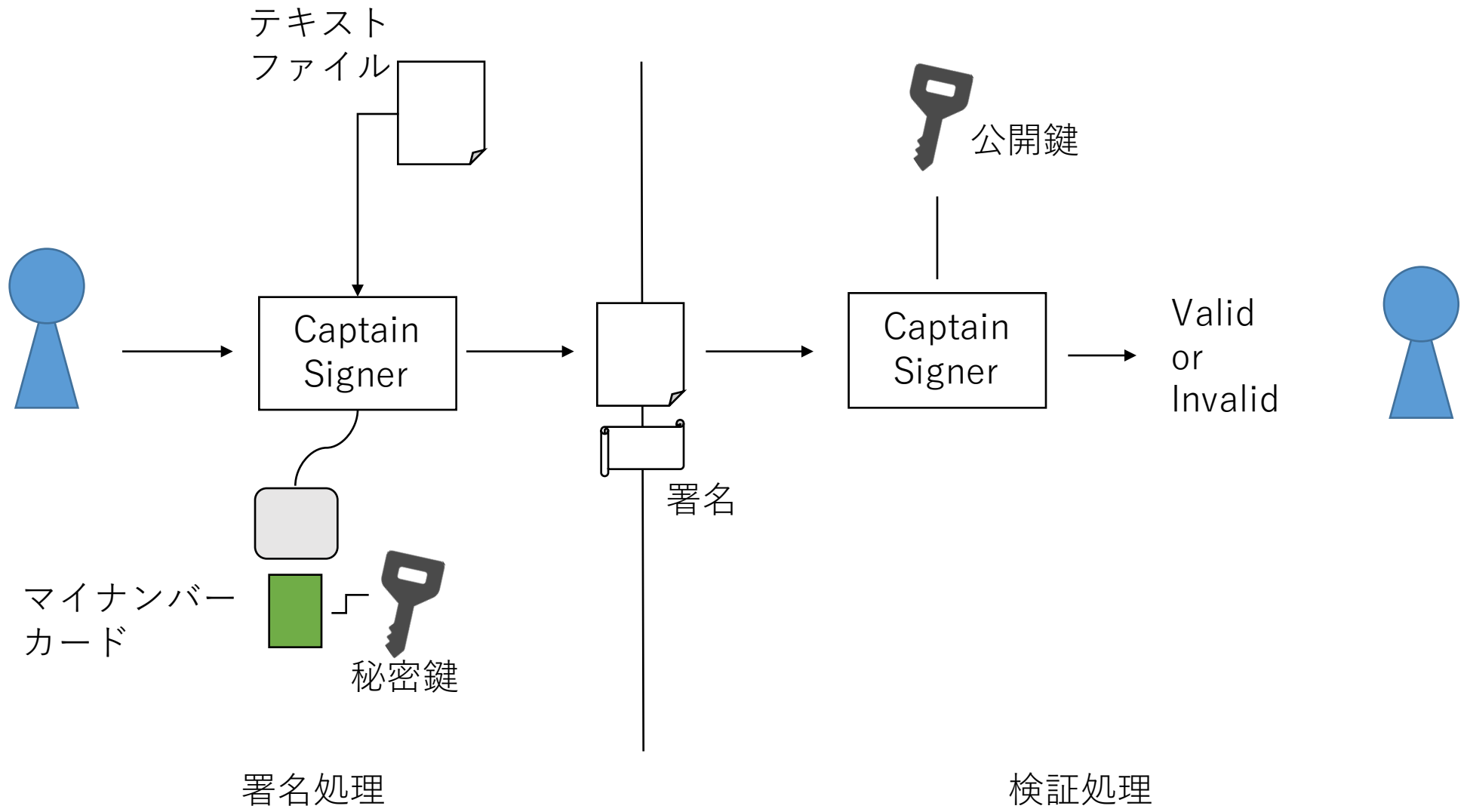
Bさん(攻撃者)

秘密鍵がコピーできない！

電子署名の仕組み

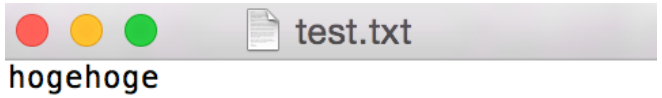

textA
SHA-256
a58c1bf69a5……
秘密鍵
署名値
署名の仕組み
公開鍵
a58c1bf69a5……
比較
a58c1bf69a5……
SHA-256
textA
検証の仕組み

Captain Signerの開発



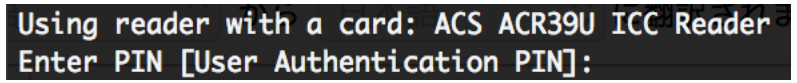
実行の様子（署名）

未署名テキスト

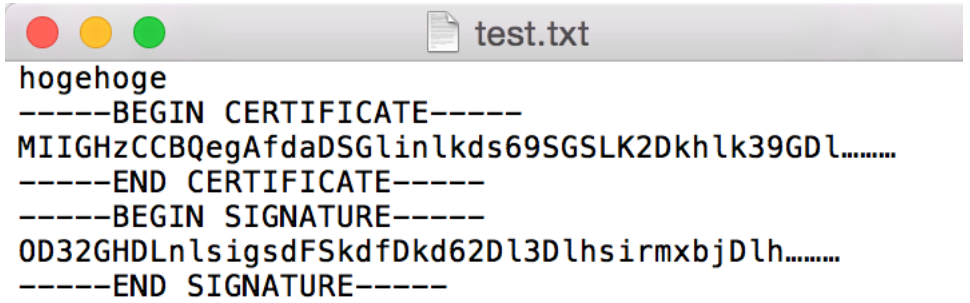


①

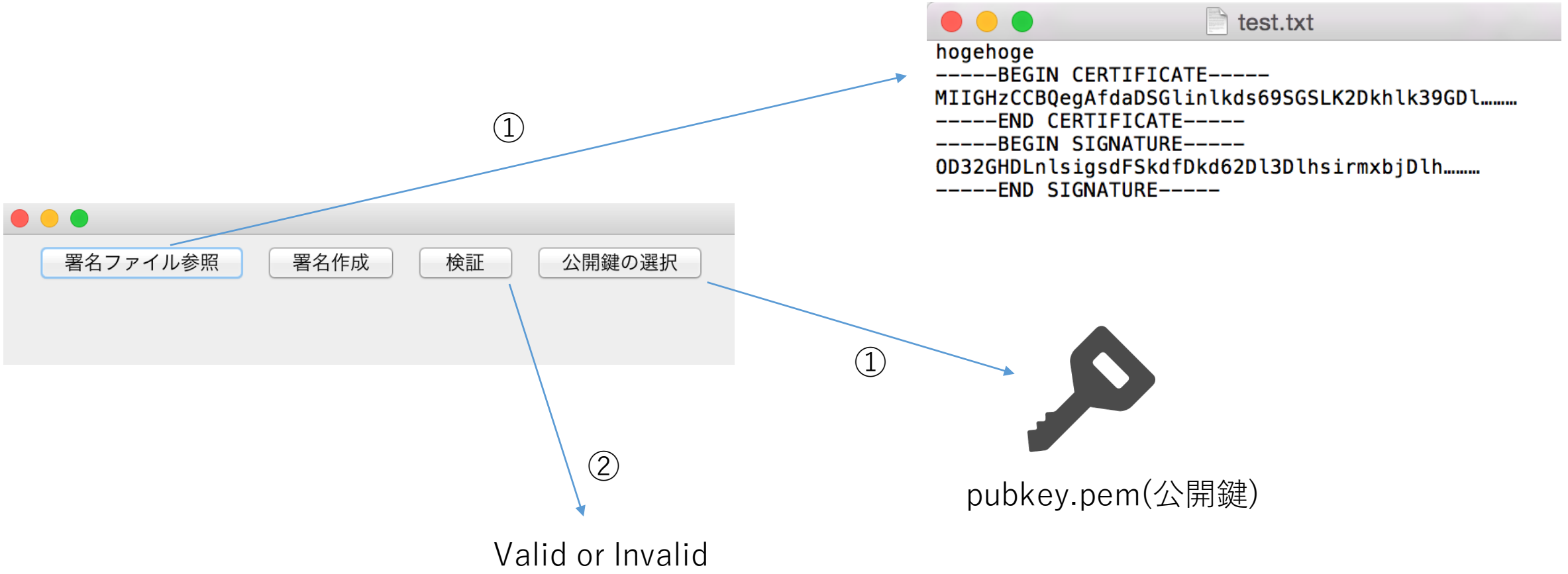
②



署名済みテキスト



実行の様子（検証）

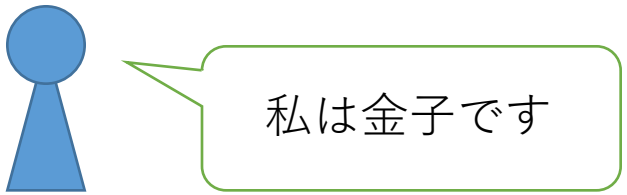

test.txt
hogehoge
-----BEGIN CERTIFICATE-----
MIIGHzCCBQegAfdaDSGlinlkds69SGSLK2Dkhlk39GDl……
-----END CERTIFICATE-----
-----BEGIN SIGNATURE-----
0D32GHDLnlsigsdFSkdfDkd62Dl3Dlhsirmxbj Dlh……
-----END SIGNATURE-----
署名ファイル参照
署名作成
検証
公開鍵の選択
①
①
②
pubkey.pem(公開鍵)
Valid or Invalid

従来の署名システムとの比較

	署名者情報	タイムスタンプ	署名できるファイル	秘密鍵の保管場所
Acrobat	◯	◯	◯	危険
Captain Signer	◯	×	△	安全

利用例

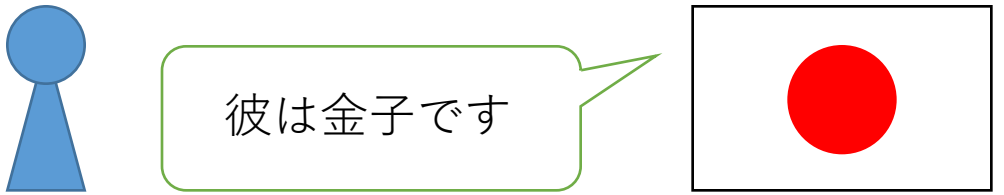
オレオレ署名



by金子

自分で自分を証明しているだけなので
公的文書には利用できない

マイナンバーを用いた署名

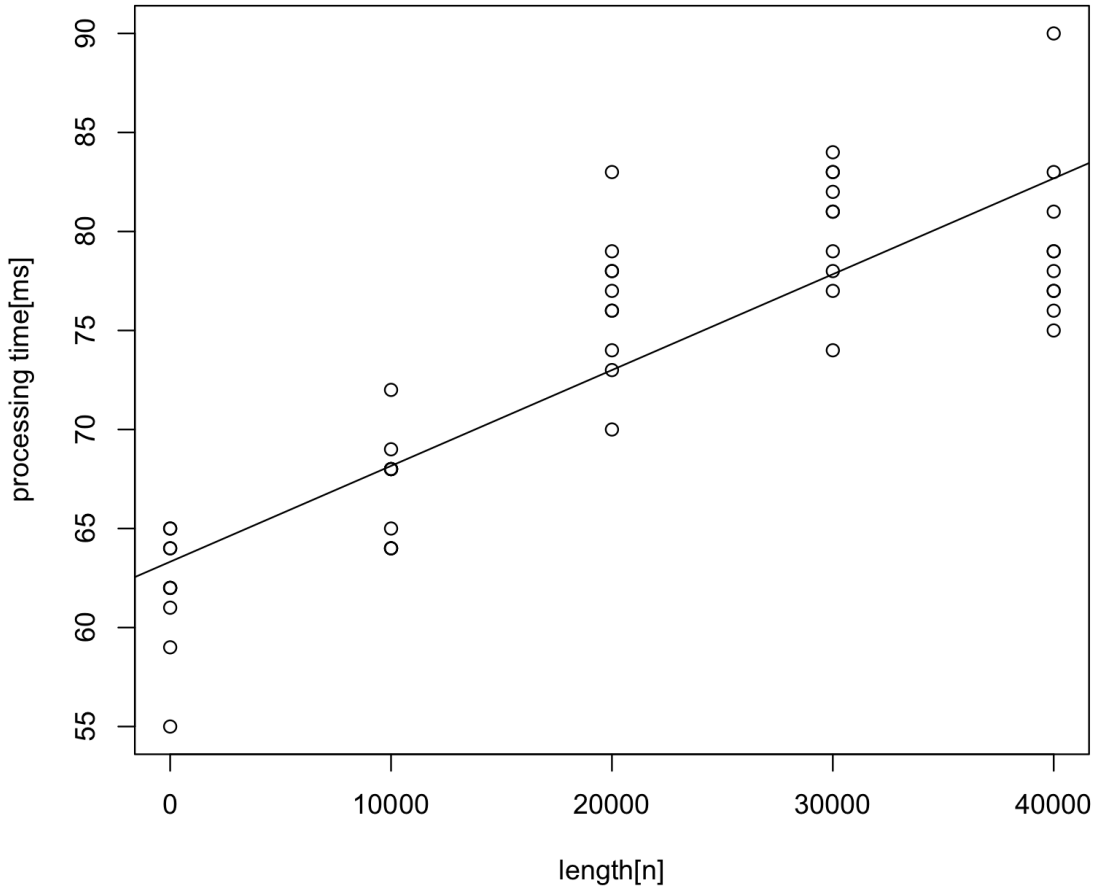


by日本

e-Taxや婚姻届等の公的文書に
用いることができる

電子署名及び認証業務に関する法律を参照

処理速度の評価



ファイルの文字数を変更した署名のパフォーマンス

ハッシュにかける時間（本文をSHA-256でハッシュ）	10000バイトにつき5ms
＋	
署名にかかる時間（ハッシュ値を秘密鍵で署名）	62.5ms

まとめ

マイナンバーカードを用いた安全性の高い電子署名アプリケーションが開発した。

テキストファイル以外への署名、タイムスタンプがないので、システムの拡張が今後の課題である。