# Study on New E-cash Systems

広橋 浩司

北陸先端科学技術大学院大学 情報科学研究科

1999 年 2 月 15 日

**キーワード**: 電子マネー、オフライン、Schoenmakers ブラインド署名、部分ブラインド署名、メッセージ・リカバリー.

ネットワークを利用して買い物をする場合、支払もネットワーク経由で電子的に行えることが望まれている。加えて、暗号技術も飛躍的に向上してきたことにより、電子マネーシステムの構築は、理論的観点だけでなく、実用的な面でも重要な研究課題となった。このシステムの特徴は、電子データ化されたマネーをコンピュータネットワーク上で、リアルタイムに移動できる点にある。電子マネーシステムは主に次の 3 つプロトコルから成る。

- **引出プロトコル**: ある利用者が、銀行から電子マネーを引き出す。
- **支払プロトコル**: 利用者は、引き出したマネーを使って、店から何かを購入する。
- **決済プロトコル**: 店は、受け取ったマネーを銀行にある自分の口座に振り込む。

また、電子マネーシステムには、以下の 2 つの支払方法が存在する。

- **オンライン型支払方式**: 利用者が店で何かを買う時、店は、利用者から受け取る電子マネーが正当なものかどうかを確認するため、銀行に問い合わせる。もし、正当であれば、店は、そのまま自分の口座に振り込み、利用者に商品 (サービス) を提供する。つまり、支払と決済がオンラインで同時に行われる。
- **オフライン型支払方式**: 利用者が、店で何かを買うつもりで電子マネーを支払う時、店は、銀行に問い合わせなくても受け取ったマネーの正当性を確認することができる。受け取ったマネーは、後から銀行で決済すればよい。

しかし、オンライン型電子マネーシステムでは、店は銀行とオンラインで繋がっていなければ、利用者から受け取ったマネーが正当であるかどうかを検証できないので、通信コストやデータベースの維持にかかるコストなどを考慮すると、実用的でない。そのため、オフライン型電子マネーシステムは、このような実用的な観点からすると望ましい。今後は、オフライン型のみを考えることにする。

オフライン型電子マネーシステムは、次の性質も満たさなければならない。

- **完全情報化:** 電子マネーの安全性は、物理的条件に依存する必要がなく、マネーが完全に情報のみで自立して実現されている。つまり、ネットワークを通して、電子マネーを転送できる。
- **安全性:** 電子マネーのコピー、偽造などによる不正利用ができない。
- **匿名性:** 支払時における利用者のプライバシは守られなければならない。つまり、利用者の購入に関するプライバシの追跡は、不可能でなければならない。

Schoenmakers は、Schnorr 署名 [21] に基づいたブラインド署名を提案した [22]。この署名の特徴は、

- 署名者は、検証者毎に異なる秘密鍵を用いて署名する。

ものである。

一方、阿部・藤崎は、部分ブラインド署名の概念を発表した [1]。これは、

- 署名者は、メッセージの一部である検証者と署名者との共有情報を使って署名するので、署名の際、メッセージに含まれる情報が正しいことを保証できる。

が特徴である。さらに、阿部・Camenisch は、この性質を持つ Schnorr 型のブラインド署名を提案した [2]。

従来の電子マネーシステム [3,4,11,12,18,19,22] と異なり、宮崎・櫻井は、Schoenmakers ブラインド署名 [22] 及び部分ブラインド署名 [2] を用いた電子マネーシステムを発表した [14]。しかし、このシステムは、だれでも簡単に電子マネーを偽造できる。これは、たとえ、利用者が銀行の秘密鍵を知らなくても、マネーの正当性を確認するのに使用する検証式を満たすようなマネーを作ることができるためである。そこで、我々は、この問題を解決した上で、2 種類の Schnorr 型のブラインド署名 [2,22] を用いた電子マネーシステムを発表した [13]。しかし、このシステムでは、利用者が引出中にマネーの価値を偽造できる危険性がある。

Nyberg・Rueppel は、以下の性質を持つ署名を開発した [16,17]。

- **メッセージ・リカバリー:** 検証者は、署名からメッセージを復元することができる。つまり、メッセージはハッシュ関数で圧縮される必要がなく、署名と一緒に送信されなくてもよい。

この性質は、今までの署名方式 (ElGamal 署名 [9]、Schnorr 署名など) では実現されておらず、従来の電子マネーシステム [3,4,7],[11]-[13],[18,19,22] も持っていない。

Nguyen 達は、メッセージ・リカバリーの性質を持つ電子マネーシステムを発表したが [15]、先程の宮崎・櫻井方式と同様の理由で、電子マネーの偽造が簡単にできる。

本研究では、[14,15] の中で提案された電子マネーシステムの問題点を具体的に考察した。これを踏まえた上で、我々は、新たなオフライン型電子マネーシステムを 2 種類提案した。一つは、Schnorr 署名に基づいた 2 種類のブラインド署名を利用した電子マネーシステムで、このシステムは、[13] で紹介した電子マネーシステムを改良したものである。もう一つは、Nyberg-Rueppel 署名の使用によってメッセージ・リカバリーを実現する電子マネーシステムである。そして、これら 2 つの提案方式の安全性 (完全性、支払時における利用者の匿名性、マネーの偽造、二重使用者の特定) について評価した。また、通信・計算コストの観点から考えると、2 種類の提案システムは、過去のシステム [3,11,12] よりも効率的である。