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

PMAC*r*x：ベクトル入力をサポートする高安全なメッセージ認証コード
PMAC*r*x: Highly Secure Message Authentication Code Supporting Vectorized Input

笠原 颯登 * 岩田 哲 *
Hayato Kasahara Tetsu Iwata

キーワード 共通鍵暗号，tweakable ブロック暗号，認証暗号，MAC，PMAC*r*x，証明可能安全性

あらまし

Rogaway と Shrimpton はベクトル入力をサポートする認証暗号方式 SIV を提案した [3]．この方式では，S2V と呼ばれるベクトル入力をサポートするメッセージ認証コード（MAC）を構成要素として用いる．一方，List と Nandi は tweakable ブロック暗号を用いた MAC である PMAC2x を構成し，ブロック長 n ビットに対して $O(2^n)$ 回の計算量の攻撃に対し安全である，beyond-birthday-bound の安全性を示した [1]．また，これを利用した認証暗号方式である SIVx を提案した．しかし，峯松と岩田により PMAC2x と SIVx は $O(2^{n/2})$ 回の計算量で攻撃が可能であることが示された [2]．これに対し List と Nandi は，PMAC2x と SIVx を修正した方式を提案した．文献 [1] にある PMAC2x，およびその修正版は単一のビット列を入力とする MAC として定義されており，S2V のようにベクトル入力をサポートしてはいない．

本稿では，PMAC2x に基づき，データベースにおける複数の入力データの同時認証を目的とし，ベクトル入力をサポートする MAC として PMAC*r*x を提案する．PMAC*r*x は長さ r のベクトル $M = (M^1, \ldots, M^r)$ を入力とし，$2n$ ビットの出力を返す．各 M^j をレコードと呼び，r をレコード数と呼ぶ．PMAC*r*x では，各 M^j を PMAC2x で用いるハッシュ関数 H_K を用いて $2n$ ビットの出力 (X^j, Y^j) を生成し，これらを図 1 のように組み合わせて $2n$ ビットの出力 (U, L) を得る．

本稿では q 回のクエリを行う任意の敵に対し，PMAC*r*x の擬似ランダム関数としての識別利得が $O(q^2/2^{2n})$ であることを証明する．ただし，入力 $M = (M^1, \ldots, M^r)$ に対し，各レコード M^j のブロック数を m^j とすると，PMAC*r*x ではレコード数 r と最大ブロック数 $m_{\max} = \max\{m^1, \ldots, m^r\}$ の間にはトレードオフの関係がある．本稿では $(r, m_{\max})$ の最大値の組み合わせの例を示す．

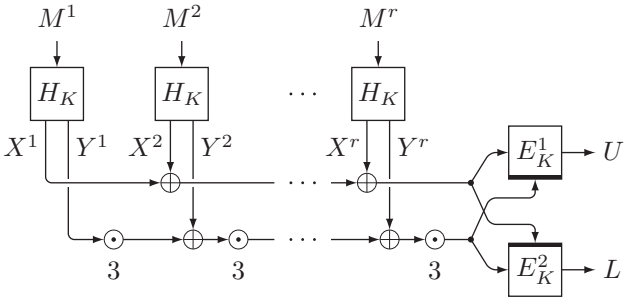

図 1: PMAC*r*x の動作概要.

謝辞

本研究は JSPS 科研費 JP20K11675 の助成を受けたものです.

参考文献

[1] E. List and M. Nandi. Revisiting full-prf-secure PMAC and using it for beyond-birthday authenticated encryption. In *CT-RSA 2017*.

[2] K. Minematsu and T. Iwata. Cryptanalysis of PMACx, PMAC2x, and SIVx. *IACR Trans. Symmetric Cryptol.*, 2017(2):162–176, 2017.

[3] P. Rogaway and T. Shrimpton. A provable-security treatment of the key-wrap problem. In *EUROCRYPT 2006*.

* 名古屋大学大学院工学研究科 〒 464-8603 名古屋市千種区不老町. Nagoya University, Furo-cho, Chikusa-ku, Nagoya 464-8603, Japan. kasahara.hayato@a.mbox.nagoya-u.ac.jp, tetsu.iwata@nagoya-u.jp