Sanjit Chatterjee and Palash Sarkar

Identity-Based Encryption: Corrigendum

July 30, 2011

Springer

Page 49, Line −6.

Replace "$e : G \times G \to \Gamma_T$" by $e : G \times G \to G_T$.

Statement and proof of Theorem 7.1.

On Page 92, the deduction of Line 6 from Line 5 is incorrect. Making the necessary correction changes the statements of Theorem 7.1 and Proposition 7.6. These changes and the corrected proof is given below.

The stated bound in Theorem 7.1 should be changed to the following bound.

$$\varepsilon_{ibe}^2 \leq 4q(n+1)\varepsilon_{dbdh}.$$

The statement of Proposition 7.6 should be changed to the following.

$$\varepsilon_{ibe} \leq \frac{\varepsilon_{dbdh}}{\lambda^+} + \frac{q}{m}.$$

The changes in the proof of Theorem 7.1 are as follows.

On Page 85, Line 26: "Let $m = 4q$" should be changed to "Let $m = 2q/\varepsilon_{ibe}$".

The material between Page 92, Line 5 to Page 93, Line 2 should be changed to the following.

$$\Pr[Y_1] - \Pr[Y_2] = \sum_{\mathbf{v}} \lambda(\mathbf{v})(\Pr[X_1 \wedge \mathsf{V} = \mathbf{v}] - \Pr[X_2 \wedge \mathsf{V} = \mathbf{v}]).$$

Using $\lambda^- \leq \lambda(\mathbf{v}) \leq \lambda^+$ and $\sum_{\mathbf{v}} \Pr[X_i \wedge \mathsf{V} = \mathbf{v}] = \Pr[X_i]$, we obtain

$$\lambda^- \Pr[X_1] - \lambda^+ \Pr[X_2] \leq \Pr[Y_1] - \Pr[Y_2] \leq \lambda^+ \Pr[X_1] - \lambda^- \Pr[X_2].$$

Dividing throughout by λ^+ and using $\lambda^-/\lambda^+ = (1 - q/m)$ we get,

$$\Pr[X_1] - \Pr[X_2] - \frac{q}{m}\Pr[X_1] \leq \frac{\Pr[Y_1] - \Pr[Y_2]}{\lambda^+} \leq \Pr[X_1] - \Pr[X_2] + \frac{q}{m}\Pr[X_2]$$

This shows

$$\Pr[X_1] - \Pr[X_2] - \frac{\Pr[Y_1] - \Pr[Y_2]}{\lambda^+} \leq \frac{q}{m}\Pr[X_1] \leq \frac{q}{m}$$

and

$$\Pr[X_1] - \Pr[X_2] - \frac{\Pr[Y_1] - \Pr[Y_2]}{\lambda^+} \geq -\frac{q}{m}\Pr[X_2] \geq -\frac{q}{m}.$$

Combining these two bounds we obtain

$$-\frac{q}{m} \leq (\Pr[X_1] - \Pr[X_2]) - \frac{\Pr[Y_1] - \Pr[Y_2]}{\lambda^+} \leq \frac{q}{m}.$$

As a result,

$$|\Pr[X_1]-\Pr[X_2]|-\left|\frac{\Pr[Y_1]-\Pr[Y_2]}{\lambda^+}\right| \leq \left|(\Pr[X_1]-\Pr[X_2])-\frac{\Pr[Y_1]-\Pr[Y_2]}{\lambda^+}\right| \leq \frac{q}{m}.$$

Assuming (ε_{dbdh}, t') hardness of DBDH, $|\Pr[Y_1]-\Pr[Y_2]| \leq \varepsilon_{dbdh}$. Using this, we get

$$|\Pr[X_1]-\Pr[X_2]| \leq \left|\frac{\Pr[Y_1]-\Pr[Y_2]}{\lambda^+}\right| + \frac{q}{m} \leq \frac{\varepsilon_{dbdh}}{\lambda^+} + \frac{q}{m}.$$

The proof of Proposition 7.6 is now completed as follows.

$$\begin{aligned}
\varepsilon_{ibe} &= \left|\Pr[X_0]-\frac{1}{2}\right| \\
&= |\Pr[X_0]-\Pr[X_2]| \\
&\leq |\Pr[X_0]-\Pr[X_1]| + |\Pr[X_1]-\Pr[X_2]| \\
&\leq \frac{\varepsilon_{dbdh}}{\lambda^+} + \frac{q}{m}.
\end{aligned}$$

□

Since m was chosen to be equal to $2q/\varepsilon_{ibe}$, the proof of Theorem 7.1 follows by substituting the value of m in the statement of Proposition 7.6. □