Forging a (variant) ElGamal Digital Signature

Frank the Forger wants to solve for \( r \) and \( s \) in:

\[
g^{H(m)} \equiv y^r \pmod{p}.
\]

He knows \( m, g, y, \) and \( p \) but not the discrete log of \( y \pmod{p} \) base \( g \). He could:

\begin{itemize}
  \item calculate the discrete log of \( y \),
  \item or he could solve \( r' \equiv g^{H(m)}/y^s \pmod{p} \) for \( r \).
\end{itemize}

We wish to shed light on the difficulty of the second attack by studying the self-power map, \( x \mapsto x^d \pmod{p} \).

Is \( x \mapsto x^x \pmod{p} \) "random"?

**Heuristic 1.** For all \( p \), if \( x, y \) are chosen uniformly at random from \( \{1, \ldots, p-1\} \) with \( \text{ord}_p x = d \), then

\[
\Pr[x^x \equiv y \pmod{p}] \approx \begin{cases} 
\frac{1}{2} & \text{if } \text{ord}_p y \mid d, \\
0 & \text{otherwise}.
\end{cases}
\]

Counts of the fixed points are not normally distributed

This work investigates the number of fixed points of the self-power map, i.e., solutions to

\[
x^x \equiv x \pmod{p}.
\]

Let \( F_d(p) \) be the number of solutions to (2) such that \( 1 \leq x \leq p-1 \) and \( \text{ord}_p x = d \). How are these counts distributed? The figures show that the distribution is not (quite) normal.

The counts for most orders are binomially distributed

Let \( F_d(p) \) be the number of solutions to (2) with \( 1 \leq x \leq p-1 \) and \( \text{ord}_p x = d \). Assume \( x \) values behave independently.

**Prediction 2.**

\[
\Pr[F_d(p) = k] = \left( \frac{\phi(d)}{d} \right) \left( \frac{1}{d} \right)^k \left( \frac{d-1}{d} \right)^{\phi(d) - k}
\]

A chi-squared goodness-of-fit test gives \( p \)-value \( \approx 0.198 \) which does not refute the prediction.

We also tried a sliding window chi-squared test on the data sorted by order. The resulting \( p \)-values should be uniformly distributed but are not for small and large \( d \).

Dependencies matter for small and large orders

For small and large orders it turns out that the independence assumption is violated.

**Theorem 3.**

(a) The \( x \)-values of order 3 cannot both be fixed points.

(b) The \( x \)-values of order 4 cannot both be fixed points.

(c) The \( x \)-values of order 6 are both fixed points or neither is.

There are similar effects for \( d = (p-1)/3 \) and \( d = (p-1)/4 \), and possibly a few others.

Our predictions based on these dependencies are not refuted by chi-squared tests.