1. 研究分野

可逆計算，暗号化

2. 目的

秘密鍵暗号化アルゴリズムに特化した可逆言語Hermesの提案

3. 背景

可逆言語Janusで書かれた暗号化アルゴリズムがある．Janusで書かれた暗号化アルゴリズムは逆実行により復号ができるため，復号アルゴリズムを書く必要がない．加えて，変数が捨てられる前に値が0となるため，サイドチャネル攻撃で使われる情報をメモリ上に残さない．ただし，サイドチャネル攻撃では，変数の値だけが使われる訳ではない．暗号化の時間がデータと暗号化鍵に依存する場合，メッセージングによって攻撃者は値や暗号化鍵を簡単に得ることができる．Janusはタイミングが変数の値に依存する制御構造を持っているため，タイミングベースの攻撃に対して保護されていない．

4. アプローチ

暗号化に特化した可逆言語であるHermesを提案する．HermesはJanusの基本的な部分である状態の可逆更新，状態の交換，プロシージャを実行と逆実行できることは同じであり，可逆性とタイミング攻撃への耐性が保証される．

5. 結果

Hermesの構文と動作を定めた．また，実行時のテストによって，可逆性と情報のリークの耐性を示した．

6. 有用性

可逆性と情報のリークの耐性が保証されている．また，構文がCに似ているため，CプログラマはHermesのプログラムを読みやすいと考えられる．

7. 限界・短所

Cにコンパイルされて動作するため，Cに問題があった場合はHermesにも同様の問題が起こる．意味が厳密に定義されているわけではないため，証明が行いづらい．

8. 次に何を読めばいいか？