

透かし暗号

KeyWord Search



氏名
Name

佐々木 勇太
Sasaki Yuta

丹羽 弘和
Niwa Hirokazu

古林 靖規
Kobayashi Yasunori

真田 淳史
Sanada Atsushi

keyword Search

ファイル検索の概要

Searching on file name Outline

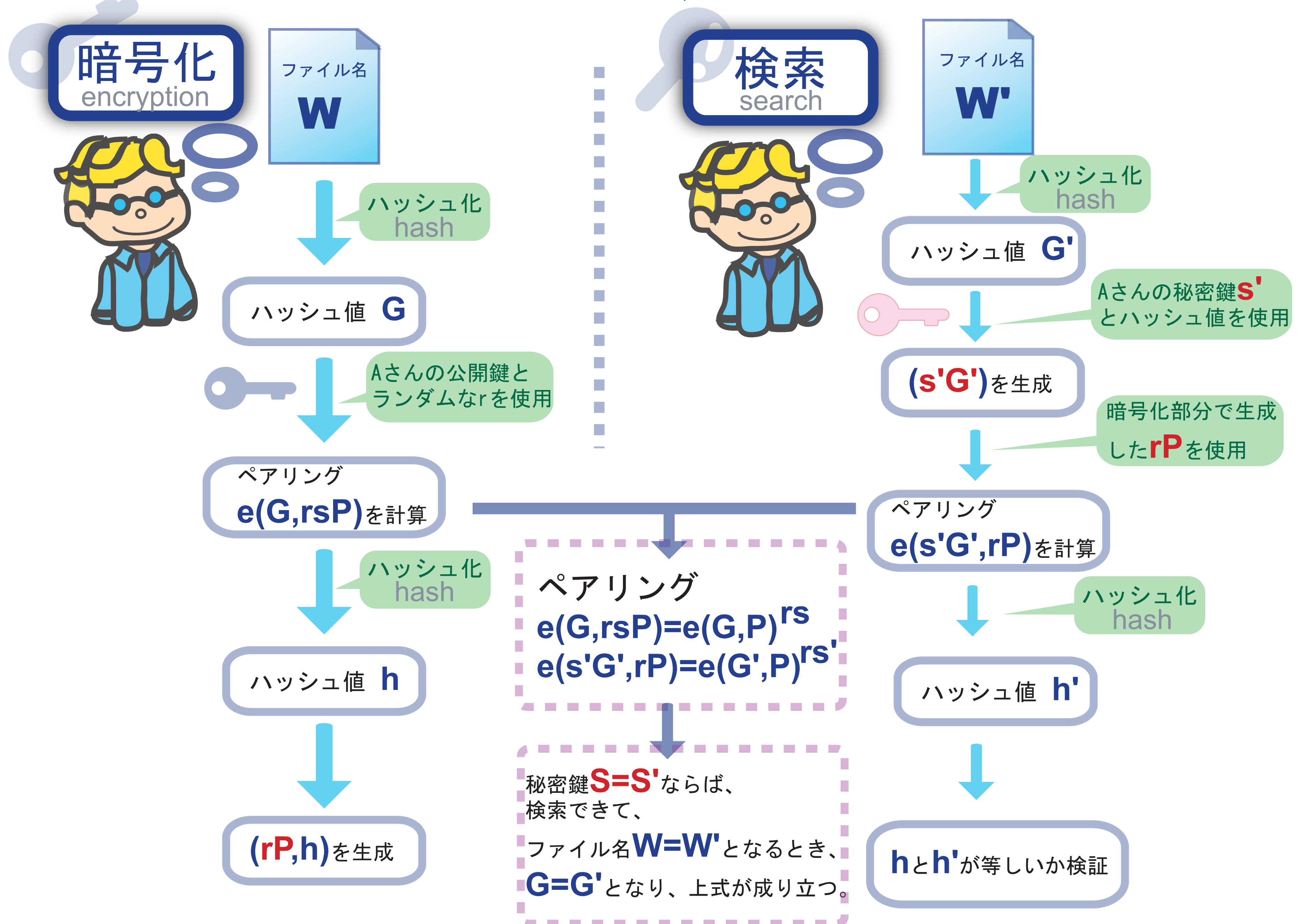
このアプリケーションは、暗号化されたファイル名を復号化せずに検索できるものである。つまり、復号化の時間を省けるという利点がある。また、アプリケーションがファイル名の検索を行うときは、秘密鍵を使用して検索する。つまり、秘密鍵を他人に知られない限り、他人は検索することができない。

keyword Search

手順

procedure

まずAさんは、自分の秘密鍵 s と公開鍵 (P,sP) を生成する。



keyword Search

検証の方法

How to the check

ペアリングは、双線形性という特性を持っている。この特性は、任意の x と y に対して $e(xg, yg) = e(g, xyg)$ となることである。その結果、ハッシュ値の g と g' が等しければ、上の等式が成り立つということになる。このとき、暗号化されたファイル名と検索のファイル名が一致するということになる。ここでは、ペアリングをハッシュ化して、ハッシュ値 h と h' を求めている。この場合、 h と h' が等しければ、暗号化されたファイル名と検索のファイル名が一致しているということになる。