中間値保存によるIncremental AEの拡張

Fast Incremental AE using storage of intermediate values

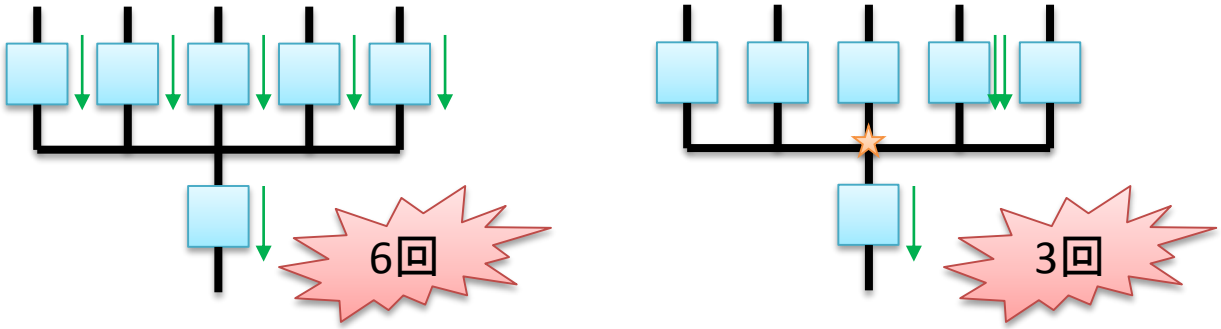
白仁友康・法政倫理分科会・中央大学大学院

局所的な時間の中では入力が変わらないことが多い

```
08 60 6e eb 6b 5b 00 a0  de c6 5e 37 08 00 45 00
00 34 3c 83 00 00 3e 06  b8 8d 85 5b 40 18 c0 a8
01 98 1f 92 cf d9 93 34  e8 af c2 f2 0b 9b 80 12
80 52 2d 23 00 00 02 04  05 b4 01 03 03 01 01 01
04 02
```

```
08 60 6e eb 6b 5b 00 a0  de c6 5e 37 08 00 45 00
00 34 44 c0 00 00 3e 06  b8 8d 85 5b 40 18 c0 a8
01 98 1f 92 c0 70 a7 47  96 05 ed a5 ab 4d 80 12
80 52 b0 bd 00 00 02 04  05 b4 01 03 03 01 01 01
04 02
```

無駄な計算が多いので、削減をする



- 現在行われている認証暗号コンテストに提案されているすべての認証暗号に対して計測
- 実際にパケットキャプチャツールでとった値（メッセージの長さや変化部分）を代入したところ、最大で70%以上の削減ができた
- 単位長あたりの関数の計算量が多い認証暗号の方が多ければ多いほど削減量が多いというわけでもなく、これといった相関性は見当たらなかった
- 数値の並べ替え次第ではもっと削減可能なので、そのようなTLS枠組みの模擬実装が今後の課題である