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

究極の本人確認のための3層構造公開鍵暗号の提案–第3報
3 Layer Public Key Cryptosystem for Ultimate Personal Identification–Rep. No.3

辻井 重男 * 吉田　昇 † 佐々木 浩二 ‡ 鈴木 伸治 ‡
Shigeo TSUJII Noboru YOSHIDA Koji SASAKI Nobuharu SUZUKI
才所 敏明 * 山澤 昌夫 * 五太子政史 * 四方 光 §
Toshiaki SAISHO Masao YAMASAWA Masahito GOTAISHI Ko SHIKATA
橋谷田　真樹 ¶
Masaki HASHIYADA

キーワード 本人確認，個人情報，プライバシー，マイナンバ，STR (Short Tandem Repeat)，DNA，公開鍵暗号，秘密鍵，ゼロ知識証明，Schnorr 認証

あらまし

DX 環境が広がる中で，公開鍵暗号の秘密鍵が人・モノの真正性証明に果たす基盤的役割が拡大している．本文は，秘密鍵が紛失・盗難されても，盗用されないシステム構成・運用方式を提案する．筆者らは，21 世紀初頭以来，究極的本人確認の為のデジタル情報である STR(Short Tandem Repeat) を秘密鍵の中に内蔵させる 3 階層公開鍵暗号を提案してきた．STR は，何兆人に 1 人でも同定可能で（1 卵生双生児を除いて）[2]，かつ，プライバシー情報を一切含まない個人情報であり，理想的な同定情報であるが，経費・同定時間の面での課題が残る．他方，現在，国策としてマイナンバーの普及が進められている．そこで，STR の導入については今後も検討を続けるとして，本文では，マイナンバー・乱数を極秘密鍵とする 3 階層公開鍵暗号を利用し，マイナンバーカードとスマートフォン等の連携的活用により，盗難者による盗用に対する安全性を高める構成を提案する．

本研究は，個人同定が完全な STR-DNA を秘密鍵に内蔵させる公開鍵暗号の研究から開始し，将来，マイナンバーカードに STR-DNA を埋め込むことも提唱したが [1]，[3]，今後，広い視野から考察を深める予定である．

運用形態は，利用者の環境に応じて多様であるが，今後，より具体的な形態について考察を進めたい．

* 学校法人中央大学研究開発機構, 〒 112–8551 東京都文京区春日 1–13–27, Faculty of Engineering, Research and Development Initiative, Chuo University, 1–13–27 Kasuga, Bunkyo-ku, Tokyo, 112–8551 Japan
† 株式会社 SRA ホールディングス, 〒 171-0022 東京都豊島区南池袋 2-32-8, SRA Holdings, Inc., 2–32–8 Minami-Ikebukuro, Toshima-ku, Tokyo 171–0022 Japan
‡ 株式会社アドイン研究所, 〒 102–0094 東京都千代田区紀尾井町 3 番地 6 紀尾井町パークビル 8 階， AdIn Research, Inc., 3–6 Kioicho, Chiyoda-ku, Tokyo, 102–0094 Japan
§ 学校法人中央大学法学部, 〒 192–0393 東京都八王子市東中野 742–1， Faculty of Law, Chuo University, 742-1 Higashinakano Hachioji-shi, Tokyo 192-0393 Japan
¶ 関西医科大学 法医学講座, 〒 573-1010 枚方市新町 2 丁目 5 番 1 号, Forensic Genetics,Faculty of Medicine,Kansai Medical University, 2–5–1 Shin-machi, Hirakata City, Osaka 573–1010 Japan

参考文献

[1] 辻井重男，他，“究極の本人確認のための 3 層型公開鍵暗号の提案–マイナンバー・STR の秘密鍵への埋め込みとその利用に向けて–,” 信学技報 IEICE Technical Report ISEC2019–52,SITE2019–46,BioX2019–44, HWS2019–47,ICSS2019-50,EMM2019–55(2019–07)，pp.341–346.

[2] 板倉征男，“個人識別用 DNA 情報の統計的検証,” 情報処理学会, CSS-2000 シンポジウム, Oct.2000 , pp.121–126 , 2000.

[3] 辻井重男，他，“究極の本人確認のための 3 層型公開鍵暗号の提案–マイナンバー・STR の秘密鍵への埋め込みとその利用に向けて–第 2 報,” 電子情報通信学会 SCIS2020.