Mis-representation of Identities in E-cash Schemes and how to Prevent it

Agnes Chan¹, Yair Frankel² *, Philip MacKenzie²,³ *, Yiannis Tsiounis¹ **

¹ Northeastern University
College of Computer Science
161 Cullinane Hall
Boston, Massachusetts 02115
ahchan@ccs.neu.edu, yiannis@ccs.neu.edu

² Sandia National Laboratories
1515 Eubank SE
Albuquerque, New Mexico 87123
yair@cs.sandia.gov

³ Department of Mathematics and Computer Science
Boise State University
Boise, Idaho 83725
philmac@cs.idbsu.edu

Abstract. In Crypto '93, S. Brands presented a very efficient off-line electronic cash scheme based on the representation problem in groups of prime order. In Crypto '95 a very efficient off-line divisible e-cash scheme based on factoring Williams integers was presented by T. Okamoto. We demonstrate one efficient attack on Okamoto's scheme and two on Brands' scheme which allow users to mis-represent their identities and double-spend in an undetectable manner, hence defeating the most essential security aspect of the schemes. The attack on Brands' scheme (which we suspect, given his previous related results, was an inadvertent omission) is also applicable to T. Eng and T. Okamoto's divisible e-cash scheme (presented in Eurocrypt '94) which uses Brands' protocols as a building block.

We present an efficient modular fix which is applicable to any use of the Brands' idea, and we discuss how to counteract the attack on Okamoto's scheme. Hence the original results remain significant contributions to electronic cash.

1 Introduction

In Crypto '95, Okamoto [Oka95] presented a very efficient off-line divisible e-cash system, whose security is based on factoring a Williams integer. We discover

* This work was performed under U.S. Department of Energy contract number DE-AC04-94AL85000.

** This author's research was partially funded by GTE Laboratories Incorporated, Waltham MA.
an attack on this scheme that allows a user to double-spend undetectably by falsifying his identity at account opening. We also discuss ways for the bank to counteract the attack, thus preserving the significance of the result.

In Crypto '93, Brands presented a very efficient off-line electronic cash scheme based on the representation problem in groups of prime order [Bra93b]. In Eurocrypt '94, Eng and Okamoto [EO94] used [Bra93b] as a building block to construct an off-line divisible e-cash scheme. We discover two flaws that are applicable in both schemes. These attacks allow a misbehaving user to deterministically construct an incorrect identity and spend his electronic coins multiple times without being identified. Though our attacks are severe, the fix is simple. Hence, we believe that the original contributions are strong and represent important electronic cash systems to be further studied and improved.

In Section 2 we review the protocol in [Oka95] and discuss an attack on the scheme and how to counteract it. In Section 3, we review the protocols in [Bra93b] and [EO94] and discuss how to break and repair them.

2 Okamoto’s Divisible Scheme

We proceed with a short description of Okamoto’s scheme; we refer the reader to [Oka95] for details.

In this scheme, each user \( \mathcal{U} \) has a composite number \( N = PQ \) such that \( N \) is a Williams integer\(^4\) associated with \( \mathcal{U} \).

In the account opening protocol the user \( \mathcal{U} \) selects random primes \( P, Q \) with \( |P| = |Q| \) and shows \( gP, gQ \pmod{P} \) to the bank \( B \), where \( g \) is a generator of the subgroup of prime order \((P - 1)/2\), \( P \) is prime and \( |P| \geq 4|P| + 10 \). The bank \( B \) provides the user with an “electronic license” on a number \( N = PQ \) after the user proves that \( N \) is indeed the product of \( P, Q \).

Withdrawal of the coin (performed over an authenticated channel between \( \mathcal{U} \) and \( B \)) is nothing more than an RSA blind signature [Cha83] on \( H(N||b) \), where \( H \) is a one-way function, \( b \) is a random value, and the private RSA key used by \( B \) to sign is dependent on the value of the coin.

The payment protocol (performed over an anonymous channel between \( \mathcal{U} \) and the shop \( S \)) consists of the coin authentication and denomination revelation stages.

At coin authentication, \( S \) verifies the bank's RSA signature on \( H(N||b) \), the correctness of the electronic license on \( N \), and that the Jacobi symbols of \(-1\) and \( 2 \) over \( N \) are \( 1 \) and \( -1 \) respectively: \((-1/N) = 1, (2/N) = -1\). This last step guarantees that \( N \) has an odd number of prime factors which are congruent to \( 3 \pmod{8} \), and an odd number of factors congruent to \( 7 \pmod{8} \).

At denomination revelation, \( \mathcal{U} \) reveals the square root \( \sqrt{N} \) of some random numbers. Also, \( S \) (indirectly) checks that \( N \) has only two prime factors.

\(^4\) \( N = PQ \) is a Williams integer iff \( P, Q \) are primes, and \( P \equiv 3 \pmod{8}, Q \equiv 7 \pmod{8} \).