Cryptanalysis of an Algebraic Privacy Homomorphism

David Wagner

U.C. Berkeley

daw@cs.berkeley.edu

Summary

Last year at ISC: A privacy homomorphism was proposed, namely, an encryption algorithm E such that $E_k(a) + E_k(b) = E_k(a+b)$ and $E_k(a) \times E_k(b) = E_k(a \times b)$.

In this talk: The ISC'02 proposal is insecure.

Warning!

Caution: My paper in the ISC'03 proceedings has a serious flaw (found by Dr. Koji Chida).

The flaw has been repaired. An erratum and a corrected revision of my paper are available.

Part I: Puzzles

"Riddle me this." —The Riddler

Puzzle #1: Guess the Divisor

Secret: A positive integer $m' \in \mathbb{N}$.

Given: Two positive integers $x_1, x_2 \in \mathbb{N}$,
where x_1, x_2 are random integer multiples of m'.

Goal: Find m', with high probability.

Puzzle #1: Guess the Divisor

Secret: A positive integer $m' \in \mathbb{N}$.
Given: Two positive integers $x_1, x_2 \in \mathbb{N}$,
where x_1, x_2 are random integer multiples of m'.
Goal: Find m', with high probability.

Solution: Compute $\gcd(x_1, x_2)$. Guess that $m' = \gcd(x_1, x_2)$.

Success probability $= 6/\pi^2 \approx 0.608$.

Puzzle #2: Find the Divisor

Secret: $m' \in \mathbb{N}$.

Given: $x_1, \ldots, x_n \in \mathbb{N}$, random integer multiples of m'.

Goal: Find m', with near-certainty.

Puzzle #2: Find the Divisor

Secret: $m' \in \mathbb{N}$.

Given: $x_1, \ldots, x_n \in \mathbb{N}$, random integer multiples of m'.

Goal: Find m', with near-certainty.

Solution 1: Compute $\gcd(x_1, x_2)$, $\gcd(x_3, x_4)$, $\ldots$, $\gcd(x_{n-1}, x_n)$. Take a majority vote.

Puzzle #2: Find the Divisor

Secret: $m' \in \mathbb{N}$.

Given: $x_1, \ldots, x_n \in \mathbb{N}$, random integer multiples of m'.

Goal: Find m', with near-certainty.

Solution 1: Compute $\gcd(x_1, x_2)$, $\gcd(x_3, x_4)$, $\ldots$, $\gcd(x_{n-1}, x_n)$. Take a majority vote.

Solution 2: Compute $\gcd(x_1, x_2, \ldots, x_n)$.

Success probability $\approx 1 - 2^{-O(n)}$.

Puzzle #3: Find the Modulus

Secret: $m' \in \mathbb{N}$.

Given: $f_1(X), \ldots, f_n(X) \in \mathbb{Z}[X]$, where $f_i(1) \equiv 0 \pmod{m'}$.

Goal: Find m'.

Puzzle #3: Find the Modulus

Secret: $m' \in \mathbb{N}$.
Given: $f_1(X), \ldots, f_n(X) \in \mathbb{Z}[X]$, where $f_i(1) \equiv 0 \pmod{m'}$.
Goal: Find m'.

Solution: Let $x_i = f_i(1)$. These are integer multiples of m'. Apply Puzzle #2.

Success probability ≈ 1.

Puzzle #4: Find the Modulus, Again

Secrets: $m' \in \mathbb{N}$, $\quad \alpha \in \mathbb{Z}/m'\mathbb{Z}$.

Given: $f_1(X), \ldots, f_n(X) \in \mathbb{Z}[X]$, where $f_i(\alpha) \equiv 0 \pmod{m'}$.

Goal: Find m'.

Puzzle #4: Find the Modulus, Again

Secrets: $m' \in \mathbb{N}, \quad \alpha \in \mathbb{Z}/m'\mathbb{Z}$.
Given: $f_1(X), \ldots, f_n(X) \in \mathbb{Z}[X]$, where $f_i(\alpha) \equiv 0 \pmod{m'}$.
Goal: Find m'.

Solution: Let $x_i = \mathrm{Res}(f_{2i-1}, f_{2i})$. These are integer multiples of m'. Apply Puzzle #2.

Puzzle #4: Find the Modulus, Again

Secrets: $m' \in \mathbb{N}$, $\quad \alpha \in \mathbb{Z}/m'\mathbb{Z}$.
Given: $\quad f_1(X), \ldots, f_n(X) \in \mathbb{Z}[X]$, where $f_i(\alpha) \equiv 0 \pmod{m'}$.
Goal: $\quad$ Find m'.

Solution: Let $x_i = \mathrm{Res}(f_{2i-1}, f_{2i})$. These are integer multiples of m'. Apply Puzzle #2.

- $\mathrm{Res}(f, g)$, the resultant of $f(X)$ and $g(X)$, is an integer, and it can be efficiently computed.
- If $f(X)$ and $g(X)$ share a common root, then $\mathrm{Res}(f, g) = 0$. If $f(X)$ and $g(X)$ share a common root modulo m', then $\mathrm{Res}(f, g) \equiv 0 \pmod{m'}$.

Puzzle #5: Find the Common Root

Secret: $\alpha \in \mathbb{Z}/m'\mathbb{Z}$.

Given: $m' \in \mathbb{N}$; $f_1(X), \ldots, f_n(X) \in \mathbb{Z}[X]$,
where $f_i(\alpha) \equiv 0 \pmod{m'}$ and $\deg f_i \leq n$.

Goal: Find α.

Puzzle #5: Find the Common Root

Secret: $\alpha \in \mathbb{Z}/m'\mathbb{Z}$.
Given: $m' \in \mathbb{N}$; $f_1(X), \ldots, f_n(X) \in \mathbb{Z}[X]$,
where $f_i(\alpha) \equiv 0 \pmod{m'}$ and $\deg f_i \leq n$.
Goal: Find α.

Solution: Consider this system of equations:

$$\begin{aligned} f_1(\alpha) &\equiv 0 \pmod{m'} \\ &\vdots \\ f_n(\alpha) &\equiv 0 \pmod{m'}. \end{aligned}$$

Notice: Each equation is linear in $\alpha, \alpha^2, \ldots, \alpha^n$.
So, apply Gaussian elimination over $\mathbb{Z}/m'\mathbb{Z}$.

Part II: Cryptanalysis

"If it's provably secure, it's probably not."

—Lars Knudsen

The ISC'02 privacy homomorphism

Key generation:

Public: $m \in \mathbb{N}$.

Private: a divisor $m' \in \mathbb{N}$ of m; $r \in (\mathbb{Z}/m\mathbb{Z})^*$.

Encryption:

Plaintext: $a \in \mathbb{Z}/m'\mathbb{Z}$.

Ciphertext: $q(X) \in (\mathbb{Z}/m\mathbb{Z})[X]$, formed as $q(X) \stackrel{\text{def}}{=} p(rX)$ where $p(X)$ is a random polynomial s.t. $p(1) \equiv a \pmod{m'}$.

Decryption:

Ciphertext: $q(X) \in (\mathbb{Z}/m\mathbb{Z})[X]$.

Message: $q(r^{-1}) \bmod m'$.

Phase 1: Find m'

Secrets: $m' \in \mathbb{N}$; $\quad r \in \mathbb{Z}/m\mathbb{Z}$.

Given: $m \in \mathbb{N}$; and, n known-plaintext pairs $(a_i, q_i(X))$ where $q_i(r^{-1}) \equiv a_i \pmod{m'}$.

Goal: Find m'.

Phase 1: Find m'

Secrets: $m' \in \mathbb{N}$; $\quad r \in \mathbb{Z}/m\mathbb{Z}$.

Given: $m \in \mathbb{N}$; and, n known-plaintext pairs $(a_i, q_i(X))$ where $q_i(r^{-1}) \equiv a_i \pmod{m'}$.

Goal: Find m'.

Attack: Define $f_i(X) \stackrel{\text{def}}{=} q_i(X) - a_i$.

Notice that, modulo m', the f_i share a common root, r^{-1}.

Apply Puzzle #4. This reveals m'.

Phase 2: Find $r \bmod m'$

Secret: $r \in \mathbb{Z}/m'\mathbb{Z}$.

Given: $m', m \in \mathbb{N}$; $\quad f_1(X), \ldots, f_n(X)$
where $f_i(r^{-1}) \equiv 0 \pmod{m'}$.

Goal: Find $r \bmod m'$.

Phase 2: Find $r \bmod m'$

Secret: $r \in \mathbb{Z}/m'\mathbb{Z}$.
Given: $m', m \in \mathbb{N}$; $\quad f_1(X), \ldots, f_n(X)$
where $f_i(r^{-1}) \equiv 0 \pmod{m'}$.
Goal: Find $r \bmod m'$.

Attack: Apply Puzzle #5. This reveals $r \bmod m'$.

How much progress have we made?

The secret key was m' and $r \in \mathbb{Z}/m\mathbb{Z}$.
We've learned m' and $r \bmod m'$.

Question: What about the rest of r?

How much progress have we made?

The secret key was m' and $r \in \mathbb{Z}/m\mathbb{Z}$.
We've learned m' and $r \bmod m'$.

Question: What about the rest of r?

Answer: The rest of r doesn't matter, and is never used during decryption.
(Corollary: The scheme has many equivalent keys.)

Conclusion: The scheme is broken.

Provably secure?

In ISC'02, the following was proven:

Theorem 1. *(Under appropriate conditions:) No attacker can learn the secret key of the ISC'02 scheme.*

. . . Paradox!

Provably secure?

In ISC'02, the following was proven:

Theorem 2. *(Under appropriate conditions:) No attacker can learn the secret key of the ISC'02 scheme.*

. . . Paradox!

Or, is it?

Provably secure?

In ISC'02, the following was proven:

Theorem 3. *(Under appropriate conditions:) No attacker can learn the secret key of the ISC'02 scheme.*

. . . Paradox!

Or, is it?

Resolution of the paradox: Equivalent keys.

Part of the key is never used. The attacker cannot learn this part of the key, but he doesn't need to.

The importance of proper definitions.

Summary

The ISC'02 scheme is insecure.