



# One Way Functions

Prof. Zeph Grunschlag

# PRG $\Rightarrow$ Stateful Symmetric Encryption

- Gave example of BG-PRG, but didn't prove.
- Desire general approach for generating PRG's from simpler primitives.

**One way permutation**

**+ hard core bit**

**$\Rightarrow$  PRG**

# One way functions

- Intuitively: Easy to calculate, hard to invert.
- Should be hard to invert *on average*.
- Candidates:
  - Multiplication? NO. A weak one way function.
  - Multiplication of equal size primes
  - Discrete Exponential
  - Modular Powers
  - Modular Squaring

# Function Families

- Define more general concept able to handle last three examples.
- Bonus: natural notion of key (function parameter in family) useful for encrypting.

DEF: A **function family** is an index set  $I$  together with parametrized domains  $D_i$ , codomains  $R_i$  and functions  $f_i : D_i \rightarrow R_i, \forall i \in I$

# OWF Families

DEF: A **one way family of functions** is family of functions with

1. PPT generator  $G$  of indices  $i$  from security parameters  $k$ .
2. PPT generator  $S$  of domain elements in  $D_i$
3. PPT algorithm  $A$  computing  $f$
4. No PPT inversion algorithm  $A'$  exists with the property that  $\Pr[f_i(A(i, f_i(x))) = f_i(x)]$  is non-negligible, where the probability is measured over random  $i$  and  $x$ .

If all  $f_i$  are bijections, family called **one way family of permutations**.

# $P = NP \Rightarrow$ Complexity Based Crypto D.N.E.

Non-deterministic versions of brute-force algorithms for decrypting, inverting functions, and detecting pseudo randomness would translate to poly-time algorithms, showing that adversaries always exist.

# Computational assumptions

- Discrete log assumption - Discrete exponential family is a one way family
- RSA assumption - Modular Powers family is one way family of permutations
- Factoring assumption - multiplying equal sized primes is a one way function (not family) - **MOST BASIC ASSUMPTION**
- Factoring assumption  $\Rightarrow$  Squaring is OWFF and when restricted to quadratic residues is a OWPF

# Hard Core Predicate

- Intuitively: a property about the inputs to a one-way function, that's as hard to compute from outputs, as inverting.
- Candidates:
  - For Discrete Exponential: MSB
  - For Modular Powers: MSB and LSB
  - For Modular Squares: LSB

# Hard Core Predicates

DEF: A **hard core predicate** for a OWFF  $f$  is a family of boolean predicates  $B$  over the same index, domain set, index-generator, domain elements generator with:

1. PPT algorithm  $A$  computing  $B$
2. No PPT algorithm  $A'$  exists for computing  $A$  from  $f$ -outputs exists with the property that  $\Pr[A(i, f_i(x)) = A(f_i(x))] - 1/2$  is non-negligible, where the probability is measured over random  $i$  and  $x$ .

# Goldreich-Levin

- If One Way Function Families exist, then One Way Function Families with Hard Core Bits exists.

THM: Let  $f$  be a family of one-way functions  $f_i$  whose domains are bitstrings. Extend the functions to  $g_i$  which for valid  $x$  and  $y \in \{0, 1\}^{|x|}$  outputs  $g(x, y) = f(x) || y$ . Let  $B_i(x, y)$  be the dot-product

$$B_i(x, y) = \langle x, y \rangle = \left( \sum_{i=1}^{|x|} x_i \cdot y_i \right) \text{ mod } 2$$

Then  $g$  is a OWFF with hard core predicate  $B$ .

NOTE: THM still holds for permutations.

# OWPF $\Rightarrow$ PRG

DEF: Let  $f$  be a OWFP with hard core bit  $B$ . Let  $L$  be any polynomial stretch function. The **pseudorandom bit generator family induced by  $f$  and  $B$**  has the same domains and is defined by

$$g(x) = \left( B_i(x), B_i(f(x)), B_i(f^2(x)), \dots, B_i(f_i^{Q(k)-1}(x)) \right)$$

for security parameter  $k$ .

THM: The family is a PRG-family as implied by the name.

COR: Symmetric stateful encryption possible, if one of the computational assumptions holds.