Криптосистеми на еліптичних кривих

Lecture 6: Classic Protocols

Грубіян Євген Олександрович

Криптосистеми на еліптичних кривих

- Мотивація: Стійкість сучасних криптосистем базується на складності задачі дискретного логарифму в групах точок еліптичних кривих.
- Основні протоколи:
  - Протокол обміну ключами (ECDH)
  - Шифрування Ель-Гамаля та інкапсуляція ключа
  - Підпис ECDSA
  - Схеми ідентифікації та підпису Шнорра
  - Криптографічні комітменти (Педерсен)

Вибір параметрів для протоколів

- Обираємо(але обережено, з деякими виключеннями) еліптичну криву над полем $\mathrm{F_p}$: $\mathrm{E/F_p}$, так що $|\mathrm{E}(\mathrm{F_p})| = \mathrm{nl}$, де n-велике просте число, l-малий кофактор.
- В якості основної групи G для протоколів беруть просту підгрупу порядку q
- Обираємо генератор групи деяку точку $\mathrm{P} \in \mathrm{G}$

Обмін ключами ECDH

ECDH (обмін ключами):

1. Аліса і Боб обирають секрети (наприклад, a i b).
2. Обмінюються публічними значеннями: $Q_A = [a]P$, $Q_B = [b]P$.
3. Обчислюють спільний секрет: $S = [a]Q_B = [b]Q_A$

Можливі атаки третього посередині (Man-in-The-Middle), а також CCA (Static-Diffie-Hellman attack by Brown, Galant 2004), тому в такому вигляді застосовувати ECDH не можна.
Існують модифікації протоколу, які передбачають автентифікацію та захищають від ряду атак, зокрема 3XDH від Signal:

- Аліса та Боб мають пари довгостроковий (ідентифікаційний) та короткостроковий (ефемерний) ключів:

$$(IK_A = [ik_a]P, EK_A = [ek_a]P) \rightarrow$$
$$\leftarrow (IK_B = [ik_B]P, EK_B = [ek_B]P)$$

- Спільний секрет $S = KDF([ik_a]EK_B, [ek_a]IK_B, [ek_a]EK_B)$

Інкапсуляція ключа ECDH-KEM

Проста KEM-схема на основі ECDH (RFC 5753):

- $\mathrm{KeyGen}(1^\lambda) \to (x_B, Q_B)$, x_B - секретний ключ, $Q_B = [x_B]P$ відкритий ключ Боба
- $\mathrm{Encap}(Q_B) \to (k, C)$, де k - симетричний ключ для шифрування повідомлення, C - інкапсульований (зашифрований) ключ, Аліса:
    1. вибирає симетричний ключ $k \leftarrow_\$$ яким потім шифрує повідомлення (наприклад AES)
    2. генерує деякий ефемерний секрет x_A, відкритий ключ $Q_A = [x_A]P$
    3. обчислює спільний секрет з Бобом: $S = \mathrm{KDF}([x_A]Q_B)$, де KDF - функція виводу ключа, може бути взята як деяка криптографічна геш-функція
    4. інкапсулює(шифрує) симетричним алгоритмом у відповідному режимі значення k: $C_k = \mathrm{Wrap}(S, k)$
    5. повертає $C = (k, (C_k, Q_A))$
- $\mathrm{Decap}(x_B, (C_k, Q_A)) \to k$
    1. знаходимо ефемерний спільний секрет з Алісою: $S = \mathrm{KDF}([x_B]Q_A)$
    2. розшифровуємо (декапсульовуємо) та повертаємо ключ $k = \mathrm{Unwrap}(S, C_k)$, яким розшировуємо потім повідомлення

Схема шифрування Ель-Гамаля

- $\mathrm{KeyGen}(1^\lambda) \to k, Q, \ \ Q = [k]P.$
- Шифрування повідомлення M:

$$\mathrm{Enc}(M, Q) = C = \big([r]P, \ M + [r]Q\big),$$

  де $r \leftarrow_\$$ — випадкове число.
- Розшифрування: $M = \mathrm{Dec}(C, k) = (M + [r]Q) - [k]([r]P).$
- Модель стійкості: Схема є IND-CPA-безпечною, але не є IND-CCA2 стійкою, тому використовуйте з обережністю
- Схема є гомоморфмною:
  $\mathrm{Enc}(M_1 + M_2, Q) = \mathrm{Enc}(M_1, Q) + \mathrm{Enc}(M_2, Q)$ що дає переваги при побудові деяких криптосистем

Підпис за ECDSA

$\mathrm{KeyGen}(1^\lambda) \to d, Q,\ \ Q = [d]P$

Підпис $\mathrm{Sign}(m, d) \to \sigma$

1. Обчислити хеш повідомлення: $e = H(m)$, де H - криптографічна геш-функція
2. Обрати випадкове k і обчислити $R = [k]P = (x_R, y_R)$; визначити $r = x_R \mod n$.
3. Обчислити $s = k^{-1}(e + d\,r) \mod n$ (де d — приватний ключ).
4. Повернути підпис: $\sigma = (r, s)$.

Верифікація $\mathrm{Verify}(\sigma, m) \to \mathrm{bool}$:

1. Обчислити хеш повідомлення: $e = H(m)$
2. Обчислити $w = s^{-1} \mod n$, $u_1 = e\,w \mod n$, $u_2 = r\,w \mod n$.
3. Обчислити $R' = [u_1]P + [u_2]Q$ та перевірити $r \equiv x_{R'} \mod n$.

Моделі стійкості:

- ECDSA забезпечує стійкість до екзистинційних підробок підпису (EUF-CMA) в моделі з випадковим оракулом

Недоліки ECDSA та атаки

Малітабельність підпису:

- Якщо (r, s) є валідним підписом, то $(r, -s \mod n)$ також є валідним підписом для того ж повідомлення.
- Це створює проблему малітабельності, оскільки підпис можна «перевернути», не змінюючи повідомлення.

Атака на повторне використання r: Нехай два підписи (r, s_1) і (r, s_2) на різні повідомлення m_1, m_2 з однаковим значенням k:

$$s_1 \equiv k^{-1}(e_1 + d\,r) \pmod n, \; s_2 \equiv k^{-1}(e_2 + d\,r) \pmod n.$$

$$s_1 - s_2 \equiv k^{-1}(e_1 - e_2) \pmod n \Rightarrow k = (e_1 - e_2)/(s_1 - s_2) \mod n$$

Далі зловмисник обчислює приватний ключ $d = r^{-1}(ks_1 - e_1)$
Висновок: криптосистема ECDSA дуже чутлива до якості випадковості

Схема ідентифікації Шнорра та підпису Шнорра

Протокол ідентифікації Шнорра

Prover переконує Verifier що він знає деяке x не розкриваючи його

$$
\begin{aligned}
\text{Prover} : x, Q = [x]P &\xrightarrow{Q} \text{Verifier} : Q \\
r \in_\$ \mathbb{Z}_n, R = [r]P &\xrightarrow{R} \\
&\xleftarrow{c} c \in_\$ \mathbb{Z}_n \\
s = xc + r \mod n &\xrightarrow{s} [s]P \stackrel{?}{=} R + [c]Q
\end{aligned}
$$

Схема ідентифікації Шнорра є доказом знання (PoK) дискретного логарифму з нульовим розголошенням в моделі з випадковим оракулом та є найпростішим Σ-протоколом.

Застосовуючи перетворення Фіат-Шаміра (перехід до неінтерактивного протоколу + додаємо в транскрипт повідомлення m, моделюємо випадковий оракул критографічною геш-функцією H): $c = H(R \| m)$ отримуємо схему підпису

Підпис Шнорра

- $\mathrm{KeyGen}(1^\lambda) \to (x, Q),\ \ Q = [x]P$
- $\mathrm{Sign}(x, m) \to (R, s)$
  1. Підписувач обирає випадкове $r \in_\$ \mathbb{Z}_n$ та обчислює $R = [r]P,\ \ e = H(R \,\|\, m)$
  2. Обчислює $s = xe + r$
  3. Публікує пару $\sigma = (e, s)$ (або альтернативно пару $\sigma = (R, s)$) як підпис повідомлення m
- $\mathrm{Verify}(\sigma, m) \to \mathrm{bool}$: перевіряючий обчислює $R_v = [s]P - [e]Q$ та перевіряє виконання рівності $e \stackrel{?}{=} H(R_v \,\|\, m)$ або $R_v \stackrel{?}{=} R$ в альтернативному варіанті
- Підпис Шнорра забезпечує сильну екзистенційну стійкість до підробок sEUF-CMA в моделі з випадковим оракулом.
- Підпис Шнорра дозволяє вкорочувати значення e, таким чином формуючи коротші підписи
- Дозволяє агрегувати відкриті ключі (в альтернативному варіанти) та формувати коротший підпис під одним і тим же повідомленням: $\mathrm{Sign}(x_1, m) + \mathrm{Sign}(x_2, m) = \mathrm{Sign}(x_1 + x_2, m)$

Криптографічні комітменти (Педерсен)

Комітмент Педерсена:

- Для значення v (наприклад, суми) та випадкового r обираються генератори G та H.
- Комітмент задається як:

$$\mathrm{C} = [\mathrm{v}]\mathrm{G} + [\mathrm{r}]\mathrm{H}.$$

Властивості:

- Прихованість: Без знання r важко відновити v.
- Обов'язковість: Коммітер не може підмінити іншу пару (v, r) при відкритті коммітменту.
- Гомоморфізм: $\mathrm{C}_1 + \mathrm{C}_2 = [\mathrm{v}_1 + \mathrm{v}_2]\mathrm{G} + [\mathrm{r}_1 + \mathrm{r}_2]\mathrm{H}$.

Вибір параметрів

Практичні рекомендації:

- Для рівня стійкості 1^λ слід обрати еліптичну криву з розміром простої підгрупи 2λ біт.
- Якщо в протоколах підпису використовується неякісне джерело випадковості слід розглянути використання детерміністичного генератора PRNG, що ініціюється значеннями $H(m), sk$, наприклад схему, що описана в RFC7969.
- Слід уникати слабких кривих (в яких задача DLP вирішується ефективніше ніж класичні алгоритми), наприклад для яких $n | p^r - 1$, де l - невелике число (так звана MOV-атака $E(F_p) \subseteq F^*_{p^r}$), багато суперсингулярних кривих також є слабкими.
- Приклади:
  - Стандарти NIST.SP800.186, ANSI X9.62, X9.63, ДСТУ4145-2002
  - Криві від спільноти: Curve25519, Brainpool та багато інших
  - Ось невелика база з кривими https://neuromancer.sk/std/

Підсумки лекції

- Еліптичні криві - важливий будівельний блок дуже багатьох криптографічних протоколів.
- Більшість припущень стійкості класичних криптосистем зводяться до складності задачі дискретного логарифмування (ECDLP) (що в свою чергу зводиться до задачі знаходження прихованої підгрупи HSP).
- Еліптичні криві дають найменші ключі серед аналогічних протоколів в інших групах, достатньо працювати в 256-бітному порядку кривої для стійкості на рівні 128 біт.
- Окрім класичних існує ряд інших криптосистем на основі еліптичних кривих, з якими познайомимось на наступних лекціях