Humboldt-Universität zu Berlin
Prof. Dr. Johannes Köbler

Übungsblatt 9

Besprechung der mündlichen Aufgaben am 5. 1. 2023
Abgabe der schriftlichen Lösungen bis 10. 1. 2023, 23:59 Uhr

Aufgabe 52 ***mündlich***

Für zwei Texte x_1 und x_2 seien die ElGamal-Signaturen (γ, δ_1) bzw. (γ, δ_2) bekannt, d.h. es wurde beidesmal dasselbe z verwendet.

(a) Beschreiben Sie, wie sich hieraus z im Fall $\mathrm{ggT}(\delta_1 - \delta_2, p-1) = 1$ effizient berechnen lässt, und wie sogar der geheime Exponent a bestimmt werden kann.

(b) Seien $p = 31847$, $\alpha = 5$ und $\beta = 25703$. Berechnen Sie z und a anhand der Texte $x_1 = 8990$, $x_2 = 31415$ sowie der Unterschriften $(23972, 31396)$ und $(23972, 20481)$.

Aufgabe 53 ***mündlich***

Angenommen, Alice verwendet das ElGamal-Signaturverfahren und möchte bei der Berechnung der beim Signieren verwendeten Zufallszahlen Zeit sparen, indem sie ein z_0 wählt und die i-te Nachricht unter Verwendung von $z_i \equiv_{p-1} z_0 + 2i$ signiert. (Es gilt also $z_i \equiv_{p-1} z_{i-1} + 2$.)

(a) Zeigen Sie, wie Bob bei Kenntnis von zwei aufeinander folgenden signierten Nachrichten $(x_i, sig(x_i, z_i))$ und $(x_{i+1}, sig(x_{i+1}, z_{i+1}))$ den privaten Schlüssel a berechnen kann, ohne einen diskreten Logarithmus zu berechnen.
Bemerkung: Für diesen Angriff muss der Wert von i nicht bekannt sein.

(b) Führen sie den Angriff durch, wenn Bob die Werte $p = 28703$, $\alpha = 5$, $\beta = 11339$, $x_i = 12000$, $sig(x_i, z_i) = (26530, 19862)$, $x_{i+1} = 24567$ und $sig(x_{i+1}, z_{i+1}) = (3081, 7604)$ kennt.

Aufgabe 54 ***mündlich***

Betrachten Sie die folgende Variante des ElGamal-Signaturverfahrens. Die Schlüssel werden ähnlich wie beim ElGamal-Signaturverfahren generiert: p ist prim, α ist ein Erzeuger von $\mathbb{Z}_p^*$, a ist der geheime Exponent und $\beta = \alpha^a \bmod p$. Allerdings wird a jetzt aus $\mathbb{Z}_{p-1}^*$ (anstelle von $\mathbb{Z}_{p-1}$) gewählt. Ein Text $x \in \mathbb{Z}_{p-1}$ wird unter $\hat{k} = (p, \alpha, a)$ mit $sig(\hat{k}, x, z) = (\gamma, \delta)$ signiert, wobei gilt:

$$\gamma = \alpha^z \bmod p \text{ und } \delta = (x - z\gamma)a^{-1} \bmod (p-1) \ .$$

Dieses Verfahren unterscheidet sich also auch in der Berechnung von δ.

(a) Beschreiben Sie, wie sich die Unterschrift (γ, δ) eines Textes x bei Kenntnis des Verifikationsschlüssels $k = (p, \alpha, \beta)$ verifizieren lässt.

(b) Welchen Vorteil bei der Berechnung der Signatur besitzt diese Variante gegenüber dem ursprünglichen Verfahren?

Aufgabe 55 ***mündlich***

(a) Falls sich bei der Berechnung einer ElGamal-Signatur der Wert $\delta = 0$ ergibt, muss eine neue Zufallszahl z gewählt werden. Überlegen Sie, wie sich aus einer ElGamal-Signatur (γ, δ) mit $\delta = 0$ und dem öffentlichen Verifikationsschlüssel der geheime Signaturschlüssel berechnen lässt.

(b) Beim DSA muss auch im Fall $\gamma = 0$ eine neue Zufallszahl z gewählt werden. Überlegen Sie, wie aus einer DSA-Signatur (γ, δ) mit $\gamma = 0$ die benutzte Zufallszahl z bestimmt werden kann, und wie sich daraus für einen beliebigen Text x eine gefälschte Signatur (γ, δ) mit $\gamma = 0$ erhalten lässt.

Aufgabe 56 ***10 Punkte***

In der Vorlesung wurde ein Angriff gegen das ElGamal-Signaturverfahren vorgestellt, mit dem sich eine gültige Signatur (γ, δ) für einen zufälligen Text x berechnen lässt (nichtselektive Fälschung bei bekanntem Verifikationsschlüssel). Hierbei berechnet der Gegner für beliebige Parameter $u \in \mathbb{Z}_{p-1}$ und $v \in \mathbb{Z}^*_{p-1}$ die Fälschung (x, γ, δ) mittels

$$\gamma := \alpha^u \beta^v \bmod p, \qquad \delta := -\gamma v^{-1} \bmod p-1 \qquad \text{und} \qquad x := u\delta \bmod p-1.$$

(a) Berechnen Sie eine Fälschung (x, γ, δ) für den Verifikationsschlüssel $k = (p, \alpha, \beta)$ mit $p = 467$, $\alpha = 2$ und $\beta = 132$. (Wählen Sie $u = 99$ und $v = 179$.)

(b) Ähnlich wie oben lässt sich auch eine nichtselektive Fälschung (x', γ', δ') bei bekannter Signatur (x, γ, δ) vornehmen, indem für beliebige Parameter $u, v, w \in \mathbb{Z}_{p-1}$ mit $\mathrm{ggT}(w\gamma - v\delta, p-1) = 1$

$$\begin{aligned}
\gamma' &:= \gamma^w \alpha^u \beta^v \bmod p, \\
\delta' &:= \delta\gamma'(w\gamma - v\delta)^{-1} \bmod p-1 \text{ und} \\
x' &:= \gamma'(wx + u\delta)(w\gamma - v\delta)^{-1} \bmod p-1
\end{aligned}$$

gewählt werden. Zeigen Sie, dass die Signatur (x', γ', δ') als echt akzeptiert wird.

(c) Der Text $x = 100$ hat unter ElGamal (mit $p = 467$, $\alpha = 2$ und $\beta = 132$) die Signatur $y = (\gamma, \delta) = (29, 51)$ erhalten. Berechnen Sie hieraus eine Fälschung (x', y') unter Verwendung der Werte $w = 102$, $u = 45$ und $v = 293$. Überprüfen Sie die Verifikationsbedingung.