Сложностная криптография

Эдуард Алексеевич Гирш

http://logic.pdmi.ras.ru/~hirsch

ПОМИ РАН

6 апреля 2008 г.

Общая картина

one-way functions

Общая картина

one-way functions

$\Updownarrow$

PRG, prff, uowhff

$\Updownarrow$

private-key cryptosystems

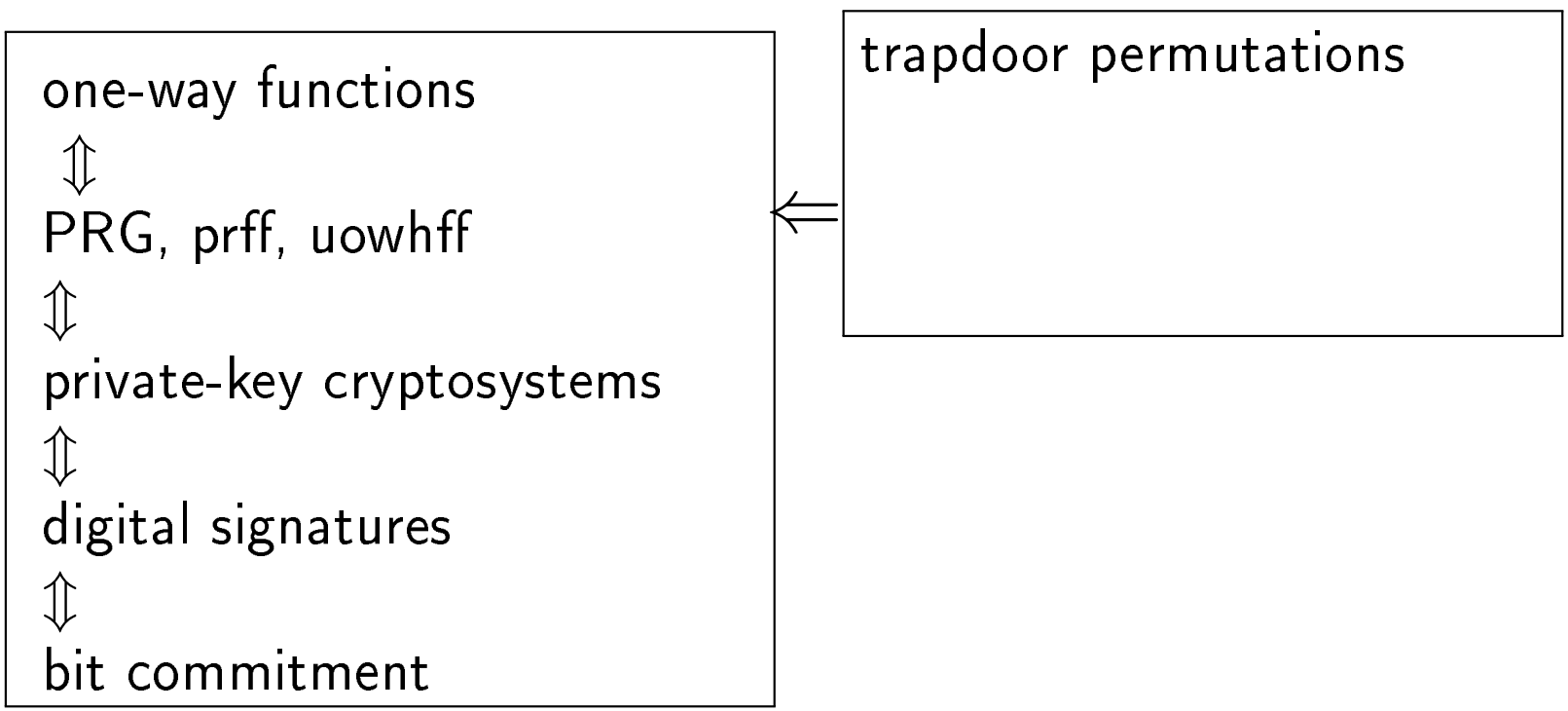
$\Updownarrow$

digital signatures

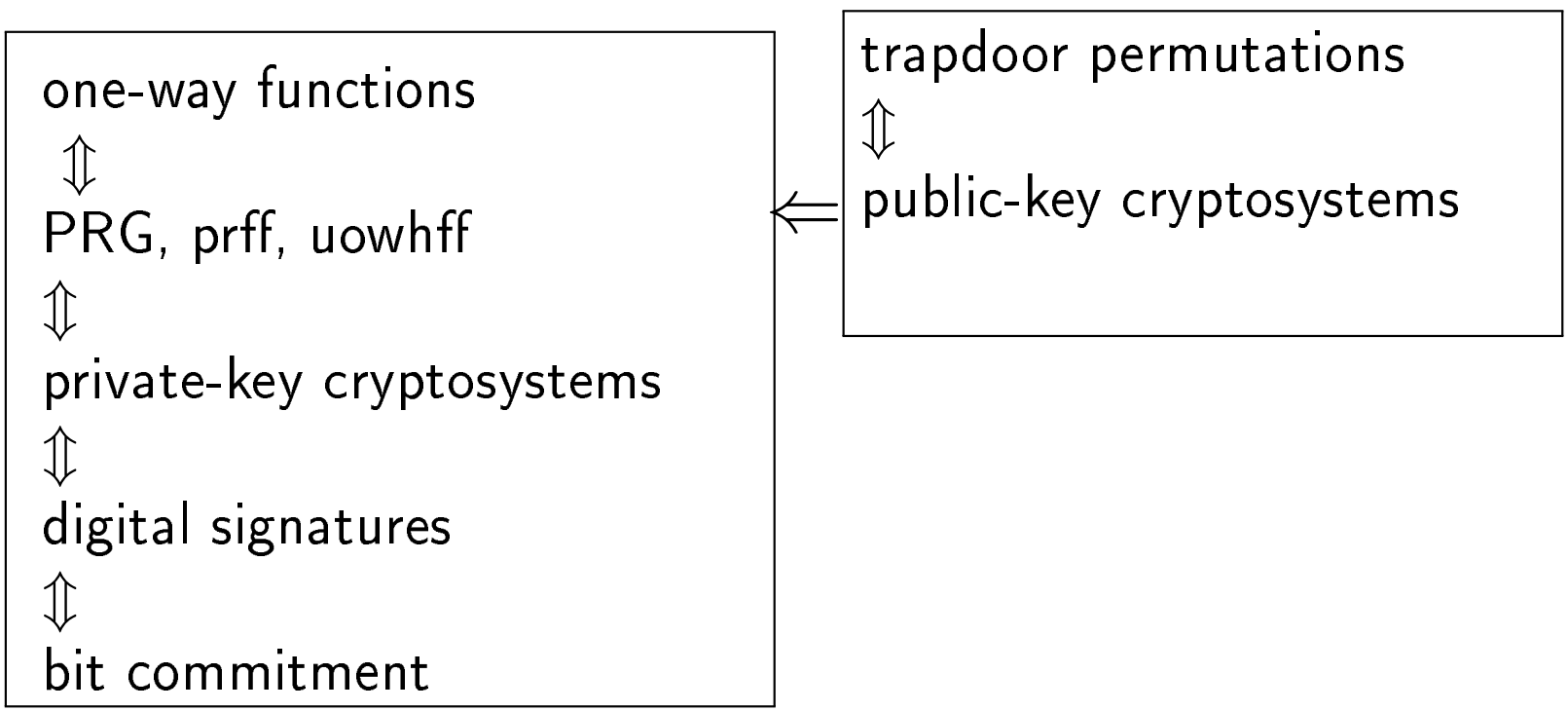
$\Updownarrow$

bit commitment

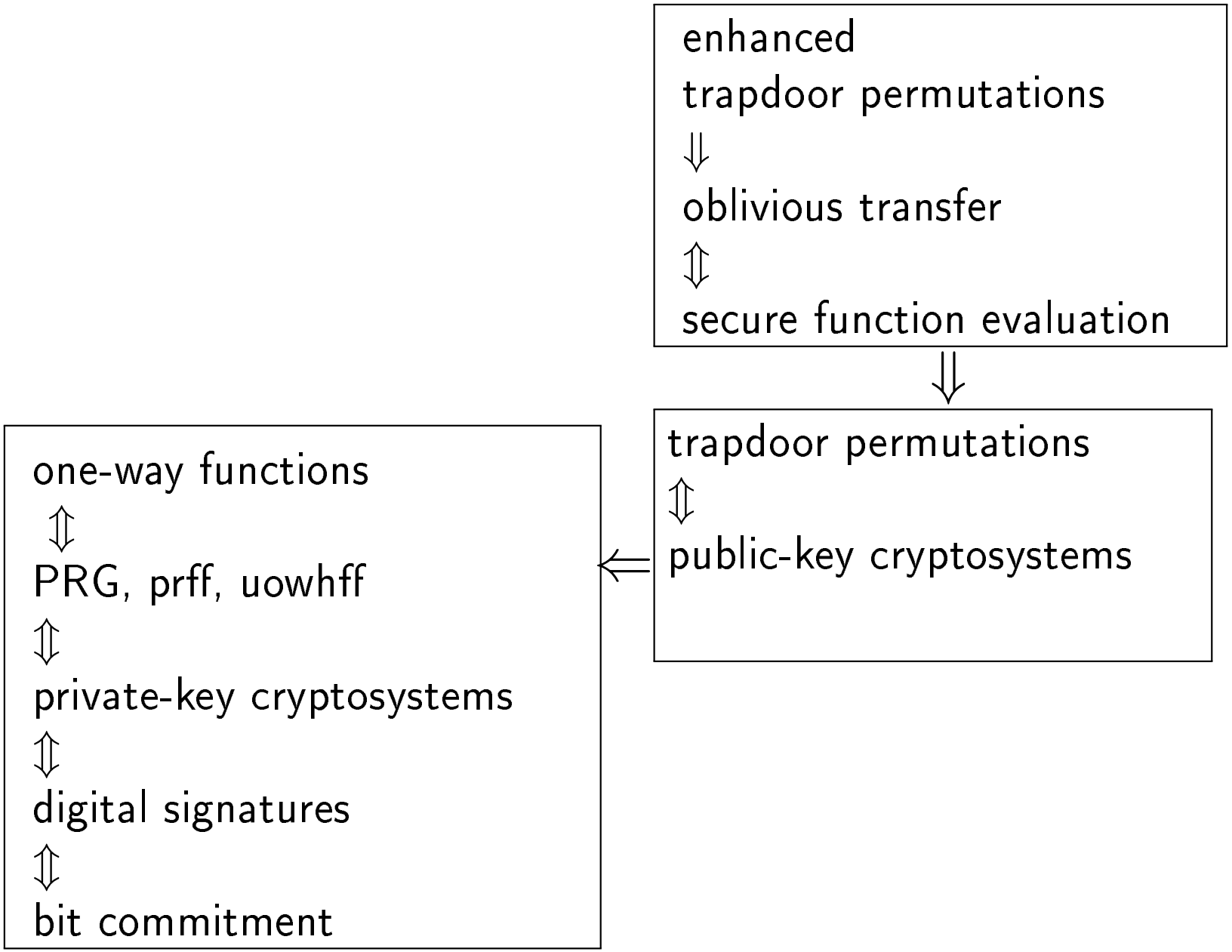
Общая картина



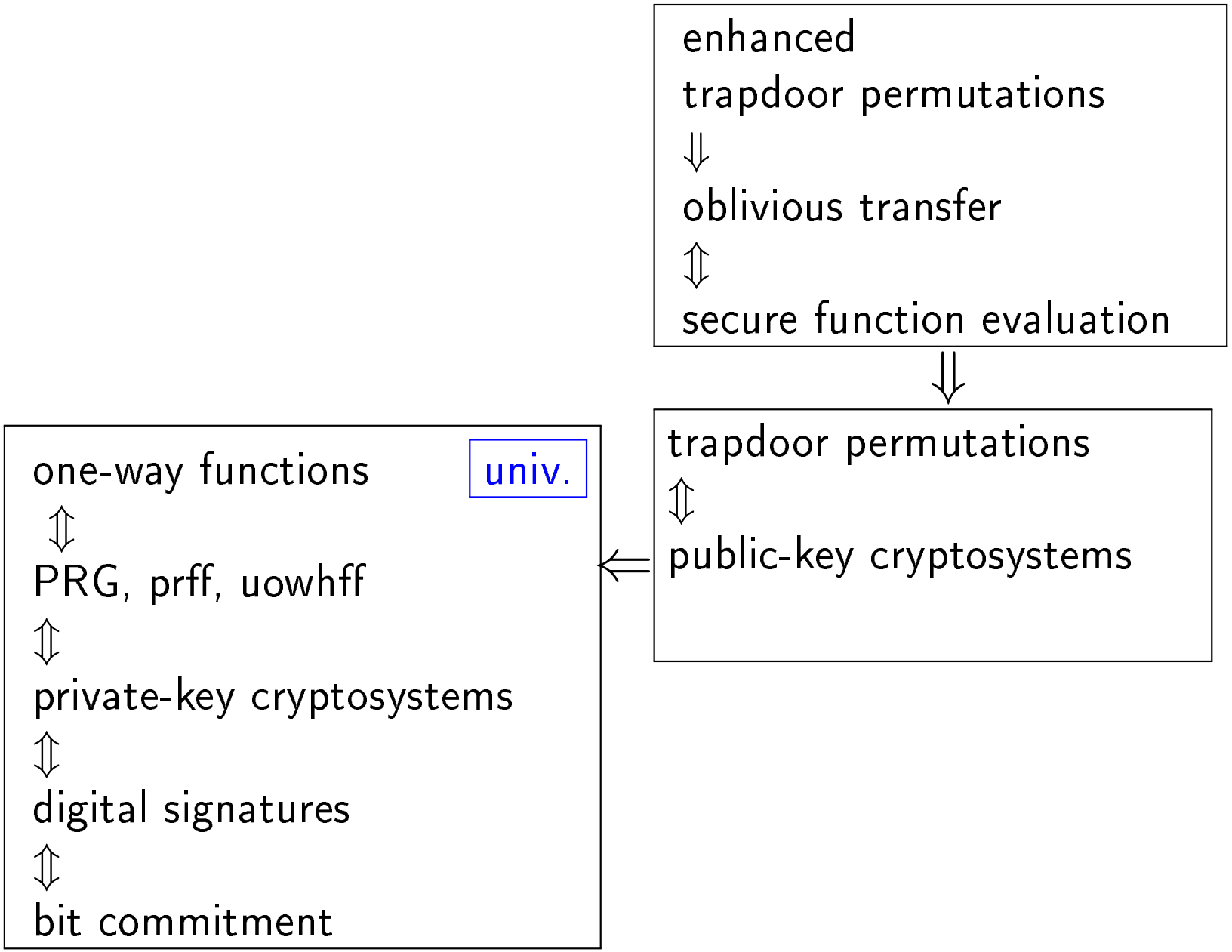
Общая картина



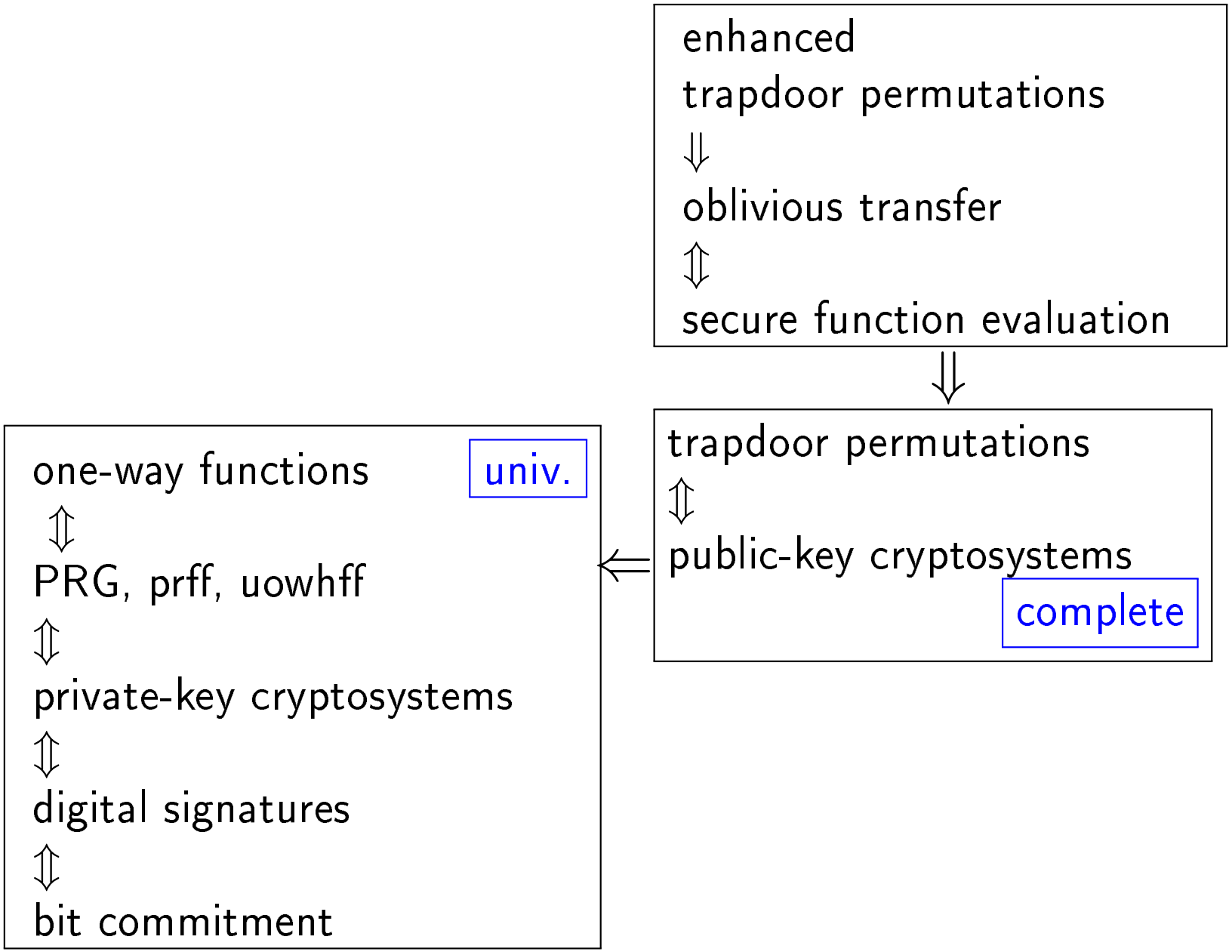
Общая картина



Общая картина



Общая картина



Криптосистемы с открытым ключом

. . . кодирующие 1 бит

Определение

δ-корректная криптосистема с открытым ключом (δ-PKCS) — это полиномиальный по времени алгоритм $G: (1^n, r_g) \mapsto (e, d)$, (порождающий булевы схемы "надёжности n"), т.ч.

- $e: (\mathtt{msg}, r_e) \mapsto \mathtt{code}$,
- $d: \mathtt{code} \mapsto \mathtt{msg}$.
- $\forall \mathtt{msg} \in \{0,1\} \qquad \Pr_{r_e, r_g}\{d(e(\mathtt{msg}, r_e)) = \mathtt{msg}\} \geq \delta$.

Определение

δ-PKCS *надёжна*, если $\forall$ ВПМТ A $\forall k \in \mathbb{N}$ $\exists N$ $\forall n > N$

$$\Pr\{A(e(\mathtt{msg}, r_e), 1^n, e) = \mathtt{msg}\} < \frac{1}{2} + \frac{1}{n^k},$$

где $G(1^n, r_g) = (e, d)$, а вероятность берётся по случайным числам, используемым A, и по (равномерно распределённым) r_g, r_e и $\mathtt{msg}$.

Криптосистемы с открытым ключом

. . . кодирующие 1 бит

Определение

δ-корректная криптосистема с открытым ключом (δ-PKCS) — это полиномиальный по времени алгоритм $G: (1^n, r_g) \mapsto (e, d)$, (порождающий булевы схемы "надёжности n"), т.ч.

- $e: \{0,1\}^{1+r(n)} \to \{0,1\}^{c(n)}$,
- $d: \{0,1\}^{c(n)} \to \{0,1\}$,
- $\forall \mathtt{msg} \in \{0,1\} \qquad \Pr_{r_e, r_g}\{d(e(\mathtt{msg}, r_e)) = \mathtt{msg}\} \geq \delta$.

Определение

δ-PKCS *надёжна*, если $\forall$ ВПМТ A $\forall k \in \mathbb{N}$ $\exists N$ $\forall n > N$

$$\Pr\{A(e(\mathtt{msg}, r_e), 1^n, e) = \mathtt{msg}\} < \frac{1}{2} + \frac{1}{n^k},$$

где $G(1^n, r_g) = (e, d)$, а вероятность берётся по случайным числам, используемым A, и по (равномерно распределённым) r_g, r_e и $\mathtt{msg}$.

Сведéния

Определение

$G_1 \rightsquigarrow G_2$, если $\exists T^\bullet \;\; \forall k_f \;\; \exists k_g \;\; \forall$ оракула A

$$A \text{ взламывает } G_2 \text{ с вероятностью } \frac{1}{2} + \frac{1}{n^{k_2}} \quad \Rightarrow$$
$$T^A \text{ взламывает } G_1 \text{ с вероятностью } \frac{1}{2} + \frac{1}{n^{k_1}}.$$

Здесь T — полиномиальный вероятностный алгоритм, A используется как вероятностный оракул (его случайные биты учитываются при запуске T^A).

Определение

$\frac{2}{3}$-PKCS G^* — полная PKCS с ограниченной ошибкой, если $\forall \frac{2}{3}$-PKCS G

$$G \rightsquigarrow G^*.$$

G^* — “самая надёжная”:

$\exists$надёжная PKCS с ошибкой $\Longrightarrow$ G^* — надёжная.

Увеличение корректности

Докажем, что всякая $\frac{2}{3}$-PKCS сводится к $(1 - \frac{1}{8n})$-PKCS, так что можно ограничиться только последними.

Доказательство.

$G^{(t)}$ запускает старый G t раз, порождает схемы, состоящие из t старых схем, кодирующих один и тот же бит много раз:

$$e(b, r) = (e_1(b, r_1), e_2(b, r_2), \ldots, e_t(b, r_t)).$$

При декодировании взять by majority.

□

Увеличение корректности

Докажем, что всякая $\frac{2}{3}$-PKCS сводится к $(1 - \frac{1}{8n})$-PKCS, так что можно ограничиться только последними.

Доказательство.

$G^{(t)}$ запускает старый G t раз, порождает схемы, состоящие из t старых схем, кодирующих один и тот же бит много раз:

$$e(b, r) = (e_1(b, r_1), e_2(b, r_2), \ldots, e_t(b, r_t)).$$

При декодировании взять by majority.
Корректность: неравенство Чернова:

$$\Pr\left\{\sum X_i \leq t/2\right\} = \Pr\left\{\sum X_i \leq (1 - 1/2) \cdot 2t/3\right\} < 2^{-\Omega(t)},$$

где $X_i = \{d_i(e_i(b)) = b\}$.
Остаётся показать сведéние (т.е., надёжность). □

Увеличение корректности

Сведение

Нам дали зашифрованное сообщение code для системы G. Сведение:

1. Выбрать случайное $i^* \in [1\,..\,t]$.
2. Сгенерировать ключи (e_i, d_i) для всех $i \neq i^*$.
3. Дать противнику A для $G^{(t)}$ взломать $(e_1(0), \ldots, e_{i^*-1}(0), \text{code}, e_{i^*+1}(1), \ldots, e_t(1))$.

$$\Pr\{\text{успеха}\} = \frac{1}{2}\Pr\{\text{усп.для 1}\} + \frac{1}{2}\Pr\{\text{усп.для 0}\} =$$

$$= \frac{1}{2}\left(\frac{1}{t}\Pr\{A(e_{1..t}(1)) = 1\} + \sum_{i=2}^{t}\frac{1}{t}\Pr\{A(e_{1..i^*-1}(0), e_{i^*..t}(1)) = 1\}\right) +$$

$$+ \frac{1}{2}\left(\sum_{i=1}^{t-1}\frac{1}{t}\Pr\{A(e_{1..i^*}(0), e_{i^*+1..t}(1)) = 0\} + \frac{1}{t}\Pr\{A(e_{1..t}(0)) = 0\}\right) =$$

$$= \frac{1}{2t}\left(\Pr\{A(e_{1..t}(1)) = 1\} + \Pr\{A(e_{1..t}(0)) = 0\}\right) + \frac{t-1}{t}\cdot\frac{1}{2} >$$

$$> \frac{1}{2t}\cdot 2\left(\frac{1}{2} + \epsilon\right) + \frac{t-1}{t}\cdot\frac{1}{2} = \left(\frac{1}{2t} + \frac{\epsilon}{t}\right) + \left(\frac{1}{2} - \frac{1}{2t}\right) = \frac{1}{2} + \epsilon/t,$$

Сертификация PKCS

Проверка корректности PKCS:
n раз сгенерировать e и d и попробовать применить $d(e(b))$.
Если доля неверных ответов — менее $\frac{1}{6n}$, PKCS признаётся корректной.

По неравенству Чернова
$(1 - \frac{1}{8n})$-PKCS проходит этот тест с вероятностью $1 - 2^{-\Omega(n)}$, а
не-$(1 - \frac{1}{4n})$-PKCS — с вероятностью $2^{-\Omega(n)}$.

При запуске генератора достаточно дать ему поработать n^5 шагов.
Действительно, всякая криптосистема G, работающая полиномиальное время $O(n^k)$, сводится к криптосистеме, работающей время $O(n^2)$: новый генератор $G'(1^n) = G(1^{n^{1/k}})$. Последняя же, как мы доказали, сводится к системе G'' с совсем малой ошибкой с увеличением времени до $O(n^4)$. Только такие “хорошие” системы нас и интересуют.

Конструкция полной PKCS

При параметре надёжности n генератор сертифицирует часть из "первых" n PKCS:

- $G^* = \{G_i\}_{i \in I}$.

Кодирование $e(b)$:

- выбираем случайные биты $(b_i)_{i \in I}$,
- $e(b) = \left((e_i(b_i))_{i \in I}\ ,\ b \oplus \bigoplus_{i \in I} b_i\right)$,

Декодирование:

- $d\left((c_i)_{i \in I}, \beta\right) = \beta \oplus \bigoplus_{i \in I} d_i(c_i)$.

Корректность очевидна, если $(1 - \frac{1}{4n})$-корректна каждая G_i.

Надёжность: b_i независимы и нужны все, так что для взлома надо взломать все G_i, кодирующие случайные биты.
Формально: для сведения G_i сами осуществляем кодирование во всех остальных системах.

Экзамен

A1. Сильные и слабые односторонние функции и семейства. Эквивалентность.
A2. Универсальная односторонняя функция.
A3. Трудный бит. Теорема Голдрейха-Левина.
A4. Псевдослучайные генераторы. Эквивалентность существования PRG и односторонних функций/перестановок.
A5. Семейства псевдослучайных функций. Построение из PRG.

B1. Семейства функций с секретом. Криптосистемы с открытым ключом. Надёжность, в т.ч. при взломе серии сообщений. Конструкция на основе перестановок с секретом.
B2. Криптосистемы с общим ключом. Надёжность. Конструкция на основе семейства псевдослучайных функций.
B3. Цифровые подписи. Надёжность. Конструкция одноразовой ограниченной цифровой подписи на основе односторонней функции. Конструкция многоразовой подписи из одноразовой на основе prff (без док-ва).
B4. Хеш-функции без коллизий, универсальные хеш-функции. Конструкции неограниченных цифровых подписей из ограниченных.
B5. Привязка к биту: конструкции неинтерактивного и интерактивного протоколов.
B6. Oblivious transfer и совместное вычисление функций пассивно честными противниками.
B7. Полная PKCS.