Erratum Concerning "Cryptanalysis of an Algebraic Privacy Homomorphism"

David Wagner

September 24, 2003

Summary. Dr. Koji Chida discovered [2] a serious flaw in Wagner's paper "Cryptanalysis of an Algebraic Privacy Homomorphism," as it appears in the *ISC 2003* proceedings [1]. This note describes the error in Wagner's paper, and then explains how to fix the defect. The conclusions of Wagner's paper remain accurate, but the reasoning as published was inaccurate. I assume that the reader is familiar with the proceedings version of Wagner's paper.

The flaw. Encryption in the Domingo-Ferrer scheme begin by picking a polynomial $p(X)$ at random such that $p(1) \equiv a \pmod{m'}$. Then, the encryptor computes $q(X) \stackrel{\text{def}}{=} p(rX)$ and outputs $q(X)$ as the ciphertext.

The published analysis claims that the quantity $p(1) - a$ is an integer multiple of m' (this is correct) and that this quantity can be obtained by the attacker (incorrect!). In fact, the quantity $p(1) - a$ is not available to the attacker: the attacker does learn $q(X)$, because it is the ciphertext, but $p(X)$ is never revealed. The flaw in the published analysis was that it failed to distinguish properly between $p(X)$ and $q(X)$.

As a result, the published attack [1] does not work: it will not recover m' correctly.

The fix. The attack can be repaired by a more careful analysis. If the attacker could learn the value $q(r^{-1}) - a$, this would indeed be an integer multiple of m', and the methods of Wagner's paper would suffice to learn the key. Unfortunately, because r is part of the secret key, there is no obvious way for the attacker to learn the value $q(r^{-1}) - a$. This denies the attacker access to a source of integer multiples of m', derailing the published attack.

Nonetheless, there is a different way that the attacker can obtain integer multiples of m'. The attacker can collect many pairs $(a_i, q_i(X))$ such that $q_i(r^{-1}) - a_i \equiv 0 \pmod{m'}$ holds for each i. Defining $f_i(X) \stackrel{\text{def}}{=} q_i(X) - a_i$, we obtain the following system of equations:

$$\begin{aligned} f_1(r^{-1}) &\equiv 0 \pmod{m'} \\ &\vdots \\ f_n(r^{-1}) &\equiv 0 \pmod{m'}. \end{aligned}$$

This is a system of (known) polynomials $f_i(X)$ that share a common (unknown) root r^{-1} modulo a (unknown) value m'. If the attacker could somehow solve this system of polynomial equations for the unknowns m' and $r^{-1} \bmod m'$, then the attacker would be back in business.

It turns out that it is indeed possible to solve this system of polynomial equations, by using resultants. If $f(X), g(X)$ are two integral polynomials that share a common root modulo m', then the resultant $\mathrm{Res}(f, g)$ is an integer satisfying $\mathrm{Res}(f, g) \equiv 0 \pmod{m'}$. As a result, the quantity $\mathrm{Res}(f_i, f_j)$ is an integer multiple of m', for each pair of indices i, j.

Thus, the attacker can readily obtain a set of random integer multiples of the (unknown) value m'. At this point, the published methods can be applied to learn m' and then break the Domingo-Ferrer scheme.

References

1. D. Wagner, "Cryptanalysis of an Algebraic Privacy Homomorphism," *ISC 2003*, LNCS 2851, 2003.
2. K. Chida, personal communication, August 7, 2003.