Contents lists available at SciVerse ScienceDirect

Electronic Commerce Research and Applications

A response to a critique of "A novel electronic cash system with trustee-based anonymity revocation from pairing," by Chen, Chou, Sun and Cho (2011)

Yalin Chen [a], Jue-Sam Chou [b,*], Hung-Min Sun [a], Ming-Sun Cho [b]

[a] National Tsing-hua University, No. 101, Section 2, Kuang-Fu Road, Hsinchu, Taiwan
[b] Nanhua University, No. 55, Section 1, Nanhua Road, Zhongkeng, Dalin Township, 62248 Chiayi County, Taiwan

ARTICLE INFO

Article history:
Received 12 June 2012
Received in revised form 12 June 2012
Accepted 12 June 2012
Available online 20 July 2012

Keyword:
Electronic cash

ABSTRACT

We provide a brief rebuttal of Chang (2012), who suggested that there were flaws in our article, Chen et al. (2011), that deserved further investigation and comment. We believe that these criticisms are unfounded, and offer some additional details related to the intractable *discrete elliptic curve discrete logarithm problem* to further support the case we wish to make.

The critique of our article, Chen et al. (2011), by Chang (2012) provided an opportunity for us to examine the fundamentals of our work again. He wrote: "In the e-cash withdrawal phase of the process, the customer will withdraw money from the bank in the form of uniquely identifiable e-cash. At the same time, the bank will obtain and make an entry for it in a database." We admit that some mathematics related to cryptography that we used could have been introduced more clearly. Nevertheless, we will offer a rebuttal for this and one other supposed flaw, since we believe that our research findings were improperly interpreted.

Regarding the alleged first flaw, the items in the database entry that the bank will record when a withdrawal transaction occurs are a *customer's identity*, a *blind e-coin* (*E-Coin*), a *blind license* (*License*), and a *blind signature* (R, S). After the customer completes a withdrawal, the e-cash, defined in terms of the set {*E-Coin*, *License*, R, S}, will not be linkable to the blind messages. Here, *E-Coin* is a random e-coin number. As a result, the bank only will be able to link the *customer's identity* to the *blind e-coin* based on $b^2 \cdot H(E\text{-}Coin)$, the *blind license* based on $b^{-1} \cdot License$, and the *blind signature* based on (R', S'). It cannot link the *customer's identity* to the e-cash though.

So, could Chang (2012) have meant that the license based on $b^{-1} \cdot License$ is problematic? Our view is that this isn't possible. This is due to the intractable *elliptic curve discrete logarithm problem* that is embedded here. We will offer more details shortly.

Chang (2012) noted a possible second flaw also: "Based on a test involving a *greatest common denominator condition*, the dishonest bank will be able to retrieve information about the honest customer's blind factor." We think that Chang misunderstood the operations of elliptic curve cryptography though (Forouzan 2008). This method involves a group of points on an elliptic curve in a plane. Each point has coordinates denoted by the integers (x, y). They form an *additive cyclic algebraic group* $G = \{P, 2P, \ldots, nP\}$, with P the base of group G of order n. Two operations can be applied to the group: addition and point multiplication. *Point multiplication* is defined as $aP = P + P + \cdots + P$, and it involves *addition* $(a - 1)$ times, with P representing points, and the integer $a < n$. We use a capital letter to represent a point, and lowercase to represent an integer. Thus, given two elliptic curve points – $X = abP$ and $Y = acP$, where a, b, c are integers and P is a point – one cannot extract a via the *greatest common denominator* because division on G is not defined.[1]

A similar well-known intractable problem in digital cryptography is the *CONF problem*: given P, aP and abP, compute bP (Sakurai and Shizuya, 1995). Now, recall Chang's (2012) critique of our

[1] In computational complexity theory, when an integer n is sufficiently large, it will be computationally infeasible to find a's value, for a given random point $Q = aP$. P and Q are points here. This is a elliptic curve discrete logarithm problem, which is an intractable problem (Menezes et al. 1993). Problems that can be solved in theory (under given infinite time) but take too much time for the solutions to be useful in practice, are known as intractable problems (Hopcroft et al., 2007).

* Corresponding author.
E-mail address: jschou@mail.nhu.edu.tw (J.-S. Chou).

1567-4223/$ - see front matter © 2012 Published by Elsevier B.V.
http://dx.doi.org/10.1016/j.elerap.2012.06.005

work. He suggested that we computed a blind factor based on an integer b by testing for the greatest common denominator for the *blind e-coin* and *blind license* ($b^2 \cdot H(E\text{-}Coin)$ and $b^{-1} \cdot License$. Both $H(E\text{-}Coin)$ and *License* are points on an elliptic curve. Based on our arguments in this rebuttal, the operation implied by the criticism will be computationally infeasible. The reason is that, if Chang's attack works, then it also will solve the CONF problem in polynomial time, which research has not yet proven to be possible.

References

Chang, Y. F., A critique of ''A novel electronic cash system with trustee-based anonymity revocation from pairing,'' by Chen, Chou, Sun and Cho (2011), *Elec. Comm. Res. Appl.*, 2012. http://dx.doi.org/10.1016/j.elerap.2012.04.003.

Chen, Y. L., Chou, J. S., Sun, H. M., and Cho, M. H. A novel electronic cash system with trustee-based anonymity revocation from pairing. *Elec. Comm. Res. Appl.*, 10, 6, 2011, 673–682.

Forouzan, B. A. Introduction to cryptography and network security. In *Elliptic Curve Cryptosystem*, McGraw Hill, New York, NY, 2008, 321–330.

Hopcroft, J. E., Motwani, R., and Ullman, J. D. Introduction to automata theory, languages, and computation, Addison Wesley, Boston/San Francisco/New York, 2007, 368.

Menezes, A. J., Okamoto, T., and Vanstone, S. A. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Trans. Inform. Theory*, 39, 5, 1993, 587–594.

Sakurai, K., and Shizuya, H. Relationships among the computational powers of breaking discrete log cryptosystems, EUROCRYPT 1995, Springer LNCS 921, 341–355.