Kryptografia - Zadanie 2.3

Rafał Włodarczyk

INA 6, 2026

1 Wprowadzenie

Obliczenia prowadzone są w grupie cyklicznej $G = \langle g \rangle$, gdzie g jest generatorem grupy, a $q = \text{ord}(G)$ jest rzędem grupy. Osoba podpisująca posiada parę (a, A) - a jest kluczem prywatnym, $g^a = A$ jest kluczem publicznym. Zakładamy, że logarytm dyskretny w grupie G jest trudny do obliczenia, tj. nie istnieje efektywny algorytm który przy danych G, g, A wyznacza $a : g^a = A$. Wszystkie działania skalarne są wykonywane w obrębie grupy $\mathbb{Z}_q$.

2 Zadanie 2.3

W tym zadaniu funkcja skrótu oznaczona jest wzorem $h = mR$, gdzie m - wiadomość oraz $R \in G$. Mamy do czynienia z następującym schematem podpisu:

1. Podpisujący losuje skalar $r \in \mathbb{Z}_q$ i oblicza $R = g^r$.
2. Podpisujący wyznacza $h = mR$.
3. Podpisujący oblicza $s = [r + ah] \mod q$ i zwraca $\sigma = (R, s)$ - podpis wiadomości m.
4. Weryfikator wyznacza $h = mR$, a następnie weryfikuje podpis za pomocą warunku:

$$g^s = RA^h$$

3 Podpunkt 1

3.1 Poprawność Algebraiczna

W nagłówku listy 2 wskazane jest dowiedzenie m.in poprawności algebraicznej u uczciwego podpisującego. Zakładamy że posiada on klucz a, wybiera r, liczy $R = g^r$, wyznacza $h = mR, s = r + ah \mod q$ i zwraca $\sigma = (R, s)$.

Pokażmy, że taki podpis przechodzi weryfikację:

$$P = RA^h = g^r \cdot g^{ah} = g^{r+ah} = g^s = L_\square$$

Schemat jest algebraicznie poprawny.

3.2 Polecenie

Wyjaśnij, w jakiej domenie iloczyn $m \cdot R$ miałby być liczony.

3.3 Rozwiązanie

Wiemy, że R jest elementem grupy G, a m_{original} jest wiadomością o nieokreślonej długości. Wynikiem działania $h = m \cdot R$ musi być element grupy $\mathbb{Z}_q$ - ponieważ h jest elementem wykładnika (w weryfikacji $g^s = RA^h$). Naturalnym przedstawieniem mR w $\mathbb{Z}_q$ jest reprezentacja wiadomości m przez liczbę całkowitą m_{int} oraz R rzutowanego na element grupy $\mathbb{Z}_q$ poprzez funkcję $f : G \to \mathbb{Z}_q$ (można np. przyjąć porządek z generatora g), oraz następnie zredukowanie tych wartości modulo q:

$$h = ((m_{\text{int}}) \cdot (f(R) \bmod q)) \mod q$$

W bezpiecznym schemacie funkcja h brałaby obie wartości $m \in M$ oraz $R \in G$ w taki sposób, że $h : M \times G \to \mathbb{Z}_q$ oraz charakteryzowałaby się cechami bezpiecznej funkcji skrótu, np. $h = H(m||R)$, gdzie H jest bezpieczną funkcją skrótu.

4 Podpunkt 2

4.1 Polecenie

Sprawdź, czy takie związanie wiadomości z R daje odporność na fałszerstwo, czy tylko pozór związania.

4.2 Rozwiązanie

Związanie $h = mR$ nie daje odporności na fałszerstwo, a jedynie pozór związania, umożliwiając atak `Existential Forgery`.

Przyjmujemy, że fałszerstwo to zdolność do znalezienia **dowolnej wiadomości** m dla której istnieje sposób wyznaczenia (R, s) przechodzący weryfikację, a uzyskany **bez znajomości klucza prywatnego** a. Niech $R \in G$ jest przedstawiony następująco:

$$R = g^x A^y \text{ dla pewnych } x, y \in \mathbb{Z}_q$$

Zobaczmy warunek weryfikacji:

$$g^s = RA^h = g^x A^y A^h = g^x A^{y+h}$$

Chcemy zredukować wykładnik A do postaci $A^0 = 1 (\bmod q)$, aby pozbyć się części wymagającej klucza prywatnego.

$$\begin{aligned} y + h &\equiv 0 \mod q \\ y &\equiv -h \mod q \\ y &\equiv -mR \mod q \\ m &\equiv -yR^{-1} \mod q \end{aligned}$$

Przyjmujemy, że wyznaczenie odwrotności R^{-1} jest w grupie G łatwe, np. na mocy rozszerzonego Algorytmu Euklidesa. Wtedy s jest dany jako $s = x \pmod q$.

Zobaczmy, że dla tak spreparowanej trójki $(m, R, s) = (-yR^{-1}, g^x A^y, x)$ warunek weryfikacji jest spełniony:

$$\begin{aligned} P &= RA^h \\ &= g^x A^y \cdot A^{-mR} \\ &= g^x A^{y+((-yR^{-1})\cdot R)} \\ &= g^x A^{y+(-y\cdot(R^{-1}R))} \\ &= g^x A^{y-y} \\ &= g^x A^0 \\ &= g^x \\ &= g^s = L_\square \end{aligned}$$

Związanie wiadomości z R poprzez funkcję $h = mR$ daje pozór związania, ponieważ h jest w istocie funkcją liniową od R. Zaburza to jedną z kluczowych własności funkcji skrótu h, która powinna być trudna do odwrócenia.

5 Podpunkt 3

5.1 Polecenie

Zbadaj, czy można dobrać podpis dla wybranej wiadomości bez znajomości sekretu a.

5.2 Rozwiązanie

`Universal Forgery Attack` jest w tym wypadku niemożliwy.

Pomimo braku odporności na fałszerstwo, nie można w prosty sposób dobrać podpisu dla wybranej wiadomości bez znajomości sekretu a. Zobaczmy, że jeśli m jest już wybrane to po stronie weryfikatora ustalona jest zależność $h = mR$, a zatem musi zajść weryfikacja:

$$g^s = RA^h = Rg^{amR}$$

Co jest równoznaczne z $g^s = g^{\log_g(R)+amR}$, a zatem $s = \log_g(R) + amR \pmod q$.

Wobec tego musielibyśmy wykorzystać prawdziwą parę (r, R) z relacją $g^r = R$, a to jest niemożliwe z ustalonym m i bez znajomości a, ponieważ R jest elementem grupy G i jego logarytm dyskretny jest trudny do obliczenia. W podpunkcie drugim udało się dobrać podpis, ponieważ akceptowaliśmy arbitralną z punktu widzenia weryfikatora wiadomość m.

6 Podpunkt 4

6.1 Polecenie

Porównaj ten schemat z zadaniem 2: czy problem jest zasadniczo ten sam, czy inny?

6.2 Rozwiązanie

Problem jest zasadniczo ten sam.

W zadaniu drugim prezentowany schemat to $h = m + R$ zamiast $h = mR$. Schematy są błędne ze względu na niepoprawne własności funkcji h, która nie jest bezpieczną funkcją skrótu. W obu przypadkach funkcja h jest złożona z prostych operacji algebraicznych, przez co jest odwracalna.
Możemy w obu przypadkach wykonać atak `Existential Forgery` (tj. w podpunkcie 2):

- Dla $h = m + R$: $m = -y - R \pmod{q}$
- Dla $h = mR$: $m = -yR^{-1} \pmod{q}$

7 Wnioski

Pomimo że schemat jest algebraicznie poprawny, to jednak jest niebezpieczny
- podatny na atak
`Existential Forgery`, czyli dobranie takiej trójki (m, R, s) (bez znajomości klucza prywatnego a), która pozytywnie przechodzi weryfikację.

Schemat jest podatny na atak, ale nie pozwala na wykradnięcie klucza prywatnego a (poza sytuacją, gdy podpisujący powtórzy R dla różnych wiadomości), wobec tego nie jest najgorszym schematem podpisu, wciąż jednak jest niebezpieczny.

Kluczowa dla bezpieczeństwa schematu podpisu jest bezpieczna funkcja skrótu charakteryzująca się odpornością na kolizję oraz trudnością odwracania - uwydatnione w zadaniu, ale również m.in. determinizmem.