Generic Homomorphic Undeniable Signatures - Erratum

Jean Monnerat ⋆ and Serge Vaudenay ⋆⋆

EPFL, Switzerland
http://lasecwww.epfl.ch

17th February 2005

This document provides an erratum of the article "Generic Homomorphic Undeniable Signatures" which was published in the proceedings of Asiacrypt '04, LNCS **3329**, pp. 354-371, Springer, 2004. At page 360, the last approximation in the following expression

$$\varepsilon_2 \leq \Phi\left(-\sqrt{n}\frac{\theta}{2\sqrt{p^{-1}(1-p^{-1})}}\right) \approx \frac{1}{\sqrt{2\pi}}\left(e^{\frac{-n\theta^2}{4(p^{-1}(1-p^{-1}))}}\right),$$

is false. Let $\varphi(x) := \frac{1}{\sqrt{2\pi}}e^{\frac{-x^2}{2}}$. In the above approximation, we have used the false approximation $\Phi(-x) \approx \frac{1}{\sqrt{2\pi}} \cdot e^{-x^2}$ instead of

$$\Phi(-x) \approx \varphi(x)/x$$

which is correct when x is large. Note also that $\varphi(x)/x \leq \varphi(x)$ when x is large. Hence, if we set $n = 8\theta^{-2}(p^{-1}+\theta)\log(p/\varepsilon)$ we get

$$\varepsilon_2 \leq \frac{1}{\sqrt{2\pi}}\left(e^{\frac{-n\theta^2}{8(p^{-1}(1-p^{-1}))}}\right) = \frac{1}{\sqrt{2\pi}}\left(\frac{\varepsilon}{p}\right)^{\frac{p+p^2\theta}{p-1}},$$

for n large enough. The rest of the paper remains correct except that the complexity becomes $8\theta^{-2}\log(p/\varepsilon)$ oracle calls.

Below we rewrite Lemma 5 and its proof sketch in a correct form.

Lemma 5. *Given two finite Abelian groups G and H, and a set of s points $S = \{(x_i, y_i) \mid i = 1, \ldots, s\}$, we assume that $x_1, \ldots, x_s$ H-generate G. We*

⋆ Supported in part by a grant of the Swiss National Science Foundation, 200021-101453/1.

⋆⋆ Supported in part by the National Competence Center in Research on Mobile Information and Communication Systems (NCCR-MICS), a center supported by the Swiss National Science Foundation under grant number 5005-67322.

assume that we are given the order d of H whose smallest prime factor is p and that we can sample elements in G with a uniform distribution. We assume that we have an oracle function $f : G \longrightarrow H$ such that

$$\Pr_{(r,a_1,\ldots,a_s)\in_U G\times \mathbf{Z}_d^s}[f(dr + a_1x_1 + \cdots + a_sx_s) = a_1y_1 + \cdots + a_sy_s] = \frac{1}{p} + \theta$$

with $\theta > 0$. Let $\varepsilon > 0$ be arbitrarily small. There exists a group homomorphism which interpolates S and which is computable within $8\theta^{-2}\log(p/\varepsilon)$ oracle calls with an error probability less or equal to ε.

Proof (sketch). Due to Lemma 4, the homomorphism g exists and we have $\Pr_{x\in_U G}[f(x) = g(x)] = p^{-1} + \theta$. We use the same techniques which are used in linear cryptanalysis and consider the following algorithm.

Input: $x \in G$
repeat
  pick $r \in G, a_1, \ldots, a_s \in \mathbf{Z}_d$ at random
  $y = f(x + dr + a_1x_1 + \cdots + a_sx_s) - a_1y_1 - \cdots - a_sy_s$
  $c = 0$
  for $i = 1$ to n **do**
    pick $r \in G, a_1, \ldots, a_s, a \in \mathbf{Z}_d$ at random
    if $f(dr + a_1x_1 + \cdots + a_sx_s + ax) = a_1y_1 + \cdots + a_sy_s + ay$ (**T**) **then**
      $c = c + 1$
    end if
  end for
until $c > \tau n$
Output: y

We choose $n = 8\theta^{-2}(p^{-1} + \theta)\log(p/\varepsilon)$ and $\tau = p^{-1} + \frac{1}{2}\theta$ and we estimate the error probability of the acceptance test. We consider two types of error:

$$\varepsilon_1 = \Pr_{x\in_U G}[c \le \tau n \mid y = g(x)] \qquad \varepsilon_2 = \Pr_{x\in_U G}[c > \tau n \mid y \ne g(x)]$$

We will now estimate these two values and show that they are negligible. If $y \ne g(x)$, then the test (**T**) works with probability $t_2 \le 1/p$ due to Lemma 4. We also notice that if $y = g(x)$, the probability that the test works is $\frac{1}{p} + \theta$. Hence, using the central limit theorem we obtain

$$\varepsilon_1 \approx \Phi\left(\sqrt{n}\frac{\tau - p^{-1} - \theta}{\sqrt{(p^{-1} + \theta)(1 - p^{-1} - \theta)}}\right) \qquad \varepsilon_2 \approx \Phi\left(-\sqrt{n}\frac{\tau - t_2}{\sqrt{t_2(1 - t_2)}}\right),$$

when n is large enough and where Φ denotes the distribution function of the standard normal distribution. By looking at the logarithmic derivative of the function $f(t) = (\tau - t)/(\sqrt{t(1-t)})$ and noticing that this one is negative on the interval $[0, \tau]$ we deduce that

$$\varepsilon_2 \leq \Phi\left(-\sqrt{n}\frac{\tau - p^{-1}}{\sqrt{p^{-1}(1-p^{-1})}}\right).$$

Using $\tau = p^{-1} + \frac{1}{2}\theta$ provides

$$\varepsilon_2 \leq \Phi\left(-\sqrt{n}\frac{\theta}{2\sqrt{p^{-1}(1-p^{-1})}}\right) \approx \frac{2\sqrt{p^{-1}(1-p^{-1})}}{\theta\sqrt{n}} \cdot \frac{1}{\sqrt{2\pi}} e^{\frac{-n\theta^2}{8(p^{-1}(1-p^{-1}))}},$$

where the last approximation holds when n is large enough (ε small). Since n is large, we also have

$$\varepsilon_2 \leq \frac{1}{\sqrt{2\pi}} e^{\frac{-n\theta^2}{8(p^{-1}(1-p^{-1}))}}.$$

Now, we substitute the expression of n in the above inequality and we obtain

$$\varepsilon_2 \leq \frac{1}{\sqrt{2\pi}} \left(\frac{\varepsilon}{p}\right)^{\frac{p+p^2\theta}{p-1}}.$$

Since $\frac{p+p^2\theta}{p-1} \geq 1$ and $\frac{\varepsilon}{p} < 1$ when ε is small, we finally get $\varepsilon_2 \leq \varepsilon/(p\sqrt{2\pi}) \leq \rho\varepsilon/2$ where $\rho = p^{-1} + \theta$. In a similar way, we can show that $\varepsilon_1 \leq \varepsilon/2$. It remains to compute the complexity and the error probability of the algorithm. At first, we observe that the probability α that $c \leq \tau n$ in the algorithm is equal to $\rho\varepsilon_1 + (1-\rho)(1-\varepsilon_2)$. From the estimate of ε_1, ε_2, we see that $\alpha \approx 1-\rho$. Moreover, the number of iterations is equal to $\sum_{i=1}^{\infty} i\alpha^{i-1}(1-\alpha) = 1/(1-\alpha) \approx 1/\rho$. Hence, the complexity is $n/\rho = 8(\log(1/\varepsilon) + \log(p))/(\rho - \frac{1}{p})^2$. The probability of error is given by $\sum_{i=1}^{\infty} \alpha^{i-1}(1-\rho)\varepsilon_2 \approx \varepsilon_2(1-\rho)/\rho \leq \varepsilon_2/\rho \leq \varepsilon/2$. $\square$