Attacks on the Legendre PRF

Aleksei Udovenko[2]
joint work with
Ward Beullens[1], Tim Beyne[1], Giuseppe Vitto[2]

[1]imec-COSIC, ESAT, KU Leuven, Belgium

[2]SnT, University of Luxembourg

Dagstuhl Seminar 20041
January 22, 2020

Plan

Legendre Symbol, PRG, PRF

Let p be an odd prime.

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a = b^2 \text{ for some } b \neq 0, \\ 0, & \text{if } a = 0, \\ -1, & \textit{otherwise}. \end{cases}$$

Legendre Symbol, PRG, PRF

Let p be an odd prime.

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a = b^2 \text{ for some } b \neq 0, \\ 0, & \text{if } a = 0, \\ -1, & \textit{otherwise}. \end{cases} \equiv a^{(p-1)/2} \pmod{p}.$$

Legendre Symbol, PRG, PRF

Let p be an odd prime.

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a = b^2 \text{ for some } b \neq 0, \\ 0, & \text{if } a = 0, \\ -1, & \textit{otherwise}. \end{cases} \equiv a^{(p-1)/2} \pmod{p}.$$

Damgård (CRYPTO 1988), *conjecture*:

$$\left(\frac{k}{p}\right), \left(\frac{k+1}{p}\right), \left(\frac{k+2}{p}\right), \ldots \text{ is } \textit{pseudorandom}.$$

Legendre Symbol, PRG, PRF

Let p be an odd prime.

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a = b^2 \text{ for some } b \neq 0, \\ 0, & \text{if } a = 0, \\ -1, & \textit{otherwise}. \end{cases} \equiv a^{(p-1)/2} \pmod{p}.$$

Damgård (CRYPTO 1988), *conjecture*:

$$\left(\frac{k}{p}\right), \left(\frac{k+1}{p}\right), \left(\frac{k+2}{p}\right), \ldots \text{ is } \textit{pseudorandom}.$$

Grassi *et al.* (CCS 2016):

$$\left(\tfrac{k+x}{p}\right) \text{ is a very efficient } \textit{PRF} \text{ for MPC.}$$

Cryptanalysis of the PRF

Ref.	Time	#Queries	Comment
Initial claim (CCS 16)	$O(p)$	$O(\log p)$	exhaustive search
Khovratovich (ia.cr/2019/862)	$\tilde{O}(\sqrt{p})$	$\tilde{O}(\sqrt{p})$	birthday-bound
Beyne *et al.* (ia.cr/2019/1357)	$\tilde{O}(\sqrt{p})$	$O(\sqrt[4]{p})$	reduced data complexity

Cryptanalysis of the PRF

Ref.	Time	#Queries	Comment
Initial claim (CCS 16)	$O(p)$	$O(\log p)$	exhaustive search
Khovratovich (ia.cr/2019/862)	$\tilde{O}(p/Q)$	Q	birthday-bound
Beyne *et al.* (ia.cr/2019/1357)	$\tilde{O}(p/Q^2)$	Q	reduced data complexity

Plan

Notation

$$\ell(a) := \left\lfloor \frac{1}{2}\left(1 - \left(\frac{a}{p}\right)\right) \right\rfloor$$ *0 - quadratic residue, 1 - non-residue*

Notation

$$\ell(a) := \left\lfloor \frac{1}{2}\left(1 - \left(\frac{a}{p}\right)\right)\right\rfloor$$ *0 - quadratic residue, 1 - non-residue*

$$L_k(a) := \ell(k + a)$$

Notation

$$\ell(a) := \left\lfloor \frac{1}{2}\left(1 - \left(\frac{a}{p}\right)\right)\right\rfloor$$ *0 - quadratic residue, 1 - non-residue*

$$L_k(a) := \ell(k+a)$$

$$L_k(a+[m]) := \big(L_k(a),\ L_k(a+1),\ \ldots,\ L_k(a+m-1)\big)$$

Notation

$$\ell(a) := \left\lfloor \frac{1}{2}\left(1 - \left(\frac{a}{p}\right)\right) \right\rfloor \quad \textit{0 - quadratic residue, 1 - non-residue}$$

$$L_k(a) := \ell(k + a)$$

$$L_k(a + [m]) := \big(L_k(a),\ L_k(a+1),\ \ldots,\ L_k(a+m-1)\big)$$

Assumption (heuristic):
$L_k([m])$ has few collisions when $m = \Omega(\log p)$.

Table-based Attack

Let $m = \lceil \log p \rceil$

Step 1: Fill Table $\mathcal{T}_k$

query and store

$$L_k(a_i + [m])$$

for Q/m
randomly sampled a_i

Table-based Attack

Let $m = \lceil \log p \rceil$

Step 1: Fill Table $\mathcal{T}_k$

query and store

$$L_k(a_i + [m])$$

for Q/m
randomly sampled a_i

Step 2: Sample & Match

compute and lookup

$$L_0(b_i + [m])$$

for pm/Q
randomly sampled b_i

Table-based Attack

Let $m = \lceil \log p \rceil$

Step 1: Fill Table $\mathcal{T}_k$

query and store

$$L_k(a_i + [m])$$

for Q/m
randomly sampled a_i

Step 2: Sample & Match

compute and lookup

$$L_0(b_i + [m])$$

for pm/Q
randomly sampled b_i

A collision (a_i, b_j) reveals the key: $k = b_j - a_i$.

Complexity: Time: $O(Q + p \log^2 p/Q)$,
Memory: $O(Q)$ bits

Reducing Queries (1)

Let's exploit *multiplicativity* of the Legendre symbol:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \quad \text{for all } a, b \in \mathbb{F}_p.$$

In terms of ℓ:

$$\ell(ab) = \ell(a) \oplus \ell(b) \quad \text{for all } a, b \in \mathbb{F}_p^*,$$

Reducing Queries (2)

Consider a sequence $(a, a+1, a+2, \ldots) \subseteq \mathbb{F}_p$.

$a+0 \quad a+1 \quad a+2 \quad a+3 \quad a+4 \quad a+5 \quad a+6 \quad a+7$

Reducing Queries (2)

Consider a sequence $(a, a+1, a+2, \dots) \subseteq \mathbb{F}_p$.

$$\begin{array}{cccccccc} a+0 & a+1 & a+2 & a+3 & a+4 & a+5 & a+6 & a+7 \\ & & & & \big\downarrow /2 & & & \\ \frac{a+0}{2} & \frac{a+1}{2} & \frac{a+2}{2} & \frac{a+3}{2} & \frac{a+4}{2} & \frac{a+5}{2} & \frac{a+6}{2} & \frac{a+7}{2} \end{array}$$

Reducing Queries (2)

Consider a sequence $(a, a+1, a+2, \ldots) \subseteq \mathbb{F}_p$.

$$a+0 \quad a+1 \quad a+2 \quad a+3 \quad a+4 \quad a+5 \quad a+6 \quad a+7$$

$$\big\downarrow /2$$

$$\tfrac{a+0}{2} \quad \tfrac{a+1}{2} \quad \tfrac{a+2}{2} \quad \tfrac{a+3}{2} \quad \tfrac{a+4}{2} \quad \tfrac{a+5}{2} \quad \tfrac{a+6}{2} \quad \tfrac{a+7}{2}$$

$$||$$

$$\tfrac{a}{2}+0 \quad \tfrac{a+1}{2}+0 \quad \tfrac{a}{2}+1 \quad \tfrac{a+1}{2}+1 \quad \tfrac{a}{2}+2 \quad \tfrac{a+1}{2}+2 \quad \tfrac{a}{2}+3 \quad \tfrac{a+1}{2}+3$$

Reducing Queries (2)

Consider a sequence $(a, a+1, a+2, \dots) \subseteq \mathbb{F}_p$.

$$
\begin{array}{cccccccc}
a+0 & a+1 & a+2 & a+3 & a+4 & a+5 & a+6 & a+7
\end{array}
$$

$$\Big\downarrow /2$$

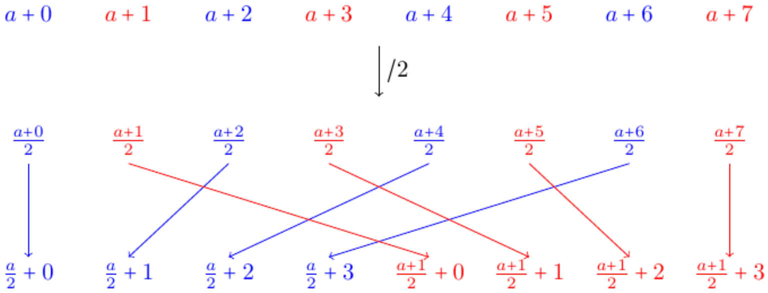
$$
\begin{array}{cccccccc}
\frac{a+0}{2} & \frac{a+1}{2} & \frac{a+2}{2} & \frac{a+3}{2} & \frac{a+4}{2} & \frac{a+5}{2} & \frac{a+6}{2} & \frac{a+7}{2}
\end{array}
$$

$$\Big\|$$

$$
\begin{array}{cccccccc}
\frac{a}{2}+0 & \frac{a+1}{2}+0 & \frac{a}{2}+1 & \frac{a+1}{2}+1 & \frac{a}{2}+2 & \frac{a+1}{2}+2 & \frac{a}{2}+3 & \frac{a+1}{2}+3
\end{array}
$$

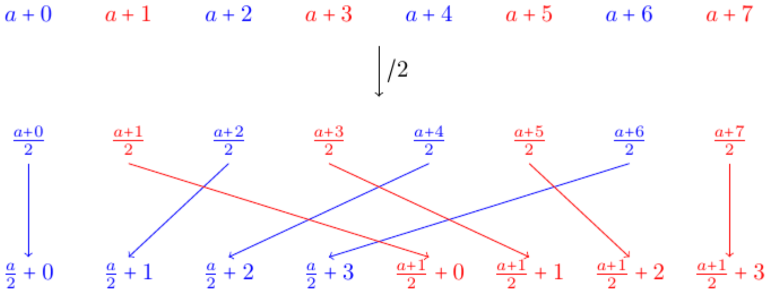
Reducing Queries (2)

Consider a sequence $(a, a+1, a+2, \ldots) \subseteq \mathbb{F}_p$.



Reducing Queries (2)

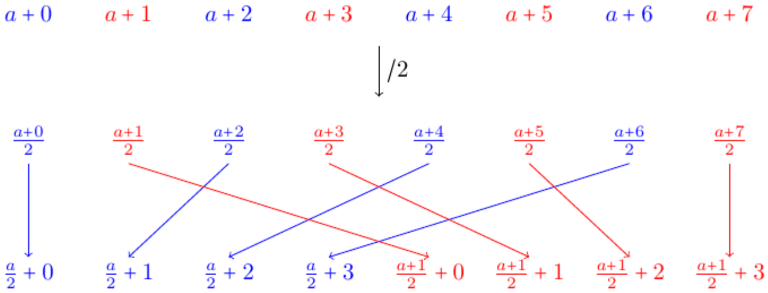
Consider a sequence $(a, a+1, a+2, \ldots) \subseteq \mathbb{F}_p$.



Two new sequences starting at $\frac{a}{2}$ and $\frac{a+1}{2}$!

Reducing Queries (2)

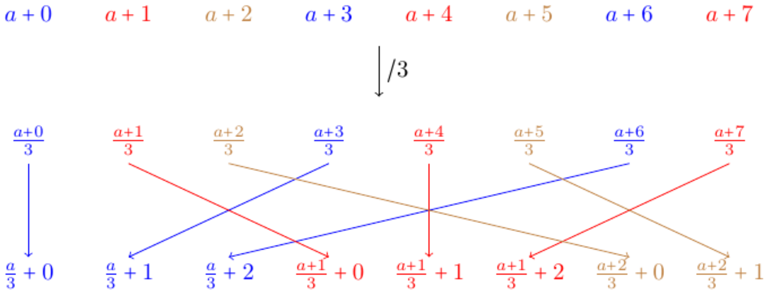
Consider a sequence $(a, a+1, a+2, \ldots) \subseteq \mathbb{F}_p$.



Legendre symbols ℓ match up to the constant $\ell(2)$.

Reducing Queries (2)

Consider a sequence $(a, a+1, a+2, \ldots) \subseteq \mathbb{F}_p$.



Can use any other (small) number instead of 2,
as long as sequence length allows.

Reducing Queries (2)

Q consecutive bits queried $\rightarrow \sim Q^2/m$ sequences of length m

Reducing Queries (2)

Q consecutive bits queried $\to \sim Q^2/m$ sequences of length m

Improved attack complexity:
Time: $O(Q^2 + p \log^2 p / Q^2)$,
Memory: $O(Q^2)$ bits

(reduces query complexity but still only up to the birthday bound)

Reducing Queries (2)

Q consecutive bits queried $\rightarrow \sim Q^2/m$ sequences of length m

Improved attack complexity:
Time: $O(Q^2 + p \log^2 p / Q^2)$,
Memory: $O(Q^2)$ bits

(reduces query complexity but still only up to the birthday bound)

Open Problem: better data structure/algorithm for subsequence lookup?

Plan

Higher-order PRF

Linear Legendre PRF:

$$L_{k}(a) := \ell(k + a),$$

secret: $k \in \mathbb{F}_p$

Higher-order PRF

Linear Legendre PRF:

$$L_k(a) := \ell(k + a),$$
$$\text{secret: } k \in \mathbb{F}_p$$

Degree-d Legendre PRF:

$$L_{f(x)}(a) := \ell(f(a)),$$
$$\text{secret: } f \in \mathbb{F}_p[x] \text{ monic}, \deg f = d$$

Example for $d = 3$:

$$L_{x^3+k_2x^2+k_1x+k_0}(a) = \ell(a^3 + k_2a^2 + k_1a + k_0),$$
$$\text{secret: } k_0, k_1, k_2 \in \mathbb{F}_p$$

Cryptanalysis

Degree-d Legendre PRF:

$$L_{f(x)}(a) := \ell(f(a)),$$
$$\text{secret: } f \in \mathbb{F}_p[x] \text{ monic}, \deg f = d$$

- Generally, no birthday-bound attacks

Cryptanalysis

Degree-d Legendre PRF:

$$L_{f(x)}(a) := \ell(f(a)),$$
$$\text{secret: } f \in \mathbb{F}_p[x] \text{ monic}, \deg f = d$$

- Generally, no birthday-bound attacks
- Khovratovich: attack with time $\tilde{O}(p^{d-1}d)$

Cryptanalysis

Degree-d Legendre PRF:

$$L_{f(x)}(a) := \ell(f(a)),$$
$$\text{secret: } f \in \mathbb{F}_p[x] \text{ monic}, \deg f = d$$

- Generally, no birthday-bound attacks
- Khovratovich: attack with time $\tilde{O}(p^{d-1}d)$
- Similar multiplicativity trick: $\tilde{O}(p^2 + p^{d-2}d)$

Cryptanalysis

Degree-d Legendre PRF:

$$L_{f(x)}(a) := \ell(f(a)),$$
$$\text{secret: } f \in \mathbb{F}_p[x] \text{ monic}, \deg f = d$$

- Generally, no birthday-bound attacks
- Khovratovich: attack with time $\tilde{O}(p^{d-1}d)$
- Similar multiplicativity trick: $\tilde{O}(p^2 + p^{d-2}d)$
- Weak key attacks!

Weak Keys

Let f be a secret polynomial of degree d.

Weak Keys

Let f be a secret polynomial of degree d.

Assume it *splits* completely over $\mathbb{F}_p$ ($\Pr \approx 1/d!$):

$$f(x) = (x + r_1)(x + r_2) \dots (x + r_d)$$

Weak Keys

Let f be a secret polynomial of degree d.

Assume it *splits* completely over $\mathbb{F}_p$ ($\Pr \approx 1/d!$):

$$f(x) = (x + r_1)(x + r_2)\dots(x + r_d)$$

$$\ell(f(x)) = \ell(x + r_1) \oplus \ell(x + r_2) \oplus \dots \oplus \ell(x + r_d)$$

Weak Keys

$$\ell(f(x)) = \ell(x + r_1) \oplus \ell(x + r_2) \oplus \ldots \oplus \ell(x + r_d)$$

Weak Keys

$$\ell(f(x)) = \ell(x + r_1) \oplus \ell(x + r_2) \oplus \ldots \oplus \ell(x + r_d)$$

1. Choose an arbitrary sequence $a_1, a_2, \ldots, a_m$.

Weak Keys

$$\ell(f(x)) = \ell(x + r_1) \oplus \ell(x + r_2) \oplus \ldots \oplus \ell(x + r_d)$$

1. Choose an arbitrary sequence $a_1, a_2, \ldots, a_m$.
2. Query the vector

$$\tilde{v} := \big(\ell(f(a_1)), \ell(f(a_2)), \ldots, \ell(f(a_m))\big) \in \mathbb{F}_2^m$$

Weak Keys

$$\ell(f(x)) = \ell(x + r_1) \oplus \ell(x + r_2) \oplus \ldots \oplus \ell(x + r_d)$$

1. Choose an arbitrary sequence $a_1, a_2, \ldots, a_m$.
2. Query the vector

$$\tilde{v} := \big(\ell(f(a_1)), \ell(f(a_2)), \ldots, \ell(f(a_m))\big) \in \mathbb{F}_2^m$$

3. Compute all p vectors with $r \in \mathbb{F}_p$:

$$v_r := \big(\ell(a_1 + r), \ell(a_2 + r), \ldots, \ell(a_m + r)\big) \in \mathbb{F}_2^m$$

Weak Keys

$$\ell(f(x)) = \ell(x + r_1) \oplus \ell(x + r_2) \oplus \ldots \oplus \ell(x + r_d)$$

1. Choose an arbitrary sequence $a_1, a_2, \ldots, a_m$.
2. Query the vector

$$\tilde{v} := \big(\ell(f(a_1)), \ell(f(a_2)), \ldots, \ell(f(a_m))\big) \in \mathbb{F}_2^m$$

3. Compute all p vectors with $r \in \mathbb{F}_p$:

$$v_r := \big(\ell(a_1 + r), \ell(a_2 + r), \ldots, \ell(a_m + r)\big) \in \mathbb{F}_2^m$$

4. d-XOR-SUM:

$$\tilde{v} = v_{r_1} \oplus v_{r_2} \oplus \ldots \oplus v_{r_d}$$

Weak Keys

d-XOR-SUM:

$$\tilde{v} = v_{r_1} \oplus v_{r_2} \oplus \ldots \oplus v_{r_d}$$

- Unique solution! Wagner's algorithm does not directly apply...

Weak Keys

d-XOR-SUM:

$$\tilde{v} = v_{r_1} \oplus v_{r_2} \oplus \ldots \oplus v_{r_d}$$

- Unique solution! Wagner's algorithm does not directly apply...
- Factors of $f(x)$ do not have to be linear.
- Birthday-bound attack when there is a factor of degree $\lfloor d/2 \rfloor$.

The End

Open Problems

1. Better data structure/algorithm for subsequence lookup?
2. Birthday-bound attacks for all keys? (Higher-degree L.PRF)
3. Beyond-birthday-bound attacks?

ia.cr/2019/1357