Security of Polynomial Transformations of the Diffie–Hellman Key

Igor E. Shparlinski
Department of Computing, Macquarie University
Sydney, NSW 2109, Australia
igor@ics.mq.edu.au

Abstract

D. Boneh and R. Venkatesan have recently proposed an approach to proving that a reasonably small portions of most significant bits of the Diffie–Hellman key modulo a prime are as secure the the whole key. Some further improvements and generalizations have been obtained by I. M. Gonzales Vasco and I. E. Shparlinski. E. R. Verheul has obtained certain analogies of these results in the case of Diffie–Hellman keys in extensions of finite fields, when an oracle is given to compute a certain polynomial function of the key, for example, the trace in the background field. Here we obtain a new result in this direction concerning the case of so-called "unreliable" oracles. The result has applications to the security of the recently proposed by A. K. Lenstra and E. R. Verheul XTR cryptosystem.

1 Introduction

Let $\mathbb{F}_q$ denote a finite field of q elements.

D. Boneh and R. Venkatesan [1] have proposed an approach to proving that about $n^{1/2}$ of most significant bits of the Diffie–Hellman key modulo an n-bit prime are as secure as the whole key. Their results have been generalized (and slightly corrected) by I. M. Gonzales Vasco and I. Shparlinski [7, 8]. A detailed survey of several other results of this type (including the RSA cryptosystem and the discrete logarithm problem) has recently been given in [5], see also [6, 9, 13, 14, 15, 17, 18, 19, 20] for several more recent results.

E. R. Verheul [21] among several other results, considers a similar problem for the Diffie–Hellman key in arbitrary finite fields. However instead of studying the security of the most significant bits the paper [21] deals with the security of values of sparse polynomials at the values of the Diffie–Hellman keys. More precisely, let us fix an element $\gamma \in \mathbb{F}_q$ and a polynomial $F(X) \in \mathbb{F}_q[X]$. It has been shown in [21], under certain natural conditions, that if we are given an oracle which for each pair (γ^x, γ^y) with some integers x and y returns the value of $F(\gamma^{xy})$, than this oracle can be used to construct a polynomial time algorithm to compute the Diffie–Hellman key γ^{xy}. We remark that polynomials F can be of very large degree (thus direct solving the equation $F(\gamma^{xy}) = A$ is not feasible) but contain a reasonably small number of monomials. The result has been motivated by applications to the proof of security of a certain new cryptosystem, see [2, 10, 11, 12, 21].

Here we obtain a generalization of Theorem 24 of [21] to the "unreliable" case, when oracle returns the result only for a certain very small fraction of inputs and returns an error message for other inputs.

2 Preparations

The following estimate on the number of zeros of sparse polynomials is a version of the similar result from [3, 4].

Lemma 1 *For $r \ge 2$ elements $a_1, \ldots, a_r \in \mathbb{F}_q^*$ and integers $\tau_1, \ldots, \tau_r \in \mathbb{Z}$ let us denote by Q the number of solutions of the equation*

$$\sum_{i=1}^{r} a_i z^{\tau_i} = 0, \qquad z \in \mathbb{F}_q^*.$$

Then

$$Q \le 3(q-1)^{1-1/(r-1)} d^{1/(r-1)},$$

where

$$d = \min_{1 \le i \le r} \max_{j \ne i} \gcd(\tau_j - \tau_i, q-1).$$

Proof. It has been shown in Lemma 7 of [3] (see also Lemma 4 of [4] and Lemma 3.4 of [16]) that

$$Q \le 2 \left\lfloor \frac{q-1}{\lceil L^{1/(r-1)} \rceil - 1} \right\rfloor$$

where $L = (q-1)/d$.

If $L \le 3^{r-1}$ then

$$Q \le q-1 \le 3(q-1)L^{-1/(r-1)} \ge q > Q.$$

Otherwise $\lceil L^{1/(r-1)} \rceil - 1 \ge 2L^{-1/(r-1)}/3$ and the result follows. $\square$

Let us fix an element $\vartheta \in \mathbb{F}_q$ of multiplicative order t.

Lemma 2 *For $m \ge 2$ elements $a_1, \ldots, a_m \in \mathbb{F}_q^*$ and integers $e_1, \ldots, e_m$ we denote by W the number of solutions of the equation*

$$\sum_{i=1}^{m} a_i \vartheta^{e_i u} = 0, \qquad u \in [0, t-1].$$

Then the bound

$$W \le 3t^{1-1/(m-1)} D^{1/(m-1)},$$

holds, where

$$D = \min_{1 \le i \le m} \max_{j \ne i} \gcd(e_j - e_i, t).$$

Proof. We write $\vartheta = g^{(q-1)/t}$ where g is a primitive root of $\mathbb{F}_q$ and note that each solution $u \in [0, t-1]$ of the previous exponential equation gives rise to $(q-1)/t$ distinct solutions

$$z_j = g^{u+tj}, \qquad j = 0, \ldots, (q-1)/t - 1,$$

of the equation

$$\sum_{i=1}^{m} a_i z^{\tau_i} = 0, \qquad z \in \mathbb{F}_q^*,$$

where $\tau_j = e_j(q-1)/t$. Remarking that

$$\gcd(\tau_j - \tau_i, q-1) = \frac{q-1}{t} \gcd(e_j - e_i, t),$$

from Lemma 1 we obtain that

$$W \le 3\frac{t}{q-1}(q-1)^{1-1/(m-1)} \left(\frac{q-1}{t} D\right)^{1/(m-1)} = 3t^{1-1/(m-1)} D^{1/(m-1)}$$

as claimed. $\square$

3 Security of Polynomial Transformations of the Diffie–Hellman Key

Let $\gamma \in \mathbb{F}_q$ be an element of multiplicative order t.

As in [21] we consider an m-sparse polynomial

$$F(X) = \sum_{i=1}^{m} c_i X^{e_i} \in \mathbb{F}_q[X], \tag{1}$$

where $c_1, \ldots, c_m \in \mathbb{F}_q^*$ and $e_1, \ldots, e_m$ are pairwise distinct modulo t.

Let $0 < \varepsilon \le 1$.

Assume that we are given an *oracle* $\mathcal{O}_{F,\varepsilon}$ such that for every $x \in [0, t-1]$, given the values of γ^x and γ^y, it returns $F(\gamma^{xy})$ for at least εt values of $y \in [0, t-1]$ and returns an error message for other values of $y \in [0, t-1]$.

The case $\varepsilon = 1$, that is, the case of a "noise-free" oracle has been considered in [21].

We are ready to prove the main result. For simplicity we assume that t is a prime number, although analogues of our result hold for composite t as well. Nevertheless this case allows us to simplify some arguments and it is also one of the most practically important cases, see [2, 10, 11, 12, 21].

Theorem 3 *Let t be prime, $m \ge 2$ and let an m-sparse polynomial F be given by (1). Assume that*

$$1 \ge \varepsilon \ge 6t^{-1/(m-1)}.$$

Given an oracle $\mathcal{O}_{F,\varepsilon}$, there exists a probabilistic algorithm which given γ^x and γ^y makes the expected number of at most $2m\varepsilon^{-1}$ calls of the oracle $\mathcal{O}_{F,\varepsilon}$, executes polynomial number $(m \log q)^{O(1)}$ arithmetic operations in $\mathbb{F}_q$ per each call and returns γ^{xy} for all pairs $(x, y) \in [0, t-1]^2$.

Proof. If $x = 0$ the result is trivial. Let us consider a pair $(x, y) \in [0, t-1]^2$ with $x \ne 0$.

Let $\mathcal{U}$ be the set of $u \in [0, t-1]$ for which the oracle, given the values of γ^x and γ^{y+u} returns the value of $F\left(\gamma^{x(y+u)}\right)$. By the conditions of the theorem $|\mathcal{U}| \ge \varepsilon t$. We also remark that if γ^y is known then for any $v \in [0, t-1]$ the value of γ^{y+v} can easily be computed as well.

Put $\vartheta = \gamma^x$.

Select a sequence of elements v uniformly and independently at random in the interval $[0, t-1]$ and for each of them feed γ^x and γ^{y+v} in the oracle $\mathcal{O}_{F,\varepsilon}$ until we find an element $u \in \mathcal{U}$ and thus find the values of $F\left(\gamma^{x(y+u)}\right)$. Let us call this element u_1. The expected number of oracle calls to find such an element is $\varepsilon^{-1} \leq 2\varepsilon^{-1}$.

Assume that for some integer k, $2 \leq k \leq m$, we have selected $k-1$ elements $u_1, \ldots, u_{k-1} \in \mathcal{U}$ with

$$\det\left(\vartheta^{e_i u_j}\right)_{i,j=1}^{k-1} \neq 0. \tag{2}$$

We select elements v uniformly and independently at random in the interval $[0, t-1]$ until we find an element $u_k \in \mathcal{U}$ such that

$$\det\left(\vartheta^{e_i u_j}\right)_{i,j=1}^{k} \neq 0. \tag{3}$$

We remark that if the last determinant vanishes then u_k satisfies an equation of the form

$$\Delta_1 \vartheta^{e_k u_k} + \ldots + \Delta_k \vartheta^{e_1 u_k} = 0$$

where, by the assumption (2), we have

$$\Delta_1 = \det\left(\vartheta^{e_i u_j}\right)_{i,j=1}^{k-1} \neq 0.$$

Applying Lemma 2 we obtain that the number of elements $u_k \in \mathcal{U}$ which satisfy the condition (3) is at least

$$|\mathcal{U}| - 3t^{1-1/(k-1)} \geq |\mathcal{U}| - 3t^{1-1/(m-1)} \geq \frac{1}{2}|\mathcal{U}|.$$

Thus such an element $u_k \in \mathcal{U}$ can be found in the expected number of at most $2\varepsilon^{-1}$ oracle calls with γ^x and γ^{y+v} where elements v are selected uniformly and independently at random in the interval $[0, t-1]$. More precisely, we call the oracle $\mathcal{O}_{F,\varepsilon}$ with γ^x and γ^{y+v} for a random $v \in [0, t-1]$ until both it returns $F\left(gx(y+v)\right)$ and

$$\Delta_1 \vartheta^{e_k v} + \ldots + \Delta_k \vartheta^{e_1 v} = 0,$$

and call the corresponding value u_k. Because there are at least $0.5|\mathcal{U}| \geq 2\varepsilon t$ such values of v, the expected number of call is at most $2\varepsilon^{-1}$.

Therefore after the expected number of at most $2m\varepsilon^{-1}$ oracle calls we obtain m elements $u_1, \ldots, u_m \in \mathcal{U}$ with corresponding values of $A_j = F\left(\vartheta^{y+u_j}\right)$ for each $j = 1, \ldots, m$ and such that

$$\det\left(\vartheta^{e_i u_j}\right)_{i,j=1}^{m} \neq 0.$$

The rest of the proof follows essentially the same arguments as the proof of Theorem 24 of [21]. Indeed, we see from our construction that we have a nonsingular system of linear equations

$$\sum_{i=1}^{m} c_i \vartheta^{e_i u_j} \vartheta^{e_i y} = A_j, \qquad j = 1, \ldots, m,$$

from which the vector $(c_1\vartheta^{e_1 y}, \ldots, c_m\vartheta^{e_m y})$ can be found and thus we obtain the values of $\gamma^{e_1 xy}, \ldots, \gamma^{e_m xy}$. Because $m \geq 2$ and t is prime, at least one of $e_1, \ldots, e_m$ (which are pairwise distinct modulo t) is relatively prime to t. Say if $\gcd(e_1, t) = 1$ we define an integer $f_1 \in [1, t-1]$ from the congruence $f_1 e_1 \equiv 1 \pmod{t}$ and compute

$$\gamma^{xy} = \left(\gamma^{e_1 xy}\right)^{f_1}.$$

Remarking that besides the expected number of oracle calls is $2m\varepsilon^{-1}$ and that the rest of the algorithm can be implemented in deterministic polynomial in $m \log q$ time, we obtain the desired result. $\square$

4 Remarks

Let $q = p^r$. Then the trace function

$$\mathrm{Tr}(X) = \sum_{i=0}^{r-1} X^{p^i}$$

provides a natural example of a polynomial of the form (1). This function as well as the function

$$L(X) = \sum_{0 \leq i \neq j \leq r-1} X^{p^i + p^j}$$

have been studied in [2] (with $r = 6$). Our results imply a stronger version of Lemma 3.1 of [2] and thus give more security assurance to the proposed there cryptosystem. The same comment also applies to the proposed in [10, 11, 12] *XTR* public key cryptosystem which is based on a more computationally efficient modification of the ideas of [2].

It is easy to see that making more oracle calls one can replace the oracle $\mathcal{O}_{F,\varepsilon}$ with a more natural and general oracle $\widetilde{\mathcal{O}}_{F,\varepsilon}$ which returns $F(\gamma^{xy})$ for at least εt^2 pairs $(x, y) \in [0, t-1]^2$. For $x \in [0, t-1]$, let M_x denote the number $y \in [0, t-1]$ for which the oracle $\widetilde{\mathcal{O}}_{F,\varepsilon}$, given the values of γ^x and γ^y, returns $F\left(\gamma^{xy}\right)$. Thus,

$$\sum_{x=0}^{t} M_x \geq \varepsilon t^2.$$

Let L be the number of $x \in [0, t-1]$ for which $M_x \geq 0.5\varepsilon t$. Then

$$\sum_{x=0}^{t} M_x \leq 0.5\varepsilon t(t-L) + Lt = 0.5\varepsilon t^2 + (1-0.5\varepsilon)Lt.$$

Therefore

$$L \geq \frac{\varepsilon}{2(1-0.5\varepsilon)} t \geq 0.5\varepsilon t.$$

Now we select a random $u \in [0, t-1]$ and compute γ^{x+u}. Using polynomially many random values of $v \in [0, t-1]$ with high probability we can test whether $M_{x+u} \geq 0.5\varepsilon t$. If this is not the case we select another value of u. After the expected number of $t/L \leq 2\varepsilon^{-1}$ random choices of u we find a value with $M_{x+u} \geq 0.5\varepsilon t$. Now we apply the same arguments as in the proof of Theorem 3 with γ^{x+u} and γ^y, recovering $\gamma^{(x+u)y}$. Now we can find $\gamma^{xy} = \gamma^{(x+u)y}\left(\gamma^y\right)^{-u}$.

In fact we do not even need the oracle to return the error message. It is enough to assume that, when it does not compute $F\left(\gamma^{xy}\right)$, it returns just a random element of $\mathbb{F}_q$. Then repeating each oracle call polynomially many times one can distinguish between correct outputs and random outputs with overwhelming probability.

On the other hand, it would also be very important to obtain similar results for the case where the oracle returns the correct value of $F\left(\gamma^{xy}\right)$ for a certain portion of inputs and returns wrong (but consistent) results for other inputs (instead of the error message or a random element of $\mathbb{F}_q$, thus wrong outputs cannot be immediately identified).

Acknowledgment. The author would like to thank Arjen Lenstra and Eric Verheul for useful discussions and sending preprints of [10, 11, 12].

References

[1] D. Boneh and R. Venkatesan, 'Hardness of computing the most significant bits of secret keys in Diffie–Hellman and related schemes', *Proc.*

Crypto'96, Lect. Notes in Comp. Sci., Springer-Verlag, Berlin, **1109** (1996), 129–142.

[2] A. E. Brouwer, R. Pellikaan and E. R. Verheul, 'Doing more with fewer bits', *Proc. Asiacrypt'99*, Lect. Notes in Comp. Sci., Springer-Verlag, Berlin, **1716** (1999), 321–332.

[3] R. Canetti, J. B. Friedlander, S. Konyagin, M. Larsen, D. Lieman and I. E. Shparlinski, 'On the statistical properties of Diffie–Hellman distributions', *Israel J. Math.*, **120** (2000), 23–46.

[4] J. B. Friedlander, M. Larsen, D. Lieman and I. E. Shparlinski, 'On correlation of binary M-sequences', *Designs, Codes and Cryptography*, **16** (1999), 249–256.

[5] M. I. González Vasco and M. Näslund, 'A survey of hard core functions', *Proc. Workshop on Cryptography and Computational Number Theory*, Singapore 1999, Birkhäuser, 2001, 227–256.

[6] M. I. González Vasco, M. Näslund and I. E. Shparlinski, 'The hidden number problem in extension fields and its applications', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **2286** (2002), 105–117.

[7] M. I. González Vasco and I. E. Shparlinski, 'On the security of Diffie-Hellman bits', *Proc. Workshop on Cryptography and Computational Number Theory*, Singapore 1999, Birkhäuser, 2001, 257–268.

[8] M. I. González Vasco and I. E. Shparlinski, 'Security of the most significant bits of the Shamir message passing scheme', *Math. Comp.*, **71** (2002), 333–342.

[9] N. A. Howgrave-Graham, P. Q. Nguyen and I. E. Shparlinski, 'Hidden number problem with hidden multipliers, timed-release crypto and noisy exponentiation', *Math. Comp.*, (to appear).

[10] A. K. Lenstra and E. R. Verheul, 'The XTR public key system', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **1880** (2000), 1–19.

[11] A. K. Lenstra and E. R. Verheul, 'Key improvements to XTR', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **1976** (2000), 220–233.

[12] A. K. Lenstra and E. R. Verheul, 'An overview of the XTR public key system', *Proc. the Conf. on Public Key Cryptography and Computational Number Theory, Warsaw 2000*, Walter de Gruyter, 2001, 151–180.

[13] W.-C. W. Li, M. Näslund and I. E. Shparlinski, 'The hidden number problem with the trace and bit security of XTR and LUC', *Proc. Crypto'02, Santa Barbara 2002*, Lect. Notes in Comp. Sci., Springer-Verlag, Berlin, (to appear).

[14] M. Näslund, I. E. Shparlinski and W. Whyte, 'On the bit security of NTRU', *Preprint*, 2002, 1–10.

[15] P. Q. Nguyen and I. E. Shparlinski, 'On the insecurity of a server-aided RSA protocol', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **2248** (2001), 21–35.

[16] I. E. Shparlinski, *Number theoretic methods in cryptography: Complexity lower bounds*, Birkhäuser, 1999.

[17] I. E. Shparlinski, 'On the generalised hidden number problem and bit security of XTR', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **2227** (2001), 268–277.

[18] I. E. Shparlinski, 'Security of most significant bits of g^{x^2}', *Inform. Proc. Letters*, **83** (2002), 109–113.

[19] I. E. Shparlinski, 'Playing "Hide-and-Seek" in finite fields: Hidden number problem and its applications', *Proc. 7th Spanish Meeting on Cryptology and Information Security*, Univ. of Oviedo, 2002, (to appear).

[20] I. E. Shparlinski, 'Exponential sums and lattice reduction: Applications to cryptography', *Proc. 6th Conference of Finite Fields and their Applications, Oaxaca 2001*, Springer-Verlag, Berlin, (to appear).

[21] E. R. Verheul, 'Certificates of recoverability with scalable recovery agent security', *Proc. Inter. Workshop on Practice abnd Theory of Public Key Cryptography (PKC'2000)*, Lect. Notes in Comp. Sci., Springer-Verlag, Berlin, **1751** (2000), 258–275.