Copyright ©2022 The Institute of Electronics,
Information and Communication Engineers

SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

暗号のための脳機能拡張：信用できる計算機が不要な署名方式の提案

Brain function extension for cryptography : How to realize digital signature without trustworthy terminal

松本 彩花 * 尾形 わかは * 高橋 健太 † 西垣 正勝 ‡
Ayaka Matsumoto Wakaha Ogata Kenta Takahashi Masakatsu Nishigaki

キーワード 信用できない計算機，マルウェア，署名方式，CAPTCHA

現代の暗号技術の利用には，秘密情報の安全な管理と，ユーザの意思を正しく反映した計算の実行が必須である．しかし近年では，man-in-the browser やキーロガーなどのマルウェアによって，端末の全ての入出力情報が攻撃者に漏れたり情報が改ざんされるなど，端末が信用できない場面が増えている．また，サーバが攻撃されて秘密情報が流出する事件もある．このため，完全に信用できる計算機は存在しないという状況設定で安全性を確保できる方法を検討することが大切である [1]．本論文では，通信において重要な役割を担うデジタル署名について，全ての計算機が信用できなくても安全な署名方式，計算機援用脳内署名方式を提案する．

この方式では，計算機は全て信用できないとし，信用できるのは人間の脳のみとする．この設定で要件は２つある．まず，１つ目の要件は署名鍵の安全な管理である．署名鍵は計算機で管理するのが一般的であるが，マルウェアに署名機能を悪用されてしまう可能性がある．そこで本研究では計算機に署名鍵を保存せず，人間の脳に署名鍵の元となるパスワードを保存することにする．人間は何らかの覚えやすいが十分なエントロピーをもつパスワードを記憶できると仮定する．

２つ目の要件は署名生成のユーザの意思を正しく反映した計算である．パスワードから署名鍵を出力する計算，署名鍵を用いて署名を出力する計算などは一般的には信用できる端末で行うが，今回の設定では信用できる端末が存在しない．また，人間の脳では簡単な計算はできるが，高度な計算はできない．このため，高度な計算は委託計算サーバに委託せざるを得ないが，サーバも一時的に攻撃者によって支配される可能性があり，完全には信用できない．これに対処するために，提案方式では複数のサーバによるしきい値署名を利用する．また，署名の委託のたびに秘密鍵の元となるパスワードを委託計算サーバに送ることで，委託計算を実行する時以外にはサーバが秘密情報を保管しないようにする．

ここで必要になるのは，信用できない端末を用いてパスワードをサーバへ届ける方法である．本論文では，パスワード送信方法が異なる３つの計算機援用脳内署名方式を提案する．１つはマルウェアが結託していない２つの端末を用いることで，能動的な攻撃者に対する安全性を実現している．他の２つは，CAPTCHA[2] を利用することで複数の端末を不要とする方式であり，CAPTCHA に適切な安全性を仮定することで，受動的な攻撃者に対する安全性を証明することができる．この２つの方式は CAPTCHA に求められる安全性が異なり，CAPTCHA の実現性と方式の効率がトレードオフである．

参考文献

[1] 向平浩貴，神農泰圭，土屋貴史，大木 哲史，高橋健太，尾形わかは，西垣正勝，“Man-In-The-Browser 攻撃対策を実現する人間・銀行サーバ間のセキュア通信プロトコル,” 研究報告マルチメディア通信と分散処理，pp.1–7，2017

[2] Luis von Ahn，Manuel Blum，Nicholas J. Hopper，John Langford，“CAPTCHA: Using Hard AI Problems for Security,” EUROCRYPT，pp.294–311，2003

* 東京工業大学，〒 152-8550，東京都目黒区大岡山 2-12-1，Tokyo Institute of Technology, 2-12-1 Ookayama, Meguro-ku, Tokyo 152-8550 Japan
† (株) 日立製作所　研究開発グループ，〒 244-0817，神奈川県横浜市戸塚区吉田町 292 番地，Hitachi Ltd., 292 Yoshidacho Totsuka-ku, Yokohama-shi, Kanagawa 244-0817 Japan
‡ 静岡大学，〒 432-8011，静岡県浜松市中区城北 3-5-1， Shizuoka University, 3-5-1 Johoku Naka-ku, Hamamatsu-shi, Shizuoka 432-8011 Japan