【2007/最終】プロジェクトNo.1 セキュリティパラダイムの革命 ペアリング暗号

担当教員
高木　剛 Takagi Tsuyoshi
宮本　衛市 Miyamoto Eiichi
小西　修 Konishi Osamu

墨塗り署名
The Sanitize Signature

Mr.Sumith

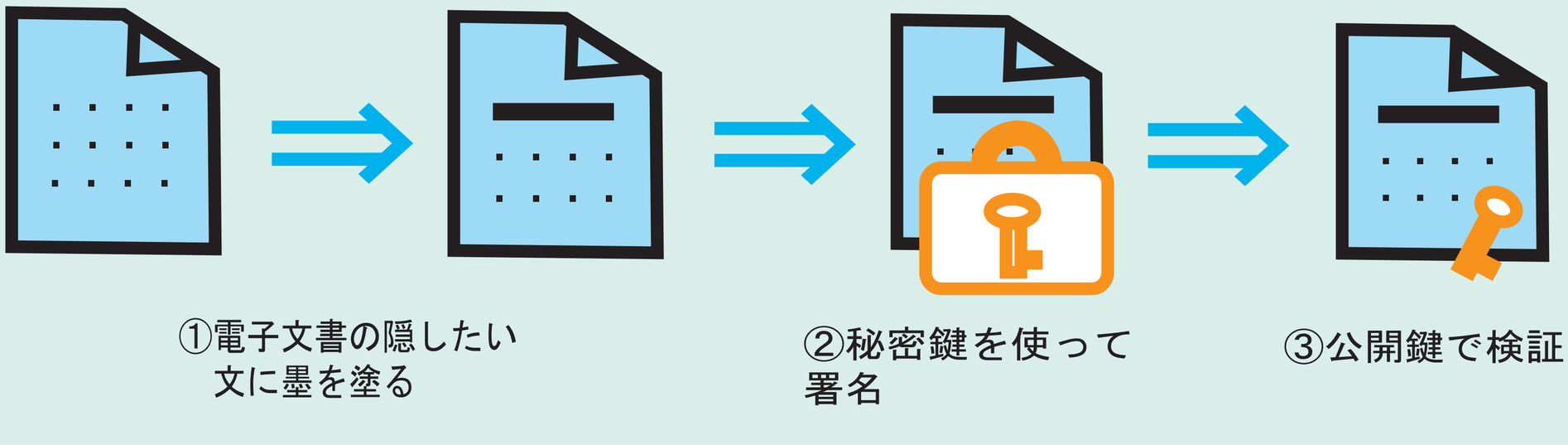
氏名 Name
久岡　直史 Hisaoka Naofumi
宮崎　行規 Miyazaki Yukinori
本間　匠 Honma Takumi
宮本　義弘 Miyamoto Yosihiro

概要

前期で用いたペアリングアルゴリズムを使い、墨塗り署名のアプリケーションを作成した。

墨塗り署名とは

文書に署名を施した後も、第三者に公開する際に開示すべきでないデータ（個人情報など）
が存在する場合、それらの情報を秘匿する必要が出てくる。
しかし、電子署名を施した後の文書に情報の秘匿などの処理を行うと、
たとえそれが正当なものであったとしても不正な改竄とみなされてしまう。
墨塗り署名は、電子署名を施した後もセル単位での情報の秘匿が可能であり、
かつ改竄とみなされないというものである。
つまり、「墨塗りした部分以外に不正な改竄はされていない」ということを証明するためのものである。
署名をする際、公開鍵暗号方式を利用する。



①電子文書の隠したい文に墨を塗る

②秘密鍵を使って署名

③公開鍵で検証

アプリケーション
Mr.Sumithとは

墨塗り署名技術の実装例として、墨塗りアプリケーション『Mr.Sumith』を開発した。
『Mr.Sumith』は、英文書の一部に墨塗りを施し、秘匿することができる。
また、このアプリケーションによって墨塗りされた部分を不正な改竄として扱わない検証を行うことができる。

Mr.Sumith

まず最初に、署名と検証のボタンが出る。
署名ボタンを押してGO!!

次に参照を押して文を出力し墨塗りしたい単語を入力。

ペアリング値と公開鍵を入力して署名した文を検証する。

検証できれば「本人の文章です」とでる。

HeをSheに変えると署名が改竄されたので検証できなくなる