

検証柔軟型電子署名(その2)

櫻井幸一¹

概要: 検証に確率性を導入し、検証者が、計算効率対検証信頼度効果を柔軟に制御できる電子署名を論じる。さらに一般的な構成法と確率検査証明の理論との関係も論じる。

キーワード: 電子署名, 乱択アルゴリズム, 確率検査証明, Fiat-Shamir 法, Merkle 木,

Digital Signature with Flexible Verification: Revisited

Kouichi SAKURAI¹

Abstract: We introduce a probabilistic approach to the verification of a digital signature, which allows a verifier to flexibly control the computation efficiency versus verification reliability effect. We also discuss the relationship between generic construction methods and the theory of probability check proofs.

Keywords: Digital Signature, Probabilistic algorithms, PCP-theory, Fiat-Shamir, Merkle-tree

1. はじめに

暗号に乱数は重要な役割を演じる。原始 RSA 署名は、署名生成も検証も、決定性アルゴリズムであるが、ECDSA やその原型である ElGamal 署名は、乱数を利用した生成アルゴリズムで、原始 RSA の欠点を補っている。電子署名への乱数アルゴリズムの適用は、署名生成段階のみ、1980 年代の電子署名で、検証に乱数を利用したものは、筆者が知る限り知られていなかった。

PCP 定理[AS'92]により、NP 型の検証（つまり乱数を利用しない決定性）は、乱数を利用した確率検査型に変換できる。従って、RSA や ElGamal の検証も、適当な変換により、確率型で可能と言える。しかし、適当な変換が効率的でない限り実用的ではない。この時期に筆者が考えたのは

挑戦課題：実用的な確率検証型の電子署名を設計せよ。
筆者[Sa'93]は、それまで決定性の Fiat-Shamir 署名の検証を、その元となる Fiat-Shamir 認証プロトコルの着目し、確率検証型署名の一実現例を与えた。2018 年になって、V.Le ら[LKK'18]が同じ研究動機に基づき、確率検証署名を提案した。ただし、L.Le らは、Lamport-Diffie one-time signature と Merkle authentication tree とを利用する。

2. 乱数検証型電子署名: Naor 変換

電子署名の検証に乱数を利用する一つ方式には、Naor 変換がある[CFH+07,FGH+17]。Shamir[Sha'84]が提起し、境ら[SOK'00]や Boneh-Franklin[BF'01]によって開拓された ID ベ

ース暗号から、電子署名を構成する一般的な変換である。ただし、ここでの乱数の利用は、PCP 理論とは関係ない。また、Freitag ら[FGH+17]は、Naor 変換の非乱数化までも論じている。

3. 乱択検証アルゴリズム

行列の積演算の効率化と限界解明において演算量 $O(n^2)$ がよく知られているが、3 つの行列 (A, B, C) が $AB=C$ を満たすかどうかは乱数ベクトル r を利用し $ABr=?Cr$ と、次元を下げた計算量で可能であることは乱択検証アルゴリズムの基本である。

4. 柔軟検証型署名: Merkle 認証応用

V.Le ら[LKK'18]は、Lamport-Diffie のワンタイム署名と Merkle 木の応用で、柔軟検証が可能な電子署名の構成に成功している。これは、筆者が提起した挑戦課題への解の 1 つとなっている。また、V.Le らは、他の Merkle 木型署名への適用や Fiat-Shamir 型署名の縦貫検証性も議論している。

5. 最後に: 今後の課題

V.Le らが明示的に検討課題としているのが、GPV 法[GPV'08]をはじめとする Lattice 署名の検証柔軟化である。検証が行列演算となっている署名系には、行列積に対する乱択検証技法が適用できることに留意する。特に耐量子系電子署名では、署名や公開鍵のサイズが大きい場合、乱択行列積検算による効率化が期待できる。

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

謝辞 太田和夫先生（電気通信大学名誉教授）からは、1991-1992 年当時、客員研究員として MIT 滞在中に、PCP 理論の最新情報と、下名の質問に丁寧な回答とをいただきました。ここに感謝します。

参考文献

- [AS'92] S.Arora and S. Safra “Probabilistic checking of proofs: a new characterization of NP” FOCS 1992
- [Sa'93] 櫻井幸一 “Digital Signatures with User-Flexible Reliability” Proc. SCIS1993
- [Sha'84] A.Shamir, “ID-based Cryptosystems and signature schemes” CRYPT'84.
- [SOK'00] R.Sakai, K.Ohgishi, and M.Kashara, “Cryptosystem based on Paring” Proc.SCIS2000.
- [BF'01] D. Boneh and M. K. Franklin. “Identity-based encryption from the Weil pairing,” CRYPTO 2001.
- [FGH+'17] C. Freitag, R. Goyal, S. Hohenberger, V. Koppula, E. Lee, T. Okamoto, J. Tran, and B. Waters “Signature schemes with randomized verification,” SCNS'17
- [CFH+'07] Y. Cui, E. Fujisaki, G. Hanaoka, H. Imai, and R. Zhang, “Formal Security Treatments for IBE-to-Signature Transformation: Relations among Security Notions”. ProvSec 2007
- [BKP'14] O. Blazy and E. Kiltz and J. Pan “(Hierarchical) Identity-Based Encryption from Affine Message Authentication” CRYPTO2014
- [DKPW'12] Y. Dodis, E. Kiltz, K. Pietrzak, and D. Wichs. “Message authentication, revisited.” EUROCRYPT 2012,
- [BM'89]M. Bellare and S. Goldwasser “New paradigms for digital signatures and message authentication based on non-interactive zero knowledge proofs” CRYPTO'89.
- [Lam'79] L. Lamport, “Constructing digital signatures from a one way function” SRI intl. CSL-98 (1979)
- [LKK'18] D.V. Le, M.Kelkar, and A. Kate “Flexible signatures: Towards making authentication suitable for real-time environments,” Cryptology ePrint Archive, Report 2018/343 (2018) Also in ESORICS'19(2019).
- [Mer'89] R.C. Merkle, “A certified digital signature,” CRYPTO 1989.
- [GPV'08] C. Gentry, C.Peikert, V.Vaikuntanathan, “Trapdoors for hard lattices and new cryptographic constructions,” STOC 2008
- [Sch'80] J.T Schwartz. “Fast probabilistic algorithms for verification of polynomial identities,” Journal of the ACM, 27(4) 1980.
- [MR'] R.Motowani and P.Raghavan “Randomized Algorithms” Cambridge Univ. Press (1995)