Gregor Leander **Fakultät für Mathematik**
16.06.2008 **Ruhr-Universität Bochum**

Kryptographie II – Lösungsvorschläge für Übungsblatt 9

Aufgabe 1 *Decisional Diffie-Hellman Problem*

Seien $(G_1, +, 0)$ und $(G_2, \cdot, 1)$ zyklische Gruppen mit einer Paarung $e : G_1 \times G_1 \to G_2$. In der Vorlesung wurde gezeigt, dass das diskrete Logarithmus-Problem (DLP) in G_1 nicht schwerer als das DLP in G_2 ist.
Das *Decisional Diffie Hellman-Problem (DDH-Problem)* ist: Gegeben $g, g^a, g^b \in G$ und einer nichtgeordneten Menge von zwei Elementen $\{x, y\} = \{g^{ab}, g^r\}$ mit $a, b, r \in \mathbb{Z}$, bestimme welches Element in der Menge $\{x, y\}$ ist g^{ab}.
Beweise folgenden Satz: *In der Gruppe G_1 ist das DDH-Problem leicht zu lösen.*

Lösung
Da der Beweis für die additive Gruppe G_1 zu führen ist, kann zuerst die Notation geändert werden:

Aufgabenstellung		Beweis
g	$\to$	P
g^a	$\to$	aP
g^b	$\to$	bP
g^{ab}	$\to$	abP
g^r	$\to$	rP

Beweis: Da man Beweisen soll, dass DDH in additiven Gruppen, für die eine solche Paarung existiert, effizient zu lösen ist, kann man die Paarung für den Beweis verwenden. Man berechnet also die Werte

$$\begin{aligned} e(aP, bP) &= e(P, P)^{ab} &= x \\ e(P, abP) &= e(P, P)^{ab} &= y \\ e(P, rP) &= e(P, P)^{r} &= z \end{aligned}$$

Aus den Eigenschaften der Paarung folgt, dass $e(aP, bP) = a(P, P)^{ab} = e(P, abP)$ und gleichzeitig $e(P, rP) \neq e(P, abP)$ (da $abP \neq rP$) gelten müssen. Damit kann man abP eindeutig und effizient (die Berechnung von Paarungen ist per Definition effizient) identifizieren. □
□

Aufgabe 2 *Folge der Existenz einer kleinen Untergruppe*

1. Sei G eine endliche zyklische Gruppe mit einer Untergruppe der Ordnung 5. Finde einen effizienten Algorithmus, der das DDH Problem in G mit guter Wahrscheinlichkeit löst.

2. Sei nun $G = (\mathbb{Z}_p^*, *) \times (\mathbb{Z}_5, +)$, wobei p eine grosse Primzahl sei ($\log_2 p \approx 1024$). In G ist damit das DL Problem schwer und das DDH Problem leicht. Kann man G für eine Signatur analog zu dem BLS Schema nutzen?

Lösung

1. Sei n die Ordnung von G und g ein Erzeuger von G (damit ist $g^{n/5}$ ein Erzeuger der Untergruppe der Ordnung 5). Hier berechnet man einfach den DL in der Untergruppe der Ordnung 5. Das geht einfach, genau wie bei Silver-Pohlig-Hellman. Seien also $g^a, g^b \in G$ gegeben und weiterhin $d \in G$ so das entweder $d = g^{ab}$ oder $d = g^r$ für ein zufälliges r gilt. Dann berechnet man den DL von $(g^a)^{n/5}$ und $(g^b)^{n/5}$ zur Basis $g^{n/5}$. Sei also

   $$x = \log_{g^{n/5}}((g^a)^{n/5}) \text{ und } y = \log_{g^{n/5}}((g^b)^{n/5})$$

   sowie

   $$z = \log_{g^{n/5}}((d)^{n/5}).$$

   Wenn $xy = z \bmod 5$ gilt dann nimmt man an, das $d = g^{ab}$ war und sonst nimmt man an das $d = g^r$ war. Die Wahrscheinlichkeit für zufälliges a, b und r sich richtig zu entscheiden liegt bei $4/5$.

2. Das BLS Schema kann man wie folgt verallgemeinern:

   (a) Systemparameter: Eine Gruppe G in der das DH Problem schwer und das DDH Problem leicht ist, sowie ein Generator von G. Zusätzlich eine Hashfunktion von $\{0,1\}^* \to G$.

   (b) Geheimer Schlüssel: ein Element $x \in \{1, \ldots, n-1\}$. Öffentlicher Schlüssel ist g^x.

   (c) Signaturerzeugung: Berechne $\sigma = h(m)^x$.

   (d) Signaturverifikation: Teste ob das Tupel $(g, g^x, h(m), \sigma)$ ein gültiges DH-tupel ist, dass heist ob für $h(m) = g^y$ gilt das $\sigma = g^{xy} = h(m)^x$ gilt.

   Jetzt zur eigentlichen Aufgabe: Nein, so eine Gruppe kann man nicht nutzen. Es ist ganz leicht hier Signaturen zu fälschen, da man dafür nur sicherstellen muss, dass

   $$(g^{n/5}, (g^x)^{n/5}, (h(m))^{n/5}, \sigma^{n/5})$$

ein gültiges DH Tupel in der Untergruppe ist. Das ist leicht. Also: es geht nicht und das Problem ist, dass es nicht reicht für zufällig gewählte Instanzen das DDH Problem mit guter Wahrscheinlichkeit zu lösen. Man muss das DDH Problem für alle Instanzen lösen können und zwar mit Wahrscheinlichkeit 1.

□