**概 要**

近年，使用されている暗号は大きく共通鍵暗号と公開鍵暗号に大別される．共通鍵暗号が暗号化と復号に同一の鍵を使用するのに対し，公開鍵暗号は暗号化と復号に異なる鍵（公開鍵と秘密鍵という）を使用する方式である．共通鍵暗号は鍵の秘匿が絶対条件であり，暗号通信に先立って送信者と受信者の間で如何に安全に鍵の交換を行うかという課題がある．一方，公開鍵暗号に比べ短い鍵長で良く，処理時間も早くなる特徴がある．公開鍵暗号は公開鍵と秘密鍵から構成され，公開鍵は一般に開示可能であるため，暗号通信に先立って送信者と受信者の間での鍵の交換が不要となる長所がある．一方，共通鍵暗号に比べ長い鍵長を必要とするため，処理時間が長い課題がある．このため，公開鍵暗号は暗号通信前の共通鍵の交換やディジタル署名などに主に利用され，共通鍵暗号は主に暗号通信に利用されている [**?**].

楕円曲線暗号は公開鍵暗号の 1 つであり，同じく公開鍵暗号で先行開発された RSA 暗号に比べ，小さい鍵長で同等の安全性を確保できるため，処理能力の小さいスマートカードなどの小型の組み込みデバイスを中心に普及が期待されている．楕円曲線暗号の更なる普及のためには，その暗号化処理の高速化が重要となり，活発に研究が行われている．

楕円曲線暗号の暗号化処理は，主にスカラー倍算と呼ばれる処理，すなわち，楕円曲線上のベースポイント $P$ に対して，$kP = P + \cdots + P(k$ 回) を計算する処理により構成される．また，スカラー倍算は，楕円曲線上における演算（加算，2 倍算等），有限体上の四則演算から構成され，これらの演算数を減らすことが必要になる．加算，2 倍算等を構成する有限体上の四則演算を減らす手法としては，座標系を変換 [**?**] したり，同一演算の再利用等の手法が提案されている．一方，前者の楕円曲線上における演算（加算，2 倍算等）数を減らすには，non-zero digit の密度を減らすことが重要になり，バイナリ法，NAF，$w$-NAF などの手法が提案されている．

DBNS(Double-Base Number System) は，スカラー $k$ を 2 つの整数（2 及び 3) のべき乗の和で表す表現手法で，non-zero digit の密度をバイナリ法，NAF，$w$-NAF に比べ，大幅に削減可能な特徴がある．例えば，160 ビットのスカラー $k$ に対し，バイナリ法，NAF がそれぞれ平均で 80 個，53 個の non-zero digit が出現するの対し，DBNS では 22 個の non-zero digit で表現可能である [**?**]．本研究では，DBNS を利用した既存研究に対し，DBNS 表現の導出方法に課題があることを示し，その解決手法の提案を行う．実験の結果，提案手法では，既存研究に比べ約 7 が可能であることを示した．また，スカラー $k$ から DBNS を導出する処理の効率化に取り組み，既存研究の $O(\log k)$ の手法に対し，$O(\log(\log k))$ の手法を提案した．