3つのひかり　未来をつくる
広島市立大学
Hiroshima City University

【　IoT 環境に適したハッシュ連鎖による認証　】

【　研究キーワード：　セキュリティ、認証、IoT、ハッシュ関数、ハッシュ連鎖　】

情報科学部・システム工学科　　准教授　双紙　正和　Masakazu Soshi

研究シーズの概要

本研究では，ハッシュ連鎖の新しい構成法（ハッシュ連鎖アグリゲーション）を提案し，柔軟で効率の良い認証を実現します。特に本研究で実現する認証は、効率がよく、IoT 環境（計算機リソースが乏しくデジタル署名が困難な環境を想定）における相互認証に適しています。

研究シーズの詳細

◆研究例◆

ハッシュ関数は，一方向性を持ち，効率よく計算できる関数で、量子コンピュータに対しても安全ということから注目されています．さらに，ハッシュ関数を繰り返し適用した，ハッシュ連鎖と呼ばれる技術があります．本研究では，ハッシュ連鎖の新しい構成法（ハッシュ連鎖アグリゲーション）を提案し，柔軟で効率の良い認証を実現できることを示しました（図 1 参照）。

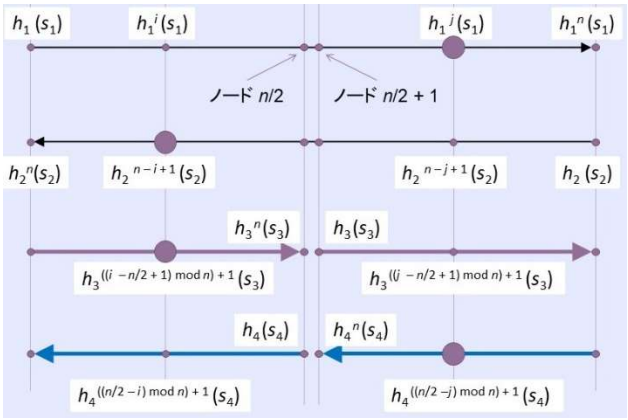

図 1．ハッシュ連鎖アグリゲーション（n = 4）

◆研究例◆

ここで、図 1 では、h_1, h_2, h_3, h_4 はそれぞれハッシュ関数、s_1, s_2, s_3, s_4 はそれぞれハッシュ連鎖の種を表します。そして、n = 4 のハッシュ連鎖アグリゲーションでは、i 番目のハッシュ値を、$h_1^{\,i}(s_1)$, $h_2^{\,n-i+1}(s_2)$, $h_3^{\,((i-[n/2]-1) \bmod n)+1}(s_3)$, $h_4^{\,(([n/2]-i) \bmod n)+1}(s_4)$ とすることができます（一般の n では、より複雑な構成となります）。こうして、図 1 では 4 方向のハッシュ連鎖を構成できます。一方、ワンタイムパスワードなどの従来のハッシュ連鎖は、一方向のみしか考えられませんでした。

本研究で提案するハッシュ連鎖アグリゲーションの大きな利点は、デジタル署名を使わず、ハッシュ関数のみを使って、相互認証を実現しているという点です。そこで効率よく計算を行うことができ、IoT 環境（計算機リソースが乏しくデジタル署名が困難な環境を想定）における相互認証を実現するのに適しています。

想定される用途・応用例

- ◆ IoT 環境（計算機リソースが乏しくデジタル署名が困難な環境を想定）における相互認証
- ◆ キーエスクロー（政府や裁判所が認めた場合、ユーザの鍵を強制的に公開する）の実現
- ◆ 一般に、さまざまなユーザグループの相互認証やワンタイムパスワード

セールスポイント

本研究は、以下の国際会議で発表されました：

Y. Kurihara and M. Soshi. “A Novel Hash Chain Construction for Simple and Efficient Authentication.” In 14th Annual Conference on Privacy, Security and Trust, PST 2016, December 2016.

問い合わせ先：広島市立大学　社会連携センター　　〒731-3194
TEL:082-830-1764　FAX:082-830-1555　　広島市安佐南区大塚東三丁目４番１号
E-mail:office-shakai@m.hiroshima-cu.ac.jp　　（情報科学部棟別館１F）