A new APN function which is not equivalent to a power mapping

Yves Edel[*]
Mathematisches Institut der Universität
Im Neuenheimer Feld 288
D-69120 Heidelberg
Germany
and
Gohar Kyureghyan[†] and Alexander Pott[‡]
Institute for Algebra and Geometry
Otto-von-Guericke-University Magdeburg
D-39016 Magdeburg
Germany

Abstract

A new almost perfect nonlinear function (APN) on $\mathbb{F}_{2^{10}}$ which is not equivalent to any of the previously known APN mappings is constructed. This is the first example of an APN mapping which is not equivalent to a power mapping.

Keywords. almost perfect nonlinear function, finite field, boolean function

1 Introduction

In cryptography, one is interested in functions $F : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ which are highly nonlinear. There are basically two concepts to measure the linearity of a function: We may use the Walsh transform (which is a special case of the Discrete Fourier transform) or we may use differential properties of F. These two concepts yield to the notion of almost bent (AB) and almost perfect nonlinear (APN) functions. Not many examples of such functions are known, and it was an open problem to decide whether the list of known APN and AB functions is complete. Moreover, all the examples constructed so far have been equivalent to power mappings. In this paper we discuss the mapping

$$F : \mathbb{F}_{2^{10}} \to \mathbb{F}_{2^{10}}, \quad x \mapsto x^3 + ux^{36}$$

where u is a suitable element in the multiplicative group $\mathbb{F}_{2^{10}}^*$ of $\mathbb{F}_{2^{10}}$, see Theorem 2. It turns out that these mappings are inequivalent to any power mappings, hence they are new. This is the first example of a new APN mapping for several years, see [8], and it is the first example of a mapping which is inequivalent to any power mapping. Moreover, the mapping is crooked or, in other words, differentially affine.

[*] y.edel@mathi.uni-heidelberg.de
[†] gohar.kyureghyan@mathematik.uni-magdeburg.de
[‡] alexander.pott@mathematik.uni-magdeburg.de

We emphasize that our function is inequivalent to a power mapping in the general way described in [4] and [2]. It seems that not much attention has been paid so far to the question whether the known classes of APN or AB functions are inequivalent in this general sense or not. We are not aware of any reference that shows whether the known classes are equivalent or not.

In this paper, we use a dimension argument (that has not been used before in order to distingish APN or AB functions) to prove that the function mentioned above is really new. This argument is motivated by the dimension arguments that are used in order to distinguish difference sets, and it may be applied also to distinguish the known classes of APN and AB mappings.

Throughout this paper, let $\mathbb{F}_{2^m}$ denote the finite field with 2^m elements. This field is also a vector space $\mathbb{F}_2^m$ of dimension m over $\mathbb{F}_2$, or simply an elementary abelian group of order 2^m. The differential and the linear properties of a function F are only related to the additive structure of $\mathbb{F}_{2^m}$ and have nothing to do with the multiplicative group. However, in order to construct functions with good linear and differential properties, we will use the multiplication in $\mathbb{F}_{2^m}$. For a description of the differential and linear properties of functions F, it is enough to consider F to be a mapping between two abelian groups, no matter whether these are the additive groups of finite fields or not.

The paper is organized as follows. In the next Section, we describe the notion of AB and APN and crooked mappings. In Section 3, we discuss the problem to determine the equivalence classes of functions. In the final Section, we apply the results of Section 3 to show that our new APN function is inequivalent to the known ones. We conclude the paper with some interesting open problems and related questions.

2 Nonlinear functions

Let U and V be arbitrary groups. If $F : U \to V$ is a function, then we define the **graph** G_F of F as follows:

$$G_F := \{(x, F(x)) \ : \ x \in U\} \subseteq U \times V.$$

We define

$$\delta_F(a,b) := |\{(x-y, F(x)-F(y)) = (a,b) \ : \ x,y \in U\}|.$$

Note that $\delta_F(a,b)$ is the number of solutions (x,y) to the equations

$$(1) \qquad x - y = a, \qquad F(x) - F(y) = b$$

or the number of solutions

$$F(y+a) - F(y) = b.$$

If F is linear (hence U and V are the additive groups of vector spaces) then

$$\delta_F(a,b) \in \{0, |U|\}.$$

A function F is **differentially highly nonlinear** if

$$\mathcal{D}(F) := \max_{a \in U, b \in V, (a,b) \neq (0,0)} \delta_F(a,b)$$

is small.

We are now going to describe the differential properties of F in terms of group algebras. Let G be an arbitrary multiplicatively written group, and let $\mathbb{K}[G]$ denote the group algebra of G over the field $\mathbb{K}$. The group algebra consists of the formal sums

$$\sum_{g\in G} a_g g,$$

where $a_g \in \mathbb{K}$. We can define an addition

$$\left(\sum_{g\in G} a_g g\right) + \left(\sum_{g\in G} b_g g\right) = \sum_{g\in G} (a_g + b_g) g$$

and a multiplication

$$\left(\sum_{g\in G} a_g g\right) \cdot \left(\sum_{g\in G} b_g g\right) = \sum_{g\in G} \sum_{h\in G} (a_h \cdot b_{h^{-1}g}) g$$

In order to distinguish the addition in $\mathbb{K}[G]$ from the composition of elements in G, we prefer to write the group multiplicatively if we use group algebra notation. However, the groups that we are really using are always additively written.

If $D \subseteq G$, we identify D with the element $\sum_{g\in D} g$, which we denote, by abuse of notation, D again. Moreover, if $A = \sum_{g\in G} a_g g$, then $A^{(-1)} := \sum_{g\in G} a_g g^{-1}$. Using this notation, we obtain easily the equation

$$G_F G_F^{(-1)} = \sum_{(a,b)\in U\times V} \delta_F(a,b)(a,b).$$

This shows that the $\delta_F(a,b)$'s are the coefficients of the elements in $G_F G_F^{(-1)}$. The set (or multiset if we also count multiplicities)

$$\{\delta_F(a,b) \;:\; (a,b) \in U \times V\}$$

is called the differential spectrum of F.

Characters are an important concept in the theory of group algebras. We restrict ourselves to abelian groups, otherwise we have to replace characters by higher dimensional representations. Characters are precisely the one-dimensional representations of a group G.

A **character** is a homomorphism $G \to \mathbb{C}^*$. In the abelian case, there are $|G|$ characters which form a group $\hat{G}$ which is isomorphic with G. The transformation

$$\mathbb{C}[G] \to \mathbb{C}^{|G|}, \quad \sum a_g g \to (\sum a_g \chi(g))_{\chi\in\hat{G}}$$

is called the **discrete Fourier transform**. The character that maps every group element to 1 is denoted χ_0.

We look at the case of functions $F : U \to V$ and the elements $G_F \in \mathbb{C}[U \times V]$. If F is linear or affine linear, then G_F is a coset of a subgroup of $U \times V$, and then

$$\chi(G_F) \in \{0, \pm|U|\}.$$

This follows from the well known orthogonality relations for characters. Therefore, it is natural to call a mapping **highly nonlinear** if

$$\mathcal{LN}(F) := \max_{\chi\in\widehat{U\times V}, \chi\neq\chi_0} |\chi(G_F)|$$

is small. The set (or multiset) of character values

$$\{\chi(G_F) \;:\; \chi \in \widehat{U \times V}\}$$

is called the Fourier spectrum of F. We may define the Fourier and the differential spectrum also for arbitrary sets $A \subseteq G$ or arbitrary group algebra elements $A \in \mathbb{C}[G]$.

Now let us look at the special case of elementary abelian 2-groups U and V. We return to the general case of abelian groups in the next section, since, in our opinion, the term "equivalence of functions" is best explained in this more general context.

If U and V are elementary abelian 2-groups, then $\delta_F(a,b)$ is always even hence we have

$$\mathcal{D}(F) \geq 2: \tag{2}$$

The numbers $\delta_F(a,b)$ are even since the two equations (1) have always an even number of solutions, you may just change x and y. We say that a function is **almost perfect nonlinear (APN)** if $|U| = |V|$ and we have equality in (2).

Similarly, one can show

$$\mathcal{LN}(F) \geq 2^{|U|/2}. \tag{3}$$

This can be proved easily using some well known properties of the discrete Fourier transform. If $|U| = |V| = 2^m$, we have the improvement

$$\mathcal{LN}(F) \geq 2^{(m+1)/2}, \tag{4}$$

see [14]. Functions which satisfy (4) with equality are called **almost bent (AB)**, whereas functions which satisfy (3) are called bent. Sometimes the term bent is reserved just for the case of functions with $|V| = 2$. It is well known that AB functions (which can exist only in the case m odd) are APN.

The development of the concept of nonlinearity does not make use of finite fields. However, in order to construct examples of APN and AB functions it is useful to equip U and V with the structure of a finite field. In this case, we can describe our mappings by polynomials. The degree of this polynomial will play an important role in the next section.

The best studied functions are the power mappings x^d. So far, all known constructions of APN and AB functions are related to power mappings. It has been checked at least up to $m = 15$ (see [5]) that the following table gives a complete list of power APN mappings on $\mathbb{F}_{2^m}$:

Table 1
Known APN power functions on $\mathbb{F}_{2^m}$.

	Exponents d	Conditions	Reference
Gold functions	$2^i + 1$	$gcd(i,m) = 1,\ 1 \leq i \leq \frac{m-1}{2}$	[9],[14]
Kasami functions	$2^{2i} - 2^i + 1$	$gcd(i,m) = 1,\ 1 \leq i \leq \frac{m-1}{2}$	[11],[10]
Welch function	$2^t + 3$	$m = 2t + 1$	[7]
Niho function	$2^t + 2^{\frac{t}{2}} - 1$, t even $2^t + 2^{\frac{3t+1}{2}} - 1$, t odd	$m = 2t + 1$	[6]
Inverse function	$2^{2t} - 1$	$m = 2t + 1$	[14],[1]
Dobbertin function	$2^{4i} + 2^{3i} + 2^{2i} + 2^i - 1$	$m = 5i$	[8]

It turns out that, in the odd dimension case, the Gold, Kasami, Welch and Niho functions are AB. The condition $i \leq \frac{m-1}{2}$ in the Gold and Kasami case is not really restrictive: It just means that the functions with $i > \frac{m-1}{2}$ are affine equivalent to those with $i \leq \frac{m-1}{2}$. For a thorough discussion of the notion of equivalence, we refer the reader to Section 3.

If a function is APN and bijective, then the inverse is also APN. The inverse functions are not included in the table above.

3 Equivalence of functions

Let $D = \sum_{g \in G} a_g g$ be an arbitrary element in the group algebra $\mathbb{C}[G]$, and let $\mathcal{L}$ be an automorphism of G. We define

$$\mathcal{L}(D) := \sum a_g \mathcal{L}(g).$$

Obviously, the differential spectra of D and $\mathcal{L}(D)$ are the same, and also the Fourier spectra of D and $\mathcal{L}(D)$ are the same. For the statement about the Fourier spectrum note that the mapping

$$\chi' : g \mapsto \chi(\mathcal{L}(g))$$

is a character if χ is a character. More generally, for $g \in G$, the elements Dg and $\mathcal{L}D$ have the same differential and Fourier spectra.

Therefore it is natural to call two group algebra elements D_1 and D_2 equivalent if there is an automorphism $\mathcal{L}$ of G and a group element $g \in G$ such that $\mathcal{L}(D_1) = D_2 g$.

Now we want to specialize this concept of equivalence to functions. This has been first done in [4], Proposition 3, therefore we will call the notion of equivalence of functions that stems from the notion of equivalence of group algebra elements **CCZ equivalence**.

$F : U \to V$ and the corresponding group algebra elements G_F. The problem is that $\mathcal{L}(G_F)$ is not necessarily a group algebra element that correponds to a function $F' : U \to V$.

We call two functions $F_1 : U \to V$ and $F_2 : U \to V$ **CCZ equivalent** if there is an automorphism $\mathcal{L}$ of $U \times V$ such that $\mathcal{L}(G_{F_1}) = G_{F_2} \cdot g$ for some element $g \in U \times V$. This generalizes the concept of affine equivalence. The original definition of affine equivalence is as follows:

Let U and V be elementary abelian groups of order 2^m, i.e. the additive groups of verctor spaces over $\mathbb{F}_2$. We say that $F_i : U \to V$, $i = 1, 2$ are affine equivalent if there are linear mappings $\mathcal{L}_1$ and $\mathcal{L}_2$ on $\mathbb{F}_{2^m}$ and elements $a \in U$, $b \in V$ auch that

$$F_2(x) = \mathcal{L}_2(F_1(\mathcal{L}_1(x + a))) + b.$$

Proposition 1 *Two functions F_1 and F_2 are affine equivalent if and only if they are CCZ equivalent via an automorphism $\mathcal{L}$ of $U \times V$ such that $\mathcal{L}(V) = V$.*

Given two functions F_1 and F_2 it is sometimes easy to decide whether they are affine equivalent. It turns out that the algebraic degree of a function F is an affine invariant (we refer the reader to [4] for the precise definition of algebraic degree; it is the largest 2-weight of the exponents that occur in the polynomial representation of F). But it seems that the important question whether affinely inequivalent functions are CCZ equivalent has not been investigated. In [2], several classes of functions are constructed which are CCZ equivalent to the Gold power mapping but not affinely equivalent to any power mapping. This shows that CCZ equivalence is really a coarser equivalence relation than affine equivalence. As far as we know there is no proof that none of the APN mappings described in Table 1 are CCZ equivalent.

If m is odd, it is known that the Fourier spectra of the inverse function and the Dobbertin function are different, hence these two functions are not CCZ equivalent. Moreover, there spectrum has more than three values. However, the Gold, Kasami, Welch and Niho functions all have the same 3-valued Fourier spectrum, hence they can be distinguished from the inverse and the Dobbertin function, but they cannot be distinguished between themselves using the Fourier spectrum.

In the case m even, the Fourier spectrum of the Gold and Kasami power functions are equal. It is always different from the spectrum of the Dobbertin function, see [3]. It turns out that our new function has the same spectrum as Gold and Kasami. Therefore, in order to decide whether APN functions are CCZ equivalent or not, we have to find other invariants than just the Fourier spectrum.

If $F : U \to V$ is an APN mapping (i.e. U and V are elementary abelian groups of order 2^m), we define

$$A_F := \frac{G_F^2 - 2^m}{2} \in \mathbb{C}[G].$$

We have $(a, b) \in A_F$ if and only if $F(x + a) + F(x) = b$ has two solutions in x. If F_1 and F_2 are CCZ equivalent, then A_{F_1} and A_{F_2} are obviously equivalent. Now we view A_F as an element in $\mathbb{F}_2[U \times V]$. If F_1 and F_2 are CCZ equivalent, then A_{F_1} and A_{F_2} are also equivalent in $\mathbb{F}_2[U \times V]$. Hence the dimension of the ideal generated by A_F is invariant under CCZ equivalence.

We note that the ideal generated by A_F may be also viewed as the $\mathbb{F}_{2^m}$ span of the following matrix $\mathbf{A}$ of size $2^{2m} \times 2^{2m}$: We index the rows and columns with elements from $U \times V$. We have

$$\mathbf{A}_{(a,b),(u,v)} = \begin{cases} 1 & \text{if } (a+u, b+v) \in A_F \\ 0 & \text{otherwise.} \end{cases}$$

4 The new APN function

Theorem 2 *Let ω be an element of order 3 in $\mathbb{F}_{2^{10}}$. Let $\mathbb{F}_{2^5}$ denote the subfield of order 32 in $\mathbb{F}_{2^{10}}$. The mapping*

$$(5) \qquad \begin{array}{rccc} F: & \mathbb{F}_{2^{10}} & \to & \mathbb{F}_{2^{10}} \\ & x & \mapsto & x^3 + u \cdot x^{36} \end{array}$$

is an APN mapping if and only if

$$(6) \qquad u \in \{\omega \mathbb{F}_{2^5}^*\} \cup \{\omega^2 \mathbb{F}_{2^5}^*\}$$

This function is not CCZ equivalent to any power mapping.

It is possible to give a "theoretical" argument why these functions have the APN property. Since this argument is quite involved, and since it does not really give insight why the function is APN, we skip it. The APN property of the function can be easily checked by computer. One can easily show that the 62 examples in (5) are affine equivalent: In (5), replace x by ax and then divide the resulting equation by a^3 to obtain

$$x \mapsto x^3 + \frac{ua^{36}}{a^3} x^{36} = x^3 + ua^{33} x^{36}.$$

But ua^{33} satisfies (6) if and only u satisfies this condition (note $2^{10} - 1 = 3 \cdot 11 \cdot 31$).

The function has the interesting property to be crooked. This means that the sets

$$H_a := \{F(x + a) + F(x) \ : \ x \in \mathbb{F}_{2^{10}}\}$$

are affine hyperplanes in $\mathbb{F}_2^{10}$. We refer the reader to [13, 12] for recent progress on the problem to classify crooked mappings.

We want to distinguish our mapping from the known APN's. Table 1 shows that the only known APN mappings on $\mathbb{F}_{2^{10}}$ are (up to affine equivalence)

$$x^3, x^9 \text{ Gold }, x^{57} \text{ Kasami }, x^{339} \text{ Dobbertin }.$$

As mentioned above, the Fourier spectrum of our new function is different from the Fourier spectrum of the Dobbertin function. This shows that our function is inequivalent to x^{339}.

The function F is quadratic, therefore one may suspect that our function is affine or CCZ equivalent to one of the Gold power mappings. Since the Fourier spectrum of our function is the same as those of the Kasami and Gold function, we cannot use it to distinguish the functions.

We computed the dimensions of the ideals I_F generated by A_F for the Gold power functions x^3 and x^9 as well as the Kasami power mapping x^{57}. The following table summarizes our results:

Table 2
Dimensions of the ideals I_F in $\mathbb{F}_2[\mathbb{F}_2^{10} \times \mathbb{F}_2^{10}]$

F	dimension
x^3	1804
x^9	1804
x^{57}	5734
Theorem 2	1896

This shows that our function is new. We can show that the power mappings x^3 and x^9 on $\mathbb{F}_{2^{10}}$ are not affine equivalent, but according to Table 2, the dimensions of the corresponding ideals are the same. This shows that the dimension can not always be used as a criteria to distinguish mappings.

It has been checked (by computer) that in finite fields of order $\mathbb{F}_{2^m}$, $m \leq 15$, there are no more power APN mappings besides those listed in Table 1. Therefore, our function is not CCZ equivalent to any power mapping. It was known before (see [2]) that there are functions which are not affine equivalent to any power mapping. Our example gives the first APN mapping which is not CCZ equivalent to any power mapping.

We can also use another argument if we want to show just affine inequivalence to power mappings different from the Gold case: Our function is crooked, and it is known that the only crooked power mappings are quadratic, see [13]. Hence the only chance to be affine equivalent is equivalence to the Gold power mapping, since affine equivalence preserves the property being crooked. This property is not preserved by CCZ equivalence!

The example in Theorem 2 has been found through a computer search for APN binomials $x^{d_1} + ux^{d_2}$ on $\mathbb{F}_{2^n}$. The search was complete in the range $n \leq 10$. Up to affine equivalence, the example in Theorem 2 is the only new APN binomial. We also found an example in $\mathbb{F}_{2^{12}}$ where we can show that the function is not affine equivalent to the Gold power mappings.

Theorem 3 *The mapping*

$$\begin{array}{rccc} F' : & \mathbb{F}_{2^{12}} & \rightarrow & \mathbb{F}_{2^{12}} \\ & x & \mapsto & x^3 + u \cdot x^{528} \end{array}$$

is an APN mapping if and only if

$$\begin{array}{rcl} u & \in & \{x \in \mathbb{F}_{2^{12}} : \textit{order of } x \textit{ is divisible by } 45 \textit{ and divides } 45 \cdot 13\} \\ & & \cup \{x \in \mathbb{F}_{2^{12}} : \textit{order of } x \textit{ is divisible by 7 and divides } 3 \cdot 7 \cdot 13\}. \end{array}$$

The proof that the functions are not affine equivalent to the Gold power mappings is rather involved and therefore omitted. We did not yet check the dimension of the ideal generated by $A_{F'}$ since the ambient space is too large (it has dimension 2^{24}). We also found some more examples of binomials in larger fields where we are not yet able to prove that they are affine inequivalent to the known APN functions.

5 Summary and open problems

In this paper, we reported about two new examples of APN functions in $\mathbb{F}_{2^{10}}$ and $\mathbb{F}_{2^{12}}$. Both examples are quadratic, which implies that the functions are crooked. In both cases, the new functions are not affine equivalent to any power mapping, and in one case we know that the example is not CCZ equivalent to the Gold power mappings. Using computer assistance, we computed the dimensions of the ideals generated by A_F for different functions F. These dimensions showed that the function on $\mathbb{F}_{2^{10}}$ is different from all previously known APN mappings. Since all APN power mappings on $\mathbb{F}_{2^{10}}$ are known, our function is not CCZ equivalent to any power mapping.

We want to finish with the following open problems:

- Show that the function in Theorem 3 is not CCZ equivalent to any of the known functions.
- Try to generalize the examples. Perhaps, one can also use sums of more than just two Gold power mappings.
- Give a theoretical proof that our new functions are not CCZ equivalent to the known ones.
- Compute the ranks of the ideals generated by A_F or D_F for the known classes of APN or AB mappings.
- Show that the known APN or AB functions are not CCZ equivalent.
- Find more invariants for CCZ equivalence.

Acknowledgment

We thank Jürgen Bierbrauer for many helpful discussions. He actually initiated our search for new APN mappings.

Note

After finishing this paper and making it available as a preprint, a new infinite series of APN functions has been constructed (L. Budaghyan, C. Carlet, P. Felke and G. Leander: An infinite class of quadratic APN functions which are not equivalent to power mappings, **http//eprint.iacr.org/2005/359**). The series covers some of the examples presented here.

References

[1] Thomas Beth and Cunsheng Ding. On almost perfect nonlinear permutations. In *Advances in Cryptography. EUROCRYPT'93*, volume 765 of *Lecture Notes in Computer Science*, pages 65–76, New York, 1994. Springer-Verlag.

[2] Lilya Budaghyan, Claude Carlet, and Alexander Pott. New constructions of almost bent and almost perfect nonlinear polynomials. In Pascale Charpin and Øyvind Ytrehus, editors, *Abstract Book of the International Workshop on Coding and Cryptography, Bergen (Norway)*, pages 306–315, 2005.

[3] Anne Canteaut, Pascale Charpin, and Hans Dobbertin. Weight divisibility of cyclic codes, highly nonlinear functions on $\mathbf{F}_{2^m}$, and crosscorrelation of maximum-length sequences. *SIAM J. Discrete Math.*, 13(1):105–138 (electronic), 2000.

[4] Claude Carlet, Pascale Charpin, and Victor Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Des. Codes Cryptogr.*, 15(2):125–156, 1998.

[5] Hans Dobbertin. One-to-one highly nonlinear power functions on GF(2^n). *Appl. Algebra Eng. Commun. Comput.*, 9(2):139–152, 1998.

[6] Hans Dobbertin. Almost perfect nonlinear power functions on GF(2^n): the Niho case. *Inform. and Comput.*, 151(1-2):57–72, 1999.

[7] Hans Dobbertin. Almost perfect nonlinear power functions on GF(2^n): the Welch case. *IEEE Trans. Inform. Theory*, 45(4):1271–1275, 1999.

[8] Hans Dobbertin. Almost perfect nonlinear power functions on GF(2^n): a new case for n divisible by 5. In *Finite fields and applications (Augsburg, 1999)*, pages 113–121. Springer, Berlin, 2001.

[9] R. Gold. Maximal recursive sequences with 3-valued recursive cross-correlation function. *IEEE Trans. Inf. Th.*, 14:154–156, 1968.

[10] H. Janwa and R. M. Wilson. Hyperplane sections of Fermat varieties in $\mathbf{P}^3$ in char. 2 and some applications to cyclic codes. In *Applied algebra, algebraic algorithms and error-correcting codes (San Juan, PR, 1993)*, volume 673 of *Lecture Notes in Comput. Sci.*, pages 180–194. Springer, Berlin, 1993.

[11] T. Kasami. The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes. *Information and Control*, 18:369–394, 1971.

[12] Gohar M. Kyureghyan. The only crooked power mappings are $x^{2^k+2^l}$. submitted, 2004.

[13] Gohar M. Kyureghyan. Differentially affine maps. In Pascale Charpin and Øyvind Ytrehus, editors, *Abstract Book of the International Workshop on Coding and Cryptography, Bergen (Norway)*, pages 296–305, 2005.

[14] Kaisa Nyberg. Differentially uniform mappings for cryptography. In *Advances in Cryptography. EUROCRYPT'93*, volume 765 of *Lecture Notes in Computer Science*, pages 55–64, New York, 1994. Springer-Verlag.