Сравнительный обзор схем личностного шифрования, использующих билинейные отображения конечных групп

Гуселев Антон Михайлович, ТК 26
Косолапов Дмитрий Олегович, к.ф.-м.н., ЕМС

Москва
2015 г.

Введение

В 1984 году Ади Шамир представил новую концепцию защиты данных, получившую название личностная криптография (Identity-Based Cryptography).

Для получения закрытых/открытых ключей зашифрования/расшифрования и/или выработки/проверки подписи возможно использовать личную информацию пользователей.

Общая схема личностного шифрования

Основные участники:

Генератор секретных ключей (**ГСК**), абоненты **A** и **B**.

Подготовительный этап.

1. **ГСК** формирует набор системных параметров ($parms$), а также закрытый и открытый ключи (msk, mpk).
2. **ГСК** публикует системные параметры $parms$ и открытый ключ mpk.
3. Абонент **B** передает в **ГСК** свой идентификатор $\mathtt{ID}_B$.
4. **ГСК** формирует $\mathcal{D}_{\mathtt{ID}_B}$ закрытый ключ абонента **B**.

Общая схема личностного шифрования

Передача сообщения Msg.

1. Абонент **A** вычисляет шифрсообщение

$$\mathrm{c} = \mathtt{Enc}(\mathrm{Msg}, \mathtt{ID}_B, \mathit{mpk}).$$

2. Абонент **A** передает c абоненту **B**.
3. Абонент **A** расшифровывает полученное сообщение

$$\mathrm{Msg} = \mathtt{Dec}(\mathrm{c}, \mathcal{D}_{\mathtt{ID}_B}).$$

Билинейное отображение

Определение

Пусть $(\mathbb{G}, +)$ – аддитивная группа порядка p, $(\mathbb{F}, \cdot)$ – мультипликативная группа порядка p, где p – простое. Билинейным называется отображение

$$\hat{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{F},$$

которое обладает следующими свойствами

- билинейность: $\hat{e}(aR_1, bR_2) = \hat{e}(R_1, R_2)^{ab}$, где $R_1, R_2 \in \mathbb{G}$ и $a, b \in \mathbb{Z}_q^*$.
- невырожденность: $\forall R \in \mathbb{G}^* : \hat{e}(R, R) \neq 1$.
- эффективная вычислимость: Для всех $R_1, R_2 \in \mathbb{G}$ отображение $\hat{e}(R_1, R_2)$ эффективно вычислимо (на ЭВМ).

Пример: схема BasicIdent

Подготовительный этап

1. **ГСК** определяет:
   - группу $\mathbb{G}$, порожденную $Q \in \mathbb{G}^*$;
   - билинейное отображение $\hat{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{F}$;
   - две хэш-функции $\mathsf{H}_1 : \{0,1\}^* \to \mathbb{G}^*$ и $\mathsf{H}_2 : \mathbb{F} \to \{0,1\}^\delta$, где δ – длина открытого текста (параметр стойкости);
   - число $s \in_R \mathbb{Z}_q^*$, в соответствии с которым вычисляется $\mathcal{R} = sQ$.

   В рамках схемы $msk = s$, $mpk = \mathcal{R}$.
2. **ГСК** публикует Q, описание групп $\mathbb{G}$ и $\mathbb{F}$, отображение $\hat{e}$, хеш-функции H_1, H_2 и открытый ключ mpk.
3. Получатель, **B**, получает из **ГСК** секретный ключ $\mathcal{D}_B = sM_{\mathtt{ID}_B}$, где $M_{\mathtt{ID}_B} = \mathsf{H}_1(\mathtt{ID}_B)$.

Общая схема личностного шифрования

Передача сообщения Msg.

1. Отправитель, **A**, с использованием идентификатора **B** $\mathtt{ID}_B$, зашифровывает сообщение $\mathrm{Msg} \in \{0,1\}^\delta$. Для этого случайно выбирает $r \in_R \mathbb{Z}_q^*$ и вычисляет

$$\mathrm{c}_1 = rQ,$$
$$\mathrm{c}_2 = \mathsf{H}_2(\hat{e}(M_{\mathtt{ID}_B}, \mathcal{R})^r) \oplus \mathrm{Msg}.$$

2. **A** передает **B** шифрсообщение $\mathrm{c} = (\mathrm{c}_1, \mathrm{c}_2)$.
3. **Б** расшифровывает c, вычисляя для этого

$$\mathrm{Msg} = \mathrm{c}_2 \oplus \mathsf{H}_2(\hat{e}(\mathcal{D}_B, \mathrm{c}_1)).$$

Теоретико-сложностные задачи

- Билинейная задача Диффи-Хеллмана (Bilinear Diffie-Hellman problem, BDH) $\sim$ Вычислительная билинейная задача Диффи-Хеллмана (Computational Bilinear Diffie-Hellman problem, CBDH).
- Билинейная инверсионная задача Диффи-Хеллмана (Bilinear Diffie-Hellman Inversion problem, k-BDHI).
- Билинейная распознавательная задача Диффи-Хеллмана (Decisional Bilinear Diffie-Hellman problem, DBDH).

Билинейная задача Диффи-Хеллмана

Определение

Заданы две группы $\mathbb{G}$ и $\mathbb{F}$ простого порядка q и P образующий элемент $\mathbb{G}$. Задано билинейное отображение $\hat{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{F}$. Тогда билинейная задача Диффи-Хеллмана (BDH) над $(\mathbb{G}, \mathbb{F}, \hat{e})$ состоит в следующем:

Для некоторых $a, b, c \in \mathbb{Z}_q^*$ даны $\langle P, aP, bP, cP \rangle$. Необходимо вычислить $\hat{e}(P, P)^{abc} \in \mathbb{F}$.

Билинейная инверсионная задача Диффи-Хеллмана

Определение

Заданы две группы $\mathbb{G}$ и $\mathbb{F}$ простого порядка q и P образующий элемент $\mathbb{G}$. Задано билинейное отображение $\hat{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{F}$ и набор $(P, aP, a^2P, \ldots, a^kP) \in (\mathbb{G}^*)^{k+1}$, где P – элемент группы $\mathbb{G}$. Задача заключается в вычислении элемента $\hat{e}(P, P)^{(1/a)} \in \mathbb{F}^*$.

Билинейная распознавательная задача Диффи-Хеллмана

Определение

Пусть заданы две группы $\mathbb{G}$ и $\mathbb{F}$ простого порядка p. Заданы билинейное отображение $\hat{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{F}$, образующий элемент $P \in_R \mathbb{G}$ и некоторый случайный элемент $Q \in_R \mathbb{F}$. Тогда говорится, что алгоритм $\mathcal{A}(\epsilon)$ (ϵ – параметр алгоритма), на выходе которого может быть получено значение $\gamma = 0, 1$, способен разрешить билинейную распознавательную задачу Диффи-Хеллмана над $(\mathbb{G}, \mathbb{F}, \hat{e})$, если для случайных элементов $a, b, c \in \mathbb{Z}_p^*$ выполняется:

$$|\Pr[\mathcal{A}(P, aP, bP, cP, \hat{e}(P, P)^{abc}) = 1] - \\ - \Pr[\mathcal{A}(P, aP, bP, cP, Q) = 1]| \geq \epsilon,$$

где $\Pr[A]$ – вероятность события A. Вероятность вычисляется при условии, что бит, получаемый на выходе алгоритма $\mathcal{A}$, является случайным.

Адаптивные атаки на схемы личностного шифрования

- Стойкость относительно атаки на основе адаптивно подобранных идентифицирующей информации и шифрованного текста (Indistinguishability under adaptive identity and adaptive chosen ciphertext attack, IND-ID-CCA2).
- Стойкость относительно атаки на основе адаптивно подобранных выбранной идентифицирующей информации и шифрованного текста (Indistinguishability under selective adaptive identity and adaptive chosen ciphertext attack, IND-sID-CCA2).

Некоторые критерии сравнения схем личностного шифрования

1. Открытые параметры, публикуемые ГСК.
2. Закрытые параметры, вырабатываемые ГСК.
3. Закрытые параметры пользователя.
4. Хэш-функции.
5. Вычислительная эффективность на интерактивных этапах (операции).
6. Вид и размер шифртекста.
7. Модель, в рамках которой оценивается стойкость.
8. Базовая теоретико-сложностная задача.

Схемы личностного шифрования

- Схема Боне-Франклина (BasicIdent);
- Модификация схемы Боне-Франклина № 1 (BF, FullIdent(-1));
- Модификация схемы Боне-Франклина № 2 (FullIdent-2);
- Модификация схемы Боне-Франклина № 3 (NewFullIdent);
- Сакаи-Казахары (SK);
- Схема Боне-Бойен в стандартной модели (BBSM);
- Схема Боне-Бойена (BB(-1));
- Схема Вотерса в стандартной модели (WSM);

Выбор схемы

Среди рассмотренных схем привлекательными с точки зрения стойкости являются схемы Боне-Бойен в стандартной модели (BBSM) и Вотерс в стандартной модели (WSM), однако они являются вычислительно неэффективными и, кроме того, обладают большим набором генерируемых на этапе инициализации параметров.

Фактический выбор

	BF	**SK**	**BB-1**
Стойкость	IND-ID-CCA2	IND-ID-CCA2	IND-sID-CPA2
Модель	сл. оракул	сл. оракул	сл. оракул
Задача	BDH	k-BDHI	DBDH

Основные различия

Известно, что сложность k-BDHI задачи эквивалентна сложности BDH задачи при $k = 1$. При этом k-BDHI задача является более простой, чем BDH при $k > 1$.

При $k > 1$ предположение стойкости схемы SK k-BDHI является более слабым, чем аналогичное BDH для схемы BF. При этом, в случае $k = 1$ предположения стойкости обоих схем эквивалентны.

Основные различия

	BF	SK	BB-1
Билин. отобр. зашифр./расшифр.	1/1	0/1	0/2
Возв. в степ. зашифр./расшифр.	1/0	1/0	1/1
Хэш-финкции зашифр./расшифр.	4/3	4/3	2/0
Вид ш.т.	$\langle \mathbb{G}, \{0,1\}^\delta, \{0,1\}^\delta \rangle$	$\langle \mathbb{G}, \{0,1\}^\delta, \{0,1\}^\delta \rangle$	$\langle \{0,1\}^\delta, \mathbb{G}, \mathbb{G} \rangle$
Закр. ключ ГСК	$\mathbb{Z}_p^*$	$\mathbb{Z}_p^*$	$\langle \mathbb{Z}_p, \mathbb{Z}_p, \mathbb{Z}_p \rangle$
Отображение ID	группа	поле	поле
Закр. ключ ID	$\mathbb{G}$	$\mathbb{G}$	$\langle \mathbb{G}, \mathbb{G} \rangle$

Компромисс

Схема SK является вычислительно более эффективной, чем схема BF, при этом ее стойкость основана на более простой задаче, чем стойкость схемы BF.

СПАСИБО ЗА ВНИМАНИЕ!