# A correction to 'efficient and secure comparison for on-line auctions'

Ivan Damgård*, Martin Geisler and Mikkel Krøigård

BRICS, Department of Computer Science,
University of Aarhus,
Denmark
E-mail: ivan@daimi.au.dk
E-mail: mg@daimi.au.dk
E-mail: mk@daimi.au.dk
*Corresponding author

**Abstract:** In this paper, we describe a correction to the cryptosystem proposed in Damgård et al. from *Int. J. Applied Cryptography,* Vol. 1, No. 1. Although, the correction is small and does not affect the performance of the protocols from Damgård et al., it is necessary, as the cryptosystem is not secure without it.

**Keywords:** comparison; protocols; public-key cryptography.

**Reference** to this paper should be made as follows: Damgård, I., Geisler, M. and Krøigård, M. (2009) 'A correction to 'efficient and secure comparison for on-line auctions'', *Int. J. Applied Cryptography*, Vol. 1, No. 4, pp.323–324.

**Biographical notes:** Ivan Damgård is a Professor at the Department of Computer Science, University of Aarhus, Denmark. Currently, he is working on the Secure Information Management and Processing (SIMAP) project. His main research interests are cryptography, data security, discrete math, quantum information, algorithms and complexity.

Martin Geisler is currently pursuing a PhD degree at the Department of Computer Science, University of Aarhus, Denmark. Currently, he is working on the Secure Information Management and Processing (SIMAP) project. He began his PhD study in 2006 and works on the efficient and elegant implementations of secure multiparty computation protocols.

Mikkel Krøigård is a PhD Student at the Department of Computer Science, University of Aarhus, Denmark. Currently, he is working on the Secure Information Management and Processing (SIMAP) project. He began his PhD in 2006 with a focus on developing efficient protocols for secure multiparty computation.

## 1 Introduction

In Damgård et al. (2007, 2008), the authors of this paper proposed a protocol for secure comparison of integers. A homomorphic cryptosystem was also proposed upon which the protocol is based. The cryptosystem works as follows: to generate keys on input security parameters $k$, $t$, a $k$-bit RSA modulus $n = pq$ is chosen, along with a small $l$ -bit prime $u$ and a $t$-bit prime $v$. It is required that both $u$ and $v$ divide $p - 1$ and $q - 1$. Finally, elements $g, h \in \mathbb{Z}_n^*$ are chosen, such that $h$ has order $v$ modulo both $p$ and $q$, and $g$ has order $uv$ modulo both $p$ and $q$. The public key is pk = $(n, g, h, u)$, the secret key is sk = $(p, q, v)$.

To encrypt a number $m \in \mathbb{Z}_u$, choose $r$ as a random $2t$-bit integer and let the ciphertext be

$$E_{\text{pk}}(m, r) = g^m h^r \bmod n$$

It would be natural to choose the randomiser $r$ uniformly in $\mathbb{Z}_u$, but this cannot be done since $v$ is secret, instead it is chosen to be much larger than $v$ since then $h^r \bmod n$ has distribution statistically indistinguishable from uniform in the group generated by $h$.

To decrypt ciphertext $c = E_{\text{pk}}(m, r)$, one first computes $c^v \bmod n = g^{vm} \bmod n$. The protocols from Damgård et al. (2007, 2008) only requires checking if $m = 0$, so one can just verify whether $c^v \bmod n = 1$. For a small $u$, all of $m$ can be recovered by just building a table of containing values of $g^{vm} \bmod n$ and the corresponding $m$.

Define $G$ to be group generated by $g$, $H$ to be the group generated by $h$. It is shown in Damgård et al. (2007, 2008) that this system is semantically secure under

Conjecture 1: *For any constant l and appropriate choice of t as a function of k, the tuple (n, g, h, u, x) is*

*computationally indistinguishable from (n, g, h, u, y), where (n, g, h, u) are generated as in the above key generation, x is uniform in G and y is uniform in H.*

Various attacks against the assumption are studied in Damgård et al. (2007, 2008), and the conclusion is that if $k$ is large enough to make factoring infeasible and $t$ large enough so that $2^{t/2}$ modular exponentiations are infeasible, the assumption is believed to hold.

Unfortunately, it was overlooked in Damgård et al. (2007, 2008) that if $v$ is chosen to divide both $p-1$ and $q-1$, then $v$ also divides the (public) $n-1$. This means that if one first computes $a = (n-1)/u^l$, where $u^l$ is the maximal power of $u$ that divides $n-1$, then raising a number to power $a$ outputs 1 if the number was in $H$ and something different from 1 otherwise. Thus, the assumption is false for the construction from Damgård et al. (2007, 2008).

Note that while it may seem natural to 'solve' the problem by having $v$ divide only $p-1$, say, this would not be secure either: if $h$ still has to have order $v$ or this would force $h$ to be 1 modulo $q$, and so one could factor $n$ just by computing GCD $(n, h-1)$.

## 2 The correction

The correction is very simple and consists of choosing in the key generation two $t$-bit primes $v_p, v_q$, and constructing $p$, $q$ such that $v_p|(p-1)$ and $v_q|(q-1)$. Then, we choose $g$ to be of order $uv_pv_q$ and $h$ to be of order $v_pv_q$. The public key is pk = $(n, g, h, u)$, the secret key is $sk = (p, q, v_p, v_q)$. The encryption and decryption are as before, except that one raises to exponent $v_pv_q$ to decrypt, and in the encryption, the randomiser $r$ should be chosen somewhat longer than $2t$ bits (see more details on this below).

The system is easily seen to be semantically secure under exactly the same assumption as before, however, we can now hope that the assumption is true for the new way to generate $n, g, h$. There is no longer an easy connection between $n-1$ and the secret key, so the attack described earlier no longer works. The study of other attacks as done in Damgård et al. (2007, 2008) is still valid for the corrected system.

As in Damgård et al. (2007, 2008), we recommend choosing $k$ between 1,000 and 2,000 and $t = 160$.

The original as well as the corrected system are closely related to the schemes proposed by Groth (2005). The main difference is that we specifically go for a small plaintext space defined by a small prime $u$ that divides both $p-1$ and $q-1$. This means that our system leaves a large factor $p-1$ and $q-1$ free to be chosen at random, and this may make $n$ harder to factor. A more practical difference is that we can decrypt faster by computing only modulo $p$ or $q$. Indeed $m$ is uniquely determined from $c^{v_p} \bmod p = g^{v_p m} \bmod p$.

A final word on performance of encryption: if we want to make sure that $h^r \bmod n$ is uniform in the group generated by $h$, we should choose $r$ somewhat longer than $2t$ bits, say of length $3t$ bits – since in the corrected system, the order of $h$ is $2t$ bits long. This will cause the encryption to take about 50% more time compared to the original system. However, if one is willing to make the additional assumption that raising $h$ to a $2t$-bit exponent produces an element that is indistinguishable from uniform in $H$, then one can keep the original encryption algorithm and this means that using the corrected system in the protocols from Damgård et al. (2007, 2008) will produce exactly the same performance as reported there.

## Acknowledgement

Thanks to Claudio Orlandi for helping us to realise the problem with the original scheme.

## References

Damgård, I., Geisler, M. and Krøigaard, M. (2007) 'Efficient and secure comparison for on-line auctions', in J. Pieprzyk, H. Ghodosi and E. Dawson (Eds.), *ACISP*, Vol. 4586 of *Lecture Notes in Computer Science*, Springer, pp.416–430.

Damgård, I., Geisler, M. and Krøigaard, M. (2008) 'Homomorphic encryption and secure comparison', *Int. J. Applied Cryptography*, Vol. 1, No. 1.

Groth, J. (2005) 'Cryptography in subgroups of $\mathbb{Z}_n^*$', in J. Kilian (Ed.), *TCC '05*, Vol. 3378 of *Lecture Notes in Computer Science*, Springer, pp.50–65.