Предъявление полной сильной односторонней функции, перспективной с практической точки зрения

Наумов Сергей, 544 гр.

19 мая 2008 г.

Научный руководитель - А. А. Кожевников
Рецензент - Д. Ю. Булычев, С. И. Николенко ?

Краткая история и суть криптографии

- Криптография с закрытым ключом.

Краткая история и суть криптографии

- Криптография с закрытым ключом.
- Криптография с открытым ключом, 1976 год.

Краткая история и суть криптографии

- Криптография с закрытым ключом.
- Криптография с открытым ключом, 1976 год.
- Принцип Керкхоффа.

Краткая история и суть криптографии

- Криптография с закрытым ключом.
- Криптография с открытым ключом, 1976 год.
- Принцип Керкхоффа.
- Полные конструкции.

Открытые проблемы криптографии

- Большинство утверждений в криптографии постороены на предположении о существовании односторонних функций.

Открытые проблемы криптографии

- Большинство утверждений в криптографии постороены на предположении о существовании односторонних функций.
- Даже в этом предположении не предъявлено конкретного кода односторонней функции или ослабленных аналогов.

Открытые проблемы криптографии

- Большинство утверждений в криптографии постороены на предположении о существовании односторонних функций.
- Даже в этом предположении не предъявлено конкретного кода односторонней функции или ослабленных аналогов.
- Как следствие ни для одной из функций, используемых на практике, не доказана их односторонность.

Открытые проблемы криптографии

- Большинство утверждений в криптографии постороены на предположении о существовании односторонних функций.
- Даже в этом предположении не предъявлено конкретного кода односторонней функции или ослабленных аналогов.
- Как следствие ни для одной из функций, используемых на практике, не доказана их односторонность.
- В теоретической криптографии большой интерес представляют полные односторонние функции, однако пока что они абсолютно неприменимы на практике.

Определение односторонней функции

Определение

Функция f - сильная односторонняя (strong one-way), если
1. $\exists A$ - детерминированный, полиномиальный по времени, такой что $\forall x$ - входа $A(x) = f(x)$.

$$2.\ \forall A'\ \forall p\ \exists N : \forall n > N \Pr_{x \in U_n}(A'(f(x), 1^n) \in f^{-1}f(x)) < \frac{1}{p(n)}.$$

Определение

Функция f - слабая односторонняя (weak one-way), если
1. $\exists A$ - детерминированный, полиномиальный по времени, такой что $\forall x$ - входа $A(x) = f(x)$.

$$2.\ \exists p\ \forall A'\ \exists N : \forall n > N \Pr_{x \in U_n}(A'(f(x), 1^n) \notin f^{-1}f(x)) > \frac{1}{p(n)}$$

Теоремы о композиции

Теорема (С. Наумов)

Пусть f - сильная односторонняя, g - полиномиально вычислимая, регулярная по длине, инъекция, увеличивает длину не больше чем на $O(\log_2 n)$.
Тогда $f(g)$ - сильная односторонняя.

Теорема (С. Наумов)

Пусть f - сильная односторонняя, регулярная по длине, g - полиномиально вычислимая, инъекция, тогда $g(f)$ - сильная односторонняя.

Увеличение числа односторонних функций

Лемма

Пусть односторонние функции существуют, то есть $\exists N \exists x : |x| = N \wedge x = Code(f) \wedge f$ *- односторонняя, и пусть* g *- функция, умножающая вход на число, записанное на второй ленте, и* $|Code(g)| = \alpha$*, тогда* $\forall n : n > N + \log_2 N + \alpha$

$$\Pr_{x \in \{0,1\}^n}(x \in \{x_i : x_i = Code(f_i) \wedge f_i \text{ - one-way}\}) \geq 2^{-(N+\alpha+\log n)}$$

Лемма

$$\exists p \; \exists M : \forall n > M \quad \Pr_{x \in \{0,1\}^n}(x = Code(f) \wedge f \text{ - one-way }) > \frac{1}{p(n)}.$$

Полная односторонняя функция - односторонняя

Теорема (С. Наумов)

Пусть односторонние функции существуют. Тогда любая полная односторонняя функция - односторонняя, если вход моделируемой MT использовать не только как вход, но и как сам код моделируемой MT, то есть можно считать, что $x = Code(f)$*, и если* U *- полная односторонняя, то* $U(x, x)$ *- слабая односторонняя.*

Диагонализированная полная односторонняя-инъекция?

Лемма

Пусть U - полная односторонняя функция, увеличивающая длину максимум в $c(n)$ раз. Обозначим за D_n множество возможных значений функции $U(x,x)$, где $x \in U_n$, то есть $D_n = \bigcup_{k \le c \cdot n} U_k$.

Также пусть $\forall x \in U_n \quad \Pr(U(x,x) = y, y \in D_n) = \frac{1}{|D_n|}$.

Тогда $\Pr(\forall x, y \in U_n \quad U(x,x) \neq U(y,y)) > (\frac{2^{(c-1)n+1} - 1}{2^{(c-1)n+1}})^{2^n}$.

При $c = 2$ вероятность того, что $U(x,x)$ - инъекция, сходится к $60,65\%$, если $c > 2$, то к 100%, причем при $c = 3, n = 5$ вероятность инъекции уже $99,99\%$.

Композиция с RSA

Теорема

Слабые односторонние функции существуют если и только если существуют сильные односторонние.

Из слабой односторонней $U(x, x)$ мы можем получить сильную одностороннюю $U^*(x, x)$.
Теперь применим $U^*(x, x)$ к *RSA*. По первой теореме о композиции эта функция - сильная односторонняя в предположении о существовании односторонних. Так как $U(x, x)$ - скорее всего инъекция, то композиция обратима скорее всего не лучше чем *RSA*.

Итоги

Как результат мы получили функцию, которая:

1. Сильная односторонняя в предположении о существовании односторонних.

Итоги

Как результат мы получили функцию, которая:

1. Сильная односторонняя в предположении о существовании односторонних.
2. Полная.

Итоги

Как результат мы получили функцию, которая:

1. Сильная односторонняя в предположении о существовании односторонних.
2. Полная.
3. Предположительно хорошо работает на практике.