Notes on a family of preimage-resistant functions

János Folláth

follathj@inf.unideb.hu

University of Debrecen

Research supported partially by the TARIPAR3 project grant Nr. TECH 08-A2/2-2008-0086

One-Way Functions

- Applications
- Notion
- Complexity theory

One-Way Functions

- RSA
- Discrete logarithm problem
- Ideal class groups of algebraic number fields

Security requirements

- Preimage resistance
- Second preimage resistance
- Collision resistance

The old construction

Let $P(X) \in \mathbb{Z}[X]$ be a fixed monic polynomial of degree $n \geq 3$ having no multiple roots. Denote by $\alpha_1, \ldots, \alpha_n$ the roots of P and put

$$L_i(\underline{X}) := \sum_{j=1}^{m} \alpha_i^{j-1} X_j \quad for \quad i = 1, \ldots, n \quad and \quad m \leq n.$$

Define the norm form corresponding to the polynomial P by

$$\mathcal{N}_P(\underline{X}) := \prod_{i=1}^{n} L_i(\underline{X}).$$

Aumassons attack

- Non-standard notion of collision resistance
- Iterated scheme
- Circulant matrices
- Implementation flaws

New construction

Theorem 1 *Let* $f(\underline{X}) \in \mathbb{F}_q[X_1, \ldots, X_m]$ *be a polynomial such that*

$$f(\underline{X}) := b(X_1, \ldots, X_m) + a(X_1, \ldots, X_m)$$

with homogeneous polynomials $a(\underline{X}), b(\underline{X})$ *satisfying* $k = \deg a(\underline{X}) < \deg b(\underline{X}) = n$, $\deg_{X_i} b(\underline{X}) = n$ *for* $1 \leq i \leq m$. *Further, s uppose that there exist indices* $1 \leq j_1 < j_2 \leq n$ *such that the binary form*

$$b_0(X_{j_1}, X_{j_2}) := b(0, \ldots, 0, X_{j_1}, 0, \ldots, 0, X_{j_2}, 0, \ldots, 0) \tag{1}$$

has no multiple zero.

Let $N(f, \gamma, q)$ *denote the number of solutions of the equation* $f(x_1, \ldots, x_m) = \gamma$ *in* $x_1, \ldots, x_m \in \mathbb{F}_q$. *Then*

$$|N(f, \gamma, q) - q^{m-1}| \leq (n-1)(n-2)q^{m-3/2} + 5n^{13/3}q^{m-2}. \tag{2}$$

Moreover, if $q > 15n^{13/3}$, *then*

$$|N(f, \gamma, q) - q^{m-1}| \leq (n-1)(n-2)q^{m-3/2} + (5n^2 + n + 1)q^{m-2}. \tag{3}$$

Practical considerations

Lemma 1 *Let* $f(\underline{X}) := b(\underline{X}) + a(\underline{X})$ *such that* $b(\underline{X}) = \beta_1 X_1^r + \cdots + \beta_m X_m^r$, $a(\underline{X}) = \alpha_1 X_1^s + \cdots + \alpha_m X_m^s$ *and* $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_m \neq 0$. *If* $0 < s < r < q$ *and* r *is odd if* $q = 2^f$, *then* $f(\underline{X})$ *satisfies all assumptions of Theorem 1.*

Practical considerations

Hash length	Implementation	Kilobyte/second
254	old	8
509	old	6
254	new	56
509	new	49

Strict avalanche criterion

If a function is to satisfy the strict avalanche criterion, then each of its output bits should change with a probability of one half whenever a single input bit is complemented.

Lemma

Lemma 2 *Let $q = p^k$, n be a non-negative integer and $f \in \mathbb{F}_q[X]$ be the trinomial $f(X) = X^{p^n} - aX - b$ where $a \in \mathbb{F}_q^*$. Set $d = gcd(n, k)$ and $m = k/d$. Let Tr_d be the trace function from $\mathbb{F}_q$ onto $\mathbb{F}_{q^d}$. For $0 \leq i \leq m-1$ define $t_i = \sum_{j=i}^{m-2} p^n(j+1)$. Put $\alpha_0 = a$ and $\beta_0 = b$. If $m > 1$, then for $1 \leq r \leq m-1$, set $\alpha_r = a^{1+p^n+\ldots+p^{nr}}$ and*

$$\beta_r = \sum_{i=0}^{r} a^{s_i} b^{p^{ni}}$$

where $s_i = \sum_{j=i}^{r-1} p^{n(j+1)}$ for $0 \leq i \leq r-1$ and $s_r = 0$. The trinomial f has no roots in $\mathbb{F}_q$ if and only if $\alpha_{m-1} = 1$ and $\beta_{m-1} \neq 0$. When $\alpha_{m-1} \neq 1$ then f has a unique root in $x \in \mathbb{F}_q$, namely, $x = \beta_{m-1}/(1-\alpha_{m-1})$. Otherwise f has p^d roots in $\mathbb{F}_q$ given by $x + \delta\tau$ where $\delta \in \mathbb{F}_{p^d}$, τ is a fixed element of $\mathbb{F}_q$ satisfying $\tau^{p^n-1} = a$ and, for any $c \in \mathbb{F}_q^*$ satisfying $Tr_d(c) \in \mathbb{F}_{p^d}$,

$$x = \frac{1}{Tr_d(c)} \sum_{i=0}^{m-1} \left(\sum_{j=0}^{i} c^{p^{nj}} \right) a^{ti} b^{p^{ni}}$$

.

Lemma

Lemma 3 *Let us define* $f \in \mathbb{F}_{2^k}[x_1, \ldots, x_m]$ *as* $f(x_1, \ldots, x_m) = \sum_{i=1}^{m} \alpha_i x_i^n + \sum_{i=1}^{m} \beta_i x_i$ *where* $n = 2^l + 1$ *such that* $(l, k) = 1$*. Let* Tr *be the absolute trace function of* $\mathbb{F}_q$*.* $f(x_1, \ldots, x_m) - f(x_1, \ldots, x_j + \delta, \ldots, x_m) = \gamma$ *holds if and only if* $Tr((\beta_j \delta + \gamma)\alpha_j^{-1}\delta^{-n} + 1) = 0$*, and only for exactly 2 distinct values of* x_j*.*

Main Theorem

Theorem 2 *Let us define* $f \in \mathbb{F}_{2^k}[x_1, \ldots, x_m]$ *as* $f(x_1, \ldots, x_m) = \sum_{i=1}^{m} \alpha_i x_i^n + \sum_{i=1}^{m} \beta_i x_i$ *where* $n = 2^l + 1$ *such that* $(l, k) = 1$. *Then*

$$(1 - q\varepsilon)^{m-1}(\frac{1}{q} - \varepsilon) \leq$$

$$P(f(x_1, \ldots, x_m) - f(x_1 + \delta_1, \ldots, x_m + \delta_m) = \gamma)$$

$$\leq (1 + q\varepsilon)^{m-1}(\frac{1}{q} + \varepsilon)$$

where $0 \leq \varepsilon \leq (q - n)q^{-\frac{3}{2}}$.

Thank you for your attention!

References

[1] R. Lidl and H. Niederreiter “Finite Fields”, Encyclopedia of Mathematics and its Applications, vol. 20, 1997

[2] R. Coulter and M. Henderson “A note on the roots of trinomials over a finite field”, Bull. Austral. Math. Soc., vol. 69, 429-432, 2004

[3] R. Forré “The strict avalanche criterion: spectral properties of boolean functions and an extended definition”, Advances in cryptology—CRYPTO ’88 (Santa Barbara, CA, 1988), 450–468

[4] A. Béreczes, J. Folláth, A. Pethő “On a family of preimage resistant functions”, to appear