

情報通信研究機構

NICT 先端研究

⑥2

TYPE OF
INDUSTRY

科学技術・大学

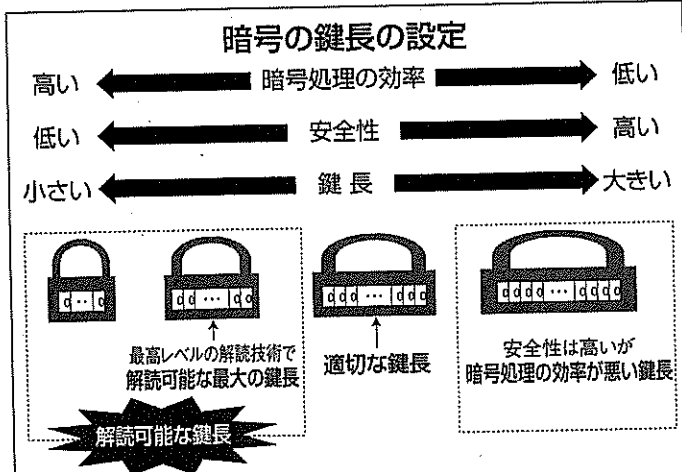
ウェブページのURL
Lでよく見かけるht
tp、しかし、例えば
カード決済をする場合
のURLを見るとht
tpsになっているこ
とに気付く。このsは
secure(安全)
を意味しており、実は

自動的に公開鍵暗号等
の暗号技術が使用さ
れ、クレジットカード
の番号等を安全に送
信できるようになって
いる。このように暗
号技術は我々にとつ
て身近で重要な技
術である。公開鍵暗
号の鍵長を大きくす
ると、暗号の解読に
かかる時間が膨大な
時間がかかりすぎる
ことになる。鍵長を
小さくすると、暗号
の解読が容易になり
安全性が低下する。
鍵長の設定は、安全
性と効率性の両方を
満たす必要がある。
鍵長の設定は、安全
性と効率性の両方を
満たす必要がある。

鍵長暗号の安全・効率担保

サイバーセキュリティ研究所・
セキュリティ基盤研究室主任研究員
篠原 直行

09年より現職。公開鍵暗号の安全性評価に関する研究に従事。専門は
計算数論・計算代数。博士(数理学)。



暗号の鍵長の設定

近年では、九州大
学、富士通研究所と共
同でペアリング暗号の
解読で世界記録を達成
した。また、東京大
学、九州大学と共同で
格子暗号について世界
記録を更新している。
これらの暗号は現在広
く使われている公開鍵
暗号方式と比べて、新
しい機能を持つこと
や、量子コンピュータ
でも解読が難しい等
の特徴を持つため、未
来の暗号方式の候補と
して研究が進められて
いる。

(火曜日に掲載)