人間計算可能なパスワード認証の現状と課題：AI 複雑性の観点から

櫻井　幸一 [1]

概要：Blum らは、人間が記憶可能であり、自身で計算できる新しいパスワード方式を提案した[Manuel Blum, Santosh S. Vempala: The Complexity of Human Computation: A Concrete Model with an Application to Passwords. (2017)] .本稿ではその概要と現状と課題を論じる。Blum らの安全性評価は、SAT-solver を利用する組み合わせ計算論的解析であった。これに対し、発表者の研究グループは、深層学習的な手法の安全性評価を行った[I. Murata et al. Towards Evaluating the Security of Human Computable Passwords using Neural Networks. WISA2022]ので、この概要も紹介する。

キーワード：パスワード認証　深層学習　人間計算可能

An　Approach to Security Evaluation of Human Computable Password Authentication from the Point of View of AI Complexity

Kouichi SAKURAI [1]

Abstract: M. Blum et al. proposed a new password scheme that humans can memorize and compute by human themselves. [Manuel Blum, Santosh S. Vempala : The Complexity of Human Computation: A Concrete Model with an Application to Passwords. (2017)] .This paper discusses its outline, current status, and issues. The securtity evaluation by Blum et al. is a combinatorial computational analysis utilizing the SAT-solver. On the other hand, the presenter's research group conducted another security evaluation with a deep learning method [I, Murata et al. Towards Evaluating the Security of Human Computable Passwords using Neural Networks. WISA2022], so we will also introduce this overview.

Keywords: Password, Authentication, Deep Learning, Human Computable

1. はじめに

典型的なパスワード認証では PIN 番号や文字記号列を使うが、人間が覚えやすいパスワードは辞書式攻撃の対して脆弱という弱点がある。、この対策として、自動ソフトや専用デバイスが生成する乱数パスワードがある。これは、人間が覚えるというよりも、使い切りワンタイム用で、実際には、利用者自身では覚えにくい場合が多い。

そこで Blum らは、人間自身で計算できるパスワード方式で、可能な限り安全な方式の設計を研究している[Blum]。ここでは、ある秘密のパスワードを利用者が記憶し、その記憶をもとに、相手からの質問(チャレンジ)に、利用者自身で答えることでユーザー認証を可能にする。特に、この質問に答える際の計算が、利用者自信で、計算機に頼らすに、暗算のみのため、人間計算可能なパスワードと呼ばれる。

Blum らの具体的な提案方式は、次の通りである。(1) まずユーザーは事前に複数の画像から数字群への対応表を記憶する。(2) 次にサーバー（機械）は、ユーザーが記憶した画像群からランダムに選択した数枚の画像を、ユーザーに与える。(3)ユーザーは、受け取った複数の画像を、ユーザーが記憶している対応表に従い、数字の列に変換する。(4)さらに、ユーザーはこの数列をもとに、サーバーと事前に共有している“人間計算可能な”関数に従って暗算することでパスワードとしての入力得る。

サーバーとユーザーとは、画像群と、“人間計算可能な”関数とを事前に共有し、上記の手順に従い、この画像のようにユーザーが計算に必要なものを、サーバーからのチャレンジとし、ユーザーは、その答えを応答（レスポンス）とする。

特に Blum らが導入した関数の具体例は、次である：

$$f(x0, x1, x2, x3, x4, x5, \ldots, x13) = x13 + x12 + x(x10+x11 \bmod 10) \bmod 10 .$$

ここでは、画像群から選ばれた 14 枚の各画像に、ユーザーは自身が記憶していた 0 から 9 までの数値を割り当て、関数 f

1 九州大学 Kyushu University University
sakurai@inf.kyushu-u.ac.jp

を、暗算で計算する。3つの xi の法 10 の下での和演算であるが、3つ目の x の添字 x10＋x11 mod 10 に注意する。

Blum らは、提案方式の安全性として、制約充足性問題 (Constraint Satisfaction Problem, CSP) の解法機 CSP-solver による組み合わせ論的な議論により、チャレンジと応答のペアと関数情報から、画像から数字への対応を解読する困難性を解析している。彼らの結論では、事前に記憶する画像が 50 枚以下であれば、解読可能であると評価している。この既存研究では解読者が、人間計算可能な関数を既知と仮定していることに注意する。

これに対し、村田ら[WISA]は、実際の通信路盗聴者である攻撃者が、関数まで既知することは、強すぎる仮定であり、最近の人工知能は多くの関数の近似が可能であることに着眼した。そこでは、攻撃者は、たとえ関数も未知の状態でも、人工知能的手法と計算機を利用した解析を行うと仮定することが現実的であると設定した。村田らは、多層パーセプトロンを用い、画像から数値への対応変換と暗算に用いる関数との合成関数の出力が、AI でも予測可能であるか否かについて実験的解析を行った。結果として、予測精度は 10 %前後であった。彼らは、さらに、関数を Blum らの非線形から、単純な

$$g(x_0, x_1, \cdots, x_{13}) = x_2 + x_{12} + x_{13} \mod 10$$

に変更した場合での実験も行なった結果、予測精度が 80%に向上したという。これらの実験結果より、関数の計算複雑性が、認証方式に与える効果を、深層学習による評価で明らかにできたと、村田らは主張している。

Blum の人間計算可能な関数の暗号認証への応用は、その後いくつかの研究で展開されている[12,13,14]。

その一方で Blum 自身は、パスワード応用に限らずに、人間計算可能性を追求し続けている[3]。村田らの結果は、人間計算可能であるが、人工知能(AI では予測困難な関数の存在かを明らかにしたとも言える。 発表では、Blum らの人間計算可能性に加えて、計算問題に対する AI 複雑性の研究方向も議論する。

謝辞 本研究は、認証に関してはテレコム先端技術研究支援センター(SCAT)の助成を、人工知能応用に関しては電気通信普及財団(TAF)の支援を受けている。また、本研究の一部は DST-JSPS 日印２ヶ国間共同研究の一環である。

参考文献

[1] I. Murata, P. He, Y.Gu and K.Sakurai: Towards Evaluating the Security of Human Computable Passwords using Neural Networks WISA2022

[2] 村田壱生　人間計算可能なパスワード認証に対する深層学習による安全性評価　火の国シンポジウム 2022

[3] Manuel Blum, Lenore Blum:A Theoretical Computer Science Perspective on Consciousness. J. Artif. Intell. Conscious. 8(1): 1-42 (2021) also from CoRR abs/2011.09850 (2020)

[4] Manuel Blum, Santosh S. Vempala: The complexity of human computation via a concrete model with an application to passwords. Proc. Natl. Acad. Sci. USA 117(17): 9208-9215 (2020) also from CoRR abs/1707.01204 (2017)

[5] Elan Rosenfeld, Santosh S. Vempala, Manuel Blum: Human-Usable Password Schemas: Beyond Information-Theoretic Security. CoRR abs/1906.00029 (2019)

[6] Jeremiah Blocki, Manuel Blum, Anupam Datta, Santosh S. Vempala: Towards Human Computable Passwords. ITCS 2017: 10:1-10:47

[7] Manuel Blum: Cybernetics: A mathematician of mind. Nat. 538(7623): 39-40 (2016)

[8] Manuel Blum, Santosh Srinivas Vempala: Publishable Humanly Usable Secure Password Creation Schemas. HCOMP 2015: 32-41

[9] Jeremiah Blocki, Manuel Blum, Anupam Datta: Naturally Rehearsing Passwords. ASIACRYPT (2) 2013: 361-380. Also from CoRR abs/1302.5122 (2013). A minor revision from IACR Cryptol. ePrint Arch. 2015: 166 (2015)

[10] Jeremiah Blocki, Manuel Blum, Anupam Datta: GOTCHA password hackers! AISec 2013: 25-34. Also from CoRR abs/1310.1137 (2013)

[11] Luis von Ahn, Manuel Blum, John Langford: Telling humans and computers apart automatically. Commun. ACM 47(2): 56-60 (2004)

[12] Luis von Ahn, Manuel Blum, Nicholas J. Hopper, John Langford: CAPTCHA: Using Hard AI Problems for Security. EUROCRYPT 2003: 294-311

[13] Nicholas J. Hopper, Manuel Blum: Secure Human Identification Protocols. ASIACRYPT 2001: 52-66

[12] Ruthu Hulikal Rooparaghunath, T. S. Harikrishnan & Debayan Gupta Trenchcoat: Human-Computable Hashing Algorithms for Password Generation, CANS2020.

[13] Sławomir Matelski: Human-Computable OTP Generator as an Alternative of the Two-Factor Authentication, EICC '22: Proc. of the 2022 European Interdisciplinary Cybersecurity Conference (June 2022).

[14] Samadi, Samira: Human aspects of machine learning Georgia Tech Theses and Dissertations [23403] (2020 April)

付録（はありません）

【 この位置に改ページを入れ, 以降のページを印刷対象外とする 】