

ランポート署名

Hirotsugu Seike

2026年2月16日

1 導入

ランポート署名 (Lamport signature) は、一方向性関数を用いて構成されるデジタル署名方式であり、1979年に L. Lamport により提案された [1]。一般には暗号学的ハッシュ関数を用いて実装される。また、量子計算機に対しても安全性を保てると期待されている。ランポート署名では、1つの鍵は1回の署名にしか使用できない。One-time signature である。

2 ランポート署名の形式化

2.1 記法

- k : メッセージ長 (ビット長. 任意長のメッセージは一方向性関数で k ビットにする)
- f : 一方向性関数 (通常は暗号学的ハッシュ関数)
- $m = (m_1, m_2, \dots, m_k) \in \{0, 1\}^k$: メッセージ

2.2 鍵生成

署名者は、ランダムに以下の値を生成する:

$$(y_{1,0}, y_{2,0}, \dots, y_{k,0}), \quad (1)$$

$$(y_{1,1}, y_{2,1}, \dots, y_{k,1}). \quad (2)$$

これらに一方向関数 f を適用して

$$z_{i,0} = f(y_{i,0}), \quad z_{i,1} = f(y_{i,1}). \quad (3)$$

を計算する。秘密鍵、公開鍵は $2k$ 個の値であり、この値の候補空間はランポート署名の安全性のために、十分に大きくする。秘密鍵はシード値から計算される暗号学的に安全な疑似乱数列、公開鍵は暗号学的ハッシュ関数により圧縮可能である。

- 秘密鍵:

$$(y_{1,0}, \dots, y_{k,0}, y_{1,1}, \dots, y_{k,1}).$$

- 公開鍵:

$$(z_{1,0}, \dots, z_{k,0}, z_{1,1}, \dots, z_{k,1}).$$

2.3 署名生成

メッセージ $m = (m_1, \dots, m_k)$ に対して,

$$\text{sig}(m) = (y_{1,m_1}, y_{2,m_2}, \dots, y_{k,m_k}) \equiv (s_1, s_2, \dots, s_k). \quad (4)$$

を署名とする. すなわち, 各ビット m_i に対して, 以下を署名の値として採用する.

- $m_i = 0$ の場合: $y_{i,0}$,
- $m_i = 1$ の場合: $y_{i,1}$.

2.4 署名検証

署名 (s_1, \dots, s_k) を受け取った検証者は, すべての i について

$$f(s_i) = z_{i,m_i}. \quad (5)$$

が成立するか確認する. すべて成立すれば, 署名を正当と認める.

参考文献

- [1] L. Lamport, "Constructing digital signatures from a one-way function," SRI International, Tech. Rep. CSL-98, Oct. 1979.

付録 A 特になし